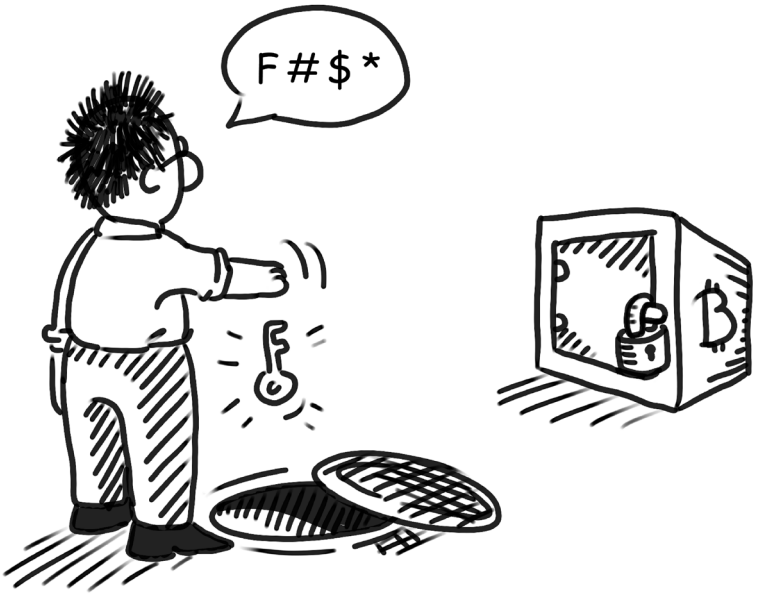
CUSTODY SOLUTION

New Year Edition

Table of contents

Introduction

In the world of digital assets and cryptocurrencies, a private key is the cornerstone that provides control and security of the assets that are assigned to it. Since the management of digital assets is completely controlled by cryptographic keys, the loss of the latter equals the loss of the asset itself (in the case of cryptocurrencies, there is no responsible party that can restore access to funds).



Note:

1. As of August 2020, 3.69 million BTC did not make movements.
2. After the death of Matthew Mellon – XRP for $ 500 million was lost.
3. After the "death" of the owner of QuadrigaCX, 26,500 BTC and 1 billion XRP and 430,000 ETH were lost.
4. According to some estimates, about 10,000 users lose their keys every year.

Crypto custodial services solve the problem of storing keys and restoring access. In fact, such services fully control cryptographic keys, and provide customers with a mechanism for communicating with the service itself. In order to initiate a transaction, the client requests the custodial service with the corresponding request. The request is processed by the service and the service itself signs the final transaction.

Although this approach involves the transfer of direct control over assets by the client to the service, it is quite effective for a number of reasons:

- High security of keys. The crypto custodian service / module directly specializes in ensuring the security of stored keys. Such services often use HSMs and a multi-signature mechanism to minimize the risks of hacking and crashes. Additional backup mechanisms eliminate risks in the event of a server denial of service, etc.
- A simple mechanism to restore user access. Losing passwords (or something else depending on which authentication mechanism is used) does not affect the loss of access to keys by the service.
- Possibility of regulation at all stages of operation and ease of connecting monitoring tools. Since each transaction must be signed by the custodian service on the basis of a request received from the accounting system, at any stage of the request confirmation (in case there are any suspicions), it can be stopped and processed manually by the responsible administrator.

At the same time, with the proper organization of interaction, the custodial service does not have access to the accounting system - architecturally it processes only requests received from the system.

After setting the stage by introducing different crypto assets and examples of common implementation approaches, this document sheds some light on the existing crypto custody market situation before presenting in detail our solution approach.

Current Crypto Custody Market State

There are several companies that propose crypto custody solutions.

GK8

GK8 is using a high secured cold wallet (without any external connections - only data receiving ability) for keeping the main part of funds. They are using the additional hot wallet for management of moderate amounts and support users and limits management, whitelisting and auditing options as well as integration with 3rd-party KYC/AML services.

Solaris

Solaris stores assets in a distributed manner by using threshold signature (multi-party computation) to avoid any single point of failure. An internal bookkeeping system performs off & on-chain transactions. The solution is integrated with Solarisbank's KYC for identity and monitoring end customers.

Metaco

They are offering a single infrastructure for hot and air-gapped wallets. It combines tamper-proof hardware with advanced key management options in a unified hot-to-cold storage solution and offers sophisticated access rules to all entities and functionalities of the platform (risks and workflows controlling for transaction execution and administration). Finally, it is able to integrate KYC providers from the provided list.

Tangany

They are using a combination of the cold and warm wallets certified by US-governmental and banking standards. Tangany is supervised by the German Federal Financial Supervisory Authority. They offer a white label frontend and are more focused on Bitcoin and Ethereum ecosystems.

Curv

Curv is a cloud-cased wallet service that provides an opportunity to flexible employment of the end infrastructure - a combination of approaches to business requirements satisfying. The solution provides also the ability to full managements of end users (flexible policies setting on the users with different categories) and API integration with needed services.

Gemini custody

Gemini provides offline storage systems with multisignature supporting, role-based governance protocols, and multiple layers of biometric access controls and physical security to safeguard customer assets. Process of user's management presumes mandatory whitelisting and customizable approval processes for withdrawal operations.

Anchorage

Anchorage solution actually provides cold wallet management technology and allows to customize the solution for individual needs of particular business. Supports API integration with existing tools and solutions. A feature of the system is the flexibility of asset management policies: setting up high-level logic of accounts, separated storage management, etc.

Vo1t

This solution also presumes the use of cold storages to manage assets. The solution emphasizes the greatest emphasis on ensuring the security of the process of information storing using technical (physical protection) and cryptographic methods (multilayer encryption).

HexTrust

HexTrust solution allows to configure several wallets (with different types) for differentiation of access policies during access to the funds. There are several levels of security in these wallets: from wallets that use distributed shared secrets with instant (relatively) access to cold wallets with insurance and multisig access models.

Falcon

The approach presumes that keys have to be protected using Shamir's Secret Sharing algorithm and multi-signature signing of transactions (for all supported cryptocurrencies). Falcon solution has an insurance policy issued by a major Swiss insurance provider for cases of crypto-relevant risks including professional indemnity, crime and cyber security breaches.

Competition analysis

		GK8	Solaris	Metaco	Tangany
Security and funds management opportunity	Hot wallets supporting	⚠️	✅	✅	❌
	HSMs supporting	✅	❌	✅	✅
	Cold wallets supporting	✅	✅	✅	✅
	Manual backup	✅	✅	✅	✅
	Shared secret backups supporting	✅	❌	✅	❌
	Insurance	✅	❌	✅	✅
	Manual funds distribution	✅	✅	✅	✅
	Authomatic rebalansing	✅	❌	❌	❌
User management and KYC features	User groups	✅	❌	✅	❌
	User roles	❌	⚠️	❌	❌
	Limits	✅	❌	✅	⚠️
	KYC supporting	✅	✅	✅	✅
	Pre-set KYC provider	❌	✅	✅	✅
	Ability for different KYC providers integration	✅	❌	❌	❌
Accounting systems supporting and customizing	Most popular cryptocurrencies and digital currencies	✅	✅	✅	✅
	Private blockchains integration	⚠️	❌	❌	✅
	Customized solution for exchanges	❌	✅	✅	✅
	Customized solution for funds	✅	❌	❌	❌
	Customized solution for tokenisation platforms	✅	✅	✅	✅

Bird-eye view

Curv	Gemini Custody	Anchorage	Vo1t	HexTrust	Falcon
✅	✅	⚠️	❌	✅	❌
❌	✅	✅	❌	✅	❌
✅	✅	⚠️	✅	✅	✅
✅	✅	✅	✅	✅	✅
✅	✅	✅	❌	✅	✅
✅	✅	✅	✅	✅	✅
✅	✅	✅	✅	✅	✅
❌	❌	❌	❌	❌	❌
❌	✅	❌	❌	❌	❌
✅	✅	❌	✅	✅	❌
❌	⚠️	❌	⚠️	❌	❌
✅	✅	✅	✅	✅	✅
✅	✅	✅	✅	✅	✅
❌	❌	❌	❌	❌	❌
✅	✅	✅	✅	✅	✅
✅	⚠️	⚠️	❌	✅	❌
❌	⚠️	⚠️	⚠️	✅	✅
❌	⚠️	✅	❌	✅	❌
❌	⚠️	✅	❌	❌	✅

Competition analysis

	GK8	Solaris	Metaco	Tangany
Different wallet types supporting	Combination of cold and warm wallets. Ability to integrate with 3rd party any type wallets.	Combination of cold and hot wallets.	Combination of cold (manually operated), warm (manually operated) and hot (API-operated) wallets.	HSMs. Additional ability for cold wallet and multisignature usage (only for cryptocurrencies).
Funds management flexibility	Ability to easily distribute funds between used wallets. Automatic rebalancing.	Ability to manual distribution funds between wallets. Several types of transaction approval	Ability to easily distribute funds between used wallets.	Amount of possible wallets is not limited. Manual cross wallet transfers.
User management flexibility	Ability to create the policy for a particular group (segregation).	Segregated and pooled wallets with different control types.	Customizable access rights for different accounts. Segregated and omnibus accounts.	Manual settings (disability to automatization of role management processes for today).
Limits management	Hour, weekly, monthly, total limits.	Absent (can be implemented in the nearest future).	Present in basic form: two main types of accounts (1th has restrictions for the assets management, the 2nd - does not)	Absent by default.
KYC / AML supporting	Presumed.	Presumed.	Presumed.	Presumed.
KYC integration	Opportunity to integrate with a 3rd party KYC provider.	Integrated with centralized Solarisbank's KYC solution.	Several KYC providers (Metaco's partners).	Supervised by the German Federal Financial Supervisory Authority.
Accounting systems supporting (digital and cryptocurrencies)	Most popular ryptocurrencies, ability to integrate with permissioned accounting systems (customizing).	Bitcoin, Ethereum (including Ethereum-based tokens).	Bitcoin and Ethereum-based ecosystems supporting.	Most popular public (Bitcoin, Ethereum, Tether) and private systems.
Backup functionality	Decentralized recovery scheme (threshold).	Manual backuping.	Ability to distribute backup secret into several shares	Manual backuping.
Liability of potential losses for assets	Digital assets insurance by AON via Lloyds of London.	Absent.	Presumed via GIANT BROKER AON	Present.
Additional provided services	Custody solutions for securities, real estate, derivatives, etc.	STO platforms and exchanges.	Exchange and tokenization platform solutions.	Trading and tokenization solutions.

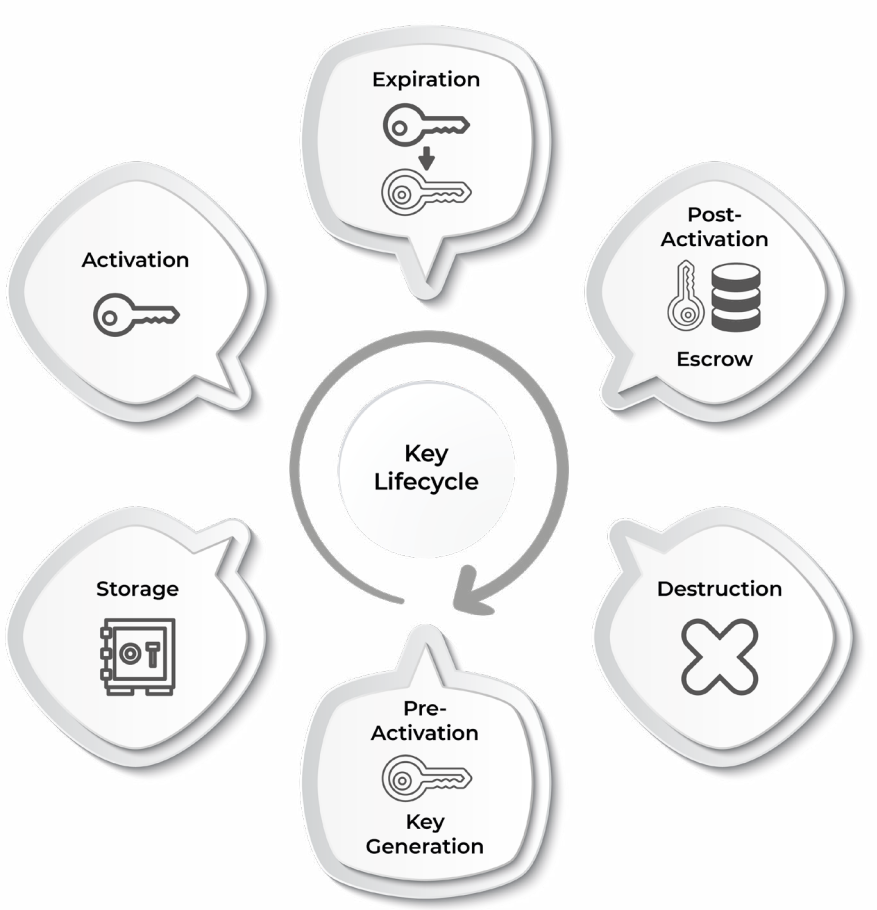
Detailed

Curv	Gemini Custody	Anchorage	Vo1t	HexTrust	Falcon
Combination of cold and hot wallets.	Combination of cold, hot wallets and HSMs.	HSM usage. Verification of access to the funds on HSM via whitelisted devices.	Cold storages.	Combination of cold, hot wallets and HSMs.	Cold storages.
Manual distribution funds between wallets.	Manual distribution funds between wallets.	Manual distribution funds between wallets.	Manual distribution funds between wallets.	Ability to manual distribution funds between wallets. Several types of transaction approval	Manual distribution funds between wallets.
Ability to define different profile types and enforce granular policies to ensure only authorized transactions are allowed.	Role-based access control and multisig supporting. Ability to sub accounts creation.	Ability to create different policies for different accounts and vaults	Manual settings (disability to automatization of role management processes for today)	Hierarchical role based model of access control	Manual settings (disability to automatization of role management processes for today).
Absent (can be implemented in the nearest future).	Absent (can be implemented in the nearest future).	Absent by default. Can be implemented.	Absent (can be implemented in the nearest future).	Absent by default. Can be implemented.	Absent by default. Can be implemented.
Presumed.	Presumed	Presumed. Behavior analysis and theft / suspicious activity detection.	Presumed	Presumed	Presumed
Integration with a centralized Elliptic solution.	Integrated with centralized KYC solution.	Absent. Audit performed by Anchorage team by default.	Integrated with centralized KYC solution.	Integrated with centralized KYC solution.	Integrated with centralized KYC solution (compliance with Swiss AML).
Potentially supporting all types of cryptocurrencies and digital assets. Most popular cryptocurrencies are supported by default (200+).	About 50+ most popular digital and cryptocurrencies.	About 30+ most popular digital and cryptocurrencies.	Bitcoin and Ethereum-based ecosystems supporting.	100+ coins and tokens from the most popular 10 blockchain-based accounting systems,	Bitcoin and Ethereum-based ecosystems supporting.
Decentralized recovery scheme (keys sharing).	Manual backuping.	Manual backuping.	Manual backuping.	Manual backuping.	Seeds are securely stored in multiple geographical locations in bank vaults by default.
Partnership with insurance powerhouse Munich RE.	Additional insurance in the cold storage (about $200m).	Insurance is presented.	London insurance companies. Customized insurance solutions from S&P A-rated insurers	Insurance is presented.	Insurance policy issued by a major Swiss insurance provider.
Air gap functionality.	Trading solutions.	Trading, financing, staking and tokenization solutions.	Trading and lending solutions.	Exchange, staking, lending, OTC solutions	Exchange and tokenization platform solutions.

Crypto custody solutions vs. HSMs

Key lifecycle

The key life cycle consists of the main processes described below. Note that the security of user funds lies in the plane of ensuring the security of all the mentioned processes. The most important processes: generation, storing, expiration and destruction (these processes are basic regardless of the system where keys are used).



Key generation

This point is one of the most critical in the context of key management. If during key generation some of the used processes were not protected, this may lead to its leak at this stage. Key generation approaches can (and most likely will) differ for different custodians: keys can be generated using different software and hardware methods, but it is important that these processes are standardized (FIPS-140) and protected.

Key storing

Key storage features depend on the selected type of wallet and will be described below.

Key expiration

Keys with an infinite lifetime do not exist. And the custodian service must make sure that the keys exist for a certain time, after which they are generated anew.

Destruction

Before destroying keys, it is important to check that they are not assigned assets in the corresponding accounting systems. Keys are usually destroyed after their expiration date or if they have already been used to transfer funds to another account / address. Sometimes the key management policy suggests keeping keys for longer periods of time to prove ownership of funds later.

Wallets classification

There are some options for the responsible party to organize the processes of storing private keys and signing the transactions that are reflected in the choice of a wallet class.

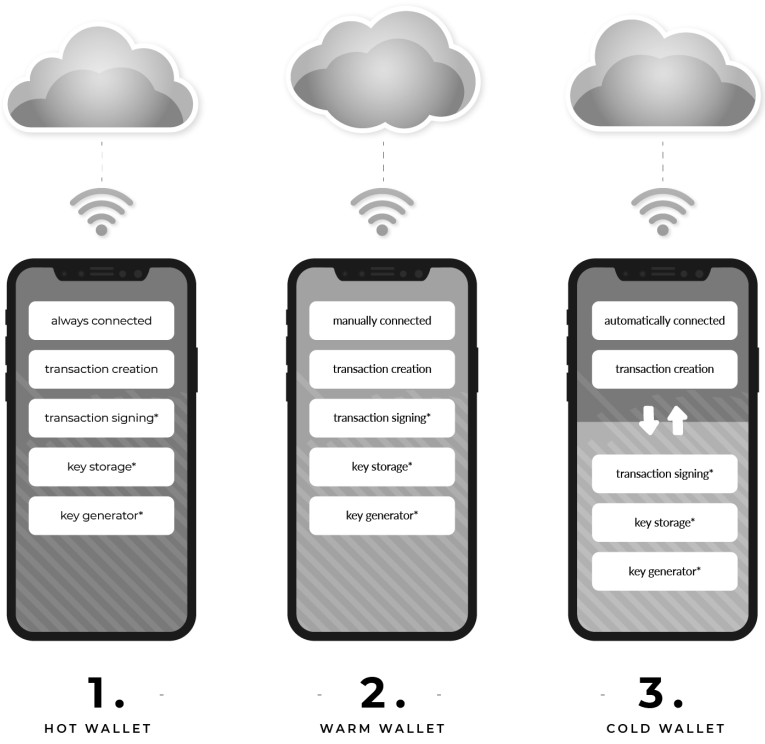
- Hot storage wallet;
- Warm storage wallet;
- HSM (hardware security module).
- Cold storage wallet.

A **hot storage wallet** is a digital wallet where private keys are stored and processed by a device that has a permanent connection to the global network.

A **warm storage wallet** is a digital wallet where private keys are stored only on devices that support the connection to the global network but not permanently—only according to the user's decision (for example, for sending transactions or updating their status).

A **cold storage wallet** is a digital wallet where private keys are stored and processed only on devices that do not have the ability to directly connect to the global network.

Hardware security modules are built on top of specialized hardware. The hardware is well-tested and certified in special laboratories, has a security-focused OS and limited access via a network interface that is strictly controlled by internal rules. Simply put, this is a warm wallet with a high level of security and control.



Potential attack vectors (for different wallet types)

Software wallets

- Theft of wallet file:
  The wallet file can be stolen by a malicious program or by someone, who has access to the computer. Even if the wallet file is encrypted, you can just lose it (other case - password for encryption could be logged by the malicious program).

- Fake wallet:
  Fake wallets imitate the work of the real one. As soon as the user installs the wallet and enters his seed phrase / imports his keys, the fake wallet sends all funds to the attacker address / account.

- Backdoors (deliberate and accidental):
  You have to trust your wallet manufacturer and in the best case to perform the audit used software. In practice, the best software in this regard is open source software with a lot of collaborators.

- Phishing (for web wallets):
  facebok.com, fasebook.com and 100 different close combinations. Facebook has thought about a solution to this problem. What about the producer of your wallet?

- Other PCs using:
  Have you already conducted the audit of your wife's PC?

- DNS hijacks (for web wallets):
  Host substitution (redirecting or blocking pages) can lead to the attacker's web page (it can be performed by substituting the «host file» on the PC or changing the DNS server record - the latter is more difficult, but potentially possible).

- Bookmarks changing (for web wallets):
  This is a very primitive and funny (for those who were not so attacked) way, which consists in using malicious code that changes the link of your bookmark in the browser.

- Clipboard and buffer hijack:
  In this case, there are 2 types of attacks. The first is related to the fact that a malicious program can log all user actions (and potentially this can lead to theft of a password or key if it is entered or copied). The second vector also consists of buffer control - in the case when the user copies the address / account ID of the recipient, the program automatically changes it in the buffer (to the address / account ID of the attacker).

- Convenience thread:
  Users like primitive passwords (for wallet encryption etc) for their needs. Attackers like it too =)

Hardware wallets

- Theft and losing:
  The most popular way of losing funds by end users if the keys were not previously reserved.

- Preconfigured device:
  Classic attack vector for hardware wallets: the wallet comes already “pre-configured” by the attacker. Using this wallet can lead to the funds losing.

- Hardware manipulation:
  Controlling the display of a hardware wallet is a more complex task (then for example buffer controlling) but not impossible.

- Ransom attack:
  The attack is based on the fact that the modified wallet generates an address that belongs to your private key, but was chosen very randomly (a large index value is used to generate the key). As a result, if you restore the wallet, you will not immediately be able to access your coins (you must first know the index used to generate the corresponding keys).

Naturally, this list is not exhaustive. We have shown only the most basic attacks (and some very interesting ones) to emphasize the importance of choosing wallets and their management mechanisms.

Crypto custody solution high-level architecture

The main difference between one of the above mentioned wallet classes and a crypto custody solution is that the latter, in addition to the software and hardware for key management, must provide functionality related to the administration and regulation of the system (a set of policies and mechanisms for their implementation) as well as communication with the necessary accounting systems and services. That is, in fact, wallets are only a functional part of the service.

Key storage component

Set of the wallets with securities. Different services may use various wallets, methods of distributing funds on these wallets, as well as backup and recovery mechanisms.

Communication module with external systems

Set of gates with different systems (including bank and external systems - depends on keeped assets). This module also performs the initial validation of the client's request and protects other components from external attacks. As an additional module can be used the software of the external system (auditor-node) for audit and communication with the external system.

Regulative tools

Perform the validation of clients' requests. An operation / transaction can be processed by administrators and confirmed only if it has passed an approval of this component. Transactions with different values may require different confirmation procedures from this component and be processed differently.

Access control component

List of custody service administrators with their permissions and weights. Access to the wallets and their backups can be performed only by designated administrators.

Approaches to the custody solution development

Let’s take a short tour of custodian solutions, possible approaches to the implementation of these approaches and compare the described approaches according to the following criteria:

Security
(the ability to resist technical attacks)

Low security (there are trivial methods to system hacking).

Medium security (requires a certain amount of resources to carry out an attack).

High security (requires a significant amount of resources to carry out an attack).

The highest level of security (the probability of a successful attack strives to 0).

Convenience
(simplicity and speed of operations)

Low level of convenience (operations take a long time and organizationally complex).

Medium level of convenience (performing operations takes a long time, but at the same time does not cause significant discomfort for clients).

High level of convenience (optimal time for operations performing).

The highest level of convenience (users are as happy as possible with the speed of operations).

Cost
(system implementation cost)

Low (cheap solution: several basic elements with low cost).

Medium (close to standard solution that does not require additional unique changes).

Upper the medium (standard solution with additionally implemented functional components).

Hign (too complex and expensive custom solution).

Risks
(risks of losing funds due to attacks of various types)

Low (the probability of losing funds strives to 0).

Medium (there is some possibility of loss of funds)

Upper the medium (significant probability of loss of funds).

High (very high probability of loss of funds).

First generation solutions

Single party with hot wallet

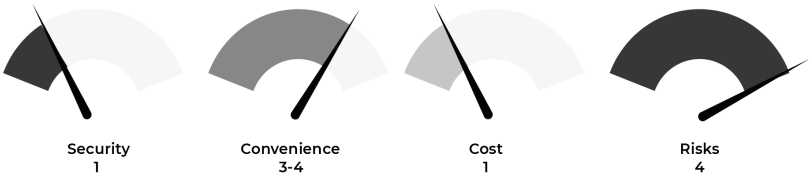
This method consists in the fact that a single responsible party manages a hot wallet, on which all funds are stored.

Pros:

- Easy funds management;
- Requests for withdrawal and transfer can be quickly processed.

Cons:

- As a result of hacking a wallet (for a hot wallet, it's quite simple to provide), all funds will be lost;
- Pressure (no matter what kind) on a single responsible party can lead to loss of collateral.



Single party with cold wallet

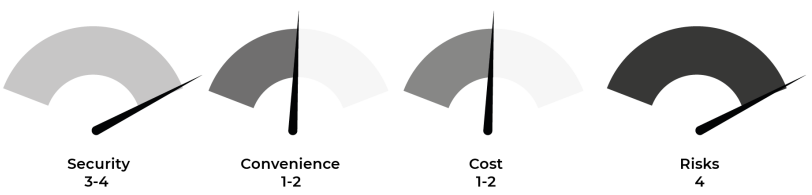
This method consists in the fact that a single responsible party manages a cold wallet, on which all funds are stored.

Pros:

- Higher level of security (cracking a specialized cold wallet is almost impossible);
- A withdrawal request can be processed quite quickly.

Cons:

- Pressure (no matter what kind) on a single responsible party can lead to loss of collateral.
- A more complex process of managing funds (it is almost impossible to achieve a high level of automation without losing security).



Several responsible parties with hot wallets and using the multisignature

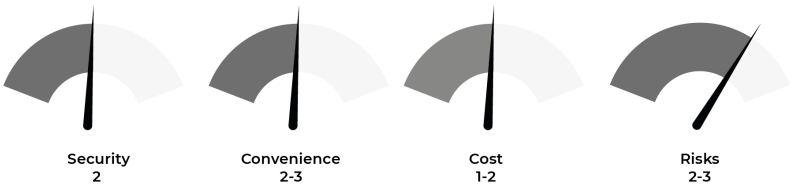
This method consists in the fact that funds locked with multisignature and several parties manage it via hot wallets.

Pros:

- Request for withdrawal can be quickly processed;
- Reduces the possibility of pressure on a single responsible party.

Cons:

- As a result of hacking wallets (for a hot wallet, it's quite simple to provide, even if they are from different manufacturers), all funds will be lost.
- More difficult to implement.



Several responsible parties with cold wallets and using the multisignature

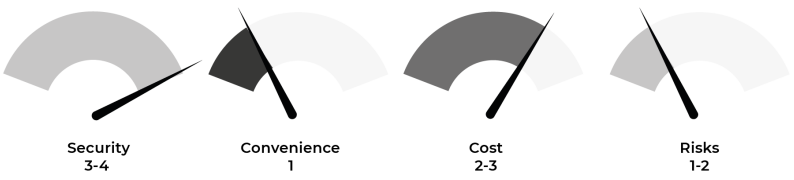
This method consists in the fact that funds locked with multisignature and several parties manage it via cold wallets.

Pros:

- Higher level of security (cracking a specialized cold wallet is almost impossible);
- Reduces the possibility of pressure on a single responsible party.

Cons:

- Slow operations confirmation;
- More difficult to implement.



Second generation solutions

Using a combination of hot and cold wallets (welcome to the exchanges world)

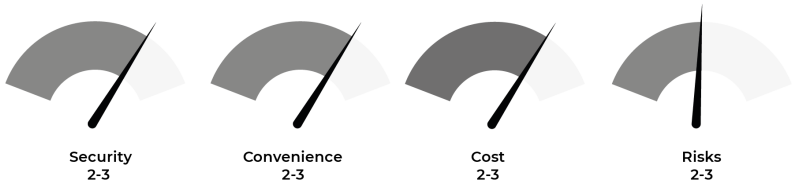
In this case, it is assumed that part of the funds (assume 1% of the total) is stored in a hot wallet, which is managed (most often) by a single responsible party / module. The remaining funds are stored in a cold wallet that can be managed by several trusted parties.

Pros:

- All funds cannot be stolen at once (in our case - 1%);
- Reliable protection of the main part of funds;
- Quick access to small amounts.

Cons:

- Money can still be stolen (yes, not so much, but still);
- If the funds run out on a hot wallet, you must perform a manual withdrawal from a cold wallet to a hot one (more difficult process).



Using HSMs and several responsible parties for the accesing to its

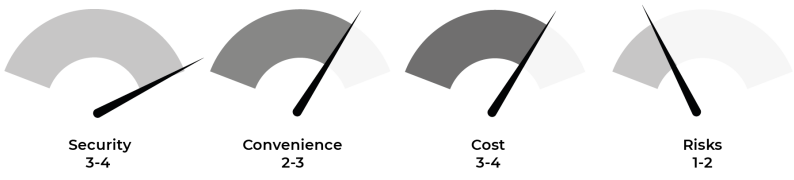
In this case, the keys are stored by the hardware security modules, and they sign the transaction only if several responsible parties contact it (+ multisignature mechanism).

Pros:

- Such repositories can be considered quite secure;
- There is no single point of pressure on a single responsible party;
- Quite quick access to funds;
- Even if you do not fully trust the hardware security modules, you can combine this approach with a cold wallet.

Cons:

- Some difficulty in managing funds.



As you can see, there is no single existing solution (and never will be) that would immediately satisfy the needs of all possible parties. Either you pay for performance by lowering the security level, or you accept the risk by lowering the cost of the system. Therefore, our target proposal is not to provide some unique solution that will allow providing all the properties, but to provide a set of tools that will allow the custodian to distribute the influence of the described properties for their own needs.

But more on that later...

Product vision

As the analysis of existing solutions on the market shows, each of them provides for an emphasis on certain properties offered to the end consumer.

Some of them strictly focus on the security of storing keys, and have a rigid storage architecture that does not allow the end users to adapt it to their needs (for example, they imply cold storage from which a hot wallet can be replenished for a small amount), while allowing integration with external KYC providers.

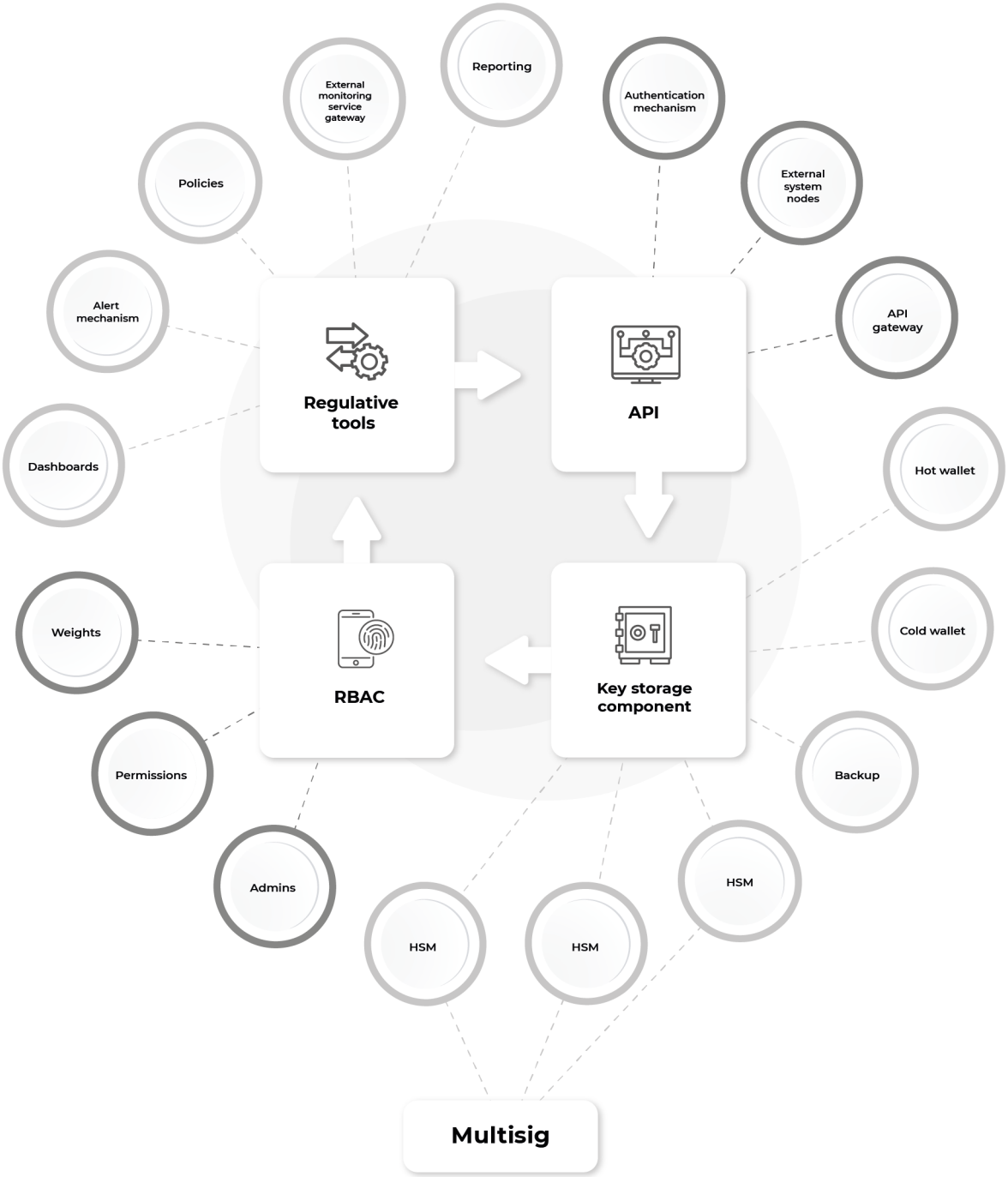
Others have the opposite situation - they have a set of different solutions / wallets, with different levels of security, but the centralized KYC provider is a certain bank.

Each of the solutions we mentioned above definitely has very strong points on which it focuses, but none of them provide flexibility in building all the components of the system.

The key feature and thus the overall product vision of the proposed solution is the full management of the ultimate custodian of the system:

- the ability to choose any type of wallets, their required number and the ratio of funds that will be stored on them (independent distribution of risks and convenience);
- the ability to choose a wallet administration option: the use of multisignature, threshold signatures and other tools for diversifying responsibility
- the ability to choose a backup method (as an example - creating a shared secret, encrypting keys from wallets with it and sharing between any number of administrators with different weights)
- the ability to connect any identity provider (subject to an open API)
- the ability to create roles and set limits and flow verification of transactions depending on the role;
- the ability to create groups and connect different providers to monitor different groups.

Rough architecture overview



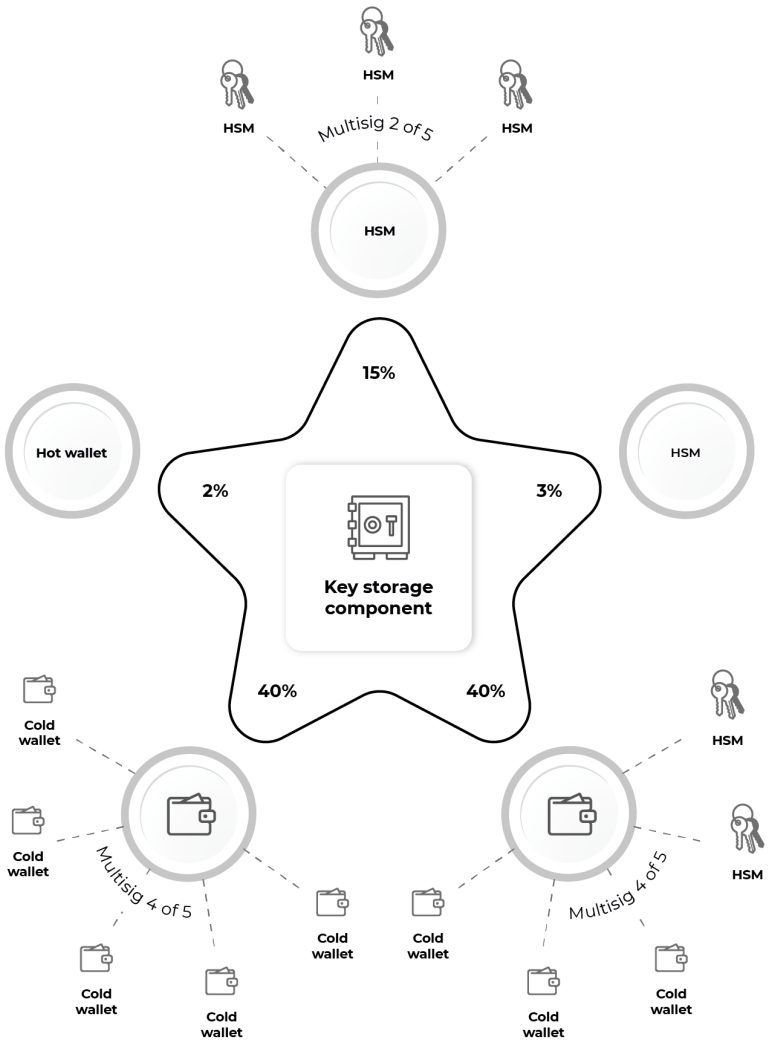
Key storage component

Choosing wallets and funds distribution

The main element of the funds storage system is the wallets. The architecture and principles of functioning of wallets have been described above, so let's move on to the mechanism for selecting them. Since we focused on the flexibility of the solution, the choice of wallets should be based on the decision-making model depending on the business requirements. That is, the owner of the final system can choose the optimal solution for each of their stored digital assets.

For example, the system owner wants to:

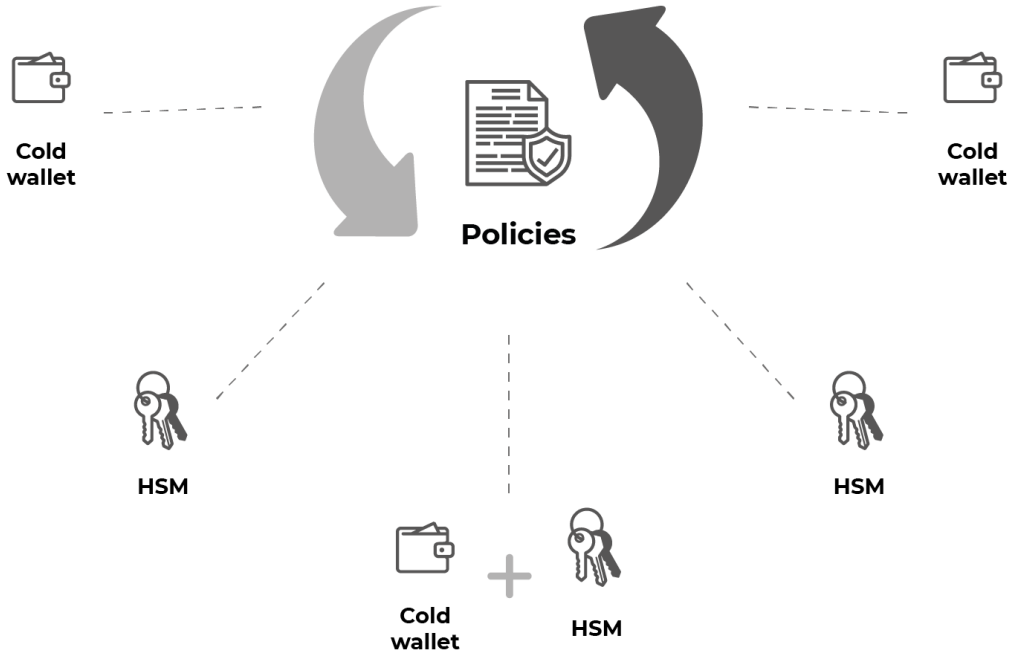
1. 40% of funds were stored on a 3-of-5 multisig address and all keys for multisignature were stored in cold wallets;
2. 40% of funds were stored on a 4-of-5 multisig address, with 3 private keys stored in cold wallets and 2 in HSMs;
3. 15% of funds were stored in HSM and required a 2-of-3 multisignature;
4. 3% of the funds were stored on HSM and only 1 signature was required to unlock it;
5. 2% of funds were stored in a hot wallet.



In this case, the business requirement is to flexibly manage 5% of the total amount of funds stored - for small and medium-sized transactions (with the HSM and hot wallet being managed by separate parties). HSMs and 2-of-3 multisig allow organizing wallet replenishment from 15% of the fund. All other funds are in a locked state (transfer of these funds is a complicated and time-consuming procedure, but security requirements are met).

Also, the following policies can be configured:

1. Transfers that do not exceed X (small transfers) are sent to the hot wallet;
2. Transfers that do not exceed Y (below average) are sent to HSM;
3. Transfers that do not exceed Z (average) are sent to HSM 2-of-3;
4. Transfers that exceed Z are sent to one of the high security wallets;
5. If the amount on the hot wallet exceeds A, then a certain amount of funds is transferred to the HSM;
6. If the amount on the HSM exceeds B, then a certain amount of funds is transferred to the HSM 2-of-3;
7. If the balance of the hot wallet is lower than C, then it:
    a. is replenished from the HSM wallet if the amount on it is not less than D.
    b. or top-up from HSM 2-of-3 wallet.



In fact, the number of such policies can be anything large. At the same time, it is important to determine the needs of the end customer and create a flexible and secure system for managing funds.

Backup

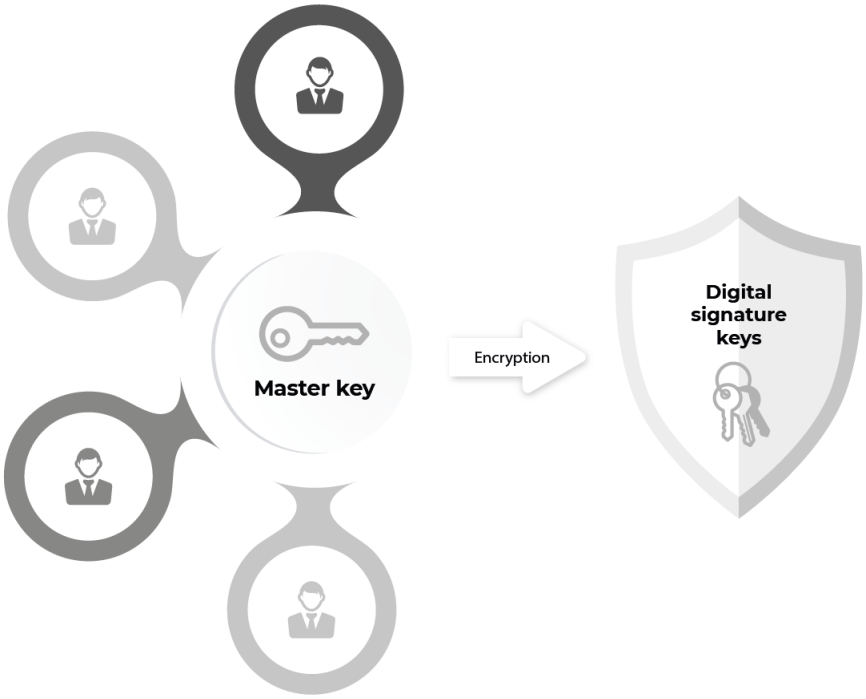
A separate issue that needs to be resolved when building a key storage component is their backup. In this case, there are also cryptographic tools that allow you to ensure the confidentiality of keys and assign responsibility when gaining access to them.

For example, imagine a business needs to create a storage that is managed by 2-of-2 administrators. In this case, if you just distribute the keys to the appropriate administrators, then in this case there is a risk of losing one of the keys (which will lead to a loss of funds). Therefore, an additional security element can be backing up these keys, for example, as follows:

1. A new secret is formed, with which the keys for multisignature are encrypted.
2. The secret is distributed among 3 different participants using the Adi-Shamir key distribution scheme (administrators and owner) with the required 2-of-3 threshold.
3. The encrypted keys are stored in a storage (preferably in several different storages).

In this case, if one of the administrators loses the private key, the system owner can generate a shared secret (having a part of the secret provided by another administrator) and decrypt the required key with it. After that, a multisignature can already be generated and the funds can be unlocked.

Again, this flow shows how this interaction can be organized and that such a possibility exists - however, the requirements and mechanisms for solving such problems will proceed from the requirements of a particular business.

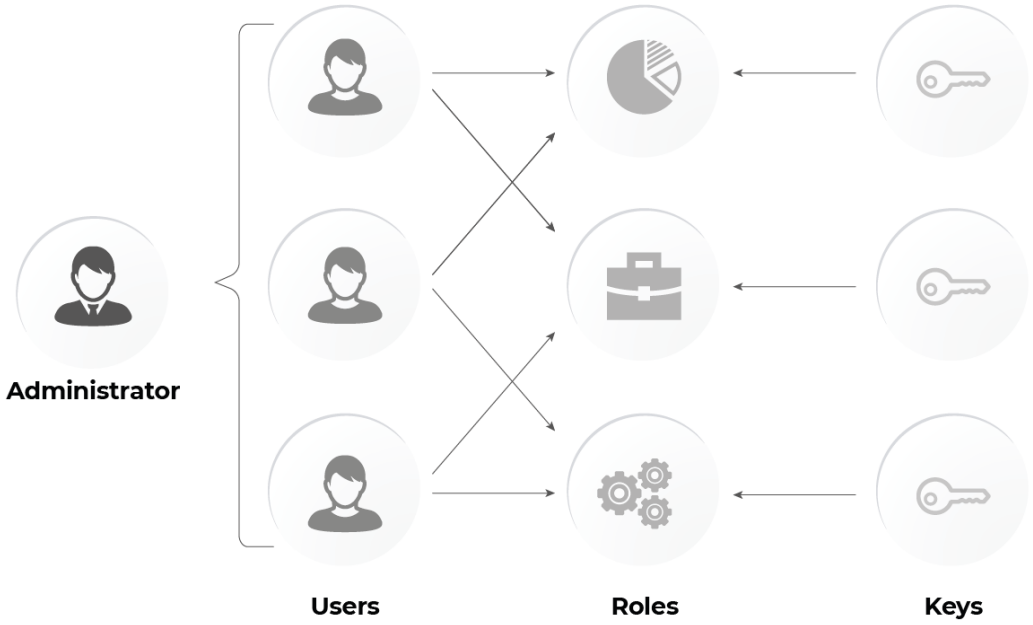


Access control component

In our approach, we use the RBAC model of gaining access to system services: for each role created within the system, a set of permissions, limits, etc. is defined. Each platform member is assigned one of the existing roles (after registration and passing the identification procedure), after which all specific policies are assigned for the target account in particular.

Each user of the system has an account on behalf of which all actions in the system are performed. Therefore, each request is checked against the permissions that are defined for the user account. In case of receiving requests for operations for which the account does not have permissions, as well as in the case, for example, of exceeding the limits (daily, monthly, annual, etc.) - the operations are rejected by the system and are not processed. Only if the request satisfies the permissions and has been confirmed - interactions with stored assets (i.e. wallet management) are performed.

The creation of roles and the definition of policies for them is performed by system administrators. In this case, a mechanism for diversifying responsibilities between platform administrators is also provided (the ability to configure the threshold signature and weights for performing administrative actions within the system). Due to this, it is possible to organize a model in which key (critical) operations in the system cannot be performed only by a single party. Such operations include, for example: blocking users, changing limits on operations in the system, creating / deleting roles, etc.



Regulative tools

Also, one of the basic requirements for the system is the need to comply with a certain legal field, which entails the need to provide tools for monitoring transactions, mechanisms for detecting suspicious actions within the boundaries of the system, reporting and providing data to external regulatory bodies.

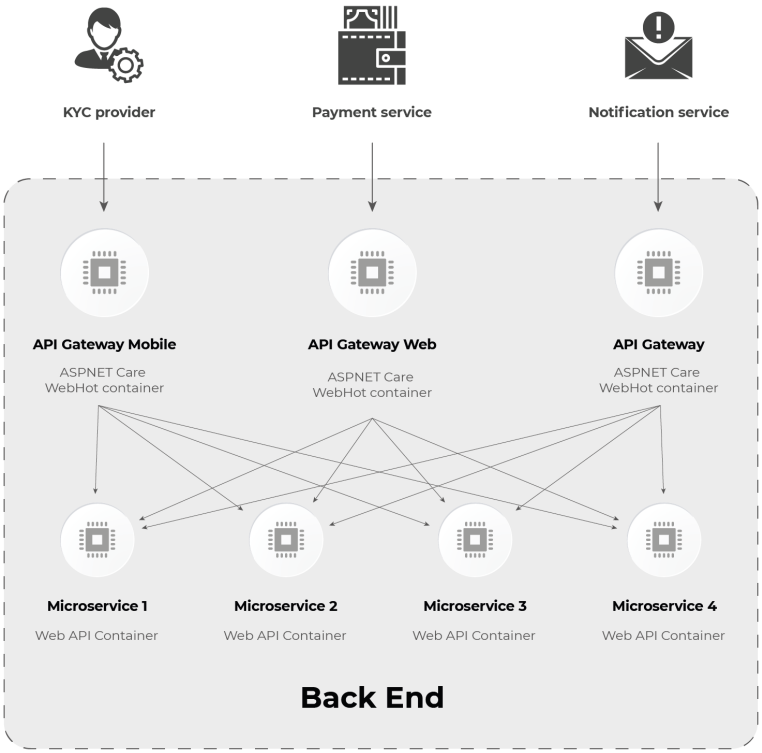
The architecture of the proposed system provides for the provision of the described mechanisms with an increased level of security. In particular, the mechanism for logging events in the system is built in such a way that it is possible to provide the auditor's software to an external party (which will monitor the activities of the custody service). In this case, the outside party gets the opportunity to synchronize logs in realtime and identify attempts to change the history of user actions in the system.

This approach is aimed at automating the processes associated with checking events in the system and increases the level of trust in the system due to its verifiability by parties who have received the appropriate permissions.

External systems gateways

A separate component of this system is tools for integration with external systems. Among such tools are:

- Full nodes of accounting systems of corresponding digital assets;
- API for integration with:
    a. 3rd-party identity services (KYC providers);
    b. Payment services and gateways;
    c. Notification services;
    d. Issues tracking, reporting and monitoring services.



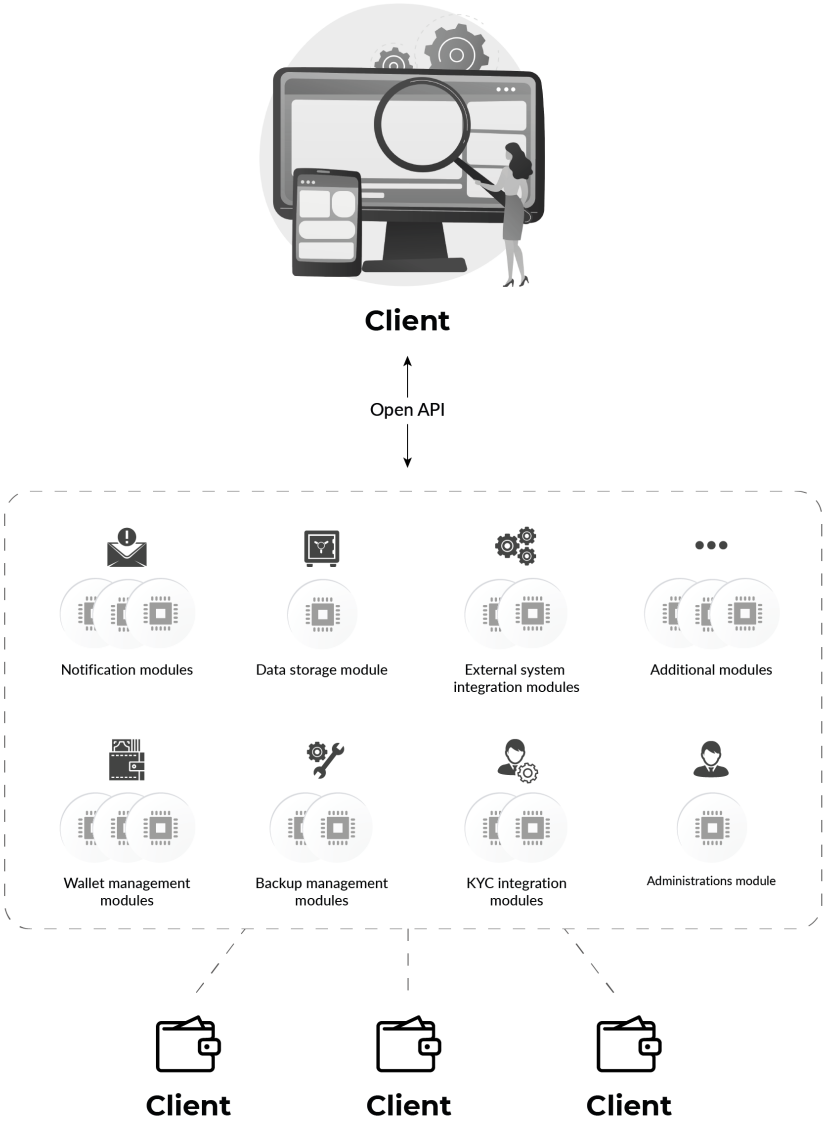
Proposal

We see middleware as our solution, which will allow managing wallets using an API. In this case, we leave the opportunity to use any software and hardware for the implementation of wallets, which will be managed by separate modules that will be called using the API by end clients. At the same time, there remains the possibility of complete customization of the final software.

That is, at the lower levels there will be storages (of different types and with a different way of managing them) - ***flexibility in security mechanisms selecting***.

Middle layer (actually the proposed system) - a set of modules for managing wallets (and additional administrative and integration functionality) - ***flexibility in system functionality selecting***.

Top layer - clients (web, iOS, android) with ability to call system API methods - **flexibility in client design implementation**.



Particular architecture proposal

From what can be considered as a piece for patenting for custody solutions, these are the principles of storing and distributing keys. In this case, it is better to focus on the mechanism for diversifying responsibility and improving the multisig approach. I marked the most important components in yellow.

The description refers to a separate accounting unit / accounting system. If the custodian is managing various digital assets, the approach described below can be used for each of them.

Key storage

Hot wallets

2 hot wallets with 0.5-0.7% coins each. A single party signature is required to manage a particular wallet. This approach allows you to quickly withdraw a small amount of funds. If the amount of coins exceeds 0.8%, the funds are transferred to the cold wallet storage. If the amount of funds on this wallet is less than 0.2%, it is replenished up to 0.5% from the HSMs 2-of-3 wallet.

Purpose of this type of wallets is to receive payments with a small amount. Fast withdrawals for small amounts. If one of the wallets denies service, continue functioning at the expense of the second.

Wallet backup - creating a copy of private keys and storing them in a centralized storage in encrypted form. Encryption/decryption of copies is performed by administrators who are responsible for managing funds. The storage contains an associative pair: wallet identifier :: encrypted container. The administrator receives the container by its identifier, then locally decrypts it and receives the keys.

HSMs + multisig 2-of-3

5-7% of funds are held locked on 2-of-3 multisig. The wallets used by the respective administrators are HSMs. This approach allows you to provide a higher level of security of funds and at

the same time enable the parties to make a payment quickly enough. If the amount of funds in the wallet exceeds 8%, the surplus (up to 5%) is transferred to cold storage. If the amount of funds on this wallet is less than 2%, it is replenished up to 0.5% from the HSMs 3-of-5 wallet.

The purpose of this type of wallet is to receive payments with an average amount. Increased level of security.

Wallet backup: the same option as for hot wallets.

HSMs + multisig 3-of-5

20-25% of funds are held locked on 3-of-5 multisig. The wallets used by the respective administrators are HSMs. If the amount of funds in the wallet exceeds 30%, the surplus (up to 20%) is transferred to cold storage. If the amount of funds on this wallet is less than 15%, it is replenished up to 0.5% from cold storage.

The purpose of this type of wallet is to receive payments with an amount above average. High level of security.

Wallet backup: when generating an address, administrators generate only 4 keys (out of 5 possible). The last secret is generated by the responsible party and distributed according to the Adi-Shamir scheme among the staff of a higher management level, with an m-of-n threshold (after which it is destroyed). In this case, if 3 out of 4 administrators agree with each other, they can jointly form and sign a transaction that initiates the withdrawal of funds from the wallet. However, if a dispute arises and the opinions of administrators are divided in half, the responsible parties of a higher level can form a secret using their parts and use the resulting value to resolve the disagreement in favor of one of the parties (calculating an additional signature).

All administrator secrets are encrypted in the repositories.

Cold storage

Cold storage stores an amount between 71.2% and 82.8% and assumes a 2-of-3 multisig. Two of the keys are kept by

designated administrators in cold wallets, with no access to the environment. The third secret is calculated similarly to the approach described above: the generation of a secret and the distribution of its constituent parts among the n number of participants who can, if something happens, sign the necessary transaction.

The purpose of a wallet is only to replenish other wallets, to receive funds when it comes to large payments and to receive surplus wallets in the event of overflow.

Encrypted key storage

Above we mentioned about the storage, which stores containers with encrypted administrator keys (and is necessary for their backup). In this case, the designated administrator can encrypt the key locally and place it in the vault. The storage stores this container and transfers it at the request of the administrator using the container identifier (after verifying its identity). For identity verification, any approaches that currently perform the function of 2FA can be used. Depending on the administrator access level, these approaches may differ (for lower-level administrators - checking mail, owning a token, for higher-level administrators biometrics, personal visits, etc.).

Core requirements

For the system to enter the B2B market, it must meet a set of requirements. These requirements can be divided into three main areas - compliance with regulatory requirements, the technology stack used and security aspects.

Regulations requirements

Today, there are no strict regulatory documents that are entirely related to the regulation of asset storage services. However, at the same time, services must be subject to applicable legal acts, including UCITS (Undertakings for Collective Investments in Transferable Securities), AIFMD (The Alternative Investment Fund Managers Directive), GDPR (The General Data Protection Regulation), 5MLD (Fifth Money Laundering Directive) etc. If the custodian decision does not comply with the above-mentioned acts, its chances of entering the market are reduced to 0.

Technical requirements

The main business requirements for this area are generally based on the use of advanced automation technologies (artificial intelligence and robotization), advanced audit (DLT) and management (digital signatures) capabilities.

The automation element can be aimed at solving problems related to simplifying mutual settlements and managing wallet balances, as well as providing increased performance of exchange functions. AI, in turn, can perform the function of analytics of actions within the system: analysis of user actions in order to form predictions and track suspicious activity.

The requirements associated with the use of DLT are fully justified by the need to audit the system in real time (plus the ability to check the integrity and authenticity of the history of events over time). This approach can potentially greatly reduce the costs associated with the need to conduct periodic comprehensive checks of the correctness of the interaction of system elements. A related activity is the tokenization process - the digitization of user property rights, which also requires the use of blockchain technology and digital signatures to implement a secure and automated process for transferring these rights between their owners.

In the context of digital signatures, there is also a certain feature - the use of different signature mechanisms in different countries (defined at the level of regulatory support). Therefore, an additional feature of the system should be the ability to connect various libraries to implement signatures in accordance with business requirements.

Security requirements

Security, in general, is the most important reason why users place their assets for storing in custody services. In accordance with this, cybersecurity is the most demanded in the market for storage of digital assets. To meet market requirements, the ability to flexibly adapt to an ever-changing cyber threat environment does not slow down the implementation of the technologies described above.

Risk and Compliance

Global aspects of compliance

For crypto custody, the opportunities presented by crypto and DLT are tied to significant operational and regulatory challenges, such as implementation of anti-money laundering and counter terrorist financing regimes, development of clear compliance and monitoring procedure.

The purpose of compliance is to provide guidance on following for the crypto custody on the Anti-Money Laundering and Know Your Client policy to achieve full compliance with the relevant anti-money laundering legislation.

Crypto custody needs to identify cryptocurrency risk considerations for them, focusing on:

- risks posed by customers who hold cryptocurrencies to a significant degree;
- risks posed by identification of the source and lineage (historical origination) of clients funds and appropriate monitoring of their transactions.
- risks posed by evaluation of the legal and regulatory of custody of a crypto in a selected jurisdiction.

The Financial Action Task Force (FATF) view is that cryptocurrency payment service providers should be subject to the same obligations as their non-crypto-counterparts. From an EU regulatory perspective, the most significant act is Fifth Anti-Money Laundering Directive (5AMLD). The reason for this is that the directive extends the Fourth Anti-Money Laundering Directive by bringing virtual currency exchange platforms and custodian wallet providers within the scope of the EU's anti-money laundering requirements.

Accompanying risks

There are two key risks at the asset custody service level:

- The risk associated with the inability to return funds by the custodian (failure to fulfill obligations related to the return of funds to end users).
- The risk of losing funds due to errors or attacks on the service.

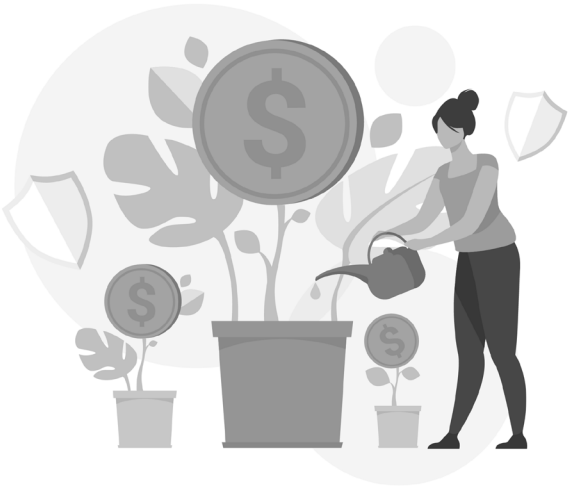
Risks that are of the first type can be mitigated by choosing a custodian who has some financial stability.

The second type of risk can potentially be solved by distributing funds among several custodians (the likelihood of occurrence of the same kind of errors and vulnerabilities for different services is quite low), however, flexibility in their management can be lost.

Target Markets and Business Potential

End users

Digital asset custody services provide users with the ability to manage funds while reducing the risk of losing funds (providing recovery mechanisms and multi-level authentication). Also, the threshold for user entry is reduced, since now the key management mechanisms (which require a certain level of competence from users) are being replaced by the usual methods of authentication on the service.

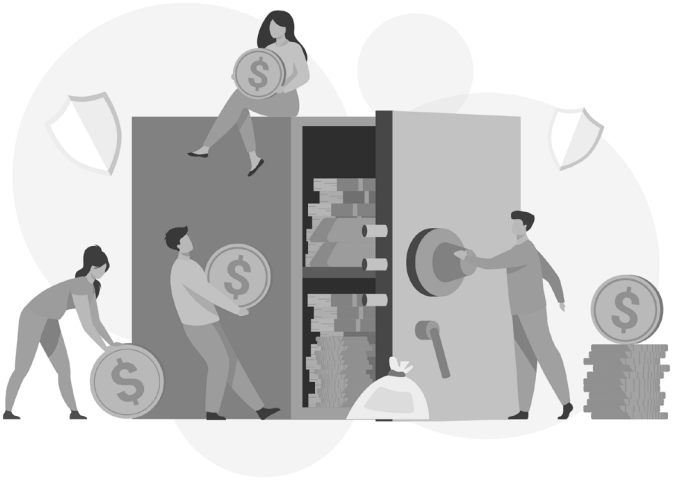


Exchanges

Exchanges are prominent representatives of clients who require a combination of hot and cold wallet technologies and risk diversification mechanisms to manage user funds. Very often, an additional requirement when building exchanges is to automate the processes of transferring funds between wallets with different levels of security (automatic replenishment of hot wallets in case of reaching a certain lower threshold, as well as transferring funds from hot wallets to cold ones in case of accumulation of some surplus).

Banks

Banks and other organizations whose activities are related to the storage of user assets when using storage services can offer end customers control, security and liquidity of the digital assets they hold with the ability to exchange with fiat currencies.



Funds

Funds, venture capital firms, and other companies that deal with asset management can use custody services to provide users with control over their shares and funds in accordance with established policies. Full control over the differentiation of access to digital rights management and the use of modern cryptographic mechanisms will allow you to maintain compliance with regulatory standards and increase the audibility and security of funds management.

Bibliography

1. Anti-money laundering (AMLD V) - Directive (EU) 2018/843.
2. Markets in Financial Instruments Directive (2004/39/EC).
3. ECON COMMITTEE Crypto-assets – Key developments, regulatory concerns and responses
4. Payment Card Industry Data Security Standard.
5. Di Nicola, Vincenzo. «Methods and Systems for Safe Creation, Custody, Recovery, and Management of a Digital Asset.» (2019).
6. Krimminger, Michael H., et al. «Custody and transfer of digital assets: Key US legal considerations.» Blockchain & Cryptocurrency Regulation (2018).
7. Gągol, Adam, et al. Threshold ECDSA for decentralized asset custody (2020).
8. Lekkas, Nikolaos. «Legal Aspects of the Custody of Digital Assets.» (2020).
9. Chen, Zhaohua, and Guang Yang. «Decentralized Custody Scheme with Game-Theoretic Security.» (2020).
10. Deloitte, The evolution of a core financial service. Custodian & Depositary Banks (2019).