Il futuro del DeFi: Ethereum vs Bitcoin

La cara vecchia frase “Bitcoin no, la blockchain si” che ormai sentiamo ripetere da anni è stato solo l’incipit di una grottesca carnevalata che ancor oggi non sembra avere fine. La buzzword “blockchain” rimane nel 2020 sulla bocca di tutti i businessmen più fighetti dei canali mainstream, impegnati a osannare improbabili trovate come la blockchain per certificare la filiera produttiva, la blockchain per tracciare i polli venduti al Carrefour o la blockchain per verificare il consenso dato al partner sessuale[1].

Uno degli use case più promettenti di sempre per la blockchain: ve la sta dando spontaneamente o sta cedendo controvoglia alla vostra brutale virilità? Nel dubbio, fateglielo notarizzare sulla blockchain.

Alla lunga però anche i markettari più convinti si stufano, e allora è bene coniare un nuovo termine in grado di generare hype: “DeFi” per “decentralized finance”. Si tratta anche a questo giro di baggianate? O la blockchain sta davvero rivoluzionando il mondo della finanza?

Indice:

1. Quali sono gli usi della blockchain
2. In cosa consiste l’attuale mondo defi
3. Tokenizzazione
    - 3.1 Il token come moneta
    - 3.2 Gli utility token
    - 3.3 Il security token e le stablecoin
4. Il DEX: Decentralized Exchange

5. I problemi di Ethereum

- 5.1 L’archival node di Ethereum: una bestia in via d’estinzione
- 5.2 AWS e Infura come single point of failure
- 5.3 Centralizzazione della governance

6. Ethereum 2.0: dalla padella alla brace

- 6.1 La centralizzazione del POS
- 6.2 Gli ASICS dell’Ethereum foundation nel POS: si, per davvero!
- 6.3 Far finta di scalare: lo sharding con node relayers giganteschi

7. DeFi su Bitcoin: RGB e Mintlayer

- 7.1 RGB
- 7.2 Mintlayer

1. Quali sono gli usi delle blockchain oggi

Il mondo crypto è molto vasto, ma se guardiamo ai volumi transati su blockchain, quindi all’utilizzo effettivo della tecnologia, sono essenzialmente tre grandi realtà a dominare l’intero mercato: Bitcoin (BTC), Ether (ETH) e Tether (USDT). In termini quantitativi, le altre altcoin praticamente scompaiono dal grafico se messe a confronto.

Tether (USDT), che ha il **primato dei volumi** con circa 3,4 miliardi di dollari transati al giorno, fino all’anno scorso viaggiava quasi esclusivamente sulla blockchain di Bitcoin (tramite l’Omni protocol) mentre dal 2020 è usato principalmente come token erc20 di Ethereum (oggi 2,36 miliardi scambiati) e più recentemente su Tron (887 milioni).

In coda, molto distanti dalle big, vediamo i volumi di NEO, ADA, XRP, TRX, BCH e LTC. Un po’ più sotto, non riportati in

grafico, ZEC e BSV e altra “polvere” (DASH raggiunge i 10 milioni, Doge 6 milioni, ETC 4 milioni). Non ci sono invece dati disponibili per Monero (XRM).

Per farla breve, **l’intera economia crypto ha finora visto protagoniste esclusivamente due blockchain**, **quella di Bitcoin e di Ethereum**[2], mentre soltanto da questa estate Tron ha recepito un innalzamento nei volumi, grazie a Tether che sta sperimentando l’emissione su soluzioni diverse, al fine di pagare meno commissioni di transazione.

Dei volumi di utilizzo, la quota parte del DeFi è una nicchia molto specifica. In generale, non sono considerati DeFi i trasferimenti monetari come ad esempio spostare Bitcoin o Tether: il che nei fatti esclude dalla cosiddetta decentralized finance la blockchain di Bitcoin[3].

Guardando quindi ad Ethereum, abbiamo una metrica molto significativa per misurare e catalogare l’utilizzo della blockchain: la distribuzione delle fee pagate. Infatti, qualsiasi movimento su Ethereum deve pagare ai miner le commissioni di transazione espresse nel token nativo ETH, perciò la distribuzione della spesa del gas “Ether” ci restituisce un quadro molto dettagliato (analisi di Glassnode[4]).

Il 14% delle fee viene impiegato per muovere Tether, il 12% per transazioni monetarie in Ether. Soltanto il 7,2% per tutti gli altri token erc-20, a dimostrazione che gli oltre 200 mila token creati su Ethereum costituiscono in realtà una fetta minuscola dell’economia crypto. Quello che rimane fuori, ovvero ben il 65% dei movimenti (in termini di spazio occupato, non di volume in dollari)[5], è riconducibile al mondo DeFi.

2. In cosa consiste l’attuale mondo DeFi

Di quel 65% dei movimenti su Ethereum che rappresentano smart contracts, **la maggior parte (il 70%) sono movimenti sui "decentralized exchange" (DEX)** e transazioni di arbitraggio fra gli stessi. Il 16% sono schemi Ponzi fraudolenti (come Forsage o Lionshare), il restante applicazioni di gambling (es. Dice2Win) o schemi piramidali (11%) che si distinguono dai Ponzi solo perché sono open source e quindi nessun ente centralizzato può scappare col malloppo, ma sostanzialmente la logica è la stessa: porta un amico, vinci una reward. Fra questi, ad esempio, Million.money e Easy Club. Per farla breve, il mercato DeFi propriamente detto coincide strettamente col mondo dei DEX.

I movimenti diretti sul DEX riguardano gli scambi fra coppie di valute (vari token erc20 ed Ether) eseguiti dai traders, oppure le transazioni per rifornire le pool di liquidità. Gli arbitraggi invece sono movimenti di denaro fra diverse pool e smart contracts alla caccia di differenze di prezzo fra i mercati. Tali differenze sono accentuate rispetto agli exchange centralizzati per via delle **inefficienze intrinseche che gli smart contracts hanno nella scoperta del prezzo**. Per assurdo, il rischio associato a tali inefficienze è l'elemento che ha attirato così tanti speculatori. Per capire come funziona facciamo un esempio (ricalcando il funzionamento di Uniswap).

Immaginiamo un DEX costituito da una pool dove i liquidity providers abbiano caricato 100 USDT e 1 ETH. I liquidity providers sono utenti che caricano fondi nelle pool per permettere ai trader di operare, e in cambio ottengono delle commisioni per ogni trade eseguito. Il prezzo di ETH rispetto a USDT è dato dal rapporto fra le quantità presenti nella pool, in questo caso 1 ETH vale 100 USDT secondo la semplice formula[6]:

$$\textbf{quantità}_{\text{token1}} * \textbf{quantità}_{\text{token2}} = \textbf{prezzo}$$

Se il prezzo su un altro mercato, come un exchange centralizzato o altro DEX, è diverso (ad esempio 120 dollari a

ETH anziché 100), allora i traders avranno convenienza a fare arbitraggio. Il trader acquisterà ad esempio 50 USDT, prelevandoli dalla pool in cambio di 0,5 ETH, per rivendere i 50 USDT a un prezzo maggiore altrove. A valle del trade, nella pool sono rimasti 1,5ETH e 50USDT al nuovo prezzo di 33 Tether per Ether (in base alla formula riportata sopra), presentando così un incentivo per un altro trader ad eseguire il movimento opposto (vendere Tether acquistando Ether).

Tale meccanismo è intrinsecamente inefficiente nella scoperta dei prezzi di mercato rispetto a un book tradizionale e risente anche di lunghi tempi di attesa fra un trade e l'altro, poiché gli scambi avvengono **onchain**, il che li rende **lenti e molto costosi** (è conveniente tradare solo importi elevati). I tempi d'attesa comportano ancor maggiori **disequilibri nei prezzi**. L'esistenza di più DEX, ciascuno soggetto a tali squilibri, crea ulteriori opportunità di arbitraggio attirando più speculatori[7]. Paradossalmente, i DEX su Ethereum sono un mondo autoreferenziale che ha successo proprio per via delle proprie inefficienze. Si tratta di **un territorio per trader molto esperti con elevate conoscenze tecniche** e capaci di sviluppare BOT efficaci**[8]**.

A dominare il mercato DEX è il protocollo **Uniswap**, seguito dalle transazioni effettuate dai vari **BOT di arbitraggio**. Fra i protocolli DeFi associati al mondo DEX annoveriamo anche applicazioni come Kyber, dxdy o AAVE che facilitano l'aggregazione di fondi fra utenti diversi al fine di creare delle pool di liquidità, o che fanno prestiti (lending) per permettere ad altri utenti di aprire posizioni di trading. Yield Farming si occupa invece dello spostamento di fondi fra una pool o uno smart contract e l'altro, alla ricerca del più redditizio. Vi sono poi DEX come curve.fi che cercano di limitare le perdite che i liquidity providers incorrono in caso di alta volatilità, permettendo cioè solo i trade fra

stablecoins.

Nel 2017 Ethereum viveva sostanzialmente di speculazione, con utenti che investivano milioni alla caccia della ICO più profittevole. Abbiamo visto proliferare un numero mostruoso di token: su etherscan sono oggi riportati i dettagli di solo 981, ma pare siano in effetti oltre 287 mila. La maggior parte promettevano di diventare il Bitcoin 2.0 del futuro, ma oggi sono praticamente inesistenti nell'economia della blockchain di Ethereum (pesano per il 7% delle transazioni) e presto o tardi saranno tutti dimenticati. Quella del DeFi è solo una nuova moda a rimpiazzo dell'era ICO, o avrà dei risvolti positivi nel lungo termine?

Anche se il mondo DeFi è oggi trainato principalmente dalla speculazione, vi sono almeno due idee di fondo che val la pena salvare: 1) **la tokenizzazione di assets e** 2) **il DEX.**

3. Tokenizzazione

Per quanto riguarda la tokenizzazione, la grande quantità di progetti fuffa che si sono susseguiti negli ultimi anni ha generato numerosi fraintendimenti relativamente a quale sia l'utilità della tecnologia, perciò è bene fare chiarezza. Sostanzialmente ci sono tre tipi di token:

1. Token come moneta o mezzo di scambio
2. Utility token per pre-payment
3. Security token e stablecoin

3.1 Il token come moneta

Il token monetario per eccellenza è Bitcoin, che non ha alcun sottostante non digitale e basa il suo valore sulle sue proprietà intrinseche, che lo rendono molto semplicemente **la migliore forma di moneta possibile dal punto di vista tecnico-scientifico**[9], oltre che sull'aspettativa che questo fatto venga socialmente riconosciuto sempre più nel tempo, accrescendone costantemente l'adozione. Premessa la bontà

tecnologica della soluzione, creare dei cloni non ha senso per via delle proprietà stesse della moneta: avrà successo solo quello standard condiviso dal numero maggiore possibile di persone. Creare uno standard alternativo significa sotto-segmentare il mercato, riducendo l'effetto network e l'utilità stessa della moneta. Con tutta probabilità, **se sentite di un token che rimpiazzerà Bitcoin, quel progetto non è serio** al pari delle migliaia di token che hanno tentato la scalata negli ultimi 10 anni, fallendo.

3.2 Gli utility token

L'utility token può essere considerato come forma di pre-pagamento per un servizio o per finanziare un progetto in crowdfunding: ad esempio può essere un titolo rappresentativo ceduto in cambio di una donazione, come un badge onorifico "io ho donato!". A questo punto però, c'è da chiedersi a cosa possa servire una blockchain al posto di una qualsiasi altra tecnologia, inclusa la cara vecchia carta stampata: perché un asset come un buono Amazon, un buono pasto, o una gift card dovrebbero essere emessi in forma di token?

Fra gli ipotetici vantaggi, potremmo dire che la possibilità di trasferire comodamente assets di questo tipo a terzi potrebbe essere un valore aggiunto. Inoltre, se la tecnologia di tokenizzazione e management dei token fosse semplice ed efficace, creare un buono pasto su blockchain potrebbe essere più veloce ed economico rispetto all'installazione e configurazione di un software alternativo per la sua emissione e certificazione. Se si è fortunati, eventualmente, in certe giurisdizioni potrebbe anche aiutare ad evitare qualche noia burocratica e gabelle istituzionali. Sono queste motivazioni sufficienti?

Forse l'utility token su blockchain ha un senso, ma in generale il grosso del valore aggiunto di una tale soluzione si ha solo ed esclusivamente se i destinatari dei token possedessero già un wallet che è in grado di processarli, cioè

se esistesse già un effetto network. Poiché difficilmente questo è il caso odierno – salvo situazioni molto particolari, ad esempio token pensati per una nicchia specifica di utenti – viene anche a mancare la motivazione principale che renderebbe più comodo utilizzare tale tecnologia. Rimangono invece i problemi di scalabilità che rendono costoso scambiare tali token onchain e complicato scambiarli offchain: è plausibile che nasca spontaneamente un network di nodi molto ben interconnessi per muovere bitcoin su Lightning Network, ma è improbabile che lo stesso accada per ogni singolo utility token sul mercato.

In definitiva, l'utility token su blockchain può avere degli usi limitati, ma non stupisce che ad oggi non ci siano esempi significativi di successo.

3.3 Il security token e le stablecoin

Tokenizzare una security significa **rappresentare in un token un diritto di proprietà** (come le quote di un'azienda) o un credito. Tale diritto è solitamente garantito da chi emette il token, che si vincola contrattualmente a riconoscere il token come titolo al portatore. Il token può anche essere rappresentativo di un asset in custodia presso l'ente emittente: un esempio è proprio la stablecoin Tether che ha il dollaro come sottostante. A livello teorico si può ricomprendere le stablecoin all'interno della più ampia definizione di security token, anche se in alcune giurisdizioni la classificazione può essere diversa per questioni legali.

Il dollaro oggi viaggia sostanzialmente in tre forme: **la banconota, il dollaro digitale e Tether** su blockchain[10]. La prima permette transazioni decentralizzate e anonime, il secondo è iper-centralizzato e controllato da banche e autorità monetarie, il terzo ha proprietà di anonimità e anti-censura simili alla banconota, ma è molto più facile, veloce ed economico da scambiare in grandi quantità e senza frizioni

dovute alla distanza fisica. Nel mondo crypto, Tether diminuisce i costi operativi e i tempi di trasferimento, avvicinando i mercati e facilitando la price discovery dei token. Inoltre, permette ad exchange senza KYC/AML di tradare crypto contro “dollari”.

Di fatto, il vantaggio di Tether rispetto ai dollari digitali delle banche è quello di **scavalcare dei vincoli imposti dalle autorità e le loro lungaggini burocratiche**, perciò si potrebbe pensare che il vantaggio tecnico sia solo immediato, cioè fintanto che le autorità non aggiornino le proprie leggi così da regolare anche questo nuovo ambito. Dopotutto, se Bitcoin è emesso in maniera decentralizzata, l’emissione di una security è invece sempre centralizzata, perciò in qualche modo perseguibile dalle autorità. Eppure, il vantaggio di una blockchain per una security è palpabile: **la blockchain è la prima tecnologia in grado di *trasferire* i titoli al portatore in forma digitale senza affidarsi a un sistema centralizzato.** Nel caso dei security token parliamo solo di *trasferimento*, non di *emissione*, ma fa comunque la differenza e lo vediamo con un esempio.

Pensiamo a una società per azioni iraniana che volesse raccogliere investimenti dal resto del mondo. Un utente americano non può acquistare quelle azioni sul Tehran Stock Exchange, ma potrebbe acquistare dei security token direttamente dall’azienda (o su un DEX) in cambio di bitcoin. Potrebbe persino **esercitare i propri diritti amministrativi sull’azienda, dimostrando crittograficamente e nell’anonimato l’ownership di una security**, usando la propria chiave privata. Se anche il legislatore americano fosse contrario a tali pratiche, potrebbe diventare cattivo cattivo e battere i pugni sul tavolo forte forte, ma difficilmente riuscirebbe ad essere efficacemente d’intralcio.

Possiamo immaginare un futuro in cui aziende o lavoratori

autonomi emettano liberamente azioni, obbligazioni o quote sociali su blockchain che vengono poi trasferite senza alcuna frizione. Arbitri privati eletti dalle parti gestiranno casi di frode da parte dell'emettitore del token: ad es. se l'utile aziendale non è redistribuito come pattuito in base alla distribuzione dei token assegnati, se i diritti amministrativi associati al token vengono negati o se l'inflazione del token non rispetta i termini dell'offerta pubblica. Qualora si sollevassero dei contenziosi, la natura del token e la **totale assenza di frizioni negli scambi** porterebbe nell'immediato a una caduta del suo valore.

Sono prospettive futuristiche, ma è doveroso provare a innovare in questo ambito: dove arriva la tecnologia, prima o poi arriverà la società. Almeno nell'ambito finanziario si profilerebbe **un mondo più libero**, dove lo Stato non è più necessario, o quantomeno è relegato a un ruolo minimo ben lontano da quell'autorità coercitiva totalitaria che è oggi, guidata da una maggioranza parassitaria[11] di cittadini che non producono ricchezza.

4. Il DEX

Sia l'idea che le prime implementazioni di DEX sono senz'altro antecedenti a Ethereum stessa[12] e l'utilità va oltre a quello che è il mero trading a zero-sum-game: poter scambiare senza la necessità di dare in custodia i propri fondi a un'entità centralizzata, nel rispetto dell'anonimato e al riparo da censura e costi dovuti alle ingerenze di autorità istituzionali e intermediari. I DEX su Ethereum però soffrono di cinque principali problemi, dovuti al modello architetturale della blockchain di Ethereum stessa, motivo per cui negli ultimi anni sono nati alcuni progetti con l'obiettivo di abilitare il mondo DeFi/DEX su Bitcoin.

1. Ethereum è un sistema architetturalmente **instabile** che soffre **problemi di governance**. Questa è un'affermazione forte che verrà discussa a breve con un approfondimento

dedicato.

2. I DEX permettono di scambiare **solo erc-20 ed Ether**. Per scambiare Bitcoin è necessario usare un suo derivato erc20, ovvero è necessario che un'entità custodisca BTC come sottostante di un nuovo token su Ethereum
3. Gli scambi su Ethereum vengono effettuati **esclusivamente onchain.** Il che sostanzialmente comporta che ogni exchange basato su smart contracts abbia una sorta di "data di scadenza": quella in cui i costi fissi delle transazioni iniziano ad essere troppo elevati per la stragrande maggioranza di utenti, lasciando il campo alle sole whales.
4. **Gli smart contracts** richiedono un certo ammontare di gas (Eth da pagare ai miners per vedere la transazione inclusa nella blockchain), generalmente proporzionale alla quantità di codice presente nel contratto. Se però il **gas pagato <u>non</u> è sufficiente** per essere appetibile per un miner, perché compete con altre transazioni che pagano maggiori fee, allora quel contratto rimarrà in stallo non aggiornando più il suo stato, quantomeno finché non diminuisce il livello di congestione della blockchain. Da smart a poco smart è un attimo.
5. La tanto sbandierata **Touring completeness di Ethereum rende imprevedibili e inaffidabili gli smart contracts**, poiché il loro esito dipende dallo stato della blockchain in un certo momento e può essere imprevedibile nel futuro. **Uno sviluppatore non sa necessariamente quale sarà l'esito di un contratto nel futuro o quanto gas questo consumerà**, perciò tendenzialmente provvede ad alimentarlo con una quantità di Eth sufficiente a coprire lo scenario peggiore. Non sempre però è facile tenere conto di tutte le variabili, come dimostrano il famoso **DAO hack[13] che ha poi portato a un "rollback" dell'intera rete o il fallimento del multiple signature validation program di Parity[14]**'[15] che ha provocato la perdita di oltre 500

mila ETH.

5. I problemi di Ethereum ed Ethereum 2.0

L'eccessivo peso di Ethereum sta portando problemi di sicurezza e affidabilità del network. È significativo che, recentemente, Vitalik Butherin abbia persino chiesto a Bitfinex di smettere di usare Ethereum per muovere Tether[16], che è il token in assoluto più di successo della storia di Ethereum. Nel frattempo, le fee stanno salendo a dismisura ed è iniziata la corsa per il lancio di Ethereum 2.0. Vediamo di chiarire cosa sta succedendo.

Adam Back la tocca piano. Ma proseguendo nella lettura inizierete a pensarla un po' come lui…

5.1 L'archival node di Ethereum, una bestia in via d'estinzione

L'archival node (o full sync in modalità "archive"[17]) è quel nodo che valida e salva su disco l'intera blockchain, mentre gli altri nodi di Ethereum mantengono solo lo stato attuale della rete, scartando tutti i passaggi intermedi. Quindi un nodo non archival non conosce quale fosse lo stato di un contratto o il valore di un account a una certa data nel passato. Il problema è che Ethereum è utilizzato principalmente in ambito finanziario – quantomeno per quanto riguarda le applicazioni DeFi – per cui dovrebbe poter essere sempre possibile avere un record dello storico e sapere cosa è successo nel passato. Gli archival node sono però sempre più rari.

Il problema è che la blockchain di Ethereum arriva a 5 terabyte di dati e cresce di circa 2 terabyte all'anno. **È impraticabile mantenere un archival node per qualsiasi utente che non sia un grosso servizio o block explorer**. I nodi di

questo tipo rimasti online sono così rari che Vitalik stesso ne ha fatto menzione parlando di “one of those big, scary nodes”. È possibile che un ecosistema pensato per la “finanza decentralizzata” debba affidarsi a un numero di nodi che – forse – si conta sulle dita di una mano, per certificare[18] un qualsiasi record nel passato?

Oltre alla centralizzazione di queste informazioni, il problema è anche che questi nodi potrebbero effettivamente estinguersi. **Infatti, se per un problema tecnico, o per un upgrade del software buggato i nodi cadessero (come storicamente capitato[19]), ci vorrebbero mesi per rilanciarlo o per ricostruire l’intera chain** a partire da un fullnode. Il problema non è la mole di dati, poiché pressoché chiunque può permettersi un HDD da 10 terabyte, quanto piuttosto il tempo necessario a validarli e processarli. La più recente versione del nodo Ethereum Geth impiega oltre 1 mese[20] per sincronizzare dal genesis block su un server professionale AWS EC2 (8 core, 32 GB RAM, almeno 6 terabyte SSD). È impossibile farlo per un utente comune senza sobbarcarsi i costi di noleggio e configurazione delle macchine. Ricostruire un archival node a partire da un fullnode è altrettanto lungo e costoso[21].

5.2 Il network centralizzato: AWS e Infura come single point of failure?

Il problema di Ethereum non è limitato alla questione degli archival node. Un qualsiasi nodo in fast synch richiede le stesse risorse di un archival, eccetto che salta la validazione delle transazioni dello storico e inizia a processare dallo stato corrente della rete in poi[22]. Una volta “in pari” rispetto allo stato attuale, le risorse utilizzate nella sincronizzazione sono simili. Oggi un nodo Ethereum Geth occupa 474gb su un SSD, in crescita di circa 300GB all’anno (pesava 173GB nel settembre scorso)[23]. La spesa iniziale soltanto in hardware per far girare tale nodo, senza calcolare la banda richiesta, l’elettricità e la

manutenzione, è di circa 850 dollari per uno sviluppatore che si assembli e configuri autonomamente la macchina[24]. Un impianto interamente dedicato di questo tipo richiedrebbe, per sincronizzare un solo mese di blockchain, circa 4 giorni[25], cosa che Bitcoin fa in meno di 1 ora.

Il noto modello di sicurezza e decentralizzazione del network di Ethereum

I costi di manutenzione e banda rendono complicato il mantenimento di tale nodo in loco, perciò ci si affida sempre più a server specializzati. **Secondo uno studio[26] il 60% dei nodi Ethereum gira su Amazon Web Services**. Inoltre, ci sono servizi estremamente centralizzanti, come Infura, che si appoggia ad AWS e gestisce fino al 10% dei nodi dell'intera rete. **Infura ospita i nodi di moltissimi sviluppatori**, poiché permette comodamente all'utente di interfacciarsi col nodo via web e operare come se l'avesse in casa. Secondo Michael Wuehler, il co-founder di Infura, **con la loro infrastruttura stanno "effettivametne supportando l'intero ecosistema di decentralized application di Ethereum**"[27]. Se davvero la gran parte dei liquidity providers delle DEX pool si appoggiasse a Infura, cosa succederebbe agli smart contracts in caso di crash delle loro macchine? O se un'autorità desse mandato di sospendere le attività? Insomma, AWS e Infura potrebbero costituire un enorme "single point of failure". Per di più, **Infura colleziona i dati personali degli utenti che si registrano al servizio, gli indirizzi dei loro wallet e gli IP in cui sono localizzati**. Il tutto alla mercé del primo burocrate o giudice che ci voglia mettere il naso. Insomma, non si configura propriamente con un network decentralizzato.

Infine, i continui errori tecnici rendono il network instabile, con numerosi e continui crash e malfunzionamenti dei nodi, come il recente bug nell'upgrade di Parity[28] che

richiede un riavvio manuale dei nodi (che può durare mesi, se sono archival). Non è raro avere cadute nel numero di nodi e, in base alle statistiche di Ethernodes[29], sembrerebbe persino che in aprile di quest'anno ci sia stato un crash – o un aggiornamento massivo di qualche grosso servizio[30] –, che ha portato offline quasi l'80% di tutti i nodi della rete (presumibilmente tutti i nodi Geth, a giudicare dal numero).

Misterioso drop dei nodi Ethereum l'11 aprile di quest'anno? Chi ha info in merito si faccia avanti!

5.3 La governance centralizzata

La centralizzazione dei nodi non comporta solo dei possibili single point of failure, ma anche problemi più generali di governance del network. Una blockchain è governata dai suoi utenti, nello specifico quelli che hanno nodi validatori: in Ethereum sono i fullnode (inclusi gli archival) e i fastnode. Se però questi nodi non sono distribuiti fra gli utenti vi è un accentramento del potere decisionale in mano a pochi. Facciamo alcuni esempi concreti di fork avvenuti nella storia recente:

- L'inflazione di Ethereum è stata modificata continuamente da vari upgrade: con l'upgrade Byzantium dell'ottobre 2017 la creazione di ETH in ogni blocco è scesa da 5 a 3[31], mentre con l'upgrade Constantinople del febbraio 2019 l'inflazione è scesa da 3 a 2 ETH per blocco. Si tratta sempre di hard fork upgrade, che rendono cioè incompatibili i nodi precedenti. Il punto non è tanto che un upgrade sia deflattivo o inflattivo, quanto piuttosto che tali upgrade su questioni fondamentali, come l'inflazione del token, vengano applicati e accettati praticamente senza discussione da parte della community
- Lo stesso succede per il Gas Limit, che è

sostanzialmente il block size di Ethereum, ovvero quanto gas può essere speso in un blocco. Tale parametro ha ovviamente un effetto diretto sulle dimensioni della blockchain. Nel giugno 2017 è stato aumentato il Gas Limit mentre oggi i miners stanno discutendo di un ulteriore aumento per mitigare le fee[32].

- L'evento più emblematico rimane comunque il "rollback" di Ethereum dopo il DAO hack: è stata cancellata e riscritta parte della storia e dei blocchi di Ethereum, al fine di restituire i fondi rubati a chi aveva programmato uno smart contract vulnerabile a un attacco hacker, attacco che si è puntualmente verificato. Si tratta a tutti gli effetti della modifica della blockchain ai fini di censurare una transazione. Un evento analogo potrebbe accadere con la stessa facilità qualora un'autorità politica volesse censurare transazioni o imporre le proprie decisioni.

In Bitcoin, dei fork di questo tipo genererebbe senza dubbio uno split della rete, con i proponenti che si ritroverebbero nella parte minoritaria, schiacciati dal numero di nodi dei bitcoiners. Abbiamo già visto degli esempi nella storia. In merito, non è tanto interessante lo split della rete fra Bitcoin e Bitcoin Cash, quanto piuttosto il braccio di ferro fra massimalisti di Bitcoin e SegWit2x. Nel caso del fork di Bitcoin Cash infatti, i sostenitori di un aumento del blocksize partivano da una posizione minoritaria e sono rimasti una minoranza, che presto o tardi verrà totalmente dimenticata. Nel secondo caso invece, i proponenti di SegWit2x erano oltre il 70% dei miners e una lista di 72 aziende[33] (servizi, exchange, block exlorers, payment processors), oltre che alcuni noti sviluppatori di Bitcoin (Jeff Garzik aveva commit access alla repository del codice di Bitcoin su github). Una potenza schiacciante di questo tipo avrebbe potuto guidare qualsiasi tipo di upgrade, se non fosse che gli holders hanno fatto fronte comune. Gli utenti che facevano girare un nodo Bitcoin semplicemente non hanno scaricato la

versione SegWit2x, impedendo così che l'hard fork potesse prevalere su un'unica catena. Si sarebbero inevitabilmente create due catene in competizione, e gli holders hanno dimostrato in anticipo la loro intenzione di sbarazzarsi dei token Bitcoin SegWit2x preferendo la catena legacy di Bitcoin (BTC), scambiando i rispettivi future su exchange. Di fronte al rischio di una disfatta contro la community Bitcoin, la maggioranza di miners e aziende si sgretolò, rinunciando all'upgrade[34].

Su Ethereum non ci sarebbe stata partita, in quanto l'utente medio non ha alcun peso nelle decisioni di governance, poiché fa girare un lightnode o si appoggia a un custodian, quindi in ogni caso si deve affidare a terzi.

Vitalik già da piccolo dava cattivi consigli agli amici

6. Ethereum 2.0: dalla padella alla brace

6.1 La centralizzazione del POS

Ethereum 2.0 non fa che peggiorare l'accentramento della rete. Anzitutto, introduce una Proof of Stake dove i più grandi holders mantengono una rendita di posizione. Quantomeno, con il POW i miners potevano avere un ricambio dovuto a una questione di merito, favorendo chi riesce ad essere più efficiente in termini energetici o nella produzione o fornitura di hardware di qualità. Nel POS invece, chi è più ricco guadagna tutti i coin di nuova creazione semplicemente tenendo fermi in un indirizzo i propri soldi, senza alcuno sforzo. Bisogna ricordare che Ethereum è stato lanciato il 30 luglio 2015 con 72 milioni di coin pre-minati, che ancora oggi contano per il 64% dell'intero supply di ETH.

6.2 Gli ASICS dell'Ethereum foundation nel POS: si, per davvero!

In secondo luogo, il POS è ancora una tecnologia altamente sperimentale, che presenta alcune criticità di tipo tecnico. Non ci sono ad oggi tecniche comprovate per introdurre un elemento di “casualità” in un sistema digitale decentralizzato e chiuso. La casualità deve essere introdotta “dall’esterno”. In particolare, nel POS di Ethereum esistono “round” in cui i validatori dei blocchi si alternano in “commissioni”. La creazione di tali commissioni deve prevedere un elemento di casualità affinché questi validatori non possano “giocare sporco” ed essere eletti più frequentemente del dovuto come creatori del blocco. Ironia vuole che questo elemento di casualità su Ethereum 2.0 sia dato da dei nodi specifici che fanno a gara nel trovare una funzione, utilizzando degli ASICS creati ad hoc per il calcolo di quella funzione VDF (una verifiable delay function). Esatto, proprio come in un POW! E il bello deve ancora venire: quegli ASICS sono stati prodotti e distribuiti dall’Ethereum Foundation, parola di Justin Drake![35]

> Sembrerebbe che per Justin Drake Ethereum 2.0 sia sviluppato non dalla community, ma dall’Ethereum Foundation. Loro (“We”) svilupperanno la funzione di randomizzazione e sempre loro producono gli ASICs per calcolarla. Non sembra nemmeno toccarlo l’idea che un singolo produttore di ASICS possa essere un vettore d’attacco (qualche reminiscenza della backdoor sugli Antminer di Jihan Wu?)

6.3 Far finta di scalare: lo sharding con node relayers giganteschi

I piani di lungo termine per la scalabilità di Ethereum 2.0 non sono per nulla promettenti, oltre che davvero poco eleganti dal punto di vista tecnico. Mentre Bitcoin punta sugli scambi Lightning Network da wallet a wallet, senza

occupare spazio su blockchain e quindi anche istantanei, privati e a fee quasi nulle, la strategia di Ethereum è invece quella di creare una serie di “sidechain” che fanno capo a una sola (la Beacon chain). Questo è sostanzialmente il concetto di sharding: dividere il peso di una sola blockchain fra tante catene parallele, così che la gran parte dei nodi possa sopportare il peso di una soltanto, validando una parte delle transazioni del network.

In realtà, perché questo sistemi funzioni, riesca a calcolare le fee e assicuri un corretto coordinamento fra tutti gli shards (le “sidechain”), ha bisogno di supernodi che si occupino della comunicazione fra le varie catene e la beacon chain, che sono detti node relayer. Inizialmente, Vitalik Butherin aveva pensato alla possibilità di avere fino a 1024 shards: se tutti attivi e operativi, i supernodi processerebbero “solo” 20 Megabyte al secondo. Vitalik stesso nel discutere il design di Ethereum 2.0 linka un hard drive da 14 Terabyte, dicendo[36] che un node relayer necessiterebbe “soltanto” di un hard drive a settimana dal costo di 449,99$[37], spesa che sarebbe accessibile per un block explorer. Alla faccia della decentralizzazione.

Ma diciamo pure che 1024 “sidechain” siano il massimo previsto nel lunghissimo periodo. Ipotizziamo che nei primi anni ne sia sufficiente un centinaio. Si tratterebbe comunque di 2MB di dati al secondo, ovvero 1.5GB in 10 minuti, mentre un fullnode e relayer Bitcoin occupa 1,5MB in 10 minuti, ovvero 1000 volte meno!

Visto l’esagerato carico sulle spalle dei node relayers, in un’ipotesi più recente[38] il numero di shards possibili sarebbe diminuito da 1024 a 64. Insomma, si parla di un aumento lineare della capacità fino a un massimo di 64 volte (quando per una reale adozione di massa occorrerebbe invece un aumento esponenziale), sacrificando però il modello di

decentralizzazione che dovrebbe essere alla base del progetto.

Alla luce di tutto ciò, ora il lettore potrà comprendere perché Adam Back affermi che Ethereum è alla stregua di qualsiasi altro scam presente nel mercato crypto[39]. Un approccio serio alla scalabilità di lungo termine è quello di Bitcoin, ben riassunto nell'articolo "Sopravvivere alla bull run: scalare con Bitcoin": https://www.albertodeluigi.com/2019/07/18/sopravvivere-alla-bull-run/

7. DeFi su Bitcoin

Visti da un lato i limiti di Ethereum, ma dall'altro anche l'importanza di un'idea sana di tokenizzazione e Decentralized Exchange, sono nati recentemente alcuni progetti per abilitare questo mondo su Bitcoin.

7.1 RGB

RGB è nato da un'idea di Peter Todd e Giacomo Zucco e permette di creare e trasferire token incapsulandoli nelle transazioni Bitcoin. Sarà possibile anche trasferire token con Lightning Network ed effettuare scambi sul DEX battezzato Spectrum. Il vantaggio rispetto a soluzioni già esistenti su Bitcoin come Omni Layer (che è stato per anni il principale vettore di Tether) è che la transazione Bitcoin sottostante non è più voluminosa e costosa di una transazione qualsiasi e non è più distinguibile da transazioni standard, per una migliore privacy. Poiché un exchange effettua sempre transazioni Bitcoin con una buona frequenza, incapsulare in queste anche movimenti di altri asset, come ad esempio Tether, sarebbe gratuito per l'exchange. Se tuttavia un utente volesse trasferire esclusivamente il token Tether, dovrebbe comunque effettuare una transazione Bitcoin, almeno finché non troverà applicazione pratica l'idea di Peter Todd di "proof Marshall". Da questo punto di vista quindi, RGB è adatto ad un exchange che fa abitualmente transazioni in BTC con una buona

frequenza, ma crea “inquinamento” sulla blockchain Bitcoin se l’obiettivo dell’utente è esclusivamente quello di effettuare transazioni nel mondo DeFi.

Scopri di più su https://rgb-org.github.io/ o sul gruppo telegram https://t.me/rgbtelegram

7.2 Mintlayer

MEGA-DISCLAIMER: Mintlayer è un progetto scaturito dalle mie idee e quelle di Enrico Rubboli (former Bitfinex senior engineer). Siccome mi farà diventare schifosamente ricco e diaboliko (mika come voi povery!) il mio consiglio nell’approcciare questa sezione è don’t trust niente di quello che scrivo qui e verify tutto personalmente.

Scherzi a parte, leggete il consensus paper di Mintlayer miei piccoli nerd

Mintlayer può essere visto come una sorta di add-on al wallet Bitcoin e che ne abilita le funzionalità DeFi: oltre a permettere la creazione e il trasferimento di token (anche su Lightning Network) abilita veri e propri scambi decentralizzati da wallet a wallet. Nel DEX è possibile scambiare token creati su Mintlayer, ma anche direttamente BTC, tramite il primo atomic swap sicuro di Bitcoin inter-chain[40].

Dal punto di vista tecnologico, si tratta di un progetto ibrido fra un sistema POS e una sidechain Bitcoin. Sfruttando Bitcoin, riesce a superare i limiti intrinseci al POS:

- l’algoritmo di selezione dei validatori delle transazioni non necessita di ASICs che calcolino funzioni VDF come avviene in Ethereum 2.0, perché la sorgente di randomizzazione è direttamente l’hash del

blocco Bitcoin (esito della POW).
- I long-range attack tipici del POS sono scongiurati, grazie ai checkpoint sulla catena BTC. Quindi nel lungo termine la catena Mintlayer eredita la sicurezza della Proof of work di Bitcoin.

Diversamente da un POS tradizionale non esiste mining, ovvero non c'è creazione di "coin" in concomitanza alla creazione di blocchi.

Il grande vantaggio rispetto ad altri sistemi di tokenizzazione su Bitcoin è che per confermare un trasferimento su Mintlayer non sono necessarie transazioni BTC e fee pagate sulla blockchain di BTC: ogni transazione viene validata esclusivamente sulla sidechain e le fee possono essere pagate ai validatori in qualsiasi token creato su Mintlayer, come ad esempio in Tether. Inoltre, i token possono essere emessi con Access Control List (ACL), che per esempio permette di fare whitelisting o blacklisting dei destinatari, o pone dei limiti nell'ammontare massimo o minimo delle transazioni: è un meccanismo utile ad esempio per chi emette una security che sia vincolata a delle policy aziendali o altri requisiti legali.

L'ambizione dietro a questo progetto è quella di spostare l'intero ecosistema di token crypto dall'Ethereum erc20 ad un "layer" costruito su Bitcoin e che si interfacci direttamente con Bitcoin, su cui forgiare ("mint") qualsiasi asset in forma di token. Immagino cioè un futuro in cui l'intero ecosistema crypto non sia più composto da decine di token e blockchain, in cui gli utenti non useranno più MyEtherWallet con la sua selva di erc20, ma soltanto un wallet Bitcoin e i token creati con l'add-on Mintlayer.

Nella progettazione di Mintlayer due fattori sono stati tenuti principalmente in considerazione:

1. Rimanere **accessibile a qualsiasi utente**, con fullnode

economici.

Per rimanere a misura d’utente è necessario avere un tetto alle dimensioni onchain, perciò il blocksize è fissato a 1MB. A questo punto però, è necessario sfruttare al massimo quello spazio. Oltre all’uso di Lightning Network, Mintlayer punta all’aggregazione di pagamenti: gli utenti possono unire le loro transazioni direttamente tramite una funzionalità del wallet, prima di trasmetterle alla blockchain. Si tratta di **batching peer-to-peer**, ovvero di un meccanismo ispirato ai coinjoin di Wasabi wallet e che fa perno sull’aggregazione delle signature per **comprimere ogni pagamento a circa un terzo del suo peso**. Poiché i trasferimenti con batching hanno **maggiore privacy e pagano fee più basse**, gli utenti avranno un incentivo naturale ad effettuare questo tipo di transazioni, facendo così della loro convenienza personale un comportamento virtuoso per l’ecosistema della blockchain, che vedrà un gran risparmio dello spazio altrimenti occupato. Il batching è inter-token, ovvero è possibile aggregare pagamenti diversi fatti in qualsiasi token su Mintlayer.

2. La possibilità di raggiungere un **effetto network**.

Parlando con big player nel mercato crypto, come Giancarlo Devasini di Bitfinex/Tether, è emerso che il problema principale di sidechain come Liquid è che non vengono adottate da exchange e servizi, perciò chi crea un token preferisce utilizzare blockchain già note e utilizzate nell’ecosistema. Per esempio, Tether su erc20 o Tron lo accetteranno tutti gli exchange che già processano Ethereum e Tron, mentre per accettare Tether su Liquid sarebbe necessario mantenere un nuovo nodo, coi costi connessi. Un exchange non ha alcun incentivo a installare nuovi nodi senza che questi supportino token che possano fruttare commissioni di trading, una volta listati sull’exchange.

Mintlayer introduce il token MLT per la validazione della chain e la raccolta delle fee, e che quindi può anche essere

attrattivo per traders e speculatori. Questo fatto rappresenta un incentivo per exchange e servizi a installare il nodo e quindi, a quel punto, a essere pronti per ricevere qualsiasi token di nuova creazione su quel sistema, esattamente come avviene oggi per gli erc20 su Ethereum.

Quindi c'è un token? Si. Abbiamo discusso a lungo questa scelta, sapendo che potesse essere controversa per alcuni massimalisti. Un'alternativa sarebbe stata quella di finanziare lo sviluppo tramite la vendita di un gettone infungibile che garantisse all'holder una posizione di partecipante della rete (un blocksigner che raccoglie le fee di transazione), ma in realtà il token fungibile MLT è una soluzione migliore per molte ragioni:

1. Permette di distribuire l'ownership di uno "slot" da blocksigner aggregando i token di più utenti in un unico "stake"
2. Un token fungibile è una migliore misura del valore dello slot e in generale della sidechain, perché in quanto divisibile è più facilmente vendibile e misurabile nel valore rispetto ad altri beni nell'economia
3. In conseguenza di 1 e 2, dà la possibilità di avere un mercato più dinamico dei partecipanti alla rete Mintlayer, favorendone la decentralizzazione
4. Non costringe a pagare fee di transazione in una qualsiasi altra security/stablecoin presente sulla rete, che per loro natura saranno comunque sempre più centralizzate del token MLT
5. È una migliore attrattiva per investitori e quindi agevola il finanziamento dello sviluppo

Scopri di più su mintlayer.org o sul gruppo telegram https://t.me/mintlayer

[1] Al di là della facile ironia, mentre l'uso della

blockchain per verificare la provenienza di un prodotto come una pera o un pollo è veramente un'idiozia, la notarizzazione sulla blockchain può spesso avere un senso. Ergo, trasmettere alla blockchain l'hash di un documento che prova il proprio consenso all'atto sessuale potrebbe anche avere valore legale ed essere un caso d'uso valido della tecnologia. Insomma, a legalfling sono meno cialtroni di Carrefour? Può darsi.
https://www.reuters.com/article/us-carrefour-blockchain-ibm/chickens-and-eggs-retailer-carrefour-adopts-blockchain-to-track-fresh-produce-idUSKCN1MI162
https://legalfling.io/

[2] In realtà la stessa blockchain di Ethereum fino al 2020 è rimasta una piccola nicchia rispetto a Bitcoin: i volumi transati di ETH sono raddoppiati negli ultimi tre mesi e quelli in erc20 USDT sono quintuplicati da inizio anno.
https://www.theblockcrypto.com/linked/74975/bitcoin-ethereum-on-chain-volume-july

[3] La quasi totalità dei volumi sulla blockchain Bitcoin rappresenta trasferimenti monetari in BTC, o comunque transazioni di apertura dei canali Lightning Network col fine ultimo di transare BTC (offchain). Da notare che nel grafico comparativo dei volumi trasportati sulle varie blockchain, il transato su Lightning Network non è incluso.

[4]
https://insights.glassnode.com/defi-spike-ethereum-gas-price/
Another one: https://insights.glassnode.com/ethereum-fees/

[5] Non necessariamente la transazione che paga più fee è quella che occupa più spazio, ma ai fini di questa analisi si può considerare un buon proxy

[6] Vedi ad esempio Uniswap: https://uniswap.org/docs/v2/protocol-overview/how-uniswap-works/

[7] Il grosso delle transazioni di arbitraggio avvengono fra

Uniswap e Balancer

[8] Il seguente articolo presenta un ottimo esempio delle complessità tecniche in cui si può incorrere, la qualità dei BOT presenti e l'importanza di arrivare per primi su un trade, possibilmente avvalendosi di una collaborazione con un miner per validare immediatamente le transazioni onchain: https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dff

[9] https://www.albertodeluigi.com/2020/07/14/il-denaro-caratteristiche-intrinseche

[10] o più recenti alternative come USDC e altre stablecoins

[11] https://www.albertodeluigi.com/2020/05/12/la-tragedia-della-moneta-fiat/#a3

[12] il primo codice di Bitsquare – oggi Bisq – è stato rilasciato nel 2014

[13] https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability (V. Buterin. CRITICAL UPDATE Re: DAO Vulnerability, June 2016)

[14] https://www.parity.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/

https://paritytech.io/blog/the-multi-sig-hack-a-postmortem.html (Parity. The multi-sig hack: A postmortem, July 2017)

[15] Vedi anche: https://blockstream.com/simplicity.pdf

[16] Dichiarazione di Paolo Ardoino, CTO Bitfinex: https://youtu.be/VxSKy7x7Wiw

[17] Ci sono quattro tipi di nodo Ethereum:

Archival node (full sync): scarica i block header, i block body (tutte le transazioni) e valida ogni elemento dal genesis block. Quindi salva e conserva su disco tutta la blockchain (è sostanzialmente una Full synch con modalità: **–gcmode=archive**)

Full node (full sync): scarica i block header, i block body (tutte le transazioni) e valida ogni elemento dal genesis block. Non salva su disco tutta la blockchain, facendo pruning (potatura) degli stati intermedi.

Fast node (fast sync): scarica i block headers e i block body dal genesis block, quindi prende uno snapshot dello stato attuale e inizia a validare tutte le transazioni solo dal 64esimo blocco prima del blocco corrente

Light node (light sync): scarica solo lo stato attuale. Per validare ogni elemento, necessita di comunicare con un full node (come un light node di Bitcoin, ovvero un wallet mobile)

[18] Un wallet verosimilmente salva in locale alcune informazioni come il proprio storico, ma non è una fonte certificabile da terzi

[19] https://cointelegraph.com/news/rushed-upgrade-made-12-of-ethereum-clients-unusable

[20] https://blog.ethereum.org/2019/07/10/geth-v1-9-0/
Il test è eseguito nell'aprile 2019 quando la blockchain cubava 2.32 TB, oggi pesa 5terabyte. Perciò il tempo di sync è ragionevolmente più che raddoppiato. Questo il dato riportato per il test:

Version	Sync time	Disk size
Geth v1.9.0	13d 19h	2.32TB

Macchina: AWS EC2 instances (8 core, 32 GiB RAM, 3TiB EBS SSD) with –cache=4096 –syncmode=full –gcmode=archive.

[21] Il test effettuato nell'aprile 2019 ha impiegato 28 giorni su una macchina da 16gb RAM e 2 TB SSD. Ad oggi verosimilmente impiegherebbe più di 2 mesi (calcolando che nel tempo richiesto per arrivare allo stato della mainnet, la blockchain intanto continua ad aumentare di volume). https://medium.com/@marcandrdumas/are-ethereum-full-nodes-really-full-an-experiment-b77acd086ca7

[22] Qui le weaknesses: https://github.com/ethereum/go-ethereum/pull/1889
L'archival node in realtà è sensibilmente più lento nelle operazioni su disco rispetto a un fullnode per via dell' "indicizzazione" dei dati, essendo più grande la mole di informazioni conservate. Si veda: https://github.com/ethereum/go-ethereum/issues/18984#issuecomment-460624422
"Regarding the huge disk IO, that's leveldb compaction. Trie nodes are hash->value mapping, so every trie node we insert into the database gets dumped at a random location. Since leveldb stores everything sorted by key, the more random stuff we insert, the more maintenance overhead it is to keep them sorted. Hence where the insane disk IO comes from. Unfortunately this is a limitation of the data model Ethereum was designed to use (Merkle Patricia trees)."

[23] https://etherscan.io/chartsync/chaindefault
I nodi Geth sono la stragrande maggioranza all'interno della rete (oltre 7000 su circa 9000).

[24] La configurazione usata per questo test con nodo Parity a 16gb ram e 2tb SSD: https://medium.com/@marcandrdumas/are-ethereum-full-nodes-really-full-an-experiment-b77acd086ca7

[25] Vedi l'intero thread: https://twitter.com/ercwl/status/1171554491491131392

[26] Lo studio risale al settembre 2019, un anno fa. Secondo

l’analisi, 2195 nodi (il 60% dei nodi in quella data) giravano su AWS. https://thenextweb.com/hardfork/2019/09/23/ethereum-nodes-cloud-services-amazon-web-services-blockchain-hosted-decentralization/

[27] “[We’re] effectively supporting the entire ethereum dapp ecosystem with the RPC traffic” https://bravenewcoin.com/insights/ethereum-price-analysis-on-chain-fundamentals-increasing

[28] I nodi Parity dalla versione 2.7.2 hanno un bug che provoca apparentemente in maniera casuale il blocco del nodo. Il bug colpisce il 50% dei nodi Parity e tutti I nodi OpenEthereum (il 12% dell’intero network secondo Ethernodes.https://cointelegraph.com/news/rushed-upgrade-made-12-of-ethereum-clients-unusable
Un altro bug segnalato nell’aprile 2020, questa volta in Geth (1.9.12 e 1.9.13), che consuma tutta la memoria e si disconnette dalla rete di peers: https://github.com/ethereum/go-ethereum/issues/20963

[29] https://ethernodes.org/history

[30] Non trovo altre fonti in merito. Se avete informazioni scrivete a mail@albertodeluigi.com

[31] Per bilanciare l’effetto deflattivo dell’upgrade, al contempo la frequenza di generazione dei blocchi si è alzata, prevedendo circa 10 secondi in meno fra un blocco e l’altro e aumentando di conseguenza l’inflazione di ETH creati con ogni blocco.

[32] https://cointelegraph.com/news/ethereum-miners-vote-to-increase-gas-limit-causing-community-debate

[33] https://www.albertodeluigi.com/segwit2x-statement/

[34] https://www.albertodeluigi.com/2017/12/08/battaglia-per-bitcoin/#8

[35] Vedi

[36] Vedi

[37] https://www.newegg.com/seagate-ironwolf-st14000vn0008-14tb/p/N82E16822184759?Item=N82E16822184759&source=region&nm_mc=KNC-GoogleAdwords-PC&cm_mmc=KNC-GoogleAdwords-PC-_-pla-_-Hard%20Drives-_-N82E16822184759&gclid=EAIaIQobChMI7ZOcx6Sh4gIVCZezCh3qowccEAQYAiABEgK-DvD_BwE

[38] Vedi

[39] https://cointelegraph.com/news/blockstreams-adam-back-slams-ethereum-as-a-ponzi-scheme

[40] Essendo ogni blocco Mintlayer legato a un blocco Bitcon, un reorg su Bitcoin provoca un reorg anche su Mintlayer, perciò un atomic swap inter-chain fra Bitcoin e Mintlayer è sicuro anche in caso di chain reorganization. Inoltre, il fullnode Mintlayer funziona in accoppiata con Bitcoin Core e aggiunge a quest’ultimo un modulo per l’atomic swap con la catena Mintlayer. Il lightwallet è invece multi-token poiché integra sia BTC che tutti i token creati su Mintlayer.