(Draft)



Key management of decentralized custody

**

# 

# Introduction

This document explains

|  |
| --- |
| Text to be provided by Governance WG. |

# 

# Table of contents

[**Introduction**](#_1je30v6slvx) **2**

[**Table of contents**](#_449nw28pn5sf) **3**

[**1. Scope**](#_wck0xj18f0a1) **5**

[**2. Normative reference**](#_k0l7gypjirp) **5**

[**3. Terms and definitions**](#_hw5re93zqy4o) **5**

[**4. Abbreviations and symbols**](#_94rx0gilt6ii) **6**

[**5. Models of cryptoasset custody system**](#_rectvz5nqq1g) **6**

[5.1 Definition and types of decentralized custody](#_1ddzni1erlk9) 6

[5.1.1. Definition of decentralized custody](#_pn1zqdvq613w) 6

[5.1.2. Self-custody](#_ckv6597c53cr) 6

[5.1.3. Self-custody multi-signature](#_nubhvscdopj6) 6

[5.1.4. Smart contract custody](#_e0qwy48c6da) 6

[5.1.5. Decentralized network custodian](#_85sd0dgzfq46) 6

[5.2. Reference Architecture](#_c8p7izjkudb) 6

[5.2 Information assets and cryptographic keys](#_z4mk1bgoy1xt) 6

[5.2.1 List of Information assets](#_c6uylt3craj4) 6

[5.2.2 Key Lifecycle](#_uu6lmn3tnlnq) 6

[**6. Incident response**](#_mndgom9hzlu2) **7**

[6.1 Responsible entities and framework](#_jfj97ljvq2on) 7

[6.2 Process](#_mztgwx6b1907) 7

[6.3 Tracing the stolen cryptoassets](#_u0td2v4t0r7h) 7

[**7. Identity management**](#_7mid4teqa8yx) **7**

[7.1. AML requirements](#_47q2zrjhvwwf) 7

[7.2. Privacy enhancing mechanisms](#_kfnvc1f622my) 7

[**8. Security considerations**](#_i0aygael3uc4) **7**

[**9. Privacy considerations**](#_wtu5eykzl62t) **7**

[**10. Regulatory considerations**](#_9c54v8y2fg6j) **7**

[**11. Informative reference**](#_1mzntpvl6vsl) **7**

[**Appendix A – Acknowledgement**](#_yb83ibahglw7) **8**

[A.1 Editors and Co-editors](#_5m8h2u463cbi) 8

[A.2 Contributors](#_myj72dkh1kz6) 8

# 

# 1. Scope

“Decentralized key custody” is Aa service provided bydescribed is a decentralized provider or a protocol that operates functionally similarly to a centralized key custodian, yet is never in control of the keysfunds, and thus is not a custodian in the conventional sense of the word.

This is a rapidly evolving area, but the most common example would be so-called “social recovery”, where key shards or keys are distributed amongst user’s friends, family, and other trusted individuals.

* Model(s) of decentralized cryptoasset custodians system that provides cryptoassets custodians work to customers (consumers and other exchanges)
  + Types of decentralized custodians:
    - Self-Custody
    - Self-Custody Multisignature
    - Smart Contract Custody
    - Decentralized Network Custodian (e.g. Liquid Network)
* A list of information assets managed by the decentralized cryptoassets custodians system (including the signature key of the cryptoasset)
* The (social) impact which can be exerted by imperfect security measures of the cryptoassets custodians system
  + a list of well-defined risks that allows businesses to understand their posture, and auditors
* Key lifecycle and its management
* Incident response upon data breach
* Identity management
* AML/CFT
  + concern/requirements from regulators
  + inputs by engineers, including descriptions on infeasibility of regulations/requirements.
  + conflict between privacy regulations and AML, not every country is aligned in that sense, and these regulations vary widely around the world.
* Other regulatory requirements (e.g. Japanese regulation, European MiCA)

Implications to stakeholders

* Engineers
  + Requirements for key management
    - key generation
    - key lifecycle
    - physical security
  + Standard key protection mechanism
    - Protocol
    - Implementation (HW/SW)
  + Identity management mechanism
* Regulators
  + Points of audit
  + A guide for incident response
* Business entities
  + Agreed key management and operation process
  + Agreed identity management process
  + A guide for incident response
* Customers
  + Criteria to evaluate business entities

# 2. Normative reference

This document has no normative reference.

# 3. Terms and definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the term.

**3.1**

**term**

shortcut of the definition

# 4. Abbreviations and symbols

In this document, the following abbreviations and symbols are used.

BGIN Blockchain Governance Initiative Network

NOTE: All the abbreviations SHALL appear in this clause.

# 5. Models of cryptoasset custody system

## 5.1 Definition and types of decentralized custody

### 5.1.1. Definition of decentralized custody

### 5.1.2. Self-custody

### 5.1.3. Self-custody multi-signature

### 5.1.4. Smart contract custody

### 5.1.5. Decentralized network custodian

## 5.2. Reference Architecture

## 5.3. Information assets and cryptographic keys

### 5.3.1 List of Information assets

### 5.3.2 Key Lifecycle

# 6. Incident response

## 6.1 Responsible entities and framework

## 6.2 Process

## 6.3 Tracing the stolen cryptoassets

# 7. Identity management

## 7.1. AML requirements

## 7.2. Privacy enhancing mechanisms

# 8. Security considerations

This document has no security considerations.

# 9. Privacy considerations

Acknowledgement section contains PII of those people. Editors SHALL make sure to obtain the consent of the people to be included. Sometimes, a contributor MAY want to remain pseudonymous and just appear as an initial etc.

# 10. Regulatory considerations

# 11. Informative reference

This document has no informative reference.

# 

# Appendix A – Acknowledgement

(Informative)

## A.1 Editors and Co-editors

## A.2 Contributors