Bitcoin slavechain: una rivoluzione del concetto di sidechain

In questo articolo introduco il concetto di slavechain, che rivoluziona il concetto di "sidechain" di Bitcoin, fino ad oggi definita come una blockchain che utilizza un derivato di Bitcoin (tramite peg-in) come token nativo per pagare le transazioni.

[L'articolo originale è pubblicato in data 23/10/22 qui https://sequentia.io/bitcoin-slavechain]

1. Innovazione senza speculazione

Adam Back è fra i padri del concetto di sidechains e co-autore del paper che presenta al mondo l’idea, descrivendola come una blockchain che non introduce un nuovo token nativo per pagare le commissioni di transazione, ma impone un derivato di Bitcoin. Qual è lo scopo? “Innovation without speculation”.

In un panel di Bitcoin Amsterdam, Paul Sztorc, ideatore della proposta BIP300 detta “drivechains”, concorda apertamente con Adam Back sul fatto che l’idea fondamentale alla base delle sidechain sia proprio la sperimentazione di nuove tecnologie, senza inflazionare l’offerta monetaria oltre i 21 milioni bitcoin, senza cioè generare monete alternative Bitcoin.

Se è difficile, talvolta impossibile, sperimentare o sviluppare innovazioni direttamente sulla blockchain di Bitcoin, con le sidechain è possibile innovare senza dover lanciare una nuova moneta sul mercato.

2. Il token si, la cryptovaluta no

Token di qualsiasi tipo possono avere una valida ragione d’esistere su blockchain, tant’è che la tokenizzazione di asset reali è fra le funzionalità comunemente supportate in qualsiasi sidechain ad oggi presente sul mercato. Tuttavia, si tratta di “token”, non di “cryptovalute”. I token hanno un caso d’uso particolare e non intendono rappresentare un’alternativa monetaria a Bitcoin.

La **prima ragione** per stare alla larga dalle crypto è che le **altcoin** (coin alternative a BTC) sono viste come **concorrenti dell'unica moneta.** La moneta è uno standard di mercato e in un libero mercato digitale e globale, di moneta può essercene solo una, con un'offerta limitata e nota a tutti. Utilizzare altcoin introduce solo frizioni negli scambi e incertezza, aumentando l'effettiva inflazione di contante digitale scambiabile in modo peer-to-peer, che deve rimanere fissa a 21 milioni (l'offerta massima di BTC).

Una **seconda ragione** è che creare altcoin può introdurre **incentivi perversi** che vanno a detrimento del corretto sviluppo di una data tecnologia, come team o entità che centralizzano la governance della blockchain nelle loro mani, talvolta trascurando i tempi e le giuste modalità di sviluppo in favore di obiettivi "aziendali", come la massimizzazione del profitto, intraprendendo iniziative di marketing ingannevoli o che possono essere diseducative per la community o, addirittura, soccombere alle tentazioni di corruzione, soldi facili e speculazione.

3. Cosa non va nelle sidechains

Ogni nuova blockchain, che si tratti di federazione, merged mining o Proof of Stake, comporta un grado di centralizzazione più elevato di Bitcoin. Ognuna ha i suoi trade-offs, anche se non li trattiamo in questa sede. Ma di tutti gli elementi centralizzanti, la necessità di utilizzare un BTC peg come asset nativo come "carburante" (gas o fee) di ogni transazione, è nella maggioranza dei casi il fattore più centralizzante, e questo vale sia che l'emissione sia fatta tramite Coinswitch, un nodo PowPeg o un funzionario della federazione.

Tuttavia, questo fatto per lo più non è nemmeno percepito come un problema. Infatti, finché non viene esplicitata la ragione d'essere di una sidechain in una prospettiva business, non vi

è nemmeno alcun fondamento per supportare né criticare la relativa architettura tecnologica.

Forse, questo è proprio il motivo principe per cui le sidechain di Bitcoin non hanno (ancora?) raggiunto un'adozione diffusa nel mercato: manca una definizione del loro **business scope** e della domanda di mercato che si suppone debbano soddisfare.

4. Lo scopo delle sidechain

Le sidechain non sono fatte per sperimentare tecnologie che possano essere portate, in un futuro indefinito, su Bitcoin, sebbene possano anche aiutare al riguardo. Se questo fosse l'unico scopo, nessuno stretto vincolo di tipo economico dovrebbe essere imposto, come la necessità dell'uso di derivati di BTC, né un effettivo lancio sul mercato.

Se ragioniamo in una prospettiva di business e in termini di domanda di mercato, l'obiettivo finale di una nuova blockchain con un derivato Bitcoin può essere soltanto la **tokenizzazione di asset,** come la creazione di token "di utilizzo" (in genere token spendibili per specifici servizi, siano essi parte delle logiche della blockchain o esterne ad esse, come buoni sconto o badges) e securities (in genere token che rappresentano un diritto reale, azioni, obbligazioni, altri strumenti finanziari).

Al di là di sogni e speranze per il futuro, a partire dai Volcano bonds in El Salvador, fino a un futuro in cui l'intero mondo finanziario può viaggiare su blockchain, già oggi vediamo un enorme mercato su blockchain per dApp finanziarie, trading peer-to-peer (DEX) e asset tokenizzati come le stablecoin e un valore di 8 miliardi di dollari di BTC peg in altre blockchain (es. wBTC, hBTC, renBTC etc.)

Lo scopo di avere tokenizzazione su blockchain è la decentralizzazione del trasferimento, della custodia e del

“settlement” degli asset tokenizzati. Ma le attuali sidechain non hanno un’architettura ottimizzata per tale scopo, vuoi per via dell’uso di derivati tramite “peg-in” usati come token nativo per pagare le commissioni di transazione, vuoi per via della gestione della governance sulla blockchain: ad esempio le federazioni richiedono un insieme definito di “funzionari” che creino i blocchi, finendo inevitabilmente per essere organismi semi-centralizzati.

5. Un cambio di prospettiva: l’interoperabilità

Facendo un sunto dei concetti finora discussi, possiamo dire che una sidechain dovrebbe avere le seguenti caratteristiche:

1. Permettere la tokenizzazione di assets
2. Non introdurre una nuova moneta alternativa a Bitcoin
3. Essere il più decentralizzata possibile, il che implica anche che l’uso di derivati come token nativi dovrebbe essere evitato

A queste, aggiungo una quarta caratteristica che, sebbene sia già pubblicizzata come elemento desiderabile (per esempio in Liquid), finora non è – a mia conoscenza – mai stata considerata una priorità nel design di una sidechain Bitcoin.

4. Massimizzare la possibilità di usare Bitcoin o interagire con Bitcoin direttamente (come moneta di scambio)

Possiamo chiamare quest’ultima caratteristica “**interoperabilità”** con la blockchain Bitcoin. Più nello specifico, si tratta di scambiare direttamente BTC per asset tokenizzati sulla sidechain tramite operazioni cosiddette “cross-chain”, come gli atomic swap o altri contratti HTLC (hashed timelock contracts).

Per quest'ultimo obiettivo è vantaggioso adottare un'architettura che è più vicina a Bitcoin, con una struttura UTXO e che utilizza Bitcoin script, piuttosto che le alternative quali l'architettura in stile Ethereum di Rootstock. Ma si può andare molto oltre per integrare ancora meglio Bitcoin.

Infatti ad oggi, un semplice atomic swap richiede lunghi intervalli temporali dovuti alla possibile inconsistenza degli stati di un'operazione cross-chain presenti sulle due blockchain coinvolte. Ma anche a questo c'è un rimedio.

6. Slavechain di Bitcoin

Introduco qui l'idea di una sidechain che segue la blockchain di Bitcoin in un modalità puramente master-slave.

Il fullnode della "slavechain" si appoggia a un fullnode Bitcoin e considera validi solo i blocchi della slavechain che incorporano l'hash di un blocco Bitcoin uguale o successivo a quello incorporato nel blocchi precedenti della slavechain. Se la blockchain Bitcoin scarta ("orfana") un blocco o effettua una riorganizzazione ("reorg"), anche la slavechain ne è affetta, scartando tutti i blocchi creati al di sopra dei blocchi Bitcoin "orfanati". Abbiamo battezzato questo meccanismo "**anchoring**".

Tale meccanismo annulla la possibilità che un'operazione cross-chain sparisca dalla blockchain Bitcoin per via di un reorg, rimanendo però presente sulla sidechain. Tuttavia, non garantisce che avvenga il contrario. Che succede se l'operazione sparisse invece dalla sidechain?

Per risolvere questo problema, possiamo sfruttare un concetto detto "finalità immediata" delle transazioni. In sostanza, la sidechain deve avere un'architettura che non permette i fork ("**forkless**"). Una Proof of Authority (PoA) o un'alternativa semi-centralizzata (come la federazione di Liquid) hanno tale

architettura. Per esempio, in Blockstream Liquid ogni blocco è pre-approvato con un quorum di 11 di 15 membri della federazione.

Il problema con tali approcci è che sono troppo centralizzanti. Fortunatamente, c'è un'alternativa. Sistemi di Proof of Stake (PoS) come Tendermint e Algorand sono basati su una finalità immediata delle transazioni, tramite il raggiungimento a monte di un quorum di co-firmatari dei blocchi. Sebbene queste presentino i tipici trade-off dei PoS, tale design è senz'altro molto più decentralizzato di una PoA o una federazione chiusa. Effettivamente, possono essere concepiti come "**federazioni aperte**".

In ogni caso, vi è un grosso problema "ideologico" che si può sollevare a questo punto: la Proof of Stake richiede una cryptovaluta, non si può fare con un peg-in. E anche se si potesse, sarebbe comunque alle spese della decentralizzazione. Introdurre una cryptovaluta contraddice i principi che abbiamo dichiarato poc'anzi, riguardo le forme alternative di moneta?

7. Federazione aperta con un governance token

Per assicurarci la massima interoperabilità con Bitcoin, o rinunciamo alla decentralizzazione (PoA o federazione "chiusa") o introduciamo una altcoin per un PoS. A prima vista, pare che non ci siano altre opzioni. Tuttavia, possiamo mitigare tale problema modificando la "cryptovaluta" usata in un meccanismo PoS al fine di renderla soltanto un "token", cioè rimuovendone tutti gli elementi e funzioni di tipo monetario e, di conseguenza, il ruolo di concorrente a Bitcoin.

Anzitutto, la slavechain **non deve avere un token nativo** per pagare le commissioni di transazione. Questo significa che deve essere possibile pagare le commissioni di transazione ai

creatori dei blocchi in qualsiasi tipo di token emesso sulla slavechain (ovviamente, replace by fee è un must-have per i wallet).

Questo **libero mercato delle commissioni di transazione** è un nuovo esperimento che potrebbe essere rivoluzionario per il settore. È probabile che i token con maggiore liquidità (ad esempio le stablecoin più note), saranno accettate come standard, mentre i creatori dei blocchi recupereranno informazioni relative al prezzo e caratteristiche degli assets (es. volatilità, liquidità) in tempo reale da piattaforme exchange centralizzate, dai DEX, oppure da oracoli che si pronuncino sulla desiderabilità di ogni token.

Secondariamente, non deve esserci generazione di nuove monete, ovvero **inflazione**. Il token di "governance" sottostante al meccanismo PoS deve cioè rappresentare soltanto una quota fissa del potenziale di capacità di creazione dei blocchi presente nel network. Insomma, il sistema PoS non rappresenta altro che un tentativo di creare un Consenso più inclusivo per una sidechain Bitcoin, che sia anche più trasparente e aperto al mercato rispetto a una Proof of Authority o una "federazione chiusa".

8. L'approccio giusto alla speculazione

Anche se aggiriamo il problema della presenza di una cryptovaluta, rimane sempre l'emissione di un token, potenzialmente con una ICO per un lancio sul mercato. Questo ovviamente viene con tutti i rischi descritti sopra, come un approccio aziendale che guarda al profitto, o la possibilità di corruzione. Tuttavia, vi sono tre considerazioni che possiamo fare al riguardo.

Primo, il fatto che lo sviluppo non sia finanziato tramite una ICO non significa necessariamente che non vi sia speculazione.

Sebbene non impossibile, è molto raro il caso in cui una tecnologia di qualsiasi tipo sia sviluppata senza incentivi economici, fra i quali vi sono spesso i profitti di tipo aziendale. Senz'altro, questo si applica anche a varie sidechain. Sarebbe naïve pensare altrimenti.

Secondo, anche se il problema del vil danaro non può essere rimosso a livello teorico, nella pratica molte azioni possono essere adottate per mitigare questi rischi e trasformare un approccio "corporate" in un sistema inclusivo guidato alla community ("community-driven"). In questo articolo, per esempio, spieghiamo l'approccio che stiamo adottando per Sequentia.

E **terzo**, dobbiamo considerare anche l'altro lato della medaglia: la speculazione porta più soldi per lo sviluppo, più utenti, un maggiore effetto network e – come dato di fatto – più servizi e piattaforme exchange che installeranno il nodo. Questo significa anche che ogni progetto che emette asset sulla sidechain avrà automaticamente accesso a un mercato molto più grande. Se un progetto sidechain avesse mai la possibilità di detronizzare Ethereum o Binance Smart Chain (giusto per nominarne un paio ad oggi in voga), ci vuole un'enorme potenza di fuoco. È davvero possibile ottenerla senza speculazione?

9. Costruire una slavechain

Sequentia (sequentia.io) è il nome del progetto slavechain che stiamo portando avanti. Per massimizzare l'interoperabilità con Bitcoin si tratta di una UTXO chain con Bitcoin script e implementa sia l'anchoring che il concetto di immediate finality, in un sistema ibrido fra alcuni elementi di un Pos (ispirati ad Algorand) e PoW (sfruttando il protocollo Bitcoin per determinare i partecipanti nei round di creazione dei blocchi). Parte della codebase è costruita su Elements (sfruttata da Blockstream Liquid) così da avvantaggiarsi del

prezioso lavoro già prodotto dalla community.

Grazie alla peculiare architettura “forkless” con ancoraggio a Bitcoin, permette atomic swaps veloci e affidabili, così come anche i lightning swaps.

Non si affida ad alcuno specifico meccanismo di peg-in (seguendo l’approccio “multisignatures are not sidechains”) usato come token nativo, né alcun nuovo OP_CODE o cambiamento in Bitcoin come BIP300 Drivechains.

Ogni token può essere utilizzato per pagare le commissioni di transazione (open fee market) e non c’è inflazione, per evitare che il token di governance sia etichettato come “altcoin”.

Il full node deve rimanere accessibile e la blockchain potenzialmente sempre verificabile dall’utente medio, mantenendo una portata (throughput) relativamente bassa di transazioni on-chain.

Infine, la governance del progetto limita i rischi speculativi derivati dall’emissione di un token, sia grazie a una struttura community-driven con un’entità non-profit, sia tramite una distribuzione trasparente dei token nella community e con tempi di vesting lunghissimi (ad esempio, i token allocati al team sono bloccati per 4 anni dal lancio della mainnet e si sbloccano completamente soltanto in 8 anni).

Più informazioni si possono trovare nella documentazione qui di seguito docs.sequentia.io, incluso un Theoretical Paper per i più tecnici.

Se ti interessa discutere di questa tecnologia, portare critiche costruttive o qualsiasi tipo di contributo, unisciti alla chat telegram cliccando qui sotto (inglese) o quella italiana qui


SEQUENTIA
JOIN THE TELEGRAM COMMUNITY