n. 2

Digital Gold Institute

Scarcity in the Digital Realm

Report Trimestrale

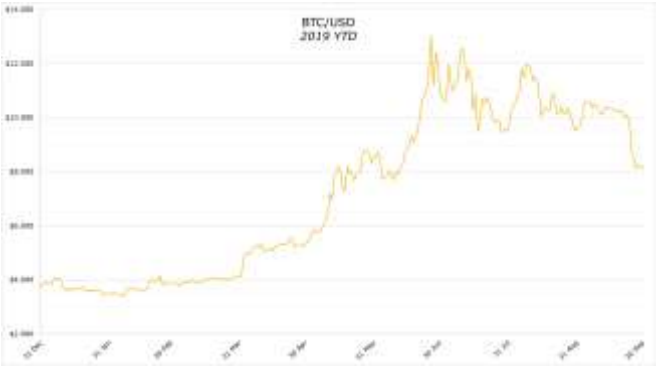
2019-Q3

Editoriale

Questo trimestre è stato caratterizzato dalle vicende legate a Libra, la valuta dell'omonimo consorzio promosso da Facebook. Nella sezione dedicata alla regolazione commentiamo (con qualche punta di provocazione intellettuale) quella che ci sembra una vicenda straordinariamente rivelatoria: il monopolio governativo della moneta è una delle trincee più calde della battaglia culturale liberale e libertaria. Se pensiamo a quanto travagliata è stata la separazione storica della Chiesa dallo Stato, possiamo avere idea di quanto sarà impervia e controversa la separazione tra Moneta e Stato. Ex-post sembrerà a tutti una ovvia conquista di civiltà e libertà, di cui beneficeranno sia la Moneta che lo Stato, ma ad oggi la "sovranità monetaria delle nazioni" è un paradigma che preserva l'ultimo tra i monopoli logicamente indifendibili.

Se pensiamo a quanto travagliata è stata la separazione storica della Chiesa dallo Stato, possiamo avere idea di quanto sarà impervia e controversa la separazione tra Moneta e Stato

Il fronte dei servizi finanziari per crypto-assets continua a presentare spunti di vivacità: questo trimestre ha debuttato il molto atteso contratto *futures* di Bakkt, caratterizzato da *physical delivery*, differentemente dal cugino di CME che è invece *cash settled*. La partenza è stata senza particolari trionfalismi, in linea con un trimestre in cui Bitcoin ha registrato una pesante performance negativa: il prezzo ha perso il -25% portando il rendimento dall'inizio dell'anno a +97%. Gli alt-coin si sono accodati, senza alcun velleitarismo, con la solita altissima correlazione che li rende sostanzialmente inutili anche dal punto di vista di diversificazione del rischio finanziario.



Rendimento Bitcoin da inizio 2019

Il fronte che a noi sembra invece più promettente nell'ambito della nuova finanza per l'economia bitcoin e blockchain è quello dei servizi di custodia per crypto-assets, cruciale per l'ingresso nel mercato di investitori istituzionali e *high-net-worth individuals*: Coinbase, leader di mercato, ha acquisito il business istituzionale di Xapo; Bryan Bishop propone tecniche avanzate di *self-custody*. Il nostro istituto sta seguendo questi sviluppi con grande attenzione e sono imminenti novità della nostra ricerca che potrebbero avere una significativa rilevanza industriale.

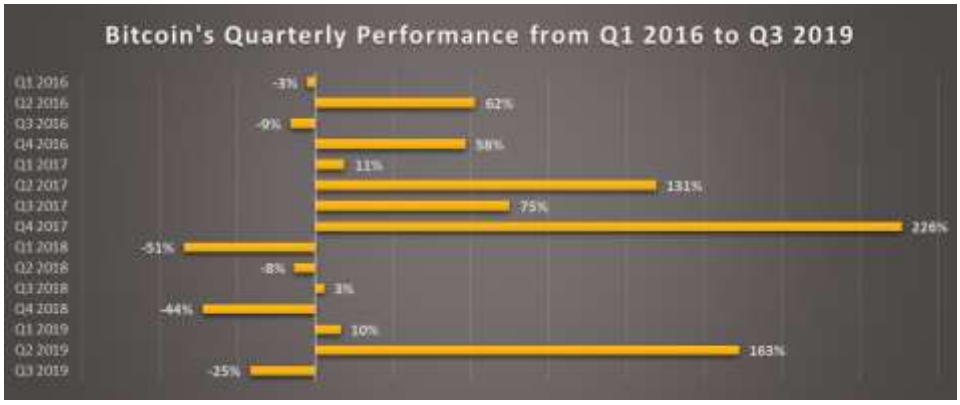
Nel frattempo, lo sviluppo del protocollo Bitcoin prosegue la sua strada, sostanzialmente incurante tanto del dibattito regolamentare, quando delle dinamiche di prezzo. Nel nostro piccolo abbiamo contribuito sostenendo come Crypto Asset Lab (la joint-venture tra il nostro Istituto e l'Università Milano-Bicocca) la conferenza *Scaling Bitcoin* questo settembre a Tel Aviv. Scaling Bitcoin resta a nostro avviso il punto di riferimento tecnico a livello internazionale e siamo orgogliosi di essere "academic supporting organization" assieme a Stanford, MIT, Imperial College ed altre prestigiose università.

Indice

1. Mercato

Performance Bitcoin

Il terzo trimestre del 2019 ha visto una interruzione della corsa rialzista che aveva caratterizzato il trimestre precedente.



Il risultato negativo di questo periodo è stato fortemente condizionato dal crollo del prezzo che si è registrato nell'ultima settimana di settembre, in modo particolare nella giornata del 24 settembre[1] con un calo superiore all'11%. Il giorno precedente erano stati lanciati i *futures* contrattati su Bakkt (gruppo ICE, New York Stock Exchange), che a differenza di quelli scambiati su CME sono *physically settled*, cioè regolati a scadenza con la consegna effettiva del sottostante invece che *cash*. Nonostante fossero attesi da molto tempo, l'accoglienza del mercato è stata al di sotto delle attese e questo secondo alcuni analisti, potrebbe aver innescato il declino[2] nel prezzo.

Nonostante il ritracciamento, le aspettative di crescita rimangono positive. Un report pubblicato da Greyscale Investment[3], la più grande società di asset manager nel mondo crypto, ha evidenziato come il 36% degli investitori statunitensi sia interessato a investire in Bitcoin come modo per diversificare il portafoglio; questo numero porterebbe a un significativo aumento rispetto agli attuali utenti, con un evidente effetto positivo sulla quotazione.

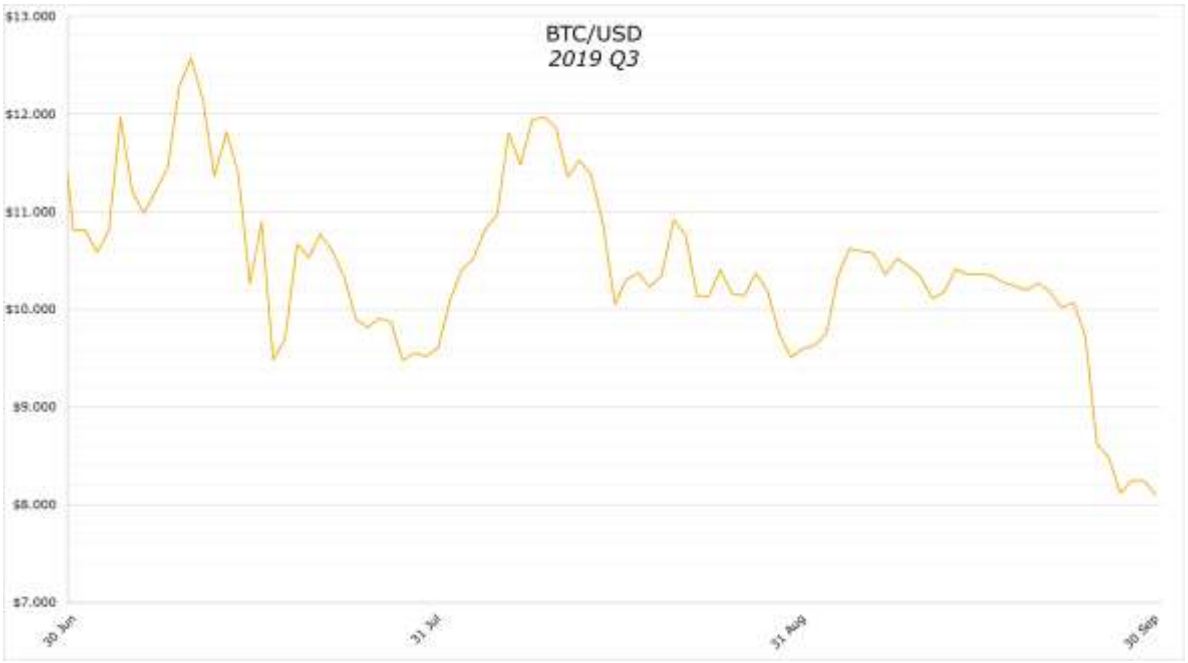


Figura 1: rendimento Bitcoin secondo trimestre 2019

[1] https://www.forbes.com/sites/ktorpey/2019/09/24/bitcoin-price-collapses-by-more-than-15-in-an-hour/#5672cb0462ca
[2] https://www.iol.co.za/business-report/technology/four-reasons-for-bitcoins-20-price-drop-in-the-past-month-luno-33962114
[3] https://dropgold.com/bitcoin-investor-report/

Un altro interessante punto di analisi, emerso sempre più in quest'ultimo periodo, è l'idea che bitcoin possa identificarsi come un bene rifugio al pari dell'oro[4]. Come evidenziato dagli analisti di Bloomberg, sembrerebbe infatti che nell'ultimo anno e in modo particolare negli ultimi mesi la correlazione tra il prezzo di bitcoin e quello dell'oro sia salita considerevolmente, arrivando a punte di 0,827 se ci si limita agli ultimi 3 mesi.

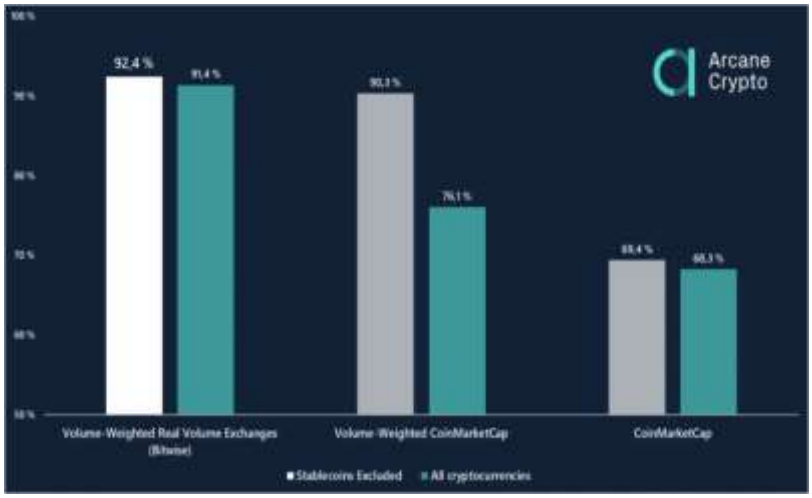


Figura 2: Market dominance di Bitcoin rispetto agli altcoin

È importante ricordare che il mercato, a differenza di quanto si potrebbe desumere dalla "Market Capitalization" degli alt-coin, è sempre più dominato da Bitcoin. Una analisi combinata basata su volumi di scambio e capitalizzazione di mercato svolta da Arcane Crypto ha evidenziato come la *market dominance* di Bitcoin sia in realtà superiore al 90%[5], mentre limitando l'analisi alla sola capitalizzazione si avrebbe una *dominance* del 69,4%.

Performance alt-coin

Al solito analizziamo anche le performance delle principali alt-coin: Ethereum, Ripple, Litecoin, Bitcoin Cash, Stellar, Ethereum Classic, Zcash, Monero. In figura 3 sono riportati i rendimenti espressi in Bitcoin, cioè quanto avrebbe reso investire 1 BTC in ognuno degli alt-coin considerati ad inizio periodo.

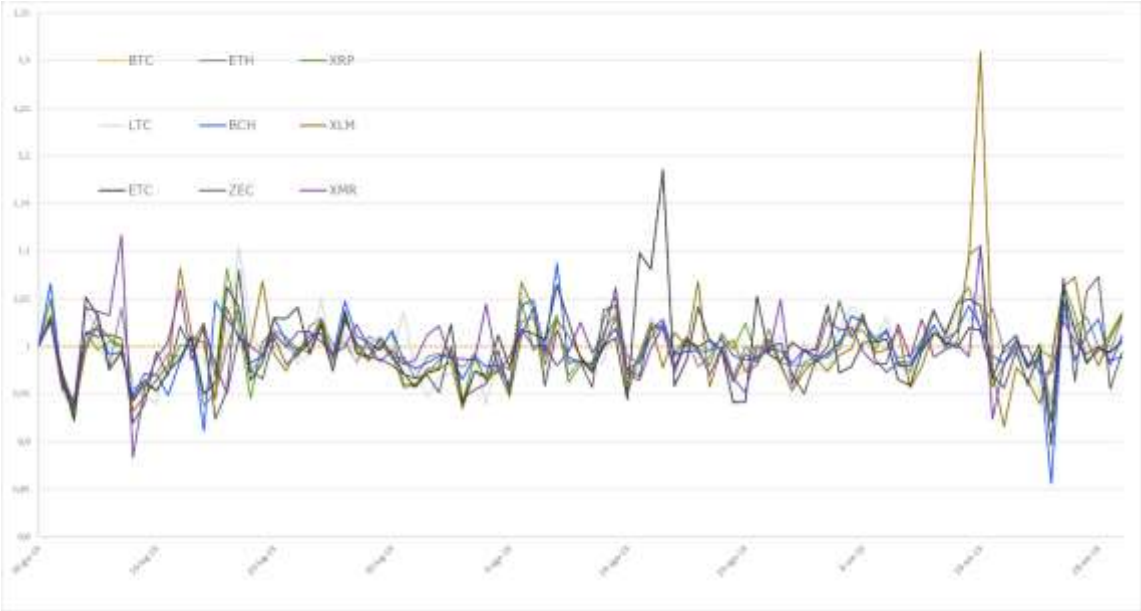


Figura 3: rendimenti alt-coin rispetto a Bitcoin

[4] https://www.ilsole24ore.com/art/bitcoin-come-l-oro-si-riscopre-bene-rifugio-e-corre-quando-crollano-borse-ACEmipd
[5] https://kryptografen.com/news/bitcoins-reported-market-dominance-is-approaching-70-but-in-reality-it-is-above-90/

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 in questo periodo il rendimento di tutti gli alt-coin è stato in linea con quello di Bitcoin, evidenziando una altissima correlazione con esso.

Futures su Bitcoin: l'arrivo di Bakkt e lo stop a LedgerX

Il trimestre appena concluso ha visto il lancio ufficiale dei Futures proposti da Bakkt (gruppo ICE, New York Stock Exchange). Il lancio, inizialmente previsto per dicembre 2018[6], è stato soggetto a continui ritardi dovuti a una mancanza di autorizzazione da parte del regolatore (CFTC e Department of Financial Services, DFS). A differenza dei contratti Futures emessi da CME (Chicago Mercantile Exchange) quelli proposti da Bakkt prevedono la consegna a scadenza dell'asset sottostante il contratto (*physically settled*), in questo caso Bitcoin. Il regolatore ha quindi richiesto lo sviluppo di una soluzione di custody affidabile.

Il 23 settembre 2019 sono ufficialmente iniziate le contrattazioni dei Futures physically settled offerti da Bakkt. I contratti sono proposti con due scadenze: a un giorno e a un mese

Dopo continui rimandi, il 16 agosto il Department of Financial Services di New York ha formalmente approvato[7] la richiesta da parte di Bakkt di costituire la *Bakkt Trust Company*, un custodian di Bitcoin qualificato che tramite la Bakkt Wharehouse offrirà i servizi di custody per i futures *physically settled*. Questo passaggio ha finalmente permesso a Bakkt di ufficializzare per il 23 settembre 2019 il lancio dei propri contratti Futures[8]. I contratti sono proposti con due diverse scadenze: a un giorno (sostanzialmente un mercato spot travestito da futures) e a un mese.

Nonostante il gran rumore che questo nuovo prodotto ha scatenato, l'accoglienza del mercato è stata piuttosto tiepida, causando un crollo del valore di Bitcoin che era cresciuto negli ultimi mesi anche grazie all'attesa per questo nuovo contratto[9]. Bisognerà attendere qualche mese per capire realmente i volumi che questi contratti potranno raggiungere[10].

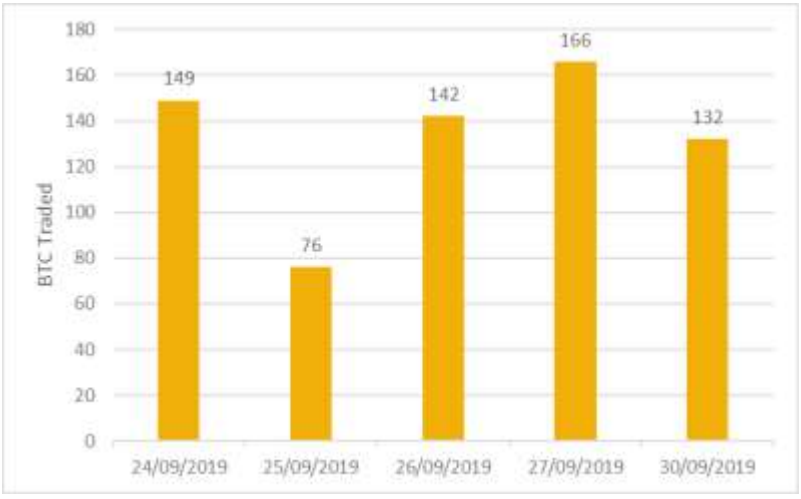


Figura 4: Volumi giornalieri dei Futures BAKKT

Diversa è invece la situazione dei Futures di LedgerX. Avevamo scritto nello scorso report dell'approvazione da parte della CFTC, ma è emerso invece in questo trimestre come LedgerX non sia però ancora in possesso della licenza necessaria per operare nel mercato Futures, non sia cioè in possesso della *Derivatives Clearing Organization (DCO) license*. La situazione creatasi è stata particolarmente imbarazzante per LedgerX, in quanto ha annunciato pubblicamente su Twitter il lancio della propria piattaforma

[6] https://www.coindesk.com/bakkt-is-supposed-to-start-testing-its-bitcoin-futures-contracts-today
[7] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1908161
[8] https://medium.com/bakkt-blog/cleared-to-launch-8dfc3e6f9ed0
[9] https://www.reuters.com/article/us-crypto-currencies-bitcoin/bitcoin-near-three-month-lows-after-tepid-response-to-nyse-owners-futures-idUSKBN1W92UY
[10] https://www.coindesk.com/trading-volume-for-bakkts-bitcoin-futures-totaled-just-5-million-in-first-week

di scambio per poi ritrattare poco dopo in seguito alle dichiarazioni della CFTC[11]. Al momento non sono disponibili ulteriori aggiornamenti circa la situazione di LedgerX.

ETF su Bitcoin: la strada di VanEck e SolidX

Dopo continui rifiuti e ritardi da parte della SEC all'autorizzazione di ETF su Bitcoin, a inizio settembre VanEck Securities Corp. e SolidX Management LLC hanno trovato uno stratagemma per riuscire a lanciare il loro prodotto. Sfruttando infatti la *Rule 144A del Securities Act del 1933* hanno potuto aggirare la necessità di una autorizzazione da parte della SEC, offrendo share del loro ETF a solo investitori istituzionali[12].

VanEck e SolidX hanno dichiarato che nonostante il raggiungimento di questo obiettivo, continueranno comunque a sollecitare la SEC per l'approvazione di un ETF accessibile anche al mercato *retail*.

[11] https://www.theblockcrypto.com/post/34307/actually-ledgerx-might-not-have-launched-physically-settled-bitcoin-futures-contracts-after-all
[12] https://www.bloomberg.com/news/articles/2019-09-03/vaneck-solidx-offer-etf-like-bitcoin-product-to-large-investors

2. Tecnologia

2.1 Bitcoin

Il trimestre appena concluso è stato un periodo vivace per quanto concerne gli sviluppi del protocollo Bitcoin, in particolare per *Core*, l'implementazione di riferimento. Questo anche perché durante il mese di settembre a Tel Aviv si è tenuta *Scaling Bitcoin*, la principale conferenza tecnica su Bitcoin dove tradizionalmente vengono presentati gli sviluppi più avanzati.

Presentiamo nel seguito le due proposte che a nostro avviso si sono rivelate essere le più interessanti per i risvolti che potranno avere sul network.

Bitcoin Vault

Un Bitcoin *Vault* è un meccanismo pensato per la custodia sicura dei propri Bitcoin. In un *Vault* i Bitcoin vengono bloccati attraverso uno script che richiede che passi un predeterminato intervallo temporale, osservabile pubblicamente, prima di rendere i Bitcoin sottostanti spendibili. Durante questo intervallo temporale il reale possessore di quei Bitcoin possiede una chiave di recovery che gli permette sempre di ritornare in possesso di quei Bitcoin, difendendosi quindi da un tentativo di furto. Come avviene per *Lightning Network*, uno user può avvalersi di una *Watchtower* (vedi box) per monitorare le transazioni che vengono propagate e inserite nella blockchain e reagire prontamente in caso di tentativo di furto.

> *In un Vault i Bitcoin vengono bloccati attraverso uno script che richiede che passi un prede-terminato intervallo temporale, osservabile pubblicamente, prima di rendere i Bitcoin sottostanti spendibili.*

Watchtower

Con *Watchtower* si intende un nodo che viene delegato a osservare le transazioni propagate in rete e a reagire, attraverso il *broadcast* di una transazione precedentemente firmata dal legittimo possessore, in caso venga rilevata una transazione che non rappresenta l'ultimo stato legittimo del canale di pagamento. L'utilizzo delle *Watchtower* è fondamentale, ad esempio, in *Lightning Network* per impedire questo tipo di attacchi anche quando il proprietario dei fondi non è online e pronto a reagire all'attacco.

L'idea dei Bitcoin *Vault* non è nuova, originariamente proposta da Malte Möser, Ittay Eyal, e Emin Gün Sirer nel 2016. La loro formulazione, però, necessitava di un *fork* nel network per essere utilizzata e per questo motivo l'implementazione non è mai decollata.

Figura 5: Brian Bishop

Ad agosto Bryan Bishop, sviluppatore di Bitcoin Core, ha proposto una idea alternativa per la realizzazione dei *Vault* che ha il vantaggio di sfruttare il codice esistente, evitando quindi *fork*[13]. La soluzione proposta da Bishop sfrutta una sequenza di "*pre-signed transaction*", ovvero transazioni precedentemente firmate e non propagate al network delle quali vengono poi eliminate le chiavi private utilizzate per generare le firme. Eliminando le chiavi si rende impossibile la generazione di transazioni diverse da quelle originarie. Le transazioni necessarie sono tre, una transazione per bloccare i fondi nel *Vault*, una transazione che spende i coin del *Vault* con un ritardo temporale (*delayed-spend transaction*) e una transazione di recovery che rimanda i coin nel *Vault* (*revault transaction*) e che viene utilizzata in caso di tentativo di furto.

Se la chiave è stata correttamente eliminata dopo aver firmato le transazioni, non è possibile per un attaccante generare transazioni diverse da quelle inizialmente firmate. Il limite di questa soluzione è che richiede un trust iniziale: è fondamentale assicurare di aver eliminato tutte le copie delle chiavi. Per questo motivo questa soluzione di custody di Bitcoin si adatta solamente ad un utilizzo da parte di un singolo privato, dove tutta la procedura può essere effettuata dal solo possessore di quei Bitcoin.

L'idea è stata proposta sulla mailing list *bitcoin-core-developer* ed è attualmente in corso una discussione circa l'implementazione.

Miniscript

Dopo aver presentato una implementazione per *Taproot* (vedi precedente numero del report), Peter Wuille, Bitcoin Core developer e uno dei founder di Blockstream, ha rilasciato durante il mese di agosto un nuovo linguaggio di scrittura per le transazioni Bitcoin e gli smart contract dal nome *Miniscript*[14] . Lo sviluppo di *Miniscript* è durato circa un anno e ha visto il coinvolgimento, oltre a Peter Wuille, di Andrew Poelstra, direttore della ricerca a Blockstream, e Sanket Kanjalkar, ricercatore presso Blockstream.

Miniscript si pone l'obbiettivo di semplificare la scrittura di transazioni complesse, attraverso l'utilizzo di un linguaggio strutturato che facilita l'analisi del codice scritto.[15] [16]

Grazie a queste caratteristiche *Miniscript* si candida a diventare il linguaggio di riferimento per la scrittura di tutte le transazioni più complesse e smart contract, riducendo le possibilità di errore e quindi le superfici di attacco.

Bitcoin Script

Script è il linguaggio di programmazione utilizzato per comporre le transazioni Bitcoin. È interessante notare che a differenza del linguaggio di scripting utilizzato in Ethereum, Script offre meno possibilità nella creazione di smart-contract, in modo da limitare il più possibile la superficie di attacco al network.

[13] https://www.coindesk.com/the-vault-is-back-bitcoin-coder-to-revive-plan-to-shield-wallets-from-theft
[14] https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2019-August/017270.html
[15] http://bitcoin.sipa.be/miniscript/
[16] https://www.coindesk.com/pieter-wuille-unveils-miniscript-a-new-smart-contract-language-for-bitcoin

Lightning Network updates

Passata l'euforia generata dalla *Lightning Torch*, un pagamento su Lighting Network che è passato come una torcia di mano in mano tra più di 275 partecipanti, l'incessante crescita del network è continuata: è notizia recente il raggiungimento dei 10,000 nodi attivi[17]. Questo è un grande traguardo per il network, che nonostante i problemi e le complessità di utilizzo continua a generare un grande interesse.

Lightning Network è in continua crescita, nel mese di settembre ha raggiunto e superato i 10,000 nodi attivi.

Quanto ai problemi, a settembre è stata scoperta una grave vulnerabilità nel codice che poteva causare la perdita dei fondi[18]. Rusty Russel e Olaoluwa Osuntokun, due degli sviluppatori più importanti del network, hanno tempestivamente reso disponibile versioni del software con correzione della vulnerabilità, i cui dettagli sono stati chiariti solo successivamente, per evitare nel periodo di aggiornamento software potenziali attacchi che sfruttassero questa bug.

Bitcoin mining: la crescita del network e l'ingresso di Blockstream

Per valutare la sicurezza e l'immutabilità di una blockchain che utilizza la *Proof-of-Work* (PoW) come algoritmo di consenso è fondamentale misurare la potenza computazionale del network; tale potenza viene calcolata come numero di *hash* al secondo che il network è in grado di calcolare.

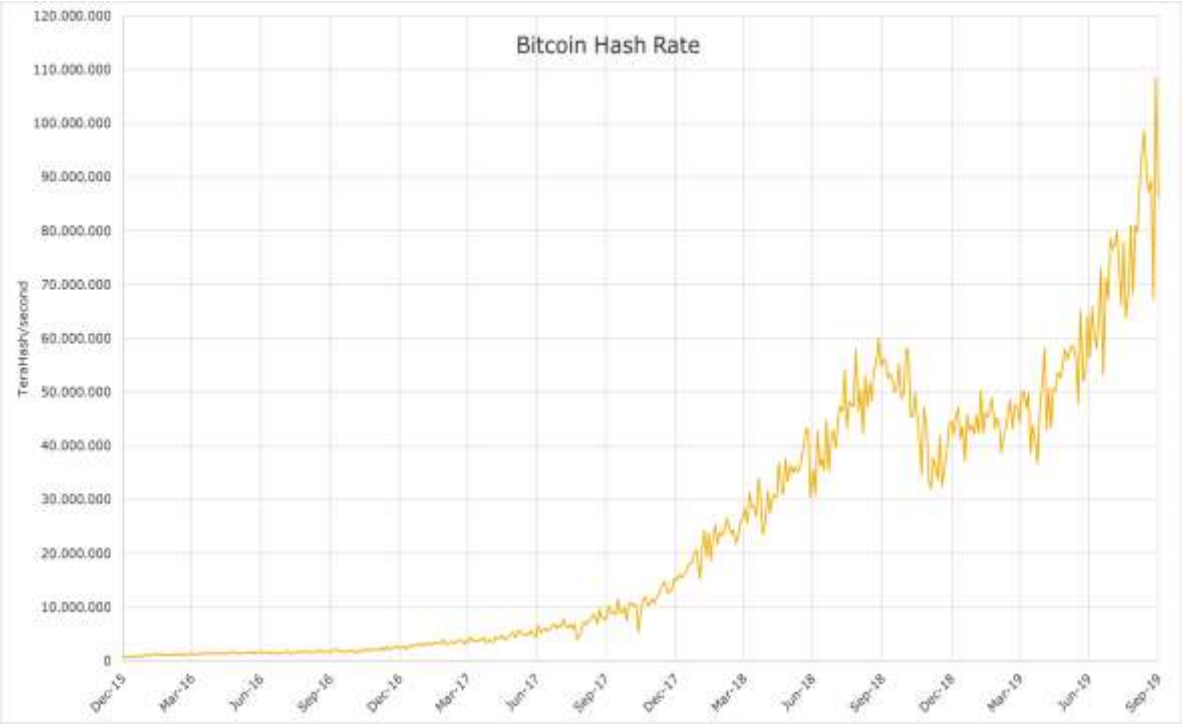


Figura 6: Hash rate globale del network Bitcoin da dicembre 2015

Dopo un periodo di flessione durante l'ultimo trimestre del 2018 e il primo del 2019, *l'hash-rate* globale del network Bitcoin è tornato a crescere in maniera significativa, raggiungendo

[17] https://decrypt.co/9662/bitcoin-lightning-network-hits-10000-nodes
[18] https://www.forbes.com/sites/billybambrough/2019/09/01/bitcoin-warning-as-serious-security-vulnerabilities-uncovered/

e superando i 100 *TeraHash* al secondo (TH/s), nuovo massimo storico, alla fine del trimestre. È interessante notare come l'attuale potenza computazione della rete Bitcoin sia circa 10 volte superiore al valore registrato a dicembre 2017 quando il prezzo aveva raggiunto la sua quotazione massima intorno ai $20,000: insomma, il prezzo lontano dall' *all-time-high* non ha rallentato gli investimenti infrastrutturali.

A questa crescita della potenza computazionale del net-

> *La mining farm di Blockstream vanta una potenza di 300 megawatt, capace di generare un hash-rate pari a circa il 10% del network*

work ha contribuito anche Blockstream. In questo trimestre infatti, l'azienda ha rivelato il possesso di una mining farm in Quebec, Canada e Adel in Georgia[19]. Secondo quanto rivelato il mining hardware utilizzato da Blockstream vanta una potenza di 300 megawatt, capace di generare un *hash-rate* pari a circa il 10% del valore globale. Dalle dichiarazioni ufficiali è emerso che oltre al mining center, Blockstream lancerà il proprio mining pool che dovrebbe implementare il nuovo protocollo di mining *BetterHash*, sviluppato per attribuire maggior rilevanza decisionale ai singoli miner facenti parte del pool.

BetterHash

BetterHash è il nome di un nuovo protocollo di mining, alternativo a quelli attualmente utilizzati dai mining pools. È importante tener presente che BetterHash non è una nuova implementazione dell'algoritmo di consenso utilizzato da Bitcoin, ma semplicemente un nuovo protocollo utilizzabile dai pools per fare mining.

L'idea di base è di dare un maggior potere nelle mani del singolo partecipante al pool, piuttosto che al pool manager. Attualmente è il pool manager che costruisce il blocco, seleziona le transazioni e decide che fork della blockchain seguire; con BetterHash, invece, il singolo partecipante avrà il potere di scegliere direttamente, lasciando al pool il solo compito di coordinare i vari partecipanti e dividere le ricompense.

[19] https://www.forbes.com/sites/ktorpey/2019/08/08/blockstream-reveals-massive-bitcoin-mining-facilities-fidelity-an-early-customer/

2.2 Altcoin

Litecoin Halving

A inizio agosto Litecoin, uno dei principali altcoin, ha dimezzato il tasso di emissione di nuovi coin, effettuando il cosiddetto "*Halving*"[20].

I nuovi coin emessi, a favore del Miner che ha effettuato il lavoro di validazione del blocco, sono passati da 25 a 12,5

Dal blocco 1,680,000 i nuovi coin emessi, a favore del *Miner* che ha effettuato il lavoro di validazione del blocco, sono passati da 25 a 12,5. In Litecoin un blocco viene validato in media ogni 2 minuti e 30 secondi, generando quindi in media 7,200 nuovi coin ogni giorno.

L'Halving è sempre un momento molto delicato per la vita di una crypto-currency: il dimezzamento del tasso di emissione di nuovi coin potrebbe, infatti, rendere non più profittevole il business di alcuni *Miner* spingendoli a spegnere il loro hardware e causando quindi una diminuzione della potenza computazionale.

Per Bitcoin il prossimo *Halving* è previsto per maggio 2020 e porterà a un tasso di emissione di 6.25 nuovi coin per blocco contro gli attuali 12.5[21].

Ton: la Blockchain di Telegram

Telegram ha rilasciato il codice della blockchain TON (Telegram Open Network) e una prima rete di test[22]. Questo rilascio viene in seguito alla ICO da record che ad inizio 2018 aveva portato Telegram a raccogliere $1.7 Miliardi per lo sviluppo di questa blockchain e del suo asset nativo GRAM, divenendo la seconda più grande ICO dopo EOS[23].

L'idea alla base di questa nuova blockchain è quello di diventare un sistema di pagamento sicuro e scalabile per abilitare i pagamenti all'interno dell'applicazione di messaggistica Telegram, sulla falsa riga di quanto fatto da Facebook con Libra.

Attualmente la *testnet* di TON può contare su più di 100 nodi manutenuti dalla stessa Telegram. Insieme al codice sorgente è stato anche rilasciato un block-explorer per la visualizzazione delle transazioni.

L'algoritmo di consenso scelto per questa blockchain sarà la *Proof-of-Stake*. È interessante notare che secondo le prime dichiarazioni ufficiali TON sarà compatibile con *Solidity*, uno dei linguaggi di scrittura di smart contract di Ethereum. Questa caratteristica permetterà di avere una grande interoperabilità tra le due blockchain.

Il rilascio della *mainnet*, la rete di produzione, è previsto per il 31 di ottobre.

[20] https://www.coindesk.com/litecoin-just-halved-its-crypto-rewards-for-miners
[21] https://www.bitcoinblockhalf.com/
[22] https://www.coindesk.com/telegram-finally-releases-code-for-its-1-7-billion-ton-blockchain
[23] https://www.bloomberg.com/news/articles/2018-12-14/crypto-s-15-biggest-icos-by-the-numbers

3. Regolazione

Libra: i primi stop normativi

Questo trimestre è stato caratterizzato dalle vicende legate a Libra, la valuta dell'omonimo consorzio promosso da Facebook. Il momento topico è stato certamente la testimonianza di David Marcus davanti al Senato degli Stati Uniti[24]. L'obiettivo era verificare come funzioni e sia gestita Libra, il livello di accesso alle informazioni dei consumatori, le garanzie in termini di privacy e l'interazione tra Facebook il suo wallet Calibra. I senatori hanno sparato praticamente a zero, partendo dalla generica mancanza di fiducia originata dagli scandali come Cambridge Analytica e la minaccia che Facebook rappresenterebbe per la democrazia, ma sottolineando nello specifico le preoccupazioni per la stabilità finanziaria e per il ruolo del dollaro statunitense come bene di riserva per eccellenza a livello internazionale. Quest'ultimo timore è stato esplicitamente confermato dal Segretario del Tesoro Steven Mnuchin che, dopo le rituali preoccupazioni per l'utilizzo delle crypto-currency per attività illecite (evasione fiscale, traffico di droga ed esseri umani, ecc.), nel caso specifico di Libra ne ha ribadito la pericolosità come potenziale concorrente del dollaro, rimarcando che è strategico per gli Stati Uniti preservare il ruolo internazionale della sua valuta[25].

> *Il momento topico è la testimonianza di David Marcus davanti al Senato degli Stati Uniti*

Figura 7: David Marcus

Questo è uno snodo cruciale per comprendere il dibattito su Libra e Bitcoin: l'economia statunitense presenta un gigantesco debito pubblico ed un altrettanto significativo debito privato, l'accettazione più o meno incondizionata del dollaro è essenziale per importare beni e servizi in cambio di moneta. Come ha chiarito più volte Alan Greenspan *"The United States can pay any debt it has because we can always print money to do that"*, ma questo è sostenibile solo finché il mondo considererà la moneta statunitense il bene di riserva per eccellenza.

> *Europa: il delitto di Libra sarebbe quello di lesa maestà, cosa che risuona alquanto paradossale*

Anche in Europa c'è stata una levata di scudi. Il ministro delle finanze francese Bruno Le Maire[26], da sempre antagonista critico di bitcoin ed affini, pur senza ricevere incarico formale dalla Commissione Europea, ha decretato che siccome Libra metterebbe a rischio la sovranità dei governi, allora il suo sviluppo non può essere autorizzato in Europa[27][28]. Alla base del ragionamento del ministro c'è la tesi che la moneta deve essere sovrana, senza riguardo per secoli di esperienza di monete private e locali (si pensi al free-banking negli Stati Uniti del 1800, piuttosto che alle banconote stampate dal Saddam Hussein ed utilizzate dai suoi nemici curdi dopo la caduta del dittatore per assenza di alternative praticabili) e disprezzo verso la scuola austriaca dell'economia (Hayek in primis) che ha portato critiche severe al monopolio governativo della moneta. Insomma: il delitto di Libra sarebbe quello di lesa maestà, cosa che risuona alquanto paradossale provenendo dal paese che i sovrani all'occorrenza li ha decapitati in piazza.

Figura 8: Bruno Le Maire

[24] https://bitcoinmagazine.com/articles/senate-hearing-facebooks-iffy-reputation-looms-libra-plans
[25] https://www.cnbc.com/2019/07/15/treasury-secretary-mnuchin-will-hold-a-news-conference-on-cryptocurrencies-at-2-pm-et.html
[26] https://www.france24.com/en/20190914-french-finance-minister-bruno-le-maire-war-with-facebook-cryptocurrency
[27] https://www.cnbc.com/2019/09/12/france-says-it-will-block-development-of-facebooks-libra-in-europe.html
[28] https://www.theguardian.com/technology/2019/sep/12/france-block-development-facebook-libra-cryptocurrency

Purtroppo per l'occasione anche il governo tedesco si è accodato: in un comunicato congiunto i due governi hanno affermato che *"no private entity can claim monetary power, which is inherent to the sovereignty of nations"*. Ed entrambi si sono rivolti verso ECB invitandola a svulippare lei una forma di contante digitale al passo coi tempi: *"We encourage European central banks to accelerate work on issues around possible public digital currency solutions"*[29]

Qualche segno di riflessione aperta e franca sul tema arriva dal canadese Mark Carney, ex governatore di Bank of England: senza mezzi termini dichiara che la crescita e la cooperazione internazionale beneficerebbero dalla fine del dominio del dollaro statunitense come moneta di riserva, da rimpiazzato con qualcosa di simile a Libra[30] [31].

Figura 9: Mike Carney

Più timida, ma comunque aperta al futuro, si mostra la ricerca del Fondo Monetario Internazionale quando nella nota *"The Rise of Digital Money"* evidenzia che gli *stable-coin* (le criptovalute non speculative, costruite per avere potere d'acquisto stabile nel tempo, proprio come Libra) siano un punto di innovazione finanziaria che potrebbe combinarsi con le garanzie di stabilità offerte dalle banche centrali[32].

> *FMI: gli stable-coin punto di innovazione finanziaria che potrebbe combinarsi con le garanzie di stabilità offerte dalle banche centrali*

Ma non si riesce ad esultare abbastanza per qualche sparuto contributo autorevole e intellettualmente libero, che il quadro torna surreale con Benoît Cœuré, membro del comitato esecutivo di ECB: in una reazione pavloviana per tranquillizzare Francia e Germania afferma la necessità di rilanciare il sistema di pagamenti istantanei nell'euro zona e la necessità di ripensare la possibilità del contante digitale di banca centrale[33]. Il banchiere è evidentemente tranquillo che nessuno ricordi come solo un anno prima avesse dichiarato: *"there are no clear benefits from allowing the general public to hold digital central bank reserves, in particular in economies where demand for cash remains robust, such as in the euro area. This assessment includes considerations related to the potential impact of central bank digital currencies"*.

D'altronde la coerenza su questi temi non è il punto forte delle istituzioni europee: nel luglio 2014 la European Banking Authority invitava i regolatori nazionali a dissuadere le istituzioni finanziarie dal detenere, acquistare o vendere valute virtuali, fintanto che queste non mettessero in atto uno schema di governo responsabile della loro integrità; quando cinque anni dopo la Libra Association si candida al governo responsabile della sua valuta e chiede autorizzazione ai regolatori, si scopre invece che questo non basta perché viola la sovranità monetaria. Aveva già capito tutto, come sempre, il vecchio saggio Friedrich Hayek: *"I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop"*. Amen.

Figura 10: Friedrich Hayek

[29] https://www.reuters.com/article/us-facebook-cryptocurrency-france-german/france-and-germany-agree-to-block-facebooks-libra-idUSKCN1VY1XU
[30] https://www.bloomberg.com/news/articles/2019-08-25/carney-s-libra-idea-shows-how-the-dollar-is-everyone-s-problem
[31] https://www.bloomberg.com/news/articles/2019-08-23/carney-urges-libra-like-reserve-currency-to-end-dollar-dominance
[32] https://www.coindesk.com/traditional-money-could-be-surpassed-by-e-money-stablecoins-imf-paper
[33] https://www.reuters.com/article/us-facebook-cryptocurrency-france/france-germany-blast-facebooks-libra-back-public-cryptocurrency-idUSKCN1VY0H3

4. Ecosistema

Coinbase acquisisce Xapo

Anche in questo trimestre i servizi di custody per asset digitali sono stati al centro delle discussioni, dimostrando il sempre più grande interesse verso queste soluzioni.

La vera protagonista di questo trimestre è stata Coinbase, che prima ha aggiunto tra i suoi clienti del servizio di custody Grayscale[34], il più grande fondo di investimento Bitcoin e crypto al mondo, e successivamente ha acquisito tutto il business istituzionale di Xapo[35], il custodian di riferimento fino a quel momento. Grazie a queste operazioni Coinbase ha superato i $7 miliardi di asset under custody, diventando il servizio di custody più popolare e fidato da parte delle istituzioni per la custodia sicura dei propri asset digitali.

L'acquisizione di Xapo da parte di Coinbase era nell'aria da qualche mese. Le prime indiscrezioni di questo accordo risalgono infatti al secondo *quarter* 2019. L'ingresso di Grayscale, precedentemente cliente di Xapo, tra i clienti di Coinbase è stata sicuramente la mossa decisiva verso la chiusura della trattativa tra i due servizi di custody. L'operazione si è conclusa con il versamento di $55 milioni a Xapo da parte di Coinbase.

Figura 7: Asset Under Custody di Coinbase

Grazie a queste due operazioni Coinbase ha visto esplodere il proprio business di custody: in un solo anno di operatività ha infatti raggiunto gli oltre $7 miliardi di *asset under custody*, detenendo oltre il 5% di tutti i Bitcoin in circolazione. Coinbase custody non si limita però al solo Bitcoin, ma supporta tutte le maggiori crypto e i token ERC20 emessi su Ethereum (in pratica tutti i token emessi tramite le ICO).

Il servizio di custody di Coinbase è volto soprattutto agli istituzionali, con un livello minimo di accesso di $1 milione di asset e una *fee* annuale di 50 bps.

L'ampia gamma di digital asset supportati getta a nostro avviso alcuni dubbi sulla effettiva affidabilità del servizio: seppur simili sotto alcuni aspetti, ognuna di queste crypto ha delle peculiarità che richiedono delle specializzazioni ad-hoc. Inoltre, Coinbase non fornisce alcuna informazione circa le modalità di custody utilizzate, percorrendo la strada della *security-by-obscurity*, standard condiviso dei diversi player di mercato.

> *In un solo anno di operatività Coinbase Custody ha raggiunto gli oltre $7 miliardi di asset under custody, arrivando a detenere oltre il 5% di tutti i Bitcoin in circolazione*

[34] https://blog.coinbase.com/welcoming-grayscale-the-worlds-largest-crypto-fund-to-coinbase-custody-72e6694e9ea3
[35] https://blog.coinbase.com/coinbase-custody-acquires-xapos-institutional-business-becoming-the-world-s-largest-crypto-2c1b46fc94c4

Coinbase: bug nella sicurezza della gestione degli account

Coinbase, uno dei più grandi exchange crypto attualmente operativo, ha rivelato un bug nei propri sistemi di sicurezza che comportava il salvataggio in chiaro delle password di alcuni utenti sui propri server[36]. Dalla dichiarazione ufficiali sarebbero stati affetti da questa problematica 3420 utenti, che Coinbase ha prontamente avvisato richiedendo l'aggiornamento delle proprie credenziali di accesso.

Questo incidente è particolarmente imbarazzante per l'exchange che proprio in questo trimestre si è mosso per accrescere la propria credibilità come custodian sicuro e affidabile di crypto-asset.

Furto di identità a Binance

Nello scorso numero del report avevamo parlato del furto di 7,000 Bitcoin ai danni di Binance. Gli hacker, sfruttando una falla nei sistemi di sicurezza dell'exchange erano riusciti a raggiungere le chiavi dell'*hot-wallet* e a rubare i Bitcoin per un equivalente, all'epoca del furto, di 40 milioni di dollari.

Sono state diffuse su Telegram le foto, utilizzate da Binance per l'identificazione, di alcuni utenti con in mano un documento e un foglio con la scritta "Binance 02/24/18". Questo furto di informazioni riguarderebbe circa 60,000 individui

Durante questo trimestre è emerso come durante quell'attacco siano allo stesso tempo state rubate le informazioni private degli utenti (da loro fornite in fase di registrazione) ed in generale i dati collezionati per ottemperare al *know-your-customer* (KYC)[37]. In particolare, sono state diffuse su un gruppo Telegram le foto, utilizzate da Binance per l'identificazione, di alcuni utenti con in mano un documento e un foglio con la scritta "Binance 02/24/18". Questo furto di informazioni riguarderebbe circa 60,000 individui. Secondo le dichiarazioni di Binance gli hacker avrebbero richiesto 300 bitcoin come riscatto. Non sono ad oggi disponibili aggiornamenti sulla notizia.

Questo furto evidenzia come gli exchange soffrano continuamente di attacchi informatici e anche quelli ritenuti più sicuri non siano esenti da perdita di dati e coin. Depositare i propri asset digitali presso un exchange è ad oggi ancora una scelta molto rischiosa.

Colu ricompra i token

La startup blockchain Colu ha deciso di abbandonare la tecnologia blockchain alla base della propria soluzione tecnologica[38]. Colu è una applicazione per pagamenti basata sull'idea di valute locali emesse all'interno di una comunità (un quartiere di una città ad esempio) e utilizzate per le spese quotidiane. Il loro sistema di pagamenti era inizialmente basato su *colored-coin* bitcoin; questa soluzione però non è mai riuscita a scalare e a diventare realmente utilizzabile nei pagamenti quotidiani, per questo motivo hanno deciso di abbandonare la strada dell'utilizzo della blockchain.

[36] https://blog.coinbase.com/post-mortem-a-closer-look-at-a-password-storage-issue-affecting-3-420-customers-e23cfc8a0363
[37] https://www.coindesk.com/binance-kyc-issue
[38] https://www.coindesk.com/colu-may-buy-back-ico-tokens-in-pivot-away-from-blockchain

I token emessi verranno riacquistati da Colu all'originale prezzo di acquisto, nonostante la quotazione attuale sia inferiore

È sicuramente lodevole l'iniziativa di ricomprare tutti i token emessi durante la loro ICO ridando indietro ai richiedenti gli Ether inviati allo smart contract. Colu ha fatto sapere che i token emessi verranno riacquistati all'originale prezzo di acquisto, nonostante la quotazione attuale sia inferiore. La procedura di riacquisto non coinvolgerà però tutti i partecipanti alla ICO: gli stati dove le ICO sono proibite o problematiche, come ad esempio USA, Canada e Cina, saranno infatti esclusi dall'operazione; inoltre solo chi completerà una procedura di identificazione completa (KYC e *anti-money-laundering*) potrà ricevere gli Ether dovuti[39].

[39] https://cln.network/

5. News dall’Istituto

Blockchain Dates

Il Digital Gold Institute ha tenuto a fine settembre una giornata di formazione a Milano su Bitcoin e tecnologia Blockchain dal nome *Blockchain Dates*. Questa prima edizione dell'evento è stata organizzata da Craon.

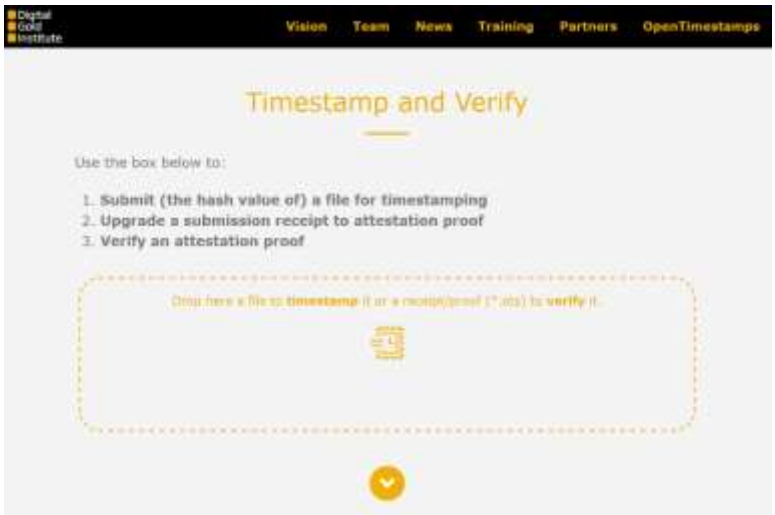
La partecipazione è stata numerosa e molto vivace, con esponenti provenienti da diversi settori: banche, società di consulenza, istituzioni finanziarie, privati e studenti. Alla fine della giornata è stato consegnato ai partecipanti un breve quiz e i migliori sono stati invitati a una giornata più tecnica sull'argomento, durante la quale sono stati approfonditi il funzionamento del *mining*, delle transazioni e del *timestamping* su blockchain.

Visto il successo di questa iniziativa, verranno organizzate altre giornate di formazione aperte a tutti. Forniremo ulteriori informazioni sul sito internet dell'istituto nella sezione Training[40].

Rilascio del Calendario OpenTimestamps del Digital Gold Institute

Uno dei principali ambiti di ricerca del Digital Gold Institute è la marcatura temporale su Blockchain. In particolare, l'Istituto è promotore dell'utilizzo del protocollo *vendor-indipendent* e *open-source OpenTimestamps*[41].

Durante il trimestre appena concluso abbiamo pubblicato sul nostro sito internet un tool[42] che permette di effettuare il *timestamping* e la verifica sulla blockchain di Bitcoin attraverso l'utilizzo del protocollo OpenTimestamps. Il servizio è offerto gratuitamente grazie alla presenza di server pubblici, chiamati *calendar server*, che collezionano le richieste di timestamping ed effettuano la transazione pagando le relative fee transazionali.



Attualmente sono disponibili quattro *calendar server* pubblici, due manutenuti da Peter Todd (ideatore del protocollo), uno da Riccardo Casatta (il principale contributore al protocollo) e uno da Catallaxy. Abbiamo configurato e reso disponibile anche il nostro *calendar server*[43], utilizzabile attraverso la nostra pagina web.

È inoltre disponibile una ulteriore pagina[44] nella quale è presente un dettagliato *step-by-step tutorial* sul funzionamento del protocollo OpenTimestamps.

[40] https://dgi.io/#training
[41] https://opentimestamps.org/
[42] https://dgi.io/ots/
[43] https://btc.ots.dgi.io/
[44] https://dgi.io/ots-tutorial/

Crypto Asset Lab a supporto di Scaling Bitcoin

Il *Crypto Asset Lab*, laboratorio di ricerca congiunto tra DGI e Università degli studi di Milano-Bicocca è stato inserito tra le *Academic Supporting Organizations* di *Scaling Bitcoin*[45]. *Scaling Bitcoin* negli anni si è sempre confermato come la conferenza scientifica di riferimento per quanto concerne gli sviluppi su Bitcoin. L'edizione di settembre a Tel Aviv[46] è stata la sesta e una nostra delegazione ha come sempre partecipato ai lavori. È un significativo riconoscimento per il CAL essere inserito tra le istituzioni accademiche che supportano questo evento.

La ricerca dell'Istituto sul tema della *custody*

Durante il trimestre abbiamo continuato l'attività di studio e analisi delle soluzioni di *custody* bitcoin, arrivando a definire l'idea di base di un protocollo per la custodia sicura dei Bitcoin. Questa attività di ricerca sfocerà nel mese di ottobre nella costituzione di una start-up dedicata alla implementazione di una prima versione commerciale del protocollo sviluppato dall'Istituto.

[45] https://scalingbitcoin.org/
[46] https://telaviv2019.scalingbitcoin.org/

Autori

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