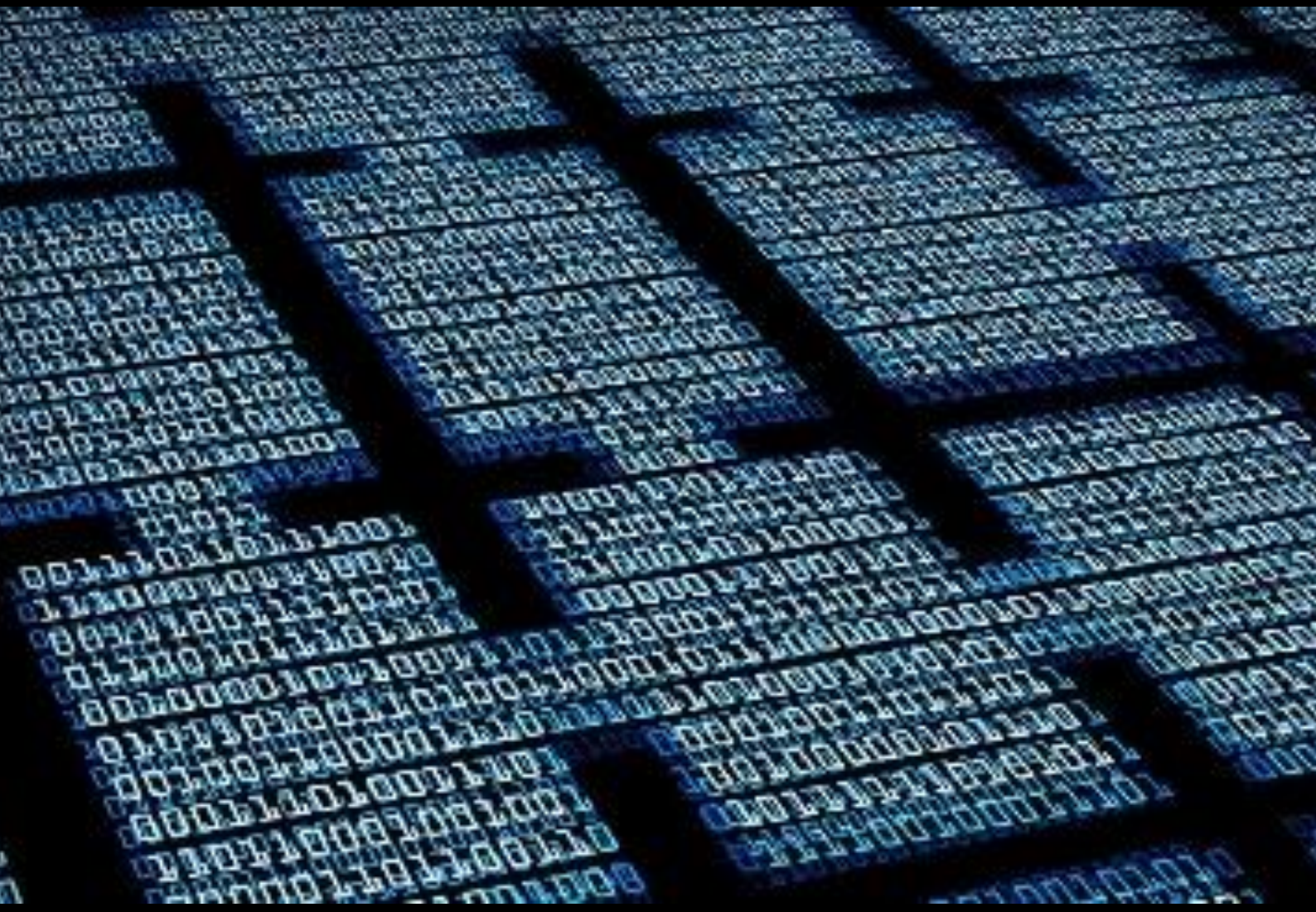
n. 1

Digital Gold Institute

Scarcity in the Digital Realm



Report Trimestrale

2019-Q2

Editoriale

Dopo il caloroso apprezzamento che avete riservato al numero zero di aprile (2019-Q1), ecco il numero uno nella serie dei report trimestrali prodotti dal Digital Gold Institute. L'intento resta quello di offrirvi uno sguardo sintetico ma ampio agli eventi che hanno caratterizzato l'ultimo trimestre, in questo caso 2019-Q2.

Senza girarci troppo attorno, è inevitabile che la notizia principale sia stata l'apprezzamento di Bitcoin che ha chiuso il trimestre a $10817, con una crescita del 163% rispetto al prezzo di riferimento del 31 marzo ($4105): ne discutiamo nella sezione mercato.

L'altra notizia principale è l'annuncio di Libra, il *coin* promosso da Facebook attraverso la Libra Association, che dovrebbe arrivare nel primo semestre 2020. Si tratta di un evento estremamente significativo perché "sdogana" definitivamente l'idea che sia possibile e persino realistico trasferire valore attraverso strumenti di scambio digitali emessi da privati. Che Libra si concretizzi davvero come opportunità per gli oltre due miliardi di utenti Facebook o che sia fermata dai regolatori, si tratterà in entrambi i casi di uno snodo cruciale nella storia della moneta. Analizziamo il fenomeno Libra nella sezione ecosistema.

Con questo numero debutta anche una sezione dedicata alle news del nostro Istituto: con la velocità di evoluzione e cambiamento che caratterizza le nostre giornate, noi stessi possiamo talvolta trascurare o dare per scontati i passi avanti che l'Istituto sta compiendo; a maggior ragione ci siamo accorti che voi, i nostri partner, non siete puntualmente aggiornati su tutte le novità. Fare il punto delle attività è quindi l'occasione per apprezzare il percorso comune, riconsiderare le scelte di indirizzo, fissare nuovi obiettivi. Tra le diverse attività del trimestre, la notizia principale è il lancio del "Crypto Asset Lab", iniziativa di ricerca congiunta tra il Digital Gold Institute e l'Università degli Studi di Milano-Bicocca: vi raccontiamo del Lab, del suo convegno di lancio e delle sue linee di ricerca.

Non resistiamo alla tentazione di chiudere questo editoriale senza indulgere, almeno brevemente, nel folklore. Se lo scorso trimestre festeggiavamo i 10 anni di Bitcoin, questo trimestre ha visto l'anniversario del pizza-day: il 22 maggio 2010 Laszlo pagava 10000 Bitcoin per due pizze[1]. All'epoca si trattava della prima transazione che dava un controvalore a Bitcoin (0.0032 dollari per Bitcoin), al cambio attuale sono oltre 100 milioni di dollari: difficile immaginare pizze così buone da meritare un investimento simile.

Al solito l'ultimo paragrafo è per ribadire che il report è pensato e scritto per voi: partner, sostenitori e collaboratori dell'Istituto; per renderlo sempre più utile sono indispensabili i vostri suggerimenti, così come eventuali richieste per ulteriori approfondimenti.

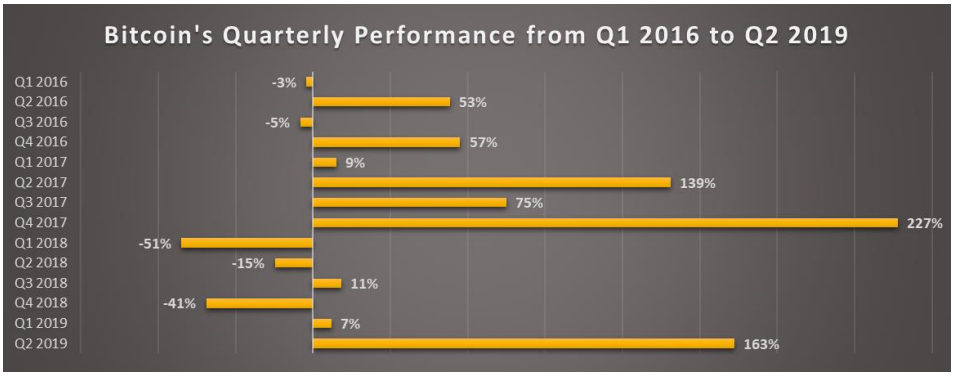
Buona estate.

[1] https://bitcoinmagazine.com/articles/the-man-behind-bitcoin-pizza-day-is-more-than-a-meme-hes-a-mining-pioneer/#1558493045

Indice

1. Mercato

Performance Bitcoin



Quello appena concluso è stato senza dubbio uno dei migliori trimestri per il valore di mercato di Bitcoin. Durante questo periodo infatti il prezzo è salito del 163%, con un rialzo quasi paragonabile a quello registrato a fine 2017, in un momento di piena euforia di mercato, e che si colloca al secondo posto tra i migliori trimestri da inizio 2016 ad oggi.

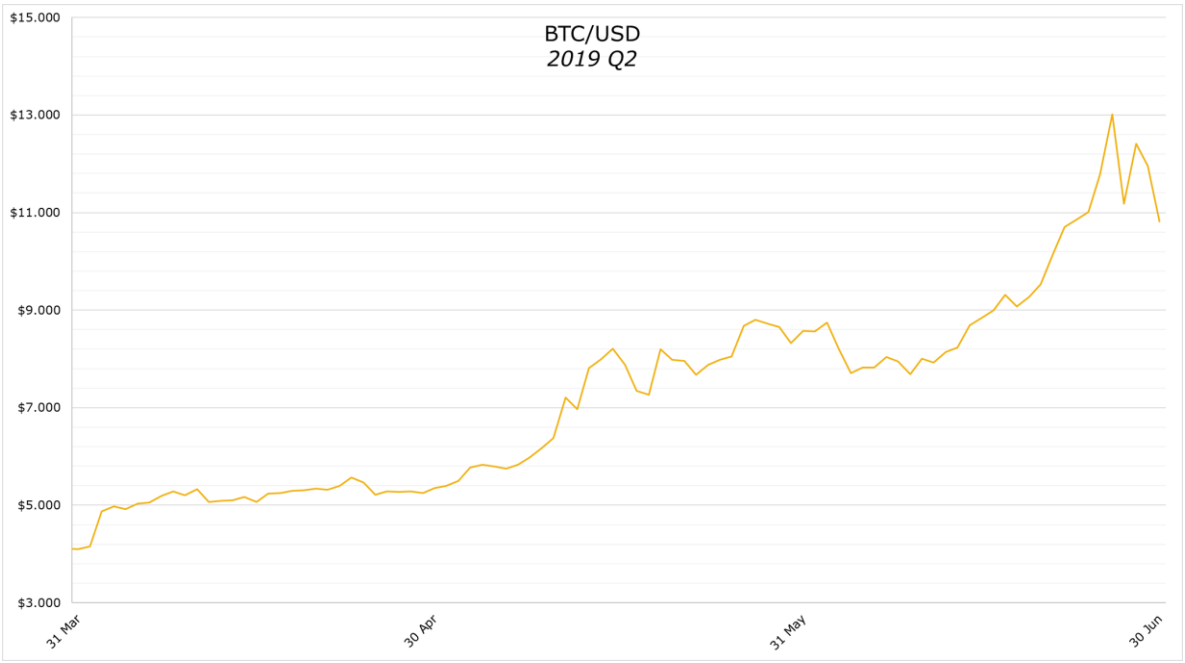


Figura 1: rendimento Bitcoin secondo trimestre 2019

Performance alt-coin

Come fatto nello scorso report, proponiamo anche il grafico della performance delle principali alt-coin: Ethereum, Ripple, Litecoin, Bitcoin Cash, Stellar, Ethereum Classic, Zcash, Monero. In figura sono riportati i rendimenti espressi in Bitcoin: quanto avrebbe reso un Bitcoin investito ad inizio periodo in ognuno degli alt-coin considerati.

Ricordiamo che è qualificante denominare la performance degli alt-coin in Bitcoin: qualsiasi investimento in crypto-asset che non sia Bitcoin si pone intrinsecamente come alternativo a Bitcoin e su quel metro va misurato.

Come si può vedere dal grafico (figure 2), in questo periodo di mercato rialzista Bitcoin ha fatto meglio della maggior parte dei *peers*; solo Ethereum ha avuto nel periodo una performance paragonabile.

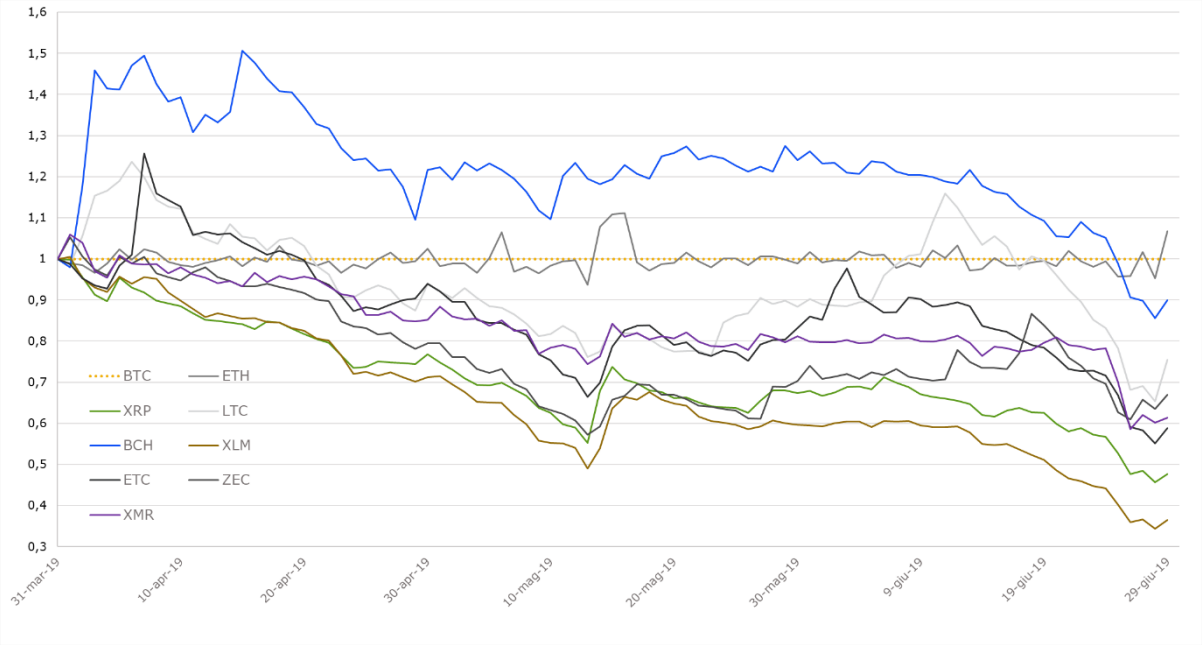


Figura 2: redimenti alt-coin rispetto a Bitcoin

È interessante notare la crescita anomala e notevole di Bitcoin Cash nei primi giorni del trimestre. Tale crescita però è stata totalmente riassorbita nella restante parte del trimestre, portando a un valore di chiusura inferiore a quello di Bitcoin.

Performance BSV

Un capitolo a parte lo merita Bitcoin SV (BSV). A fine maggio, dopo un periodo di significativi e continui ribassi, le quotazioni di questo alt-coin sono esplose all'improvviso. Il motivo del rialzo è da ricondurre ad una falsa notizia[2], pubblicata dal sito cinese di news Coinbull, secondo la quale il creatore di BSV, Craig Wright, avrebbe dimostrato di essere Satoshi Nakamoto. La notizia, grazie anche ai bassi volumi di scambio di BSV, ha portato ad un rimbalzo del valore della currency di 60$ in meno di 10 ore. Questo dimostra ancora una volta come i valori degli alt-coin siano facilmente manipolabili.

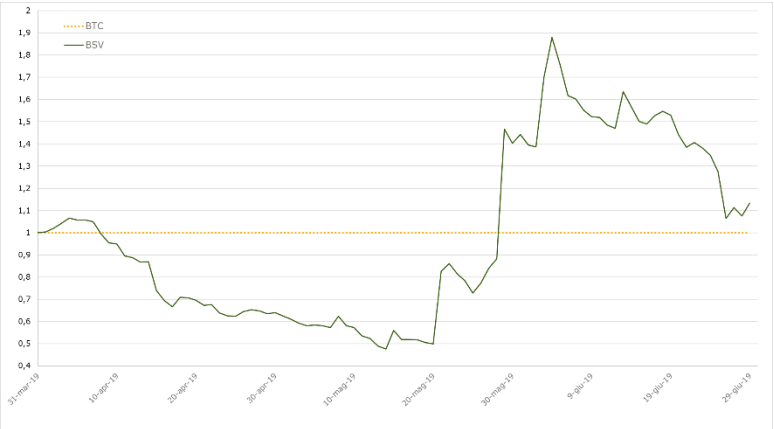


Figura 3: Rendimento BSV rispetto a Bitcoin

Bitcoin SV

Bitcoin SV è un acronimo per Bitcoin *Satoshi's Vision* ed è nato a seguito di un cambiamento contenzioso (*hard-fork*) di Bitcoin Cash effettuato il 15 novembre 2018. Questo fork è stato proposto dai developer del software Bitcoin ABC, utilizzato da Bitcoin Cash, per aumentare la scalabilità del network cambiando il modo in cui venivano conservati i dati nella blockchain. Craig Wright, colui che si è più volte auto-dichiarato Satoshi Nakamoto, senza particolari riscontri o riconoscimenti, si è opposto a questo fork ed ha fortemente supportato la versione precedente del software, dando il via ad una nuova currency.

[2] https://www.coindesk.com/scammers-boost-bsv-price-with-fake-satoshi-confirmation

CoinMarketCap e volume reali

Lo scorso trimestre abbiamo analizzato il report[3] che Bitwise ha presentato alla SEC per proporre il suo ETF, in cui emergeva come degli 81 exchange crypto analizzati, solamente 10 pubblicavano volumi reali.

Sull'onda di questi risultati CoinMarketCap, il data provider di riferimento per il mondo crypto, ha promosso una iniziativa[4] di trasparenza, in collaborazione con le principali borse di scambio, con l'obiettivo di poter rappresentare metriche affidabili di mercato. L'iniziativa può già vantare un buon numero di *exchange*, tra cui Binance, Bittrex, OKEx, Huobi, Liquid, Upbit, KuCoin, HitBTC Gate.io, OceanEx e Bitfinex. CoinMarketCap ha dichiarato che tutti gli exchange dovranno pubblicare i dati live di trading e degli ordini entro 45 giorni, pena l'esclusione dal calcolo dei volumi aggiustato.

Questa iniziativa di CoinMarketCap fa ben sperare e potrebbe aiutare il mercato a diventare sempre più trasparente e in linea con gli standard tradizionali dei mercati finanziari.

Futures su Bitcoin: CFTC approva LedgerX

L'approvazione[5] da parte di CFTC (*U.S. Commodity Futures Trading Commission*) del futures su Bitcoin offerto da LedgerX potrebbe essere un punto di svolta nella storia di questo prodotto finanziario[6]. Infatti, i futures finora offerti da CME (ed in passato da CBOE) sono *cash-settled* e non implicano quindi la consegna di Bitcoin, bensì il regolamento delle plusvalenze o minusvalenze in Dollari Statunitensi. LedgerX sarà, invece, *physically settled* consegnando Bitcoin; questa è la stessa scelta di Bakkt (gruppo ICE, cioè New York Stock Exchange) che però non ha ancora ricevuto il via libera da CFTC. La competizione per chi possa offrire i migliori servizi e prodotti su Bitcoin al mondo finanziario tradizionale è solo agli inizi. Sono due gli snodi principali: la ritrosia del regolatore che, dopo le aperture della CFTC guidata da Christopher Giancarlo, vede oggi un generale irrigidimento e la problematica della custodia dei Bitcoin, da risolvere in modo affidabile se si vuole operare sul "fisico" e non su prodotti "sintetici".

> *I futures finora offerti da CME (ed in passato da CBOE) sono cash-settled e non implicano quindi la consegna di bitcoin, bensì il regolamento delle plusvalenze o minusvalenze in Dollari Statunitensi. LedgerX sarà, invece, physically settled consegnando Bitcoin*

[3] https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf
[4] https://www.coindesk.com/coinmarketcap-forms-alliance-to-tackle-concerns-over-price-data-integrity
[5] https://www.cftc.gov/PressRoom/PressReleases/7945-19
[6] https://www.coindesk.com/cftc-approves-ledgerx-to-settle-futures-in-real-bitcoin

2. Tecnologia

2.1 Bitcoin

Lightning Torch raggiunge la destinazione finale

Come anticipato nello scorso numero del report, il 2018 ha visto nascere *Lightning Network*, un *layer* tecnologico di secondo livello che aumenta tramite i suoi *payment channel* la scalabilità del protocollo Bitcoin. In questo primo semestre del 2019 il network ha raggiunto una dimensione considerevole: oltre 4000 nodi con più di 35000 canali di pagamento[7].

Durante il primo trimestre del 2019 era stata lanciata la cosiddetta *Lightning Torch*: un pagamento su Lighting Network che è passato come una torcia di mano in mano tra dozzine di partecipanti, ognuno dei quali ha incrementato l'importo della torcia. Dopo essere passata da 275 persone diverse, inclusi molti personaggi di spicco del mondo Bitcoin tra cui il CEO di Twitter Jack Dorsey, la torcia ha raggiunto l'importo massimo per ora consentito su Lightning Network (4.29M satoshi) e la sua destinazione finale[8] nelle mani della associazione benefica *Bitcoin Venezuela*.

> *La torcia ha raggiunto l'importo massimo per ora consentito su Lightning Network (4.29M satoshi) e la sua destinazione nelle mani della associazione benefica Bitcoin Venezuela.*

Durante il suo tragitto non sono mancate le criticità dovute allo stato ancora iniziale di sviluppo del network, che ha reso molto tecnico e delicato il passaggio della torcia da una mano all'altra; la torcia ha dimostrato però senza alcun dubbio la capacità del network Bitcoin di spostare valore istantaneamente e senza limiti di frontiere o politici: è infatti passata anche per stati sotto embargo economico come l'Iran e il Venezuela, dove Bitcoin rappresenta una reale opportunità per proteggersi dall'altissima inflazione della moneta locale. Tutto questo è servito a portare molta visibilità al network e questo si rifletterà in una accelerazione degli sviluppi nei prossimi mesi.

[7] https://explorer.acinq.co/
[8] https://bitcoinmagazine.com/articles/vidi-vici-satoshi-lightning-torch-has-reached-its-final-destination/#1555019294

Lightning Labs rilascia l'applicazione desktop

Quello passato è stato sicuramente un trimestre molto importante nello sviluppo di *Lightning Networks*: la società *Lightning Labs* ha infatti rilasciato la versione per *mainnet* Bitcoin delle sue applicazioni *desktop*[9] (macOS, Windows e Linux) e *mobile*[10] (Android e iOS) finora disponibili solo per *testnet* (per la differenza tra i diversi network Bitcoin si veda il box di approfondimento). L'applicazione consente la gestione le transazioni sul network e rappresenta anche un significativo passo in avanti in termini di *user experience*; ad oggi infatti, come ha mostrato l'esperienza della Lightning Torch, l'utilizzo del network è limitato a chi possiede significative competenze tecniche, quindi avanzamenti nella direzione di semplificazione ed utilizzabilità sono fondamentali. Le applicazioni rilasciate sono per ora in versione *alpha*, quindi comunque destinate a un pubblico di sviluppatori e tester, in vista della versione finale per tutti gli utenti attesa nei prossimi mesi.

Nuovo rilascio per *Bitcoin Core*

Durante il trimestre è stata rilasciata la versione 0.18.0[11] di *Bitcoin Core*, la nuova versione del client software lanciato 10 anni fa da Satoshi Nakamoto e che ancora oggi rappresenta il 97%[12] dei client Bitcoin utilizzati dai nodi del network. Questo indica come lo sviluppo di Bitcoin sia, ancora oggi, fondamentalmente coincidente con lo sviluppo del client Core, progetto *open-source* accessibile a chiunque tramite il portale di sviluppo GitHub.

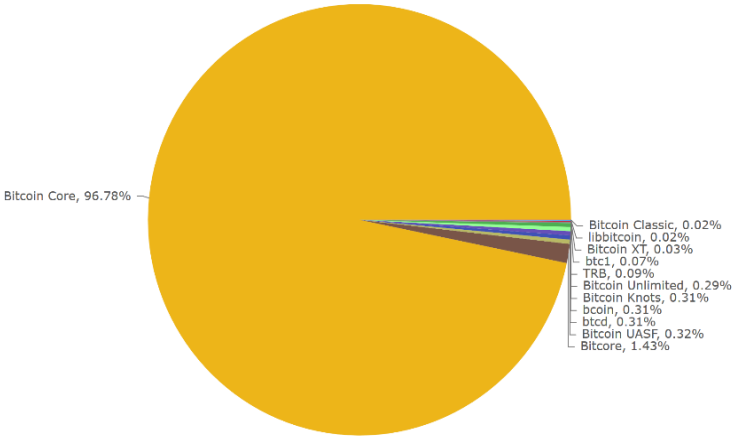


Figura 4: Distribuzione dei diversi client usati dai nodi Bitcoin, secondo il sito Coindance.

Questa nuova versione arriva a 6 mesi dalla precedente e vede il contributo di centinaia di sviluppatori da tutto il

Mainnet, Testnet, Regtest

In Bitcoin esistono 3 differenti network: mainnet, testnet e regtest.

Mainnet è la rete originale di Bitcoin, quella lanciata il 3 gennaio 2009 da Satoshi Nakamoto, i cui coin hanno un valore economico sul mercato.

Testnet è, come suggerisce il nome, un network di test pubblico, similare a mainnet, ma senza valore economico, dove gli sviluppatori possono provare in anteprima gli aggiornamenti del protocollo. Il funzionamento di questa rete è in tutto similare a mainnet, inclusi i minatori che validano i blocchi, ma ovviamente ha una potenza di calcolo molto più bassa ed instabile, risultando quindi meno affidabile di mainnet. La rete viene utilizzata da tutti gli attori tecnologici per testare le soluzioni software prima di utilizzarle su mainnet; anche i minatori lo fanno, sfruttando hardware obsoleto non più utilizzabile su mainnet. La rete di test viene periodicamente resettata, per evitare che acquisisca valore economico: ad oggi siamo alla terza versione.

Infine, **regtest** è una testnet privata instanziabile per lo sviluppo in locale: non prevede il mining e gli utilizzatori controllano anche la generazione dai blocchi.

[9] https://blog.lightning.engineering/announcement/2019/04/23/mainnet-app.html
[10] https://blog.lightning.engineering/announcement/2019/06/19/mobile-app.html
[11] https://bitcoincore.org/en/2019/05/02/release-0.18.0/
[12] https://coin.dance/nodes/share

mondo. Le principali novità sono[13] il supporto all'utilizzo degli *hardware wallet* (inclusi i wallet sviluppati da Ledger, Trezor, Digital BitBox, KeepKey e Coldcard) e le funzionalità multi-wallet che permettono la gestione di più wallet utilizzando il medesimo client.

Liquid Securities Platform

Anche in questo trimestre Blockstream ha portato avanti la sua campagna di rilasci, che ha visto una significativa accelerazione nel 2019, presentando a maggio, durante la conferenza Consensus a New York, la *Liquid Securities Platform*[14].

Liquid è una *sidechain*, cioè una blockchain che si appoggia a quella di Bitcoin. Su questa sidechain, gestita da una federazione di *exchange*, è possibile scambiare in sicurezza e con tempi di conferma dell'ordine del minuto i *Liquid-Bitcoin* (L-BTC), token garantiti da Bitcoin reali congelati sulla blockchain pubblica: l'utilità principale è quella di consentire arbitraggi efficienti tra le diverse borse, superando il problema dei tempi di conferma del network Bitcoin che, lo ricordiamo, sono dell'ordine di un'ora (per raggiungere le 6 conferme considerate come finali).

	bitcoin	Liquid
TRUST MODEL	Trustless	Multi Party Trust
TRANSACTION INCLUSION	Miners	Block Signers
PRIVACY	None	Confidential Assets
SPEED	~ 10 Minutes	~1 Minute
COST	Variable	Variable
SECURITY	Self-Sovereign Funds	Multiple Attacks Needed
FINALITY	~60 Minutes	2 Minutes

Figura 5: Tabella di comparazione Bitcoin - Liquid

Tramite la nuova piattaforma *Liquid Securities* è ora possibile anche l'emissione di *digital asset* diversi da L-BTC. La piattaforma è stata lanciata in collaborazione con quattro partner iniziali: *TokenSoft* (compagnia specializzata nella *token economy*), *BnkToTheFutures* (piattaforma di investimento online specializzata in FinTech), *Zenus Bank* (banca che permette di aprire conti in Dollari Statunitensi da ogni parte del mondo) e *Pixelmatic* (società di sviluppo di videogame che sta lavorando allo sviluppo di un gioco *token-based*).

Con questo rilascio Blockstream cerca di promuovere la nascita di una *token-economy* su Liquid attraverso una piattaforma dotata di *user experience* semplice e guidata. Uno dei benefici di Liquid Securities è che le transazioni di asset sono private (o, in gergo tecnico, *confidenziali*) per tutti, ma allo stesso tempo verificabili da una terza parte scelta dall'emittente, che svolge la funzione di auditor. Questo è un enorme beneficio per le aziende, che possono emettere i loro token utilizzando la tecnologia più sicura (sostanzialmente la blockchain di Bitcoin), senza dover rinunciare alla privacy ma rimanendo rispettosi dei tipici requisiti regolamentari[15] in ambito di audit.

> *Blockstream cerca di promuovere la nascita di una token-economy su Liquid attraverso una piattaforma dotata di user experience semplice e guidata.*

Electrum sotto attacco

Electrum, probabilmente il wallet Bitcoin per desktop più diffuso, ha subito un *DoS* (*Denial of service*) *attack*[16] che ha causato la perdita di molti Bitcoin (si parla di un controvalore in milioni di dollari) da parte degli utenti meno esperti del wallet.

[13] https://bitcoinmagazine.com/articles/bitcoin-core-0180-release-heres-whats-new#1556802139
[14] https://blockstream.com/liquid/securities/
[15] https://bitcoinmagazine.com/articles/blockstream-releases-first-enterprise-grade-product-liquid/#1557936882
[16] https://twitter.com/ElectrumWallet/status/1114987055736655873

L'attacco, tutt'ora in corso, è orchestrato tramite un sofisticato bot che coordina, si stima, circa 140mila server Electrum malevoli che si presentano agli utenti come server regolari. I server malevoli, superando di gran lunga il numero di server onesti, catturano statisticamente la maggioranza degli utenti; quando l'utente tenta una transazione riceve un errore, il cui messaggio di testo è gestito dal server malevolo ed invita ad aggiornare il software con una versione fraudolentemente modificata e scaricabile da siti non ufficiali. Accentando l'aggiornamento, gli utenti iniziano a quel punto ad utilizzare un software che li deruba dei propri Bitcoin[17].

Bitcoin Improvement Proposal

Una Bitcoin Improvement Proposal, comunemente chiamata BIP, è un documento che dettaglia una proposta di modifica al codice sorgente di Bitcoin Core.

Il documento della BIP deve contenere una spiegazione concisa delle specifiche tecniche di implementazione e i razionali di questa modifica.

Le nuove più recenti versioni di Electrum hanno corretto questa falla di sicurezza: il testo dei messaggi di errore non può più essere gestito dal server ed è il client a verificare se sono presenti aggiornamenti sul sito originale.

Taproot: la nuova *Bitcoin Improvement Proposal*

Uno degli sviluppi più promettenti per il futuro di Bitcoin è l'introduzione di *Taproot*, proposta sulla mailing list dei developer Bitcoin da Pieter Wuille, uno degli sviluppatori più attivi.

Figura 6: Pieter Wuille

Originariamente presentato per la prima volta da Gregory Maxwell, ex CTO di Blockstream, Taproot permette di aumentare la flessibilità degli *smart contract* in Bitcoin, aumentando allo stesso tempo la *privacy*: anche uno smart contract molto complicato diventerebbe non distinguibile da una normale transazione.

Taproot[18] è proposto come *soft-fork*, cioè modifica retro-compatibile al protocollo Bitcoin, ma necessita della preventiva introduzione della firma digitale secondo l'algoritmo di Schnorr[19]: se queste nuove funzionalità verranno accettate è quindi molto probabile che saranno aggregate alla proposta, sempre di Peter Wuille, per l'introduzione di Schnorr[20].

> *Originariamente presentato per la prima volta da Gregory Maxwell, ex CTO di Blockstream, Taproot permette di aumentare la flessibilità degli smart contract in Bitcoin aumentando allo stesso tempo la privacy*

[17] https://thenextweb.com/hardfork/2019/04/08/bitcoin-wallet-electrum-dos-attack-botnet-phishing/
[18] https://github.com/sipa/bips/blob/bip-schnorr/bip-taproot.mediawiki
[19] https://blog.bitmex.com/the-schnorr-signature-taproot-softfork-proposal/
[20] https://github.com/sipa/bips/blob/bip-schnorr/bip-schnorr.mediawiki

2.2 Applicazioni blockchain

Nestlé, Carrefour e IBM per la tracciatura del purè

Nel precedente report abbiamo parlato di blockchain nella filiera produttiva (*supply chain*) per la tracciatura di beni e prodotti, evidenziando i limiti che questa applicazione presenta: aggiungere un QR code di per sé non garantisce (tantomeno può certificare) provenienza o genuinità. Il QR code rimanda a una pagina web dove sono dichiarate tutte le informazioni sul bene in questione fornite da produttore e distributore; la dichiarazione è di solito marcata temporalmente su una blockchain. La datazione della dichiarazione è quindi incontrovertibile, ma la veridicità delle informazioni non lo è; inoltre, anche assumendo veritiere le informazioni riportate, lo stesso QR code può essere copiato ed incollato sulla confezione di qualsiasi altro prodotto, magari merceologicamente simile ma di incerta provenienza, sostanzialmente annullando il valore probatorio delle informazioni a cui rimanda.

> *La datazione della dichiarazione è incontrovertibile, ma la veridicità delle informazioni non lo è; inoltre lo stesso QR code può essere copiato ed incollato sulla confezione di qualsiasi altro prodotto sostanzialmente annullando il valore probatorio delle informazioni a cui rimanda*

È notizia di questo trimestre la collaborazione[21] tra Nestlé, Carrefour e IBM per tracciare il purè su blockchain Hyperledger: nonostante la popolarità di cui gode in questi mesi l'utilizzo di blockchain nella filiera produttiva rimaniamo scettici sui reali benefici ed anzi ribadiamo che si tratta piuttosto di tecniche di marketing disonesto.

ABI e la spunta interbancaria

L'Associazione bancaria italiana (ABI) ha annunciato[22] l'utilizzo della tecnologia Blockchain per il *settlement* delle operazioni interbancarie, la cosiddetta spunta interbancaria, a partire da marzo 2020.

La spunta interbancaria

La spunta interbancaria verifica la corrispondenza delle attività che interessano banche diverse, ad esempio le operazioni effettuate fra due clienti che utilizzano istituti diversi.

La sperimentazione si basa sulla piattaforma *Corda*, ha NTT Data e SIA come partner tecnologici, vede la partecipazione di 18 banche (il 78% del mondo bancario italiano in termine di numero di dipendenti) ed è durata 10 mesi. In questo periodo ogni banca partecipante ha messo in piedi un nodo *Corda* e sono state processate oltre un milione di transazioni.

I principali benefici riconosciuti da ABI all'utilizzo della soluzione blockchain sono[23] "*l'esecuzione del riscontro automatico tra transazioni non corrispondenti eseguita sulla base di un algoritmo condiviso, la standardizzazione del processo e del canale di comunicazione unico e la visibilità sulle transazioni tra le parti. Il processo quindi riguarda la riconciliazione dei flussi e delle operazioni che generano scritture sui conti reciproci in Italia e la gestione dei sospesi. Le attività sono relative al colloquio interbancario.*"

[21] https://cointelegraph.com/news/nestle-carrefour-work-with-ibm-to-track-mashed-potato-brand-with-blockchain
[22] https://www.finextra.com/newsarticle/33991/italys-banks-to-use-dlt-for-reconciliations/wholesale
[23] https://www.abi.it/Pagine/news/Spunta-Project-blockchain-.aspx

Non abbiamo avuto modo di approfondire l'argomento per mancanza di dati pubblici riscontrabili. L'impressione, per ora, è che ABI abbia sfruttato l'idea di una *sand-box* sperimentale per efficientare un processo farraginoso, ma non decisivo, delle banche tradizionali. L'efficientamento si poteva ottenere centralizzando in ABI le operazioni di spunta tramite tecnologia tradizionale, ma questo avrebbe creato un precedente per ABI come *clearing house*, non ben visto dalle banche partecipanti: la scusa della sperimentazione tecnologica è stata invece usata come cavallo di Troia. Vedremo nei prossimi mesi se si passerà davvero dalla parte sperimentale alla produzione, quali saranno i benefici reali, le difficoltà di integrazione nella filiera di processo tradizionale, la percentuale di adozione da parte degli istituti bancari. Per ora l'unico risultato evidente è che tante banche hanno un nodo Corda: potrebbe essere il volano decisivo per le applicazioni che dovrebbero arrivare su questa piattaforma e che finora stentano a palesarsi, nonostante le centinaia di milioni investiti dalle banche di tutto il mondo nel consorzio R3 che sviluppa Corda.

L'efficientamento del processo si poteva ottenere centralizzando in ABI le operazioni di spunta tramite tecnologia tradizionale, ma questo avrebbe creato un precedente per ABI come clearing house, non ben visto dalle banche partecipanti: la scusa della sperimentazione tecnologica è stata invece usata come cavallo di Troia

2.3 Altcoin

Bitcoin Cash: 51% attack

Dopo l'attacco 51%[24] [25] ad Ethereum Classic di cui abbiamo discusso nello scorso report, questo trimestre è stato il turno di Bitcoin Cash. I due principali *mining pool* (*BTC.com* e *BTC.top*) si sono coordinati per cancellare una transazione effettuata da un miner anonimo che spendeva Bitcoin Cash dei quali non aveva possesso sfruttando un bug, subito corretto, del protocollo.

Il dilemma morale di questo attacco è molto forte: se da un lato i pool hanno cercato di ottenere un beneficio per la community, cancellando una transazione "illecita", d'altro lato hanno mostrato la fragilità del network: basta il coordinamento di due pool per poter riscrivere la storia transazionale. È l'ennesima dimostrazione che sono resilienti ad attacchi di questo tipo solo i network con alta potenza computazionale (*hash rate*), con una reale distribuzione di questa potenza tra attori diversi e, soprattutto, con una maggioranza economicamente significativa che rifiuta questi interventi dando maggior valore di mercato alla catena non manipolata. Si veda da questo punto di vista, nella sezione Ecosistema, la reazione della comunità Bitcoin alla richiesta della borsa di scambio *Binance* di riscrivere la storia transazionale per cancellare un furto subito.

> *Sono resilienti ad attacchi di questo tipo solo i network con alta potenza computazionale (hash rate), con una reale distribuzione tra attori diversi di questa potenza e con una maggioranza economicamente significativa che rifiuta questi interventi*

Algorand lancia la sua testnet

Questo trimestre ha visto anche il rilascio della rete pubblica di test per la blockchain di Algorand[26]. Dopo un periodo di test su rete privata, Algorand sta ora invitando aziende e sviluppatori a provare realmente la loro blockchain e fornire feedback sul funzionamento.

Figura 7: Silvio Micali

Algorand è stata disegnata da Silvio Micali, professore del MIT e premio Turing (l'equivalente del premio Nobel per l'informatica), con l'obiettivo di creare una blockchain pubblica più efficiente e scalabile di quelle attualmente disponibili. Gli investimenti iniziali sul progetto sono stati consistenti, circa 66 milioni di dollari, ma il progetto ha incontrato molte difficoltà e reazioni non sempre positive da parte dell'ecosistema, soprattutto per l'assenza di chiarezza sull'algoritmo di consenso *Proof-of-stake* scelto.

Questo rilascio è una importante milestone per il progetto e sarà finalmente una occasione per testare realmente le funzionalità promesse: vi terremo aggiornati sugli sviluppi.

Attacco 51%

Un attacco 51% avviene quando un attore malevolo detiene almeno il 51% della potenza computazionale del network: viene meno il concetto di decentralizzazione perché l'attaccante, potendo riscrivere a piacere la blockchain, decide cosa debba entrare, o non entrare, nella storia transazionale.

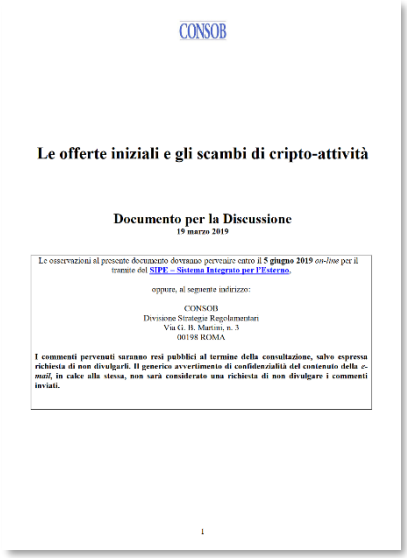
[24] https://twitter.com/TheCryptoconomy/status/1131962447823278080
[25] https://www.coindesk.com/bitcoin-cash-miners-undo-attackers-transactions-with-51-attack
[26] https://business.financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/algorand-publicly-opens-test-net

3. Regolazione

Consob: consultazione sulle ICO

Consob ha lanciato a marzo una consultazione[27] pubblica sulle ICO. L'Istituto ha scelto di contribuire alla risposta del Crypto Asset Lab di Milano-Bicocca, iniziativa di ricerca congiunta di cui potete leggere nella sezione dedicata alla vita dell'Istituto.

La risposta integrale è disponibile online[28], ma si seguito riportiamo una sintesi per punti salienti:


CONSOB

Le offerte iniziali e gli scambi di cripto-attività

Documento per la Discussione
19 marzo 2019

Le osservazioni al presente documento dovranno pervenire entro il **5 giugno 2019** *on-line* per il tramite del SIPE – Sistema Integrato per l'Esterno,

oppure, al seguente indirizzo:

CONSOB
Divisione Strategie Regolamentari
Via G. B. Martini, n. 3
00198 ROMA

I commenti pervenuti saranno resi pubblici al termine della consultazione, salvo espressa richiesta di non divulgarli. Il generico avvertimento di confidenzialità del contenuto della *e-mail*, in calce alla stessa, non sarà considerato una richiesta di non divulgare i commenti inviati.

1

- Il fenomeno delle ICO ha avuto successo perché ha permesso a una significativa liquidità, disponibile nella forma di criptovalute, di diversificare su investimenti non regolamentati.
- Questi capitali sono stati raccolti da start-up che hanno disintermediato gli attori tradizionali come *Venture Capitalist*, banche e regolatori. Sebbene il contesto in cui questo è avvenuto sia discutibile, il fenomeno è indubbiamente interessante: promuovere nuovi canali di finanziamento per le PMI è obiettivo strategico dell'UE nell'ambito della *Capital Markets Union*.
- Queste forme di investimento si prefigurano come *utility token* fondamentalmente per evitare la classificazione di security. Nella gran parte sono state deludenti come investimento, fallimentari come progetto imprenditoriale, talvolta configurandosi persino come vere e proprie frodi. D'altronde non si tratta qui di proibire fenomeni difficilmente contrastabili dal punto di vista tecnologico, né di fornire una alternativa eccessivamente stringente dal punto di vista regolamentare.
- Si tratta piuttosto di consentire la trasparenza e garantire un quadro regolamentare per le registrazioni digitali rappresentative di diritti, negoziate all'interno di uno o più sistemi di scambio. L'investitore beneficerebbe di maggiori tutele se il regolatore fornisse un quadro di riferimento che consenta di identificare le ICO strutturalmente più affidabili.
- L'utilizzo di tecnologia blockchain di per sé non qualifica l'asset scambiato: in particolare blockchain private *permissioned* che identificano le controparti in nulla sembrano diversificarsi dai tradizionali sistemi. Al massimo si potrebbe trattare di una innovazione di processo, neutrale per il regolatore.
- Appare opportuno ribadire invece l'elemento chiave del successo delle ICO: blockchain pubbliche *permissionless*, con controparti che operano sul secondario non necessariamente identificate. Questa sembra essere la ricetta per ottenere liquidità e afflusso di capitali. In questo caso, evidentemente, l'identificazione degli attori può avvenire solo in fase di emissione e ovunque lo scambio coinvolga valute tradizionali a corso legale, per le quali sono già chiariti i presidi in termini di *KYC* (identificazione degli attori) e *AML* (presidi antiriciclaggio).
- In questa sede, noi abbiamo inteso che Consob voglia indirizzare la sua attenzione verso la categoria dei c.d. *hybrid token*, ossia quei token che offrono agli investitori la possibilità di fruire di un servizio o di un bene (*utility token*), implicando però anche un profilo/elemento finanziario (che a sua volta ne giustifica la negoziabilità in un mercato secondario).
- È auspicabile che gli *hybrid token* possano, tramite procedure di *opt-in*, essere offerti su piattaforme regolate ed ottenere quindi la certificazione se capaci di

[27] http://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/64251cef-d363-4442-9685-e9ff665323cf
[28] https://cryptoassetlab.diseade.unimib.it/docs/20190605/Risposta-Consob.pdf

soddisfare alcuni criteri minimi di qualità. Non si tratta di creare presidi per la selezione dei progetti imprenditoriali meritevoli di accedere alle ICO, bensì di verificare che gli investitori abbiano accesso agli elementi per valutare correttamente l'opportunità loro offerta (ad esempio, criteri minimi di completezza per il *white-paper* che descrive la ICO).

- Quanto alle piattaforme per le offerte di crypto-attività ci sembra fondamentale chiarire l'equivoco tra queste e le blockchain. Le piattaforme di offerta possono costituirsi con tecnologie diverse (ad esempio anche semplici portali web): sono i token che per venire a esistenza devono alla fine essere registrati su una blockchain.
- In particolare, le ICO che volessero una approvazione regolamentare dovrebbero dare garanzie quanto a:
    - forma giuridica di società per l'emittente, per poter valutare esplicitamente quali garanzie di capitali (pur ridotte) e responsabilità possano essere fornite;
    - logiche di emissione, per evitare inflazionabilità arbitraria del token;
    - connessione con un chiaro e individuato progetto imprenditoriale;
    - criteri di redistribuzione della profittabilità del progetto sponsorizzato dall'emittente, specificando i diritti incorporati nei token.
- Potrebbe essere in carico ai gestori delle piattaforme di offerta la richiesta ai soggetti emittenti di tutte le informazioni necessarie e la loro valutazione.
- Con riferimento al mercato secondario permane l'equivoco tra blockchain e piattaforme di scambio. Le piattaforme di scambio, per essere efficienti, non sono sostanzialmente mai blockchain e possono essere regolate con identificazione degli attori, presidi antiriciclaggio e di contrasto al finanziamento del terrorismo; viceversa, le blockchain (pubbliche o private che siano) sono intrinsecamente inefficienti per il trading in quanto tecnologie distribuite e nella loro versione pubblica *permissionless* (l'unica finora esistente) non possono essere regolate.
- In fase di secondario sarebbero opportune regole di condotta che le piattaforme di scambio devono essere tenute a rispettare nel rapporto con gli investitori, di nuovo tramite *opt-in*. Le garanzie che dovrebbero essere fornite per qualificarsi includono:
    - continuità e sicurezza informatica circa l'operatività della piattaforma;
    - trasparenza sulle metodologie di custodia e le coperture assicurative collegate. Qui sarebbe da auspicare l'emergere di un processo di custodia aperto e standardizzato, che possa essere sottoposto all'audit di terze parti.
- Sembra essenziale per la liquidità del secondario consentire la contrattazione anche su blockchain pubbliche *permissionless*, altrimenti sarebbe snaturata la caratteristica innovativa delle ICO, diminuendone l'*appeal*.

Europol chiude un servizio di coinmixer

Il *Fiscal Information and Investigation Service* (FIOD) olandese in collaborazione con l'Europol, ha fatto chiudere Bestmixer.io[29], accusato di essere uno dei principali servizi di riciclaggio basato sull'utilizzo di cryptocurrency.

Bestmixer.io era attivo da circa un anno e supportava Bitcoin, Bitcoin Cash e Litecoin: in questo periodo ha raggiunto volumi considerevoli, anonimizzando almeno 200 milioni di dollari. L'anonimizzazione, chiamata in gergo tecnico *crypto-mixing*, si basa sulla raccolta di fondi crypto da diversi attori e tramite una moltitudine di transazioni riesce a far perdere le tracce del reale possessore.

[29] https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

4. Ecosistema

Bitfinex accusata di aver perso 850 milioni di dollari

Bitfinex, uno dei più grandi *crypto exchange* al mondo, è stato citato in giudizio dal procuratore generale di New York Letitia James[30], per aver nascosto una perdita di 850 milioni di dollari usando i fondi a riserva dello *stable-coin* Tether, posseduto da una sua affiliata, Tether Limited. La causa è ufficialmente emessa contro iFinex Inc., la holding che controlla sia Bitfinex sia Tether Limited.

Secondo la procura, Bitfinex avrebbe spostato 850 milioni di dollari, posseduti da clienti e corporate, senza nessuna autorizzazione scritta, ad una società con sede a Panama chiamata Crypto Capital Corp. Al fine di nascondere questa perdita, Bitfinex avrebbe utilizzato le riserve in dollari poste a *collateral* dello *stable-coin* Tether[31], appartenenti a Tether Limited.

Stable-coin e Tether

Tether è uno *stable-coin,* cioè un coin con valore fissato (in questo caso 1:1 col dollaro statunitense) tramite la garanzia di una riserva di valore posta a collaterale. Tether è emesso dall'omonima società, Tether Limited, posseduta da una holding di cui fa parte anche l'exchange Bitfinex.

Tether è nata soprattutto per facilitare gli arbitraggi tra i diversi exchange, fornendo un equivalente digitale del dollaro facilmente trasferibile fra le diverse piattaforme di scambio senza le complicazioni e lentezze dei tradizionali sistemi di pagamento.

Ad oggi la capitalizzazione di Tether è superiore ai 4 miliardi di dollari, collocandola tra le prime 10 crypto currency attualmente disponibili sul mercato.

Questa causa ha fatto emergere chiaramente i dubbi sulla reale collateralizzazione di Tether. Infatti, nonostante le dichiarazioni ufficiali, i dollari posti a riserva per garantire la stabilità del valore di Tether (USDT) non sarebbero sufficienti, configurandosi quindi come una riserva frazionaria. A seguito di questa evidenza Tether Limited ha aggiornato il proprio sito dichiarando che le riserve coprono il 100% dei Tether emessi, ma potrebbero non essere tutte in fiat-currency[32]: *"Every tether is always 100% backed by our reserves, which include traditional currency and cash equivalents and, from time to time, may include other assets and receivables from loans made by Tether to third parties, which may include affiliated entities[33]".*

> *I dollari statunitensi posti a riserva per garantire la stabilità del valore di Tether (USDT) non sarebbero sufficienti, configurandosi quindi come una riserva frazionaria.*

Questa pratica di Bitfinex di usare fondi derivanti dall'emissione di nuovi Tether per coprire le proprie perdite non sarebbe nuova, già in passato in situazioni di pressione economica avrebbe utilizzato questo stratagemma per superare le criticità. I dubbi circa la solidità e correttezza di uno degli exchange più grandi nel mondo crypto, emersa poco dopo i risultati del report Bitwise circa la veridicità dei volumi di scambio dichiarati dagli exchange (vedi sezione Mercato) non fanno altro che confermare la poca trasparenza e affidabilità del mondo finanziario crypto.

Bitfinex in una nota ufficiale ha smentito le accuse dichiarando che gli 850 milioni di dollari sotto accusa sono stati in realtà spostati a Crypto Capital Corp esclusivamente per motivi di custodia sicura: *"The New York Attorney General's court filings were written in bad faith and are riddled with false assertions, including as to a purported $850 million "loss" at*

[30] https://ag.ny.gov/press-release/attorney-general-james-announces-court-order-against-crypto-currency-company-under
[31] https://www.coindesk.com/bitfinex-ny-prosecutors-tether-850-million-allege
[32] https://www.coindesk.com/tether-says-its-usdt-stablecoin-may-not-be-backed-by-fiat-alone
[33] https://tether.to/

Crypto Capital. On the contrary, we have been informed that these Crypto Capital amounts are not lost but have been, in fact, seized and safeguarded."

Rubati 700,000 Bitcoin a Binance

Il 7 maggio Binance, uno dei più grandi exchange crypto per volumi, ha subito un attacco che ha causato la perdita di 7,000 Bitcoin[34], per un controvalore di 40 milioni di dollari.

Gli hacker hanno sfruttato una falla nei sistemi di sicurezza riuscendo a raggiungere gli hot wallet (che secondo le dichiarazioni ufficiali detengono il 2% dei Bitcoin totali) e a disporre una richiesta di prelievo verso indirizzi posseduti dagli attaccanti.

La reazione da parte di Binance non si è fatta attendere: il CEO Changpeng Zhao ha tentato di raggiungere un accordo con i miner per cancellare dalla blockchain la transazione con il furto. La comunità Bitcoin si è subito espressa contro questa possibilità, manifestando tutta la propria contrarietà: il danno subito in termini di reputazione e valore economico che Bitcoin avrebbe subito da questa mossa sarebbe stato molto superiore al furto a Binance. A fronte di questa levata di scudi, Changpeng Zhao ha poi annunciato sul suo profilo Twitter la decisione di non procedere ulteriormente su questa strada[35].

> *Changpeng Zhao, CEO of Binance, ha dichiarato di valutare la possibilità di raggiungere un accordo con i miner per cancellare la transazione con il furto dalla blockchain. La comunità Bitcoin si è subito espressa vigorosamente contro questa possibilità*

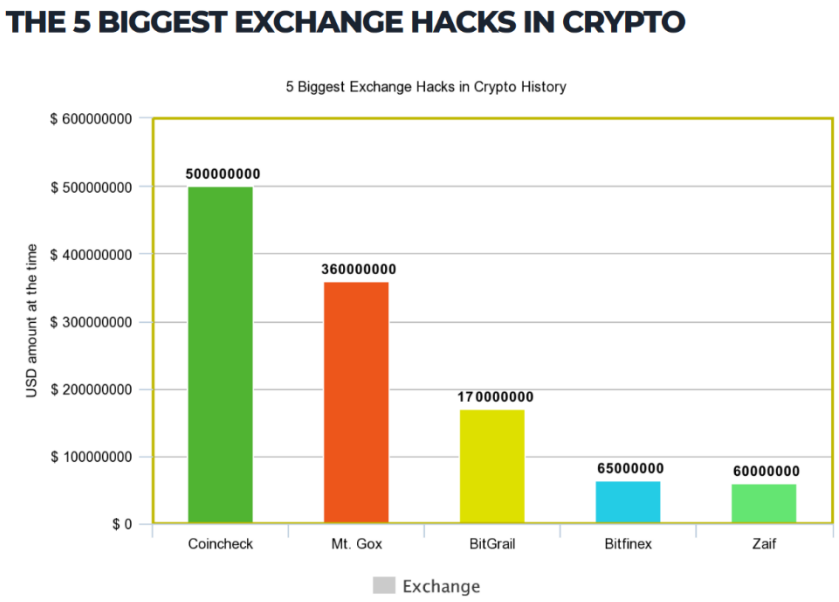


Figura 8: 5 maggiori furti a crypto exchange. *(fonte: bitcoinist.com)*

Nonostante la rilevanza economica di questo furto, è interessante notare come non si collochi nemmeno trai i primi 5 furti ad exchange[36]. Il più grande furto rimane quello a Coincheck avvenuto nel gennaio 2018, quando furono rubati più di 500 milioni di dollari in cryptocurrency. Al secondo posto si colloca il celebre furto del febbraio 2014 a Mt Gox, dove vennero rubati 200,000 Bitcoin per un controvalore, al momento del furto, di 360 milioni.

Local Bitcoin rimuove le transazioni in contanti

Local Bitcoin ha rimosso dalle opzioni della sua piattaforma la possibilità di effettuare scambi tra i suoi utenti di contanti contro Bitcoin[37]. Il cambiamento è radicale,

[34] https://cointelegraph.com/news/hackers-withdraw-7-000-bitcoins-in-binance-crypto-exchange-security-breach
[35] https://twitter.com/cz_binance/status/1125996194734399488?
[36] https://bitcoinist.com/top-5-biggest-crypto-exchange-heists-in-history/
[37] https://www.coindesk.com/localbitcoins-removes-cash-for-crypto-trading-option

specialmente tenendo conto che Local Bitcoin era nata proprio come piattaforma di incontro diretto tra venditori e compratori per evitare le procedure di Know Your Customer (KYC) e Anti Money Laundering (AML).

Questa modifica nel funzionamento della piattaforma arriva poco dopo l'introduzione di procedure di autenticazioni dei clienti più stringenti[38] e si colloca nel solco del maggior controllo che le autorità stanno imponendo per contrastare le attività di riciclaggio.

Custody di Asset digitali

Tra le applicazioni sempre più richieste negli ultimi mesi (e per questo ad alto potenziale di crescita) c'è sicuramente la custodia di asset digitali. Scambiare criptovalute sul mercato è diventato più semplice grazie ad un numero crescente di borse che offrono interfacce applicative per l'utente sempre più versatili. Quando invece si arriva ad affrontare il problema della gestione sicura, specialmente su orizzonti temporali medio-lunghi, la situazione si complica. Ad oggi infatti non esistono ancora *custodian* affidabili e regolamentati, accessibili anche agli investitori istituzionali. Ad esempio, è proprio per questo motivo che la SEC continua a bloccare le richieste di emissione di ETF su Bitcoin.

Non sorprende quindi che anche grandi attori del mercato digitale come Samsung inizino ad investire in questa direzione. È notizia di aprile, infatti, l'investimento di 3 milioni di euro in Ledger, società specializzata nello sviluppo di soluzioni hardware per i wallet[39], cioè per gli strumenti (tipicamente software) utilizzati nella gestione delle chiavi private.

Bakkt, in collaborazione con ICE, sta cercando invece di introdurre sul mercato Bitcoin *futures* con consegna del sottostante (*physically delivered*). Per ottenere l'approvazione deve smarcare le tematiche di custody: i Bitcoin sottostanti i contratti *futures* dovranno essere depositati presso un *custodian* regolato. In un messaggio[40] di Adam White, COO di Bakkt, viene presentata ad alto livello la soluzione pensata per ottenere l'approvazione: prevede, come tutte le altre soluzioni già presenti sul mercato, l'utilizzo distinto di *hot* (*online*) e *cold* (*offline*) wallet e la presenza di una polizza assicurativa di $100 milioni a copertura dei rischi ed offerta da un leader globale del mondo assicurativo. Le chiavi privati dei wallet saranno detenute tramite *hardware wallet*, distribuiti geograficamente e depositati in casseforti controllate 24/7. Per sviluppare questa soluzione hanno acquisito la società DACC (Digital Asset Custody Company), da tempo attiva sui temi di custody.

Per ribadire il ruolo fondamentale che la presenza di custodian regolati avrà nello sviluppo dell'ecosistema, non possiamo che ribadire la conclusione del messaggio di Adam White: "launching a regulated custodian for digital asset represents a key milestone".

Figura 9: Adam White

Per ribadire il ruolo fondamentale che la presenza di *custodian* regolati avrà nello sviluppo dell'ecosistema, non possiamo che ribadire la conclusione del messaggio di Adam White: *"launching a regulated custodian for digital asset represents a key milestone"*.

[38] https://localbitcoins.com/blog/aml-features-update/
[39] https://www.coindesk.com/samsung-invests-2-9-million-into-crypto-hardware-startup-ledger
[40] https://medium.com/bakkt-blog/custody-at-our-core-15f6b26d16d6

Libra: la moneta promossa da Facebook

La notizia principale del trimestre è senza alcun dubbio l'annuncio di *Libra*[41], il *coin* promosso da Facebook attraverso la Libra Association[42], che dovrebbe arrivare nel primo semestre 2020. Si tratta di un evento estremamente significativo perché "sdogana" definitivamente l'idea che sia possibile e persino realistico trasferire valore attraverso strumenti di scambio digitali emessi da privati.

Durante l'annuncio sono stati presentati il white paper[43] che descrive Libra, la Libra Association, il primo wallet *custodian* per Libra coin sviluppato da Facebook chiamato Calibra[44] e la rete di test per gli sviluppatori. Una analisi del codice sorgente di Libra fatta da Jameson Lopp[45] ha rilevato come in realtà non si possibile ad oggi sincronizzare veramente un *full node* e interagire con il codice sorgente; di fatto Libra fornisce per ora solo una interfaccia (API) che permette solo di effettuare richieste a un *full node*.

Per spiegare meglio Libra e la sua relazione con Bitcoin e le altre criptovalute, abbiamo provato a rispondere ad alcune domande comuni sull'argomento.

Che differenza c'è tra Bitcoin e Libra, il coin di Facebook?

Bitcoin vuole essere l'equivalente digitale dell'oro: scarsità in ambito digitale incensurabile, non controllata da nessuno, decentralizzata. Libra sarà, invece, una soluzione centralizzata controllata dalla Libra Association, una no-profit costituita in Svizzera da Facebook ed i suoi partner. Nell'associazione sono presenti tra gli altri: Mastercard, Visa, PayPal, Vodafone, Uber, Spotify, Andreessen Horowitz, Coinbase, Xapo, Stripe; mancano invece le banche e le grandi aziende tecnologiche che competono con Facebook.

Libra	con questo termine si indica il protocollo che sta alla base del funzionamento della cryptovaluta
Libra coin	primo asset emerso sul protocollo Libra; la cryptovaluta globale che punta alla stabilità dei prezzi rispetto a un paniere di riferimento
Libra Association	si riferisce alla associazione no-profit che sta alle spalle del protocollo ed è responsabile del processo di validazione delle transazioni e dello sviluppo. Al momento fanno parte di questa associazione 28 società, tra cui Mastercard, Visa, Paypal, Vodafone, Illiad, ect..
Calibra	primo custodian-wallet sviluppato per custodire e transare i Libra coin. Questo wallet è sviluppato da una subsidiary di Facebook e conterrà tutte le necessario procedure di KYC e AML previste dal regolatore. Al momento non sono disponibili altri wallet.

Libra è una criptovaluta?

Utilizza tecniche crittografiche ed un network peer-to-peer, soddisfa quindi i requisiti che il senso comune attribuisce al concetto di criptovaluta. Ha anche l'ambizione di essere *permissionless*, ma il controllo centralizzato avrà molte sfide, sia in termini di governo della piattaforma (cosa succede in caso di contrasti tra i partner?) che di requisiti regolamentari (ad esempio, il rispetto della normativa antiriciclaggio e di contrasto al finanziamento del terrorismo). Preoccupa, inoltre, il tema della privacy, su cui già in passato Facebook ha avuto episodi pessimi: è inquietante l'idea che domani possa conoscere anche tutte le nostre transazioni finanziarie.

Come si potrà utilizzare Libra?

[41] https://www.coindesk.com/facebook-launches-subsidiary-to-support-new-libra-crypto
[42] https://libra.org/en-US/
[43] https://libra.org/en-US/white-paper/#introduction
[44] https://calibra.com/
[45] https://twitter.com/lopp/status/1140976191182180353?s=19

Per ora sappiamo che dovrebbe essere una criptovaluta non speculativa, perché con valore stabile grazie a riserve in valute e titoli di stato. Mira ad essere una moneta globale, sfruttando gli oltre 2 miliardi di utenti Facebook, utilizzabile per i pagamenti e le rimesse internazionali, integrata anche nei sistemi di messaggistica come WhatsApp e Messenger. Il lancio è previsto per il primo semestre 2020, sempre che i regolatori internazionali non si oppongano o rallentino/snaturino il progetto.

Cosa cambia con l'arrivo di Libra?

Potrebbe smarcare definitivamente la diffidenza verso le cosiddette criptovalute ed in generale le forme digitali e private di trasferimento del valore, ponendo fine al "paleolitico" delle transazioni finanziarie lente (anche oltre due giorni), costose, costrette in definiti confini nazionali o valutari. E questo potrebbe avvantaggiare anche Bitcoin, che di suo aggiunge il non essere inflazionario (non è creato per perdere valore in termini di potere d'acquisto): Libra moneta transazionale, stabile nel potere di acquisto ed utile per i pagamenti, Bitcoin bene rifugio incensurabile, attraente dal punto di vista speculativo. Perdono invece terreno R3, PayPal, SatisPay, le alt-coin con ambizioni velleitarie come Bitcoin Cash, Ripple, LiteCoin, Tether ed in generale gli *stable coin*. Anche Lightning Network, se inteso come piattaforma per un Bitcoin transazionale, potrebbe soffrire della concorrenza di Libra.

Libra potrebbe smarcare definitivamente la diffidenza verso le cosiddette criptovalute ed in generale le forme digitali e private di trasferimento del valore, ponendo fine al "paleolitico" delle transazioni finanziarie lente (anche oltre due giorni), costose, costrette in definiti confini nazionali o valutari.

Se arriva Libra che bisogno c'è di Bitcoin?

Oggi Libra non ci sarebbe se la strada non l'avesse aperta Bitcoin dieci anni fa. E di Bitcoin c'è bisogno come e più di prima, se si comprende il suo ruolo nella storia della moneta: bene di riserva che si potrà utilizzare a garanzia di nuove monete private. Il punto debole di Libra, oltre alla censurabilità, sono proprio le riserve a garanzia, denominate in valute inflazionarie che perdono valore: qualcuno, infatti, parla già della possibilità di includere anche Bitcoin.

Il regolatore consentirà a Facebook di battere moneta?

Per ora abbiamo visto una levata di scudi: il ministro del Tesoro francese ha chiesto a G7 e G20 di intervenire, il governo giapponese ha costituito subito una commissione di studio, negli Stati Uniti governo e diversi parlamentari hanno manifestato preoccupazione e contrarietà. Il quadro non è però omogeneo: pur rimarcando la necessità di una regolazione, *Bank of England* si è dichiarata disponibile a fare da custode per le riserve a garanzia di Libra.

Di Bitcoin c'è bisogno come e più di prima, se si comprende il suo ruolo nella storia della moneta: bene di riserva che si potrà utilizzare a garanzia di nuove monete private

Come andrà a finire?

Difficile dirlo oggi, ma siamo senza alcun dubbio in un momento storico, una svolta decisiva. Non solo, evidentemente, se Libra dovesse partire; ma anche se dovesse essere bloccata: si dovrà infatti chiarire chi può fermare una no-profit svizzera dal fare quello che da un decennio si fa con Bitcoin, e con quali ragioni la si fermerà. Ma è certo che il dollaro statunitense non può amare un contendente sovranazionale che possa indebolire il suo ruolo come asset di riserva internazionale.

Approfondimento tecnico su Libra

Analizziamo più nel dettaglio il funzionamento del protocollo.

Struttura Libra blockchain

La Libra blockchain è un "*cryptographically authenticated database*", mantenuto e aggiornato tramite le regole definite dal *Libra protocol*. Questo database può contenere al suo interno diverse risorse, asset, uno dei quali, nonché l'unico per il momento, è il Libra coin.

Tutte le informazioni sulle transazioni sono inserite in un singolo database, i cui stati sono individuati da un numero di versione, definito come *ledger*. A ogni nuova validazione viene aggiornato il numero di versione di riferimento, che allo stesso tempo indica anche il numero di transazioni eseguite fino a quel momento. Per poter validare nuove transazioni ogni validatore deve conoscere lo stato del ledger nell'ultima versione.
La struttura del database non è quindi a blocchi: *"There is no concept of a block of transactions in the ledger history".* I blocchi vengono solo funzionalmente utilizzati in fase di validazione delle transazioni, quando viene creato un blocco virtuale contenente un insieme di transazioni da validare, *"The consensus protocol batches transactions into blocks as an optimization and to drive the consensus protocol".*
La struttura dati del protocollo Libra è invece organizzata con un *Merkle-Tree*, soluzione che permette di ottimizzare le performance in fase di verifica della validità del database.
Il data model utilizzato da Libra prevede una struttura *account-based*, differente quindi da quella di Bitcoin che è *UTXO-based* (*Unspent Transaction Output*), ma similare ad esempio a quella utilizzata da Ethereum. Ogni account è generato tramite una coppia chiave privata chiave pubblica, dove l'hash della chiave pubblica indica l'indirizzo dell'account. Per spendere i fondi associati a un account è necessario firmare digitalmente la transazione con la corrispondente chiave privata.
Da questo punto di vista Libra è pseudonimo: un account non è riferito a una identità nel mondo reale. Un utente è libero di creare multipli accounts.

Transazioni

Per aggiornare lo stato della blockchain i client creano le transazioni. Una transazione consiste in una sequenza di istruzioni (scritte nello *scripting language* di Libra, chiamato *Move*), l'indirizzo del destinatario, l'ammontare e la firma digitale del possessore dei coin spesi.
I validatori eseguono lo script e tutte le informazioni presenti nella transazione e se l'esecuzione ha successo la transazione è valida. Per l'esecuzione dello script i validatori vengono remunerati ricevendo unità di "gas", similmente a quanto avviene per Ethereum. In ogni transazione viene specificato il prezzo in Libra coin di ogni unità di gas.
L'introduzione delle *fee* serve per ridurre la pressione nei momenti di forte stress. Durante l'operatività normale il livello di fee sarà molto basso: *"The system is designed to have low fees during normal operation, when sufficient capacity is available".*

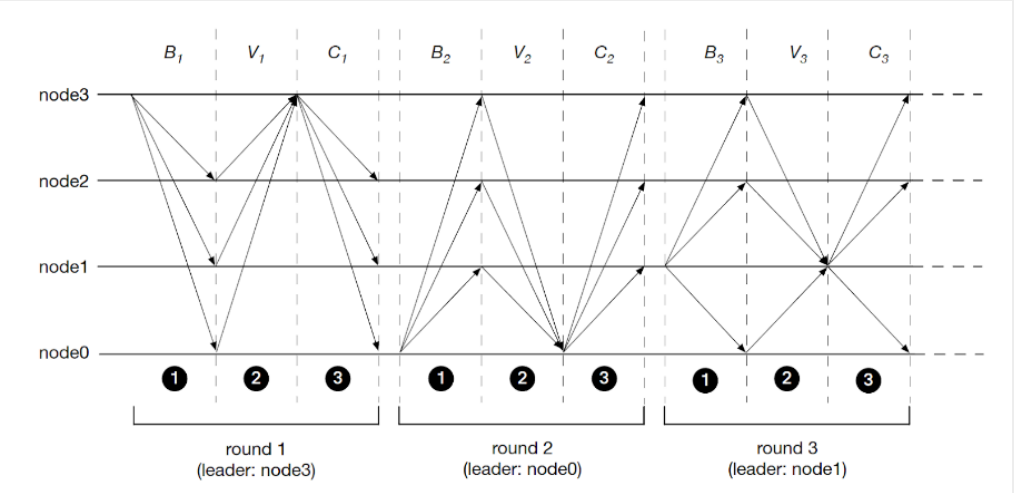
Ogni transazione è un messaggio firmato con la chiave pubblica del mittente contenente:

- Indirizzo del mittente: usato per verificare la disponibilità di fondi;
- Chiave pubblica del mittente: usata per verificare la firma digitale;
- Program: sequenza di comandi in linguaggio "Move" da eseguire per verificare la transazione;
- Gas Price: prezzo in Libra coin di ogni unità di gas;
- Gas massimo: unità di gas utilizzabili al massimo dalla transazione prima di essere annullata;
- Numero di sequenza: numero utilizzato per versionare la transazione ed evitare la doppia spesa.

Consenso

Libra utilizza un algoritmo di consenso definito LibraBFT. Tale algoritmo garantisce il raggiungimento del consenso, prevenendo doppia spesa e fork, a patto che al massimo *f* validatori siano fraudolenti su un totale di *3f + 1*
I validatori che possono aggiornare il database transazionale fanno parte di un gruppo di 28 società facente parte della Libra Association.
La struttura logica di validazione delle transazioni, e quindi di aggiornamento del database distribuito, può essere riassunta nei seguenti passaggi:

1. A turno uno dei validator agisce da leader e propone un blocco di transazioni da validare a tutti gli altri validatori;
2. Gli altri validatori eseguono le transazioni proposte dal leader e se d'accordo mandano un voto di approvazione (tramite firma digitale) al leader;
3. Il "leader" raccoglie tutti i voti favorevoli e se i voti sono superiori a *2f + 1,* il quorum è raggiunto e viene propagata la conferma a tutti gli altri validatori
4. La validazione dell'ultimo stato del database implicitamente valida tutti gli stati precedenti
5. Viene scelto il nuovo leader



5. News dall’Istituto

Intervista con Deloitte

In collaborazione con il nostro partner Deloitte, abbiamo realizzato una lunga intervista a Ferdinando Ametrano sul tema Bitcoin.

L'intervista, a cura di Nicole Vismara (manager di Deloitte Consulting), è suddivisa in 11 parti ed è pensata per dare una introduzione approfondita sul mondo Bitcoin affrontando diversi temi, dal mondo della regolazione fino alla parte più speculativa, attraverso approfondimenti di natura più tecnica su funzionamento e privacy e con un occhio critico sulle possibili applicazioni della tecnologia Blockchain.

L'intervista è disponibile sul nostro canale YouTube[46], mentre nella sezione news del nostro sito è possibile trovare la trascrizione integrale[47].

Btclib

Il trimestre ha visto anche il rilascio[48] della nuova versione della **btclib**, la libreria open-source python sviluppata e manutenuta dal Digital Gold Institute. **btclib** è nata con finalità didattiche per i corsi *Bitcoin and Blockchain Technology*[49] tenuti da Ferdinando Ametrano all'Università Milano-Bicocca e al Politecnico di Milano. La libreria è principalmente focalizzata sull'implementazione della crittografia su curva ellittica utilizzata da Bitcoin. La libreria adotta la licenza MIT e per questo motivo può essere utilizzata da chiunque senza nessuna limitazione.

In questa nuova release, v2019.6.12, è stata aggiunta la documentazione generata automaticamente del codice[50] ed è possibile firmare messaggi generici (non transazioni) utilizzando l'encoding previsto per questo nel protocollo Bitcoin.

Presentazione del *Crypto Asset Lab*

Il 5 giugno si è tenuto il workshop di presentazione del *Crypto Asset Lab* (CAL), iniziativa di ricerca congiunta con l'Università degli Studi di Milano-Bicocca[51].

Il CAL è un osservatorio focalizzato sul tema dei crypto-asset come opportunità di investimento, innovazione fintech e sfida regolatoria. Allo stesso tempo si occupa di ricerca in ambito crittografico e studio della tecnologia blockchain e delle sue applicazioni non monetarie, principalmente la marcatura temporale. La *faculty* del CAL è composta, oltre che da Ferdinando Ametrano e Paolo Mazzocchi del Digital Gold Institute, da professori dell'università Milano-Bicocca: Fabio Bellini, Paolo Bongini, Gianfranco Forte e Francesca Mattassoglio. Il CAL può inoltre vantare un prestigioso *Advisory Board* con la partecipazione di Gregorio De Felice (*Chief Economist* di Intesa Sanpaolo), Paolo Gianturco (*Senior Partner* di Deloitte Consulting), Antonella Sciarrone Alibrandi (Vicerettore dell'Università Cattolica del Sacro

[46] https://www.youtube.com/playlist?list=PLTLa2tRY91LKw5CrWIFFeIws08Sr7q-jC
[47] https://dgi.io/2019/06/17/intervista-bitcoin-01.html
[48] https://dgi.io/2019/06/12/btclib-release.html
[49] https://www.ametrano.net/courses/
[50] https://btclib.readthedocs.io/en/latest/
[51] https://dgi.io/2019/05/10/cryptoassetlab.html

Cuore), Valentina Sidoti (*Head of Global Buy-Side & Market Analysis and Italian Regulation* di Borsa Italiana) e Angelo Tantazzi (fondatore e presidente di Prometeia).

L'evento di presentazione del CAL è stato caratterizzato da una numerosa e vivace partecipazione da parte di diversi esponenti dell'ecosistema Blockchain e Crypto Asset. Il programma dettagliato degli interventi con le relative slide è online sul sito del Crypto Asset Lab[52]. Visto il successo dell'iniziativa, diamo già appuntamento a giugno 2020 per la seconda edizione del workshop, quando si potranno anche tirare le somme del primo anno di attività del Lab.

Webinar su sostenibilità economica e ambientale di Bitcoin

Il Digital Gold Institute è stato invitato da Harvard Extension Students Environment Club[53] alla realizzazione di un webinar sulla sostenibilità economica e ambientale di Bitcoin, temi molto delicati e spesso affrontati senza il dovuto livello di dettaglio. Il video del webinar è disponibile sul canale YouTube[54] dell'Istituto, mentre le slide sono pubblicate sul nostro sito internet[55].

Report di analisi dei volumi di The Rock Trading

Nello scorso report trimestrale avevamo presentato i risultati del report che Bitwise aveva presentato alla SEC per proporre il suo ETF Bitcoin. In questo report venivano analizzati i volumi dichiarati dagli exchange e dalla loro analisi emergeva come la maggioranza di essi pubblicasse volumi fittizi e artificiosamente gonfiati.

Sull'onda di questi risultati abbiamo deciso di analizzare i volumi pubblicati da The Rock Trading, il più longevo exchange Bitcoin ancora operativo, con base in Italia. Dalle nostre analisi è emerso come i volumi dichiarati da TRT siano affidabili, confermando l'affidabilità di questa borsa di scambio. Il report con tutti i risultati dettagliati è disponibile sul nostro sito[56].

[52] https://cryptoassetlab.diseade.unimib.it/2019/06/12/workshop.html
[53] https://hesec.extension.harvard.edu/webinars
[54] https://www.youtube.com/watch?v=36slArIgsbw
[55] https://dgi.io/docs/2019-05-13-hesec-webinar.pdf
[56] https://dgi.io/docs/2019-04-23-trt-volumes.pdf

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 crypto-asset) 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