n. 3

Digital Gold Institute

Scarcity in the Digital Realm

Report Trimestrale

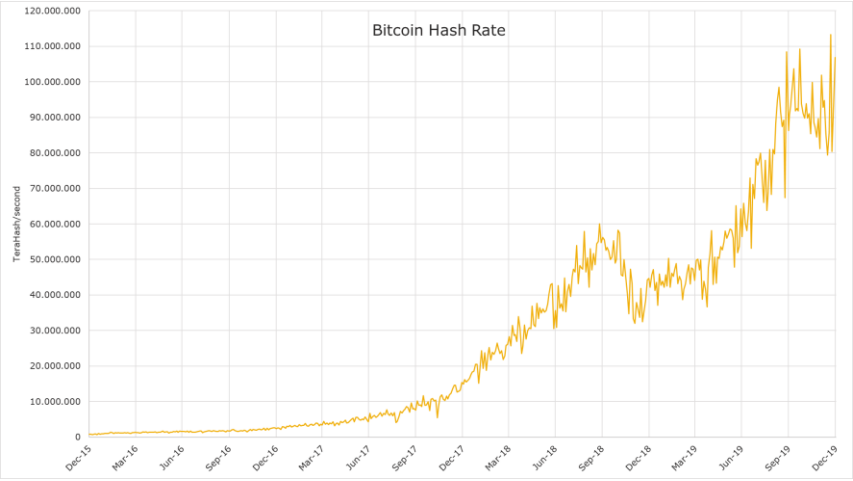
2019-Q4

Editoriale

La chiusura dell'anno è inevitabilmente tempo di bilanci, per cui il nostro sguardo, pur focalizzato sul quarto trimestre, inevitabilmente abbraccia tutto il 2019.

È sempre opportuno partire dal mercato, che rappresenta il luogo dove viene messo a fuoco il valore di asset, idee e progetti. Bitcoin ha registrato una performance del 92%, nonostante il secondo semestre sia stato significativamente negativo. Ed altrettanto effervescente è stata l'offerta di prodotti finanziari denominati in Bitcoin: futures, opzioni, ETN, ETP. Grayscale Trust ha superato il miliardo di dollari di crypto-asset gestiti ed i fondi pensione americani iniziano timidamente a sondare l'investimento in Bitcoin.

Tra i servizi finanziari per Bitcoin e crypto-assets, svolge un ruolo cruciale la custodia, precondizione per l'ingresso dei capitali istituzionali nel mercato. Questo trimestre il tema è esploso e ve lo raccontiamo nella sezione ecosistema. Crediamo molto nella custodia: nello scorso semestre la nostra ricerca ha messo a fuoco un protocollo innovativo che riteniamo superiore a tutte le soluzioni attualmente sul mercato. Ci crediamo talmente tanto che abbiamo costituito una startup dedicata alla custodia: CheckSig. Lo dichiariamo senza timore di conflitti di interesse: da sempre *we walk the talk*, diciamo quello che pensiamo e facciamo quello che diciamo. La credibilità accumulata in questi anni ci ha consentito di raccogliere capitali con sorprendente facilità: un milione di euro per il 20% di CheckSig, con una valutazione implicita di cinque milioni di euro al momento della costituzione dell'azienda. E questo è ovviamente solo l'inizio…



Potenza computazionale del network Bitcoin

Dal punto di visto tecnologico, il 2019 è stato l'anno delle soluzioni di secondo livello: Lightning Network e Liquid. Nonostante gli sviluppi intensi, noi siamo rimasti poco convinti di efficacia ed utilità… il tempo giudicherà. Gli sviluppi sul protocollo vero e proprio, come nel 2018, hanno covato sotto la cenere: in realtà la qualità e quantità di lavoro fatto è enorme ed i risultati ottenuti (*Taproot* e *Schnorr* su tutti) sono adesso pronti per essere valutati in funzione dell'adozione nel protocollo Bitcoin. Il tema ci affascina ed entusiasma: siamo pronti a raccontarvelo nel nuovo anno. Nel frattempo, non manchiamo di segnalare che la potenza computazionale della rete Bitcoin ha segnato un nuovo record superando i 100EH/s (exa-hash al secondo)

La notizia della *quantum supremacy* dimostrata da Google ha sollevato qualche preoccupazione per la sicurezza crittografica di Bitcoin e del sistema finanziario e militare. Il tema merita una disanima seria ed approfondita: la trovate sempre nella sezione tecnologia di questo numero. La conclusione è che per ora non c'è davvero da preoccuparsi.

Sul fronte tecnologico il 2019 ha segnato anche un generale ridimensionamento delle tendenze a cui non abbiamo mai fatto mancare le nostre critiche: la blockchain magica, le ICO e per certi aspetti anche Ethereum. Introdotti spesso come alternativa a Bitcoin, alla prova del tempo stanno mostrando i loro limiti.

Rilevantissimo invece il dibattito su Libra e *stablecoin*, che occupa gran parte della sezione regolazione. Se vi hanno appassionato le puntate precedenti, non potete perdervi questo aggiornamento che vede tutte le banche centrali rincorrere Zuckerberg. Per quanto ci riguarda, riteniamo che il tema possa rappresentare una tra le sfide più decisive del prossimo decennio. Bitcoin ha innescato il potenziale per una svolta senza precedenti nella storia della moneta: Libra è solo la prima bomba culturale che scoppia.

Nella sezione regolazione trovate anche un aggiornamento sullo sviluppo da parte di FAFT-GAFI delle linee guida per il contrasto a riciclaggio, finanziamento del terrorismo e reati finanziari compiuti con crypto-assets. Il tema è delicato perché risulta tecnicamente difficile riproporre in ambito crypto i paradigmi tradizionali. Considerando l'esplosione dei servizi finanziari basati su Bitcoin, sarà essenziale monitorare anche questo tema.

Infine, qualche cenno sulla vita dell'istituto: il lancio del nostro programma di formazione, l'ingresso nel gruppo Global Digital Finance del Crypto Asset Lab (la nostra iniziativa di ricerca congiunta con l'Università degli Studi di Milano-Bicocca), interviste e tavole rotonde.

Da ultimo il trasferimento dei nostri uffici al *Fintech District* di Milano: veniteci a trovare!

Indice

1. Mercato 1
Performance Bitcoin 2
Performance alt-coin 4
Bakkt: lancio dei futures a Singapore e opzioni a New York 4
ETF su Bitcoin 5
WisdomTree lancia un ETP su Bitcoin 6
La grande crescita di Grayscale nel 2019 6
Fondi pensioni statunitensi aumentano l'esposizione sul mondo crypto 7
2. Tecnologia 8
2.1 Bitcoin 9
Nuovo rilascio per *Bitcoin Core* 9
Bitcoin: che cosa è avvenuto nel 2019 10
Soluzioni di secondo livello: Lightning Network e Liquid 10
La crescita continua del *mining*: inaugurate nuove *mining farm* 11
2.2 Blockchain, crittografia ed applicazioni non monetarie 13
Quantum Supremacy 13
La chimera della *blockchain revolution* 14
2.3 Altcoin 15
Ethereum: l'aggiornamento *Istanbul* 15
3. Regolazione 16
Libra e *stablecoin* 17
FAFT: linee guida per la prevenzione di reati finanziari 19
Il mondo delle ICO 20
4. Ecosistema 21
Crypto-assets custody 22
BitMex rivela mail utenti, furto di Ether su Upbit 24
Poloniex abbandona il KYC 24
5. Vita dell'Istituto 25
DGI Training Program 26
SIAT Magazine: intervista a Ferdinando M. Ametrano 26
Crypto Asset Lab membro del Global Digital Finance 27
Il Salone dei pagamenti – Payvolution 27
DGI entra nella community del Fintech District 27

1. Mercato

Performance Bitcoin

Il quarto trimestre 2019, come il precedente, è stato caratterizzato da un calo della quotazione del prezzo Bitcoin: -11%.

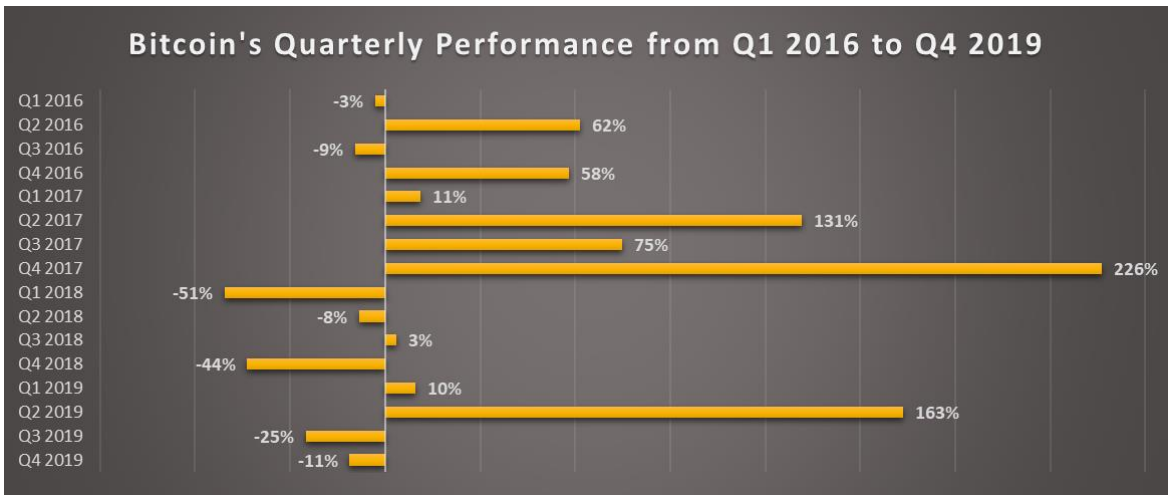


Figura 1: Redimenti trimestrali di Bitcoin

Dopo il crollo di prezzo di fine settembre che aveva portato Bitcoin da $10,000 a $8,000 in poche ore, l'ultimo trimestre 2019 si era aperto con un periodo di sostanziale stabilità. Questo periodo si è bruscamente interrotto tra il 25 e il 26 di ottobre, quando nell'arco di 24 ore Bitcoin ha visto un rialzo superiore al 40%, segnando il terzo maggior rialzo giornaliero della storia[1]. Questo dato è ancora più significativo se si pensa che i due rialzi giornalieri più alti di sempre si sono registrati prima del 2011, quando il mercato aveva volumi di scambio molto più contenuti. I motivi di questa corsa al rialzo si possono ricondurre alle dichiarazioni del leader cinese Xi Jinping, che ha pubblicamente dichiarato l'interesse della Cina a cogliere le opportunità che la tecnologia blockchain può offrire[2]. È importante ricordare che in Cina le crypto-valute sono fortemente osteggiate dalla banca

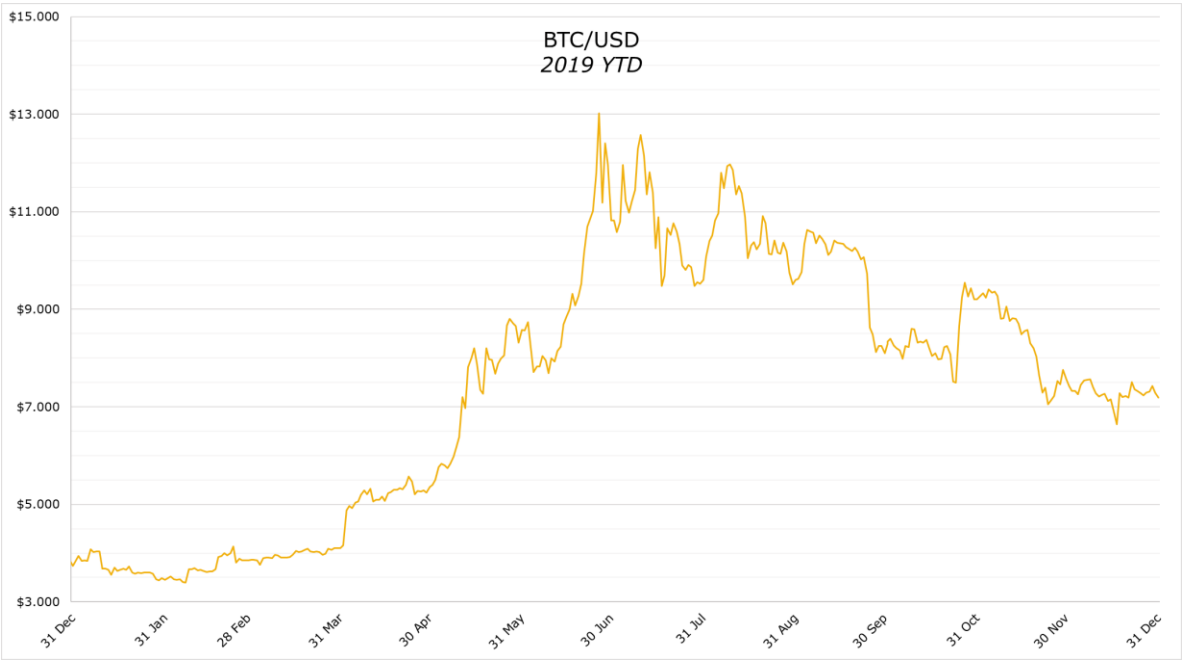


Figura 2: Rendimento Bitcoin 2019

[1] https://www.coindesk.com/Bitcoin-price-hits-five-week-high-above-10000
[2] https://www.coindesk.com/president-xi-says-china-should-seize-opportunity-to-adopt-blockchain

Figura 3: Rendimento Bitcoin quarto trimestre 2019

Il 2019 rimane un anno molto positivo per Bitcoin. Dopo un 2018 caratterizzato dal segno meno (-74%), il 2019 si è concluso con un +92%.

centrale *People Bank of China*. Il forte entusiasmo del momento è stato però seguito da una fase di ritracciatura che ha riportato i livelli al di sotto del valore di inizio trimestre (si veda *Figura 1*).

Il 2019 rimane comunque un anno molto positivo per Bitcoin. Dopo un 2018 caratterizzato dal segno meno (-74%), il 2019 si è concluso con un +92%, indubbiamente grazie alla forte crescita che ha fatto registrare il secondo trimestre (+163%).

Come già evidenziato in passato, una delle migliori metriche per valutare la crescita di Bitcoin è la serie dei minimi per anno: anche il 2019 conferma la tendenza di crescita sostanzialmente inarrestabile, con l'unica eccezione nel 2015 quando si è registrato un minimo inferiore al precedente. Ed a meno di tracolli clamorosi, nel 2020 un Bitcoin che dovesse marcare dei minimi in zona $7000 segnerebbe comunque l'ennesimo raddoppio di valore.

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

Figura 3: Prezzo minimo Bitcoin per anno

Vale la pena segnalare un altro indicatore: il numero di indirizzi a cui è associato un quantitativo non nullo di Bitcoin. In costante crescita esponenziale fino alla "bolla" di fine 2017, questo numero ha ripreso a crescere registrando a fine ottobre il massimo di sempre: 28,384,557 indirizzi[3]. Non è un indicatore eccessivamente significativo (perché facile da manipolare), ma è comunque l'ennesimo segno della resilienza di Bitcoin.

[3] https://Bitcoinmagazine.com/articles/Bitcoin-addresses-balance-hit-time-high

Performance alt-coin

Come sempre documentiamo anche le performance delle principali alt-coin: Ethereum, Ripple, Litecoin, Bitcoin Cash, Stellar, Ethereum Classic, Zcash, Monero. In figura sono riportati i rendimenti espressi in Bitcoin: quanto avrebbe reso un Bitcoin investito ad inizio periodo in ognuno degli alt-coin considerati.

Come si può vedere dal grafico (Figura 4), nonostante la performance negativa di Bitcoin nel trimestre, il rendimento degli alt-coin è stato peggiore, con la sola eccezione di Ethereum Classic e Bitcoin Cash, che hanno chiuso in leggero rialzo rispetto a Bitcoin.

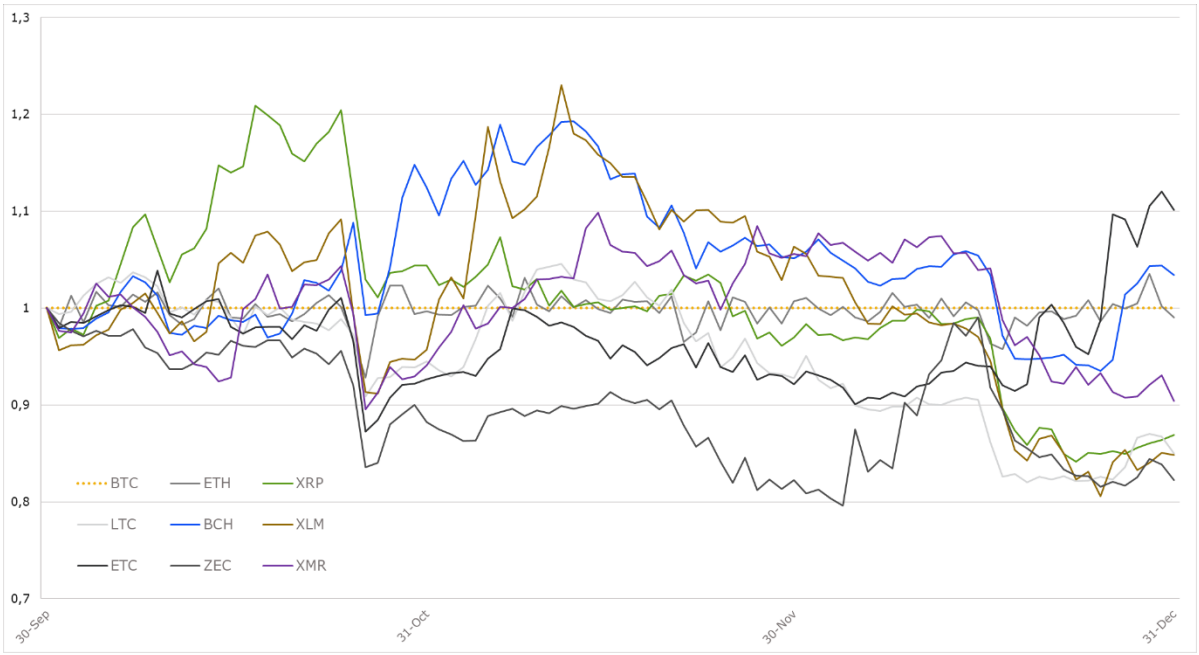


Figura 4: Rendimenti alt-coin rispetto a Bitcoin. È qualificante denominare la performance degli alt-coin in Bitcoin: qualsiasi investimento in crypto-asset che non sia Bitcoin si pone intrinsecamente come alternativo a Bitcoin e su quel metro va misurato.

Bakkt: lancio dei futures a Singapore e opzioni a New York

Nel precedente numero avevamo riportato la tiepida accoglienza riservata dal mercato al lancio ufficiale dei futures proposti da Bakkt (gruppo ICE, New York Stock Exchange). Dopo un avvio in sordina, nel quarto trimestre i volumi sono aumentati significativamente, mostrando una significativa crescita (si veda Figura 5).

Se la partenza aveva sofferto i continui rinvii da parte delle autorità americane sulla concessione a quotare i contratti, il trimestre appena concluso è stato in realtà molto proficuo per Bakkt che ha concluso l'anno presentando una gamma ampia di prodotti finanziari denominati in Bitcoin.

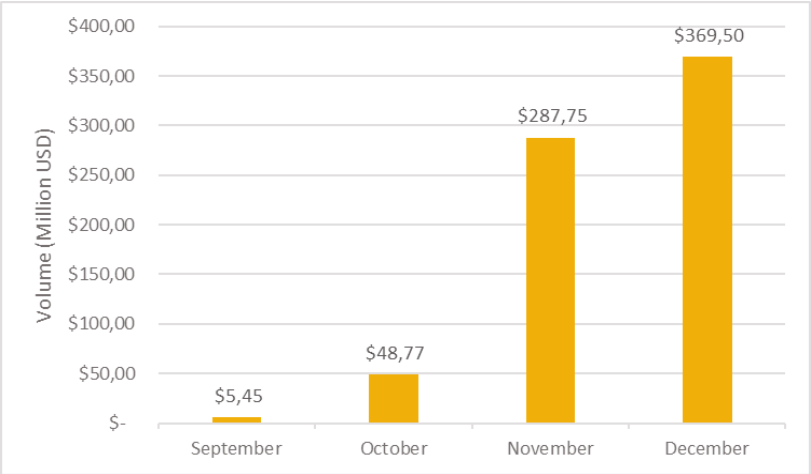


Figura 5: Volumi mensili contratti scambiati in Milioni di dollari

Spiccano in particolare i futures mensili per il mercato asiatico: questi contratti

sono scambiati dal 9 dicembre su ICE Futures Singapore, con clearing presso ICE Clear Singapore[4]. A differenza dei futures scambiati sul mercato americano, questi sono *cash-settled*, non prevedono cioè la consegna "fisica" di Bitcoin a scadenza del contratto. Il *reference settlement price* dei contratti asiatici è comunque quello dei contratti scambiati sul mercato americano[5].

The Bakkt Bitcoin Options contract represents another important step in developing this asset class for institutional investors, their customers and investors.

Oltre a l'estensione dell'operatività a Singapore, Bakkt ha introdotto a New York i primi contratti di opzioni su Bitcoin. Il CEO di Bakkt, Kelly Loeffler, ha dichiarato[6]: *"The Bakkt Bitcoin Options contract represents another important step in developing this asset class for institutional investors, their customers and investors".*

ETF su Bitcoin

Nel precedente numero del report abbiamo parlato dell'autorizzazione ottenuta da VanEck e SolidX per l'emissione di ETF aperti ai soli clienti istituzionali o accreditati. L'autorizzazione della SEC per ETF aperti risulta invece ancora distante.

Nel mese di ottobre SEC si è infatti nuovamente espressa contro la proposta di ETF promossa da Bitwise Asset Management insieme a NYSE Arca[7] (la borsa di scambio sulla quale verrebbero effettivamente scambiate le quote del fondo) a causa delle manipolazioni di mercato e attività illecite ancora largamente diffuse sul mercato Bitcoin. Citando il documento pubblicato dalla SEC[8]: *"NYSE Arca has not met its burden under the Exchange Act and the Commission's Rules of Practice to demonstrate that its proposal is consistent with the requirements of Exchange Act Section 6(b)(5), and, in particular, the requirement that the rules of a national securities Exchange be designed to prevent fraudulent and manipulative acts and practices".*

Come è possibile che il mercato Bitcoin sia trasparente ed affidabile per la CFTC ma quello stesso mercato sia fraudolentemente manipolato secondo la SEC da ritenere il prezzo di riferimento dei futures inutilizzabile per il NAV di un fondo?

Bitwise nella sua proposta aveva fornito un accurato approfondimento su questa tematica, evidenziando effettivamente come il mercato sia affollato da Exchange che pubblicano volumi falsi e manipolano il mercato a proprio vantaggio. Bitwise propone però di risolvere il problema semplicemente usando gli Exchange ritenuti affidabili sulla base di accurate analisi. Peraltro, questo approccio è simile a quanto fa CME per i suoi futures: il prezzo di riferimento viene calcolato utilizzando un panel di Exchange selezionati. Noi ci limitiamo a ripetere una osservazione scontata che rivela le contraddizioni logiche dei regolatori americani: come è possibile che il mercato Bitcoin sia trasparente ed affidabile per la CFTC (*Commodity Futures Trading Commission*), tanto da autorizzare i contratti futures che ogni giorno fissano un prezzo di riferimento, ma quello stesso mercato sia fraudolentemente manipolato secondo la SEC (*Securities and Exchange Commission*) tanto da ritenere il prezzo di riferimento dei futures inutilizzabile per il NAV di un fondo? Del resto, i giochi non sono ancora chiusi: la SEC ha annunciato la riapertura del fascicolo sull'approvazione dell'ETF[9].

[4] https://ir.theice.com/press/press-releases/all-categories/2019/11-21-2019-235911370
[5] https://www.theice.com/products/73194874/Bakkt-Bitcoin-USD-Cash-Settled-Monthly-Futures
[6] https://medium.com/bakkt-blog/bakkt-Bitcoin-options-on-futures-to-launch-december-9-an-industry-first-8fb2bd686abb
[7] https://www.nyse.com/markets/nyse-arca
[8] https://www.sec.gov/rules/sro/nysearca/2019/34-87267.pdf
[9] https://www.federalregister.gov/documents/2019/11/18/2019-24874/self-regulatory-organizations-nyse-arca-inc-order-scheduling-filing-of-statements-on-review-for-an

WisdomTree lancia un ETP su Bitcoin

Bakkt non è stata la sola società a lanciare nuovi prodotti finanziari su Bitcoin. WisdomTree, uno dei più grandi emittenti di ETF al mondo, ha annunciato[10] a inizio dicembre il lancio di un *physically-backed Exchange Traded Product* (ETP) quotato su Six Swiss Exchange[11]. Il nuovo ETP andrà a competere direttamente con l'analogo prodotto lanciato a inizio 2019 da Amun[12].

Questo ETP acquista fisicamente Bitcoin ed emette delle azioni scambiabili sul mercato che replicano quindi l'andamento del prezzo del sottostante. Lo scopo dell'ETP è fornire esposizione finanziaria a Bitcoin al costo di una *fee* annuale di gestione, consentendo ai suoi azionisti di non dover acquistare direttamente Bitcoin e non doverne gestirne la custodia. I Bitcoin acquistati da WisdomTree sono attualmente dati in custodia a Coinbase.

La grande crescita di Grayscale nel 2019

Grayscale è tra i protagonisti dell'ultimo trimestre 2019 ed in generale di tutto l'anno Bitcoin.

Grayscale è stata la prima società al mondo a proporre un Trust su Bitcoin scambiabile sul mercato dal 2013. Da allora il Trust è cresciuto continuamente divenendo il più grande prodotto di investimento nel mondo crypto. Negli anni Grayscale ha affiancato al Bitcoin Trust altri prodotti di investimento similari denominati in altre criptovalute.

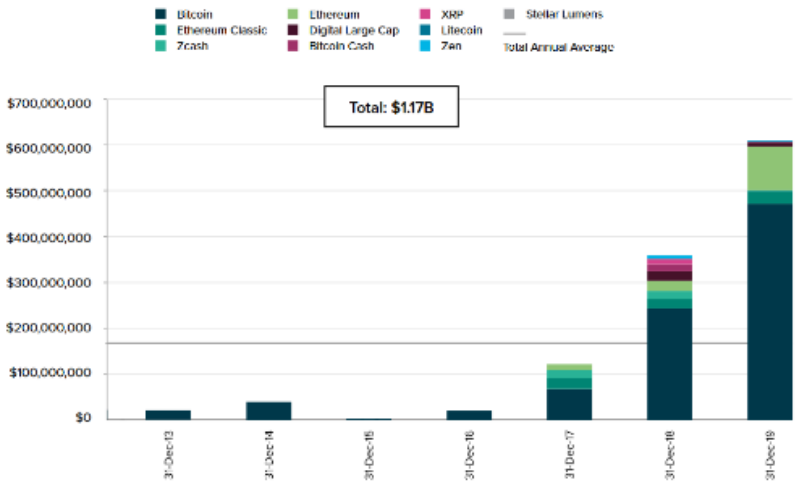


Figura 6: Investimenti annuali nei prodotti Grayscale

Durante il 2019 la crescita è stata vigorosa, raggiungendo una raccolta pari a $607.7 milioni[13], una cifra superiore alla somma di tutti gli investimenti nel periodo 2013-2018 (si veda figura 6). Grazie a questa annata record, Grayscale ha superato il miliardo di raccolta, giungendo a $1.17 miliardi. Vale la pena sottolineare come il solo Bitcoin Trust abbia contributo per il 77,6% della raccolta totale, raggiungendo la cifra record di $471.7 milioni.

> *Durante il 2019 Grayscale ha superato il miliardo di raccolta, giungendo a $1.17 miliardi. Il solo Bitcoin Trust ha contributo per il 77,6% della raccolta totale, raggiungendo la cifra record di $471.7 milioni.*

Sulla scia di questi risultati record, Grayscale ha deciso di intraprendere la strada per accreditarsi come "Reporting Company"[14] (*Section 12(g) of the Securities Exchange Act of 1934*) presso la SEC, divenendo di fatto il primo veicolo di investimento nel mondo crypto con questa qualifica. In questo modo il Trust potrebbe attrarre nuovi investitori istituzionali che oggi sono impossibilitati a investire in fondi che non riportano direttamente alla SEC.

[10] https://www.wisdomtree.eu/en-ch/-/media/eu-media-files/uncategorized/wisdomtree-Bitcoin-launch-final.pdf
[11] https://www.six-group.com/exchanges/exchange_traded_products/security_info_de.html?id=GB00BJYDH287USD4
[12] https://www.amun.com/product/abtc
[13] https://grayscale.co/wp-content/uploads/2020/01/Grayscale-Digital-Asset-Investment-Report-2019-January-2020.pdf
[14] https://medium.com/grayscale-investments/gbtc-sec-filing-8b4cb229088

Fondi pensioni statunitensi aumentano l'esposizione sul mondo crypto

Nel report 2019-Q1 avevamo scritto dei due fondi pensione di Fairfax County Virginia (precisamente il *Police Officer's Retirement System* e l'*Employees' Retirement System*) che avevano deciso di investire in fondi di investimento crypto tramite Morgan Creek, società di asset management specializzata nel settore.

È notizia dell'ultimo trimestre la decisione dei due fondi pensione di investire insieme ulteriori $50 milioni in un nuovo prodotto emesso da Morgan Creek, superando quindi ampiamente l'investimento iniziale di $20 milioni fatto a febbraio e portando l'esposizione complessiva a circa l'1%[15]. Questa decisione deriva dalle ottime performance che il primo investimento ha generato nel fondo pensione.

Ricordiamo che un investimento in *crypto-assets* aiuta molto in termini di diversificazione del portafoglio. Uno studio[16] effettuato da Samuele Vianello, *alumnus* dell'istituto, ha infatti mostrato come i crypto-assets e in particolare Bitcoin non siano correlati con le altre asset class.

	BITCOIN	GOLD	WTI	GRAIN	IND. METALS	EUR	GBP	CHF	JPY	MSCI BRIC	EURO STOXX50	NASDAQ	S&P500	VIX	Euro Bonds	US Bonds
GOLD	0,02%															
WTI	1,42%	14,50%														
GRAIN	3,41%	13,82%	18,05%													
IND. METALS	3,41%	31,63%	35,30%	20,14%												
EUR	2,94%	36,61%	17,10%	14,05%	29,73%											
GBP	0,72%	24,47%	21,27%	11,64%	25,30%	57,03%										
CHF	3,47%	36,69%	6,25%	7,76%	20,11%	59,52%	35,99%									
JPY	-1,42%	39,52%	-6,81%	2,30%	-3,77%	31,27%	14,43%	35,71%								
MSCI BRIC	1,39%	12,67%	29,67%	15,19%	42,94%	19,17%	23,54%	7,92%	-16,57%							
EUROSTOXX50	5,01%	8,96%	31,94%	15,12%	46,06%	47,44%	41,78%	21,34%	-17,26%	57,04%						
NASDAQ	4,00%	-1,54%	28,59%	13,54%	31,62%	13,42%	17,60%	-1,95%	-21,58%	47,17%	55,39%					
S&P500	5,07%	-1,04%	34,34%	14,72%	34,15%	16,74%	20,46%	0,07%	-22,29%	48,06%	61,16%	94,92%				
VIX	-5,31%	0,95%	-25,97%	-13,75%	-24,04%	-7,55%	-14,38%	3,40%	21,83%	-38,76%	-46,10%	-77,56%	-80,32%			
Euro Bonds	2,06%	42,61%	13,45%	12,20%	25,33%	91,87%	61,72%	59,71%	39,74%	18,75%	41,31%	9,78%	12,26%	-6,07%		
US Bonds	-1,27%	21,11%	-21,26%	-6,10%	-17,44%	-0,59%	-5,00%	12,91%	37,90%	-15,00%	-28,01%	-30,82%	-33,69%	26,60%	19,36%	
EUR Bonds	2,59%	40,46%	13,29%	11,96%	26,57%	94,39%	53,34%	58,05%	36,77%	18,94%	43,95%	11,12%	13,84%	-6,78%	98,37%	14,31%

Positive correlation
Uncorrelated
Negative correlation

Figura 7: Correlazione Bitcoin e altre asset class

Una allocazione di portafoglio alla Markowitz mostra come inserire un 2-3% di questi assets nel portafoglio alza la frontiera efficiente e quindi i rendimenti attesi a parità di rischio (o, specularmente, abbassa il livello di rischio a parità di rendimento atteso).

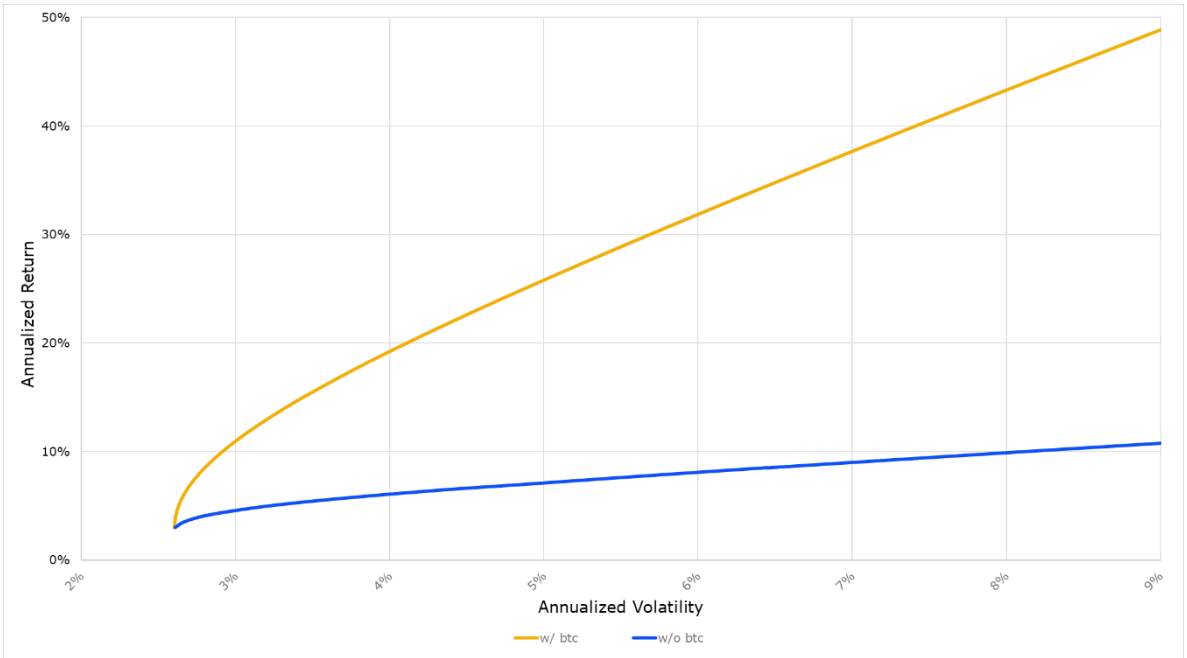


Figura 8: Frontiera efficiente del portafoglio con e senza Bitcoin

[15] https://www.coindesk.com/pension-funds-double-crypto-asset-exposure-in-morgan-creeks-fund-to-1
[16] https://github.com/SamueleVianello/MasterThesis/blob/master/Latex/thesis-master/main.pdf

2. Tecnologia

2.1 Bitcoin

Nuovo rilascio per *Bitcoin Core*

Il 2019 è stato un anno molto proficuo anche dal punto di vista degli update a *Bitcoin Core,* il client software lanciato originariamente da Satoshi Nakamoto nel 2009 e che ancora oggi rappresenta oltre il 97% dei nodi del network Bitcoin. Dopo il rilascio della versione 0.18.0 nel secondo trimestre, nell'ultimo trimestre è stata rilasciata la versione 0.19.0.[17]

Le novità principali di questa release sono l'utilizzo degli indirizzi *bech32* come *default* nel wallet di *Bitcoin Core* e l'incremento del numero di connessioni ad altri nodi del network. Questa ultima modifica è importante per evitare i cosiddetti *partitioning attacks*. Questi attacchi possono essere performati da un attaccante che controlla un numero sufficientemente grande di nodi del network; in questa situazione l'attaccante può partizionare un soggetto, relegandolo in un sotto-network scollegato da quello principale. Per ridurre questo tipo di attacchi è sufficiente aumentare il numero di nodi del network a cui ogni *client* si connette. Questa soluzione comporta però un aumento dei requisiti di banda necessari a tenere attivo un nodo Bitcoin. Per mitigare il problema del *partitioning attack* e allo stesso tempo non aumentare significativamente i requisiti di banda, gli sviluppatori di *Bitcoin Core* hanno scelto quindi di limitare le funzionalità delle 2 connessioni aggiuntive riducendo al minimo il

Indirizzi *bech32*

Gli indirizzi *bech32* iniziano con "bc1" (mentre i vecchi indirizzi *base58* iniziano con "1" o "3"). Per questi indirizzi non vale più la distinzione tra lettere maiuscole e minuscole ed hanno un avanzato sistema di correzione che permette di rilevare fino a cinque lettere sbagliate. Gli indirizzi bech32 fanno parte dell'aggiornamento al protocollo Bitcoin del 2017, noto come SegWit: in due anni hanno raggiunto ormai un'ottima diffusione e consentono una flessibilità funzionale che sarà utile per i prossimi sviluppi.

[17] https://Bitcoincore.org/en/2019/11/24/release-0.19.0/

loro carico in termini di banda: servono solo per trasmettere e ricevere i blocchi validati e non le transazioni.

Bitcoin: che cosa è avvenuto nel 2019

In questo primo anno di report abbiamo seguito i numerosi sviluppi tecnologici che hanno portato molte novità in Bitcoin sia in termini di usabilità che in termini di sicurezza. Con la fine dell'anno facciamo il punto sulle novità che riteniamo più importanti e significative.


Pieter Wuille

Il protagonista del 2019 è stato sicuramente ancora una volta Pieter Wuille, che ha chiuso l'anno con due proposte molto interessanti. La prima di queste è Taproot[18] (per maggiori dettagli si veda il report 2019-Q2). Taproot permette di incrementare la flessibilità degli *smart contract* in Bitcoin, aumentando allo stesso tempo la privacy: anche uno *smart contract* molto complicato diventerebbe non distinguibile da una normale transazione. Per essere introdotta nel protocollo Bitcoin questa proposta necessita preliminarmente dell'adozione di uno nuovo algoritmo di firma digitale, *Schnorr signature,* che è attualmente in fase avanzata di sviluppo.

La seconda novità di Sipa (il *nickname* con cui è conosciuto universalmente Pieter Wuille) è stato Miniscript[19], un nuovo linguaggio di scrittura per gli smart contract (per maggiori dettagli si veda 2019-Q3). Questo linguaggio permette una scrittura semplificata di alto livello delle condizioni logiche di una transazione (lo smart contract, appunto), garantendo che la traduzione automatica nello script di basso livello avrà una eseguibilità efficace ed uso di risorse ottimizzato. In questo modo viene notevolmente ridotta la possibilità di errore in fase di scrittura di una transazione.


Brian Bishop

Un'altra proposta innovativa che ci sentiamo di evidenziare è *Bitcoin Vault*[20] (per maggiori dettagli si veda il report 2019-Q3). Bitcoin Vault è un meccanismo pensato per la custodia sicura dei propri Bitcoin. In un Vault le condizioni di spendibilità dei Bitcoin custoditi sono sospese per un predeterminato intervallo temporale, osservabile pubblicamente. Durante questo intervallo temporale il possessore dei Bitcoin può difendersi da tentativi di furto tramite una *recovery key* che gli permette di invalidare eventuali transazioni iniziate senza il suo consenso. Brian Bishop ha proposto una possibile implementazione del concetto di Bitcoin Vault che non richiede modifiche al protocollo Bitcoin: l'ha proposta sulla mailing list dei *core developer* che la stanno valutando.

Soluzioni di secondo livello: Lightning Network e Liquid

Il 2019 è stato sicuramente un anno di grande sviluppo per le applicazioni di secondo livello, cioè quelle applicazioni che viaggiano in parallelo alla blockchain di Bitcoin portando benefici in termini di scalabilità, privacy e velocità. Le principali applicazioni di secondo livello sono le *sidechain*, in particolare Liquid, e Lightning Network.

> *Il 2019 ha visto l'esplosione del numero di nodi Lightning Network: a settembre è stata superata la soglia record di 10.000 nodi.*

Lightning Network incrementa la scalabilità del network Bitcoin tramite la creazione di *payment channels:* le transazioni sono rese sicure da uno stratagemma crittografico anche senza essere diffuse nel network Bitcoin, aggirando quindi il limite di sette transazioni al secondo che caratterizza la blockchain Bitcoin. Il 2019

[18] https://github.com/sipa/bips/blob/bip-schnorr/bip-taproot.mediawiki
[19] http://Bitcoin.sipa.be/miniscript/
[20] https://lists.linuxfoundation.org/pipermail/Bitcoin-dev/2019-August/017270.html

ha visto l'esplosione del numero di nodi Lightning Network: a settembre è stata superata la soglia record di 10.000 nodi.

Il 2019 verrà sicuramente ricordato anche per la *Lightning Torch*[21]*:* un pagamento su Lighting Network che è passato come una torcia di mano in mano tra dozzine di partecipanti, ognuno dei quali ne ha incrementato l'importo. Dopo essere passata da 275 persone diverse, inclusi molti personaggi di spicco del mondo Bitcoin e non solo, tra cui il CEO di Twitter Jack Dorsey, la torcia ha raggiunto l'attuale limite massimo consentito su Lightning Network (4.29M satoshi) e la destinazione finale nelle mani della associazione benefica *Bitcoin Venezuela*. La torcia è stato un esperimento del funzionamento del network su scala globale che ha mostrato le grandi potenzialità di questa soluzione, ma anche gli attuali limiti di usabilità: Lighting Network è ancora lontano da un utilizzo semplice ed affidabile. Nonostante ciò nel corso dell'anno sono nati diversi nuovi wallet che cercano di semplificarne l'utilizzo. Il 2020 sarà un anno fondamentale per capire il futuro di questa soluzione: rimarrà un interessante esperimento o diventerà davvero una applicazione usabile?

Anche nell'ultimo trimestre 2019 lo sviluppo di Lightning Networks è andato avanti senza sosta, cercando di arrivare a quell'usabilità tanto attesa e oggi ancora lontana. È notizia dell'ultimo trimestre la proposta di utilizzo del network come sistema di messaggistica istantaneo, sicuro e incensurabile[22]. Un aggiornamento del network ha infatti standardizzato il modo con cui costruire messaggi, ad ogni transazione si può così aggiungere un campo testuale che di fatto diventerebbe il messaggio. Questa nuova applicazione del network è sicuramente molto interessante e promettente: monitoreremo gli sviluppi futuri.

È invece stato in tono minore il primo anno di Liquid[23], la *sidechain* creata da Blockstream (per maggiori dettagli si veda il report 2019-Q1). Una *sidechain* è una blockchain alternativa che viaggia in parallelo a quella principale, in questo caso quella di Bitcoin. Una *sidechain* può differenziarsi su alcuni punti: algoritmo di consenso, dimensione blocchi, transazioni. Liquid, ad esempio, è una *sidechain* gestita da una federazione di *exchange* che validano le transazioni e aggiungono nuovi blocchi rendendo possibile lo scambio in sicurezza e con tempi di conferma dell'ordine del minuto dei *Liquid-Bitcoin* (L-BTC), token emessi su questa *sidechain* garantiti da Bitcoin reali congelati sulla blockchain pubblica. L'utilità principale è quella di consentire arbitraggi efficienti tra le diverse borse, superando il problema dei tempi di conferma del network Bitcoin. L'adozione è cresciuta, coinvolgendo diversi exchange, ma i volumi scambiati non sono per ora significativi.

La crescita continua del *mining*: inaugurate nuove *mining farm*

Il 2019 si è concluso con la corsa alla realizzazione della più grande *mining farm*: i protagonisti sono Bitmain, la principale società che produce hardware per il mining, e Whinstone, società di sviluppo di data center.

Il primo a scendere in campo è stato Bitmain[24] che ha inaugurato il nuovo centro di mining a Rockdale in Texas sfruttando una vecchia fonderia ora abbandonata della Alcoa. La nuova *farm* è stata inaugurata con una

[21] https://www.coindesk.com/Bitcoins-lightning-torch-has-blazed-through-37-countries-so-far
[22] https://www.coindesk.com/how-Bitcoins-lightning-can-be-used-for-private-messaging
[23] https://blockstream.com/2019/03/11/en-introducing-liquid-core/
[24] https://www.coindesk.com/why-bitmain-is-building-the-worlds-largest-Bitcoin-mine-in-rural-texas

capacità di 25MW con l'obiettivo di arrivare a 300MW nel 2020, divenendo così la più grande al mondo. Bitmain ha scelto il Texas come sede della nuova *facility* per il basso costo dell'elettricità. Poco dopo l'inaugurazione di Bitmain è arrivato l'annuncio[25] di Whinstone riguardante il piano di una nuova *mining farm*, sempre a Rockdale, anche qui in una vecchia fonderia abbandonata della Alcoa. L'obiettivo, in questo caso, è di essere operativi nel primo trimestre del 2020 con una capacità di 300MW per arrivare a fine 2020 con una capacità di 1GW.

Se un tempo la Cina pesava per circa l'80% del mining mondiale, ora questa percentuale è scesa sotto il 60% ed è in continuo calo.

Queste due nuove *mining farm* contribuiscono al generale spostamento del mining all'esterno della Cina. Se un tempo la Cina pesava per circa l'80% del mining mondiale, ora questa percentuale è scesa sotto il 60% ed è in continuo calo. Oltre al Nord America, stanno infatti nascendo *mining farm* in Norvegia, Russia, Venezuela e Paraguay[26].

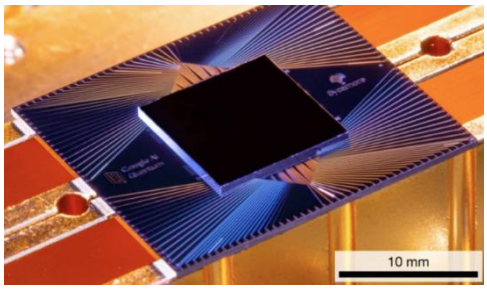
Nello scorso numero avevamo anche parlato di *BetterHash*, un protocollo di mining che aumenta la decentralizzazione nei pool. Sulla scia di *BetterHash*, nell'ultimo trimestre 2019 è stata presentata la nuova versione del protocollo *Stratum*, *Stratum V2*[27]. A detta di molti esperti se il funzionamento di questo protocollo venisse confermato anche in pratica, la centralizzazione dei pool potrebbe scomparire completamente[28]: questo porterebbe un grande beneficio in termine di decentralizzazione del consenso, obiettivo principale del protocollo Bitcoin.

STRATUM V2

[25] https://www.coindesk.com/1-gigawatt-Bitcoin-mine-under-construction-in-texas-would-dwarf-bitmains
[26] https://Bitcoinmagazine.com/articles/beyond-china-and-north-america-the-decentralization-of-Bitcoin-mining
[27] https://stratumprotocol.org/
[28] https://www.coindesk.com/a-plan-to-decentralize-Bitcoin-mining-again-is-gaining-ground

2.2 Blockchain, crittografia ed applicazioni non monetarie

Quantum Supremacy



Con un articolo su Nature[29], ad ottobre Google ha annunciato la cosiddetta *quantum supremacy*. I commenti più superficiali hanno decretato l'imminente fine delle tecniche crittografiche su cui si basa non solo Bitcoin, ma anche la sicurezza di tutte le comunicazioni (comprese quelle finanziarie) e dei sistemi di controllo dell'arsenale militare e nucleare. Come accade spesso in ambiti tecnici e specialistici, i commenti non colgono davvero nel segno.

Un quantum computer utilizza quantum bits, detti anche qubits, che per le proprietà della fisica quantistica esistono in "sovrapposizione", per cui possono essere zero ed uno allo stesso tempo.

Un computer tradizionale ha nel bit l'unità di base dell'informazione ed un bit può assumere due stati: zero o uno; un *quantum computer*, invece, utilizza *quantum bits*, detti anche *qubits*, che per le proprietà della fisica quantistica esistono in "sovrapposizione", per cui possono essere zero ed uno allo stesso tempo. Insomma, se con otto bit un computer tradizionale può rappresentare un singolo stato tra 2^8 = 256 possibili stati, otto qubits in *coerenza quantistica* possono invece rappresentare 256 stati *contemporaneamente*. Questo parallelismo esponenziale permette di risolvere problemi irrisolvibili con computer tradizionali: il termine *quantum supremacy* indica proprio la dimostrazione di questo fatto.

Dario Gil

E questo sarebbe esattamente il risultato ottenuto dai tecnici di Google: con 53 qubits hanno risolto in 200 secondi un problema che con un supercomputer tradizionale avrebbe richiesto circa 10mila anni. In realtà IBM ha pubblicamente refutato il risultato[30] dichiarando che il problema sarebbe risolvibile in due giorni e mezzo con tecnologia tradizionale. In ogni caso, è lo stesso Dario Gil, direttore dei laboratori IBM, a sostenere[31] che prototipi e simulatori di quantum computer stanno diventando realtà ed è indubbio che tra qualche decennio po tremmo vederne applicazioni interessanti[32].

Il dibattito è rilevante per la crittografia *asimmetrica* a chiave pubblica/privata su cui si basa anche Bitcoin. Infatti, la sicurezza di questa tecnica crittografica è fondata sulla non risolvibilità del *problema del logaritmo discreto*: se è facile derivare da una chiave privata la corrispondente chiave pubblica, l'inverso (dedurre dalla chiave pubblica la corrispondente chiave privata) richiederebbe invece l'impiego di tutta la potenza computazionale (tradizionale) oggi disponibile per miliardi di volte l'età dell'universo.

Non solo siamo lontani dal violare la crittografia asimmetrica, ma non è detto nemmeno che si riuscirà mai a raggiungere questo risultato.

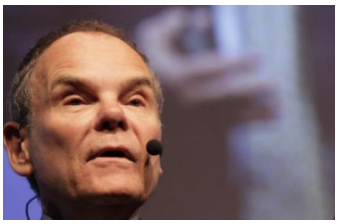
La notizia della quantum supremacy non va comunque enfatizzata eccessivamente: i qubits perdono facilmente coerenza per cui le computazioni possono durare solo frazioni di secondo; inoltre, gli inevitabili errori dovuti al rumore delle interazioni in molti casi non possono essere corretti, proprio per la loro natura quantistica[33].

[29] https://www.nature.com/articles/s41586-019-1666-5
[30] https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/
[31] https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html
[32] https://www.bbva.com/en/what-is-quantum-supremacy/
[33] https://www.livescience.com/quantum-supremacy-debate.html

Per questo, non solo siamo lontani dal violare la crittografia asimmetrica, ma non è detto nemmeno che si riuscirà mai a raggiungere questo risultato. Ad ogni buon conto, la ricerca crittografica sta già studiando e sperimentando tecniche di crittografia asimmetrica *quantum-resistant* ed il NIST (National Institute of Standards and Technology) sta addirittura lavorando alla loro standardizzazione: la vera sfida potrebbe essere non tanto lo sviluppo di queste nuove tecniche, quanto la complessità del processo di aggiornamento dei sistemi informatici ed industriali[34]. In ogni caso è facile scommettere che, per preservare il valore di Bitcoin ed evitare che l'oro digitale "arrugginisca", il protocollo Bitcoin sarà certamente in prima linea nell'adottare aggiornamenti tecnologici difensivi.

La chimera della *blockchain revolution*

Anche Don Tapscott, uno dei principali araldi della *blockchain revolution*, è costretto ad ammettere che le ambizioni di applicazione generalizzata della tecnologia blockchain hanno avuto una battuta d'arresto nel 2019[35]: riconosce che la rilevanza mediatica è diminuita, che non ci sono applicazioni in produzione, che la tecnologia sembra marginale. Nonostante questo, Tapscott insiste che sarebbe sbagliato accettare questa visione negativa e che la blockchain avrebbe solo problemi di pubbliche relazioni, regolamentazione e maturità. A noi, che da sempre siamo critici ferocissimi della *blockchain magica* capace di risolvere qualunque problema, sembra invece che null'altro negli ultimi cinque anni abbia goduto di una attenzione più significativa da parte di stampa, regolatori ed investitori.



Don Tapscott

> *Don Tapscott, uno dei principali araldi della blockchain revolution, è costretto ad ammettere che le ambizioni di applicazione generalizzata della tecnologia blockchain hanno avuto una battuta d'arresto.*

Non riteniamo qui utile commentare molti casi patologici di applicazioni blockchain; ma, come per Turnbull, lascia basiti l'insistenza di IBM e E&Y nel promuovere la blockchain per la tracciabilità e la trasparenza[36]. Dopo il vino, il pollo e la bufala blockchain di cui abbiamo parlato nei numeri scorsi, non potevano non arrivare anche la pasta[37] e le uova[38] sul fronte agrifood ed in generale la tutela del Made in Italy[39] con il supporto della commissione blockchain del MISE.

Abbiamo precedentemente spiegato che la blockchain come registro distribuito non è affatto immodificabile ed affidabile, a meno che non sia protetta dai costi altissimi della proof-of-work di Bitcoin (circa otto miliardi di dollari l'anno). Anche utilizzando la blockchain di Bitcoin, quello che si può fare è apporre la *marcatura temporale ad un documento digitale*, ma questo non garantisce né chi sia l'autore (a meno che non apponga anche firma digitale) né tantomeno in alcun caso può garantire la veridicità del documento. Insomma, si possono rafforzare processi di business fornendo per la loro digitalizzazione un elemento chiave come la marcatura temporale, ma non esistono soluzioni facili per i problemi di trasparenza e tracciabilità.

[34] https://Bitcoinmagazine.com/articles/op-ed-quantum-computing-crypto-agility-future-readiness
[35] https://www.coindesk.com/blockchain-faces-big-challenges-but-the-opportunity-is-enormous
[36] https://www.ey.com/en_gl/news/2019/10/ey-launches-public-finance-management-blockchain-solution-to-improve-efficiency-and-transparency-in-governments
[37] https://www.blockchain4innovation.it/mercati/agrifood/pasta-certificata-con-la-blockchain-gruppo-grigi-entra-in-ibm-food-trust/
[38] https://www.blockchain4innovation.it/mercati/agrifood/alleanza-coop-ibm-ecco-la-blockchain-per-la-tracciabilita-delle-uova/
[39] https://www.blockchain4innovation.it/fashion/mise-e-ibm-con-la-blockchain-per-la-tutela-del-made-in-italy/

2.3 Altcoin

Ethereum: l'aggiornamento *Istanbul*

Continua la lunga serie di aggiornamenti di Ethereum introdotti tramite *hard-fork*, cioè una modifica del codice non *backward-compatible* che causa l'esclusione dal network di tutti i nodi che non effettuano l'aggiornamento. È bene sottolineare che questo tipo di aggiornamenti, sebbene potenti dal punto di vista del numero di novità che possono introdurre, sono molto pericolosi per il network e dovrebbero essere evitati il più possibile. In Bitcoin un aggiornamento del codice di questo tipo sarebbe ai limiti del possibile, per via dell'assenza di una guida centrale che decide e impone questi aggiornamenti. Ethereum invece, grazie a una *governance* diversa e sostanzialmente centralizzata nelle mani della Ethereum Foundation, riesce a percorrere questa strada con cadenza quasi semestrale.

Dopo il faticoso rilascio in produzione dell'aggiornamento *Constatinople* e *Petersburg* di inizio 2019 (per maggiori dettagli si veda il report 2019-Q1), durante l'ultimo trimestre del 2019 è stato rilasciato con successo il nuovo aggiornamento, chiamato *Istanbul*[40]: le novità sono numerose, soprattutto in termini di scalabilità, sicurezza ed interoperabilità.

Questo nuovo rilascio non è stato però indolore per tutti: durante la fase di test della nuova versione è emerso come il funzionamento di 680 *smart contract* emessi utilizzando la piattaforma Aragon è stata compromessa[41]. Aragon è una piattaforma che permette di creare smart contract per la gestione di organizzazioni decentralizzate (DAO). Per risolvere il problema Aragon stessa ha rilasciato un comunicato ufficiale in cui invita tutti gli utenti ad aggiornare manualmente i contratti emessi prima dell'11 settembre 2019[42].

[40] https://blog.ethereum.org/2019/11/20/ethereum-istanbul-upgrade-announcement/
[41] https://www.coindesk.com/ethereums-istanbul-upgrade-will-break-680-smart-contracts-on-aragon
[42] https://blog.aragon.org/istanbul-hard-fork-impact/

3. Regolazione

Libra e *stablecoin*

Dopo averne parlato negli ultimi due numeri (a cui rimandiamo per le "puntate" precedenti) è necessario tornare ancora sugli sviluppi riguardanti Libra e, ne siamo convinti, il dibattito terrà banco ancora a lungo.

Al Congresso degli Stati Uniti non è bastata la testimonianza di David Marcus, responsabile di Libra, ma si è dovuto presentare Mark Zuckerberg in persona[43]. Al fondatore di Facebook è stata presentata una lunga serie di accuse per i comportamenti messi in atto in passato (*fake news*, Cambridge Analytica, violazioni della *privacy*), elementi che inducono il Congresso a temere il peggio se il progetto Libra andasse avanti: a poco è servito che Zuckerberg ribadisse l'intenzione a procedere solo se arriverà il beneplacito dei regolatori. Il passaggio più cruciale e rivelatorio è stato la domanda sulle ragioni per l'abbandono del consorzio Libra da parte di molti membri (PayPal, Mastercard, Visa, eBay e Stripe tra gli altri[44]): Zuckerberg ha risposto individuando le cause nei rischi associati al progetto e nell'intenso scrutinio da parte dei regolatori. A noi sembra che le due ragioni sostanzialmente coincidano[45]: i rischi sono tutti associati all'attività dei regolatori, secondo due direttrici, una genuinamente tecnico-regolamentare e l'altra politica-monetaria.

Il punto tecnico-regolamentare riguarda l'equilibrio della *privacy* tra i due possibili estremi: anonimato (che favorirebbe evasione fiscale, riciclaggio e finanziamento al terrorismo) e trasparenza (che permetterebbe a Facebook di accedere anche alle informazioni finanziarie). In realtà, per quanto è dato di capire del disegno originario, il network Libra favorirebbe l'anonimato (o meglio lo pseudonimato: non c'è identificazione dell'utente, ma le sue transazioni sono visibili), mentre il wallet Calibra gestito direttamente da Facebook sarebbe in conformità regolamentare (*know-your-customer*, *anti-money-laundering* e *countering-terrorism-financing*). Insomma, Calibra potrebbe rispondere a tutte le richieste regolamentari (ed accedere ai dati dei suoi utenti), mentre il network Libra non presidiato soddisferebbe quello spettro di esigenze tra il legittimamente libertario e l'oggettivamente criminale. Né più né meno come succede col dollaro statunitense, tra un sistema bancario in *compliance* regolamentare ed un circuito transazionale internazionale (elettronico e contante) spesso più spregiudicato. Per Libra il bilanciamento tra i due estremi potrebbe essere regolato in funzione delle autorizzazioni da ottenere[46], con buona pace del segretario del Tesoro Steven Mnuchin, che incalzato per aver opposto un diniego pregiudizievole ed illiberale a Libra, si dichiara favorevole a Libra solo se sarà completamente conforme alle richieste regolamentari[47].

Calibra potrebbe rispondere a tutte le richieste regolamentari, mentre il network Libra non presidiato soddisferebbe quello spettro di esigenze tra il legittimamente libertario e l'oggettivamente criminale. Né più né meno come succede col dollaro statunitense, tra un sistema bancario in compliance regolamentare ed un circuito transazionale internazionale spesso più spregiudicato

[43] https://www.bloomberg.com/news/articles/2019-10-23/zuckerberg-set-to-convince-skeptical-congress-on-libra-privacy
[44] https://www.theverge.com/2019/10/11/20910330/mastercard-stripe-ebay-facebook-libra-association-withdrawal-cryptocurrency
[45] https://www.aljazeera.com/ajimpact/major-payment-firms-hesitate-facebook-libra-191002041634035.html
[46] https://www.ft.com/content/7df7fa22-ea6f-11e9-a240-3b065ef5fc55
[47] https://www.coindesk.com/mnuchin-fine-with-libra-launch-but-*crypto*-project-must-fully-comply-with-aml-rules

Ma l'aspetto insormontabile è quello politico-monetario. La preoccupazione è che Libra possa diventare la moneta utilizzata da miliardi di esseri umani, mettendo le monete nazionali in una situazione di concorrenza se non addirittura minorità. Il sogno del premio Nobel per l'economia Hayek di concorrenza tra monete private e monete governative a corso legale, rappresenta per politici e banchieri centrali l'incubo della possibile separazione tra Moneta e Stato, tanto inaudita e dirompente quanto quella tra Chiesa e Stato avvenuta alcuni secoli fa. Abbiamo commentato nel numero scorso il netto stop arrivato a Libra dall'Europa, ribadito recentemente anche da Christine Lagarde[48], nuovo presidente di ECB; per tentare di ammorbidire gli Stati Uniti, il consorzio promosso da Facebook si è spinto a considerare la possibilità di avere il solo dollaro statunitense come riserva collaterale della sua moneta[49], abbandonando quindi l'idea di un paniere di valute internazionali. In questo modo diminuirebbe la discrezionalità di politica monetaria di Libra, che si ritroverebbe ad essere un dollaro digitale emesso da privati, cioè uno *stablecoin* ancorato al potere di acquisto del biglietto verde.

Il sogno del premio Nobel per l'economia Hayek di concorrenza tra monete private e monete governative a corso legale, rappresenta per politici e banchieri centrali l'incubo della possibile separazione tra Moneta e Stato.

E se la condanna per gli stablecoin non-governativi è pressoché unanime (BIS[50], FAFT[51]) l'alternativa degli stablecoin di banca centrale è stata oggetto di un intenso dibattito. Per contrastare Libra, praticamente tutte le banche centrali hanno rilanciato i loro progetti di *central bank digital currency* (CBDC). Allo studio in Banca Centrale Europea[52], analizzata dalla Riksbank svedese[53], auspicabile per J. Christopher Giancarlo[54] e Daniel Gorfine[55] (ex responsabili della *Commodity Futures Trading Commission*), inevitabile secondo Patrick Harker[56] (presidente della Federal Reserve di Philadephia), in fase di lancio per la People Bank of China[57] (banca centrale cinese) pressata in tal senso dal leader supremo Xi Jinping[58], la moneta digitale di banca centrale è finalmente entrata anche nell'orizzonte di IMF[59], BIS[60] e G7[61].

Christine Lagarde

Questo intensa attenzione si configura però più come reazione istintiva che non come strategia chiara. Quasi nessuno tenta infatti di risolvere il vero nodo della questione: l'accesso indiscriminato a moneta digitale di banca centrale disincentiverebbe completamente il deposito di liquidità presso le banche commerciali. Infatti, perché affidare i propri risparmi a banche che possono fallire se si possono invece affidare a banche centrali? Queste ultime sono per definizione sempre capaci di onorare impegni denominati nella loro

L'accesso indiscriminato a moneta digitale di banca centrale disincentiverebbe completamente il deposito di liquidità presso le banche commerciali.

[48] https://www.coindesk.com/facebooks-social-media-platforms-may-give-libra-unfair-advantage-says-ecbs-lagarde
[49] https://www.reuters.com/article/us-imf-worldbank-facebook/facebook-open-to-currency-pegged-stablecoins-for-libra-project-idUSKBN1WZ0NX
[50] https://www.coindesk.com/Bitcoin-has-failed-but-global-stablecoins-a-threat-say-bis-and-g7
[51] http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-virtual-assets-global-stablecoins.html
[52] https://www.ecb.europa.eu/pub/pdf/other/ecb.other191204~f6a84c14a7.en.pdf e https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785
[53] https://www.riksbank.se/en-gb/payments--cash/e-krona/
[54] https://www.coindesk.com/ex-cftc-chair-giancarlo-to-push-for-digital-dollar-in-new-role-at-white-shoe-law-firm
[55] https://www.coindesk.com/fearing-usd-decline-ex-cftc-heads-propose-a-blockchain-based-digital-dollar
[56] https://www.coindesk.com/fed-official-says-digital-central-bank-currency-is-inevitable
[57] https://www.coindesk.com/unlike-libra-digital-yuan-will-not-need-currency-reserves-to-support-value-pboc-official
[58] https://www.scmp.com/economy/china-economy/article/3034741/beijing-rushes-embrace-blockchain-facebooks-libra-just-around
[59] https://blogs.imf.org/2019/09/19/digital-currencies-the-rise-of-stablecoins/ e https://blogs.imf.org/2019/09/26/from-stablecoins-to-central-bank-digital-currencies/
[60] https://www.bis.org/speeches/sp191205.htm
[61] https://www.bis.org/cpmi/publ/d187.pdf

valuta. Le banche commerciali sarebbero quindi danneggiate nella raccolta e quindi nella collegata attività di erogazione del credito, fondamentale per la politica monetaria. Uno shock insostenibile oggi per un sistema bancario che è già piuttosto fragile. Inoltre, non si capisce bene se uno *stablecoin* di banca centrale sarebbe contante digitale (ad accesso universale, al portatore, *privacy-preserving*) o piuttosto moneta elettronica (accessibile solo da agenti economici identificati): la prima ipotesi vanificherebbe lo sforzo finora fatto per contrastare il contante, la seconda pregiudicherebbe mortalmente tutta l'industria dei pagamenti e significativamente il sistema bancario. In passato avevano messo chiaramente a fuoco questi problemi sia Mark Carney (ex-governatore di Bank of England) sia Jens Weidmann[62] di Bundesbank; questo trimestre l'unica voce che lo ha fatto è stato il governo svizzero[63].

FAFT: linee guida per la prevenzione di reati finanziari

La *Financial Action Task Force* (FATF, anche noto come *Groupe d'action financière* GAFI) è un organismo intergovernativo fondato nel 1989 con l'obiettivo di fissare gli standard e promuovere una implementazione efficace delle misure legali, regolatorie ed operative per combattere il riciclaggio, il finanziamento al terrorismo e le altre minacce all'integrità dei mercati finanziari. FATF ha quindi sviluppato una serie di Raccomandazioni riconosciute come standard internazionale; oggi la sua attenzione copre anche quelli che loro chiamano *virtual assets* (l'estensione di quelle che una volta si chiamavano *virtual currencies*, oggi meglio note *crypto-assets*): la pagina dedicata[64] rimanda a tutti i documenti di riferimento[65], a cui si sono appena aggiunte le indicazioni sul tema dell'identità digitale[66]. Più in generale, FATF ha raccomandato ai regolatori nazionali la creazione di registri o licenze per i *virtual asset service providers* (VASP) ed in particolare spinge affinché sia adottata la cosiddetta *travel-rule*[67], cioè l'identificazione e registrazione di tutti i dati di ogni transazione, inclusi originatore e beneficiario. Sul tema sta lavorando per e con FATF anche Global Digital Finance (GDF), organizzazione che promuove l'accelerazione e l'adozione dei crypto-asset e delle tecnologie per la finanza digitale nei servizi finanziari tradizionali (si veda nella sezione Vita dell'Istituto l'ingresso del Crypto Asset Lab tra i membri di GDF).

> *FATF ha raccomandato ai regolatori nazionali la creazione di registri o licenze per i virtual asset service providers (VASP) ed in particolare spinge affinché sia adottata la cosiddetta travel-rule.*

Vale la pena osservare che l'identificazione di originatore e beneficiario rischia di essere problematica e pericolosa per Bitcoin ed affini. Anzitutto, realizzarla tecnicamente è difficile ai limiti dell'impossibile: le *best-practices* in tema di sicurezza e *privacy* prevedono che un utente utilizzi un indirizzo Bitcoin diverso per ogni transazione Bitcoin: pertanto non esiste un indirizzo unico che possa essere utilizzato come identificativo univoco come accade, ad esempio, per il codice IBAN. Impedire questa pratica o complicarla con la creazione di gigantesche *white-list* di indirizzi nominativamente associati, il cui aggiornamento risulterebbe comunque improbo e difficile da disegnare funzionalmente, spingerebbe il mercato verso quegli intermediari che non effettuano alcun tipo di identificazione. Il risultato sarebbe quello di danneggiare, ad esempio, le borse più adempienti in termini di KYC, AML, CTF, perdendo quindi la più solida base dati oggi a disposizione di investigatori e regolatori.

[62] https://www.coindesk.com/bundesbank-chief-warns-on-risks-of-central-bank-digital-currencies
[63] https://www.coindesk.com/new-risks-swiss-government-skeptical-on-central-bank-digital-currency
[64] http://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html e http://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets-fatf-standards.html
[65] Si veda in particolare https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html
[66] https://www.coindesk.com/fatf-releases-guidance-on-global-digital-ids-as-use-cases-grow
[67] https://www.forbes.com/sites/forbestechcouncil/2019/12/02/the-travel-rule-new-compliance-guidance-for-cryptocurrency-exchanges/#391253e315f6

Speriamo al regolatore non sfugga il concetto di eterogenesi dei fini, conseguenze non intenzionali di azioni intenzionali, che producono risultati contrari a quelli auspicati.

Il mondo delle ICO

Nel 2019 il fenomeno ICO ha visto un marcato crollo di significatività: noi che non abbiamo mai perso l'occasione di criticarlo come fraudolento nella sostanza (e talvolta anche nelle intenzioni) ce ne rallegriamo. L'unica notizia di interesse questo trimestre è la prima ICO autorizzata in Francia[68] dall'autorità di mercato: qualche mese fa avrebbe ottenuto un risalto straordinario, oggi è riportata solo da sparuti commentatori nostalgicamente affezionati all'argomento. L'attenzione dei regolatori al tema, che abbiamo visto nel 2019, sembra quasi una specie di "bacio della morte": in ogni caso leggeremo il resoconto di Consob alla consultazione dello scorso giugno (abbiamo dato conto della nostra risposta come Crypto Asset Lab nel numero 2019-Q2) e seguiremo le iniziative regolamentari di cui pare si discuterà a livello europeo.

[68] https://www.coinlex.it/2019/12/21/prima-ico-autorizzata-in-francia/

4. Ecosistema

Crypto-assets custody

A conferma di una forte tendenza di crescita che ha interessato tutto il 2019, anche il quarto trimestre ha evidenziato grandi novità per quanto riguarda le soluzioni di custodia per cripto-valute.

La prima novità del trimestre, sebbene fosse nell'aria già da qualche tempo, è stata quella di Bakkt (gruppo ICE, New York Stock Exchange) che ha aperto l'utilizzo dei propri servizi di custodia fino ad allora riservati ai clienti dei Futures Bakkt anche a istituzioni non clienti[69]. Ricordiamo che ad agosto 2019 la Bakkt Wharehouse[70] ha formalmente ottenuto l'autorizzazione da parte del *Department of Financial Services* di New York ad operare come custode certificato di Bitcoin. Questo annuncio è arrivato insieme all'elenco dei primi clienti, tra cui Pantera Capital (Venture Capital), Galaxy Digital (società di asset management che ha lanciato contestualmente un fondo di investimento in Bitcoin[71]) e Tagomi (società di broker in Crypto).

> *Chris Tyrer:" The demand we've seen for Fidelity's digital asset custody has been borderless, and we're scaling our business to operate in a variety of jurisdictions."*

L'altro annuncio rilevante della fine 2019 riguarda Fidelity Investment che, come Bakkt, ha ottenuto per la sua società Fidelity Digital Asset Services l'autorizzazione da parte del Department of Financial Services di New York ad operare come custode certificato di Bitcoin[72]. Forte di questa certificazione, Fidelity ha annunciato[73] a dicembre anche l'ingresso nel mercato europeo con i propri servizi. Chris Tyrer, scelto da Fidelity Digital Assets per guidare l'ingresso nel mercato europeo, ha dichiarato: "*The demand we've seen for Fidelity's digital asset custody and trade execution services has been borderless, and we're scaling our business to operate in a variety of jurisdictions to support this industry for the long-term. In doing so, we're building on the commitment to make digitally native assets, such as Bitcoin, more accessible to institutional investors."* Fidelity Digital Assets entra nel mercato europeo fornendo ai propri investitori un pacchetto completo che parte dalla custodia dei crypto assets, include la *trade execution* e arriva fino a un servizio clienti dedicato.

State Street, una delle maggiori banche depositarie al mondo, ha annunciato[74] a dicembre l'avvio di un progetto pilota sugli asset digitali in collaborazione con Gemini Custody, società posseduta dall'omonima borsa dei fratelli Winklevoss. Lo scopo del pilota è quello di testare l'integrazione del servizio di custodia di Gemini con i servizi tradizionali offerti ai clienti da State Street. Inizialmente il focus sarà su due crypto-assets scelti in base alla maggiore liquidità, ma lo scopo è quello di estendere in futuro il servizio a molti asset. Attualmente Gemini Custody è in grado di gestire Bitcoin, Ether, Bitcoin Cash, Litecoin, zCash e gli ERC-20 Token (sostanzialmente tutti i token emessi come ICO sulla blockchain di Ethereum). L'interesse mostrato da un grande gruppo come State Street ad aggiungere alla lista dei suoi servizi di custodia anche quello sui crypto-assets

[69] https://medium.com/bakkt-blog/raising-the-bar-announcing-bakkt-institutional-custody-ed5e2ad0da9a
[70] https://www.bakkt.com/custody
[71] https://www.newswire.ca/news-releases/galaxy-digital-launches-Bitcoin-funds-899988215.html
[72] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1911191
[73] https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/press-release/fdas-ltd-121719.pdf
[74] https://newsroom.statestreet.com/press-release/corporate/state-street-and-gemini-launch-digital-asset-pilot

dimostra come il mercato stia diventando sempre più maturo e che la spinta del mondo istituzionale ad entrare è sempre più evidente.

Che la tendenza del mercato sia fortemente orientato allo sviluppo di soluzioni per la custodia di crypto assets anche in Europa è evidenziato, oltre che dall'ingresso di Fidelity, dalle banche che stanno iniziando ad investire in questo mondo. Reuters riporta indiscrezioni secondo le quali ING starebbe lavorando internamente allo sviluppo di una soluzione di custodia[75]. La banca tedesca Solaris Bank ha invece aperto una sussidiaria dedicata a questo tipo di servizi per digital assets, Solaris Digital Assets GmbH[76].

Per tutte queste soluzioni di custodia ci sono legittime perplessità circa la loro effettiva robustezza: nessuno dei player fa *disclosure* del protocollo di sicurezza utilizzato, preferendo invece una opaca *security-by-obscurity* che si tenta di far passare inosservata facendo leva sul "credito reputazionale" accordato dal mercato.

Anche il mercato italiano si muove verso la creazione di società specializzate nello sviluppo di soluzioni di custodia. Una delle prime società a muoversi in tal senso è stata Conio. Conio è un wallet Bitcoin multi-firma, dove cioè per muovere i fondi è necessaria l'autorizzazione, tecnicamente una firma digitale, di più entità. In Conio specificamente per muovere i fondi sono necessarie almeno due firme su tre possibili. Le chiavi per firmare digitalmente le transazioni sono detenute una dal cliente, una da Conio e una da una terza parte (es. una banca)[77].

Un'altra soluzione per la custodia sicura di Bitcoin sviluppata in Italia è quella di CheckSig[78], startup innovativa costituita a fine ottobre 2019[79]. L'idea innovativa di CheckSig è quella di andare oltre la prassi di mercato di *security-by-obscurity* per offrire un protocollo di custodia aperto, completamente verificabile, che offre coperture assicurative ed è basato su una sicurezza a due livelli. Per la maggior parte del tempo i Bitcoin sono custoditi in un wallet multi-firma gestito da una federazione di differenti entità legali e non accessibili da CheckSig. Ogni membro della federazione ha un dispositivo HSM (*hardware secure module*) che è in grado di firmare solo ed esclusivamente le transazioni che muovono i fondi verso il wallet gestito da CheckSig, rifiutando tutte le altre transazioni. Quando viene effettuata una richiesta di prelievo la federazione firma una transazione che manda l'ammontare richiesto al wallet di CheckSig, la quale, dopo le opportune verifiche circa la correttezza della richiesta di prelievo, manda i fondi al cliente

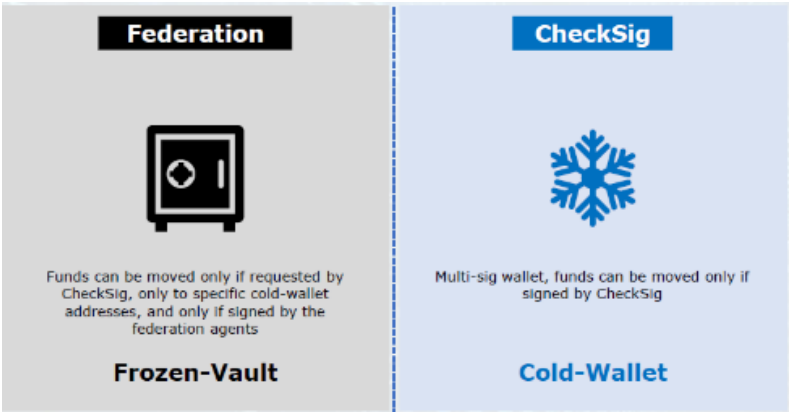


Figura 4: Custodia a 2 livelli di CheckSig

[75] https://www.reuters.com/article/us-crypto-currencies-ing-exclusive/exclusive-ing-working-on-digital-assets-custody-technology-sources-idUSKBN1YF2GN
[76] https://solarisbank.pr.co/184220-solarisbank-launches-subsidiary-solaris-digital-assets-to-drive-adoption-of-crypto-and-further-digital-assets
[77] https://medium.com/conio/custody-at-conio-part-1-ddbe81a106ce
[78] https://checksig.io/
[79] https://legalcommunity.it/sza-checksig-custodia-criptovalute/

finale. La soluzione di custodia pensata da CheckSig è attualmente in fase di sviluppo, con l'obiettivo di andare live entro la fine del primo trimestre 2020.

BitMex rivela mail utenti, furto di Ether su Upbit

Anche in questo trimestre non sono mancati gli incidenti di sicurezza negli Exchange.

Nel caso di BitMex non si è trattato di un attacco esterno ma di un problema interno che ha comportato l'esposizione dei dati privati dei clienti. In una mail inviata ai propri clienti a inizio novembre tutti gli indirizzi e-mail dei destinatari sono stati inseriti in chiaro[80] e resi quindi visibili a tutti. La borsa è tempestivamente intervenuta per assicurare che il problema di sicurezza è stato risolto e che non sono stati esposti ulteriori dati sensibili. È importante evidenziare come questo tipo di falle nelle procedure di sicurezza, in particolar modo per un Exchange, sono molto pericolose. L'esposizione delle mail dei clienti può infatti portare a successivi attacchi di *social engineering* finalizzati al furto di credenziali di accesso all'Exchange e quindi ai relativi asset detenuti.

L'esposizione delle mail dei clienti può infatti portare a successivi attacchi di social engineering finalizzati al furto di credenziali di accesso all'Exchange e quindi ai relativi asset detenuti.

Bitmex non è il solo Exchange ad essere finito alla ribalta nel trimestre. Nello stesso periodo infatti anche la borsa sud-coreana Upbit ha subito un attacco che ha portato al furto di 342.000 Ether, per un controvalore al momento del furto di circa $49 milioni[81].
Upbit ha prontamente sospeso gli scambi e dichiarato che le perdite subite in questo attacco saranno interamente coperte tramite le risorse finanziarie aziendali. I fondi prelevati irregolarmente dall'Exchange sono stati inviati tramite una singola transazione a un indirizzo unico[82].

Poloniex abbandona il KYC

In questa fase storica di crescenti pressioni regolamentari sugli Exchange per incrementare i controlli sui clienti in fase di registrazione, ha fatto rumore la decisione di Poloniex di eliminare la procedura di verifica (KYC) per alcune fasce di clienti[83]. In particolare, Poloniex ha annunciato che non sarà più necessario effettuare il KYC per i clienti a patto che non vengano effettuati prelievi di importo superiore a 10.000$. Tramite l'utilizzo di una e-mail è quindi ora possibile iniziare ad operare sull'Exchange, senza limiti in fase di deposito e trading.

Questo allentamento regolamentare è stato reso possibile grazie all'interruzione di tutte le operazioni in territorio statunitense. L'Exchange ha infatti spostato la propria sede dal Delaware a Bermuda e ha dato tempo fino al 15 dicembre agli utenti US per prelevare i propri fondi e chiudere gli account[84].

[80] https://blog.bitmex.com/updated-statement-on-the-email-privacy-issue-impacting-our-users/
[81] https://www.coindesk.com/crypto-exchange-upbit-confirms-theft-of-49m-in-ether
[82] https://etherscan.io/tx/0xca4e0aa223e3190ab477efb25617eff3a42af7bdb29cdb7dc9e7935ea88626b4 e https://etherscan.io/address/a09871aeadf4994ca12f5c0b6056bbd1d343c029
[83] https://medium.com/poloniex/a-new-account-tier-is-here-bebb4a8919e0
[84] https://www.coindesk.com/poloniex-drops-kyc-for-withdrawals-below-10000-following-us-exit

5. Vita dell’Istituto

DGI Training Program

In linea con la domanda crescente di tecnici qualificati sui temi Bitcoin e blockchain, l'Istituto ha deciso di proporre il proprio percorso formativo accademico al mondo corporate, qualificandolo dal punto di vista tecnico ed industriale. Il 2020 vede quindi la nascita del *DGI Training Program*, piano formativo dedicato a chiunque voglia approfondire il tema della scarsità in ambito digitale e le sue applicazioni tra industria, assicurazione, finanza, fin-tech, reg-tech e venture capital[85]. Docenti del corso: Ferdinando Ametrano e Paolo Mazzocchi.

> *Il 2020 vede la nascita del DGI Training Program, piano formativo dedicato a chiunque voglia approfondire il tema della scarsità in ambito digitale e le sue applicazioni tra industria, assicurazione, finanza, fin-tech, reg-tech e venture capital.*

L'offerta formativa è strutturata su due giornate full-time, fruibili anche singolarmente. La prima giornata è rivolta a tutti, senza particolari prerequisiti: prevede una solida e ampia introduzione sui temi Bitcoin e blockchain, per poi approfondire, in maniera funzionale, la natura di blockchain e *distributed consensus*. Completa la giornata un panorama sui servizi finanziari ed assicurativi per i crypto-asset (futures, custodia, ecc.) e le applicazioni non finanziarie della blockchain. La seconda giornata è invece un *dev-day* rivolto agli sviluppatori o comunque a chi vuole comprendere anche gli aspetti strettamente tecnologici ed implementativi: è richiesta una buona attitudine al pensiero logico, matematico e computazionale. I contenuti della prima giornata sono evidentemente dati per già acquisiti in questa seconda giornata, da considerarsi strettamente come un *deep-dive.*

Il primo evento formativo è programmato per il 21 e il 22 aprile: il corso si potrà acquistare sia interamente (due giornate) sia scegliendo solo una delle giornate proposte.

SIAT Magazine: intervista a Ferdinando M. Ametrano

SIAT – Società Italiana Analisi Tecnica – è un'istituzione italiana che riunisce gli analisti tecnici dei mercati finanziari[86]. SIAT promuove una rivista aperta, non commerciale, dove convergono il punto di vista del mondo accademico, del trading e dell'asset management.

Nel terzo numero di SIAT Magazine, pubblicato a dicembre 2019, la *financial journalist* Maddalena Liccione intervista il nostro direttore Ferdinando M. Ametrano in un articolo dal titolo "Bitcoin: l'oro digitale". Questo l'attacco dell'intervista: «Se ne discute molto, ma su Bitcoin la divisione è radicale, tra scettici che parlano di bolla ed entusiasti che descrivono una rivoluzione globale. Tra questi ultimi, Ferdinando Maria Ametrano è uno degli esperti più controversi ed interessanti: fisico di formazione, per decenni si è occupato di derivati finanziari, fino al 2014 quando scopre Bitcoin; oggi dirige il Digital Gold Institute ed insegna "Bitcoin and Blockchain Technology" all'Università Milano Bicocca ed al Politecnico di Milano.» L'intervista è scaricabile nella sezione magazine del sito web del SIAT[87].

[85] https://dgi.io/training_it/
[86] https://www.siat.org/
[87] http://bit.ly/2NrmdXp

Crypto Asset Lab membro del Global Digital Finance

Il trimestre ha visto anche l'ingresso tra i membri del Global Digital Finance (GDF)[88] del Crypto Asset Lab (CAL)[89], l'iniziativa di ricerca congiunta tra il Digital Gold Institute e l'Università degli Studi di Milano-Bicocca, già presentata nel report 2019-Q2. GDF è una organizzazione che promuove l'accelerazione e l'adozione dei crypto-asset e delle tecnologie per la finanza digitale nei servizi finanziari tradizionali. L'accordo di partnership è l'opportunità per il CAL di integrarsi all'interno della più grande community di finanza digitale internazionale e permette il mutuo scambio in materia industriale, tecnologica e accademica. Inoltre, GDF è in prima linea nel seguire le attività di FAFT.

Il Salone dei pagamenti – Payvolution

Venerdì 8 novembre, in occasione de Il Salone dei Pagamenti – Payvolution, si è svolta la tavola rotonda "Criptovalute e nuovi player nel mercato dei Pagamenti: uno sguardo sul mondo" [90]. Il direttore dell'istituto *Ferdinando Ametrano* ha moderato il confronto sul tema del cambiamento del sistema finanziario tradizionale, a seguito dell'introduzione delle criptovalute nel mondo dei pagamenti. Relatori del panel: *Andrea Alemanno (*Senior Client Officer Ipsos), *Luca Fantacci (*Docente di Storia Economica Università Bocconi), *Paolo Gianturco* (Business Operations & FinTech Leader Deloitte Consulting) e *Claudia Segre (*Presidente Global Thinking Foundation).

Dai commenti dei partecipanti alla tavola rotonda è emersa evidente la crescita del fenomeno delle criptovalute che però si sviluppa in un ecosistema selvaggio: l'assenza di una sponda regolamentare chiara per i nuovi possibili modelli operativi rende difficile l'implementazione dei nuovi strumenti di pagamento e delle tecnologie complementari ai nuovi servizi finanziari. Sono necessari, quindi, una regolamentazione adeguata alla protezione del suo potenziale sviluppo e strumenti tecnologici in grado di supportarne le potenzialità. Fatti confermati dai dati dell'ecosistema retail: il fenomeno delle criptovalute è ancora di nicchia e l'attesa per i servizi di innovazione finanziaria non è significativa.[91]

DGI entra nella community del Fintech District

A dicembre scorso Digital Gold Institute ha spostato la propria sede operativa presso il Fintech District di Milano (via Filippo Sassetti 32), entrando a far parte di un ecosistema fintech italiano composto ad oggi da 136 entità del settore[92]. Il Digital Gold Institute rappresenta l'eccellenza nella formazione e consulenza sui temi della scarsità in ambito digitale e sulla tecnologia blockchain; il Fintech District raccoglie le eccellenze fintech italiane: il matrimonio era inevitabile.

[88] https://www.gdf.io/
[89] https://cryptoassetlab.diseade.unimib.it/
[90] http://bit.ly/2thvkmD
[91] https://dgi.io/2019/11/08/il-salone-dei-pagamenti.html
[92] https://www.fintechdistrict.com/community/

Autori

Ferdinando M. Ametrano

ferdinando@dgi.io

Paolo Mazzocchi

paolo@dgi.io

Lucia Mandelli

lucia@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