Third Party Risk Management
Crypto Asset Products and Services

Crypto Assets – Unique Risks

- Knowledge of a private key provides instant and total control over the crypto asset held at the corresponding address. Once compromised, an attacker can move crypto assets in the very next block (less than 10 minutes depending on the blockchain).

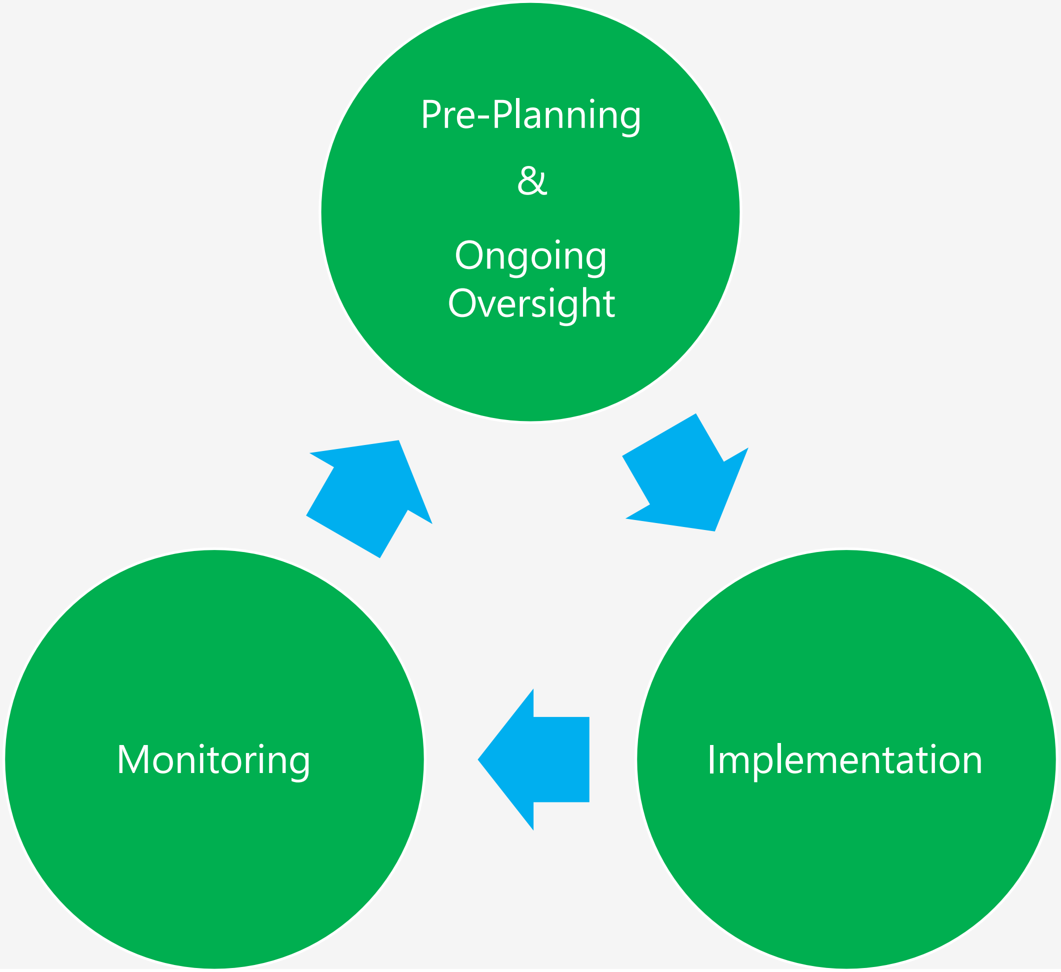
- A private key can facilitate crypto asset movement from any where in the world with an internet connection.

- Accordingly, crypto assets are subject to rapid total loss events where there may be no recovery.

- Lax KYC at certain exchanges, privacy coins (Monero), and mixing services aid cyber criminals' efforts to cash out stolen crypto assets.

- Even where the risk of financial loss is low, the financial institution may incur additional expenses related to a loss event.

3 Phase Risk Management Process



Pre-Planning

&

Ongoing Oversight

Implementation

Monitoring

Pre-Planning – Risk Assessment

- Performed by responsible bank personnel with the requisite knowledge and skills to adequately perform the analysis.
- Assess unique risks including private key management practices, legal permissibility, BSA/AML compliance, insurance coverage, capital and pledge positions.
- Identify the parties that will own and operate critical hardware and software needed to support the product or service.
- Adequacy of FI insurance coverage.

Institutions should maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight.

Pre-Planning – Third Party Due Diligence

- Performed by responsible bank personnel with the requisite knowledge and skills to adequately perform analysis.
- Due diligence should assess the third party's ability to mitigate identified risks, and overall ability to deliver on the contracted services.
- Is the third party experienced providing the service the FI requires? Do they provide the same service to other FIs?
- What risks does the third party's insurance cover and to what extent?
- Preliminary cyber vulnerability assessment.

Institutions should maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight.

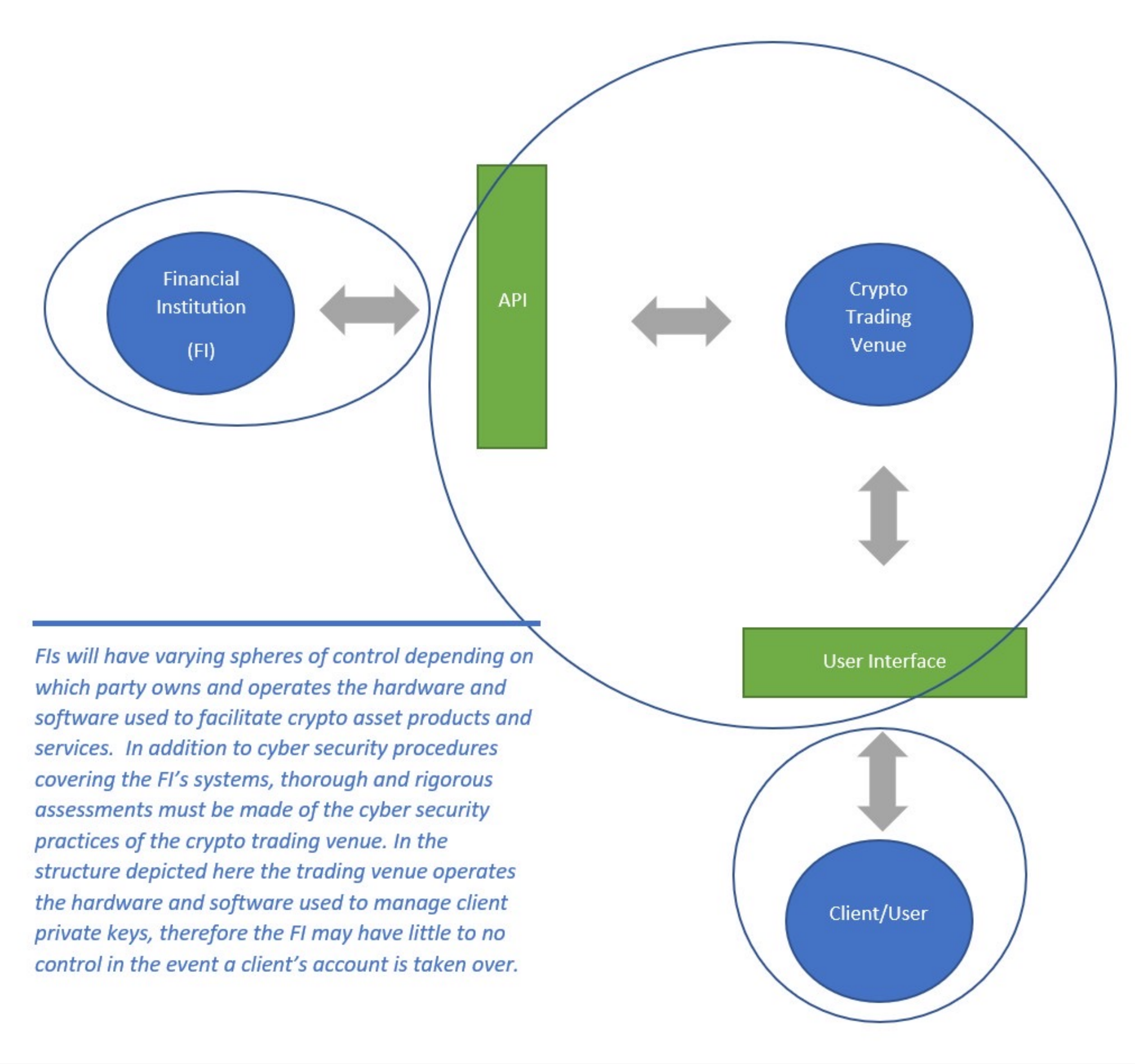
Example: Trading Venue Vulnerability Assessment

- FI does not control any hardware or software used to facilitate on chain movement of crypto assets.

- Third party service provider manages crypto private keys, client user interface, and FI interface e.g. application programing interface (API).

- Vulnerability assessment should assume client and FI access points to the third party may be compromised. With that in mind seek to minimize the damage.

- Leverage internal IT personnel or engage qualified third party for full assessment.



FIs will have varying spheres of control depending on which party owns and operates the hardware and software used to facilitate crypto asset products and services. In addition to cyber security procedures covering the FI's systems, thorough and rigorous assessments must be made of the cyber security practices of the crypto trading venue. In the structure depicted here the trading venue operates the hardware and software used to manage client private keys, therefore the FI may have little to no control in the event a client's account is taken over.

Implementation – Contract Structuring

- Performance standards e.g. uptime, etc.
- Support services e.g. must have access to a live person at the sub custodian.
- Required reporting systems e.g. blockchain analytics, usage rates, etc.
- Access to oversight information e.g. audits, financials statements, insurance polices, policies and procedures, etc.
- Required audits e.g. type, internal, external, etc.
- Indemnification language
- Limits on liability language

Institutions should maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight.

Implementation – Incident Response Procedures

- Response procedures that include on timelines. What to do, who to contact in the first minute, first hour, first day.
- State and Federal Law enforcement reporting/notification (FBI/Secret Service/Homeland/State regulatory authority).
- Incident response service providers e.g. public relations, law firms, forensic blockchain recovery, etc.
- Customer notifications.
- Insurance notifications.

Institutions should maintain documents and records on all incident aspects.

Monitoring

- Real time blockchain monitoring tools (Chainalysis/Elliptic/Ciphertrace/Solidus). May be helpful for certain products and services.

- Establish notifications with open sources e.g. Twitter, Google, etc.

- Allocate sufficient and qualified staff to monitor significant third parties.
    - Review performance standards, reports, records and audits specified in the contract.

- Does the third party maintain adequate licenses and registrations? Monitor for issues.

Institutions should maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight.

Planning for Risk Mitigation

- Does the product/service require movement of on chain assets? Can private key risk be eliminated?
  - Domestic Bitcoin ETFs use cash settled futures contracts (no private keys to steal).

- "Walled garden" or "closed box" platforms?
  - Some spot trading venues do not allow transfers off the platform. Private key could still be compromised but there is no risk of a fraudulent withdrawal request.

- Verbal/video verification prior to on chain crypto asset movement?
  - Extra verification before moving assets off platform.

- Strong authentication, multi-factor, "one time" codes, etc.? e.g. Yubikey.
  - Support strong MFA for users and employ MFA for internal systems.

- Will the FI client know the unique public address?
  - Client will be able to transfer assets to FI. Client will make mistakes.
  - Client will monitor. (Pros vs. Cons).