Digital Gold Institute

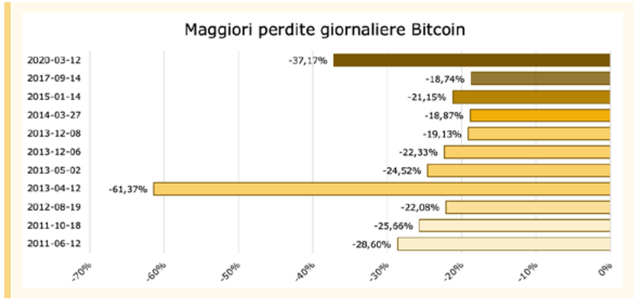
Scarcity in the Digital Realm

N. 04

REPORT TRIMESTRALE 2020 Q1

Editoriale

Covid-19 ha segnato anche il mondo cripto: se speravate di trovare tra queste pagine un diversivo al tema che domina le nostre giornate **non** sarete delusi, ma i conti col fenomeno pandemico bisogna farli comunque.



Ci riferiamo ai movimenti del prezzo di Bitcoin nella crisi globale innescata dalla diffusione del virus: un tracollo dei corsi contestuale a quello di tutti gli indici azionari (sebbene il trimestre complessivamente si chiuda con un consuntivo di "solo" -7%). In tanti ce ne avete chiesto ragione, sottolineando la delusione per questo "equivalente digitale dell'oro" che non ha mostrato il comportamento anticiclico che legittimamente ci si poteva aspettare da un bene rifugio.

La prima constatazione è che, evidentemente, molti investitori ritengono ancora Bitcoin un asset speculativo: comprano quando l'appetito per il rischio è alto, vendono quando vogliono le certezze che trovano nella liquidità e nei titoli di stato e che Bitcoin non può dare. Il tempo giudicherà se questa visione è corretta, altri (tra cui noi) hanno una visione opposta; nel frattempo questo è un primo punto saliente che rende Bitcoin diverso dalle altre asset class: la sua percezione è ancora controversa.

Questa mancanza di consenso sulla natura di Bitcoin lo rende di fatto inassimilabile ad altri beni di investimento: nel secondo semestre 2017 Bitcoin si muoveva assieme all'indice azionario S&P500, nel secondo semestre 2019 assieme all'oro, in quest'ultimo trimestre nuovamente con l'azionario. Evidentemente, in ogni finestra temporale di osservazione la misurazione della correlazione fornisce un dato la cui affidabilità, però, si può cogliere solo allargando la finestra a periodi adeguati quanto a significatività statistica e appropriati come orizzonte di investimento. Ad esempio, usando una finestra fissa di durata un anno e facendola muovere nel tempo (*rolling window*) vediamo che la correlazione tra Bitcoin e tutte le altre asset class è stabile ed è sempre prossima allo zero; viceversa, gli altri beni di investimento mostrano alla stessa analisi una correlazione chiaramente attestata su livelli lontani dallo zero. Più lunga è la finestra, cioè meno è influenzata da situazioni di breve periodo, più marcata è l'osservazione. È inequivocabile: sul medio periodo Bitcoin mostra un andamento indipendente da tutto il resto, forse perché non abbiamo ancora capito a cosa sia comparabile o, come riteniamo noi, perché è diverso da tutto il resto. È opportuno rimarcare questo concetto, su cui è facile fare confusione: mancanza di correlazione (correlazione zero) non vuol dire anti-correlazione (correlazione negativa). In altri termini, Bitcoin non si muove in controtendenza (ad esempio sale quando l'azionario scende); semplicemente si muove in modo indipendente.

Insomma: se una rondine non fa primavera, un trimestre non definisce la natura di Bitcoin; statisticamente Bitcoin conferma la sua unicità come asset class capace di una straordinaria riduzione dei rischi se inserito in un portafoglio di investimento diversificato. Pubblicheremo nei prossimi mesi uno studio più ampio e dettagliato per chiarire questa conclusione forte.

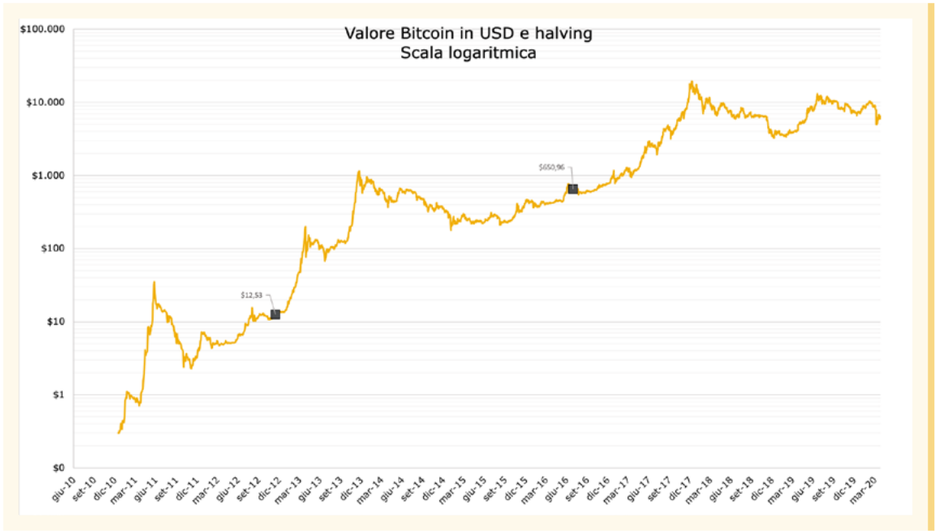
Un'altra considerazione, più sofisticata, la stiamo mettendo a fuoco assieme

ad altri ricercatori in un lavoro su *hidden Markov model*: si tratta di modelli tipicamente utilizzati nell'ambito dei sistemi di apprendimento di intelligenza artificiale. Nel nostro caso il mercato viene modellato come un processo stocastico le cui variabili di controllo sono nascoste (*hidden*), definite appunto stati latenti. Il mercato cripto si può parametrizzare con un numero arbitrario di stati latenti, ma l'evidenza è che il modello è sempre dominato dallo stato fortemente ribassista e da quello fortemente rialzista, con gli stati intermedi a bassa significatività; le matrici di transizione tra gli stati dominanti dicono che al 70% il mercato resta nello stato in cui si trova, al 30% passa nell'altro stato. È una evidenza che conferma il senso comune: volatilità estrema nelle transizioni tra cicli rialzisti e cicli ribassisti, con lunghi periodi trascorsi nello stesso ciclo. Un comportamento chiaramente accentuato da quella mancanza di consenso di cui abbiamo scritto sopra, nonché da un mercato con volumi ancora limitati e non regolamentato, soggetto pertanto ai movimenti estremi provocati da grandi operatori (le cosiddette "balene") e da esagerate posizioni a leva, senza nessuno dei cosiddetti *circuit breaker* come la sospensione per eccesso di ribasso.

Infine, se anche Bitcoin marcasse quest'anno una quotazione minima al livello finora osservato di circa $5000, sarebbe comunque un incremento del +46% rispetto al minimo osservato nel 2019. Quando si tratta di Bitcoin, meglio osservare la *bottom line* e non farsi confondere dagli eccessi di volatilità.

Oltre all'analisi di mercato, in questo numero vi presentiamo molto altro: gli sviluppi di Bitcoin ed Ethereum, AVA e Algorand, gli aggiornamenti su Libra e il contante digitale di banca centrale, ecc. Non manca un pezzo surreale sulla significatività del numero 42 che speriamo vi strapperà un sorriso.

Quanto ai prossimi mesi: occhi puntati a metà maggio[1] sull'*halving*, il dimezzamento della quantità di Bitcoin emessi per ogni blocco. Il modello *stock-to-flow*[2], che finora ha perfettamente descritto la crescita delle quotazioni di Bitcoin in funzione del rapporto tra Bitcoin già emessi (*stock*) e la quantità di nuovi Bitcoin per blocco (*flow*), prevederebbe nei prossimi 18 mesi un incremento del prezzo di un fattore 10. Ne parleremo il prossimo trimestre.



[1] https://www.bitcoinblockhalf.com/
[2] https://medium.com/@carloclerici/il-concetto-di-scarsita-nella-determinazione-del-valore-di-bitcoin-c716c0ad3fff

INDICE

1. Mercato
Bitcoin 4
Altcoin 7
Futures e opzioni 8
ETF e Trust 9

2. Tecnologia
Bitcoin 12
Aggionamento del protocollo 12
Mining 13
Lightning Network 13
Altcoin 14
Ethereum: l'aggiornamento Muir Glacier 14
Altcoin e centralizzazione 15
Blockchain 17
Algorand e AVA: i professori della blockchain 17

3. Regolazione
Libra 20
Central Bank Digital Currency 20
ESMA, Consob, G20 e BaFin 21

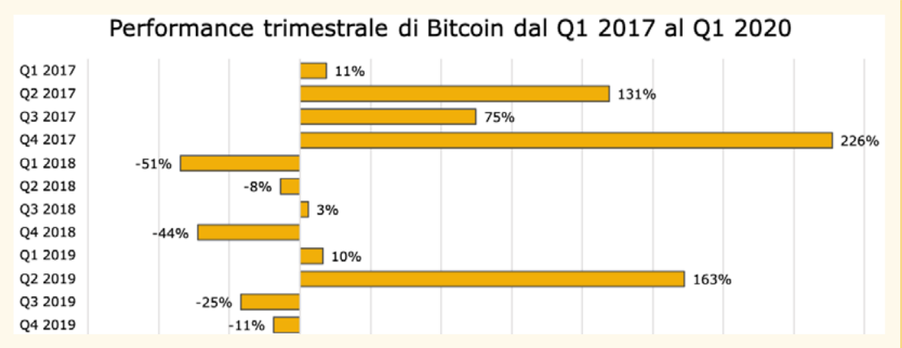
4. Ecosistema
La custodia dei crypto-asset 24
Finanza tradizionale e DeFi 26
Chainalysis: criptovalute e attività criminali 27

5. Vita dell'Istituto
Presentazione del report 2019-Q4 30
Dal sesterzio al Bitcoin. Vecchie e nuove dimensioni del denaro 31
Blockchain Education Network: premio miglior tesi alla prima *alumna* DGI 32
42: la vita, l'universo e il tutto; incluso Bitcoin 33

1. MERCATO

Bitcoin

Nel primo trimestre 2020 tutti i mercati finanziari sono stati fortemente influenzati dalle conseguenze negative della pandemia dovuta al Covid-19.

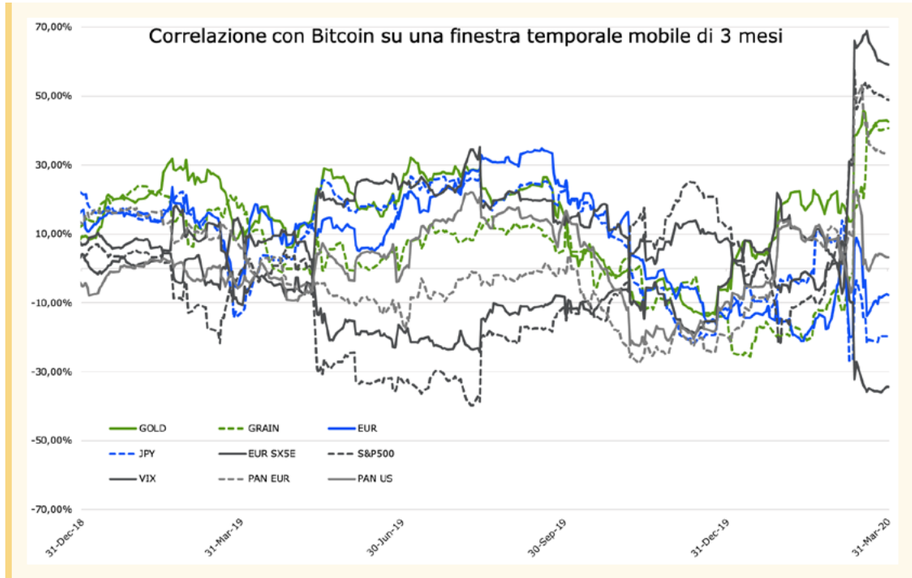


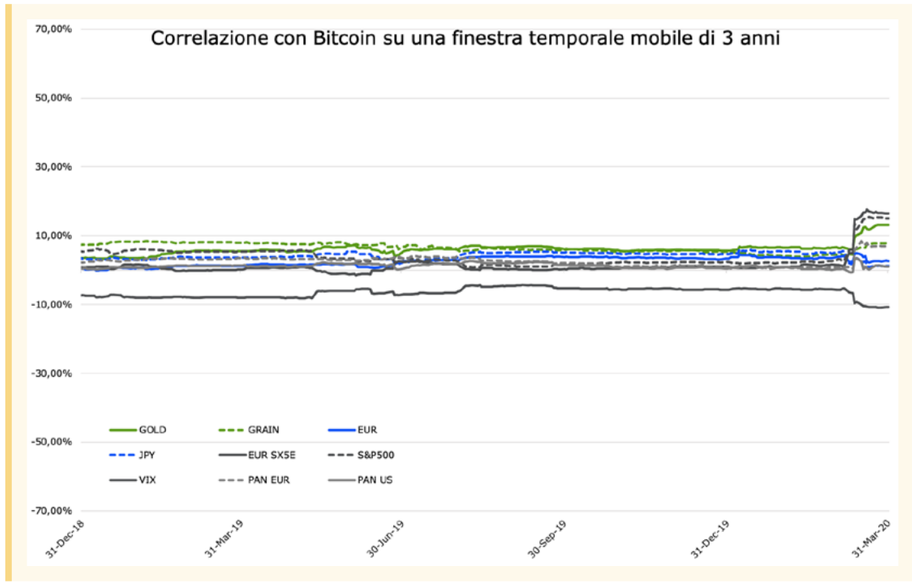
l trimestre era partito con una tendenza positiva, portando la quotazione di Bitcoin a superare $10,000 a metà febbraio, segnando un rialzo da inizio anno del 43,5%. Con la scoperta dei primi casi di Covid-19 in Italia e la successiva crescita dei contagi a livello globale, la tendenza si è nettamente invertita. Il crollo dei corsi ha raggiunto l'apice nella giornata del 12 marzo, quando Bitcoin ha toccato il minimo di $4970 segnando un calo giornaliero di quasi il 40%. Il 12 marzo verrà ricordato come il giorno nero dei mercati finanziari, nella stessa giornata infatti il FTSE MIB ha segnato un calo del 17%, l'EUROSTOXX50 del 12% e gli indici US (S&P500 e NASDAQ) hanno perso circa il 9,50%. Anche la quotazione dell'oro ha segnato il calo maggiore del trimestre in quella stessa giornata con un -3,54%.

Anno	Prezzo Minimo
2011	$ 0,30
2012	$ 4,33
2013	$ 13,40
2014	$ 310,74
2015	$ 178,10
2016	$ 364,33
2017	$ 777,76
2018	$ 3.236,76
2019	$ 3.399,47
2020	$ 4.970,79

Nonostante il crollo della quotazione, il minimo toccato nel 2020 rappresenta un incremento del 46% rispetto al 2019, confermando la crescita sostanzialmente continua dei minimi per anno (si veda box in questa pagina e grafico nell'editoriale).

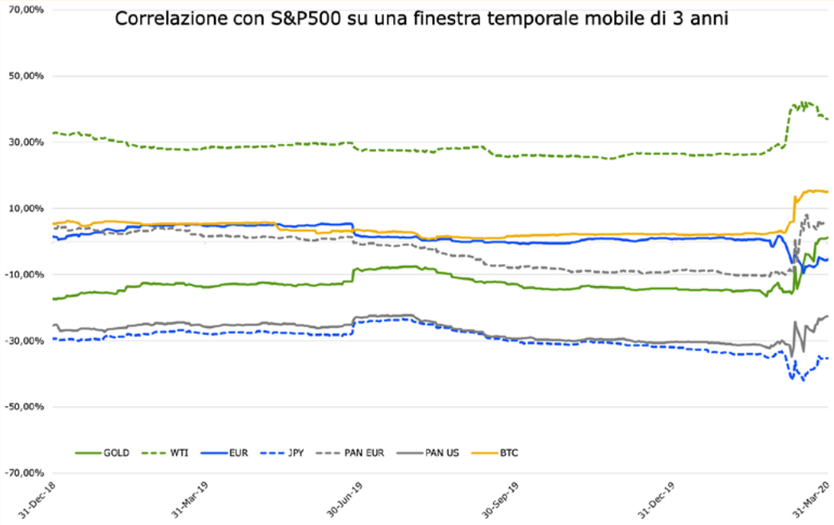
L'evidenza empirica del trimestre è stata quella di un Bitcoin positivamente correlato all'azionario, ma sarebbe sbagliato trarne conclusioni senza significatività statistica. Come si osserva nei grafici i comportamenti osservati su brevi periodi sono variabili e contraddittori nel tempo; non appena la scala di osservazione si allarga (su finestre più adeguate a considerazioni statistiche quantitativamente affidabili e quindi rilevanti per gli investimenti), la correlazione di Bitcoin con le altre asset class va a zero.



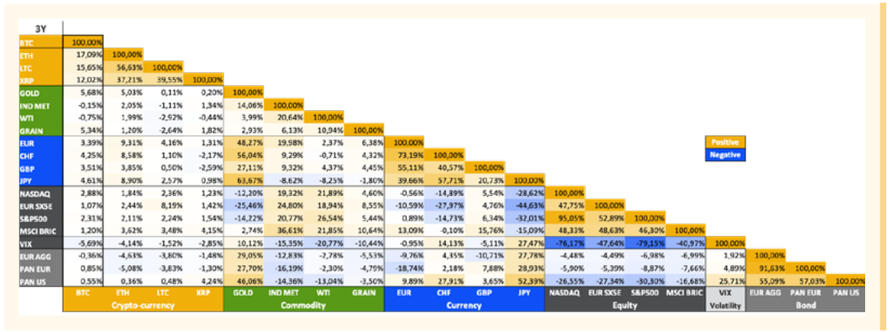


Se partiamo, ad esempio, da una finestra temporale mobile di un trimestre vediamo che il comportamento della correlazione è molto variabile: la correlazione con l'azionario passa da valori negativi (-30%) durante l'estate 2019 a valori marcatamente positivi (60%) nell'ultimo trimestre, come conseguenza della crisi innescata dal Covid-19. Se invece estendiamo gradualmente la finestra temporale mobile fino a 3 anni, perido statisticamente più significativo, i valori della correlazione si appiattiscono su valori vicini allo 0% (nell'intervallo [-10%, 10%]).

Il comportamento è qualitativamente diverso, invece, per altre asset class: la stessa analisi per lo S&P500 mostra correlazioni chiaramente attestate su livelli diversi da zero.



Questa evidenza è confermata dalla matrice di correlazione completa che considera i dati di mercato degli ultimi tre anni. La colonna relativa a Bitcoin e in generale alle crypto-currency ha valori prossimi allo 0 (colore chiaro), le altre colonne hanno valori marcatamente distanti da zero (colori scuri).

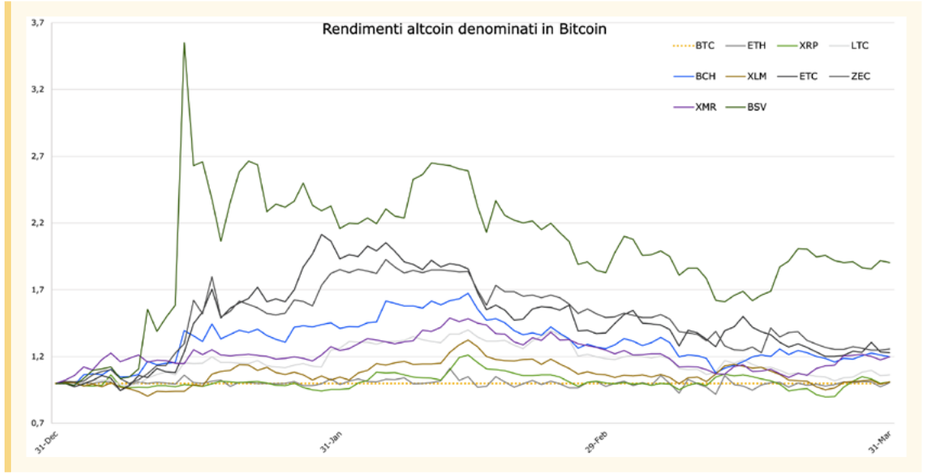


Inoltre, la matrice chiarisce che la correlazione tra i diversi altcoin è molto più alta (superiore al 40%) rispetto a quella con Bitcoin (intorno al 15%). Insomma il mercato differenzia chiaramente Bitcoin dai suoi cloni: a questi ultimi attribuisce un comportamento relativamente indipendente da Bitcoin, ma molto correlato fra di loro. Questa evidenza si conferma restringendo la finestra di osservazione all'ultimo anno: la correlazione tra i vari altcoin si attesta, infatti, a valori compresi tra 80% e 90%, mentre quella degli altcoin con Bitcoin si attesta per tutte le coppie intorno al 18%. Insomma, inserire in portafoglio un altcoin oltre a Bitcoin ha un valore per la diversificazione del rischio, ma aggiungerne altri non migliora significativamente la diversificazione.

Altcoin

Come sempre documentiamo anche le performance dei principali altcoin: 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 altcoin considerati.

Come si può vedere dal grafico, in questo periodo il rendimento di tutti gli altcoin è stato tendenzialmente superiore a quello di Bitcoin. L'altcoin che meglio ha performato nel trimestre è Bitcoin-SV (BSV). Ricordiamo che BSV è nato nel novembre 2018 su iniziativa di Craig Wright tramite un cambiamento contenzioso (tecnicamente un *hard-fork*) del protocollo di Bitcoin-Cash, nato a sua volta da un *hard-fork* di Bitcoin nell'agosto 2017.



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

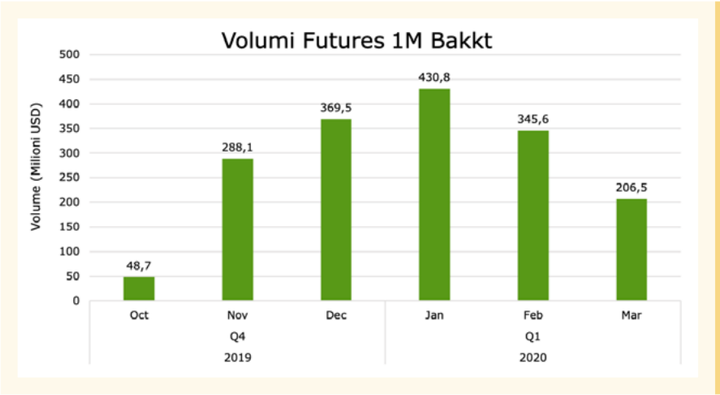

Craig Wright

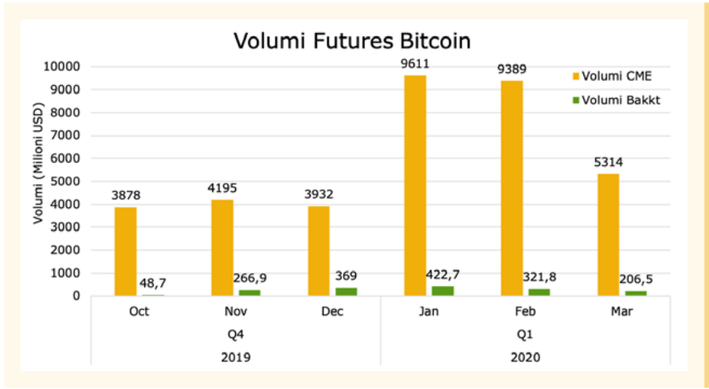
L'alto rendimento di questo altcoin è stato influenzato dalla giornata del 14 gennaio in cui ha guadagnato il 123%, segnando un rialzo da inizio anno del 255% su Bitcoin[3]. Il movimento è dovuto alle voci secondo le quali Craig Wright, il fondatore di BSV, avrebbe fornito documentazione importante a favore della sua dichiarazione di essere Satoshi Nakamoto. Sono oramai diversi anni che Craig Wright cerca invano di portare prove per avvalorare questa sua dichiarazione, accumulando in realtà un crescente e generalizzato discredito. È bene sottolineare come i volumi di questo altcoin siano stati manipolati diverse volte nel passato attraverso la diffusione di notizie false proprio su questo punto (si veda il nostro report 2019-Q2). Per questo non riteniamo il fenomeno significativo nel medio periodo.

[3] https://www.newsbtc.com/2020/01/14/here-are-the-main-reasons-why-bitcoin-sv-went-parabolic-today/

Futures e opzioni

Continua anche in questo trimestre la crescita degli scambi su strumenti derivati: gennaio è stato un mese da record sulla nuova borsa Bakkt, non confermato però nei due mesi successivi per il contraccolpo del Covid-19; in particolare a marzo abbiamo visto volumi praticamente dimezzati. Discorso analogo per il contratto leader sul mercato regolamentato: i futures di CME. Anche in questo caso, gennaio ha segnato una impennata dei volumi scambiati con un valore aggregato mensile superiore ai $9.5 miliardi, triplicando il risultato ottenuto nel mese precedente. Grazie a questo deciso incremento, CME è riuscita il 29 gennaio a superare i $100 miliardi di volumi totali scambiati da dicembre 2017, data di lancio del prodotto[4]. Dopo il 18 febbraio, giornata con scambi giornalieri superiori al miliardo di dollari[5] (era successo solo altre due volte nella storia), anche per i futures CME è iniziato il calo dei volumi, con un dimezzamento degli scambi a marzo. È interessante notare come, nonostante l'incremento, i futures di Bakkt rimangano ancora trascurabili rispetto a CME. Ricordiamo che la differenza principale tra Bakkt e CME riguarda il settlement del contratto che nel caso di CME è *cash* (dollari) mentre nel caso di Bakkt è *physical* (consegna del sottostante Bitcoin).



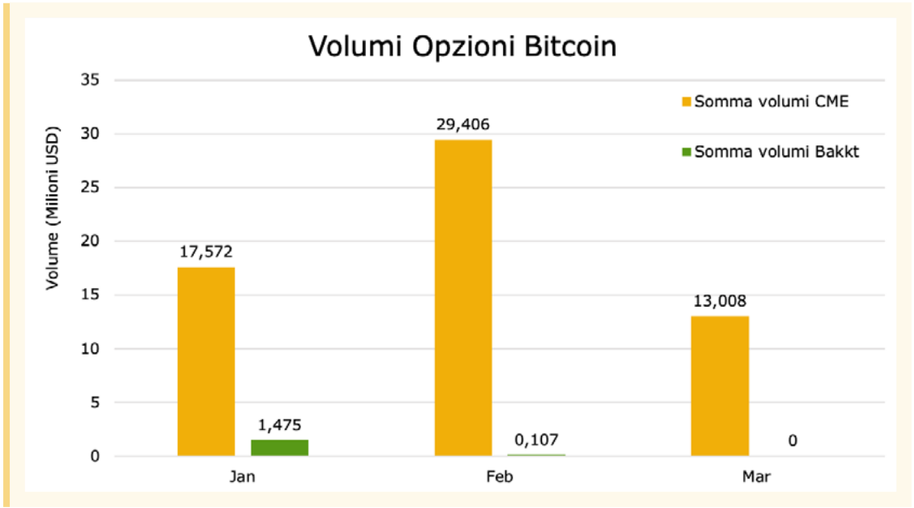


Nel precedente report 2019-Q4 avevamo parlato dell'inizio di negoziazione di opzioni su Bitcoin sulla borsa Bakkt (Deribit aveva già lanciato opzioni su Bitcoin nel 2016 ma non era un mercato regolamentato). CME, che per prima si era mossa sul mercato Futures, a settembre 2019 aveva annunciato che a inizio 2020 avrebbe avviato anche lei la negoziazione delle opzioni su Bitcoin. Come per i Futures, la sostanziale differenza tra Bakkt e CME si trova nel sottostante di tali contratti. Per quanto riguarda Bakkt, il sottostante dell'opzione sono Bitcoin "fisici"; per CME, invece, il sottostante è legato al valore in dollari del suo indice Bitcoin.

[4] https://cointelegraph.com/news/cme-bitcoin-futures-hit-100b-in-volume-since-2017-director-mccourt-says

[5] https://www.coindesk.com/cme-bitcoin-futures-daily-trading-volume-hits-2020-low-thats-a-bullish-sign

Nonostante Bakkt abbia anticipato di un mese la rivale, i volumi mostrano una vittoria schiacciante per CME: del 27 febbraio in poi Bakkt non ha più avuto volumi di scambio sul proprio prodotto[6].



ETF e Trust

Continua negli Stati Uniti la rincorsa per l'approvazione del primo ETF su Bitcoin. Nel precedente numero avevamo parlato della riapertura da parte della SEC del fascicolo presentato da Bitwise. Questa riapertura aveva colto tutti di sorpresa perché segnava un cambio di approccio da parte dell'autorità statunitense che in precedenza aveva a più riprese bocciato ogni richiesta di autorizzazione. In realtà, Bitwise ha formalmente ritirato la proposta nei primi giorni di gennaio per poter lavorare nuovamente alla documentazione e rispondere puntualmente alle questioni aperte più critiche[7]. Ricordiamo che la SEC aveva bocciato ad ottobre la proposta di Bitwise a causa delle manipolazioni degli scambi e delle attività illecite che comprometterebbero l'affidabilità del mercato Bitcoin.

Ad ogni modo, quella di Bitwise non è l'unica proposta di ETF. Il 26 febbraio la SEC ha annunciato di aver nuovamente rifiutato[8] la proposta di Wilshire Phoenix, adducendo ancora una volta come motivazione la scarsa affidabilità del mercato, per via delle frequenti manipolazioni e numerose frodi presenti nel mondo cripto. In questa nuova richiesta di approvazione, Wilshire Phoenix aveva sperato di aggirare il problema inserendo nell'ETF anche una quota di *Treasury Bond*[9]. Nella struttura dell'ETF proposta la quota di Treasury sarebbe stata automaticamente ribilanciata, incrementandosi nei momenti di alta volatilità di Bitcoin, riducendo di fatto l'influenza della manipolazione del prezzo della crypto-currency.

Il primo trimestre 2020 è stato, invece, ancora una volta molto positivo per Grayscale, che è riuscita a diventare una *SEC Reporting Company*, la prima nel mondo cripto. Questo risultato è un passo fondamentale per la trasparenza del Trust verso i suoi investitori.[10]

[6] https://www.theblockcrypto.com/post/54294/bakkts-bitcoin-options-saw-zero-volume-last-week

[7] https://www.coindesk.com/bitwise-withdraws-bitcoin-etf-application-with-the-sec

[8] https://www.sec.gov/rules/sro/nysearca/2020/34-88284.pdf

[9] https://www.coindesk.com/sec-rejects-latest-bitcoin-etf-bid

[10] https://www.globenewswire.com/news-release/2020/01/21/1973013/0/en/Grayscale-Bitcoin-Trust-Becomes-SEC-Reporting-Company.html

2. TECNOLOGIA

2.1 Bitcoin

Aggiornamento del protocollo

Il 2020 sarà un anno fondamentale per Bitcoin: la pressione sempre maggiore per aggiungere il nuovo algoritmo di firma digitale *Schnorr* (e tutti i benefici che esso comporta, primo fra tutti *Taproot*) potrebbe innescare un contenzioso all'interno del network. Nel mese di gennaio Pieter Wuille aveva già proposto alcune BIP (*Bitcoin Improvement Proposal*) alla comunità Bitcoin; le ha oggi riproposte formalmente, accompagnate da *pull-request* che, se accettate, modificano opportunamente il codice sorgente[11] di Bitcoin.

Pieter Wuille

Gli aggiornamenti di Bitcoin sono da sempre un tema estremamente delicato: nel passato ci sono stati accesi dibattiti ed addirittura, in alcuni casi, la nascita di *hard-fork* contenziosi come ad esempio Bitcoin Cash. In un network decentralizzato come Bitcoin, senza una figura centrale che governi e guidi le evoluzioni di protocollo, trovare un accordo è sempre complicato.

Nel caso di Schnorr l'aggiornamento del codice non sembra però essere controverso, a differenza di quanto avvenuto nel passato con Segwit: ha una relativa semplicità concettuale, bassi rischi per il funzionamento del protocollo e vede di conseguenza la comunità apparentemente favorevole. Questa volta il dibattito ruota fondamentalmente attorno alla modalità con cui l'aggiornamento dovrebbe essere attivato[12]. Esistono due principali alternative: una lascia il potere nelle mani dei miner e richiede che almeno il 95% della loro potenza computazionale approvi esplicitamente l'aggiornamento per attivarlo; l'altra metodologia, invece, coinvolge tutti gli attori dell'ecosistema, compresi gli utenti (UASF: *User Activated Soft Fork*). Quest'ultima tipologia è nata del 2017 come reazione all'oligarchia dei miner che volevano imporre un aggiornamento al quale la stragrande maggioranza degli utenti si opponeva: è più lenta rispetto ad una attivazione effettuata dai miner, ma ha il vantaggio di mostrare chiaramente quale sia la volontà della comunità Bitcoin. Il dibattito tra quale dei due metodi dovrà essere utilizzato per l'attivazione di Schnorr è ancora lontano dall'essere risolto e probabilmente l'accordo si troverà nel mezzo. Ad esempio, la proposta del core-developer Matt Corallo è quella di utilizzare i miner in prima istanza; se dopo un certo periodo di tempo non viene attivato l'aggiornamento, allora si passerà all'utilizzo di UASF. Questo approccio dilata notevolmente i tempi richiesti in caso di disaccordo tra i miner, ma rende il processo più sicuro.

Matt Corallo

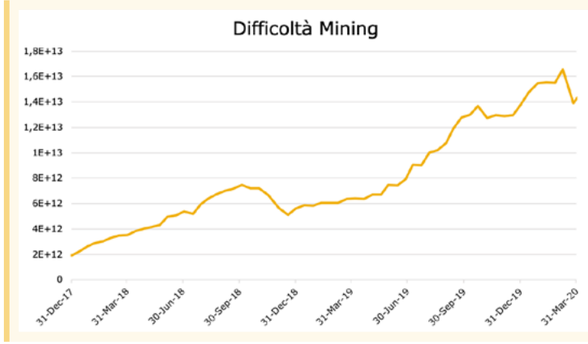
[11] https://github.com/bitcoin/bitcoin/pull/17977
[12] https://www.coindesk.com/bitcoin-coders-confront-an-old-quandary-how-to-upgrade-an-entire-network

Mining

Nei mesi scorsi avevamo raccontato della gara tra Bitmain, il maggiore produttore di hardware per mining al mondo, e Whinstone[13] per la realizzazione della più grande mining farm in Texas. Questa competizione ha contribuito da un lato alla continua crescita dell'*hash rate* del network (a gennaio è stato toccato il nuovo record storico di 119 EH/s[14]), dall'altro alla ridefinizione del panorama geografico, col generale spostamento del mining al di fuori della Cina (scesa dall'80% dell'hash rate globale a meno del 60%).

In questo trimestre, il crollo del valore di Bitcoin ha portato diversi operatori a spegnere il proprio hardware. Il marcato calo del prezzo ha provocato la diminuzione dell'hash rate, con conseguente correzione al ribasso della difficoltà computazionale richiesta per finalizzare un blocco: a fine marzo l'aggiustamento di difficoltà è stato -15,95%, per ampiezza la seconda maggiore correzione negativa della storia[15].

Inoltre nel 2020 ci sarà l'*halving*, il dimezzamento dell'emissione di Bitcoin che passerà da 12,5 per blocco a 6,25. Ogni 210000 blocchi (circa quattro anni) il tasso di emissione viene dimezzato, fino al raggiungimento di 21 milioni intorno al 2140: questo aggiustamento periodico è comunemente chiamato *halving*[16]. Fino ad oggi è avvenuto due volte: il 28 novembre 2012 (da 50 a 25 BTC) e il 9 luglio 2016 (da 25 a 12,5 BTC). Nella prima metà di maggio è previsto il prossimo[17], da 12,5 a 6,25 BTC per blocco. Sarà un banco di prova per la tenuta del network: dimezzandosi la profittabilità del mining, senza un sostanziale apprezzamento di Bitcoin, molti miner potrebbero spegnere il loro hardware innescando una ulteriore riduzione dell'hash rate.



Lightning Network

Continua lo sviluppo di *Lightning Network* (LN), la soluzione di secondo livello pensata per aumentare la scalabilità di Bitcoin, superandone i limiti intrinseci all'attuale protocollo. Purtroppo, lo stato di avanzamento di Lightining Network non è adeguato per applicazioni industriali reali e l'usabilità è ancora troppo complicata.

Nel mese di febbraio Jian-Hong Lin, Kevin Primicerio, Tiziano Squartini, Christian Decker and Claudio J. Tessone hanno pubblicato una ricerca, dal titolo *Lightning Network: a second path towards centralisation of the Bitcoin economy*[18], nella quale si evidenzia come il network LN sia ad oggi estremamente centralizzato: il 10% dei nodi attivi possiede infatti più dell'80% dei fondi totali presenti. Questo rappresenta una criticità: un malfunzionamento o un attacco a questi nodi causerebbe un'assenza di liquidità nel network e quindi l'impossibilità di effettuare transazioni. Gli sviluppatori confidano questa sia solo una situazione momentanea, che si risolverà una volta raggiunta maturità e usabilità, cioè quando anche utenti non tecnici saranno in grado di unirsi al network.

BITCOIN LIGHTNING NETWORK

Queste ultime evidenze si aggiungono alle perplessità che abbiamo da tempo manifestato su LN: a distanza di cinque anni dalla pubblicazione dell'idea, l'implementazione è ancora deficitaria e l'utilità tutta da dimostrare. Si avvicina forse il momento in cui dovremo costatare che il percorso immaginato è risultato non percorribile.

[13] https://www.coindesk.com/childhood-friends-battle-over-ownership-of-north-americas-largest-bitcoin-mine
[14] https://www.coindesk.com/bitcoin-mining-power-hits-fresh-all-time-high
[15] https://www.coindesk.com/bitcoin-mining-difficulty-posts-biggest-percentage-drop-ever
[16] https://www.coindesk.com/bitcoin-halving-explainer
[17] https://www.bitcoinblockhalf.com/
[18] https://arxiv.org/pdf/2002.02819.pdf

2.2 Altcoin

Ethereum

L'aggiornamento *Muir Glacier*

A nemmeno un mese dal precedente *Istanbul*, Ethereum ha effettuato l'aggiornamento *Muir Glacier*[19], con il solito approccio hard-fork non retrocompatibile, che lascia indietro chi non si aggiorna. Con Istanbul gli sviluppatori avevano infatti dimenticato di disinnescare la *time-bomb* del protocollo Ethereum, cioè l'aumento della difficoltà del mining originariamente previsto per forzare il passaggio dal consenso *proof-of-work* (dove l'influenza di ogni attore è proporzionale al lavoro svolto, cioè al consumo di energia elettrica dissipata, e crea inevitabilmente economie di scala e centralizzazione) a *proof-of-stake* (dove l'influenza di ogni attore è proporzionale alla quantità di coin posseduti).

Il passaggio a proof-of-stake, originariamente pianificato per il 2018, di certo non avverrà prima del 2021 e ci sono seri dubbi sulla sua fattibilità.

Per questo alcuni sviluppatori[20] propongono nel frattempo l'adozione di *ProgPoW*[21], un algoritmo di consenso *ASIC-resistant*, cioè difficile da implementabile in hardware appositamente specializzato (*Application Specific Integrated Circuits*).

Questo ridurrebbe il ruolo dominante dei grandi operatori, favoriti nell'accesso a hardware specializzato, contrastando la centralizzazione del mining. Anche qui, nonostante le buone intenzioni, emerge un certo velleitarismo. È infatti evidente sia dal punto di vista empirico sia da quello teorico che è impossibile impedire la specializzazione; per questo l'approccio migliore per avere risorse di mining accessibili a tanti è quello di avere algoritmi *ASIC-friendly*, così da abbassare per nuovi attori la soglia di ingresso al mining.

La confusione strategica sul destino dell'algoritmo di consenso è uno degli aspetti che meglio mettono in luce la precarietà dello sviluppo di Ethereum e la sua incerta sostenibilità nel tempo. Anche per questo, esperimenti di relativo successo come *Caspar Labs*[22] e *CryptoKitties*[23] (con i sui gattini virtuali, versione digitale dei vecchi *Tamagotchi*, la vera *killer-app* della piattaforma Ethereum) stanno passando a piattaforme alternative e/o proprietarie.

Soft-fork vs Hard-fork

Con il termine *soft-work* si indica una modifica retrocompatibile al protocollo Bitcoin, che si afferma solo se la maggioranza della rete la adotta. Viceversa, un *hard-fork* è coercitivo e partiziona il network in due reti non più compatibili: i nodi che adottano la modifica e quelli che non la recepiscono si ritrovano con due distinte blockchain.

[19] https://www.coindesk.com/muir-glacier-ethereum-hard-forks-for-second-time-in-one-month
[20] https://www.coindesk.com/ethereums-progpow-call-features-frustration-but-little-progress
[21] https://www.coindesk.com/a-101-guide-to-ethereums-progpow-controversy
[22] https://www.coindesk.com/casperlabs-pivots-away-from-ethereum-to-fundraise-with-its-own-blockchain
[23] https://www.coindesk.com/the-team-behind-cryptokitties-is-one-step-closer-to-leaving-ethereum

Questi ultimi in particolare soffrono i limiti transazionali di Ethereum (circa 15 transazioni al secondo): all'apice del successo il loro progetto aveva di fatto preso tutte le risorse disponibili, rendendo Ethereum inutilizzabile per altre applicazioni. Anche per questo Vitalik Buterin (fondatore di Ethereum) assieme a Joseph Poon avevano lanciato *Plasma*, per portare Lightning Network (di cui Poon è uno degli inventori) su Ethereum: ennesimo fallimento, oggi cambiano il nome del progetto in *Optimism*[24], scaramanticamente o forse per abbandonare il precedente marchio ormai percepito come fallimentare.

> *Impacchettare i fallimenti presentandoli in nuove vesti evolutive è pratica diffusa.*

Impacchettare i fallimenti presentandoli in nuove vesti evolutive è pratica diffusa: JP Morgan, campione nel promuovere dal 2016 *Quorum* come versione privata e scalabile di Ethereum, oggi fa confluire[25] il suo progetto in ConsenSys; in realtà abbandona semplicemente il campo[26] con grandi incertezze legate al futuro del suo team dedicato. ConsenSys, dal canto suo, entra in un consorzio con Microsoft ed Ernst & Young per un *Baseline Protocol* comune alle Ethereum private[27]; anche in questo caso la mossa sembra difensiva per cercare di salvare qualcosa da tentativi ad oggi abbastanza deludenti.

Ovviamente il dibattito pubblico più superficiale coglie poco di questi aspetti tecnici e così la notizia del trimestre è la donazione della Ethereum Foundation all'UNICEF, per rafforzare l'utilizzo di Ethereum nei progetti pilota[28] dell'organizzazione mondiale per l'infanzia abbandonata: la chiave del successo di Ethereum è da un lato la versatilità tecnologica (che però non funziona) dall'altro la capacità di relazioni pubbliche.

Altcoin e centralizzazione

La situazione generale

Se ad alcuni già Ethereum sembra avere uno sviluppo eccessivamente centralizzato e coercitivo con i suoi hard-fork, gli altri altcoin se la passano anche peggio.

Addirittura, di Steem si può dire che è stata "acquistata" da Justin Sun. Steem è basata su *Delegated Proof-of-Stake* (*DPoS*: "governano" un limitato numero di attori, con influenza proporzionale alla quantità di coin che posseggono o di cui ottengono delega) e Sun aveva ottenuto il controllo a febbraio di Steemit, il sito che possiede una grande quantità di Steem. I leader della comunità hanno fatto fronte comune[29] contro l'acquisizione[30] ed hanno promosso un controverso cambio di protocollo[31], dimostrando per l'ennesima volta che per alcuni coin le regole valgono solo fino a quando piacciono ai pochi determinati individui che controllano l'ecosistema. Sun ha però l'appoggio di molte borse di scambio[32], le quali hanno delegato a lui il potere di voto dei token scambiati sulle loro piattaforme: insomma, uno scenario di cordate e battaglie politiche ben distanti da una genuina decentralizzazione, una lezione da tenere bene a mente[33].

[24] https://www.coindesk.com/plasma-became-optimism-and-it-might-just-save-ethereum
[25] https://www.reuters.com/article/us-jp-morgan-blockchain-exclusive/exclusive-jpmorgan-in-talks-to-merge-blockchain-unit-quorum-with-startup-consensys-sources-idUSKBN2051AW
[26] https://www.coindesk.com/jpmorgan-may-merge-its-blockchain-project-with-ethereum-studio-consensys-report
[27] https://decrypt.co/21394/making-ethereum-a-safe-place-for-big-companies
[28] https://www.coindesk.com/how-the-ethereum-foundation-got-unicef-to-embrace-blockchain
[29] https://steemit.com/steem/@softfork222/soft-fork-222
[30] https://www.coindesk.com/justin-sun-bought-steemit-steem-moved-to-limit-his-power
[31] https://www.coindesk.com/steem-will-hard-fork-in-just-hours-over-community-fears-of-justin-sun-power-grab
[32] https://bitcoinist.com/steem-goes-down-after-major-exchanges-hijack-consensus-mechanism/
[33] https://www.coindesk.com/why-crypto-should-care-about-justin-suns-steem-drama

Justin Sun

Il controverso magnate asiatico ha recentemente donato $4.5M in beneficenza per il privilegio di cenare con Warren Buffet spiegandogli, senza successo, la rilevanza delle criptovalute.

Anche su EOS (che condivide DPoS con Steem) pare ci siano cartelli di controllo, sebbene non ci siano ancora delle evidenze. In generale PoS si presta alle manipolazioni dei gruppi di controllo: piaccia o meno, meglio comprendere che la dinamica è inevitabile anche quando apparentemente va tutto bene[34].

Se la qualifica di incidente principale del trimestre va a Steem, merita attenzione un altrettanto grave episodio che ha riguardato IOTA. Non ha fatto in tempo a celebrare l'entrata di Dell[35] in un working group su IOTA che due giorni dopo la *IOTA Foundation* ha dovuto fermare la rete. A seguito di una penetrazione malevola che aveva ottenuto i privilegi per rubare $2m ai nodi della rete, è stato fermato il nodo di coordinamento centrale e gli utenti sono stati invitati a non usare i loro *Trinity Wallet*[36]. Il nodo di coordinamento è stato fermo per 12 giorni[37], dimostrando come persino su una rete che dovrebbe essere dedicata all'*Internet of Things* (IOT) non c'è alcuna decentralizzazione reale ed esiste un singolo punto di vulnerabilità globale. Per rimediare, il fondatore di IOTA si è offerto di rimborsare personalmente le vittime dell'incidente ed ha garantito che la fondazione ha risorse significative, certificando definitivamente come l'esperimento sia personalistico e gestito centralmente.

Chiudiamo il tema delle criptovalute centralizzate menzionando il dibattito che ha lacerato Bitcoin Cash. Alcuni tra i leader di quella comunità hanno richiesto che il 12,5% della ricompensa usualmente destinata ai minatori per l'attività da loro svolta andasse invece a finanziare una fondazione dedicata allo sviluppo del protocollo. Ovviamente i minatori si sono opposti minacciando un hard-fork "scismatico" se la modifica fosse stata implementata.

La polemica è rilevante perché Bitcoin Cash nasce come piattaforma dove le prerogative di "governo" sono attribuite al mining e non distribuite tra tutti i nodi economicamente significativi come nel caso di Bitcoin. Ne è seguito un paradossale braccio di ferro[38] alla fine del quale la richiesta di sussidio allo sviluppo è stata abbandonata. Le tasse, come si sa, le può disporre solo il governo e lo fa solo a suo vantaggio.

[34] https://www.coindesk.com/on-eos-blockchain-vote-buying-is-business-as-usual
[35] https://www.coindesk.com/dell-among-founding-members-of-new-iota-working-group
[36] https://www.coindesk.com/iota-foundation-suspends-network-probes-fund-theft-in-trinity-wallet
[37] https://www.coindesk.com/iota-being-shut-off-is-the-latest-chapter-in-an-absurdist-history
[38] https://www.coindesk.com/roger-vers-mining-pool-pulls-support-for-bitcoin-cash-dev-fund-over-chain-split-threat

REPORT 2020-Q1

2.3 Blockchain

Algorand e AVA
I professori della blockchain

Silvio Micali

Silvio Micali è uno scienziato italiano di fama internazionale: ha vinto il premio Turing (l'equivalente del Nobel per l'informatica) e insegna al MIT. Da anni promuove Algorand come nuovo algoritmo di consenso distribuito. Nonostante il suo prestigio, la proposta non aveva mostrato i necessari elementi di significatività e praticabilità, sembrava pertanto destinata ad un caritatevole oblio. Ma il professore è riuscito a raccogliere l'anno scorso[39] $200m di finanziamenti ($60m dei quali tramite ICO) e recentemente ha debuttato la versione di test della piattaforma. La notizia del trimestre è che le Isole Marshall avrebbero selezionato Algorand per la loro moneta digitale[40].

Emin Gün Sirer

Anche Emin Gün Sirer è professore, in questo caso alla Cornell University, e direttore della *Initiative for Cryptocorrencies and Smart Contract*: da anni segue il fenomeno criptovalute, con maggiore competenza e coinvolgimento rispetto a Micali. Anche lui nel 2018 aveva proposto un nuovo protocollo, chiamato Avalanche, che aveva avuto scarso successo, ed ovviamente ha promosso una raccolta di fondi nel 2019 per portarne avanti lo sviluppo. In questo caso sono stati raccolti "solo" $6m, abbastanza comunque da consentire in questo trimestre l'allargamento del team di sviluppo di AVA Labs a 30 persone e spostare gli uffici da Brooklyn a Manhattan per stare più vicini alla comunità finanziaria a cui si rivolge[41].

Gün Sirer ha nel settore blockchain competenze migliori rispetto a Micali, ma in entrambi i casi riteniamo si tratti del solito fuoco di paglia blockchain, di cui sentiremo parlare solo finché non finiranno i fondi raccolti.

[39] https://finance.yahoo.com/news/second-chance-saloon-algorand-raised-101635928.html
[40] https://www.coindesk.com/algorand-blockchain-chosen-as-underlying-tech-for-marshall-islands-digital-currency
[41] https://www.coindesk.com/emin-gun-sirers-ava-labs-seeks-wall-street-business-after-open-sourcing-avalanche-protocol

3. REGOLAZIONE

Libra

Trimestre di assestamento relativamente più calmo per Libra, la criptovaluta promossa dal consorzio omonimo costituito in Svizzera e sostenuta principalmente da Facebook.

Sono entrati nel consorzio Shopify[42] e Tagomi[43], ma si registra l'abbandono di Vodafone[44], che segue l'uscita nello scorso trimestre di altri pesi massimi come PayPal, Mastercard, eBay e Visa. Il management di Libra non manifesta nervosismo[45] e lascia la porta aperta, adottando un modello consortile fluido.

Probabilmente anche per gettare acqua sulle polemiche incendiarie degli ultimi mesi, Libra non appare tra le priorità di Facebook, come delineate nella visione per il 2030[46] di Mark Zuckerberg.

Permangono le incertezze regolamentari: se il governo svizzero ammorbidisce i toni (dopo aver definito Libra un fallimento[47]) e sostiene di continuare il suo attento monitoraggio nei riguardi di quale forma Libra prenderà in futuro, è il regolatore europeo a lamentare[48] la mancanza di dettagli ed informazioni ufficiali sulla base delle quali poter decidere.

> *"Libra sta considerando di emettere sulla sua piattaforma una pluralità di token, ognuno con parità di cambio rispetto ad una diversa valuta sovrana, avvicinandosi più ad un sistema di pagamento che ad una valuta privata e indipendente."*

Il profilo più basso tenuto da Libra questo trimestre è, probabilmente, proprio l'ordine di scuderia mirato a consentire un riposizionamento del progetto rispetto ai regolatori. Di fronte al muro di critiche negli Stati Uniti derivanti dalla preoccupazione che il dollaro possa perdere il suo ruolo di asset di riferimento internazionale, Libra aveva già ipotizzato una parità di cambio con la valuta statunitense. Oggi sta addirittura considerando di emettere sulla sua piattaforma una pluralità di token, ognuno con parità di cambio rispetto ad una diversa valuta sovrana, avvicinandosi più ad un sistema di pagamento che ad una valuta privata e indipendente[49].

Central Bank Digital Currency

In scia al fenomeno Libra si muovono tutte le banche centrali. Lo ha chiarito esplicitamente il vicegovernatore di Bank of Canada, Timothy Lane: la sua istituzione non vede la necessità di una valuta sovrana digitale, a meno che non decolli un concorrente privato al contante[50]. Più aperturista nella forma, ma allineata nella sostanza, anche Christine Lagarde[51] che posiziona Banca Centrale Europea come interessata al fenomeno delle valute digitali, senza per questo scoraggiare iniziative private.

La banca centrale canadese ed europea sono in un gruppo di lavoro comune[52], assieme alla banca centrale svedese, svizzera, inglese e giapponese, sul tema Central Bank Digital Currency (CDBC). Il coordinamento è affidato alla Banca dei Regolamenti Internazionali (BIS: la "banca centrale delle banche centrali"). La stessa BIS, da sempre posizionata dal suo presidente su una linea di contrasto esplicito alle criptovalute, ha toccato l'argomento nel suo recente rapporto[53] sui sistemi di pagamento.

[42] https://www.coindesk.com/shopify-joins-libra-association
[43] https://www.coindesk.com/prime-broker-tagomi-becomes-22nd-member-of-facebooks-libra-association
[44] https://www.coindesk.com/vodafone-is-the-latest-big-company-to-quit-facebook-founded-libra-association
[45] https://www.coindesk.com/libra-head-not-worried-about-the-leavers
[46] https://www.coindesk.com/facebooks-zuckerberg-highlights-digital-commerce-but-not-libra-in-2030-vision
[47] https://www.coindesk.com/switzerland-softens-tone-on-libra-after-ex-president-says-project-failed
[48] https://www.coindesk.com/eu-official-we-cant-regulate-libra-without-more-details
[49] https://www.bloomberg.com/news/articles/2020-03-03/facebook-weighs-libra-revamp-to-win-over-reluctant-regulators
[50] https://www.coindesk.com/bank-of-canada-wont-issue-its-own-crypto-unless-libra-succeeds-deputy-governor
[51] https://www.coindesk.com/ecbs-lagarde-we-want-to-develop-digital-currencies-but-wont-discourage-private-initiatives
[52] https://www.coindesk.com/6-central-banks-form-digital-currency-use-case-working-group
[53] https://www.coindesk.com/bis-paper-reckons-with-p2p-payments-tokenized-securities-central-bank-digital-currencie

Ma il leader in ambito CBDC resta Bank of England, che già da anni aveva iniziato ad analizzare l'argomento con focus su innovazione e stabilità finanziaria[54]: ha rilasciato questo trimestre un'analisi[55] molto approfondita e un webinar che segnaliamo ai nostri lettori interessati; si tratta di un lavoro che segna anche il commiato di Mark Carney[56], il canadese alla guida di Bank of England negli ultimi sette anni, che si è sempre distinto per lucidità e pragmatismo sull'argomento.


Mark Carney

La Federal Reserve statunitense non fa invece parte del gruppo di lavoro comune in BIS: in tutti i possibili scenari gli Stati Uniti hanno solo da perdere (almeno potenzialmente) per un ruolo a qualsiasi titolo diminuito della loro valuta come riferimento internazionale. Dall'altra parte dell'Atlantico non manca comunque chi ritiene inevitabile un dollaro digitale accessibile a tutti, come l'ex presidente della CFTC Chris Giancarlo[57], o almeno una possibilità da non escludere come ammette lo stesso presidente della Fed Jerome Powell[58], se non altro per la marea di proposte sul tema dibattute nel Congresso degli Stati Uniti[59].

Il gruppo di lavoro BIS aveva annunciato[60] per metà aprile una prima riunione a Washington, probabilmente proprio per coinvolgere la Fed; nel ribaltamento di priorità dovuto alla pandemia Covid-19 non abbiamo evidenze pubbliche della conferma del meeting.

ESMA, Consob, G20 e BaFin

Non manca l'attenzione anche di altri attori internazionali come IOSCO[61] o il Word Economic Forum[62], a dimostrazione che Libra ha detonato la bomba costruita da Bitcoin: è ormai impossibile non riflettere sulla moneta al di fuori degli schemi consolidati ma obsoleti dell'ultimo secolo.

> *"Libra ha detonato la bomba innescata da Bitcoin: è ormai urgente riflettere sulla moneta al di fuori degli schemi consolidati ma obsoleti dell'ultimo secolo."*

In Europa ESMA (la *European Securities and Markets Authority*) ha concluso a marzo la raccolta dei pareri[63] per la definizione di un framework adeguato ai mercati di crypto-asset e nel secondo trimestre dovrebbe pubblicarne le evidenze[64]. A conferma di quanto il tema sia al centro delle sue preoccupazioni, lo ha esplicitato tra le priorità chiave per il biennio 2020-2022[65]: "*The dangers of cyberthreats to the financial system as a whole and a sound legal framework for crypto-assets are increasingly becoming areas of focus for ESMA together with the other ESAs, the ESRB, the ECB and the European Commission*". Nel frattempo, è intervenuta per limitare a 2:1 la leva[66] nei *Contracts for Differences* (CFD) su crypto-asset (per le valute tradizionali la leva è 30:1).

[54] https://www.coindesk.com/bank-of-englands-stablecoin-ruling-targets-financial-stability-exec-says
[55] https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discus-sion-paper
[56] https://www.coindesk.com/digital-pound-could-present-challenges-for-uk-says-mark-carney
[57] https://www.coindesk.com/when-will-we-see-the-digital-dollar-the-former-cftc-chairman-speaks-out
[58] https://www.coindesk.com/could-a-digital-dollar-compete-on-privacy-fed-chairman-powell-hints-it-might
[59] https://www.coindesk.com/how-a-flurry-of-digital-dollar-proposals-made-it-to-congress
[60] https://www.coindesk.com/new-central-bank-group-to-discuss-digital-currency-benefits-at-april-meeting-report
[61] https://www.coindesk.com/global-stablecoins-may-be-subject-to-securities-regulation-says-iosco
[62] https://www.theblockcrypto.com/post/53845/in-first-the-world-economic-forum-issues-framework-for-central-bank-digital-currencies
[63] https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf
[64] https://ec.europa.eu/eusurvey/runner/crypto-assets-2019
[65] https://www.esma.europa.eu/press-news/esma-news/esma-announces-key-priorities-2020-22
[66] https://www.esma.europa.eu/sites/default/files/library/esma35-43-1000_additional_information_on_the_agreed_product_intervention_measures_relating_to_contracts_for_differences_and_binary_options.pdf

In Italia la Consob ha pubblicato le evidenze della sua consultazione[67] sulle ICO ("Le offerte iniziali e gli scambi di cripto-attività"), a cui anche noi avevamo risposto[68] tramite il Crypto Asset Lab, la nostra iniziativa di ricerca congiunta con l'Università di Milano-Bicocca. Il documento Consob è sembrato a molti operatori del settore alquanto deludente; in effetti anche l'inusuale data di pubblicazione (il 2 gennaio) sembra suggerire la fretta di chiudere una consultazione partita a marzo 2019 e che rischiava ormai di sovrapporsi a quella di ESMA.

Ma sono due, a nostro avviso, i fronti davvero caldi del dibattito regolamentare.

Riunione del G20

Il primo riguarda la cosiddetta *travel rule*: l'obbligo per gli operatori in crypto-asset di identificare beneficiario ed originante di qualsiasi transazione. Nel mondo dei virtual asset, dove gli indirizzi coinvolti in una transazione non sono permanenti ma per lo stesso soggetto possono cambiare ad ogni transazione, il requisito è tecnicamente molto difficile da rispettare. Inoltre, una sua stringente applicazione rischia di spingere l'operatività dalle piattaforme di scambio regolamentate verso quelle più "corsare". Eppure, questa è la preoccupazione principale espressa su questi temi dal G20[69] di febbraio a Riyadh: che siano adottati gli standard proposti da FATF-GAFI di cui abbiamo parlato nel precedente report, primo fra tutti proprio la travel rule.

Il secondo fronte è europeo e riguarda la definizione di "strumento finanziario" applicata a bitcoin ed affini da BaFin, l'autorità di mercato tedesca[70]. Il diritto di mercato non è il punto di forza del nostro Istituto, ma condividiamo con molti dei nostri partner più qualificati in materia la preoccupazione su una definizione[71] che dal punto di vista del diritto comunitario ha diversi aspetti contestabili; il rischio è che una tale definizione, oltre che impropria, possa essere estremamente dannosa: se accolta a livello europeo, porterebbe agli obblighi di conformità regolamentare tipici del mercato finanziario tradizionale (ad esempio MIFID II). Analizzeremo meglio la situazione in questi mesi e riferiremo le nostre evidenze nel prossimo numero.

[67] http://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1
[68] https://cryptoassetlab.diseade.unimib.it/docs/20190605/risposta-consob.pdf
[69] https://www.coindesk.com/g20-urges-countries-to-adopt-tough-fatf-rules-on-cryptocurrencies
[70] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2020/meldung_2020_03_02_mb_kryptoverwahr-geschaeft.html
[71] https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html

4. ECOSISTEMA

La custodia dei crypto-asset

Anche nel primo trimestre del 2020 non sono mancate le novità nel mondo della custodia di asset digitali.

La grande protagonista è stata senza dubbio Gemini che nel mese di gennaio ha dato due importanti annunci. Il primo riguarda la polizza assicurativa che l'exchange offre ai clienti del proprio servizio di custodia. Il 23 gennaio la borsa di scambio dei fratelli Winklevoss ha infatti annunciato di aver lanciato la prima società assicurativa *captive* nel mondo cripto, la Nakamoto Ltd. con licenza emessa dalla Bermuda Monetary Authority[72]. Lo scopo di una assicurazione captive è quello di assicurare o riassicurare solamente i rischi della società controllante, in questo caso Gemini. Una tale società permette a Gemini di auto-assicurare il suo rischio, o almeno parte di esso, ed incassare quindi i premi derivanti da questa attività. Inoltre, la copertura di tale assicurazione è superiore a quella ottenibile tramite un assicuratore esterno. La copertura garantita da Nakamoto Ltd. è pari a $200 milioni, quasi il doppio dei valori usuali delle società di custodia che si affidano ad un assicuratore esterno, tipicamente Lloyds. Teniamo a precisare che questa assicurazione copre gli asset che sono depositati presso Gemini Custody, quelli invece detenuti sull'*hot wallet* dell'exchange (il portafoglio sempre collegato ad internet e quindi più insicuro), sono coperti da un'altra polizza assicurativa. Il record è stato comunque rapidamente superato: Bittrex ha annunciato[73] a fine gennaio il raggiungimento di un nuovo accordo con Marsh per l'estensione della copertura assicurativa a $300 milioni per gli asset depositati presso il proprio *cold wallet* (il portafoglio non collegato ad internet e quindi più sicuro). L'evidenza del momento è che l'appetito per questo tipo di prodotti assicurativi è alto: ci possiamo attendere altri significativi sviluppi nel corso dell'anno.

Il secondo annuncio del trimestre da parte di Gemini ha riguardato invece l'ottenimento della certificazione SOC 2 (System and Organization Controls 2) Type 2[74]. Nel gennaio 2019 Gemini aveva già ottenuto SOC 2 Type 1, una certificazione sul design e l'implementazione delle procedure di sicurezza ad un preciso istante temporale, il momento in cui avviene la valutazione. La certificazione Type 2, invece, certifica le medesime procedure di sicurezza ma su un intervallo di tempo, garantendo quindi la robustezza delle soluzioni implementate nel tempo. Gemini è stato il primo exchange e custode ad ottenere entrambe le certificazioni SOC 2: in entrambi i casi il certificatore è stato Deloitte & Touche LLP.

Da sinistra: Tyler Winklevoss (Gemini), E. David Burt (premier del governo di Bermuda) e Cameron Winklevoss (Gemini)

Il vantaggio competitivo di cui Gemini ha goduto in per le certificazioni SOC 2 è durato però solo qualche settimana. A metà febbraio, infatti, anche Coinbase ha annunciato[75] l'ottenimento della certificazione SOC 2 Type 2; il certificatore questa volta è stato Grant Thornton LLP. Allo stesso tempo Coinbase ha anche annunciato di aver ottenuto SOC 1 Type 2, divenendo di fatto la prima società di custodia di asset digitali a detenere sia SOC 1 che SOC 2. A differenza del SOC 2, incentrata sui controlli interni alla società per sicurezza e privacy, SOC 1 certifica i controlli interni effettuati sulla revisione dei financial statement dei clienti.

Ma la vera novità del trimestre per Coinbase riguarda il lancio ufficiale dei propri servizi di custodia anche in Europa[76], attraverso la creazione della Coinbase Custody International Ltd. con sede a Dublino in Irlanda. I servizi di custodia di Coinbase erano in realtà già presenti in Europa, ma con la creazione di questa nuova società localizzata in territorio europeo, Coinbase vuole mostrare una maggiore presenza e cura del cliente al di fuori degli Stati Uniti, probabilmente anche come reazione all'analoga mossa di Fidelity dello scorso dicembre.

Nel corso del trimestre non sono mancati anche nuovi attori. Il primo player ad investire nella custodia è stata la banca svizzera Julius Bear che attraverso una partnership con SEBA Bank AG ha aggiunto anche questo servizio alla sua offerta commerciale[77].

Un passo importante verso una maggiore adozione di Bitcoin in Italia è stato fatto da Banca Sella che ha aggiunto un wallet Bitcoin alla sua app di pagamenti Hype[78]. Questo risultato è il risultato della collaborazione con Conio, un wallet italiano, e permette agli utenti di Hype di comprare, vendere e scambiare Bitcoin direttamente tramite l'app della banca, semplificando notevolmente la *user experience* globale. Monitoreremo nei prossimi mesi l'avanzamento di questo progetto.

[72] https://gemini.com/blog/gemini-launches-captive-insurance-company-now-has-the-most-custody
[73] https://medium.com/bittrex/bittrex-inc-secures-300-million-in-digital-asset-insurance-to-enhance-protection-16fff23a98d1
[74] https://gemini.com/blog/gemini-completes-soc-2-type-2-examination-another-first-in-crypto
[75] https://blog.coinbase.com/in-another-first-coinbase-custody-attains-its-soc-1-and-soc-2-reports-836f836ec60a
[76] https://blog.coinbase.com/coinbase-custody-officially-launches-internationally-e4fee2ef4d84
[77] https://www.juliusbaer.com/ch/en/news/julius-baer-launches-digital-assets-services-2/
[78] https://sellanews.it/-/hype-lancia-il-wallet-digitale-per-l-acquisto-di-bitcoin-dalla-ap

Finanza tradizionale e DeFi

Il mondo della finanza tradizionale mostra ancora diffidenza verso bitcoin e crypto-asset; se intraprende qualche iniziativa innovativa, l'attenzione è comunque ancora sulla blockchain con intenti spesso implausibili e risultati alquanto goffi.

Jack Dorsey, Twitter, Square e Bitcoin

Jack Dorsey, CEO di Twitter e Square, ha lanciato sulla sua piattaforma di *messaging* un *emoji* automaticamente associato all'*hashtag #bitcoin*. La mossa è stata immediatamente popolare tra i bitcoiner e rappresenta probabilmente un ringraziamento: la metà dei ricavi di Square nell'ultimo trimestre 2019 sono stati legati alla compravendita di Bitcoin da parte dei suoi utenti. Square ha anche ottenuto questo trimestre un brevetto legato a transazioni tra cripto e valute tradizionali e continua a sostenere economicamente un team dedicato allo sviluppo del protocollo Bitcoin.

Ad esempio, Paxos e Credit Suisse avrebbero fatto il regolamento di liquidità contro azioni utilizzando la blockchain[79]: ammesso e non concesso che l'operazione abbia un qualche realismo, non si capisce quali sarebbero i benefici rispetto ai sistemi tradizionali.

Bank von der Heydt in Germania avrebbe emesso un suo *stablecoin* euro funzionale al collocamento di strumenti finanziari come token su blockchain: sostiene che le compravendite su un tale sistema sarebbero più economiche e meno complicate, senza necessità di un intermediario; insomma, la banca propone un sistema in cui lei come intermediario non serve più...

O ancora, HSBC avrebbe fatto un collocamento privato da dieci miliardi di dollari sulla blockchain Corda di R3[80], con l'obiettivo di arrivare a venti miliardi: ovviamente a parte la stampa specializzata che rilancia queste notizie folkloristiche, i mercati finanziari restano completamente indifferenti a queste iniziative senza reale sostanza che vada oltre l'effetto annuncio.

> *Dopo i fallimenti blockchain, distributed ledger, smart contracts e ICO, DeFi è l'ultima moda fatua.*

Dall'altro lato della barricata si contrappone il velleitarismo di *DeFi, Decentralized Finance*. Dopo i fallimenti blockchain, distributed ledger, smart contracts e ICO, DeFi è l'ultima moda fatua[81]. Si tratta di smart contract finanziari, ad esempio i popolari *flash loans*: prestiti istantanei in cui, contestualmente alla concessione del prestito, il capitale prestato viene automaticamente ed istantaneamente restituito, ma tra concessione e restituzione viene utilizzato per arbitraggi tra mercati. E si vedono anche i primi esperimenti su contratti assicurativi[82].

Questo trimestre DeFi ha superato il miliardo di dollari[83] ma ovviamente le promesse degli smart contract si sono rivelate ben poco smart: abbiamo visto il primo attacco[84] ai *flash loans*[85] che ha sottratto circa $350mila in ETH[86] e nel crollo delle quotazioni[87] legato al Covid-19 il sistema degli oracoli (sostanzialmente i fornitori dati con cui si regolano gli smart contract) non ha funzionato bene facendo collassare le funzionalità del sistema.

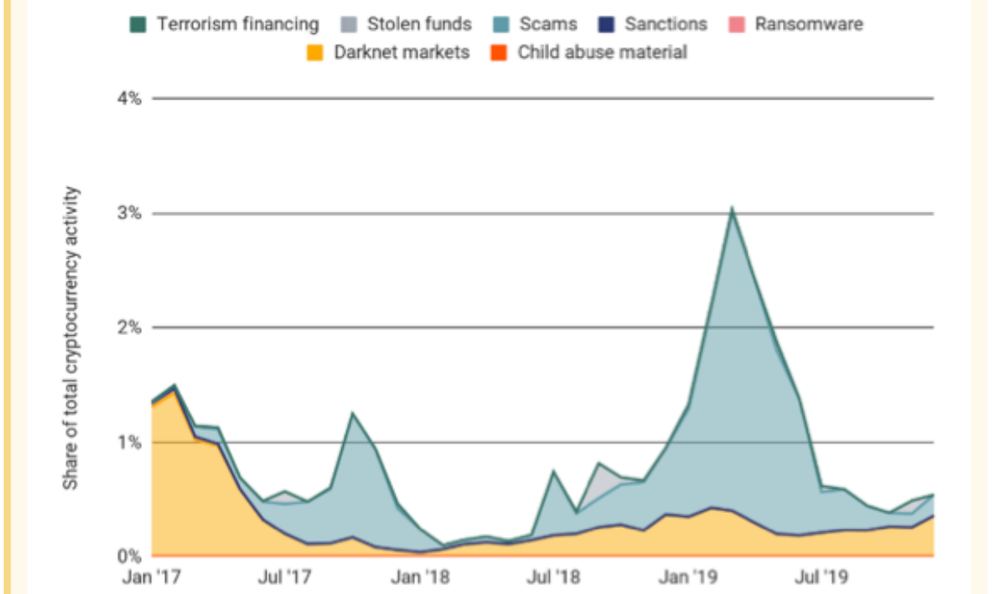
[79] https://www.coindesk.com/paxos-credit-suisse-claim-first-blockchain-based-settlement-of-us-equities
[80] https://www.coindesk.com/hsbc-puts-10b-of-private-placements-on-r3s-corda-blockchain
[81] https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4
[82] https://www.coindesk.com/defi-insurance-firm-nexus-mutual-makes-its-first-payout-following-bzx-attacks
[83] https://www.coindesk.com/why-defis-billion-dollar-milestone-matters
[84] https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack
[85] https://www.coindesk.com/the-flash-loan-attacks-explained-for-everybody
[86] https://blog.coinbase.com/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in-1289f7f77137
[87] https://www.coindesk.com/thursdays-market-madness-strained-ethereums-killer-app-defi

Chainalysis

Criptovalute e attività criminali

L'attenzione sulle attività criminali legate al mondo delle criptovalute è sempre alta. L'Interpol è intervenuta contro gli attacchi *malware* che infettavano router[88] internet, la società di sicurezza Kaspersky ha segnalato come alcuni hacker nord-coreani sottraessero crypto-asset agli utenti[89] della piattaforma di messagistica Telegram, l'FBI continua le sue indagini su Quadriga[90] (si veda il nostro report 2019-Q1).

In realtà, come chiarisce Chainalysis, società leader a livello internazionale per la forensica su blockchain, solo l'1% degli oltre 1000 miliardi di dollari transati in cripto ha collegamenti illeciti[91]: il *Crypto Crime Report* 2019[92] di Chainalysis è come sempre ricchissimo di dati ed analisi, ne suggeriamo la lettura. Non mancano le perplessità sulla relazione tra Chainalysis, il governo statunitense[93] e l'FBI: in realtà, è noto che governi ed agenzie di sicurezza usano la società per indagini basate sulla intrinseca trasparenza blockchain; inoltre, aiutare il contrasto al crimine è una attività legittima ed encomiabile. Diverso è il fatto che a valle delle loro indagini il Dipartimento del Tesoro metta in *blacklist* alcuni indirizzi bitcoin associati al team di hacker nord-coreani noto come *Lazarous Group*[94]: la creazione di blacklist è preoccupante per la fungibilità di bitcoin perché mette tutti nella situazione di non poter accettare bitcoin senza accertarne prima la provenienza, per escludere che arrivino da indirizzi proibiti. Qui il dibattito si complica (noi ricordiamo sempre che gli atomi di oro non raccontano nulla della loro storia), perché scarica sugli utenti responsabilità improprie, coprendo l'incapacità o pigrizia delle agenzie di indagine e sicurezza nell'incalzare direttamente il crimine.



[88] https://www.coindesk.com/interpol-leads-operation-to-tackle-cryptojacker-infecting-over-20000-routers
[89] https://www.coindesk.com/north-korean-hackers-now-using-telegram-to-steal-crypto-kaspersky
[90] https://www.coindesk.com/the-fbi-is-now-reaching-out-to-quadrigacx-victims
[91] https://cointelegraph.com/news/chainalysis-only-1-of-1-trillion-transacted-in-crypto-in-2019-was-illicit
[92] https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report
[93] https://www.coindesk.com/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government
[94] https://www.cryptopolitan.com/btc-addresses-north-korean-lazarus-group/

5. VITA DELL'ISTITUTO

Presentazione del report 2019-Q4

Raffaele Mauro

Il 28 gennaio, presso il Fintech District di Milano, si è tenuto il primo evento di presentazione del nostro report trimestrale; entrambi, report ed evento, sono in esclusiva per i nostri partner ed i loro ospiti. I fatti più rilevanti dell'ultimo trimestre del 2019, presentati nel report 2019-Q4, sono stati commentati dal nostro direttore Ferdinando Ametrano[95]; Raffaele Mauro di Endeavor Italia ha invece curato un approfondimento tecnico su Quantum Computing[96].

Hanno partecipato all'evento rappresentanti di diverse aziende: 981 Ventures Ltd, Banca d'Italia, Banca IMI, Borsa Italiana, CATTRe (Cattolica Assicurazioni), CheckSig, Crypto As-set Lab, Cryptofiduciaria, CryptoValues, Deloitte Consulting, DEPObank, Endeavor Italia, Fintech District, Generali Investment Asset and Wealth Management, Il Sole 24 Ore, Intesi Group, Kairos Partners SGR, London Stock Exchange Group, Ministero della Difesa, Oasi (CEDACRI), Par-Tec, Prometeia, SIA S.p.A., SIAT, Solution Bank, Studio Annunziata e Conso, Studio Avella, SZA Studio Legale, The Boston Consulting Group, The Rock Trading, Università Milano-Bicocca, Virgilius Wealth e Young Platform.

L'intenzione è di riproporre un evento di presentazione per ogni rapporto trimestrale, ma ovviamente questo trimestre Covid-19 ci costringerà ad una presentazione in streaming.

Ferdinando Ametrano

[95] https://dgi.io/docs/reports/2019Q4-presentation.pdf
[96] https://dgi.io/docs/reports/2019Q4-quantumcumputing.pdf

Dal sesterzio al Bitcoin

Vecchie e nuove dimensioni del denaro

"Dal sesterzio al Bitcoin. Vecchie e nuove dimensioni del denaro" (Rubbettino, 2020, euro 14)[97] è il nuovo volume collettaneo curato da Angelo Miglietta e Alberto Mingardi[98]. In equilibrio tra filosofia, storia ed economia ("vecchie e nuove dimensioni", come recita il suo sottotitolo), il libro si fa strumento al servizio di "un'autentica e feconda provocazione intellettuale"[99]: chiarisce come il denaro costituisca uno strumento di libertà e un vettore della società aperta, poiché riduce i pregiudizi per mezzo delle transazioni e dei contatti commerciali, innalza il tasso di tolleranza e il rispetto reciproco[100].

Come ci spiegano bene i diversi autori[101] che hanno contribuito al volume, tra cui il nostro direttore Ferdinando Ametrano, il denaro entra in connessione non solo con la libertà individuale, ma anche con il suo opposto: l'autorità pubblica. Benché "il denaro preceda, storicamente e logicamente, le zecche pubbliche" (Miglietta e Mingardi), è innegabile che esso sia ormai un'espressione tipica della sovranità statuale. Mai come nei nostri giorni, le Banche centrali, un tempo espressione neutrale, si sono scoperte luoghi di straordinaria concentrazione del potere. D'altra parte, lo "strapotere" delle Banche centrali non è insidiato solo dalle minacce governative, ma anche da nuovi tentativi di "liberalizzazione" del denaro: le criptovalute, tra cui la migliore è sicuramente Bitcoin.[102]

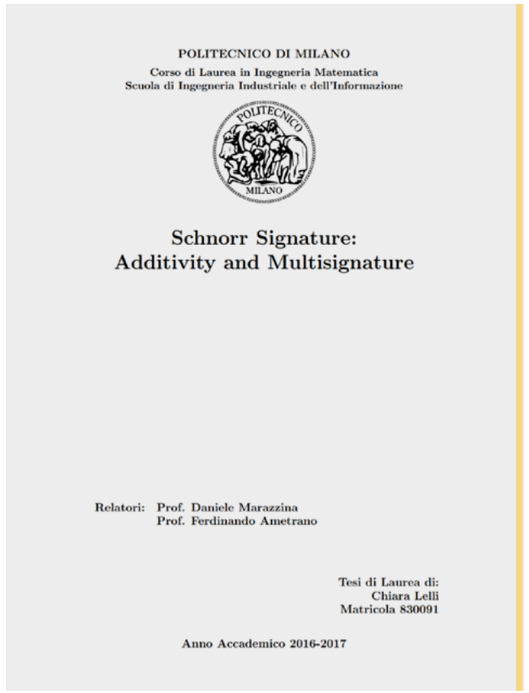
Come evidenziato dal capitolo curato da Ametrano all'interno del volume – *Bitcoin come oro digitale: asset di riserva per nuovi standard monetari* – sebbene Bitcoin sia un esperimento ardito che potrebbe fallire, e nonostante si siano osservati usi impropri, è indubbio che le criptovalute servano a rispondere a problemi che le valute statali non sono in grado di risolvere, specie quando è in gioco la libertà personale. Emerge quindi anche la prospettiva di adottare una moneta digitale di banca centrale per rispondere alle sfide aperte dalle cosiddette stablecoin (su tutte Libra di Facebook), dimostrando come l'innovazione sui temi monetari sia oggi spinta dall'iniziativa privata.

Temi affrontati anche dal vicedirettore generale della Banca d'Italia, Luigi Federico Signorini, nel suo intervento all'Università IULM di Milano in occasione della presentazione del volume il 17 febbraio.[103]

Insomma, consigliamo vivamente la lettura di questo volume, quale spunto di riflessione su moneta, banche centrali e Bitcoin. Riflessioni a caldo su un argomento che vede evoluzioni nuove e dirompenti: non ci si può esimere da un approfondimento su questi temi.

[97] https://www.store.rubbettinoeditore.it/dal-sesterzio-al-bitcoin.html
[98] http://www.brunoleoni.it/chi-siamo/executive-team/alberto-mingardi
[99] http://www.brunoleoni.it/dal-sesterzio-al-bitcoin-le-strade-della-liberta
[100] http://www.brunoleoni.it/dal-sesterzio-a-oggi-il-denaro-come-strumento-di-liberta
[101] Il volume presenta saggi di Alejandro Chafuen, Maria Pia Paganelli, Alberto Mingardi, Hans L. Eicholz, GeoffreyWood, Pedro Schwartz e Juan Castañeda, e Ferdinando M. Ametrano.
[102] http://www.brunoleoni.it/dal-sesterzio-al-bitcoin-le-strade-della-liberta
[103] http://www.brunoleoni.it/valute-digitali-i-due-ostacoli-sulla-via-delle-banche-centrali

Blockchain Education Network
Premio miglior tesi alla prima *alumna* DGI



POLITECNICO DI MILANO
Corso di Laurea in Ingegneria Matematica
Scuola di Ingegneria Industriale e dell'Informazione

Schnorr Signature:
Additivity and Multisignature

Relatori: Prof. Daniele Marazzina
Prof. Ferdinando Ametrano

Tesi di Laurea di:
Chiara Lelli
Matricola 830091

Anno Accademico 2016-2017

Il Blockchain Education Network (BEN) nasce all'inizio del 2014 dall'unione dei "Bitcoin Club" di Stanford, MIT, e University of Michigan col fine di educare gli studenti riguardo al potenziale delle criptovalute e della tecnologia alla base del Bitcoin. Da allora il network si è esteso in tutti i continenti: è nato anche BEN Italia.

Tra le attività promosse da BEN Italia, è istituito il "premio tesi BlockchainEdu" che premia la miglior tesi di laurea su blockchain e criptovalute.

Vincitrice del premio di questa prima edizione è Chiara Lelli, prima *alumna* del nostro centro di ricerca nel 2017, con la tesi dal titolo "*Schnorr Signature: Additivity and Multisignature*". Il risultato raggiunto dall'Ing. Lelli è conferma della lungimiranza del Digital Gold Institute sull'ecosistema Bitcoin e blockchain.

La tesi è consultabile nella pagina dedicata ai lavori di ricerca degli *alumni* DGI[105]; riportiamo sotto l'*abstract*, in inglese come nella tesi.

> *In 1991, Claus Peter Schnorr published on the Journal of Cryptology a paper titled "Efficient Signature Generation by Smart Cards", where he presented his idea for a new efficient signature scheme. It had many interesting features and benefits, but it had not been standardised due to a patent preventing widespread usage; researchers have recently proposed some possible approach, notably Pieter Wuille, Bitcoin Core developer. We followed his proposal and present our implementation of Schnorr Signature using Elliptic Curve Cryptography, based on the assumption of the Discrete Logarithm Problem.*
> *We start with an overview of the mathematic foundations of Elliptic Curve Cryptography and the assumptions on which it is based. Then we focus on Schnorr signature, starting from the analysis of the idea behind the algorithm, and presenting our Python implementation, explained step by step.*
> *A key point in our dissertation is the analysis of the benefits of Schnorr signature algorithm, among which one of the most important is additivity. This one is not present in other signature schemes and leads to a relevant feature: multisignature, a protocol through which a group of signers sign a common message, is reduced to be indistinguishable from a single signature.*
> *We implement this multisignature scheme showing the several benefits of it. Finally, we introduce Elliptic Curve Digital Signature Algorithm, currently used in Bitcoin, to appreciate how big an improvement Schnorr Signature Algorithm is compared to that.*

[104] https://www.blockchainedu.net/
[105] https://dgi.io/full-team/#alumni

REPORT 2020-Q1

42: la vita, l'universo e il tutto
Incluso Bitcoin

I matematici hanno finalmente risolto[106] un problema che era stato posto nel 1954: è possibile esprimere i numeri interi come somma di tre cubi[107]? Il quesito cerca, dato un numero intero k, la soluzione dell'equazione

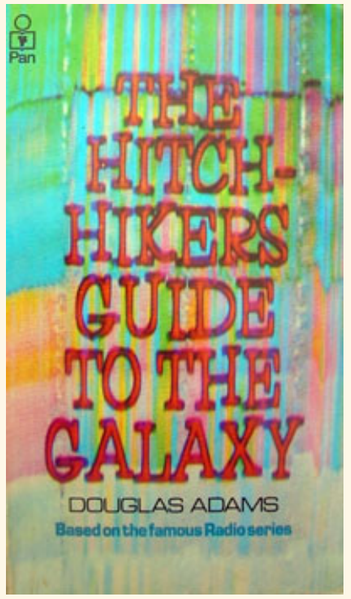
$$k= x^3+y^3+z^3$$

Che valore hanno x, y e z per ogni k?

Se era stato relativamente semplice trovare la risposta per quasi tutti i numeri inferiori a 100, la risposta per 33 e 42 tardava ad arrivare. Nel 2019 Andrew Booker ha trovato la soluzione per 33, facendo lavorare per tre settimane i supercomputer dell'*Advanced Computing Research Centre* dell'università di Bristol, ma 42 restava difficilissimo. Infine, affiancato da Andrew Sutherland del MIT, esperto di calcolo massivamente parallelo, la coppia ha finalmente scoperto che

$$42=-80538738812075974^3+80435758145817515^3+12602123297335631^3$$

42 e Bitcoin



Che 42 fosse straordinariamente elusivo, lo aveva rivelato per primo Douglas Adams nel 1983; infatti, in *The Hitchhiker's Guide to the Galaxy*[108] Adams aveva sostenuto che 42 fosse la risposta alla domanda fondamentale sulla vita, l'universo e il tutto, calcolata da un potentissimo supercomputer chiamato *Deep Thought* (Pensiero Profondo) dopo computazioni durate ben 7,5 milioni di anni. La relazione con Bitcoin è stata chiarita[109] dal direttore del nostro Istituto, Ferdinando Ametrano, che per primo ha rivelato un fatto finora ignoto: "Satoshi Nakamoto ha scelto il limite di 21 milioni per Bitcoin come umile omaggio al numero 42. Il creatore di Bitcoin voleva così esprimere la speranza che la sua invenzione potesse essere la risposta a tutte le esigenze monetarie dell'universo, ma si è umilmente limitato a 21, sperando potesse essere rilevante almeno quanto la metà di 42, la risposta alla domanda di significato di tutto".

Siamo certi che questi risultati scientifici avranno un ruolo decisivo nel dibattito dei prossimi anni.

[106] https://www.sciencealert.com/mathematicians-solve-a-long-standing-42-problem-using-planetary-supercomputer
[107] https://en.wikipedia.org/wiki/Sums_of_three_cubes
[108] https://en.wikipedia.org/wiki/42_(number)#The_Hitchhiker's_Guide_to_the_Galaxy
[109] https://twitter.com/Ferdinando1970/status/1224075453155233793?s=20

Save the date

Il Digital Gold Institute (DGI) aiuta i suoi partner ed il loro business con eventi, attività e corsi di formazione, mirati alla corretta comprensione di Bitcoin, asset crittografici e tecnologia blockchain. Sotto riportiamo le iniziative in programma nei prossimi mesi e vi invitiamo a consultare la pagina "eventi" del nostro sito per essere sempre aggiornati; potete anche contattaci direttamente scrivendo a events@dgi.io

Bitcoin e blockchain

21-22 aprile e 21-22 luglio

Bitcoin e blockchain è il *training program* di DGI: due workshop rivolti a chi vuole approfondire Bitcoin e la sua tecnologia blockchain. Strutturato per diversi livelli di competenza, é acquistabile sia interamente sia scegliendo solo una delle due giornate proposte. Per i partner DGI sono riservati due biglietti gratuiti; per ulteriori biglietti lo sconto è del 50% utilizzando al checkout il codice PARTNERDGI.

Presentazione report trimestrale

7 luglio

Presentazione dell'attività di ricerca svolte nell'ultimo trimestre dal nostro Istituto: scenari di mercato, normativi e tecnologici saranno analizzati evidenziandone criticità e opportunità. L'incontro è dedicato ai protagonisti di industria, accademia ed informazione più sensibili su questi temi.

Bitcoin, blockchain e crypto-asset: impatti nei settori finanziari e assicurativi

15 settembre

Il corso è organizzato dalla London Stock Exchange Academy con relatori Ferdinando Ametrano (Digital Gold Institute), Vito Barbera (Crypto Asset Lab), Francesca Mattasoglio (Università Milano-Bicocca), Paolo Mazzocchi (CheckSig), Andrea Medri (The Rock Trading) e Stefano Rossi (CryptoValues). Ha l'obiettivo di fornire ai partecipanti, anche senza pregressa esperienza sul tema, un'occasione per comprendere i meccanismi di funzionamento della blockchain e del suo collegamento con Bitcoin, conoscere lo stato dell'arte della regolamentazione di questo settore ed analizzare le modalità di prevenzione dei rischi finanziari collegati, anche richiamando casi pratici, in particolare in ambito antiriciclaggio.

CAL2020

16 Settembre

CAL2020 è la seconda edizione della conferenza organizzata da Crypto Asset Lab, *joint venture* tra il nostro Istituto e l'Università di Milano-Bicocca. La conferenza vanta un eccellente *program committee* che valuta la proposta di lavori scientifici in materia di investimenti, economia e regolamentazione per Bitcoin e criptoasset; i *paper* selezionati potranno essere pubblicati sulla rivista scientifica *Economic Notes*. La partecipazione alla conferenza è gratuita: si rivolge principalmente a ricercatori, docenti, professionisti, aziende ed istituzioni; sono benvenuti anche studenti e semplici interessati. Maggiori informazioni disponibili sulla pagina dedicata alla conferenza: https://cryptoassetlab.diseade.unimib.it/cal2020

Autori

Ferdinando M. Ametrano
ferdinando@dgi.io

Lucia Mandelli
lucia@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 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

@DigitalGoldInst

@DigitalGoldInstitute

@DigitalGoldInstitute

@dginst

@DigitalGoldInstitute