Associazione dei Professionisti di Banca AnalisiBanka

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

DEPOSITI BANCARI, WALLET E CRIPTOMONETE

prof. Salvatore Carrano

Febbraio 2018

"Sicuro come in banca": è una frase che si soleva dire quando il denaro risparmiato e depositato in un'azienda di credito non destava nessuna preoccupazione di disponibilità e di rientro. E in effetti, dagli anni successivi al secondo dopoguerra, in Italia ma anche negli altri paesi più industrializzati, non c'è stata notizia che un risparmiatore avesse perso il proprio denaro depositato in banca. Sicuramente la protezione attuata attraverso il fondo di garanzia che, di fatto, esclude i depositi fino a centomila euro da qualsiasi rischio di perdita sia in caso di *bail in* e sia in caso di liquidazione coatta amministrativa, ha contribuito significativamente ad accrescere, o almeno a confermare, la fiducia dei risparmiatori nella capacità di rimborso delle banche. La recente crisi finanziaria e il fallimento di qualche azienda di credito hanno però indotto i risparmiatori a diversificare l'investimento delle somme tesoreggiate orientandole verso beni immobili, titoli azionari, beni preziosi e altro ancora. Inoltre, l'assenza di remunerazione dei depositi spinge i risparmiatori alla ricerca di investimenti, magari meno protetti e più a rischio, ma potenzialmente più vantaggiosi in termini di rendimento. Così, nonostante una raccolta bancaria che in Italia supera

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

nel 2017 i 1700 miliardi, qualcosa come 500 miliardi di euro, da ogni parte del mondo, sono segretamente e attentamente custoditi in un "portafoglio" nella speranza che con il tempo e con delle circostanze favorevoli possano tanto lievitare com'è successo con i bitcoin. Questi speciali portafogli, tuttavia, non hanno nessuna somiglianza materiale con quegli eleganti e rassicuranti oggetti di pelle che servono a contenere delle banconote e possono essere dei semplici *accounts*, un pezzo di carta con sopra stampati due codici *Qr* e dei caratteri, oppure un software da installare o ancora, quando si tratta di qualcosa di materiale, anche piccoli oggetti che a prima vista possono essere tranquillamente confusi con delle *pen drive*. Sono i *wallet*s, servono a dimostrare la proprietà delle criptovalute consentendone anche la gestione. I *wallet*s non possono contenere valuta come un normale portafoglio, ma si limitano a custodire (memorizzare) le chiavi pubbliche e private che sono indispensabili, rispettivamente, per ricevere e inviare denaro. La chiave pubblica assolve all'incirca la stessa funzione di un iban e viene utilizzata come indirizzo dove inviare le valute digitali. A differenza di un iban, però, conoscendo la chiave pubblica e il tipo di valuta, volendolo, chiunque può curiosare nell'*address* corrispondente alla chiave pubblica e avere informazioni sulle movimentazioni in esso avvenute; ed è soprattutto per questo motivo che si preferisce usare più indirizzi come deposito anche riferiti a una stessa criptomoneta.

La chiave segreta è l'indispensabile "firma" che consente di disporre dell'ammontare in criptovalute contenuto in un indirizzo pubblico.

Conviene ricordare che possedere delle criptovalute non significa avere banconote, preziosi o titoli; si possiede solo una chiave di accesso che attribuisce la proprietà di

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

una transazione di un determinato importo, ricevuta in una determinata data, inviata da uno specifico indirizzo e registrata in un blocco della *blockchain*.

Si potrebbe immaginare la *blockchain* come un'indefinita stanza con dentro tante inviolabili casseforti, ordinate a blocchi, nelle quali sono contenute tutte le transazioni avvenute per una specifica criptovaluta. Per disporre del contenuto di queste casseforti è necessario essere in possesso dell'unica chiave che consente di aprirle. Perdere la chiave privata, o in alcuni casi l'ordinata sequenza dei caratteri utilizzati per generarla, significa perdere definitivamente la possibilità di ritirare l'ammontare in criptovalute posseduto. Prima di investire in una valuta digitale conviene, perciò, munirsi di un *wallet* e, in base alle movimentazioni che si intende compiere con l'investimento, sceglierne la tipologia fra le quattro esistenti che sono:

- *Web wallet*;
- *Desktop wallet*;
- *Paper wallet*;
- *Hardware wallet*.

I primi sono i più semplici, sono i più diffusi tra chi compie frequenti operazioni di investimento in valute digitali e sono i meno sicuri. La semplicità di utilizzo è dovuta alla possibilità di gestire direttamente da un *exchange* e tramite *account* la movimentazione delle criptovalute. La scarsa sicurezza deriva, invece, dal mancato possesso della chiave privata che viene utilizzata direttamente dall'*exchange* ogni volta che si compie un'operazione di prelievo o trasferimento di moneta digitale. Per

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

aumentare la sicurezza, alcuni *exchange* offrono agli utenti l'autenticazione a due fattori (password e codice telefonico), ma se l'*exchange* smette di funzionare, decide di utilizzare le chiavi private a proprio piacimento oppure viene *hackerato*, si corre il serio rischio di subire delle truffe. In sostanza, la sicurezza di non essere derubati si misura unicamente con l'affidabilità della piattaforma di *trading* scelta e l'utente, delegando quest'ultima alla custodia della chiave privata, per la sicurezza del suo deposito in criptovalute può contare unicamente sull'affidabilità dell'*exchange*. Appare ovvio, quindi, che chiunque decida di dedicarsi a un investimento di tipo speculativo in criptovalute, per aumentare la propria sicurezza, debba porre attenzione nella scelta dell'*exchange* da utilizzare. Attualmente alcuni tra i più conosciuti e affidabili *exchange* di criptovalte sono: Coinbase, Binance, Kraken, Bittrex e Spectrocoin.

I *desktop wallet* sono dei programmi che si installano sui computers e consentono di generare e custodire gli indirizzi alfanumerici delle chiavi pubbliche e di quelle private. Rispetto ai *web wallet*, i *desktop wallet* sono utilizzabili unicamente con il dispositivo (*pc*, *smartphone o tablet*) sul quale sono installati e consentono di ricevere e inviare le criptovalute senza connettersi a un *exchange*. La sicurezza di un *desktop wallet* è proporzionale alla sicurezza dell'ambiente in cui è stato installato e all'isolamento da contatto con altri computer. Un pc senza virus, utilizzato unicamente per le operazioni con le criptovalute e mai connesso in rete, offre una sicurezza elevatissima. Tuttavia, per eseguire un trasferimento in valute digitali è necessario essere connessi a internet e ciò espone il *wallet* al rischio di sottrazione della chiave privata. In ogni caso utilizzando un *desktop wallet* installato su un pc,

che dopo il download e prima ancora dell'installazione sarà sempre *offline*, insieme a un secondo *wallet*, con la chiave pubblica importata dal *wallet offline*, con la firma disabilitata e che servirà solo per ricevere valuta digitale, si può ottenere un margine di sicurezza pressoché assoluto.

Volendo, con l'utilizzo di due computers, si potrà sempre inviare criptomoneta dal *wallet* installato sul pc online, ma la transazione firmata sarà importata, tramite penna usb, dal *wallet offline* e, quindi, senza esporre la chiave privata ai rischi della rete.

Solitamente questi portafogli dopo l'installazione necessitano di un'attenta configurazione che si riesce a ottenere con una preventiva lettura di qualche (meglio leggerne più di una) guida che, tra l'altro, non sempre è scritta nella nostra lingua. Ragion per cui, la gestione di questi portafogli richiede anche una certa competenza informatica e una comprensione della lingua inglese. I consigli e i *link* per il *software* (*wallet*) da scaricare e installare sono contenuti nel sito della valuta che si intende comprare; conviene fidarsi delle indicazioni e utilizzare un portafoglio già testato e approvato dal team informatico che ha creato la valuta.

Di norma serve un *wallet* per ogni criptomoneta, ma esistono anche dei *wallet* multivaluta che consentono la gestione di più monete digitali. Exodus è uno dei più utilizzati *wallet* multivaluta e permette di conservare circa trenta monete digitali tra le quali bitcoin ed Ethereum.

Nella stessa categoria cui appartengono i *desktop wallet*, è possibile catalogare i *mobile wallet* che sono delle applicazioni che si installano su di uno smartphone e

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

consentono di ricevere, inviare e prelevare criptovalute direttamente con il cellulare e senza utilizzare il computer.

I *paper wallet*, com'è facile dedurre dal loro nome, sono dei fogli di carta con sopra stampato i caratteri delle due chiavi e i codici *Qr*. Sono utilizzati da cassettisti che perseguono obiettivi di investimento a lungo termine e, quindi, non intendono compiere frequenti movimentazioni in criptovalute. E, d'altronde, i *paper wallet*, essendo solo dei fogli di carta, non offrono la possibilità di inviare o prelevare moneta digitale e per farlo si deve ricorrere a una delle altre tre tipologie di *wallet*. Se creati osservando scrupolosamente le dovute precauzioni, i *paper wallet* offrono un grado di sicurezza elevatissimo e l'unico rischio di essere frodati può derivare dalla sottrazione materiale del foglio che contiene stampato il codice della chiave privata. La primaria precauzione da osservare dopo essersi collegati al sito per creare o scaricare il *paper wallet*, è di scollegarsi da internet per generare e stampare le chiavi; così facendo si evita il rischio di essere "spiati". Se i *paper wallet* hanno il vantaggio di offrire un'elevata sicurezza perché le chiavi sono memorizzate su carta e non sul *pc*, questo stesso punto di forza rappresenta, però, un limite notevole in termini di gestione delle criptomonete. Dopo aver generato un *paper wallet*, infatti, si può solo ricevere e per inviare o prelevare occorre inserire la chiave privata in un *web wallet* o importarla in un *desktop wallet*. Quando si decide di utilizzare la chiave privata memorizzata su un foglio di carta, più che all'importazione, è preferibile ricorrere allo *sweeping* (spazzamento) che consiste nell'inviare l'intero ammontare in criptomonete memorizzato nell'indirizzo da "spazzare" in un nuovo *address* che avrà associata un'inedita, e più sicura, chiave privata.

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

Praticità e sicurezza sono coniugate nei *wallet hardware* che offrono la possibilità di conservare le criptomonete possedute e di effettuare anche operazioni di invio o di prelievo. Questi *wallet* supportano nativamente una ventina di monete digitali ma, installando una specifica applicazione, è possibile utilizzarli con altre criptovalute ERC20 (*Ethereum token standard*). Prima dell'acquisto è comunque buona regola interrogare la lista completa delle criptomonete supportate, presente sul sito del *wallet hardware* che si intende comprare, per verificare quali valute compaiono. I dispositivi in questione, per effettuare le transazioni, hanno bisogno di essere collegati a un computer tramite porta usb con un processo di installazione (necessario solamente al primo collegamento) che risulta, comunque, elementare e sbrigativo. È fondamentale annotare e conservare con cura l'ordinata sequenza delle 24 parole inserite al termine dell'installazione perché, in caso di rottura, perdita o furto del dispositivo, questa "*recovery phrase*", rappresenta l'unica possibilità per il suo ripristino. Gli accessi *all'hardware wallet* successivi al primo sono preceduti dall'autenticazione tramite l'inserimento del *PIN* scelto durante l'installazione; in caso di *PIN* errato, dopo il terzo tentativo, il dispositivo si autoresetta.

Le transazioni, anche se eseguite tramite un *pc* collegato in rete, devono sempre essere confermate manualmente premendo uno dei tasti presenti sul piccolo dispositivo; quest'autenticazione a due fattori aumenta la sicurezza del portafoglio perché rende molto improbabile, ma non impossibile, un attacco *hacker* di tipo "*man in the middle*" mirato all'intercettazione di *password* e chiave privata. Trezor e Ledger Nano sono gli *hardware wallet* più utilizzati; i due dispositivi, pur diversi nella forma, hanno dimensioni e caratteristiche di funzionamento simili.

Registrazione Atto sociale Agenzia delle Entrate Milano il 03/03/2016
- Codice Fiscale 93549790157
- www.analisibanka.it

Portafogli di ogni tipo che si adattano alle esigenze degli investitori in criptovalute e promettono, alcuni più e alcuni meno, adeguata protezione delle monete digitali che devono custodire. In fondo i *wallet* sono degli strumenti, essenziali e indispensabili, ma pur sempre strumenti che servono per proteggere e disporre la proprietà di una transazione depositata in una rete che gestisce un database decentralizzato.

Riflettendo, sembrerebbe che la moneta resti affezionata e fedele a chi la origina: le banconote, create da una banca, prediligono il luogo natio e in esso principalmente si depositano. Le criptomonete nascono da un computer, restano lì e mai andranno altrove, potrà cambiare solo il soggetto che ne godrà della disponibilità mediante un *wallet*. Se le valute digitali avranno il sopravvento sulle monete fiat allora cosa potrà accadere?