Bitcoin: una nuova grande depressione come negli anni 2014-2016?

scritto da Alberto De Luigi | 26 Giugno 2018
I crolli di inizio 2014 e 2018 hanno patterns molto simili, si tratta solo di coincidenze?

2013 | Gennaio -> Dicembre: il prezzo di Bitcoin sale da circa 10 a 1.000 dollari.
2014 | Gennaio: avviene il tracollo e il prezzo attende **3 anni**, ovvero il 2017, per riprendere il massimo storico. Questo è stato il periodo più lungo di "depressione" del prezzo prima di tornare ai massimi.

2017 | Gennaio -> Dicembre: il prezzo di Bitcoin sale da circa 1.000 a 20.000 dollari.
2018 | Gennaio: avviene il tracollo che dura ormai da 6 mesi.

I grafici del prezzo disegnano figure molto simili nel 2014 e 2018, anche se su finestre temporali diverse (più allungata nel 2014).

È curioso notare che proprio in questo periodo escono su varie testate articoli relativamente alle mining pools di Bitmain

(Antpool e BTC.com) che si stanno avvicinando al 51% dell'hashrate mondiale (vedi questo esempio). Nel 2014 c'era una situazione analoga in cui la pool GHash aveva raggiunto addirittura il 55% dell'hashrate, fra il 12 e il 13 giugno. Oggi si parla degli stessi temi, è cambiato solo il soggetto: Bitmain piuttosto che GHash. Non è però la paura di un attacco 50+1 a incidere sul prezzo, piuttosto è il calo del prezzo a spingere una ricerca di spiegazioni, che talvolta gli utenti trovano in un capro espiatorio, non comprendendo le vere ragioni di questo momento di ribasso. In realtà le motivazioni del crollo, che ho presentato in un precedente articolo, non hanno nulla a che fare coi miners. Seppur ci siano blockchain che prestino il fianco a svariati attacchi, la paura di un 50+1 su Bitcoin è per lo più infondata, come analizzato nell'ultimo articolo che approfondisce il tema specifico degli attacchi alle blockchain POW.

Concentrazione del mining a parte, se il prezzo di Bitcoin rispetta rigorosamente delle fasi cicliche che si ripetono, potrebbe significare che, come nel 2014, dovremo aspettare altri **3 anni**, ovvero il **Gennaio 2021**, per tornare ai massimi storici. Tuttavia non è ragionevole fare previsioni basate unicamente sulla somiglianza di due bolle, che spesso hanno strutture analoghe semplicemente perché ricalcano fasi ben note a chi fa analisi dei mercati e della psicologia dei traders.

Allora quando potremo prevedere una nuova ripresa? Nessuno può avere certezze, ma per rispondere a questa domanda possiamo fare alcune considerazioni.

La situazione è molto diversa rispetto al 2014.

Nel 2014 non c'è stato alcun upgrade del protocollo Bitcoin e da ben due anni non erano più state portate innovazioni rivoluzionarie alla tecnologia. Ovviamente lo sviluppo non si è mai fermato, ad esempio fra il 2012 e il 2014, coi Bitcoin Improvement Proposal BIP32 e BIP44 si è lavorato molto sui

wallets, introducendo gli HD wallets (Hierarchical Deterministic). Tali software permettono la creazione di un seed unico, facilmente memorizzabile e "portabile", da cui vengono generati un numero indefinito di indirizzi e chiavi private. Il seed è perciò una grande comodità per gli utenti e garantisce anche una buona sicurezza. Ma queste innovazioni fanno parte più dell'ecosistema che gira intorno a Bitcoin piuttosto che del protocollo in sé. L'ultimo upgrade strutturale (fork) era avvenuto il 1 aprile 2012 con BIP16: pay-to-script-hash.

In effetti, il vero evento del 2014 che tutti ricordiamo non è un'innovazione tecnologica, ma è rappresentato dalla più grande catastrofe finora sperimentata nel mondo delle cryptovalute: il crollo dell'exchange MtGox, che contava ai tempi il 70% dei volumi di trading globali. La situazione dunque era del tutto *sui generis*. Gli utenti non avevano ancora fatto esperienza di eventi tanto drammatici e persino alcuni fra i più esperti conservavano grandi quantità di bitcoin su wallets di terzi. Ad esempio alcuni Core developers possedevano un conto su MtGox e al crollo hanno subito perdite ingenti: quasi 1.000 bitcoin da parte di Gregory Maxwell e quasi 500 da parte di Luke Dash jr.

Da allora molto è cambiato. Oggi l'ecosistema è più maturo, vi sono decine di exchange e nessuno di questi singolarmente supera il 7% del traffico globale. I volumi di trading sono circa 50 volte superiori, chiunque ha almeno sentito nominare Bitcoin in un telegiornale e la tecnologia blockchain è sulla bocca di tutti. Ci sono più wallets, più servizi, le carte di debito permettono di spendere Bitcoin pressoché ovunque (su circuito Mastercard, mentre Wirex è la prima Visa ad essere reintrodotta dopo l'esclusione di WaveCrest). Inoltre oggi c'è maggiore compliance di piattaforme e servizi con le leggi in ogni paese, c'è una maggiore consapevolezza di rischi e benefici associati all'uso delle cryptovalute e le istituzioni per lo più non si stanno approcciando con un'attitudine

probizionistica, anzi talvolta è proprio l'opposto. Soprattutto però, si sta costituendo una community estremamente vivace: proliferano i bloggers, vloggers, guru, esperti e appassionati. Basta vedere la mole di utenti sui forum e gli attivissimi gruppi Facebook per rendersi conto di quanto la community sia partecipata. E una volta che si scopre il mondo delle cryptovalute, è molto difficile che se ne esca. Anche se il prezzo è calato, i capitali continuano a fluire nelle casse degli exchange, come si vede anche dalla crescita di Tether, di cui parlato estensivamente nell'ultimissimo articolo.

I developers e i contributors di Bitcoin Core sono aumentati ed è aumentato il loro costante lavoro di volontariato. Questo è un video che sintetizza l'attività del 2017 solo su Bitcoin Core, con una rappresentazione grafica:

La tecnologia sta evolvendo in modo del tutto rivoluzionario, preparando lentamente ma inesorabilmente la strada a Lightning Network, su cui gli sviluppatori del protocollo Bitcoin stanno puntando tutto ormai da tre anni. In poche parole, la roadmap prevede un unico grande traguardo, ciò che potrà finalmente portare Bitcoin alla maturità:

1. Nel **Febbraio 2015** esce la prima draft del **White Paper di Lightning Network**. Finalmente si teorizza una possibile soluzione definitiva al problema della scalabilità della blockchain; soluzione che ha anche il beneficio di permettere transazioni istantanee e con maggiore privacy. Ma ci vogliono alcune modifiche al protocollo perché Lightning possa funzionare.

2. Il **14 Dicembre 2015** avviene un **upgrade** di Bitcoin, ovvero il "**check lock time verify**", che dà la possibilità di fare una transazione per cui il ricevente può spendere i bitcoin solo a una condizione precisa: ovvero solo al tempo x (misurato in numero di blocchi della blockchain). Questa modifica **permette**

a Lightning Network la creazione di canali di pagamento istantaneo in modo sicuro, poiché al tempo del blocco x l'utente potrà recuperare i fondi impegnati nel canale (se non vengono spesi nel canale). Tuttavia, ancora non basta.

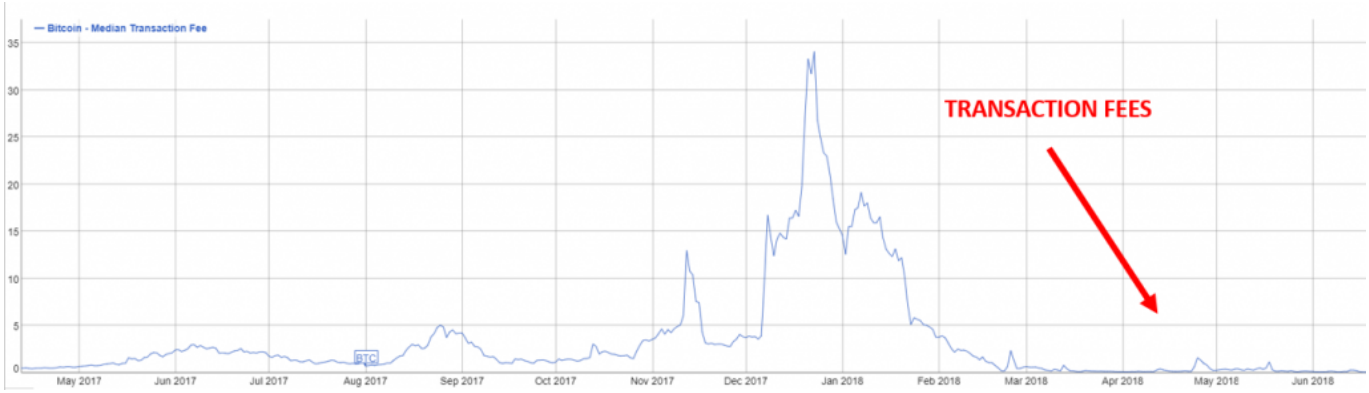
3. Il **4 Luglio 2016** infatti c'è un altro **upgrade** del protocollo di Bitcoin che porta un fondamentale "upgrade" del check lock time, ovvero il "**check sequence verify**": il ricevente può spendere i bitcoin solo dopo un certo periodo, calcolato in un numero n di blocchi creati dal momento in cui una data transazione viene scritta nel blocco x. Questa modifica **permette a Lightning Network di tenere i canali creati aperti a tempo indeterminato**, senza doverli continuamente rinnovare con nuove transazioni.

A quel punto eravamo già vicini a rendere funzionante Lightning Network, ma mancava un ultimo tassello del puzzle: la risoluzione del malleability bug, ovvero un bug da sempre presente nel protocollo Bitcoin per cui l'ID di una transazione in certi casi può essere modificato, per cui non risulta più univoco. Per fare un esempio: se una transazione richiede 2 firme su 4 e due utenti firmano, questa può essere già validata in blockchain con un suo ID. Se anche il terzo o il quarto utente firmano la transazione, l'ID cambia e la transazione potrebbe essere quindi validata in blockchain con un ID diverso dal primo. Questo fa sì che gli utenti possano confondersi e non vedere o riconoscere le proprie transazioni, ma soprattutto costituisce un'elevata complicazione a livello di programmazione del software. Con l'upgrade Segregated Witness le firme (witness) sono separate (segregated) dal resto della transazione e quindi non hanno un impatto sull'ID, che rimane così univoco.

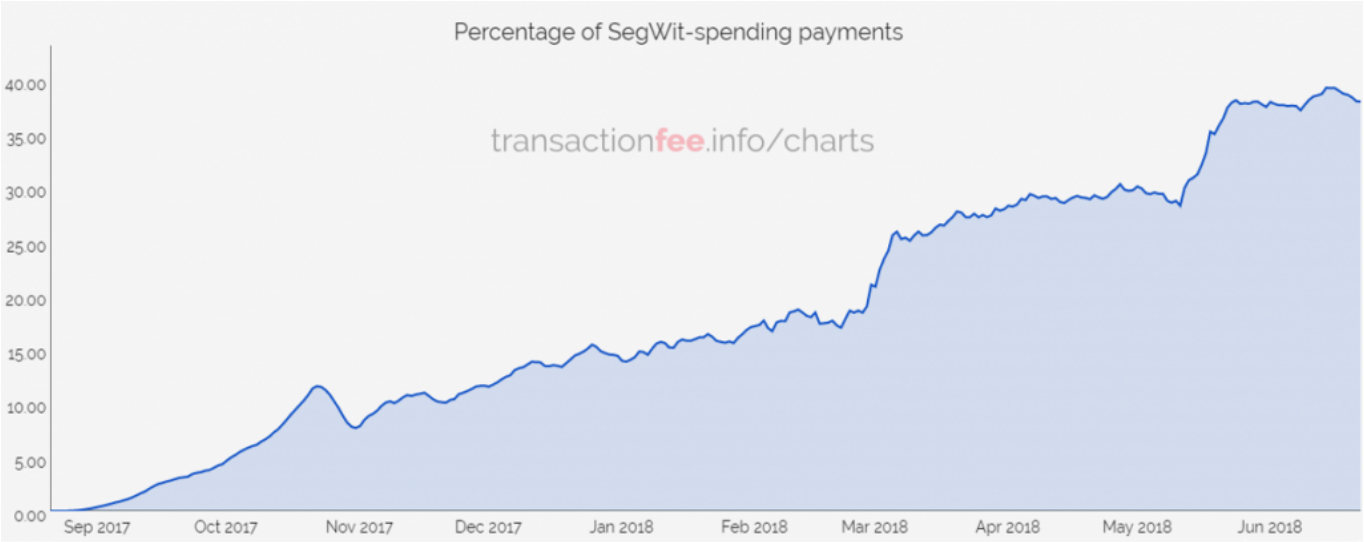
4. Il **24 Agosto 2017** avviene finalmente il consensus fork con SegWit, l'ultimo degli upgrade che erano necessari per l'utilizzo di Lightning Network.

Oggi Lightning Network è in fase di attivissimo sviluppo, con

oltre 5000 canali creati (per lo più per il testing) e diverse implementazioni. Alcuni servizi online (come la ricarica telefonica su Bitrefill) permettono già di pagare con Lightning Network ed entro un paio di anni possiamo immaginare che ci saranno dei software più semplici, affidabili e adatti all'uso da parte di una base utenti meno tecnica. Anche se nei primi anni rimarrà uno scoglio tecnico per gli utenti comuni, già l'adozione da parte di exchange e servizi permetterà enormi passi avanti in termini di scalabilità. A dire il vero, ad oggi non sembra nemmeno ci sia urgenza, poiché grazie al batching degli exchange e all'allargamento del blocco dato da SegWit (che aggiunge la parte blockweight), lo spazio occupato dalle transazioni quotidiane si è molto ridotto e la mempool oggi è semivuota, perciò non ci sono transazioni in coda a intasare la rete e i costi di transazione con SegWit sono minori di un dollaro.



Col tempo, i pagamenti effettuati in SegWit stanno aumentando, abbiamo recentemente raggiunto il 40%, quando a marzo eravamo solo al 20%.



Nel frattempo, il **27 Aprile 2018** abbiamo superato i **17 milioni di bitcoin minati al mondo, su 21 milioni totali**. Oltre l'**80%** dei bitcoin che verranno mai ad esistenza sono quindi già stati prodotti. Ogni giorno, fino al prossimo halving, vengono minati circa 1.800 bitcoin, ma nel 2020 l'**halving ridurrà l'offerta giornaliera dimezzandola a soli 900 bitcoin.** Per quella data, avremo anche raggiunto la produzione dell'87% dei bitcoin, avvicinandoci al 90%, una soglia psicologica importante. Quando non saranno più creati nuovi bitcoin, chiunque ne possieda uno intero avrà la consapevolezza di avere un raro gioiello in mano, che pochi fortunati sono riusciti ad acchiappare.

Insomma, le prospettive future sembrano rosee. Siamo sicuri di dover aspettare il 2021 per il prossimo viaggio sulla Luna? Io non credo. Ma se anche fosse, attenderò volentieri, significa che avrò più tempo per comprare il maggior numero di bitcoin possibile.

Tieniti aggiornato sulle news quotidiane più importanti seguendo la pagina facebook: https://www.facebook.com/albertodeluigi.news

Iscriviti alla newsletter del blog, riceverai una mail ad ogni nuovo articolo pubblicato