



Marco Dal Prà (m_dalpra)

BITCOIN, FINE DEGLI IDEALI

24 December 2017

Bitcoin con il mese di dicembre ha perso lo scopo per il quale era stato concepito originariamente, cioè entrare in concorrenza con il denaro contante emesso dagli Stati. Sembra impossibile, ma questo software è ormai diventato terreno di investimenti e anche di importi rilevanti. Qualcuno potrebbe incolpare di questo avvenimento i mercati finanziari, ma invece la colpa non è né degli speculatori professionisti né degli investitori dell'ultimo minuto. La colpa è tutta degli sviluppatori del software, dei programmatori del team "Bitcoin Core". **Un vero e proprio autogol.** Soprattutto per i developer che si sentivano come dei supereroi inattaccabili.

Questa non è una notizia definitiva, ma poco ci manca. Qualcuno ha sottovalutato la velocità di azione che hanno i mercati. O meglio ha semplicemente trascurato l'azione umana.

Ma vediamo cosa è successo.

Dicembre 2017

Mettiamo subito le mani avanti : qui non si parla delle vicissitudini finanziarie delle criptovalute. L'andamento altalenante delle "monete matematiche" riempie già a sufficienza giornali, blog e siti specializzati; inoltre nel grafico storico di bitcoin contro dollaro dal 2009 a oggi sono già presenti sufficienti alti e bassi che gli addetti ai lavori ne possono scrivere più di un libro.

Vorrei invece analizzare un problema tecnico di bitcoin accaduto durante il mese di Dicembre che ritengo fondamentale per il suo futuro : **è l'aumento vertiginoso dei costi delle commissioni**, cioè quanto è necessario pagare per ottenere una transazione; costi che all'inizio della storia valevano quasi nulla, qualche centesimo di dollaro.

Siete pronti a pagare 55\$ per un bonifico o per una "strisciata" con la carta di credito ?

Ecco con bitcoin siamo arrivati a queste cifre, ma anche maggiori.

Vediamo perché.



2 birre pagate in Bitcoin : che siano le ultime ?

Democrazia Monetaria

Ricordo che bitcoin funziona come una banca nella quale gli utenti si scambiano denaro virtuale tramite una sorta di "bonifici", soltanto che il database è duplicato su migliaia di PC (nodi), ma senza che uno sia più importante degli altri. Cioè non esiste una autorità centrale che ne coordina il funzionamento.

Il software Bitcoin oggi è in esecuzione **in circa 12.000 PC sparsi in tutto il mondo** ([QUI TROVATE LA MAPPA](#)), ognuno dei quali conserva anche una copia della Blockchain, ossia il database di tutte le transazioni, che essendo organizzato per blocchi, assomiglia ad un registro contabile, dove ogni blocco rappresenta virtualmente una pagina.

Si dice anche che bitcoin usa la tecnologia del registro distribuito (DLT).

Ebbene, con questa architettura ogni eventuale aggiornamento del software **deve trovare d'accordo tutti**, altrimenti si creerebbe una scissione con due monete "diverse" : quella dei nodi con il software vecchio e quella dei nodi con il software nuovo. Monete che andrebbero ognuna per la sua strada.

Questo episodio, **che nel gergo si chiama FORK**, cioè biforcazione, è alla base di un problema che io chiamo "democrazia monetaria", un qualcosa che gli esperti di Diritto non avevano mai affrontato prima di bitcoin.

Un problema trascurabile sulla criptovaluta Ethereum, perché c'è un leader (il giovanissimo Vitalik Buterin) che con il suo team decide quale evoluzione dare alla moneta. Come accade anche in altre valute come Zcash o Stellar.

Invece, Satoshi Nakamoto, lo sconosciuto ideatore di bitcoin, **è scomparso nel nulla** lasciando la nave senza capitano. Le decisioni vengono quindi prese a maggioranza cercando di ottenere almeno un 80% del consenso (dei nodi), proprio per evitare il sopra citato FORK.

E, data la natura umana, questo risultato "elettorale" **è molto difficile da raggiungere.**

Stato di Fatto

Attualmente l'ultima release di bitcoin, detta "**Bitcoin Core**", è la [versione 0.15.1](#).

Se volete i sorgenti, sono nel repository mondiale dei software Open Source : Github.com ([LINK QUI](#)).

E' quella che sta funzionando in questo momento nei nodi, i quali procedono raggruppando le transazioni, cioè i pagamenti, in blocchi che vengono "validati" ogni 10 minuti.

Un blocco, come si diceva poco fa, è assimilabile ad una pagina di un registro contabile nella quale sono scritte le operazioni con relativo mittente e destinatario. **Soltanto che ogni blocco non può occupare oltre 1 MegaByte.**

Con questo limite, in ogni blocco si riescono a "caricare" mediamente 2000 pagamenti, ma dato che viene emesso un nuovo blocco ogni 10 minuti, significa che bitcoin **può gestire al massimo circa 3 pagamenti al secondo.**

E' un limite che la comunità di sviluppatori ha inserito nel software in tempi remoti, anche se non era stato imposto dall'ideatore nel celebre PDF "Bitcoin: A Peer-to-Peer Electronic Cash System" (LINK QUI <https://bitcoin.org/bitcoin.pdf>).

La Banca è Stretta

Ai primi tempi, cioè dal 2009 e negli anni seguenti, il valore di 3 transazioni al secondo poteva essere anche enorme, visto che funzionava per.... 4 amici al bar, ma se si vuole portare bitcoin ai livelli di una applicazione reale/commerciale, soprattutto tenendo conto che gli utenti bitcoin sono sparsi su tutto il pianeta, quindi sono potenzialmente milioni, **si tratta di un numero "ridicolo"**.

Tanto per fare un confronto, un circuito di carte di credito come ad esempio VISA o MASTERCARD, può fare oltre **50.000 operazioni al secondo.**

La conseguenza, sempre più evidente dal 2015 in avanti, è che le operazioni attese di essere approvate sono sempre maggiori, causando un "intasamento" della MEMPOOL, la memoria dove appunto i pagamenti impartiti dagli utenti aspettano di essere inserite in un blocco.

Se volete vedere come si riempie la Mempool Bitcoin in tempo reale, guardate [QUESTO LINK](#).

Confronto Serrato

Da qualche anno nella comunità di sviluppatori si sta dibattendo sulle modalità di togliere questo limite, oppure elevarlo, oppure modificare bitcoin in modo da aumentarne le prestazioni per arrivare a quanto necessita il mercato reale.

Per certi versi si deve passare dall'attuale versione, quasi prototipale, ad una versione "industriale"; **è la questione che viene denominata "scaling", cioè potenziamento.**

Purtroppo dopo mesi (o meglio anni) di dibattiti, la comunità non ha trovato ancora un accordo, soprattutto a causa di alcuni irriducibili che per motivi ideologici o economici, votano sempre contro tutte le soluzioni che sono state proposte.

Purtroppo ci sono sviluppatori che ritengono bitcoin intoccabile, come dogma, pertanto formano uno "zoccolo duro" che non si riesce a smuovere. Se non fosse vero potrebbe essere una barzelletta.

Non mi dilungo a raccontare tutta la storia, che altri conoscono meglio di me (vedi ad esempio il blog dell'ottimo Alberto De Luigi), fatto sta che qualcuno si è "scocciato" di tutto questo rimandare ed **ha proseguito per un'altra strada creando delle nuove versioni di bitcoin**, diverse dalla versione originale, detta "core".

Si è cioè verificato il già citato FORK, cioè la scissione tra i nodi che mantengono il database bitcoin, facendo nascere delle vere e proprie nuove criptovalute, come ad esempio : **Bitcoin Cash** (ad Agosto 2017) e **Bitcoin Gold** (a fine ottobre).

Un terzo... è previsto per il 28 Dicembre 2017 (<http://b2x-segwit.io/>) !

Arrivano gli elefanti

Torniamo ora ai giorni nostri, in particolare all'annuncio fatto ai primi di Novembre dell'arrivo alla borsa di Wall Street (anzi, al CME di Chicago) dei **bitcoin futures**, cioè degli strumenti finanziari fatti per "scommettere" sul valore futuro.

Questa notizia ha per certi versi sdoganato le criptovalute nel mondo della finanza reale, scatenando una corsa all'acquisto.

Soltanto che bitcoin e le criptovalute in generale non sono attualmente accessibili attraverso i canali tradizionali; è necessario iscriversi nei portali specializzati che si occupano di acquistare e vendere bitcoin.

Tanto per fare un esempio l'exchange "Coinbase", che ha sede a San Francisco, in Novembre **avrebbe ricevuto oltre 100.000 nuove iscrizioni al giorno** (come riportato da Zero Hedge).

Questo boom di nuovi utenti, oltre ad aver comportato l'aumento del prezzo del bitcoin, ha "intasato" la blockchain di transazioni dovute agli utenti che spostano bitcoin, tipicamente dall'exchange al proprio wallet e viceversa.

Soltanto che la blockchain di bitcoin **era già intasata già questa estate...** figurarsi cos'è successo da novembre.

Il grafico storico del numero di pagamenti in attesa nella Mempool di Bitcoin potete [VEDERLO QUI](#).

Fine della Birra al bar

Con Novembre e Dicembre bitcoin ha visto un crescendo di operazioni tanto da **oltrepassare i 10 Miliardi di dollari movimentati complessivamente al giorno**, un numero stratosferico.

Un numero 100 volte maggiore di quanto avveniva a Gennaio, che dimostra palesemente la presenza di grossi "investitori".

Ma molti di questi non acquistano bitcoin per "parcheggiarli", ma al contrario **per fare speculazione** e arbitraggio, cioè attività di compravendita che richiedono tempi molto rapidi. Rapportata alla Blockchain, questa esigenza si tramuta nella necessità di veder convalidate le transazioni più rapidamente possibile, cioè nel blocco che sta per essere emesso.

Pertanto, cosa fanno questi operatori finanziari per essere sicuri che la propria transazione venga validata prima possibile ?

Pur di saltare la coda, fanno a gara a chi offre di più.

E' come se in banca fosse possibile scegliere quanti soldi pagare per un bonifico. Vedrete che lo speculatore che deve spostare 50.000 Dollari non si fa problemi ad offrirne 100.

In questo modo accade che chi vuole usare bitcoin per pagare la colazione al bar resta tagliato fuori, perché per pagare 5 Euro dovrebbe anche spendere ulteriori 30 Euro di commissioni (o più) per vedere inserita la propria transazione in un blocco.

E' praticamente la fine di bitcoin come strumento di pagamento.

Lo ha sottolineato, in un post su Twitter, anche Erik Voorhees, amministratore delegato di Shapeshift, azienda Svizzera che si occupa dello scambio tra criptovalute, molto nota a livello mondiale.



Erik Voorhees su Twitter

E'un autogol pazzesco che si sono fatti gli sviluppatori "fondamentalisti" che non vogliono sentir parlare di modificare il software Bitcoin Core, l'attuale erede dei quanto aveva proposto Satoshi Nakamoto.

Ora potrà succedere solo una cosa : i piccoli utenti scapperanno verso criptovalute alternative.

Situazione Assurda

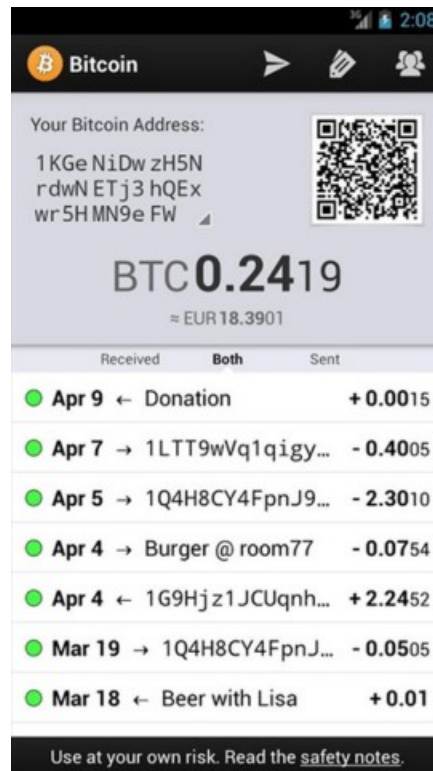
Con l'aumento delle commissioni, si è venuta a creare oggi una situazione assurda.

Succede cioè che **chi ha nel proprio wallet piccole cifre, rischia di non poterle più usare.**

Il motivo è paradossale, ma già oggi un utente potrebbe trovarsi nella condizione in cui la commissione da pagare per spostare i propri bitcoin sia maggiore del valore del pagamento.

Che senso ha avere nella APP del Cellulare cifre come 0,010 bitcoin (150\$) se poi sono necessari 0,011 bitcoin per pagare le commissioni per qualunque movimentazione ?

Nessuna, perchè il wallet non impartisce il pagamento se i fondi non sono sufficienti a coprire anche le spese delle commissioni ! Queste cifre rischiano di finire nel folto cumulo di bitcoin "perduti" o comunque non più movimentati.



bitcoin wallet per smartphone

Ho volutamente fatto un esempio eccessivo, ma già cifre intorno ai 30 dollari oggi non sono utilizzabili. Quindi cosa succederà domani se entreranno in questa criptovaluta investitori ancora più grandi di quelli di questi giorni ?

Colpa dei Minatori

Qualcuno sta già accusando i minatori di "avidità", ma è un errore. **Chi lo dice non conosce il funzionamento della blockchain e di bitcoin.**

I minatori sono coloro che vidimano i blocchi mediante calcoli matematici, operazione per la quale sono richieste risorse hardware molto potenti (spesso ne hanno capannoni pieni).

I minatori sicuramente sorridono di tutta questa "beneficenza", ma sono gli utenti ad offrire queste cifre per ciascuna transazione; lo fanno di loro spontanea iniziativa, per assicurarsi il posto.

Per questa situazione i minatori **non possono che ringraziare l'ottusità degli sviluppatori bitcoin core**, che hanno creato un sistema troppo stretto.

Non è altro che la legge della domanda e dell'offerta : i blocchi sono rari e tutti si affannano a chi offre di più.

Altre iniziative in forse

Purtroppo i problemi non finiscono qui.

Ricordo infatti che il database di bitcoin (la Blockchain) non è utilizzato solo per effettuare pagamenti ma anche per offrire svariati servizi. Ad esempio per tenere traccia indelebile della fornitura di prodotti, oppure per offrire ai cittadini una carta di identità digitale con la gestione dei dati personali. Oppure per tenere traccia dei diritti d'autore su un brano musicale (è un progetto di Spotify), ecc...

Questi servizi, se prima costavano 10 centesimi di dollaro a transazione, oggi hanno costi molto più impegnativi se non anche proibitivi. Le software house dovranno quindi scegliere tra aspettare una revisione del software bitcoin, ad esempio Segwit2x annunciato durante una conferenza a New York la primavera scorsa ma mai attuato, **oppure passare a soluzioni più radicali**, come ad esempio migrare i loro software su altre piattaforme, come Bitcoin Cash, Litecoin o Ethereum.

Con lo svantaggio che talvolta le altre criptovalute utilizzano linguaggi di programmazione diversi. Come avete capito è un bel caos. Altro che i poteri forti che manovrano bitcoin; **qui si paga lo scotto di aver voluto usare su scala "industriale" un software che nei fatti è ancora in stato prototipale.**

Cosa succederà domani ?

La sfera di cristallo ancora non la abbiamo, quindi provo a presentare qualche scenario su quali possibili pieghe potrebbe prendere la vicenda.

Primo Scenario : Nuova Release del Software

La prima soluzione al problema dei blocchi intasati e dei costi alti delle commissioni (**nel gergo, fee**), è che il team di sviluppo "bitcoin core" pubblichi rapidamente una nuova release del software, aumentando il quantitativo di operazioni processabili da Bitcoin, portandole ad esempio da 3 a 10-15 al secondo.

Un numero sufficiente per guadagnare qualche mese per poi attuare soluzioni strutturali di maggior portata.

Si scarica la MEMPOOL dell'attuale sovraccarico e scendono i costi delle transazioni. Ma per quanto ? Per sostenere le operazioni che arrivano nella Blockchain dal mondo "reale" bisogna infatti **quantomeno centuplicare** le attuali 3 operazioni al secondo, con soluzioni tecnologiche molto più impegnative, sia a livello computazionale che a livello di traffico.

Una soluzione esiste ed è in corso di test, si chiama Bitcoin Lightning Network, ma non sembra molto accettata da tutta la comunità, nè di utenti nè di sviluppatori, soprattutto per la presenza ingombrante della software house Blockstream, che stride con il concetto Open Source di Bitcoin. Ricordo comunque che l'aggiornamento del software, come detto prima, **richiede un largo consenso** (prima tra gli sviluppatori e poi della maggioranza dei nodi). Cosa che fino a ieri non è mai stata raggiunta.

Consenso che per il quale ci potrebbero volere 2-3 mesi, **un tempo che i piccoli utenti non possono permettersi di aspettare.**

In poche parole questo scenario non è impossibile ma ha una strada molto impervia. Aggiungo infine una considerazione: non ho sentito nessuna benché minima "voce di corridoio" che segnali accordi tra le parti per un qualsiasi tipo di scaling.

Potrei anche sbagliare, ma con questi elementi **vedo il primo scenario piuttosto improbabile.**

Secondo Scenario : Bitcoin spazio per Grandi Capitali

La seconda ipotesi, che ritengo più probabile, è **che dal punto di vista tecnico non succeda "nulla"** (quantomeno in tempi brevi).

Significa che continuerà quanto sta succedendo ora, ossia avremo la blockchain intasata.

E significa che bitcoin "core" continuerà ad essere usato anche dai mercati finanziari, come è successo da Novembre **Solamente che, per fare posto all'entrata delle balene, i pesci piccoli dovranno uscire.**

Ossia, visto il costo elevato delle transazioni in bitcoin, i piccoli utenti tenderanno a spostarsi verso altre criptovalute meno costose e magari anche più veloci, come ad esempio Bitcoin Cash, Ethereum, Litecoin ed altre.

Naturalmente questa è la mia opinione, che può anche essere sbagliata.

Ma è suffragata dai grafici delle operazioni giornaliere che avvengono su queste piattaforme : **ad esempio Ethereum ne registra 1 milione**, contro bitcoin che è fermo a 300.000 (appunto il limite massimo).

Conclusione

Per i fondamentalisti bitcoin gli avvenimenti di dicembre sono la fine del dogma intoccabile. Il loro sogno doveva sostituire i contanti, invece sta diventando uno strumento finanziario.

Un sogno che sta diventando un incubo: bitcoin, software nato per contestare le banche... sta diventando uno strumento che potrebbe restare ad uso esclusivo dei grandi player della finanza mondiale !

Per fortuna che il mondo open source delle criptovalute è **attivo e reattivo.**

Molti infatti stanno già raccogliendo l'eredità, **Ethereum e Bitcoin Cash** primi tra tutti, ma altri stanno seguendo.

Basta dare un'occhiata a [COINMARKETCAP](#) per rendersene conto.

Bitcoin Core era il software deputato a rappresentare l'idea di Satoshi Nakamoto di una valuta elettronica decentralizzata sostitutiva del denaro contante, ma questo ruolo sta passando ad altri.

E a meno di improbabili colpi di scena, succederà piuttosto rapidamente.

Link Utili

In questo [LINK](#) potete vedere l'aumento del costo delle transazioni.

La storia di Bitcoin nel blog di [ALBERTO DE LUIGI](#)

Bitcoin's Average Transaction fee Surpasses \$50 as Network Issues Remain

<http://www.newsbtc.com/2017/12/22/bitcoins-average-transaction-fee-surpasses-50-network-issues-remain/>

ZeroHedge - Coinbase

<http://www.zerohedge.com/news/2017-11-02/coinbase-adds-record-100000-bitcoin-traders-one-day>

Il grafico storico della MEMPOOL [IN QUESTO LINK](#).

Estratto da "http://www.electroyou.it/mediawiki/index.php?title=UsersPages:M_dalpra:bitcoin-autogol"