La blockchain come base di funzionamento delle criptovalute

di Nomos

Pubblicato il 23 Luglio 2021

Negli ultimi anni le criptovalute hanno assunto sempre maggiore rilievo nell'economia globale, con un *"approccio"* a tale strumento anche da parte dei *"piccoli risparmiatori"*. Ed infatti ultimamente si assiste ad un andamento esponenziale nell'utilizzo e acquisto di queste *"rappresentazioni digitali di valore"*. Tuttavia al sempre maggiore utilizzo delle criptovalute corrisponde tuttora una scarsa regolamentazione di tale *"fenomeno"*, che determina delle forti criticità, sia a livello civilistico che, in particolar modo fiscale. Iniziamo a spiegare cosa è la blockchain e perché è la base di funzionamento delle criptovalute.

Le criptovalute[1] consistono in una forma di rappresentazione digitale di valore, che si basa sull'utilizzo della tecnologia informatica.

In linea generale esse si fondano su **una serie di regole** (il c.d. *"protocollo"*), tradotte in codice informatico, che specificano **il modo in cui i partecipanti possono effettuare** *"le transazioni"* **e compiere le operazioni**; il tutto (istruzioni e transazioni) risulta memorizzato su una nuova struttura dati decentralizzata detta **blockchain** (un registro c.d. *"ledger"*) che tiene traccia delle transazioni avvenute.

Si tratta di nuova **struttura decentralizzata** (costruita su una rete di computer connessi via internet – una rete c.d. *"peer to peer"*) che garantisce la corretta esecuzione delle transazioni senza dovere *"sottostare"* ad un sistema centralizzato o *"istituzionale"*.

Questo è il motivo per cui spesso le criptovalute vengono contrapposte a forme centralizzate di distribuzione di valore, come le banche o altre entità centralizzate.

Come riportato, la tecnologia alla base delle criptovalute risulta la **blockchain**, emersa con prepotenza dopo la pubblicazione nel 2008[2] di un *"whitepaper"* scritto da un autore (sotto lo pseudonimo di *Satoshi Nakamoto*) tutt'oggi sconosciuto, intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*".

Si tratta di una breve pubblicazione (9 pagine), tramite la quale sono state poste le basi del primo sistema di pagamento c.d. "*trustless*", il quale risulta basato in gran parte su tecnologie già note, ma che

risolve in modo brillante la possibilità di scambiarsi valore (in questo caso, bitcoin) in un ambiente decentralizzato (una rete di computer - peer to peer - dove tutti i partecipanti rivestono gli stessi ruoli), fornendo una soluzione al problema del *"double spending"* (senza dovere utilizzare un sistema centralizzato per la convalida delle transazioni) ovvero della **possibilità per il possessore di una criptovaluta di non spenderla più di una volta.**

In effetti, mentre per quanto riguarda le banconote è molto difficile creare una copia identica all'originale, quando si tratta di informazioni digitali tutto ciò diventa molto più semplice. Si pensi a come risulta facile duplicare un file o inviare la stessa email a più persone.

L'esigenza di non dipendere dal sistema bancario ufficiale per potersi scambiare *"valore"* è stata amplificata negli anni della crisi dei *"subprime"* a seguito della bancarotta di Lehman Brothers e di salvataggi eccellenti dove, **seguendo l'assioma del** *"too big to fail"***, si legittimava in parte l'azzardo morale fatto dai giganti della finanza**, principali artefici della bolla immobiliare.

Bitcoin risulta sostanzialmente *"figlio"* del **movimento di** *"cypherpunks"* [3], nato sul finire degli anni '80 del secolo scorso: una nuova forma di *"corrente"* anarchica che vedeva l'avvento di Internet come una nuova possibilità di libertà, non governato da regole, dove le persone potessero interagire e fare affari in modo anonimo, liberate dalle normative dello Stato.

L'**aspetto dell'anonimato** è uno dei fondamenti concettuali che costruiscono la blockchain, anche se spesso risulta fonte di confusione.

Questo perché le informazioni memorizzate nella blockchain sono sostanzialmente visibili a tutti (non sono quindi propriamente anonime), essendo la blockchain una struttura dati decentralizzata e quindi per sua natura disponibile a tutti i partecipanti della rete peer to peer.

Noto un indirizzo, risulta quindi possibile ricostruire tutte le transazioni riferite a quell'indirizzo, ma è molto difficile risalire all'identità del possessore di quel *"conto"***.**

Per questo motivo si parla spesso di **pseudo-anonimato**[4].

Per meglio comprendere la blockchain, occorre capire come viene eseguito un programma informatico.

Oramai quasi tutti possiedono un computer e, conseguentemente, utilizzano programmi come la posta elettronica, un browser per accedere a Internet o un editor di testo.

Volendo analizzare uno di questi programmi, si può agevolmente constatare che si tratta di un insieme di istruzioni che vengono eseguite dal computer.

In informatica per descrivere l'esecuzione di questo insieme di istruzioni si utilizza un concetto chiamato *"macchina di Turing"*: un modello astratto che definisce una macchina in grado di eseguire algoritmi; tutti i programmi informatici che si utilizzano sono eseguiti attraverso un insieme limitato di istruzioni che possono scrivere e leggere dati sia su una memoria fisica che su una memoria temporanea.

La blockchain dovrebbe essere vista come una *"macchina di Turing"* **decentralizzata, un computer** *"globale"***, un'architettura informatica peer to peer capace di eseguire le stesse istruzioni e salvare gli stessi dati su tutti i computer che partecipano alla rete.**

Occorre fare attenzione: *"eseguire lo stesso codice e salvare gli stessi dati"* non vuol però dire farlo nello stesso tempo, ma nello stesso ordine.

Questo viene ottenuto utilizzando **una particolare struttura per memorizzare le istruzioni che sono ordinate e raggruppate in blocchi consecutivi** (da qui il termine *blockchain*).

Se le istruzioni che tutti i computer della rete eseguono in modo ordinato risultano principalmente istruzioni per trasferire valore da una entità a un'altra e i dati salvati sono principalmente *"transazioni"*, ecco che si ottiene **qualcosa di simile a un libro giornale**, ed è per questo che molti descrivono la blockchain come una sorta di **libro giornale decentralizzato**.

La blockchain risulta sostanzialmente, quindi, una sequenza ordinata di blocchi dove sono memorizzate istruzioni.

Ogni blocco è identificato da un identificatore unico ottenuto usando una funzione matematica che considera tutti i byte (le informazioni binarie, sequenze di zeri e uno, con cui vengono rappresentati i dati in informatica) del blocco generando una specie di **impronta digitale** (chiamata *'hash'*); tale identificatore è inserito nel blocco.

La sequenza è realizzata in quanto **ogni blocco riporta anche l'identificativo del blocco precedente**.

La **sicurezza delle informazioni**, ossia la garanzia che i dati contenuti nel blocco risultino corretti e non manomessi da qualcuno, è ottenuta in quanto:

- **il riferimento al blocco precedente è un dato inserito all'interno del blocco**, è quindi considerato dall'algoritmo che calcola l'hash o impronta digitale del blocco;

- il **processo di creazione del blocco viene rallentato attraverso un meccanismo** (*"proof of work"*) che rende questo processo **costoso in termini di risorse macchina** (computer + energia elettrica).

Il **primo punto** ha come conseguenza che **se qualcuno intendesse manomettere un blocco**, per esempio modificando l'importo trasferito da un *"conto"* a un altro, **l'impronta risultante sarebbe diversa da quella contenuta nel blocco successivo**, così che un eventuale hacker dovrebbe manomettere tutta la sequenza.

Il **secondo punto** rende questo **processo molto costoso** per l'impegno di risorse macchine ed energia elettrica necessarie allo scopo, **rendendolo praticamente impossibile**.

Quando un blocco è creato (da uno o più **miner**), **il blocco è inviato a tutti i nodi o computer che partecipano alla rete**, così che possa essere svolta una prima verifica formale, di modo da essere inserito nella blockchain.

Il fatto che un altro blocco arrivi e riporti l'hash del blocco appena inserito fa considerare quel blocco valido.

Questo meccanismo è chiamato **consenso**.

Per incentivare i nodi della rete a validare le transazioni e creare il blocco competendo tra di loro, viene creata cripotvaluta e accreditata all'indirizzo del creatore del blocco (la prima delle transazioni in esso contenuto), il tutto governato dai protocolli informatici che definiscono l'infrastruttura della blockchain.

Dopo avere ricevuto e validato il blocco, il nodo esegue le istruzioni che sono contenute al suo interno, aggiornando lo stato (per esempio in Bitcoin lo stato può essere visto come il saldo di tutti i partecipanti alla rete[5]).

Tutti i computer al termine dell'esecuzione delle istruzioni del medesimo blocco condividono lo stesso stato.

Le caratteristiche distintive della blockchain risultano dunque:

- dato **non modificabile.**
- il dato è sempre
- il dato è *'a-territoriale'*: lo stesso dato è memorizzato su tutti i computer della rete.
- le transazioni sono validate senza la necessità di una entità centralizzata: c.d. **disintermediazione**.
- il dato è a disposizione di tutti: c.d.

Occorre inoltre considerare che **la prima cosa che necessita per potere ricevere o spedire criptovaluta è un wallet.**

Un **wallet** è un **programma informatico che può essere installato sul computer e serve per poter accedere alla blockchain.**

In precedenza la blockchain è stata descritta anche come rete peer to peer, sottolineando che in tale rete tutti i nodi hanno le stesse funzioni.

In realtà, nelle blockchain ci sono diverse tipologie di nodi che svolgono attività differenti; i principali tipi sono:

- *'full node'*: partecipano al processo di verifica delle transazioni e dei blocchi seguendo le regole di consenso del sistema; inoltre, salvano tutta la sequenza di blocchi della blockchain ed eseguono

tutte le istruzioni;

- *'miner'*: oltre a essere *'full node'* sono responsabili della creazione dei blocchi competendo tra di loro per la risoluzione matematica dell'algoritmo detto *'proof of work'*.
  Chi risolve per primo l'algoritmo riceve una quantità di bitcoin (o altre criptovalute) definita dal protocollo;

- *'wallet'*: usati per creare transazioni, in genere scaricano solo pochi dati, ossia tutte le transazioni che hanno come destinatario o come mittente gli indirizzi *"conto"* che gestiscono.

I wallet sono quindi programmi che, una volta in esecuzione, si collegano alla blockchain attraverso Internet, diventando uno dei nodi della rete peer to peer.

Risulta quindi errato pensare al wallet come a una sorta di *"portafoglio"*: infatti il **compito del wallet** non è quello di memorizzare le transazioni o il saldo (informazioni memorizzate nella blockchain), ma quello di **generare un sistema di chiavi private/pubbliche**, del tutto equivalente al sistema di firma digitale, **con cui accedere alla blockchain**.

Analogamente al processo di firma digitale…continua nella *Linea Guida n. 3/2021: Criptovalute: inquadramento e questioni civilistiche e tributarie ?*

***

NOTE

[1] Le quali rappresentano una forma – la più comune – di "crypto-asset", ossia di asset finanziari digitali basati sulla tecnologia di un registro distribuito (c.d. "distributed ledget technology" – DLT). Nonostante attualmente non esista una definizione "standard", ossia concordata a livello internazionale, di "crypto-asset", il Gruppo d'azione finanziaria internazionale (GAFI, o anche Financial action task force – FATF) definisce l'asset virtuale come "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations".

[2] Testo originale del withepaper: https://bitcoin.org/bitcoin.pdf.

[3] È opportuno rilevare il "tipo" il contesto culturale in cui nasce il sistema della blockchain: il movimento cypherpunk aveva difatti quale principale scopo quello di contrastare le possibili restrizioni delle libertà e del diritto alla privacy, le quali derivavano dalla sempre più pervasiva diffusione delle tecnologie informatiche. Tecnologie che avrebbero difatti consentito ai governi ed alle istituzioni di monitorare e controllare le informazioni sugli individui, potendo interferire sui loro stili di vita tramite l'associazione dei dati raccolti nelle transazioni di consumo

[4] Questo è vero per le principali blockchain come Bitcoin e Ethereum, ci sono altre blockchain come Monero o Zcash dove anche le transazioni sono anonime.

[5] In realtà e costituito dall'insieme delle transazioni ancora non spese

A cura del Comitato Scientifico di NOMOS

Mercoledì 21 luglio 2021

Questo intervento è estrapolato dalla Linea Guida n. 3/2021 di NOMOS:

NOMOS
CENTRO DI RICERCA IN DIRITTO TRIBUTARIO

LINEA GUIDA N. 3/2021

Le Criptovalute nell'ordinamento nazionale:

inquadramento dell'istituto e questioni in ambito civilistico e tributario

Formato: PDF

N. pagine: 34

Pubblicazione: Luglio 2021

INTRODUZIONE

Negli ultimi anni le **criptovalute** hanno assunto sempre maggiore rilievo nell'economia globale, con un *"approccio"* a tale strumento anche da parte dei c.d. *"piccoli risparmiatori"*.

Ed infatti ultimamente si assiste ad un andamento esponenziale nell'utilizzo e acquisto di queste *"rappresentazioni digitali di valore"*.

Tuttavia al sempre maggiore utilizzo delle criptovalute corrisponde tuttora una **scarsa regolamentazione** di tale *"fenomeno"*, che determina delle forti criticità, sia a livello civilistico che, in particolar modo, fiscale.

Con la presente Linea Guida si prenderà quindi in considerazione la caratterizzazione delle criptovalute, al pari delle principali problematiche per gli operatori, esaminandone il relativo trattamento sia a **livello giuridico** che in termini di **adempimenti tributari**.

INDICE

5. Criptovalute e monitoraggio fiscale: l’adempimento dichiarativo del contribuente tra fraintendimenti amministrativi e corretto inquadramento della fattispecie

6. Conclusioni

SCOPRI DI PIU' >>>