n. 0

Digital Gold Institute

Scarcity in the Digital Realm

Report Trimestrale

2019-Q1

Editoriale

Quello che avete tra le mani (o più probabilmente sul vostro schermo) è il numero zero nella serie dei report trimestrali prodotti dal Digital Gold Institute. L'intenzione è offrire uno sguardo, ampio come copertura e interessante nei giudizi, su cosa è accaduto nel mondo Bitcoin, cryptoasset e tecnologia blockchain.


THE TIMES

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

99p


THE TIMES

Romps, royals and lesbians

Costume drama tipped for Oscars glory

Would you drink wine from a can?

Universities face credit crunch as debt spirals

Police failed women sent to Somalia for 'marriage'

Thanks, Satoshi. We owe you one.

Happy 10th birthday, Bitcoin.

L'evento principale del primo trimestre 2019 non può che essere il lancio del nostro Istituto… ehm... no… :-) il "compleanno" di Bitcoin, che ha compiuto 10 anni il 3 gennaio. È stato divertente trovare *"Happy 10th birthday, Bitcoin"* proprio sulla copertina del Times, il cui titolo dieci anni fa era stato inserito da Satoshi Nakamoto nel primo blocco della blockchain; con la scelta del titolo ("*Il Cancelliere dello Scacchiere è sull'orlo del secondo piano di salvataggio per le banche*") Nakamoto manifestava una chiara consapevolezza del momento di crisi finanziaria e qualificava implicitamente Bitcoin come risposta alla crisi; dieci anni dopo i pareri se quella crisi sia stata risolta sono discordanti: tra *quantitative easing* e tassi di interesse negativi c'è chi teme che il peggio non sia davvero alle spalle. E cresce il numero di persone nel mondo che guardano a Bitcoin come possibile equivalente digitale dell'oro, *asset* di riserva sovranazionale ed incensurabile per una economia digitale e globale.

Vale la pena apprezzare anche la valenza tecnica della scelta di Nakamoto di utilizzare un titolo di giornale per marcare temporalmente la creazione del primo blocco: l'inventore di Bitcoin dimostra di non aver creato alcun blocco prima di quella data, di non essersi quindi riservato una quota di Bitcoin a titolo di privilegio (nella forma di blocchi creati prima del lancio pubblico, o *preminati* come si dice in gergo tecnico).

In questi dieci anni Bitcoin è andato da zero a quattromila dollari, ma il compleanno non ha rappresentato una giornata celebrativa dal punto di vista delle quotazioni di mercato, arrivando pochi giorni dopo il minimo di $3271 (16 dicembre 2018) che concludeva un crollo dei prezzi del 74% iniziato un anno prima quando Bitcoin era ai massimi di sempre ($19200 il 17 dicembre 2017).

Bitcoin ci aveva già abituato in passato ad impressionanti *drawdown*: il -84.67% nel periodo 2013-2016 e soprattutto il -93.46% del 2011; la sua resilienza si è però confermata anche nel primo trimestre 2019 che ha visto un notevole recupero del +10,91%. Peraltro, una delle migliori metriche per valutare la crescita di Bitcoin è la serie dei minimi per anno, in crescita sostanzialmente continua ed esponenziale (si veda figura 1).

Il raffreddarsi dell'euforia sul mercato ha paradossalmente favorito nel 2018 l'attenzione ai processi di sviluppo tecnologico piuttosto che alle dinamiche di

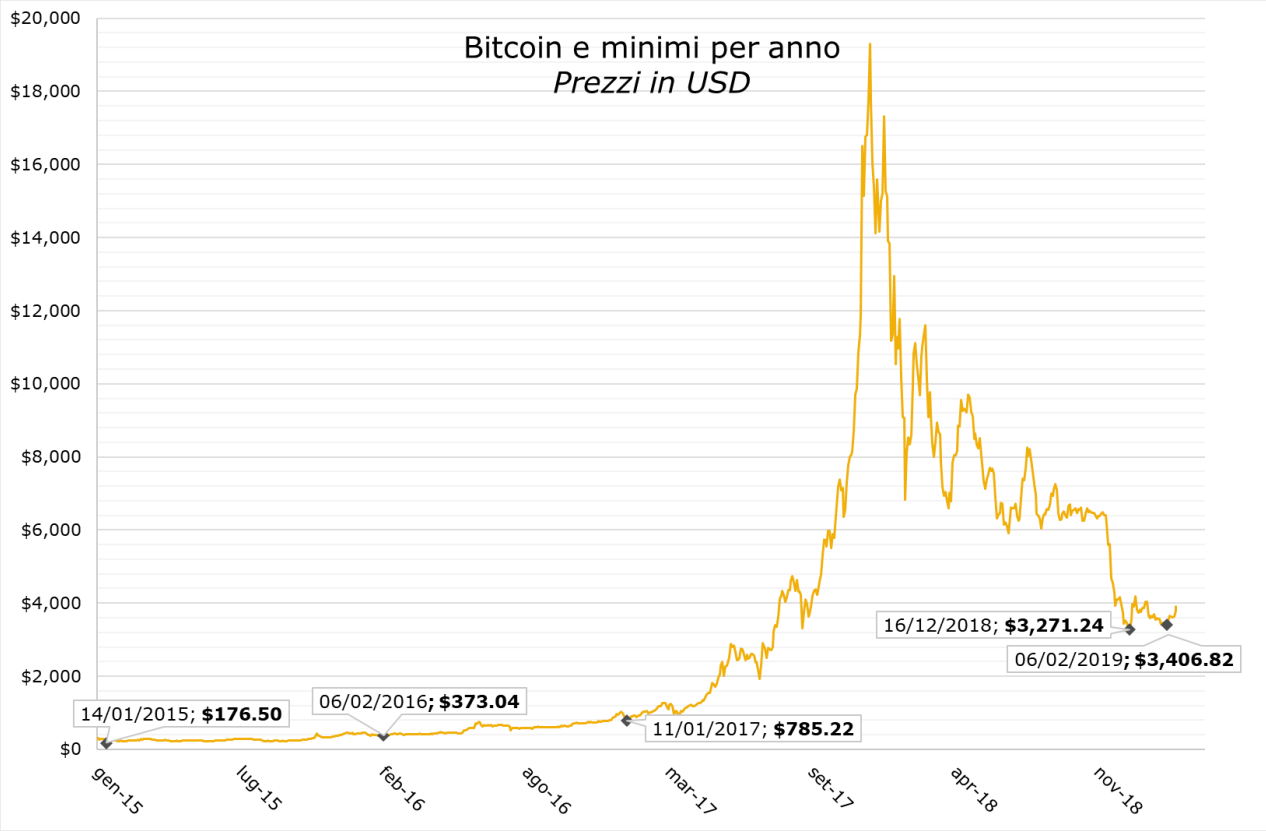
Anno	Prezzo Minimo
2011	$0.30
2012	$4.33
2013	$13.40
2014	$314.45
2015	$176.50
2016	$373.04
2017	$785.22
2018	$3,271.24
2019	$3,406.82

Figura 1: Prezzo minimo Bitcoin per anno

prezzo: i regolatori hanno avuto il tempo di metabolizzare alcuni degli aspetti più innovativi e dirompenti, l'ecosistema si è in generale rafforzato e consolidato. Il primo trimestre 2019 ne ha raccolto molti frutti ed ha visto al tempo stesso anche una significativa ripresa dei corsi.

Questi temi verranno approfonditi nel seguito del report che è diviso nelle sezioni mercato, tecnologia, regolamentazione ed ecosistema, che rappresentano le nostre chiavi di lettura privilegiate.

Ogni riscontro su questo report è molto gradito essendo pensato e scritto per voi: partner, sostenitori e collaboratori dell'Istituto; l'intenzione è di renderlo sempre più utile a voi e per questo i suggerimenti sono indispensabili, così come richieste di approfondimento ulteriore.



Indice

1. Mercato

Performance Bitcoin

Abbiamo già commentato nell'editoriale la performance di questo primo trimestre; vale la pena sottolineare che è la migliore da fine 2017[1].

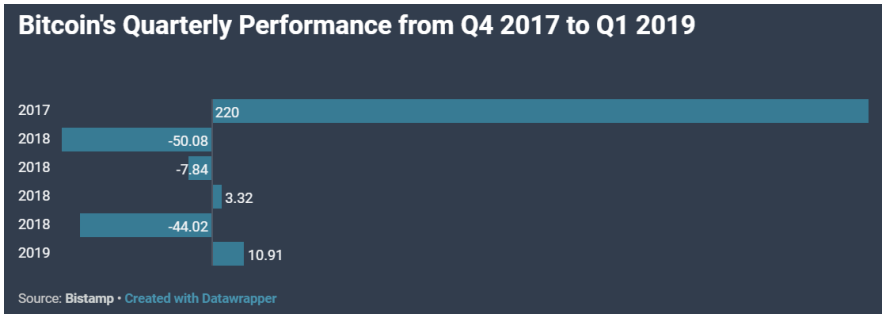


Figura 2: Performance trimestrali di Bitcoin, fonte Coindesk

ETF e report Bitwise

Ha fatto molto rumore il report che BitWise[2] ha presentato alla SEC per proporre il suo ETF Bitcoin: l'attenzione mediatica è fondata perché l'analisi è eccellente per qualità e ampiezza. In particolare, spiccano alcune osservazioni contenute nel report: *in primis*, quella sulla liquidità del mercato. BitWise mostra come, sebbene la maggioranza degli *exchange* dichiarino volumi che si dimostrano fittizi ad una analisi rigorosa, anche solo considerando gli *exchange* affidabili emergono volumi scambiati assolutamente appropriati alla capitalizzazione di Bitcoin. Ad esempio, in figura 3 è rappresentato il confronto con l'oro.

Questa osservazione è rilevante perché la SEC ha bocciato a settembre scorso proposte per ETF Bitcoin con due motivazioni, la prima delle quali afferma che il mercato non sarebbe abbastanza liquido per fissare un prezzo di riferimento affidabile per Bitcoin. CFTC, l'autorità finanziaria americana competente sui mercati futures, ha invece autorizzato i contratti su Bitcoin e questi fissano ogni giorno un prezzo di riferimento: difficile capire come lo stesso mercato possa essere ritenuto affidabile per i futures e non affidabile per un ETF. La seconda motivazione usata dalla SEC per fermare gli ETF è invece più fondata e concerne la mancanza di *custodian* affidabili e regolamentati. Anche su questo secondo punto le risposte di Bitwise sono interessanti, ma l'argomento meriterà un successivo approfondimento, magari già nel nostro prossimo report trimestrale.

Futures su Bitcoin

L'altra notizia rilevante è lo stop alle contrattazioni dei contratti futures Bitcoin su CBOE: non si tratta di un annuncio particolarmente sorprendente o negativo, ma la naturale conseguenza del fatto che i futures scambiati sulla piazza rivale CME raccolgono volumi maggiori ($85M contro $6M) e le negoziazioni si stanno quindi consolidando presso CME. Il tutto avviene mentre il mercato attende anche il debutto del nuovo contratto futures promesso da Bakkt (ICE, New York Stock Exchange) rallentato finora certamente dallo *shutdown* dell'amministrazione americana, ma anche dall'atteggiamento di alcuni regolatori che ancora sperano di poter fermare il fenomeno Bitcoin. Non dimentichiamo infatti che la maggioranza degli operatori globali (con l'eccezione della sola Goldman Sachs) boicottano pubblicamente l'operatività sui futures, evitando di offrirla ai propri clienti. Nonostante questo, le contrattazioni sul mercato *futures* sono significative,

	Capitalizzazione	Volume Scambi Spot	Turnover Giornaliero
Gold	~$6.7T	$37B	0.55%
Bitcoin	~$70B	$250M	0.39%

Figura 3: Bitcoin e oro a confronto

[1] https://www.coindesk.com/bitcoin-price-posts-biggest-quarterly-gain-since-late-2017

[2] https://www.sec.gov/comments/sr-nysearca-2019-01/srny-searca201901-5164833-183434.pdf

comparabili a quelle delle principali borse *spot* con volumi veritieri.

Performance alt-coin

Per concludere l'analisi di mercato del trimestre proponiamo il grafico della performance in Bitcoin delle principali alt-coin: *Ethereum, Ripple, Litecoin, Bitcoin Cash, Stellar, Ethereum Classic, Zcash, Monero*. In figura 4 sono riportati i rendimenti espressi in Bitcoin; quanto avrebbe reso un Bitcoin investito ad inizio periodo in ognuno degli alt-coin considerati.

È qualificante denominare la performance degli alt-coin in Bitcoin, così come si denominano in dollari statunitensi il prezzo dell'oncia d'oro o del barile di petrolio: qualsiasi investimento in cryptoasset che non sia Bitcoin si pone intrinsecamente come alternativo a Bitcoin e su quel metro va misurato.

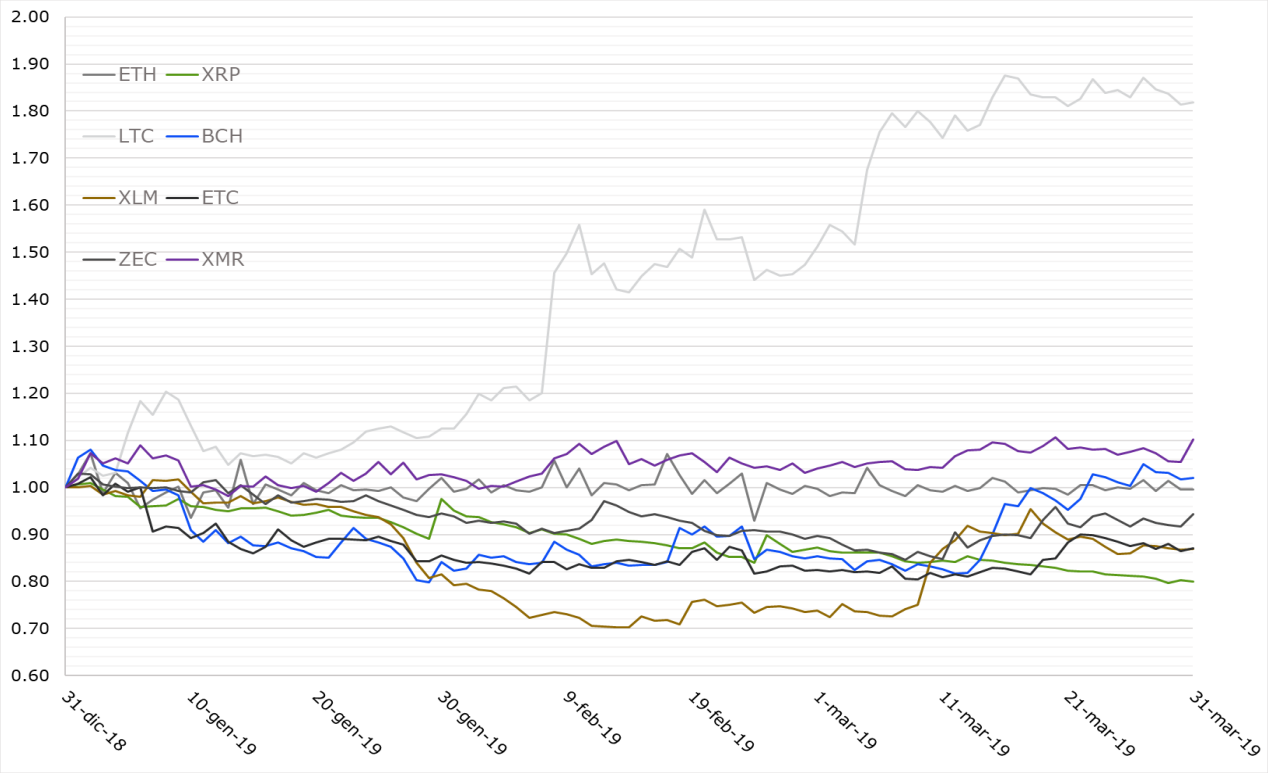


Figura 4: Grafico dei rendimenti degli alt-coin rispetto a Bitcoin

In generale quando il mercato è ribassista Bitcoin perde meno degli alt-coin, mentre in fasi rialziste guadagna meno, con un comportamento tipico da "bene rifugio" in ambito cryptoasset. È interessante notare che invece in questo trimestre rialzista Bitcoin ha fatto meglio della maggior parte dei *peers*, a parte la crescita eccezionale (e difficile da capire) di Litecoin.

Investitori istituzionali

Il principale competitor di Bitcoin, Ethereum, risulta una scelta problematica per gli investitori istituzionali: Fidelity ad esempio osserva che gli upgrade del protocollo tramite *hard fork* (si veda più avanti nella sezione tecnologia) generano incertezza. Questa osservazione si somma alle difficoltà nel gestire un *full-node* Ethereum ed ai problemi che emergono nei tentativi di *custody* (su cui torneremo in futuro). Insomma, Bitcoin resta per ora la scelta principe tra i cryptoasset, l'unico e vero oro digitale.

L'appetito degli investitori istituzionali si è progressivamente raffreddato nel 2018 con la discesa del prezzo Bitcoin, ma resta in realtà significativo e l'impressione è che sotto la cenere stia covando un fuoco pronto a riaccendersi. Una buona indicazione è ad esempio il terzo Crypto Fund lanciato da Pantera, in grado di superare agilmente l'obiettivo dichiarato di

$100M raggiungendo $125M[3]. O ancora, la notizia di due fondi pensione statunitensi che sono diventati *anchor investor* del nuovo *Venture Fund* di Morgan Creek[4]. Sono invece a nostro parere segnali di confusione quelli che emergono dalla quotazione di un ETF Blockchain al London Stock Exchange[5]: è difficile capire quanto la blockchain sia caratterizzante per un fondo che include[6] titoli tecnologici (*SAMSUNG, APPLE, MICROSOFT, AMAZON, ORACLE, IBM, NTT DATA*), semiconduttori (*INTEL, AMD, NVIDIA, QUALCOMM*), telefonici (*VERIZON*), finanziari (*MITSUBISHI UFJ, NOMURA, SBI, SOFTBANK*), materie prime (*ALUMINUM CORPORATION OF CHINA, NIPPON GAS CO LTD, ALCOA*), industriali (*GENERAL MOTORS*), borse di scambio (*CBOE, CME, NASDAQ*) e sistemi di pagamento (*SQUARE*). A parte un paio di nomi tra gli ultimi, per il resto il massimo "contagio blockchain" rilevabile tra le aziende selezionate è qualche sbiadita *press release*.

D'altronde l'*hype* blockchain resta sempre resistente: anche un guru dei mercati come Warren Buffet, da sempre scettico su Bitcoin, sembra credere all'idea di una blockchain come soluzione geniale e dirompente[7].

[3] https://www.coindesk.com/pantera-has-already-raised-125-million-for-its-third-crypto-fund
[4] https://www.coindesk.com/two-public-pensions-anchor-morgan-creeks-new-40-million-venture-fund
[5] https://www.coindesk.com/a-blockchain-etf-is-launching-on-the-london-stock-exchange-today
[6] https://www.solactive.com/ordinary-adjustment-elwood-blockchain-global-equity-index-block-january-2019/
[7] https://www.coindesk.com/warren-buffet-bitcoin-is-a-delusion-but-blockchain-is-ingenious

2. Tecnologia

2.1 Bitcoin

Gli sviluppi crittografici

È estremante rilevante il consolidamento progressivo degli sviluppi crittografici portati avanti dai *core developer* Bitcoin per la standardizzazione dello schema di Schnorr per la firma digitale: da sempre considerato la migliore scelta crittografica (in termini di sicurezza, scalabilità e flessibilità) non era stato considerato da Nakamoto perché coperto fino al 2008 da un brevetto che ne aveva di fatto limitato l'utilizzo ed impedito la standardizzazione. Bitcoin usa, quindi, lo schema ECDSA per la firma digitale, standardizzato in ambito crittografico come sub-ottimale *work-around*. Schnorr permette di verificare un insieme di firme con uno sforzo computazionale che non cresce linearmente col numero di firme[8], risultando quindi efficiente nel verificare contemporaneamente tutte le firme contenute in un blocco; ha una serializzazione compatta in termini di byte, occupando quindi poco spazio nella blockchain che cresce più lentamente rispetto alle firme tradizionali; consente meccanismi di firma congiunta che non richiedono un *setup* interattivo e che appaiono come fossero una singola firma, aumentando quindi la privacy perché non rivelano il numero di soggetti dietro una singola firma; inoltre abilita una serie di sviluppi innovativi come *MAST*, *Taproot* e *Grafroot* che sono molto promettenti per migliorare privacy e fungibilità di Bitcoin.

Al di là degli aspetti strettamente tecnici, sono utili due osservazioni di carattere generale; la prima è che i brevetti in ambito tecnologico, come si è visto in Bitcoin con la mancata adozione di Schnorr a causa proprio di un brevetto, ormai non promuovono più l'innovazione, ma la rallentano, non tutelano i benefici economici dei loro inventori, ma spesso li danneggiano: restano strumenti nelle mani delle *corporation* per azioni aggressive o difensive rispetto ai *competitor*, spesso a danno delle piccole società che devono cedere i loro brevetti sotto la minaccia di costose cause legali da parte di *incumbent*. La seconda osservazione: come nel periodo 1978-2008 la ricerca nell'ambito della teoria della misura trovò nei mercati finanziari e nello sviluppo dei derivati la sua spinta propulsiva, oggi la rinascita

[8] https://blockstream.com/2019/02/18/en-musig-a-new-multisignature-standard/

della ricerca crittografica è innescata da rivoluzione Bitcoin e cryptoasset.

Blockstream cambia marcia: *sidechain*, *block-explorer* e *wallet*

Dopo anni di promesse non proprio mantenute e di aspettative spesso frustrate, Blockstream, una delle principali aziende dell'ecosistema Bitcoin (quella che in passato dava lavoro a molti dei principali sviluppatori Bitcoin), ha avuto una notevole sequenza di rilasci in questo trimestre. Anzitutto Liquid[9], la prima implementazione di quelle sidechain proposte proprio nel paper[10] fondativo della società. Liquid è una blockchain privata, gestita da una federazione di borse di scambio, dove Liquid-Bitcoin (LBTC, garantiti da Bitcoin reali congelati sulla blockchain pubblica) possono essere scambiati in sicurezza e con tempi di conferma dell'ordine del minuto. Inoltre, su Liquid possono essere emessi anche altri asset. L'utente può quindi spostare Liquid-Bitcoin e gli altri asset velocemente tra diverse borse di scambio per effettuare arbitraggi, senza peraltro doversi fidare di una singola borsa perché i suoi cryptoasset potrebbero essergli tolti solo se la maggioranza delle borse nella federazione colludessero ai suoi danni.

Altro rilascio significativo è stato Esplora, un *block-explorer*[11] per la rete Bitcoin (e Liquid); si tratta di una interfaccia web per l'esplorazione di transazioni e blocchi non dissimile in termini di esperienza utente da quanto visto con soluzioni simili in passato. La novità qui è l'estrema efficienza e velocità delle risposte, l'attenzione alla privacy, il supporto dello stato dell'arte del protocollo Bitcoin.

Ciliegina sulla torta, Blockstream ha anche rilasciato la versione aggiornata del *wallet* GreenAddress/GreenBits, nell'occasione semplicemente ribattezzato Green[12]. Il wallet si era caratterizzato negli anni scorsi per essere sempre all'avanguardia rispetto agli sviluppi più avanzati del protocollo Bitcoin. Aveva però accumulato alcuni *legacy deficit* che la nuova versione punta a risolvere riscrivendo l'app completamente e basandola sulla libreria *libwally*[13].

È indubbio che l'accelerazione di questi sviluppi sia strettamente collegata al ruolo sempre più rilevante di Lawrence Nahum, l'italiano autore di GreenAddress, recentemente nominato *Chief Architect* di Blockstream. Nahum[14] ha saputo raccogliere nell'ufficio milanese di Blockstream i migliori talenti italiani, tra cui Riccardo Casatta ed i fratelli Vaccaro (noti per Eternity Wall ed il protocollo OpenTimestamps) ed anche un *alumnus*[15] del Digital Gold Institute: Leonardo Comandini.

La crescita di Lightning Network

Sulla scia del *major upgrade* al protocollo noto come *Segregated Witness* (*SegWit*, accettato dal network nel novembre 2017) il 2018 ha visto nascere *Lightning*

[9] https://blockstream.com/2019/03/11/en-introducing-liquid-core/
[10] https://blockstream.com/sidechains.pdf
[11] https://blockstream.com/2019/02/15/it-blockstream-esplorer-update-nojs-and-more/
[12] https://github.com/ElementsProject/libwally-core
[13] https://github.com/ElementsProject/libwally-core
[14] https://blockstream.com/2018/12/03/en-lawrence-ca/
[15] https://dgi.io/fullTeam/

Network, un *layer* tecnologico di secondo livello che aumenta tramite i suoi *payment channels* la scalabilità del protocollo Bitcoin e che in questo primo trimestre del 2019 è cresciuto enormemente[16]: oltre 4000 nodi, più di 35000 canali di pagamento, per una liquidità complessiva superiore ai 1000 BTC ($4M). Ha fatto notizia la cosiddetta *Lightning Torch*: un pagamento su Lighting Network che è passato come una torcia di mano in mano tra dozzine di partecipanti[17], ognuno dei quali ha incrementato l'importo della torcia[18]. All'iniziativa hanno partecipato anche molti dei personaggi di spicco del mondo Bitcoin, compresi alcuni dei core developer. Si è trattato di una sfida all'onestà (a parte due incidenti rapidamente risolti, nessuno dei partecipanti ha tentato di interrompere la catena) ma anche agli attuali limiti del network[19]: in questa fase sperimentale i nodi allocano solo piccoli importi nei canali di pagamento e questo rende problematico il trasferimento di importi significativi[20].

Altri problemi (ad es. corruzione dei dati in assenza di backup) affliggono la stabilità di Lightning Network che è per ora da considerarsi in beta, ancora lontano dalla produzione, ma gli sviluppatori manifestano ottimismo.

[16] https://bitcoinvisuals.com/lightning
[17] https://www.coindesk.com/bitcoins-lightning-torch-has-blazed-through-37-countries-so-far
[18] https://www.coindesk.com/twitter-ceo-jack-dorsey-becomes-latest-to-take-bitcoins-lightning-torch
[19] https://www.coindesk.com/im-freaking-out-how-it-feels-to-hold-the-bitcoin-lightning-torch
[20] https://www.coindesk.com/its-getting-harder-to-send-bitcoins-lightning-torch-heres-why

2.2 Blockchain

Filiera produttiva

L'idea di utilizzare la blockchain nella filiera produttiva (*supply chain*) per tracciare provenienza e genuinità viene continuamente rilanciata, nonostante la sua implausibilità. Era già stato Di Maio ad annunciare di voler contrastare la contraffazione tramite blockchain (anche per certificare il pomodoro *made in Italy*), seguito a Novembre 2018 da Carrefour (con IBM) che ha puntato sul pollo blockchain; questo trimestre abbiamo visto la bufala DOP blockchain[21]. Dovrebbe essere evidente che etichettare un prodotto con un QR code non ha nulla a che fare con la blockchain[22]: il QR code è semplicemente l'indirizzo web di una pagina che riporta dichiarazioni del distributore[23]; le dichiarazioni sono magari anche marcate temporalmente su una blockchain, ma questo non garantisce in alcun modo la veridicità delle stesse e nemmeno l'identità dell'autore (per quello serve la firma digitale). Di fatto il distributore non è dispensato dal dover garantire con la propria diligenza e le proprie verifiche la provenienza dei prodotti.

Pubblicità mozzarella su blockchain

Voto elettronico

Altro tema spinoso che spesso qualcuno vuole affrontare con la blockchain è quello delle elezioni. Anche qui il Movimento 5 Stelle spinge la sperimentazione, in particolare per le forme di democrazia diretta rappresentativa della sua piattaforma Rousseau[24] [25], che in passato hanno mostrato il fianco a diverse critiche. Il voto deve essere diretto, privato, verificabile, resiliente alla coercizione e manipolazione: tutte proprietà difficili da ottenere allo stesso tempo tramite strumenti elettronici.

Nel mondo è infatti fortissimo lo scetticismo verso le forme di voto elettronico: l'hardware può essere manipolato, il software non riesce a conciliare la protezione delle schede elettroniche e l'anonimato dei votanti, è improbo assicurare l'integrità, l'autenticità e la segretezza delle espressioni di voto, ecc.[26] Di fatto il voto cartaceo in cabina, presidiato da funzionari pubblici e controllori privati, è difficilmente superabile quanto a verificabilità indefinita nel tempo, impossibilità di violare la privacy dopo il voto, è praticato nell'assenza di intermediari (anche solo tecnologici), è manipolabile solo su base strettamente locale (e quindi statisticamente poco rilevante), è difficile da controllare con la forza[27]. Aggiungere la blockchain non aggiunge alcun elemento qualificante.

Jamie Dimon

È interessante vedere il video[28] della presentazione del sistema di votazione su blockchain fatta da Vincenzo Di Nicola a Di Maio a marzo, leggendo anche i commenti (tra cui il parere di Stefano Zanero, uno dei massimi esperti italiani di cybersecurity: "il problema da risolvere è nel processo, e usare un DLT non serve a nulla").

[21] http://www.authentico-ita.org/arriva-la-mozzarella-certificata-blockchain/
[22] https://www.ametrano.net/2018/10/11/Not-a-blockchain/
[23] https://www.youtube.com/watch?v=-4sPiZf69rk
[24] https://www.agi.it/blog-italia/cybersecurity/blockchain_rousseau_voto_elettronico_casaleggio-5117572/post/2019-03-09/
[25] https://cryptonomist.ch/en/2019/03/11/code-rousseau-platform-blockchain/
[26] https://twitter.com/peterktodd/status/1105443187341094913
[27] https://twitter.com/Ferdinando1970/status/1105738060610916352
[28] https://www.facebook.com/vdinicola/videos/10104521107116893

Facebook e JP Morgan coin

All'interno di Facebook la squadra blockchain, che già conta 60 persone[29], dovrebbe crescere di altre 20 posizioni, per le quali sono state pubblicate delle inserzioni. I piani strategici non sono ancora dichiarati, ma non è difficile immaginare che possano prevedere l'utilizzo della tecnologia per forme di pagamento[30] sulle piattaforme social Facebook, Messenger, WhatsApp e Instagram. Se quella di Facebook non potrà che essere una strategia *consumer*, un equivalente posizionamento istituzionale sembra essere quello di JP Morgan, il cui coin[31] mira a diventare strumento di pagamento interbancario, per ora in test con selezionati clienti istituzionali. Non una *crypto currency*[32] (se non altro per le note virulente prese di posizione contro bitcoin del CEO Jamie Dimon), anche nel caso di JP Morgan l'ambizione è di trasformare il *business* dei pagamenti[33].

Mark Zuckerberg

[29] https://www.theblockcrypto.com/2019/03/08/facebook-ramps-up-hiring-as-blockchain-team-tops-60-employees/
[30] https://www.coindesk.com/facebook-seeks-counsel-to-forge-blockchain-partnerships-for-new-products
[31] https://www.jpmorgan.com/global/news/digital-coin-payments
[32] https://www.forbes.com/sites/madhvimavadiya/2019/02/17/jp-morgans-cryptocurrency-jpm-coin-is-not-a-cryptocurrency
[33] https://www.cnbc.com/2019/02/13/jp-morgan-is-rolling-out-the-first-us-bank-backed-cryptocurrency-to-transform-payments--.html

2.3 Ethereum e altre crypto

Nuove release Ethereum

Dopo diverse difficoltà nell'upgrade *Constantinople* del protocollo[34], Ethereum l'ha finalmente mandato in produzione assieme all'upgrade noto come *Petersburg*[35]. La crescente difficoltà nell'eseguire questi upgrade è a nostro parere un indicatore preoccupante per la sostenibilità nel tempo del protocollo Ethereum: la complessità tecnica e gestionale sembra essere arrivata ad un livello faticosamente gestibile.

Mettere in piedi un *full-node* Ethereum è diventato quasi impossibile, in senso letterale: l'ultimo tentativo pubblico e documentato, fatto da Jameson Lopp[36], ha fatto emergere bug che impedivano la sincronizzazione del nodo; le bug sono state fissate, ma l'episodio ha dimostrato che ormai nessuno usa davvero un full-node, cioè che la rete Ethereum è di fatto centralizzata e fiduciaria. In meno di 4 anni la blockchain di Ethereum è già a oltre 2TB (contro i 200GB di Bitcoin in 10 anni; si veda la figura 5): gli sviluppatori stanno faticosamente tentando di implementare una qualche forma di *sharding*, cioè di split della blockchain su diversi nodi, evitando la necessità di un full-node. Se a questo aggiungiamo lo scarso utilizzo delle DApp, i piani di riscrivere la *virtual machine*, la pianificata sostituzione di *proof-of-work* con *proof-of-stake*, l'assenza di chiarezza sul futuro della politica monetaria di Ethereum

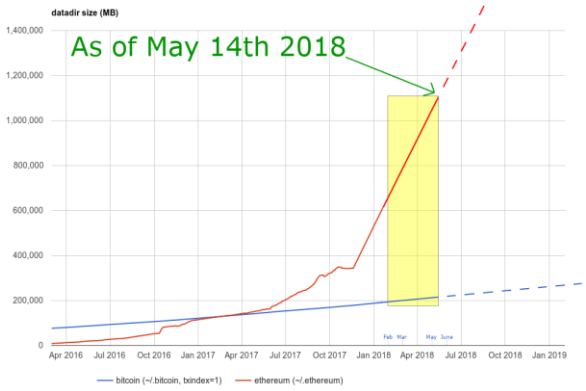


Figura 5: Blockchain size Bitcoin vs Ethereum, dati aggiornati al 14 Maggio 2018, estrapolati per il periodo successivo

[34] https://hackernoon.com/what-is-going-on-with-the-ethereum-hard fork-update-constantinople-f453af698c0c
[35] https://cointelegraph.com/news/ethereums-constantinople-st-peters-burg-upgrades-have-been-activated
[36] https://twitter.com/lopp/sta-tus/1057254691007053825?ref_src=twsrc %5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E105 7254691007053825&ref_url=https%3A%2F%2Fblog.keys.casa%2Fbitc oin-full-validation-sync-performance%2F

(ad oggi discrezionale), il quadro complessivo non ci fa essere ottimisti.

Nonostante le difficoltà e i timori inziali, gli upgrade *Constantinople* e *Petersburg* non sono stati contenziosi: non hanno quindi dato luogo a *hard fork*[37] come quello che aveva visto la nascita nel luglio 2016 di Ethereum Classic.

Attacchi a Ethereum Classic e EOS

Ethereum Classic, l'*hard fork* di Ethereum, ha sofferto a gennaio un attacco 51%[38]: qualcuno con la maggioranza della potenza computazionale ha "riscritto" la storia transazionale cancellando alcune transazioni passate con cui erano stati acquistati sulla borsa Coinbase altri cryptoasset; in questo modo ha realizzato tecnicamente una "doppia spesa" stimata per un controvalore di oltre un milione di dollari. Questo episodio è la conferma che alt-coin difesi da una bassa potenza computazionale non sono sicuri[39], in particolare se il loro algoritmo *proof-of-work* utilizza la stessa funzione di *hash* di altri coin più robusti: i minatori possono prestare, anche solo temporaneamente e parzialmente, le loro *server farm* o cedere hardware obsoleto utilizzabile in questo tipo di attacchi.

Diverso il caso di EOS[40], dove il centralizzato e complesso sistema di *governance* basato su *block producers* e *Community Arbitration Forum* continua ad arrancare: prima hanno tentato di creare una *blacklist* di coin congelati perché coinvolti in malversazioni, poi non riescono a tenerli bloccati perché un *block producer* convalida una transazione che li muove. Le problematiche di sistemi combattuti tra centralizzazione e decentralizzazione è qui evidente.

Grin: la prima implementazione di MimbleWimble

Durante il trimestre è stato lanciato il network Grin, prima implementazione del protocollo MimbleWimble[41]. In un mondo di alt-coin spesso velleitari e fondamentalmente fraudolenti, Grin è partito in maniera trasparente e corretta (niente fondazioni, *pre-mine* per i fondatori, ICO, ecc.) e rappresenta una innovazione crittografica reale ed interessantissima: una blockchain che "dimagrisce" sfrondando la storia transazionale a favore di *privacy* e compattezza dei dati[42]. L'applicazione diretta di questa tecnologia a Bitcoin non è per ora possibile, ma soluzioni di secondo livello potrebbero offrirla a complemento e, in generale, questi risultati sorprendentemente innovativi innescano sempre opportunità di ricerca che potrebbero poi generalizzarli, estenderli o superarli.

È interessante notare che i principali sviluppatori di Grin sono finora retribuiti tramite *fundraising* tra i membri della community. Per ora le quotazioni di mercato non hanno premiato Grin, che è scesa dai livello di prezzo osservati nell'euforia delle prime giornate, ma riteniamo sia uno dei cryptoasset più interessanti e promettenti, anche in termini di ritorni speculativi.

[37] https://www.coindesk.com/constantinople-incoming-tomorrows-two-ethereum-hard forks-explained
[38] https://www.coindesk.com/ethereum-classic-price-stumbles-amid-suspected-51-attack
[39] https://www.coindesk.com/the-ethereum-classic-attacker-has-sent-a-bigger-message
[40] https://breakermag.com/heres-how-the-2-09-million-eos-hack-really-happened/
[41] https://www.coindesk.com/grin-launch-crypto-interest-from-deep-pocketed-investors
[42] https://www.coindesk.com/grin-goes-live-as-mimblewimble-privacy-crypto-hits-first-transaction-block

3. Regolamentazione

Valore probatorio della marcatura temporale blockchain

L'Italia è stata in *pole position* in questo trimestre sul fronte degli sviluppi regolamentari. Se il gruppo di esperti blockchain del MISE viene descritto da alcuni insider come confuso, il legislatore ha messo a segno nel "decreto semplificazioni" una semplice ma decisiva indicazione sul valore probatorio nell'ambito della validazione temporale della blockchain e dei registri distribuiti[43]. In realtà già la normativa eIDAS suggeriva questa possibilità, ma questa volta il pronunciamento è inequivocabile. Le specifiche tecniche sono state rimandate all'AGID[44] che, sebbene non possa anticipare i suoi orientamenti, da noi contattata ci ha comunicato la possibilità che si organizzi un evento di condivisione, prima della consultazione pubblica che è comunque obbligatoria. Seguiremo con attenzione gli sviluppi.

Consob: consultazione sulle ICO

Ha sorpreso in positivo anche la lucidità della Consob, che è intervenuta sulle ICO con una consultazione pubblica basata sul documento[45] per la discussione "Le offerte iniziali e gli scambi di cripto-attività". Il testo proposto offre spunti interessanti e merita certamente risposte qualificate. Speriamo non capiti come con la consultazione del 2016 della *European Securities and Markets Authority*[46] (ESMA) che poneva tutte le domande giuste, anche con un salutare scetticismo, sull'applicabilità della blockchain ai mercati regolamentati: fu sommersa di risposte senza senso che declamavano applicazioni velleitarie, tanto che tre anni dopo non vi è alcuna traccia di quanto proposto[47].

Banca d'Italia: *paper* su cryptoasset

Non si può non citare anche la pubblicazione[48] all'interno della serie "Questioni di Economia e Finanza" di Banca d'Italia dell'articolo "Aspetti economici e regolamentari delle «cripto-attività»" di A. Caponera e C. Gola. Si tratta purtroppo in questo caso di un documento che tradisce una non piena comprensione del fenomeno unita ad un atteggiamento conservatore. Basti qui notare che per la natura stocastica del processo di *partial hash inversion* tipico del mining, che secondo gli autori "*permette di vincere Bitcoin attraverso l'impiego di computer e algoritmi specifici*", l'articolo arriva ad ipotizzare che "*si potrebbe decidere di regolare queste piattaforme tramite una licenza rilasciata dalle autorità che si occupano di gioco d'azzardo*". Peccato davvero che la nostra Banca Centrale pubblichi contributi che diffondono messaggi confusi che aumentano preoccupazione ed indebita criminalizzazione.

[43] https://www.coindesk.com/italys-senate-moves-to-set-legal-foundation-for-blockchain-timestamps
[44] https://www.agendadigitale.eu/documenti/al-via-la-blockchain-revolution-ecco-tutte-le-novita-e-cosa-si-potra-fare/
[45] http://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/64251cef-d363-4442-9685-e9ff665323cf
[46] https://www.esma.europa.eu/press-news/esma-news/esma-assesses-usefulness-distributed-ledger-technologies
[47] https://www.esma.europa.eu/press-news/consultations/consultation-distributed-ledger-technology-applied-securities-markets
Per una risposta estremamente pertinenente si veda invece Ametrano, Barucci, Marazzina e Zanero https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265776
[48] http://www.bancaditalia.it/pubblicazioni/qef/2019-0484/QEF_484_19.pdf

4. Ecosistema

Neutrino e Coinbase

La polemica più calda del trimestre ha riguardato l'acquisto da parte di Coinbase della società italiana Neutrino, specializzata in analisi su blockchain. L'acquisizione è stata per Coinbase l'occasione di colmare il deficit di conformità regolamentare su monitoraggio, reportistica e segnalazioni di attività sospette.

Le polemiche non hanno riguardato direttamente questi aspetti, ma il passato dei fondatori di Neutrino, tutti coinvolti nelle attività di Hacking Team, l'azienda di spionaggio informatico che ha venduto i suoi servigi a mezzo mondo, inclusi paesi totalitari ed antidemocratici: l'attività di Hacking Team avrebbe contribuito a perseguitare i difensori dei diritti civili. Per Coinbase si è trattato certamente di uno scivolone dal punto di vista di immagine; forse anche peggiore è stata però la difesa pubblica[49] di Brian Armstrong, CEO di Coinbase, secondo cui tutti coloro che hanno partecipato ad Hacking Team sarebbero stati rimossi da ruoli operativi[50]. Peccato non si capisca bene chi siano e di quali ruoli operativi si parli, mentre è chiarissimo che gli ex di Hacking Team hanno sicuramente realizzato profitti significativi dalla vendita di Neutrino, anche se non dovessero più avere ruoli operativi. Per reazione è partito sul web il movimento #DeleteCoinbase[51], che ha visto molti personaggi pubblici cancellare il loro conto presso Coinbase; era difficile credere che il movimento potesse avere un impatto significativo ed infatti sembra già aver perso mordente, ma indubbiamente sono sempre più cruciali le responsabilità culturali, politiche e civili dell'innovazione nell'ambito delle tecnologie web[52].

Brian Armstrong

Blythe Masters, copertina Bloomberg Markets

Digital Asset ed R3 perdono il management

Negli ultimi mesi c'è stata una emorragia di top manager da R3[53] e Digital Asset[54], due delle aziende tra i principali proponenti di tecnologia blockchain. Nel caso di Digital Asset a lasciare è addirittura la fondatrice e CEO Blythe Masters[55]: ex JP Morgan, la donna che può vantare di aver inventato i Credit Default Swap, Masters è nota per lucidità e capacità esecutiva. Quando si era mossa in ambito blockchain, tutta Wall Street aveva mostrato interesse ed attenzione. Il fatto che oggi lasci rappresenta secondo molti l'evidenza che blockchain non manterrà le sue promesse nel mercato dei capitali e della finanza tradizionale: la lettura è infatti che la Masters lasci per non essere troppo direttamente coinvolta in un fallimento. Commenti simili spiegano anche il declino di attrattività professionale di R3, abbandonata tra gli altri proprio da uno dei suoi tre co-fondatori, Jesse Edwards: dopo tre anni e mezzo e centinaia di milioni di investimento non si vedono all'orizzonte risultati significativi, pertanto chi può lascia la barca prima che affondi. *Sic transit gloria mundi*.

[49] https://blog.coinbase.com/living-up-to-our-values-and-the-neutrino-acquisition-ba98174cdcf6
[50] https://www.coindesk.com/coinbase-pushes-out-ex-hacking-team-employees-following-uproar
[51] https://www.coindesk.com/bitcoin-delete-coinbase-neutrino-crypto
[52] https://www.coindesk.com/what-coinbase-needs-to-learn-from-the-neutrino-scandal
[53] https://www.coindesk.com/2-executives-are-leaving-blockchain-startup-r3-in-management-shake-up
https://www.coindesk.com/r3s-former-chief-sales-officer-joins-blockchain-startup-alphapoint
https://www.coindesk.com/r3-co-founder-jesse-edwards-leaving-enterprise-blockchain
[54] https://www.coindesk.com/digital-asset-loses-another-exec-and-a-high-profile-board-member
https://www.coindesk.com/digital-assets-europe-head-is-latest-to-leave-enterprise-blockchain-startup
https://www.coindesk.com/digital-asset-loses-second-cto-in-6-months-as-startup-shake-up-continues
[55] https://www.coindesk.com/digital-asset-names-new-ceo-to-succeed-blythe-masters
https://www.bloomberg.com/news/articles/2019-03-19/blockchain-firm-once-run-by-blythe-masters-names-yuval-rooz-ceo

Muore (?) il CEO, addio ai Bitcoin di Quadriga

Non poteva mancare il solito "scandalo" Bitcoin, che questo trimestre ha preso forma nella presunta morte di Gerald Cotten, CEO di Quadriga, borsa di scambio canadese. Con lui scompaiono anche le chiavi private di $135M in Bitcoin[56] ed in molti ipotizzano si tratti in realtà di una truffa deliberatamente architettata: il certificato di morte viene dall'India, c'è un testamento compilato 12 giorni prima della presunta morte, la vedova aveva appena messo in sicurezza molti bene al riparo di trust e fondazioni.

Gerald Cotten

Al di là dei pettegolezzi e delle doverose indagini, l'incidente gravissimo getta la luce ancora una volta su prassi di custodia di cryptoasset che sono insicure ed inaccettabili dal punto di vista tecnico e professionale.

Ricerca ed aggiornamenti

Si sono progressivamente sempre più affermate negli ultimi mesi due fonti informative di ottima qualità: la *Bitcoin Optech Newsletter*[57] aggiorna con frequenza settimanale sugli sviluppi tecnologicamente più rilevanti del protocollo Bitcoin, mentre la ricerca di BitMEX[58] ha pubblicato una serie di studio di sicuro interesse.

Jack Dorsey: supporto allo sviluppo Bitcoin

Jack Dorsey, CEO di Square e Twitter, ha lasciato il segno in questo trimeste. Non tanto, o almeno non solo, per aver preso parte alla catena della Lightning Torch; ma soprattutto per la sua recente iniziativa a supporto dello sviluppo del protocollo Bitcoin. Ha, infatti, offerto a sviluppatori che oggi lavorano sul protocollo nel tempo libero di essere retribuiti da Square per lavorare a tempo pieno su Bitcoin, con totale indipendenza e senza vincoli aziendali. Nel solco di Blockstream e ChainLab, questo è un segnale che l'ecosistema Bitcoin potrebbe nel futuro sempre più assomigliare all'ecosistema Linux, dove diverse aziende trovano economicamente ragionevole sostenere lo sviluppo open-source a vantaggio di tutti.

Jack Dorsey

[56] https://www.bbc.com/news/world-us-canada-47203706
https://edition.cnn.com/2019/02/05/tech/quadriga-gerald-cotten-cryptocurrency/index.html
https://www.investinblockchain.com/is-quadriga-ceo-actually-dead-or-140-million-exit-scam
https://www.newsbtc.com/2019/02/06/quadriga-crypto-will/
https://www.coindesk.com/stewart-mckelvey-quadriga-law-firm

[57] https://bitcoinops.org/en/newsletters/
[58] https://blog.bitmex.com/research/

Contatti

Ferdinando M. Ametrano

ferdinando@dgi.io

Paolo Mazzocchi

paolo@dgi.io

Chi siamo

Il Digital Gold Institute è un centro di ricerca e sviluppo sui temi di scarsità nel mondo digitale (Bitcoin e cryptoasset) e sulla tecnologia blockchain (crittografia e marcatura temporale). L'istituto promuove queste tematiche nel dibattito pubblico e nel mondo accademico attraverso ricerca e sviluppo, formazione, consulenza operativa e strategica.

Digital Gold Institute

Scarcity in the Digital Realm


www.dgi.io


info@dgi.io