Cybersecurity Information Sharing and Utilization Framework for the Blockchain Ecosystem (DRAFT)

7/31/2025
Blockchain Governance Initiative Network
Cyber Security Working Group

1. Scope

This document provides a cybersecurity information sharing and utilization framework tailored to~~for~~ the blockchain ecosystem. It defines guiding principles, stakeholder ~~processes,~~ roles, ~~and~~ trust mechanisms, and operational processes to facilitate timely, relevant, and secure exchange of cybersecurity-related information among diverse stakeholders.

The framework is appli~~es~~cable to both public and permissioned blockchain systems, and encompasses~~includes~~ a wide range of actors such as protocol developers, node operators, smart contract developers, wallet providers, infrastructure operators, regulators, and community participants.

It is designed~~intended~~ to complement and align with internationally recognized standards and best practices such as ISO/IEC 27010 (information sharing), ISO/IEC 27035 (incident management), ISO/IEC 29147 (vulnerability disclosure), ISO/IEC 30111 (vulnerability handling), NIST Cybersecurity Framework (CSF), as well as~~and~~ other related international standards and best practices such as the MITRE ATT&CK ~~framework~~ and ADAPT frameworks.

Importantly, this document serves as guidance and does not prescribe requirements for certification or conformity assessment. Its purpose is to support voluntary collaboration and improve ecosystem-wide resilience though structured yet adaptable information sharing and utilization practices.

~~This document provides guidance and does not specify requirements for certification or conformity assessment.~~

2. Normative References

The following referenced documents are indispensable for the application of this document:

- ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27035-1 — Information security incident management — Principles and process
- ISO/IEC 27035-2 — Information security incident management — Guidelines to plan and prepare for incident response
- ISO/IEC 29147 — Vulnerability disclosure
- ISO/IEC 30111 — Vulnerability handling processes
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27002 — Information security controls

3. Terms and Definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply:

3.1. Blockchain Ecosystem

A network of interrelated stakeholders, including infrastructure operators, developers, service providers, users, regulators, and communities, that interact within or across blockchain-based systems.

3.2. Information Sharing

The act of exchanging data, knowledge, or intelligence concerning cybersecurity threats, vulnerabilities, incidents, indicators, tactics, or mitigations among stakeholders.

3.3. Threat Intelligence

Evidence-based knowledge about existing or emerging threats, including indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), and contextual information that can inform decisions about response and mitigation. (Aligned with MITRE ATT&CK)

3.4. Vulnerability Disclosure

The process of reporting and communicating security vulnerabilities to the affected parties, coordinators, and potentially the public, in accordance with responsible or coordinated disclosure practices. (See ISO/IEC 29147)

3.5. Incident

An identified occurrence of a system, service, or network indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that warrants investigation. (See ISO/IEC 27035-1)

3.6. Node Operator

An individual or organization responsible for running and maintaining one or more nodes in a blockchain network, which may validate, propagate, or archive transactions and blocks.

3.7. Protocol Developer

An entity responsible for designing, maintaining, or updating the consensus rules, core logic, and cryptographic mechanisms of a blockchain protocol.

3.8. Coordinated Vulnerability Disclosure (CVD)

A structured process where a vulnerability is reported to the vendor or maintainer, who works collaboratively with the reporter to verify and remediate the issue prior to public disclosure.

3.9. Cybersecurity Information Sharing Community (CISC)

A group of stakeholders that establishes~~establish~~ trust and rules to exchange cybersecurity information within or across sectors. (See ISO/IEC 27010)

3.10. TLP (Traffic Light Protocol)

A system of classification for controlling the dissemination of sensitive information based on color codes (TLP:RED, TLP:AMBER, TLP:GREEN, TLP:CLEAR), commonly used in cybersecurity communities.

3.11. Attribution

The process or decision to link an action (e.g., an attack or discovery) to a specific actor, organization, or identity. May be pseudonymous, anonymous, or fully disclosed depending on policy and context.

3.12. Anonymized Reporting

A reporting mechanism where the identity of the reporter is hidden or protected to reduce the risk of retaliation, reputational harm, or legal exposure.

3.13. Indicator of Compromise (IOC)

A piece of data (e.g., hash value, domain, IP address, file name) that is used to identify potentially malicious activity on a system or network.

3.14. Blockchain Security Incident

A cybersecurity event involving a blockchain system that results in unauthorized access, disruption, data loss, or protocol-level integrity compromise.

3.15. Trust Anchor

A recognized entity or mechanism that serves as a root of trust in information exchange, such as a public key infrastructure (PKI), governance body, or signed registry.

4. Abbreviated terms

ADAPT — Analysis of Defensive, Adversarial, and Protective Tactics

ATT&CK — Adversarial Tactics, Techniques, and Common Knowledge

CERT — Computer Emergency Response Team

CSIRT — Computer Security Incident Response Team

CISC — Cybersecurity Information Sharing Community

CNA — CVE Numbering Authority

CVD — Coordinated Vulnerability Disclosure

DAO — Decentralized Autonomous Organization

DID — Decentralized Identifier

IOC — Indicator of Compromise

ISAC — Information Sharing and Analysis Center

PKI — Public Key Infrastructure

STIX — Structured Threat Information Expression

TAXII — Trusted Automated Exchange of Intelligence Information

TLP — Traffic Light Protocol

5. Context and Justification

The blockchain ecosystem introduces unique challenges and opportunities for cybersecurity information sharing. Unlike traditional centralized systems, blockchain networks often claim to be ~~are~~ inherently decentralized, open-source, and globally distributed. Their resilience and transparency also make them susceptible to novel classes of threats, such as protocol-level vulnerabilities, smart contract exploits, and cross-chain bridge attacks.

The absence of centralized control and the diversity of stakeholders — from pseudonymous developers to regulated financial institutions — complicate the establishment of clear reporting channels, trust models, and response coordination mechanisms.

Traditional information sharing frameworks were not designed to accommodate~~handle~~ the decentralized and borderless nature of blockchain systems. One key reason is the fundamental difference in stakeholder composition compared to conventional systems. This leads to a lack of standardized norms regarding who shares what kind of information, how it is shared, and how it should be utilized.

As a result, information sharing within the blockchain ecosystem often occurs in an ad hoc and fragmented manner, lacking the structure and reliability found in traditional cybersecurity frameworks. This results in a gap where malicious actors can exploit systemic vulnerabilities while defenders remain siloed. Timely and trusted information sharing is thus critical to ensure ecosystem-wide resilience.

To address this gap, it is essential to leverage applicable elements from existing frameworks while designing a new information sharing model tailored to the unique characteristics of blockchain systems. This new framework should facilitate trusted, timely, and effective communication among diverse stakeholders, thereby enhancing ecosystem-wide resilience.

The Blockchain Governance Initiative Network (BGIN) identified these gaps through active engagement with diverse stakeholders including protocol maintainers, node operators, wallet developers, digital asset service providers, CERTs, standards setting organizations, and financial ~~-~~regulators. Stakeholders expressed a need for:

- A common language for classifying, prioritizing, and responding to threats and vulnerabilities~~incidents~~.
- Trust mechanisms that work in pseudonymous or community-based environments.
- Integration with existing standards and best practices (e.g., ISO/IEC 27035, MITRE ATT~~\~~&CK).
- Recognition of blockchain-specific risks and sharing models.

This framework addresses th~~ese~~ unique cybersecurity information sharing needs of blockchain ecosystems by first defining the relevant stakeholders. Recognizing the diversity and decentralization of these~~s~~ actors, the framework then outlines action flows for information sharing and utilization, specifying how incidents, vulnerabilities, and threat intelligence should be communicated, validated, and acted upon across different layers of the ecosystem. To support these flows, the framework introduces governance models that facilitate trust, accountability, and coordination among stakeholders. ~~roles, lifecycles, exchange formats, and governance models that support secure and effective cybersecurity information sharing within and across blockchain networks~~. While it~~It~~ aligns with internationally accepted frameworks, it extends ~~and enhances~~ them with practices grounded in the realities of distributed ledger environments.

By offering an open, adaptable, and standards-compatible structure, the framework encourages adoption across public, permissioned, and hybrid blockchain ecosystems.

5.1. Guiding Principles

- **Purpose-limitation and reciprocity** Share only what is necessary for defence and expect reciprocal behaviour.
- **Timeliness and accuracy** Provide actionable detail quickly and correct inaccuracies promptly.
- **Protection and minimization** Classify (e.g., TLP), encrypt in transit, and minimize sensitive data.
- **No-fault reporting and learning** Encourage reports without initial blame to foster transparency and improvement.
- **Risk-based prioritization** Use severity and risk to drive escalation and external sharing triggers.
- **Transparency and accountability** Record decisions, handoffs, and outcomes; maintain audit trails.
- **Inclusivity and accessibility** Support global participation, language access, and smaller projects.
- **Cryptographic assurance** Authenticate sources and artifacts using signatures or verifiable credentials.

コメントの追加 [1]: Post-incident transparency without compromising trust
Voluntary collaboration through lightweight trust anchors

5.2. Purpose-Limitation and Reciprocity

Information sharing should be strictly limited to what is necessary for defensive purposes. Participants are encouraged to share only the data that directly contributes to threat mitigation or incident response. In return, they should expect reciprocal behaviour from others in the ecosystem. This principle fosters trust and discourages misuse or overreach in data collection and dissemination.

コメントの追加 [2]: Post-incident transparency without compromising trust
Voluntary collaboration through lightweight trust anchors

5.3. Timeliness and Accuracy

Cyber threats evolve rapidly, and delayed information can result in missed opportunities to prevent or contain incidents. Therefore, shared information must be timely and actionable. Additionally, accuracy is critical—any errors or outdated data should be corrected promptly to avoid misinformed decisions or unnecessary panic.

5.4. Protection and Minimization

Sensitive information must be protected throughout its lifecycle. This includes classifying data using schemes, encrypting data in transit, and minimizing the inclusion of personally identifiable or proprietary information. The goal is to reduce exposure while maintaining the utility of shared intelligence.

5.5. No-Fault Reporting and Learning

To encourage transparency and continuous improvement, the framework supports a no-fault reporting culture. Stakeholders should be able to report incidents or vulnerabilities without fear of blame or reputational damage. This approach promotes openness, facilitates root cause analysis, and helps the entire ecosystem learn from past events.

5.6. Risk-based Prioritization

Not all threats are equal. Information sharing should be guided by risk assessments that consider severity, potential impact, and likelihood. This ensures that the most critical threats are escalated and addressed first, and that external sharing is triggered appropriately based on predefined thresholds.

5.7. Transparency and Accountability

All decisions, handoffs, and outcomes related to information sharing should be documented. Maintaining audit trails helps ensure accountability, supports post-incident reviews, and builds trust among stakeholders. Transparency also enables better governance and continuous refinement of sharing practices.

5.8. Inclusivity and Accessibility

Blockchain ecosystems are global and diverse. Information sharing mechanisms must be inclusive, supporting participation from small projects, independent developers, and communities across different languages and regions. Accessibility ensures that security is not limited to well-resourced actors but is a shared responsibility.

5.9. Cryptographic Assurance

To ensure the integrity and authenticity of shared information, cryptographic techniques such as digital signatures and verifiable credentials should be employed. These mechanisms help verify the source of information and prevent tampering, thereby enhancing trust in the shared data.

6. Stakeholders and Roles

Effective cybersecurity information sharing in the blockchain ecosystem relies on the coordinated participation of a diverse set of stakeholders. Each role contributes unique perspectives, data types, responsibilities, and risk exposures. This section outlines key stakeholder categories, their typical responsibilities, and their information sharing interactions.

6.1. Blockchain Protocol Developers

- Maintain and update core blockchain protocols.
- Respond to reported vulnerabilities and incidents affecting consensus logic or cryptographic mechanisms.
- Share post-incident analysis, zero-day alerts, and upgrade schedules with node operators, exchanges, and application developers. ~~and patch details with relevant parties.~~

6.2. Blockchain Network~~ode~~ Operators

- Operate full or validating nodes, participate in consensus, and observe network behaviour.
- Share observations on abnormal network traffic, forks, or denial-of-service attacks.
- Receive alerts, updates, and mitigation guidance from developers and security experts.

6.3. DeFi Protocol~~Smart Contract~~ Developers

- Write and deploy application logic on blockchain platforms.
- Share and receive vulnerability reports, bug bounty outcomes, and secure coding practices.
- Coordinate disclosure and remediation activities in collaboration with affected projects.

6.4. Application Developers

- Detect vulnerabilities in contract interactions and frontend logic
- Remediate unsafe flows, and share intelligence on phishing or impersonation campaigns.
- Collaborate with protocol and wallet providers to contain and mitigate threats.

書式を変更: フォントの色 : 自動

書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))

書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))

書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))

書式を変更: フォントの色 : 自動

書式を変更: フォントの色 : 自動

書式を変更: フォントの色 : 自動

書式変更: アウトライン番号 + レベル : 1 + 番号のスタイル : 行頭文字 + 整列 : 6.3 mm + インデント : 12.7 mm, 罫線 : 上揃え: (罫線なし), 下揃え: (罫線なし), 左: (罫線なし), 右: (罫線なし), 間 : (罫線なし)

~~6.4.~~6.5. Wallet and Transaction Management Providers

- Develop and operate client applications for asset custody and transaction signing.
- Share telemetry or incident reports related to phishing, malware, or signing key compromise.
- Disseminate threat intelligence to users and monitor upstream infrastructure alerts.

~~6.5.~~6.6. Exchange Operators and Infrastructure Providers

- Operate centralized exchanges, bridges, oracles, and hosting platforms.
- Share attack reports, fraud signals, and traffic anomalies.
- Receive intelligence on emerging threats targeting system components.

~~6.6.~~6.7. End Users and Community Members

- Report suspicious activity, phishing attempts, or anomalous application behaviour.
- Receive alerts, software updates, and safety guidance.
- Participate in decentralized trust-building via community moderation and peer reviews.

~~6.7.~~6.8. Security Researchers and Experts

コメントの追加 [3]: Include blockchain analytics firms

- Identify, analyze, and report vulnerabilities, exploits, and system-level risks.
- Share structured threat intelligence, indicators of compromise (IOCs), and technical advisories.
- Share blacklists, scam typologies, and laundering patterns with other stakeholders.

書式を変更: フォントの色：自動

- Engage in Coordinated Vulnerability Disclosure (CVD) with developers and CERTs.

6.9. Auditors and Certification Bodies

書式を変更: フォント：16 pt, フォントの色：ユーザー設定の色 (RGB(47,84,150))

- Share anonymized audit insights, methodology updates, and vulnerability patterns.

書式を変更: フォントの色：自動

- Conduct structured security assessments and provide remediation guidance

書式を変更: フォントの色：自動

- Evaluate compliance with technical standards and issue certifications

書式を変更: フォントの色：自動

- Share anonymized assessment data with industry partners and standards developing organizations.

書式を変更: フォントの色：自動

~~6.8.~~6.10. Cybersecurity Information Sharing Communities (CISCs)

- Facilitate structured information exchange using established trust models.
- Operate under frameworks such as ISO/IEC 27010 and employ confidentiality markings (e.g., TLP).
- Provide anonymized reporting and deconfliction services.

~~6.9.~~6.11. Computer Emergency Response Teams (CERTs)/CSIRTs

- Coordinate technical response to incidents across organizations and jurisdictions.
- Share validated incident reports, remediation steps, ~~and~~ attack campaign analysis, and relevant threat group insights
- Act as trusted intermediaries in the disclosure and escalation process.
- Create and maintain protected safe havens for sharing sensitive threat intelligence, private customer activity data, and vulnerabilities (similar to CVE, 314a/b models)

書式を変更: フォントの色：自動

~~6.10.~~6.12. Regulators and Supervisory Authorities

- Receive mandatory incident notifications and compliance-related disclosures.

- Issue guidance, enforce reporting obligations, and share sector-wide alerts.
- Participate in inter-agency information sharing frameworks.

6.13. Standards Developing Organizations (SDOs)

- Develop and maintain technical and procedural standards.
- Coordinate with other communities and SDOs to extend standards for digital assets.
- Promote adoption and integration of updated standards across blockchain stakeholders.

~~6.11. Governance Bodies and Foundations~~

- ~~Define response policies, approve upgrades, and fund security initiatives.~~
- ~~Share strategic threat assessments and foster collaboration with public and private entities.~~

~~6.14. Foster collaboration with public and private entities, and~~

- ~~Publish public postmortems and improvement proposals.~~

~~6.12.~~6.15. Law Enforcement Authorities (LEAs)

- Investigate cybercrime incidents involving blockchain systems.
- Issue legal preservation requests and coordinate investigations.
- Engage with CERTs and governance bodies to ensure deconfliction during active probes.

This classification is not exhaustive. Stakeholders may play multiple roles or shift responsibilities depending on context and maturity of the blockchain project. The following sections elaborate on their interactions across the incident lifecycle. See Section 7 for lifecycle interactions among these stakeholders.

7. Information Sharing and Utilization Lifecycle

The cybersecurity information sharing and utilization lifecycle in the blockchain ecosystem comprises~~encompasses~~ a series of coordinated stages designed to~~that~~ enable the ~~facilitate~~ timely detection, validation, disclosure, remediation, and continuous learning from cybersecurity threats and incidents. The lifecycle builds upon principles outlined in ISO/IEC 27035, integrates best practices from the NIST i~~I~~ncident response~~R~~ lifecycle~~s~~, and aligns with collaborative norms such as coordinated vulnerability disclosure (CVD).

7.1. Discover

- Detection of anomalous behaviour, vulnerabilities, or indicators of compromise (IOCs).
- Observation by node operators, researchers, automated systems, or users.
- Initial threat signals may be weakly corroborated and require contextual enrichment.

7.2. Alert

- Submission of findings to relevant stakeholders (e.g., developers, infrastructure providers, CERTs).
- Reporting may be anonymous or attributed, using secure communication channels.
- Use of standardized formats such as CVE, STIX, or internal templates is encouraged.

7.3. Remediate

- Development, testing, and deployment of fixes or mitigations (e.g., patch, network parameter change).

書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))

書式を変更: フォントの色 : 自動

書式を変更: フォントの色 : 自動

書式を変更: フォントの色 : 自動

書式変更: インデント : 左 : 14 mm, 行頭文字または番号を削除

書式変更: 見出し 2, アウトライン番号 + レベル : 2 + 番号のスタイル : 1, 2, 3, … + 開始 : 1 + 配置: 左 + 整列 : 6.3 mm + インデント : 14 mm, 罫線 : 上揃え: (罫線なし), 下揃え: (罫線なし), 左: (罫線なし), 右: (罫線なし), 間 : (罫線なし)

書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))

書式を変更: フォントの色 : 自動

- Notification to downstream services, exchanges, and affected users.
- Temporary or emergency measures may be enacted (e.g., circuit breakers, halts).

7.4. Report

- Communication of verified vulnerability or threat details to affected stakeholders
- Usage of secure and reliable channels for dissemination
- Inclusion of contextual information to aid timely response

7.5. Disclose

- Internal or public sharing of validated cybersecurity information.
- May follow a responsible disclosure timeline or coordinated public announcement.
- Accompanied by mitigation advice, TLP markings, and acknowledgments where applicable.
- See Section 8.2 for TLP classification practices applied to disclosure.

~~7.3.~~7.6. Assess~~Validate~~

- Technical verification and risk assessment of reported information.
- Evaluation of project-specific risks using available vulnerability and threat data.
- Involves reproducing findings, impact analysis, and determination of scope for decision making.
- Prioritize risks based on potential impact and likelihood.~~Collaboration between reporters, maintainers, and potentially third-party validators.~~

~~7.4.~~7.7. Analyze

- Deep investigation into root causes, exploitation techniques, and systemic weaknesses.
- Identification of patterns, trends, and possible root causes.
- Mapping to MITRE ATT&CK TTPs, attribution assessments, and cross-chain implications.
- Assessment of implications at the industry-wide or cross-chain level.
- Coordination across domains to assess whether threat is isolated or part of a broader campaign.

~~7.5.~~7.8. Contribute~~Learn~~

- Participation in the creation or refinement of standards.
- Share expertise and lessons learned from past incidents.
- ~~Post-incident analysis and lessons learned documentation.~~
- Contribution to common knowledge bases, code quality improvements, and threat intelligence feeds.
- Updating detection rules, training data, and community playbooks.

~~7.6.~~7.9. Standardize

- Formalization of lessons and practices into reusable patterns, protocols, or control measures.
- Publication of findings to standards bodies (e.g., BGIN, ISO, IETF) and open repositories.
- Contributing to sector-wide maturity through shared norms and benchmarks.

7.10. Promote and Use Standard

- Encouragement of adoption of established standards across the ecosystem.
- Provision of tools, templates, or guidelines to facilitate implementation.
- Highlighting benefits and best practices for compliance.
- Adopting and following established standards in day-to-day operations.
- Training relevant personnel on correct application of standards

書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォント : (英) Arial, (日) Arial, 11 pt, フォントの色 : 黒
書式変更: アウトライン番号 + レベル : 1 + 番号のスタイル : 行頭文字 + 整列 : 6.3 mm + インデント : 12.7 mm, 罫線 : 上揃え: (罫線なし), 下揃え: (罫線なし), 左: (罫線なし), 右: (罫線なし), 間 : (罫線なし)
書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))
書式を変更: フォント : 16 pt, フォントの色 : ユーザー設定の色 (RGB(47,84,150))
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動
書式を変更: フォントの色 : 自動

Reviewing adherence regularly and updating practices as needed.

This lifecycle supports continuous improvement in the blockchain ecosystem's resilience by enabling structured, trustworthy, and effective exchange of cybersecurity information across distributed actors.

書式を変更: フォントの色 : 自動

書式変更: 間隔 段落後 : 0 pt, アウトライン番号 + レベル : 1 + 番号のスタイル : 行頭文字 + 整列 : 6.3 mm + インデント : 12.7 mm, 罫線 : 上揃え: (罫線なし), 下揃え: (罫線なし), 左: (罫線なし), 右: (罫線なし), 間 : (罫線なし)

書式を変更: フォントの色 : 自動

8. Trust, Confidentiality, and Attribution

Trust is the cornerstone of any~~foundational to any~~ cybersecurity information sharing ecosystem. In ~~the~~ blockchain environments~~context~~, where stakeholders may be pseudonymous, distributed, or transient, establishing trust and maintaining confidentiality while enabling actionable attribution requires thoughtful design and adherence to consistent protocols.

In this context, attribution does not necessarily mean revealing real-world identities. Instead, it refers to the ability to trace the origin of information to a trusted source – whether that source is a known organization, a verified pseudonymous actor, or a cryptographically authenticated entity.

Balancing confidentiality with actionable attribution is critical. The framework supports flexible trust models that accommodate both anonymous and identified participation, depending on the sensitivity of the information and the operational needs of the stakeholder involved.

8.1. Trust Models and Communities

Participants may form Cybersecurity Information Sharing Communities (CISCs) as defined in ISO/IEC 27010, which operate on mutual agreements of confidentiality, reciprocity, and purpose limitation. Trust anchors such as governance foundations, technical maintainers, or designated coordinators can help bootstrap confidence.

Blockchain-native trust mechanisms (e.g., signed disclosures using protocol keys or DAOs as trust arbiters) may supplement traditional models.

8.2. Confidentiality Levels

Information exchanged within and between CISCs must be classified using systems such as the Traffic Light Protocol (TLP). Recommended usage is shown in Table 1.

Label	***Intended audience***	***Dissemination guidance***
TLP:RED	Restricted disclosures within vetted response groups.	No further disclosure. For named recipients only.
TLP:AMBER	Recipient's organisation and necessary clients/partners. Operational disclosures to trusted stakeholders	Limit sharing to need-to-know within the organisation and its clients/partners.
TLP:GREEN	For community or sector peers	Share within the community; not via public channels.
TLP:CLEAR	For public advisories.	Public dissemination permitted.

8.3. Anonymity and Pseudonymity

To protect whistleblowers, researchers, or affected users, anonymized or pseudonymous reporting is encouraged. CISCs may support anonymous submission channels, and intermediaries such as CERTs can provide identity shielding. Verification of authenticity may be handled via cryptographic signatures or tokenized credentials.

8.4. Attribution Principles

Attribution of incidents, vulnerabilities, or intelligence to individuals or entities must be handled with caution. Disclosure of attribution should consider the risk of retaliation, legal exposure, and chilling effects on reporting. Framework participants are encouraged to adopt policies consistent with ISO/IEC 29147 and 27010 that limit unnecessary exposure of identity.

8.5. Authentication and Integrity

All shared information should be authenticated to ensure source integrity and prevent tampering. Blockchain-specific solutions such as decentralized identifiers (DIDs), signed messages using protocol keys, or verifiable credentials may be adopted. Transport layer encryption and digital signing practices (e.g., S/MIME, PGP, HTTPS/TLS) should be baseline requirements.

8.6. Escalation and Resolution

Mechanisms must be established for resolving trust disputes, abuse of anonymity, or misattribution. These may include appeal procedures, ombudsman channels, or community-based arbitration. Balancing transparency, privacy, and operational utility is critical. Trust-building must be an ongoing, adaptive process grounded in both technical controls and community norms.

9. Exchange Mechanisms and Formats

The effective dissemination and consumption of cybersecurity information within~~in the~~ blockchain ecosystems depends on standardized, secure, and interoperable, and context-aware exchange mechanisms. Given the diversity of stakeholders and platforms, the framework emphasizes flexibility over rigid standardization, while promoting practices that support trust, timeliness, and machine-readability. This section outlines the types of sharing channels, data formats, and operational considerations that support such practices. ~~trust, timeliness, and machine-readability.~~

While standardized formats offer interoperability, their adoption in blockchain contexts may be limited due to technical and cultural differences. Therefore, this framework does not mandate specific formats, but encourages the use of structured, extensible, and verifiable formats that suit the operational needs of each stakeholder group.

9.1. Exchange Channels

Secure Communication Protocols Email (S/MIME, PGP), HTTPS portals, and encrypted messaging platforms (e.g., Matrix, Signal) for individual or bilateral exchange.

Community Platforms Web forums, mailing lists, and issue trackers for open-source transparency and coordination.

Dedicated Sharing Hubs Blockchain-specific ISACs, CERT portals, and Cybersecurity Information Sharing Communities (CISCs) that host structured submissions.

Automated Threat Intelligence Feeds Real-time dissemination of indicators and advisories via APIs, often using TAXII transport.

9.2. Information Formats

9.2.1. Human-Readable Reports

Advisories, vulnerability disclosures, incident postmortems, formatted in markdown, PDF, or standard templates.

9.2.2. Machine-Readable Formats

STIX (Structured Threat Information Expression) Widely used format for representing threat intelligence.

CVE (Common Vulnerabilities and Exposures) and **CWE (Common Weakness Enumeration)** for standardized vulnerability identification.

OpenIOC, YARA, or **custom JSON schemas** for indicators of compromise.

Refer to Bibliography section for STIX/TAXII reference specifications.

9.3. Open vs Closed Sharing Models

Open Disclosure Public release of information, typically after validation and mitigation, aligned with TLP: CLEAR.

Controlled Sharing Restricted to trusted participants under TLP: AMBER or TLP: RED conditions.

Coordinated Release Timed publications to minimize exposure and maximize preparedness, especially in CVD workflows.

9.4. Metadata and Classification

All shared information should include metadata for:

- TLP classification
- Timestamp and versioning
- Reporter identity (pseudonymous or verified)
- Impact assessment level (e.g., critical/high/medium/low)

9.5. Blockchain-Specific Considerations

On-Chain Anchoring Hashing and anchoring of reports or indicators on-chain for transparency and auditability.

Decentralized Identifiers (DIDs) Use of W3C-standard DIDs for signer verification.

Smart Contract Notifications Automated incident triggers or subscription-based alerting via decentralized services.

These mechanisms enable multi-speed, multi-context information sharing across heterogeneous environments—from pseudonymous open networks to regulated institutional infrastructures—while fostering interoperability with international cybersecurity practices.

10. Governance, Oversight, and Feedback Loops

To ensure~~maintain~~ the effectiveness, integrity, and adaptability of ~~the~~ cybersecurity information sharing and utilization in blockchain ecosystems ~~framework~~, the framework establishes clear governance structures and continuous feedback mechanisms ~~must be established~~. These elements are essential for ~~mechanisms~~ maintaining~~ensure~~ stakeholder trust~~accountability~~, promoting~~e~~ transparency, and enabling~~e~~ iterative improvements as~~aligned with~~ technologies and threats~~ecosystem~~ evolve~~ution~~.

Effective governance requires clearly defined roles, responsibilities, and decision-making processes. In decentralized environments, governance may be distributed across multiple entities while regulatory and public sector oversight can still function. Oversight ensures that information sharing, and utilization practices remain aligned with the framework's guiding principles and stakeholder expectations. Structured feedback loops enable continuous improvement of the framework. Feedback mechanisms should be no-fault and constructive, encouraging open dialogue and collaborative problem-solving. They help the framework evolve in response to emerging threats, technological changes, and community needs.

10.1. Governance Models

Community-Based Governance Participatory governance led by ecosystem stakeholders including developers, researchers, node operators, and foundations. Policies are defined through open deliberation and consensus processes.

Regulatory and Public Sector Oversight For jurisdictions with reporting obligations or supervisory mandates, regulators and national CSIRTs may oversee specific components such as incident notification channels or disclosure timelines.

Consortium-Led Governance Multilateral groups such as BGIN, ISACs, or industry consortia may host and maintain the framework, provide secretariat functions, and coordinate periodic reviews.

10.2. Policy and Participation Rules

Governance structures should define eligibility criteria, participation rights, conflict of interest policies, and escalation procedures. Transparent decision-making and documentation (e.g., meeting minutes, policy updates) are encouraged to maintain stakeholder confidence.

10.3. Oversight Functions

Oversight bodies may include advisory panels, review boards, or technical steering committees. Their responsibilities may include validating member compliance, arbitrating disputes, reviewing disclosures, and setting roadmap priorities.

10.4. Feedback and Evolution Mechanisms

Regular feedback should be solicited from participating entities through surveys, public comment periods, and incident debrief sessions. Lessons learned from real-world incidents should be systematically reviewed and incorporated into updated guidance or lifecycle phases.

Feedback loops should inform revisions to:

- Sharing workflows and templates
- Trust evaluation criteria
- Coordination playbooks
- Integration points with emerging technologies (e.g., ZK-proofs, DAOs, AI-based threat detection)

10.5. Versioning and Change Management

All changes to the framework must follow structured version control procedures. Major revisions should be announced with clear summaries of changes, updated mappings, and transition guidance.

10.6. Inclusivity and Global Representation

The governance process must reflect the global and multi-stakeholder nature of blockchain ecosystems. Language accessibility, regional representation, and inclusion of minority voices (e.g., smaller projects, underrepresented regions) should be prioritized.

Through a balanced combination of structured governance, open collaboration, and adaptive review cycles, this framework can evolve alongside the threat landscape and support long-term resilience across the blockchain ecosystem.

11. Alignment with International Standards

This framework is designed to interoperate with and enhance existing international cybersecurity standards. Its structure, terminology, and processes intentionally align with globally accepted references to ensure consistency, promote reuse, and facilitate adoption by organizations already implementing ISO, NIST, and other best-practice frameworks.

Framework Area	***ISO/IEC Reference***	***NIST CSF***	***Other***
Threat Intel Sharing	27010, 27035-1	DE.CM-6	MITRE ATT&CK
Vulnerability Disclosure	29147, 30111	RS.AN-5	CVD, CNA guidelines
Incident Response	27035-2	RS.CO, RS.MI	FIRST Traffic Light Protocol
Evidence Handling	27002, 27037	PR.IP-3	Chain of custody
Risk Context	27005	ID.RA	ADAPT

11.1. ISO/IEC 27010

The foundational principles of inter-organizational cybersecurity information sharing in this document are derived from ISO/IEC 27010. Concepts such as Cybersecurity Information Sharing Communities (CISCs), trust establishment, information classification (e.g., TLP), and role-based dissemination mirror 27010 guidance.

11.2. ISO/IEC 27035 Series

The incident lifecycle stages (Discover, Report, Validate, etc.) are based on ISO/IEC 27035-1 and 27035-2. Roles such as incident coordinators, reporting interfaces, and validation flows are adapted for decentralized blockchain systems.

11.3. ISO/IEC 29147 and ISO/IEC 30111

The framework incorporates coordinated vulnerability disclosure (CVD) processes outlined in 29147 and remediation workflows from 30111. Adaptations include pseudonymous reporting, decentralized trust anchors, and smart contract patch notifications.

11.4. ISO/IEC 27002 and 27005

Control considerations such as access control for information exchanges, cryptographic protections, and audit logging are in line with 27002 controls. The framework complements ISO/IEC 27005 by embedding risk-based decision points throughout the sharing lifecycle (e.g., prioritization of disclosures, mitigation urgency).

11.5. NIST Cybersecurity Framework (NIST CSF 2.0)

The lifecycle maps to NIST CSF's five functions: Identify, Protect, Detect, Respond, Recover. Detect and Respond phases are enriched through decentralized and community-driven reporting mechanisms.

11.6. MITRE ATT&CK® and ADAPT Framework

The Analyze phase explicitly recommends TTP mapping using ATT&CK to contextualize threat actor behaviour and prioritize response. ATT&CK serves as a taxonomy for threat intelligence structuring and sharing.

ADAPT principles are integrated to represent adversary-defender dynamics over time. The framework encourages retrospective learning and control tuning in response to adversary evolution.

11.7. Interoperability with Global CSIRTs and CERTs

Framework outputs are designed to be consumable by national CSIRTs and regional CERTs. Metadata conventions, classification levels, and incident ticketing align with common practices in these communities.

11.8. Compatibility with Sectoral and Regional Standards

While blockchain is global, regional requirements (e.g., GDPR for disclosure, APAC sectoral obligations, U.S. Treasury alerts) are acknowledged and can be incorporated via annexes or implementation guidance.

This alignment ensures that blockchain-specific adaptations remain grounded in mature, auditable, and widely accepted cybersecurity governance practices. It allows blockchain-native organizations to bridge with traditional institutions while maintaining the flexibility and integrity required for decentralized systems.

Annex A (informative): Use Cases

This annex presents practical examples illustrating how the framework can be applied in real-world blockchain cybersecurity scenarios. Each use case highlights roles, communication flows, information types, and timing considerations aligned with the lifecycle and stakeholder models described in this document.

Coordinated Vulnerability Disclosure in a Smart Contract Platform

Actors: Security researcher, smart contract developer, CERT, bug bounty platform

Flow:

1. Researcher discovers a critical integer overflow vulnerability in a DeFi smart contract.
2. Vulnerability is reported via a pseudonymous bug bounty portal.
3. CERT validates and coordinates remediation with the developer.
4. Once mitigated, a public advisory (TLP:CLEAR) is published, including a CVE reference and mitigation details.

Incident Notification between DApp and Protocol Maintainer

Actors: DApp developer, protocol developer, node operators

Flow:

1. DApp team observes abnormal transaction behaviour suggestive of mempool manipulation.
2. Protocol team is privately notified under TLP:RED using encrypted channels.
3. Investigation confirms a subtle consensus-layer race condition.
4. Patch is deployed via an emergency network upgrade.
5. Postmortem and technical brief shared with ecosystem participants.

書式を変更: フォントの色：自動

Cross-Chain Bridge Compromise Alert

Actors: Bridge operator, wallet provider, node operators, exchanges

Flow:

1. Unauthorized withdrawals are detected from a token bridge.
2. Bridge operator issues an immediate TLP:AMBER alert to integrated platforms.
3. Affected wallets disable certain UI paths; exchanges freeze inflows.
4. Forensic indicators (e.g., attacker address, malicious payload hash) are published in STIX format.

書式を変更: フォントの色：自動

Threat Intelligence Sharing in a Permissioned Consortium

Actors: Consortium node operators, internal CERT, infrastructure provider

Flow:

1. Anomaly detection system flags unusual peer-to-peer traffic.
2. Shared intelligence within the consortium (TLP:GREEN) identifies a coordinated enumeration attempt.
3. Mitigations (e.g., network filtering) are applied across all nodes.

書式を変更: フォントの色：自動

4. Lessons integrated into consortium-wide monitoring playbook.

Regulatory Disclosure by Wallet Provider

Actors: Wallet provider, national regulator, cybersecurity sharing hub

Flow:

1. Compromise of hot wallet infrastructure results in user asset loss.
2. Provider initiates incident disclosure to regulator under jurisdictional mandate.
3. Incident details are sanitized and contributed to a public awareness report via a national ISAC.

These use cases demonstrate the framework's adaptability across permissionless and permissioned settings, support for both anonymous and attributed flows, and its alignment with cross-sector cybersecurity norms.

Annex B (informative): Stakeholder Matrix

The following matrix maps key stakeholders to their typical cybersecurity information sharing activities, highlighting the types of actions they perform and the resources they interact with. This table is designed to support role clarity, accountability, and integration with automated or manual workflows.

Stakeholder role	***Key actions***	***Information types shared/consumed***	***Sharing direction***
Protocol developers	Receive vuln reports; issue patches; publish advisories	Vulnerability data; mitigations; postmortems	Bi-directional
Node operators	Detect anomalies; forward alerts; apply patches	Network anomalies; fork reports; DDoS telemetry	Mostly outgoing
Smart-contract developers	Disclose flaws; coordinate fixes; publish secure-coding guidance	Vulnerability reports; remediation status	Bi-directional
Wallet providers	Report attacks; notify users; update software	Phishing reports; malware indicators; key/signing events	Bi-directional
Security researchers	Submit findings; provide PoCs; publish analysis	IOCs; exploit reports; threat analysis	Mostly outgoing
CISCs / hubs	Intake and triage; anonymize sources; disseminate advisories	Aggregated threat intelligence; TLP-tagged submissions	Bi-directional
CERTs/CSIRTs	Validate incidents; coordinate cross-sector response; notify stakeholders	Validated incident reports; indicators; coordination notes	Bi-directional
Regulators	Receive disclosures; issue sector alerts; request clarifications	Compliance notices; policy updates	Mostly incoming

Exchanges/infrastructure providers	Detect fraud/abuse; share logs; apply emergency controls	Fraud patterns; traffic anomalies; IOCs	Bi-directional
Users/community	Report suspicious activity; consume advisories; provide feedback	User reports; observations	Mostly outgoing
Governance bodies/foundations	Approve processes; fund security efforts; coordinate public disclosures	Strategic assessments; ecosystem impact reports	Mostly outgoing
Law enforcement	Investigate incidents; issue preservation requests; coordinate with CERTs	Legal notices; evidence-handling guidance	Bi-directional

This matrix supports use case development, access control definitions, and policy planning for information flow within blockchain cybersecurity ecosystems.

Annex C (informative): Sample Stakeholder RACI Matrix

Legend—A: Accountable; R: Responsible; C: Consulted; I: Informed.
NOTE: Assignments are illustrative. Accountability follows the component-owner principle for protocol, contract, wallet, or infrastructure issues

	Protocol developers	***Node operators***	***Smart-contract developers***	***Wallet providers***	***Security researchers***	***CISCs / hubs***	***CERTs/CSIRTs***	***Regulators***	***Exchanges/infra***	***Users/community***	***Governance bodies***	***Law enforcement***
Discover	A* / R	R	A* / R	A* / R	R	I	I	I	A* / R	R	I	I
Report	A* / C	R	A* / C	A* / C	R	R	C	I	A* / C	R	I	I
Validate	A/R	C	A/R	A/R	C	R	C	I	C	I	C	I
Analyze	A/R	C	A/R	A/R	C	R	C	I	C	I	C	C
Disclose	A/R	I	A/R	A/R	C	R	C	C/A*	C	I	C	C
Remediate	A/R	R	A/R	A/R	I/C	C	C	I	R	I	C	C
Learn	A/R	C	A/R	A/R	C	R	C	I	C	I	A/R	I
Standardize *(feed back)*	R	C	R	R	C	R	C	C	C	I	A	I

Notes: A* and edge cases

- **Component-owner rule for A*** make exactly one of these Accountable for a given incident, based on where the issue lives.
    - Protocol bug → Protocol developers hold A.
    - Contract/application flaw → Smart-contract developers hold A.
    - Wallet/client compromise → Wallet providers hold A.
    - Infrastructure/bridge/exchange issue → Exchanges/infra hold A.
- Regulators may be A* for Disclose *only* where law assigns accountability for timing/format; otherwise they are C (consulted) or I.
- Security researchers are typically R for Discover/Report and C for Validate/Analyze; they are I thereafter unless specifically engaged.
- CISCs/hubs are R for triage/coordination (Report/Validate/Analyze/Disclose) but not Accountable for fixes.
- CERTs/CSIRTs are C across validation, analysis, disclosure, and remediation; they coordinate and advise but usually don't own fixes.
- Governance bodies become A for Standardize (turning lessons into policies/playbooks) and are A/R in Learn when approving improvements.

Annex D (informative): Terminology

This annex provides additional terms relevant to the implementation of the framework, especially where blockchain-specific cybersecurity nuances may not be fully captured in existing ISO terminology. These definitions are intended to supplement the main body and serve as guidance for consistent interpretation across communities.

Smart Contract

A self-executing program deployed on a blockchain that runs deterministically and automatically enforces rules or agreements encoded in its logic.

Zero-Day Vulnerability

A previously unknown vulnerability that has not been disclosed publicly or mitigated by the software maintainer.

Coordinated Disclosure Window

A negotiated timeframe between a reporter and maintainer during which a vulnerability is privately remediated before public disclosure.

Decentralized Identifier (DID)

A globally unique identifier associated with an entity that does not require a centralized registration authority, often used in trust verification.

Bridge (Cross-Chain Bridge)

A protocol or infrastructure that allows the transfer of assets or data between two or more blockchain networks. Often a high-risk component.

Fork

A divergence in the blockchain ledger, typically resulting from protocol upgrades, consensus errors, or competing rule interpretations. May be soft (backward-compatible) or hard (non-compatible).

Flash Loan Attack

A manipulation technique exploiting instantaneous, uncollateralized loans for arbitrage or malicious actions within a single transaction.

On-Chain Anchoring

The practice of publishing a cryptographic hash of a document or artifact onto a blockchain to provide tamper-evident timestamping and auditability.

Bug Bounty Program

A coordinated reward mechanism that incentivizes external security researchers to responsibly disclose vulnerabilities.

Dusting Attack

A technique in which tiny amounts of cryptocurrency are sent to wallets to deanonymize or track users.

DAO (Decentralized Autonomous Organization)

An organization governed by code and executed via smart contracts without centralized leadership.

Chain Reorganization (Reorg)

The replacement of recent blocks on the blockchain by a competing branch, often due to temporary forks or malicious mining behaviour.

Cyber Hygiene

Routine practices and policies that ensure baseline security, such as patching, MFA, secure coding, and key management.

These terms serve to standardize communications and interpretations across global and decentralized stakeholder groups.

Bibliography

- NIST, Cybersecurity Framework (CSF) 2.0
- MITRE, ATT&CK Enterprise Matrix
- FIRST.org, Traffic Light Protocol (TLP) v2.0
- OASIS, STIX™ Version 2.1 (OASIS Standard).
- OASIS, TAXII™ Version 2.1 (OASIS Standard).
- W3C, Decentralized Identifiers (DIDs) v1.0.
- MITRE, ADAPT Framework