Keep Implementation of Cryptocurrency Exchanges Healthy: Lessons from Japan's Experience with Mt. Gox and CoinCheck

No Author Given

No Institute Given

Abstract. After the original publication of the Bitcoin paper [1], cryptocurrency exchanges emerged to connect the fiat currency world to the cryptocurrency world. Although many users of cryptocurrency exchanges demonstrate confidence in this simple role for an exchange, recent security incidents suggest that a gap exists between the perception of users and the reality. In this paper, we summarize the results of an investigation of 32 cryptocurrency exchanges by Japanese regulators, then analyze the reality of functionalities, implementation, and operations of cryptocurrency exchanges. Then, from ISMS point of view, we analyze relevant features of the blockchain protocol, cryptographic key management, system security, and operation, and clarify the required actions to secure the implementation and operation of cryptocurrency exchanges.

Keywords: Cryptocurrency exchange, Information security management

1 Analysis of the reality of "Cryptocurrency Exchanges"

1.1 Trends of the shortage of governance and security management

After the CoinCheck incident, JFSA issues 20 administrative penalties to 17 cryptocurrency exchanges. Each release for the administrative penalty explains problems to be fixed. There are 22 kinds of problems are explained. There are 6 major problems and which problems are applicable to each cryptocurrency exchange. They are Corporate management issue, system risk issue, anti-money laundering, segregation of customers' asset, customer protection and consideration to deal with new cryptocurrencies. Though corporate management and AML are the most crotical issues, the other things to be noted is the segregation of customers' asset.

1.2 Functionalities which real cryptocurrency exchanges have

There are many perception gaps between what user of cryptocurrency exchange think and real cryptocurrency exchange. A user has an account at the cryptocurrency exchange, then deposit some amount of money to the account. This implies the cryptocurrency exchange has similar functionality as a bank. Moreover, most cryptocurrency exchanges keep a (private) signing key of each user inside their server. This means such cryptocurrency exchanges have a functionality of custodian. Some cryptocurrency exchanges do not record transfer of cryptocurrency into the original blockchain. In such case, cryptocurrency is “sold” in exchange of customer’s money, but nothing is sold and the customer buys something without the existence of the cryptocurrency. In some case, cryptocurrency is sold by the exchange itself with some information as it seems matched with some order. In th3se cases, the “exchange.” is not true exchange, but a currency shop. There is an essential reason why an average customer deposits the private signing key to the cryptocurrency exchange is, it is not easy to securely manage the private cryptographic key for such an average person.

1.3 Shortage of security consideration

From the analysis of functionalities described in the previous subsection, most of the existing cryptocurrency exchanges have more functionalities than any one of the stock exchange, bank, custodian, and shop.

However, unfortunately, most cryptocurrency exchanges are startup companies. Thus, they do not have enough capability to hire enough experts to design, implement and operate secure cryptocurrency exchange. The number of such qualified experts is quite limited, thus attracting the sufficient number of qualified experts is not entirely a matter of money. As a result, most cryptocurrency exchanges are not designed by general security management methodology for infrastructure. They include not only cryptography but for security for the entire system, like protocol, authentication and access control, authorization, network security, implementation and certification, key management, and operation. However, such system-level security consideration was omitted. For example, the early stage discussion right after the CoinCheck incident was a treatment of cold wallet, which is only a part of security management.

1.4 Discussion on key management

In the CoinCheck incident, the stolen cryptocurrency was NEM, of which the underlying consensus mechanism is based on Proof-of-Stake (PoS). There are many reasons including transaction throughput, to manage the assets of many customers by using one key. In general, PoS type cryptocurrency may give cryptocurrency exchange terrible incentive to manage all assets with one key, because the cryptocurrency exchange can gain mining (or similar) reward by utilizing the vast amount of customer’s cryptocurrency. As a result, cryptocurrency exchange produces a new single point of failure, and it is things should be avoided from the security point of views. Of course, this type of operation is out of the scope of cryptocurrency, but we need to care about the possibility to happen this kind of things. Each consensus mechanism has pros. and cons. generally. However, this is one issue of the downside of PoS type cryptocurrency, and we need to have clear operation policy for PoS type cryptocurrency.

2 Reconsidering governance and security management

2.1 Threat modeling and security requirements

In parallel to the investigation by JFSA, we conducted making a document on security management of cryptocurrency exchange right after the CoinCheck incident. Even now, there is no standardized architecture and implementation of software/hardware for cryptocurrency exchange. Therefore, we cannot edit one standard document toward secure implementation and operation of cryptocurrency exchange. The group gathered information of real cryptocurrency exchanges from their engineers, then create a model of cryptocurrency exchange system. Fig. 3. shows an example of system model of cryptocurrency exchange.

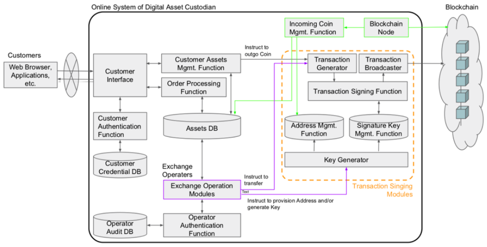
Online System of Digital Asset Custodian
Blockchain
Customers
Web Browser, Applications, etc.
Customer Interface
Customer Assets Mgmt. Function
Order Processing Function
Instruct to outgo Coin
Incoming Coin Mgmt. Function
Blockchain Node
Transaction Generator
Transaction Broadcaster
Transaction Signing Function
Customer Authentication Function
Customer Credential DB
Assets DB
Address Mgmt. Function
Signature Key Mgmt. Function
Key Generator
Exchange Operaters
Exchange Operation Modules
Instruct to transfer
Text
Instruct to provision Address and/or generate Key
Transaction Singing Modules
Operator Audit DB
Operator Authentication Function

Fig. 3. System model of cryptocurrency exchange

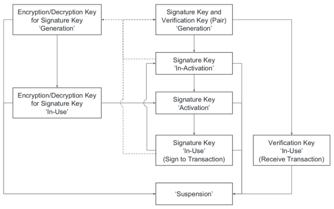
Encryption/Decryption Key for Signature Key 'Generation'
Signature Key and Verification Key (Pair) 'Generation'
Signature Key 'In-Activation'
Encryption/Decryption Key for Signature Key 'In-Use'
Signature Key 'Activation'
Signature Key 'In-Use' (Sign to Transaction)
Verification Key 'In-Use' (Receive Transaction)
'Suspension'

Fig. 4. Key life-cycle at cryptocurrency exchange

The model consists of Customer Interface for UI for login and transaction, Customer Authentication Function, Customer Credential Database, Customer Assets Management Function, Blockchain Node for incoming transactions, Incoming transaction management Function, Order processing function, Assets Database, Transaction Singing Function for outgoing transactions, Exchange Operation Modules, Operator Authentication Function and Operator Audit Database. We defined each functional element to distinguish functions logically, and do not show the actual arrangement on the actual system. After a pair of a signature key and a verification key (hereafter "key pair") is generated, an address to receive transactions is generated from the verification key. By notifying a sender of crypto assets this address, the sender is able to transfer the asset to the address. When the recipient transfers the asset to the other address, the original recipient signs the transaction data which includes the transfer order. Inactive state of the signature key is the state such that the signature key

Table 1. Keys in cryptocurrency exchange

Types	Description
Signature Key	A private key for signing transactions (asymmetric key cryptography)
Verification Key	A public key for verification of transactions (asymmetric key cryptography)
Encryption/decryption key for signature key	Secret key to keep confidentiality of signature key (symmetric key cryptography)
Master Seed	A seed to generate a signature key in decisional wallet

is stored in confidential manner in the signature key management function of Fig. 3. An example of inactivation is encryption by encryption/decryption key (e.g. pass phrase), that is, the signature key is encrypted. In contrary, activation is the process to make the key usable to sign, by decrypting the inactivated key. The activation is assumed to be executed in transaction signing function of Fig. 3. Activation and inactivation may be executed in an implementation of wallet, when the wallet have both functions. The signature key is not needed after its generation until execution of signing to transaction. Thus, there is a way to manage the signature key in offline manner with storing the verification key and address online(cold wallet).

On the usage of multiple keys: In some crypto assets system, it is recommended not to use the same key pair twice, thus it produces multiple key pairs. This feature is for preventing trace and not relevant to the business efficiency of a cryptocurrency exchange.

On the suspension of keys: Suspension of key usage is only an operation inside a cryptocurrency exchange. By definition of blockchain based crypto assets system, any user cannot cancel transaction once it is made. As another case, it is difficult to revoke signature key even after the suspension of key. For example, a customer accidentally operate some crypto assets for suspended address. In such case, the suspended signature key is needed to make an reimbursement. Thus, suspension of keys should be conducted with considering such cases.

2.2 Analysis based on security management standard

On stakeholders [1] It is needed to consider protection of customer’ s assets, as well as division of responsibility with outsourcers including security of private key management for crypto asset, and mattes by which a cryptocurrency exchange may give social impacts like money laundering.

On security policy [2] A cryptocurrency exchange should define a security policy which includes security objectives and controls. Especially, it is recommended to disclose the security policy on the management of crypto assets to customers to facilitate self evaluation.

Continuous risk evaluation and improvement [3] A cryptocurrency exchange should watch security risks of crypto assets in addition to aligning the general security management framework, because the risks change and increase due to rapid development of related technology. It is especially important to continuously evaluate risk and improve security objectives, policy and controls to keep effectiveness of security controls after starting their operations. A cryptocurrency exchange should decide security objectives and controls with considering viewpoint as countermeasure to threat as lost, theft, leak and abuse of customer’ s assets data and private key for crypto assets, requirements for actual business, compliance to laws and rules and social responsibilities to prevent crimes in use of crypto assets like scam and money laundering.

[1] ISO 27001 [5] Clause 4

[2] ISO 27001 [5] Clause 5

[3] ISO 27002 [6] Clause 6, 8, 9 and 10

The cryptocurrency exchange conducts threat analysis, vulnerability evaluation, risk evaluation and defining security objectives and controls according to its actual business and system. Security objectives and controls should be decided with considering threats and risks specific to crypto assets, as well as general security objectives and controls described in ISO 27002 [6].

Risk analysis of signing secret key Risk analysis differs depending on the assumed threats, system configuration, threat modeling, and so on. Here, the threat concerning the signature secret key and the factors that can cause the threat are assumed as follows. the following as the actor giving input to the signing secret key based on Fig. 3

- Threats: lost, leakage, theft and fraudulent use.
- Factors of Threats: mis-operations, legitimate users' malice, spoofing, intrusions from outside and unintended behaviors of implementations.
- Actors: exchange operation modules, transaction signing modules, customer asset management function implementation and incoming coin management function implementation.

Of these threat factors, theft and fraudulent use are regarded as threats that can only be caused by explicit malicious factors.

3 Directions to secure cryptocurrency exchanges

3.1 Required technologies

From above analysis, there are six issues where we need to consider to introduce enhanced technologies to make cryptocurrency exchange trustable.

Authenticity and integrity of segregated ledger: Many cryptocurrency exchanges manage customers' assets by using the segregated ledger, and they record not all transactions on the public blockchain, because of efficiency and latency reasons. Assuring integrity and authenticity of segregated ledger is essential part of security of their business. Introducing transparent way, such as cryptographic timestamp, to assure such characteristics is needed.

Muti-signature: Multi-signature is a major technology to avoid loss of customers' asset when loss of one or minor part of keys occurs.

Underlying cryptography and implementation: HSM is the trust anchor of cryptocurrency exchange. In general, HSM supports standard cryptographic algorithms. However, cryptocurrency may implement special algorithm or parameter as curve of ECC. Standardization of underlying cryptography and selecting HSM which supports more algorithms are needed.

Kay management and wallet: Most cryptocurrency exchanges manage assets using hot wallet for online transaction and cold wallet to protect keys from attack from network. For online wallet, utilizing certification program like FIPS 140-2 or CMVP and products with such certification is needed.

Audit: Internal audit and third party audit is needed to provide transparency to customers and regulators. Technology to make such audit easy such as cryptographic time stamp is needed.

External evaluation: To clarify the security level of implementation, certification as common criteria (ISO/IEC 15048) is needed. Establishing protection profile is helpful to conduct external evaluation.

3.2 Required operations

Basics of key management In general private cryptographic keys. should be isolated from other informational assets, the number of access to private keys should be limited as minimum as possible and be prepared for unintentional lost of private keys. Three security controls as State management of private keys, Administrator role separation and mutual check-and-balance and Backup of private key are needed.

Backup Backup is the most fundamental and effective measure against lost of signing key. On the other hand, there are risks of leakage and lost of backup device. These risks depend on the kind backup device, thus security controls on such devices should be considered independently. Typical ways are Cloning to tamper-resistant cryptographic key management device, Backup to storage for digital data and Backup to paper.

Offline management There is a type of offline key management (as known as "cold wallet") which isolates private keys from the system network to prevent leakage and theft caused by intrusion.

Distributed management It is also a good security control to distribute the right to use private key to multiple entity. There are two examples; division of secret key and multi-signature.

3.3 Toward standardization

Though it is too early to define some technology and operational standards, some standardization bodies started already their activities and study toward the future standard. On the security of cryptocurrency exchange, ISO TC307 started two projects to make a technical report on the security of blockchain and distributed ledger technology (ISO TR23245) and a technical report on security practice of digital asset custodians (ISO TR23576).

4 Conclusion

The analysis implies the needs of a feedback loop for continuous enhancement. We conducted modeling and risk analysis on the cryptocurrency exchange, aligning to ISO/IEC 27000, and created an example system and key management model. We found that the key lifecycle and management model is largely different from ordinary PKI. We showed typical key management model from the analysis. Establishing a concrete loop and new key management especially for PoS, is essential to not re-invent the wheel and to make a healthy cryptocurrency ecosystem.

References

1. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *https://bitcoin.org/bitcoin.pdf.*
2. Japanese Financial Services Agency, “Guidelines for Administrative Processes: Financial Companies No16,” *https://www.fsa.go.jp/policy/virtual_ currency/02.pdf*
3. Japanese Financial Services Agency, “Interim report of inspection and monitoring on cryptocurrency exchanges,” *https://www.fsa.go.jp/news/30/virtual_ currency/20180810-2.pdf*
4. MUFG, “Annual Report (USGAAP),” *https://www.mufg.jp/english/ir/annualreport/2018mufg/pdf/mar/ar2018.pdf*
5. “ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements,” *https://www.iso.org/standard/54534.html*
6. “ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls,” *https://www.iso.org/standard/54533.html*