Bcademy

#CRYPTOKNOWLEDGE

Bcustody ₿

22|03|20

Cosa?

Bcustody è un servizio offerto da **B**cademy che permette di mettere in sicurezza i propri bitcoin grazie alla custodia delle chiavi private garantita da un design originale. Questo design non solo permette di mettere in sicurezza il proprio valore, ma anche di accedere ad esso, dunque spenderne una parte, in qualsiasi momento, mantenendo in sicurezza il resto.

Bcustody si basa sull'installazione di un *wallet multisig* (una funzione presente nel protocollo bitcoin), letteralmente un portafoglio che richiede più di una firma (multi-firma) per poter transare il valore presente, dove ogni firma è associata ad una diversa chiave (nella fattispecie 2 su 3).

Il core del servizio si basa su:

- **consulenza nell'installazione e nel setting del software** (wallet multisig), garantendo una creazione e distribuzione sicura delle chiavi
- **consulenza nell'installazione e nel setting di un wallet semplice**, creazione e mantenimento di un indirizzo bitcoin (dove far dirigere il valore in caso di decesso del cliente o interruzione del servizio)
- **formazione e documentazione** relativamente all'uso di entrambi i wallet
- **assistenza in caso di problematiche** relative all'uso del wallet multisig
- **custodia della terza chiave** per mezzo di un professionista (notaio, commercialista o avvocato)
- **assistenza nello spostamento del valore in caso di perdita di una delle tre chiavi,** grazie alla creazione di un nuovo wallet e conseguente creazione e distribuzione delle tre (nuove) chiavi
- **assistenza nello spostamento del valore in caso in caso di decesso del cliente o interruzione del servizio**, sull'indirizzo collegato al wallet semplice (punto 2)

Perché?

A differenza dell'ambito bancario tradizionale , dove chi custodisce valore ne diviene anche proprietario (art. 1834 del Codice Civile), mentre il conferente rimane un mero depositario, **in Bitcoin grazie alla crittografia a doppia chiave la proprietà è definita esclusivamente dal possesso della chiave privata**. Questa è una caratteristica fondamentale nelle crittovalute, poiché esclude categoricamente che qualcuno non in possesso della chiave privata possa bloccare o spendere valore. Ma genera altresì un problema: **nel caso venga perduta la chiave privata non vi è modo di accedere al proprio valore, che diviene letteralmente inaccessibile**.

La funzione multisig, letteralmente multifirma (*multisignature*) implica che per spendere qualsiasi somma di valore non sia sufficiente la firma generata da una chiave privata, ma un numero *n su m* di firme, solitamente *2 su 3*. Attraverso questa funzione dunque, correttamente inserita in un design strutturato e con differenti player, **è possibile superare il trade-off tra sicurezza (di non perdere o vedersi spostato o bloccato il proprio valore) e riservatezza (di poter accedere al proprio valore *bypassando* un intermediario malevolo)**.

Dove?

La dicitura *wallet* non sarebbe appropriata, poiché più che un portafoglio un wallet è un *portachiavi*. **Di fatto i bitcoin non sono custoditi all'interno di un wallet, ma sono informazioni custodite all'interno di un registro distribuito, una struttura dati chiamata *blockchain*. L'accesso a queste informazioni, inteso come la possibilità di transare i propri bitcoin è definita dal possesso di una chiave: la chiave privata permette di spendere i bitcoin inviati in precedenza ad un determinato indirizzo associato alla chiave stessa.**

La crittografia a doppia chiave, privata e pubblica, è la base del funzionamento delle crittovalute. La chiave privata, una stringa alfanumerica generata randomicamente, è la chiave che garantisce la capacità di spesa del proprio valore. La chiave pubblica, generata dalla chiave privata attraverso una funzione unidirezionale (ergo da una chiave pubblica non è possibile ricostruire la chiave privata, mentre è sempre possibile il contrario) è la chiave che viene utilizzata per generare a sua volta gli indirizzi bitcoin, ovvero i luoghi dove ricevere e verso cui inviare valore, e che dunque possono essere condivisi liberamente. Detto in altri termini: la chiave privata è necessaria per inviare valore (spendere denaro) mentre la pubblica per ricevere valore (accumulare denaro).

Banalizzando il concetto, è possibile pensare alla chiave privata come ad una password per spendere il proprio denaro. Una chiava privata ha la seguente forma, mostrata nella sua rappresentazione esadecimale (256 cifre mostrate come 64 cifre esadecimali, ognuna da 4 bit):

1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

È importante capire il ruolo delle chiavi, poiché la crittografia a doppia chiave è una delle tecnologie su cui è stato costruito Bitcoin così come le successive crittovalute.

Come?

In una videoconferenza dove i custodi delle chiavi vengono mantenuti autonomi Bcademy guida le tre figure nell'installazione e nel setting del *wallet multisig*. Il ruolo di Bcademy è quello di consulenza e assistenza, in nessun caso entra in possesso o a conoscenza di nessuna delle chiavi. Il rapporto tra **B**cademy e le tre figure è normato da contrattualistica, e il design di **B**custody garantisce:

- L'accesso al proprio valore, compresa la possibilità di effettuare operazioni quotidiane
- Il recupero del proprio valore anche a fronte della perdita o del furto di una delle tre chiavi
- Un passaggio generazionale immediato, avulso da pratiche burocratiche (semplicemente il valore viene rediretto su un indirizzo bitcoin fornito al momento della sottoscrizione al servizio)
- L'assistenza continua in caso di problematiche inerenti l'utilizzo del software.

Chi?

Le figure chiave che compongono il design del servizio sono:

- **Il proprietario** che intende mettere in sicurezza il proprio valore mantenendo la possibile di accedere costantemente ad esso, incrementandone l'ammontare o transandolo, detentore della prima chiave (OWNER)
- **Un professionista**, legale o semplicemente **una persona di fiducia** che il proprietario designa come custode della seconda chiave (BROKER)
- **Un professionista** designato da **B**cademy, sconosciuto ai detentori delle altre chiavi, custode della terza chiave (LEGAL)

OWNER è l'unico intestatario, formale e sostanziale, della crittovaluta, ergo ne è pieno ed esclusivo proprietario e si avvale della seconda e terza figura (**BROKER** e **LEGAL**) esclusivamente per la conservazione di due delle tre chiavi private (una per ciascuno). La seconda e terza figura, meri custodi di un'informazione (la chiave privata) che da sola è insufficiente per disporre della crittovaluta, non hanno rapporti tra loro, ergo non possono colludere per spostare valore. BROKER e LEGAL non sono in grado, in nessun caso, di disporre del valore custodito, ed il loro compito è limitato alla prudente e diligente conservazione dell'informazione, della sua riservatezza.

I destinatari del servizio sono dunque:

- **Professionisti** (PRO) che si occupano di gestire il patrimonio dei propri clienti, ricoprendo in questo caso il ruolo sopra definito BROKER. Gestire un patrimonio non significa soltanto farlo crescere, ma soprattutto difenderlo da possibili interferenze esterne, quali i rischi di inflazione delle valute nazionali, azioni creditorie di terzi, prelievi forzosi, etc. Tra i potenziali professionisti che potrebbero costituire un punto di accesso per il risparmiatore al servizio **B**custody vi sono **tutti i soggetti autorizzati alla raccolta di denaro che possano ad oggi spendere un valore reputazionale di fiducia per il risparmiatore finale**. A questa categoria appartengono **Banche, SGR, SIM e comunque ogni intermediario finanziario** che risponda alla categoria 107 e che quindi ne abbia debita autorizzazione. Tali intermediari finanziari offrono prodotti di investimento quali **Fondi Comuni d'Investimento, SICAV, Fondi Pensione, Polizze Vita e Gestioni Patrimoniali** (servizio quest'ultimo ad esempio offerto da Poste Italiane o da piattaforme digitali quali ad esempio Moneyfarm) e potrebbero quindi considerare di diversificare gli investimenti allocando una parte del capitale a bitcoin
- **Business** (BIZ) che già accettano bitcoin o che desiderano diversificare i propri asset aziendali, mantenendoli in sicurezza ma mantenendosi la possibilità di accederne liberamente ad esempio per pagare fornitori, stipendi, etc.
- **Privati** (PRI) interessati alla custodia sicura del propri

bitcoin, senza rinunciare alla possibilità di disporne liberamente.

Vanno valutati, in base allo statuto e alla normativa anche soggetti diversi quali, ad esempio, **Fondi previdenziali e assicurativi privati e Fondi interaziendali previdenziali di accantonamento per i dipendenti e *family offices***.

Quanto?

Il *pricing* del servizio, implicando differenti variabili, si definisce a seconda delle esigenze del cliente, ed è diviso in:

- Un canone di attivazione (privato o business)
- Un canone di tenuta della terza chiave (ed eventualmente della seconda)
- Un canone annuo di assistenza completa (per un monte ore)

Il canone di servizio si differenzia per clienti privati e imprese in base alle esigenze specifiche.

Specials

Per chi è nuovo al sistema Bitcoin l'acquisto di bitcoin è sempre un primo scoglio. Questo può avvenire in diverse modalità, dai BATM (bitcoin-ATM) all'acquisto online tramite portali dalle differenti sfumature, più o meno affidabili e dalle fees molto variabili.

Bcademy offre agli acquirenti di **B**custody una via estremamente semplice per acquistare bitcoin, occupandosi dell'intero processo e depositando direttamente sul wallet multisig del proprietario la somma desiderata, applicando delle commissioni estremamente minori rispetto al mercato.

Ulteriori acquisti possono essere inoltre effettuati in qualsiasi momento, in maniera sicura e senza correre rischi di divulgare informazioni ai vari provider in rete, evitando a priori la possibilità di incappare in frodi e/o blocchi da parte del sistema bancario e del regolatore.

Il team di **B**cademy rimane disponibile a proposte di collaborazione e/o eventuali customizzazioni del servizio.

Bcademy
Sviluppo Prodotto
bcustody.it