ATTUALITÀ

Amministrazione della Blockchain una scelta tecnica o una scelta politica. Quis costodiet custodes?

di **Fondazione AIDR** · 25 maggio 2021, 12:01

di Andrea Barella, Socio Aidr, Head of trading di Banca Intermobiliare e Research fellow presso International University College of Turin

Contesto storico

Negli anni 90 del secolo scorso nacque un movimento culturale definito Cyberpunk che coniugava attenzione per la tecnologia avanzata e volontà di ribellione o quanto meno cambiamento radicale dell'ordine sociale. Questa sottocultura influenzò vari aspetti delle arti e delle scienze. Il mondo letterario e artistico ma anche il mondo informatico. Gli attivisti del mondo dell'information tecnology appartenenti a questa corrente svilupparono, tra le altre, l'idea di utilizzare la crittografia per migliorare la privacy delle persone.

Facendo un salto cronologico in avanti fino al 2008, ci troviamo durante la crisi economica che porta molti dissesti finanziari tra cui il fallimento di Lehman Brothers. La fiducia dei cittadini verso il sistema finanziario è minima, poca fiducia riscuotono anche gli organismi che avrebbero dovuto gestire ed evitare questa crisi, governi, banche centrali e enti sovranazionali. L'opinione pubblica ritiene che, da un lato gli enti di garanzia abbiano perso il controllo e dall'altro che i costi dei salvataggi delle aziende private saranno pagati dallo stato e quindi dai cittadini.

Questo è il contesto quando nel 2009 Satoshi Nakamoto, prima annuncia all'interno di una mailing list di matematici crittografi il suo progetto, e poi inizia la storia della blockchain (Blockchain maiuscolo, a quei tempi), propagando nella rete embrionale di Bitcoin il primo blocco, il genesis block. Satoshi insieme alla evidente rivoluzione tecnologica si premura di chiarire che è in atto anche una rivoluzione politica o quanto meno di politica economica. Al di là dei contenuti innovativi che possono essere compresi da esperti informatici, riporta a chiare lettere e a futura

memoria nella Coinbase (la stringa di testo libero all'interno del blocco) "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" ovvero "Il Cancelliere dello scacchiere ipotizza un secondo salvataggio per le banche", titolo del quotidiano The Times di quei giorni. Se uniamo questa dichiarazione alla politica monetaria di Bitcoin (passiva e predefinita) diventa esplicita la volontà di Satoshi di creare un sistema monetario indipendente dalla gestione politica e governativa.

La situazione attuale

A distanza di 12 anni vediamo come si è evoluto quell'intento.

Quando si legge o si parla di blockchain l'immaginario collettivo per lo più ipotizza che il suo funzionamento sia stato codificato dal suo inventore nel 2008 e da allora di fatto immutabile, sia negli aspetti più prettamente tecnici (es. la sicurezza crittografica) che nei parametri economici (es. inflazione). Un preconcetto molto lontano dalla realtà dei fatti.

La blockchain di Bitcoin è un database gestito da un software, tale software è freeware e ha numerose versioni (attualmente 8) compatibili, gestite da altrettanti team di sviluppo, che apportano in continuazione modifiche per, a loro giudizio, migliorare il funzionamento della rete e del database.

Gli utilizzatori di questi software sono gli utenti dell'ecosistema:

- Miners, che lo usano per aggiornare la blockchain con blocchi di dati validi
- Software house che creano programmi che si appoggiano alla blockchain (es wallet o exchange)
- Utenti generici, anche semplici privati cittadini, che usano il software per detenere una copia della blockchain sul proprio server

Quando gli sviluppatori realizzano modifiche che incidono in maniera più pesante sulla logica di evoluzione della blockchain realizzano dei così detti "fork" (inteso come biforcazione non forchetta), in quanto da quel momento in poi gli utenti che usano la versione vecchia e quelli che usano la versione nuova creano due blockchain separate e diverse (con un passato comune) e ai nostri fini, di fatto, due criptovalute. Non tratteremo qui i dettagli tecnici che differenziano soft-fork da hard-fork, diciamo solo che uno allarga i parametri, quindi i blocchi precedenti sono compatibili con le nuove regole mentre il secondo propone dei parametri più limitati, quindi i vecchi blocchi non sarebbero compatibili con le nuove regole.

Ai nostri fini invece è interessante sapere che esistono due tipi di fork, quelli condivisi, dove tutta o la maggior parte della comunità accetta la modifica, e quelli contenziosi, dove la comunità si

divide in due gruppi dove anche il più piccolo dei due è sufficientemente numeroso (utenti, miners, sviluppatori) da sopravvivere.

Esempi rilevanti di fork contenzioni sono:

Nel 2018 alcuni sviluppatori hanno modificato il parametro che limitava a 1 mb il singolo blocco della blockchain di bitcoin, alcuni hanno seguito questa modifica, altri (la maggior parte) no, da quel momento esistono due bitcoin, Bitcoin (blocchi dati da 1 mb) e Bitcoincash (blocchi dati molto più grandi fino a 10 mb)

Nel 2016 un utente sfruttando una vulnerabilità in uno smart contract scritto nella blockchain di Ethereum (the DAO) è riuscito ad impossessarsi di un ingente importo destinato da alcuni utenti ad investimenti. La fondazione che controlla Ethereum ha deciso di annullare questa operazione (e tutte quelle successive) eliminando un pezzo delle blockchain, molti hanno seguito questa nuova versione, una minoranza è rimasta "fedele" alla versione contenete la transazione definita illecita. Da allora esistono due blockchain di questa valuta, Ethereum e Ethereum Classic.

Esempi di fork condivisi sono numerosi e meno eclatanti, e hanno portato modifiche che hanno migliorato il funzionamento in maniera quasi trasparente per l'utente, qualcosa di molto simile a un aggiornamento dei programmi che avviene periodicamente sul nostro computer.

La governance del consenso di alcune criptovalute

Ogni blockchain e quindi ogni comunità ha una modalità per gestire gli aggiornamenti ed ottenere il massimo consenso possibile in modo da evitare frammentazioni potenzialmente dannosi per l'integrità e la crescita della blockchain.

Riporto di seguito degli esempi, per ovvie ragioni riassunti, di come diverse comunità gestiscono questa esigenza.

Bitcoin

A fronte di una modifica potenziale elaborata da un team di sviluppatori (BIP Bitcoin Improvement Proposal), i miners votano la proposta in essere valorizzando un apposito campo nel blocco appena creato, si ha modo quindi di valutare la popolarità di una proposta contando i miners favorevoli. Il voto però non è capitario (1 miners 1 voto) ma proporzionale alla potenza di calcolo espressa da ogni miners.

Nel caso, precedentemente citato, particolarmente controverso le due fazioni (UASF vs bigblokers), impegnate anche in una piccola "campagna" per coalizzare il consenso, si contesero il

predominio della scelta evolutiva nell'ambito di una riunione dei rappresentanti degli sviluppatori e dei miners, per decidere l'adozione o meno della modifica della size del blocco. La decisione di compromesso fu quindi prettamente "politica", la decisone stessa fu poi ratificata con una richiesta di voto da parte dei miners che, se d'accordo, scrivevano NYA (New York Agreement) nell'apposto campo del blocco minato. Un gruppo minoritario ma rilevante non approvò questa decisione e diede origine ad una biforcazione.

Potenzialmente ogni parametro conosciuto di Bitcoin potrebbe essere modificato, anche quelli con conseguenza rilevanti sul valore della moneta, come ad esempio la modalità produzione quotidiana di valuta, la così detta inflazione delle criptovalute. La salvaguardia della integrità del valore della moneta è affidata a due principi logici e matematici in parte derivanti dalla teoria matematica dei giochi:

- I decisori (miners) sono fortemente coinvolti e partecipi del valore della moneta e sarebbe contro i loro interessi approvare iniziative contrarie all'interesse delle comunità
- Una decisione approvata, che portasse vantaggi a una parte minoritaria della comunità, condurrebbe ad un fork contenzioso della parte maggioritaria e danneggiata, abbandonando gli organizzatori del "colpo di stato" con una blockchain e una valuta inutilizzata e quindi probabilmente fortemente svalutata.

Ethereum

Le decisioni vengono prese dalla fondazione che ha creato Ethereum dopo una consultazione con la comunità. Sono attualmente in corso modifiche molto rilevanti su aspetti sostanziali (passaggio a da Proof Of Work a Proof of Stake), la decisione è stata presa dopo una consultazione con la comunità.

La fondazione e il suo leader nonché inventore, Vitalik Buterin, agiscono come un sovrano illuminato che prende decisioni per il bene di tutti dopo una consultazione non vincolante con la comunità.

Ripple

La società che ha inventato i Ripple e ne detiene la maggioranza decide autonomamente modifiche del software o di altri parametri, ad esempio al momento detiene 50 miliardi di monete in un conto segregato e sta valutando se annullarle, dimezzando così il totale delle monete esistenti.

Polkadot

Ha elaborato un articolato sistema di consenso della comunità che prevede l'interazione tra il concilio (24 membri eletti dalla comunità) e i detentori attivi della moneta (utenti che bloccano le loro monete in prossimità del voto) per gestire le innovazioni. La votazione prevede numerose regole su come contare i voti e su quali maggioranze siano qualificate per ogni tipo di modifica.

Conclusioni

Un insieme di modalità di governance diverse tra di loro e in buona parte giovani e acerbe, poco testate nella pratica rende difficile estrapolare delle conclusioni univoche. Possiamo però trarre almeno le seguenti considerazioni:

- Il software **è modificabile**
- Le modifiche **non sono neutrali** sulle caratteristiche della moneta
- Le modifiche sono decise dalla parte attiva della comunità e hanno conseguenze su tutti gli utenti

In dettaglio possiamo dire che, le tecnicalità di gestione delle blockchain sono modificabili nel tempo e tali modifiche possono variare aspetti così rilevante da incidere pesantemente sul valore economico della criptovaluta sottostante.

Gli individui o gli enti deputati a gestire il cambiamento svolgono un ruolo simile ai governi nazionali o alle banche centrali nel mondo delle valute FIAT.

Tanto maggiore è la concentrazione del potere decisionale in un gruppo ristretto di figure, tanto più lontano dall'idea rivoluzionaria di Satoshi diventa la governance delle blockchain. Ovvero l'idea che il principio degli interessi contrapposti e concorrenti possa evitare che una oligarchia prenda il sopravvento sulla maggioranza degli utenti verrebbe meno.

A questo proposito vale la pena riportare un'analisi effettuata dall'università di Cambridge (https://cbeci.org/mining_map) su un aspetto di questa concentrazione sulla rete di Bitcoin. Tale monitoraggio attualmente riesce a tracciare un po' meno della metà della potenza di calcolo mondiale dedicata al mining, da questa analisi emerge che il 65% della potenza di calcolo di questo campione è concentrata in Cina al secondo posto molto distaccati troviamo gli USA 7%.

Scenari futuri

L'introduzione di concetti come "cloud" "mining" o "valute digitali" hanno diffuso nel pensiero comune l'idea, molto lontana dalla realtà, di attività o beni del tutto eterei e immateriali lontani dalla fisicità. Mentre dati e informazioni transitano su cavi fatti di fibra ottica e risiedono su

apparati realizzati in metallo e custoditi con attenzioni dalle nazioni leader mondiali, ad esempio i principali cavi dati sottomarini sono posati da enti americani e pattugliati dalla flotta militare Usa. L'ubicazione geografica dei server che contengono i dati dei social network che tutti usiamo è oggetto di aspre contese tra gli Usa e le altre potenze emergenti.

Sembra incoerente, che le grandi potenze abbiano finora tentato di controllare il mondo delle criptrovalute tramite norme nazionali, un tentativo destinato a fallire per la natura sovranazionale e distribuita delle blockchain. Mentre non abbiano ancora, ufficialmente, tentato un controllo sulle attività più fisicamente individuabili, come il mining.

Azzardando una analisi geopolitica sugli scenari evolutivi del controllo delle criptovalute possiamo ipotizzare che qualunque ente o governo che volesse controllare o almeno influire sulle scelte evolutive di una criptovaluta non avrebbe altra scelta logica se non quella di coinvolgersi nella sua amministrazione, ad esempio per la blockchain di Bitcoin tramite un coinvolgimento nel mining. Una sorta di attività di "mining istituzionale".

In conclusione possiamo dire che la conoscenza profonda dei metodi di governance di una blockchain unita alle risorse di uno stato o ente sovranazionale potrebbero di fatto consentire a quella realtà di mettere sotto il proprio "controllo" una criptovaluta, andando a influire sulla gestione monetaria di una valuta usata al di fuori dei propri confini, e nel caso di Bitcoin sempre più diffusa a livello mondiale.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/05/25/amministrazione-della-blockchain-una-scelta-tecnica-o-una-scelta-politica-quis-costodiet-custodes/

© 2026 Istituzioni24