

(19) **United States**

(12) **Patent Application Publication**
SMITH et al.

(10) **Pub. No.: US 2019/0132350 A1**

(43) **Pub. Date: May 2, 2019**

(54) **SYSTEM AND METHOD FOR VALIDATION
OF DISTRIBUTED DATA STORAGE
SYSTEMS**

H04L 9/06 (2006.01)

H04L 12/24 (2006.01)

(52) **U.S. Cl.**

CPC **H04L 63/1433** (2013.01); **G06F 17/30371**
(2013.01); **G06F 9/54** (2013.01); **H04L 41/22**
(2013.01); **H04L 2209/38** (2013.01); **H04L**
9/0637 (2013.01)

(71) Applicant: **PricewaterhouseCoopers LLP,**
New York, NY (US)

(72) Inventors: **Alfred Michael SMITH,** Madison, NJ
(US); **Muhammad Emad KHAN,** New
York, NY (US)

(21) Appl. No.: **16/175,715**

(22) Filed: **Oct. 30, 2018**

Related U.S. Application Data

(60) Provisional application No. 62/579,093, filed on Oct.
30, 2017, provisional application No. 62/579,095,
filed on Oct. 30, 2017.

Publication Classification

(51) **Int. Cl.**

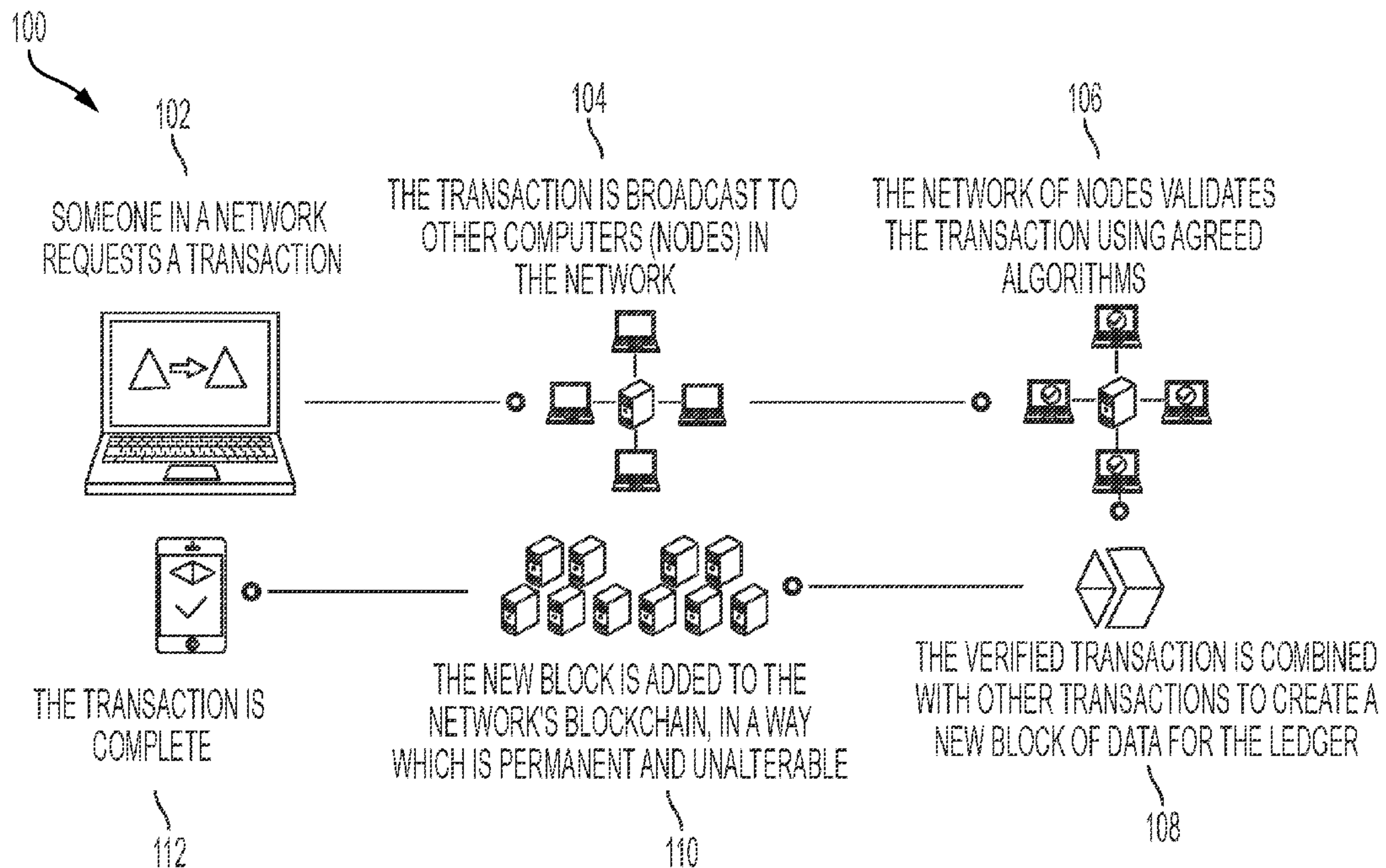
H04L 29/06 (2006.01)

G06F 17/30 (2006.01)

(57)

ABSTRACT

Provided herein is a risk framework tool for a distributed ledger-based computing system (i.e., blockchain) that can present a common risk framework to a user that can then allow for the user to determine what risks are important for it to manage. The risk framework can then take those specified risks and convert them in to a plurality of tests that can be used to validate the organization's blockchain system. In one or more examples, the risk framework can provide a graphical user interface to user that allows them specify the risks they wish to manage within the blockchain computing system, and based on the user's inputs, can determine one or more continuous real-time validation tests to be performed on the blockchain computing system so as to characterize the risk specified by user using the risk framework.



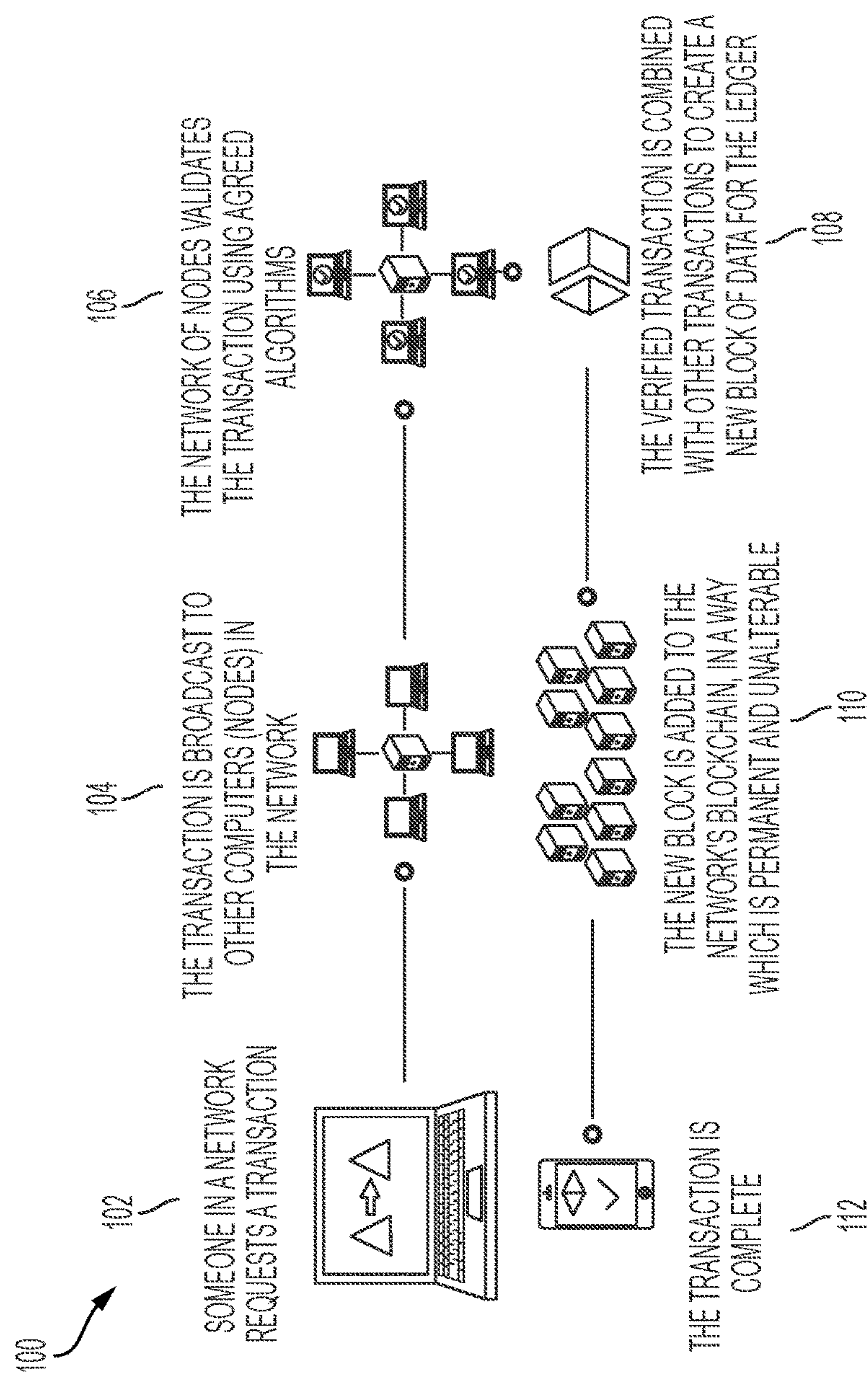


FIG. 1

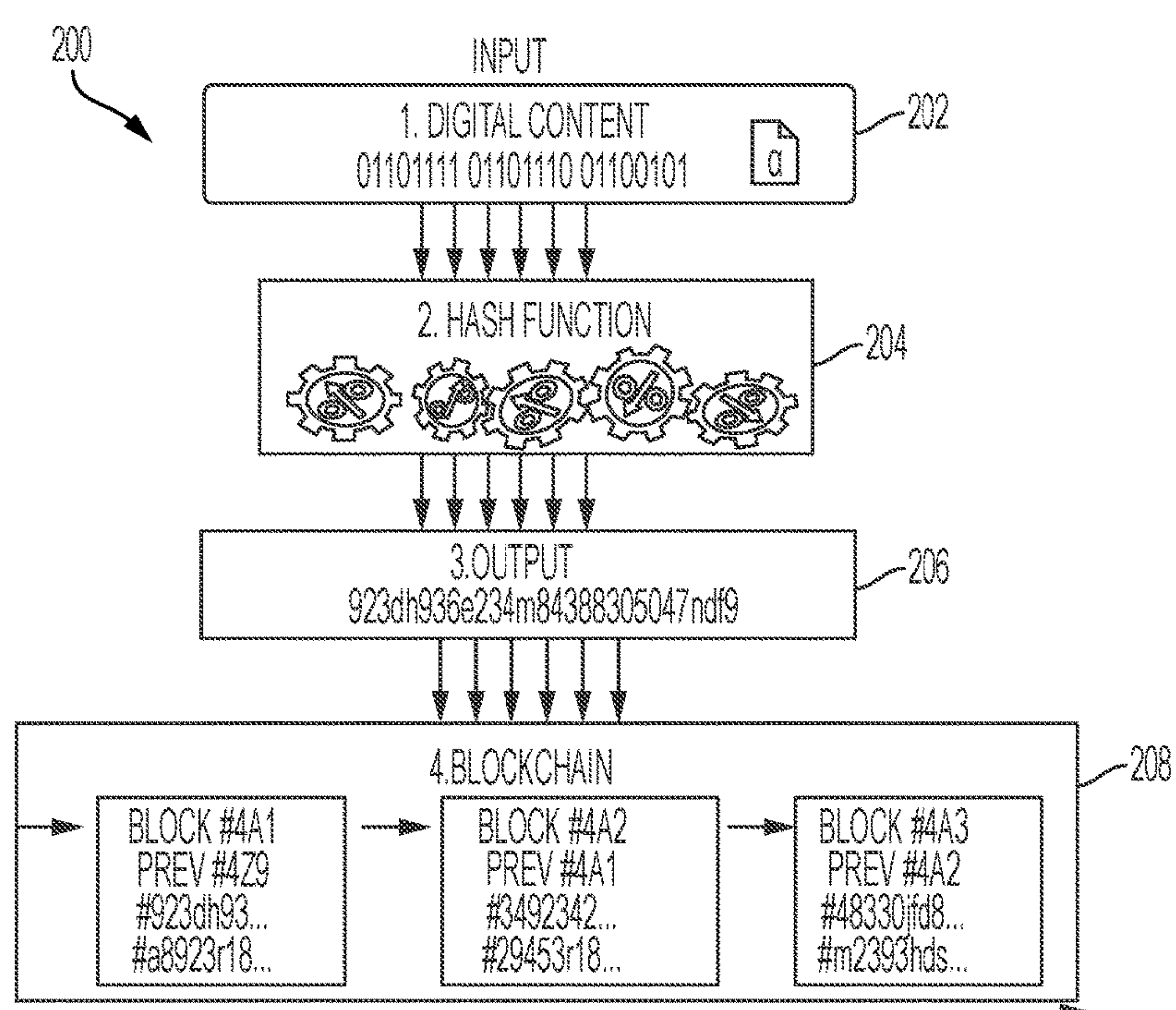


FIG. 2

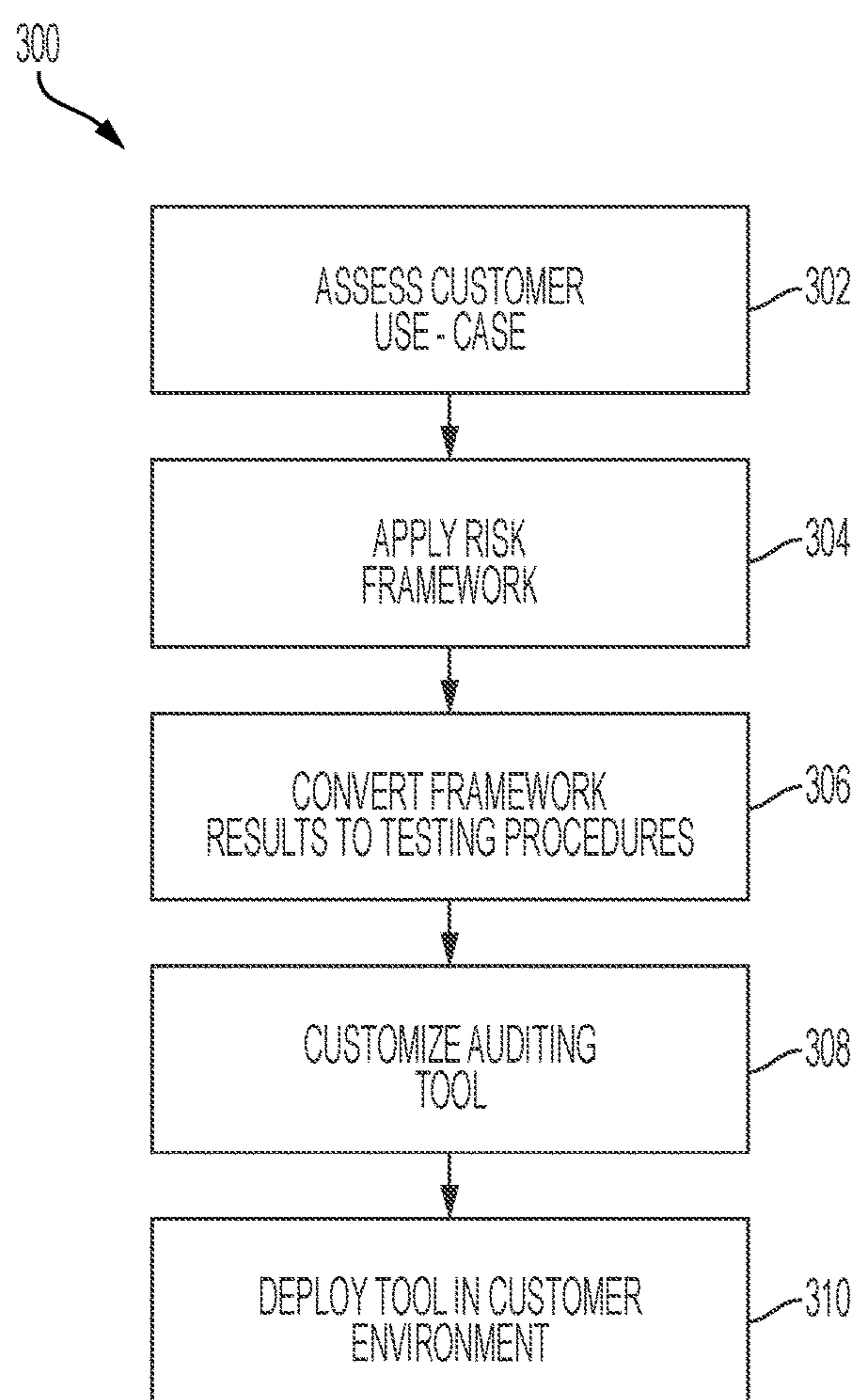


FIG. 3

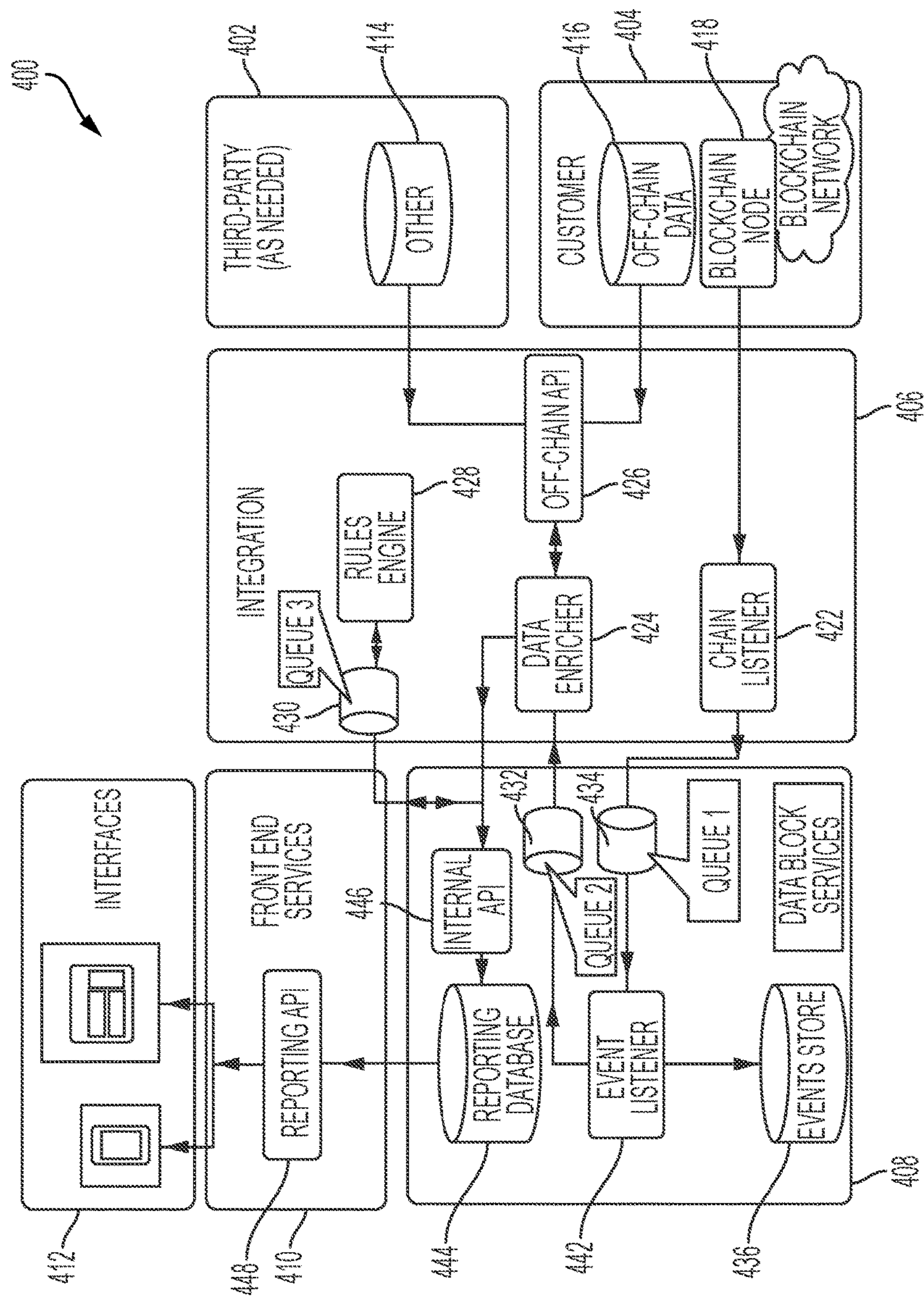


FIG. 4

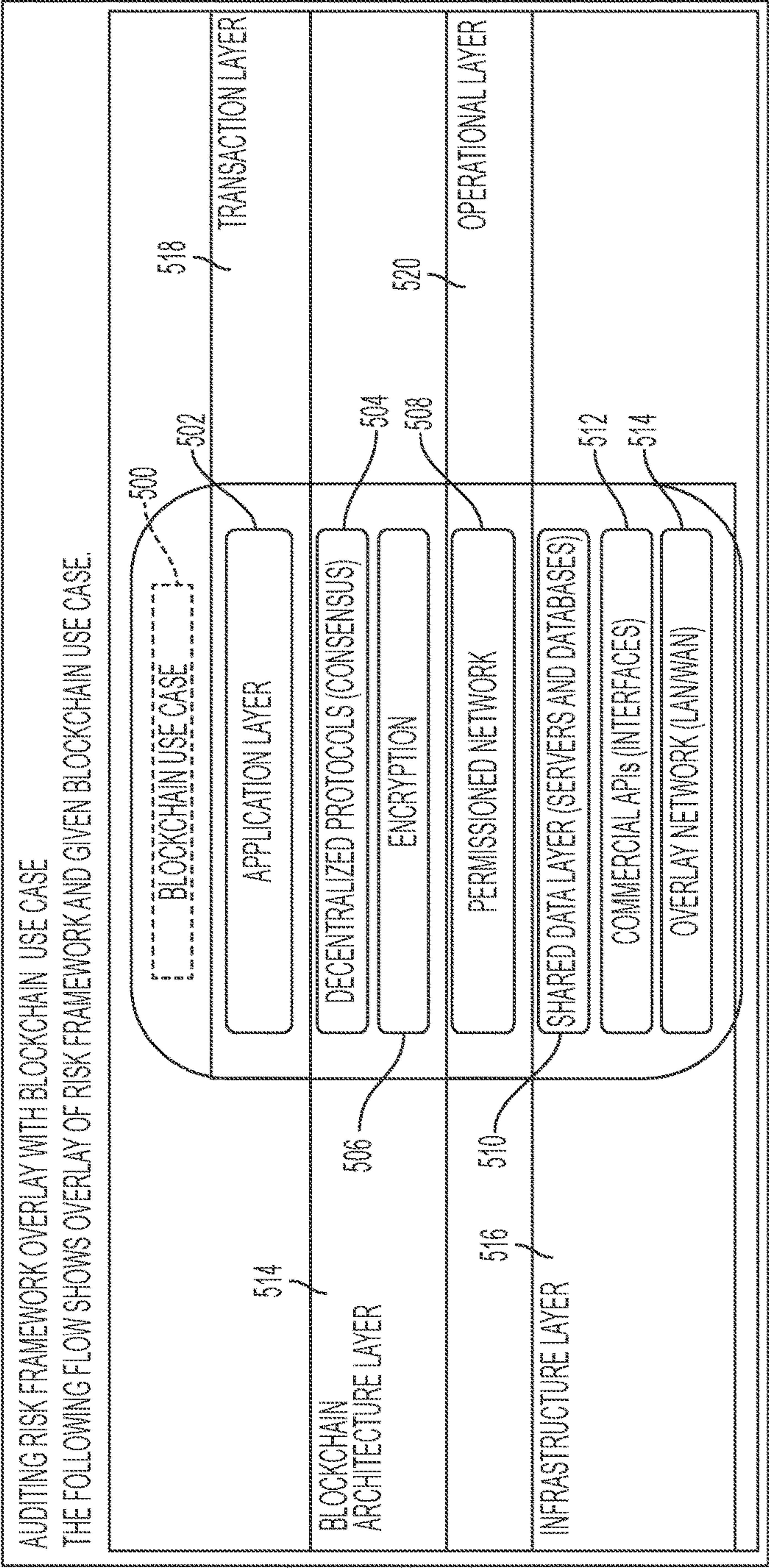


FIG. 5A

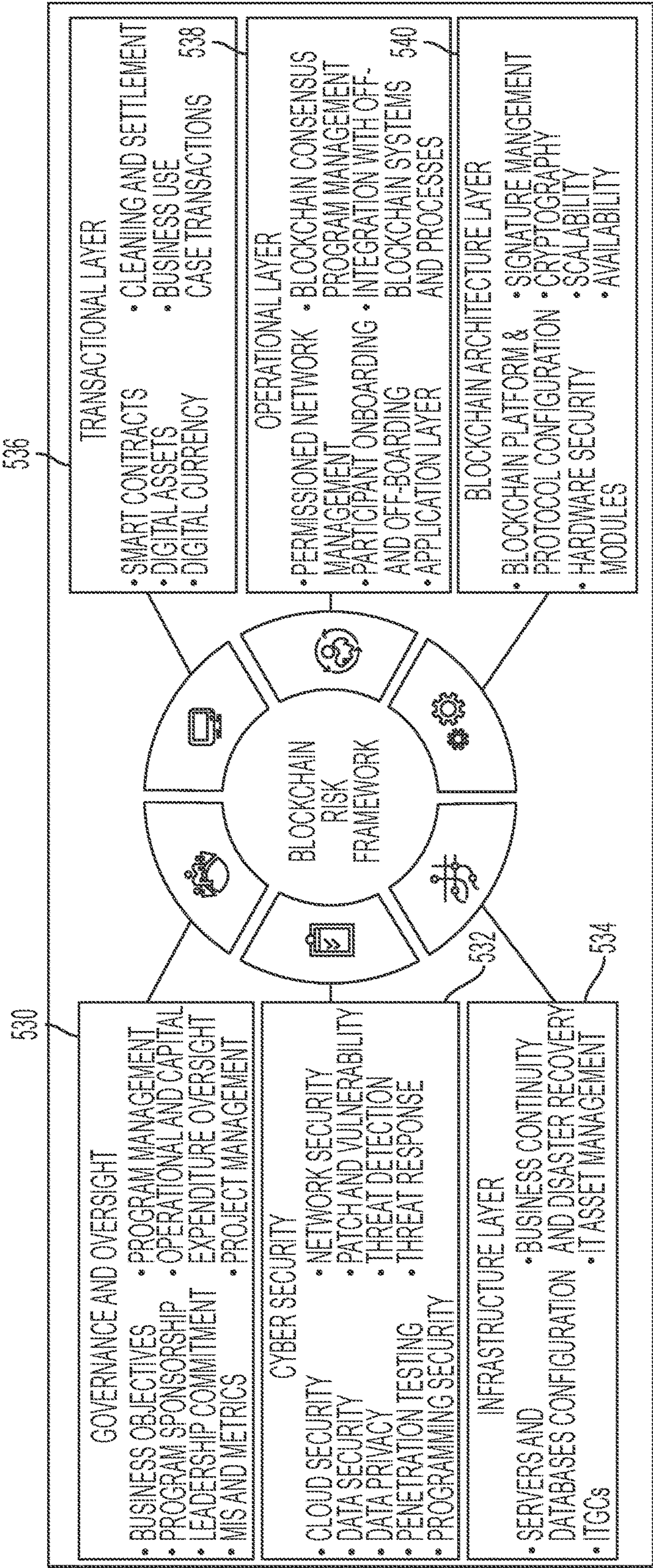


FIG. 5B

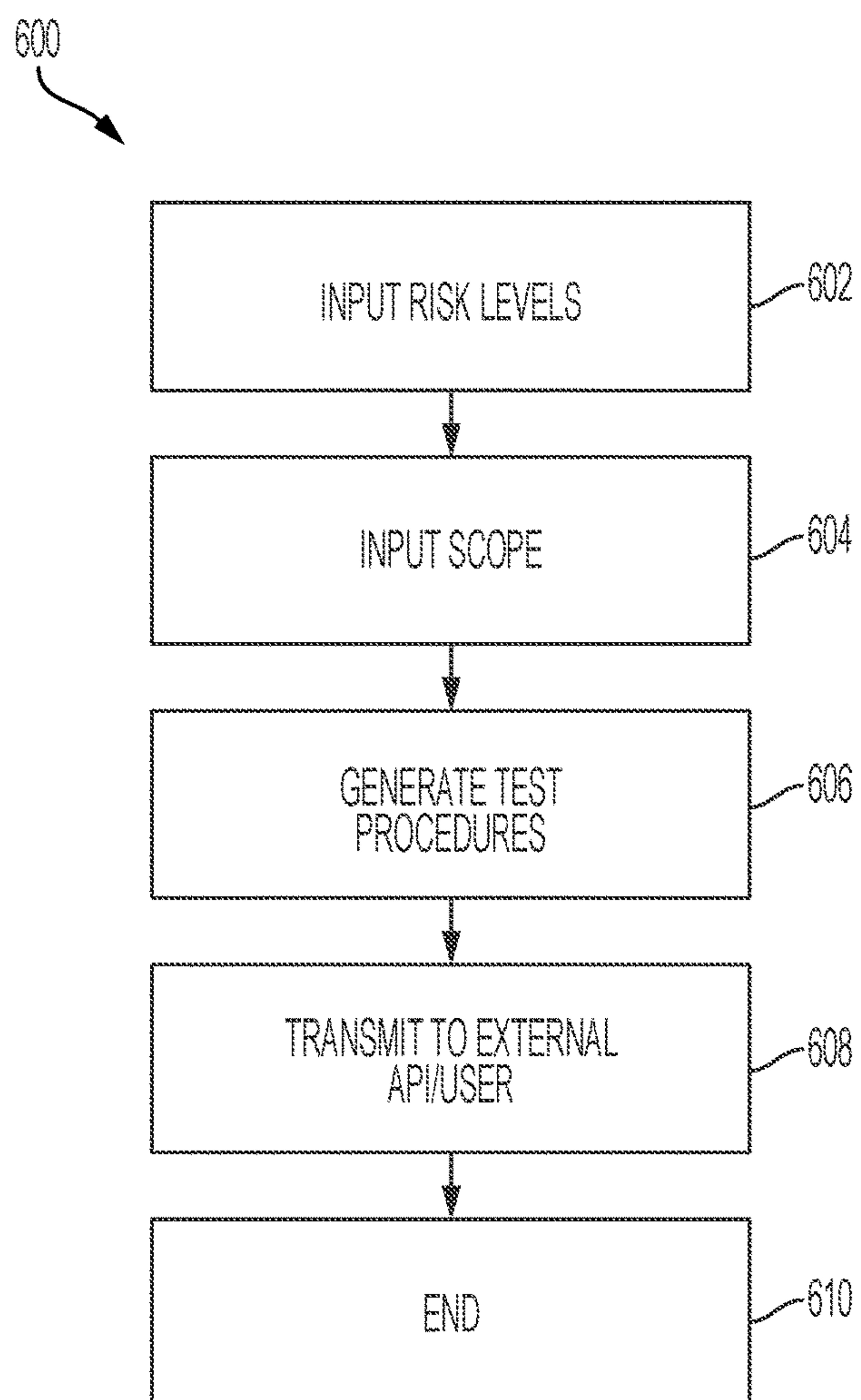


FIG. 6

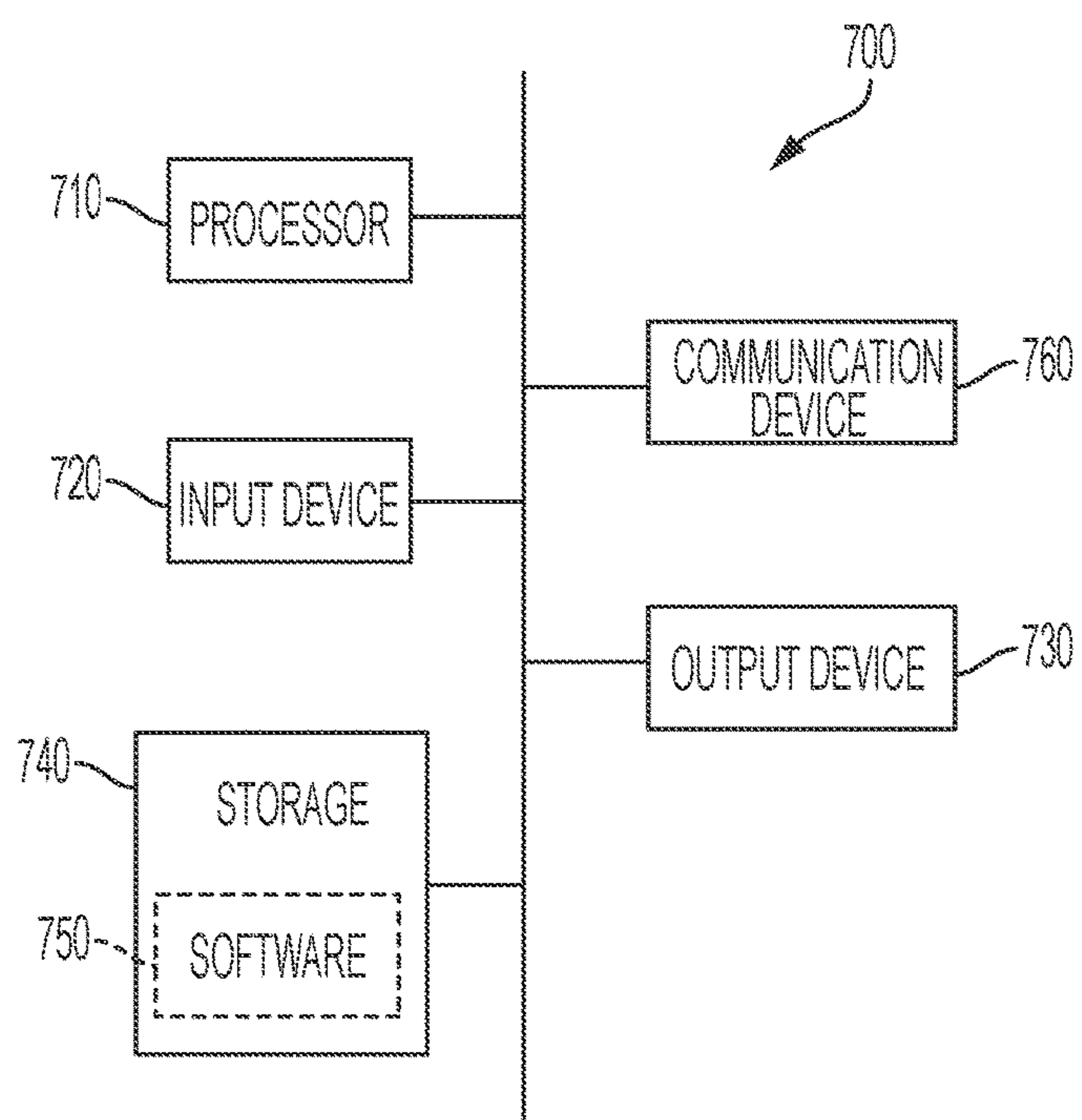


FIG. 7

SYSTEM AND METHOD FOR VALIDATION OF DISTRIBUTED DATA STORAGE SYSTEMS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application which claims the benefit of U.S. Provisional Patent Application Ser. No. 62/579,093, filed Oct. 30, 2017, and U.S. Provisional Patent Application Ser. No. 62/579,095, filed Oct. 30, 2017, each of which are incorporated herein by reference in their entirety and for all purposes.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates generally to validation of distributed data storage systems, such as, for example, blockchain-based data storage systems.

BACKGROUND OF THE DISCLOSURE

[0003] A distributed data storage (which may be referred to as a distributed database) system may include data storage devices that are not connected to a common processing unit, but are in different computing systems located at the same physical location or dispersed across one or more networks of interconnected computing systems at different physical locations. The data storage devices may communicate with each other via one or more wired or wireless communication networks. Typically, each of the data storage devices includes a copy of the stored data. Storing copies of the data in different data storage devices may eliminate a single point-of-failure and may induce both higher availability and increased reliability of the stored data.

[0004] Blockchain technology may be used to implement a distributed data storage system. In the blockchain technology, a system of networked nodes, e.g., computers or servers, each store a copy of the entire distributed data storage system. The blockchain-based distributed data storage system is often referred to as a blockchain. Whenever a group of data records is to be added to the distributed database, i.e., blockchain, each node may independently verify the group of data records in a batch process known as generating a block (also referred to as a data block). In the batch process, a node verifies the group of data records based on its copy of the blockchain storing previously verified data records. A node that generates the block may transmit the generated block to every other node in the system. In current implementations, only after the block has been verified by each node in the system may each node add the block to its copy of the blockchain. As each of the nodes independently verifies the block, blockchain technology may reduce the risk of a single point-of-attack or a single point-of-failure. Further, since a copy of the blockchain is maintained at each node, the data can be stored in a redundant manner.

[0005] A blockchain is a record of data activities. These data activities can be transactions in a distributed ledger, and/or any movement of money, goods, and/or secured or unsecured data involved, for example, in a purchase at a supermarket, in the creation and storage of a user's digital identification, in the assignment of a government ID number, in energy data exchange in the energy industry, in an e-voting service, or in the recording, tracking, and transferring of deeds and contractual agreements.

[0006] FIG. 1 illustrates a blockchain process flow in accordance with examples of the disclosure. The blockchain process flow **100** can begin at step **102**, wherein a user/party can request to implement a transaction in the blockchain. Examples of transactions can be storing data such as a record to a distributed ledger. Once the request has been made at step **104**, the transaction can be broadcast to other computers (known as nodes) in the network. At step **106**, the network of nodes can then validate the transaction using a mutually a priori agreed upon algorithm. Once each node in the network of nodes validates the transaction, the process can move to step **108**, wherein the verified transaction can be combined with other transactions (described in detail below) to create a new block of data for the ledger. Once the verified transaction has been combined, the process can move to step **110** wherein the new block can be added to the network's block chain. The new block can be added in such a way as to make it permanent and unalterable (i.e., through the use of cryptography). Once the new block has been added the process can move to step **112** wherein the transaction is completed.

[0007] As shown in FIG. 1, a blockchain needs to do two things: gather and order data into blocks, and then chain them together securely using cryptography. A blockchain is a decentralized ledger of all transactions in a network. Using blockchain technology, participants in the network can confirm transactions without the need for a trusted third-party intermediary.

[0008] FIG. 2 illustrates the process of generating a data block in a blockchain in accordance with examples of the disclosure. In the process **200**, a piece of digital content (i.e., a new transaction represented in binary) can be received. Once received, the process can move to step **204** wherein a hash function is applied to the received transaction, so as to combine it with data from a pre-existing block in the blockchain. The output of the hash function can produce a fixed and smaller-in-length unique digital output. Hash algorithms can carefully designed to flow one-way making it impossible to determine the original digital content from the output once the hash algorithm is applied. Every new block in the blockchain may be linked with the hash function of the previous block to create a chain. At step **206**, once the has function has been applied, an output can be generated. The output of the hash function can be a part of the data that is used in the creation of blocks, and these blocks can then cryptographically chained together at step **208**. This process of creating blocks allows the blockchain system to prove that a file existed in a particular format at a given time without having to reveal the data in the file.

[0009] One of the benefits of blockchain is that every participant in the network has simultaneous access to a view of the information, thus allowing almost real-time data availability and transparency that can eliminate the need for reconciliation. Also, the integrity and security of the information on the blockchain are ensured with cryptographic functions that can prevent unwanted intrusion on the network from non-authenticated participants. In blockchain technology, verification can be achieved by participants confirming changes with one another, thus replacing the need for a third party to authorize transactions and providing a facility for peers in the network to validate updated information, thereby ensuring the validity and integrity of the data on the blockchain. Another benefit of blockchain includes the ability to run additional business logic; this

means that agreement on the expected behavior of financial instruments can be embedded in the blockchain, which can facilitate the ability to design and implement shared workflow and enhance automation. Also, the ability to issue a digital currency or a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units facilitates the ability to create and move assets without a trusted third party in the blockchain.

SUMMARY OF THE DISCLOSURE

[0010] Blockchain presents a challenge to the traditional validation (also referred to as audit) approach, given there's no practical way to use point-in-time forensic analysis—the standard validation tool. Attempting to conduct a point-in-time forensic retrospective analysis can be ineffective and wildly inefficient. The conventional approach to auditing can negate one of the benefits of implementing blockchain in the first place: the promise of increased administrative efficiency. Also, the traditional validation approach can require the entire blockchain hash function to be reversed to obtain transparency of the digital content without breaking the chain or sequential order of the blocks. Such approach could cause significant technical complexities, challenges, and inefficiencies in the validation of a blockchain-based data storage system.

[0011] Increases in the volume of data activities and rapidly evolving complex technologies are creating a critical need for business, technology, and compliance functions to be prepared, adaptive, and agile to emerging challenges. Due to the increase in data activities, current validation methodologies that are manual, sample-based, and point-in-time do not provide the needed level of confidence. Validation methodologies need to shift from a manual to an automated and continuous approach to address a significant increase in data activities and emerging, complex new technologies. Current audit methodologies cannot provide the necessary assurance in areas where a blockchain is used.

[0012] Accordingly, there is a need for systems and methods to replace the conventional validation approach with a real-time validating process to build confidence and assurance in the blockchain technology. The concept behind real-time validating is to inspect data activities closer and closer to the point of occurrence. Real-time validating eliminates the concept of sampling in the conventional validating process. The purpose of sampling is to perform backwards-looking assessments of segments of populations to draw conclusions about the rest of the population. The embodiments described herein provide blockchain assurance-related baselines that eliminate the need for sampling in blockchain validating.

[0013] The type of validation and auditing required for a given a distributed ledger-based system such as blockchain can be user specific. No two organizations may need the same validation regime to audit its blockchain system. Often times, various risks and concerns may be important in one context, but not as critical in others. Therefore, there is a need to specify the types of tests that will be used based on a specific user/organization's risk priorities. The present disclosure thus provides a common risk framework that can allow for a user to conveniently determine what risks are important for it to manage. The risk framework can then take those specified risks and convert them in to a plurality of tests that can be used to validate the organization's block-

chain system. The risk framework can thus be used to customize a software tool that can then be used to perform real-time validation of an organizations blockchain computing infrastructure and system.

[0014] In some embodiments, a validation tool/system for any given blockchain use case may include tools for monitoring and validating of data activities (also referred as transactions) in one or more data blocks of the blockchain, risk evaluation of the data activities, business and technical risk and reporting assessments, and software that enables transaction level assurance for operational processes running on any given blockchain use case. The continuous assurance, compliance, monitoring, and validating methodology may be a combination of services and software intended to provide transparency in meeting the assurance and compliance needs of stakeholders. In some embodiments, the continuous assurance, compliance, monitoring, and validating of blockchains may be based on an acceptance criteria. In some embodiments, the acceptance criteria may include evaluating the current state of a blockchain use case against different risk categories (e.g., six or more different risk categories) and across sub-categories (e.g., 100 or more different sub-categories) in order to address assurance and compliance needs of stakeholders. This evaluation may be performed by a risk evaluation system that is industry, use case and Blockchain platform agnostic.

[0015] In some embodiments, a method for validating a blockchain-based data storage system is provided. The method comprising: conducting a risk analysis of using the blockchain-based data storage system in a specified environment; generating a risk profile of one or more data activities in a data block of the blockchain-based data storage system based on the risk analysis of using the blockchain-based data storage system in the specified environment; determining a number of times a validity test is to be performed on the one or more data activities in the data block to achieve a predetermined level of assurance, wherein the validity test tests compliance of the one or more data activities with an operating protocol of the blockchain-based data storage system; performing the validity test on the one or more data activities; and generating one or more validity test reports based on output of the validity test.

[0016] In some embodiments of the method, further comprising: displaying a user interface for selecting one or more test parameters of the validity test for testing compliance of the one or more data activities with the operating protocol of the blockchain-based data storage system; receiving from a user using the user interface one or more selections of the one or more validity test parameters based on the risk profile; and configuring the validity test based on the selection of the one or more validity test parameters.

[0017] In some embodiments of the method, the conducting the risk analysis comprises determining one or more risk categories of one or more risks involved in using the blockchain-based data storage system in a specified environment

[0018] In some embodiments of the method, the validity test is selected based on the risk categories.

[0019] In some embodiments of the method, the one or more risk categories are selected from a group consisting of government and oversight, cyber security, infrastructure layer, architecture layer, operational layer, and transaction layer.

[0020] In some embodiments of the method, the one or more data activities comprise storing one or more data in the data block.

[0021] In some embodiments of the method, the performing the validity test comprises performing the validity test continuously on the stored one or more data.

[0022] In some embodiments of the method, the generating the one or more validity test reports comprises: receiving from the user using the user interface a selection of one or more time periods within the one or more validity test; analyzing the output of the validity test during the one or more time periods; and generating the one or more validity test reports at end of each of the one or more time periods.

[0023] In some embodiments of the method, the performing the validity test comprises displaying, using the user interface, the output of the validity test; and wherein, in response to the output indicating that the one or more data activities failed the validity test, receiving from the user using the user interface a selection of whether the one or more data activities are exceptions to the operating protocol of the blockchain-based data storage system.

[0024] In some embodiments, a system comprising one or more processors and a memory comprising one or more programs, which when executed by the one or more processors, cause the one or more processors to: conduct a risk analysis of using the blockchain-based data storage system in a specified environment; generate a risk profile of one or more data activities in a data block of the blockchain-based data storage system based on the risk analysis of using the blockchain-based data storage system in the specified environment; determine a number of times a validity test is to be performed on the one or more data activities in the data block to achieve a predetermined level of assurance, wherein the validity test tests compliance of the one or more data activities with an operating protocol of the blockchain-based data storage system; perform the validity test on the one or more data activities; and generate one or more validity test reports based on output of the validity test.

[0025] In some embodiments of the system, the one or more processors are further caused to: display a user interface for selecting one or more test parameters of the validity test for testing compliance of the one or more data activities with the operating protocol of the blockchain-based data storage system; receive from a user using the user interface one or more selections of the one or more validity test parameters based on the risk profile; and configure the validity test based on the selection of the one or more validity test parameters.

[0026] In some embodiments of the system, the one or more processors are caused to determine one or more risk categories of one or more risks involved in using the blockchain-based data storage system in a specified environment

[0027] In some embodiments of the system, the validity test is selected based on the risk categories.

[0028] In some embodiments of the system, the one or more risk categories are selected from a group consisting of government and oversight, cyber security, infrastructure layer, architecture layer, operational layer, and transaction layer.

[0029] In some embodiments of the system, the one or more data activities comprises storing one or more data in the data block.

[0030] In some embodiments of the system, the validity test is performed continuously on the stored one or more data.

[0031] In some embodiments of the system, the one or more processors are caused to: receive from the user using the user interface a selection of one or more time periods within the one or more validity test; analyze the output of the one or more validity tests during the one or more time periods; and generate the one or more validity test reports at end of each of the one or more time periods.

[0032] In some embodiments of the system, the one or more processors are caused to display, using the user interface, the output of the validity test; and wherein, in response to the output indicating that the one or more data activities failed the validity test, the one or more processors are caused to receive from the user using the user interface a selection of whether the one or more data activities are exceptions to the operating protocol of the blockchain-based data storage system.

[0033] In some embodiments, a non-transitory computer-readable storage medium storing one or more programs for validating a blockchain-based data storage system, the one or more programs configured to be executed by one or more processors and including instructions to: conduct a risk analysis of using the blockchain-based data storage system in a specified environment; generate a risk profile of one or more data activities in a data block of the blockchain-based data storage system based on the risk analysis of using the blockchain-based data storage system in the specified environment; determine a number of times a validity test is to be performed on the one or more data activities in the data block to achieve a predetermined level of assurance, wherein the validity test tests compliance of the one or more data activities with an operating protocol of the blockchain-based data storage system; perform the validity test on the one or more data activities; and generate one or more validity test reports based on output of the validity test.

BRIEF DESCRIPTION OF THE FIGURES

[0034] FIG. 1 illustrates a blockchain process flow in accordance with some embodiments.

[0035] FIG. 2 illustrates generation of a data block in a blockchain in accordance with some embodiments.

[0036] FIG. 3 illustrates shift in validating and control processes in distributed data storage systems in accordance with some embodiments.

[0037] FIG. 4 illustrates steps of a validation method for validating data activities in a data block of a blockchain data storage system in accordance with some embodiments.

[0038] FIG. 5A illustrates a correspondence of the risk framework testing procedures to a technology stack of a blockchain system according to examples of the disclosure.

[0039] FIG. 5B illustrates sub-categories corresponding to each risk framework category according to examples of the disclosure.

[0040] FIG. 6 illustrates an exemplary process for generating blockchain test procedures according to examples of the disclosure.

[0041] FIG. 7 illustrates an example of a computing device in accordance with examples of the disclosure.

[0042] Illustrative embodiments will now be described with reference to the accompanying drawings. In the drawings, like reference numerals generally indicate identical, functionally similar, and/or structurally similar elements.

DETAILED DESCRIPTION

[0043] Embodiments of the present disclosure may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the present disclosure may also be implemented as instructions stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices, and others. Further, firmware, software, routines, instructions may be described herein as performing certain actions. However, it should be appreciated that such descriptions are merely for convenience and that such actions in fact result from computing devices, processors, controllers, or other devices executing the firmware, software, routines, instructions, etc.

[0044] The embodiments described herein may be implemented within a local computer system. The computer system may be implemented in the contexts of the likes of computing systems, networks, servers, or combinations thereof. The computer system includes one or more processors and main memory. Main memory may store, in part, instructions and data for execution by processors. Main memory stores the executable code when in operation, in this example. The computer system may further include a mass data storage, a portable storage device, output devices, user input devices, a graphics display system, and/or peripheral devices.

[0045] The components of the computer system may be connected to a communication infrastructure (e.g., a bus or network). Processors and main memory may be connected via a local microprocessor bus, and the mass data storage, peripheral device(s), portable storage device, and graphics display system may be connected via one or more input/output (I/O) buses.

[0046] Mass data storage, which can be implemented with a magnetic disk drive, solid state drive, or an optical disk drive, is a non-volatile storage device for storing data and instructions for use by processor. Mass data storage may store the system software for implementing embodiments of the present disclosure for purposes of loading that software into main memory.

[0047] Portable storage device may operate in conjunction with a portable non-volatile storage medium, such as a flash drive, floppy disk, compact disk, digital video disc, or Universal Serial Bus (USB) storage device, to input and output data and code to and from the computer system. The system software for implementing embodiments of the present disclosure may be stored on such a portable medium and input to the computer system via the portable storage device.

[0048] User input devices can provide a portion of a user interface. User input devices may include one or more microphones, an alphanumeric keypad, such as a keyboard, for inputting alphanumeric and other information, or a pointing device, such as a mouse, a trackball, stylus, or cursor direction keys. User input devices can also include a touchscreen. Suitable output devices include speakers, printers, network interfaces, and monitors.

[0049] Graphics display system may include a liquid crystal display (LCD) or other suitable display device. Graphics

display system may be configurable to receive textual and graphical information and processes the information for output to the display device.

[0050] Peripheral devices may include any type of computer support device that adds additional functionality to the computer system.

[0051] The components provided in the computer system are those typically found in computer systems that may be suitable for use with embodiments of the present disclosure and are intended to represent a broad category of such computer components that are well known in the art. Thus, the computer system can be a personal computer (PC), hand held computer system, telephone, mobile computer system, workstation, tablet, phablet, mobile phone, server, minicomputer, mainframe computer, wearable, or any other computer system. The computer may also include different bus configurations, networked platforms, multi-processor platforms, and the like. Various operating systems may be used including UNIX, LINUX, WINDOWS, MAC OS, PALM OS, QNX ANDROID, IOS, CHROME, TIZEN, and other suitable operating systems.

[0052] The processing for various embodiments may be implemented in software that is cloud-based. In some embodiments, the computer system described above may be implemented as a cloud-based computing environment, such as a virtual machine operating within a computing cloud. In other embodiments, the computer system may itself include a cloud-based computing environment, where the functionalities of the computer system are executed in a distributed fashion. Thus, the computer system, when configured as a computing cloud, may include pluralities of computing devices in various forms.

[0053] The cloud may be formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the computer system, with each server (or at least a plurality thereof) providing processor and/or storage resources. These servers may manage workloads provided by multiple users (e.g., cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

[0054] Computer program code for carrying out operations for aspects of the present disclosure may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the “C” programming language or similar programming languages. The program code may execute entirely on the user’s computer, partly on the user’s computer, as a stand-alone software package, partly on the user’s computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be coupled with the user’s computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0055] Aspects of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the present

invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0056] These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0057] The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0058] While various embodiments have been described below, it should be understood that they have been presented by way of example only, and not limitation. The descriptions are not intended to limit the scope of the invention to the particular forms set forth herein. Thus, the breadth and scope of a preferred embodiment should not be limited by any of the exemplary embodiments described herein. It should be understood that the description is illustrative and not restrictive. To the contrary, the present descriptions are intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims and otherwise appreciated by one of ordinary skill in the art.

[0059] Blockchain validation tool/system (may be referred as Blockchain Continuous Assurance, Compliance, Monitoring and Validating Solution or Blockchain Continuous Validating Solution) can include a Continuous Assurance, Compliance, Monitoring and Validating Methodology (may be referred as continuous validating methodology), Continuous Assurance, Compliance, Monitoring and Validating Criteria (may be referred as blockchain validating criteria or acceptance criteria), blockchain risk evaluation system (may be referred as blockchain risk framework), business and

technical risk and reporting assessments, and software that enables transaction level assurance for any given Blockchain use case. The validation system can include a combination of services and software designed for practitioners to provide transparency in meeting the assurance and compliance needs of users of blockchain-based data storage systems.

[0060] FIG. 3 illustrates an exemplary process for deploying a distributed ledger validation tool according to examples of the disclosure. In the example of FIG. 3, the process 300 can begin at step 302 wherein the customer's (who will be using the validation system) blockchain use-case is analyzed. The use-case analysis performed at step 302 can include as an example, determining the type of blockchain that is being used by the customer, analyzing how the customer is using the block chain to effect transactions and what solutions the blockchain is meant to deliver to the customer.

[0061] Once a use-case analysis is completed at step 302, the process can move to step 304, wherein a risk framework analysis is applied to the customer blockchain. A risk framework is a tool that can be used by stakeholders or auditors to assess and define the assurance and compliance needs of a particular blockchain use-case. The framework can allow the user to step through a series of categories of risks (i.e., risks to an organization engendered by their use of blockchain) to determine what risks they wish to audit for, and to determine the extent to which those risks would harm the organization. The risk framework described above can be industry, use-case, and blockchain technology agnostic so that practitioners across all industries and sectors can use to address the risk assurance and compliance needs independent of the Blockchain technology variant and use case.

[0062] Practitioners can use the risk framework as a standard approach and framework to evaluate the current state of a Blockchain use case which can be inclusive of upstream and downstream (on-Blockchain and off-Blockchain) processes, technologies, and underlying data elements (people, processes, technologies) against 6 different risk categories, applicable domains, and 100+ sub-risk categories in order to address assurance and compliance needs (risks, control objectives, controls, testing objectives and procedures, and reporting parameters) of the following stakeholders simultaneously or exclusively. The risk categories, domains and sub-risk categories can be used exclusively or mutually exclusively to determine targeted and/or upstream and downstream impacts. These parameters can be used to customize and personalize an assurance or auditing software/tool to achieve required level of assurance and compliance as by-product of processed transactions.

[0063] In one or more examples, the risk framework can include such categories as: governance and oversight of the blockchain, cybersecurity issues with the blockchain, infrastructure risks, blockchain architecture risks, operational risks, and transactional risks. As part of using the risk framework, a user can (via user interface) go over each risk category and the sub-categories within each risk category and indicate which risks are pertinent to their organization (or that they wish to be analyzed), and also indicate the degree and scope of those risks using the risk framework.

[0064] Once a user has engaged the risk framework at step 304 to identify the risks they want analyzed during an audit, the process can move to step 306 wherein the user-preferences supplied to the risk framework can be converted in to one or more testing procedures to be performed during the

real-time compliance testing of the customer's blockchain. As will be described in further detail below, the testing procedures can then be used by the validation/auditing software to in real-time audit the blockchain.

[0065] Once the results from the risk framework are converted to testing procedures at step **306**, the process can move to step **308**, wherein the real-time auditing tool is customized using the results gleaned from the risk framework. In one or more examples, customizing the auditing tool can include setting up one or more testing procedures that the tool will engage in during its operation, and also setting up the formatting of the reports that the tool will ultimately produce for review by the customer (described in further detail below).

[0066] Finally, once the tool has been customized per based on the assessment of the use-case established at step **302** and the application of the risk framework at step **304**, the process can move to step **310** wherein the tool is deployed in the customer environment. As will be described in further detail below, deploying the tool can refer to the creation of a validation node that becomes part of the customer blockchain environment. The validation node can be a read only node that includes the software to run the test procedures discussed with respect to step **306** on blockchain transactions as they occur in real time in the customer environment.

[0067] In one or more embodiments, the validation system created by the process described with respect to FIG. 3, may utilize a permanent planning file that can contain the details and results of the risk framework application, that can then be used at step **306** to convert the risk framework results into testing procedures. In other embodiments, the permanent planning file can instead be directly created by a user without the need to engage in the risk framework analysis above.

[0068] In some embodiments, the above set of activities of the validating methodology may be executed systematically (e.g., via software, hardware, or a combination thereof) with manual input by the auditor or compliance practitioner. In one or more examples, the validating methodology described above with respect to steps **302** may be divided into three phases (e.g., planning, fieldwork, and reporting sprints). The three phases are described below.

[0069] Planning Phase: In some embodiments, steps **302**, **304**, and **306** of FIG. 3 may constitute the planning phase. During the planning phase, an assessment is performed to identify validating test procedures using blockchain validating criteria and risk framework. In order to provide a required level of assurance for any given blockchain use case, a standardized acceptance criterion is developed to capture inputs and outputs and set the right assurance threshold level based on stakeholders' requirements, as needed. A blockchain risk framework can be used to identify inputs and define outputs in order to create the required level of assurance. Based on the assessment results obtained from using the criteria and risk framework of step **304**, validity test and reporting parameters are determined (at step **306**).

[0070] Fieldwork Phase: In some embodiments, step **308** and **310** of FIG. 3 may constitute the fieldwork phase. During the fieldwork phase, the validating software may be customized with the test and reporting parameters determined in the planning phase. Once the customized software is deployed at step **310**, transactional information can be captured based on the defined data parameters and passed

through a rules engine (described in further detail below), which can host the validity test rules. Practitioner uses the validity software to execute real-time evidence gathering and testing across a data activities—level data population set on a real-time basis (or some other interval if preferred, e.g., bi-monthly or monthly).

[0071] As will be described in further detail below, the software can classify testing results as either an observation (visual or virtual alert) when the rule breaks/fails, or a no-observation if the transaction passes the test rule with no breaks/fails. A practitioner classifies an observation as either an exception/deviation noted, or no exception/deviation noted. Further, the practitioner raises exception(s)/deviation (s) noted per test procedure as an issue, including exception/deviation details, investigation results, issue summaries and details, impact rankings and details, and management action plan details.

[0072] Reporting Phase: In some embodiments, step **310** of FIG. 3 may constitute the reporting phase. Once the validity tests and other fieldwork activities (i.e., exceptions/deviations and issues) are complete, the deployed tool can produce an issue and interim audit report, including ratings and details at the process and subprocess levels to achieve continuous reporting and monitoring (or some other interval if preferred, e.g., bi-monthly or monthly. In some embodiments, after the interim reporting cycle for the quarter (or some other interval if preferred) is complete, practitioner produces and issues a quarterly audit report including ratings and opinions at the process and subprocess levels to the stakeholders.

[0073] The testing and reporting can provide the required assurance level information at the process and subprocess levels based on the applicable risks, controls, testing objectives, and reporting parameters across the entire population data set to address stakeholders' needs.

[0074] In some embodiments, the exception can be replaced with the deviation in the flow described above to address the process and functional needs of the stakeholders in compliance or non-compliance areas (outside of audit).

[0075] In some embodiments, the validating methodology provides a practitioner with an end-to-end standardized audit process and sets of activities that can be used to obtain real-time transparency around given business processes (i.e., non-blockchain and blockchain) and provide compliance and audit-type reporting automatically or manually. In some embodiments, the methodology enables the practitioner to execute set of audit and compliance activities by the computer in a continuous fashion, which can bring a significant increase in efficiency and effectiveness, achieving a higher/maximum level of confidence.

[0076] In some embodiments, the blockchain validation tool/system is designed and developed to provide real-time transaction-level assurance with immediate results across a full population data set, which can be used by stakeholders and end-users simultaneously or exclusively to address their assurance, audit, and/or compliance needs. Some examples of stakeholders would be such personnel as the head of innovation, head of corporate development, chief technology officer, head of business segment(s), and chief audit executive. Some examples of end-users would be internal users (e.g., operations (first line of defense), enterprise risk management (second line of defense), internal audit (third line of defense), and tax); and external users (e.g., legal and regulatory).

[0077] Some assumptions in performing real-time assurance may include that: (1) off-chain data (i.e., data not stored within the blockchain) exists and may be required for key assurance reporting; (2) ordering, integrity, and completeness of data activities in a blockchain can be critical to assurance; (3) while the integrity of blockchain data can be validated, third-party “off-chain” data is not immutable and subject to change; and (4) assurance is being conducted on the qualitative and quantitative data activities of the blockchain, rather than the technical blockchain implementation (consensus protocols, block formation rules, blockchain forks, etc.).

[0078] The blockchain validation system may include major five components: (1) customer environment **404**, (2) integration unit **406**, (3) data block service unit **408**, (4) front-end service or reporting unit **410**, and (5) interfaces **412**. In addition, the system **400** may interface with third-party computing systems (as indicated by block **402**) as well as the customer blockchain **404**. The following sections discuss these architectural components of the blockchain validation system (which may be referred to as the blockchain assurance and validation solution, blockchain assurance and validating software, or blockchain assurance solution).

[0079] FIG. 4 illustrates an exemplary blockchain validation system according to examples of the disclosure. The following discussion with reference to FIG. 4 outlines a structure to establish a validation node capable of performing real-time assurance off third-party blockchains. The validation system consists of individual microservices performing discrete pieces of functionality, which, when holistically viewed, can enable real-time assurance and validation of data activities in data blocks of blockchains in a blockchain network. The blockchain network may have a plurality of blockchain nodes having blockchain-based data storage systems in each blockchain node as described above with respect to FIG. 1. In some embodiments, the blockchain network and the blockchain node of FIG. 4 may be represented by the network and nodes shown in FIG. 1. The discussion below provides insight into the primary responsibilities of each service as a new blockchain event or data block is added to a node in the blockchain network.

[0080] Some assumptions in performing real-time assurance may include that: (1) off-chain data (i.e., data not stored within the blockchain) exists and may be required for key assurance reporting; (2) ordering, integrity, and completeness of data activities in a blockchain can be critical to assurance; (3) while the integrity of blockchain data can be validated, third-party “off-chain” data is not immutable and subject to change; and (4) assurance is being conducted on the qualitative and quantitative data activities of the blockchain, rather than the technical blockchain implementation (consensus protocols, block formation rules, blockchain forks, etc.).

[0081] The blockchain validation system may include major five components: (1) customer environment **404**, (2) integration unit **406**, (3) data block service unit **408**, (4) front-end service or reporting unit **410**, and (5) interfaces **412**. In addition, the system **400** may interface with third-party computing systems (as indicated by block **402**) as well as the customer blockchain **404**. The following sections discuss these architectural components of the blockchain validation system (which may be referred to as the blockchain assurance and validation solution, blockchain assur-

ance and validating software, or blockchain assurance solution) with reference to FIG. 4.

[0082] To illustrate the functionality of the components contained within system **400**, a description of the data flow in the architecture of FIG. 4 can be pertinent. The process of validating blockchain transaction can begin with the addition of a new data block from one of the blockchain nodes **418** residing in the customer’s blockchain environment. When a node **418** attempts to introduce new data into the blockchain, that activity can be sent to chain listener **422**. The chain listener can serve as the initial integration point between the blockchain assurance and validation tool, and the customer blockchain. The goals of the chain listener can be to emit transactional blockchain events occurring within the blockchain. In most cases, blockchains provide varying levels of “feed” data in instances where generic events or transactions are published to subscribers of its services; in these cases, the chain listener can leverage those existing services to provide events for downstream service consumers.

[0083] Events trigger the initial action that results in a transaction or data activity (or the addition of a block) within the blockchain. Events should trigger one or more transactions within the blockchain, indicating that some key information should be delivered across the blockchain network. These transactions will manifest as a simple key-value pair, as illustrated below:

```
{
  //on the blockchain
  _id: 3199444, //a unique identifier
  dateTime: 2103323223 //unix timestamp,
    transaction; 2193298439843984381212211 //a transaction,
  sender: John Doe, //string
  receiver: Jane Doe, //string
  amount: 10 //integer
}
```

[0084] In most industry use-cases, blockchains will not actually store transactional data. The use of a shared ledger implies the likely scenario in which sensitive-data transactions occur. Moreover, storage costs can escalate, and blockchains are not intended to store items such as images, documents, etc. As such, an event transaction may have a simple encrypted “hash,” which can contain a secret location that can be unencrypted by the asset owner. The same object described above can easily be represented as such:

```
{
  // on the blockchain
  _id: 3199444, //a unique identifier
  dateTime: 2103323223 //unix timestamp,
    hash; 2193298439843984381212211 //an encrypted value that could
    represent anything
}
{
  // off the blockchain (such as in a relational database).
  _id:2193298439843984381212211,
  transaction; 2193298439843984381212211 //a transaction,
  sender: John Doe, //string
  receiver: Jane Doe, //string
  amount: 10 //integer
}
```

[0085] A “push” feed (built within the blockchain protocol) is the ideal setup, because it properly segregates the

responsibilities across the blockchain network and the assessment and validating software. As such, it is up to the blockchain to provide guarantees that ensure transactions are emitted while the chain listener is responsible for relaying those events into the validation system. If this service is ever stopped or interrupted, it should possess enough awareness and understanding to resume starting with its last acknowledged transaction. This ensures that transactions are not “duplicated” within the environment and that unnecessary work to “reprocess” blockchain transactions will not occur.

[0086] Thus, once the chain listener detects that a new transaction is occurring on the blockchain, it can tag the event and send them to event listener 442 by placing the events onto a queue 434. The event listener 442 may then pick up the new data block from queue 434 and perform a series of tasks with the new data block acquired from queue 434. In one or more examples, the event listener 442 may store a copy of the new data block by storing in event store 436. The event store 436 can be the principal “record of truth” that represents a historical copy of the blockchain from which all downstream systems derive their system state. Records that live as unstructured data, and events transacted from the blockchain listener, will live as JSON objects within this document store (e.g., MongoDB), and will live in its nearest representation to data on the blockchain. The primary goals of the event store can be twofold: (1) separating querying and data, extraction responsibilities from the validation node (to avoid directly querying the blockchain for events); and (2) creating a consistent storage abstraction that can be leveraged regardless of the blockchain platform.

[0087] The event store can also enable additional capabilities such as data “snapshots,” where events or transactions can be “replayed” as they occur. The event log provides a strong audit capability (e.g., accounting transactions are an event source for account balances) where historic states can be recreated by replaying past events.

[0088] Simultaneously to storing the event at event store 436, the event listener 442 can transmit the new data block to data enricher 424 by placing it into a queue 432. The data enricher 424 can take the data block stored at queue 432 and request information from external data sources (e.g., from a customer or third party) through the off-chain API 426 that collects third-party data stored at 414, and off-chain data stored at 416. External data sources can be centrally managed through the use of an off-chain API 426 that can federate requests to one or many external data sources such as third party data 414 or off-chain data 416. External data sources are centrally managed through the off-chain API 426, which federates requests to one or many external data sources. Off-chain data (sometimes referred to as oracles) provide, contextual information about blockchain data, including real-time data elements (e.g., stock prices), personally identifiable or sensitive information (e.g., names or addresses), or extraneous metadata, which could bloat the size of the blockchain ledger. Through the creation of its own independent service, the application reduces the tight coupling between internal and external application logic, and limits exposure to third-party systems.

[0089] Customer environment 404 which can store off-chain data 416, as well as third party data coming from data store 414 can describe the spectrum of tasks occurring within third-party networks and the original inception of the transaction, data activities, or data block onto the block-

chain-based data storage system. While upstream (i.e., actions prior to hitting the blockchain) activities should be considered “out of scope” of the tool 400—need for assurance can require that examination occurs as close to the original “source of truth” as possible—it can therefore be essential for critical data elements or keys to exist within the blockchain, or else they will not be captured by the downstream processes. Careful design of blockchain metadata is needed to enable the ability for assurance and validation. Thus, customer environment 404 can collect and store various “off-chain” data at data store 416.

[0090] As an example of off-chain data, if a distributed ledger is storing emails being sent back and forth from the customer, the names associated with each email address could be an example of “off-chain data” that could be used to help validate and audit the blockchain itself. Thus, the type of data that while not needed for action block creation itself, may be needed to validate transactions occurring in real-time can be stored at data store 416. Off-chain storage contains data that is not readily available for public consumption. Off-chain storage may reference anything from trade data to vendor/sales information, or anything that provides context to the transactions inscribed on the block.

[0091] While blockchain data is historic and immutable, off-chain data is not immutable or immune to tampering. This makes logical sense: off-chain data will likely be sensitive, business-contextual data and will often be used by multiple consumers within an organization. The duplication of data across off-chain and on-chain data which poses consistency issues and the two are in-sync. It is possible that records reflected within the blockchain are not represented off-chain. Downstream processes will need to reflect this known hazard when they are working with off-chain data by properly rebuilding or reconstructing records that require updates to ensure the audit solution accurately reflects the historic state.

[0092] Once the data enricher 424 adds in the off-chain data, it can then transmit the augmented even to rules engine 428 via queue 430. Customer-specific business assurance rules can applied to the data block in the rules engine 424. Rules can be highly specific to the business and industry concerned and be customized according to each customer as described above with respect to the risk framework. Rules can the cornerstone of the validation solution, providing the basis of when/why transactions violate specified conditions.

[0093] The rules engine 428 can be implemented as a worker with a specified set of instructions on how to apply rules against transactions. Because the user interface also relies on the awareness and knowledge of rules, the rules engine can retrieve the latest inventory of rules from a shared database (not pictured). While this extra network request may seem unnecessary, it also can enable user-features such as the dynamic toggling of rules, the addition/subtraction of rules without hard resets, etc.

[0094] Two categories of rules may be applied to transactions or data activities in the blockchain: streaming rules that assess against individual transactions, and batch rules that assess against an aggregate of transactions.

[0095] Streaming Rules: Incoming transactions can be evaluated against a set of one or many business rules that can assess validity across a variety of dimensions (e.g., completeness of a transaction, blacklisting of specific values, application of transaction logic such as input=output, etc.).

[0096] Batch Rules: Incoming transactions that possess some relationship to historical or past events can leverage the event store to identify patterns that may violate assurance rules (e.g., aging transactions, number of transactions from an account, etc.).

[0097] These rules are generators of “observations” within the solution. Observations indicate the violation of a pre-defined guideline set by business or assurance rules, which Users of the system will evaluate within the web interface. As will be described in detail below, the observations can be collected and presented to a user, who can then review each observation and determine whether the observation warrants further scrutiny.

[0098] Once the rules engine 428 applies the one or more rules to the data block, the results of the tests performed by the rules engine can be sent to reporting database 444. Reporting database can store the results of the application of the rules to the data block.

[0099] The reporting DB is the final staging area where business-oriented data structures can be queried and analyzed. Any blockchain transaction saved within the event store will create one or many transactions within the reporting DB; this will allow a variety of views to be “staged” and immediately ready for analytics, assurance reports, etc.

[0100] In order to create this reporting state for user interfaces, any off-chain data must be already “enriched” and co-located with other blockchain events. The integration of off-chain and on-chain data will require a high degree of collaboration and integration between the third party and the tool.

[0101] Reliability and uptime of external systems can be unpredictable, and the present invention anticipates “offline” scenarios where external systems are unavailable. Moreover, the current state of the reporting DB can be off-sync with its original source of truth if records have been updated within the host system.

[0102] To resolve these issues, the architecture should incorporate several precautionary measures to ensure the reporting DB is in an accurate representation of its source of truth. In the “offline” scenario, worker jobs should fail, persist, and retry to ensure transactions are not lost. Additionally, periodic background validation jobs should have the ability to check the accuracy and updates of records. This integration has the potential to be complex, depending on the auditability and traceability of third-party systems.

[0103] The results stored in reporting database 444 can be sent to user interface 412 for further evaluation via reporting API 448. The reporting platform will be the sole interface through which users interact and communicate with blockchain data. A separate “reporting API” provides external users with access into data that has already been relayed, saved, and transformed into contextual and relevant pieces of information. This information is ready to be consumed by the web interface, which enables risk assurance professionals to make decisions according to real-time events on the blockchain.

[0104] The user interface presents the results of the test procedures to the rules engine. The user interface may be a web page, a web dashboard, a mobile device, or any other device that is configured to display or output the validation report.

[0105] Referring back to FIG. 3, at step 304 a risk framework can be used to generate one or more tests. Those tests can then be transmitted to rules engine 428 in the system

described in FIG. 4 to perform real-time and continuous validation of a blockchain system. The risk framework can allow for a user to specify the risks they wish to monitor for during their testing and the level of assurance they are seeking, and those inputs can be converted into a plurality tests that are run during the operation of the blockchain. Thus, while all users of the validation tool can be presented with a common risk framework, the output of the risk framework can be specific to each individual user/organization to ultimately generate a unique validation tool that addresses the specific needs of the organization.

[0106] The discussion below can illustrate how the risk framework described above can fit in with an overall approach to risk management for validating a blockchain system.

[0107] In some embodiments, determining the acceptance criteria (may be referred to as assurance threshold formula) may include the five steps discussed below.

[0108] 1—Purpose (P1)—Gain an understanding of the blockchain use case, business purpose, and the resultant effect on the risks and control objectives.

[0109] 2—Process (P2)—Assess on and off blockchain processes and technologies to understand continuous assurance methodology affects, up and downstream, on audit expectations and the entire process risk profile.

[0110] 3—Risks (Rs)—Assess the blockchain architecture variant and identify applicable control objectives using the blockchain risk framework.

[0111] 4—Stakeholder (Sr)—Identify assurance related stakeholders, determine and inventory their expectations and needs for reporting purposes.

[0112] 5—Assurance Threshold Formula (ATx)—Total number of test procedures required to achieve the required level of assurance. The test procedures can be coded into the rule engine of the audit software/tool for automated testing and transaction level assurance.

[0113] Based on the results obtained from these four activities in combination of the blockchain risk framework, the following Assurance Threshold Formula (ATx) is determined:

$$P1+P2+Rs+Sr=ATx$$

[0114] The solution sum of Y (Continuous Audit) must always be equal or greater than ATx in order to create the necessary level of assurance. Therefore Y ATx.

[0115] As shown above, the risk framework (step 3) can work to provide a required level of assurance to a customer that their blockchain system is operating with minimal risk.

[0116] In some embodiments, the blockchain risk evaluation system or risk framework may assess the current state of a blockchain use case against different risk categories (e.g., six or more different risk categories) and across sub-categories (e.g., 100 or more different sub-categories) in order to address assurance and compliance needs of stakeholders. This assessment may be performed by a risk evaluation system that is industry, use case and Blockchain platform agnostic. In some embodiments, the results of these assessments provide the necessary information to identify applicable risks, control objectives, testing reporting and reporting parameters that are used to customize our the continuous validating software.

[0117] The blockchain risk framework is a component of the blockchain continuous validating solution. Due to availability and use of several variants of blockchain technology

for use cases and lack of a standard approach or risk frameworks that can be used to obtain required level of transparency for a given blockchain use to meet compliance, assurance, and audit requirements, an approach has been designed and the supporting framework is developed that is industry, use case and blockchain technology variant agnostic so that practitioners across all industries and sectors can use to address the risk assurance and compliance needs independent of the blockchain technology variant and use case.

[0118] Practitioners can use blockchain risk evaluation system as a standard approach and framework to evaluate the current state of a Blockchain use case which can be inclusive of upstream and downstream (on-Blockchain and off-Blockchain) processes, technologies, and underlying data elements (people, processes, technologies) against 6 different risk categories, applicable domains, and 100+ sub-risk categories in order to address assurance and compliance needs (risks, control objectives, controls, testing objectives and procedures, and reporting parameters) of the following stakeholders simultaneously or exclusively. The risk categories, domains and sub-risk categories can be used exclusively or mutually exclusively to determine targeted and/or upstream and downstream impacts. These parameters can be used to customize and personalize an assurance or validating software/tool to achieve required level of assurance and compliance as by-product of processed transactions.

- [0119] Some examples of stakeholders provided below:
- [0120] Chief Executive Officer
 - [0121] Chief Financial Officer
 - [0122] Chief Technology Officer
 - [0123] Chief Information Security Officer
 - [0124] Chief Audit Executive (3rd Line of defense)
 - [0125] Head of Enterprise Risk Management (2nd line of defense)
 - [0126] Head of Operations (1st line of defense)
 - [0127] Head of Innovation
 - [0128] Head of Corporate Development
 - [0129] Head of Compliance and legal
 - [0130] Head of Tax
 - [0131] External Regulators
 - [0132] Head of Business Segment(s)

[0133] Risk Categories:

[0134] In Some Embodiments, Some Examples of Risk Categories and their relevant domains are provided in Table 1.

TABLE 1

Risk Category	Domain
Governance and Oversight	Business Objectives
	Program Sponsorship
	Leadership Commitment
	MIS and Metrics
	Program Management
	Operational and Capital Expenditure Oversight
Cyber Security	Project Management
	Third-party Risk
	Cloud Security
	Data Security
	Data Privacy
	Penetration Testing
	Programming Security
	Network Security
	Patch and vulnerability

TABLE 1-continued

Risk Category	Domain
Infrastructure Layer	Threat detection
	Threat response
	Servers and Databases Configuration
	ITGCs
Architecture Layer	Business Continuity and Disaster Recovery
	IT Asset Management
	Blockchain Platform & Protocol Configuration
	Hardware Security Modules
	Signature Management
Operational Layer	Cryptography
	Scalability
	Availability
	Permissioned network management
	Participant Onboarding and Off-boarding
	Application layer
Transactional Layer	Blockchain consensus program management
	Integration with off-Blockchain systems and processes
	Smart Contracts
	Digital Assets
	Digital Currency
	Clearing and settlement
	Business Use Case Transactions

[0135] The sub-risk categories, control and testing objectives, test procedures and request lists for each for the above risk categories and domains of Table 1 are provided below. When engaging with the risk framework, a user using a computer/laptop or some other computing device, can be guided through each risk category and specify parameters relating to the category. In one or more examples, the user can specify if a particular risk is to be classified as low, medium, or high. In one or more examples, the categories, low, medium, high, can change for one risk, from one blockchain system to another. As an example, because there may be other surrounding controls in place or there may be some compensating controls in place, a particular risk may be categorized as low. Alternatively another in another blockchain environment, a user may assess that risk to be high because the system doesn't have certain compensating controls in place or certain processes or technology or checks and balances in place. In such a system the risk maybe categorized as high. Thus classifying a risk as low, medium, high, can mean that there's a possibility that this can fall into either of these three categories, depending on the use case and depending on the environment, that is being examined.

[0136] In some embodiments, governance and oversight risk category in the blockchain risk framework covers relevant risks, control objectives and descriptions, testing objectives and procedures, and reporting parameters designed to address assurance and compliance needs for the blockchain portfolio and program management, governance, and oversight. Focus areas for this category includes blockchain strategy, research and development, investment, business, operations, product and use case solution development activities.

[0137] The sub-risk categories, control and testing objectives, test procedures and request lists for Governance and Oversight risk category are provided below in Tables 2-4. Table 2, is an exemplary sub-risk category table for the governance and oversight risk category. The table below can be presented to a user accessing the risk framework from a computing device configured to receive inputs from a user. The table below can include a risk category indicator that

specifies the category of risk as defined above. Each of the Risk Categories cover Blockchain including upstream and downstream processes, technologies stacks, and people and associated risk profiles.

[0138] The table below can include a domain column can identify the areas relevant to the blockchain that is covered by each risk category. In one or more examples, the table below can include a risk classification column that identifies the applicable processes and technologies within each domain, where the risk is present. In one or more examples, the table below can also include a risk number that simply

provides a method for identifying the risk in numerical form. In one or more examples, the table below can also include a risk description that describes the risk applicable to/associated with the processes and technologies within each domain. In one or more examples, and as described above, the table can also include a risk level rating (low, medium, high) as described above.

[0139] When the user is presented with the framework, they can initially review each risk category, and specify whether such a risk is a low, medium, or high concern. Presented below is an example risk table for the government and oversight risk category.

TABLE 2

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Governance and Oversight	Business Objectives	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-BO1	At the senior management level, business objectives and justification is not clearly defined leading to failure of program and misalignment with strategy and overarching governance framework.	L, M, H
Governance and Oversight	Business Objectives	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-BO2	The Blockchain Program is implemented in silos without a formal oversight committee resulting in inefficient utilization and duplication of efforts.	L, M, H
Governance and Oversight	Business Objectives	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-BO3	Unapproved or miscommunicated scope can lead to failure of program or poor utilization of program resources.	L, M, H
Governance and Oversight	Program Sponsorship	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PS1	Lack of involvement from Senior Management can lead to low organizational awareness and failure of the Blockchain program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM1	Failure to define and monitor Key Performance Indicators (KPIs) may lead to failure of the program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM2	Failure to formalize methodology for inventorying, analyzing, prioritizing and selecting eligible the Blockchain use cases may lead to failure of the program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM3	Failure to define and effectively monitor project progress may lead to failure of the program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM4	Failure to assess the level of change readiness for the organization when implementing Blockchain may lead to failure of program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM5	Failure to define the go-live criteria within the program objectives may lead to failure of the program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM6	Failure to identify proper resources to fulfill roles with the Blockchain	L, M, H

TABLE 2-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
		Financial, Compliance, Legal, or Reputational		program and lack of learning and development to ensure that employees skills are in line with the needs of the Blockchain program leads to excessive turnover and inadequate resources.	
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM7	Failure to consider changes in the business process due to Blockchain technology could lead to loss of institutional knowledge.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM8	Lack of acceptance from users and employees of the Blockchain program could lead to failure of the program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM9	Lack of acceptance from users and employees of the Blockchain program could lead to failure of the program.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM10	Inadequate processes to setup Blockchain vendor software could lead to increased risks to security requirements.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM11	Inadequate assessment of hardware, applications, software and software components may leave information systems vulnerable and unable to fulfill business objectives.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM12	Lack of a standard process to document functional specifications for each business process can lead to incomplete or inaccurate documentation.	L, M, H
Governance and Oversight	Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM13	Failure to define and develop a clear benefits strategy could lead to failure of the Blockchain program.	L, M, H
Governance and Oversight	Project Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM14	Failure to assign appropriate resources to aid in the design of application security and controls may result in increased risks to the business and insufficient controls around the business processes.	L, M, H
Governance and Oversight	Project Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM15	Employees who are not appropriately trained may result in an increased risk of bypassed or forgotten considerations essential to the Blockchain Program.	L, M, H
Governance and Oversight	Project Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM16	Failure to allocate appropriate representation and resources for the duration of the program, may lead to the misuse of organizational funds and unintended risks to business objectives.	L, M, H
Governance and Oversight	Project Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-PM17	Lack of monitoring activities in place could lead to inaccurate and incomplete transactions processed within the Blockchain application.	L, M, H

TABLE 2-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Governance and Oversight	Leadership Commitment	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-LC1	Poor stakeholders and leadership commitment can lead to a lack of unity on program goals, objectives and performance.	L, M, H
Governance and Oversight	MIS and Metrics	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-MM1	Failure to allocate appropriate resources, while considering business requirements, may lead to the misuse of organizational funds and unintended risks to business objectives.	L, M, H
Governance and Oversight	MIS and Metrics	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-MM2	Inadequate controls to monitor the capacity, availability, and functionality of the application may lead to interruption and/or failure to key applications.	L, M, H
Governance and Oversight	Operational and Capital Expenditure Oversight	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-OC1	Failure to allocate appropriate resources, while considering business requirements, may lead to the misuse of organizational funds and unintended risks to business objectives.	L, M, H
Governance and Oversight	Operational and Capital Expenditure Oversight	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-OC2	Failure to allocate appropriate resources, while considering business requirements, may lead to the misuse of organizational funds and unintended risks to business objectives.	L, M, H
Governance and Oversight	Operational and Capital Expenditure Oversight	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-OC3	Failure to allocate appropriate resources, while considering business requirements, may lead to the misuse of organizational funds and unintended risks to business objectives.	L, M, H
Governance and Oversight	Operational and Capital Expenditure Oversight	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-OC4	Inadequate controls to govern and address security risks in a project may lead to loss of sensitive data.	L, M, H
Governance and Oversight	Smart Contracts	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-SC1	Blockchain software use cases are not consistent with participants' business or industry-specific requirements; smart contracts cannot be effectively leveraged for normal operations	L, M, H
Governance and Oversight	Smart Contracts	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-SC2	Blockchain implementation lacks a coherent governance model for development, execution, and oversight	L, M, H
Governance and Oversight	Smart Contracts	Strategic, Operational, Financial, Compliance, Legal, or Reputational	GO-SC3	Lack of IP safeguards compromise the organization's DLT innovations	L, M, H

[0140] After categorizing the risks as described above, the framework can then present the user with series of control/test objectives (with corresponding descriptions) which the user can review and determine whether such controls/test

objectives should be considered in-scope to the audit or out of scope to the audit. An exemplary control/test objective table is provided below for the governance and oversight risk category.

TABLE 3

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
Governance and Oversight	Business Objectives	At the senior management level, business justification and objectives for the Blockchain Program is documented and aligns with business strategy. The Blockchain Program is considered in the overarching governance framework with alignment to risk, compliance and IT/data frameworks.	The Blockchain Program Charter is created and includes specific details of goals and business objectives of the overall Blockchain Program. The Blockchain steering committee reviews and approves The Blockchain Program Charter to ensure it is in alignment with the firm's organizational and governance strategies.	In-scope
Governance and Oversight	Business Objectives	The Blockchain Program is appropriately prioritized against other initiatives within the organization.	A Blockchain steering committee, which includes executive leadership and senior members of the business, risk, compliance and the Blockchain program management, meets on a quarterly basis to conduct business performance reviews of how the Blockchain Program aligns with business strategy.	In-scope
Governance and Oversight	Business Objectives	The Blockchain program project plan has been defined addressing each phase of the Blockchain program project and is consistent with the scope and objectives defined within the program charter. The scope of the Blockchain Program has been approved and communicated by all participants.	The scope of the Blockchain program is outlined in the Blockchain project plan/roadmap. The project plan is reviewed and approved by the steering committee to ensure the plan is in alignment with the Blockchain Program Charter.	In-scope
Governance and Oversight	Program Sponsorship	Senior Management is actively involved in creating organizational awareness, championing the Blockchain program.	The Blockchain Program Charter is created and includes specific details of the communication strategy to the broader organization. The Blockchain steering committee reviewed and approved The Blockchain Program Charter.	In-scope
Governance and Oversight	Program Management	Key Performance Indicators (KPIs), specific to the Blockchain use case, to monitor program performance have been developed.	Key Performance Indicators (KPIs) are established to monitor the Blockchain program performance.	In-scope
Governance and Oversight	Program Management	Formalized methodology for inventorying, analyzing, prioritizing and selecting eligible the Blockchain use cases exists. This method is formally documented to ensure consistently across business units that may potentially utilize the technology.	The Blockchain program policies and procedures, which includes methodology for inventorying, analyzing, prioritizing and selecting eligible the Blockchain use cases, are reviewed and approved on a periodic basis.	In-scope
Governance and Oversight	Program Management	The Blockchain program project plan has been defined addressing every phase of the Blockchain program project and is consistent with the scope and objectives defined within the program charter. Individual project work plans are well defined and effectively monitored for project progress; an integrated master plan that provides a comprehensive view of work effort and dependencies across all project teams has been defined.	The Blockchain Program steering committee reviewed and approved The Blockchain program project plan. The Blockchain program management monitors individual project work plans to measure progress against The Blockchain project plan.	In-scope
Governance and Oversight	Program Management	Affected stakeholders are actively involved in the planning process and the Blockchain Program team has formally assessed the level of change readiness for the	The processes selected for Blockchain implementation are evaluated on a quarterly basis by the Blockchain program management team to ensure the Blockchain technology is being optimized and decisions adhere to the	In-scope

TABLE 3-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
		organization and its business units, stakeholders, and customers.	Blockchain selection criteria outlined in the Blockchain program policies and procedures. The results of this evaluation are reported to the Blockchain steering committee.	
Governance and Oversight	Program Management	Formal go-live criteria for each application/use case is adequately linked back to the program scope and objectives.	Formal policies and procedures have been established and documented to outline the methodology for the Blockchain configuration and maintenance, including decision making criteria to go live being formally documented. Policies and procedures are reviewed and approved on a periodic basis.	In-scope
Governance and Oversight	Program Management	Management has updated staffing and hiring practices to ensure the right people within the organization are identified and assigned as the Blockchain program resources. Learning and development personnel have been engagement to ensure training program has been instituted to train the Blockchain Program staff.	The Blockchain program policies and procedures, which includes details of the formal the Blockchain organization structure, staffing and training requirements are reviewed and approved on a periodic basis.	In-scope
Governance and Oversight	Program Management	There has been adequate considerations for loss of institutional knowledge as the Blockchain technology alters/eliminates steps in business processes.	Periodically, management performs a risk assessment of the Blockchain technology and evaluates the risk associated with loss of institutional knowledge.	In-scope
Governance and Oversight	Program Management	There is adequate considerations for the organizations resistance to change and appropriate people and change management processes are put into place to clearly articulate the future state and address possible disruption discomfort with a new technologically sophisticated process that will result in large decreases in manpower requirements.	Management has considered the impact that the Blockchain program will have on resources and has designed a formal people and change process to mitigate possible disruptions and resistance across the organization.	In-scope
Governance and Oversight	Program Management	A formal process to address organizational changes, including the ability to perform tasks in case of the Blockchain failure.	The Blockchain Program Charter outlines a formal process to address organizational changes. The organizational change process is analyzed and evaluated on a monthly basis by the Blockchain program management team. The results of this evaluation are reported to The Blockchain steering committee.	In-scope
Governance and Oversight	Program Management	The setup of the Blockchain vendor software includes consideration of new security requirements to maintain confidentiality, integrity, and availability have been considered.	The Blockchain vendor software for initial integration into the firm's environment follows a well-defined integration plan and is monitored by the Blockchain program management.	In-scope
Governance and Oversight	Program Management	Hardware (including configurations, locations, capacity/capacity utilization, and age and data requirements), applications, software and software components impacted by the Blockchain integration have been identified, evaluated and reported on.	Impact of software integration on the firm's existing hardware configurations, software and applications is documented and evaluated. The results of this evaluation are reported to the Blockchain Program steering committee.	In-scope
Governance and Oversight	Program Management	The process to create functional specifications for each new Blockchain business process	The Blockchain program policies and procedures, which includes the process to create functional specifications for	In-scope

TABLE 3-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
		follows a standard process documented in the Blockchain Program policies and procedures.	each new the Blockchain business process, are reviewed and approved on a periodic or as needed basis.	
Governance and Oversight	Program Management	A benefits realization strategy has been developed and approved.	The Blockchain Program Charter is created and includes the Blockchain Benefits Management process. The Blockchain Program steering committee reviews and approves the Blockchain Program Charter to ensure it is in alignment with the firm's organizational and governance strategies.	In-scope
Governance and Oversight	Project Management	Appropriate members of the business, the Blockchain program team, risk, and compliance are actively involved in design of application security and controls.	The Blockchain program management team includes members from risk and compliance responsible for designing and implementing key controls being executed by the Blockchain technology. The functional specifications for each new the Blockchain business process are reviewed by the Blockchain Program risk & compliance team member to assure the appropriateness of the design and operating effectiveness of controls the Blockchain is executing.	In-scope
Governance and Oversight	Project Management	Individuals are properly trained to configure the Blockchain technology.	The Blockchain Program configuration analysts are required to complete training prior to being involved with functional or technical Blockchain design. On an ongoing basis, individuals involved in the Blockchain program receive updated education to keep current with emerging technology issues.	In-scope
Governance and Oversight	Project Management	There is adequate commitment to provide appropriate representation and resources for the duration of the Blockchain program.	The Blockchain policies and procedures are defined and include a description of key Blockchain program management positions, responsibilities and overall organization structure for governance.	In-scope
Governance and Oversight	Project Management	Post implementation, there are monitoring activities in place to monitor the completeness and accuracy of processing for the Blockchain transactions.	Post implementation reviews are performed by the required business and/or technology management or designee to test the completeness and accuracy of processing for the Blockchain transactions.	In-scope
Governance and Oversight	Leadership Commitment	The Blockchain program stakeholders have been adequately engaged and understand the Blockchain program goals and objectives.	Leadership discusses and engages with the business to determine Blockchain goals and objectives. The Blockchain Program Charter is created and includes specific details of goals and business objectives of the overall the Blockchain Program. The Blockchain steering committee reviews and approves The Blockchain Program Charter to ensure it is in alignment with the firm's organizational and governance strategies.	In-scope
Governance and Oversight	MIS and Metrics	There is a formal process for monitoring the Blockchain program project performance and details of performance is communicated to appropriate stakeholders.	The Blockchain project plan/roadmap details the financial needs of each individual project work stream. The Blockchain program management has a formal process to monitor project costs as it relates to project progress, milestones, and deliverables, as well as specifics to measure KPI, ROI per process and overall ROI. Monthly, the project costs are reported back to the Blockchain steering committee.	In-scope
Governance and Oversight	MIS and Metrics	There is sufficient oversight over the application by to	Daily, the Blockchain Operational management reviews capacity,	In-scope

TABLE 3-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
		ensure the Blockchain is logged, functioning, and workloads, availability and capacity are being efficiently and effectively balanced.	availability and performance metrics of the Blockchain in production. Deviations from standard metrics are noted, researched and resolved. Monthly these metrics are report to the Blockchain Program steering committee.	
Governance and Oversight	Operational and Capital Expenditure Oversight	Financial needs of the program have been reviewed and approved by senior management and assessment of those needs are reassessed on an ongoing basis.	The Blockchain Program Charter is created and includes the financial needs of the Blockchain program. The Blockchain steering committee reviews and approves the Blockchain Program Charter. Additionally, the Blockchain project plan/roadmap details the financial needs of each individual project work stream.	In-scope
Governance and Oversight	Operational and Capital Expenditure Oversight	The organization allocates appropriate resources to information security and risk management.	The organization establishes a plan for the allocation of appropriate resources to projects and programs based on assessing organizational, operational, and strategic considerations.	In-scope
Governance and Oversight	Operational and Capital Expenditure Oversight	The organization allocates appropriate resources to information security and risk management.	Resources (human, technology, finance) required to achieve security objectives are allocated for the establishment, implementation, maintenance and continual improvement of the information security management system.	In-scope
Governance and Oversight	Operational and Capital Expenditure Oversight	Implement security controls in projects.	Information security is addressed in project management, regardless of the type of the project.	In-scope

[0141] Finally once the user has identified the risks (including their particular levels), and has determine which test objectives are in-scope and out-of-scope to the validation, the risk framework can then provide the user with the applicable tests that will be applied to the user's blockchain validation system. The table below can be created based on the user's inputs to the reference framework described above. The table below can indicate the test procedures to be performed that determine the design or operating effectiveness of a control specified in table 3. The table below can

also specify the test type which can be inquiry, inspection and observation, as well as attribute or substantive type of testing using a manual or automated approach. Finally, the table below can also present the user with a request list that can show the user requested items to be gathered to provide supporting information such as documentation or evidence including data parameters to execute test procedures in order to obtain the specified level of assurance and confidence surrounding the process and technology.

TABLE 4

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Governance and Oversight	Business Objectives	1. Verify the Blockchain Program Charter has been created and review the overall goals and business objectives. 2. Inspect the Blockchain Program Charter to ensure the Steering committee has reviewed and approved it.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Meeting minutes from the Steering committee meeting where the Blockchain Program charter was reviewed.
Governance and Oversight	Business Objectives	1. Inquire with Blockchain steering committee members to determine criteria for business reviews to assess the Blockchain program's alignment with business strategy 2. Inspect Quarterly meeting minutes to confirm that business performance reviews were conducted by the established criteria.	Inquiry, Inspection, and/or observation	1. Meeting minutes from the Steering committee where business performance reviews of how the Blockchain Program aligns with business strategy are discussed and reviewed.

TABLE 4-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Governance and Oversight	Business Objectives	1. Inspect the Blockchain project plan/roadmap to confirm that scope of program is outlined. 2. Inquire with Steering committee to ensure that plan was reviewed and approved, as evidence that plan is in line with Blockchain Program Charter.	Inquiry, Inspection, and/or observation	1. Blockchain project plan/roadmap 2. Blockchain Program Charter 3. Meeting minutes from the Steering committee where project plan/roadmap was reviewed and approved.
Governance and Oversight	Program Sponsorship	1. Inquire and inspect the Blockchain Program Charter to confirm details regarding the communication strategy to the broader organization. 2. Inspect that the Blockchain Program Charter has been reviewed and approved.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Evidence that the Blockchain Program Charter was reviewed and approved.
Governance and Oversight	Program Management	1. Inquire with Blockchain Operational Management to ensure Key Performance Indicators (KPIs) have been established and monitored. 2. Inspect evidence to determine KPIs are monitored periodically.	Inquiry, Inspection, and/or observation	1. Blockchain Program KPIs
Governance and Oversight	Program Management	1. Inquire with management on methodology for inventorying, analyzing, prioritizing and selecting eligible the Blockchain use cases. 2. Obtain and inspect Blockchain program policies and procedures and confirm that methodology for inventorying, analyzing, prioritizing and selecting eligible the Blockchain use cases is included. 3. Inquire with management and inspect that program policies and procedures are reviewed and approved on a periodic basis.	Inquiry, Inspection, and/or observation	1. Blockchain program policies and procedures. 2. Evidence of review and approval on a periodic basis of the Blockchain program policies and procedures.
Governance and Oversight	Program Management	1. Inquire with Steering committee to ensure that plan was reviewed and approved, as evidence that plan is in line with Blockchain Program Charter. 2. Inquire with the Blockchain program management to determine the criteria of monitoring the individual project work plans to ensure the progress is measured against the Blockchain project plan.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Meeting minutes from the Steering committee meeting where the Blockchain Program charter was reviewed. 3. Blockchain Project Plan
Governance and Oversight	Program Management	1. Inquire with the Blockchain program management team to determine that the Blockchain implementation processes are evaluated on a quarterly basis and to ensure they adhere to the Blockchain selection criteria outlined in the Blockchain Program Charter. 2. Inquire with Steering Committee to ensure they receive the evaluation of the Blockchain implementation processes.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter (policies and procedures) 2. Evidence of Blockchain selection criteria within the Blockchain Program Charter 3. Blockchain implementation processes 4. Blockchain implementation evaluation report
Governance and Oversight	Program Management	1. Inspect the Blockchain Configuration and Maintenance methodology to ensure formal policies and procedures have been documented and include decision making criteria to go live. 2. Inspect the Blockchain Configuration and Maintenance methodology to ensure the policies and procedures have been reviewed and approved on a periodic basis.	Inquiry, Inspection, and/or observation	1. Blockchain Configuration and Maintenance Methodology 2. Evidence of decision making criteria to go live 3. Evidence of review and approval of the Blockchain Configuration and Maintenance Methodology on a periodic basis

TABLE 4-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Governance and Oversight	Program Management	1. Obtain and inspect the Blockchain program policies and procedures, and review for details of the formal the Blockchain organization structure, staffing and training requirements. 2. Inquire with management and inspect the policies and procedures to confirm that they have been reviewed and approved on a periodic basis.	Inquiry, Inspection, and/or observation	1. Blockchain program policies and procedures 2. Evidence of review and approval on a periodic basis of the Blockchain program policies and procedures.
Governance and Oversight	Program Management	1. Inquire with management about the process to evaluate the risks regarding loss of institutional knowledge. 2. Obtain and inspect the risk assessment performed by management, review that the risk has been evaluated.	Inquiry, Inspection, and/or observation	1. Risk assessment performed by management
Governance and Oversight	Program Management	1. Inquire with management about the people and change process. 2. Obtain and inspect the formal people and change process.	Inquiry, Inspection, and/or observation	1. Formal people and change process document
Governance and Oversight	Program Management	1. Inquire with management regarding the formal process to address organizational changes. 2. Obtain and inspect the Blockchain Program Charter to confirm that is outlines a formal process to address organizational changes. 3. Inquire with the Blockchain program management team to confirm that the change process is analyzed and evaluated on a monthly basis. 4. Inquire with Blockchain steering committee to confirm that results of the evaluation are reported.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Evidence that evaluation of the change process is evaluated and presented to the Blockchain steering committee.
Governance and Oversight	Program Management	1. Inquire with management on the integration procedure in place for new vendor software. 2. Obtain and inspect the integration plan and review to confirm that the Blockchain program management team	Inquiry, Inspection, and/or observation	1. Integration procedures for vendors
Governance and Oversight	Program Management	1. Inquire with management on the documentation and evaluation of hardware, applications, software and software components related to the Blockchain. 2. Obtain and inspect the formal documentation and evaluation of hardware, applications, software and software components related to the Blockchain. 3. Inspect evidence that the results of the evaluation are presented and reported to the Blockchain Program steering committee.	Inquiry, Inspection, and/or observation	1. Documentation and evaluation of hardware, applications, software and software components related to the Blockchain 2. Evidence of evaluation reported to the Blockchain Program steering committee.
Governance and Oversight	Program Management	1. Inquire with management on policies and procedures to create the functional specifications. 2. Obtain and inspect the policies and procedures to create the functional specifications. 3. Inspect evidence that the process is reviewed and approved on a periodic or as needed basis.	Inquiry, Inspection, and/or observation	1. Policies and procedures to create the functional specifications. 2. Evidence that the process was reviewed and approved.
Governance and Oversight	Program Management	1. Inquire and inspect the Blockchain Program Charter to confirm details regarding the Benefits Management process.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Evidence that the Blockchain Program Charter was reviewed and approved.

TABLE 4-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Governance and Oversight	Project Management	2. Inspect that the Blockchain Program Charter has been reviewed and approved by the Blockchain program steering committee. 1. Inquire with management on the process and appropriateness of resources used to design functional specifications and confirm that they are reviewed by the Blockchain program risk and compliance team. 2. Inspect functional specifications to assure appropriateness of the design and operating effectiveness of controls.	Inquiry, Inspection, and/or observation	1. Functional specifications 2. Evidence that employees involved in the design are appropriate and possess the proper qualifications
Governance and Oversight	Project Management	1. Inquire with management about the training requirements for analysts involved with the functional and/or technical design. 2. Inspect training plan or training materials provided to analysts, including any on-going training.	Inquiry, Inspection, and/or observation	1. Training plan 2. Training materials
Governance and Oversight	Project Management	1. Inquire with management on policies and procedures that provide a description of key Blockchain program management positions, responsibilities and overall organization structure for governance. 2. Obtain and inspect the policies and procedures that provide a description of key Blockchain program management positions, responsibilities and overall organization structure for governance.	Inquiry, Inspection, and/or observation	1. Policies and procedures that provide a description of key Blockchain program management positions, responsibilities and overall organization structure for governance.
Governance and Oversight	Project Management	1. Inquire with management on the reviews performed to test completeness and accuracy of processing for the Blockchain transactions. 2. Obtain and inspect the reviewed performed to test completeness and accuracy of processing for the Blockchain transactions.	Inquiry, Inspection, and/or observation	1. Reviews performed to test completeness and accuracy of processing for the Blockchain transactions.
Governance and Oversight	Leadership Commitment	1. Verify the Blockchain Program Charter has been created and review the overall goals and business objectives. Review the members of the organization who have contributed to the Blockchain Program Charter to confirm appropriate leadership engagement. 2. Inspect the Blockchain Program Charter to ensure the Steering committee has reviewed and approved it.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Meeting minutes from the Steering committee meeting where the Blockchain Program charter was reviewed.
Governance and Oversight	MIS and Metrics	1. Inspect the Blockchain project plan/roadmap to confirm the financial needs are outlined. 2. Inquire with the Blockchain program management to determine there is a formal process to monitor project costs and measure performance in place. 3. Inquire with the Blockchain steering committee to ensure the project costs are reported to them on a monthly basis.	Inquiry, Inspection, and/or observation	1. Blockchain Project Plan/roadmap 2. Evidence of formal process to monitor and report project costs 3. Evidence of performance metrics
Governance and Oversight	MIS and Metrics	1. Obtain daily Blockchain capacity, availability, and performance metrics. 2. Inquire with Blockchain Operational Management to	Inquiry, Inspection, and/or observation	1. Daily Blockchain Capacity, Availability, and Performance Metrics 2. Evidence of daily review of the metrics by the Blockchain Operational Management

TABLE 4-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		determine the criteria for reviewing the metrics daily and inspect the evidence to ensure the metrics are reviewed daily and if there are deviations they are noted, researched and resolved. 3. Inspect the evidence of the metrics to ensure they are reported monthly to the Blockchain Program Steering Committee.		3. Evidence of reporting the metrics to the Blockchain Program Steering Committee
Governance and Oversight	Operational and Capital Expenditure Oversight	1. Inquire with the Blockchain steering committee members to determine criteria for financial needs are included in the Blockchain Program Charter. 2. Inspect the Blockchain Program Charter to ensure the Steering committee has reviewed and approved it. 3. Inspect the Blockchain Project Plan/Roadmap to ensure the financial needs of each individual project work stream is included and outlined.	Inquiry, Inspection, and/or observation	1. Blockchain Program Charter 2. Meeting minutes from the Steering committee meeting where the Blockchain Program charter was reviewed. 3. Blockchain Project Plan/Roadmap 4. Evidence of each individual Blockchain project work stream's financial needs
Governance and Oversight	Operational and Capital Expenditure Oversight	1. Obtain a copy of the organizations process and/or plans for allocating resources and verify it takes the following factors into consideration: people, skills, experience and competence; resources needed for each step of the risk management process; the organization's risk processes, methods and tools to be used for managing risk; documented processes and procedures; information and knowledge management systems; training programs.	Inquiry, Inspection, and/or observation	1. Organizations plans and/or documents for allocation of funds
Governance and Oversight	Operational and Capital Expenditure Oversight	1. Inquire with the control owner and confirm if the organization has processes in place to identify additional expertise needed to improve information security defenses. 2. Determine if the size and quality of the organization's security staff is adequately staffed and structured handle the impact of staff turnover.	Inquiry, Inspection, and/or observation	1. Documentation for the most recent annual budget planning exercise. 2. Evidence that the organization has processes in place to identify additional expertise needed to improve information security defenses. 3. Provide a list the organization's security staff, including their positions and expertise.
Governance and Oversight	Operational and Capital Expenditure Oversight	1. Inquire with management how security is embedded in the project management process/lifecycle. 2. Obtain project methodology or process documentation and validate that it considers security risks as part of the process.	Inquiry, Inspection, and/or observation	1. Project management methodology or process documentation. 2. Population: System extract or register of projects 3. For a sample of projects selected, evidence of risk assessment activities being performed as part of the project management lifecycle. 4. ISMS manual - Description of the security requirements department managers are to include in projects.

[0142] In some embodiments, cybersecurity risk category in the blockchain risk framework covers relevant risks, control objectives and descriptions, testing objectives and procedures, and reporting parameters designed to address assurance and compliance surrounding the cybersecurity and privacy management activities.

[0143] The sub-risk categories, control and testing objectives, test procedures and request lists for Cyber Security risk category are provided below in Tables 5-7. The tables below are formatted in the same manner as tables 2-4 described above, and thus for an explanation of each column below, the corresponding discussion above can be referenced.

TABLE 5

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Cyber Security	Cloud Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-CS1	Without clearly defined roles and responsibilities with cloud service providers and SLA in place, accountability is lost when issues in the relationship arise.	L, M, H
Cyber Security	Cloud Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-CS2	Without clearly defined roles and responsibilities with cloud service providers and SLA in place, accountability is lost when issues in the relationship arise.	L, M, H
Cyber Security	Cloud Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-CS3	Lack of established and implemented safeguards may lead to supply chain information, system component, and information system vulnerabilities	L, M, H
Cyber Security	Cloud Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-CS4	Lack of adherence to the documented production network standards may lead to increased security risk.	L, M, H
Cyber Security	Cloud Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-CS5	Unauthorized access of information stored in shared resources can result in inappropriate access, changes or loss.	L, M, H
Cyber Security	Data Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DS1	Data exchanged through communication facilities may be intercepted and accessed by unauthorized agents within or outside the organizations network.	L, M, H
Cyber Security	Data Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DS2	Procedures which do not facilitate appropriately classifying, labeling and handling information based on its value, business and legal requirements may expose information to deliberate or accidental misuse.	L, M, H
Cyber Security	Data Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DS3	Lack of controls to protect information can lead to data leaks or exposures that threaten the organization's reputation and could lead to litigation.	L, M, H
Cyber Security	Data Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DS4	Lack of alignment with the organization's risk strategy and risk appetite in the protection of data may compromise the confidentiality, integrity and availability of information in Blockchain systems.	L, M, H
Cyber Security	Data Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DS5	Failure to establish and communicate policies and procedures for information security relevant to Blockchain use case may result in gaps in security capabilities needed to reduce the organization's cyber risk exposure in accordance with its risk appetite.	L, M, H
Cyber Security	Data Privacy	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DP1	Lack of controls to protect information can lead to data privacy or exposures that threaten the organization's reputation and could lead to litigation.	L, M, H

TABLE 5-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Cyber Security	Data Privacy	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DP2	Failure to establish and communicate policies and procedures for privacy may result in gaps in privacy capabilities needed to reduce the organization's privacy risk exposure in accordance with its risk appetite.	L, M, H
Cyber Security	Data Privacy	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-DP3	Lack of a privacy policy may increase the risk that information is disclosed or used without the owner's consent, resulting in litigation and reputational damage.	L, M, H
Cyber Security	Penetration Testing	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PT1	Inadequately defined processes for technical vulnerability management and ineffective testing or detection of vulnerabilities may result in inappropriate or unauthorized access to information.	L, M, H
Cyber Security	Network Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-NS1	Failure to protect network perimeter may result in unauthorized access.	L, M, H
Cyber Security	Patch and Vulnerability Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PVM1	Lack of proper information system management flaw management may result in security vulnerabilities	L, M, H
Cyber Security	Patch and Vulnerability Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PVM2	Inadequately defined processes for technical vulnerability management and ineffective testing or detection of vulnerabilities may result in inappropriate or unauthorized access to information.	L, M, H
Cyber Security	Patch and Vulnerability Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PVM3	Inadequate processes for system updates and patch management may result in compromise of system security due to the latest updates and patches not being installed in a timely manner.	L, M, H
Cyber Security	Threat Detection	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-TD1	The lack of logging mechanisms results in the inability to track unauthorized activity.	L, M, H
Cyber Security	Threat Detection	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-TD2	Inadequate processes for logging and monitoring Blockchain system activities may result in unauthorized information processing activities going undetected.	L, M, H
Cyber Security	Threat Detection	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-TD3	Lack of monitoring mechanisms may result in breaches and sensitive data exposure.	L, M, H
Cyber Security	Threat Response	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-TR1	Absence of a formalized Security Incident Response Program may result in uncoordinated processes in response to a security incident.	L, M, H

TABLE 5-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Cyber Security	Threat Response	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-TR2	Absence of a formalized Security Incident Response Program may result in uncoordinated processes in response to a security incident.	L, M, H
Cyber Security	Threat Response	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-TR3	Incidents that are not controlled may lead to pervasive problems throughout the organization.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS1	In adequate security measures within the development lifecycle of information systems may lead to unauthorized changes.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS2	Systems with vulnerabilities may be developed and implemented in the production environment.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS3	Systems with vulnerabilities may be developed and implemented in the production environment.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS4	Systems with vulnerabilities may be developed and implemented in the production environment.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS5	Untested changes may lead to interruption and/or unintended consequences to the organization.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS6	Insecure coding practices, especially within the application layer, can introduce security vulnerabilities and increase the risk to internal and external threats.	L, M, H
Cyber Security	Programming Security	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-PS7	Use of production or live data for development and/or testing purposes can cause unintended corruption or manipulation of the data.	L, M, H
Cyber Security	Smart Contracts	Strategic, Operational, Financial, Compliance, Legal, or Reputational	CS-SM1	Input validation mechanisms for fields and records are not in place, creating the risk of failed conversion of data from input to outputs	L, M, H

TABLE 6

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
Cyber Security	Cloud Security	Contracts with the Cloud Service provider specify	Contracts between the Cloud Service Provider and the	In-scope

TABLE 6-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
		required information security and processing measures.	organization specifies appropriate security and processing measures, and establish data are not processed for any non-specified purpose without approval.	
Cyber Security	Cloud Security	Cloud service providers and understand roles & responsibilities, including requirements to address information security risks for confidentiality, and the secure transfer of information.	A contract is signed between both parties detailing the roles and responsibilities of each party, including information security requirements, confidentiality/non-disclosure agreements, obligations, and the obligations of employees and subcontractors.	In-scope
Cyber Security	Cloud Security	The organization employs measures to protect against supply chain threats from cloud service providers that impact the Blockchain information system, system component, or information system service.	Organizational safeguards such as the identification, management and reduction of vulnerabilities are employed to protect the supply chain against information system, system components, and information system services threats.	In-scope
Cyber Security	Cloud Security	Cloud services are secured using standard network protocols, and interoperability and portability standards are available to customers.	Secure standardized network protocols are in place to manage the cloud service and documentation detailing relevant interoperability and portability standards are made available to customers.	In-scope
Cyber Security	Cloud Security	Blockchain systems are configured to prevent unauthorized access and transfer of information through shared system resources.	The Blockchain system are configured to prevents unauthorized and unintended information transfer via shared system resources. Re-use of shared resources is monitored and controlled to prevent unauthorized access.	In-scope
Cyber Security	Data Security	Data exchange is controlled, encrypted, and protected while the information is at rest or transferred between systems.	Formal information exchange requirements have been established and Blockchain systems are configured to protect the exchange of information through the use of all types of communication facilities and interfaces.	In-scope
Cyber Security	Data Security	Resources (e.g., hardware, devices, data, and software) are classified based on their criticality and business value.	Information assets (e.g., hardware, devices, data, and software) are classified based on their criticality and sensitivity. Information is handled and protected in accordance with its classification, criticality, and business value to the organization.	In-scope
Cyber Security	Data Security	Protections against data leaks are implemented.	The organization employs data mining prevention and detection techniques for data storage objects supporting Blockchain use case to adequately detect and protect against data mining.	In-scope
Cyber Security	Data Security	Data in Blockchain systems is protected according to the risk strategy and risk appetite of the organization.	Information and records (data) in Blockchain systems are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	In-scope
Cyber Security	Data Security	Policies and procedures for direction and support of organizational systems and applications exist in	Information security policies and applicable procedures have been formally documented in accordance with organization's	In-scope

TABLE 6-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
		accordance with business requirements and relevant laws and regulations.	risk objectives, applicable legal and regulatory requirements, have been approved by Management, and have been communicated to all employees and relevant external parties. The policies and procedures are reviewed on a periodic basis based on changes to the internal and external environment and to support management's objective of continuous improvement of the organization's information security capabilities.	
Cyber Security	Data Privacy	Protections against data privacy are implemented in Blockchain systems to prevent unauthorized view or exposures of confidential information.	Unauthorized leaks of data, specifically PII and PHI, are prevented or detected. The processor prevents or monitors for unauthorized leakage of data, or enables the capability for its customers to prevent or monitor for the unauthorized leakage of data. DLP tools monitor outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at interior points within the system (e.g., subsystems, subnetworks) to detect covert exfiltration of information.	In-scope
Cyber Security	Data Privacy	Policies and procedures for direction and support of information privacy exist in accordance with business requirements and relevant laws and regulations.	Information security policies and procedures around information privacy are documented and available to personnel on accessible resources. The policies and procedures are reviewed/updated periodically.	In-scope
Cyber Security	Data Privacy	The organization discloses how it uses PII in accordance with the public notice requirement.	The privacy policy discloses the ways that the organization gathers, uses, discloses, and manages PII. It fulfills the legal requirement to protect PII and declares the company's policy on how it collects, stores, and releases the PII it collects, and inform whether PII is kept confidential, shared with partners, or sold to other firms or enterprises.	In-scope
Cyber Security	Penetration Testing	Asset vulnerabilities are monitored, identified and documented.	Penetration tests of the production environment are performed on a periodic basis or after any significant infrastructure or application upgrade or modification. Remediation plans are developed to address the risks. The penetration testing methodology aligns with industry standard practices and covers application-layer and network-layer. Testing is performed both inside and outside the network. Test results are retained for a specific period of time.	In-scope
Cyber Security	Network Security	Network perimeter is protected using managed boundary protection devices.	Firewalls and routers are configured to: Restrict inbound and outbound traffic to that which is necessary (e.g., deny by default, permit by exception)	In-scope

TABLE 6-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
			Restrict connections between untrusted networks and any system components Fail securely in case of an operational failure Permit only authorized traffic between wireless environment and cardholder data environment Firewall and router configuration standards are in place to define network connection requirements. The firewall and router configuration standards include the following: Business justification and approval for use of all services, protocols, and ports allowed, including security features implemented for those protocols considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP v1 and v2) Roles and responsibilities for management of network components. Exceptions to the standards are documented and reviewed on a periodic basis. There is a formal process for testing and approval of all network connections and changes to firewall and router configurations. For any public-facing Web applications, an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) has been installed, to continually check all traffic. A DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Inbound Internet traffic is limited to IP addresses within the DMZ. A firewall is required at each internet connection and between any DMZ and the intranet. The information system routes internal communications traffic to external networks through authenticated proxy servers (e.g., web content filters with a defined list of authorized and unauthorized websites) Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the network.	
Cyber Security	Patch and Vulnerability Management	Identify, report and correct information systems flaws in a timely manner.	A vulnerability management program exists to identify and manage vulnerabilities in a centralized, streamlined and organized manner. The technical vulnerability management program is evaluated on a quarterly basis.	In-scope
Cyber Security	Patch and Vulnerability Management	System vulnerability scanning is performed to identify threats.	Vulnerability scans and rescans are performed by qualified personnel on both external and internal facing production	In-scope

TABLE 6-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
			systems using internal scanning resources on a periodic basis and when new vulnerabilities affecting the systems are known. Commercial and proprietary vulnerability scanning tools are configured to identify vulnerabilities. Identified critical vulnerabilities are remediated timely. Remediation status is monitored and non-compliance is escalated.	
Cyber Security	Patch and Vulnerability Management	System vulnerabilities are mitigated through patches.	A patch management program exists to incorporate, test, and implement firmware updates and patches in a timely fashion	In-scope
Cyber Security	Threat Detection	Logging mechanisms and the ability to track activity is established, tracked, and monitored.	Logging mechanisms are configured to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity: The following events are tracked: General user access and activities Root access and activities Access to audit logs Invalid access attempts Changes to identification and authentication mechanisms Changes to or elevation of privilege access rights Initialization, stopping, or pausing of the audit logs Creation and deletion of system-level objects exceptions system faults information security events system/network events For each event, the following details are captured: Type of event Time Where the event occurred Source of the event Outcome of the event (success/failure) Unique identity of individuals associated with the event Identity or name of affected data, system component, or resource.	In-scope
Cyber Security	Threat Detection	Risk-based monitoring to detect unauthorized connections, devices, events, and network services.	Risk based monitoring is performed using automated tools (e.g., SIEM tools) to detect unauthorized connections, devices, events, and network services. Automated tools are used to perform analysis of events. Monitoring is performed in compliance with legal and regulatory requirements. Events are analyzed to understand attack targets and methods.	In-scope
Cyber Security	Threat Detection	Automated mechanisms communicate security alert and advisory information following indicators of compromise.	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization when indicators of compromise are found.	In-scope

TABLE 6-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
Cyber Security	Threat Response	Incident response program is in place to provide timely and effective response to user requests and resolution to all types of incidents.	A formal security incident response program is established to respond, report, escalate and treat breaches and reported security events or incidents. A comprehensive incident response plan exists to identify, manage, respond to, and recover from security (e.g., system breach) and IT operational (e.g., process errors) incidents and is communicated to appropriate stakeholders. The incident response plan is reviewed and modified on a periodic basis.	In-scope
Cyber Security	Threat Response	Incident response program is in place to provide timely and effective response to user requests and resolution to all types of incidents.	The organization develops, documents, and disseminate an incident response policy. The policies and procedures are reviewed and updated, at a minimum, on an annual basis.	In-scope
Cyber Security	Threat Response	Security incidents are contained and mitigated to prevent additional impact to business operations and loss of information.	Incident alert thresholds have been established and all incident detection tools have been calibrated with the thresholds. Incidents (operational or IT security) are identified, logged, documented, reported to different levels within the organization, and tracked to closure.	In-scope
Cyber Security	Programming Security	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	The organization establishes and appropriately protects secure development environments for system development and integration efforts that cover the entire system development lifecycle.	In-scope
Cyber Security	Programming Security	Systems are developed securely.	An established system development lifecycle (SDLC) process and methodology is in place, documented, maintained, and applied for system and software design, acquisition, implementation, configuration, integration, testing, modification, and maintenance. The process also specifies the tools to be used for system development. The secure SDLC process, methodology, and tools are reviewed on a periodic basis.	In-scope
Cyber Security	Programming Security	Systems are developed securely.	The SDLC process is inclusive of information security considerations. Security roles and responsibilities during the development lifecycle have been defined. Organization's information security team and the risk management methodology is appropriately integrated into the SDLC process.	In-scope
Cyber Security	Programming Security	Systems are developed securely.	The Security team coordinates with the system developers to define and develop system security plans. System security plans that outline the security requirements are documented and maintained for information systems. The plans are communicated to relevant and	In-scope

TABLE 6-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD - As per engagement)
Cyber Security	Programming Security	Test data should be selected carefully, protected and controlled.	authorized internal and external users. Test data shall be selected carefully, protected and controlled. Operational data is protected when used for test purposes. Test data and accounts are removed from system components before the system becomes active/goes into production.	In-scope
Cyber Security	Programming Security	Applications should be developed using secure coding guidelines, in order to address common coding vulnerabilities.	Developers employ secure coding guidelines to software and mobile applications. Developers are trained at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. (Refer the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.)	In-scope
Cyber Security	Programming Security	Production data are not used for testing or development.	Production data are not used for testing or development.	In-scope

TABLE 7

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Cyber Security	Cloud Security	1. Obtain and review contracts with cloud service providers to determine whether contracts include information security provisions to protect against cybersecurity and data security/data privacy risks.	Inquiry, Inspection, and/or observation	1. Contracts with cloud service providers.
Cyber Security	Cloud Security	1. Inquire with the control owner and determine if all relevant information security requirements are established and agreed with each supplier/vendor that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. 2. Inspect a sample of agreements and validate that they include the following: Roles and responsibilities Service definitions and SLAs Information security controls to be implemented System functions, ports, protocols, and other services required for the use of such services. Requirement to provide notification of changes to services or controls Requirement to provide notification of 3rd party personnel transfers and terminations Laws and regulations that the third party needs to comply with Penalties or claw back clauses Locations that they can provide services out of Limitations on data storage locations Incident management procedures Breach notification Right to audit Limitations and constraints of access Termination conditions Data disposal/return upon termination Ownership of products after development Quality requirements Security training requirements for employees Business-critical or customer-impacting application design, development, and deployment	Inquiry, Inspection, and/or observation	1. Policies and procedures related to contracts between the organization and suppliers/vendors. 2. Evidence of agreements between the organization and suppliers/vendors. 3. Population - System generated list of contract amendments during the audit period. 2. Evidence that a new customer or vendor contract addendum or new vendor contract was signed for a sample of changes to confidentiality commitments requiring customer or vendor notification.

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		Business-critical or customer-impacting system designs and configurations design, development, and deployment Business-critical or customer-impacting infrastructure network and system components design, development, and deployment IT Governance and service management policies and procedures Customer requirements policies and procedures for service-to-service application Customer requirements policies and procedures for information processing, interoperability, and portability for application development Customer requirements policies and procedures for information exchange, usage, and integrity persistence 3. Inquire with the control owner to determine if confidentiality commitments with vendors/suppliers are changed during the normal course of business. If changes to confidentiality commitments are required, verify through inquiry with the control owner that a vendor contract addendum or new vendor contract is established. 4. Obtain the population of tickets related changes to confidentiality commitments requiring vendor/supplier notification. 5. For a sample from the above #4 population, verify that a vendor contract addendum or new vendor contract was signed.		
Cyber Security	Cloud Security	1. Inquire with the control owners and observe the organization's processes for defining the safeguards that protect systems against supply chain threats, as well as the automated mechanisms supporting supply chain threat safeguards. Determine if the organization protects its information systems, system components, or information system services from supply chain threats by implementing security safeguards as defined by the information security strategy. 2. Inspect system and services acquisition policies and procedures, procedures for the integration of security requirements into the development process, and supporting documentation to determine the following: if the organization defines the security safeguards to implement as protection to information systems, system components, or system services against supply chain threats. if the organization assures reasonable information security across their information supply chain by performing annual reviews, including reviews of all partners and third-party providers that the organization's information supply chain depends on. 3. Inspect service delivery agreements and determine the following: that third party service providers are required to demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery-level agreements defined. that third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Inquiry, Inspection, and/or observation	1. System and services acquisition policies and procedures. 2. Procedures for the integration of security requirements into the development process. 3. Service delivery agreements
Cyber Security	Cloud Security	1. Inquire with the control owner and determine the following: The organization uses secure standardized network protocols (e.g., non-clear text and authenticated) to manage services.	Inquiry, Inspection, and/or observation	1. Cloud service policies and procedures

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		The organization makes available to customers documentation detailing relevant interoperability and portability standards. If the organization, as a cloud service provider, uses an industry-recognized virtualization platform and standard virtualization format to help ensure interoperability. if any custom changes made to any hypervisor in use and to all solution-specific virtualization hooks are documented and made available to customers for review. 2. Inspect cloud service security policies and procedures and determine the following: The organization uses secure standardized network protocols (e.g., non-clear text and authenticated) to manage services. The organization makes available to customers documentation detailing relevant interoperability and portability standards The industry-recognized virtualization platforms and standard virtualization formats are used to help ensure interoperability. The custom changes made to any hypervisor in use and to all solution-specific virtualization hooks shall be documented and made available to customers for review.		
Cyber Security	Cloud Security	1. Determine through inquiry with control owner whether processes are in place to remove any previous content from shared resources when it is being allocated for reuse to new set of users.	Inquiry, Inspection, and/or observation	
Cyber Security	Data Security	1. Confirm the following have been addressed within policies and procedures for the use of electronic communication facilities: procedures designed to protect exchanged information from interception, copying, modification, incorrect routing, and destruction procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications procedures for protecting communicated sensitive electronic information that is in the form of an attachment, policy or guidelines outlining acceptable use of electronic communication facilities procedures for the use of wireless communications, employee, contractor and any other users' responsibilities not to compromise the organization, use of cryptographic techniques, retention and disposal guidelines for all business correspondence in accordance with relevant national and local legislation and regulations, not leaving sensitive or critical information on printing facilities controls and restrictions associated with the forwarding of communication facilities, not leaving messages containing sensitive information on answering machines, reminding personnel not to register demographic data in any software to avoid collection for unauthorized use.	Inquiry, Inspection, and/or observation	
Cyber Security	Data Security	1. Inquire with the control owner to determine whether the business value of each information asset has been established and documented. 2. Inquire with the control owner and obtain the Data Classification Guide to determine if classification schemes and procedures for handling, processing, storing and communicating information consistent with its classification, criticality, and business value are documented. 3. Inquire with the control owner to determine whether critical assets have been identified and documented.	Inquiry, Inspection, and/or observation	1. Data Classification Policy and procedures. 2. Evidence that critical assets have been identified and documented. 3. Evidence that the security categorization decision is reviewed and approved by the authorizing official or

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		4. Determine whether logical and physical protection levels offered for data stored in databases, removable media, etc. is in alignment with the classification level of the data. 5. Inspect if the security classification decision is reviewed and approved by an authorizing official or authorizing official designated representative. 6. Inspect if all media has been classified so that the sensitivity of the data can be determined. 7. Validate whether all assets have been assigned an owner.		authorizing official designated representative. 4. Sample of media to determine whether they have been classified so that sensitivity of the data can be determined. 5. Evidence that assets are assigned to an owner.
Cyber Security	Data Security	1. Obtain and inspect relevant documents to determine if the organization implements various data mining protection program for the information system, system component, or information system service. For example: limiting the types of responses provided to database queries; limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and notifying organizational personnel when atypical database queries or accesses occur. 2. Inquire with control owners to determine that established policies and procedures are in place and define data mining prevention and detection techniques, define that data storage objects are to be protected, and define the organization-defined techniques for data mining prevention and detection techniques for data storage 3. Inspect the organizations Account Management Procedures, Information Security Technical Standard, Access Management Procedures, Database Access Management Procedure, and determine that the established policies and procedures outline and define data mining prevention and detection techniques and storage protection:	Inquiry, Inspection, and/or observation	1. Account Management Procedures. 2. Information Security technical standard. 3. Access Management procedures. 4. Database access management procedures.
Cyber Security	Data Security	1. Obtain and inspect relevant documents to determine if the organization aligns with its risk strategy and risk appetite when implementing data protection measures. 2. Inquire with control owners to determine that policies and procedures are in place that prescribe data protection measures based on information classification and risk ranking.	Inquiry, Inspection, and/or observation	1. Relevant policies and procedures. 2. Evidence of review (e.g., sign off/approvals documented in policy revisions history). 3. Screenshot of the location of policies and procedures showing that they are available to company personnel. 4. Evidence showing that policies are part of annual security awareness.
Cyber Security	Data Security	1. Inquire with the control owner and determine if information security policies and procedures are documented, available and communicated to personnel on accessible resources (internal network, shared drive, etc.). 2. Inspect policies and procedures to confirm if they are reviewed/updated at least annually or more frequently if required based on changes in the environment. 3. Security policies and operational procedures should address organization-determined areas and best practices, examples include: Business Continuity/Disaster Recovery; Data Protection/DLP; Access Management; Vendor Management; Physical Security;	Inquiry, Inspection, and/or observation	1. Relevant policies and procedures. 2. Evidence of review (e.g., sign off/approvals documented in policy revisions history). 3. Screenshot of the location of policies and procedures showing that they are available to company personnel. 4. Evidence showing that policies are part of annual security awareness.

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Cyber Security	Data Privacy	SDLC; Security Awareness training; Mobile device management; Legal/regulatory requirements; System/service acquisition; User agreements. Incident Management Network Security Configuration Management Application Security Cryptography and Key Lifecycle Management Risk Assessment and Treatment Data confidentiality, integrity and availability across multiple system interfaces, jurisdictions, business functions	Inquiry, Inspection, and/or observation	Special Note: Personally identifiable information (“PII”) and Protected Health Information (“PHI”) fall under “Customer Data” and is thus subjected to the company’s data classification schema and controls. 1. Data Classification and Protection policies and procedures. 2. Policies and procedures related to Data Loss Prevention and the handling of customer data. 3. Evidence of the organizations capabilities to prevent or monitor data leaks. 4. Evidence that data loss prevention processes and procedures are aligned with legislative, regulatory, or contractual obligations.
		1. Inquire of management and obtain evidence to validate whether the organization has capabilities to prevent or monitor data leaks. 2. Determine if the organization performs activities to analyze potential opportunities for covert channels. If so, determine if testing is performed to identify exploitable channels and the bandwidth associated with those channels. 3. Inquire with the control owner to determine if the above-mentioned capabilities in test procedure #1 are aligned with legislative, regulatory, or contractual obligations, 4. Obtain and inspect policies, procedures, and other supporting documentation to validate whether the aforementioned capabilities in test procedure #1 are in place to enable the organization to meet their obligations to customers in accordance with contractual requirements.		
Cyber Security	Data Privacy	[General Privacy Requirements; Notice, Choice, Consent] 1. Inquire with the control owner and determine where information security policies and procedures are documented and available to personnel with access to PII on accessible resources (internal network, shared drive, etc.). 2. Review policies and procedures to confirm they are reviewed/updated at least annually or more frequently if required based on changes in the environment, 3. Inspect the information security policies on the company’s internal network and determine they are available and communicated to company personnel with access to PII and include security roles, responsibilities, and procedures. Specifically, privacy policies and operational procedures for the confidentiality and non-disclosure agreements. [Storage Location of PII] 1. Inquire with the control owner and determine that the organization has documented data localization policies and procedures available to personnel on accessible resources (company intranet, shared drive). 2. Inspect the data localization policy on the company’s internal network and determine they	Inquiry, Inspection, and/or observation	1. Privacy policies and procedures regarding confidentiality and non-disclosures. 2. ISMS manual (Executive Leadership, CTO) 3. Evidence to demonstrate that documents are available to personnel with access to PII on accessible resources such as internal network, shared drive, etc. 4. Data localization policy 5. List of countries that might have access to the organization’s customers’ PII. 6. Evidence documenting the review and update procedures performed

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		are available and communicated to company personnel and address that the organization documents and makes available the countries where PII might be stored as required. 3. Inspect policies and procedures to confirm they are reviewed and updated based on changes in the environment. 4. Obtain and inspect the list of countries that might have access to the organization's customers' PII. 5. Obtain and inspect the list of countries to determine the review and update procedures performed by the organization to ensure that the listing is accurate and up to date.		by the organization to ensure that the list of countries is accurate and up to date.
Cyber Security	Data Privacy	1. Inquire with control owners to understand where, within the organization's data policies, the expectations for the return, transfer, and/or destruction of PII is defined. In addition, determine how this is communicated to the customers (i.e. website, contract/amendments). 2. Obtain and observe the appropriate documentation (i.e. data policy) showing the expectations for the return, transfer, and/or destruction of PII by the organization for the customers.	Inquiry, Inspection, and/or observation	1. Data privacy policy showing the expectations for the return, transfer, and/or destruction of PII by the organization for the customers. 2. Data Classification policy for restricted class protection.
Cyber Security	Penetration Testing	1. Inquire with the control owner to determine whether penetration tests are performed on a periodic basis and remediation plans are developed to address the risks. 2. Inspect the results of the most recent penetration test to determine whether it was completed within the organization-specified time period and performed by an independent penetration agent or team. 3. Inspect ticket details and supporting documentation for a sample of risks identified in the most recent penetration test to determine whether the risks were remediated or were being actively worked to remediation.	Inquiry, Inspection, and/or observation	1. Copy of most recent penetration test and penetration test methodology utilized. 2. Population of risks from most recent penetration test. 3. For a sample of risks, please provide ticket/supporting details to document remediation. 4. Please provide evidence that both external and internal penetration tests are performed at least annually and after any significant infrastructure or application modification.
Cyber Security	Network Security	1. Inspect documented procedures and determine that there is a formal process for testing and approval of all: Network connections; and Changes to firewall and router configurations 2. Obtain a population of changes to network connections, firewalls, and router configurations. 3. Select samples and obtain tickets. 4. Inspect tickets from selected sample to validate that changes to network connections, firewalls, and router configurations were tested and approved. 5. Validate whether the network diagrams are updated if there is a change in the network connection.	Inquiry, Inspection, and/or observation	1. Firewall and router configuration standards 2. Evidence of firewall rule review. 3. Router rule sets 4. Network diagrams 5. Population of changes to network connections, firewalls, and router configurations. 6. Tickets for samples of changes to network connections, firewalls, and router configurations. 7. Population of firewall reviews, from which a sample will be selected. 8. Evidence of firewall reviews for the sample selected.
Cyber Security	Patch and Vulnerability Management	1. Inquire with the control owner to determine if a formal vulnerability management program exists and tools are in place to detect, report, and correct vulnerabilities.	Inquiry, Inspection, and/or observation	1. Policies and procedures related to vulnerability management.

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		2. Determine if there is a formally documented vulnerability management methodology and procedures. 3. Through interviews with the control owner, inspection of reports, determine whether system vulnerabilities are identified and tracked. 4. Inspect tickets to determine if the vulnerability was ranked, worked to resolution based on criticality, authorized, tested, and approved prior to implementation into production. 5. Verify whether the program is evaluated on a quarterly basis.		2. Population of vulnerability/patch tickets. 3. Sample evidence of ticket resolution including risk ranking. 4. Information Security Policies and procedures.
Cyber Security	Patch and Vulnerability Management	1. Inquire with the control owner and determine if vulnerability scans were performed on both external and internal facing production systems using internal scanning resources on an organization-defined frequency. 2. Inspect the internal scanning resource configurations and determine vulnerability scans were scheduled to run with an appropriate frequency and were configured to run against internal and external IP ranges. 3. Inspect the vulnerability scan report for a sample of weeks and determine an internal and external vulnerability scan was completed in accordance with the configured schedule. 4. Inspect if the organization performs privileged/authenticated vulnerability scans 5. Inspect if the organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked). 6. Inspect if the organization employs vulnerability scanning procedures that updates the information system vulnerabilities scanned.	Inquiry, Inspection, and/or observation	1. Evidence that vulnerability scans were performed on both external and internal facing production systems using internal scanning resources. 2. Scanning resource configuration. 3. Reference of internal IPs from a source that is independent from the team responsible for vulnerability scanning 4. Internal and external vulnerability scan reports for the for the selected weeks (to be specified).
Cyber Security	Patch and Vulnerability Management	1. Determine the number of vulnerabilities identified. 2. Validate that patch management process is initiated to address the known vulnerabilities. 3. Validate that patch is tested and applied timely to mitigate the known vulnerabilities.	Inquiry, Inspection, and/or observation	1. Obtain a listing of application systems with vulnerabilities. 2. Obtain a listing of patches deployed to address identified vulnerabilities in a timely manner. 3. Obtain evidence showing that the patches were tested before deployed into production
Cyber Security	Threat Detection	1. Inquire with the control owners and inspect evidence to validate whether or not the organization performs logging related to both unauthorized actions and access. The following items are examples of logging mechanisms that should be in place: Action-related logging events: all changes, additions, or deletions to any account with root or administrative privileges; Initialization, stopping, or pausing of audit logs; creation and deletion of system level objects; creation, modification, enabling, disabling, and removing of accounts; initialization and the stopping or pausing of audit logs. system security configuration changes activation and de-activation of protection systems (e.g., A/V and IDS) management activities, system and application startup/shutdown/errors, file changes, and security policy changes. Access-related logging events: successful and unsuccessful account logon events;	Inquiry, Inspection, and/or observation	1. System generated list of production servers and network devices as of present day with source, filter/query details, etc. 2. Log configurations for a sample of production servers and network devices. 3. Evidence that the organization performs logging related to both unauthorized actions and access. 4. Policies and procedures related to access control, account management, audit and accountability, storage engineering, and audit record content. 5. Evidence that the organization

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		all individual access to cardholder data; access to all audit trails; elevation of privileges. 2. Inquire of management and inspect evidence to validate whether the organization: includes user identification, event type, date and time stamp, indication of success or failure, event origination, and identity of affected data, system component, or resources in log entries; monitors information system accounts for abnormal usage and activity; reports abnormal usage and activity on information system accounts to specified personnel; configures information systems to generate audit records that contain information on what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of individuals associated with the event; continuously writes logs from production servers, network devices, databases and storage management hosts to system logs and forwards them to the logging and alerting system in real-time in order to provide backup media for records other than the audited system; configures the information system to provide the capability to generate audit records for defined auditable events for specified information system components; configures the information system to allow specified personnel to select which auditable events should be audited by specific system components; configures the information system to provide capabilities for specified individuals to change the performed audits on information system components based on defined selectable event criteria within specified thresholds. 3. Inspect policies and procedures around access control, account management, audit and accountability, storage engineering, and audit record content and validate whether or not the organization. defines abnormal information system account usage and the personnel to be notified upon the identification of abnormal system usage; configures the information system to generate audit records that contain information on what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of individuals associated with the event; defines the additional detailed information required to be included in audit records that the information system generates; defines the information system components that provide audit record generating capabilities for defined auditable events; defines the personnel whom are allowed to select which auditable events are to be audited by specified information system components, and change the validating performed on specified information system components; defines the information system components that validating is performed on; defines the time thresholds that must be met for specified individuals to change the audit functions performed on information system components; defines the event criteria that can be selected by specified individuals or roles to support the capabilities of changing audit functions		configures information systems to allocate storage space for the retention of audit records.

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Cyber Security	Threat Detection	performed on information system components; continuously writes logs from production servers, network devices, databases and storage management hosts to system logs and forwards them to the logging and alerting system in real-time in order to provide backup media for records other than the audited system 4. Inspect audit record storage capacity related to information system configuration settings and determine that the organization configures information systems to allocate storage space for the retention of audit records and that it is sufficient in accordance to defined requirements. 1. Inquire with the control owner to determine if documented procedures for monitoring are in place to detect vulnerabilities, indicators of potential attacks in accordance with (organization-defined) monitoring objectives, unauthorized local, network, and remote connections; 2. Inquire with the control owner to verify whether monitoring tools are implemented in high risk systems and environments to detect anomalous events and activities: Inbound and outbound communications Internal system activities, including unauthorized system use and transactions Unauthorized connections Unauthorized users Unauthorized devices Unauthorized software Unauthorized remote access connections 3. Verify whether action is taken as part of incident response and vulnerability management plan when anomalous events are detected 4. Inspect the monitoring tools to verify their configuration and validate whether they are configured to detect anomalous events.	Inquiry, Inspection, and/or observation	1. Evidence that the organization monitors the Blockchain information system to detect unauthorized/ malicious activity. 2. Provide a list of tools and processes in place to monitor the Blockchain information system and their configurations. 3. Provide a system generated list of vulnerability tickets for the period under review, from which a sample will be selected. 4. Provide the internal tickets from the selected sample.
		1. Inquire with management to determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization. 2. Inspection information security policies to determine if the organization has defined requirements regarding automated mechanisms to make security alert and advisory information available throughout the organization. 3. Inspect organizational processes in place for defining, receiving, generating, and disseminating security alerts and advisories, including automated mechanisms supporting and/or implementing dissemination of security alerts and advisories.		
		1. Verify that a formal incident response program exists and includes formally defined roles and responsibilities, an incident response plan, and resources to support incident response. 2. Obtain the copy of the incident response plan. Verify that it is formally documented and has been approved by a senior Management executive. 3. Validate that the incident response plan document has been recently (within the last year) reviewed and the latest plan has been shared with and communicated to personnel with incident response responsibilities. 4. Verify whether the incident response plans covers both IT operational and security incidents. 5. Verify that the incident response plan contains the following: Roles and responsibilities, and structure and organization of the incident response capability; Incident response process flows and procedures		

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		that include steps for preparation, detection and analysis, containment, eradication, and recovery; Defines reportable incidents and incident classification; Incident communication and notification; Analysis of legal requirements for reporting compromises; Provides metrics for measuring the incident response capability within the organization; Defines the resources and management support needed to effectively maintain and mature an incident response capability; System and data recovery; Data backup processes. 6. Verify if the incident response plan is periodically updated to address system/organizational changes or problems encountered or lessons learned during plan implementation, execution, training, or testing. 7. Review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.		
Cyber Security	Threat Response	1. Inquire with control owner to determine if the organization develops, documents, and disseminate an incident response policy. 2. Examine the incident response plan to determine if an incident response policy exists and whether the policy address the specific purpose, scope, roles and responsibilities, management commitment, and compliance. 3. Examine the information security policies and procedures (see evidence), CSIRT Incident Response Plan, Security Incident Response Process, Corporate Critical Incident Process and determine if the incident response procedures are disseminated to appropriate personnel. 4. Observe location of incident response plan on the organization intranet (or other location) to determine how the incident response policies are disseminated. 5. Examine the incident response plan to determine if the organization has reviewed and updated on an annual basis.	Inquiry, Inspection, and/or observation	1. CSIRT Incident Response Plan 2. Security Incident Response Process 3. Corporate Critical Incident Process 4. Information Security Policies 5. Crisis Management Team Plan
Cyber Security	Threat Response	1. Inquired of the control owner to determine whether security incidents were tracked and documented from initiation through closure. 2. Obtain a listing of incidents for the period under review and select an appropriate number of samples. 3. Obtain tickets or documentation to validate that the incidents were documented (categorized/prioritized), reviewed, tracked and resolved in a timely manner and includes the following details: The identified solutions or workaround are documented, applied and tested, and recovery actions are performed to restore the IT-related service. The satisfactory resolution of incidents and/or request fulfillment is verified and is closed. 4. Determine whether incident thresholds have been established and whether the tools have been calibrated with the thresholds.	Inquiry, Inspection, and/or observation	1. Listing of recent incidents for the period under review and parameters/query used to generate the report. 2. Documentation of incident containment and mitigation, such as IT tickets.
Cyber Security	Programming Security	1. Inquire with the control owner to determine whether the organization establishes guidelines for the secure development environment for critical systems. 2. Inspect the information security policies to determine whether the policies outline guidance for technical roles and secure development environment for critical systems. 3. Validate whether management reviewed the policy within the past 12 months and communicated it to employees.	Inquiry, Inspection, and/or observation	1. Information Security Policies containing technical roles that address development activities, and established guidelines for the secure development environment for critical systems.

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Cyber Security	Programming Security	4. Review the secure development standards to validate whether appropriate measures have been described for security of development environments. 5. Review the access list for a sample of development environments and validate whether the access has been approved. Also validate whether any non-developers have access to the development environment.	Inquiry, Inspection, and/or observation	2. Evidence that management reviewed the Information Security Policies within the past 12 months and communicated it to employees.
		1. Inquire with control owner to whether an established system development lifecycle process is in place, documented, maintained, and applied for all system and software design, acquisition, implementation, configuration, integration, testing, modification, and maintenance. 2. Obtain and inspect SDLC policies and procedures to determine whether an established system development lifecycle process is documented. 3. Verify whether security requirements for information systems and information services are identified as part of SDLC efforts, business process re-design, etc.		1. SDLC policies and procedures. 2. Evidence that an established system development lifecycle process is in place, documented, maintained. 3. Security requirements for information systems and information services are identified
Cyber Security	Programming Security	1. Obtain the SDLC process/methodology documentation and verify whether it specifies that the developers should consider information security during the requirements gathering, high level design, low level design, development, and systems integration phases of developing an information system. 2. Verify whether the SDLC process/methodology documentation specifies whether the testing phase should include security testing of information systems. 3. Verify that during the functional requirements gathering phase, the information security requirements are captured and consider the following: the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements access provisioning and authorization processes required protection needs of assets involved requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements requirements mandated by other security controls, e.g., interfaces to logging and monitoring or data leakage detection systems information users and operators of their duties and responsibilities 4. Verify whether the SDLC process/methodology defines the security roles and responsibilities during the development lifecycle. 5. Verify whether there is a clear integration between the organization risk management methodology and SDLC methodology and whether it outlines how information systems can be classified based on their inherent risk.	Inquiry, Inspection, and/or observation	1. Policy for the SDLC process 2. System and Services Acquisition Policies, Procedures and Standards 3. Information Security Procedures (SDLC process)
Cyber Security	Programming Security	1. Inspect if the organization: Develops a security plan for the information system that: Is consistent with the organization's enterprise architecture Explicitly defines the authorization boundary for the system; Describes the operational context of the information system in terms of missions and business processes; Provides the security categorization of the information system including supporting rationale;	Inquiry, Inspection, and/or observation	1. Security program plans, budget, procedures, and policies 2. Information Security Governance Program documentation

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		Describes the operational environment for the information system and relationships with or connections to other information systems; Provides an overview of the security requirements for the system; Identifies any relevant overlays, if applicable; Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; Distributes copies of the security plan and communicates subsequent changes to the plan to organization-defined personnel or roles; Reviews the security plan for the information system per organization-defined frequency; Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and Protects the security plan from unauthorized disclosure and modification. 2. Inspect if the organization. Identifies organization-defined user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.		
Cyber Security	Programming Security	1. Inquire with control owner/interview responsible personnel to understand how production data is sanitized, transferred, and used for test purposes. 2. Obtain and inspect written software-development procedures to verify that operational data is sanitized, transferred, when used for test purposes. 3. Observe testing processes and interview personnel to verify operational data is protected through testing. 4. Obtain a population of project plans/checklists for the period under review. 5. Select a sample of project plans and checklists to determine whether data protection activities are built into the overall test approach.	Inquiry, Inspection, and/or observation	1. Provide written software-development procedures. 2. Provide a population of project plans/checklists, from which a sample will be selected. 3. Provide the project plans and checklists for the sample selected. [PCI] 1. Provide a population of data and accounts from production systems recently installed or updated for the period under review, from which a sample will be selected. 2. Provide supporting evidence for the selected sample of data and accounts from production systems.
Cyber Security	Programming Security	1. Inquire with the control owner to determine the following: that documented software and mobile secure coding guidelines are available to outline development and implementation guidance for software and mobile code that the organization authorizes, monitors, and controls mobile code use within the information system 2. Inspect the Secure Coding Guidelines and determine that acceptable and unacceptable software and mobile coding guidelines along	Inquiry, Inspection, and/or observation	1. Secure Coding Guidelines; Infrastructure Hardening Guidelines and Secure Coding Guidelines. 2. System and Communications Protection Policies and procedures

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
		with implementation guidance are outlined within the documents, including: a. Secure coding techniques training is required for developers at least annually, based on industry best practices and guidance; b. Software-development process procedures: defines software-development processes based on industry standards and leading practices defines information security throughout the software development lifecycle defines that developers must develop software applications in accordance with standards determine that the software-development standards are implemented. c. Injection flaws: Validate inputs to determine that user data cannot modify meaning of commands and queries. Utilizing parameterized queries. d. Buffer overflows: Validate buffer boundaries. Truncating input strings. e. Insecure cryptographic storage Prevent cryptographic flaws. Use strong cryptographic algorithms and keys. f. Insecure communication Determine that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications. g. Improper error handling Validate that improper error handling is addressed by coding techniques that do not leak information via error messages h. All “high risk” vulnerabilities identified in the vulnerability identification process Verify that coding techniques address any “high risk” vulnerabilities that could affect the application i. Cross-site scripting (XSS) Validating all parameters before inclusion Utilizing context-sensitive escaping j. Improper Access Control Proper authentication of users Sanitizing input Not exposing internal object references to users User interfaces that do not permit access to unauthorized functions. k. Cross-site request forgery (CSRF) to determine that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. 1. Broken authentication and session management: Flagging session tokens (for example cookies) as “secure” Not exposing session IDs in the URL Incorporating appropriate time-outs and rotation of session IDs after a successful login. 3. Inspect system and communications protection policy and procedures addressing mobile code and determine the following: that the organization defines the mobile code and mobile code technologies that are acceptable and unacceptable; that the organization establishes restrictions for acceptable mobile code and mobile code technology use;		

TABLE 7-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD - As per engagement)	Request List (#)
Cyber Security	Programming Security	that the organization documents implementation guidance for the defined acceptable mobile code and code technologies. 4. Observe the organization's defined processes for controlling, authorizing, monitoring, and restricting mobile code and determine that the organization authorizes, monitors, and controls mobile code use within the information system.	Inquiry, Inspection, and/or observation	1. Policies and procedures related to production data (live PANs). 2. Population of data and accounts from recently installed or updated production systems. 3. Sample of test data and accounts from the obtained population.
		1. Inquire with the control owners and determine if procedures clearly define that production data (live PANs) are not used for testing or development. 2. Observe the testing processes and determine that the organization's personnel do not use production data (live PANs) in testing or in development. 3. Obtain a population of data and accounts from recently installed or updated production systems. 4. Select a sample of data and accounts and inspect test data to determine whether production data (live PANs) are used for testing or development.		

[0144] In some embodiments, infrastructure layer risk category in the blockchain risk framework covers relevant risks, control objectives and descriptions, testing objectives and procedures, and reporting parameters designed to address assurance and compliance needs for the blockchain infrastructure stack/layer supporting functioning of the

underlying hardware, software, servers, databases, networks, interfaces technologies (e.g. APIs etc.).

[0145] The sub-risk categories, control and testing objectives, test procedures and request lists for Infrastructure Layer risk category are provided below in Tables 8-10.

TABLE 8

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Infrastructure Layer	Servers and Databases Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-SD1	Lack of guidance and policy of functional requirements and migration to production may lead to inaccurate Blockchain logic.	L, M, H
Infrastructure Layer	Servers and Databases Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-SD2	Lack of an established baseline for information technology systems and Blockchain may affect operational environments and compromise security.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT1	Unauthorized or untested changes, or the failure to make necessary changes to operating system, network or application configurations or programs prevent systems from processing transaction records completely and accurately	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT2	Lack of segregation for roles and responsibilities and instance environments may lead to unauthorized changes to productions.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal or Reputational	IL-IT3	Lack of segregation for roles and responsibilities and instance environments may lead to unauthorized changes to productions.	L, M, H

TABLE 8-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT4	Transaction records are lost (e.g. due to system failure) and data is not recoverable or is corrupted/duplicated in the recovery process	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT5	Transaction records transferred between systems are incomplete or inaccurate.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT6	As business processes are redesigned and modified to reflect use of Blockchain technology, they embed an agreed set of appropriate controls	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT7	Application end-users bypass systems-enforced authorization and segregation of duties controls	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT8	Application end-users bypass systems-enforced authorization and segregation of duties controls	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT9	High-risk/powerful accounts (e.g., super-user, etc.) bypass systems-enforced authorization and segregation of duties controls	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT10	Unauthorized access to facilities, equipment and resources is not prevented	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT11	Unauthorized access (by business users, IT users or outsiders) to data causes data destruction or improper amendment of records.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT12	Unauthorized access (by business users, IT users or outsiders) to data causes data destruction or improper amendment of records.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT13	Duties are not appropriately segregated	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT14	Weak password controls or security configurations allow access rights to be circumvented	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT15	Unauthorized access (by business users, IT users or outsiders) to Blockchain Operational governance tools.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational,	IL-IT16	Unauthorized or untested changes, or failure to make	L, M, H

TABLE 8-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
		Financial, Compliance, Legal, or Reputational		necessary changes to scheduled job processes prevent systems from processing transaction records completely and accurately	
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT17	Unauthorized or untested changes, or failure to make necessary changes to scheduled job processes prevent systems from processing transaction records completely and accurately	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT18	Blockchain processing errors are not resolved.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT19	Unauthorized access to the Blockchain technology (i.e. code configuration tools) is prevented.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT20	Management release management policies and procedures include processes for making emergency configuration changes, including formal review processes for all changes categorized as emergency.	L, M, H
Infrastructure Layer	ITGCs	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT21	Unauthorized or untested changes, or failure to make necessary changes to scheduled job processes prevent systems from processing transaction records completely and accurately	L, M, H
Infrastructure Layer	Business Continuity and Disaster Recovery	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-BC1	A lack of backups or ineffective backups may lead to information loss.	L, M, H
Infrastructure Layer	Business Continuity and Disaster Recovery	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-BC2	Lack of Business Continuity and Disaster Recovery plans may inhibit the organization's ability to recover from an outage.	L, M, H
Infrastructure Layer	Business Continuity and Disaster Recovery	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-BC3	A lack of backups or ineffective backups may lead to information loss.	L, M, H
Infrastructure Layer	Business Continuity and Disaster Recovery	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-BC4	Lack of Business Continuity and Disaster Recovery plans may inhibit the organization's ability to recover from an outage.	L, M, H
Infrastructure Layer	Business Continuity and Disaster Recovery	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-BC5	A lack of Business Continuity plan and Disaster Recovery plan testing may result in an effective or failed recovery process.	L, M, H
Infrastructure Layer	Business Continuity and Disaster Recovery	Strategic, Operational, Financial, Compliance,	IL-BC6	Lack of communication to key stakeholders regarding their responsibilities may result in ineffective recovery activities in	L, M, H

TABLE 8-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
		Legal, or Reputational		the event of an outage.	
Infrastructure Layer	IT Asset Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT1	Without clearly defined roles and responsibilities with Blockchain vendors, accountability is lost when issues arise within the relationship	L, M, H
Infrastructure Layer	IT Asset Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT2	Without clearly defined roles and responsibilities with Blockchain vendors, accountability is lost when issues arise within the relationship	L, M, H
Infrastructure Layer	IT Asset Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT3	Without a comprehensive due diligence process, vendor risks may not be completely identified, leaving the organization susceptible to direct and indirect risks.	L, M, H
Infrastructure Layer	IT Asset Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IT-IL4	Without clearly defined roles and responsibilities with Blockchain vendors, accountability is lost when issues arise within the relationship	L, M, H
Infrastructure Layer	IT Asset Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IT5	Lack of required level of throughput and performance can compromise Blockchain use cases objectives.	L, M, H
Infrastructure Layer	IT Asset Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	IL-IF1	Data exchanged through APIs, system interfaces may be intercepted and accessed by unauthorized agents within or outside the organization's network	L, M, F

TABLE 9

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Infrastructure Layer	Servers and Databases Configuration	References to internal and external sources (including interaction with external platforms, systems, networks, and third parties) in the Blockchain logic are accurate.	Once the Blockchain has been configured, a test plan is developed to ensure meeting all functional requirements and approved by the Blockchain program management. The Blockchain configurations are tested by the impacted/required business and/or the Blockchain program management team. Test exceptions are appropriately recorded, monitored and tracked for resolution prior to migration to production	In-scope
Infrastructure Layer	Servers and Databases Configuration	A baseline configuration of information technology systems and Blockchain is created, implemented, and maintained	A configuration management program and database exists to implement, maintain and control configuration of systems and other infrastructure elements.	In-scope
Infrastructure Layer	ITGCs	Change Management controls are defined, established, and enforced	Changes to Blockchain Application and Operating	In-scope

TABLE 9-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
		including proper documentation and approval	System/Network configurations and enhancements are adequately tested and approved before being migrated into production and are monitored for appropriateness.	
Infrastructure Layer	ITGCs	Segregation of Duties is maintained and enforced for any changes, in addition the development, test, and production environments are separated.	Access to migrate the Blockchain process configurations into production is restricted to personnel who are independent of the configuration team. Development, testing, and production environments are segregated for changes to application configurations and periodically reviewed to ensure access is restricted to authorized personnel.	In-scope
Infrastructure Layer	ITGCs	Segregation of Duties is maintained and enforced for any changes.	Policies are maintained for segregation of duties within IT	In-scope
Infrastructure Layer	ITGCs	Backups of information are conducted, maintained, and tested periodically.	Data is appropriately backed up and recoverable	In-scope
Infrastructure Layer	ITGCs	Information input and output checks are performed.	Errors in production processing are identified and resolved	In-scope
Infrastructure Layer	ITGCs	Change Management controls are defined, established, and enforced including proper documentation and approval,	For each new Blockchain business process the associated controls are documented and approved by the business and the Blockchain program management.	In-scope
Infrastructure Layer	ITGCs	Access permissions are revoked based upon access reviews and/or user terminations.	Terminated employee's/third party or employee's/third party access no longer needed to Blockchain, database, and operating system/network is disabled and/or removed in a (timely manner).	In-scope
Infrastructure Layer	ITGCs	Access to systems and assets is controlled by incorporating the principle of least privilege.	Access requests to the application, database, and operating system/network are properly reviewed and authorized by management	In-scope
Infrastructure Layer	ITGCs	Privileged user roles and responsibilities are managed and tracked.	Super-user/administrative application, database, and operating system/network transactions or activities and sensitive generic IDs are monitored	In-scope
Infrastructure Layer	ITGCs	Physical access controls are in place to properly authorize employees, contractors, and visitors to facilities, center/facility and the equipment and resources,	Employees', contractors', and visitors' access to data center/facility and the information system components located within the facility is provided on a 'need to know' basis and requires organizational approval.	In-scope
Infrastructure Layer	ITGCs	Physical access to the secure areas are monitored.	There is physical security in place over the data center from which financially significant applications are run. Key card system is implemented in the data center for access control. And video surveillance is also in place to monitor the activities in the data center.	In-scope

TABLE 9-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Infrastructure Layer	ITGCs	Access permissions are reviewed periodically for appropriateness.	The key card system logs the visit to the data center per user and ID card. If any incident happens, IT department will look into the system log and video footage for investigation. Data Center Operations performs a semi-annual recertification of all users with physical access to Data Centers	In-scope
Infrastructure Layer	ITGCs	Segregation of Duties is maintained and enforced for critical business processes and in production environments.	Policies and procedures are maintained for segregation of duties within IT	In-scope
Infrastructure Layer	ITGCs	Access to applications, database, operating system and network is password protected on a global level and complies with documented policies or working practices detailing password configurations and configurable security parameters.	Passwords to applications, database/data file, operating system/network, and security configurations are set in an effective manner	In-scope
Infrastructure Layer	ITGCs	Access to the Blockchain Operational governance tools is restricted to appropriate personnel.	Access to the Blockchain operational governance tools is recertified by appropriate management at regular intervals as defined by policy guidelines. The approver confirms access remains commensurate with the individual's job responsibilities or requests changes/revocation to access.	In-scope
Infrastructure Layer	ITGCs	As changes to the Blockchain are contemplated, appropriate controls are in place to ensure that they are approved and rolled out across the network in a manner consistent with the Blockchain governance framework.	The Blockchain policies and procedures on change approval and propagation across the network are defined and include a description of key controls, oversight and escalation procedures.	In-scope
Infrastructure Layer	ITGCs	As changes to the Blockchain are contemplated, appropriate controls are in place to ensure that they are approved and rolled out across the network in a manner consistent with the Blockchain governance framework.	Only approved and tested changes are made to the job scheduler and rolled out across the network in a manner consistent with the Blockchain governance framework.	In-scope
Infrastructure Layer	ITGCs	Formal policies and procedures have been established to identify the Blockchain processing errors.	The Blockchain management has a documented problem management process for the Blockchain configurations during which errors or exceptions are identified, tracked, escalated, root causes identified and resolved.	In-scope
Infrastructure Layer	ITGCs	Access permissions are revoked based upon access reviews and/or user terminations,	Access to the Blockchain configuration tools is recertified by appropriate management at regular intervals as defined by policy guidelines. The approver confirms access remains commensurate with the individual's job responsibilities or requests changes/revocation to access.	In-scope
Infrastructure Layer	ITGCs	Change Management controls are defined, established and enforced including proper documentation and approval	The formal policies and procedures include detailed processes and required approvals necessary to make	In-scope

TABLE 9-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Infrastructure Layer	ITGCs	Consideration of Blockchain has been incorporated into ongoing business operations procedures, forms and processes.	an emergency change to the Blockchain configuration. A formal review is conducted for all emergency changes to ensure proper protocol and SODs were followed. Prior to a Blockchain change being placed into production, operations policies and procedures have been updated to include integration with Blockchain to ensure the business end users are aware of the Blockchain impact.	In-scope
Infrastructure Layer	Business Continuity and Disaster Recovery	Upon identified of a processing error, management enables back out/back up plan including the Blockchain being removed from production.	Back out plans for Blockchain configuration and plan to roll over to human processors in case of a Blockchain failure are formally documented for each Blockchain configuration and routinely reviewed to ensure still complete and accurate	In-scope
Infrastructure Layer	Business Continuity and Disaster Recovery	IT disaster recovery and business continuity plans have been developed based on the framework and designed to reduce the impact of a major disruption on the Blockchain functions and processes. The plans are based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services including the Blockchain use case. The plan is tested on a semi-annual basis.	Disaster recovery plan for the Blockchain technology exists for prolonged outages (with internal systems or 3rd party vendors) and has been tested to limit impact business operations.	In-scope
Infrastructure Layer	Business Continuity and Disaster Recovery	Backups of information are conducted, maintained, and tested semi-annually	The Blockchain configuration tools and data is included in management standard backup and recovery plan to ensure data is backed up within data centers or the cloud and available if needed.	In-scope
Infrastructure Layer	Business Continuity and Disaster Recovery	IT disaster recovery and business continuity plans have been developed based on the framework and designed to reduce the impact of a major disruption on the Blockchain Instance functions and processes. The plans are based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services including the Blockchain use case. The plan is tested on a semi-annual basis.	Risks to business continuity due to prolonged outages (with internal systems or with 3rd party vendor) have been identified and procedures have been formally documented to mitigate any risks.	In-scope
Infrastructure Layer	Business Continuity and Disaster Recovery	Business Continuity and Disaster Recovery plans are tested semi-annually to validate that the plans meet the organizational requirements.	Business Continuity and Disaster Recovery plans are tested semi-annually to verify the validity of established and implemented information security controls and to take appropriate corrective actions.	In-scope
Infrastructure Layer	Business Continuity and Disaster Recovery	Recovery activities are communicated to internal stakeholders and executive and management teams prior to and during declared outages.	Communication occurs to the individuals and teams involved in the recovery plan to ensure key stakeholders understand their responsibilities in the event of an outage.	In-scope

TABLE 9-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Infrastructure Layer	IT Asset Management	The Blockchain vendors are monitored for compliance with contractual agreements.	The Blockchain vendors are monitored on an ongoing basis to ensure compliance with contractual agreements.	In-scope
Infrastructure Layer	IT Asset Management	Licensing agreements are monitored and renewed as needed.	The Blockchain licensing agreements are reviewed, tracked and renewed as needed.	In-scope
Infrastructure Layer	IT Asset Management	The Blockchain program policies and procedures, which includes formal the Blockchain vendor selection methodology and standard contract templates and requirements, are reviewed and approved on a periodic basis.	The Blockchain vendor selection was based on formal selection methodology and detailed business requirements.	In-scope
Infrastructure Layer	IT Asset Management	The Blockchain program policies and procedures, which includes The Blockchain contract policies including clarification of the Blockchain ownership, are reviewed and approved on a periodic basis.	The Blockchain vendor contracts clarifies resource ownership and hardware procurement requirements for client and vendor.	In-scope

TABLE 10

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
Infrastructure Layer	Servers and Databases Configuration	1. Inquire with the control owners to determine if the organization identifies and documents established configuration settings. Review existing documentation around test exceptions to ensure the test plans identifies all functional requirements. 2. Verify the test exceptions are recorded, monitored and tracked for resolution prior to migration to production	Inquiry, Inspection, and/or observation	1. Policies and procedures related to configuration settings, specifically regarding the test plan of all functional requirements for configuration. 2. Log of test exceptions.
Infrastructure Layer	Servers and Databases Configuration	1. Verify whether a configuration management program is documented and maintained	Inquiry, Inspection, and/or observation	1. Policies, procedures, related to the baseline configuration settings on production infrastructures.
Infrastructure Layer	ITGCs	1. Inquire with the control owner and determine that the organization has a documented Change Management Process and it is reviewed at least annually and updated as needed. 2. Obtain a list of changes that were migrated to production for the testing period. 3. Select a sample of changes made to the production environment and determine if it was documented, tested prior to migration to production, and approved by the appropriate personnel. 4. Inspect that appropriate SOD is implemented for roles and environments.	Inquiry, Inspection, and/or observation	1. Change Management policies, procedures, and standards 2. Evidence of the last review of documented Change Management Process. 3. Population of changes for the applications and systems 4. Evidence of change requests and approvals
Infrastructure Layer	ITGCs	1. Inquire with control owners to determine that the development/testing environments are separate from the production environment. 2. Obtain and inspect screen-prints of the development, testing, and production environment to determine that they are in different environments.	Inquiry, Inspection, and/or observation	1. Screen-prints for each of the following environments: development testing production 2. Evidence of access control settings to enforce separation between development/testing and production environments.

TABLE 10-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD- As per engagement)	Request List (#)
Infrastructure Layer	ITGCs	1. Determine through interviews with control owners whether access controls are defined, documented, approved and enforced for changes to information systems.	Inquiry, Inspection, and/or observation	1. Evidence of segregation of duties in place for each in-scope information system.
Infrastructure Layer	ITGCs	1. Inspect relevant backup documentation and inquire with the control to validate whether the following considerations have been determined, documented, and implemented. 2. Inspect the backup confirmation settings and frequency to determine whether it is in accordance with policies and procedures. 3. Review activity logs for backups to determine the completeness of the organizations backup efforts. 4. Review activity logs for backups to determine if an alert is configured to notify administrators of successful and failed backups. 5. Review detailing testing efforts and the results of the testing efforts.	Inquiry, Inspection, and/or observation	1. Backup policies and procedures 2. Screenshot of backup configuration settings 3. Backup log showing status of backups 4. Evidence of successful backup restoration 5. Reports detailing testing efforts and the results of the testing efforts 6. Evidence of backup schedule
Infrastructure Layer	ITGCs	1. Inquire with management to determine if the production systems and applications have built in detective alerts if an invalid input is received and an error message is generated. 2. Inspect the input validation rules and program logic on the production systems and applications to determine if input validation checks are appropriately configured to validated information entered into a data field.	Inquiry, Inspection, and/or observation	1. Provide the input validation rules/configuration on the production systems and applications.
Infrastructure Layer	ITGCs	1. Inquire with control owners to determine the review and approval process for additional controls from a redesign. 2. Review an updated risk and control matrix and inspect for evidence of approval	Inquiry, Inspection, and/or observation	1. Blockchain use case risk and control matrix with approval
Infrastructure Layer	ITGCs	1. Inquire with control owners to determine whether the organization revokes user account access in response to terminations. 2. Obtain and inspect policies and procedures to determine the requirements are clearly stated for the removal of logical access as a result of terminations. 3. Select a sample of terminated users and inspect the evidence to determine that access is revoked within the timeframe specified by the access control procedures.	Inquiry, Inspection, and/or observation	1. Information Security Policy of Access Provisioning/Deprovisioning Policy 2. Population of total terminated users 3. Evidence that access is revoked within the timeframe specified by the access control procedures
Infrastructure Layer	ITGCs	1. Inquire with control owners to determine the review and approval process for access requests. 2. Obtain the population of access requests and inspect the evidence to determine that access is properly reviewed and approved by management.	Inquiry, Inspection, and/or observation	1. Information Security Policy of Access Provisioning/Deprovisioning Policy 2. User access requests 3. Evidence that access is reviewed and approved by management
Infrastructure Layer	ITGCs	1. Inquire with control owners who is responsible for assigning access to verify that access to privileged user IDs are appropriate and restricted. 2. Obtain and inspect documentation to determine that privileged access requests are evaluated for appropriateness and follow the principles of least privilege.	Inquiry, Inspection, and/or observation	1. Information Security Policy of Access Provisioning/Deprovisioning Policy 2. Population of users with privileged access 3. Evidence for selected samples, indicating the job function(s) or role(s)

TABLE 10-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD- As per engagement)	Request List (#)
		3. Obtain a population of users with privileged access and select a sample of users and inspect evidence to determine the access is necessary and approved by the designated authority.		requested, as well as the approval for the access requested. 4. List of privileged user accounts and associated roles. 5. Access approval matrix
Infrastructure Layer	ITGCs	1. Inquire with management and inspect the documented process to determine if procedures are defined for authorizing and granting physical access to employees, contractors, and visitors based on role or function. 2. Obtain a population of new users who have been granted access to the in-scope facilities and equipment. 3. Select a sample of new users and inspect that physical access was authorized and documented prior to physical access granted.	Inquiry, Inspection, and/or observation	1. Physical access policies and procedures 2. Population of new users 3. Access lists to in-scope facilities and equipment
Infrastructure Layer	ITGCs	1. Inquire with management the key card system implementation process. 2. Inquire/Observe with management that video surveillance is in place at the data centers. 3. Obtain the key card system logs to the data centers. 4. Select a sample of users granted access to the data center and inspect that key card access was authorized and documented prior to physical access granted.	Inquiry, Inspection, and/or observation	1. Key card system implementation policy 2. Key card system access list 3. Key card system logs to the data centers
Infrastructure Layer	ITGCs	1. Obtain the key card system log to the data center operations and select a sample of users to inspect the recertification occurs on a semi-annual basis.	Inquiry, Inspection, and/or observation	1. Key card system logs to the data center operations 2. Evidence of recertifications for users with physical access
Infrastructure Layer	ITGCs	1. Determine through interviews with control owners whether access controls are defined, documented, approved and enforced for changes to information systems and critical business processes.	Inquiry, Inspection, and/or observation	1. Evidence of segregation of duties in place for each in-scope information system.
Infrastructure Layer	ITGCs	1. Examine the documentation and security parameters to verify they are aligned	Inquiry, Inspection, and/or observation	1. Screenshots of password configurations 2. Password policy
Infrastructure Layer	ITGCs	1. Inquire with control owner and determine that the organization has a documented recertification policy and it is reviewed at least annually and updated as necessary. 2. Select a sample of recertifications for the Blockchain Operational governance tools over the testing period and inspect the evidence to determine the appropriate personnel confirmed the access and the access based on the job function and role is appropriate.	Inquiry, Inspection, and/or observation	1. Information Security Policy of Access Provisioning/Deprovisioning Policy 2. Evidence of recertifications for the Blockchain Operational governance tools 3. Evidence of users job function and role
Infrastructure Layer	ITGCs	1. Inquire with control owner and determine that the organization has a documented Blockchain change approval policy and procedure and inspect it includes key controls, oversight and escalation procedures.	Inquiry, Inspection, and/or observation	1. Change Management Policy inclusive of Blockchain policies 2. If available, Blockchain policy
Infrastructure Layer	ITGCs	1. Inquire with control owner and determine that the organization has a documented Blockchain governance framework. 2. Select a sample of approved changes and inspect the appropriate personnel approved the change and it was tested in accordance with the Blockchain governance framework.	Inquiry, Inspection, and/or observation	1. Blockchain Governance Framework 2. Evidence of approved changes 3. Job Scheduler

TABLE 10-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD- As per engagement)	Request List (#)
Infrastructure Layer	ITGCs	1. Inquire with control owner and determine that the organization has a documented problem management process for Blockchain Configurations. 2. Select a sample of errors or exceptions and inspect the evidence to ensure they were tracked, escalated, root causes identified and resolved.	Inquiry, Inspection, and/or observation	1. Problem Management Process for Blockchain Configurations 2. Blockchain Configurations error or exceptions log
Infrastructure Layer	ITGCs	1. Inquire with control owner and determine that the organization has a documented recertification policy and it is reviewed at least annually and updated as necessary. 2. Select a sample of recertifications for the Blockchain configuration tools over the testing period and inspect the evidence to determine the appropriate personnel confirmed the access and the access based on the job function and role is appropriate.	Inquiry, Inspection, and/or observation	1. Information Security Policy of Access Provisioning/Deprovisioning Policy 2. Evidence of recertifications for the Blockchain configuration tools 3. Evidence of users job function and role
Infrastructure Layer	ITGCs	1. Inquire with control owner to determine if a Change Management policy exists and it is updated as needed. 2. Inspect the policy to ensure emergency changes to Blockchain configuration is included. 3. Select a sample of emergency changes to Blockchain configurations and inspect the evidence to ensure policies were followed and the appropriate personnel approved the change.	Inquiry, Inspection, and/or observation	1. Change Management policies, procedures, and standards 2. Evidence of the last review of documented Change Management Process. 3. Population of emergency changes for the applications and systems 4. Evidence of emergency change and approvals
Infrastructure Layer	ITGCs	1. Inquire with control owner to determine if a Blockchain Operations policy exists and it is updated as needed. 2. Inspect the evidence of a Blockchain change to ensure the policies and procedures have been updated to include the updated integration	Inquiry, Inspection, and/or observation	1. Blockchain Operations policy and procedures 2. Evidence of a Blockchain change
Infrastructure Layer	Business Continuity and Disaster Recovery	1. Inquire with the control owner to determine if a formal Blockchain failure plan exists. 2. Obtain the most recent version of business continuity and disaster recovery plans and verify a back out plan is included for Blockchain.	Inquiry, Inspection, and/or observation	1. Back out plan 2. Blockchain failure plan 3. Business Continuity plan
Infrastructure Layer	Business Continuity and Disaster Recovery	1. Inquire with the control owner to determine if a formal business continuity and disaster recovery management program exists (i.e., governance, resources, plans) 2. Obtain the most recent version of business continuity and disaster recovery plans and verify whether it has been approved by a Senior Management executive and includes the following: Business continuity objectives Business processes and critical information assets in scope Information security continuity Business impact analysis Recovery objectives and priorities, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) Roles and responsibilities Dependencies and critical functions for delivery of critical services	Inquiry, Inspection, and/or observation	1. Business Continuity and Disaster Recovery plan 2. Evidence of the organization conducting tests of outages and documenting the results.

TABLE 10-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD- As per engagement)	Request List (#)
		3. Inquire with the control owner to determine whether the business continuity and disaster recovery plans have been communicated and shared with stakeholders with associated responsibilities. 4. Inquire with control owner to determine how often the business continuity and disaster recovery plans are tested and how they document the results of the test.		
Infrastructure Layer	Business Continuity and Disaster Recovery	1. Verify the standard backup and recovery plan includes a section regarding Blockchain configuration tools and data. 2. Inspect the agreements with the data center or cloud providers to determine whether they exist and cover the current period.	Inquiry, Inspection, and/or observation	1. Standard backup and recovery plan 2. Agreements for the data center or cloud if applicable
Infrastructure Layer	Business Continuity and Disaster Recovery	1. Inquire with control owner and inspect evidence to determine whether the risks identified and documented have been mitigated within the business continuity and disaster recovery plan.	Inquiry, Inspection, and/or observation	1. Business Continuity and Disaster Recovery plan 2. Evidence of risks identified
Infrastructure Layer	Business Continuity and Disaster Recovery	1. Inquire with control owner and inspect evidence to determine whether the business continuity and disaster recovery plans are tested on a semi-annually basis, if test results are reviewed and corrective actions are taken if necessary.	Inquiry, Inspection, and/or observation	1. Business continuity and disaster recovery plan testing report. 2. Evidence that corrective actions are taken if necessary.
Infrastructure Layer	Business Continuity and Disaster Recovery	1. Inquire with control owner to determine whether communication occurs to the individuals and teams involved in the recovery processes so that key stakeholders understand their responsibilities in the event of a disaster.	Inquiry, Inspection, and/or observation	1. Information Security policies and procedures 2. Business Continuity Management Policy 3. Technology Operations Disaster Recovery Plan
Infrastructure Layer	IT Asset Management	1. Inspect a sample of vendors and validate that the vendor contracts are monitored periodically.	Inquiry, Inspection, and/or observation	1. Vendor contracts 2. Population of vendors
Infrastructure Layer	IT Asset Management	1. Inspect a sample of vendors and validate that the vendor licensing agreements are monitored periodically and renewed as needed.	Inquiry, Inspection, and/or observation	1. Vendor licensing agreements 2. Population of vendors 3. Log of tracking vendor licensing agreements
Infrastructure Layer	IT Asset Management	1. Inquire with the control owner and determine if a vendor management policy exists. 2. Inspect a sample of agreements and validate that the policy and procedures were reviewed and approved on a periodic basis. 3. Verify each Blockchain vendor includes the standard contract, templates and requirements that are aligned with the vendor selection	Inquiry, Inspection, and/or observation	1. Vendor management policy and procedure 2. Vendor contracts 3. Population of new vendors for the testing period
Infrastructure Layer	IT Asset Management	1. Inquire with the control owner and determine if all relevant information security requirements are established and agreed with each supplier/vendor that may access, process, store, communicate, or provide IT infrastructure components for, the organizations information. 2. Inspect a sample of agreements and validate they include resource ownership, hardware procurement requirements, and Blockchain ownership.	Inquiry, Inspection, and/or observation	1. Vendor management policy and procedure 2. Vendor contracts 3. Population of new vendors for the testing period

4.4 Architecture Layer Assessment Work Program

[0146] In some embodiments, blockchain architecture layer risk category in the blockchain risk framework covers relevant risks, control objectives and descriptions, testing objectives and procedures, and reporting parameters designed to address assurance and compliance needs for the

blockchain architecture stack/layer supporting blockchain permissioned and/or permissioned networks operations and participant lifecycle management.

[0147] The sub-risk categories, control and testing objectives, test procedures and request lists for Architecture Layer risk category are provided below in Tables 11-13.

TABLE 11

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP1	Lack of an established baseline for Blockchain systems may affect operational environments and compromise security.	L, M, H
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP2	If hardening standards have not been developed, defined, or implemented. Blockchain systems are unprotected and vulnerable to malicious attacks.	L, M, H
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP3	Inadequate processes in the design phase of the Blockchain implementation may negatively impact core system performance.	L, M, H
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP4	Lack of configuration standards and/or lack of adherence to established configuration standards may lead to failures or inefficiencies in the Blockchain production environment.	L, M, H
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP5	Lack of configuration standards and/or lack of adherence to established configuration standards may lead to failures or inefficiencies in the Blockchain production environment.	L, M, H
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP7	Insufficient test plans lead to the inability to meet the requirements identified in the analysis and design phase.	L, M, H
Architecture Layer	Blockchain Platform & Protocol Configuration	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP8	Insufficient test plans lead to the inability to meet the requirements identified in the analysis and design phase.	L, M, H
Architecture Layer	Hardware Security Modules	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BP9	HSM devices are properly configured and maintained which may expose the Blockchain use case supporting systems or sensitive data to unauthorized parties.	L, M, H
Architecture Layer	Signature Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-SM1	Lack of effective cryptographic keys management may expose the keys to potential modification, loss, destruction or disclosure to unauthorized parties.	L, M, H
Architecture Layer	Signature Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-SM2	Lack of effective cryptographic keys management may expose the keys to potential modification, loss, destruction or disclosure to unauthorized parties.	L, M, H
Architecture Layer	Signature Management	Strategic, Operational, Financial, Compliance,	AL-SM3	Lack of effective cryptographic keys management may expose the keys to potential modification, loss, destruction or disclosure to	L, M, H

TABLE 11-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
		Legal, or Reputational		unauthorized parties.	
Architecture Layer	Signature Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-SM4	Lack of effective cryptographic keys management may expose the keys to potential modification, loss, destruction or disclosure to unauthorized parties.	L, M, H
Architecture Layer	Cryptography	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-C1	Inadequate protection of information in Blockchain systems through cryptographic techniques and effective key management may result in the potential compromise of confidentiality or integrity of information in transmission or storage.	L, M, H
Architecture Layer	Cryptography	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-C2	Inadequate protection of information in Blockchain systems through cryptographic techniques and effective key management may result in the potential compromise of confidentiality or integrity of information in transmission or storage.	L, M, H
Architecture Layer	Cryptography	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-C3	Inadequate protection of information in Blockchain systems through cryptographic techniques and effective key management may result in the potential compromise of confidentiality or integrity of information in transmission or storage.	L, M, H
Architecture Layer	Cryptography	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-C4	Inadequate protection of information in Blockchain systems through cryptographic techniques and effective key management may result in the potential compromise of confidentiality or integrity of information in transmission or storage.	L, M, H
Architecture Layer	Cryptography	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-C5	Lack of compliance may result in ineffective controls thereby heightening organization's security and compliance risks.	L, M, H
Architecture Layer	Scalability /Capacity Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-SC1	System capacity is not monitored which may lead to interruption and/or failure to key systems.	L, M, H
Architecture Layer	Scalability/Capacity Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-SC2	Inadequate procedures to monitor the capacity and performance of IT resources may lead to delivery failure of service performance agreements.	L, M, H
Architecture Layer	Scalability/Capacity Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-SC3	Failure to define, agree, record and manage the levels of service as required by the business may result in the agreed service continuity and availability commitment to customers not being met in all circumstances.	L, M, H
Architecture Layer	Availability	Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-A1	Lack of redundant information processing facilities may lead to disruption of critical services in the event Blockchain information processing facilities are unavailable due to excess capacity or other threats.	L, M, H

TABLE 11-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN01	Privileged access is not appropriately restricted, logged, and monitored for unencrypted data, which can lead to unauthorized access	L, M, H
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN02	Data in transit is not secure and may be compromised or accessed by unauthorized participants, compromising the integrity of the data	L, M, H
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN03	Data at rest or in storage is not secure and may be accessible by unauthorized participants, compromising the integrity of the data	L, M, H
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN04	Databases lack encryption to protect and recover data in the case of loss or theft	L, M, H
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN05	Data is not retained for DLT inputs. PKIs, or other critical systems; lack of availability limits backup and recovery capability	L, M, H
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN06	PKI Certificate Authority (CA) is insufficiently isolated from tire rest of the network	L, M, H
Architecture Layer Encryption (EN)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN07	No PKI Certificate Authority (CA) is present in the organization's network to validate data transmission or transactions on the blockchain	L, M, H
Architecture Layer Key Management		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-EN07	Lack of proper physical and logical custody of the keys (private and public) can compromise a single or multiple users on the Blockchain.	L, M, H
Architecture Layer Data Retention (DR)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-DR01	Data is not retained for DLT inputs, PKIs, or other critical systems; lack of availability limits backup and recovery capability	L, M, H
Architecture Layer Consensus (CS)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	TL-CS01	No formal consensus protocol is established, system validators for DLT entries lacks authentication	L, M, H
Architecture Layer Consensus (CS)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-CS02	Implementation processes for system coding related to consensus have not been defined; no formal channel for change management exists	L, M, H
Architecture Layer Consensus (CS)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-CS03	System development and management life cycle does not exist or does not apply to consensus system architecture	L, M, H
Architecture Layer Consensus (CS)		Strategic, Operational,	AL-CS04	The organization has no approvals process for change management	L, M, H

TABLE 11-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Architecture Layer Consensus (CS)		Financial, Compliance, Legal, or Reputational	AL-CS05	affecting consensus or docs not secure against improper approvals being issued	L, M, H
Architecture Layer Consensus (CS)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BC1	There is no access review or audit mechanism for the consensus protocol or any users, systems, or participants affiliated with DLT validation	L, M, H
Architecture Layer Consensus (CS)		Strategic, Operational, Financial, Compliance, Legal, or Reputational	AL-BC2	Consensus mechanisms implemented do not provide comfort on the immutability of the data stored on the Blockchain.	L, M, H

TABLE 12

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Architecture Layer	Blockchain Platform & Protocol Configuration	The organization has created a configuration management database (CMDB) that houses all Blockchain systems and infrastructure. A baseline configuration of the Blockchain system is created, implemented, and maintained.	A configuration management program and database exists to implement, maintain and control configuration of Blockchain systems and oilier infrastructure elements (including hardware, software, firmware, and documentation). The program requires the identification of baseline configurations (original versions) of Blockchain infrastructure elements (hardware, software etc.). A central repository of configuration items (CI), their attributes, and their inter-linkages is established and maintained. CIs are linked to the services that they support. Current and prior configuration for all CIs, including Blockchain production servers, network devices, and databases is captured and maintained in the central repositon. in order to support rollback	In-scope
Architecture Layer	Blockchain Platform & Protocol Configuration	Blockchain systems hardening standards are established and maintained. Blockchain system configuration and hardening standards are consistent with industry-accepted standards, vendor specific guidelines and address all known security vulnerabilities	Blockchain system configuration and hardening standards are developed, communicated, implemented and maintained. The standards followed address all known security vulnerabilities and are consistent with industry-accepted system hardening standards and any vendor specific guidelines	In-scope
Architecture Layer	Blockchain Platform & Protocol Configuration	The Blockchain Instance impact on core processing system performance has been determined and appropriately addressed as part of functional specification process	The Blockchain Instance process impact on core system performance is documented and approved by IT and the Blockchain Instance program management.	In-scope

TABLE 12-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Architecture Layer	Blockchain Platform & Protocol Configuration	Newly implemented the Blockchain Instances are configured to completely or accurately process data. The Blockchain Instances are configured to effectively meet the business requirements.	Once the Blockchain Instance has been configured, a test plan is developed to ensure meeting all functional requirements and approved by the Blockchain Instance program management. The Blockchain Instance configurations are tested by the impacted/required business and/or the Blockchain Instance program management team. Test exceptions are appropriately recorded, monitored and tracked for resolution prior to migration to production.	In-scope
Architecture Layer	Blockchain Platform & Protocol Configuration	Auditability of the Blockchain Instance processing has been enabled within the tool.	The audit logging of the Blockchain Instance software tool has been enabled. The ability to change the audit capacities is restricted to authorized personnel outside of the configuration function.	In-scope
Architecture Layer	Blockchain Platform & Protocol Configuration	Testing architecture and requirements have been defined and documented. Test plan including test cases and procedures are formally defined.	Once the Blockchain Instance has been configured, a test plan is developed to ensure meeting all functional requirements and approved by the Blockchain Instance program management. The Blockchain Instance configurations are tested by the impacted/required business and/or the Blockchain Instance program management team. Test exceptions are appropriately recorded, monitored and tracked for resolution prior to migration to production.	In-scope
Architecture Layer	Blockchain Platform & Protocol Configuration	Technical test environments are stable and managed properly.	The Blockchain Instance configuration testing take place in environments which are logically segregated from and mirror the legacy system production environment.	In-scope
Architecture Layer	Hardware Security modules	HSM devices are properly configured and maintained which may expose the Blockchain use case supporting systems or sensitive data to unauthorized parties	HSM devices are deployed, properly configured and maintained to prevent the Blockchain use case supporting systems or sensitive data exposure to unauthorized parties	In-scope
Architecture Layer	Signature Management	The integrity of the Blockchain cryptosystem is maintained through the proper management of encryption keys. Public and private keys are securely managed through formal management processes.	A formal key management system and associated processes exist to securely manage (i.e., generate, distribute, store, access, backup and destroy) secret/private keys and public keys issued by trusted Certification Authorities. Formal procedures are in place to protect keys used to secure stored cardholder data against disclosure and misuse. Public key certificates are issued per defined standards or from an approved service provider.	In-scope
Architecture Layer	Signature Management	The integrity of the Blockchain cryptosystem is maintained through the proper management of encryption keys. Cryptographic key access and storage is restricted and controlled.	1. Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary 2. Verify whether equipment used to generate, store, and archive keys are protected.	In-scope

TABLE 12-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Architecture Layer	Signature Management	The integrity of the Blockchain cryptosystem is maintained through the proper management of encryption keys. Cryptographic keys are securely stored. The integrity of the Blockchain cryptosystem is maintained through the proper management of encryption keys.	Cryptographic keys are stored in the fewest locations possible. Secret mid private keys used to encrypt/decrypt cardholder data are stored in one (or more) of the following forms at all times: Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) As at least two full-length key components or key shares, in accordance with an industry-accepted method	In-scope
Architecture Layer	Signature Management	The integrity of the Blockchain cryptosystem is maintained through the proper management of encryption keys. Cryptographic key change management is followed in accordance with best practices and guidelines.	Cryptographic keys are changed at the end of their cryptoperiod. as defined by the associated application vendor or key owner, and based on industry best practices and guidelines. Keys are retired or replaced (for example, archiving, destruction, and/or revocation) as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	In-scope
Architecture Layer	Cryptography	Control: Stored classified data are encrypted and access controlled. Control Objective: Data-at-rest is protected through cryptographic techniques.	Classified data (e.g., CUI, PHI, CHD, PII) is stored in an encrypted format regardless of the medium (including mobile devices). Access to the encryption keys is restricted to authorized personnel.	In-scope
Architecture Layer	Cryptography	Data-at-rest is protected through cryptographic techniques. Disk encryption managed independently of the native operating system authentication.	Logical access for disk encryption is managed separately and independently of native operating system authentication.	In-scope
Architecture Layer	Cryptography	Data-in-transit is protected through cryptographic techniques. Data integrity in transmission protected with secure cryptography.	Cryptographic techniques are used to protect the confidentiality and integrity of data in transmission. While transmitting cardholder data, the following measures are implemented: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use.	In-scope
Architecture Layer	Cryptography	Data-in-transit is protected through cryptographic techniques. Data is protected in transmission through secure messaging utilities and facilities.	Secure messaging utilities and facilities are used to protect data in transmission. Electronic messaging such as MQ Series, middleware, system to system application calls, batch processing, email. Electronic Data Interchange (EDI), and instant messaging, has security provisions in place to protect messages from unauthorized access, modification, and denial of service.	In-scope

TABLE 12-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-Scope (TBD-As per engagement)
Architecture Layer	Cryptography	Cryptographic controls comply with relevant agreements, legislation, and regulations. Cryptographic controls have been established to comply with all business relevant agreements, legislation, and regulations.	Cryptographic controls are used in compliance with all relevant agreements, legislation, and regulations. FIPS-validated cryptography is leveraged to protect the confidentiality of CUI. If cryptography is required based on the selection of other security controls, each type of cryptography required is clearly defined.	In-scope
Architecture Layer	Cryptography	System capacity is monitored in real time to meet availability requirements. System capacity is monitored for operations regarding information processing facilities	Real time monitoring of system capacity is performed to enable the implementation of additional capacity to help meet availability commitments and requirements, and reports are made available for management review.	In-scope
Architecture Layer	Scalabiltiy/Capacity Management	Adequate capacity is maintained to prevent interruptions. System capacity is adequately monitored to ensure system availability is maintained.	Availability requirements are agreed upon with customers. Availability, capacity, and performance baselines have been established based on customer needs, business impact analysis, organizational policies etc. Adequate capacity, performance, and availability is maintained to prevent business disruptions, and to meet existing and changing business needs.	In-scope
Architecture Layer	Scalabiltiy/Capacity Management	Baselines are monitored for deviations and are resolved or followed up. Maintain service availability, efficient management of resources, and optimization of system performance through prediction of future performance and capacity requirements.	Deviations from established availability, performance, and capacity baselines are monitored, reported, and resolved. After monitoring, measuring, analyzing, reporting, and reviewing availability, performance, and capacity deviations from established baselines, all outstanding issues are followed up.	In-scope
Architecture Layer	Availability	Blockchain production system availability is monitored and incidents are documented. Technical capabilities exist to enable resiliency of Blockchain information processing facilities in accordance with availability objectives in the event of disruption.	Blockchain production systems are monitored for availability and any incidents are documented in a ticketing system.	In-scope

TABLE 13

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
Architecture Layer	Blockchain Platform & Configuration	1. Inquire with the control owner to determine whether a configuration management database (CMDB) that includes Blockchain configuration items (CI) is maintained. 2. Verify whether a configuration management plan is documented and maintained and includes the following: Roles and responsibilities Process for identifying and managing CIs	Inquiry, Inspection, and/or observation	1. Policies, procedures, related to the Blockchain baseline configuration settings on production infrastructures. 2. Enterprise Blockchain production infrastructure configuration management plan.

TABLE 13-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
Architecture Layer	Blockchain Platform & Protocol Configuration	Definitions of CI Interlinkages between CIs 3. Inspect the CMBD and determine for a sample of systems, where the Blockchain baseline configuration is maintained. Also, validate whether previous versions of the CIs and corresponding documentation is archived and maintained to support rollback. 4. Verify whether the CMDB is reviewed for accuracy and consistency on a periodic basis. Verify whether the organization reviews and updates the baseline configuration of the Blockchain system on a periodic basis or upon any upgrades or installations. 1. Inquire with control owner to determine if the organization: Establishes and documents configuration settings for Blockchain technology products employed within the information system using the appropriate security configuration baseline that reflect the most restrictive mode consistent with operational requirements: Implements the configuration settings; 2. Inquire of the control owner and determine the Blockchain system configuration standards are consistent with industry-accepted configuration and hardening standards and are applied when new systems are configured and verified as being in place before a Blockchain system is installed on the network. 3. Inspect the Network Hardening Guidelines. Production Network Security Standard, and Change Management methodology and determine if the organization has documented and implemented a change management methodology for the production environment to govern the Blockchain configuration management process.	Inquiry, Inspection, and/or observation	1. Provide evidence of the organization's documented change management methodology for the production environment. 2. Provide evidence of Blockchain Network Hardening Guidelines. Production Network Security Standard, and Change Management methodology. 3. Change Management methodology 4. Production Network Security Standard. 5. Blockchain Infrastructure Hardening Guidelines.
		1. Inquire with control owner to whether an established system development lifecycle process is in place, documented, maintained, and applied for all Blockchain system and software design, acquisition, implementation, configuration, integration, testing, modification, and maintenance. 2. Obtain and inspect SDLC policies and procedures to determine whether mi established Blockchain system development lifecycle process is documented. 3. Verify whether an impact assessment and performance requirements for Blockchain information systems and information services are identified as part of SDLC efforts, business process re-design, etc.		
Architecture Layer	Blockchain Platform & Protocol Configuration	1. Obtain Blockchain systems configurations. 2. Assess configuration relative to functional requirements.	Inquiry, Inspection, and/or observation	1. Obtain Blockchain systems configurations.
Architecture Layer	Blockchain Platform &	1. Obtain Blockchain systems configurations.	Inquiry, Inspection, and/or	1. Obtain Blockchain systems configurations.

TABLE 13-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
	Protocol Configuration	2. Assess Audit logging capabilities in the Blockchain system relative to internal guidelines and leading practices.	observation	
Architecture Layer	Blockchain Platform & Protocol Configuration	1. Obtain Blockchain systems test plans and requirements. 2. Determine if the test plans are executed as per requirements.	Inquiry, Inspection, and/or observation	1. Obtain Blockchain systems executed test plans and requirements.
Architecture Layer	Blockchain Platform & Protocol Configuration	1. Obtain information including version numbers of the test and production environments for Blockchain systems. 2. Determine if the testing takes place in environments which are logically segregated from and mirror the legacy system production environment.	Inquiry, Inspection, and/or observation	1. Obtain information including version numbers of the test and production environments for Blockchain systems.
Architecture Layer	Hardware Security Modules	Determine if HSM device(s) are deployed, properly configured and maintained to prevent the Blockchain use case supporting systems or sensitive data exposure to unauthorized parties.	Inquiry, Inspection, and/or observation	1. Obtain HSM information including vendor, configuration and leading practices guidelines.
Architecture Layer	Signature Management	1. Review key management procedures and determine if they address secure generation, distribution, storage, backup, and access management of keys. 2. Review key management standards to determine key strength aligns with industry leading standards. 3. Determine through interview with control owner that formal roles and responsibilities have been established for management keys. 4. Examine key-management policies and procedures to verify processes are specified to protect keys against disclosure and misuse and include at least the following: Access to keys is restricted to the fewest number of custodians necessary. Key-encrypting keys are at least as strong as the data encrypting keys they protect. Key-encrypting keys are stored separately from data encrypting keys. Keys are stored securely in the fewest possible locations and forms. 5. Verify that key-management procedures specify how to generate strong keys. 6. Observe the method for generating keys to verify that strong keys are generated. 7. Observe the method for distributing keys to verify that keys are distributed securely. 8. Observe the method for storing keys to verify that keys are stored securely.	Inquiry, Inspection, and/or observation	1. Encryption and Key Management policies and procedures. 2. User access list of cryptographic key custodians. 3. Information Security policies and procedures 4. Security Incident Response Process 5. Audit and accountability policies. 6. Procedures addressing non-repudiation. 7. Automated mechanisms configured with non-repudiation capabilities.
Architecture Layer	Signature Management	1. Inquire about Key Management process. 2. Review the key Management process and determine if appropriate level of approval, SOD, and ownership mechanisms are in place. 3. Test approval, SOD, and ownership mechanisms to determine if the Key Management process is safe, secure and does not lack required level of integrity.	Inquiry, Inspection, and/or observation	1. Obtain Key Management policies and procedure 2. Test approval, SOD and ownership activities for Key Management
Architecture Layer	Signature Management	1. Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations. 2. Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must	Inquiry, Inspection, and/or observation	1. Identify and assess key storage locations, documented procedures, system configurations.

TABLE 13-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
		only exist in one (or more) of the following forms at all times. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) As key components or key shares, in accordance with an industry-accepted method 3. Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one (or more) of the following form at all times. Encrypted with a key-encrypting key Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) As key components or key shares, in accordance with an industry-accepted method 4. Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: Key-encrypting keys are at least as strong as the data-encrypting keys they protect Key-encrypting keys are stored separately from data-encrypting keys.		
Architecture Layer	Signature Management	1. Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod (s) (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key) 2. Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s). 3. Verify that key-management procedures specify processes for the following: The retirement or replacement of keys when tire integrity of the key has been weakened The replacement of known or suspected compromised keys. Any keys retained after retiring or replacing are not used for encryption operations 4. Interview personnel to verify the following processes are implemented: Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. Keys are replaced if known or suspected to be compromised. Any keys retained after retiring or replacing are not used for encryption operations.	Inquiry, Inspection, and/or observation	1. Identify and assess encryption mechanism for Key Management
Architecture Layer	Cryptography	1. Inquire with the control owner to determine how classified data is encrypted at rest in all formats	Inquiry, Inspection, and/or observation	1. Information Security Policies. 2. Data Classification

TABLE 13-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
		(databases, media, mobile devices, removable storage, etc.) and how access to the encryption keys is restricted to authorized personnel in accordance with encryption requirements. For data at rest, assess whether one of the following is implemented: Full disk encryption: Partial encryption where the access control will only allow writing to the encrypted partition. 2. Obtain and inspect the cryptographic controls policy to determine whether it aligns to industry standards. 3. Obtain a system generated list of individuals with access to the encryption keys and determine whether access is restricted to the authorized personnel. 4. Inspect that only approved hard drive encryption software has been deployed to mobile devices and systems that hold sensitive data.		Policy 3. Information Security Policy for encryption requirements. 4. System generated list of individuals with access to the encryption keys with names and respective job title. 5. Configuration or evidence showing systems components/backups are encrypted using AES-256 via FIPS 140-2 validated encryption 6. Evidence indicating the use of either full disk encryption, or partial encryption with access controls to allow writing to the encrypted partition
Architecture Layer	Cryptography	1. Inquire with the control owner to determine if disk encryption is used (rather than file or column-level database encryption). 2. Inspect policies and procedures and the configurations for the in scope systems to ensure that logical access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). 3. Validate that decryption keys are not associated with user accounts.	Inquiry, Inspection, and/or observation	1. Provide the policies and procedures related to access management. 2. Provide the configurations for the in scope systems validating that logical access is managed separately and independently of native operating system authentication and access control mechanisms. 3. Evidence that decryption keys are not associated with user accounts.
Architecture Layer	Cryptography	1. Inquire with control owners to determine that sensitive data is encrypted while being exchanged between systems within the network and also when transmitted over public networks. 2. Identify all locations where sensitive data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. 3. Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all sensitive data is encrypted with strong cryptography during transit.	Inquiry, Inspection, and/or observation	1. Information Security Policies and procedures related to Encryption. 2. Screenshots of the applicable encryption or network protection utility. 3. TLS implementation system configurations. 4. Security Implementation Guide.
Architecture Layer	Cryptography	1. Inspect if the organization ensures that the transmission, movement, and removal of information is restricted to authorized users and processes, and is protected. Thus enabling the entity to meet its commitments and requirements as they relate to security, availability, processing integrity, or confidentiality or any combination thereof. 2. For the electronic messaging systems, provide screenshots and/or documentation that controls have been implemented to address the following : protecting messages from unauthorized access, modification or denial of service, ensuring correct addressing and	Inquiry, Inspection, and/or observation	1. Evidence that secure messaging utilities and facilities are used to protect data in transmission. 2. Policies and procedures related to the protection of data-in-transit.

TABLE 13-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
Architecture Layer	Cryptography	transportation of the message, general reliability and availability of the service, legal considerations, obtaining approval prior to using external public services such as instant messaging or file sharing, stronger levels of authentication controlling access from publicly accessible networks. 1. Inquire with control owner to determine whether cryptographic controls are used in compliance with relevant agreements, legislation, and regulations. 2. Obtain and inspect the Encryption, and Cryptographic Controls. Encryption and Key Management security policies and procedures to determine that each type of cryptography is defined. Determine whether the policies outline the following: - Tenant-specific encryption; - Security requirements on cryptographic keys; - Use of standardized cryptographic methods; - Use of cryptographic keys.	Inquiry, Inspection, and/or observation	1. Relevant agreements and guidance for applicable legislation and regulations 2. Policies and procedures related to encryption and key management.
Architecture Layer	Scalability/Capacity Management	1. Inquire with the control owner and determine if real time monitoring of system capacity is performed and the dashboard report is available for management review. 2. Inspect the capacity monitoring tools for a sample of production and sandbox instances and determine if they are monitored in real time for. among others. CPU, API request time, web request time, transaction processing time, and report request times. 3. Inspect if monitoring dashboards are available for management review, for individual instances and in aggregate, to enable real-time monitoring and future capacity planning	Inquiry, Inspection, and/or observation	1. Provide Capacity Planning report 2. Provide screenshots of monitoring dashboards 3. ISMS Statement of Applicability
Architecture Layer	Scalability/Capacity Management	1. Verify that there is a formally documented capacity plan associated with critical systems and infrastructure. 2. Inquire with the control owner to determine whether business continuity objectives are considered while developing capacity plans. 3. Review the capacity plan and validate that: - Required capacity is provided, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles; - Provisions such as prioritizing tasks, fault-tolerance mechanisms and resource allocation practices are in place; - Business criticality of systems are taken into account while determining capacity; - Projections of future capacity requirements take into account business strategy and plans.	Inquiry, Inspection, and/or observation	1. Audit and accountability policies and procedures addressing audit storage capacity 2. Evidence showing storage capacity.
Architecture Layer	Scalability/Capacity Management	1. Examine security policies and procedures to validate a process to follow up on availability, performance, and capacity baselines exists 2. Examine sample of deviations from availability, performance, and capacity	Inquiry, Inspection, and/or observation	1. Security policies and procedures detailing process of remediating capacity deviations 2. Record of capacity deviations and subsequent

TABLE 13-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD-As per engagement)	Request List (#)
Architecture Layer	Availability	baselines and records which indicate appropriate actions were taken to address outstanding issues. 3. Determine through inquiry and inspection of reporting how follow up activities to deviations are tracked, measured, and reported to executives or the Board of Directors.	Inquiry, Inspection, and/or observation	remediation actions taken 3. Executive/Board reporting on handled capacity management incidents.
		For in-scope Blockchain production systems: 1. Inquire with the control owner and determine whether production systems are monitored for availability and capacity, and any incidents are documented in a ticketing system. 2. Obtain a population of incident tickets, select a sample, and inspect the ticket details for the selected sample of organization services incident tickets from the workflow ticketing system and determine whether the incident determine the incidents were assigned an impacted environment, impacted account, subject and description, incident type, severity rating, and customer impacted and were resolved or are being actively worked to resolution. 3. Inspect the configurations within the monitoring tool for a sample of production servers, selected from the inventory management system, and determine whether the servers were configured to be monitored for availability and capacity and notify personnel in the event an issue was identified. 4. Obtain a population of incident tickets, select a sample of high severity performance incident tickets, and inspect the sample of incident tickets to determine the incidents were assigned an impacted environment, impacted account, subject and description, incident type, severity rating, and customer impacted and were resolved or are being actively worked to resolution.		1. System generated list of incident tickets for the period under review (to be specified) with screenshot of parameters used to generate the listing. 2. Incident tickets for selected sample. 3. Incident dashboard for population of performance incidents tickets for the period under review (to be specified). 4. Tickets for the samples of high severity performance incidents

[0148] In some embodiments, blockchain architecture layer risk category in the blockchain risk framework covers relevant risks, control objectives and descriptions, testing objectives and procedures, and reporting parameters designed to address assurance and compliance needs for the blockchain architecture stack/layer supporting blockchain

permitted and/or permitted networks operations and participant lifecycle management.

[0149] The sub-risk categories, control and testing objectives, test procedures and request lists for Operational Layer risk category are provided below in Tables 14-16.

TABLE 14

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Operational Layer	Permissioned Network Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-PN1	As the Blockchain is implemented, the nature of the instance (permissioned/non permissioned. use case etc.) is not aligned with and the governance practices put in place.	L, M, H
Operational Layer	Participant Onboarding and Off-	Strategic, Operational, Financial,	OL-PO1	User access controls are not enforced, allowing unauthorized individuals to have access to	L, M, H

TABLE 14-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
	boarding	Compliance, Legal, or Reputational		systems and SOA services.	
Operational Layer	Application Layer	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-AL1	The Blockchain technology's impact on the controls attestations (SOC 1/SOC 2 reports) or the Financial Statement/SOX audit scope is not assessed and therefore the potential impact is unknown and not managed.	L, M, H
Operational Layer	Application Layer	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-AL2	Risk and audit plans are not updated and therefore do not reflect and address the risks associated with the Blockchain technology.	L, M, H
Operational Layer	Blockchain Consensus Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-BC1	Consensus mechanisms implemented do not provide comfort on the immutability of the data stored on the Blockchain.	L, M, H
Operational Layer	Blockchain Consensus Program Management	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-BC2	Consensus mechanisms implemented do not provide comfort on the immutability of the data stored on the Blockchain.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW1	The setup of the Blockchain software lacks consideration of new security requirements to maintain confidentiality, integrity, and availability.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW2	Hardware (including configurations, locations, capacity/capacity utilization, and age and data requirements) impacted by the Blockchain integration have not been collected and evaluated, potentially causing an unknown impact.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW3	Applications, software and software components impacted by the Blockchain software integration have not been identified and evaluated.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW4	User access and segregation of duties controls are not enforced, allowing unauthorized users to migrate Blockchain process configurations into production.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW5	System development or maintenance on a system with Blockchain dependencies are not identified and evaluated, potentially causing an unknown impact.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW6	The legacy system Software Development Lifecycle methodology for change management processes does not reflect the integration with the Blockchain program management.	L, M, H
Operational Layer	Integration with off-Blockchain Systems and Processes	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-IW7	Business process changes with Blockchain dependencies are not identified and evaluated, potentially causing an unknown impact.	L, M, H

TABLE 14-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Operational Layer	Smart Contracts	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-SC2	Blockchain data is stored on off-chain databases that are unsecure	L, M, H
Operational Layer	Smart Contracts	Strategic, Operational, Financial, Compliance, Legal, or Reputational	OL-SC3	The organization lacks a complete governance structure to provide oversight and security for hard forks in the blockchain architecture	L, M, H

TABLE 15

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-scope (TBD-As per engagement)
Operational Layer	Permissioned Network Management	As the Blockchain is implemented, there is alignment with the nature of the instance (permissioned/non permissioned. use case etc.) and the governance practices put in place. An appropriate governance regime is designed and agreed, if required across all participants in the network.	A Blockchain steering committee, which includes executive leadership and senior members of the business, risk, compliance and the Blockchain program management, meets on a quarterly basis to conduct business performance reviews of how the Blockchain aligns with IT Governance.	In-scope
Operational Layer	Participant Onboarding and Off-boarding	All access is logged and monitored and SOA services maintain the appropriate restricted access.	All access is logged and monitored. SOA services are restricted from being accessed by anyone other than whitelisted processes/clients.	In-scope
Operational Layer	Application Layer	Management has engaged appropriate members of internal and external audit to assess if the Blockchain technology will have an impact on the controls attestations (SOC 1/SOC 2 reports) or the Financial Statement/SOX audit scope.	The Blockchain Program management meets with external SOC 1/Financial Statement audit teams to review the status of the project plan and future the Blockchain process considerations and management's assessment on impact of the Blockchain technology to the audit scope.	In-scope
Operational Layer	Application Layer	Internal audit has been properly engaged and the Blockchain program is being considered in the internal audit scoping exercises.	The Blockchain management team meets regularly with members of risk and internal audit in each business unit leveraging the Blockchain technology to ensure the risk and audit plans are evolving to address the Blockchain risks.	In-scope
Operational Layer	Blockchain Consensus Program Management	As Blockchain programs are designed and implemented, appropriate consensus mechanisms are agreed upon, implemented and controlled to provide comfort on the immutability of the data stored on the Blockchain. Appropriate controls are designed and implemented to safeguard the immutability of data captured on the blockchain.	Blockchain consensus mechanisms that assure immutability are designed implemented and the associated controls are documented and approved by the business and the Blockchain program management. Blocks are created for transactions validated through blockchain consensus mechanism and cannot be modified once written.	In-scope
Operational Layer	Blockchain Consensus Program Management	Conesus mechanism automatically determines whether the trade details match between counterparties or not. Automatic validation will not take place if consensus is not reached.	Economic trade terms are validated through blockchain consensus mechanism and automatically recorded on the blockchain network in a timely manner.	In-scope

TABLE 15-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-scope (TBD-As per engagement)
Operational Layer	Integration with off-Blockchain Systems and Processes	The Blockchain software is aligned with new security requirements to maintain confidentiality, integrity, and availability.	The Blockchain software for initial integration into the firm's environment follows a well-defined integration plan and is monitored by the Blockchain program management.	
Operational Layer	Integration with off-Blockchain Systems and Processes	Hardware impacted by the Blockchain integration is documented and evaluated, and results are escalated to the Blockchain steering committee.	Impact of software integration on the firm's existing hardware configurations, software and applications is documented and evaluated. The results of this evaluation are reported to the Blockchain steering committee.	In-scope
Operational Layer	Integration with off-Blockchain Systems and Processes	Applications and software impacted by the Blockchain integration is documented and evaluated, and results are escalated to the Blockchain steering committee.	Impact of software integration on the firm's existing hardware configurations, software and applications is documented and evaluated. The results of this evaluation are reported to the Blockchain steering committee.	In-scope
Operational Layer	Integration with off-Blockchain Systems and Processes	Operations policies and procedures have been updated to include integration with the Blockchain prior to the Blockchain change being placed into production.	Access to migrate the Blockchain process configurations into production is restricted to personnel who are independent of the configuration team. Access to migrate the Blockchain process configurations into production is periodically reviewed to ensure access is restricted to personnel.	In-scope
Operational Layer	Integration with off-Blockchain Systems and Processes	Impact of legacy system development and maintenance on the Blockchain configuration is considered during legacy System Development Lifecycle for legacy systems. Impacts to interfaces between legacy systems have been identified., e.g. data flow architecture	Business Unit IT management notifies the Blockchain program management if system development or maintenance on a system has been identified as having the Blockchain dependencies. The Blockchain program management evaluates the impact the legacy system change will have on the Blockchain. Details of the evaluation are documented. If the Blockchain process is impacted, the Blockchain is removed from production and a back out plan is enabled while a configuration change order is processed.	In-scope
Operational Layer	Integration with off-Blockchain Systems and Processes	An inventory, including functional use, of all key interfaces and legacy systems utilized by the Blockchain is maintained. Impacts to interfaces between legacy systems have been identified., e.g. data flow architecture	The legacy system Software Development Lifecycle methodology for change management processes has been updated to include integration with the Blockchain program management prior to making changes to the Blockchain impacted systems or interfaces.	In-scope
Operational Layer	Integration with off-Blockchain Systems and Processes	The Blockchain is reconfigured when changes in business processes affect the Blockchain. Management considers both the downstream and upstream impact of changes to business processes and the use of the Blockchain technology.	Business Unit Operations management notifies the Blockchain program management if a business process change has been identified as having the Blockchain dependencies. The Blockchain program management evaluates the impact the business process change will have on the Blockchain configuration. Details of the evaluation are documented. If a Blockchain process is impacted, the	In-scope

TABLE 15-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/Out-of-scope (TBD-As per engagement)
			Blockchain is removed from production and back out plan is enabled while a configuration change order is processed.	

TABLE 16

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Request List (#)
Operational Layer	Permissioned Network Management	1. Inquire with management about the process of ensuring alignment with the nature of the instance and the government practices put in place. 2. Obtain relevant documentation evidencing the consideration of the alignment. 3. Obtain a listing of the individuals on the Blockchain steering committee. 4. Obtain evidence for the most recent quarterly meeting (meeting minutes/meeting invites) to verify that meeting took place and included members of the Blockchain steering committee. 5. Through inspection of the results of business performance review, verify an appropriate review was performed of how the Blockchain aligns with IT Governance.	Inquiry, Inspection, and/or observation	1. Listing of the individuals on the Blockchain steering committee 2. Evidence for the most recent quarterly meeting (meeting minutes/meeting invites/emails) showing the meeting took place 3. Documentation/ results of the quarterly business performance review of how the Blockchain aligns with IT Governance 4. Documentation leveraged when considering the alignment
Operational Layer	Participant Onboarding and Off-boarding	1. Inquire with management about the process and frequency in which access is logged and monitored. 2. Obtain a listing of users with access to the SOA services. 3. Obtain documentation showing that all access is logged and monitored and through inspection, verify that only users with permissioned access appear on the listing.	Inquiry, Inspection, and/or observation	1. Listing of users with access to the SOA services 2. Documentation showing all access is logged and monitored 3. Screenshot showing how access is logged and monitored
Operational Layer	Application Layer	1. Obtain evidence for the most recent meeting (meeting minutes/meeting invites) to verify the meeting took place and included members of the Blockchain Program management team. 2. Through inspection of the documentation of the assessment, verify the assessment was performed and the results were documented.	Inquiry, Inspection, and/or observation	1. Evidence for the most recent meeting (meeting minutes/meeting invites/emails) showing the meeting took place 2. Documentation of management's assessment on the impact of the Blockchain technology to the audit scope
Operational Layer	Application Layer	1. Obtain evidence for the most recent meeting (meeting minutes/meeting invites) to verify the meeting took place and included members of the Blockchain management team. 2. Through inspection of an updated risk and audit plan, verify changes and updates have been made to reflect the Blockchain program.	Inquiry, Inspection, and/or observation	1. Evidence for the most recent meeting (meeting minutes/meeting invites/emails) showing the meeting took place 2. Risk and audit plan updated to address Blockchain risks
Operational Layer	Blockchain Consensus Program Management	1. Inquire with management about the process in which appropriate consensus mechanisms are agreed upon, implemented and controlled, 2. Obtain documentation of the associated controls.	Inquiry, Inspection, and/or observation	1. Documentation of the associated controls for a new Blockchain consensus mechanism 2. Evidence of the

TABLE 16-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Request List (#)
Operational Layer	Blockchain Consensus Program Management	3. Through inspection of documentation evidencing associated controls have been documented, verify these controls were reviewed and approved by the business and the Blockchain program management. 1. Inquire with management about the process in which appropriate consensus mechanisms are agreed upon, implemented and controlled. 2. Obtain documentation of the associated controls. 3. Through inspection of documentation evidencing associated controls have been documented, verify these controls were reviewed and approved by the business and the Blockchain program management.	Inquiry, Inspection, and/or observation	review and approval by the business and the Blockchain program management
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Inquire with management about the process of ensuring alignment with new security requirements. 2. Obtain the integration plan used for initial integration. 3. Through inspection of the integration plan, verify that there is evidence that the integration plan is monitored by the Blockchain program management.	Inquiry, Inspection, and/or observation	1. Integration plan used for initial integration 2. Evidence showing the integration plan is monitored
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Obtain the documentation of the impact of software integration 2. Through inspection of the documentation, verify any impacts identified were appropriately evaluated. 3. Obtain evidence of the communicated results and through inspection, verify the results of the evaluation were reported to the Blockchain steering committee.	Inquiry, Inspection, and/or observation	1. Documentation showing the evaluation performed of the impact of software integration on the firm's existing hardware configurations 2. Evidence of communication to the Blockchain steering committee
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Obtain the documentation of the impact of software integration. 2. Through inspection of the documentation, verify any impacts identified were appropriately evaluated. 3. Obtain evidence of the communicated results, and through inspection, verify the results of the evaluation were reported to the Blockchain steering committee.	Inquiry, Inspection, and/or observation	1. Documentation showing the evaluation performed of the impact of software integration on the firm's existing hardware configurations 2. Evidence of communication to the Blockchain steering committee
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Obtain a listing of users with access to migrate the Blockchain process configurations. 2. Obtain evidence for the most recent periodic review performed of access, and through inspection verify access was restricted to personnel. 3. Obtain the Operations policies and procedures Blockchain evidencing the updates made to include integration with the Blockchain with a date in which these updates were made. 4. Obtain evidence of the Blockchain change being placed into production and the date in which this occurred. 5. Through inspection, verify the updates were made to the policies and procedures prior to the change being placed into production.	Inquiry, Inspection, and/or observation	1. Listing of users with access to migrate the Blockchain process configurations 2. Evidence that a periodic review was performed of restricted access and including evidence of the review 3. Operations policies and procedures updated with the integration with Blockchain with the date in which the updates were made 4. Evidence of the change being placed into production (change order ticket including the date in which the request was processed and completed)

TABLE 16-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Request List (#)
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Obtain evidence of communication between Business Unit IT management and the Blockchain program management of a system identified as having Blockchain dependencies. 2. Verify the Blockchain program management performed an evaluation of the impact the legacy system change has on the Blockchain. 3. Obtain documentation verifying the details of the evaluation were documented. 4. Obtain evidence of a processed change order request to remove the Blockchain from production and through inspection, verify the request was completed. 5. Obtain documentation of the back out plan and through inspection, verify that the back out plan was enabled while a configuration change order was processed.	Inquiry, Inspection, and/or observation	1. Evidence of communication between Business Unit IT management and the Blockchain program management for a system identified as having Blockchain dependencies 2. Evaluation performed by the Blockchain program management 3. Evidence that the Blockchain was removed from production 4. Change order ticket showing this request was processed and completed 5. Back out plan that was enabled
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Inquire with management about the process of updating the methodology to include integration with Blockchain program management. 2. Obtain documentation verifying change management processes have been updated with the date in which these updates were made. 3. Obtain evidence of the changes made to the Blockchain and the date in which these changes were made. 4. Through inspection, verify that the updates were made to the methodology prior to the changes being made. 5. Obtain the inventory listing and through inspection, verify the listing includes functional use of all key interfaces and legacy systems utilized by the Blockchain and that the listing is properly maintained.	Inquiry, Inspection, and/or observation	1. The legacy system Software Development Lifecycle methodology for change management processes updated with Blockchain with the date in which the updates were made 2. Evidence of the changes made to the Blockchain impacted system (change order ticket including the date in which the request was processed and completed) 3. Inventory listing with evidence of how the listing is maintained
Operational Layer	Integration with off-Blockchain Systems and Processes	1. Obtain evidence of communication between Business Unit Operations and the Blockchain program management of a business process identified as having Blockchain dependencies. 2. Verify the Blockchain program management performed an evaluation of the impact the legacy system change has on the Blockchain. 3. Obtain evidence verifying the details of the evaluation were documented. 4. Obtain evidence of a processed change order request to remove the Blockchain from production and through inspection, verify the request was completed. 5. Obtain documentation of the back out plan and through inspection, verify that the back out plan was enabled while a configuration change order was processed.	Inquiry, Inspection, and/or observation	1. Evidence of communication between Business Unit IT management and the Blockchain program management 2. Evaluation performed by the Blockchain program management 3. Evidence that the Blockchain was removed from production 4. Change order ticket showing this request was processed 5. Back out plan that was enabled

4.6 Transactional Layer Assessment Work Program

[0150] In some embodiments, transaction layer risk category in the blockchain risk framework covers relevant risks, control objectives and descriptions, testing objectives and procedures, and reporting parameters designed to

address assurance and compliance needs for the blockchain application stack/layer supporting business and transaction level processing.

[0151] The sub-risk categories, control and testing objectives, test procedures and request lists for Transactional Layer risk category are provided below in Tables 17-19.

TABLE 17

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC1	Incorrect SC terms are not selected for execution.	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC2	SC terms and conditions are not inclusive of required information or standard terms and conditions.	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC3	SC is executed with wrong/incorrect participants or SC does not include right/correct participants.	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC4	SC is not reviewed, appraised, and approved by appropriate participants during or before execution.	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC5	SC is completed without execution of required terms and conditions by all participants.	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC6	Required events (e.g. invoicing, payments, change or ownership) are not initiated and completed successfully during or after SC execution.	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC7	Privileged access is not appropriately restricted, logged, and monitored for Smart Contracts, which can create a risk of unauthorized access to Smart Contracts by developers/admins/database admins	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC8	End-user access is not appropriately restricted, creating the risk of unauthorized changes/deployments/executions/updates/modifications performed for the Smart Contract and workflow	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC9	Smart Contract development and change management process is not in place and followed, which may lead to unauthorized unilateral actions by developers to modify or remove Smart Contract functions or introduce unnecessary or insecure functions	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC10	Smart Contract development and change management process is not in place and followed, which may lead to inappropriate and incorrect terms and conditions [e.g. timeline, pricing, resources, invoicing, settlement, etc.] defined for the Smart Contract	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC11	Smart Contract development and change management process is not in place and followed, which may lead to inappropriate and incorrect assets and services defined for the Smart Contract	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC12	Smart Contract development and change management process is not in place and followed, which may lead to inappropriate and incorrect participants defined for the Smart Contract	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC13	Smart Contract development and change management process is not in place and followed, which may lead to unauthorized or incorrect Smart Contracts being introduced into the production environment	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC14	Unauthorized access to Blockchain metadata or PII by unauthorized parties for development or testing purposes	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC15	Data is not retained for DLT inputs. PKIs. or other critical systems; lack of availability limits backup and recovery capability	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC16	Input validation mechanisms for fields and records are not in place, which may compromise the Smart Contract execution	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC17	Security mechanisms are not in place or effective in protecting output (data), creating the risk of unauthorized access or changes made to output	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC18	Security mechanisms are not in place or effective in protecting Smart Contracts mid their exposure to unauthorized parties via export and sharing functionalities	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC19	Mechanisms are not in place or effective in ensuring subsequent Smart Contracts are only triggered when appropriate and when needed	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC20	Mechanisms are not in place or effective in ensuring subsequent smart contracts, invoicing, billing is triggered and processed appropriately as and if needed	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC21	Mechanisms are not in place or effective in ensuring subsequent movement of digital assets is triggered and processed appropriately as and if needed	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC22	Mechanisms are not in place or effective in ensuring subsequent digital tokens are triggered and processed appropriately as and if needed	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC23	Monitoring mechanisms are not in place for Smart Contracts, which can lead to non-detection of Smart Contracts not performing as intended in the production environment	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC24	Monitoring mechanisms are not in place for Smart Contracts, which can create a risk of impaired network performance or latency	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC25	Monitoring mechanisms are not in place for Smart Contracts, which can create a risk of the Smart Contract not being executed and completed as per defined terms	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC26	Monitoring mechanisms are not in place for Smart Contracts, which can create a risk of the Smart Contract not being retired appropriately if necessary	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC27	Monitoring mechanisms are not in place for Smart Contracts, which can create a risk of the Smart Contract being deployed, modified, or changed by unauthorized participants	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC28	Smart Contract privacy is not maintained throughout the Smart Contract lifecycle, creating the risk of private information being divulged, shared, or disseminated	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC29	Interfaces are not configured to ensure all process data transmissions within the blockchain are complete, accurate, and secure	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC30	Interfaces are not configured to ensure all process data transmissions to off-chain platforms or systems are complete, accurate, and secure	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC31	Smart Contract architecture is unable to be updated/modified and therefore does not comply with new requirements or regulations or is vulnerable to newly-discovered security issues	L, M, H
Transactional (Business)	Smart Contracts (SC)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-SC32	Insufficient side chain safeguards increase risk of incidents leading to loss or invalidation of assets or transactions related to Smart Contracts	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA1	Incorrectly DA onboarding may cause delay or compromise transactional level processing.	L, M, H
	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA2	DA ownership is transferred incorrectly which may compromise transactional level processing.	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA3	DA is not managed and maintained appropriately during its lifecycle.	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA4	DA is not retired appropriately at the end of the lifecycle.	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA5	Privileged access is not appropriately restricted, logged, and monitored for Digital Assets, which can lead to unauthorized access	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA6	End-user access is not appropriately restricted, creating the risk of unauthorized changes/deployments/executions/updates/modifications performed for the Digital Assets and workflow	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA7	Digital Assets are not configured with strong login credentials and account security protocols to restrict unauthorized access	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA8	Digital Assets are stored in an unsecure environment, and hot/warm/cold risk factors systemic to each Digital Asset platform are not taken into account, creating greater risks to Digital Asset operations and security of transaction data	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA9	Participants are not appropriately and correctly defined which can lead to unauthorized access or operation of the Digital Asset	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA10	Digital Assets are not appropriately or correctly protected, managed, and monitored throughout their life cycle	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA11	Unauthorized or incorrect Digital Asset platforms are introduced, compromising the security of the organization's Digital Asset environment	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA12	Digital Asset software is not updated in accordance with required updates, leading to version mismatching and potential compromises to security or operational limitations	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA13	Digital Asset management platforms are not configured with recover) procedures to recover loss of data and information	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA14	Mechanisms are not in place or effective in ensuring Digital Asset transactions are triggered as and if needed	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DA15	Monitoring mechanisms are not in place for Digital Assets, which can lead to non-detection of Digital Assets not performing as	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Digital Assets (DA)	Legal, Reputational Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA16	intended in the production environment Monitoring mechanisms are not in place for Digital Assets, which can create a risk of impaired network performance or latency	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA17	Monitoring mechanisms are not in place for Digital Assets, which can create a risk of a Digital Asset not being utilized per defined terms	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA18	Monitoring mechanisms are not in place for Digital Assets, which can create a risk of the Digital Asset not being retired appropriately if necessary	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA19	Monitoring mechanisms are not in place for Digital Assets, which can create a risk of the Digital Asset being utilized, modified, or changed by unauthorized participants	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA20	Digital Asset privacy is not maintained throughout the Digital Asset lifecycle, creating the risk of private information being divulged, shared, or disseminated	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA21	Interfaces are not configured to ensure all process data transmissions within the blockchain are complete, accurate, and secure	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA22	Interfaces are not configured to ensure all process data transmissions to off-chain platforms or systems are complete, accurate, and secure	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA23	Without price fluctuation monitoring and defined response/action plan, assets, contracts, tokens can be processed with incorrect value at a given point in time	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA24	Fluctuations in prices for commodity items like Digital Asset storage create opportunities for sunk costs or deadweight loss expenditures	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA25	Digital Assets within the organization are not linked with soft or intangible assets (i.e. human resources) causing lack of operational alignment across the organization	L, M, H
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA26	Digital Assets within the organization are not linked with other real world assets (i.e. real estate, property, etc.) causing lack of operational alignment across the organization	L, M, H
Transactional (Business)	Digital Assets	Strategic, Operational,	TL-DA27	The existence of physical/ logical assets is not tracked	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
	(DA)	Financial, Compliance/ Legal, Reputational		or managed on a regular basis, causing inaccurate and incomplete representation of physical assets in a digital form	
Transactional (Business)	Digital Assets (DA)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DA28	The organization's legacy system accounts are not linked with DLT associated Digital Assets, causing lack of operational alignment across the organization	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT1	Participants are not on-boarded for DC transactions.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT2	Account balance cannot support DC transaction request for processing.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT3	DC-in requests are not processed correctly.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT4	DC-out requests are not processed correctly.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT5	DC duplicate transactions are processed.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT6	DC transactions are approved.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT7	DC transaction information is missing which may compromise transaction processing.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT8	Address is not generated or shared with participants for DC transactions.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT9	Cancelled or failed transactions are not tracked or processed correctly.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT10	DC is not moved from one participant to the other (e.g. payor and payee) correctly and in a timely manner.	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT11	DC is not evaluated correctly relative to underlying asset or currency.	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT12	Privileged access is not appropriately restricted, logged, and monitored for Digital Tokens, which can lead to unauthorized access	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT13	End-user access is not appropriately restricted, which can lead to unauthorized changes/updates/modifications performed for the Digital Tokens and workflow	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT14	Digital Tokens are not configured with strong login credentials and account security protocols to restrict unauthorized access	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT15	Digital Token development and change management process is not in place and followed, which may lead to inappropriate and incorrect participants defined for authorized use of Digital Tokens	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT16	Digital Tokens are not appropriately or correctly protected, managed, and monitored throughout their life	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT17	Digital Tokens are not monitored appropriately throughout their life cycle causing inaccurate records for when tokens were created, converted, updated, and retired	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT18	Digital Token development and change management process is not in place and followed, which may lead to unauthorized or incorrect Digital Tokens being introduced into the operational environment	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT19	Lack of a clearly defined Digital Token platform can potentially endanger the organization's transactional data or create unauthorized operational redundancies	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT20	Digital Token platforms are not configured with recovery procedures to recover loss of data and information	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT21	Ownership of assets linked to Digital Tokens is not defined or managed by the organization	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DT22	Data is not retained for DLT inputs, PKIs, or other critical systems; lack of availability	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
		Compliance/ Legal, Reputational		limits backup and recovery capability	
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT23	Mechanisms are not in place or effective in ensuring Digital Token transactions are triggered as and if needed	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT24	Digital Tokens are not monitored to ensure tokens are utilized appropriately for authorized transactions or operations	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT25	Digital Token ownership and management of ownership is not monitored appropriately	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT26	The DLT and off-chain ledger or accounting mechanisms are not monitored, compromising the ability to accurately track usage of tokens during normal operations and transactions	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT27	Monitoring mechanisms are not in place for Digital Tokens, which can create a risk of Digital Tokens being utilized, modified, or changed by unauthorized participants	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT28	Interfaces are not configured to ensure all process data transmissions within the blockchain are complete, accurate, and secure	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT29	Interfaces are not configured to ensure all process data transmissions to off-chain platforms or systems are complete, accurate, and secure	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT30	Without price fluctuation monitoring and defined response/ action plan, tokens, contracts, tokens can be processed with incorrect value at a given point in time	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT31	Fluctuations in prices for commodity items like Digital Token storage create opportunities for sunk costs or deadweight loss expenditures	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT32	The existence of digital tokens or funds used for blockchain transactions are not validated	L, M, H
Transactional (Business)	Digital Tokens (DT)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DT33	Digital tokens are not configured with strong login credentials and account security protocols to restrict unauthorized access	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial,	TL-DW01	Privileged access is not appropriately restricted, logged, and monitored for Digital Wallets,	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
		Compliance/ Legal, Reputational		which can lead to unauthorized access to Digital Wallets	
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW02	End-user access is not appropriately restricted, creating the risk of unauthorized changes/deployments/executions/updates/modifications performed for Digital Wallets and workflow	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW03	Digital Wallets are not configured with strong login credentials and account security protocols to restrict unauthorized access	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW04	Digital Wallets, ledgers, and access points are stored in an insecure environment, and hot/warm/cold risk factors systemic to each wallet platform are not taken into account, creating greater risks to Digital Wallet operations and security of transaction data	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW05	Digital Wallet development and change management process is not in place and followed, which may lead to inappropriate and incorrect participants defined for the Digital Wallet	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW06	Digital Wallet development and change management process is not in place and followed, which may lead to unauthorized or incorrect Digital Wallets being introduced into the environment	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW07	Digital Wallet software is not updated in accordance with required updates, leading to version mismatching and potential compromises to security or operational limitations	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW08	Lack of a clearly defined Digital Wallet platform can potentially endanger the organization's transactional data, create unauthorized operational redundancies, or inhibit consistent and effective risk management of specific Digital Wallet platforms (i.e. software, hardware, ledger, etc.)	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW09	Digital Wallet platforms are not configured with recovery procedures to recover lost data and information	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW10	Data is not retained for DLT inputs, PKIs, or other critical systems, lack of availability limits backup and recovery capability	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/ Legal, Reputational	TL-DW11	Input validation mechanisms for fields and records are not in place, which may compromise the Digital Wallet's operations	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW12	Security mechanisms are not in place or effective in protecting output (data), creating the risk of unauthorized access or changes made to output	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW13	Security mechanisms are not in place or effective in protecting Digital Wallets and their exposure to unauthorized parties via export and sharing functionalities	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW14	Mechanisms are not in place or effective in ensuring Digital Wallet transactions are only triggered when appropriate and when needed	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW15	Mechanisms are not in place or effective in ensuring off-chain invoicing and billing is triggered and processed by authorized participants appropriately as and if needed	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW16	Mechanisms are not in place or effective in ensuring digital token transactions are triggered and processed appropriately as and if needed	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW17	Mechanisms are not in place or effective in ensuring subsequent Digital Wallet transactions are triggered and processed by authorized participants and appropriately as and if needed	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW18	Monitoring mechanisms are not in place for Digital Wallets, which can lead to non-detection of Digital Wallets not performing as intended in the environment	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW19	Monitoring mechanisms are not in place for Digital Wallets, which can create a risk of impaired network performance or latency	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW20	Mechanisms are not in place to monitor Digital Wallet transactions and ensure transactions are executed per defined terms	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW21	Monitoring mechanisms are not in place for Digital Wallets, which can create a risk of the Digital Wallet not being retired appropriately if necessary	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW22	Monitoring mechanisms are not in place for Digital Wallets, which can create a risk of the Digital Wallet being utilized, modified, or changed by unauthorized participants	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW23	Digital Wallet privacy is not maintained throughout the Digital Wallet lifecycle, creating the risk of private information being divulged, shared, or disseminated	L, M, H

TABLE 17-continued

Risk Category	Domain	Risk Classification	Risk Number	Risk Description	Risk Level (L, M, H) (As applicable)
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW24	Interfaces are not configured to ensure all process data transmissions within the blockchain are complete, accurate, and secure	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW25	Interfaces are not configured to ensure all process data transmissions to off-chain platforms or systems are complete, accurate, and secure	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW26	Mechanisms are not in place or effective in ensuring Digital Wallets are configured with appropriate transaction thresholds to prevent failed detection of transferred funds	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW27	Security mechanisms are not in place for Digital Wallets, compromising private keys or PKIs, which may result in breaches of Digital Wallet security or risk of unauthorized access to assets stored on the wallet platform	L, M, H
Transactional (Business)	Digital Wallets (DW)	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-DW28	The organization's legacy system accounts are not linked with PKIs or DLTs associated with the Digital Wallet, causing lack of operational alignment across the organization	L, M, H
Transactional (Business)	Clearing and Settlement	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-CS1	Movement of underlying asset or currency is not synchronized with books of records.	L, M, H
Transactional (Business)	Buisness Use case transactions	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-BU1	Transactions are not approved.	L, M, H
Transactional (Business)	Buisness Use case transactions	Strategic, Operational, Financial, Compliance/Legal, Reputational	TL-BU2	Transactions are not processed accurately, completely or within approved guidelines.	L, M, H

TABLE 18

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/ Out-of-Scope (TBD—As per engagement)
Transactional (Business)	Smart Contracts (SC)	Control(s) is in place to ensure correct template is used for SC execution.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Smart Contracts (SC)	Control(s) is in place to ensure that required information or standard terms and conditions are included in the SC before execution.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope

TABLE 18-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/ Out-of-Scope (TBD—As per engagement)
Transactional (Business)	Smart Contracts (SC)	Control(s) is in place to ensure that required and correct participants associated with the SC before execution.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Smart Contracts (SC)	Control(s) is in place to ensure that SC is reviewed, appraised, and approved by appropriate participants.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Smart Contracts (SC)	Control(s) is in place to ensure that SC is executed after terms and conditions are met by all participants.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Smart Contracts (SC)	Control(s) is in place to ensure that required events (e.g. invoicing, payments, change or ownership) are initiated and completed successfully during or after SC execution. Upon consensus, smart contracts automatically executes the exchange of position and cash in a complete, accurate and timely manner.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Assets (DA)	Control(s) is in place to ensure that DAs are classified and created correctly and successfully for transactional level processing.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
	Digital Assets (DA)	Control(s) is in place to ensure that DA ownership is transferred to the right/correct participants in a timely manner.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Assets (DA)	Control(s) is in place to ensure that DA is managed and maintained (e.g. classification, valuation, and handovers) appropriately throughout the lifecycle.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Assets (DA)	Control(s) is in place to ensure that DA is retired appropriately at the end of the lifecycle.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that valid participants are on-boarded and assigned with a digital wallet for DC transactions.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that a payor account balance is checked and verified to validate that sufficient DC is available before the transaction is processed or completed.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that DC-in (Cash-in) requests are processed completely and accurately.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that DC-out (Cash-out) requests are processed completely and accurately.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that a duplicate DC transactions are not processed.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency	Control(s) is in place to ensure that a DC transactions are approved appropriately for	Inquire management of the control activities that are	In-scope

TABLE 18-continued

Risk Category	Domain	Control/Test Objective	Control Description	In-scope/ Out-of-Scope (TBD—As per engagement)
	(DC)	processing.	in place to meet applicable risks and relevant control objectives.	
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that a DC transactions contain required information for processing.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that a valid unique address is generated and shared with appropriate participants in safe and secure manner for DC transactions processing.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that cancelled and failed transactions are monitored, processed and recorded in the books accurately.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that DC is moved from one participant to the other (e.g. payee and payor) correctly and in a timely manner. Also, the movement of DC is recorded in the books of records accurately.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Digital Currency (DC)	Control(s) is in place to ensure that DC is evaluated correctly relative to underlying asset or currency in a timely manner.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Clearing and Settlement	Control(s) is in place to ensure that books of records are updated when the underlying asset or currency is processed. Reconciliation and verification between books of records and underlying asset or currency position is performed to validate integrity, accuracy and completeness of transactional and business information. Control(s) is in place to ensure that trades/transactions processing meet the following financial statements assertion requirements: 1—Rights and obligations 2—Completeness, accuracy, cutoff 3—Existence 4—Valuation	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Business Use case transactions	Control(s) is in place to ensure that business transactions are authorized and executed in accordance with approved guidelines.	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope
Transactional (Business)	Business Use case transactions	Control(s) is in place to ensure that trades/transactions meet the following financial statements assertion requirements: 1—Rights and obligations 2—Completeness, accuracy, cutoff 3—Existence 4—Valuation	Inquire management of the control activities that are in place to meet applicable risks and relevant control objectives.	In-scope

TABLE 19

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Re-quest List (#)
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	

TABLE 19-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Re-request List (#)
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Smart Contracts (SC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Assets (DA)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
	Digital Assets (DA)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Assets (DA)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Assets (DA)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	

TABLE 19-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Re-request List (#)
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
		results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software		
Transactional (Business)	Digital Currency (DC)	Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	

TABLE 19-continued

Risk Category	Domain	Test Procedure (#)	Test Type (TBD—As per engagement)	Re-request List (#)
Transactional (Business)	Digital Currency (DC)	results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
Transactional (Business)	Digital Currency (DC)	results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
Transactional (Business)	Clearing and Settlement	results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
Transactional (Business)	Business Use case transactions	results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	
Transactional (Business)	Business Use case transactions	results test procedures will be designed and data parameters will be identified to configure and operationalize the Blockchain Auditing software Based on the inquiry of the management regarding the control activities in place assessment	Inquiry, Inspection, observation, and/or Automated	

[0152] In one or more embodiments, the blockchain risk framework is designed to produce testing procedures that align with a technology stack associated with a blockchain. FIG. 5A illustrates a correspondence between the testing procedures produced by a risk framework and a technology stack of a blockchain system according to examples of the disclosure. In FIG. 5A, a block chain use-case technology stack can include multiple technology stacks that are integrated together to form the overall blockchain computing system. For instance in the example of FIG. 6, a block-chain use-case technology stack 600 can include an application layer 502, encryption (cryptography) layer 506, a permissioned or unpermissioned network layer (i.e., operational layer) 508, a shared data layer 510, a commercial API layer 512, and an overlay network layer 514.

[0153] In one or more examples, an application layer 502 can include decentralized applications (i.e., a digital application or program) that can be run by many users or nodes on a decentralized network with consensus and other trustless protocols. They can be designed to avoid any single

point of failure. The applications in the application layer provide workflow and processing logic to execute transactional activity using shared communications protocols and interface methods used by hosts in a communications network.

[0154] In one or more examples, an encryption (cryptography) layer 506 can include cryptography used to cipher (encrypt) and de-cipher (decrypt) information by using a mathematical function or algorithm. Encryption can refer to the process of transforming information so it is unintelligible/inaccessible/unreadable to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible/accessible/readable again.

[0155] In one or more examples, a permissioned or unpermissioned network layer 508 can refer to both permissioned networks and unpermissioned networks. Unpermissioned networks can refer to an open blockchain network that anyone can join and participate in. The community operates and administers the blockchain, and one or more participants

can provide consensus. Any user can join a permissionless network, i.e., exchanging digital currency on a public currency exchange. A permissioned network refers to a blockchain model that requires permission to join, read, write to, operate and administer. Multiple participants administer the blockchain under consortium or group leadership. There may be restrictions on how participants can contribute to the system state or consensus of transactions. In one or more examples network layer **508** can also include private blockchains. In a private blockchain, only a centralized entity or single participant has permission to write to the blockchain. Platform architects can decide how to assign permissions.

[0156] In one or more examples, shared data layer **510** can include organized collections of data that are stored and accessed electronically. In one or more example a commercial API layer **512** can include elements dealing with an interface in software that can act as a shared boundary across which two or more separate components of a computer system exchange information. The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these. Finally, in one or more examples, an overlay network layer **514** includes different types of LAN and WAN networks that are used to access the blockchain system. The network layer provides the means of transferring variable-length network packets from a source to a destination host via one or more networks.

[0157] One or more of the risk categories described above can correspond to one or more layers of the stack **500**. For instance, in the example of FIG. 5A, transaction layer risks **518** can correspond to the application layer **502** of the stack **500**. This can mean that test procedures created in response to the “transactional layer” risk framework can create test procedures that validate the application layer of the blockchain use-case stack **500**. Likewise, blockchain architecture layer risks **514** can generate test procedures that test and validate the decentralized protocols layer **504**, and the encryption layer **506**. The operation layer risks **520** can generate tests that can validate and test permissioned network layer **508**. Finally the infrastructure layer risks **516** of the risk framework can create test procedures that can validate and test shared data layer **510**, commercial API layer **512**, and overlay network **514**.

[0158] FIG. 5B illustrates sub-categories corresponding to each risk framework category according to examples of the disclosure. As illustrated in FIG. 5B, each category of risk can include one or more subcategories. For instance, the governance and oversight risk category **530** can include one or more sub-categories including (but not limited to): business objectives, program sponsorship, leadership commitment, MIS and metrics, program management, operational and capital expenditure oversight, and project management. The cyber security risk category **530** can include one or more sub-categories including (but not limited to): cloud security, data security, data privacy, penetration testing, programming security, network security, patch vulnerability, threat detection, and threat response. The infrastructure risk category **534** can include one or more sub-categories including (but not limited to): servers and databases configuration, ITGCs, business continuity and disaster recovery, and IT asset management. The transactional layer risk category **536** can include one or more sub-categories including (but not limited to): smart contracts, digital assets, digital currency, cleaning and settlement, business use and case transactions. The operation layer risk category **538** can include one or

more sub-categories including (but not limited to): permissioned network management, participant over boarding and off-boarding, application layer, blockchain consensus program management, and integration with off-blockchain systems and processes. Finally the blockchain architecture risk category **540** can include one or more sub-categories including (but not limited to): blockchain platform and protocol configuration, hardware security modules, signature management, cryptography, scalability, and availability.

[0159] In some embodiments, the results (i.e. testing procedures and parameters) of an assessment performed using the blockchain risk framework can be used to consolidate the audit and compliance activities into categories by nature of activity at the transaction layer and embed them into an validating software/tool. By drawing data from the underlying blockchain ledger as well as from other up and down stream systems affecting the use case, any and all necessary audit or assurance based procedures can be fully automate and active transparency for them on a real time basis (or some other cadence if preferred) can be provided to the practitioner.

[0160] As illustrated in the discussion above, the risk framework can provide a user interface that translates a user’s blockchain auditing preferences into tangible tests and procedures that are then used to perform real-time continuous monitoring of the block chain system. FIG. 6 illustrates an exemplary process for generating blockchain test procedures according to examples of the disclosure. The process **600** described with respect to FIG. 6 can be performed on a computing system that includes a display and devices that are configured to accept input from a user such as a keyboard, touchpad, mouse, etc.

[0161] The process can begin at step **602**, wherein the user is presented with the risk framework and is prompted by the risk framework to specify a risk level associated with each risk category and sub-category as described above. Once the user specifies the risk levels, the process can move to step **604** wherein the user can be presented with a series of controls of the blockchain that relate to the risks identified in step **602** (as described above). When presented with the series of controls, the user can then be prompted by the risk framework to input which controls are to be in-scope of the assessment, and which ones are to be considered out of scope as described above.

[0162] Once the user indicates which controls are in scope versus out of scope at step **604**, the process can move to step **606**, wherein the risk framework generates one or more test procedures based on the user’s inputs into the risk framework. Once the tests are generated at step **606**, the process can move to step **608** wherein the test procedures are transmitted to an external user. In one or more examples, transmitting the test procedures can include generating a planning file that can be used by a validation software (like the one described with respect to FIG. 4) to perform real-time and continuous validation of a blockchain.

[0163] FIG. 7 illustrates an example of a computing device in accordance with one embodiment. Device **700** can be a host computer connected to a network. Device **700** can be a client computer or a server. As shown in FIG. 7, device **700** can be any suitable type of microprocessor-based device, such as a personal computer, workstation, server, or handheld computing device (portable electronic device) such as a phone or tablet. The device can include, for example, one or more of processor **710**, input device **720**,

output device **730**, storage **740**, and communication device **760**. Input device **720** and output device **730** can generally correspond to those described above and can either be connectable or integrated with the computer.

[0164] Input device **720** can be any suitable device that provides input, such as a touch screen, keyboard or keypad, mouse, or voice-recognition device. Output device **730** can be any suitable device that provides output, such as a touch screen, haptics device, or speaker.

[0165] Storage **740** can be any suitable device that provides storage, such as an electrical, magnetic, or optical memory, including a RAM, cache, hard drive, or removable storage disk. Communication device **760** can include any suitable device capable of transmitting and receiving signals over a network, such as a network interface chip or device. The components of the computer can be connected in any suitable manner, such as via a physical bus or wirelessly.

[0166] Software **750**, which can be stored in storage **740** and executed by processor **710**, can include, for example, the programming that embodies the functionality of the present disclosure (e.g., as embodied in the devices as described above).

[0167] Software **750** can also be stored and/or transported within any non-transitory computer-readable storage medium for use by or in connection with an instruction execution system, apparatus, or device, such as those described above, that can fetch instructions associated with the software from the instruction execution system, apparatus, or device and execute the instructions. In the context of this disclosure, a computer-readable storage medium can be any medium, such as storage **740**, that can contain or store programming for use by or in connection with an instruction execution system, apparatus, or device.

[0168] Software **750** can also be propagated within any transport medium for use by or in connection with an instruction execution system, apparatus, or device, such as those described above, that can fetch instructions associated with the software from the instruction execution system, apparatus, or device and execute the instructions. In the context of this disclosure, a transport medium can be any medium that can communicate, propagate, or transport programming for use by or in connection with an instruction execution system, apparatus, or device. The transport readable medium can include, but is not limited to, an electronic, magnetic, optical, electromagnetic, or infrared wired or wireless propagation medium.

[0169] Device **700** may be connected to a network, which can be any suitable type of interconnected communication system. The network can implement any suitable communications protocol and can be secured by any suitable security protocol. The network can comprise network links of any suitable arrangement that can implement the transmission and reception of network signals, such as wireless network connections, T1 or T3 lines, cable networks, DSL, or telephone lines.

[0170] Device **700** can implement any operating system suitable for operating on the network. Software **750** can be written in any suitable programming language, such as C, C++, Java, or Python. In various embodiments, application software embodying the functionality of the present disclosure can be deployed in different configurations, such as in a client/server arrangement or through a Web browser as a Web-based application or Web service, for example.

[0171] The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the disclosure to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the techniques and their practical applications. Others skilled in the art are thereby enabled to best utilize the techniques and various embodiments with various modifications as are suited to the particular use contemplated.

[0172] Although the disclosure and examples have been fully described with reference to the accompanying figures, it is to be noted that various changes and modifications will become apparent to those skilled in the art. Such changes and modifications are to be understood as being included within the scope of the disclosure and examples as defined by the claims.

[0173] This application discloses several numerical ranges in the text and figures. The numerical ranges disclosed inherently support any range or value within the disclosed numerical ranges, including the endpoints, even though a precise range limitation is not stated verbatim in the specification because this disclosure can be practiced throughout the disclosed numerical ranges.

[0174] The above description is presented to enable a person skilled in the art to make and use the disclosure and is provided in the context of a particular application and its requirements. Various modifications to the preferred embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the disclosure. Thus, this disclosure is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein. Finally, the entire disclosure of the patents and publications referred in this application are hereby incorporated herein by reference.

What is claimed is:

1. A method comprising:

at an electronic device with a display and an interface configured to accept one or more inputs from a user of the electronic device:

displaying one or more risk categories to a user using the display;

prompting the user to input one or more risk levels via the interface, wherein each risk level on the one or more risk levels corresponds to the one or more risk categories displayed;

displaying one or more test objectives or controls via the display;

prompting the user to indicate which of the one or more test objectives are to be evaluated via the displaying; and

wherein in response to the user providing one or more risk levels and one or more test objectives, the electronic device is caused to:

convert the one or more user provided risk levels and one or more test objectives into one or more test procedures to be implemented by a real-time distributed ledger-based computing system validation tool; and

transmit the generated one or more test procedures to an external user.

2. The method of claim 1, wherein the one or more risk categories are selected from a group consisting of government and oversight, cyber security, infrastructure layer, architecture layer, operational layer, and transaction layer.

3. The method of claim 2, wherein if the user selects a transaction layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate an application layer of a distributed ledger-based computing system technology stack.

4. The method of claim 2, wherein if the user selects a blockchain architecture risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a decentralized protocols and encryption layer of a distributed ledger-based computing system technology stack.

5. The method of claim 2, wherein if the user selects an operational layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a permissioned network layer of a distributed ledger-based computing system technology stack.

6. The method of claim 2, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a shared data layer of a distributed ledger-based computing system technology stack.

7. The method of claim 6, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a commercial API layer of a distributed ledger-based computing system technology stack.

8. The method of claim 7, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate overlay network layer of a distributed ledger-based computing system technology stack.

9. The method of claim 1, wherein transmitting the generated one or more test procedures to an external user includes transmitting the generated one or more test procedures to a real-time continuous distributed ledger-based computing system auditing tool.

10. The method of claim 9, wherein transmitting the generated one or more test procedures includes writing the generated one or more test procedures to a planning file, and transmitting the planning file to the real-time continuous distributed ledger-based computing system auditing tool.

11. A computing system, comprising:

a display;

a user interface configured to receive inputs from a user of the system;

a memory;

one or more processors; and

one or more programs, wherein the one or more programs are stored in the memory and configured to be executed by the one or more processors, the one or more programs when executed by the one or more processors cause the processor to:

display one or more risk categories to a user using the display;

prompt the user to input one or more risk levels via the interface, wherein each risk level on the one or more risk levels corresponds to the one or more risk categories displayed;

display one or more test objectives or controls via the display;

prompt the user to indicate which of the one or more test objectives are to be evaluated via the displaying; and

wherein in response to the user providing one or more risk levels and one or more test objectives, the electronic processor is caused to:

convert the one or more user provided risk levels and one or more test objectives into one or more test procedures to be implemented by a real-time distributed ledger-based computing system validation tool; and

transmit the generated one or more test procedures to an external user.

12. The computing system of claim 11, wherein the one or more risk categories are selected from a group consisting of government and oversight, cyber security, infrastructure layer, architecture layer, operational layer, and transaction layer.

13. The computing system of claim 12, wherein if the user selects a transaction layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate an application layer of a distributed ledger-based computing system technology stack.

14. The computing system of claim 12, wherein if the user selects a blockchain architecture risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a decentralized protocols and encryption layer of a distributed ledger-based computing system technology stack.

15. The computing system of claim 12, wherein if the user selects an operational layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a permissioned network layer of a distributed ledger-based computing system technology stack.

16. The computing system of claim 12, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a shared data layer of a distributed ledger-based computing system technology stack.

17. The computing system of claim 16, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a commercial API layer of a distributed ledger-based computing system technology stack.

18. The computing system of claim 17, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate overlay network layer of a distributed ledger-based computing system technology stack.

19. The computing system of claim 11, wherein transmitting the generated one or more test procedures to an external user includes transmitting the generated one or more test

procedures to a real-time continuous distributed ledger-based computing system auditing tool.

20. The computing system of claim **19**, wherein transmitting the generated one or more test procedures includes writing the generated one or more test procedures to a planning file, and transmitting the planning file to the real-time continuous distributed ledger-based computing system auditing tool.

21. A computer readable storage medium storing one or more programs, the one or more programs comprising instructions, which, when executed by an electronic device with a display and a user input interface, cause the device to:

display one or more risk categories to a user using the display;

prompt the user to input one or more risk levels via the interface, wherein each risk level on the one or more risk levels corresponds to the one or more risk categories displayed;

display one or more test objectives or controls via the display;

prompt the user to indicate which of the one or more test objectives are to be evaluated via the displaying; and wherein in response to the user providing one or more risk levels and one or more test objectives, the device is caused to:

convert the one or more user provided risk levels and one or more test objectives into one or more test procedures to be implemented by a real-time distributed ledger-based computing system validation tool; and

transmit the generated one or more test procedures to an external user.

22. The computer readable storage medium of claim **21**, wherein the one or more risk categories are selected from a group consisting of government and oversight, cyber security, infrastructure layer, architecture layer, operational layer, and transaction layer.

23. The computer readable storage medium of claim **22**, wherein if the user selects a transaction layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate an application layer of a distributed ledger-based computing system technology stack.

24. The computer readable storage medium of claim **22**, wherein if the user selects a blockchain architecture risk

category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a decentralized protocols and encryption layer of a distributed ledger-based computing system technology stack.

25. The computer readable storage medium of claim **22**, wherein if the user selects an operational layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a permissioned network layer of a distributed ledger-based computing system technology stack.

26. The computer readable storage medium of claim **22**, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a shared data layer of a distributed ledger-based computing system technology stack.

27. The computer readable storage medium of claim **26**, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate a commercial API layer of a distributed ledger-based computing system technology stack.

28. The computer readable storage medium of claim **27**, wherein if the user selects an infrastructure layer risk category, the electronic device is caused to convert the one or more user provided risk levels into one or more test procedures configured to validate overlay network layer of a distributed ledger-based computing system technology stack.

29. The computer readable storage medium of claim **21**, wherein transmitting the generated one or more test procedures to an external user includes transmitting the generated one or more test procedures to a real-time continuous distributed ledger-based computing system auditing tool.

30. The computer readable storage medium of claim **29**, wherein transmitting the generated one or more test procedures includes writing the generated one or more test procedures to a planning file, and transmitting the planning file to the real-time continuous distributed ledger-based computing system auditing tool.

* * * * *