di Lorenzo Savastano*

FOLLOWING THE (VIRTUAL) MONEY: IL VALORE PROBATORIO DELLE TRANSAZIONI ELETTRONICHE IMPRESSE SULLA BLOCKCHAIN

“Inseguire il denaro” è una lezione operativa ed un metodo investigativo che - attualmente - informa tutte le principali indagini a sfondo economico-finanziario. Oggi, tuttavia, l’impiego delle cc.dd. Distributed Ledger Technologies (DLT) per il trasferimento di capitali e l’oscuramento delle tracce della ricchezza criminale, impone un ripensamento degli schemi procedurali tradizionalmente impiegati dagli Organi investigativi: a partire dal corretto valore probatorio da assegnare alle transazioni elettroniche riportate in una blockchain nel corso di un procedimento giudiziario

1. Following the money… but where?

Nata nel campo della lotta al fenomeno mafioso, “**inseguire il denaro**” (“*follow the money*”) è oggi una regola investigativa ed un modello operativo alla base di tutte le principali indagini a sfondo economico-finanziario. La tenuta di tale assioma operativo è stata, tuttavia, messa alla prova dalla progressiva dematerializzazione (e contestuale) digitalizzazione dei flussi finanziari. Un fenomeno che – sospinto dalla globalizzazione dei mercati e dal progresso tecnologico – ha ora raggiunto il suo apice con la comparsa del denaro virtuale e dei cc.dd. *digital asset*: una modalità inedita, decentralizzata e quasi istantanea di trasferimento di capitali resa possibile dalla sottostante tecnologia *blockchain*.

Nel presente contributo, si tenterà di rispondere – dal punto di vista degli Organi investigativi – ad un problema di natura procedurale ma di carattere pregiudiziale nell’approccio all’investigazione finanziaria (e non solo):

quale valore assumono giuridicamente le transazioni riportate sul grande registro della *blockchain*?

2. *Prima di tutto: cos'è la blockchain*

La tecnologia *blockchain* è una particolare forma di *Distributed Ledger Technology* (DLT), ovvero un registro elettronico condiviso tra più utenti di un medesimo network informatico, i cui dati sono protetti sia tramite tecniche crittografiche che attraverso la c.d. ridondanza dei dati (copie delle stesse informazioni possono essere validate e archiviate presso tutti i partecipanti attivi al registro).
Nello specifico, si parla di *blockchain* perché le transazioni memorizzate sono raggruppate in una sequenza di "blocchi" collegati tra loro per via crittografica, creando così una registrazione in *ordine cronologico e non modificabile* di tutte le transazioni effettuate fino a quel momento.
Più in dettaglio, caratteristiche tecniche peculiari della *blockchain* sono:
- *la cifratura a chiavi asimmetriche*: consente di assicurare la paternità di un messaggio e la sua integrità, attraverso il diverso utilizzo di una chiave pubblica ed una chiave privata di cifratura (assegnate alla medesima entità/user);
- *un network peer-to-peer*: i singoli computer degli utenti operano come nodi della rete, agendo contemporaneamente da distributori e fruitori delle informazioni, eliminando in tal modo la presenza di un ente centrale che operi quale validatore delle varie transazioni ed eliminando – in tal modo – il rischio di una loro alterazione;
- *il principio della proof of work*: impiegato sia come meccanismo di *creazione del consenso* al fine della validazione delle transazioni, sia come strumento di incentivazione per i partecipanti a mettere a disposizione risorse computazionali, con ciò risolvendo, indirettamente, eventuali pericoli di condotte fraudolente all'interno del sistema.

L'insieme di queste tecnologie viene combinato nell'ormai celebre *paper* di Satoshi Nakamoto del 2008[1], descrittivo del protocollo di funzionamento del *Bitcoin*, un protocollo di comunicazione innovativo, che non solo funziona come un registro immodificabile, in cui le transazioni di *bitcoin* vengono iscritte attraverso il predetto meccanismo di consenso, ma che al contempo consente di evitare ab origine il problema di *double spending* (ovvero l'utilizzo plurimo delle stesse risorse), scoraggiando eventuali comportamenti illeciti.

In Italia esiste una definizione giuridica di DLT, ovvero di "*tecnologie basate su registri distribuiti*", contenuta nell'art. 8 *ter* della Legge 11 febbraio 2019, n. 12[2], ove la stessa è descritta come l'insieme delle "*tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*".
Esaltando la descritta funzione di *timestamp* propria delle *blockchain*, il successivo terzo comma della citata disposizione, sancisce che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce i medesimi effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (in avanti: Regolamento *eIDAS*).
Un testo normativo dal quale, quindi, occorre partire per esaminare l'eventuale ingresso dei dati, riportati all'interno di un registro DLT, nel procedimento penale.

3. Il valore probatorio del documento informatico

Allo scopo di istituire un mercato unico digitale all'interno dei confini politici dell'Unione europea, il citato Regolamento *eIDAS* introduce – tra gli altri – una serie di strumenti utili alla certificazione digitale di dati ed informazioni contenute in "*tracce elettroniche*".
Il riferimento è, nello specifico, alle categorie di "*firme elettroniche*": una peculiare procedura informatica di validazione dei dati nel cui alveo rientrano, oltre alla "*firma elettronica*" c.d. *pura* (dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare), anche la "firma elettronica avanzata" (firma elettronica connessa univocamente al firmatario, idonea ad identificarlo, creata con mezzi che il firmatario può utilizzare sotto il proprio esclusivo controllo e collegata ai dati sottoscritti in modo da poterne far rilevare l'eventuale modifica), nonché la "*firma elettronica qualificata*" (firma elettronica avanzata a cui è associato un certificato rilasciato da un prestatore di servizi qualificato).

Sul piano nazionale, il D. Lgs. 7 marzo 2005, n. 82 (*Codice dell'Amministrazione Digitale* - CAD), affianca infine a tali strumenti la c.d. "*firma digitale*", ovvero una tipologia di firma elettronica qualificata basata su un peculiare sistema di chiavi crittografiche.
Ciò posto, con riferimento al valore probatorio del documento informatico – validato con una delle predette procedure – all'interno dei procedimenti giudiziari, corre evidenziare come il Regolamento *eIDAS,* all'art. 25 (rubricato *"Effetti giuridici delle firme elettroniche*") stabilisca che "*a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per*

il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate".
Una regola procedurale, quest'ultima, mutuata in Italia nell'art. 20, comma 1 bis CAD, ove è disposto che il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 del codice civile (ovvero fa piena prova fino a querela di falso) "*[…] quando vi è apposta la firma digitale, altro tipo di forma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID … in modo da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivocabile la sua riconducibilità all'autore*".
In tutti gli altri casi, "*l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità*".
Più specificamente, l'apposizione di una firma elettronica sul documento produce l'effetto di c.d. "*marcatura temporale*", definito dalla Corte di Cassazione come "*il processo di generazione …, ad opera di una terza parte fidata, di una "firma digitale del documento" cui è associata l'informazione relativa ad una data e ad un'ora certa*"[3]. L'apposizione della marca temporale consente, così, di "stabilire l'esistenza di un documento informatico a partire da un certo istante e di garantirne la validità nel tempo, costituendo un servizio specificamente volto ad associare data e ora certe e legalmente valide ad un documento informatico, consentendo, quindi, di attribuirgli una validazione temporale opponibile a terzi"[4].
Un effetto giuridico, come evidente, molto simile alla descritta funzione di *timestamp* propria della tecnologia *blockchain*. Tuttavia, prima di approfondire se ed in quale misura una transazione riportata su un registro DLT possa essere considerato un documento informatico, il cui contenuto è certificato ai sensi dell'art. 20 CAD, occorre introdurre una fondamentale distinzione fra due tipologie di *blockchain*, basata, in particolare, sul peculiare modello di *governance* sottostante.

4. Il valore probatorio delle transazioni su *blockchain*

A seconda del modello di governo della rete da parte dei suoi utenti, si suole distinguere tra due tassonomie di DLT[5]:
- pubblica o *permissionless*, particolarmente utilizzata nel settore delle cc.dd. criptovalute (e.g. le *blockchain* di *Bitcoin* ed *Ethereum*), nelle quali ogni partecipante può fare accesso e operare nel *network* senza che sia necessario rendersi identificabile o essere previamente autorizzato.
Pertanto, le reti *permissionless* consentono l'accesso a ogni utente che decida di connettersi e partecipare, generando nuove transazioni, effettuando il compito di *miner* (processo di validazione e finalizzazione delle transazioni) o semplicemente leggendo il registro delle transazioni memorizzate;
- privata o *permissioned*, in cui è prevista la presenza di una "*Autorità centrale*" preposta alla validazione dei

nuovi blocchi della catena e che può decidere quale *node* può fare ingresso nella rete. Si tratta della tipologia di reti che opera prevalentemente per conto di una comunità che condivide un interesse comune, dove l'accesso al ruolo di *miner* è limitato ad un numero esiguo di individui considerati fidati (il livello di lettura del registro e di partecipazione nella generazione di nuove transazioni può essere soggetto a limitazioni o meno a seconda dell'organizzazione che controlla la rete).

Posta tale basilare distinzione, può dunque agevolmente evincersi come la validità "*giuridica*" delle transazioni su *blockchain* muti a seconda della tipologia di "*rete*" in cui sono impresse le transazioni.
Per quanto detto, difatti, nelle *blockchain* cc.dd. *aperte*, non essendo richiesta la previa identificazione degli utenti, sussiste un problema di riconducibilità della transazione ad un determinato soggetto, dal momento che le chiavi elettroniche non sono rilasciate da soggetti deputati al rilascio di certificati digitali (c.d. *Trust Service Provider*).
Per tale ragione, in tale tassonomia di DLT, appare non configurabile un'assimilazione della rilevanza probatoria delle transazioni a quella dei documenti sottoscritti con firma elettronica avanzata, non essendo equiparabili le chiavi crittografiche utilizzate nella *blockchain* a tale tipologia di firma elettronica. Varrà dunque, in tali casi, la regola della *libera valutazione del giudice*, che dovrà decidere sull'idoneità del soddisfacimento della forma scritta del documento sulla base dei parametri positivizzati nel richiamato comma 1 bis dell'art. 20 CAD.
Viceversa, nelle cc.dd. *blockchain permissioned*, la circostanza che l'accesso sia consentito solo a soggetti già identificati dalla piattaforma che rende disponibile la fruizione del registro informativo, consente di superare in maniera più lineare il problema dell'identificazione dei titolari effettivi delle chiavi crittografiche. Nelle soluzioni tecnologiche più avanzate sarà, quindi, possibile creare un sistema di firma elettronica avanzata con cui sottoscrivere le transazioni basate sulla *blockchain*, vestendo tali informazioni della dignità probatoria prevista dall'art. 2702 del codice civile.

5. Un nuovo vettore investigativo

Il ricorso ai protocolli informatici della *blockchain* per l'esecuzione del trasferimento di fondi ed *asset* finanziari, alla luce del peculiare funzionamento di tale tecnologia, sembra non solo aver proiettato la regola "*follow the money*" in uno scenario inesplorato per gli Organi delle indagini, ma anche aver mutato il naturale vettore investigativo del paradigma: sul registro della "*catena dei blocchi*" le informazioni da ricercare sono difatti pubbliche, ricercabili, trasparenti.
Nel prossimo futuro, dunque, il dilemma operativo in tale genere di investigazioni non sarà più (*semplicemente*) la ricerca degli indizi e delle tracce del denaro, quanto (*necessariamente*) la loro corretta interpretazione e la correlata valorizzazione operativa.

Capitano della Guardia di Finanza

Note

1- Una copia del documento in lingua italiana è disponibile sul sito bitcoin.org.
2- Di conversione con modificazioni del D.L. 14 dicembre 2018, n 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la Pubblica Amministrazione.
3 - Cassazione Civ. Sez. I Ord., 13 febbraio 2019, n. 4251.
4 - *Ibidem*.
5 - In materia, tra i vari contributi, si segnalano: POTENZA G., *Fintech e Blockchain*, in AA.VV. (a cura di CORAPI E. e LENER R.), *I diversi settori del Fintech. Problemi e Prospettive*, Milano, 2019, p. 76; ANNUNZIATA F. – CONSO A., *Le criptovalute nell'ordinamento italiano ed internazionale*, in AA.VV. (a cura di AVELLA F.), *Bitcoin e Criptovalute*, Milano, 2021, pp. 20 e ss.