TRUST IMPRESA FAMIGLIA

Rivista trimestrale
Anno II • N. 1 / aprile 2023

In copertina opera di Mario Rigamonti
Perso nel bosco

fd Riviste

Rivista registrata: Tribunale di Bologna 22.07.2021, n. 8571
ISSN: 2785-2822

inFOROmatica S.r.l., Via Castiglione, 81, 40124 Bologna
inforomatica.it

tel. 051 9843125 - fax 051 9843529
commerciale@filodiritto.com
segreteriariviste@filodiritto.com

Progetto fotografico di © Mario Rigamonti – *Perso nel bosco*

© Mario Rigamonti – *Perso nel bosco*

Trust interno di criptovalute: un approccio critico – II parte

Cryptocurrencies held on trust in the internal system: a critical approach – II part

di *Salvatore Tramontano* e *Carola Cinetto*

ABSTRACT

La seconda parte di questo contributo, senza alcuna pretesa di fornire una soluzione operativa, prende in considerazione i problemi legali e pratici che i trustee devono affrontare quando il fondo in trust è composto anche da criptovalute.

The second part of this contribution, without any claim to provide an operational solution, considers the legal and practical problems that trustees have to face when the trust fund is also made up of cryptocurrencies.

Sommario

Summary

1. Premessa

L'ingresso delle transazioni in criptovalute, sotto forma di dotazione o incremento del fondo, presenta criticità di notevole entità anche nell'ambito del diritto dei trust. **In particolare, la detenzione in trust di criptovalute si traduce per il trustee in una duplice sfida riconducibile, da un lato, alla connaturata volatilità che contraddistingue la maggior parte delle valute virtuali, dall'altro, all'esigenza di custodire in modo sicuro queste "*novel technologies*" assumendo, di conseguenza, rischi non convenzionali**.

Oggettive difficoltà riguardano, inoltre, il c.d. "pseudo-anonimato" intrinseco del possesso di valori digitali che circolano nell'ecosistema cripto nel momento in cui detta caratteristica si confronta con il regime normativo dei controlli antiriciclaggio in ottemperanza del quale il trustee è tenuto ad operare.

2. Volatilità

In quanto mero costrutto di tipo informatico, privo di un intrinseco valore, diretto e indiretto, e slegato da una sottostante attività economica reale, **la criptovaluta poggia la sua valutazione su di una fonte esclusivamente esterna, condizionata dal volume di scambi con altre valute e rispondente ad una logica di domanda-offerta fortemente instabile, caratterizzata da operazioni**

(troppo) spesso speculative di tipo "*buy and hold*" e priva di qualsiasi supporto istituzionale: invero, in una rete decentralizzata di utenti di criptovalute, basata su di un protocollo di tipo *blockchain,* manca, per definizione, un intermediario od emittente centrale incaricati di stabilizzare, mediante politiche monetarie *ad hoc*, il valore della valuta virtuale. Ne discende, inevitabilmente, una elevata volatilità di breve periodo della risorsa digitale alla quale si accompagna, di riflesso, un corrispondente potere d'acquisto profondamente mutevole e poco prevedibile nel tempo.

Non stupisce, dunque, se il fenomeno cripto, etichettato ormai comunemente come l'archetipo informatico di una dimensione – "bolla" – altamente speculativa, rappresenti per qualunque trustee una realtà "*uncomfortable*", scomoda.

Invero, come può il trustee esercitare un'attività gestoria connessa ad un mercato nuovo, altamente speculativo e volatile, come quello virtuale, agendo nel contempo in ossequio al "*duty of care*" al quale è improntato lo svolgimento del suo ufficio?

Entrando più nello specifico, il trustee che accetti criptovalute, in dotazione o sotto forma di incremento del fondo in trust, o che consideri affidabile "investire" i beni in trust nella sfera cripto, sarebbe in grado di coniugare la gestione di valori, dalla natura giuridica attualmente incerta ed aperta[1] e caratterizzati da un rapporto rischio(volatilità)-rendimento non ponderabile, con il dovere di salvaguardare il fondo in trust preservandone l'integrità (e incrementandone, ove possibile, il valore) in funzione dell'attuazione del programma negoziale imposto dal disponente?

In verità, l'impressione che si ha è quella di trovarsi di fronte ad un ossimoro.

La questione, d'altro canto, non ha un'implicazione puramente teorico-astratta: il mancato rispetto dell'obbligo da parte del trustee di preservare la consistenza dei beni in trust può, come noto, integrare un'ipotesi di violazione della fiducia, *breach of trust*, con conseguente responsabilità patrimoniale a suo carico e, se del caso, correlativa condanna personale mediante revoca del medesimo trustee e nomina di un nuovo trustee.

3. Custodia

La salvaguardia del patrimonio in trust ricomprende, a cascata, uno specifico dovere di custodia: il trustee è tenuto a proteggere i beni in trust conservandone l'integrità, sia materiale che giuridica, e curando che siano assicurati qualora si tratti di beni soggetti ad andare perduti o ad essere danneggiati.

È evidente come la custodia delle risorse virtuali detenute in trust comporti per il trustee un'ulteriore sfida, la cui dinamica si presenta, se possibile, ancor più delicata e complessa, in quanto reclama la sicurezza delle chiavi crittografiche, pubblica e privata, gestite in un portafoglio digitale, necessarie per movimentare le unità di conto virtuali ad esse associate.

Ebbene, dal momento che il possesso della chiave privata equivale nella sostanza ad esercitare il controllo sulle transazioni in criptovalute, il trustee è tenuto ad acquisire una **solidità infrastrutturale, giuridica e tecnologica**, indispensabile per prevenire o (almeno) circoscrivere il rischio di subire ingenti e irreversibili perdite economiche in danno del fondo in trust, cagionabili tanto da eventi intenzionali (basti pensare, ad esempio allo smarrimento della perdita dal parte del trustee della chiave privata o al verificarsi di un guasto nel funzionamento della stessa[2]), quanto da eventi intenzionali, come l'attuazione di condotte fraudolente e malevoli di terze parti, intermediarie e non (*ex multis* furti informatici, attacchi *hacker, malware*).

Sotto un profilo giuridico sarebbe d'aiuto, anche se certamente non risolutivo,

[1] Almeno alla stregua del nostro ordinamento giuridico.

[2] Non esistono, infatti, autorità centrali che "registrino" le chiavi privati o ne possano emettere altre in sostituzione.

predisporre coperture assicurative specifiche e mirate. Al riguardo, il settore assicurativo italiano si è dimostrato estremamente cauto e poco ricettivo, per non dire riluttante; **né risposte più soddisfacenti sono giunte dal mercato internazionale: recentemente, gli esperti del team DART (*Digital Asset Risk Transfer*) di Marsh hanno descritto il mercato assicurativo delle criptovalute "*hesitant and uncertain*"**.

Sul piano informatico la conservazione delle chiavi private sembra, invece, aver trovato maggiori garanzie di sicurezza attraverso l'adozione di portafogli digitali che implementano un sistema c.d. multi-firma (*multi-sig*), ovvero un protocollo che richiede l'utilizzo di più chiavi private, e quindi più firme, per validare le transazioni: devono essere impiegate m-di-n[3] (*m-of-n*) chiavi private affinché dette transazioni vengano autorizzate.

L'impiego della funzione *multi-sig* con ridondanze presenta due fondamentali vantaggi: rende il portafoglio digitale meno vulnerabile e permeabile da reati informatici[4] e riduce, allo stesso tempo, la sua dipendenza dal singolo utente[5]. **In questo modo, nell'ipotesi in cui si verificasse lo smarrimento o il furto di una delle chiavi private o il decesso di uno dei possessori, il valore digitale associato non andrebbe perduto, ma potrebbe essere "recuperato" mediante le chiavi private rimaste e non corrotte senza, quindi, alcun nocumento patrimoniale per l'utente**[6].

Nel caso di gestione in trust di criptovalute, si potrebbe ricorrere ad un protocollo *multi-sig* 2:3, basato cioè su 3 (tre) chiavi private, affidate a tre soggetti distinti; condizione necessaria e sufficiente per effettuare validamente una transazione è la disponibilità di (solamente) 2 (due) chiavi su 3 (tre), l'una nel possesso del trustee, la seconda del guardiano. Ne scaturisce che se il trustee non è in grado di gestire autonomamente le risorse digitali senza la firma e, quindi, il controllo del guardiano, a sua volta, il guardiano, nella sua qualità, può autorizzare una transazione in criptovalute o rifiutare la sua validazione ove ne riscontrasse la contrarietà ai dettami contenuti nell'atto istitutivo.

Una soluzione progettuale di questo tipo sembra replicare in linea teorica la dinamica del rapporto che si instaura tra il trustee, proprietario e gestore fiduciario dei beni in trust, e il guardiano, soggetto preposto a collaborare e a vigilare sull'attività del primo "affinché l'affidamento trovi il proprio felice compimento"[7].

Ad uno sguardo più attento, tuttavia, la realtà dei fatti è cosa ben diversa. Nell'ambiente *bitcoin* frequente è l'asserzione secondo la quale il possesso della chiave privata costituisce titolo di proprietà delle valute virtuali ad essa associate[8]; ma se ciò è vero, viene spontaneo chiedersi: **il guardiano, che ha la gestione e, quindi, il controllo diretto su una delle chiavi private, potrebbe essere considerato (co)proprietario, del pari e unitamente al trustee, delle criptovalute detenute in trust? Conseguentemente, la sua veste non dovrebbe essere più correttamente riqualificata, in fatto e in diritto, nei termini di co-trustee?!**

A ciò si aggiunga un'ulteriore questione, spinosa e di non semplice soluzione: **a chi e in quali termini affidare la terza chiave così da superare il *trade-off* tra la sicurezza di non perdere o vedere "spostato" o bloccato il valore digitale e la riservatezza di potervi accedere (bypassando eventuali**

[3] "M" rappresenta il numero richiesto di firme; "n" il numero totale delle firme della transazione.

[4] La tecnologia integrata in questi portafogli riduce il numero di potenziali punti di errore che gli *hackers* incontrano.

[5] E dal singolo dispositivo.

[6] Questo *backup* di ridondanza del portafoglio è la differenza di "n" meno "m".

[7] M. Lupoi, "Trusts", Milano, 2001, pag. 402.

[8] Letteralmente "*not your keys, not your coins*". In realtà sulla valenza giuridica da attribuirsi al possesso delle chiavi crittografiche la dottrina è ancora divisa. Dubbi in proposito sono stati sollevati anche nel n. 3 di questa Rivista, 2022, pag. 6.

condotte malevoli o pregiudizievoli)? La soluzione più logica sarebbe – forse – che il trustee depositasse la terza chiave presso un "terzo garante", estraneo alla vita del trust, affidandone la custodia al limitato scopo di provvedere alla sua prudente e diligente conservazione. Conservata separatamente, la terza chiave potrebbe essere utilizzata in casi di emergenza, quali la perdita o il furto di una delle altre chiavi private, su richiesta congiunta del trustee e del guardiano.

Resta da capire chi designare quale custode della terza chiave: un fornitore di servizi, confidando nel suo *background* informatico o, piuttosto, privilegiare la scelta di un notaio, la cui funzione di "guardiano della certezza dei traffici giuridici" costituisce, *ex se*, una garanzia incontrovertibile?

4. Antiriciclaggio

Ultima, ma non per questo meno importante, criticità che il trustee si trova a dover affrontare in un trust di criptovalute, trova esplicitazione nel tentativo di conciliare l'assolvimento degli obblighi antiriciclaggio (D.Lgs. n. 231/2007 e sue successive modifiche ed integrazioni), improntati alla massima tracciabilità dei flussi economico-finanziari, con lo pseudo-anonimato criptovalutario.

Difatti la fisiologica garanzia della riservatezza e della sicurezza dei dati personali degli utenti che interagiscono sulla rete informatica propria della tacnologia *blockchain* mal si concilia con le finalità della normativa antiriciclaggio.

Se è pur vero che le operazioni in criptovalute sono totalmente tracciabili e pubbliche, nel rispetto dell'enunciato per cui "*the only way to confirm ... a transaction is to be aware of all transactions*"[9], è altrettanto vero che il registro transazionale *blockchain* poggia su di un regime di sostanziale opacità in ordine alla riferibilità di un'operazione in criptovalute ad un soggetto fisicamente identificato: le uniche "informazioni" accessibili in rete sono gli indirizzi dei *wallet* – pure sequenze alfanumeriche derivate algoritmicamente dalle chiavi pubbliche. Detti indirizzi sono associati univocamente alle criptovalute e utilizzati per definire dove si trovano tali valori, da dove provengono e dove vengono inviati.

Si può allora ben comprendere come questa tecnologia informatica sia d'ostacolo ad una adeguata profilatura del disponente/apportatore e, per l'effetto, frustri gli obblighi imposti dalla disciplina antiriciclaggio diretti a verificare l'origine lecita delle risorse digitale conferite in trust.

Inoltre, rende difficile verificare la coincidenza tra l'effettivo titolare del portafoglio digitale e colui che, nel concreto, ne dispone o effettua l'apporto. In quest'ottica, la possibilità di ricollegare l'utente al suo pseudonimo e ricostruire in totale trasparenza la catena di scambio delle transazioni sembra essere rimessa alla sola dichiarazione del disponente/apportatore[10].

Per ricostruire in modo completo il traffico dati delle transazioni in criptovalute, il trustee potrebbe affidarsi alle tecniche di "*digital forensic*", servizi complessi, molto onerosi e, purtroppo, non totalmente affidabili ed efficaci: molteplici sono infatti gli *escamotages* che la pratica informatica ha sviluppato negli ultimi anni allo scopo di raggirare lo pseudo-anonimato rendendolo, a tutti gli effetti, un vero e proprio "anonimato"[11]. Esistono, ad esempio, *software* di varia natura, diversamente nominati ("*anonymiser*", "*mixer laundry service o tumbler*", "*Tor*", etc.…), capaci di oscurare l'origine delle transazioni in criptovalute o confonderne i termini di identificazione.

---

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, in https://bitcoin.org/bitcoin.pdf.

[10] Minori difficoltà si pongono ove il disponente/apportatore abbia agito tramite *exchange*. In questi casi sembra infatti ritenersi ragionevolmente sufficiente dar prova dell'acquisto di criptovaluta attraverso l'esibizione del bonifico o della transazione con carta di credito effettuati in valuta tradizionale verso *exchange*. L'*exchange* e il *wallet provider*, a loro volta, sono assoggettati alla normativa antiriciclaggio.

[11] Alcune *Altcoin* – come *Monero e ZCash* – offrono di *default* sistemi di oscuramento delle operazioni consentendo agli utenti un anonimato pressoché totale.

Sembrano dunque mancare, al momento, validi strumenti che consentano di garantire sempre, con un certo grado di certezza, l'imputazione di un certo atto di disposizione criptovalutario ad un determinato soggetto.

5. Una considerazione conclusiva

Dalla disanima esposta sorge spontaneo un quesito conclusivo: in che modo un trustee, avveduto ed accorto, può venire a patti con le risorse digitali? Attualmente, l'unico dato certo – a parere di chi scrive – è che **occorre avvicinarsi alle transazioni criptovalutarie con consapevole prudenza e, possibilmente, con appropriate conoscenze. Per cui: "*caveat* trustee!"**.

© Mario Rigamonti – *Perso nel bosco*