Una questione di Consenso

di Edoardo Calia, CTO Fondazione LINKS

Il 15 Settembre 2022 è una data storica per la rete Ethereum, che con una operazione dal nome in codice TheMerge ha abbandonato il meccanismo della Proof of Work sostituendolo con la Proof of Stake. Vediamo insieme cosa questo significa, e le implicazioni per la rete che supporta la seconda criptovaluta per capitalizzazione di mercato.

---

consènso s. m. [dal lat. *consensus* -*us*, der. di *consentire* «consentire»]. – **1. a.** Conformità di voleri: *agire di consenso*, d'accordo. **b.** In diritto, elemento essenziale del negozio giuridico bilaterale o plurilaterale, consistente nell'incontro delle manifestazioni di volontà di due o più soggetti contrapposti (sinon. perciò di *accordo*)

Il meccanismo che consente la approvazione di una determinata situazione o decisione da parte di una community costituita da un numero arbitrario di membri indipendenti è noto a tutti come procedura di consenso. In una community gestita in modo democratico, che conferisce a tutti i propri membri lo stesso diritto di esprimere il proprio parere (il *voto*), il consenso si basa su due principi fondamentali:

- Tutti i partecipanti devono avere accesso alle stesse informazioni per poter esprimere il proprio voto in modo informato
- Il consenso su una particolare decisione si intende raggiunto quando si ottiene la maggioranza dei "voti". Tutti i partecipanti a questo punto si allineano a questa decisione.

Il problema del raggiungimento del consenso ricorre nella nostra vita quotidiana - personale o lavorativa - ogni volta che un gruppo di persone deve prendere una decisione: cosa si mangia questa sera, dove si va in vacanza, quale strategia aziendale perseguire, approvare un investimento aziendale. E in tutte queste situazioni la decisione è influenzata da soggetti che nel loro contesto specifico esprimono maggiore affidabilità e leadership.

In termini molto simili si parla di consenso (e di come raggiungerlo) anche nell'informatica, e in particolare nell'informatica distribuita: quella cioè che prevede di suddividere un compito particolarmente complesso tra elaboratori (nodi) diversi e indipendenti tra loro - nessuno dei quali cioè ricopre un ruolo di arbitro o coordinatore. Anche in questo caso occorre trovare una procedura per la quale i diversi sistemi raggiungano ad un certo punto un accordo sui risultati via via raggiunti dai vari (nodi) partecipanti, e in ultima istanza sul risultato finale del lavoro.

La distribuzione del lavoro tra diversi soggetti porta, a seconda di come viene configurata, vantaggi in termini di resilienza ai guasti o a malfunzionamenti di varia natura, incluse le conseguenze di eventi catastrofici (in questo caso si parla di architetture progettate per la *business continuity* e/o per il *disaster recovery*).

Un ambito delle tecnologie digitali nelle quali il consenso gioca un ruolo fondamentale è quello dei sistemi decentralizzati, tra i quali la blockchain è senz'altro il più noto (ma certamente non il primo, di sistemi distribuiti si parla da più di 50 anni!). Queste particolari sistemi, introdotti circa 15 anni fa con la nascita del Bitcoin, risolvono un problema specifico che le accomuna tutte: gestire e mantenere un *ledger*, ovvero un registro che memorizza eventi *certificati* e *ordinati nel tempo*. Nel pieno rispetto del principio ispiratore di avere una *governance priva di enti centrali*, questo registro è *replicato* su ciascuno dei nodi partecipanti al sistema, ottenendo come *byproduct* una forte resilienza agli attacchi e ai guasti[1].

Il consenso quindi consiste nel raggiungere un accordo su quale sia l'ordine temporale delle informazioni contenute nel registro. Per proseguire questa esposizione con riferimento a un caso d'uso semplice e noto nei suoi requisiti, consideriamo uno scenario nel quale i dati contenuti in questo registro siano transazioni di tipo economico, ovvero informazioni relative a trasferimento di asset (digitali in questo caso) da un utente ad un altro.

La gestione della liquidità e della sua allocazione sugli account di diversi utenti è un problema che oggi viene risolto grazie all'intervento di enti centrali che garantiscono la correttezza e la liceità dei vari trasferimenti: in altre parole tali istituzioni ricoprono un ruolo di *garanti* a tutela degli utenti, proteggendoli da episodi illeciti o errori (con la conseguente assunzione di rischio e responsabilità).

L'obiettivo di trovare un sistema informativo che consenta di *gestire gli asset degli utenti di una community in modo del tutto autonomo e democraticamente distribuito, offrendo garanzie di affidabilità e protezione da eventi avversi paragonabili a quelle offerte dalle istituzioni bancarie* è la motivazione che ha portato allo studio e alla realizzazione dei sistemi di distributed ledger.

Diverse sono le caratteristiche che un simile sistema informativo deve avere per poter soddisfare gli ambiziosi requisiti. Tra queste le principali sono:

- *Verifica della identità* di chi genera una transazione (senza possibilità di ripudio)
- Robustezza dei dati, ad esempio tramite *replica della stessa base dati su più elaboratori*
- Verifica delle condizioni per poter considerare valida una transazione, ad esempio la *disponibilità degli asset* da trasferire
- Garanzia che uno stesso asset digitale non possa essere speso o inviato più di una volta, problema noto come *double spending*
- Garanzia che la base dati che memorizza tutte le transazioni sia *unica, verificata e accettata da tutti i nodi* partecipanti al funzionamento del sistema (principio del consenso)

Nella parte rimanente di questo articolo ci concentreremo sull'ultimo punto per capire come sia possibile che un gruppo di elaboratori totalmente indipendenti gli uni dagli altri possa raggiungere il consenso sul contenuto di un registro di transazioni, le quali possono essere inserite (proposte) da uno o più dei nodi della rete. Il sistema deve essere robusto e deve operare in condizioni di massima apertura e libertà. L'obiettivo deve essere garantito in presenza di condizioni quali:

- Non sia nota la identità dei diversi partecipanti / votanti

[11] È importante notare un aspetto spesso trascurato trattando questi argomenti: di per sé i principi tecnologici alla base delle DLT non richiedono una rete di elaboratori (ovvero una blockchain può funzionare anche su un singolo nodo o server). In questo caso però si perderebbe la caratteristica di democratizzazione della *governance*: per questa ragione si è introdotto il requisito che prevede la replica su più elaboratori della base dati e dell'effort di calcolo necessario per la sua gestione

- Non sia certa la affidabilità e correttezza dei partecipanti, ovvero sia tollerabile la presenza nella community di uno o più membri che si comportano in modo fraudolento
- Nessuno dei nodi abbia un ruolo di coordinatore centrale o arbitro

Trattandosi di un sistema sul quale non è possibile esercitare un controllo, si deve accettare che ogni decisione votata e accettata a maggioranza dai partecipanti sia considerata valida. Si assume quindi che almeno metà dei membri della community siano *onesti* e lavorino nella direzione dell'ottenimento del *bene comune*.

L'occasione di trattare il complesso ma affascinante tema del consenso è data da una imminente e radicale modifica di questo meccanismo in uno dei più noti sistemi decentralizzati, ovvero la blockchain che sta alla base della rete Ethereum.

Validazione delle transazioni e costruzione della blockchain

Nei sistemi blockchain le transazioni da aggiungere al ledger (sulle quali quindi è necessario raggiungere il consenso) vengono processate in blocchi: in modo del tutto democratico qualunque nodo che partecipa al sistema distribuito può comporre e proporre il prossimo blocco da aggiungere alla catena (la blockchain appunto, catena di blocchi).

Le transazioni non ancora inserite nel ledger (ovvero generate dagli utenti ma non ancora validate) risiedono in un luogo visibile e accessibile da tutti, che si chiama *mempool*. È dalla *mempool* che un nodo che si candidi a generare un nuovo blocco preleva le transazioni che intende validare[2], ed esegue successivamente le seguenti operazioni:

- Validazione di ogni transazione: verifica di identità del mittente e di disponibilità di risorse
- Costruzione del nuovo blocco contenente le transazioni verificate
- Validazione del blocco
- Invio del blocco a tutti i nodi della rete

I nodi che ricevono un blocco preparato in questo modo eseguono due semplici operazioni:

- Validazione di tutte le transazioni
- Verifica della validazione del blocco nel suo complesso
- Se il blocco è valido, viene aggiunto alla copia locale del *ledger* (blockchain) che ciascuno mantiene indipendentemente[3]

Il processo di generazione di un nuovo blocco da *appendere* alla blockchain presenta due punti critici che devono essere affrontati per giungere ad un sistema effettivamente utilizzabile. Più precisamente occorre introdurre:

- un incentivo per motivare i nodi che partecipano al sistema a svolgere il lavoro necessario alla predisposizione del nuovo blocco

[2] In assenza di un coordinatore, la scelta delle transazioni da validare è *eseguita individualmente* dal nodo che prova a preparare il prossimo blocco. Elaboratori diversi nella rete possono quindi generare blocchi che contengono transazioni diverse. Questo non ha influenza sulla validità del ledger, che prima o poi conterrà tutte le transazioni *valide* inserite dagli utenti

[3] Si ricordi che ciascuno dei nodi principali nelle architetture blockchain mantiene una copia dell'intero *ledger* per finalità di resilienza e robustezza dell'intero sistema

- un meccanismo che disincentivi, rendendole costose, attività fraudolente mirate a proporre blocchi contenenti transazioni illecite.

A questo ultimo requisito rispondono soluzioni diverse, tra le quali le due che sono protagoniste dell'epocale cambiamento al quale sta andando incontro la rete di Ethereum: la *Proof of Work (PoW)* e la *Proof of Stake (PoS)*.

Proof of Work

Il meccanismo della ***Proof of Work*** si basa sull'uso di una operazione crittografica particolarmente complessa per la validazione dei blocchi in fase di preparazione. Su ogni nuovo blocco, dopo aver validato ognuna delle transazioni in esso inserite, il nodo proponente deve eseguire questa operazione affinché il blocco nel suo complesso risulti valido. Una particolarità di questa operazione è che la *verifica* che essa sia stata effettuata (ovvero che sia stato svolto questo calcolo complesso) è invece estremamente semplice. I nodi che ricevono un nuovo blocco candidato ad essere aggiunto alla blockchain possono quindi verificarne la integrità e correttezza in modo molto rapido. Questa verifica si chiama Proof of Work, ovvero dimostrazione che qualcuno (il nodo proponente) abbia dedicato risorse imponenti di calcolo per predisporre il blocco contribuendo al mantenimento in operatività della blockchain.

L'operazione crittografica di preparazione del blocco è talmente complessa che la probabilità che un nodo predisponga un blocco e riesca a risolvere il quiz crittografico è estremamente bassa. La probabilità di avere un blocco valido entro un tempo ragionevole diventa accettabile solo mettendo in competizione tutti i nodi della rete, ciascuno dei quali – in modo indipendente – prova a costruire un blocco e candidarlo ad essere aggiunto alla blockchain. Al vincitore della competizione (ovvero il primo nodo che riesce a costruire un blocco valido e proporlo agli altri nodi della rete) va una ricompensa – nella "valuta" nativa della blockchain - costituita da due componenti: un premio predeterminato per aver "vinto" la competizione, al quale viene aggiunta la somma di tutte le *fee* associate alle transazioni inserite nel blocco. Il premio per la generazione del blocco viene conferito generando monete (token) che fino a quel momento non erano in circolazione: questa caratteristica conferisce all'intero processo di generazione dei blocchi il nome di *mining*, per analogia con il lavoro che viene fatto per estrarre oro (ad esempio) da una miniera.

Il meccanismo della Proof of Work rende più robusta a rete da diversi punti di vista:

- Ogni blocco e ogni transazione all'interno del blocco viene controllato e validato da tutti i nodi della rete: l'inserimento di una transazione illecita non avrebbe nessuna speranza di essere accettata e inserita nel ledger
- Tutte le transazioni devono essere autenticate con un meccanismo di firma digitale, che solo chi è in possesso della chiave privata può eseguire. Nessuno quindi può impersonare un utente e generare una transazione a suo nome
- La predisposizione di un blocco è talmente complessa che un nodo che agisce in modo fraudolento non avrebbe praticamente alcuna speranza di vincere la competizione facendo approvare al resto della rete il suo blocco contenente transazioni illecite
- I blocchi sono tra loro collegati (ancora una volta sfruttando lo stesso algoritmo crittografico citato in precedenza) in modo tale che l'inserimento di una modifica in un blocco richiederebbe non solo di ripetere il meccanismo di validazione per quel blocco, ma anche per tutti quelli generati successivamente fino al tempo presente. Questo principio è alla base della immutabilità dei dati scritti nella blockchain, una delle sue caratteristiche più note.

La Proof of Work di Ethereum era stata progettata in modo che la competizione tra i suoi più di 5800 nodi generi un blocco ogni 13 secondi circa. Questo significa che – nel caso più comune - ogni 13 secondi uno solo di quei nodi riesce a risolvere il quesito crittografico per il blocco che sta costruendo, e a proporre (di fatto *imporre*) al resto della rete di aggiungere quel blocco alla catena. Ricevendo questa segnalazione tutti gli altri nodi, che erano anch'essi impegnati nella stessa competizione ma che sono stati meno fortunati del vincitore, interrompono la lavorazione, aggiungono alla propria copia del ledger il blocco ricevuto e iniziano una nuova sessione di *mining* selezionando un nuovo gruppo di transazioni dalla *mempool*.

Se la Proof of Work comporta significativi vantaggi per la stabilità e robustezza della rete (e di fatto costituisce una delle principali innovazioni introdotte dalla blockchain), essa porta con sé anche aspetti di grande inefficienza. I quasi 6000 nodi che compongono la rete Ethereum, e che erano in competizione costante gli uni con gli altri per riuscire a generare il prossimo blocco, consumavano circa 45 TWh all'anno, equivalente ad un impianto da 5GW operativo 24 ore al giorno. Per collocare dimensionalmente questo valore, il consumo della rete Ethereum prima di *TheMerge* era equivalente a un settimo del consumo elettrico del nostro paese, e ampiamente superiore al consumo di diversi paesi del mondo.

Queste constatazioni hanno portato la community dei *miner* o *minatori* della rete Ethereum a riconsiderare uno dei meccanismi più sofisticati e critici della architettura della seconda blockchain più nota al mondo, proponendo che il processo di consenso migrasse dal sistema Proof of Work a quello differente e più efficiente della Proof of Stake (PoS).

Proof of Stake

Il meccanismo della Proof of Work ha come effetto ultimo la selezione casuale del nodo che genera e propone il prossimo blocco della catena. La casualità è conseguenza del fatto che sia impossibile prevedere quale sarà il nodo che si aggiudica la competizione: in teoria nella PoW di Ethereum tutti i nodi avevano ogni 13 secondi la stessa possibilità di vincere la gara e aggiudicarsi la ricompensa[4].

La ***Proof of Stake*** condivide con la Proof of Work l'obiettivo di selezionare in modo casuale, equo e imparziale il *nodo che propone il prossimo blocco*. Il metodo usato per questa selezione è però del tutto diverso: nel meccanismo della PoS viene nominato un gruppo di nodi –a rotazione, scegliendo tra tutti quelli che soddisfano i requisiti di *staking* (vedi sotto) - incaricati di verificare la validità e correttezza dei nuovi blocchi per poi propagarli a tutti gli altri nodi della rete. Tra questi nodi viene selezionato casualmente anche quello incaricato di generare il prossimo blocco.

I nodi che desiderano operare come generatori o validatori di blocchi devono candidarsi depositando una sorta di *cauzione* (operazione di *staking* appunto) a garanzia del loro corretto operato. Per indicare che la costosa operazione del mining non è richiesta, nelle reti che utilizzano un protocollo di consenso basato sul paradigma della Proof of Stake il termine *miner* è sostituito con il termine *validator*.

[4] In realtà, ricordando come funziona la *Proof of Work*, i nodi che hanno maggiore potenza di calcolo a disposizione hanno anche maggiore probabilità di aggiudicarsi la generazione del prossimo blocco valido. Questa situazione, che di fatto crea uno scostamento rispetto alla vera equità di trattamento dei nodi, è spesso oggetto di critiche da parte dei puristi della democratizzazione dei servizi digitali

Un nodo che si comporta in modo non conforme alle attese –che venga ad esempio sorpreso a generare un attacco proponendo un blocco che contiene transazioni fraudolente - si vede sottratta (in modo insindacabile e automatico, utilizzando un apposito *smart contract*) la somma depositata.

I due principali vantaggi introdotti dalla Proof of Stake sono quindi la *riduzione estrema del consumo di risorse energetiche e di calcolo*, e la *introduzione di un meccanismo punitivo* per scoraggiare attività fraudolente e attacchi alla rete[5].

Gestione della transizione da PoW a PoS

È facile intuire che la modifica del protocollo utilizzato per il consenso, cuore pulsante che sostiene tutta la operatività della rete Ethereum, rappresenti un fattore di estrema complessità e criticità per il corretto funzionamento della blockchain. E in questo caso il termine *cuore pulsante* é particolarmente adatto, in quanto la operazione è stata predisposta e resa operativa senza interruzioni significative dei servizi offerti, e preservando tutte le informazioni associate al *ledger*.

Come è stato possibile progettare un intervento di questa complessità su un sistema attivo e funzionante?

La progettazione del meccanismo di Proof of Stake è stata messa a punto su una catena chiamata *Beacon,* separata dalla rete principale (la *Mainnet*). La Mainnet è la catena che mantiene tutte le transazioni inserite e verificate dall'inizio della storia di Ethereum, nel Luglio 2015. La catena Beacon è stata attivata il 1° Dicembre del 2020, e da allora è rimasta completamente separata dalla Mainnet ma ha dato la possibilità di testare le funzionalità e il corretto funzionamento del nuovo metodo per selezionare i nodi incaricati di validare i blocchi. Alla rete Beacon partecipavano i cosiddetti *stakers*, cioè i nodi che intendevano candidarsi ad essere i validatori dei blocchi nella nuova rete Ethereum. Dal punto di vista operativo questo ha richiesto a tali nodi di installare ed eseguire il software relativo alla Beacon Chain (che implementa la PoS) in parallelo a quello utilizzato per la Mainnet.

Questo software, che fa parte della nuova architettura che i nodi candidati validatori devono mantenere operativa, può essere eseguito solo se il nodo che lo ospita esegue preventivamente lo *staking* di token Ethereum a garanzia del proprio operato.

La mattina del 15 Settembre 2022 le due catene si sono fuse (*merged*, da cui il nome dell'operazione *TheMerge*), rendendo disponibili i dati storici (transazioni) degli ultimi 7 anni e applicando il nuovo metodo di validazione ai prossimi blocchi generati. È importante notare che dal punto di vista operativo i blocchi validati in passato e le transazioni in essi contenute non sono influenzati dal nuovo processo di Proof of Stake, che riguarda solo il modo in cui viene scelto il nodo che genera e propaga il prossimo blocco da inserire nella blockchain. Negli scorsi 7 anni questa scelta derivava dalla competizione rappresentata dalla PoW.

[5] A dire il vero un meccanismo punitivo è implicito anche nel meccanismo della Proof of Work: in quel caso la *punizione* per chi tenta di mettere in atto un attacco senza successo è rappresentata dal costo delle ingenti risorse di calcolo ed energetiche necessarie per eseguire l'algoritmo crittografico