101 cose che non sapevi su Bitcoin

scritto da Alberto De Luigi | 3 Marzo 2019

Ecco una carrellata di curiosità, notizie, informazioni e spiegazioni in comode “pillole”, in ordine sparso, che tutti i bitcoiner dovrebbero sapere, ma che troppo pochi sanno. Se sei un novizio tuffatici, ma anche i più esperti troveranno tante curiosità di cui non erano al corrente!

1. Al picco del prezzo di Bitcoin del dicembre 2017 la potenza di calcolo della rete ammontava a 15 exahashes al secondo. Nonostante la fase di bear market, la potenza computazionale è continuamente cresciuta e oggi tocca i 50 exahashes al secondo. L’investimento dietro la blockchain Bitcoin e che ne garantisce la sicurezza è quindi più che triplicato nonostante la caduta dei prezzi.
2. MtGox contava nel 2014 per il 70% dei volumi di trading globali in cryptovalute. Oggi l’exchange coi volumi più elevati di cambio in dollari è Bitfinex (32% dei volumi

mondiali) seguito da Coinbase (21%) e Bitstamp (18%). In euro è Kraken (50%) seguito da Coinbase (15%) e Bistamp (14%)

3. Al crollo dell'exchange MtGox anche alcuni Core developers possedevano un conto sulla piattaforma e hanno subito perdite ingenti: quasi 1.000 bitcoin da parte di Gregory Maxwell e quasi 500 da parte di Luke Dash jr.
4. Satoshi Nakamoto pubblicò il White Paper di Bitcoin sulla cryptography mailing list il 31 ottobre 2008. Il primo feedback che ricevette fu di James A. Donald il 2 novembre, il quale disse che Bitcoin non può funzionare: "abbiamo davvero, davvero bisogno di questo sistema, ma per come capisco la proposta, non sembra scalare al livello richiesto". Donald aveva ragione, solo anni dopo si inizia a immaginare una reale soluzione di scalabilità, con Lightning Network.
5. Nel 2020 l'halving ridurrà l'offerta giornaliera di bitcoin dimezzandola da 1800 a 900 bitcoin circa. Per quella data saranno stati prodotti l'87% dei bitcoin che verranno mai ad esistenza
6. La prima traduzione del software Bitcoin in una lingua diversa dall'inglese è stata l'italiano. Quando il 27 maggio 2010 Franco Cimatti (con l'utenza "Hostfat") allega sul form bitcointalk le traduzioni in italiano, Satoshi Nakamoto esulta postando in risposta: "Hurray! We have our first language!"
7. Il primo blog in italiano a parlare di Bitcoin è stato probabilmente Il Portico Dipinto (Alessandro Polverini) nell'aprile 2011.
8. Il glossario Bitcoin in italiano più completo si trova qui, su questo blog: http://www.albertodeluigi.com/glossario-bitcoin/
9. Tutte le modifiche del protocollo Bitcoin pianificate e realizzate negli ultimi 4 anni sono state necessarie per adattare il protocollo alla tecnologia Lightning Network: il 14 dicembre 2015 è stato introdotto

checklock time verify; 4 luglio 2016 checksequence verify, il 24 Agosto 2017 segregated witness.

10. Una primissima idea di Lightning Network è stata concepita da Satoshi Nakamoto stesso, come testimonia una mail a Mike Hearn, dove addirittura Satoshi presenta un concetto molto simile a checksequence verify (che Satoshi chiama “IsNewerThan”) il quale sarà introdotto su Bitcoin solo col fork del 4 luglio 2016
(vai alla mail di Hearn)
11. Pieter Wuille e Wladimir van Der Laan sono estremamente attivi nello sviluppo di Bitcoin sin dal 2011 e hanno effettuato in 8 anni oltre 2700 contributi (commit) al codice. Per fare un paragone, Satoshi Nakamoto ha scritto circa 2000 righe del codice di Bitcoin Core, Pieter Wuille ne ha scritte dieci volte tante.
12. Dei 20 upgrade o “consensus fork” eseguiti nella storia su Bitcoin, tre sono legati a dei “bug”, riscontrati rispettivamente il 15 agosto 2010, l’11 marzo 2013 e il 17 settembre 2018. Nel caso del 2013, la soluzione al bug è stata in realtà un downgrade, anziché un upgrade.
13. Nell’aprile 2014 è stato implementata una modifica (BIP42) per evitare che, fra circa 256 anni, i miner avebbero potuto produrre più di 21 milioni di bitcoin, aggiungendone altri 21 per i seguenti 256 anni, e così via all’infinito. Essendo questa modifica a tutti gli effetti un soft fork, possiamo contare ben venti consensus fork fatti nella storia di Bitcoin
14. La proposta di upgrade BIP42 del 2014 è scritta con un “tono” molto diverso dal solito. BIP42 evita che l’offerta monetaria di Bitcoin sia effettivamente infinita a cicli di 256 anni. Il responsabile di questa grave svista nel codice scritto in C++ è stato proprio Satoshi Nakamoto (che però nel 2014 non era già più in circolazione da molto tempo). Pieter Wuille, che ha scritto la proposta di BIP42, nel testo ufficiale si prende bonariamente gioco di Satoshi con queste parole: “Come è ben noto, Satoshi è stato un maestro

programmatore, la cui padronanza di C++ era superata soltanto dalla sua conoscenza della cultura giapponese. Il codice qui di seguito […] è scritto in modo da fare accuratamente affidamento su un comportamento indefinito delle specifiche di C++”

15. Prima del 2014 esistevano meno di 4 esemplari di Bitcoin ATM. Nel corso del 2018 sono raddoppiati passando da 2000 a 4000. (https://coinatmradar.com/charts/growth/)
16. Sotto il Bitcoin Relay network di Matt Corallo del 2016, il 90% dei blocchi della blockchain vengono distribuiti nella rete in 570 millisecondi, nel FIBRE network sviluppato da Corallo nel 2018, questi impiegano soltanto 141 millisecondi.
17. l’11 febbraio 2019 c’è stato un blocco orfanato dalla rete. Nel corso del 2018 ci sono stati 6 blocchi orfani. Oggi la frequenza di blocchi orfani è molto diminuita, grazie alla maggiore velocità di relay dei blocchi nella rete Bitcoin, grazie ai progressi tecnici. Un blocco orfano avviene quando due miner scoprono contemporaneamente un nuovo blocco alla stessa altezza (block height) ed entrambi i blocchi iniziano a diffondersi in rete. Uno dei due verrà orfanato nel momento in cui il miner successivo scoprirà il nuovo blocco a partire da soltanto uno dei due precedenti blocchi. Ogni blocco orfano è come un piccolo fork della rete Bitcoin, la cui catena è immediatamente abbandonata.
18. Il 15 agosto 2010 un miner ha sfruttato una falla presente del protocollo per creare bitcoin oltre la quantità prevista. In 5 ore il bug del codice è stato identificato e riparato, quindi i miner “onesti” hanno scaricato il nuovo software e forkato la blockchain, convogliando la potenza di calcolo sulla catena “onesta”. Nell’arco di 3 ore questa ha prevalso ed è stato ripristinato l’ordine. Non c’è notizia di alcun danno economico per nessun utente avvenuto in questa occasione.

19. Il network Bitcoin ha costantemente funzionato senza alcun intoppo per il 99.9833807% del tempo, dalla nascita della blockchain il giorno 3 gennaio 2009 (alle ore 02:54:25 GMT) fino ad oggi
20. L'11 marzo 2013 un bug nel codice presente nel nuovo rilascio di una versione del client Bitcoin Core, già installato da alcuni miners, provocò inavvertitamente un fork dalla catena dei miners che non avevano ancora installato l'upgrade. Il problema è durato 6 ore, finché tutti i miners sono tornati alla versione precedente di Bitcoin Core (downgrade).
21. Si ha notizia di un utente che riuscì, nella finestra di tempo del fork dell'11 marzo 2013, a fare double spending ai danni del servizio Okpay. È l'unico caso noto di double spending effettivamente riuscito della storia di Bitcoin (che sia avvenuto dopo le canoniche 3-6 conferme di attesa), dato che la transazione spesa due volte ai danni di Okpay aveva ben 15 conferme.
22. In origine, il codice sorgente di Bitcoin si trovava su Bitcoin.org. Una volta concordata una modifica, gli sviluppatori inviavano una mail con il codice a Satoshi Nakamoto, Martti Malmi oppure Gavin Andresen, i quali aggiornavano direttamente il codice sorgente. Il processo di revisione del codice di Bitcoin Core è diventato sempre più trasparente, passando prima su SourceForge (dove Martti Malmi creò la repository) e poi, con Gavin Andresen, su Github
23. L'ultimo fork upgrade si è verificato il 17 settembre 2018 per correggere una falla nel protocollo, scoperta il giorno stesso, che avrebbe permesso la crezione di virtualmente infiniti bitcoin. Il bug era presente nel codice da quasi 2 anni, introdotto il 10 novembre 2016 per via di una modifica minore del client che ebbe scarsa revisione del codice.
24. Matt Corallo, lo sviluppatore che scrisse la parte di codice fallata il 10 novembre 2016, è stato lo stesso sviluppatore che ha distribuito la patch risolutiva del

bug il 17 settembre 2018. Chi ha scoperto la falla invece è uno sviluppatore che stava lavorando a Bitcoin Cash. Guido Dassori ha provato poi a sfruttare il bug in testnet, provocando il fork dei nodi non aggiornati e ha scritto questo report in merito. Altre info all'articolo dedicato su questo blog

25. Il 96% dei fullnode della rete Bitcoin sono software Bitcoin Core. Ma chiunque può creare un software alternativo, anche in altri linguaggi di programmazione, compatibile con lo stesso protocollo Bitcoin. Ad oggi ci sono una decina di implementazioni di fullnode diversi.
26. Il codice di Bitcoin Core può essere distribuito, discusso e pubblicato su qualsiasi piattaforma, ma per prassi viene utilizzato Github, oggi di proprietà di Microsoft. A garanzia del fatto che non sia stato introdotto malware nel codice rilasciato su Github, vengono generalmente riconosciute 5 firme digitali con cui sono rilasciate nuove versioni di Bitcoin Core, ciascuna detenuta da uno sviluppatore Bitcoin molto noto e quindi "fidato" nella community
27. I 5 sviluppatori che ora controllano le chiavi digitali con cui è firmato il codice Bitcoin Core sono: Wladimir J. Van Der Laan, Pieter Wuille, Jonas Schnelli, Marco Falke, Samuel Dobson
28. Il "Bitcoin Core maintainer" è Wladimir J. Van Der Laan dal 2011, ruolo prima spettante a Gavin Andresen. A livello pratico, a tale ruolo corrisponde una posizione su Github che permette di dare il commit access ad utenti che possano così mettere direttamente mano al codice sorgente.
29. Nella storia di Bitcoin, pochissime persone hanno goduto degli accessi per modificare il codice sorgente (su bitcoin.org e SoundForge prima, Github poi). Gli unici noti sono: Satoshi Nakamoto, Martti Malmi, Laszlo Hanyecz, Gavin Andresen, Chris Moore, Jeff Garzik, Nils Schneider, Gregory Maxwell; più i cinque che hanno ancora oggi l'accesso ovvero: Wladimir J. van der Laan,

Pieter Wuille, Jonas Schnelli, Marco Falke, Samuel Dobson

30. Nel corso della storia di Bitcoin, oltre 600 persone hanno contribuito a scrivere il codice di Bitcoin Core che oggi utilizziamo (607 contributors su Github)
31. Coloro che non hanno commit access su Github e a cui vengono negate le modifiche alla repository di Bitcoin Core, possono fare forking del codice e creare un software Bitcoin alternativo a Bitcoin Core. Tale software può essere programmato per lavorare sulla catena stessa di Bitcoin (quindi un'implementazione alternativa di nodo Bitcoin che sia compatibile con lo stesso protocollo), oppure creare una catena alternativa, come il fullnode Bitcoin ABC che ha dato il via a Bitcoin Cash
32. Su Github nel 2018 sono stati scritti oltre 26 mila commenti e revisioni (70 al giorno) al codice di Bitcoin Core, sono state inoltrate quasi 1500 richieste di modifica di cui 1300 accettate (merged). Gli sviluppatori che hanno contribuito al codice nel 2018 sono stati 194.
33. Gli sviluppatori pubblicano il codice, ma quale sarà il protocollo vigente è una scelta della community nel suo complesso. SegWit è uno degli upgrade più noti della storia di Bitcoin, proposto dal "Core" team di sviluppatori di Bitcoin Core tramite BIP144 (scritto da Pieter Wuille con Erik Lombrozo). L'upgrade era stato pensato dal team Bitcoin Core con la segnalazione BIP141. Tuttavia, SegWit non è mai stato approvato con BIP141. Non è infatti il team di sviluppo a scegliere quale software upgrade installerà la community e quando lo installerà, bensì è la maggioranza economica a decidere spontaneamente.
34. La segnalazione di upgrade di SegWit è avvenuta tramite BIP91 (presente nel client BTC1, diverso da Bitcoin Core), che forzava la segnalazione di BIP148 (quest'ultimo conosciuto come UASF). Nessuno dei due BIP

è stato integrato in Bitcoin Core, anzi il team principale di sviluppo di Bitcoin Core era contrario ad entrambe le varianti. L'upgrade a SegWit è stato quindi determinato da due client diversi da Bitcoin Core: BTC1 e Bitcoin Core UASF.

35. Quando i valori di Bitfinex erano ancora custoditi, tramite Noble, presso la Bank of New York Mellon (la custodian bank più grande del mondo), i 4 miliardi di dollari "cash" presenti nel suo conto costituivano probabilmente uno degli account in dollari cash (ovvero immediatamente liquidabili) più ricchi del pianeta. Vale la pena ripeterlo: "uno degli account più ricchi del pianeta"
36. Tether è l'unica stable coin realmente utilizzata (98% dei volumi di tutte le stable coin). Contrariamente a quanto dicono i detrattori, non ha mai dato segnali di non essere realmente garantito da 1 dollaro per ogni tether esistente. Anzi, nel solo mese di ottobre 2018 c'è stata una conversione massiccia di tether, per cui sono stati prelevati oltre 1 miliardo di dollari (distruggendo i rispettivi tether). Tale prelievo è stato fronteggiato da Bitfinex senza battere ciglio.
37. Le banche, super-regolamentate, sorvegliate e talvolta nazionalizzate, non sono in grado di far fronte a prelievi un po' più consistenti dell'ordinario senza ricorrere ad aiuti statali (pagati dai contribuenti), per via del meccanismo della riserva frazionaria. È probabile che nessuna banca tradizionale al mondo di deposito e investimento possa sostenere un prelievo di 1 miliardo di dollari senza fallire (escluse le custodian bank, istituti esistenti negli USA). Alla prova dei fatti, l'exchange Bitfinex si è rivelato sorprendentemente uno degli istituti finanziari più solidi al mondo.
38. Secondo una ricerca di CipherTrace, tramite tutte le cryptovalute ci sarebbe stato un riciclaggio, dal 2009 ad oggi (in 10 anni), di 2.5 miliardi di dollari. Si

stima che le banche europee riciclino denaro per una quantità pari all'1% del PIL europeo all'anno, quindi circa 140 miliardi di dollari ogni anno.

39. La quantità di valore spostato sul layer di base di Bitcoin, ovvero la blockchain (senza considerare Bitcoin transati su layer secondari o servizi fiduciari), ha superato di gran lunga Paypal e si sta avvicinando all'ordine di grandezza dei volumi di Mastercard e Visa (circa un decimo di Visa).
40. Nonostante il bear market, nel corso del 2018 il valore delle transazioni Bitcoin su blockchain è aumentato del 30% rispetto al 2017, da mille miliardi di dollari (1T $) a mille e trecento miliardi di dollari (1.3 T). Visa muove circa 10 mila miliardi di dollari l'anno (10 T $).
41. Una transazione Bitcoin può essere "bruciata" rendendo il suo output non più spendibile. Si consuma così una minuscola frazione di Bitcoin, ma è possibile in questo modo scrivere dei dati a piacere all'interno della blockchain (OP_RETURN).
42. Tether funziona su blockchain bitcoin tramite l'omni-protocol che sfrutta l'OP_RETURN. Nel 2018 il numero di output OP_RETURN su blockchain è aumentato da 4 milioni a 10 milioni, il 53% di questi è fatto con l'omni layer protocol (Tether).
43. Tramite Tether oltre 200 milioni di dollari vengono trasferiti ogni giorno sulla blockchain Bitcoin (in proiezione, 70 miliardi di dollari l'anno) (blockspur data)
44. Se, per ipotesi, tutte le transazioni della storia di Bitcoin fossero state moderne confidential transactions (garantendo maggiore garanzia di anonimato), oggi la blockchain di Bitcoin peserebbe 650gb. Il maggior peso è uno dei motivi principali per cui non è stato proposto un upgrade del protocollo Bitcoin che permetta tali transazioni. Anche con bulletproof (implementato poi su Monero) il peso è elevato e la blockchain quindi meno efficiente rispetto all'attuale standard

45. Mimble Wimble è un protocollo rivoluzionario che permette di fare confidential transactions (quindi transazione completamente anonime) senza aumentare il peso della blockchain, anzi diminuendolo
46. Grin, nuova cryptovaluta che implementa Mimble Wimble, permette di fare transazioni tre volte meno costose (in termini di spazio) rispetto a quelle di Bitcoin, pur aggiungendo maggiore privacy alle transazioni. Se ci fosse un volume di transazoini su Grin pari a quello presente su Bitcoin (e sullo stesso arco temporale di 10 anni), la blockchain di Grin peserebbe circa 70gb contro i 200gb di Bitcoin.
47. Grin è pensata da sviluppatori del mondo Bitcoin per studiare e testare al meglio Mimble Wimble, ma eventualmente anche per costituire una sidechain di Bitcoin e, forse in futuro, utilizzarla direttamente con Bitcoin tramite un "extension block" fork. Grin soltanto non può costituire una soluzione di scalabilità definitiva, poiché una cryptovaluta, per essere veramente scalabile, deve poter permettere "migliaia o milioni di transazioni in più" rispetto all'attuale Bitcoin onchain, a parità di spazio occupato, e non soltanto "il triplo in più" come Grin. È quindi necessaria una soluzione offchain come Lightning Network (oggi non implementabile sulla blockchain di Grin)
48. I volumi giornalieri di trading in Bitcoin si aggirano negli ultimi mesi intorno ai 5-10 miliardi di dollari e da oltre un anno non scendono sotto i 3 miliardi, valore toccato per la prima volta nel novembre 2017, quando il prezzo di Bitcoin ebbe un'impennata a 7000 dollari arrivando poi, nel corso del mese successivo, a 19 mila. Facendo un paragone, i valori medi del volume di trading precedenti sono praticamente inesistenti. A inizio 2017 i volumi si attestavano sui 100 milioni giornalieri, quindi 100 volte più bassi di oggi, eppure il prezzo di Bitcoin era già solo un quarto di quello attuale.
49. Quando un fullnode Bitcoin si connette a internet, deve

trovare degli altri nodi della rete peer-to-peer di Bitcoin per partecipare alla rete, inviare e ricevere transazioni, fare download e relay dei blocchi della blockchain. Per iniziare è quindi necessario conoscere almeno l'indirizzo IP di un nodo qualsiasi. Salvo che non ci connettiamo manualmente a un indirizzo di nostra conoscenza, Bitcoin Core si connetterà a uno dei seguenti server che provvederanno a fornire una lista di indirizzi. Sono server mantenuti da alcuni dei più famosi sviluppatori di Bitcoin Core:

- bitcoin.sipa.be (Pieter Wuille)
- bluematt.me (Matt Corallo)
- bitcoin.dashjr.org (Luke Dash Junior)
- bitcoin.jonasschnelli.ch (Jonas Schnelli)
- btc.petertodd.org (Peter Todd)
- bitcoinstats.com

50. In italia ci sono numerosi negozi e punti fisici in cui personale dedicato può insegnarvi i primi passi nell'acquisto delle cryptovalute, e per prestare un aiuto agli utenti novizi per orientarsi in questo mondo. Ad esempio c'è lo store di Coin Society a Milano in via del Torchio 10, oppure Cripton in viale Piacenza 39 a Parma, o Bitcoinyou in via Conchiglia 103 a Civitanova Marche. Oltre che, ovviamente, la Bitcoin valley di Rovereto, nata grazie all'assidua attività di Inbitcoin sin dal giugno 2016
51. L'attuale sistema monetario in moneta fiat non è in grado di garantire transazioni elettroniche/digitali non reversibili per servizi non reversibili. Per fare un esempio: se mangio la pizza, non posso restituirla (se non già parzialmente digerita dai miei enzimi), perciò il servizio prestato dal pizzaiolo non è reversibile, ma il pagamento effettuato in carta di credito è reversibile. Questa "asimmetria" può divenire causa di truffe ed elevati costi di gestione. Negli USA le frodi con carta di credito hanno rappresentato un costo di quasi 17 miliardi solo nel 2018. Bitcoin è anche una

soluzione tecnologica a questo problema

52. Una normale transazione Bitcoin non è reversibile, ma se i due contraenti dovessero avere bisogno di reversibilità, possono utilizzare un servizio escrow. Per un servizio simile non è necessario conoscere le informazioni personali della controparte (come nome e cognome, indirizzo, dati bancari etc.), cosa che invece è sempre necessaria per le transazioni elettroniche in moneta fiat
53. Questa transazione è la più grande della storia in quanto a numero di bitcoin trasferiti, ben 550 mila: vedi la transazione su blockchair
54. Lightning Network permette, per la prima volta nella storia della civiltà umana, di effettuare convenientemente microtransazioni, grazie all'abbattimento dei costi per movimentare minuscole quantità di valore. Nuovi modelli di business, ma anche di sicurezza informatica, possono essere costruiti su questo nuovo sistema. Ad esempio, si possono sostituire gli anti-spam che richiedono potenza computazionale per superare un filtro (proof-of-work), con sistemi in cui viene effettuata una micro-transazione di acconto, trattenuta solo se l'utente si rivela malevolo (spammer, ddos attack etc.)
55. Coinbase è probabilmente l'exchange che custodisce più bitcoin al mondo, controllando vari wallets che contano, in totale, 856 mila Bitcoin (è questo l'ammontare di una somma mossa fra il 1 e il 6 dicembre 2018 molto probabilmente riferibile a Coinbase – fonte).
56. Sono noti due wallet dell'exchange Binance la cui somma ammonta a 190 mila bitcoin. Bitfinex e Bittrex hanno wallet rispettivamente cold wallet per 120 e 130 mila bitcoin ciascuno. È estremamente raro che wallet di singoli individui contino più di mille bitcoin (vi sono ad oggi solo 1886 indirizzi che conservano più di 1000 Bitcoin)
57. Bitwala è il primo servizio che permette di mantenere un

conto in moneta fiat garantito dalla Bundesbank fino a 100 mila euro e, al contempo, a fornire un webwallet da e verso cui si possono trasferire liberamente bitcoin, o spenderli tramite la carta di debito associata al conto

58. Molte blockchain sono insicure e a rischio attacco 50+1. Alcune delle più famose che hanno subito un attacco di successo sono state Verge ed Ethereum Classic. Attaccare una blockchain non è una questione di hacking informatico, ma solo di potenza computazionale, ovvero di quanto un attaccante è in grado di investire economicamente nell'attacco, tenendo ovviamente conto del profitto atteso da tale attacco e della probabilità di successo
59. Un attaccante ben organizzato che intende effettuare un 50+1 su una blockchain si assicurerà probabilmente anche la connivenza di un exchange. Infatti gli exchange hanno sistemi di alert e non autorizzano facilmente prelievi di somme ingenti, per cui un attaccante potrebbe spendere molto in potenza computazionale senza tuttavia riuscire a ottenere double spending remunerativi. Non si può escludere che Gate.io fosse in qualche modo coinvolto nell'attacco a Ethereum Classic, poiché la famosa "somma restituita" il 10 gennaio 2019 per cui si parla di "white hacking" è piuttosto sospetta. Chissà che non si trattasse invece di una "mazzetta".
60. Fidarsi troppo degli exchange non è mai buona cosa, specialmente se sono piccoli e poco noti. QuadrigaCX è fallito poiché aveva livelli di sicurezza inesistenti, dato che le chiavi del cold wallet erano in mano ad un'unica persona (deceduta), senza alcun meccanismo di multifirma né sblocco tramite locktime (o altri smart contracts) che exchange più strutturati implementano per assicurarsi al contempo la sicurezza e l'accesso ai propri wallet.
61. Oltre all'utilizzo come scambio di valore (ad es. bitcoin) la tecnologia blockchain non serve "quasi" a niente ed è un errore il fatto di pensare che possa

essere utile a molte strutture di business già esistenti. Tuttavia, un utilizzo della blockchain che è rivoluzionario rispetto ai sistemi pre-esistenti è il timestamping decentralizzato, che può sostituire completamente i principali servizi notarili. Opentimestamp è il fiore all'occhiello di questi sistemi.

62. Un team italiano ha sviluppato dei videogiochi che sfruttano Lightning Network: ad esempio Super Mario Bro https://satoshis.games/, dove ogni coin che raccogliete in gioco è un satoshi che vi viene inviato tramite Lightning Network. Si può giocare anche gratis, ma se perdete la vita, perderete anche i satoshi raccolti. Acquistando più vite invece, i satoshi saranno ancora disponibili sino ad esaurimento delle vite rimanenti.
63. Il batching è l'aggregazione di transazioni richieste dagli utenti in un'unica transazione. È uno strumento molto potente poiché permette di risparmiare tantissimo spazio sulla blockchain. Questa è una transazione unica con ben 13.007 outputs (13 mila) e pesa 445 kilobytes
    vedi la transazione su blockchair
    Questa transazione ha 19.900 input e pesa 840 kilobytes
    vedi la transazione su blockchair
64. In questo momento (marzo 2019) vi sono meno di 2000 indirizzi/wallet con oltre 1.000 bitcoin ciascuno. Per lo più sono tutti indirizzi di grandi exchange. Vi sono più di cento indirizzi che contengono esattamente 8000 e 5000 bitcoin e sembra che molti di questi siano sotto il controllo di Coinbase
65. Il più antico exchange Bitcoin ancora operativo è l'exchange italiano The Rock Trading, sul mercato dal giugno 2011
66. Lo sviluppo di Lightning Network ha visto da vicino l'impegno di varie società che hanno iniziato in maniera indipendente lo sviluppo di nodi e wallet LN. Fra queste: Lightning Labs, Blockstream, Acinq, Bitfury, Amikopay, Blockchain Luxembourg S.A

La necessità di rendere possibile l’interoperabilità fra le varie implementazioni sviluppate dalla community ha portato alla stesura di un protocollo condiviso, il BOLT (Basis of Lightning Technology). Il primo meeting fra queste aziende per la condivisione del protocollo è stato organizzato da BHB Network di Giacomo Zucco a Milano, tant’è che inizialmente BOLT era informalmente chiamato “Milan protocol” Vai al protocollo

67. La società italiana di Thomas Bertani “Oraclize”, fondata nel 2015, è la prima società italiana (la seconda in Europa) con capitale sociale conferito in Bitcoin. Vedi

101. Il mondo delle cryptovalute è pieno di scammer e ogni minuto almeno una persona viene truffata. Non so se il conto è davvero di una al minuto, ma quel che è certo è che abbiamo una vittima qui e ora. Questa lista infatti non contiene 101 curiosità come riportava il titolo, ma poco più della metà. Scam! Maledetto De Luigi e i suoi click-bait!

~~Ti è piaciuta la lista? Fammi sapere quale punto hai preferito nei commenti! E ricorda, puoi essere estratto per vincere 0.1 bitcoin se condividi l’articolo sui social!~~

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