



Blockchain Governance
Initiative Network

Governance of the Security Supply Chain

Cyber Security WG — Session 1-6: Introduction

Shin'ichiro Matsuo — Session Chair

BGIN Block 15 — Georgetown University Capitol Campus, Washington, D.C.

Thursday, 15 October 2026 | 15:40–17:10 | Room A (2416) | Hybrid

Goal: agree what the BGIN security-supply-chain document must cover, and how we get it published.

Time	Part	Lead
15:40–15:50	1. Introduction — where the work stands: the vendor-management guideline documented after the DMM Bitcoin incident	Shin'ichiro Matsuo
15:50–16:15	2. JFSA presentation — the April 2026 cybersecurity policy for crypto-asset exchanges and the June 2026 research paper	Takaya Sugino (JFSA)
16:15–16:35	3. New case — the October 2026 hardware-wallet distribution incident	Discussion
16:35–16:55	4. Additional perspectives for the supply-chain document	Discussion
16:55–17:10	5. Roadmap toward publication: scope, owners, timeline	Discussion

Timings are indicative. Remote participants: please use the chat or raise a hand to speak.

The Attack Surface Has Moved Down the Supply Chain

Attackers go for the weakest link — increasingly one the operator does not directly control.



- Signing keys can be perfectly protected and still be lost through the **people, software, cloud and hardware** around them.
- Many of these suppliers sit **outside the regulatory perimeter** — the operator remains accountable for them.

What happened

- A recruiter on LinkedIn sent a **fake “pre-employment test”** to an employee of Ginco, the exchange’s wallet-system vendor
- Stolen session cookies gave access to the vendor’s **unencrypted communications system**
- A **legitimate DMM transaction request was manipulated**
- Loss: **4,502.9 BTC** (about US\$308M / ¥48.2bn); the exchange later closed

Attribution: TraderTraitor (DPRK), FBI / DC3 /
National Police Agency of Japan, 24 Dec 2024

Lessons

- The vendor was **outside the regulatory perimeter**, yet could influence transactions
- Social engineering of **vendor staff** is a key-management risk
- The operator needs to **verify what it signs**, not only who it contracts with
- Contracts alone do not give **visibility of vendor controls**

What Has Been Documented So Far

Third-party management guideline (JPCrypto-ISAC)

- Written by the industry ISAC in response to the DMM Bitcoin incident
- Built on the **FISC** framework used across Japanese finance
- Focus: **wallet-system vendors** and **cloud** configuration
- Main document + appendices: **MOU template** for vendor contracts, reference architecture, and a **checklist of about 100 controls**
- Presented to BGIN at **Block 14** (Tokyo, March 2026)

BGIN Cyber Security WG

- **Block 13** (Oct 2025): audit frameworks and a shared threat-response knowledge base
- **Block 14** (Mar 2026): the guideline; mapping existing frameworks (NIST CSF, SBOM / EU CRA) to avoid reinventing them; crypto-specific gaps

Regulation is catching up

JFSA supervisory guidelines now flag vendors that temporarily receive key-generation or transfer information as an outsourcing-management risk.

Open question from Block 14: what should a BGIN document add that is *specific* to crypto and digital assets?

Policy on Strengthening Cybersecurity at Crypto-Asset Exchange Service Providers (JFSA, April 2026)

Self-help

Focused monitoring; self-assessment for all exchanges; raising the supervisory guideline's bar on staffing, external audit and **outsourcing management**

Mutual aid

Stronger self-regulatory audit capacity; active participation in information-sharing bodies such as **JPCrypto-ISAC**

Public support

Analysis of past attacks (the June 2026 research paper); Delta Wall exercises; threat-led penetration testing pilots

Research paper: *Cybersecurity Issues and Countermeasures in Crypto-Asset-Related Businesses* (Deloitte Tohmatsu, 30 June 2026) — recommends stronger management of vendors **and their subcontractors**, change management against code tampering, strict verification at signing, and control of external dependencies in DeFi and cross-chain protocols.

New Case: Hardware Wallets Modified in Distribution (Oct 2026)

As reported (investigation ongoing)

- › Ledger devices sold via a Malaysia-based reseller (CryptoBilis) contained a **covert LTE / eSIM implant**
- › The implant read the **24-word recovery phrase from the screen** at setup and sent it out over the mobile network
- › Secure element, firmware and signing were **not modified** — the genuine-device check **cannot detect** an added implant
- › Modified units also bought via **Amazon Japan** and **Yahoo! Auctions Japan**; reports in Singapore and Germany
- › Reported losses: over US\$86M across hundreds of wallets

Industry response so far

- › Ledger halted sales by all distributors in Southeast Asia and Hong Kong
- › MediaMarkt suspended Ledger sales in Europe (13 Oct)
- › Trezor is cutting its reseller network (from 1 Jan 2027); OneKey revoked the reseller

Sources: Ledger Donjon update; BleepingComputer, CoinDesk, The Block, The Verge (10–13 Oct 2026)

Discussion: What Does This Case Add?

The device was genuine — the supply chain around it was not.

- 1 Distribution-channel assurance** — what should manufacturers require of distributors and resellers, and how is it verified?
- 2 Limits of attestation** — genuine-device checks prove the secure element, not the enclosure. What would detect an added component?
- 3 Institutional use** — exchanges and custodians also buy HSMs and hardware wallets: what belongs in procurement, receiving inspection and key ceremonies?
- 4 Accountability** — how are responsibilities split between manufacturer, distributor, reseller, marketplace and operator?
- 5 Link to Day 2** — what should the wallet ST/PP (session 2-10) and offline key management (session 2-8) say about delivery and initialisation?

Discussion: Additional Perspectives for the Document

Layer	Example risk	Coverage today
Wallet-system vendors & contractors	Vendor staff compromised; transaction requests altered	JPCrypto-ISAC guideline
Cloud & CI/CD	Misconfiguration; build-pipeline tampering	Partly (guideline)
Software & open source	Malicious or vulnerable dependency; no SBOM	<i>Gap</i>
Signing interfaces & front-ends	Tampered UI shows one transaction, signs another	<i>Gap</i>
Hardware & distribution	Implanted devices; counterfeit units	<i>Gap — new case</i>
Smart contracts, oracles, bridges	External dependency failure or exploit	Research paper
People & social engineering	Fake recruiters; insider access	<i>Cross-cutting</i>
Assurance & certification	Audits that miss supply-chain risk	ST/PP work (Day 2)

Which layers are **crypto-specific** enough for BGIN to write, and where do we **reference** existing frameworks (NIST CSF 2.0, SSDF, EU CRA, FISC)?

To confirm before we leave the room: scope, structure, editors and section owners, and the timeline.

When	Step
Today (Block 15)	Agree scope and outline; confirm editors and owners per layer
Nov–Dec 2026	Section drafts through Cyber Security WG calls; incorporate the JFSA policy, research paper and the hardware-wallet case
Early 2027	Consolidated draft for WG review
Next Block (2027)	Review in session; resolve open comments
After the next Block	Public comment period, then publication as a BGIN document; consider input to ISO/TC 307

Volunteers needed: editors, a lead for each layer, and case-study contributors.

- › **Session page**, with the research paper, the JFSA policy and earlier meeting reports
- › **Cyber Security WG calls** — drafting continues after Block 15
- › Discussion on the **BGIN Discourse** (bgin.discourse.group)
- › **Related Day 2 sessions:** Security AI Agent (2-4), Offline Key Management (2-8), Wallet ST/PP (2-10)



Session 1-6 page