Come sopravvivere alla Bull Run: scalare con Bitcoin

scritto da Alberto De Luigi | 18 Luglio 2019
La ciclicità dettata dagli halving ci renderà tutti ricchi? Può darsi, ma la Bull Run sarà favorevole a una progressiva e sana adozione, o al contrario Bitcoin dovrà scappare dai tori scatenati?

Contenuti:

- INTRODUZIONE ALLA FOLLIA
- ALTE COMMISSIONI E NIENTE MASS ADOPTION A QUESTO CICLO
- LA TASSONOMIA DELLE BUONE NOTIZIE

I LAYER SUPERIORI:

1. I CUSTODIAN: LAYER SUPERIORE CENTRALIZZATO
2. FEDERAZIONE (LIQUID SIDECHAIN): LAYER SUPERIORE PARZIALMENTE DECENTRALIZZATO
3. LIGHTNING NETWORK: LAYER SUPERIORE DISTRIBUITO

LA BLOCKCHAIN:

1. UPGRADE CAPACITÀ: INCREMENTO DEL BLOCCO E SEGWIT
2. UPGRADE EFFICIENZA: BECH32 E SCHNORR
   2.1 BECH32
   2.2 SCHNORR
3. ORGANIZZAZIONE: BATCHING, COINJOIN, CHANNEL FACTORIES
   3.1 BATCHING
   3.2 COINJOIN CON SCHNORR E SIGNATURE AGGREGATION
   3.3 CHANNEL FACTORIES

- CONCLUSIONE: SCRUTANDO NELLE VISCERE DEL POLLO

INTRODUZIONE ALLA FOLLIA

Molti holder e speculatori di vecchia data si aspettano che il prezzo di Bitcoin rispetti la ciclicità dettata dall'halving, esattamente come si è verificato negli ultimi 8 anni con gli halving del 2012 e del 2016. Il famoso grafico del prezzo in scala logaritmica, quello che correla le fasi di bull and bear coi cicli quadriennali di halving, rappresenta in effetti il pattern più logico e costante che si possa riconoscere fra le montagne russe del prezzo di Bitcoin. Secondo quella proiezione, il prezzo di Bitcoin raggiungerà l'All Time High (ATH) precedente nell'estate prossima, per poi scattare verso l'alto in piena bolla. Per quanto nessuno possa prevedere il futuro, è anche vero che, rispetto alle analisi tecniche da chiromante, una proiezione che si basi su questo pattern ha dalla sua un elemento imprescindibile che non può non impattare anche il prezzo: l'espansione monetaria di Bitcoin si dimezza ogni 4 anni.

Nella primavera 2020 l'espansione monetaria di Bitcoin, intesa come nuova emissione sull'attuale base monetaria esistente, passerà da circa il 3,7% all'1,8%. Ogni anno verranno prodotti 328.500 Bitcoin anziché l'attuale produzione di 657.000. Inoltre, ad oggi esistono circa 17.770.000 Bitcoin, nell'estate 2020 saliremo a 18.400.000, avvicinandoci sempre più al tetto massimo di 21 milioni. Il bull market chiama.

Queste cifre saranno pure fonte di gioia per voi malvagi speculatori, che con la bava alla bocca vi fregate già le mani al pensiero di quanti soldi farete, ma in verità miei cari, per noi idealisti con il cuore puro che crediamo nell'amicizia, nell'amore e nei Bitcoin, questi dati da FOMO sono solo fonte di pensieri tenebrosi. È proprio così, lo vedo già: noi con la Lambo a Portofino, nel nostro yatch da 800 piedi, mentre sul ponte ci cercano per servirci l'aperitivo di ostriche e Armand de Brignac, ebbene noi rimarremo chiusi al buio, in bagno. Ci chiamano, ma noi non rispondiamo. Corrucciati, introversi, rintanati in posizione fetale nell'oscurità, l'espressione attonita e vuota, non riusciremo a fare altro che concentrare ogni nostra energia sulla domanda fondamentale, quella che ci corrode dentro, consumandoci nello

spirito:

“ma allora questo Bitcoin, scala o non scala?”

Eh già, perché col bull market uno tsunami si abbatte sull’economia crypto, e riparte la giostra. TG e quotidiani nazionali ci bombarderanno ogni giorno. Tutti vogliono provarli, sti Bitcoin. C’è traffico nella rete e le commissioni per transazione salgono, salgono, salgono, salgono.

Le prime mutazioni genetiche nella popolazione avvengono in alcune classi specifiche.

Al primo giorno, gli assicuratori si reinventano come hipsters esperti dei mercati: il CV dice AXA e Generali, ma loro millantano vent’anni di trading sul forex e 6 mesi di stage da Blockstream. Al secondo giorno i mutageni colpiscono consulenti, bancari, mariouli, markettari. Pare che Saruman forgi nuovi scammer a ripetizione nelle fabbriche di Uruk-hai. Sembra arrivato il peggio, ma dal terzo giorno compaiono i mutanti di un nuovo fenotipo: quelli che non ti vogliono truffare, ti vogliono solo prosciugare i maroni. Persino il saccente che fino a ieri ripeteva, ancora, la frase più da ritardo mentale del mondo, quella che abbiamo sentito tipo 7 miliardi di volte: “la blockchain si, Bitcoin no…”. Ecco, lui ora ti fa le poste per strada, sbuca da dietro una colonna come per caso, per chiederti se è meglio comprare su Kraken o Coinbase Pro.

Insomma il popolo tutto va in vacca, è l’apocalisse zombie. Li vedi correre affamati per le strade della FOMO col cervello fritto in salsa di fast market e cocaina, gridando le più insensate scemenze di ogni fatta pro e contro Bitcoin. E nel dubbio, comprano.

Al settimo giorno di ATH segnalato dai TG, il demonio è arrivato a lambire persino la signora Giacoma. Ora l’incontro sul pianerottolo è diventato inquietante. Non ti sorride più

come prima. Prima tu eri il bravo giovinotto nerd che sale le bottiglie di acqua e scende la spazzatura, e il suo sorriso era sincero, disinteressato, quasi materno. Oggi in quel sorriso, qualcosa rimane in sospeso, un silenzio protratto, un momento di imbarazzo. Lo sai, vuole dire qualcosa la Giacoma, ma non lo dice. Aspetta il momento giusto? Pensa di essere inopportuna? Si farà coraggio solo stasera dopo l'ennesima notizia al tg nazionale? Tu sei sospettoso, ormai cammini rasente i muri, te lo aspetti da chiunque. E dietro quel sorriso apparentemente innocente, sul pianerottolo, ecco si, lo vedi, lo riconosci, quel brillio in fondo agli occhi. Quell'aura maligna di avidità si è presa anche lei! Alla fine cala la maschera e non ci sono più dubbi: "uagliò comm' accatt' sti baatcoin?".
Anche la Giacoma è posseduta.

ALTE COMMISSIONI E NIENTE MASS ADOPTION A QUESTO CICLO

Così, sempre più gente prova a trasferire qua e là Bitcoin, mediante transazioni onchain, sembra quasi per dispetto. Ci riempiono la mempool e noi siamo costretti ad aprirci i canali Lightning scucendo milioni di satoshi. E il dubbio può assalire anche le menti più pure: "ma non costerà troppo aprire un canale Lightning per un utente qualsiasi senza Lambo né yatch?"

A onor del vero, dopo il famoso crollo del prezzo di gennaio 2018, le commissioni per transazione Bitcoin sono scese sotto la soglia dell'euro e fee più alte sono state rare eccezioni. Oggi, a luglio 2019, si può ottenere una conferma nel primo blocco pagando 5 centesimi di commissione. Servizi che basano il loro business sulle micro-transazioni onchain possono ancora prosperare tranquilli. Una transazione pesa mediamente circa 250 bytes e allo stato attuale della mempool è conveniente impostare una fee di 2 satoshi per byte, quindi 500 satoshi, che equivalgono a 5 centesimi di euro con un prezzo del bitcoin a 10 mila euro. Chi è ancora poco avvezzo, dovrebbe abituarsi a ragionare in satoshi, perché presto sarà

l’unità di misura più utilizzata nel mondo delle cryptovalute.

Tuttavia, anche nell’ultimo anno e mezzo ci sono stati dei brevi periodi in cui il traffico di transazioni sulla rete ha spinto le commissioni intorno a picchi di 200 satoshi per byte, quindi fino a 5 euro (al prezzo di oggi). Da questo marzo, questi periodi si sono fatti sempre più frequenti, e in prospettiva non sarà che peggio. Perché se anche la tecnologia per scalare c’è, gli utenti non la usano, non si è ancora sviluppato l’ecosistema giusto, manca una vera rete di canali di pagamento su layer 2 (non necessariamente Lightning Network, come vedremo). Insomma, gli utenti non hanno i mezzi per usare la tecnologia o non sono ancora istruiti a sufficienza. Quasi tutti transeranno onchain, finché smetteranno di transare perché sarà troppo costoso.

Insomma l’anno 2021 potrà essere epico per tante ragioni, forse sarà ricordato come l’anno in cui Benetazzo, allo squeeze dell’ennesimo short, si prostrerà ai piedi di Barrai in segno di definitiva sconfitta, come L dinanzi a Kyra. O sarà l’anno in cui Marco Casario potrà finalmente pagarsi la vacanza su spiaggia deserta anche senza vendere un solo corso di trading. Penserete che tutto ciò è sicuramente eccitante – e avete ragione – purtroppo però, rimane il fatto che il 2021 non sarà ricordato come l’anno della mass adoption. Dovremo aspettare almeno un altro ciclo.

LA TASSONOMIA DELLE BUONE NOTIZIE

Ma non c’è affatto da essere pessimisti. Chi è all’avanguardia sta già usando tutti gli strumenti disponibili nel modo giusto. Bitcoin può scalare e tecnicamente può sostenere una mass adoption, la quale è comunque una questione più culturale che tecnologica. Come dicevo nell’articolo pluripremiato con 7 Pulitzer e il blessing di Zucco “Bitcoin è libertà”, dieci anni sono ridicolmente pochi per una rivoluzione epocale come Bitcoin, la cui utilità non viene nemmeno compresa dalla maggioranza della popolazione. Non abbiamo di cui

preoccuparci, la tecnologia senz'altro precede la trasformazione culturale delle masse.

Si dice spesso che, anche con Lightning Network pienamente funzionante, per scalare a decine o centinaia di milioni di transazioni al giorno (Visa ne processa 150 milioni) sia necessario un blocco enorme rispetto a quello attuale, poiché soltanto la chiusura e apertura dei canali richiede un throughput molto elevato onchain. Non è così. La forza della scalabilità di Bitcoin non sta solo in Lightning Network, ma nelle evoluzioni in due distinte macroaree, che a loro volta suddivido in tre tipologie, giusto per il sadico gusto di farvi venire il mal di testa con tassonomie pseudo-scientifiche.

Una macro-area concettuale comprende tutte le strutture costruite sulla blockchain Bitcoin (i famosi layer 2, come Lightning Network), l'altra macro-area è ovviamente la tecnologia blockchain stessa, in continua evoluzione, e l'utilizzo che ne viene fatto a livello di ecosistema (che può essere più o meno bene organizzato). Di seguito riporto questa tassonomia con esempi che discuteremo punto per punto.

STRUMENTI DI SCALABILITÀ DI BITCOIN:

LAYER SUPERIORI

CENTRALIZZATO	CUSTODIAN
DECENTRALIZZATO	FEDERAZIONE (SIDECHAIN)
DISTRIBUITO	LIGHTNING NETWORK

BLOCKCHAIN

UPGRADE CAPACITÀ	BLOCKSIZE INCREASE
UPGRADE EFFICIENZA	SCHNORR, SEGWIT BECH32
ORGANIZZAZIONE	BATCHING, COINJOIN, CHANNEL FACTORIES

I LAYER SUPERIORI:

1. I CUSTODIAN: LAYER SUPERIORE CENTRALIZZATO

Decentralizzare, essere autonomi, incensurabili e poter controllare a piacere i propri soldi non sono concetti necessariamente incompatibili con l'utilizzo (anche) di banche o, più in generale, custodian come exchange, carte prepagate, o qualsiasi servizio di intermediazione finanziaria.

Riconoscere i difetti dell'attuale regime monetario non significa che debba essere considerato un atto di vergogna il fatto di caricare dei soldi o bitcoin su una prepagata, sulla carta del supermercato o su paypal. Dopotutto, finché il grosso dei nostri risparmi è al sicuro in un wallet Bitcoin, e se abbiamo modo di eseguire in totale autonomia le transazioni per cui necessitiamo di privacy, o per quelle che altrimenti rischierebbero di essere censurate, possiamo comunque avvalerci degli intermediari che ci fanno comodo per altri pagamenti. Anzi, maggiore è il numero e la varietà di questi intermediari presenti sul mercato e meglio è.

Pagare tramite un layer 2 è preferibile piuttosto che transare onchain intasando la mempool, se è possibile farlo senza mettere a repentaglio la nostra sicurezza e autonomia. Se per incapacità o impossibilità dettata dalla situazione non siamo in grado di utilizzare Lightning Network, anche i libri contabili di un custodian possono costituire un buon layer 2, a patto di depositare presso di esso una quantità di valore non più elevata di quanto necessario per processare i propri pagamenti ordinari.

Un custodian permette di scalare perché svolge la funzione di camera di compensazione, sia internamente (fra account di utenti che usano lo stesso custodian) che esternamente (canali fra custodian diversi).

- **Internamente**, perché se A e B si scambiano bitcoin e il custodian detiene in riserva fondi di entrambi, quest'ultimo non farà altro che scrivere su un database

la contabilità del passaggio di denaro, potendo così gestire potenzialmente infinite transazioni senza che la blockchain venga toccata. Ad esempio, spostare soldi fra un account e l'altro di Coinbase, Coinsbank o moltissimi altri servizi, è gratuito ed istantaneo.

- **Esternamente**, tramite due vie: 1) un semplice contratto fra custodian, oppure 2) un layer superiore alla blockchain sfruttabile da un custodian (ad esempio sidechain come Liquid, ma anche Lightning Network). Per quanto riguarda il semplice contratto, diversi custodian possono accordarsi fra loro e costituire camere di compensazione bilaterali, dove ad esempio due custodian permettono agli utenti di spostare fondi dall'uno all'altro e tracciano questi spostamenti solo nei rispettivi libri contabili, eseguendo una transazione onchain di compensazione solo – ad esempio – a fine mese. Ad oggi queste soluzioni non sono molto adottate (non vi è notizia di casi significativi), anche perché per un contratto di questo tipo è richiesta molta fiducia fra i due custodian, mentre vi sono layer più sofisticati e che richiedono di fidarsi meno di una singola controparte, come approfondito nel prossimo paragrafo.

2. FEDERAZIONE (LIQUID SIDECHAIN): LAYER SUPERIORE PARZIALMENTE DECENTRALIZZATO

"Liquid: parzialmente decentralizzato!". Sembra quasi la recensione di un nuovo latte +, e invece è la sidechain creata da Blockstream. Si tratta solo di un esempio di layer di questo tipo, ma è senz'altro il più significativo, avendo come partner e tester 23 aziende fra cui Bitfinex, BitMEX, XAPO, OKCoin, The Rock Trading.

Il funzionamento prevede che ogni exchange blocchi sulla blockchain di Bitcoin un certo ammontare di btc, per cui vengono sbloccati i "btc Liquid" sulla sidechain. Dopo un numero potenzialmente infinito di transazioni usando "btc

Liquid", quando un exchange vuole uscire dalla sidechain perde i suoi "btc Liquid" e torna in possesso dei btc sulla blockchain Bitcoin. In questo modo tutte le transazioni che gli utenti effettuano fra un exchange e l'altro possono essere processate dalla sidechain anziché intasare la mempool e aumentare il traffico sulla blockchain di Bitcoin.

La sidechain è una catena di blocchi conservata presso i nodi dei custodian. Non ha proof of work, i "miner" che creano il blocco sono gli exchange/custodian stessi che concordano nel "firmare" il blocco successivo tramite "voto" a maggioranza. Insomma, la sidechain è come la camera di compensazione che processa i pagamenti fra custodian, con la differenza che non è necessario fidarsi solo di una singola controparte, ma della maggioranza dei partecipanti che aderiscono alla "federazione". Il sistema continua a funzionare finché almeno *n* exchange su *m* aderiscono firmando i nuovi blocchi. Possono esserci dei problemi (ad esempio i fondi vengono tenuti in stallo perché la maggioranza è corrotta o subisce un attacco), perciò il custodian aderisce a un progetto simile solo se pensa che sia vantaggioso fidarsi della maggioranza di un gruppo di aziende note piuttosto che di una sola controparte. Soprattutto però, il vantaggio più grande e che rende questo strumento molto più efficace per la scalabilità è il fatto che, in una federazione, tutti i partecipanti possano liberamente scambiare fra loro offchain, anziché dover aprire un canale bilaterale con un'unica controparte.

Fino ad ora abbiamo parlato di layer che dal punto di vista della decentralizzazione sono peggiorativi rispetto agli scambi onchain di Bitcoin, perciò è lecito chiedersi se un utilizzo a livello aggregato di questi layer possa comportare dei problemi sul piano socio-economico. Non c'è dubbio che, in un'economia Bitcoin, custodian e federazioni non abbiano il potere distruttivo e distorsivo delle dinamiche produttive che invece è in mano a banche e banche centrali del regime vigente in moneta fiat. Infatti, per chi custodisce bitcoin è molto

più difficile praticare in modo non trasparente la riserva frazionaria e, di conseguenza, un'espansione monetaria. I bitcoin su blockchain non si possono "duplicare" e una verifica dei bilanci dei custodian (proof of reserve) è molto più semplice e pratica, oltre che trasparente al pubblico, rispetto alla verifica dei bilanci bancari e al calcolo dell'espansione monetaria effettuata tramite l'attività creditizia, che crea moneta fiat dal nulla. Dall'altro lato, anche i layer 2 sono completamente trasparenti da questo punto di vista, perché sono creati tramite un "peg" uno-a-uno coi bitcoin in blockchain (il che vale per Liquid come per Lightning Network).

In ogni caso, anche in un'economia Bitcoin utilizzare un custodian per quanto possa essere utile, va fatto con cautela: è bene mantenere la maggior parte del proprio valore altrove. Lo stesso vale per una federazione di più custodian, che può sì essere "decentralizzata", almeno da un punto di vista geografico e anche di giurisdizione (aziende che lavorano in continenti diversi, sotto regole e "sovrani" diversi), ma non si può escludere che la collaborazione mafiosa fra Stati, tiranni o maggioranze democratiche parassitarie possa minare l'integrità della maggioranza di tali custodian, mettendo a repentaglio il sistema.

3. LIGHTNING NETWORK: LAYER SUPERIORE DISTRIBUITO

La soluzione principe è ovviamente Lightning Network, di cui si parla estensivamente **qui** (per i meno tecnici) o **qui** (per i più tecnici), oltre che nella relativa voce di glossario. La critica principale che si muove a Lightning Network è il fatto che, nonostante permetta di transare a livelli esponenzialmente più elevati rispetto alla blockchain, richieda comunque un aumento molto consistente della dimensione dei blocchi.

Per rispondere a queste critiche, è bene anzitutto immaginare un caso pratico di come un canale Lightning sarà

effettivamente utilizzato in caso di adozione di massa, per poi tirare le somme relativamente a quanto sia lo spazio necessario su blockchain a livello aggregato.

Nello scenario descritto non si considererà l'impatto di alcuna tecnologia LN ancora non funzionante o non adeguatamente testata: nemmeno Atomic Multipath Payments (che permette a un pagamento di grandi dimensioni di essere diviso fra più canali) né i Dual Funded Channels (per aprire un canale tramite il funding di entrambe le controparti anziché una sola) né di conseguenza i Multi-party Funded Channels (le così dette Channel Factories di cui parleremo poi).

Quanto espongo qui è dunque una mia ipotesi dell'operatività di LN che è possibile già oggi. L'ipotesi del seguente scenario prevede quindi l'utilizzo di una tecnologia che, pur essendo acerba rispetto agli sviluppi potenziali, è comunque perfettamente funzionante. Possiamo quindi aspettarci che quando arriveremo alle prime fasi di reale "mass adoption" sarà ben consolidata, con wallet user friendly alla portata di tutti.

È un'opinione personale, ma a differenza di quanto si possa leggere in rete, credo che i canali Lightning, in questo primo stadio di adozione su larga scala, saranno di dimensioni relativamente grandi, con un valore che raggiunge anche alcune migliaia di euro, o comunque abbastanza capienti da permettere di trasferire un intero stipendio in un solo canale.

Pensiamo ad esempio ad un lavoratore dipendente:

- Per gestire qualsiasi entrata ordinaria (lo stipendio), l'utente può utilizzare un solo canale, quello aperto col datore di lavoro
- Anche per gestire le uscite (le spese), l'utente può utilizzare il canale aperto col datore di lavoro come principale router. Poiché generalmente un individuo non spende nell'arco di un mese più di quanto guadagna in un

mese, il canale avrà capienza sufficiente per coprire qualsiasi uscita ordinaria.

- Tendenzialmente, un utente potrebbe avere un solo canale Lightning, o comunque un canale principale che è il veicolo di quasi tutte le sue transazioni.
- Ipotizzando che un lavoratore dipendente ogni mese riesca a risparmiare una limitata quantità di bitcoin del suo salario mensile, allora dovrà integrare (o chiudere e riaprire) quell'unico canale Lightning molto raramente nell'arco di un anno.
- Stando alle ipotesi 1-4, una regola che permetta di stimare la frequenza di utilizzo della blockchain da parte di tale lavoratore dipendente è la seguente: *dati "s" il salario e "c" la capacità del canale, avverrà una nuova transazione onchain in un lasso di tempo equivalente al tempo in cui il dipendente riesce a risparmiare una quantità di denaro* $d > c - s$

Di seguito spieghiamo quest'ultimo punto (5) con un esempio. Se annoiato dal tecnicismo, il lettore è invitato a passare direttamente all'ultimo capoverso di questo capitolo, passando quindi poi alla sezione **BLOCKCHAIN**.

Ipotizziamo di essere Bob, un operaio specializzato che lavora per FCA (Fiat Chrysler Automobiles) con uno stipendio di 2000 euro (in btcoin). Ipotizziamo anche che la sua spesa media mensile sia di 1500 euro, quindi se un mese spende 1000 euro, quello successivo ne spenderà 2000 e così via, per tornare a una media di 1500. Per semplicità, rappresenteremo il valore spostato sui canali Lightning in euro, ma ovviamente verranno transati solo dei bitcoin.

All'atto di assunzione, FCA apre un canale di credito da 3000 euro con l'operaio dipendente. Immaginiamo che quest'ultimo spenda gran parte del suo stipendio su Amazon e all'Esselunga. Possiamo ipotizzare che FCA, Amazon ed Esselunga, in quanto grosse aziende, abbiano vari canali Lightning aperti e che vi sia almeno 1 canale diretto fra di esse (il che ci aiuta anche

a semplificare la nostra rappresentazione).

Al momento, il canale aperto fra Bob e FCA ha 3 mila euro, tutti in possesso di FCA. Lo rappresentiamo quindi come segue, dove “0” (zero) sono i soldi di Bob sul canale, e “3” i tre mila euro di FCA:

Bob-FCA: 0 | 3

Rappresentiamo quindi lo stato iniziale del canale al giorno del primo salario di Bob, ovvero quando 2 mila euro vengono versati da FCA al suo dipendente Bob:

Bob-FCA: 2 | 1 (Bob riceve 2k euro di stipendio)

Sempre per ipotesi, anche il canale fra le aziende è di 3 mila euro, di cui 2 mila detenuti da FCA in entrambi i canali

FCA-Amazon: 2 | 1

FCA-Esselunga: 2 | 1

Durante il primo mese, Bob fa la spesa varie volte all’Esselunga, spendendo in totale mille euro, perché ha molta fame. FCA fa da canale intermediario, per cui ad ogni spesa prende dei soldi da Bob e ne rilascia altrettanti all’Esselunga, nel rispettivo canale, per un totale di mille euro. Siamo nello Stato 1.

STATO 1:

- **Bob-FCA: 1 | 2 (Bob paga 1k euro)**
- **FCA-Amazon: 2 | 1**
- **FCA-Esselunga: 1 | 2 (Esselunga incassa 1k euro)**

Ora il balance di FCA è invariato poiché detiene in totale 5 mila euro come prima (se sommiamo la disponibilità fra tutti i suoi canali), ma la distribuzione fra canali è cambiata, per via del pagamento che Bob ha fatto all’Esselunga usando i

canali di FCA come intermediario.

Bob a fine mese ha un risparmio di 1000 euro. I 2000 euro restanti sono perciò sufficienti ad accogliere un nuovo stipendio, di conseguenza si può continuare ad utilizzare quel canale Lightning.

Passa il secondo mese e FCA paga il secondo stipendio a Bob:

STATO 2:

- **Bob-FCA: 3 | 0 (Bob riceve 2k euro di stipendio)**
- **FCA-Amazon: 2 | 1**
- **FCA-Esselunga: 1 | 2**

Abbiamo detto che Bob spende mediamente 1500 euro. Avendone spesi 1000 il mese precedente, questo mese ne spenderà 2000. A questo giro fa acquisti sia all'Esselunga che da Amazon, sempre avvalendosi del canale di FCA. Alla fine del mese la situazione sarà:

STATO 3:

- **Bob-FCA: 1 | 2 (Bob spende 2k euro)**
- **FCA-Amazon: 1 | 2 (Amazon incassa 1k euro)**
- **FCA-Esselunga: 0 | 3 (Esselunga incassa 1k euro)**

Percepisce quindi lo stipendio del terzo mese:

STATO 4:

- **Bob-FCA: 3 | 0 (Bob riceve 2k euro di stipendio)**
- **FCA-Amazon: 1 | 2**
- **FCA-Esselunga: 0 | 3**

Questo mese Bob spenderà solo 1000 euro, ipotizziamo presso Amazon:

STATO 5:

- **Bob-FCA: 2 | 1 (Bob spende 1k euro)**
- **FCA-Amazon: 0 |3 (Amazon incassa 1k euro)**
- **FCA-Esselunga: 0 | 3**

Alla fine del terzo mese, Bob ha superato la soglia di risparmio di 1000 euro, avendone accumulati 2000. Si è avverata la condizione che avevamo enunciato: d > *c* – *s.* Al quarto mese quindi FCA non ha spazio nel canale aperto per pagare uno stipendio di 2 mila euro a Bob, poiché supererebbe la somma limite per la capacità del canale aperto con FCA. È quindi necessaria una nuova transazione onchain, dove FCA "ricarica" il canale, mentre Bob sposta i suoi risparmi, che può trasferire:

1. in un suo wallet LN alternativo tramite una transazione offchain, oppure
2. nel proprio cold wallet tramite una transazione onchain.

L'opzione (a) è la più interessante: avere un canale aperto con sé stessi è comodo perché significa avere accesso alla "liquidità" di LN (facilità di movimentazione dei propri soldi nell'istantaneo, pagando commissioni minime) pur non necessitando di monitorare il canale né tramite watchtower, né tornando online periodicamente per controllare lo stato della rete. Infatti, in un canale aperto con se stessi, nessuno può frodarvi, salvo che dentro di voi non si nasconda un Tyler Durden che anziché tirare cazzotti si diverte a fare i dispetti coi canali LN (spoiler alert: se non sapete di cosa parlo, non googlate).

Per quanto semplificato, questo schema ci permette di capire che un utente come Bob può utilizzare LN effettuando tutti i pagamenti ordinari di cui necessita nell'arco di un anno, pur transando molto raramente onchain. Nelle condizioni dello scenario presentato, il canale Bob-FCA va rinnovato 4 volte all'anno, rappresentando quindi solo 4 transazioni onchain, a cui vanno sommate le transazioni per trasferire btc da e verso un cold wallet, per mettere via dei risparmi o per affrontare

delle spese straordinarie.

Essendo il modello molto semplificato, ci sono varie precisazioni da fare:

- FCA ha un “costo” dettato dal creare un canale con Bob per il fatto che funge da provider di liquidità (all’apertura il canale è superiore di 1000 euro rispetto a quanto necessario per il pagamento del primo salario). Tuttavia, in merito ci sono due considerazioni da fare:

1. Tenere Bitcoin “fermi” presenta un costo piuttosto basso, dato il regime deflattivo della moneta. L’incentivo a sbarazzarsi al più presto del proprio denaro è cosa propria delle monete inflattive dell’ultimo secolo, non di un’economia sana.
2. Il costo, comunque presente, è ammortizzato dal fatto che FCA fa da intermediario per i pagamenti di Bob, guadagnando una piccola fee sul routing dei pagamenti Lightning.
3. Se il punto b non bastasse, FCA potrebbe anche calcolare questi costi all’interno del rapporto contrattuale col dipendente.

- Il fatto che Bob spenda tutto solo presso Esselunga e Amazon è una semplificazione. Cosa succederebbe se dovesse pagare un piccolo commerciante? È molto probabile che quel commerciante sia legato da un canale LN con una buona disponibilità quantomeno col suo più diretto distributore, e che questo distributore abbia canali diretti o indiretti con Amazon, Esselunga o FCA, per cui in caso di mass adoption è difficile pensare che l’operaio Bob non riesca a pagare il commerciante né utilizzando LN né, magari, tramite i canali di un provider di liquidità a cui entrambi si appoggiano (esempi di tali provider già esistono, come Bitrefill con il servizio “Thor”).

Può comunque sempre capitare il caso in cui due utenti non sono collegati da alcun canale con sufficiente disponibilità, né diretto né indiretto. Se non hanno nemmeno un servizio custodian in comune, gli utenti dovranno fare una transazione onchain. Vedremo più avanti come questo può pesare sulla blockchain.

- Nello "Stato 4" dei canali, Esselunga e Amazon hanno 3 mila euro ciascuno nel loro lato del canale e FCA zero. Sembrerebbe che sia richiesta una transazione onchain per continuare ad usare il canale se Bob vuole spendere altri soldi, tuttavia è probabile che, come FCA faccia da intermediario per Bob, anche Esselunga e Amazon facciano da intermediari per FCA: pensiamo a un dipendente di Amazon che compra una Fiat. Contrariamente quindi alla dimostrazione estremamente semplificata presentata qui, i canali si bilanceranno in entrambi i sensi.

La rete LN come è presentata qui è già ben distribuita, ma con una capillarità limitata poiché gli utenti sono soliti utilizzare quasi sempre gli stessi canali. Si tratterebbe quindi di una rete LN estremamente semplice e poco sviluppata, possibile già nei primi anni di mass adoption. Questo è il motivo dei canali "grossi". Se il numero di transazioni onchain effettuate da Bob nello scenario qui analizzato sembra troppo basso, possiamo anche ipotizzare che Bob ne richieda dieci volte tante. Un aumento di dieci volte non ci sposta, in questo contesto, su un ordine di grandezza tanto differente. Se per accontentare il bisogno di Bob di effettuare pagamenti onchain si dovesse aumentare il blocksize da 1mb a 10mb, allora si tratterebbe certamente di un intervento molto impattante, ma come vedremo facendo un po' di conti, non c'è proporzionalità diretta fra numero di pagamenti onchain e peso delle transazioni.

Per capire dunque se questo sistema scala a sufficienza per supportare un'economia mondiale in Bitcoin, bisogna vedere

quale sia la reale capacità della blockchain al netto di tutte le migliorie tecnologiche e organizzative che permettono incredibilmente di moltiplicare i pagamenti a fronte di uno stesso numero di transazioni. Solo alla fine di questo articolo tireremo le fila del discorso, immaginando quale possa essere il risultato della combinazione di tutte le innovazioni qui discusse.

LA BLOCKCHAIN:

Lo scenario di Lightning Network sopra descritto, come abbiamo già detto, è una semplificazione ottimistica. Non ci sono solo le spese ordinarie e previste, con controparti già collegate da canali esistenti come nel modello presentato, né vi sono solo le transazioni di ricarica dei canali. Vi sono anche quelle fatte per errore o per un calcolo sbagliato dell'utilità ed efficacia di un certo canale che viene aperto (e che sarà quindi poi chiuso), transazioni verso i cold wallet, transazioni che non rientrano nelle previsioni ordinarie o comunque spostamenti di valore di grandi dimensioni, trasferimenti verso custodian e servizi, utilizzo della blockchain per scopi notarili, utenti che creano canali più "capillari" e con capacità molto più limitate e che quindi necessitano di maggior "ricambio", etc.

Visa processa 150 milioni di pagamenti al giorno. Ipotizziamo di voler non solo battere Visa, ma superarla in modo netto. Diciamo di arrivare a 500 milioni di pagamenti al giorno. Ad oggi la blockchain è arrivata a processare un picco di quasi 500 mila transazioni al giorno (490 mila). Non sappiamo quanti siano i pagamenti che avvengono offchain, ma se vogliamo arrivare a 500 milioni dobbiamo aggiungere tre zeri rispetto al numero di transazioni onchain. Per ogni transazione onchain, devono esserci quindi mille trasferimenti effettuati su Lightning Network, o all'interno di Custodian, Federazioni e sidechain. È realizzabile uno scenario di questo tipo? Chi è scettico, probabilmente sarà sorpreso dalle potenzialità della blockchain Bitcoin.

1. UPGRADE CAPACITÀ: INCREMENTO DEL BLOCCO E SEGWIT

Il modo più noto per aumentare la capacità della blockchain è quello di effettuare un fork (un upgrade di Bitcoin) per aumentare la grandezza del blocco. SegWit, approvato nell'agosto 2017, ha portato con sé anche un aumento del blocco senza toccare il parametro di blocksize, rimasto a 1mb: poiché con SegWit le firme (Witness) sono divise (Segregated) dal blocksize e inserite in una nuova struttura detta blockweight, e poiché le firme pesano per buona parte dello spazio occupato da una transazione, transando con SegWit si può ottenere un raddoppio circa della capacità (una cifra esatta non c'è, poiché varia molto in base al tipo di transazioni effettuate). Ad oggi SegWit è utilizzato per nemmeno metà delle transazioni, semplicemente perché molti utenti o servizi non hanno ancora aggiornato i loro wallets.

Esemplificando quindi, se prima di SegWit potevamo fare solo 100 transazioni, dopo SegWit è possibile farne 200, ma ad oggi siamo ancora fermi a 150. Nel momento in cui tutti passeranno a SegWit otterremo lo sfruttamento massimo della capacità del blockweight (sfruttando un 25% circa di spazio ancora inutilizzato). Se avete ancora un vecchio indirizzo Bitcoin (quelli che iniziano con il numero 1) vi conviene aggiornare, anche per pagare meno commissioni quando transate!

2. UPGRADE EFFICIENZA: BECH32 E SCHNORR

2.1 BECH32

Attualmente gli indirizzi SegWit più utilizzati iniziano con il numero 3, poiché sono stati i primi implementati su wallets e servizi. Tuttavia, i veri indirizzi nativi SegWit sono i bech32, i quali sono ben riconoscibili perché anziché iniziare con 1 o con 3, iniziano con bc. Per esempio, questo è un mio indirizzo pubblico:

bc1q46zj4ww04hfz2jegympwfkd09wxe3nptchegk6
(facendo una ricca donazione potrai vincere magici sconti!!!)

Il solo utilizzo di indirizzi bech32 permette di guadagnare almeno 10% dello spazio su blockchain rispetto a quando si utilizzano indirizzi P2SH (Pay To Script Hash, i quali iniziano con il 3, anche quelli segwit). Gli indirizzi P2SH occupano rispetto ai bech32 1 byte in più per ogni output e 24 byte in più per ogni input. In media una transazione pesa sui 250 byte, qundi con una transazione da 1 input e 1 output il risparmio usando bech32 è di 25 byte. Tale risparmio però aumenta sul peso totale della transazione se aumentano gli input ed ouptut. Infatti, mentre le transazioni Ethereum hanno sempre 1 input e 1 output, la blockchain Bitcoin è in grado di organizzare le transazioni in modo incredibilmente efficiente. Spesso una transazione non corrisponde a un pagamento, anzi oggi la media è già di quasi 2 pagamenti per ogni transazione (una stima di 700 mila pagamenti al giorno in 400 mila transazioni).

Ci sono strumenti che permettono di scalare, ma spetta agli utenti iniziare a usarli. In poche parole, non è Bitcoin che scala da sé, siamo *noi* che dobbiamo *scalare con Bitcoin*. Se Lightning Network è comprensibilmente ancora qualcosa di piuttosto complicato da utilizzare al momento, per cui è bene lasciarlo ad exchange e servizi o agli utenti più smanettoni, iniziare ad utilizzare indirizzi nativi segwit bech32 è qualcosa che porta beneficio non solo all'ecosistema, ma anche a noi stessi, poiché pagheremo commissioni minori.

2.2 SCHNORR

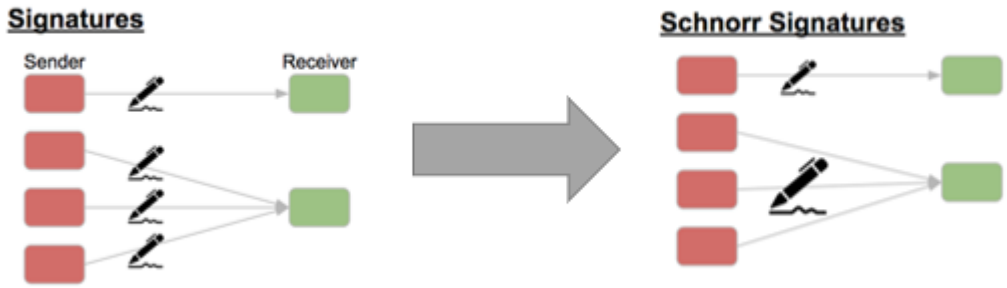
Schnorr è una tecnologia che potrà essere realmente rivoluzionaria per Bitcoin. Parliamo al futuro, ma non si tratta di vaporware in stile Half Life 3: Schnorr esiste non solo nella teoria, ma anche nella pratica. Come SegWit è stato approvato su Litecoin prima che su Bitcoin, così anche Schnorr è stato già portato su Bitcoin Cash. Avendo Schnorr un impatto pesante sulla struttura di Bitcoin, è comprensibile che ci sia la massima prudenza nel fare un fork di questo tipo. Coordinare un ecosistema in totale libero mercato verso un

upgrade di questo tipo non è un compito facile. Quello che però Schnorr permette di fare è strabiliante in termini di scalabilità.

Oggi, quando i Bitcoin vengono transati, il proprietario deve “firmare” la transazione con la propria chiave privata. Ogni input va firmato, occupando così spazio sulla blockchain per ogni firma. Ad esempio, ipotizziamo di aver ricevuto 10 pagamenti da 1 bitcoin ciascuno su un indirizzo. Per spostare quei 10 bitcoin è necessario spendere 10 input diversi, il che significa firmare 10 volte. Schnorr va a snellire questo meccanismo.

Una firma Schnorr pesa 8 bytes in meno rispetto ad una firma tradizionale, il che significa un risparmio di spazio del 3% per ogni transazione con un solo input. Quindi più sono gli input, maggiore è lo sconto.

La vera rivoluzione però sarà la possibilità di aggregare le firme (tecnologia però che richiede un ulteriore fork, ad oggi non ancora implementata su Bitcoin Cash): ovvero quando una transazione presenta più input, lo spazio occupato nella blockchain sarà soltanto quello di una firma e una chiave pubblica, e non di una per ogni input. Questo significa che, a parità di tipologia di transazioni effettuate oggi sulla blockchain di Bitcoin, guadagneremmo il 30% di spazio.



Il 30% è però niente rispetto alle vere potenzialità di tale innovazione. Se infatti wallet e servizi sfruttassero questa

caratteristica, organizzando prevalentemente transazioni di un tipo speciale, il risparmio sarebbe incredibilmente maggiore. Ed è qui che entrano in gioco concetti fondamentali come il batching, coinjoin e le channel factories.

3. ORGANIZZAZIONE: BATCHING, COINJOIN, CHANNEL FACTORIES

3.1 BATCHING

Quando un utente invia dei bitcoin da un custodian all'altro, ad esempio da Coinbase a Bitfinex, da Kraken a Wirex etc., il custodian non effettua la transazione nell'immediato, salvo che non ci sia un canale su layer 2 aperto fra le due società. Attende invece che una serie di richieste di quel tipo si accumulino, per poi avviare tutti i trasferimenti in un'unica transazione aggregata sulla blockchain di Bitcoin. Questo tipo di organizzazione dei trasferimenti richiesti dai propri utenti si chiama batching e dal 2018 è largamente utilizzato da tutti (o quasi) i principali servizi. Con una sola transazione Bitcoin si possono processare centinaia o migliaia di pagamenti.

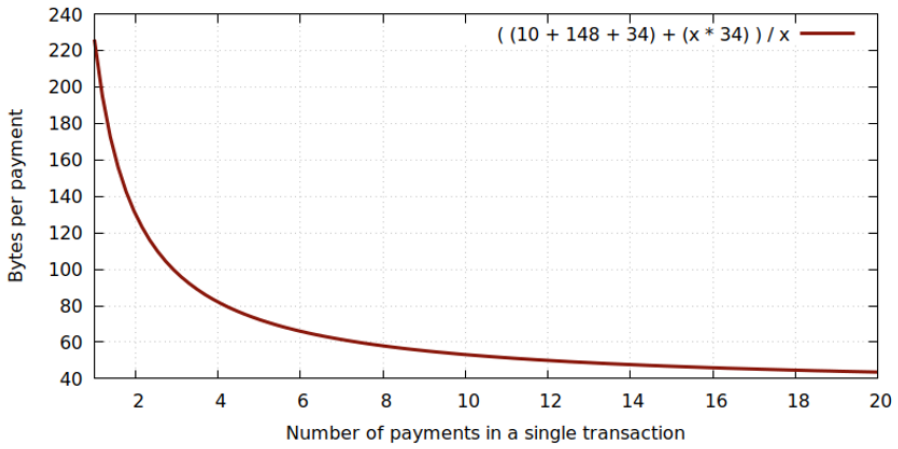
Ogni transazione è composta da diverse parti e ovviamente, oltre che input, output e firma (o firme), ha una parte "fissa". Aggregare molti output in una sola transazione, anziché eseguire tante transazioni quanti sono i pagamenti richiesti, permette di risparmiare in parte fissa, poiché questa è presente una volta sola anziché essere moltiplicata per il numero di pagamenti. Exchange come Kraken e Bitfinex hanno potuto diminuire ampiamente le fee di uscita dalla piattaforma grazie al batching, che ha così avvantaggiato sia i clienti che l'intero ecosistema, poiché il peso su blockchain è notevolmente inferiore a parità di risultato.

Maggiore è il numero di transazioni aggregate e maggiore è il risparmio. Aggregando due sole transazioni, il peso per pagamento è di circa 130 bytes. Aggregandone 50, il peso per ogni pagamento è di 34 bytes. Il risparmio è enorme e lo

spazio **S** occupato, se x è il numero di transazioni aggregate, corrisponde a:
S = (192 + x * 34) / x

In questa tabella viene indicato il peso in bytes occupato da ogni pagamento per numero di pgamenti che vengono aggregati in una sola transazione.

# pagamenti	Bytes/pagamento
2	130
3	98
4	82
5	72
10	53
20	44
50	38
100	36
1000	34



Vi sono esempi di transazioni con migliaia di output. La seguente transazione per esempio risale al 1 gennaio 2016 e ha 13 mila outputs, pesa 445 kilobytes, quindi metà della capacità di un blocco è impegnato da quest'unica transazione.

Se tutte le transazioni bitcoin fossero come questa, *ceteris paribus* i pagamenti onchain al giorno sarebbero circa 2 milioni, circa tre volte rispetto ad oggi. Inoltre, se tutti gli indirizzi sono bech32, si avrebbe un risparmio aggiuntivo del 16%. Ovviamente è assolutamente improbabile avere blocchi pieni interamente di transazioni con un solo input e migliaia di output come quella riportata, perciò il batching da solo non permette di triplicare la capacità della blockchain, salvo casi estremi. Tuttavia, l'utilizzo combinato di batching e aggregazione di firme tramite Schnorr può arrivare a risultati simili. In merito a ciò, un caso interessante da considerare è il coinjoin.

3.2 COINJOIN CON SCHNORR E SIGNATURE AGGREGATION

Coinjoin è una soluzione pensata inizialmente per la privacy degli utenti, ma con l'aggregazione di firme di Schnorr diventa il più potente mezzo di scalabilità onchain.

Anzitutto vediamo come funziona Coinjoin: ipotizziamo che Alice, Bob e Charlie vivano in tre continenti diversi, ma tutti e tre debbano, per qualsiasi ragione, fare una transazione da circa 1 bitcoin e sono interessati a nascondere le loro identità il più possibile, in modo da confondere chi tenti di effettuare chain-analysis per tracciare le loro movimentazioni.

Il wallet di Alice, se sufficientemente avanzato da permettere coinjoin (ad esempio Wasabi wallet) manderà in rete la richiesta di effettuare coinjoin per una transazione da 1 bitcoin, e attende che altri utenti facciano lo stesso tipo di richiesta. Nel momento in cui arriva anche la richiesta di transare di Bob e Charlie, i tre wallet firmano gli input effettuando un'unica transazione congiunta che abbia 3 output, ciascuno da 1 bitcoin. I destinatari di questi tre output saranno le rispettive controparti di Alice, Bob e Charlie a cui questi ultimi hanno voluto inviare 1 btc. A, B e C non si conoscono, eppure hanno sfruttato la coincidenza di interessi (tutti e tre devono transare in questo momento una stessa quantità) per "mischiare i loro bitcoin" prima di farli arrivare a destinazione.

La forza di questo tipo di organizzazione delle transazioni è il fatto di essere un sistema peer-to-peer fra gli utenti, e quindi non dipendente da un servizio come un custodian che coordini l'esecuzione del coinjoin. Maggiore è il numero di partecipanti al "mixer" e maggiore è la privacy che si ottiene. Il sistema funziona soltanto se almeno un output per tutti e tre gli utenti corrisponde a 1btc, altrimenti chi fa chain-analysis potrebbe associare la quantità di bitcoin immessa per ciascun input con la quantità di bitcoin degli output, ricostruendo i passaggi di proprietà. Se tuttavia il focus non fosse più la privacy, bensì la scalabilità, si

potrebbe tranquillamente **fare coinjoin senza prestare attenzione ad avere output identici**, quindi chiunque nel mondo quando effettua una transazione potrebbe unire i propri input con qualsiasi altra persona che sta transando.

Questa è una transazione coinjoin fra 98 utenti che hanno utilizzato Wasabi wallet. Si tratta del mix di 113 input e 211 output, per un totale di 98 pagamenti e 23kB di spazio occupato (56kB di blockweight).

Ad oggi l'unico scopo di Coinjoin è la privacy, poiché non c'è un vantaggio in termini di scalabilità nell'aggregare le transazioni. Se infatti occupassimo un blocco Bitcoin interamente con transazioni di questo tipo, ce ne starebbero circa 40, quindi 4.000 pagamenti per blocco, 576 mila pagamenti al giorno. Rispetto ad oggi essenzialmente non c'è alcun vantaggio… finché non si utilizza Schnorr.

Se al coinjoin combiniamo Schnorr, più un soft fork che permette l'aggregazione di signature e public key, verrebbero essenzialmente risparmiati oltre 100 bytes di signature e pubkey per ogni input (vedi la parte della signature in una transazione). Se quindi aggregassimo le firme degli input per transazioni come quella riportata sopra (da circa 100 pagamenti), ce ne starebbero circa 80 in un blocco, quindi 8.000 pagamenti (~1.1 milioni al giorno). Maggiore è il numero di utenti (e di pagamenti effettuati) che partecipano al coinjoin, più efficiente diventa il meccanismo, poiché meno firme vengono incluse nella transazione onchain (una sola per tutti i partecipanti). Se dovessimo immaginare una transazione coinjoin più grande possibile (da coprire l'intero blocco), avremmo un risparmio elevatissimo. Con numeri tanto grandi, è anche probabile che, anche solo per caso, vari output corrispondano esattamente in quantità di bitcoin transati, in modo da ottenere comunque un effetto mixer come benefico "effetto collaterale".

Un'unica coinjoin che occupi un blocco intero da 1mb peserebbe

70 bytes per ogni pagamento, fino a circa 14 mila pagamenti in un megabyte di blocksize, quindi oltre 2 milioni di pagamenti onchain al giorno.

Abbiamo visto che è possibile ottenere una capacità molto più elevata della blockchain sfruttando semplicemente una migliore organizzazione dell'ecosistema (nel caso del batching), o combinando l'organizzazione di wallet e servizi con Schnorr e aggregazione di signature e pubkey. Senza quindi aggiungere un solo byte di capacità al blocksize. Se si arriva, nel caso limite, a triplicare la capacità della blockchain a parità di spazio, significa anche che ogni possibile aumento futuro di blocksize è tre volte più efficiente.

3.3 CHANNEL FACTORIES

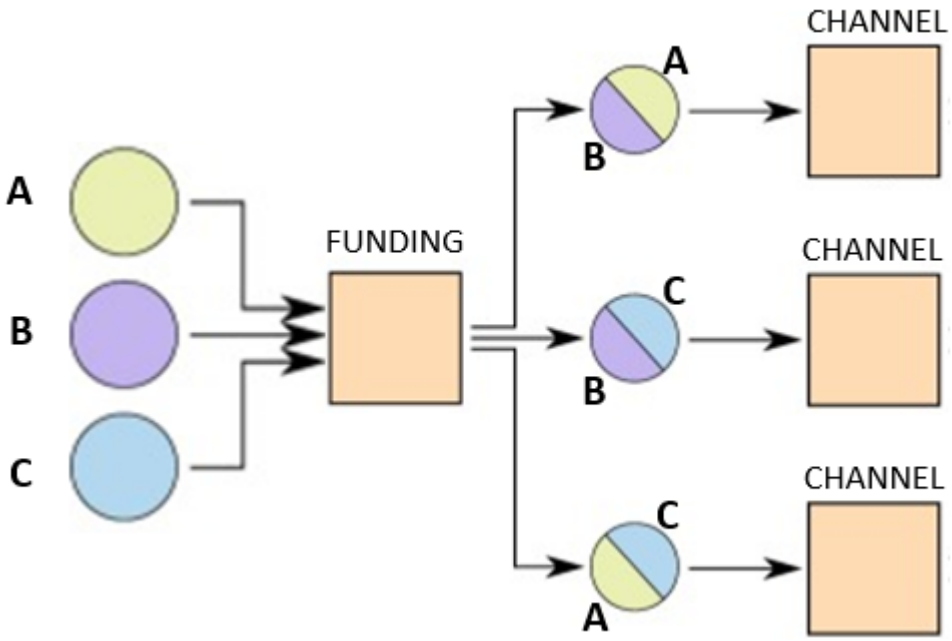
Ora che è chiaro come funziona l'aggregazione di pagamenti, manca l'ultimo passaggio, ovvero capire come si può applicare questo tipo di aggregazione anche a Lightning Network. Un miglioramento delle prestazioni della blockchain lascia più spazio per le transazioni di apertura e chiusura dei canali, ma questo è solo un lato della medaglia. Il vero beneficio è che le stesse transazioni Lightning di apertura dei canali potranno essere "aggregate", in un meccanismo che si chiama Multi-party funded channels. Questo concetto è comparso per la prima volta nel paper *Scalable Lightning Factories for Bitcoin* e poi affinato in *Scalable Funding of Bitcoin Micropayment Channel Network* che è un paper incredibilmente semplice e chiaro dal punto di vista grafico.

Anticipiamo già che le channel factories sono la vera killer application, quella che fa sperare ai puristi del blocco piccolo che il parametro blocksize possa addirittura non essere mai più modificato.

Il meccanismo di funzionamento è molto semplice: anziché aprire un canale fra due soli utenti, più utenti mettono in comune i fondi in un "recipiente" (funding), che è in effetti

l’unico output di un’unica grande transazione, contenente come input i bitcoin provenienti dai wallet di ogni utente. Nessun utente si deve fidare degli altri poiché in qualsiasi momento può decidere di sbloccare autonomamente quei fondi, essendo la transazione creata con lo stesso meccanismo di multisig e checksequence tipico di Lightning Network, semplicemente esteso a più persone.

A partire da questo output bloccato onchain, offchain vengono costruiti tutti i canali fra gli utenti: è possibile, ma non necessario, che ogni partecipante apra un canale con ogni altro utente (come nel grafico esemplificativo qui sotto, con soli tre utenti). Questi canali possono essere chiusi e riaperti senza mai tornare onchain, a patto ovviamente che i movimenti di denaro non oltrepassino le quantità immesse nella funding originaria. In poche parole, la funding è un canale Lightning Network di layer 2, mentre i canali bilaterali veri e propri tipici di Lightning sono una sorta di layer 3 che vi viene costruito sopra.



Nell’esempio in figura, ipotizziamo che A, B e C mettano in comune nella funding 1 bitcoin a testa, per un totale di 3 btc (le tre palline colorate). Ogni canale sarà aperto con 0,5

bitcoin su ogni lato, perciò ad esempio 1 bitcoin di A (la pallina verde chiaro) verrà diviso in modo da creare un canale con B e uno con C.

A avrà 0,5btc nel canale con C e gli altri 0,5 btc nel canale con B. Ogni canale avrà una capacità totale di 1btc, quindi la capacità del canale AC sarà 1 btc, di cui mezzo appartentente ad A e mezzo a C:

AC: 0,5 | 0,5

Se A paga a C mezzo bitcoin, il balance nel canale passerà ad essere:

AC: 0 | 1

Normalmente in Lightning Network, questo significa che domani A non potrà più pagare altri 0,5 btc a C, poiché significherebbe passare sul lato di C del canale ben 1,5 btc, il che sarebbe impossibile per due ragioni:

- A non ha quella disponibiltà nel canale con C
- La capacità massima del canale, calcolata sommando i fondi di A e C in AC, è già stata raggiunta, poiché limitata a 1btc

Eppure A possiede 0,5 btc disponibili nel canale con B. Grazie al fatto che tutti questi canali si trovano su un “layer 3”, A può chiudere il canale con B e C e questa operazione rimane offchain, poiché l’output onchain della FUNDING non viene toccato. I fondi nella FUNDING vengono solo “rimescolati” nella creazione di nuovi canali, in modo che A possa aprire un nuovo canale AC utilizzando quanto prima possedeva nel canale AB. Il risultato sarà:

AB: canale chiuso (non è richiesta transazione onchain)
AC: 0 | 1,5 (riaperto con 0,5btc di capacità in più, senza transazioni onchain)

Questo sistema è ottimo per tre ragioni:

1. **Si possono aprire e chiudere infinite volte i canali su layer 3 senza mai transare onchain**
2. **Le commissioni di transazione per la creazione onchain della funding originaria vengono divise fra tutti i partecipanti alla channel factory**
3. **La funding originaria aggrega le transzioni di "apertura di canale" di molti utenti, risparmiando una quantità incredibile di spazio sulla blockchain**

Pensiamo a 10 utenti che uniscono i loro fondi in un'unica funding e da qui creano 45 canali fra loro, facendo sì che ogni utente abbia un canale diretto con tutti gli altri e che possa chiudere e riaprire i canali, in base alle necessità, con qualsiasi altro di questi 10 utenti.

Nota: per 10 utenti (da A di Alice a L di Leorio) il numero minimo di canali diretti è 45, in base alla formula matematica m = n(n-1)/2; con m = numero canali e n = numero utenti. Per contarli in modo un po' meno elegante, ma più intuitivo, si procederebbe come segue:

A apre un canale con **B**,**C**,D,E,F,G,H,I,L (9 canali)

B apre un canale con **C**,D,E,F,G,H,I,L (AB esiste già, vengono aperti quindi altri 8 canali)

C apre con D,E,F,G,H,I,L (AC e BC esistono già, vengono aperti quindi altri 7 canali)

…e così via

Se analizziamo il peso di una channel factory che riunisce 10 utenti rispetto alla creazione di 45 canali bilaterali, ognuno con un'apposita transazoine onchain, notiamo che il risparmio di spazio sulla blockchain è del 90%. Se si usasse Schnorr, sarebbe addirittura il 96%.

Questo significa che le channel factories aumentano la possibilità della blockchain di ospitare canali Lightning di

oltre 20 volte a parità di spazio occupato (solo di 10 volte senza Schnorr)

Inoltre i canali di layer 3 costruiti in una factory sono molto più "utili" dei tipici canali Lightning, poiché possono essere ricombinati a piacimento, aprendo nuove opzioni di scambio fra tutti gli utenti coinvolti

Users (n)	Channels (m)	LN vbytes	Factories vbytes	Savings (%)
3	3	720	320	55.56%
4	6	1440	415	71.18%
5	10	2400	510	78.75%
6	15	3600	605	83.19%
7	21	5040	700	86.11%
8	28	6720	795	88.17%
9	36	8640	890	89.70%
10	45	10800	985	90.88%

Il problema di questa soluzione è uno solo: maggiore è il numero di utenti che partecipano e più probabile è che uno solo di essi voglia chiudere la factory. Se uno solo sceglie di chiudere (o se si vuole aggiungere anche un solo utente ad una factory già esistente) è necessario transare onchain, e ogni canale di layer 3 va chiuso. La bella notizia è che tutti i partecipanti che rimangono nella factory possono ricostruire i canali di layer 3 con la stessa transazione di chiusura del canale (che chiude la factory escludendo l'utente che vuole abbandonare, riaprendola per tutti gli altri).

Dall'altro lato, è anche vero che, maggiore è il numero di partecipanti (più grande è il canale e la sua capacità), maggiore sarà l'incentivo a rimanere in esso per ogni partecipante, poiché i bitcoin in Lightning sono più liquidi (spendibili a minor costi in termini di tempo e commissioni) rispetto ai Bitcoin onchain. Si può immaginare un network Bitcoin del futuro che sia fatto quasi interamente da channel factories di gruppi di utenti, ove tutti i principali movimenti di bitcoin avvengano quasi esclusivamente su un

terzo layer di canali Lightning.

Maggiore il numero di utenti, maggiore il risparmio. Ma anche soltanto con 10 utenti, una channel factory pesa 985 bytes, con Schnorr 435bytes (tutti i numeri hanno buone approssimazioni). Significa che in 1mb di blocco si possono creare 2.300 transazioni di questo tipo, ovvero 23 mila utenti che creano 103 mila canali. Contando 6 blocchi in un'ora e 144 al giorno, significa che ogni giorno 3 milioni di persone possono creare quasi 15 milioni di canali.

CONCLUSIONE: SCRUTANDO NELLE VISCERE DEL POLLO

Con piena adozione di Segwit si può guadagnare un 25% di spazio aggiuntivo nel blocco. Con bech32 si risparmia un 10% per transazione e il risparmio cresce all'aumentare di input e output. Con Schnorr si risparmia un altro 3%, che aumenta al maggior numero di input. Con il batching di transazioni il peso di ogni pagamento scende fino a 34 bytes (con unico input), con un risparmio di oltre l'80%, mentre con l'aggregazione di signature e public key in Schnorr ogni pagamento peserebbe circa 70bytes, con un risparmio del 65%. Queste migliorie riducono notevolmente lo spazio occupato da tutte quelle che saranno le tipiche transazioni onchain: pagamenti di importi elevati, transazioni di compensazione fra custodian, invio di denaro fra utenti e custodian o risparmi messi nei cold wallet.

Nel frattempo, chi si affida a custodian e a federazioni di custodian (sidechain come Liquid) può movimentare fondi potenzialmente all'infinito senza impattare in alcun modo sulla capacità della blockchain.

Al netto quindi di transazioni per la notarizzazione/timestamping che essenzialmente rappresentano l'unica funzione della blockchain alternativa a quella monetaria, tutto lo spazio rimanente sarà utilizzato per creare e chiudere canali Lightning Network.

Lasciando il blocksize a 1mb e implementando tutte le innovazioni su layer 1 (blockchain) descritte sopra, possiamo arrivare a 2 milioni di pagamenti onchain. Anche aumentando l'attuale throughput della rete da una stima degli attuali 700 mila pagamenti onchain a 1 milione, avremmo uno spazio significativo per i canali Lightning Network a fee ancora contenute, diciamo pure 500.000 bytes per blocco. Significa poter aprire 2.500 canali Lightning, 360 mila al giorno, 130 milioni in un anno (senza channel factories, che per il momento escludiamo dai conti).

Abbiamo visto che un utente può "vivere" utilizzando un solo canale Lightning Network per mesi senza fare altre transazioni onchain, e 130 milioni di canali l'anno può sembrare tanto, ma non facciamoci prendere troppo dall'entusiamo: il confronto con Visa è ancora perdente. Se un canale ha una vita di 3 mesi e ce ne vogliono almeno 4 per ogni utente all'anno, significa che soltanto 30 milioni di persone potranno transare quotidianamente con LN.

Un cittadino medio americano esegue circa 40 pagamenti elettronici al mese (70 pagamenti totali, di cui il 60% elettronici). Se queste abitudini di consumo rimangono invariate, è probabile che gli utenti non sfrutteranno LN per oltre 40 pagamenti al mese, perciò non più di 480 transazioni all'anno. Moltiplicate per 30 milioni, risultano 15 miliardi di transazioni annue.

Esistono 780 milioni di carte di credito Visa che processano 150 milioni di transazioni al giorno, con 55 miliardi di transazioni all'anno, contro gli ipotetici 15 miliardi su LN. Anche se ognuno dei 130 milioni di canali all'anno potenzialmente è in grado di gestire più transazioni, per raggiungere Visa servirebbero più canali per servire nuovi utenti, ma non c'è spazio per crearne altri. E la nostra stima di spazio era comunque già ottimistica.

I conti sono fatti con la mannaia e le ipotesi di partenza con

atti divinatori di previsione tramite le viscere di un pollo sacrificale, ma in questa gara approssimativa, Visa sembrerebbe averla vinta su Lightning Network. Questo non significherebbe necessariamente processare più transazioni di Bitcoin. Infatti avremmo comunque il ruolo di custodian e federazioni che, potenzialmente, può annullare completamente la distanza. E basterebbe un raddoppio del blocksize per ottenere un guadagno molto più che proporzionale.

Fermi tutti però. È davvero necessario chiamare in causa custodian e blocksize increase? Stiamo parlando comunque di miliardi di transazioni all'anno soltanto con LN. Non c'è dubbio che si possa definire come adozione di massa. A quel punto, ci si può aspettare che un numero di ricercatori e programmatori molto più elevato lavori su tecnologie Bitcoin. In un momento storico del genere, sarebbe ingenuo pensare che la tecnologia di Lightning Network non avrà ancora implementato le altre diavolerie già partorite dalla mente malata dei cypherpunk.

Se rifacessimo i conti, questa volta con le channel factories, cambia tutto: in 500.000 bytes di spazio (mezzo blocksize, ipotizzando che l'altra metà sia utilizzata per transazioni di altro tipo) potremmo effettuare 1150 transazioni da 10 utenti l'una, per un totale di oltre 50 mila canali. Sono 7 milioni di canali al giorno, due miliardi e mezzo di canali all'anno. Siamo 7 miliardi e mezzo sulla terra, compresi vecchi, bambini, nordcoreani, amish e terrapiattisti. Può quindi Bitcoin arrivare all'adoz… ?

Si.

Ciaone

Segui gli aggiornamenti quotidiani sulla pagina facebook: https://www.facebook.com/albertodeluigi.news
Iscriviti alla newsletter del blog per ricevere una notifica ad ogni nuovo articolo pubblicato