GLOBAL
DIGITAL
FINANCE

Crypto Asset Safekeeping and Custody

Key Considerations and Takeaways [Draft dated 2/2/2019]

Introduction

Currently, there are no globally consistent or detailed regulatory guidelines around safeguarding or custody of Crypto Assets (CAs) that do not fall in the definition of securities, currencies or commodities.[1] Global Digital Finance (GDF) is keen to ensure that those who decide to seek out a safekeeping or custody solution for their CAs have an understanding of the solutions currently existent and seek out those that best suit their needs and that minimize their risk of loss, and - in case of loss - the risk of non-recovery of such CAs. Accordingly we provide herein an overview of different custody solutions and different customer considerations and take-aways.

This document references a number of technical concepts and terms. Please refer to the glossary at the end for a detailed description. Also, given that there are no specific regulations for the safeguarding or custody of CAs that do not fall in standing regulatory definitions of financial instruments, securities, currencies or commodities, we use the words safekeeping and custody interchangeably. Custody should therefore not be read as "regulated custody" but rather as "safekeeping assets on behalf of others".

Definition of CA Custody

In the context of CAs, we define custody as "the safekeeping of the CA's on behalf of others, including safe-keeping of the Private Key". A private key is a sophisticated form of cryptography that represents ownership of a user's CAs and enables the owner to transact with them. A private key is an integral aspect of CAs, including bitcoin and altcoins, and its security make up helps to protect a user from theft and unauthorized access to funds.

Because ownership of CAs is determined by who holds the private keys to these assets, they are far more important than a password could ever be. Storing these keys on the public cloud can be calamitous in case of a hack, while holding them on a phone can be devastating if the device is lost, stolen or damaged. Crypto enthusiasts have heeded advice from experts by getting clever and recording them offline – using an offline wallet/ hard wallet – only to forget where they put it, throw it away without realizing its significance or having no access in the case of death.

Evolution of Financial Asset Safekeeping and Custody

Custody of CAs can be seen as the next stage in the evolution of safekeeping of financial assets. Before the movement towards dematerialization of shares, most share certificates were held in purely physical form and self-custody was common. Towards the latter half of the 20th century, more and more national regimes moved towards the dematerialization of shares and over the same period due to increased globalization of trade, financial markets grew rapidly and internationally, leading to the birth of the custodian bank as we know it today. More recently, CAs offer a new paradigm that offers both similarities and differences. We elaborate on each of these points below.

[1] CAs that are financial instruments, securities, currencies or commodities as defined in national rules are captured by standing regulation in such jurisdiction(s).

In the context of accelerating growth and globalization of financial markets,[2] the role of a custodian bank evolved to include:[3]

- holding in safekeeping assets such as stocks, bonds, currencies and commodities, domestic and foreign
- arranging settlement of any purchases and sales and deliveries in/out of such assets, and interacting with counterparties on any trade and/or settlement failures
- collecting information on and income from such assets (dividends in the case of stocks and coupons in the case of bonds) and administering related tax withholding documents and foreign tax reclamation
- administering voluntary and involuntary corporate actions on securities held such as stock dividends, stock splits, business combinations (mergers), tender offers, bond calls, etc.
- providing information on the securities and their issuers such as annual general meetings and related proxies
- maintaining currency/cash bank accounts, effect deposits and withdrawals and managing other cash transactions
- performing foreign exchange transactions
- providing other services including fund accounting, administration, legal, compliance and tax support services.

In the case of CAs, the role of the custodian and the technologies used are still in the process of being defined.[4] This role is similar in that the key role of the custodian is safekeeping, asset protection and asset servicing. However, due to the nature of CAs, the details differ. For example:

- Asset protection typically includes ensuring settlement finality, roughly defined as "I own what I have exchanged value for". In the case of CAs, this could include monitoring of developments, characteristics and risks specific to CAs such as: blockchain improvement requests, changes in consensus methods that can change settlement finality status to the investor, soft or hard forks with implications on existing crypto assets held, % of mining power that would upgrade which can either strengthen or weaken the blockchain's security to a 51% attack, risk of eclipse attack that can allow a roll-back of settlement finality, involvement in proof of stake/ delegated stake, and other consensus mechanisms.

[2] The first custodian bank goes back to the 1920's with State Street Bank & Trust acting as the custodian of the first US mutual fund in 1924. In the 70's, the introduction of floating exchange rates and - towards the end of the decade - lifting of exchange controls in many major economies resulted in rapid development of the market for international debt instruments. In the 1980s, professional traders became prominent players and the practice of arbitrage increased. Also in the 1980s, a rise in specialist fund managers running dedicated portfolios of foreign equities increased the need for global custodians. Through the last two decades, the opening up of markets in Eastern Europe and a gradual increase in investment in equities and in cross-border investments have increased the need for specialist local custodians integrated into global custodian networks.

[3] https://en.wikipedia.org/wiki/Custodian_bank

[4] The recent Ethereum Constantinople development can be an opportunity to baseline the roles of a crypto-custodian vis-a-vis its (institutional) investors' expectations.

- Asset servicing could include reviewing of ERC-20 or other tokens' smart contracts and reconciling inflation yield (e.g. to ensure circulation is equal to the inflation stated in the white papers) or to review the ERC-20 codes for back-doors or conditions that can be relevant to the investors.

A further difference is that CAs allow for certain process simplifications. For example, unlike traditional securities, CAs can be instantly transferred and settled on the blockchain which keeps a permanent record of such transfer. Also, corporate actions can be programmed into the smart contract, thereby eliminating the need for manual servicing.[5]

Furthermore, the identity of the custodian of CAs is still evolving. While in the case of traditional financial markets, most safekeeping is done by independent 3rd party custodians, in the case of CAs due to the still nascent nature of the asset class often trading platforms or funds act as safekeepers of the CAs. In addition, due to the availability of a wide choice of low-priced hard and soft wallets, self-custody is an option and, accordingly, more common in the case of CAs than in the context of traditional financial instruments. Custodial wallets are also an option.

Finally, given the still very nascent nature of CAs, there is a greater role for advocacy, including the custodian's participation in the CA ecosystem to advocate on matters relevant to safekeeping, asset protection and asset servicing integrity.

Scope of this Document

As noted above, custody in the context of CAs is presently primarily done in the following ways:

1. Custody by independent 3rd party custodians - similar to traditional 3rd party custody
2. Custody by crypto trading platforms and funds – a form of 3rd party custody
3. Custodial wallets – a form of 3rd party custody
4. Non-custodial wallets (online or offline) – self-custody.

This document only focuses on cases where the customer entrusts a 3rd party with custody of CAs and therefore expects the 3rd party to safekeep the private keys, in other words by way of options 1-3 above.

Self-custody is outside the scope of this document as in the case of self-custody the owner of the CAs entrusts the safe-keeping of the CAs onto him/ herself rather than to a 3rd party and accordingly remains him/ herself responsible for the safekeeping of the CAs.

We believe the choice of a 3rd party custody solution for CAs depends on key considerations concerning legal and regulatory status, security and operational risk. We elaborate on each of these in more detail below. The Annex shows a non-comprehensive sample list of current CA custody providers.

1 – Legal & Regulatory Status

The main risk that customers of 3rd party custodians of CAs face is the risk of loss by the 3rd party custodian of the private keys. This risk has materialized on various occasions in recent times. Accordingly, it is imperative for the customer to understand what his or her rights are in case of loss of private keys by the custodian. To this effect, it is critical for the customer to read the terms and conditions of the custody contract/ arrangement before signing them or before agreeing to them by depositing his/ her CAs with the custodian.

[5] http://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

Legal categorisation and licensing

The definition of "financial instrument" or "securities" varies by jurisdiction, including within the EU. Also, the licensing regime applicable to financial asset safekeeping, if any, differs by jurisdiction. The implication of this variance is that the liability of the 3rd party custodian towards its customers in case of loss of CAs varies very significantly depending on the actual or contractual legal status of the CAs and depending on the licensing status of the 3rd party custodian.

For example, some 3rd party custodians categorise CAs as "financial instruments" in the contract entered into with the customer, thereby possibly importing regulated custody liability and customer protections. However, others are electing to categorise CAs as "other assets" or "intangible assets", thereby significantly reducing their liability towards such customers in case of loss.

Also, most 3rd party custodians are presently not licensed for holding such CAs as most legal regimes have not yet introduced specific licensing regimes for custody of CAs, meaning 3rd party custodians are not required to hold such assets on a licensed basis or subject to regulatory oversight.

Accordingly, it is important for customers to understand both the legal categorisation of CAs in the contact and the licensing status of the 3rd party custodian.

Choice of law

It is critical to understand the governing law of the custody contract. Often the governing law is that of the custodian rather than of the customer, thereby complicating obtaining compensation or recovery in case of loss of CAs.

Choice of law is not something that can be changed easily, as custodians are unlikely to be willing to adjust this provision for specific customers.

In particular, the more remote the law is to the customer, the harder (and likely more expensive) it will be to successfully seek resolution or compensation, or to enforce a judgement against a custodian.

Conflict resolution

It is also critical to read the provisions that detail how conflict resolution will work in case of loss of the private keys by the custodian or other issue.

For example, is there a choice of the court system of a particular jurisdiction or is international arbitration chosen instead or is a combination of both? How familiar is the customer with the conflict resolution method that is chosen? Will proceedings be in the customer's native language?

As above, if the conflict resolution process is to take place in a foreign jurisdiction and/or in a foreign language, it will be more difficult for the customer to obtain a successful outcome.

Key customer takeaways / potential questions

1. Choose custodians in jurisdictions with a strong rule of law and a mature legal framework, including a reliable court system.

2. Customer terms and conditions should make clear the respective rights, obligations, responsibilities and risk allocation of the parties, plus appropriate dispute resolution mechanisms.

1. Ask/ research online which regulatory licenses, if any, the custodian holds. If the custodian holds licenses, ask/ research online whether the licenses cover the custody operations and that the custodian has not breached the terms of its licences. Note that given that regulations are still catching up with business evolution in the CA space, there are many jurisdictions where there are no licenses as yet that the custodian can apply for.

3. Ask for/ read the contract/ terms and conditions and look for the legal categorisation assigned to the CAs in the contract.

4. Ask for/ read the terms and conditions very carefully and understand each of the foregoing, including the choice of governing law and the conflict resolution mechanism.

2 – Security considerations

Based on a review of loss of CAs, it is evident that the most significant risk that custodians of CAs face is the loss of private keys as a result of hacks. Other significant risks can come from phishing (most common) and the blockchain itself, weaknesses in smart contract-based tokens (most difficult to identify). Accordingly, IT security is essential to the successful safeguarding of CAs.

Trading Platforms

At the present stage of development of the CA industry, crypto trading platforms/ exchanges often act as custodians of the private keys. Due to the sizable balances of CAs they hold, they are very attractive targets for hackers. Based on a study of past hacks of trading platforms, hackers typically take one of the following main approaches:[6]

- The first is to gain access to accounts and closed-functionality through the hacking of the founders' accounts and then to use malicious programs from the arsenal of other known hacking attacks.

- The second is an attack on the infrastructure of the trading platform/ exchange itself, through the hacking of a web application linking the customer to his money on the trading platform/exchange servers or an attack on so-called “hot wallets”.

These approaches are similar to those used in the traditional banking sector and accordingly can be reduced by robust IT security controls, many of which well-established in the traditional financial sector and some more specific to the characteristics of CA exchanges and CAs:

- **Web Security -** There are many possible malicious programs requiring solid Web Security.[7]

[6] https://cointelegraph.com/news/crypto-exchange-hacks-in-review-proactive-steps-and-expert-advice

[7] ICORating concducted a check of web security analyzing whether the exchanges were protected from the following errors and attacks, and whether they met certain security standards:
● HSTS header presence. The HTTP Strict-Transport-Security response header (often abbreviated as HSTS) lets a website tell browsers that it should only be accessed using HTTPS, instead of using HTTP.
● Clickjacking attack protection A malicious technique of tricking a web user into clicking on something different from what the user perceives they are clicking on.
● Drive-by Download attack protection Unintended download of computer software from the Internet.

- **User security and 2FA -** Methods to verify user logins to the trading platform/ exchange include use of more secure log in methods that do not have a history of repeated compromise, strong passwords, two or three factor authentication (2FA or 3FA), IP address verification and email confirmation.[8]

- **Domain and Registrar Security -** The Registry lock is a special flag in the registry that prevents anyone from making changes to your domain without out-of-band communication with the registry. Security-conscious organizations avoid leaking this kind of private information by using role accounts to register their domain names. Role accounts protect individuals in your organization from being targeted by attackers. A 6-month expiration window is recommended for high profile domains.[9]

- **Denial-of-Service (DoS) attack protection -** DDOS is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.[10]

- **Wallet aware hardware infrastructure -** Hardware (HSM) should be wallet aware e.g. the ability to verify wallet-to-wallet transactions between two wallets have the correct addresses related to the wallet owners to eliminate the risk of internal or 3rd party tampering or substitution with wallet addresses.

- **Hardware (HSM) enforced security policies -** Traditional HSM's on the market have been designed for a different purpose than crypto use cases, and are therefore limited in what they can do. These limitations don't affect the use cases for which HSM's were built, like Point of Sale, traditional payments, and CA's, where secret management, and cryptographic operations are the primary requirement. For cryptocurrency custody, enforcement of policies are just as important. Security policies should be configurable at the wallet level to enable a range of wallet types (hot to warm to cold) based on the selected security policies. Traditional HSM's are

---

● Man-in-the-middle (MITM) attack protection Attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
● POODLE attack protection An exploit that takes advantage of the way some browsers deal with encryption.
● Heartbleed attack protection Leads to a leak of memory contents from the server to the client and from the client to the server.
● Robot vulnerability protection Vulnerability that allows RSA decryption and signing operations with the private key of a TLS server to be performed.
● TLSv1.3 presence
● HIPAA, PCI-DSS, NIST guidance compliance.
The test results were as follows:
● All exchanges were protected from POODLE, Heartbleed and MITM attacks.
● 1% exchanges were not protected from Robot vulnerability.
● On average, each exchange was protected from 6 attacks and errors, the worst was only protected from 4 attacks and the best from 9 out of 10 attacks.
● Only 37% exchanges have HSTS header.
● 60% exchanges protected from Clickjacking attack.

[8] ICO Rating conducted a check of user security. Only 22% exchanges met all 4 criteria checked. 1% exchanges satisfied less than 2. criteria.
https://icorating.com/report/exchange-security-report-v-20-update/

[9] ICO Rating conducted a check for errors related to the domain and registry. Only 3% exchanges met all 4 criteria. 22% exchanges satisfied less than 2 criteria.
https://icorating.com/report/exchange-security-report-v-20-update/

[10] ICO rating also conducted a check of Denial-of-Service (DoS) attack protection. The test results were as follows: 74% exchanges were protected from DoS attacks.
https://icorating.com/report/exchange-security-report-v-20-update/

not designed to enforce user/ custodian configured policies in secure hardware. Therefore, solutions based on traditional HSM's are vulnerable to side channel attacks which target the policy decisions made in software.[11]

- **Cold storage and multi-signature vaults -** Most successful hacks have targeted private keys kept online in "hot storage". Consequently, trading platforms/ exchanges have adopted "cold storage" standards, whereby the majority of the CAs are kept offline on "air-gapped" computers/ devices not connected to the internet. Cold storage typically involves the use of physical vaults equipped with alarms, locks, and other appropriate security devices and resistant to fire, flood, heat, earthquakes, tornadoes, or other disastrous conditions. Transfer from cold storage to hot storage typically involves multi-signature approaches (e.g. requiring 3 out of 5 signatures).

- **2FA, Monitoring and queuing withdrawals -** An attacker should not be able to disguise a theft as a series of withdrawals from customers. Applying 2FA can reduce this risk Queuing withdrawals/ processing withdrawals sequentially can prevent a case where hackers withdraw from multiple wallets at the same time. Also, operating a time delay on withdrawals with a review process combined with placing limits on withdrawal amounts offers protection. Further, controls should be in place for cases where a withdrawal request exceeds the amount available in the hot wallet. For large operations/ operations at scale, an automated risk model that performs these functions and that monitors all withdrawals is essential.

- **Account statements and client notices -** Sending digitally signed account statements to customers regularly, using a key that is not on the public server, can allow the customer to identify theft if the trading platform/ exchange has failed to identify it. Also, automated client notices in case of any transactions, changes in customer fiat or CA balances and changes that are made to the customers account information can reduce fraud risk.

- **Encryption and cloning of databases -** Lack of encryption of data has also allowed for successful hacks. Consequently data encryption is key. Furthermore, it is prudent to clone important data to a place where an attacker cannot irreversibly modify or delete it from the server.

- **Protection against phishing emails -** Successful hacks have also involved phishing emails sent to trading platform/ exchange employees and messages in Skype from seemingly friendly sources. Protections against such phishing activity including , spam controls, filters, staff awareness training and automated risk models that try to detect ATO can reduce the risk of staff acting on such phishing emails/ messages, thereby preventing malware from penetrating the servers.

- **Software integrations -** Crypto trading platforms/ exchanges should regularly assess the risk of IT systems or software integrations with external parties or affiliates, particularly as they relate to the risk of unauthorised access and theft of client assets in custody, and ensure that appropriate controls are implemented to mitigate the risk.

- **Internal and external security audits and bug bounties -** Crypto trading platforms/ exchanges can further strengthen their defences by performing regular internal audits and operational risk reviews (see below) to ensure all processes are

[11] For example time locks: A traditional HSM can be used validate the signature from a trusted time stamp authority, but the result is still interpreted in the host computer – "if the signature is valid, release the funds". This decision is made in tradition x86 hardware, and is vulnerable to targeted malware attacks which can modify the logic in memory, so that an undesired decision is made, and the policy is bypassed. These types of attacks have been used extensively over the last few years to steal billions of dollars from depository institution via compromised SWIFT terminals. In the traditional payments world, you might still have a chance to track down the thieves or at least recover the funds. With CAs, this is seldom possible.

working as anticipated. They can also engage trustworthy security auditors who have proven hack-proofing expertise and white hat skills. Bug bounties are also a possible protection method.

- **Security team -** Last but not least, in order to protect themselves from hacks, crypto trading platforms/ exchanges need development resources and a security team with adequate experience. An appropriate internal function should be assigned to the safekeeping of assets, such as a security officer. Solid background screening and other operational risk management procedures (see below) should be applied to any staff involved in CA safe-keeping.

We also refer to what is said in **Part II: GDF Principles for Token Trading Platforms** regarding safekeeping:[12]

> **7. Safekeeping**
>
> *a. We will safeguard our own and our customers assets (including holding a sufficiently high proportion of cryptoassets in cold storage, where appropriate) and minimise the risk of loss on and delay in access to these assets.*

Fund Managers

Crypto fund managers depending on the case may safekeep the CAs themselves or engage a 3rd party custodian. At the present stage of development of the industry, self-custody by the fund manager is more common than independent 3rd party custody. However, cold storage managed in-house by (especially smaller) funds tends to lack institutional grade controls as well, i.e.; multi-layer approvals, multi-signature, segregation of functions between transaction signers from those investing and trading the assets.

Accordingly, it is to be expected that as more 3rd party custody solutions become available (see Annex for a non-comprehensive sample list), larger/ established fund managers will choose to use these in line with the requirements under their normal course fund mandates. Furthermore, given that cold storage impedes on speed of execution it is likely that smaller funds may adopt 3rd party custody solutions as well once they become more broadly available.

We cross-reference what is said under "Custody and Care of Customer Assets" in the GDF Principles for Fund Managers:

> **"3. Service Providers, Custody & Care of Customer Assets**
>
> a. We will disclose in our fund documentation the names of our Key Service Providers, including the administrator, external auditor, bank, custodian and depository (where applicable).
>
> b. We will exercise due care, skill and diligence in selecting and appointing Service Providers, selecting those that are independent and at arms-length from us, and always prioritising the safety of customer assets by considering reputation, legal status, financial resources or organisational capabilities of the Service Provider.
>
> c. We will formally document our relationship with the Service Provider in an agreement that sets out amongst other terms the scope of the Service Provider's responsibility and liability and that we will periodically monitor compliance with.
>
> *d. To the extent we do not use an independent Service Provider for one or more of the aforementioned roles, we will transparently explain this in our fund*

[12] [currently under consultation; will be replaced with the final version once issued] https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Additional-Principles-For-Token-Trading_Web-151018.pdf .

documentation and will put in place robust risk management, contingency and business continuity procedures.

e. For example, where we self-custody cryptoassets, we will put in place robust risk management procedures, including cold storage, multi-signature processes and involvement of employees with functional independence from those performing investment or trading functions.

f. We will make best commercial efforts to insure ourselves adequately against the risk of losses or thefts of customer assets."

Key customer takeaways / potential questions -

1. Choose well-known trading platforms, fund managers or 3rd party custodians that disclose security, contingency, external / independent audit and insurance policies.

2. Ask/ research online whether the trading platform or fund manager engages in self-custody or whether it instead has engaged a 3rd party custodian.

    a. If the former, look for/ ask for the security policies which the trading platform or fund manager deploys.[13]

    b. If the latter, ask/research online more detail on the 3rd party custodian.

3. Ask/ research online if the trading platform, fund manager or 3rd party custodian has ever experienced loss of private keys.

    a. If so, ask/ research online more detail as to how the trading platform or fund dealt with the losses and make sure you are comfortable with the method before depositing your CAs.[14]

    b. If not, ask/research online what the contingency policy is in case of loss of CAs.

4. Ask/ research online if the trading platform, fund or 3rd party custodian has taken out independent insurance to cover the risk of loss of CAs and if so how extensive the coverage is (maximum amount of coverage; coverage for loss of private keys of some CAs or of all CAs).[15]

5. In the case of trading platforms/ exchanges, use the functionality provided to the maximum, including at a minimum 2FA. Log in regularly into your account to verify your positions and ask/ research online if you can be sent regular account statements.

[13] Please understand that an explanation of general principles of custody adopted by the platform or fund may be provided to you, you may not be given the full process in detail as doing so would expose the platform or fund to the risk of loss.

[14] A review of past practices shows that after powerful hacking attacks, crypto exchanges most often use three ways to compensate the affected users: 1. rollback to a previous state or freeze transactions; 2. syndicate the losses with other/ all users; or 3. return the funds of the exchange from its own profit or by issuing exchange tokens.
https://cointelegraph.com/news/crypto-exchange-hacks-in-review-proactive-steps-and-expert-advice

[15] Note in most markets insurance coverage is only available for selected, better known CAs such as Bitcoin.

6. Ask/ research online if push notices will be sent to you and in what form if trading, CA or fiat movements occur in your account so that you can yourself verify your positions and in a worst case identify loss of assets.

7. Consider to distribute funds between several wallets and trading platforms/ exchanges to further reduce your risk.

8. Ask/ research online what attack vectors does the custodian consider in their solution.

9. Ask/ research online how does the custodian protect itself against flaws in the underlying cryptography.

10. Ask/ research online how does the custodian ensure supply chain authenticity for hardware. Also is this the first time use of the hardware.

11. Ask/ research online whether an investors' CAs are commingled with others or wether investors' CAs are sent to a unique 1-time address (akin to a segregated account).

3 – Operational considerations

Aside from/ closely linked to IT security risks, a custodian should be able to demonstrate appropriate operational controls, including an operational risk management program (ORM).

ORM program and controls

An ORM program normally encompasses:

1. Developing strategies to identify, assess, monitor and control/ mitigate operational risk;

2. Defining policies and procedures concerning operational risk management and controls;

3. Defining an operational risk assessment methodology and record keeping of completed assessments;

4. Defining and administering comprehensive backup, disaster recovery and business continuity strategies and programs;

5. Defining and administering a risk-reporting system for operational risk, including internal escalation.

6. Understand how the custodian stores and backs-up the private key, to get comfort around the method deployed. If there are any doubts, they should be clarified

We refer in this regard to the following operational controls extracted from **Part I of the GDF Code of Conduct: Overarching Principles.** The existence of these key operational controls is often closely linked to the reputability of the trading platform, fund manager or 3rd party custodian:[16]

16 https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Overarching-Principles_Web-221018.pdf .

2. Legal and Organisational Requirements

a. We will put in place a transparent legal governance and ownership structure that reasonably protects our interests and the interests of our customers.

b. We will put in place and disclose a qualified management team that combines technology and financial expertise, including expertise on financial laws, rules and regulations, and that will endeavor to comply in all material respects with the Code as well as with applicable laws, rules and regulations.

c. We will put in place know-your-customer (KYC), customer due diligence (CDD), transaction monitoring and other AML/CTF processes commensurate with the nature, complexity and size of our business in order to deter, detect and report financial crime as defined in laws applicable to us, which may include laws on money laundering, terrorist financing, bribery and corruption, sanctions breaches, tax evasion and modern slavery.

d. We will put in place appropriate systems, processes, controls, risk assessments and independent reviews to run our businesses safely and responsibly.

e. We will ensure that our technology systems and business processes are sufficiently robust and secure, proportionate to the nature, scale and complexity of our businesses.

f. We will put in place cyber security protections, denial of service protections, security patches, firewalls, resiliency and penetration testing and, independent reviews proportionate to the cyber risks inherent to our businesses.

g. We will put in place appropriate technology change management processes, crisis management processes and business continuity plans.

h. Our terms and conditions will be clearly written and will explain what our duties and responsibilities are and what fees and charges will apply.

3. Ethics, Conflicts Management and Market Integrity

a. We will apply appropriate staff background screening and due diligence to hire competent and professional people and advisors that act with honesty and integrity.

b. We will have adequate systems and controls to detect, manage and disclose material conflicts of interest within our own business or resulting from our services, activities, cross-holdings or investments.

[...]

4. Treatment of Customers and Customer Assets

a. We will treat our customers fairly and take reasonable steps to ensure that the risks and opportunities of cryptoassets are presented in a clear and balanced fashion.

b. We will ensure that customers can access information regarding their money and assets, including where the money is kept and any relevant transactions.

c. We will take reasonable steps to ensure that monies and assets held by us on behalf of customers are subjected to asset custody and safekeeping approaches that are suitable and provide the requisite level of security for cryptoassets.

d. We will put in place processes for the orderly winding down of our businesses if we cease to operate and ensure that customers retain access to and ownership of their monies, data and assets.

e. We will put in place processes to enable customers who are unhappy about any aspect of our business or service to complain, and we will treat those complaints fairly and will properly record keep such complaints and the resolution thereof.

Segregation of duties

One of the most common causes of impairment of customer assets is the lack of segregation of duties and the lack of of proper oversight. Access to significant funds or assets should be tightly controlled, with no single person having access or control.

Forks, Airdrops, Swaps and Staking

Unique to CAs include forks, airdrops, token swaps[17] and staking. It is important to understand the policies, actions, services and distributions by the custodian if any of the foregoing occur.

We refer in this regard to what is said in **Part II: GDF Principles for Token Trading Platforms:**[18]

7. Safekeeping

[...]

b. We recognise that any rights attached to tokens that we hold on behalf of customers belong to the customers. Accordingly, we will not exercise voting rights on behalf of customers without their approval, and we will not withhold in our account distributions (such as airdrops or gas) that belong to customers.

Internal Controls Audits

It is important to understand whether the custodian undergoes internal controls audits.[19]

Key customer takeaways / potential questions -

The following is a list of questions the customer should be asking their potential custodian, in regards to operational risks.

1. Choose well-known trading platforms, fund managers or 3rd party custodians that disclose security, contingency, external/ independent audit and insurance policies.

[17] These can occur in two situations: a) crypto asset is being moved from one blockchain to another (for example EOS which moved from Ethereum to its own chain); b) the original token smart contract is being replaced by another smart contract with different functionality. The crypto asset holder may in some cases be required to actively participate in the token swap within a certain time frame, otherwise the right to claim the new tokens may be lost.

[18] https://www.gdf.io/wp-content/uploads/2018/10/0003_GDF_Additional-Principles-For-Token-Trading_Web-151018.pdf

[19] For example a "Service Organization Control" (SOC) audit. A SOC 1 Type I and a SOC 1 Type II both report on the controls and processes at a service organization that may impact their user entities' internal control over financial reporting. The main difference is that a SOC 1 Type I report is an attestation of controls at a service organization at a specific point in time, whereas a SOC 1 Type II report is an attestation of controls at a service organization over a minimum six-month period.

2. Ask/ research online which polices the custodian discloses in regards to the topics covered in **Part I of the GDF Code of Conduct: Overarching Principles.**

3. Ask/ research online if the custodian has signed up to the **GDF Code of Conduct.**

4. Ask/ research online if the account opening and closing as well as the fraud control procedures are clear and transparent.

5. Ask/ research online what the custodian's approach is in relation to segregation of duties.

6. Ask/ research online what the policy of the custodian is in regards to forks, airdrops, swaps and staking.

4 – Further considerations

- **Own Checks** - As noted above, an account holder is well-advised to regularly check his/ her positions in both CAs and in fiat held in the account. If the custodian is simply safeguarding the private key on behalf of the customer, then the customer can use the public key to receive CA of the same type and safely monitor the CA balance through a block explorer.

- **Financial Audits** - If the custodian is a centralised trading platform or fund manager, then it may not be possible for the customer to monitor their individual balance through a public key. Only an audit may prove the actual balance. As such it is important to check whether the custodian is subject to an annual external audit.

- **Controls Audits** - It is important to differentiate a financial statement audit from an internal controls audit. The lack of independent controls reports, specifically SOC 1 reports, presents a major hurdle for the serviced organisations in getting a clean audit opinion.[20]

- **Capital** – The financial position of the custodian will be determinative in case of material loss of uninsured customer assets. An account holder therefore best understand the capitalization of the custodian in addition to its licensing status and its insurance coverage discussed above.

- **Conflicts** – If the custodian has a series of related operations or businesses under the same corporate roof, it is important to understand area where conflict may exist as well as conflict management procedures such as segregation of certain businesses from others.

[20] See footnote 18 above.

Annex - Sample List of CA Custody providers

SERVICE PROVIDER	CUSTODY TYPE	LOCATION	FEATURES & SERVICES	WEB
Anchorage	3rd party custodian	USA	- Institutional custody - Business wallet - Self managed storage	https://anchorage.com/
BitGo	3rd party custodian	USA	- Institutional custody - Business wallet - Self managed storage - 100+ coins supported	https://www.bitgo.com/info/
Circle	Crypto trading platform	USA	- Institutional custody - Regulated in the US by FINCEN and 47 state regulators - Regulated as an Electronic Money Institution by the FCA - customer service coverage - 50+ coins supported	https://www.circle.com
Coinbase	3rd party custodian	USA	- Institutional custody - Regulated as clearing broker-dealer & Limited Trading Trust Partner (NYDFS) - customer service coverage - 15+ coins supported - Insurance	https://custody.coinbase.com/
Copper	3rd party custodian and Crypto Prime Broker	UK	- Institutional custody - Relationship manager - 80+ coins supported	https://copper.co/
Crypto Finance	Crypto Fund	Switzerland	- Institutional fund mngt & custody offering - Quality standards ISAE3000 - 10+ coins supported	https://www.cryptofinance.ch/en/
Digital Asset Custody	3rd party custodian	USA	- Institutional custody - Offer staking support - 90+ coins supported	https://digitalassetcustody.com/
Fidelity	Crypto trading platform	USA	- Institutional custody - Regulated across many financial perimeters - Launches Jan 2109 - Established reputation - Highly capitalised	https://www.fidelitydigitalassets.com/overview

Gemini	Crypto trading platform	USA	- Institutional custody - Regulated as a New York trust company (NYSDFS), therefore a qualified custodian - 7 coins supported - Policy on forks	https://gemini.com/custody-agreement/
itBit	Crypto trading platform	USA	- Institutional custody - Regulated as a New York trust company (NYSDFS), therefore a qualified custodian - FDIC insured / Capital reserves	https://www.itbit.com/
Kingdom Trust	3rd party custodian	USA	- Institutional & retail custody - Qualified regulated custodian - FDIC insured / Capital reserves - Allows for Bitcoin to included in your IRA	https://www.kingdomtrust.com/individual-custody-solutions/digital-currency
Koine Finance	3rd party custodian	UK	- Institutional custody - Settlement services - Regulated as an Electronic Money Institution by the FCA	https://koine.com/
Ledger	Self-custody cold wallets	FRANCE	- Self-custody - Not regulated - Working on institutional custody solution with Nomura	https://www.ledger.com/
Metaco - SILO	Self-custody: hot, warm, and "cold" wallets	Switzerland	- Institutional custody infrastructure - Full wallet management system with integrated tamper proof hardware enforced security - 10+ coins supported - Not regulated	https://silo.metaco.com/#/
Onchain Custodian	3rd party custodian	Singapore	- Institutional custody - Co-managed or full custody solution - Working with Onchain as a technology provider	https://oncustodian.com
Xapo	Custodial wallet	HK & USA	- Digital wallet application sits on your mobile device - Institutional & retail offering - 150+ currencies	https://xapo.com/
Others [GDF community to insert]				

Please note the above are listed in alphabetical order. This is a small sample of each of the 3 categories available at time of writing. There are many other options available in the market.

Glossary

Air Gap (Air Gapped) = A network security measure, where the device is not connected to the internet (public network), physically isolated from an unsecure public network, or even from radio frequency communication.

Blockchain = Blockchain is the underlying technology that Bitcoin and most other digital assets use to record and validate transactions. It is a linked list of transactions which updates to a virtual digital public ledger. A blockchain consists of a group of transactions in "blocks." These blocks are cryptographically connected to one another as they are mined, creating a long "chain." The nature of the cryptographic tie from one block to previous blocks means that previous blocks cannot be altered by anyone.

Bug bounties = An incentive offered to an entity to find security issues which if not addressed could result in a security breach. Typically used in open source environments.

Crypto Assets = A digitally native asset, that can be categorised as either a Payment Token (store of value, measure of account, medium of exchange), Financial Asset Token (represents access to a value or a right) & a Consumption Token (utility value received).

Cold Storage = The custody of digital assets where the private keys are stored on a device in a secure location that is not connected to a public network. See air gapped.

Corporate actions = This is an event initiated by a public company when making a change to their debt or equity, such as stock splits, dividends, rights issues, mergers and acquisitions

Custody = We define custody as *the safekeeping of the private key*. Given that no regulations yet apply to safeguarding or custody of CAs that do not fall in standing regulatory definitions of securities, currencies or commodities, safekeeping and custody interchangeably. Custody should therefore not be read as regulated custody but rather as safekeeping on behalf of others.

Multi Factor authentication = A security measure used when accessing an account, where the user is required to verify themselves using 2 or more methods. For example using an ATM, where the user inputs a bank card and also enters a pin code.

Forking = A fork occurs when the rules of a blockchain are changed, possibly creating two (or more) distinct digital assets. This may result from an upgrade to the features of the blockchain, a bug in the consensus algorithm, or changes to the node software. See Hard Fork and Soft Fork.

Hacking Attacks (*e.g. TrickBot trojan, Vawtrak, Qadars, Triba, and Marcher*) = A computer program that has been written with the objective to cause harm, damage , inconvenience or to collect a monetary gain. The target could be an individual, group of individuals, company or public sector organisation.

Hard Fork = A hard fork is the splitting of a digital asset's blockchain in a backward-incompatible way, resulting in two distinct digital assets. The code and data are replicated from the original digital asset to create the new one, adding backward-incompatible changes. Once the hard fork occurs, the two digital assets are non-fungible with each other but share some transaction and ledger history. Hard forks occur for two key reasons: The first is when competing visions of a digital asset's future development fail to reach agreement. The second is unforeseen bugs or intentional fixes to system-critical issues. When a hard fork occurs, developer and miner support are key components in determining whether the digital assets gain or lose value and relevancy. If poorly implemented, hard forks can also cause instability in the digital asset's network, because of transactions that may be valid on both networks.

Hardware Security Module (HSM) = They are physical computing devices (hardware) that safeguard and manage cryptographic keys. The hardware secures the processes leading the use of keys to authorise transactions. HSMs come with a certain level of regulatory assurance, such as the Federal Information Processing Standard certification and Common Criteria (an international standard).

Hot Storage (Hot Wallet) = The custody of digital assets where the private keys are immediately usable (on a local network for eg.). Availability is prioritized over security e.g. Transactions may only require a single signature and that signature may also be automated.

Warm Storage (Warm Wallet)= Pre-signed transactions with fixed destinations that are not yet broadcast, but more accessible than cold storage when a liquidity need arises.

Cold Storage (Cold Wallet) = The custody of digital assets where at least part of the required private keys are stored in a physical format that is completely disconnected from any public network (internet for eg.). See air gapped.

Individual Retirement Account (IRA) = A tax free investment plan offered in the USA to incentivise people to save for the future. The equivalent in the UK is the Individual Savings Account (ISA).

Multi Signature (multi-sig) = This refers to needing a minimum number of signatures out of the total available signatures on a wallet e.g. x of y signature framework. A common form of this is to use a 2 of 3 approach, which means of 3 total available signatories; at least 2 are required to approve a transaction before broadcasting.

Phishing emails = A fraudulent email sent by a nefarious actor with the goal of extracting sensitive/personal information (username / password), to use on most occasions for a financial benefit.

Private & Private "Key pairs" = The term key pair describes public and private keys used in public-key (or asymmetric) cryptography, where the key used to encrypt data is different from the key used to perform decryption. In Bitcoin, public keys are used as a transaction output in addresses, functioning similarly to an account number or payment instruction, while the private key is known only to the funds' owner and can be used to sign transactions moving those funds.

Side Channel Attacks = A side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself. Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Man In The Middle Attack (**MITM**) = It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Safekeeping = Given that no regulations yet apply to safeguarding or custody of CAs that do not fall in standing regulatory definitions of securities, currencies or commodities, safekeeping and custody interchangeably. Custody should therefore not be read as regulated custody but rather as safekeeping on behalf of others.

Smart Contract = Instead of 2 parties agreeing to terms and a third party deciding that the obligations of each party have been met, computer code identifies when predetermined actions/events have taken place and automatically self-executes the terms of the contract, that exist in a decentralized blockchain network.

Soft Fork = A soft fork can be viewed as a backward-compatible software update for a digital asset blockchain. Soft forks can refine the governance rules and functions of a digital asset blockchain but, unlike hard forks, are compatible with the previous blockchain. This means that a soft fork does not result in a split of the blockchain into two

digital assets. For a soft fork to be implemented, a specific level of readiness to enforce the new rules must be signaled by miners. Soft forks are optional for all users in the system, and it is not necessary for users to immediately upgrade, unless they want to use the new features. See also Hard Fork.