Bcademy

#CRYPTOKNOWLEDGE

Bcustody ₿

22|03|20

What?

Bcustody is a **B**cademy's service enabling to secure bitcoins via the custody of private keys through an original design. Such design not only allows to secure one's capital, but also allows to access it, therefore spend part of it, at any time, keeping the rest safe.

Bcustody is based on the installation of a multisig wallet (a function present in the bitcoin protocol), literally a wallet that requires more than one signature (multi-signature) to be able to transact, where each signature is associated with a different key (in this case 2 out of 3).

The core of the service is based on:

- **consultancy for the installation and set-up of the software** (multisig wallet), guaranteeing the creation and secure distribution of the keys
- **consultancy for the installation and set-up of a simple wallet**, creation and maintenance of a bitcoin address (to which the assets would be transferred in the event of death of the client or service interruption)
- **training and documentation** for the use of both wallets
- **assistance in the event of issues** relating to the use of the multisig wallet
- **custody of the third key** by a professional (notary, accountant or lawyer)
- **assistance in transferring the portfolio value in case of loss of one of the three keys**, via the creation of a new wallet and consequent generation and distribution of three (new) keys
- **assistance in transferring the portfolio value in case of death of the customer or interruption of the service**, to the address connected to the simple wallet (point 2)

Why?

Unlike traditional banking, where who custodies value also becomes the owner (i.e. art 1834 of the Italian Civil Code) while the assignor remains a mere depositary, **in Bitcoin, thanks to the double key cryptography, ownership is defined solely through the possession of the private key**. This is a key feature in cryptocurrencies, as it categorically excludes that someone not in possession of the private key can block or spend capital. But it also generates a problem: **in case of loss of the private key access to the assets is precluded, making those literally inaccessible.**

The multisig function, literally *multisignature*, implies that to spend any amount the signature generated by a private key is not sufficient, but a number of signatures *n over m* would be required, usually *2 out of 3*. Through this function therefore, correctly inserted in a structured design with different players, **it is possible to overcome the trade-off between security (not to lose or see one's own capital moved or blocked) and confidentiality (to be able to access one's value by *bypassing* a malicious intermediary).**

Where?

The word *wallet* is not precise, since rather than a wallet we are referring to a *keychain*. **In fact, bitcoins are not custodied inside a wallet, but they are information kept on a distributed register, a data structure called *blockchain*. Access to this information, meaning the possibility of transacting one's bitcoins, is defined by the possession of a key: the private key allows to spend the bitcoins previously sent to a specific address associated with the key itself.**

Double-key encryption, private and public, is the basis of how cryptocurrencies work. The private key, a randomly generated alphanumeric string, is the key which guarantees the ability to spend one's capital. The public key, generated from the private key through a one-way function (ergo from a public key it is not possible to recreate the private key while the opposite is always possible) is the key that is used to generate the bitcoin addresses, i.e. where to receive and send value, which can therefore be shared freely. In other words: the private key is required to send value (spend money) while the public key is used to receive value (to accumulate money).

To simplify the concept, it is possible to think of the private key as a password to spend one's own money. A private key has the following form, shown in its hexadecimal representation (256 digits shown as 64 hex digits, each 4-bit):

1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

It is important to understand the role of the keys, since dual key encryption is one of the technologies on which Bitcoin, as well as subsequent cryptocurrencies, has been built.

How?

In a videoconference where the keepers of the keys are kept anomynous, Bcademy will lead the three actors through the installation and set-up of the *multisig wallet*. Bcademy's role is to advise and assist, and in no circumstances Bcademy will become aware of or custody any of the keys. The relationship between **B**cademy and the three actors is regulated by contracts, and the design of **B**custody guarantees:

- The access to one's own capital, including the possibility to carry out daily operations
- The recovery of one's own capital following the loss or theft of one of the three keys
- An immediate intergenerational transfer, with no paperwork (simply the portfolio's value is redirected to a bitcoin address provided at the time of subscription to the service)
- Continuous assistance in the event of problems inherent the use of the software.

Who?

The key figures that make up the design of the service are:

- **The owner** who intends to secure his own capital while still being able to retain continuous access to it, increase the amount or transact, who will be the holder of the first key (OWNER)
- **A professional,** a lawyer or a **trusted individual** that the owner designates as the keeper of the second key (BROKER)
- A **B**cademy-designated **professional**, unknown to the holders of the other keys, keeper of the third key (LEGAL)

OWNER is the only formal and substantial holder of the cryptocurrency, ergo he is the full and exclusive owner and he makes use of the second and third actors (**BROKER** and **LEGAL**) exclusively for the conservation of two of the three private keys (one each). The second and third actors, simple custodians of information (the private key) that alone is insufficient to spend the cryptocurrency, do not have any relationship with each other and therefore cannot collude to transfer value. BROKER and LEGAL are unable, under any circumstances, to dispose of the custodied value, and their task is limited to the prudent and diligent retention of information and of its confidentiality.

The recipients of the service are therefore:

- **Professionals** (PRO) who manage clients' assets, covering in this case the role of the BROKER as described above. Managing wealth does not only mean growing it, but above all it means defending it from possible external interference, such as risk of inflation of national currencies, third parties credit actions, forced withdrawals, etc. Among the possible professionals that could create a point of access for the saver to the **B**custody service there are **all the actors authorised to collect money who can as of today leverage on a reputational value of trust for the final saver**. To this category belong **banks, asset management companies, real estate management company and any intermediary financial institution** that complies with category 107 and that therefore has due authorization. Such financial intermediaries offer investment products such as **Mutal Funds, Pension Funds, Life Insurance Policies and Asset Management** (the latter service for example is offered by Poste Italiane and digital platforms such as Moneyfarm) and could therefore consider to diversify their investment portfolio by allocating a part of the capital to bitcoin.
- **Business** (BIZ) that already accept bitcoins or that want to diversify their corporate assets, keeping them safe but retaining the possibility to freely access them for example to pay suppliers, salaries, etc.
- **Private individuals** (PRI) interested in the safe custody of their own bitcoin, without giving up the possibility of transacting them freely.

Various other actors should be considered, on the basis of their statute and legislation, such as **social security funds, private insurance funds and intercompany social security funds for employees and *family offices*.**

How much?

The *pricing* of the service, as it involves different variables, is defined according to customer needs, and is divided into:

- An activation fee (private or business)
- A third key holding fee (and possibly also of the second
- An annual fee for full assistance (for a pre-agreed amount of hours)

The service fee differs for private customers and companies based on specific needs.

Specials

For those new to the Bitcoin system, buying bitcoins is always a first obstacle. Bitcoin can be purchased in several ways, via BATM (bitcoin-ATM), online through portals with different features and more or less reliable and with variable fee levels.

Bcademy offers **B**custody's buyers an extremely simple way to buy bitcoin, taking care
of the entire process and directly depositing the desired sum on the multisig wallet of the owner, applying extremely competitive commissions compared to the market.

Additional purchases can be made at any time, safely and without taking the risk of disclosing information to the various providers on the network, avoiding a priori the possibility of running into frauds and / or blocks by the banking system and the regulator.

The **B**cademy team remains available to collaborate and / or customise the service.

Bcademy
Product development
bcustody.net