Primechain Technologies

Blockchain Security Controls



Primechain-BSC

Version 1.1 dated 6th August, 2018

1 Primechain-BSC prescribes security controls for blockchain implementations. Many of the security 2 controls are based on NIST Special Publication 800-53 Revision 4 and apply to blockchain as well as 3 distributed ledger systems. 4 5 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 6 International License. 7 8 9 Primechain-BSC is maintained by Primechain Technologies Private Limited. 10 11 Primechain Technologies Pvt. Ltd. 12 410, Supreme Headquarters, 13 Mumbai-Bangalore Highway, 14 Near Audi Showroom, 15 Baner, 16 Pune - 411045 (INDIA) 17 18 Email: info@primechain.in 19 Web: http://www.primechaintech.com 20 21 When sending us your comments, please mention the line numbers of this document, if relevant.

22 Document history

29th November 2017: Version 1.0 of PT-BSC released

4th August 2018: Version 1.1 of PT-BSC released. Changes include – changes to the document layout, fonts and design, addition of a glossary and addition of a section about Primechain Technologies.

Note: Blockchains inherently involve multiple parties and organizations. In this document, the term *organization* includes, unless repugnant to the context, all participating organizations that have agreed on a common security framework, framework revision procedures, and security compliance monitoring processes.

33	Table of Contents	
34	A. Introduction to blockchain technology	6
35	B. Components of a blockchain	7
36	C. Security controls for blockchain instances	8
37	C.1 Primary considerations	
38	(a) Blockchain permissions	
39	(b) Consensus mechanisms	
40	(c) Considerations for proof-of-work based blockchain instances	
41	(d) Considerations for native blockchain currency (optional)	
42	(e) Blockchain Security Program Plan	
43	(f) Senior blockchain security officer	9
44	(g) Blockchain security resources	9
45	(h) Plan of action and milestones process	9
46	(i) Information system inventory	10
47	(j) Information security measures of performance	10
48	(k) Enterprise architecture	10
49	(I) Critical infrastructure plan	10
50	(m) Risk management strategy	
51	(n) Security authorization process	
52	(o) Mission/business process definition	
53	(p) Insider threat program	
54	(q) Blockchain security workforce	
55	(r) Testing, training, and monitoring	
56	(s) Contacts with security groups and associations	
57	(t) Threat awareness program	
58	C.2 Blockchain Access Control	
59	(a) Blockchain Access Control Policy and Procedures	
60	(b) Blockchain Account Management	
61	(c) Blockchain Access Enforcement	
62	(d) Information Flow Enforcement	
63	(e) Least Privilege	
64	(f) Permitted actions without identification or authentication	
65 66	(g) Wireless Access(g) Wireless Access	
66 67	(h) Access control for mobile devices	
68	(i) Use of external information systems	
69	C.3 Awareness & Training	
70	(a) Security awareness and training policy and procedures	
71	(b) Security awareness training	
72	(c) Role-based security training	
73	C.4 Audit and Accountability	
74	(a) Audit and accountability policy and procedures	
75	(b) Content of audit records	
76	(c) Audit review, analysis, and reporting	
77	(d) Time stamps	
78	(e) Protection of audit information	

C.5 Security assessment and authorization	18
(a) Security assessment and authorization policy and procedures	18
(b) Security assessments	18
(c) System interconnections	18
(d) Continuous monitoring	19
(e) Penetration testing	19
(f) Internal system connections	19
C.6 Contingency planning	20
(a) Contingency planning policy and procedures	20
(b) Contingency plan	20
(c) Contingency training	21
(d) Contingency plan testing	21
(e) Alternate storage site	22
(f) Alternate processing site	22
(g) Telecommunications services	22
(h) Information system recovery and reconstitution	22
C.7 Incident response	23
(a) Incident response policy and procedures	23
(b) Incident response training	23
(c) Incident response testing	23
(d) Incident handling	24
(e) Incident Monitoring	25
(f) Incident reporting	25
(g) Incident response assistance	25
(h) Incident response plan	26
(i) Information spillage response	26
(j) Integrated information security analysis team	27
C.8 Maintenance	28
(a) System maintenance policy and procedures	28
C.9 Physical and environmental protection	29
(a) Physical and environmental protection policy and procedures	29
(b) Physical access authorizations	29
(c) Physical access control	30
C.10 Risk assessment	31
(a) Risk assessment policy and procedures	31
(b) Risk assessment	31
(c) Vulnerability scanning	31
(d) Insider threat program	32
(e) Contacts with security groups and associations	32
(f) Threat awareness program	33
C.11 Blockchain Integrity	34
(a) Blockchain integrity policy and procedures	34
(b) Flaw remediation	34
(c) Malicious code protection	35
(d) Blockchain monitoring	36
(e) Security alerts, advisories, and directives	38
(f) Security function verification	38
(g) Software, firmware, and information integrity	38
	C.5 Security assessment and authorization (a) Security assessment and authorization policy and procedures. (b) Security assessments. (c) System interconnections. (d) Continuous monitoring. (e) Penetration testing. (f) Internal system connections. C.6 Contingency planning (a) Contingency planning policy and procedures. (b) Contingency planning. (c) Contingency plan testing. (e) Alternate storage site. (f) Alternate processing site (g) Telecommunications services. (h) Information system recovery and reconstitution. C.7 Incident response. (a) Incident response policy and procedures. (b) Incident response testing. (c) Incident fesponse testing. (d) Incident Monitoring. (f) Incident Response policy and procedures. (h) Incident response plan (i) Information spillage response. (i) Integrated information security analysis team. C.8 Maintenance. (a) System maintenance policy and procedures. C.9 Physical and environmental protection (a) Physical and environmental protection policy and procedures. (b) Physical access authorizations. (c) Physical access control. C.10 Risk assessment (a) Risk assessment (b) Risk assessment (c) Vulnerability scanning (d) Insider threat program (e) Contacts with security groups and associations. (f) Threat awareness program. C.11 Blockchain Integrity (a) Blockchain integrity policy and procedures. (b) Flaw remediation. (c) Malicious code protection (d) Blockchain monitoring (e) Security function verification. (g) Software, firmware, and information integrity.

127	D. Security recommendations for other Blockchain components	40
128	E. Glossary	41
129	F. References & recommended resources	43
130	G. About Primechain	44
131 132	H. License	45

133 A. Introduction to blockchain technology

Blockchain technology was announced through the paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto in 2008. Interestingly, this paper does not specifically use the word "blockchain". This paper talks about a "purely peer-to-peer version of electronic cash" where "the network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work".

Blockchain technology is an innovative mix of public key cryptography (invented in the 1970s), cryptographic hash functions (born in the 1970s) and proof-of-work (invented in the 1990s).

Over the last few years, many derivate and blockchain-inspired projects have been created. Most of them are not technically blockchains, but rather distributed ledger systems. For simplicity, we have used the terms blockchain and distributed ledger system interchangeably in this article.

Blockchain solutions can be **permissioned** (e.g. a Government run land registry) or **permission-less** (e.g. Bitcoin, where anyone can become a miner). Blockchain solutions can be **private** (e.g. a contract management system implemented in a pharmaceutical company), **public** (e.g. an asset backed cryptocurrency) or **hybrid** (e.g. a group of banks running a shared KYC platform).

There are 2 things that blockchains can do very well: data authentication & verification (immutable storage, digital signatures and encryption) and smart asset management (issuance, payment, exchange, escrow and retirement).

The original blockchain, which powers the bitcoin crypto-currency, used proof of work as a **consensus** mechanism. But today there are multiple distributed ledger systems that offer a host of consensus mechanisms such as Proof of stake, Byzantine fault tolerant, Deposit based consensus, Federated Byzantine Agreement, Proof of Elapsed Time, Derived PBFT, Redundant Byzantine Fault Tolerance, Simplified Byzantine Fault Tolerance, Federated consensus, Round Robin and Delegated Proof of Stake.

Some of the popular blockchain platforms / **frameworks** include: Hyperledger (Burrow, Fabric, Indy, Iroha & Sawtooth), Multichain & Ethereum, Quorum, Stellar.

Primechain-BSC prescribes security controls for blockchain implementations. Many of the security controls are based on *NIST Special Publication 800-53 Revision 4* and apply to blockchain as well as distributed ledger systems.

B. Components of a blockchain

There are several components of a blockchain:

#	Component	Example / description		
1	blockchain platform	Used interchangeably with the term distributed ledger system; examples - bitcoin, ethereum, multichain, sawtooth, fabric;		
2	blockchain instance	a running implementation of multichain including the block data and block headers;		
3	blockchain nodes	the systems on which a <i>blockchain instance</i> is installed; nodes replicate, access, write to and maintain a single series of linked blocks of transactions; nodes for a single blockchain may be spread across several geographies and organizations.		
4	blockchain connectors	a Macintosh laptop used to connect to the blockchain nodes through ssh;		
5	external interface	a <i>nodejs</i> based blockchain explorer;		
6	blockchain development ecosystem	the technological ecosystem of the entities where the design, development, upgrade and maintenance of the blockchain takes place;		
7	blockchain user ecosystem	the technological ecosystem of the end-users of the blockchain.		

177	C.	Security	controls	for	blockchain	instances

178179

C.1 Primary considerations

180 181

182

183

184

185

186 187

(a) Blockchain permissions

The organization has systems in place to determine:

- 1. restrictions applied to connecting to the network
- 2. restrictions applied to signing transaction inputs
- 3. restrictions applied to appearing in transaction outputs
- 4. restrictions applied to creating new assets
 - 5. restrictions applied to confirming transactions
 - 6. restrictions applied to changing permissions of other users

188 189 190

191

192193

(b) Consensus mechanisms

The organization has systems in place to determine the appropriate consensus mechanism:

- 1. proof of work
- 2. proof of stake
- 3. federated byzantine agreement

194 195 196

197

198

199200

201202

203

204

(c) Considerations for proof-of-work based blockchain instances

The organization has systems in place to determine the:

- 1. target average time between blocks
- 2. maximum size of each block
- 3. length of initial setup phase
- 4. mining diversity
- 5. minimum / initial proof-of-work difficulty
 - 6. frequency of recalculating proof-of-work difficulty level
 - 7. maximum size of a standard transaction,
- 8. maximum size of data elements in standard transactions.

205206207

210

211212

213214

215

(d) Considerations for native blockchain currency (optional)

208 The organization has systems in place to determine the:

- 209 1. initial block reward
 - 2. first block reward,
 - 3. reward halving interval,
 - 4. reward spendable delay,
 - 5. minimum quantity of native currency in every transaction output
 - 6. maximum quantity of native currency in every transaction output
 - 7. minimum relay fee
- 216 8. units per display unit of the native currency

217218

(e) Blockchain Security Program Plan

219220

221

1. The organization develops and disseminates an organization-wide blockchain security program plan that:

- 222 a. Provides an overview of the requirements for the security program and a 223 description of the security program management controls and common 224 controls in place or planned for meeting those requirements; 225 b. Includes the identification and assignment of roles, responsibilities, 226 management commitment, coordination among organizational entities, and compliance; 227 228 c. Reflects coordination among organizational entities responsible for the 229
 - different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
 - d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations.
 - 2. The organization reviews the organization-wide blockchain security program plan every month.
 - 3. The organization updates the plan to address organizational changes and problems identified during plan implementation or security control assessments.
 - 4. The organization protects the blockchain security program plan from unauthorized disclosure and modification.

Note: Blockchain security program plans can be represented in single documents or compilations of documents at the discretion of organizations.

(f) Senior blockchain security officer

The organization appoints a senior blockchain security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide blockchain security program.

(g) Blockchain security resources

- The organization ensures that all capital planning and investment requests include the resources needed to implement the blockchain security program and documents all exceptions to this requirement.
- 2. The organization ensures that blockchain security resources are available for expenditure as planned.

(h) Plan of action and milestones process

1. The organization implements a process for ensuring that plans of action and milestones for the blockchain program and associated organizational information systems are developed and maintained.

230

231 232

233 234

235 236

237 238 239

240

241 242

243 244 245

246 247 248

249

250

251

252 253

254 255

256

257

258 259

260 261 262

263 264

265 266

- 2. The organization documents the remedial blockchain security actions to adequately respond to risk to organizational operations and assets, individuals, and other organizations.
 - 3. The organization reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

(i) Information system inventory

The organization develops and maintains an inventory of its blockchain systems.

(j) Information security measures of performance

The organization develops, monitors, and reports on the results of blockchain security measures of performance.

(k) Enterprise architecture

The organization develops an enterprise architecture with consideration for blockchain security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

(I) Critical infrastructure plan

The organization addresses blockchain security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

(m) Risk management strategy

- 1. The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of blockchain systems.
- 2. The organization implements the risk management strategy consistently across the organization.
- 3. The organization reviews and updates the risk management strategy regularly to address organizational changes. An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

(n) Security authorization process

- 1. The organization manages (i.e., documents, tracks, and reports) the security state of organizational blockchain systems and the environments in which those systems operate through security authorization processes;
- 2. The organization designates individuals to fulfil specific roles and responsibilities within the organizational risk management process.

3. The organization fully integrates the security authorization processes into an organization-wide risk management program.

(o) Mission/business process definition

1. The organization defines mission/business processes with consideration for blockchain security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

2. The organization determines blockchain protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

(p) Insider threat program

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

(q) Blockchain security workforce

The organization establishes a blockchain security workforce development and improvement program.

(r) Testing, training, and monitoring

1. The organization implements a process for ensuring that organizational plans for conducting blockchain security testing, training, and monitoring activities associated with organizational information systems are developed and maintained and continue to be executed in a timely manner.

 2. The organization reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

(s) Contacts with security groups and associations

The organization establishes and institutionalizes contact with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel; to maintain currency with recommended security practices, techniques, and technologies; and to share current security-related information including threats, vulnerabilities, and incidents.

(t) Threat awareness program

The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

C.2 Blockchain Access Control

(a) Blockchain Access Control Policy and Procedures

1. The organization develops, documents, and disseminates, to relevant personnel, a blockchain access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates, to relevant personnel, procedures to facilitate the implementation of the blockchain access control policy and associated access controls.

3. The organization reviews and updates the current Blockchain Access Control Policy and Blockchain Access Control Procedures every month.

(b) Blockchain Account Management

1. The organization identifies and selects the following types of blockchain accounts to support organizational missions / business functions: (a) blockchain administrator (b) blockchain manager (c) blockchain processor.

2. The organization assigns account managers for blockchain accounts.

3. The organization establishes conditions for group and role membership.

4. The organization specifies authorized users of the blockchain, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

5. The organization requires approvals by the blockchain administrator for requests to create blockchain accounts;

6. The organization creates, enables, modifies, disables, and removes blockchain accounts in accordance with the Blockchain Access Control Policy and Procedures.

7. The organization monitors the use of blockchain accounts.

8. The organization notifies the blockchain administrator (a) when accounts are no longer required; (b) when users are terminated or transferred; and (c) when individual information system usage or need-to-know changes;

9. The organization authorizes access to the blockchain based on: (a) valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;

10. The organization reviews accounts for compliance with blockchain account management requirements every 24 hours.

11. The organization establishes a process for reissuing shared / group account credentials (if deployed) when individuals are removed from the group. 12. The organization employs automated mechanisms to support the management of blockchain accounts. 13. The organization only permits the use of shared / group accounts that meet organization-defined conditions for establishing shared / group accounts. 14. The organization disables accounts of users posing a significant risk immediately on discovery of the risk.

(c) Blockchain Access Enforcement

- 1. The organization enforces approved authorizations for logical access to the blockchain in accordance with applicable blockchain access control policies.
- 2. The organization enforces dual authorization for all actions.
- 3. The blockchain prevents access to blockchain parameters and specified cryptographic keys except during secure, non-operable system states.
- 4. The blockchain does not release information outside of the established system boundary.

(d) Information Flow Enforcement

- 1. The organization enforces approved authorizations for controlling the flow of information within the blockchain and between interconnected systems based on organization-defined information flow control policies.
- 2. The blockchain prevents encrypted information from bypassing content-checking mechanisms by decrypting the information, blocking the flow of the encrypted information and / or by terminating communications sessions attempting to pass encrypted information.
- 3. The blockchain enforces organization-defined limitations on embedding data types within other data types.
- 4. The blockchain enforces information flow control based on organization-defined metadata.
- 5. The blockchain uniquely identifies and authenticates source and destination points by organization, system, application and / or individual] for information transfer.
- 6. The blockchain binds security attributes to information using organization-defined binding techniques to facilitate information flow policy enforcement.

7. The blockchain provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

(e) Least Privilege

- 1. The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users), which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- 2. The organization explicitly authorizes access to blockchain parameters, cryptographic keys.
- 3. The organization prohibits privileged access to the blockchain by non-organizational users.
- 4. The organization reviews daily the privileges assigned to blockchain administrators, managers and processors to validate the need for such privileges; and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

(f) Permitted actions without identification or authentication

- 1. The organization identifies actions that can be performed on the blockchain without identification or authentication consistent with organizational missions / business functions.
- 2. The organization documents and provides supporting rationale in the security plan for the blockchain, user actions not requiring identification or authentication.

(g) Remote Access

- 1. The organization establishes and documents usage restrictions, configuration / connection requirements, and implementation guidance for each type of remote access allowed.
- 2. The organization authorizes remote access to the information system prior to allowing such connections.
- 3. The blockchain implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
- 4. The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

(g) Wireless Access

1. The organization establishes usage restrictions, configuration / connection requirements, and implementation guidance for wireless access.

2. The organization authorizes wireless access to the information system prior to allowing such connections.

3. The blockchain protects wireless access to the system using encryption and authentication of users & devices.

(h) Access control for mobile devices

1. The organization establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

2. The organization authorizes the connection of mobile devices to organizational information systems.

3. The organization prohibits the use of unclassified mobile devices unless specifically permitted by the authorizing official.

4. The organization employs container encryption to protect the confidentiality and integrity of information on organization-defined mobile devices.

(i) Use of external information systems

 The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the blockchain from external information systems.

2. The organization permits authorized individuals to use an external information system to access the blockchain only when the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.

3. The organization restricts / prohibits the use of portable storage devices by authorized individuals on external information systems.

C.3 Awareness & Training

(a) Security awareness and training policy and procedures

- 1. The organization develops, documents, and disseminates, to relevant personnel, a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- 2. The organization develops, documents, and disseminates, to relevant personnel, procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
- 3. The organization develops, documents, and disseminates, to relevant personnel, reviews and updates the current security awareness and training policy and security awareness and training procedures every 3 months.

(b) Security awareness training

- 1. The organization provides basic security awareness training to blockchain users (a) as part of initial training for new users (b) when required by information system changes and (c) every 3 months thereafter.
- 2. The organization includes practical exercises in security awareness training that simulate actual cyber attacks.
- 3. The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

(c) Role-based security training

The organization provides role-based security training to personnel with assigned security roles and responsibilities (a) before authorizing access to the blockchain or performing assigned duties (b) when required by information system changes and (c) every 3 months thereafter.

C.4 Audit and Accountability

(a) Audit and accountability policy and procedures

1. The organization develops, documents, and disseminates to relevant personnel, an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates to relevant personnel, procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

3. The organization reviews and updates the current audit and accountability policy and audit and accountability procedures every 6 months.

(b) Content of audit records

The blockchain generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

(c) Audit review, analysis, and reporting

The organization reviews and analyzes information system audit records in real time for indications of inappropriate or unusual activity and reports findings to the relevant personnel.

(d) Time stamps

The blockchain uses internal system clocks to generate time stamps for audit records and records time stamps for audit records that can be mapped to Greenwich Mean Time (GMT).

(e) Protection of audit information

The blockchain protects audit information and audit tools from unauthorized access, modification, and deletion.

C.5 Security assessment and authorization

(a) Security assessment and authorization policy and procedures

1. The organization develops, documents, and disseminates to relevant personnel, a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

 2. The organization develops, documents, and disseminates to relevant personnel, procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

3. The organization reviews and updates the current security assessment and authorization policy and security assessment and authorization procedures every 6 months.

(b) Security assessments

1. The organization develops a security assessment plan that describes the scope of the assessment including (a) Security controls and control enhancements under assessment; (b) Assessment procedures to be used to determine security control effectiveness; and (c) Assessment environment, assessment team, and assessment roles and responsibilities.

2. The organization assesses the security controls in the information system and its environment of operation every month to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

3. The organization produces a security assessment report that documents the results of the assessment and provides the results of the security control assessment to relevant personnel.

(c) System interconnections

1. The organization authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements.

2. The organization documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

3. The organization reviews and updates Interconnection Security Agreements every 6 months.

- 4. The organization prohibits the direct connection of a blockchain to an external network without the use of an approved boundary protection device.
 - 5. The organization employs allow-all / deny-by-exception / deny-all / permit-by-exception policy for allowing a blockchain to connect to external information systems.

(d) Continuous monitoring

The organization develops a continuous monitoring strategy and implements a continuous monitoring program.

(e) Penetration testing

- 1. The organization conducts regular penetration testing on all blockchains.
- 2. The organization employs an independent penetration agent or penetration team to perform penetration testing on the blockchain.
- 3. The organization employs exercises to simulate attempts by adversaries to compromise blockchains.

(f) Internal system connections

The organization authorizes internal connections of information system components or classes of components to the blockchain and documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

C.6 Contingency planning

679	
680	

(a) Contingency planning policy and procedures

1. The organization develops, documents, and disseminates to relevant personnel, a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates to relevant personnel, procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

3. The organization reviews and updates the current contingency planning policy and contingency planning procedures every 6 months.

(b) Contingency plan

1. The organization develops a contingency plan for the information system that:

a. Identifies essential missions and business functions and associated contingency requirements;

b. Provides recovery objectives, restoration priorities, and metrics;

c. Addresses contingency roles, responsibilities, assigned individuals with contact information;

d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

e. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

f. Is reviewed and approved by [Assignment: organization-defined personnel or roles].

2. The organization distributes copies of the contingency plan to relevant personnel.

3. The organization coordinates contingency planning activities with incident handling activities.

4. The organization reviews the contingency plan for the information system every month.

5. The organization updates the contingency plan to address changes to the organization, blockchain, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

6. The organization communicates contingency plan changes to relevant personnel.

- 724 7. The organization protects the contingency plan from unauthorized disclosure and modification.
 - 8. The organization coordinates contingency plan development (Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans) with organizational elements responsible for related plans.
 - 9. The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
 - 10. The organization plans for the resumption of essential missions and business functions within 1 hour of contingency plan activation.
 - 11. The organization plans for the resumption of all missions and business functions within 1 hour of contingency plan activation.
 - 12. The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.
 - 13. The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.
 - 14. The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
 - 15. The organization identifies critical information system assets supporting essential missions and business functions.

(c) Contingency training

The organization provides contingency training to information system users consistent with assigned roles and responsibilities (a) within 1 day of assuming a contingency role or responsibility; (b) when required by information system changes and (c) every month thereafter.

(d) Contingency plan testing

1. The organization tests the contingency plan for the information system weekly to determine the effectiveness of the plan and the organizational readiness to execute the plan.

2. The organization reviews the contingency plan test results and initiates corrective actions, if needed.

(e) Alternate storage site

1. The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information.

2. The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

3. The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

4. The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

 5. The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster (e.g., hurricane, regional power outage) and outlines explicit mitigation actions (for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted).

(f) Alternate processing site

1. The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of operations for essential missions/business functions within the organization's specified and agreed recovery time objective.

2. The organization ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption.

3. The organization ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

(g) Telecommunications services

 The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of operations for essential missions and business functions within the organization's specified and agreed recovery time objective.

(h) Information system recovery and reconstitution

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

C.7 Incident response

(a) Incident response policy and procedures

I

The organization develops, documents, and disseminates to relevant personnel, an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates to relevant personnel, procedures to facilitate the implementation of the incident response policy and associated incident response controls.

3. The organization reviews and updates the current Incident response policy and Incident response procedures every 6 months.

(b) Incident response training

 1. The organization provides incident response training to information system users consistent with assigned roles and responsibilities (a) Within 1 day of assuming an incident response role or responsibility (b) When required by information system changes and every 3 months thereafter.

2. The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

3. The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

(c) Incident response testing

1. The organization tests the incident response capability for the blockchain every week using defined tests to determine the incident response effectiveness and documents the results.

2. The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

 3. The organization coordinates incident response testing with organizational elements responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

(d) Incident handling

 The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

2. The organization coordinates incident handling activities with contingency planning activities.

3. The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

4. The organization employs automated mechanisms to support the incident handling process.

5. The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability.

6. The organization identifies classes of incidents and actions to take in response to classes of incidents to ensure continuation of organizational missions and business functions.

7. The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

8. The organization implements incident handling capability for insider threats.

9. The organization coordinates incident handling capability for insider threats across defined components or elements of the organization.

10. The organization coordinates with relevant external organizations to correlate and share incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses.

11. The organization employs dynamic response capabilities] to effectively respond to security incidents.

12. The organization coordinates incident handling activities involving supply chain security events (e.g. compromises / breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities.) with other organizations involved in the supply chain (e.g. system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers).

(e) Incident Monitoring

1. The organization tracks and documents information system security incidents. Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

2. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

(f) Incident reporting

1. The organization requires personnel to report suspected security incidents (e.g. the receipt of suspicious email communications that can potentially contain malicious code.) to the organizational incident response capability in real time.

2. The organization reports security incident information to the blockchain administrator.

3. The organization employs automated mechanisms to assist in the reporting of security incidents.

4. The organization reports information system vulnerabilities associated with reported security incidents to the blockchain administrator.

5. The organization provides security incident information to other organizations involved in the supply chain (e.g. system / product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers) for information systems or information system components related to the incident.

(g) Incident response assistance

1. The organization provides an incident response support resource (e.g. help desks, assistance groups, and access to forensics services,), integral to the organizational incident response capability that offers advice and assistance to users of the blockchain for the handling and reporting of security incidents.

2. The organization employs automated mechanisms to increase the availability of incident response-related information and support.

3. The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.

962	4.	The organization identifies organizational incident response team members to the
963		external providers.
964 965	(b) Incid	dent response plan
966	(II) IIICI	uent response pian
967	1.	The organization develops an incident response plan that:
968	1.	a. Provides the organization with a roadmap for implementing its incident
969		response capability;
970		b. Describes the structure and organization of the incident response
971		capability;
972		c. Provides a high-level approach for how the incident response capability
973		fits into the overall organization;
974		d. Meets the unique requirements of the organization, which relate to
975		mission, size, structure, and functions;
976		e. Defines reportable incidents;
977		f. Provides metrics for measuring the incident response capability within the
978		organization;
979		g. Defines the resources and management support needed to effectively
980		maintain and mature an incident response capability; and
981		h. Is reviewed and approved by specified personnel.
982		
983	2.	The organization distributes copies of the incident response plan to incident
984		response personnel.
985	0	
986	3.	The organization reviews the incident response plan every month.
987	1	The expenientian underes the incident response plan to address
988 989	4.	The organization updates the incident response plan to address system/organizational changes or problems encountered during plan
990		implementation, execution, or testing.
991		implementation, exceution, or testing.
992	5.	The organization communicates incident response plan changes to incident
993		response personnel.
994		
995	6.	The organization protects the incident response plan from unauthorized disclosure
996		and modification.
997		
998	(i) Infor	mation spillage response
999		
1000	1.	The organization responds to information spills by:
1001		a. Identifying the specific information involved in the information system
1002		contamination;
1003		b. Alerting relevant personnel the information spill using a method of
1004 1005		communication not associated with the spill; c. Isolating the contaminated information system or system component;
1005		d. Eradicating the information from the contaminated information system or
1007		component;
1007		e. Identifying other information systems or system components that may
1009		have been subsequently contaminated.

1010		
1011	2.	The organization assigns relevant personnel with responsibility for responding to
1012		information spills.
1013		
1014	3.	The organization provides information spillage response training regularly.
1015		
1016	4.	The organization implements procedures to ensure that organizational personnel
1017		impacted by information spills can continue to carry out assigned tasks while
1018		contaminated systems are undergoing corrective actions.
1019		
1020	(j) Inte	grated information security analysis team
1021	The ord	anization establishes an integrated team of forensic/malicious code analysts, tool
1022	develop	ers, and real-time operations personnel.
	-	

C.8 Maintenance

(a) System maintenance policy and procedures

1. The organization develops, documents, and disseminates to relevant personnel, a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates to relevant personnel, procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

3. The organization reviews and updates the current System maintenance policy and System maintenance procedures every 6 months.

C.9 Physical and environmental protection

1	039
1	040

(a) Physical and environmental protection policy and procedures

1. The organization develops, documents, and disseminates to relevant personnel, a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates to relevant personnel, procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

3. The organization reviews and updates the current Physical and environmental protection policy and Physical and environmental protection procedures every 6 months.

(b) Physical access authorizations

1. The organization develops, approves, and maintains a list of individuals with authorized access to the facility where the blockchain resides.

2. The organization issues authorization credentials (e.g. forge-proof badges, smart cards, or identification cards) for blockchain facility access.

3. The organization reviews the access list detailing authorized blockchain facility access by individuals every week.

4. The organization removes individuals from the facility blockchain access list when access is no longer required.

5. The organization authorizes physical access to the facility where the blockchain resides based on position or role.

6. The organization requires two forms of identification (e.g. passports, Personal Identity Verification cards, drivers' licenses, key cards, PINs, biometrics) for visitor access to the facility where the blockchain resides.

7. The organization restricts unescorted access to the facility where the blockchain resides to personnel with (a) security clearances for all information contained within the blockchain; (b) formal access authorizations for all information contained within the blockchain; (c) need for access to all information contained within the blockchain.

8. The organization ensures that individuals lacking sufficient security clearances, access approvals, or need to know, are escorted by individuals with appropriate credentials.

(c) Physical access control

1. The organization enforces physical access authorizations at entry/exit points to the facility where the blockchain resides by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility using physical access control systems / devices and guards.

2. The organization maintains physical access audit logs for entry / exit points.

3. The organization provides security safeguards to control access to areas within the facility officially designated as publicly accessible.

4. The organization ensures that visitors are escorted and visitor activity is monitored.

5. The organization ensures that keys, combinations, and other physical access devices are secured.

6. The organization ensures that combinations and keys are changed when keys are lost, combinations are compromised, or individuals are transferred or terminated.

7. The organization enforces physical access authorizations to the blockchain in addition to the physical access controls for the facility.

8. The organization performs daily security checks at the physical boundary of the facility or blockchain for unauthorized exfiltration of information or removal of information system components.

The organization employs guards and/or alarms to monitor every physical access point to the facility where the blockchain resides 24 hours per day, 7 days per week.

10. The organization uses lockable physical casings to protect the blockchain from unauthorized physical access.

11. The organization employs security safeguards to detect and prevent physical tampering or alteration of the blockchain.

12. The organization employs a penetration testing process that includes daily, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

C.10 Risk assessment

1127	(a) Risk	cassessment policy and procedures
1128		
1129	1.	The organization develops, documents, and disseminates to relevant personnel, a
1130		risk assessment policy that addresses purpose, scope, roles, responsibilities,
1131		management commitment, coordination among organizational entities, and
1132		compliance.
1133	0	The consideration decides a decimal of the contrate to the con
1134	2.	The organization develops, documents, and disseminates to relevant personnel,
1135		procedures to facilitate the implementation of the risk assessment policy and
1136		associated risk assessment controls.
1137	0	The comparison of the control of the
1138	3.	The organization reviews and updates the current Risk assessment policy and Risk
1139		assessment procedures every 6 months.
1140	/k) p:-1	
1141	(D) KISI	c assessment
1142	1	The expeniencian conducts on accomment of rick including the likelihood and
1143 1144	1.	The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption,
1144		modification, or destruction of the blockchain and the information it processes,
		·
1146 1147		stores, or transmits.
1147	2.	The organization documents risk assessment results.
1149	۷.	The organization documents risk assessment results.
1150	3.	The organization reviews risk assessment results regularly.
1151	0.	The organization reviews risk assessment results regularly.
1152	4.	The organization disseminates risk assessment results to relevant personnel.
1153	т.	The organization disseminates risk assessment results to relevant personner.
1154	5.	The organization updates the risk assessment every 1 month or whenever there are
1155	0.	significant changes to the blockchain or environment of operation (including the
1156		identification of new threats and vulnerabilities), or other conditions that may
1157		impact the security state of the blockchain.
1158		, ,
1159	(c) Vulr	nerability scanning
1160	• •	, ,
1161	1.	The organization scans for vulnerabilities in the blockchain e.g. (i) scanning for
1162		patch levels; (ii) scanning for functions, ports, protocols, and services that should
1163		not be accessible to users or devices; and (iii) scanning for improperly configured
1164		or incorrectly operating information flow control mechanisms.
1165		
1166	2.	The organization ensures that when new vulnerabilities potentially affecting the
1167		blockchain are identified and reported, it:
1168		a. Employs vulnerability scanning tools and techniques that facilitate
1169		interoperability among tools and automate parts of the vulnerability
1170		management process by using standards for (i) Enumerating platforms,

- software flaws, and improper configurations; (2) Formatting checklists and test procedures; and (3) Measuring vulnerability impact.
 - b. Analyzes vulnerability scan reports and results from security control assessments;
 - c. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and
 - d. Shares information obtained from the vulnerability scanning process and security control assessments with relevant personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
 - 3. The organization employs vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.
 - 4. The organization updates the vulnerabilities scanned prior to a new scan and when new vulnerabilities are identified and reported.
 - 5. 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. The organization determines what information about the blockchain is discoverable by adversaries and subsequently takes corrective actions.
 - 7. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.
 - 8. The organization reviews historic audit logs to determine if a vulnerability identified in the blockchain has been previously exploited.
 - 9. The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

(d) Insider threat program

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

(e) Contacts with security groups and associations

The organization establishes and institutionalizes contact with selected groups and associations within the security community: (a) to facilitate ongoing security education and training for organizational personnel; (b) To maintain currency with recommended security practices, techniques, and technologies; and (c) To share current security-related information including threats, vulnerabilities, and incidents.

Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar

organizations. Organizations select groups and associations based on organizational missions/business functions.

122012211222

1219

(f) Threat awareness program

The organization implements a threat awareness program that includes a crossorganization information-sharing capability. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral or multilateral.

C.11 Blockchain Integrity

1230		

(a) Blockchain integrity policy and procedures

1. The organization develops, documents, and disseminates, to relevant personnel, a blockchain integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. The organization develops, documents, and disseminates, to relevant personnel, procedures to facilitate the implementation of the blockchain integrity policy and associated system and information integrity controls.

3. The organization reviews and updates the current blockchain integrity policy and blockchain integrity procedures every 3 months.

(b) Flaw remediation

1. The organization identifies, reports, and corrects blockchain system flaws including those discovered during security assessments, continuous monitoring, incident response activities, and system error handling.

2. The organization tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

3. The organization installs security-relevant software (e.g. patches, service packs, hot fixes, and anti-virus signatures) and firmware updates as soon as updates are released.

4. The organization incorporates flaw remediation into the organizational configuration management process.

5. The organization centrally manages the planning, implementing, assessing, authorizing, and monitoring the organization-defined, flaw remediation security controls.

6. The organization employs automated mechanisms daily to determine the state of blockchain components with regard to flaw remediation.

7. The organization measures the time between flaw identification and flaw remediation and establishes benchmarks for taking corrective actions.

8. The organization installs relevant software and firmware updates automatically to blockchain components.

9. The organization removes previous versions of software and/or firmware components after updated versions have been installed.

(c) Malicious code protection

The organization employs malicious code protection mechanisms at blockchain entry and exit points (e.g. firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices) to detect and eradicate malicious code (e.g. viruses, worms, Trojan horses, and spyware; malicious code encoded in various formats such as UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography).

2. The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

 The organization configures malicious code protection mechanisms to perform periodic and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy.

4. The organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the blockchain.

5. The organization centrally manages malicious code protection mechanisms.

 The organization tests malicious code protection mechanisms regularly by introducing a known benign, non-spreading test case into the blockchain and verifies that both detection of the test case and associated incident reporting occur.

7. The blockchain implements non signature-based malicious code detection mechanisms (e.g. the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective)¹.

8. The blockchain detects defined unauthorized operating system commands through the kernel application programming interface and (a) issues a warning; (b) audits the command execution; and (c) prevents the execution of the command.

9. The organization analyzes the characteristics and behaviour of malicious code; and incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.

¹ This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control does not preclude the use of signature-based detection mechanisms.

(d) Blockchain monitoring 1321 1. The organization monitors the blockchain to detect attacks and indicators of

 potential attacks in accordance and unauthorized local, network, and remote connections².

2. The organization identifies unauthorized use of the blockchain.

3. The organization deploys monitoring devices to collect organization-determined essential information and to track specific types of transactions of interest to the organization.

4. The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

5. The organization heightens the level of blockchain monitoring activity whenever there is an indication of increased risk to organizational operations and assets.

6. The organization obtains legal opinion with regard to monitoring activities in accordance with applicable laws.

7. The organization provides monitoring information to relevant personnel as needed.

8. The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

9. The organization employs automated tools (e.g. host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by blockchain) to support near real-time analysis of events.

10. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

11. The blockchain monitors inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

² Blockchain monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the boundary (i.e., part of perimeter defence and boundary protection). Internal monitoring includes the observation of events occurring within the blockchain. Blockchain monitoring capability is achieved through a variety of tools and techniques e.g. intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software.

1360 12. The organization tests intrusion-monitoring tools every day. 1361 1362 13. The organization analyzes outbound communications traffic at the external 1363 boundary of the blockchain to discover anomalies (e.g. large file transfers, long-1364 time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses). 1365 1366 1367 14. The organization employs automated mechanisms to alert security personnel of 1368 inappropriate or unusual activities with security implications. 1369 1370 15. The organization analyzes communications traffic/event patterns for the blockchain; develops profiles representing common traffic patterns and/or events; 1371 1372 and uses the traffic/event profiles in tuning system-monitoring devices to reduce 1373 the number of false positives and the number of false negatives. 1374 1375 16. The organization employs a wireless intrusion detection system to identify roque 1376 wireless devices and to detect attack attempts and potential 1377 compromises/breaches to the blockchain. 1378 1379 17. The organization employs an intrusion detection system to monitor wireless 1380 communications traffic as the traffic passes from wireless to wired networks. 1381 1382 18. The organization correlates information from monitoring tools (e.g., host monitoring, network monitoring, anti-virus software) employed throughout the 1383 1384 components of the blockchain. 1385 1386 19. The organization correlates information from monitoring physical, cyber, and 1387 supply chain activities to achieve integrated, organization-wide situational 1388 awareness. 1389 1390 20. The organization analyzes outbound communications traffic at the external 1391 boundary of the blockchain to detect covert exfiltration of information. 1392 1393 21. The organization implements additional monitoring of individuals who have been 1394 identified by relevant sources (such as human resource records, intelligence 1395 agencies, law enforcement organizations, and/or other credible sources) as posing 1396 an increased level of risk.

1397 1398

22. The organization implements additional monitoring of privileged users and individuals during probationary period.

14001401

1402

1399

23. The organization implements host-based monitoring mechanisms at defined blockchain components.

1404	24.	The	blockchain	discovers,	collects,	distributes,	and	uses	indicators	of
1405		com	oromise ³ .							
1406										
1407	(e) Sec	urity a	lerts, adviso	ries, and dir	ectives					
1408										
1409	1.	The	organization	receives sec	curity alerts	s, advisories,	and d	irective	s from relev	ant'
1410		exter	nal organizat	ions on an o	ngoing bas	sis.				
1411										
1412	2.	The	organization	generates in	nternal sec	curity alerts, a	adviso	ries, ar	nd directives	as

141314141415

3. The organization disseminates security alerts, advisories, and directives to relevant personnel and external organizations.

141614171418

4. The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

14191420

(f) Security function verification

deemed necessary.

14211422

1423

1424

1. The organization verifies the correct operations of defined security functions at blockchain transitional states (e.g. system startup, restart, shutdown, and abort) upon command by user with appropriate privilege.

142514261427

2. The organization notifies relevant personnel of failed security verification tests.

1428 1429

3. The information system implements automated mechanisms to support the management of distributed security testing.

143014311432

4. The organization reports the results of security function verification to relevant personnel.

143314341435

(g) Software, firmware, and information integrity

14361437

1438

1. The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information ⁴ using state-of-the-practice

³ Indicators of compromise (IOC) are forensic artefacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs for the discovery of compromised hosts can include for example, the creation of registry key values. IOCs for network traffic include, for example, Universal Resource Locator (URL) or protocol elements that indicate malware command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that information systems and organizations are vulnerable to the same exploit or attack.

⁴ Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information.

1440 cryptographic hashes) and associated tools. 1441 2. The organization employs automated tools that provide notification to relevant 1442 1443 personnel upon discovering discrepancies during integrity verification. 1444 1445 The organization employs centrally managed integrity verification tools. 1446 1447 4. The blockchain implements cryptographic mechanisms (e.g. digital signatures and 1448 the computation and application of signed hashes using asymmetric cryptography, 1449 protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information). 1450 1451 1452 The organization incorporates the detection of unauthorized security-relevant 1453 changes to the blockchain into the organizational incident response capability. 1454 1455 The blockchain verifies the integrity of the boot process of defined devices. 1456 1457 7. The organization implements defined security safeguards to protect the integrity of boot firmware in defined devices. 1458 1459 The organization requires that defined user-installed software execute in a 1460 1461 confined physical or virtual machine environment with limited privileges. 1462 The organization requires that the integrity of user-installed software be verified 1463 1464 prior to execution. 1465 1466 10. The organization allows execution of binary or machine-executable code obtained 1467 from sources with limited or no warranty and without the provision of source code only in confined physical or virtual machine environments and with the explicit 1468 1469 approval of relevant personnel. 1470

11. The organization implements cryptographic mechanisms to authenticate software

or firmware components prior to installation.

integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks,

1471

1472

1473 D. Security recommendations for other Blockchain

components

Component	Issue	Recommended
		standards
Blockchain platform	System and software quality models	ISO/ IEC 25010:2011
	Evaluation process	ISO/ IEC 25040:2011
Blockchain nodes	Crypto Key Tamper Resistance	FIPS 140-2 Level 4
	Server Virtualization ⁵	Common Criteria EAL 5 or higher
External interface	Configuration and Deployment Management Testing	OWASP Testing Guide
	Identity Management Testing	
	Authentication Testing	
	Authorization Testing	
	Session Management Testing	
	Input Validation Testing	
	Testing for Error Handling	
	Testing for weak Cryptography	
	Business Logic Testing	
	Client Side Testing	

 $^{^{\}rm 5}\,{\rm If}$ sensitive blockchain solution components are not physically isolated.

1477 E. Glossary

1. Blockchain

A blockchain is a peer-to-peer network which timestamps records by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work⁶.

2. Distributed ledger system

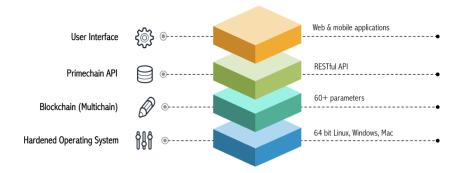
A distributed ledger is a peer-to-peer network, which uses a defined consensus mechanism to prevent modification of an ordered series of time-stamped records⁷.

3. Hash function

A hash function is an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as hash-result such that an electronic record yields the same hash-result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible to (i) to derive or reconstruct the original electronic record from the hash result produced by the algorithm; (ii) that two electronic records can produce the same hash result using the algorithm⁸.

4. Node

A blockchain node can be on-premise or on-cloud. A typical Primechain node is illustrated below



5. Cryptocurrency

According to the FATF report on *Virtual Currencies - Key Definitions and Potential AML/CFT Risks*, Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography. - i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a

⁶ A blockchain can be permissioned, permission-less or hybrid.

⁷ Consensus mechanisms include proof of stake and federated byzantine agreement.

⁸ Adapted from section 3 of the Information Technology Act. Examples of hash functions include SHA-1 and SHA-2.

randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block).

6. Virtual currency

According to the FATF report on *Virtual Currencies - Key Definitions and Potential AML/CFT Risks*, virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency⁹.

_

⁹ Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency - i.e., it electronically transfers value that has legal tender status.

F. References & recommended resources 1520 1521 1. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto. 1522 2. NIST Special Publication 800-53 Revision 4 1523 3. OWASP Testing Guide v4 1524 4. Primechain-BYOB - a Build-Your-Own-Blockchain simulation, available at: 1525 http://yobichain.centralindia.cloudapp.azure.com:2309/byob 1526 5. Consensus Immutable agreement for the Internet of Value – KPMG, available at: 1527 https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-

consensus-mechanism.pdf

1529 G. About Primechain

Primechain™ Technologies is a blockchain company with the mission of building blockchains for a better world.

1. We operate the BankChain™ community of banks for exploring, building and implementing blockchain solutions. Formed in February 2017 with State Bank of India (one of the largest banks in the world) being the first member, BankChain now has 37 members globally.

2. We maintain Primechain-BSC: Blockchain Security Controls, the world's first security controls and recommendations for blockchain implementations.

3. We operate the Autonomous Blockchain for Corporate Data (Primechain A.B.C.D.), a permissioned blockchain that enables sharing and monetizing of corporate data and records.

4. We operate the P5 permissioned blockchain for near real-time cross-border remittance at near-zero cost.

5. We are working closely with global tech companies including Microsoft, Intel, IBM and Dell.

6. We are developing Primechain BOX, the world's first multi-node, pre-configured blockchain appliance.

7. We have filed for a provisional US patent titled "Transparent self-managing Know Your Customer (KYC) program using blockchain and smart contracts".

- 8. Our open source projects include:
 - Yobichain Build your own blockchain in minutes
 - Blockchain KYC platform (Multichain)
 - Blockchain KYC platform (Hyperledger Sawtooth)
 - Blockchain KYC platform (Hyperledger Fabric)

9. We have conducted 50+ events - Future Money Conference, BlockZero Chennai, BlockZero Mumbai, blockathons, training sessions and meetings. Sponsors include IBM, Contact Singapore, Bitkan, KPMG, Fintech Valley Vizag, Government of Andhra Pradesh. Delegates from 100+ Banking, Financial Services, Insurance and Technology companies have attended these events.

10. We are recognized as a startup by the Department of Industrial Policy and Promotion, Ministry of Commerce & Industry, Government of India vide certificate no. DIPP7127 dated 12th April, 2018.

1572 H. License

- This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. You are free to:
- 1575 Share copy and redistribute the material in any medium or format
- Adapt remix, transform, and build upon the material for any purpose, even commercially.

1577

1578 The licensor cannot revoke these freedoms as long as you follow the license terms.

1579

- 1580 Under the following terms:
- 1581 Attribution You must give appropriate credit, provide a link to the license, and indicate if changes
- 1582 were made. You may do so in any reasonable manner, but not in any way that suggests the licensor
- 1583 endorses you or your use.
- 1584 ShareAlike If you remix, transform, or build upon the material, you must distribute your
- 1585 contributions under the same license as the original.
- No additional restrictions You may not apply legal terms or technological measures that legally
- restrict others from doing anything the license permits.

- 1589 Notices:
- You do not have to comply with the license for elements of the material in the public domain or
- where your use is permitted by an applicable exception or limitation.
- No warranties are given. The license may not give you all of the permissions necessary for your
- intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you
- use the material.

Primechain Technologies Pvt. Ltd. 410, Supreme Headquarters, Mumbai-Bangalore Highway, Near Audi Showroom, Baner, Pune - 411045 (INDIA)

Web: http://www.primechaintech.com

Email: info@primechain.in