GDF Code of Conduct
Part IX(i) - Principles for Custody "Custodial Wallets"

This document should be read in conjunction with the Code of Conduct Overarching Principles[1]. Also, the code will often reference the "Crypto Asset Safekeeping and Custody Key Considerations and Take Aways GDF-Crypto-Asset-Safekeeping document[2]

Goal of the GDF Code of Conduct

Global Digital Finance ("GDF") is a not-for-profit industry body that promotes the adoption of best practices for crypto and digital assets and digital finance technologies through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.

GDF believes that scaling digital finance can allow access to markets by people who currently have little or no such access, thereby increasing their level of success and financial inclusion. At the same time, GDF recognizes that capturing these opportunities requires the nascent crypto asset industry to adhere to the requisite level of self-discipline and maturity. Incidents of fraud, embezzlement, deception, and other forms of violation of existing laws, rules and regulations or bad behaviours threaten the reputation and sustainability of the industry.

Accordingly, through the principles contained in this Code of Conduct (the Code), GDF introduces standards of good behaviour that attempt to address the above.

Structure of the code

The principles contained in the Code are designed to work across a broad range of crypto custody businesses and actors including intermediaries, trading platforms and funds. This Code is intended to be a living document and as such principles may be amended and new principles may be added as new business models emerge.

Limitation of the code

While global regulatory principles and practices inform the Code, it is not law and does not carry or contend to carry any such value. Instead, the Code constitutes a set of voluntary principles.

The Code recognizes that certain activities conducted in the custody of crypto assets may enter the remit of existing laws, rules and regulations. The Code seeks to complement such laws, rules and regulations only where gaps may exist or where legal or regulatory clarity has not yet been achieved.

Adherence to the code

GDF members agree that the principles laid out in the Code are important for both businesses and individuals. To enhance transparency and assist in the evaluation of the services provided by crypto asset businesses and actors, GDF members will endeavour to publicly attest their adherence to the principles based on reasonable and good faith efforts.

Regarding the approach for custodians to attest to this code and to verify their adherence to the Code, please refer to the GDF Registry on the website[3].

Market Overview

GDF observes that there are many different types of custody services that fall into the broad definition of crypto custody. Please refer to GDF's document "Custody - Key Considerations & Take Aways[4]", where we

[1] GDF Code of Conduct Overarching Principles
[2] GDF-Crypto-Asset-Safekeeping
[3] GDF Registry
[4] GDF Crypto Asset Safekeeping and Custody Key Considerations and Takeaways

provide a non-comprehensive list of current solutions available and summarise the services that each custodian offers, together with the technical solutions that underpin the offering.

Today, we see two distinct types of custodian - Custodial and Non-Custodial wallets. It is the scope of this code to focus on custodial wallets. We also acknowledge that definitions, even within the industry itself, are still evolving. To that end, we attempt to define each relevant category for consistency within this code.

CUSTODIAL WALLETS or (Hosted Wallet)

Custodial Wallet services offer varying levels of control

Some wallet providers have partial control over the asset, with the ability to execute, transfer, sign transactions, block or recover assets and private keys on behalf of a client with their instruction. However, they would not have full control to initiate a transaction on behalf of a client if the custodian does not have the clients private key exists in their possession to enable the release of the transaction.

We appreciate that in certain circumstances, the Custodial Wallet Provider could exercise full control. However, the basis of this document defines control as partial only.

Custodians may provide services in addition to safekeeping or the holding of assets on behalf of others, which include but are not limited to reconciliation, settlement, corporate actions, maintaining bank accounts & fund management. However, due to the nascent industry, there are very few offerings in the market providing a full suite of services (see BitGo clearing and settlement services[5]).

Other current definitions of Custodial Wallets include "hosted wallets" and "custody services". We refer to the ESMA definitions published in January 2019[6] and also to the FINRA guidance published in July 2019[7]

NON-CUSTODIAL WALLETS or (Non-Hosted or Hardware Wallet)

Non-Custodial custody occurs where there is no third-party providing a service. Beneficial owners (clients) access these services directly to secure/ safeguard their own crypto assets, giving them full control over their crypto assets. The assets can be stored in hardware or software wallets.

The Custodian (Agent) creates custodial accounts and/or cryptographic business redemption conditions around the safekeeping and release of digital assets from a custodial account.

Beneficial owners (clients) check digital assets into custodial accounts and declare which fiduciaries must initiate redemption requests. Fiduciaries approve redemption requests initiated by a beneficial owner. Beneficiaries receive digital assets redeemed out of a custodial account.

We note that in some instances some wallet providers have expressed that while they do not store the private keys on behalf of their clients (which makes them close to non-custodial wallets), they retain the ability to block or freeze a transaction in the event of a suspicious transaction or the application of a court order. However, these wallet providers may be limited to prevent the client from recovering the key using another device and executing a transaction on another device/platform.

1. Compliance with Existing Laws

a. We acknowledge that financial laws, including but not limited to laws concerning money transmission, deposit-taking, e-money, payment, AML/CTF or even securities laws (together, "financial laws"), may or may not apply to custody based on a variety of factors. For example,

[5] https://www.bitgo.com/services/clearing-and-settlement

[6] ESMA Press Release: Crypto Assets Need Common EU-wide Approach to Ensure Investor Protection

[7] FINRA Joint Statement on Broker-Dealer Custody of Digital Asset Securities

i. The types of services offered by a custodian, which may include but are not limited to holding crypto assets, account reconciliation, settlement, corporate actions, maintaining bank accounts & fund management,

ii. The jurisdiction in which the custodian operates from.

b. We also understand that even if we as custodians fall outside the remit of financial laws, we remain subject to all other existing laws, as noted in the Overarching Principles[8], including;

i. Contract laws;

ii. Consumer protection laws, including safekeeping of customer assets; and

iii. Criminal laws, including the prohibition against fraud.

c. For that reason, we commit to seeking legal advice to confirm either that:

i. Our custody service falls within the remit of financial laws, in which case we will act in accordance with such laws; or

ii. Our custody service(s) does not fall within the remit of financial laws, in which case we will seek to abide by other laws applicable to our activities.

2. Legal Considerations

a. We will put in place governance arrangements that are clear and transparent, promote the safety and efficiency of the platform, conform to applicable market conduct standards and expectations.

b. We will disclose the name, address and company registration number of our legal entity, as well as appropriate selective disclosure as to our officers, directors and senior management, such as experience and achievements to date.

c. We will disclose our licensing status, if any, as well as the regulations that such licensing status subjects us to.

d. We will share with our customers our insurance status if any, and the extent of the coverage.

e. We will clearly state whether the assets we custody are considered securities in the jurisdictions we operate, thereby highlighting liability towards customers in case of a loss with respect to relevant securities regulations.

f. We will disclose the respective rights, obligations, responsibilities and risk allocation of the parties, and the conflicts and dispute resolution mechanisms.

g. Regarding privacy coins, we will deal with the "shielded" aspect with due care and attention.

3. Operational Considerations

a. We will implement the necessary operational and technological checks and balances to reduce risks associated with control and access to customer's holdings to ensure that a single person cannot execute and sign a transaction on behalf of a client.

8 GDF Code of Conduct Overarching Principles

i. The checks and balances should be part of an auditable workflow explained and understood by the client.

b. We will disclose to clients to what degree their assets are protected under insurance in the event of a loss.

c. We will ensure consistent periodic reporting to our clients in regard to account statements, corporate actions and specific crypto asset activity (forks, air-drops, etc.).
   i. When relevant and in-line with transparent policy, we will ensure that all air-drops are passed through to the client's account, unless technical innovation is required on behalf of the custodian.

d. We will ensure clients accounts are separated where appropriate.

   i. If commingling of assets occurs within omnibus accounts, we will communicate this to the client.
   ii. We will not rehypothecate clients crypto assets we hold on their behalf unless explicitly agreed with the client.

e. We will be clear and transparent on the funds at risk associated with Staking and Voting.

   i. Staking may result in potential income for the client.
   ii. We will ensure all client votes are passed through to the blockchain unless technical innovation is required.

f. We will make clear to our clients in regard to the crypto assets we custody, any relevant network structure considerations (such as the governance structure of the foundation)
   i. Also, we will make public, in the event of a 51% attack, how this would be dealt with and communicated to token holders.

g. We will design our systems to enable a high degree of security and operational reliability, with adequate and scalable capacity.

h. We will put in place third-party technological audits, including with respect to risk, compliance and cybersecurity.

i. We will take necessary actions, including technical solutions and surveillance, to prevent, detect or deter money-laundering, terrorist financing or sanctions risk, in accordance with the GDF Code of Conduct for KYC / AML[9]

j. To reduce fraud risk, we will put in place verification measures (such as multi-factor authentication), confirmation processes and notifications upon withdrawal of assets from the custody platform, as well as procedures to approve and authenticate transactions above certain limits.

k. We will conduct periodic risk mapping to identify the possible sources of risk, both internal and external and mitigate the impact of such risks through the use of appropriate systems, policies, procedures and controls.

l. We will put in place recovery measures so customer holdings may be preserved in the event of technical failings or force majeure event.
   i. Through business continuity management, we will aim for the timely recovery of operations and fulfilment of the custody platform's obligations, including in the event of a wide-scale or major disruption.

m. We will put in place defined roles and responsibilities and conduct background screening on all new hires, paying close attention to serious misdemeanours and financial distress.

[9] https://www.gdf.io/gdfcode/

n. We will ensure that periodic IT security training is provided to ensure all staff are aware of the common techniques used in malicious acts such as phishing.

o. We will put in place controls for any service outsourced or partnerships entered into, through thorough due diligence, including but limited to:
    i. external audits;
    ii. ethical hacker support for developing partners platforms and/or continued risk assessment of integrated IT systems to ensure no risk of unauthorized access.

p. We will ensure a consistent level of service for every crypto asset that we support, noting that each crypto asset may have a different protocol.

4. Technical Considerations

a. When creating seeds[10] used to generate the keys for signing transactions, we will ensure that the latest secure techniques are employed, such as;
    i. generating multiple seeds and splicing them together randomly;
    ii. disabling the internet; and
    iii. seed encryption.
    iv. Also, we will ensure that no single person will possess the seed or back up phrase in its entirety.

b. When storing keys or seeds we will ensure best practice standards are applied, such as;
    i. strong encryption;
    ii. the sum of the keys required to transact is not stored in one physical location; and
    iii. backups are not stored in the same location as primary keys or seeds.

c. We will employ state of the art processes, to avoid any form of collusion, such as multi-signature for example when authorizing a client's transaction, thus ensuring we mitigate against any possible collusion risk.

d. We will employ mechanisms to delete or destroy unwanted data, in regards to seed, key and wallet generation.

-

[10] A useful guideline for best practice can be accessed on the National Institute of Standards and Technology (NIST)

Glossary

51% Attack - A brute force attack on a crypto network. Conducted by directing more computational power than half (%51) of what the network currently uses, with the intention of manipulating the consensus mechanism (typically for gains made through double spending). Imagine this as a democratic voting procedure - majority always wins consensus.

Address - an alphanumeric string of characters that represent a reservoir/destination where crypto can be sent to and from.

AirDrop - A method of distributing cryptocurrency in which market participants do not need to exchange their existing assets for a new one; but rather receive it based on some prerequisite factors (such as holding a parallel cryptocurrency)

Air Gap - to physically isolate computers from any exterior devices or information sources. Also known as a "closed-circuit" design, the purpose of air gaping is to maximize control over data flow.

Algorithm - Coded instructions or rules that are executed by a computer to solve problems.

AML - the acronym for Anti — Money — Laundering. A legal framework that is intended to subvert criminal financial activity.

API - Application Program Interface. A software that basically tells other software's how they should interact with each other.

Block - A immutable digital file which stores information regarding any and all activity on the network. Each block has its own timestamp, Merkle Tree hash, digital signatures, and transactions. This structure helps to maintain a chronological sequencing.

Blockchain - The software that allows for a decentralized fabric of trust exists. A chronological series of "blocks" that are linked together and act as the spine or backbone of the digital ecosystem.

Block Height - The numeric representation, showing what is the current number of the block being hashed.

Block Reward - The compensation that is paid out by the internal mechanism to keep nodes/ miners incentivized to operate.

Burning - A method by which tokens become unspendable (commonly by just being sent to an unspendable address) and thus serve as deflationary mechanism.

Censorship resistant - Something that is not susceptible to being filtered by any meddling middle-entities. [tolerant to institutional opposition]

CEX - Centralized EXchange. Just an abbreviation used to express centralized exchange without actually writing it out. But in and of itself, it is any Market exchange platform: NYSE, NADAX, the list goes on.

Confirmation - validation of a transaction / series of transactions. In the Bitcoin blockchain, each individual transaction must be validated by 6 independent nodes in order to be considered as a true act.

Consensus - a brief, recurring state of the network that constitutes a widespread agreement on a subject. The term used to describe how a network conjugates in order to maintain a distributed anonymous method of guaranteeing the integrity of itself.

Crypto Asset - A digital/virtual asset that is secured by advanced cryptography and by its nature not owned by any ONE entity

Cryptography - A technique using codes and ciphers to encrypt and decrypt sensitive information, messages or data. The art of privatizing and ousting unwanted actors from information.

DAO - Decentralized Autonomous Organization. A collective of entities that converge on some unified concept and operate as one organism.

DAPP - Decentralized APPlication; the main benefits of decentralized applications are immutability, accountability, anonymity, and enormous bandwidth (not to mention control over personal data).

Deflation - the economic side effect of value accrual; when something is deflationary it is limited in supply and highly demanded, directly cascading into a self-fulfilling prophecy of Price Hike.

DEX - a Decentralized EXchange; the terminology used to quickly address and exchange that is decentralized.

Difficulty - a measure of the computational resources required to solve the hash of the next block. This is the methodology which helps the network maintain a 10 minute block time (adjusted automatically every 2016 blocks).

Double Spending - the malicious act of spending the same currency twice by subverting the networks hashrate and mining off-ledger. The entity that has to bear the price of such activities tend to be cryptocurrency exchanges.

ERC-20 - The most popular Token protocol for use on the Ethereum Network. Deciphered into: Ethereum request for Comments — 20 as in the request digital fingerprint (the numbers simply represent a unique identifier from its concurrent protocol brethren. Also known as a "Utility token", its actual functionality on the ethereum network is "access/interactivity" to DAPPS.

FIAT Currency - what we know as the political denomination of money(s). Money that is backed by political positioning and global influential strength.

Fork - A network split. Usually happens when there is some necessary software code update that requires ditching the previous copy of the code (Hard & Soft)

Genesis Block - The very first block of the Bitcoin network. Block 1. The Baby block which began the infinite future of finance, Bitcoin.

Halving - The procedure of reducing the mining rewards on a blockchain. For the Bitcoin network, this occurs once every 4 years or approximately the time it takes to mine 210,000 blocks. Starting at 50, the Bitcoin reward Halved to 25 in 2012, then halved again to 12.5 in 2016. Coming up, a halving to 6.25! (live countdown timer)

Hard Fork - A complete change to a cryptocurrency's protocol. Usually a change in some very fundamental aspect of the code (such as the privacy protocol or consensus mechanism).

Hash - a fixed length string representing some mind of input data. In Bitcoin's case, a hash is created from following a very specific set of instructions and points to previous data.

Hash Rate - The unit of measurement of a network's processing power.

ICO - Initial Coin Offering. A crowdfunding mechanism that incorporates decentralization; by being able to host a "trustless" method of value transfer, entities can now go directly to the public and raise funds; as opposed to relying on some intermediary to mediate the process & touch the funding.

Key Storage and Form Definitions

> **Keys or Tokens Stored At Rest -** Private Keys or Tokens stored physically in a digital form in any medium. This list of mediums can include but is not limited to Hardware Security Modules (HSMs), databases, data warehouses, archives, printed sheets of paper, off-site backups, mobile devices, etc.
>
> **Keys or Tokens In Transit -** Private Keys or Tokens that have been digitized to become information that flows over a computer network and are subsequently in motion over the network. The type of network (public or private) does not matter.
>
> **Ephemeral Keys/Tokens -** Private Keys or Tokens that are not stored physically in any form or medium. Ephemeral Keys or Tokens are generated as a result of completing a separate cryptographic process, such as an authenticated key exchange protocol or when participants complete a group signature algorithm, such as a threshold ring signature algorithm.

KYC - Acronym for "Know Your Customer". A set of rules laid out by the government for companies to obtain a certain amount of information from their participants.

Mixing Services / Laundry - A method of enhancing privacy and anonymity. Done by pooling transactions together and shuffling them around with the help of certain ciphering algorithms.

Layer 2 - also called second layer; is a protocol that is built ON TOP OF another protocol in order to leverage back-end systems operation to the first layer and manipulate the parameters of the first layer. (If Bitcoin can only process 9 TPS and some financial company who wants to build on it needs to handle 350 TPS then they would use a Layer 2 solution {such as lighting network} and "funnel" transactions through their portal and send the hash reference of 350 transactions as though it were just 1 transaction.

Lightning Network - a payment protocol, that can be layered on top of any blockchain-based cryptocurrency.

Mining - the process in which nodes compete with each other to verify and publish transactions. For Bitcoin, mining would include compiling all previous block metrics with current ones and trying to solve a super complex computationally demanding puzzle.

Miner - the node/ node operator which chooses to participate in the incentivized process of extracting bitcoin, for example and securing its network.

Mining Pool - A group of miners that have unified their computing resources in order to distribute the mining rewards more consistently between its participants.

Minting - rewarding users with newly created coins for their participation in securing the network. More common with Proof-of-Stake cryptocurrencies.

Node - A computer/device that connects to a cryptocurrency network and helps strengthen the network's resilience.

Nonce - A (pseudo)random number, generated in order to satisfy the parameters required by the mining and hashing algorithms.

OffChain Transactions - transactions that are not made on the native crypto chains themselves in order to avoid bloating/ congestion.

Orphaned Block - a valid block that has been abandoned by the network due to a fork. Later on, it is adopted back onto the chain to which it originally belonged.

PreMining - A term used to describe a metric of a new blockchain related to the genesis formation. Bitcoin was not premised, rather it began its operations at 1; other chains such as BTCP was only available after 5% of the total supply was already extracted into the private hands of the organizers.

Private key - one of the two Keys involved with all public cryptographic interactions. The private key is the key which proves ownership of an address.

Public key - the key that is used in order to represent the counterpart of ownership of an address. This is the key that is shared with the public in order to receive funds at an address as well as backtrack the correlating addresses history.

Rehypothecate - It is the process by which a Custodian receives a CA and then pledges that CA to cover its own exposure to a separate 3rd party, which then pledges that same collateral to a different party, and so on and so forth.

Seed - The private key used in deterministic systems. The birth of randomness on a digital scale. A technique used to initialize a random number generator.

Smart Contract/Self Executing Contract - algorithms that facilitate and enforce obligations without any outside intervention. Stored on the blockchain itself, a smart contract is an unalterable agreement that has specific logic operations akin to a real-world contract. Once signed, it can never be altered.

SegWit - Segregated Witness. a soft fork improvement to the Bitcoin code which helps the network handle more transactions.

Side Chains - Blockchain ecosystems that are designed to function in a 2-way feed. Essentially children chains pegged to the "Motherchain" for on and off-ramping. (Think Ethereum Tokens which are then converted as collateral to obtain DAI stablecoins)

Signature (Digital Signature) - a mathematical process that is utilized in order to prove digital ownership. Designed to be collision resistant, the methods currently employed are as effective as a regular biological fingerprint.

STO - Security Token Offer.

STE - Security Token Exchange.

Soft Fork- A change network protocol that is backward compatible; so nodes are not by any means forced to upgrade and still benefit from its implementation.

Staking - Proof-of-Stake ("POS") assets incentivize participants to help secure the blockchain by "staking", or "delegating" their assets to someone running the blockchain software. If you delegate to a trusted node (also known as a validator), you can share in the rewards that the validator receives for mining blocks. Anyone holding the blockchain's token can participate in this process.

Utility Token - The class of Tokens that specifies the "need for the token" being to access/utilize {hence the name} some proprietary (or in crypto's case not so proprietary) technology.

Wallet - a storage facility for cryptocurrencies. A software that allows users to store their cryptocurrencies in a UI/UX friendly way. Abundant in formats; paper wallet, web wallet, desktop wallet, hardware, and mobile wallets.