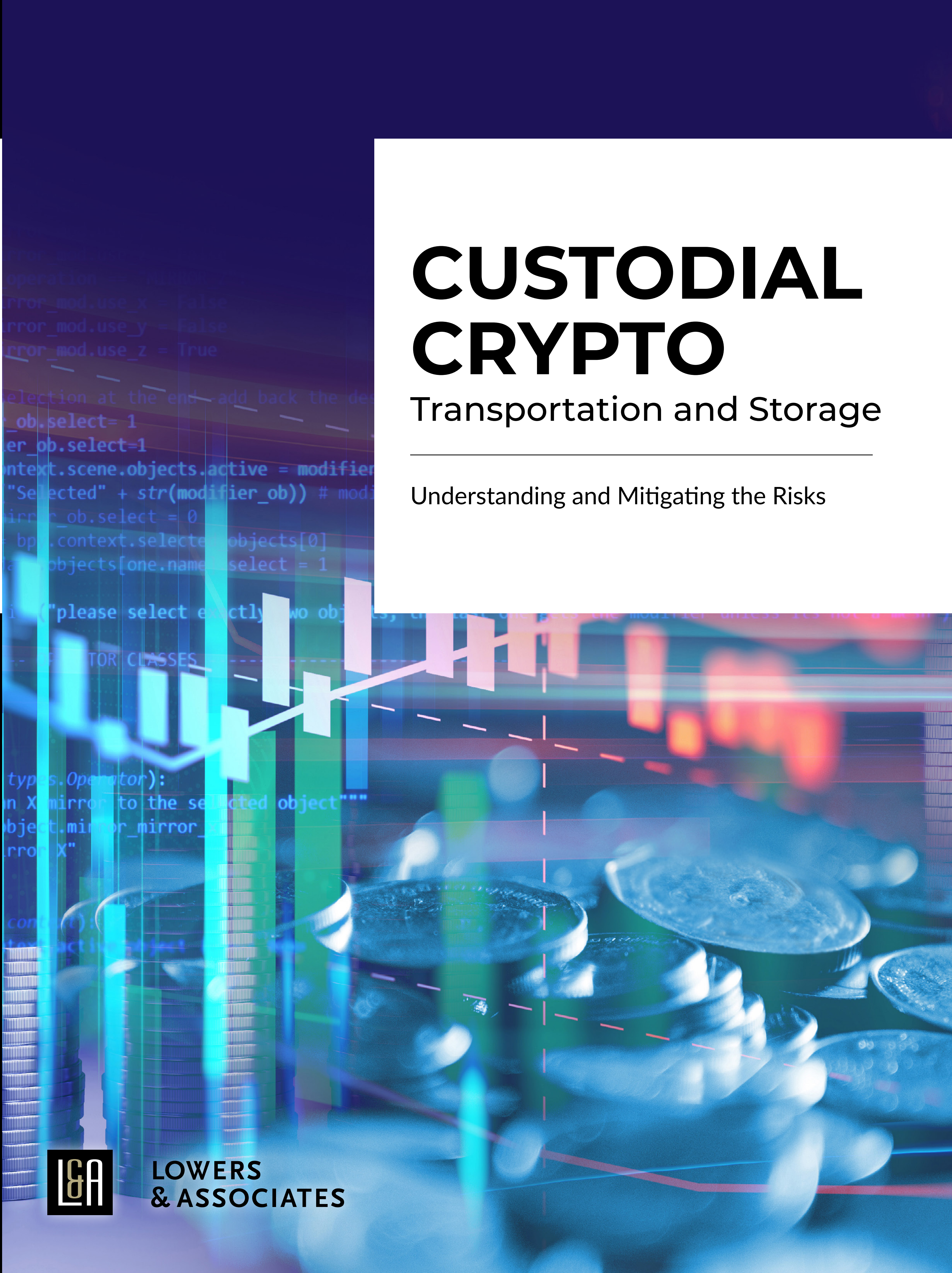
CUSTODIAL CRYPTO

Transportation and Storage

Understanding and Mitigating the Risks



LOWERS & ASSOCIATES

INTRODUCTION

After a decade of fevered speculation and extreme volatility, digital currencies (‘crypto’) are beginning to be incorporated into established financial systems. Blockchain-based crypto currencies are something new under the sun, and they are not fully protected by the security routines devised for traditional fiat currencies.

As Philip Martin, Head of Security for Coinbase, the largest crypto exchange in the U.S., says:

> **“Crypto currencies have a threat model that’s fundamentally different from what’s come before. We’re taking the lessons from the past about physical security and blending them with well-structured cryptography.”**

Coinbase is one of many businesses that is developing new custodial practices to safeguard crypto currencies in transit and storage. These custodial controls include a blend of tactics, some designed to thwart digital attacks and some to provide physical security.

Lack of sophisticated custodial solutions has been implicated in some of the spectacular losses of crypto over the past few years. Investors who suffered those losses often had no recourse to recover losses, and they were certainly not insured.

Neither large investors nor insurers will enter crypto markets unless the risk of loss can be better understood and mitigated. Development of crypto custodial solutions requires the adaptation of established practices by transit and storage companies to include elaborate digital controls as well as physical ones.

There is some irony in the fact that the imposition of these controls on crypto counter one of the main original purposes of digital currencies: to eliminate the need for the third-party validation and security that typify traditional fiat currencies. The wild west of crypto is giving way, and new forms of custodial control will be required to allow crypto to continue to grow and be used in a wide range of transactions.

This white paper is mostly concerned about best practices for the protection of crypto currency in transit, in storage, and in deposit and withdrawal transactions. It will describe the kinds of policies and practices—controls—you need to install to ensure secure custody of the crypto so that possession of it is an insurable risk.

A CAUTIONARY STORY ABOUT LOSS

Crypto has been a risky bet. CNBC reports that

$1.1 BILLION

in crypto currency was stolen in the first half of 2018.

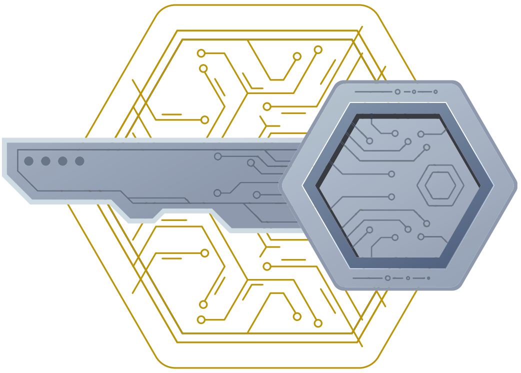
A quick recap of last year's amazing story of the theft by hackers of $530,000,000 from Coincheck, a centralized crypto exchange based in Tokyo, shows the kinds of threats facing crypto and points at how custody solutions have to evolve.

With a surprising lack of caution, Coincheck had stored NEM coins (a crypto currency) in a "hot wallet" (connected to the Internet) rather than a "cold wallet" that was not connected. The company also failed to have multiple signature requirements for the movement of currency. The company asserts that it was not an inside job, so the hackers must have been able to penetrate a wallet online and steal the critically important "private key", an encrypted piece of code that could open the wallet to the thieves.

An oddity of the crime is that we know exactly where the stolen currency is. A blockchain is a publicly transparent ledger that records all transactions in plain view, so we know which accounts the stolen coin is in. But without having the private keys to those accounts, the currency cannot be recovered. Since blockchain ledger entries are permanent and irreversible, the ledger cannot simply be rolled back to before the theft.

In a kind of rough justice, the thieves cannot easily move the currency because it would have to be done under public scrutiny enforced by the rules of the blockchain code. They own half a billion dollars they cannot use.

DEFINING THE RISK OF CRYPTO



The fundamental risk in crypto is that a huge amount of virtual money can be stored digitally in virtual reality (online) or on tiny devices (offline). Anyone who has access to the storage medium can easily move any amount of currency. Access is controlled through the use of an encrypted "private key," and the key is usable by whoever possesses it—the identity of the legitimate owner may not even be known.

When crypto is stored online (hot storage), the risk is that the private key is stolen, giving its possessor control of the funds. Online threats come in the form of hacking, phishing attacks, social engineering, and insider fraud. When crypto is stored offline (cold storage), both the currency and the private key are directly vulnerable (though holding the coin without the private key would be pointless). The threats are more familiar to custodians of cash, including forcible robbery, break and enter, loss of physical possession, and inadequate controls. In both cases, transactions should be multiple-signature and similar controls are required.

Just to be clear, crypto currencies do store enough value to make the design of custodial solutions very important. As of this writing, the total dollar-denominated value of Bitcoin in circulation is

$64.3 BILLION;

the second largest crypto, Ethereum, is valued at $16.1 billion; and Ripple (XRP), the third largest, is $15.1 billion. The total market value of all traded crypto currencies is almost $134 billion. And yes, you can exchange your crypto for U.S. dollars, or almost any other fiat currency you want.

In its basic form, crypto is a peer-to-peer, non-governmental alternative currency, and does not have systemic safeguards like those built into fiat currency financial systems. Losses are not insured. Coin that is stolen or lost may not be recoverable. Virtual peer-to-peer transactions do not carry any of the guarantees normally provided by banking institutions in typical fiat currency systems. There are no government regulations intended to protect the financial system as a whole, or ensure transparent activity.

The first step away from this basic system was the creation of exchanges like Coinbase and Coincheck. These third-party institutions, operating primarily online for transactions, have been the biggest sources of losses. As we have seen, they are beginning to develop better controls to safeguard the crypto they store.

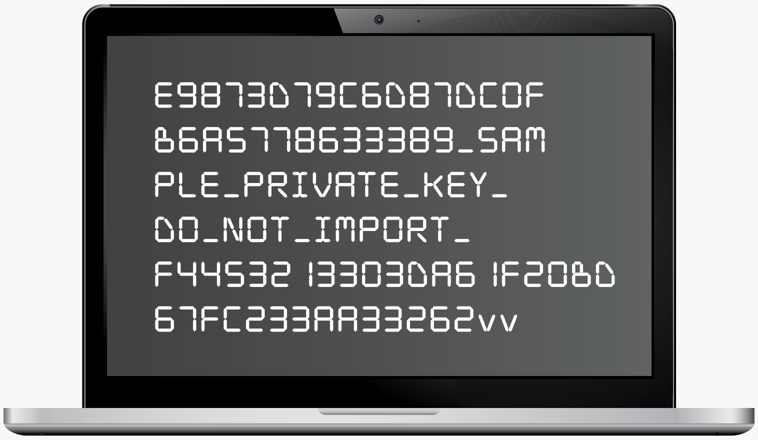
The amount of money in crypto currencies is drawing traditional financial actors into the crypto world. The way this is going to happen is by adapting some of the regulations as well as controls developed for fiat currencies to crypto. Bloomberg argues that regulation will soon be applied to crypto, and that will create an environment attractive to large traditional investors. These investors will also demand secure custodial solutions.

A new financial sector is emerging that blends traditional and crypto currency worlds. Financial giant Fidelity recently announced the creation of a new digital asset service that would facilitate buying and selling crypto and provide a custody solution as well. A Silicon Valley startup called BitGo has been approved in South Dakota as a licensed trust under Securities and Exchange rules, and will voluntarily comply with Know Your Customer and AML practices.

INSURANCE INDUSTRY PERSPECTIVE

Insurers need to know the value of what they are insuring and what the risks are. Since native blockchain-based crypto currencies are unregulated, they are highly vulnerable to criminal abuse like money laundering (Liberty Reserve founder, Arthur Budovsky, pled guilty to laundering more than $250 million using his crypto exchange, a precursor to Bitcoin). Account holders of a crypto blockchain account or on unregulated exchanges are anonymous, defeating the point of Know Your Customer rules.

The security of the private key is an urgent concern, especially in cold storage. In Bitcoin, the basic private key is a software-generated random series of 64 characters using 0 - 9 and A - F that looks like this unusable sample:



```
E9873D79C6D87DC0F
B6A5778633389_SAM
PLE_PRIVATE_KEY_
DO_NOT_IMPORT_
F44532 13303DA6 1F20BD
67FC233AA33262vv
```

This 128-bit encryption is impossible to guess or replicate (for more information about Bitcoin private keys, click here). The private key is linked to an account, and gives its possessor the ability to open the account and use the contents. Even though the headline might scream “millions of dollars-worth of crypto are in that account,” the crucial custodial issue is the private key. Many of the controls implemented by an exchange or vault, or Cash in Transit business concern the security of the private key in cold storage.

KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML) CONCERNS

Insurers will insist on practices implementing AML and KYC controls, as well as rigorous accounting and access procedures. There is still some uncertainty about the legal applicability of Securities and Exchange Commission or Bank Secrecy Act/AML rules for crypto—especially the blockchain itself—but insurance companies will require equivalent types of compliance. As the excellent brief by David Cohen shows, U.S. policy toward crypto is to foster transparency in transactions, following the standards contained in existing laws and regulations.

Controls and procedures are in place for corporate or private clients vetting to the natural person, ensuring compliance with Anti-Money Laundering, Sanctions and Bribery & Corruption regulations.

Clients complete evaluation questionnaires and surveys intended to authenticate client identity and pinpoint areas of heightened risks within client operations. Mitigation measures will be implemented as appropriate to the risks identified.

If a storage or transit custody provider claims that crypto in cold storage is insured, it must describe the controls and limits it imposes on the currency for the insurance company and receive confirmation that the procedures are acceptable.

Custody providers must have a designated compliance officer. The officer is responsible for reviewing training and tracking activities of all staff who implement controls, and maintaining records that verify compliance.

Private keys must be stored in an adequate vault. In addition to a vault that is sufficiently hardened, surveillance must be available continuously, and all access monitored. Every access episode must be recorded in detail as to who accesses the storage, when, for what purpose, and for how long. These records must be monitored, video must be retained for at least 30 days, 45 days is preferred, and all records regularly audited for accuracy.

Providers should model potential disasters and develop prevention and recovery plans appropriate to that disaster. The disaster models and plans can be the basis for “table top” simulations to evaluate them. These stress tests should be documented in the record and updated in response to on-going events in the industry.

The client contract will define the availability, frequency, timing, and procedure for withdrawal of crypto from cold storage. The withdrawal process and security controls will include:

- ✓ A method to authenticate withdrawal requests (KYC).
- ✓ A storage or transit provider procedure for pre-authorization of a withdrawal, including multiple signature reviews.
- ✓ A record of all individuals with access to the private keys, backups, and hardware, and of the specific individuals who participate in a specific withdrawal.
- ✓ At least two people whose identities are listed in the provider's employment and authenticated should be required for access to each private key.
- ✓ At least two people whose identities are listed in the provider's employment and authenticated should be required to access cold storage.
- ✓ If there are multiple layers of encryption governing access to cold storage, each layer will have a separate private key. Multiple private keys must be accessed by separate individuals.
- ✓ No single individual should have access to both a private key and its corresponding cold storage device, truck or vault.

Management procedures for private keys and backups, whether sustainable paper or hardware, must be documented and reviewed/trained periodically. Once crypto is deposited in storage or transport, records of associated private keys will not leave the secure environment. The record will include details of the location(s) where private keys are stored. These locations can be accessed according to a stated policy, and never by a single individual.

Following a withdrawal of crypto, the balance of funds assigned to that address must be deposited onto a new private key. Whether it is the entire contents of the wallet or partial contents that are transferred to a new account or exchanged, the old private key should be destroyed, and never reused for any function.

EVALUATING THE CONTENT VALUE: IS IT EVEN POSSIBLE?

In most cases, the monetary value of crypto in an account can be known as long as the chain of possession is secure. On a crypto blockchain like Bitcoin, every account displays a public record of its contents accessible through the public key, so the fiat currency value in the account can be estimated by using the current value of the currency on an exchange.

The volatility of crypto currencies poses a challenge for insurers. These markets must be monitored continuously to know when contract adjustments are needed. Cold storage and transport providers may set a maximum value for a private key to access, which could require new private keys for excess values. As crypto evolves, and with the addition of more secure controls to the crypto monetary systems, this concern may ameliorate.

- ✓ Guarding high value digital files like crypto poses special challenges. In general, online locations, such as an account at an exchange, are vulnerable to various kinds of theft. But once the crypto is moved offline to cold storage, there are still issues related to the digital character of the files.
- ✓ All devices used to store crypto and private keys must be fully offline (“air gapped”), using methods incapable of either communication via a network or memory that survives its single use. All devices used to produce or store a private key should be destroyed, especially including any element (like a solid-state drive) that might have memory.
- ✓ When necessary, private keys should be generated using new/pristine computers (randomly sourced if possible) with secure wallets. If possible, the creation of private keys should occur in a shielded space with no potential sources of data transmission.
- ✓ Machines/internal components should also be inspected to ensure no covert tampering hardware has been installed, either at the factory or intercepted during shipment.

PROVIDER CHARACTERISTICS ARE KEY

Insurers will want to understand fully how crypto cold storage and transportation vendors are organized. In addition to the general characteristics of the vendor business, every instance of moving crypto to cold storage will involve the activities of employees of the vendor. Employees have to be vetted as fully as any client under KYC rules. These details will be essential for underwriting the services.

Details about the general organization of the vendor will be required, beginning with its qualifications (licensing, certifications) and length of experience. Vendor description should include biographical and work-related background information on employees with access to crypto and private keys, including owners, major investors, and senior management. Any third-party provider with access to crypto or private keys should be subject to the same documented scrutiny.

Vendor qualifications will include both procedural and physical custody arrangements (see below). Written descriptions must be available.

Vendors will be required to demonstrate that involved employees have been properly researched, and that they have the experience and training to accomplish required tasks. Given the novel challenges of a virtual currency, sufficient training must be in place. These requirements will be continuous, with periodic review.

The client base of the vendor implies a KYC type of requirement. The number of clients, clients' crypto holdings by value and distribution, and the total exposure of the vendor must be described. Whether clients are large or small financial institutions, or individuals, their organizations and business practices are important. Some of these may be subject to regulations under the Bank Secrecy Act or other AML rules regarding money transfer, including the $10,000 limit, and appropriate reporting is required. In all cases, the natural persons controlling the 'client' must be known.

Vendors should have policies and procedures in place that are sufficient to manage client accounts. Segregation of every client/crypto combination is important, with separate, unique private keys created for each. These accounts will vary in the number of distinct stores of crypto by value, how private keys are assigned to accounts, and how they are accessed when under possession of the vendor. Very specific rules should be in place to govern withdrawals and other transactions, as described above.

SECURE TRANSPORT AND STORAGE INDUSTRY PERSPECTIVE

As Cash in Transit (CIT) operators, vault operators, and other providers look to serve the needs of the crypto industry, they must fully understand the associated risks and ensure proper components are in place to have those risks mitigated and insured to the fullest extent possible.

Providers should be well-schooled on the insurance company views about crypto, described above, and comply with those requirements. However, they have added risks due to the fact that they will be in physical possession of the crypto files and private keys.

Physical and Operational Risks

CIT, transportation and storage providers are exposed to a host of environmental threats at all times. They must deeply understand potential dangers on routes and at access points; time limits on exposure during transfers; personnel requirements to implement security controls; avenues of vulnerability to social engineering and other schemes to get access.

Physical Damage to a Device

Crypto or private keys in cold storage have to reside on a physical element that may be fragile or easily damaged. Items have to be treated as if dropping, stacking, bending and handling could destroy the value of the content.

Packaging

The containers or transmitting devices cannot be labeled that in any way indicates what the contents are. The provider may only know that the contents are highly valuable, and should also know that the asset is digital. If digital files are part of the contents, packaging should be designed to shield the files from potentially damaging electromagnetic currents.

Sustainable Devices

Hardware and paper media for storing crypto files and private keys must be able to preserve contents for a long time. Paper shards containing portions of a private key that has to be reassembled to be used have to retain their precise visual and form integrity.

Security

Security may begin with planning and surveillance, but it has to be backed up by lethal force, just as in any other high value CIT operation.

Pickups and Handoffs

CIT providers inevitably have to interface with clients at both ends of a route/storage episode. The clients will be located in a variety of types of locations, and they may or may not have carefully designed security routines. The people on the client side will have a variety of security skills and experience that could lead to mishandled transfers.

The Risk of Violence

Much like ATM servicing, the transport and transfer of crypto and private keys has an inherent risk of violence. People who want to steal the assets will be prone to escalate quickly, trying to take charge of the situation.

Unknown Monetary Value

No knowledge of what is being stored by value. The cost of the storage device or value of contents. CIT carriers have no means to validate the storage device value and could be accused of indeterminable loss.

COLD STORAGE RISK ASSESSMENT

Security planning requires assessing the risks involved, evaluating them, and devising tactics to mitigate them. For crypto assets in cold storage, a cardinal risk mitigation principle that storage and transportation providers must follow is that **physical separation of the crypto files and associated private keys must be maintained.**

Many of the questions to ask in the risk assessment will be similar to those asked in traditional CIT/vault services.

Are there adequate procedures and processes to control access to the safe?

Access points into the storage area should be under dual control and recorded by CCTV. No one—not even the owner—should have single control access into the primary storage area. These controls should stipulate who is authorized to open the safe, and audit logs should document every instance of opening it. Dual control and segregation of duties should be designed to defeat internal collaboration.

Does the storage provider have a proper safe or vault?

This would be a UL burglary-rated safe designed for high liability contents. The safe/vault opening should be set up so that physical dual control is required such as using two separate spin dials for access. Combinations should be changed for every dual control access operation. The installation of the safe should be such that it is impossible to remove it from the premises.

Are potential digital threats removed?

No digital device should be allowed into the primary storage area. Shielding the primary storage area is recommended.

Are there adequate CCTV recordings and views?

Secured CCTV recorders feeding data into secure servers should be placed for surveillance of secure areas and safes/vaults, but not so as to record encryption keys or other identifying information. Recordings should be stored at least 45 days.

Are all procedures documented, acknowledged and understood by affected employees, and audited?

Every moment in the chain of custody, especially in transit, should occur within a defined procedure, documented, with recordings retained for audit or process review. Individuals responsible for roles in the chain of custody should be identified by traditional and biometric tests, fully trained and tested in their roles, and recorded as agents in any tasks they do during transit or storage.

EXAMPLE: “COLD STORAGE” PHYSICAL SITE ASSESSMENT

Cold storage in this example refers to a physical site that can be secured as distinct from one of the many portable devices that exist for “storing” crypto. A portable wallet might be one of the items stored in such a facility.

Most of the elements of a secure physical site will be familiar to CIT and vault service providers who take custody of high value, high liability commodities.

Cold storage facilities should be located where surveillance of the entire exterior is easy and approach to the facility can be controlled. Designers may consider local building standards to ensure the facility blends in. Crime Prevention Through Environmental Design (CPTED) principles could be used to incorporate “eyes on the street” as an informal layer of security—thus, the locations may feature significant street traffic.

That said, the setting of the facility should incorporate a significant amount of unbuilt external space to prevent incursions from adjacent buildings. Upper or lower stories should be avoided, or directly controlled and secured by the cold storage facility.

A highly secure cold storage facility must be able to operate for 24 hours using internal power and water only.

Building Exterior

- ✓ The facility should be adequately hardened according to industry best practice standards for high liability storage. This will include portal designs for visibility during approach.

- ✓ The facility should be nondescript, with no exterior features that may suggest its function. It will have no signage or markings that would attract attention.

- ✓ The outer door will have limited external connectivity, and leads to a chamber that has controlled access to an inner layer that has no direct external connectivity.

Interior Features and Controls

- ✓ The exterior portal enters directly into a chamber with reception behind secure bullet-resistant glass, and a reinforced, locked door for the only access into the next layer. For entry, visitors must present physical and biometric identity to be given a visitor badge which will be collected on exit. Owners, CIT and vault service providers must exist within a list of authorized visitors, and should be required to register in advance.

- ✓ Security components should incorporate balanced protection countermeasures that create multiple points of resistance and are able to detect an intrusion at multiple points.

- ✓ Each facility may serve numerous clients such that activity among accounts might overlap. If clients are allowed to access the facility, certain features will be important both for security and to protect the identity of the clients.

Interior Features and Controls (cont.)

✓ The facility should have several elements to prevent access to any multi-tenant space. Examples Include:

- All doors are required to be closed systematically before the inner door that has access to the client work areas and breakrooms.
- Facility is managed with both unique personal code as well as a biometric scan for sensitive areas.
- Access Control Systems should always be tied into the HR Systems, especially in an event of a termination of an employee.
- Audit frequently to ensure dual controls are maintained that no one person has too much access to high liability storage areas.

✓ Highly sensitive operations require a secured and private environment. The high liability storage area is the innermost layer of the facility, and is designed to require dual control access. It will include sufficient utility service to function internally without interruption despite an external failure, even in the rest of the facility.

- Dual controls limit personnel movement and prevent unauthorized access to high liability storage areas from less secure internal layers of the facility.
- Service providers are not permitted inside high liability storage areas without representation from the client. Access is managed with multi access requirements that authenticate each visitor/provider uniquely.
- Space is designed so that multiple clients might access secure storage without physical or visual contact with each other.

CONCLUSION

The secure cold storage and transportation of cryptocurrency is required to enable crypto to migrate into the broader world of finance, off the blockchain and out of the dark corners of the web. Custody solutions are now being provided and developed by traditional financial institutions, so larger investments in crypto may be emerging. Regulators and like-thinking private businesses and insurers are developing versions of KYC and AML standards for crypto.

CIT and vault providers will recognize many of the risk mitigation tools used for crypto, since they resemble security measures implemented for other small, high liability shipments. Dual controls, hardened buildings and vaults, and carefully managed chains of custody are standard practices.

However, the digital nature of the assets and their required high-level encryption for access create some new risks. Whenever a crypto asset is in an Internet-connected location (like a 'hot' wallet or exchange), it is vulnerable to theft by hacking. It may be impossible to recover virtual coin lost to a successful hack if the coins are placed under a different private key (with 128-bit encryption), and they certainly would be.

Crypto also poses a new risk because both the digital asset and its associated private keys are absolutely required to access the value. If a private key is lost, so is the money/value. This means that for every asset, there are two items that must be protected, and they must be protected separately. In fact, if the private key is stored on multiple shards of paper, there can be many storage locations to access to accomplish one transaction.

All of these threads of a crypto storage and transportation custody episode have to be documented in a secure fashion and recovered on demand.

Should CIT and storage providers develop the complicated new procedures and policies needed to participate in this new market?

That's for each to decide, but the underlying reality is that cryptocurrencies have tremendous upside, and the innate features of blockchain-based currencies are appealing. With $134 billion of crypto now in existence, and new cryptocurrencies being invented often, it's a market with a lot of upside.

Discuss your crypto risks with an internationally-recognized partner.

Visit lowersrisk.com or call 540.338.7151

DCJS # 11-17841

LOWERS
& ASSOCIATES