Keep Cryptocurrency Exchanges Healthy: Lessons from Japan's Regulatory 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. That is, operations, informational asset to be protected, and security postures should be clarified. In this paper, we summarize the results of an investigation of 16 registered and 16 semi-registered 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. We argue that the current activities in the IETF and ISO to develop common document to secure cryptocurrency exchanges would help industry as well as regulators to move forward towards establishing a healthy ecosystem.

Keywords: Cryptocurrency exchange, Information security management, Standards

1 Introduction

1.1 Background

Eliminating the trusted third party in realizing network-based services is one of the biggest dreams in financial cryptographic research. Hence this is the main subject in this world. The main reason why we seek to eliminate the trusted party is, it is too difficult to realize expected trusted party. Such difficulties are caused by operator's mistakes, malicious activities, and collusion with other parties. Many cryptographic techniques like secret sharing scheme, threshold cryptography, and multi-party computation protocol are well studied to realize many network-based services without trusted parties. The sentence, "An electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." is the explanation of Bitcoin - one of the most attractive cryptographic protocols - described in the original paper [1]. Bitcoin is one of the most excellent cryptographic protocols which claimed to realize payment scheme among cryptographic protocols which try to eliminate the trusted party.

Despite this attractive claim of bitcoin, there are fundamental assumptions in the claim. That is, it holds only when the payment is conducted by bitcoin, and no exchange to any other methods exists. Its "without trusted third party" claim realized by the distributed protocol is applicable only on the ledger of payment record for bitcoin. If we wish to exchange Bitcoin to other assets like fiat currency, the action of exchange is outside of what original paper claims. That is, we need to assume some kinds of trust at a party which exchanges trust-less cryptocurrency to other assets. Most people believe that cryptocurrencies are operated in the "trust-less" manner, as most cryptocurrency advertisement says. However, the cryptocurrency exchanges in real life are hidden trusted parties.

Throughout the history of trust-less cryptocurrency, there are many incidents have happened. In 2013, Mt. Gox lost many Bitcoin due to their careless operation and transaction malleability. In 2018, CoinCheck was hacked by a targeted attack and lost over 500M dollar equivalent NEM, and Zaif also lost 50M dollar. Such incidents are caused by a misunderstanding of required trust in operating such a party. When considering the amount of value that such companies deal with, these companies - implicitly assumed to be trusted - should be secure enough against any kinds of attacks including cyber attacks. However, even now, such companies do not have enough expertise and human resources to secure their implementations and operations against such security concerns.

Usually, when we build an information system, we conduct design and implements of security mechanisms and operations, with aligning information security management system (ISMS) as the ISO/IEC 27000 series. The process includes threat modeling, risk analysis, and design and implementation of security countermeasure and operations. However, at the time of wringing this paper, there isn't any agreed unified security standard. Hence, the design and implementation of each cryptocurrency exchanges vary among operators. This situation makes operations challenging to secure the cryptocurrency exchange.

1.2 Contributions

The aim of this paper is giving a real status on the security of cryptocurrency exchange to consider future of uniformed security technology, management, governance, and standard. Firstly, we will show the results of investigation and audit to 32 cryptocurrency exchanges in Japan, conducted by the Japanese Financial Services Agency, the governmental regulatory authority of Japan. The investigation and audit were conducted right after the incident at CoinCheck (January 26, 2018). This includes analysis of the actual incidents, perspectives of investigation and results. From this starting point, we give a detailed analysis of what levels of security and governance are implemented and what are missing. Then we reconsider the governance and security management required to cryptocurrency exchange including threat modeling of existing form of exchange. Then we show the required technology, and operations from the above analysis, as well as the recent progress of standardization.

2 Investigation and audit to 32 cryptocurrency exchanges

2.1 Security incidents and their history

After Bitcoin was introduced in 2008, there have been many incidents happened at cryptocurrency exchange. Following are the summaries of major incidents happened in Japan.

Mt. Gox incident (2014): Mt. Gox was the world largest cryptocurrency exchange in 2014, which occupied about 70% of bitcoin transaction. The exchange did not segregate customers' assets from the exchange's asset. The customers' assets were not recorded into Bitcoin blockchain but recorded into some segregated ledger. Thus, the attacker had a chance to attack the segregated ledger instead of the attack on the blockchain and cryptographic keys itself. The CEO of Mt. Gox claimed that the incident was caused by transaction malleability of Bitcoin protocol. By utilizing this vulnerability, the adversary could convince the exchange modified transaction IDs. This was one of factors of stealing bitcoins.Several experts pointed out that the loss was caused by this vulnerability, but other significant factor of lost was internal malicious activities and attack on segregated ledger from outside.

CoinCheck Incident (2018): In January 2018, CoinCheck, one of the biggest cryptocurrency exchange, but it was semi-registered to Japan Financial Service Agency (JFSA) was hacked and about 526,800,010 XEM was stolen. It was equivalent to 500M dollar. 260,000 customers of CoinCheck where victims. This incident happened by the targeted attack as the first step. Adversary sent CoinCheck several emails to inject malware. As a result, the adversary succeeds to intrude into the CoinCheck's network. The adversary could control computers remotely; then the adversary obtained a secret cryptographic key. After that, the adversary sent XEM stored inside the CoinCheck's network outside within 30 minutes. This indicates that all XEM are associated with one secret cryptographic key, and the amount of coins which each customer have is managed with a segregated ledger. This was the same situation as the Mt. Gox incident. The XEM stored in the hot wallet, that is the device that was connected to the internal network. Multi-signature, which is a general technique to divide signing privilege among multiple persons, was not implemented. The main reason why CoinCheck did not implement was, the cryptographic algorithm and its parameter (elliptic curve) did not fit to software/hardware of key management device. This implies, the kind of coin can affect the specification and operation of cryptocurrency exchange, but such difficulties were not disclosed at that time.

Zaif Incident (2018): In September 2018, a hot wallet in Zaif was hacked and about 50M dollar equivalent Bitcoin and other cryptocurrencies were lost. The specific problems of Zaif are it is registered cryptocurrency exchange under the current regulation. Moreover Zaif was subject to administrative sanctions twice after the investigation described in this section. But, it did not compliant these sanctions.

2.2 Perspectives of investigations

In May 2016, JFSA has amended Payment Service Act to ensure the trust of cryptocurrency users and AML/CFT, and has mandated cryptocurrency exchanges to register to JFSA and comply with legal requirements since April 2017.[1] In April 2017, JFSA also introduced Guidelines for administrative processes explaining how JFSA will supervise exchanges. In it, JFSA clarifies that 1) it will check each cryptocurrency if it is appropriate for exchanges to deal with from the view point of user protection and public interests, 2) it will check management's ability to ensure the operational adequacy including a) legal compliance, b) user protection, and c) risk management, and 3) foreign exchangers which provide services to people living in Japan need to register to JFSA [2].

After the CoinCheck incident, JFSA conducted monitoring on all the 32 companies and the on-site inspections of 7 registered and all the 16 under-registeration exchanges to check if they comply with the regulation. In so doing, JFSA clarifies that it reviews the business practices, the risks and compliance management, as well as the internal audit and corporate culture/governance, especially focusing on the perspectives including 1) the practice of assessment on the risk characteristics of the cryptocurrency a company deals with, 2) adequacy of risk management, 3) practice on anti-money laundering and anti-illicit activities, and 4) Practice on segregation of customers' assets

On the basis of the findings from the on-site inspection, JFSA issued business improvement orders and business suspension orders to those companies with problems. It also turned down the registration request from one company. Receiving these orders, 12 under-registration companies gave up registration.

2.3 Results of investigation and audit

On August 10, 2018, JFSA published an interim report of the results of the on-site inspection and the monitoring with the aim of helping cryptocurrency exchanges to improve their business practices and regulatory compliance [3]. In section 2 of the report, JFSA shows numbers related to exchanges[2]. Fig 1 shows the number of total assets of 13 registered and four under-registration exchanges in the last business year and Fig 2 shows the amount in the latest business year. Fig 3 shows the change in the amount of total asset in one business year, which growth reaches on average 553%. The report explains the massive increase of the total asset was caused by the hike in the exchange rate of the cryptocurrency against fiat currency since fall in 2017. Fig 4 shows the number of employees of all exchanges and Fig 5 shows customers' assets they manage. Based on these numbers, the report calculated the amount of customers' assets that one employee manages shown in Fig 6. JFSA point out by citing this number

[1] JFSA has allowed companies which had already operated when the regulations was implemented to continue operation during the registration process. Thus registered exchanges and under-registration exchanges exisit as of September 2018.

[2] Fig 1 to 3 and Fig 4 to 6 in the following shown in Page 4 and Page 5 of the JFSA's report respectively.

that very few people manage the huge amount of customers' assets; on average, one person manages $30 million. JFSA explains that the establishment of the internal management was too slow to keep up with the rapid business expansion and management lacks awareness of the risks associated with the custody service managing the huge amount of customers' assets.

JFSA shows findings within the business practices, the risk and compliance management, and the internal audit and corporate culture/governance as summarized in the following.

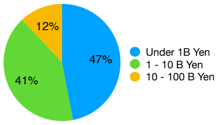

Fig 1. Amount of assets (F.Y. 2016)

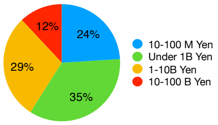

Fig 2. Amount of assets (F.Y. 2017)

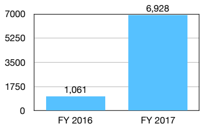

Fig 3. Total Amount of assets

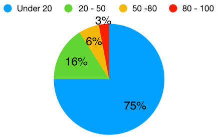

Fig. 4. Number of Employees

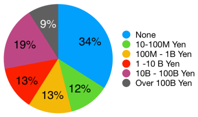

Fig. 5. Amount of assets deposited

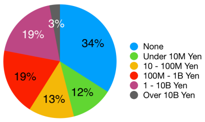

Fig. 6. Amount of assets deposited / employee

Frontline: The business practices The report points out the issues around 1) selection process of cryptocurrency to deals with, 2) inappropriate distribution of cryptocurrency and 3) advertisement. More concretely, the report explains that many[3] exchanges lack business practices to assess risks associated with each cryptocurrency while they focus only on customer convenience and the profitability. And several[4] exchanges lack internal rules that define investment limits and criteria for solicitation and transaction based on the ''principle of suitability' concerning customers' characteristics. The report even points out a case of price manipulation. There also found cases where advertisements of exchanges could mislead users.

Second line: The risk and compliance management The report points out the issues around 1) AML/CFT, 2) segregation of customers' assets, 3) system risk management, 4) customer protection, 5) third party delegation.

For AML/CFT, several exchanges lack enough experts who can provide appropriate advice to frontline staff regarding risk managment. Thus many exchanges fail to comply with the regulation that requires multi-layer countermeasures for AML/CFT such as the establishment of internal guidelines, conducting customer due diligence, and monitoring of suspicious activities. The report shows a case where an exchange allows an organized crime group member to continue transaction for a while after the exchange realized that the customer is a member the group.

[3] "Many" in this section means JFSA found similar issues in 8 or more exchanges.

[4] "Several" in this section means JFSA found similar issues in 2 to 7 exchanges.

For segregation of customers' assets, JFSA explains that several exchanges manage cryptocurrency in the hot (online) wallet, fail to reconcile on the daily basis between account balance within their server and that on the blockchain, and lack an ex-post verification process of reconciliation. Several exchanges also combine customers' assets and their own assets in order to keep the amount on the blockchain larger than the account balance within internal server. There is a case where an exchange even does not segregate customers' assets at all for some cryptocurrency. Yet another exchange, even when it recognizes that the account balance of internal server becomes below the balance on the blockchain, neither appropriately identify the cause nor address it. The report also points out the issues related to management of fiat currency in a similar manner. Furthermore, JFSA found that several exchanges fail to follow regulatory requirements on bookkeeping and an exchange even diverts money to other purposes.

For systemic risk management, JFSA shows that many exchanges lack human resources and training to manage the information system and fail to establish a contingency plan based on the risk scenario on cyber attacks. An exchange even issues new crypto assets without conducting a security evaluation of the underlining technology. JFSA also points out problems on authority management and countermeasures toward system troubles. For instance, within several exchanges, the same person develops and operates the system, and an exchange also fails to impose appropriate restrictions on holders of administrative IDs. Lack of record keeping and efforts to address the root cause of system troubles are also pointed out. In addition, lack of awareness of system limitation caused over capacityof of trading volume in an exchange.

For customer protection, the report mentions problems related to crypto assets issuance. There are several cases found in individual exchanges such as failure to keep promise that the money raised is invested in new businesses, lack of clear understanding on accounting practices for cryptocurrency issuance, failure to disclose any unfair treatment including the huge discounts for insiders or realized differences between reality and the white paper. JFSA also found issues that several exchanges fail to establish customer information management guidelines, lack access control on customer information and fail to address customer complaimnts in an appropriate way. The report also shows examples where exchanges fail to conduct the assessment on volatility and trading volume of the cryptocurrency to decide loss-cut or set leverage limitation of margin trading.

For third-party outsourcing, the report explains several individual cases. For example, an exchange neither conduct the assessment of third-party contractor nor establish a formal outsourcing contract. Another exchange using cloud service fails to establish an outsourcing contract with its provider because of the lack of awareness that the cloud server is the third party to manage.

Third line: The internal audit The report reveals that there are no internal audit or the internal audit is not based on the risk assessment within several exchanges. In many exchanges, there are not enough experts in internal audit implementation regarding AML/CFT and system risk management. For example, many exchanges fail to conduct the internal auditbecause only one person who has another position is assigned to the position in charge of internal audit. Furthermore, in an exchange, a person who is in charge of internal audit reports no problem even though the person, in fact, did not verify it.

Corporate culture and governance The reports point out that exchanges prioritize profit making and lack culture of compliance and customer protection and internal management. For example. JFSA found that many exchanges fail to hire enough staff and improve IT system to support the expansion of the business. There is a case where management meeting focuses solely on expansion and advertisement but not on internal management. In an exchange, major shareholders and the management are not separated and management prioritizes profit of these shareholders.

Even though exchanges are in essence financial institutions, engineers who lack expertise in financial business manage the company. From the first point, many exchanges even lack awareness that they are financial institution dealing with huge amount of customers' assets

The weak management by the company's Board of Directors is also an issue. It is often the case that the CEO has too much power and the Board and internal audit fail to check the management. For example, several exchanges fail to keep the record of the Board meeting and the Board members are not well informed to play an appropriate role. For another example, the Board members fail to check if the money raised by token issuance is used as promised or check if the external auditor has enough knowledge and experience to conduct the appropriate audit.

3 Analysis of the reality of "Cryptocurrency Exchanges"

3.1 Trends of the shortage of governance and security management

During JFSA did audit and investigation, it issues administrative penalties to cryptocurrency exchanges with problems. 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. Table 2 shows 6 major problems and which problems are applicable to each cryptocurrency exchange. These 6 problems are those which over 25 % of cryptocurrency exchange was requested to fix them. They are Corporate management issue, system risk issue, anti-money laundering, segregation of customers' asset, customer protection and consideration to deal with new cryptocurrencies.

From this table, the first important result is that most of all cryptocurrency exchanges which were penalized, did not have qualified corporate management, system risk management and systems and operations for anti money laundering. This indicates there is no common understandings on the implementation and operations for financial services. The lack of management of system risks is indicates that such cryptocurrency exchanges do not have enough number of qualified system designers, engineers and operators. As we described in 2.1, most of incidents were caused by attacks from outside, and the amount of assets

Table 1. Major problems which each cryptocurrency exchange was requested to fix

Problems	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)
Management	x	x		x	x	x	x		x		x	x		x		x	x
System Risk	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
AML	x	x		x	x	x	x		x	x	x	x	x	x	x	x	x
Segregation	x			x		x	x		x			x	x	x	x	x	x
Customer	x			x	x			x		x	x					x	
New coin	x			x		x			x			x				x	

should incentivize the attackers to mount actual attacks. Thus, each cryptocurrency exchange should hire a group of experienced security experts. However, the reality is not the case.

AML is the main issue from the regulatory authority point of view. However, most of all penalized cryptocurrency exchanges did not have enough operational capability in this. That is, such cryptocurrency exchanges did not hire such experts and hence they were not qualified as financial institutions.

The other things to be noted is the segregation of customers' asset. This is a quite fundamental operation as a financial institution, but over 50 % of penalized cryptocurrency exchanges manage customers' assets with the institutional assets, private assets, or assets of multiple customers co-mingled.

3.2 Functionalities which real cryptocurrency exchanges have

There are many perception gaps between what user of cryptocurrency exchange think and real cryptocurrency exchange. From the word of "Exchange," a general person think the task of the cryptocurrency exchange is matching selling orders to buying order like a general stock exchange. However, 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. By investigation described in 2, some cryptocurrency exchanges do not record transfer of cryptocurrency into the original blockchain, but manage another database (hopefully some blockchain system) as a ledger inside the exchange. 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. However, the suggested price is shown by the exchange, and the transaction is conducted by price asked. In this case, the customer thinks the transaction is conducted by the result of matching over market, but the reality is simple purchasing. In this case, 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.

From above all, the functionality of cryptocurrency exchange is apparently beyond the "exchange", and in some case, it is a simple shop, and in the worst case, this might be selling nothing in exchange of real money.

3.3 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. Thus, the cryptocurrency exchange needs to manage security risks according to all the functionality it has. Hence, the security consideration should be the sum of security management for each function and more. With considering the amount of values each cryptocurrency exchange deals with, it should be a big target of cyber attacks. Such cyber attacks cause most of past incidents described in 2.1. Thus, each cryptocurrency exchange should be tolerant to global scale cyber attacks.

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.

3.4 Issues which are common to the financial industry and specific to cryptocurrency exchange

Most of the issues described in section 2 are common to the financial industry. However, the rest is specific to cryptocurrency exchange. Among six significant problems described in 2.4, corporate management and customer protection is common to the financial industry, and there are no specific matters to cryptocurrency exchange. System risk is, of course, common to the financial industry, but the design and security management of information system depends on each specific business conditions. For example, key management is one of the biggest issues in the application of cryptography. Given the real world business of cryptocurrency exchange, many customers deposit their private cryptographic keys. The key management lifecycle is different from ordinary Public Key infrastructure (PKI). Informational assets, attack surfaces, threats, and risks vary due to each business environment. We will analyze the security management of cryptocurrency exchanges in section 4. AML is also a common issue for all financial business, but anonymous cryptocurrency causes many difficulties than ordinary financial services. In the case of CoinCheck incident, the stolen NEM coin could not be actually traced. Currently, cryptocurrency exchange is one of few targets of regulation, because it is the connecting point between cryptocurrency and real-world economy. With current regulation which fits FATF recommendation, most of all cryptocurrency exchange conducts verification of identity. Introduction of Decentralized Exchange (DEX) will eliminate the point of regulation. Thus it should increase this difficulty. Dealing with a new coin is a new issue for cryptocurrency exchange. New cryptocurrency should be evaluated on its characteristics and technical reliability.

3.5 Discussion on key management

Segregation of customers' asset has another discussion issue. In the case of CoinCheck incident, all assets deposited at CoinCheck are managed by using one cryptographic key pair (address), and this is the reason why the entire customer assets were stolen in a short time period. In this 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. It is not clear that this was the reason why CoinCheck managed the all assets by using one address. However, 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.

4 Reconsidering governance and security management

4.1 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.

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,

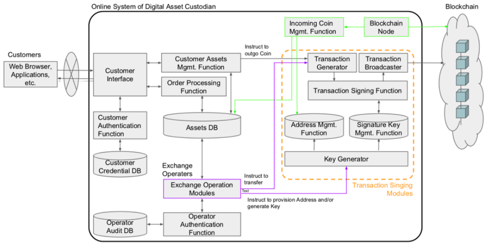
Online System of Digital Asset Custodian
Blockchain
Customers
Web Browser, Applications, etc.
Customer Interface
Customer Assets Mgmt. Function
Order Processing Function
Instruct to outgo Coin
Incoming Coin Mgmt. Function
Blockchain Node
Transaction Generator
Transaction Broadcaster
Transaction Signing Function
Customer Authentication Function
Assets DB
Address Mgmt. Function
Signature Key Mgmt. Function
Customer Credential DB
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

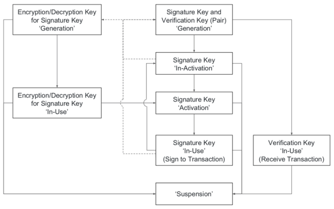
Encryption/Decryption Key for Signature Key 'Generation'
Signature Key and Verification Key (Pair) 'Generation'
Signature Key 'In-Activation'
Encryption/Decryption Key for Signature Key 'In-Use'
Signature Key 'Activation'
Signature Key 'In-Use' (Sign to Transaction)
Verification Key 'In-Use' (Receive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

Fig. 4. Key life-cycle at cryptocurrency exchange

Assets Database, Transaction Singing Function for outgoing transactions, Exchange Operation Modules, Operator Authentication Function and Operator Audit Database. Details are described in Appendix 1.B

We defined each functional element to distinguish functions logically, and do not show the actual arrangement on the actual system.

Table 2. 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

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 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.

4.2 Analysis based on security management standard

On stakeholders [5] 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 [6] 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 [7] 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.

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].

[5] ISO 27001 [5] Clause 4

[6] ISO 27001 [5] Clause 5

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

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. As a result, the possible risks for signing key to be assumed are the figured in appendix 1.C

5 Directions to secure cryptocurrency exchanges

5.1 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.

5.2 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.

5.3 Fixing pitfalls

One of the sources of problems is gaps in understandings among stakeholders. There are four major stakeholders; cryptocurrency exchange, cryptocurrency engineers/researchers, regulators, and customers. Cryptocurrency exchange might start the business without sufficient knowledge of security management, and assumptions in operating cryptocurrency system, though any technology has an assumption and limitation for operation. As a result of the investigation, most cryptocurrency exchanges do not have qualified knowledge and capability to operate as financial institutions. Some exchange does not deal with requests from the regulatory authority, that is, there might not be a common language for communication between cryptocurrency exchanges and regulators. Regulators also do not have enough technical knowledge to evaluate the technological reliability of each cryptocurrency. Customers need the knowledge to evaluate each cryptocurrency and transparency for the operation of cryptocurrency exchange. However, currently, disclosure by cryptocurrency exchange is not sufficient. Many scams occur from this asymmetry of knowledge. Such a difference of understandings is a source of difficulties to solve the problem. We need to create a common dictionary for conversation among all stakeholders and a neutral place to communicate in a multi-stakeholder manner.

5.4 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). Such standard or agreed document is needed to operate any organization associated with blockchain technology, because they store and utilize cryptographic keys. These documents are useful not only for constructing a cryptocurrency exchange, but also audit, creating and operating management lifecycle, providing pieces of evidence of secure operation to the public, and earning trust to operators of trustless financial systems.

6 Conclusion

Giving the unfortunate occurences of huge incidents at cryptocurrency exchanges, Japan is the most advanced country to deal with cryptocurrency governance issues. In spite of the advanced regulation on the exchanges in Japan, investigations by JFSA after the incidents reveal the shortage of technical, operational, and governance expertise. The analysis implies the needs of a feedback loop for continuous enhancement (Kaizen Loop). 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 kaizen 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*

Appendix 1.A Other concrete examples of issues showed in the JFSA’s report

The following is the other examples of issues showed in the JFSA’s interim report from investigation and monitoring that are not discussed in section 2.

1. First line: Issues around advertisements
    - An exchange does not have the internal review process of the contents of the advertisement.
    - An exchange used TV advertisement on which famous celebrity calls the name of the certain cryptocurrency to encourage customers to buy it while explains risks only in few seconds.
    - An advertisement shows a particular discount period and investment profitability that customers cannot verify.
2. Second line: Issues around AML/CFT
    - Many exchanges fail to confirm customers' characteristics and purpose of the transaction as well as conduct pre-examination to exclude transactions with the organized crime group.
    - There are cases of lack of appropriate guidelines regarding checking process of impersonation
    - An exchange lacks monitoring process and system to detect suspicious activities.
3. Second line: Issues around segregation of customers' assets
    - Several exchanges fail to reconcile between bank account balance for customers' assets and account balance on their own server.
    - An exchange fails to find out the cause of the frequent incident that the customers' bank account balance becomes below the balance on their own server.
    - Several exchanges create general ledger only and fail to keep books on daily transactions, the ledger of their own account, and the ledger of customers' account, all of which are required by regulation.
4. Second line: Issues around system safety management
    - Several exchanges neither keep records of system troubles that keep date/time and the number of incidents, impact, countermeasures, and changes to prevent re-emergence nor understand the root cause of the system troubles even though they had many troubles.
    - In the system development phase, an exchange neither establishes documents for requirement definition, development plan, and architecture specification nor conducts implementation tests at the frontline.
5. Second line: Issues around customer protection
    - When an exchange issues its own currency, it fails to explain the financial situation and business model of the issuing exchange to customers.
    - Another exchange issuing new currency fails to disclose important information that management of the exchange gain a huge bonus for sale of the cryptocurrency.
    - Several exchanges fail to conduct a training program on customers' information management and allow anyone in the company and third-party contractor to access to it or even bring out from the company.
    - Several exchanges fail to either keep records of the customer complains or improve the business practice based on the complaints. They just ignore them or randomly address them case by case basis.
6. Third line: Issues around internal audit
    - Many exchanges fail to establish a plan for internal audit.

  - Even when an internal audit was conducted, several exchanges fail to do it based on the risk assessment.
  - Several also fail to conduct the audit on the third party contractor.
7. Corporate culture and governance
  - Within many exchanges, board meeting fails to discuss how to mitigate risks associated with their business as financial institutions.
  - Many exchanges fail to disclose their business and financial situation to customers in an easy-to-understand manner, which other financial institutions are required.

Appendix 1.B Details of system model

- Customer Interface
  Provides screen and input functions such as login process, account management (deposit/withdrawal instruction etc.) and trade instruction for the customers(users). Web application, API, etc.
- Customer Authentication Function
  Performs user authentication process for login to the cryptocurrency exchange.
- Customer Credential Database
  Manages required IDs for login and verification information related to user authentication process (f.g password verification info.).
- Customer Assets Management Function
  A group of functions to manage customer accounts. Receive instructions for deposit or withdrawal (outgoing coins) and perform processing according to the user instructions. Refer or update asset data.
- Blockchain Node
  Connects to another blockchain nodes to retrieve blockchain data.
- Incoming transaction management Function
  Checks transaction stored in blockchain and confirm whether incoming coins are involved in the specified addresses.
- Order processing function
  A group of functions that receives sales instructions from customers and performs processing related to trading of crypto assets. Refers and updates asset data based on asset data.
- Assets Database
  Manages holdings of fiat currencies and crypto assets. It does not include the private keys for signing transactions. Managed separately from the assets of the excahnge for each customer.
- Transaction Singing Function, which includes Transaction Generator, Transaction Broadcaster, Transaction Signing Function, Address Management,
  - Transaction Generator
    Generates transactions to be sent to the blockchain based on instructions from the customer asset management system or the exchange management system, and Private Signature Key Management Function

  - Transaction Broadcaster
    Sends the signed transaction to the blockchain. Connects to nodes of the another nodes on the blockchain.
  - Transaction Signing Function
    Generates digital signatures based on the instructed transaction contents and the private signature key (with IDs and addresses).
  - Address Management
    Manages public keys with related to the private signature keys, or addresses (such as values calculated from the public keys).
  - Private Signature Key Management Function
    Manages the signing keys of the crypto assets (the keys used for the transaction signing). Sometimes it is separated into the cold-wallet as security countermeasure. " Signature key generator " creates signature keys. The generated keys are registered in the signature key management unit, and the public keys and addresses are registered in the address management units.
- Exchange Operation Modules
  A group of functions for exchanges ' administrators. Based on operations from administrators, instructs generation of generating new signature keys or transfer crypto assets.
- Operator Authentication Function
  Authenticates the administrator users.
- Operator Audit Database
  Manages verification data related to the authentication processes of the administrators.

Appendix 1.C Risk analysis

The following list shows the result of risk analysis on the model of cryptocurrency exchange.

1. Threat by lost - Risk of Unauthorized operation (with legitimate path)
   - End-user's malice
   - Operator's malice in Custodian
   - Spoofing to end users
   - internal frauds (spoofing to operators) - Risk of Intrusion from the outside
   - Intrusion into the transaction signing modules
   - Intrusion into the incoming coin management function (implementation)
   - Intrusion into the customer asset management function (implementation)
   - Intrusion into the exchange operation modules - Risk of System Behaviors different from human operation
   - Unintended behaviors of the transaction signing modules
   - Unintended behaviors of the incoming coin management function (implementation)

  - Unintended behaviors of the customer asset management function (implementation)
  - Unintended behaviors of the exchange operation modules - Risk of mis-operation (by human error)
  - Mis-operation of end user
  - Mis-operation of operator
2. Threat by leakage - Risk of Unauthorized operation (with legitimate path)
  - End-user's malice
  - Operator's malice in Custodian
  - Spoofing to end users
  - internal frauds (spoofing to operators) - Risk of Intrusion from the outside
  - Intrusion into the transaction signing modules
  - Intrusion into the incoming coin management function (implementation)
  - Intrusion into the customer asset management function (implementation)
  - Intrusion into the exchange operation modules - Risk of System Behaviors different from human operation
  - Unintended behaviors of the transaction signing modules
  - Unintended behaviors of the incoming coin management function (implementation)
  - Unintended behaviors of the customer asset management function (implementation)
  - Unintended behaviors of the exchange operation modules - Risk of mis-operation (by human error)
  - Mis-operation of end user
  - Mis-operation of operator
3. Threat by theft - Risk of Unauthorized operation (with legitimate path)
  - End-user's malice
  - Operator's malice in Custodian
  - Spoofing to end users
  - internal frauds (spoofing to operators) - Risk of Intrusion from the outside
  - Intrusion into the transaction signing modules
  - Intrusion into the incoming coin management function (implementation)
  - Intrusion into the customer asset management function (implementation)
  - Intrusion into the exchange operation modules
4. Threat by fraudulent use - Risk of Unauthorized operation (with legitimate path)
  - End-user's malice
  - Operator's malice in Custodian
  - Spoofing to end users
  - internal frauds (spoofing to operators) - Risk of Intrusion from the outside
  - Intrusion into the transaction signing modules
  - Intrusion into the incoming coin management function (implementation)
  - Intrusion into the customer asset management function (implementation)
  - Intrusion into the exchange operation modules