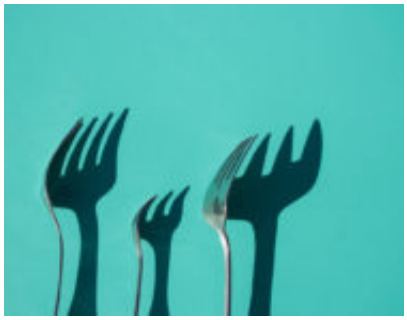
Le fork sulla blockchain: un equilibrio fra opportunità e rischi di una governance decentralizzata

Author : Roberto Garavaglia

Date : 13 Marzo 2019



Sulle blockchain di tipo permissionless [1] nelle quali la governance è decentralizzata e il modello di gestione è off-chain [2] (ad esempio la Blockchain [3] dei Bitcoin), non esistendo un unico decisore centralizzato in grado di determinare risoluzioni, quando si vogliono cambiare le regole è necessario che la rete stessa - rappresentata da programmatori e validatori - sia d'accordo. A tale situazione, spesso di compromesso, si perviene grazie al coordinamento fra la comunità degli sviluppatori, mediante la sottomissione di proposte di modifica (nel caso dei Bitcoin si chiamano BIP – Bitcoin Improvements Proposal) che saranno votate. Nel solco di tali determinazioni, all'esito delle votazioni, è possibile inserire l'avvicendarsi di particolari "momenti" nella vita di una blockchain chiamati "**fork**". Il termine inglese richiama l'immagine di una biforcazione e, nei fatti, ciò che avviene è proprio uno sdoppiamento della catena di blocchi che, in alcune circostanze, può dar luogo alla creazione di nuove criptovalute.

In questo articolo analizziamo le diverse tipologie di fork e le motivazioni che possono indurle, spiegando alcune tra le più famose avvenute sulla Blockchain dei Bitcoin e i rischi che occorrono durante il verificarsi delle medesime.

Le tipologie di fork

Le fork si possono suddividere in due macro-categorie: "**Soft fork**" e "**Hard fork**".

Le Soft fork si realizzano e si attuano dando vita a una versione aggiornata del protocollo compatibile con le versioni precedenti. Tali tipi di fork mettono in atto un cambiamento reversibile che consente la partecipazione alla blockchain anche a tutti quei nodi che, per ragioni diverse, decidono di non effettuare l'aggiornamento del software.

Le Hard fork prevedono invece un cambiamento irreversibile e impongono ai nodi di effettuare obbligatoriamente l'aggiornamento. Con le Hard fork vengono create nuove criptovalute come, ad esempio, nei casi di Bitcoin Cash.

Analizzando nel dettaglio le Hard fork, scopriamo che possono essere di tipo “Planned”, ovvero pianificate e programmate, o di tipo “Contentious”, ovvero che non riescono a trovare il consenso della comunità. In questa seconda tipologia di Hard fork il cambiamento proposto al protocollo non trova un accordo all’interno della comunità e si arriva, pertanto, a una forma di scissione della Blockchain.
Nel caso di Hard fork “Planned” il cambiamento del protocollo è pianificato e il passaggio viene approvato dai partecipanti ove sia raggiunto un *quorum* definito in fase di proposta dei cambiamenti delle regole.
Le Hard fork “Planned” non conducono allo sdoppiamento della catena e le regole vengono aggiornate in continuità.

Scalabilità, costi e rischio di concentrazione

Passiamo ora a condividere alcune riflessioni su talune caratteristiche basilari delle blockchain permissionless, volendo con ciò portare l’attenzione del lettore sui diversi rischi che devono essere opportunamente ponderati, laddove si vogliano progettare soluzioni basate sull’impiego di tali architetture.

Prenderemo come riferimento la Blockchain permissionless per antonomasia, ossia quella dei Bitcoin, premettendo tuttavia che le considerazioni in esame possono (*rectius,* devono) ritenersi altrettanto valide per tutte le blockchain di tale tipo e, cosa assai più importante, per qualsiasi impiego che delle stesse si voglia fare. Si osserva infatti che una siffatta ponderazione dei rischi deve potersi considerare anche quando l’impiego di una blockchain permissionless vuole essere impiegata – ad esempio – a supporto di servizi di marcatura temporale o finalizzata all’esecuzione di smart contract [4].

Sulla Blockchain dei Bitcoin durante il processo di validazione dei blocchi (il c.d. “mining”) vengono “coniate” nuove unità di criptovaluta come sistema di remunerazione che ripaga – almeno in parte – il costo sostenuto dai nodi validatori (risorse di calcolo, energetiche ecc.). Il modello d’incentivazione basato sulle Proof-of-Work (PoW), il sistema con cui si perviene a un “consenso distribuito” [5], assicura che questi ultimi vengano premiati per il loro lavoro di approvazione solo laddove il compito sia stato svolto correttamente, rendendo antieconomico qualsiasi tentativo di alterazione surrettizia dei blocchi precedentemente validati.
Ciononostante, esiste un ulteriore modello di incentivazione basato sulle commissioni (o “mance”) che permette ai validatori di essere ulteriormente ricompensati, in aggiunta alla ricompensa prevista per chi presenta per primo la PoW.

I nodi validatori, soprattutto nei periodi di intenso traffico transazionale, tendono a scegliere i blocchi che contengono mance più significative, creando una disparità di trattamento per quegli utenti che, non volendo spendere in commissioni esorbitanti, sono costretti ad attendere ben più di un’ora per vedersi confermate le proprie transazioni. La dimensione di un blocco della Blockchain (dei Bitcoin) non può superare 1 MB e pertanto i miner sceglieranno di inserire nei blocchi che si accingono a minare le transazioni con commissioni più alte, soprattutto nei periodi in cui sul network viene propagato un numero di transazioni particolarmente elevato; ne consegue che transazioni meno “redditizie” possono attendere ore prima che un miner scelga di inserirle nel proprio blocco.

Nel seguito vediamo quali sono stati alcuni fra i maggiori interventi che hanno animato la comunità dei principali miner sulla Blockchain dei Bitcoin, volti a trovare una sorta di ottimo paretiano tra le necessità di: rendere (più) scalabile la Blockchain, abbassare il costo delle commissioni, evitare il ricrearsi di "concentrazioni di fatto".

Come preannunciato, è opinione di chi scrive che sia utile spiegare l'avvicendarsi di tali interventi, poiché essi rappresentano un potenziale *vulnus* che deve essere noto e gestito, soprattutto laddove si pensa di impiegare una blockchain per finalità che vadano oltre il concetto di mero scambio di criptovaluta. Tali criticità minano, nella sostanza, il principio di governance tipica della Blockchain dei Bitcoin e, in generale, qualsiasi principio di governance decentralizzata tipica di una blockchain permissionless.

SegWit2X

Al fine di migliorare l'utilizzo e la scalabilità dell'infrastruttura decentralizzata che gestisce gli scambi di bitcoin proprio laddove, in particolare nei periodi di utilizzo intensivo, il calo prestazionale è avvertito maggiormente, un gruppo di miner ha proposto nel corso del 2017 una serie di modifiche strutturali alla Blockchain, suddivise in due fasi: la prima, chiamata "Segregated Witness", prevedeva di efficientare il protocollo riducendo la dimensione delle transazioni, mediante la segregazione di alcuni metadati che accompagnano le transazioni.

Tali metadati avrebbero potuto essere gestiti off-chain, ossia al di fuori della catena. In tal modo, mantenendo la stessa dimensione del blocco originaria, ci sarebbero state più transazioni validate nell'arco di 10 minuti, il tempo mediamente necessario per generare un nuovo blocco e aggiungerlo alla catena, per cui, in pratica, la gestione delle transazioni in Bitcoin sulla Blockchain è limitata a 6 o 7 al secondo.

Il secondo step (attivabile ove si fosse raggiunto il consenso richiesto) avrebbe dovuto condurre all'aumento della dimensione massima dei blocchi. Tecnicamente quanto avvenuto è stato non riuscire ad attivare la seconda parte di SegWit2x (ossia quella su cui maggiormente la comunità si era divisa), che avrebbe dovuto raddoppiare la dimensione dei blocchi portandoli a 2 MB, volendo con ciò incrementare l'efficienza del protocollo e, almeno in teoria, portare a una diminuzione delle commissioni richieste dai miner per validare più velocemente le transazioni.

I Bitcoin Cash

SegWit, la prima parte, con cui si era iniziato ai primi di agosto 2017, è avvenuta al netto di un compromesso che ha prodotto l'**Hard fork dei Bitcoin Cash**, una nuova catena dalla quale si è originata un'altra criptovaluta (il BCH), separata dalla quella core e irreversibile, dove i blocchi hanno la dimensione massima di 8 MB. Per questa nuova blockchain, i sostenitori hanno sempre dichiarato che avrebbe potuto costituire un buon mezzo per effettuare pagamenti P2P, attese le prestazioni decisamente superiori rispetto alla Blockchain parent.

I rischi che comportano le Hard Fork

Ora che abbiamo spiegato cosa sono le fork, le ragioni per cui si generano e narrato delle principali avvenute negli ultimi due anni, è il momento di descrivere quali possono essere gli effetti che le stesse ingenerano.

Nei casi di Hard fork o, meglio, durante il propagarsi degli effetti sulla rete delle Hard fork, emergono alcuni rischi che pongono in pericolo l'affidabilità e, soprattutto, l'**immutabilità delle transazioni avvenute**.
Ciò che infatti può accadere è il manifestarsi dei cosiddetti "**replay attack**", dove soggetti malintenzionati replicano le transazioni sulla nuova catena appena effettuate sulla catena di origine. Tale situazione si verifica per via del fatto che le due criptovalute (quella *legacy* e quella della *forked chain*), nel periodo in cui si sta consumando la scissione, possono essere "sbloccati"[6] con la stessa chiave privata, esponendo quindi le transazioni al rischio di essere duplicate.

Guardando oltre il mero impiego di una blockchain permissionless per gli scambi di criptovaluta, riteniamo sia sufficientemente chiaro a tutti (evitando con ciò di addentrarci oltre) quali possano essere i rischi nel caso di un "replay attack", allorché si voglia impiegare una blockchain permissionless, ad esempio, quale strumento a supporto della validazione temporale elettronica.

Le contromisure a mitigazione dei rischi di "replay attack"

Mitigare i rischi causati dai "replay attack" è possibile adottando alcuni sistemi, fra cui i più noti sono conosciuti con il nome di "**Strong replay protection**" e "**Opt-in replay protection**".
Nel primo caso viene aggiunto uno speciale marcatore alla nuova catena a posteriori dell'Hard fork, al fine di evitare che le transazioni eseguite siano (ancora) valide nella catena originaria (legacy chain) e non viceversa. Se la "Strong replay protection" è una procedura che viene eseguita in automatico al verificarsi dell'Hard fork, la "Opt-in replay protection" richiede invece un intervento manuale di "manutenzione" sulle transazioni per assicurare la loro irripetibilità.

In alternativa (o in aggiunta) alle contromisure spiegate da attuare per fronteggiare i rischi evidenziati, è possibile prevedere l'interruzione di qualsiasi trasferimento/transazione fino a quando la nuova catena di blocchi non abbia raggiunto una certa altezza [7]. Ciò implica, ovviamente, un intervento "ai morsetti" della blockchain (ossia off-chain), con tutte le conseguenze che esso comporta.

I *vulnus* della e-democracy

Concludiamo questo articolo con una riflessione più ampia che, all'avviso di chi scrive, appare utile non foss'altro come monito teso ad allertare chi, pur in buona fede, corre il rischio di subire la fascinazione delle blockchain quale panacea di ogni male.

Alcune vulnerabilità tipiche delle blockchain pubbliche, ossia quelle il cui accesso segue una logica permissionless, emergono durante il propagarsi sul network delle Hard fork. I casi di Hard fork che producono scissioni irreversibili della catena, con la conseguente nascita di nuove

criptovalute, non sono in sé deprecabili, poiché rappresentano un metodo per esprimere miglioramenti (almeno così si auspica) in cui le comunità di sviluppatori e di validatori credono.

La presenza di un modello di governance decentralizzata (o, se si preferisce, l'assenza di un modello di governo centrale) può rappresentare **l'espressione democratica di un sistema decisionale**, dove una pluralità di soggetti può esprimere il proprio voto per il conseguimento di obiettivi condivisi: una sorta di **e-democracy** [8]. Tuttavia, l'esercizio stesso di tale democrazia impone la necessità di prevedere, in molti casi, scissioni interne al sistema; è proprio in queste circostanze che, come nella vita materiale organizzata da una politica intesa quale espressione di una sovranità popolare, si indeboliscono le difese e si sguarnisce il fianco, esponendo l'intera comunità a rischi che devono sapersi mitigare, agendo preventivamente laddove possibile.

Note

[1] Una piattaforma blockchain è di tipo permissionless (da non confondere con le blockchain permissioned), quando soddisfa almeno i seguenti requisiti: è aperta al pubblico, ognuno può accedere e vedere il relativo codice (software), tutti possono leggere qualsiasi transazione riportata sul registro, chiunque può effettuare transazioni e candidarsi, a propria volta, ad eseguirne la validazione.

[2] Per le blockchain permissionless esistono almeno due tipologie di governance tecnologica: 1) "off-chain", dove è necessario raggiungere un consenso più ampio per attuare le modifiche del protocollo e dove quando ciò non avviene si verificano le Hard fork descritte in questo articolo, 2) "on-chain", dove il potere di voto è determinato dall'entità di quota (espressa in token) da ciascun attore-votante detenuta.

[3] Con il termine "Blockchain" (quando l'iniziale è maiuscola) ci si riferisce alla tecnologia che supporta i Bitcoin, mentre con il termine "blockchain" (con l'iniziale minuscola) si intende l'architettura tecnologica posta alla base di altri sistemi dove la criptovaluta non è necessariamente il Bitcoin.

[4] Il riferimento (non casuale) è al decreto-legge 14 dicembre 2018, n. 135 con cui il legislatore Italiano, correttamente non discernendo la tipologia di blockchain (permissionless o permissioned), ha provveduto ad attribuire il requisito della forma scritta - previa identificazione informatica delle parti interessate – agli smart contract, nonché ha disposto che la memorizzazione di un documento informatico mediante l'uso di tecnologie basate su registri distribuiti produca gli effetti giuridici della validazione temporale elettronica *ex* art. 41 del regolamento (UE) n. 910/2014 (c.d. "Regolamento eIDAS").

[5] Possiamo definire come "consenso distribuito" l'accordo tra i nodi sulla validità di una transazione e sull'esistenza di un insieme coerente nonché di un ordine garantito delle transazioni da memorizzare nel registro distribuito, cui si perviene in un sistema decentralizzato dove la governance è distribuita tra i partecipanti.

[6] Lo script di sblocco è solitamente una firma digitale che dimostra la proprietà dell'Address

inserito nello script di blocco del precedente Output.

[7] Nella Blockchain dei Bitcoin con altezza ci si riferisce alla posizione del blocco nella catena.

[8] Con e-democracy si intende l'utilizzo delle tecnologie dell'informazione e della comunicazione atto a favorire la partecipazione dei cittadini alla vita democratica. In questo contesto, si è ritenuto utile riferirsi a tale termine per rappresentare l'espressione democratica del sistema decisionale tipico della Blockchain.

Articolo a cura di **Roberto Garavaglia**