



Digital Gold Institute

Scarcity in the Digital Realm

N. 10



REPORT TRIMESTRALE

2021 Q3

INDICE

Opinion

Governance, criptografica e regolatori	5
--	---

Mercato

Bitcoin	14
Alt-coin	20
Futures e opzioni	23

Ecosistema

El Salvador: la genesi di bitcoin a corso legale	26
La chiusura totale della Cina	27
Binance: l'emergere delle lacune regolamentari	28
La guerra dei talenti	30
Ransomware: strategie cybercriminali ed effetti	31
Poly Network Hack: l'importanza della sicurezza informatica	32
Non-fungible token: un mercato miope	33

Regolazione

Central Bank Digital Currency: sperimentazioni in Europa e nel mondo	36
US infrastructure Bill: svolta normativa in USA	36
SEC: la vigilanza attiva sull'ecosistema	38
Coinbase: il servizio Lend al vaglio della SEC	38

Tecnologia

Bitcoin: aggiornamento al protocollo	42
Ethereum: aggiornamento al protocollo	42
Bitcoin ed Ethereum: protocollo a confronto	43
Mining: sostenibilità ambientale	44

Vita dell'Istituto

Presenza sui media	49
CryptoWeek	50
Workshop Bitcoin & Blockchain	50
Presentazione del report trimestrale	51
Crypto Asset Lab Conference	51



 **CheckSig**
TRANSPARENT BITCOIN CUSTODY

Deloitte.

Ad uso esclusivo dei collaboratori e partner del Digital Gold Institute;
è vietata la distribuzione senza autorizzazione di questo documento.

© 2021 DIGITAL GOLD INSTITUTE



Governance, crittografica e regolatori

di Ferdinando M. Ametrano, CheckSig Executive Officer

La dinamica dei prezzi di mercato delle criptovalute sembra poco reattiva rispetto agli sviluppi strettamente tecnici dei protocolli sottostanti. In passato Ethereum ha fallito molti aggiornamenti protocollari senza che le quotazioni ne risentissero negativamente. A giugno Bitcoin ha dato luce verde a Taproot, una delle innovazioni protocollari più significativa degli ultimi anni, senza che questo abbia avuto un impatto positivo. Sembra cambiare qualcosa oggi con l'aggiornamento denominato London messo in produzione sulla rete Ethereum, ma l'impressione anche in questo caso è che la percezione positiva sia dovuta più all'attività di pubbliche relazioni della Ethereum Foundation che non a genuini meriti tecnici. Proviamo a fare ordine. Il 12 giugno la rete Bitcoin ha formalmente preso atto che i minatori si dichiarano pronti a recepire Taproot, la più importante evoluzione del protocollo Bitcoin degli ultimi anni. I minatori avevano tre mesi di tempo, dallo scorso maggio, per manifestare la loro readiness, cioè la loro capacità e predisposizione tecnica a recepire il cambiamento: questa era la finestra dello Speedy Trial,



Ferdinando M. Ametrano

un processo pensato per constatare velocemente che i minatori erano pronti alla ricezione di Taproot.

La comunità tecnica ricorda ancora con angoscia la guerra civile Bitcoin nel 2015-2017 per l'approvazione di SegWit, il precedente aggiornamento protocollare: si era trattato di un processo estremamente contenzioso e che ha dato vita all'hard fork (nascita per biforcazione) di Bitcoin Cash. Chi volesse approfondire ne può leggere nell'interessante libro appena uscito *The Blocksize War*.

Per Taproot non sembravano sussistere incertezze o controversie, ma si stava delineando comunque una situazione di stallo per i diversi pareri su come i minatori potessero o dovessero manifestare la loro disponibilità; non si voleva, infatti, che il processo sembrasse un voto di approvazione dei minatori, come se questi fossero una specie di tribunale ultimo. Doveva essere chiaro che si tratta di una proposta degli sviluppatori Bitcoin, sostanzialmente approvata da utenti, investitori ed industria: i minatori sono solo una delle componenti dell'universo Bitcoin, nel processo di governance decentralizzata che vede protagonisti tutti i diversi attori appena menzionati.

Lo Speedy Trial è stato quindi un efficace compromesso: se la maggioranza qualificata dei minatori (superiore al 90%) si fosse velocemente dichiarata pronta, non sarebbe stato necessario fare verifiche più complesse o contenziose. In poche settimane il 99% dei minatori si è dichiarato pronto. La vera e propria attivazione di Taproot, nel senso della possibilità di sfruttare le sue nuove funzionalità sulla rete Bitcoin, è a questo punto fissata per il prossimo novembre (più precisamente, al blocco numero 709632).



Taproot introduce un nuovo schema di firma digitale: originariamente ideato da Schnorr, è più efficiente e flessibile del tradizionale standard di firma digitale noto come ECDSA, ma non era mai stato standardizzato o adottato perché coperto da brevetto. Il brevetto adesso è scaduto e la comunità Bitcoin è stata la prima a implementarlo in un ambito crittografico industriale (ennesima dimostrazione che in ambito tecnologico i brevetti possono essere un freno all'innovazione invece che una tutela della proprietà intellettuale).

“ Taproot migliora la riservatezza delle transazioni Bitcoin ed aumenta notevolmente la versatilità

”

La firma digitale è il modo più comune di autorizzare il trasferimento di Bitcoin, cioè di soddisfare quelle che in gergo tecnico vengono chiamate condizioni di spendibilità. Ma Taproot introduce anche la possibilità di prevedere

molteplici e più sofisticate condizioni di spendibilità, espresse da script celati in un albero di possibilità che non viene mai reso pubblico, se non per la singola condizione di spendibilità soddisfatta al momento del trasferimento. Questa possibilità migliora la riservatezza delle transazioni Bitcoin ed aumenta notevolmente la versatilità, rappresentando un passo fondamentale per gli sviluppi futuri: nei prossimi mesi ne vedremo i benefici.

July 15, 2021

R&D



London Mainnet Announcement

by Tim Beiko

L'ultimo aggiornamento al protocollo Ethereum, denominato London, è stato attivato giovedì 5 agosto. Dalla sua nascita nel luglio 2015, Ethereum ha visto dodici aggiornamenti; nello stesso periodo Bitcoin solo due. Bitcoin privilegia la stabilità e progredisce tramite soft-fork, cioè modifiche sempre retro-compatibili, che non estromettono dalla rete i nodi che non si aggiornano; Ethereum, invece, progredisce tramite hard-fork, modifiche non retro-compatibili e talvolta contenziose al punto da dar luogo a criptovalute alternative come Ethereum Classic.

Nell'evoluzione di Bitcoin non c'è una roadmap definita, ma un processo incrementale che, in assenza di un leader, deve essere approvato da tutti: sviluppatori, minatori, utenti, investitori, industria di servizi; un consenso storicamente difficilissimo da ottenere ma mirato a rendere l'infrastruttura tecnologica di base sempre

più robusta, a garantire che il trasferimento di valore tramite la criptovaluta bitcoin sia sicuro ed incensurabile, ad evitare che l'equivalente digitale dell'oro possa "arrugginire".

Viceversa, Ethereum ha un chiaro leader in Vitalik Buterin e perfino una ricchissima fondazione impegnata a sostenere lo sviluppo della piattaforma, anche con



Vitalik Buterin

attività di marketing e pubbliche relazioni. Lo zar Vitalik sono anni che indica la terra promessa di Ethereum 2.0, quando gli errori di design dell'attuale Ethereum saranno sanati e sarà rispettato l'impegno a fornire una infrastruttura tecnologica di base straordinariamente versatile. Allora ether, la criptovaluta nativa della piattaforma Ethereum, vedrà realizzato il suo ruolo di carburante consumato per far funzionare applicazioni sofisticate ed incensurabili. La roadmap evolutiva era addirittura definita in maniera ineluttabile: ad esempio, l'adozione della vagheggiata Proof-of-Stake ecologicamente sostenibile, con cui rimpiazzare la energivora Proof-of-Work copiata da Bitcoin, era forzata nel codice originario tramite l'innesco di una bomba a tempo, la cui esplosione avrebbe dovuto rendere impossibile l'utilizzo di una piattaforma Ethereum che non progredisse. Ovviamente, questa bomba viene disinnescata e rimandata in avanti ad ogni hard-fork, incluso London, certifi-

cando se non il fallimento del piano di sviluppo almeno il suo velleitarismo.

In questi anni Ethereum si è dimostrata una piattaforma versatile, capace di ospitare oltre a ether anche altri nuovi crypto-asset, resi possibili dagli smart-contract. Si tratta di programmi software la cui esecuzione sulla piattaforma Ethereum è incensurabile, perché economicamente sostenuta dal consumo di ether a vantaggio di quei nodi della rete detti minatori. Infatti, se in Bitcoin i minatori validano transazioni che verificano condizioni programmatiche molto semplici, in Ethereum le condizioni programmatiche possono essere sofisticatissime, fino a far nascere i crypto-kitties, gattini software che rappresentano l'evoluzione dei vecchi Tamagotchi, gli animaletti hardware popolari alla fine degli anni 90. O dar luogo a token collocati sul mercato come fossero azioni o immaginificamente rappresentativi di opere d'arte.

Nel primo caso si parla di fungible token, emessi tramite le cosiddette Initial Coin Offering (ICO): nella quasi totalità truffe che hanno tentato di aggirare la regolamentazione sull'emissione di securities. Nel secondo caso si tratta di non-fungible token (NFT), moda recente che ha visto il suo apice a marzo, quando l'artista americano Beeple ha venduto per oltre 69 milioni di dollari una delle sue opere in un'asta di Christie's che è entrata nella storia. Un NFT è semplicemente un token che rimanda ad una stringa alfanumerica che rimanda a sua volta all'opera d'arte; non garantisce alcun diritto particolare per il possessore del token rispetto all'opera d'arte vera e propria: non la proprietà, non l'usufrutto, non i diritti d'utilizzo, nemmeno l'esclusiva nella riproducibilità dell'opera. Se soffrite di horror vacui, state lontano dagli NFT: al confronto l'aria fritta è un concetto meglio definito.

Ma la grande storia di successo negli ultimi due anni su Ethereum è stata la Decentralized Finance (DeFi). Si tratta della replica tramite smart contract di prodotti e pratiche tipici dei mercati finanziari: riproposti in salsa decentralizzata,



cioè senza regolatori, senza garanzie per gli investitori e rispolverando dalla storia tutte quelle pratiche ormai ritenute illegali sui mercati regolati. I volumi transazionali in ambito DeFi sono esplosi, senza arrestarsi per i molteplici scandali, furti e malfunzionamenti che hanno già vorticosamente distrutto gli investimenti di tanti a vantaggio dei soliti furbi. Si sono però arrestati di fronte al fatto che Ethereum arrancava, non riusciva a sostenere il crescente traffico dati e carico computazionale, le commissioni transazionali diventavano altissime, insomma la piattaforma tecnologica si rivelava un colabrodo che non scalava di fronte alle nuove esigenze.



Qui, di nuovo, Vitalik e la fondazione hanno promesso che tutti i problemi sarebbero stati risolti. Certo, il passaggio a Proof-of-Stake non è ancora pronto, nonostante fosse stato promesso per Novembre 2016: London ha dissinnescato la bomba a tempo fino a Dicembre 2021. Anche lo sharding non è ancora pronto; si

tratta della suddivisione della ipertrofica blockchain di Ethereum tra i diversi nodi della rete: un singolo nodo non può sostenerla, perché ormai cresciuta in sei anni a oltre 6 Terabyte di dati (per contro la blockchain di Bitcoin è circa 20 volte più leggera, nonostante abbia dodici anni di vita). Certo, non è nemmeno pronta la nuova Ethereum Virtual Machine, il motore che esegue gli smart contract: avrebbe dovuto consentire quella verifica formale del codice indispensabile per ridurre le vulnerabilità all'origine dei tantissimi scandali e frodi sulla piattaforma Ethereum. Ed allora cosa c'è davvero in London?

London fondamentalmente consiste nell'implementazione di EIP1559, una modifica della gestione delle commissioni transazionali che le rende più prevedibili e, soprattutto, più economiche. Si spera così di riprendere quella DeFi che nel frattempo, alla faccia della decentralizzazione, si è spostata e sta fiorendo sulla Binance Smart Chain, blockchain privata e centralizzata promossa dalla borsa di scambio Binance. Inoltre, EIP1559 prevede che parte delle commissioni transazionali vengano distrutte invece di essere riconosciute ai minatori: scelta pericolosa, perché rischia di esacerbare il problema del Miner Extractable Value (MEV). Si tratta della massimizzazione del profitto che i minatori possono ottenere sequenziando arbitrariamente le transazioni validate, in tutte quelle situazioni in cui l'ordine può dare un vantaggio economico secondo le regole dei diversi smart contract. La distruzione di parte delle commissioni transazionali riduce anche la base monetaria di ether, con l'intento di renderli più scarsi e quindi di farne aumentare il valore. Questo perché, tra le altre incongruenze di Ethereum, la politica monetaria di ether non è fissata a priori, ma può essere decisa di volta in volta dal Governatore di Banca Centrale Buterin e/o dal comintern dei suoi collaboratori.

A questo punto, il lettore che ha avuto la pazienza di leggere fin qui si starà chiedendo: ma, allora, come è possibile che Ethereum sia così popolare ed amato? Difficile a dirsi. Sembra, però, che il combinato disposto di marketing visionario e diffusa ignoranza tecnologica abbia buon gioco in un mercato per ora sempre guidato, nel bene e nel male, dal miraggio della ricchezza facile.

“ London rende più prevedibili ed economiche le commissioni transazionali. ”

Ovviamente, le differenze tra Bitcoin e Ethereum hanno rilevanti implicazioni di metodo e di governance, anche per i regolatori che guardano all'ecosistema dei crypto-asset, spesso confusi dalla difficoltà di distinguere i fenomeni e valutarli adeguatamente.

Le differenze tra Bitcoin ed Ethereum si rintracciano subito all'atto di nascita: da una parte lo sconosciuto sviluppatore e crittografo Satoshi Nakamoto che offre al mondo un protocollo funzionante ed immediatamente utilizzabile da tutti, dall'altra parte l'Ethereum Foundation di Vitalik Buterin, fondazione svizzera che raccoglie bitcoin in cambio di ether che saranno resi disponibili sulla piattaforma solo quando questa sarà sviluppata.

Nel caso di Bitcoin, dall'annuncio del 31 ottobre 2008 al rilascio del 3 gennaio 2009 passeranno poco più di due mesi. La piattaforma Ethereum, invece, viene annunciata a cavallo tra la fine del 2013 e l'inizio del 2014, la campagna di finanziamento si svolge nell'estate 2014, il rilascio originariamente promesso entro la fine dell'anno arriva solo il 30 luglio 2015, dopo 18 mesi.

Nakamoto rilascia la sua creatura con la marcatura temporale del 3 gennaio 2009, ottenuta citando all'interno del primo blocco della blockchain il titolo giornalistico della testata The Times: “Chancellor on brink of second bailout for banks”. La citazione dimostra che Nakamoto non ha sfruttato solitariamente e segretamente la piattaforma per accumulare bitcoin prima del 3 gennaio 2009. Ovviamente nel primo anno sarà tra i pochi ad utilizzarla e sostenerla con l'attività di mining e per questo accumulerà circa un milione di bitcoin, ma la stessa opportunità è offerta a tutti, senza privilegi speciali per il fondatore. Il quale, peraltro, non ha finora mai speso nulla della fortuna accumulata e, scomparendo dalle scene a metà 2010, sembra averla abbandonata: in molti considerano quei bitcoin persi per sempre.



La Ethereum Foundation punta, invece, sul cosiddetto pre-mine, l'accumulo di ether ottenuto come privilegio del fondatore e dei finanziatori della prima ora, e manterrà sempre la leadership indiscussa e carismatica di Buterin. Fondazione e fondatore sono per questo diventati ricchissimi e restano sempre protagonisti nella gestione del protocollo.

Anche nel mondo Bitcoin, dopo la scomparsa del fondatore, era stato tentato l'esperimento di una fondazione, come voce ufficiale che potesse dialogare con regolatori e governi, gestire lo sviluppo del protocollo ed indicare le priorità strategiche. Ma fallisce miseramente perché l'ethos Bitcoin rigetta un governo centrale: in breve la fondazione resta in mano a personaggi senza arte né parte, molti dei quali avranno anche disavventure giudiziarie. Da allora la gestione del protocollo è affidata ad un processo informale e dinamico di interazione tra i diversi attori della rete: sviluppatori, minatori, utenti, investitori ed industria. Ognuno di loro ha incentivi economici a tratti sinergici, a tratti contrastanti, ma che devono inesorabilmente trovare una composizione affinché l'esperimento Bitcoin possa crescere.

Buterin ed i suoi collaboratori stretti detengono, invece, il controllo sostanziale del protocollo. Diventa evidente a tutti col fallimento nel 2016 di DAO, l'esperimen-

“ Le differenze tra Bitcoin e Ethereum hanno rilevanti implicazioni di metodo e di governance. ”



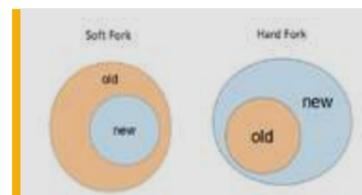
to della prima Distributed Autonomous Organization. Si trattava dell'ambizioso lancio di un Venture Capital distribuito, dove i fondi raccolti sono distribuiti tra le start-up secondo criteri rigidamente fissati dal codice di uno smart contract. Contratto non troppo smart, visto che un "imprenditore", leggendone le "clausole scritte in piccolo", trova modo di dirottare a suo vantaggio i fondi della DAO. Per bloccarlo, Buterin ed i suoi collaboratori decideranno di cambiare arbitrariamente il protocollo Ethereum per cancellare la transazione incriminata, con spreco totale per l'idea di un libro contabile distribuito ed immutabile.

Questa prassi diventerà la regola: gli aggiornamenti del protocollo Ethereum avverranno senza riguardo alla compatibilità con le applicazioni esistenti sviluppate da altri progetti sulla piattaforma, che in alcuni casi smetteranno di funzionare.

I nodi della rete saranno costretti a recepire tempestivamente gli aggiornamenti, pena ritrovarsi su una rete alternativa e secondaria perché senza la benedizione del gruppo dirigente. La fondazione si preoccuperà della comunicazione con una narrativa sempre soavemente amichevole e orientata all'innovazione. Promette dal 2016 un Ethereum che non consumerà più energia, passando da Proof-of-Work a Proof-of-Stake e copre nel frattempo l'incapacità del gruppo di sviluppo in ritardo ormai di cinque anni. Discute dello sharding che dovrebbe permettere ad ogni nodo della rete di avere almeno un pezzo della blockchain, invece di doversi fidare ciecamente della storia transazionale validata dagli sviluppatori. Valorizza la flessibilità del protocollo, silenziando l'evidenza di una rete incapace a sostenere il peso degli esperimenti di successo: i crypto-kitties prima, la Decentralized Finance (DeFi) e i Non-fungible Tokens (NFT) oggi, nati sulla rete Ethereum sono costretti a migrare su altre piattaforme, più o meno centralizzate, per sopravvivere o morire appena passa la moda (come le ICO popolari nel 2017-2018).

In Bitcoin ogni aggiornamento deve sempre essere retrocompatibile, senza lasciare indietro nessuno e nessuna applicazione. Ovviamente, questa scelta rallenta i progressi, rendendoli più faticosi, ma più robusti e sostenibili. E soprattutto non danneggia gli interessi economici di chi ha investito nel Bitcoin esistente: il Bitcoin futuro potrà estendere quello attuale, ma non modificarlo. La criptocrazia di Bitcoin è spietatamente meritocratica, intrinsecamente legata all'allineamento degli incentivi economici di mercato, non riconosce leader.

Per questo Bitcoin è più resistente di fronte alla possibilità che un regolatore possa imporre modifiche o costringere in una certa direzione.



Non c'è un gruppo dirigente che possa essere persuaso o corrotto. Bitcoin è ciò che la maggioranza economicamente significativa dei suoi attori decide che debba essere. Paradossalmente, è comunque più facile da inquadrare nel contesto



normativo internazionale: esiste, ad esempio, un contratto futures su Bitcoin, scambiato al Chicago Mercantile Exchange, la storica e prestigiosa borsa mondiale delle materie prime. Anche questa circostanza rafforza l'idea che, più che una valuta, Bitcoin sia una materia prima, equivalente digitale dell'oro. Insomma, la robustezza e semplicità di Bitcoin ne fanno un oggetto che i regolatori non possono manipolare, ma possono inquadrare in maniera tutto sommato semplice. Un oggetto che, a dispetto delle migliaia di cloni, non è stato possibile replicare davvero, per la forza del suo network effect e della subottimalità di tutte le alternative viste finora.

Per Ethereum è tutta un'altra storia: ha nella fondazione un emittente formale ed ha un gruppo informale, ma chiaramente individuato, che ne controlla lo sviluppo. Insomma, sembra più un titolo di investimento che non una materia prima. Inoltre, la sua flessibilità consente la creazione di smart contract che, di volta in volta, possono essere titoli, obbligazioni, beni, impegni, promesse o altro: un bel grattacapo definirne la natura. Insomma, potenzialmente fragile di fronte alla pressione dei regolatori e complicato da inquadrare normativamente.

Infine, tutte le funzionalità di Ethereum sono replicabili e replicate da piattaforme equivalenti totalmente centralizzate, come la Binance Smart Chain.

Il confronto delineato in questi paragrafi potrà sembrare severo o parziale, ma è corroborato da evidenze tecnologiche e di mercato. Ethereum ha avuto dozzine di incidenti tecnici, Bitcoin solo uno nei primi mesi della sua vita. Il mondo della finanza tradizionale e dei grandi capitali ha aperto tra 2020 e 2021 a Bitcoin, mentre l'interesse per Ethereum è secondario. Qualcuno può immaginare che possano convivere entrambi, ma il circo Ethereum confonde osservatori e regolatori, è il parco giochi di sviluppatori velleitari dove spesso si intrufolano ciarlatani e truffatori: rappresenta per lo scontroso Bitcoin, impegnato nel duro lavoro di rendere sostenibile l'esperimento dell'oro digitale, il fratello dissennato, tanto di successo quanto frivolo e irresponsabile, che rovina la reputazione della famiglia. Ovviamente il tempo dirà se quanto qui descritto sia un insieme di indizi sostanziali o invece solo evidenze parziali e premature. Ad ognuno l'arduo compito di comprendere e giudicare.

“ Bitcoin è ciò che la maggioranza economicamente significativa dei suoi attori decide che debba essere; Ethereum è tutta un'altra storia. ”

I tuoi Bitcoin, al sicuro.

La custodia fai-da-te di Bitcoin può essere impegnativa.

Password perse, attacchi di phishing, aggiornamenti del software: ci sono purtroppo molti modi per perdere i propri Bitcoin.

Per questo puoi affidarti a CheckSig.

CheckSig offre un servizio trasparente di custodia per chi desidera tenere al sicuro i propri Bitcoin su orizzonti temporali medio-lunghi.

Con il suo schema multi-firma e multi-livello, CheckSig fornisce una protezione incomparabilmente superiore al tradizionale hardware wallet.

Inoltre, CheckSig è l'unico custodian italiano dotato di coperture assicurative sui fondi della clientela, e che può vantare attestazioni SOC del service audit indipendente di Deloitte.

Un servizio completo, arricchito da servizi di *concierge* su investimenti e fiscalità, passaggio generazionale, soluzioni fiduciarie, accesso completo all'offerta formativa e alla ricerca del Digital Gold Institute.

CheckSig è il partner ideale per affiancarti nel tuo investimento in Bitcoin.

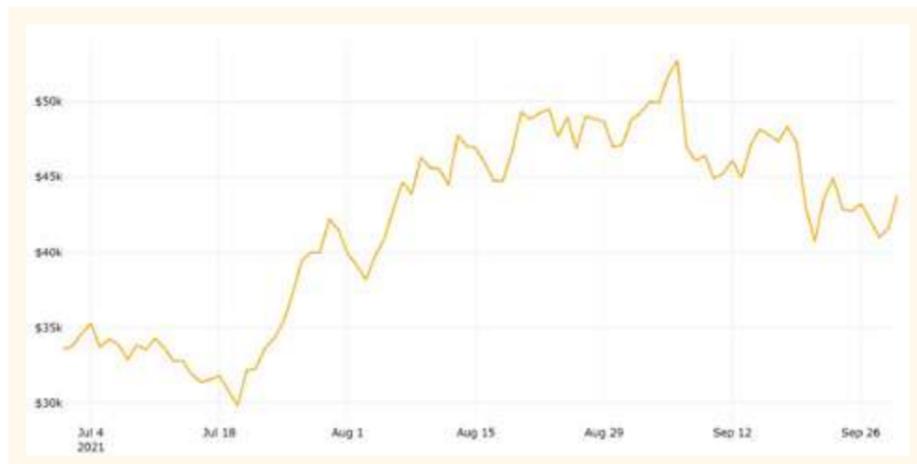
Scopri di più su [checksig.io](https://www.checksig.io)

 **CheckSig**
TRANSPARENT BITCOIN CUSTODY

MERCATO

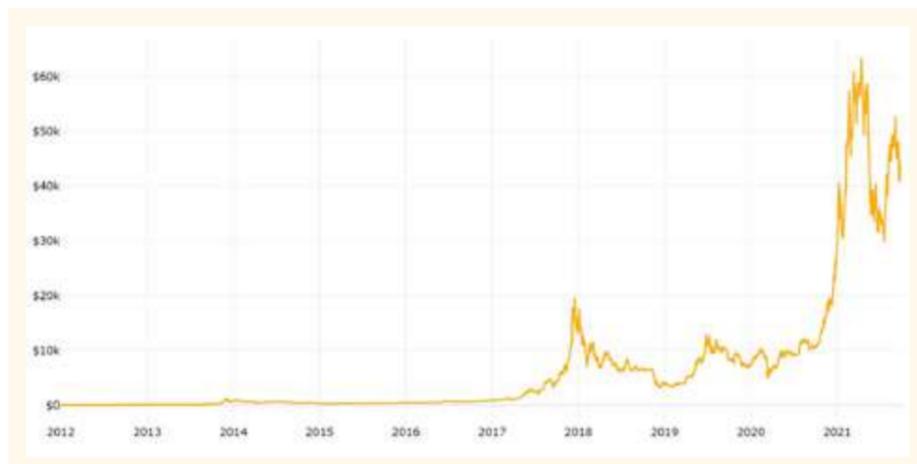
Bitcoin

Durante il Q3 Bitcoin riprende il trend di crescita che lo ha caratterizzato per l'intero 2021 arrivando ad apprezzarsi nell'ordine del 25%. Dopo aver raggiunto un nuovo record storico nel corso del Q2, seguito da un significativo ritracciamento che ha portato il prezzo a toccare i 30mila dollari nella prima parte di questo trimestre, Bitcoin riprende un consolidamento del prezzo che trova equilibrio nell'area di 45mila dollari.



Valore di Bitcoin in USD, terzo trimestre 2021

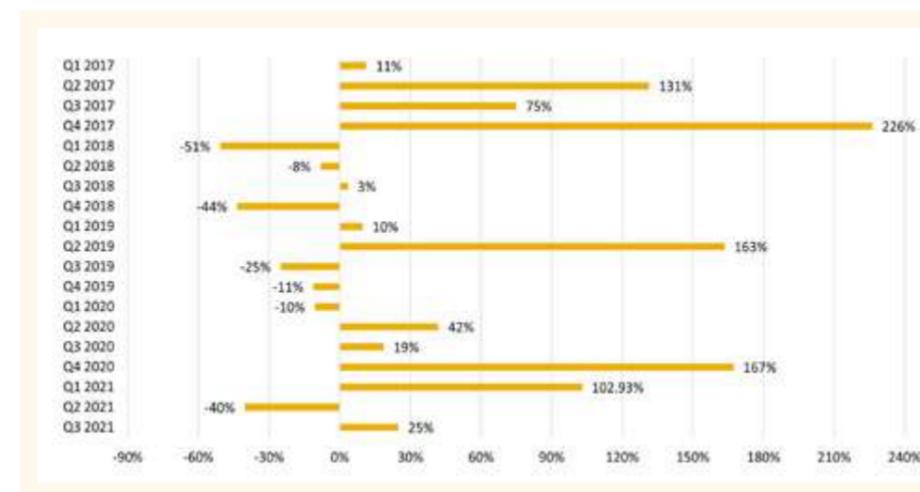
Il consolidamento del prezzo attorno ad un punto di equilibrio ci racconta l'andamento tipico di Bitcoin che si è potuto osservare nel corso di più micro-cicli: bull-run che spingono il prezzo verso nuovi record storici, ritracciamenti e consolidamenti ad un prezzo più alto che preparano la strada a nuovi record storici.



Valore di Bitcoin in USD

Dopo la flessione osservata nel corso del Q2, il trimestre riprende l'apprezzamento in atto da oltre un anno e conferma una maturazione del mercato di Bitcoin,

che pur mantiene un trend di crescita di medio-lungo periodo tipico di un asset sottovalutato. L'ampiezza delle oscillazioni del prezzo si è progressivamente ridotta nel tempo, conseguenza di una adozione istituzionale e di massa; al diminuire delle grandi posizioni concentrate in mano ai retailer (in particolare ai miner dei primi anni) caratterizzati da obiettivi di breve-medio termine e soggetti all'irrazionalità comportamentale di mercato, vedremo un asset sempre più maturo, stabile e con un valore sempre più vicino al suo fair-price.

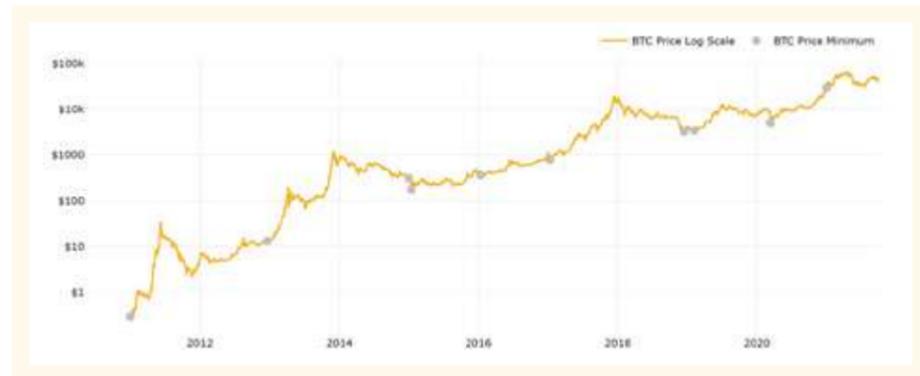


Performance trimestrale di Bitcoin

Guardando alla performance da inizio anno troviamo conferma di quanto detto: l'apprezzamento supera il 50% e il prezzo minimo è rintracciabile nei livelli visti nei primi giorni dell'anno.

DATA	PREZZO	PERFORMANCE ANNUALE	ANNO	PREZZO MIN
31-dic-2011	\$5.00	1,566.67%	2011	\$0.30
31-dic-2012	\$13.59	171.80%	2012	\$13.40
31-dic-2013	\$754.01	4,448.27%	2013	/
31-dic-2014	\$320.19	-58.49%	2014	\$310.74
31-dic-2015	\$430.57	37.02%	2015	\$178.10
31-dic-2016	\$963.74	121.89%	2016	\$364.33
31-dic-2017	\$14,156.40	1,318.01%	2017	\$777.76
31-dic-2018	\$3,742.70	-72.60%	2018	\$3,326.76
31-dic-2019	\$7,193.60	87.16%	2019	\$3,399.47
31-dic-2020	\$28,968.31	302.33%	2020	\$4,970.79
30-set-2021	\$43,799.56	51.20%	2021	\$29,386.28

La trasposizione del prezzo di Bitcoin su scala logaritmica rende possibile visualizzare in maniera più chiara l'andamento positivo nel corso degli anni e la crescita a strappi a cui si fa cenno sopra. L'alternanza di bull-run, ritracciamenti e consolidamenti caratterizza l'intera storia evolutiva di Bitcoin dove i prezzi minimi per anno, particolarmente significativi nel valutare la stabilità di un asset, confermano un trend di apprezzamento pressoché omogeneo.



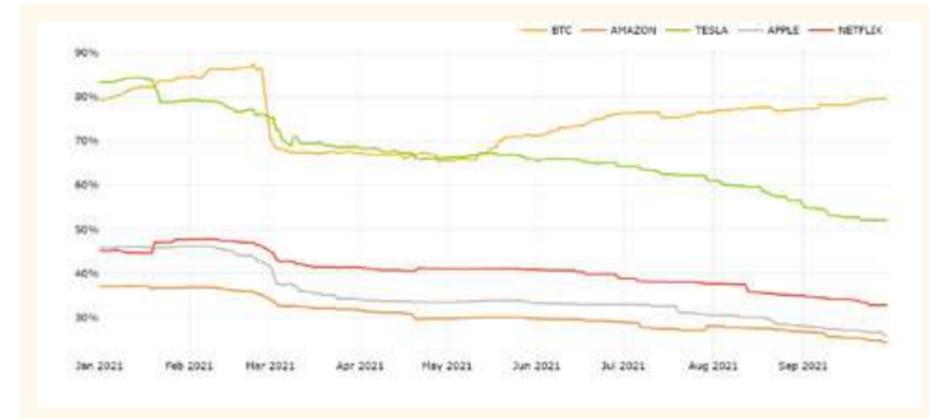
Valore di Bitcoin in USD

Il recente massimo storico a 63mila dollari durante il Q2, ha proiettato Bitcoin ad una dimensione di capitalizzazione di mercato tra le più elevate in assoluto ad oltre 1 trilione di dollari. Nonostante la successiva flessione e consolidamento, raccontati nel corso del Q3, Bitcoin può vantare una capitalizzazione media nel corso del 2021 di circa 660 miliardi di dollari che lo rende uno dei migliori 15 asset per capitalizzazione sul mercato.

DATA	PERFORMANCE ANNUALE
2021	Circa \$660B
2020	Circa \$200B
2019	Circa \$130B

La riduzione delle oscillazioni di prezzo di Bitcoin rispetto al passato viene confermata comparandone la volatilità con quella di asset come Netflix, Apple, Tesla e Amazon: questi asset a grande redditività presentano una volatilità sostanzialmente in linea con quella di Bitcoin.

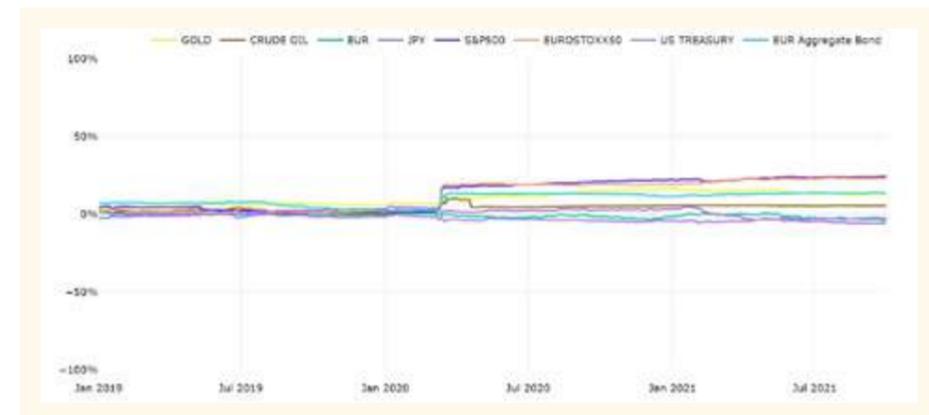
In altre parole, realtà considerate estremamente solide e redditizie remunerano il rischio comparabilmente a Bitcoin ma attestandosi a livelli di performance inferiori.



Volatilità di Amazon, Apple, Bitcoin, Netflix e Tesla su una finestra mobile di 252 giorni

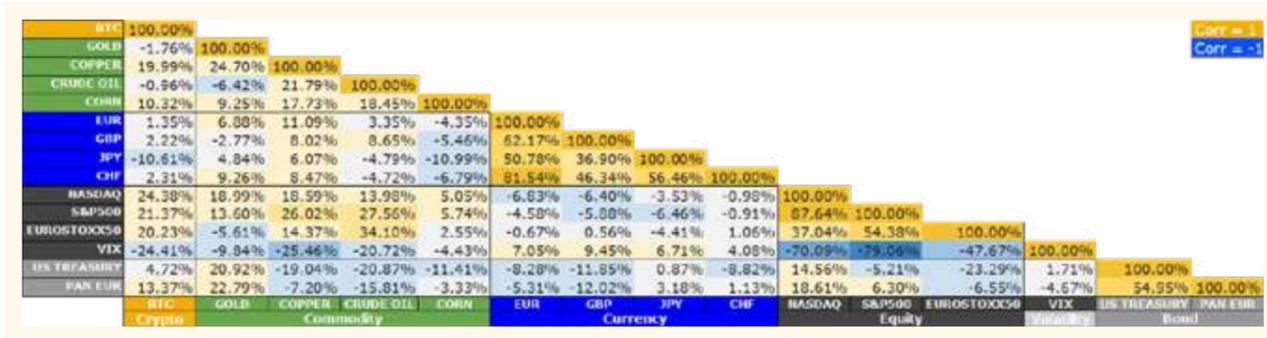
Osservando le correlazioni tra Bitcoin e le altre asset class (commodity, currency, equity, volatility e bond) si desume come Bitcoin sia il rappresentante di una nuova asset class, quella dei crypto-asset, sostanzialmente incorrelata con il resto del mercato.

È interessante analizzare l'andamento nel tempo delle correlazioni tra Bitcoin ed altri asset rappresentativi delle sopra citate asset class. I valori si mantengono stazionari ed intorno allo zero con un incremento in coincidenza dell'ingresso nella finestra di osservazione del 12 marzo 2020, la giornata nera per tutti i mercati finanziari legata alla crisi del Covid-19 (vedi report 2020Q1).



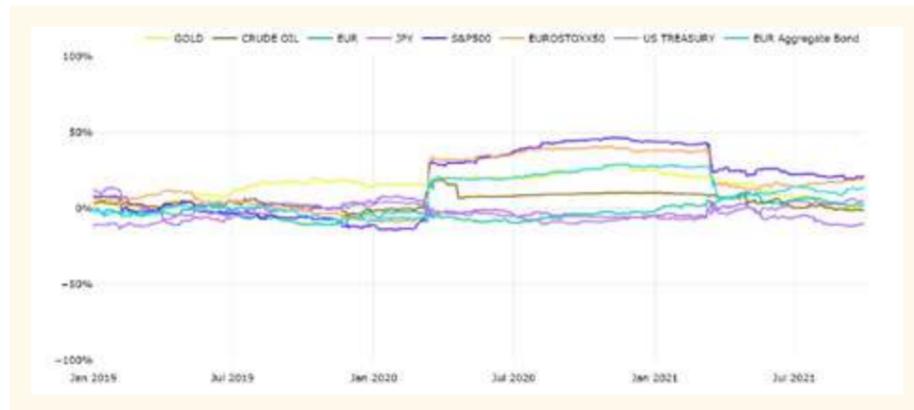
Correlazione delle principali asset class con Bitcoin su una finestra temporale di tre anni

La sostanziale incorrelazione si rende ancor più evidente osservando la matrice di correlazione a tre anni.



Matrice di correlazione, finestra temporale di tre anni

Restringendo la finestra temporale di osservazione si nota come le correlazioni si alzino ma rimangano sempre molto contenute. Considerando l'andamento delle correlazioni nella finestra di un anno è possibile apprezzare l'effetto di uscita dall'intervallo che considerava gli effetti del covid e i valori tornano ad allinearsi ai numeri precedenti.



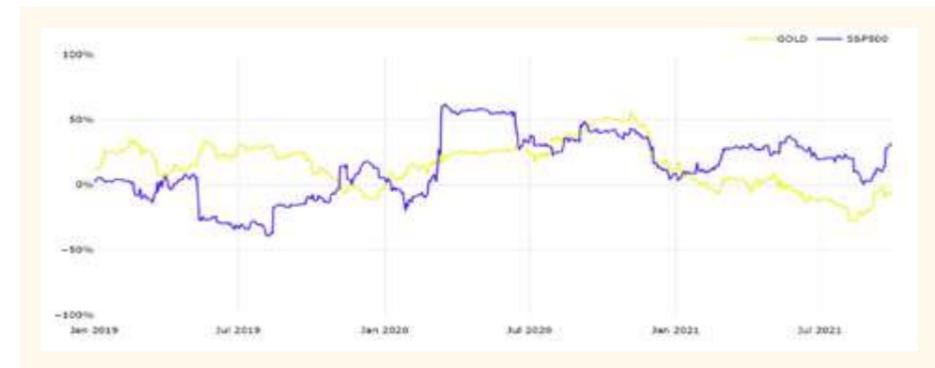
Correlazione delle principali asset class con Bitcoin su una finestra temporale di un anno

Bitcoin dunque, essendo un asset incorrelato con il resto del mercato, si presta in modo efficiente ad essere inserito in qualsiasi portafoglio con obiettivo di diversificazione e conseguente mitigazione del rischio.



Matrice di correlazione, finestra temporale di un anno

La scelta di finestre temporali ampie è cruciale al fine di ottenere una misurazione della correlazione che sia di una certa rilevanza statistica. A conferma di ciò osserviamo il confronto tra le correlazioni di oro e S&P500 con Bitcoin nell'arco temporale di 90 giorni: l'andamento è molto variabile e contraddittorio perché di fatto la correlazione reale è nulla.



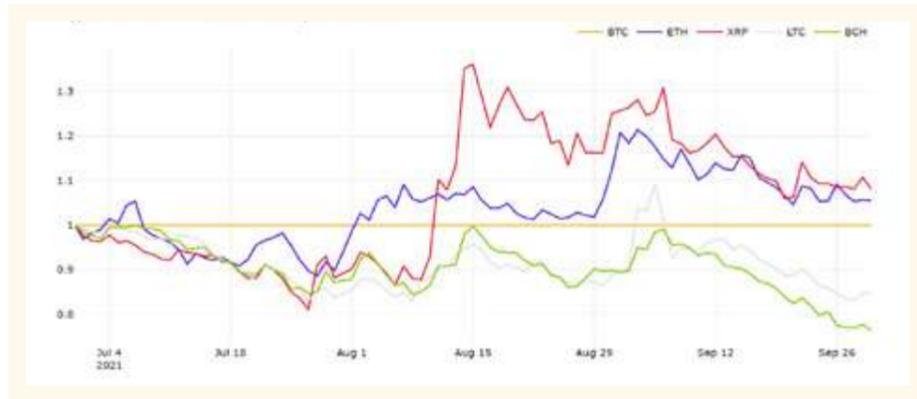
Correlazione degli asset Gold e S&P500 con Bitcoin su una finestra temporale di 90 giorni

Alt-coin

Come di consueto le alt-coin, ossia le criptovalute alternative a Bitcoin, hanno mostrato un andamento assimilabile a quello di Bitcoin ma con oscillazioni maggiori; in generale il trimestre può sintetizzarsi con una ripresa dopo il brusco crollo e progressivo consolidamento.

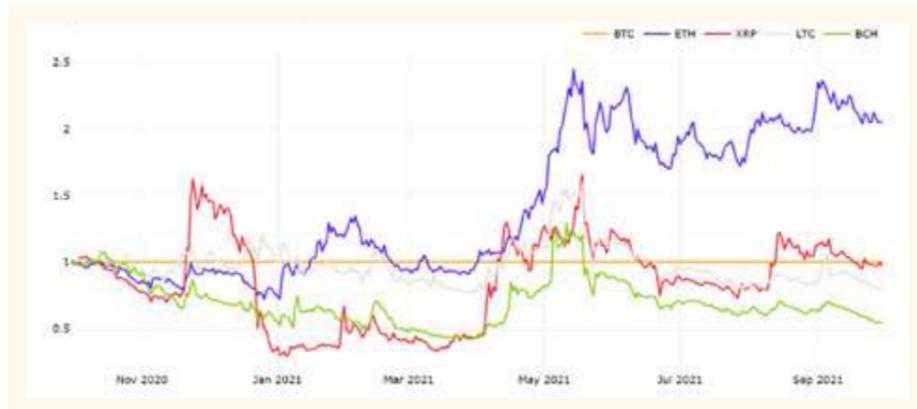
Guardiamo alle performance degli alt-coin, ricordando che queste sono denominate in Bitcoin in quanto qualsiasi investimento in crypto-asset che non sia Bitcoin si pone intrinsecamente come alternativo a Bitcoin e su quel metro va misurato.

Nel corso dell'ultimo trimestre le performance possono dirsi abbastanza simili con Ripple ed Ether che hanno leggermente sovraperformato Bitcoin.



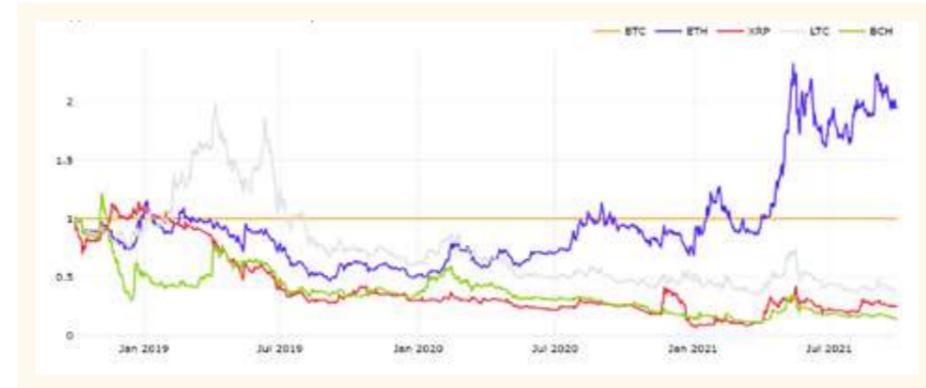
Rendimenti alt-coin denominati in Bitcoin, terzo trimestre 2021

Allargando la finestra temporale all'anno notiamo come la tendenza di Bitcoin a sovraperformare le alt-coin si renda più visibile.



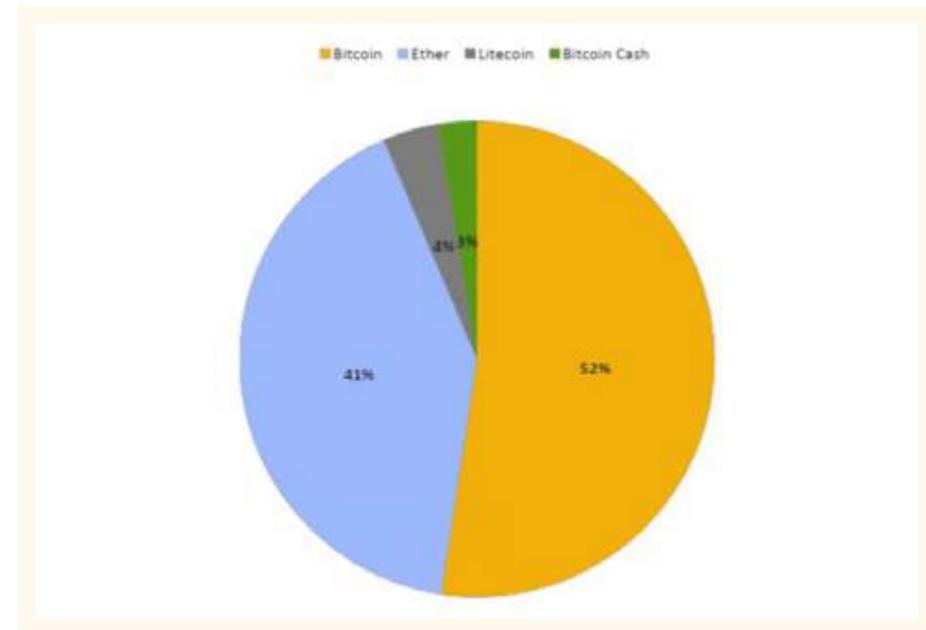
Rendimenti alt-coin denominati in Bitcoin, finestra temporale di un anno

Considerando infine la finestra di tre anni osserviamo una grande overperformance di Bitcoin su quasi tutte le alt-coin.



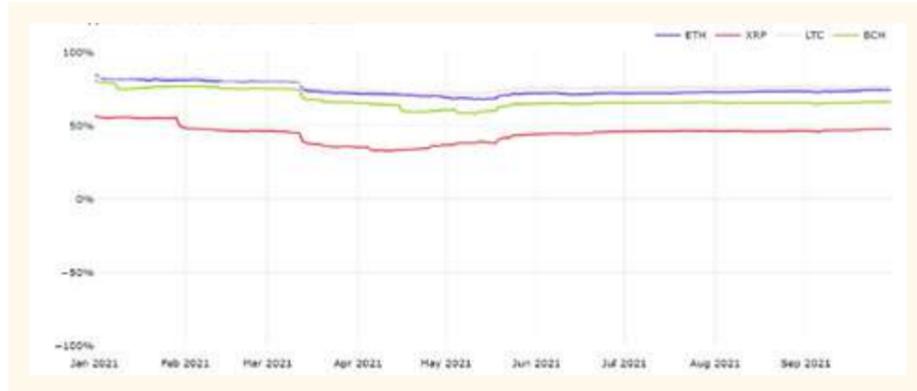
Rendimenti alt-coin denominati in Bitcoin, finestra temporale di tre anni

Ether, nonostante si tratti di un asset meno liquido e meno stabile, rappresenta in questo momento una eccezione e persiste nel sovraperformare Bitcoin anche su orizzonti temporali maggiori del trimestre. Questi risultati influenzano il peso relativo del token della piattaforma Ethereum nella composizione del Crypto-Index sviluppato dal nostro istituto, che si attesta al 41%.



DGI Crypto Index, terzo trimestre 2021

Nel considerare Bitcoin come rappresentativo dell'asset class delle criptovalute si sta commentando un dato incontrovertibile: la correlazione tra Bitcoin e le alt-coin è elevatissima e quindi l'andamento delle alt-coin è spiegabile tramite l'andamento di Bitcoin.



Correlazione ETH, XRP, LTC, BCH con BTC su una finestra temporale di un anno

Nell'ottica di composizione di portafoglio, dove la diversificazione è la chiave per la copertura al rischio, assume poco senso investire in alt-coin la cui correlazione sfiora il 90% e le oscillazioni sono più significative.

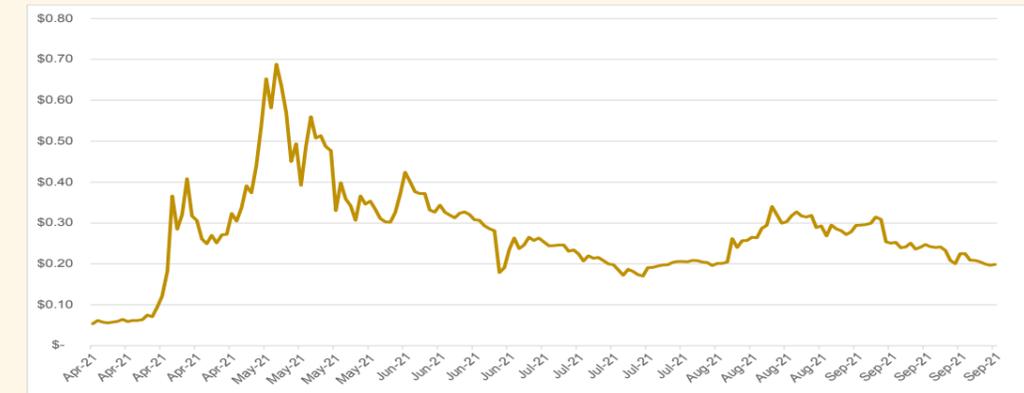
BTC	100.00%			
ETH	71.65%	100.00%		
LTC	79.37%	78.12%	100.00%	
XRP	39.59%	44.08%	51.95%	100.00%
	BTC	ETH	LTC	XRP

Matrice di correlazione, finestra temporale di un anno

BTC	100.00%			
ETH	79.20%	100.00%		
LTC	79.52%	81.38%	100.00%	
XRP	51.66%	58.38%	60.18%	100.00%
	BTC	ETH	LTC	XRP

Matrice di correlazione, finestra temporale di tre anni

DOGECOIN: LA METEORA CHE SI STA SPEGNENDO



Dogecoin, dopo l'euforia di inizio anno, si conferma un fenomeno che si è sostanzialmente sgonfiato.

Facendo un rapido riepilogo, l'inizio del 2021 ha visto una crescita straordinaria nel prezzo di Dogecoin che ha raggiunto vette di 0,70 centesimi di dollaro e performance del 500%. Il token ha subito una grandissima spinta dalla campagna mediatica social messa in atto principalmente da Elon Musk; tuttavia, una volta accantonata dal Ceo di Tesla, ha ceduto terreno chiudendo il Q3 con un valore di 0,20 centesimi di dollaro.

Come già ribadito dal nostro istituto, dogecoin «non si è mai presentato come un esperimento serio, piuttosto come uno scherzo. Potremmo azzardare che Dogecoin è un po' come il LOL del mondo crypto». Sembrano dunque lontanissimi i mesi in cui si voleva far decollare la criptomoneta meme sulla Luna (l'espressione è muskiana).

Futures e opzioni

Le notizie dal mercato dei futures e delle opzioni su Bitcoin mostrano una leggera contrazione a livello di volumi, pur riprendendosi in Agosto e Settembre e spingere verso i picchi del trimestre precedente.



Volumi futures CME Group Inc.



Volumi opzioni CME Group Inc.

CON L'UNICEF,
PER DARE VALORE
AL FUTURO DI TUTTI I BAMBINI.



Da oltre 50 anni investiamo sul futuro.
Per questo abbiamo scelto di essere a fianco dell'UNICEF,
che sostiene le donne e gli uomini di domani.

Un'iniziativa per sostenere
unicef  per ogni bambino



 ECOSISTEMA

El Salvador

La genesi di bitcoin a corso legale

La notizia del trimestre, e già papabile per essere tra le più importanti dell'anno, è senz'altro quella che arriva da El Salvador, dove il 7 settembre è stato il day one per bitcoin come valuta a corso legale. Se ne era già parlato nel Q2, quando il minuscolo paese centroamericano aveva approvato la storica Bitcoin Law, tanto voluta dal presidente Nayib Bukele. Per chi non lo sapesse, El Salvador non ha una sua moneta nazionale e finora ha utilizzato i dollari americani. A prescindere da come la si pensi, il 7 settembre 2021 sarà ricordata come una giornata storica per l'istituzionalizzazione del mercato bitcoin. Se è vero che negli ultimi anni è cresciuta l'attenzione verso l'ecosistema crypto anche nella stampa generalista, l'eco di quanto accaduto ha avuto una risonanza senza precedenti. In questo c'è stato naturalmente ampio spazio anche per le news di colore: da quel giorno, infatti, i cittadini di El Salvador possono fare acquisti in bitcoin anche da McDonald's.

Ne hanno parlato dal Wall Street Journal al Financial Times. Il dibattito, come prevedibile, è stato ricco di spunti, di storie e anche di polemiche. Per molti la scelta di El Salvador rappresenta una possibile soluzione di investimento per i cittadini e un'alternativa alle rimesse in dollari sulle quali pesano le commissioni. Il presidente Bukele ha per l'appunto calcolato che società come Western Union e MoneyGram potrebbero perdere 400 milioni di dollari all'anno in mancate commissioni ora che esiste la strada bitcoin.

Sempre il 7 settembre El Salvador ha concluso l'acquisto di 550 bitcoin complessivi in una giornata cruciale anche per il cosiddetto Flash Crash, col crollo del valore della criptomoneta. Occasione ghiotta per il paese che ne ha approfittato per fare nuove scorte. I commenti entusiasti dalla stampa di settore non si contano: Bitcoin Magazine, ad esempio, ha spiegato che El Salvador sta offrendo ai suoi cittadini – il 70% dei quali senza un conto in banca – la possibilità di possedere la propria banca. Ovviamente la condizione necessaria affinché questo avvenga è una adeguata connessione internet, sulla quale occorrerà investire.

Il day one non è stato privo di qualche inevitabile inciampo: il Chivo Wallet proposto ai cittadini di El Salvador è andato temporaneamente fuori uso, come ha avvisato lo stesso presidente Bukele su Twitter. La notizia ha fornito ovviamente l'assist alla stampa critica – Financial Times in testa – per screditare il nuovo corso. Va però precisato che l'affidabilità tecnologica di questo wallet è garantita, dal momento che è assistita dall'exchange messicana Bitso, il più grande di tutta l'area latinoamericana. Per dare un contesto basti pensare che, tra luglio 2020 e set-



Nayib Bukele



tembre 2021, Bitso ha triplicato da un milione a tre milioni il numero di utenti sulla piattaforma; in più ha assunto Vaughan Smith (ex di Facebook) come COO dopo l'aumento di capitale da 250 milioni di dollari a inizio anno. Ad oggi oltre 2 milioni di cittadini ne stanno utilizzando i servizi. Completa il quadro del Q3 un'ultima notizia che riguarda El Salvador: come ha postato su Twitter il presidente Bukele il paese ha sfruttato per la prima volta l'energia geotermica ricavata dai vulcani per minare bitcoin.



El Salvador potrebbe essere il primo di una serie di paesi pro bitcoin. Ormai il percorso è tracciato: a Panama è stata presentata una proposta di legge per incentivare i pagamenti in bitcoin; segue l'Uruguay, dove il senatore Juan Sartori ha avanzato una soluzione analoga; il quadro sudamericano vede anche Visa esporsi in Brasile con l'idea di aprire ai pagamenti in bitcoin, mentre è il paese stesso a ragionare su una possibile legge. Spostandoci infine dal Sudamerica, compare anche l'Ucraina tra gli Stati che hanno deciso di istituzionalizzare bitcoin con una norma ad hoc che ne regola l'utilizzo.

La chiusura totale della Cina

Non è la prima volta che la Cina mostra i muscoli di fronte al mondo crypto. Di recente il ban del mining da tutto il territorio nazionale aveva senz'altro scosso l'ecosistema, aggiungendosi a una lista di operazioni ostili avviate dal 2009 in poi (secondo la stampa di settore il gigante asiatico ha bandito Bitcoin quasi 20 volte, ma finora senza successo). Quello che però è accaduto al termine del Q3 a Pechino è senza precedenti: la Banca cinese, infatti, ha imposto un ban severo di tutte le transazioni di criptovalute definendole illegali. Le reazioni iniziali hanno fatto pensare a una riedizione delle precedenti puntate, in cui il potere centrale cercava di limitare l'uso di Bitcoin e altcoin senza riuscirvi. Invece, come leggiamo su Bloomberg, il nuovo corso sembra drastico e non si dovrebbe più tornare indietro.

Tra le prime conseguenze di questo giro di vite nei confronti del mondo crypto, analogo a quello che la Cina sta infliggendo in ambito Big Tech (da Alibaba a Didi), i principali exchange hanno iniziato a chiudere le porte alle iscrizioni di nuovi utenti cinesi; nel frattempo l'effetto economico si è fatto sentire con 50 milioni di dollari di liquidazioni di posizioni corte e lunghe. In questa tempesta c'è chi ha comunque cercato di mettere le cose in un'ottica diversa: Pechino, secondo Blockworks, non ha bandito le crypto dal suo territorio, ma ha semplicemente spinto tutti gli exchange a spostarsi fuori dal proprio territorio. Al momento è comunque troppo presto per capire quali saranno gli sviluppi futuri.



El Salvador: la genesi di bitcoin a corso legale

twitter.com/nayibbukele/status/1435120030245662722
 wsj.com/articles/bitcoin-comes-to-el-salvador-first-country-to-adopt-crypto-as-national-currency-11631005200
 ft.com/content/56f1f053-3ac1-424a-97d6-6bbf9a12fa1d
 blockworks.co/el-salvador-bitcoin-wallet-could-disrupt-traditional-remittance-markets
 cnbc.com/2021/09/09/el-salvador-bitcoin-move-could-cost-western-union-400-million-a-year.html
 twitter.com/nayibbukele/status/1435260422110732300
 bitcoinmagazine.com/business/president-bukele-bought-bitcoin-dip-el-salvador
 finance.yahoo.com/news/panama-introducing-legislation-bitcoin-legal-054123035.html
 coindesk.com/markets/2021/08/04/uruguayan-lawmaker-proposes-bill-to-allow-crypto-to-be-used-for-payments
 cointelegraph.com/news/visa-reportedly-aims-to-integrate-bitcoin-payments-in-brazil
 todayuknews.com/crypto-currency-law-project-establishes-period-to-decide-cryptocurrency-regulations-in-brazil-regulation-bitcoin-news
 cnbc.com/2021/09/08/ukraine-legalizes-bitcoin-and-cryptocurrencies.html

La chiusura totale della Cina

cointelegraph.com/news/crypto-has-recovered-from-china-s-fud-nearly-two-dozen-times-in-the-last-12-years
 bloomberg.com/news/articles/2021-10-05/china-s-biggest-crypto-platform-knows-there-s-no-going-home
 time.com/6094156/china-big-tech-regulation-us/
 blockworks.co/crypto-markets-tumble-on-pboc-news/
 blockworks.co/no-china-didnt-ban-crypto-its-just-pushing-exchanges-offshore/

Binance

L'emergere delle lacune regolamentari

Il terzo trimestre ha segnato di nuovo incidenti di percorso per Binance, altro noto exchange globale sotto gli occhi dei regolatori per i suoi comportamenti storicamente arrembanti sul mercato. Queste lacune nei rapporti con le istituzioni e gli attori tradizionali hanno presentato un conto davvero salato per l'azienda fondata da Changpeng Zhao nel 2017. Le montagne russe del trimestre sono partite proprio a inizio luglio, con i clienti in Gran Bretagna che non potevano né prelevare né depositare sterline sulla piattaforma per via di un intervento da parte del regolatore. Il servizio è stato riattivato nel giro di pochi giorni, ma è stato uno dei tanti segnali delle difficoltà che Binance avrebbe continuato a riscontrare nelle settimane successive. A questo si è infatti aggiunto il blocco temporaneo, scelto dall'azienda stessa, dei pagamenti sul circuito SEPA come risposta ai terremoti in corso in diverse giurisdizioni, dall'Europa fino al Giappone e alla Thailandia. Immane, ovviamente, il coro di una fetta della stampa e del potere economico/politico che ha esultato di fronte agli infortuni di un attore del mondo crypto.

La situazione d'emergenza ha richiesto perfino l'intervento del Ceo Zhao, in una lettera aperta sul blog della società: «lo e tutti a Binance siamo pronti e non vediamo l'ora di diventare un partner nello sviluppo e nel seguire le linee guida che aiuteranno l'industria a crescere in modo sostenibile. Insieme aiuteremo ad aumentare la libertà nella società in modo sostenibile e responsabile». Il ramo d'ulivo non è di certo bastato, dal momento che i warning sono arrivati anche dall'Italia: a metà luglio la Consob ha invitato Binance a oscurare alcuni suoi servizi come quello sugli stock token.

Su questi ultimi si è arrivati poi a



Changpeng Zhao

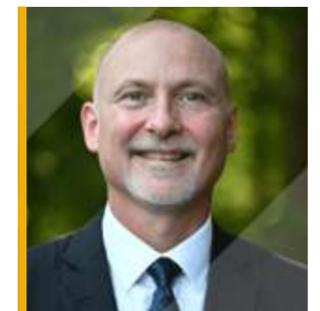


Brian Brooks

una pietra tombale: l'exchange ha dichiarato che non li venderà più dopo che anche Hong Kong aveva alzato le barricate. In sostanza una tempesta perfetta, un tutti contro uno e, in ultima analisi, una perfetta soap opera estiva. In ordine sparso la società è stata presa di mira in Malesia ed è stata poi costretta a chiudere la sua offerta di futures e prodotti derivati in Germania, Italia e Paesi Bassi con effetto immediato a fine luglio. Tutto questo vento contrario non ha comunque convinto Binance a rinunciare ai propri piani. Tra tutti, il più importante, quello di quotarsi in Borsa seguendo l'altro grande esempio del 2021 (ci riferiamo a Coinbase, sbarcata a Wall Street in primavera). Per spianare la strada verso questo obiettivo lo stesso Changpeng Zhao si è detto pronto a rinunciare alla carica di amministratore delegato.

In realtà chi ha rinunciato a un ruolo in Binance è stato Brian Brooks, che ha lasciato il ruolo di Ceo di BinanceUS dopo solo quattro mesi, motivando la scelta per differenze strategiche di fondo con l'azienda. La società lo aveva ingaggiato sperando che il suo curriculum da ex guida del Office of the Comptroller of the Currency avrebbe aiutato l'exchange a proporsi meglio agli interlocutori e al mercato.

Come vi spieghiamo in questo report, le porte girevoli tra il mondo crypto e quello tradizionale sono sempre di più. E infatti Binance non ha smesso di assumere da quel versante: Greg Monahan è stato infatti scelto per le sue esperienze in qualità di US Federal Law Enforcement Investigator. Allo stesso modo Binance.US ha optato per Brian Shroder come presidente per il suo passato in Ant Financial. Quel che è certo è che il Zhao ha ormai compreso l'urgenza di confronti frequenti con i regolatori dato che, soltanto per citare il caso britannico, la borsa è stata giudicata incapace di essere regolamentata. Dando, ca va sans dire, la stura alle critiche della stampa avversa a questo mondo, convinta che il caso Binance dimostri l'inaffidabilità in toto di questo ecosistema.



Greg Monahan



Brian Shroder

Binance: l'emergere delle lacune regolamentari 1/2

coindesk.com/markets/2021/07/06/binance-temporarily-stops-payments-from-eus-sepa-platform-report
ft.com/content/35c541b7-0387-4297-8319-4fee51f01693
binance.com/en/blog/421499824684902301/leadership/a-letter-from-our-ceo-reflecting-on-progress-and-the-road-ahead
www.consob.it/web/consob/dettaglio-news/-/asset_publisher/hZ774IBO5XPe/content/avviso-a-tutela-dei-risparmiatori-sul-grup-po-binance-15-luglio-2021-10194
theblockcrypto.com/post/111661/binance-ceases-stock-tokens-trading
reuters.com/business/finance/hong-kong-watchdog-says-binance-not-licensed-sell-stock-tokens-city-2021-07-16
sc.com.my/resources/media/media-release/sc-takes-enforcement-actions-on-binance-for-illegally-operating-in-malaysia
binance.com/en/support/announcement/f72d0ff2bd24b488213fa30284dd4cd
decrypt.co/76756/binance-us-coinbase-playbook-go-public-ipo-ceo-cz
twitter.com/BrianBrooksUS/status/1423727097323802626

Binance: l'emergere delle lacune regolamentari 2/2

newswire.ca/news-releases/binance-hires-former-us-federal-law-enforcement-investigator-greg-monahan-as-global-money-laundering-reporting-officer-837315495
blockworks.co/binance-us-taps-former-ant-financial-uber-executive-brian-shroder-as-president
theblockcrypto.com/linkedin/117855/binance-shift-away-decentralized-headquarters-pitch

La guerra per i talenti

È bastato che uno dei tanti annunci di lavoro di Amazon rimbalzasse sul web per generare un rally su Bitcoin. Quest'estate il gigante dell'e-commerce era alla ricerca di un Digital Currency and Blockchain Product Lead da inserire nel proprio team al quartier generale di Seattle. Le competenze richieste includevano una profonda conoscenza dell'ecosistema crypto. Anche la stampa non specializzata si è fondata sulla notizia che, ai più, ha suggerito un'imminente possibilità per i clienti Amazon di pagare in Bitcoin. Nulla di tutto questo, per ora, ma è comunque indicativo di quanta attenzione ruoti attorno ai Big Tech, mesi dopo l'investimento da 1,5 miliardi di dollari di Tesla in Bitcoin (è la seconda società che ne possiede di più al mondo dopo MicroStrategy).

Walmart, competitor diretto di Amazon e una delle più note catene della GDO a livello globale, sta da tempo cavalcando il trend dell'e-commerce anche per contrastare il dominio del gigante fondato da Jeff Bezos (da pochi mesi il nuovo Ceo è Andy Jassy). E, guarda caso, per farlo l'azienda sembrerebbe aver bisogno anch'essa di un "Digital Currency and Cryptocurrency product lead": l'annuncio pubblicato su LinkedIn non ha però sorpreso la stampa che segue gli affari tecnologici Oltreoceano. Si dà quasi per scontato un futuro ingresso di questi giganti nel campo Bitcoin.

Ma non ci sono soltanto le multinazionali a interessarsi di Bitcoin. Senz'altro con minor eco sulla stampa, del trimestre va segnalato un altro fatto. Ossia, è anche il mondo tradizionale a richiedere sempre più competenze

dai talenti che si sono fatti le ossa nell'ecosistema crypto. Ecco allora che, a metà agosto, il New York State Center for Recruitment & Public Service ha pubblicato su LinkedIn l'annuncio per reclutare un Deputy Superintendent for Virtual Currency da inserire nel New York The Department of Financial Services. A dimostrazione che regolatori e istituzioni più lungimiranti hanno ormai compreso l'urgenza di rientrare nell'ecosistema e non esserne invece tagliati fuori.

Se però il mondo tradizionale guarda a quello crypto, si può dire anche viceversa. Uno dei casi che avrebbero potuto fare scuola è quello di Brian Brooks, divenuto Ceo di Binance.US in aprile, il quale ha poi scelto di dimettersi in agosto per via di "differenze strategiche" non meglio specificate. La notizia di una separazione così repentina può lasciare intendere che tra l'exchange e Brooks i rapporti non siano mai decollati a causa di visioni diverse sulla finanza e sulla regolamentazione. Vale comunque la pena di sottolineare il fatto che Binance, società rampante e per alcuni corsara del mondo crypto, aveva visto proprio in Brooks, ex guida dell'Office of the Comptroller of the Currency (OCC) durante la presidenza di Donald Trump, una figura istituzionale e autorevole per migliorare la propria reputazione sul mercato.





La guerra per i talenti

amazon.jobs/en/jobs/1644513/digital-currency-and-blockchain-product-lead
 bloomberg.com/news/articles/2021-08-16/walmart-seeks-a-crypto-expert-to-oversee-digital-currency-push
 theverge.com/2021/8/16/22627111/walmart-cryptocurrency-payments-hire-amazon
 linkedin.com/jobs/view/deputy-superintendent-for-virtual-currency-at-new-york-state-center-for-recruitment-public-service-2630943109

Ransomware

Strategie cybercriminali ed effetti

«Potremmo dire che tutti gli attacchi ransomware hanno molte somiglianze fra loro. Ma come poi le vittime reagiscono è quello che fa la differenza». Per inquadrare la questione cybersecurity nel terzo trimestre 2021 ci siamo fatti aiutare



Carola Frediani

da Carola Frediani, esperta del settore. In Italia ha fatto scalpore la notizia dell'attacco alla Regione Lazio in agosto, ma le casistiche potrebbero riempire pagine e pagine di giornali e siti. Negli Stati Uniti, nel frattempo, il Presidente Joe Biden ha convocato i principali Ceo di multinazionali come Apple e Microsoft per affrontare l'emergenza. «Come ha detto lo stesso presidente Biden – ci ha spiegato Frediani – “gran parte delle nostre infrastrutture critiche sono controllate e gestite dal settore privato. E il governo federale non può affrontare da solo la sfida della cybersicurezza”. Lo abbiamo visto col recente caso dell'attacco

“
 Il governo federale non può affrontare da solo la sfida della cybersicurezza.
 Joe Biden

ransomware a Colonial Pipeline ma anche con una serie di attacchi supply chain che hanno colpito fornitori di servizi IT e grosse aziende tech negli ultimi mesi. Di qui la necessità di aumentare la collaborazione e la condivisione di informazioni, visto che l'amministrazione Usa ha deciso di dare una svolta al contrasto al cybercrime ma anche alla difesa delle proprie infrastrutture».

Per inquadrare il fenomeno abbiamo chiesto a Carola Frediani se c'è un modo per quantificare gli attacchi messi in atto negli ultimi tempi. «Non esistono dati esaustivi ed affidabili – ha risposto – Abbiamo dati parziali che arrivano da alcuni enti. Come ho scritto anche nella mia newsletter Guerre di Rete, durante il 2020, rispetto all'anno precedente, il valore dei pagamenti di riscatti sarebbe aumentato del 341 per cento fino a un totale di 412 milioni di dollari, secondo la società di analisi della blockchain Chainalysis. Mentre secondo l'Fbi il volume totale di somme pagate in ransomware sarebbe triplicato nell'ultimo anno. In generale, abbiamo visto anche la crescita della doppia estorsione: oltre a cifrare i dati c'è la minaccia di pubblicarli».

Con il caso della Regione Lazio si è tornati poi a prendere di mira Bitcoin, suggerendo quanto segue: se i criminali usano Bitcoin allora significa che bisognerebbe limitarne l'utilizzo. «I Bitcoin sono una delle innovazioni tecnologiche usate dai cybercriminali, che sono degli innovatori ed early adopter per natura. Il punto – ha argomentato Carola Frediani – non è dare la colpa a una tecnologia specifica, ma capire come funziona e prospera tutto l'ecosistema criminale per poi andare a togliergli terreno sotto i piedi sfruttando le sue vulnerabilità».

Dal momento che non è facile prevedere gli attacchi, ma è probabile che ci sia una impreparazione da parte di PMI e aziende, cosa è possibile fare per reagire? «Penso che questa esplosione di ransomware potrebbe aver raggiunto il suo cli-

Ransomware: strategie cybercriminali ed effetti

startuptitalia.eu/160431-20210802-ransomware-che-sta-succedendo-alla-regione-lazio-intervista-allesperto

max. Di sicuro alcuni settori e nazioni reagiranno per alzare le difese. Sarà interessante capire allora come evolveranno le strategie cybercriminali e se questo non comporterà la ricerca di nuovi target in settori e nazioni meno pronte. In questo

senso, questo non è il momento per rimanere indietro. A livello nazionale e sociale, penso che sia importante una educazione alla complessità del digitale, che includa anche la sicurezza. Ma ci deve essere in primo luogo un investimento e un impegno da parte dei vertici istituzionali e da parte dell'industria».



Poly Network Hack

L'importanza della sicurezza informatica

Tra gli attacchi informatici registrati nel trimestre appena concluso, quello subito dalla piattaforma Poli Network è uno dei più imponenti della storia recente. La piattaforma che consente di scambiare token su diverse smart chain, si è vista soffiare 610 milioni di dollari a causa di un bug del sistema di cui ha approfittato un anonimo esperto. La reazione immediata è stata quella di riconoscere la gravità della situazione e promettere una ricompensa da mezzo milione di dollari a chiunque avrebbe risolto la situazione, somma che – si è saputo in seguito – Poly Network sarebbe stata disposta a cedere anche all'hacker stesso in caso di ravvedimento. La storia, in realtà, ha avuto un lieto fine come spesso accade.

L'artefice di questo attacco ha iniziato a restituire la somma sottratta, fino all'ultimo centesimo. Gli asset rubati comprendevano Dogecoin, Ethereum e tokens di Binance. Questa operazione ha fruttato senz'altro visibilità all'hacker, al quale Poly Network ha subito offerto l'opportunità di diventare chief security advisor della società.

Anche la stampa non specializzata si è occupata della vicenda, definendola una delle storie più bizzarre del mondo crypto. Immane il riferimento a Bitcoin, con i soliti dubbi e insinuazioni sulla sua presunta insicurezza per chi vi investe. La differenza però è marchiana: nel caso di Poly Network si era di fronte a un codice scritto in maniera non adeguata e a palesi lacune nella sicurezza. Ad essere sul banco degli imputati, in realtà, è proprio quest'ultima e l'intero ecosistema della cosiddetta Decentralized Finance.



Poly Network Hack: l'importanza della sicurezza informatica

reuters.com/technology/crypto-platform-poly-network-rewards-hacker-with-500000-bug-bounty-2021-08-13
theverge.com/2021/8/23/22638087/poly-network-600-million-stolen-crypto-hack-restored-defi
cnbc.com/2021/08/23/poly-network-hacker-returns-remaining-cryptocurrency.html
blockworks.co/poly-network-offers-chief-security-officer-role-to-hacker-that-stole-600m
futurumresearch.com/research-notes/what-does-the-poly-network-hack-mean-for-defi

Non-fungible token

Un mercato miope

Tra gli aspetti più pop che stiamo seguendo nei report trimestrali c'è anche quello che riguarda gli NFT, i cosiddetti non-fungible token. Il terzo trimestre ha segnato altre acquisizioni notevoli come quella, ad esempio, di VISA che, in agosto, ha speso 150mila dollari per l'NFT di uno dei migliaia (sono 3840 quelli realizzati) di CryptoPunks. Si tratta del numero 7610. Del trend si è iniziato a parlare soprattutto nei primi mesi del 2021, a seguito dell'asta da quasi 70 milioni di dollari con i quali un collezionista si è aggiudicato questa



Cuy Sheffield

sorta di certificato di un'opera digitale dell'artista americano Beeple. Da allora il mercato ha registrato un'impennata. «Pensiamo che CryptoPunks sia una grande aggiunta alla nostra collezione che può tracciare e celebrare il passato, il presente e il futuro del commercio», ha detto Cuy Sheffield di VISA a The Block.

Come si spiega questo successo degli NFT? Su TechCrunch se ne motiva la crescita con il boom del mondo crypto, Bitcoin in testa, da oltre un anno. Questo ha spinto i più ricchi a investire parte del proprio portafoglio crypto in un'attività per diversificare. Ci potrebbe anche essere la cosiddetta FOMO, Fear Of Missing Out, che starebbe spingendo un sacco di soggetti, anche aziende, a buttarsi nel settore per paura altrimenti di perdere una gran-

de occasione. In settembre proprio la serie CryptoPunks ha superato il miliardo di dollari di vendite tramite NFT. Nella partita ci sono anche attori crypto come Binance che, nonostante una situazione non proprio rosea da diversi mesi a questa parte, ha scelto di lanciare una collezione di non-fungible token insieme al The State Hermitage Museum di San Pietroburgo, uno dei musei più grandi al mondo. Per i numeri più aggiornati bisogna poi guardare a OpenSea, il più grande marketplace di NFT, dove è stato raggiunto il target di 3 miliardi di dollari mensili di volume di scambio sulla piattaforma. Nella partita NFT si è inserita anche Ripple, che ha annunciato il lancio di un fondo da 250 milioni di dollari per i creatori. Nel Q3 segnaliamo anche un'asta a fine settembre di Christie's per una collezione di NFT venduta a 12 milioni di dollari.



In questo mare magnum è inevitabile il rischio frodi. Come ha riportato il Guardian a inizio settembre, un collezionista è stato gabbato in quella che, ai suoi occhi,

sembrava una sicura asta online per aggiudicarsi l'NFT di un'opera di Banksy, forse lo street artist più famoso al mondo. La sua offerta di 244mila sterline è però finita nelle mani di un hacker, fortunatamente dalle buone intenzioni. Alla fine, infatti, la vittima è riuscita a riottenere l'intera somma tranne le 5mila sterline necessarie per la tassa di transazione. «Dopo questo incidente – le sue parole – ho perso fiducia negli NFT». Della questione

cybersecurity e NFT si è occupato anche il Wall Street Journal, spiegando come la preoccupazione sia anche degli stessi artisti che notano la presenza di NFT fake che puntano alle proprie opere.



NFT: un mercato miope

larvalabs.com/cryptopunks/details/7610
theblockcrypto.com/post/115333/visa-buys-cryptopunk-first-steps-nft-commerce
techcrunch.com/2021/08/28/cryptopunks-blast-past-1-billion-in-lifetime-sales-as-nft-market-goes-wild
binance.com/en/support/announcement/2bebd933495c4fe6aac535a5b2f27bf8
decrypt.co/79698/ethereum-nft-cryptopunks-hit-1-billion-in-total-sales
blockworks.co/opensea-hits-3b-in-monthly-nft-volume
theguardian.com/technology/2021/sep/01/collector-buys-fake-banksy-nft-for-244000
wsj.com/articles/scammers-see-new-frontier-in-nft-art-11629896400



IMI

CORPORATE &
INVESTMENT
BANKING

REGOLAZIONE

Vogliamo accompagnare le aziende, le istituzioni finanziarie e gli enti pubblici verso un futuro dove crescita, sostenibilità, internazionalizzazione e innovazione siano legate in maniera indissolubile. Per questo, giorno per giorno, costruiamo per i nostri clienti un futuro da protagonisti nel mercato globale dove ognuno sia in grado di esprimere il proprio potenziale.

imi.intesasanpaolo.com

Central Bank Digital Currency

Sperimentazioni in Europa e nel mondo



In questo trimestre le notizie più rilevanti per quanto riguarda la Central Bank Digital Currency (CBDC) arrivano dalla zona euro. È infatti stato avviato un test sul digital euro, con la Banca Centrale Europea interessata a sondare l'utilità di questo strumento: l'iniziativa durerà 24 mesi, tempo utile per affrontare "questioni chiave riguardanti la progettazione e la distribuzione" di una novità simile. «Il nostro lavoro mira a garantire che nell'era digitale i cittadini e le imprese continuino ad avere accesso alla forma più sicura di denaro, il denaro della banca centrale», ha dichiarato la presidente della BCE Christine Lagarde. Pur essendo sostanziali le differenze tra Bitcoin e le stablecoin, i promotori dell'euro digitale hanno comunque voluto precisare un aspetto: la CBDC sarà sostenibile dal punto di vista ambientale. Un modo neanche troppo velato per attaccare le mining farm dipinte mai come in questo trimestre come attività inquinanti?

Tralasciando le polemiche vale comunque la pena riprendere alcune dichiarazioni di Fabio Panetta, membro del Comitato esecutivo della Banca Centrale Europea, che ha descritto il progetto in cantiere a Francoforte. «I pagamenti digitali sono usati soprattutto dai consumatori con redditi più alti; mentre la preferenza per il contante è più alta tra quelli con redditi bassi, riflettendo il ruolo essenziale di quest'ultimo per l'inclusione finanziaria». Ecco perché, spiega Panetta, «in ogni caso un euro digitale completerebbe il contante, non lo sostituirebbe». Lasciano tuttavia perplessi le tempistiche: la nascita di questa CBDC richiederebbe almeno tre anni dal termine di questa sperimentazione di 24 mesi: dunque l'euro digitale non arriverà prima di un lustro. Nel frattempo sono diversi gli istituti che hanno avviato sperimentazioni di CBDC in Europa e nel mondo: a metà luglio la Banca di Francia ha reso noto il successo ottenuto da un test condotto insieme a diversi soggetti come BNP Paribas Securities Services e Crédit Agricole Titres.

“
Un euro digitale completerebbe il contante, non lo sostituirebbe.
Fabio Panetta
”

US Infrastructure Bill

Svolta normativa in USA

Una delle notizie che ha dominato il dibattito sui crypto asset negli Stati Uniti è stata quella riguardante l'Infrastructure bill, pacchetto monstre da 3,5 trilioni di dollari così suddiviso: 1,2 da investire su infrastrutture come strade, ponti, etc; 2,5 da indirizzare invece su ciò che la stampa USA ha definito "cose che non hanno niente a che vedere" con le infrastrutture.

CBDC: sperimentazioni in Europa e nel mondo

blockworks.co/european-central-bank-launches-24-month-investigation-into-digital-euro
www.ecb.europa.eu/press/blog/date/2021/html/ecb.blog210714~6bfc156386.en.html
www.banque-france.fr/en/communiqué-de-presse/banque-de-france-conducts-successful-experiment-use-central-bank-digital-money-consortium-actors

Si tratta di un banco di prova decisivo per la presidenza Biden, ma concentriamoci sui temi Bitcoin e mondo crypto. Gli obiettivi del legislatore sono stati molteplici: contrastare il crimine, l'evasione fiscale, introdurre la regolamentazione delle stablecoin e di veicoli di investimento (come gli ETF). Alla fine dei conti, però, il Wall Street Journal ha raccolto le opinioni degli scettici, secondo i quali l'Infrastructure bill potrebbe ottenere l'effetto contrario, ossia quello di favorire le operazioni criminali e rallentare l'innovazione Oltreoceano.



Elizabeth Warren

Il caso di Binance nel trimestre corrente è la dimostrazione di quanto l'ecosistema comprenda l'esigenza di una regolazione complessiva. Sono diversi gli attori che operano con Bitcoin a richiedere tavoli di incontro con la politica e i regolatori; d'altra parte il legislatore non sempre è ricettivo e ragionevole. La senatrice Elizabeth Warren, per esempio, ha scritto al Segretario al Tesoro Janet Yellen per avvertirla

dei timori sul mondo criptoalute. Mentre la Cina ha chiuso le porte al mining, con uno schiaffo in faccia ad aziende costrette a fare i bagagli, gli Stati Uniti non sembrano aver colto la palla al balzo per facilitare la crescita dell'ecosistema. Questo perché le ricette spesso proposte suggeriscono di calare le regole della finanza tradizionale sul mondo crypto.

Fatto sta che l'infrastructure bill è passato con il voto al Senato. In agosto non è invece stato approvato l'emendamento bipartisan – bloccato da un senatore – che avrebbe consentito a sviluppatori di software, operatori e validatori di non riportare le informazioni

“
Le criptoalute fanno parte dell'infrastruttura statunitense.
”

sulle transazioni. Secondo la stampa USA il pacchetto collegato alle criptoalute rimane ancora controverso e problematico, ma non si può ignorare un importante fatto politico, riassunto così dalla CNN: le criptoalute fanno parte dell'infrastruttura statunitense. Giusto per dare un quadro, sempre secondo l'emittente USA il 6% della popolazione adulta statunitense con almeno 10mila dollari investiti possiede anche Bitcoin.

Stando a un osservatore attento come Jimmy Song, «quattro anni fa gli investitori Bitcoin rappresentavano il 2% della classe di investitori, oggi siamo al 6%. Dato che crescerà. Alcuni stimano che sarebbero 40 milioni i Bitcoiners negli Stati Uniti e sono soprattutto elettori giovani. Per i politici che guardano al futuro – suggerisce Song - ha senso prestarci attenzione».



Janet Yellen

US Infrastructure Bill: svolta normativa in USA

thehill.com/opinion/white-house/572176-if-35-trillion-infrastructure-bill-fails-its-bye-bye-for-an-increasingly
mondaq.com/unitedstates/fin-tech/1111802/the-us-infrastructure-bill-and-cryptocurrency-regulation
wsj.com/articles/infrastructure-bills-cryptocurrency-measures-risk-pushing-criminals-further-underground-11629883800
cnbc.com/2021/07/27/elizabeth-warren-presses-yellen-financial-regulator-to-manage-crypto.html
coindesk.com/policy/2021/08/09/lone-senator-rejects-crypto-compromise-in-infrastructure-bill
theverge.com/2021/8/25/22641375/cryptocurrency-infrastructure-irs-tax-developers-miners-bitcoin
wsj.com/articles/a-bipartisan-cryptocurrency-crackup-senate-infrastructure-bill-11628626924
edition.cnn.com/2021/08/09/politics/cryptocurrency-infrastructure-deal-lummi-toomey

U.S. Securities and Exchange Commission

La vigilanza attiva sull'ecosistema

«In questo momento non abbiamo abbastanza protezione per gli investitori nelle criptovalute. Francamente è come il selvaggio West. In molti casi gli investitori non sono in grado di ottenere informazioni rigorose, equilibrate e complete». Queste alcune delle parole di Gary Gensler, chairman della SEC (ovvero la Consob americana), riprese dal suo speech di fronte alla platea dell'Aspen Security Forum a inizio agosto. In un video pubblicato su Twitter, Gensler ha ribadito che la SEC è neutrale dal punto di vista della tecnologia, ma esige una tutela dell'investitore. Sono diversi, a dire il vero, i soggetti che richiedono una regolamentazione complessiva che tuteli l'investimento in Bitcoin, e non lo criminalizzi.



Gary Gensler

Tra i politici più allarmati sul fronte crypto troviamo la senatrice dem Elizabeth Warren, che ancora in questo semestre si è espressa sui rischi dell'ecosistema. In risposta a una sua lettera indirizzata alla SEC, Gensler ha spiegato che occorrerebbe senz'altro maggiore presenza delle autorità «per evitare che transazioni, prodotti e piattaforme cadano tra le crepe normative». L'attivismo del chairman è proseguito in estate con l'intervento a gamba tesa sul mondo della Decentralized Finance: Gensler ha avvertito gli attori della DeFi, dicendo che la SEC è vigile su tutto quanto accade in questo ecosistema. Per il Financial Times tale presa di posizione è necessaria dal momento che il mondo crypto avrebbe bisogno di «un buono sceriffo».

Il numero uno della Securities and Exchange Commission ha ribadito la propria posizione anche di fronte al Parlamento Europeo a settembre. «Non c'è nessun intermediario tra il pubblico e la piattaforma – ha detto riferendosi al mondo DeFi – Pertanto, in assenza di un chiaro obbligo di protezione degli investitori, il pubblico che investe è vulnerabile». Nella sua visione, la regolamentazione andrebbe a beneficio dello stesso mondo crypto.

Il numero uno della Securities and Exchange Commission ha ribadito la propria posizione anche di fronte al Parlamento Europeo a settembre. «Non c'è nessun intermediario tra il pubblico e la piattaforma – ha detto riferendosi al mondo DeFi – Pertanto, in assenza di un chiaro obbligo di protezione degli investitori, il pubblico che investe è vulnerabile». Nella sua visione, la regolamentazione andrebbe a beneficio dello stesso mondo crypto.

Coinbase

Il servizio Lend al vaglio della SEC

Dopo la quotazione nel primo trimestre 2021, è tempo di bilanci e di confronti sul piano regolamentario per Coinbase, il primo exchange al mondo ad essere sbarcato a Wall Street. Anzitutto le performance: ad agosto è stata pubblicata la prima lettera indirizzata agli azionisti della società californiana, dalla quale sono emersi dati che nemmeno gli analisti avevano previsto: le entrate di Coinbase, complice anche un entusiasmo generale nel mondo crypto, sono aumentate di oltre il 1000% per cento su base annua nel secondo trimestre del 2021.

SEC: la vigilanza attiva sull'ecosistema

sec.gov/news/public-statement/gensler-aspens-security-forum-2021-08-03
twitter.com/GaryGensler/status/1422607603708870663
theblockcrypto.com/linked/114222/gensler-asks-sen-warren-for-more-sec-authority-to-regulate-crypto-exchanges
coindesk.com/markets/2021/08/19/defi-not-immune-to-sec-oversight-gensler-says-report
ft.com/content/2b9cad9-5c72-4c38-bfda-59a8a2153b41
coindesk.com/policy/2021/09/01/sec-chair-gensler-lays-out-crypto-regulation-stance-to-european-parliament

La notizia è stata riportata anche dal Financial Times, dove leggiamo che il Ceo di Coinbase, Brian Armstrong, ha definito in questi termini gli obiettivi dell'azienda: «Vogliamo davvero essere l'Amazon degli asset», le sue parole in un incontro con gli investitori.

L'estate per Coinbase si è però chiusa con la SEC, la Consob americana che regola i mercati, impegnata a fare luce su Lend, servizio annunciato da tempo dalla società che offrirebbe a chiunque dovesse depositare dollari sulla piattaforma un interesse di circa il 4%. La Securities and Exchange Commission ha subito minacciato di fare causa alla società: secondo infatti la SEC il programma si configurerebbe come una security e, come tale, deve essere registrato dal Governo. Il lancio di Lend è stato dunque rimandato almeno a ottobre, dal momento che ogni decisione della SEC va rispettata. La reazione da parte di Coinbase non si è però fatta attendere: in un lungo thread su Twitter il Ceo di Coinbase ha dato la propria versione dei fatti, spiegando quanto il servizio bocciato dalla SEC sia in realtà già diffuso e offerto da altri soggetti del mercato non quotati.

“
Vogliamo davvero essere
l'Amazon degli asset.
Brian Armstrong
”



Spesso si ha l'idea di un ecosistema crypto arrembante e poco incline al rispetto delle regole: in questo caso va però fatto notare che Coinbase ha seguito la procedura, anticipando le proprie mosse alle SEC, dalla quale però ha ricevuto una sbrigativa risposta negativa senza ottenere troppe motivazioni nel merito.

Riferendosi esplicitamente a Gary Gensler, numero uno dell'organo regolatore USA, Brian Armstrong ha dichiarato quanto segue: «Se non volete questa attività, allora pubblicate semplicemente la vostra posizione, per iscritto, e fatela rispettare in modo uniforme in tutto il settore». Naturalmente anche la stampa specializzata ha seguito la vicenda: Blockworks ha sottolineato quanto l'exchange californiano sia stato uno dei pochi ad aver richiesto l'approvazione della SEC prima del lancio di Lend. La notizia va infine inquadrata in un lungo dibattito sulle esigenze di regolamentazione del settore, che richiede l'impegno di entrambe le parti, organi istituzionali compresi. Il timore degli osservatori è infatti che la «litigation» diventi la formula di confronto della Securities and Exchange Commission.



Coinbase: il servizio Lend al vaglio della SEC

s27.q4cdn.com/397450999/files/doc_financials/2021/q2/Coinbase-Q221-Shareholder-Letter.pdf
ft.com/content/b4daff21-6ce6-4854-a499-dc3394859708
washingtonpost.com/business/2021/09/08/coinbase-sec-wells-notice
twitter.com/brian_armstrong/status/1435439291715358721
blockworks.co/the-sec-will-sue-coinbase-if-it-launches-lend
finance.yahoo.com/news/why-the-sec-cracking-down-on-coinbase-could-level-the-crypto-playing-field-105128348.html



FinTech Talks 2021 | 6th edition

Discover the future of FinTech
and the new ideas in the FSI world

**WATCH THE EVENT
ON VIMEO**



Bitcoin

Aggiornamento al protocollo

Il 13 settembre 2021 ha segnato il rilascio ufficiale di Bitcoin Core 22.0, la ventiduesima release del client software originale di Bitcoin lanciato da Satoshi Nakamoto.



Si tratta della prima major release di Bitcoin Core a supportare l'imminente aggiornamento del protocollo Taproot, offrendo anche molti altri miglioramenti rispetto alle precedenti versioni di Bitcoin Core.

Lo sviluppo ha visto il coinvolgimento di oltre un centinaio di collaboratori in un arco di circa otto mesi, ed è stato supervisionato da Wladimir van der Laan, successore di Nakamoto e Andresen come lead maintainer.

Interessante notare come questa sia anche la prima versione di Bitcoin Core a eliminare lo 0 iniziale dal numero di versione: è Bitcoin Core 22.0, non Bitcoin Core 0.22.0. Le

comunità di sviluppatori open source tendono infatti a rilasciare le versioni iniziali con un versioning "0.", per indicare che il software è incompleto e non abbastanza affidabile per il rilascio generale.

Non è questo evidentemente il caso di Bitcoin Core, che con 13 anni di storia ed adozione industriale, manteneva il suo versioning "0." probabilmente come understatement.

Ethereum

Aggiornamento al protocollo

L'ultimo aggiornamento al protocollo Ethereum, denominato London, è stato attivato giovedì 5 agosto. London fondamentalmente consiste nell'implementazione di EIP1559, una modifica della gestione delle commissioni transazionali che le rende più prevedibili e, soprattutto, più economiche. Inoltre, EIP1559 prevede che parte delle commissioni transazionali vengano distrutte invece di essere riconosciute ai minatori: scelta pericolosa, perché rischia di esacerbare il problema del Miner Extractable Value (MEV). Si tratta della massimizzazione del profitto che i minatori possono ottenere sequenziando arbitrariamente le transazioni validate, in tutte quelle situazioni in cui l'ordine può dare un vantaggio economico secondo le regole dei diversi smart contract. La distruzione di parte delle commissioni transazionali riduce anche la base monetaria di ether, con

l'intento di renderli più scarsi e quindi di farne aumentare il valore. Questo perché la politica monetaria di ether non è fissata a priori, ma può essere decisa di volta in volta dal fondatore e dai suoi collaboratori stretti.



Ethereum: aggiornamento al protocollo

coindesk.com/ethereum-hotly-anticipated-london-hard-fork-is-now-live
 blockworks.co/eip-1559-is-live-thanks-to-ethereums-london-hard-fork
 twitter.com/nethermindeth/status/1414622903274905600
 ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698
 coindesk.com/analysts-take-cautious-stance-on-ether-as-london-hard-fork-nears
 mailchi.mp/c1e55ea9fa5c/frnt-financial-24-hours-in-crypto-august-3-2021
 mailchi.mp/152be551cdb1/frnt-financial-24-hours-in-crypto-august-6-2021

La frontiera della custodia

Trasparenza e solvibilità dimostrabile

Il 2021 ha sancito l'ingresso di attori istituzionali e investitori privati nel mondo dei digital asset, visti come una modalità di diversificazione del portafoglio.

Data la complessità nel gestire questi strumenti, qualificabili di fatto come al portatore, il mercato ha visto fiorire l'offerta di soluzioni di custodia specializzata, che liberano istituzioni e high-net individuals dall'onere di gestire le proprie chiavi private in sicurezza.

Tali soluzioni sono ad oggi però basate sulla cosiddetta "security by obscurity", cioè sul segreto industriale - in metodo che gli specialisti in sicurezza, crittografica e non, condannano dal 1851 (sì, milleottocento).

La mancanza di trasparenza ha un ulteriore impatto, quello della mancanza di certezza sulla solvibilità del custode.

Chi ci garantisce infatti che il custode abbia effettivamente sotto controllo gli asset digitali che dichiara di custodire? Anche se dovesse subire un hack, il custodian potrebbe non darne alcuna visibilità, trasformando di fatto i suoi clienti inconsapevoli in titolari di IOU basati su riserve frazionarie.

Se i grandi scandali nel mondo bitcoin sono stati hack su exchange e truffe, in questa nuova era di investitori professionali non stupirebbe vedere scandali di custodian improvvisamente insolventi.

E' perciò interessante osservare l'emergere in ambito crypto di soluzioni di custodia innovative, che mirano a fornire non solo la massima trasparenza al

proprio processo di custodia, ma anche una prova pubblica crittografica dell'esistenza e della disponibilità degli asset loro affidati.

Tale prova, nota come "Proof of Reserve" o "PoR", è oggi fornita solo dagli exchange Coinfloor e BitMEX e dal custodian CheckSig. Tuttavia la PoR non è sufficiente a scongiurare il pericolo di riserva frazionaria. L'exchange potrebbe aver perso solo parte dei fondi; ciò che è essenziale è che i fondi in custodia siano effettivamente in grado di soddisfare tutti i depositi della clientela, cioè le liabilities del custode.

Tale "Proof of Liabilities" è tuttavia molto difficile (se non impossibile) da fornire

crittograficamente senza inficiare la privacy della clientela. Chi di noi vorrebbe veder mostrato pubblicamente il saldo del proprio conto corrente? Per questo motivo, i pochi attori più seri utilizzano auditor esterni, sulla cui affidabilità gli scandali degli anni passati hanno tuttavia lasciato qualche ombra.

Questa è dunque la sfida della custodia. PoR e PoL, se fornite crittograficamente, darebbero prova pubblica della solvibilità (o "Proof of Solvency") del custode o dell'exchange.

E' la frontiera dei servizi professionali sui digital asset, e i prossimi mesi vedranno sicuramente l'emergere di standard di mercato.

“
 Security by obscurity implica
 la mancanza di certezza sulla
 solvibilità del custode.
 ”



proprio processo di custodia, ma anche una prova pubblica crittografica dell'esistenza e della disponibilità degli asset loro affidati.

Tale prova, nota come "Proof of Reserve" o "PoR", è oggi fornita solo dagli exchange Coinfloor e BitMEX e dal custodian CheckSig. Tuttavia la PoR non è sufficiente a scongiurare il pericolo di riserva frazionaria. L'exchange potrebbe aver perso solo parte dei fondi; ciò che è essenziale è che i fondi in custodia siano effettivamente in grado di soddisfare tutti i depositi della clientela, cioè le liabilities del custode.

Tale "Proof of Liabilities" è tuttavia molto difficile (se non impossibile) da fornire

crittograficamente senza inficiare la privacy della clientela. Chi di noi vorrebbe veder mostrato pubblicamente il saldo del proprio conto corrente? Per questo motivo, i pochi attori più seri utilizzano auditor esterni, sulla cui affidabilità gli scandali degli anni passati hanno tuttavia lasciato qualche ombra.

Questa è dunque la sfida della custodia. PoR e PoL, se fornite crittograficamente, darebbero prova pubblica della solvibilità (o "Proof of Solvency") del custode o dell'exchange.

E' la frontiera dei servizi professionali sui digital asset, e i prossimi mesi vedranno sicuramente l'emergere di standard di mercato.

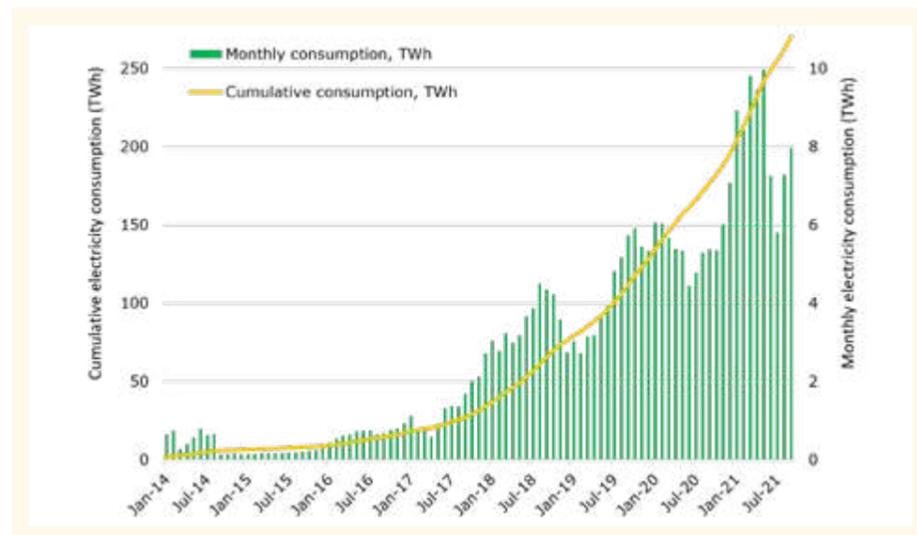


La frontiera della custodia: trasparenza e solvibilità dimostrabile

coinfloor.co.uk/hodl/proof
 checksig.io/por
 blog.bitmex.com/proof-of-reserves-liabilities-bitmex-demonstration

Mining

Sostenibilità ambientale



Consumo energetico aggregato delle operazioni di mining

Il grafico qui sopra mostra chiaramente quanto, nonostante la scelta della Cina di bandire il mining dal proprio territorio nel Q2 2021, la richiesta di energia da parte delle mining farm globali è in crescita da anni. Questo dopo un evidente calo di assestamento dovuto alla scelta drastica di Pechino.

La crescita di Bitcoin – sia nel valore, sia negli scambi – andrà inevitabilmente ad accrescere i consumi energetici necessari per le attività di mining e la garanzia di sicurezza del sistema. Se questi saranno o meno generati da fonti rinnovabili è tutto da verificare e, soprattutto, in capo agli Stati. Una delle notizie più importanti del Q2 era stata la scelta drastica della Cina di cacciare tutte le mining farm dal proprio territorio: il motivo? Inquinerebbero troppo e avrebbero rischiato di rovinare i piani di Pechino nella sua strada verso la sostenibilità. Non bisogna però nascondere anche l'altra ragione: Bitcoin e il mondo crypto non sono controllabili dal Partito. Già soltanto questa notizia avrebbe potuto suggerire ai non addetti ai lavori un conseguente e drammatico crollo del valore di Bitcoin, che invece a fine agosto è tornato a toccare i 50mila dollari.

Il dibattito sulla sostenibilità di Bitcoin è proseguito con interventi da più fronti. I critici rimangono dell'idea che il gioco non valga la candela. Se è sì dovessero avverare le previsioni di Cathie Wood di un'impennata fino a mezzo milione di dollari entro i prossimi anni il timore paventato dagli scettici è che la criptovaluta potrebbe emettere più CO2 di paesi come Messico (+33%) e Brasile (+40%).

In tale scenario saremmo però di fronte a una capitalizzazione per Bitcoin di 10 trilioni di dollari, a fronte di un prodotto interno lordo di paesi appena citati che, rispettivamente, si era attestato nel 2019 a 1,26 trilioni di dollari e 1,84 trilioni di dollari. Ne consegue che questo parallelismo estremo assegnerebbe ai miner una patente di efficienza energetica di prim'ordine. Insomma, i consumi non sarebbero di tanto superiori a fronte dell'enorme differenza tra l'ecosistema Bitcoin e quei paesi.

Per affrontare in maniera costruttiva e, perché no?, storica la questione Bitcoin e sostenibilità ci viene in soccorso un brillante articolo di Nic Carter, pubblicato su Bitcoin Magazine, nel quale l'osservatore fa notare quanto la querelle in corso riprenda in buona parte le stesse dinamiche di alcuni decenni fa per quanto riguardava l'estrazione dell'oro, giudicata costosa e inquinante.

«I costi di Bitcoin – spiega Carter – sono il denominatore nell'equazione della sua efficienza. Quanto spesso si sentono i critici ammettere che Bitcoin fornisce una preziosa libertà monetaria per decine di milioni di individui in tutto il mondo, specialmente quelli in stati instabili, privi di diritti di proprietà significativi?».

Le cifre sulla sostenibilità di Bitcoin non sono sempre concordanti. Uno studio dell'Università di Cambridge ha stimato che la porzione di fonti sostenibili utilizzate nel mining è del 39%, mentre CoinShares sosteneva sfiorasse l'80% fino a pochi anni fa. Sempre su Bitcoin Magazine si legge: è plausibile che la fetta green di energia necessaria per estrarre criptovalute valga circa il 50% del totale.



Cathie Wood



Nic Carter

Mining: sostenibilità ambientale

scmp.com/news/china/science/article/3128653/chinas-bitcoin-mines-could-derail-carbon-neutrality-goals-study
 bloomberg.com/news/articles/2021-05-19/cathie-wood-still-a-bitcoin-believer-sees-it-going-to-500-000
 fortune.com/2021/08/16/bitcoin-500k-carbon-footprint-co2-mexico-brazil
 infodata.ilsole24ore.com/2020/09/16/tutta-la-ricchezza-del-mondo-pre-covid-19-in-una-infografica
 bitcoinmagazine.com/culture/bitcoin-and-gold-energy-debate
 cnbc.com/2021/07/20/bitcoin-mining-environmental-impact-new-study.html
 fortune.com/2021/07/15/china-bitcoin-crackdown-mining-emissions-hash-rate
 fortune.com/2021/08/16/bitcoin-500k-carbon-footprint-co2-mexico-brazil
 bitcoinmagazine.com/culture/bitcoin-and-gold-energy-debate

La custodia Bitcoin professionale

I tradizionali processi di gestione aziendale sono inadatti al mondo degli *asset digitali*

Cresce di giorno in giorno il numero di investitori istituzionali e tesorerie aziendali che detengono Bitcoin per conto proprio e della propria clientela.

Gli *asset digitali* impongono tuttavia meccanismi di tutela e monitoraggio completamente nuovi, dalla gestione delle chiavi private ai processi autorizzativi.

Per questo c'è la custodia professionale di CheckSig

CheckSig offre un servizio trasparente di custodia Bitcoin per banche, fondi e tesorerie interessati a investimenti di medio-lungo termine, garantendo massima robustezza regolamentare e riservatezza.

Grazie al suo schema multi-firma e multi-livello, CheckSig fornisce una protezione incomparabilmente superiore ai tradizionali *hardware wallet* e adattabile alle esigenze di ciascuna controparte.

Inoltre, CheckSig è l'unico custode italiano dotato di coperture assicurative e che può vantare attestazioni SOC ottenute dal *service audit* indipendente di Deloitte.

Un servizio interamente disegnato per controparti istituzionali, inclusivo di *fast track* per l'accesso ai mercati attraverso le borse di scambio nostre *partner*, un *network* di esperti in ambito societario/fiscale e tutta la formazione e ricerca del Digital Gold Institute.

Concentrati sul tuo *core business*, mentre noi custodiamo i tuoi Bitcoin da attacchi esterni, problemi tecnici e frodi.

Scopri di più su [checksig.io](https://www.checksig.io)

 **CheckSig**
TRANSPARENT BITCOIN CUSTODY

VITA DELL'ISTITUTO

Presa Diretta



Riccardo Iacona

“Un doppio viaggio nel mondo delle criptovalute, un mercato in rapida crescita che già oggi vale 2000 miliardi di dollari, e in quello delle banche, che hanno attraversato la crisi scatenata dalla pandemia e si preparano a entrare in una dimensione nuova, con meno contante, meno sportelli e sempre più digitale.”

Questo il focus della puntata di “PresaDiretta” dal titolo “La guerra dei soldi” trasmessa lunedì 6 settembre su Rai3.

Tra gli esperti intervenuti troviamo anche il direttore scientifico DGI Ferdinando M. Ametrano.

Il documentario sull’ecosistema Bitcoin di Riccardo Iacona è evidenza della crescente attenzione al fenomeno, ma non solo: rappresenta un importante elemento di divulgazione sulla sua rilevanza in questo momento storico e culturale.

Siamo ancora distanti dal pieno riconoscimento del rilievo di questi temi e c’è molto da lavorare in termini di multidisciplinarietà, ma su entrambi gli aspetti la puntata di Presa Diretta è uno dei segnali incoraggianti.

E’ possibile rivedere il documentario su RaiPlay; maggiori dettagli sono disponibili alla pagina dgi.io/2021/09/07/presadiretta.



Ferdinando M. Ametrano

Presenza sui media

L’interesse su Bitcoin è aumentato enormemente: lo dimostrano le numerose interviste a Ferdinando M. Ametrano su diversi media tv, rai e web. Sotto ne riportiamo alcune rilasciate nel trimestre per le principali testate, le quali scelgono DGI come principale fonte di divulgazione sui temi legati all’ecosistema Bitcoin.

We Wealth

dgi.io/2021/08/12/we-wealth



Il Sole 24 Ore

dgi.io/2021/08/10/il-sole-24-ore



Agenda Digitale

dgi.io/2021/08/06/agenda-digitale
dgi.io/2021/09/21/agenda-digitale
dgi.io/2021/09/29/agenda-digitale



Rai 1

dgi.io/2021/07/17/codice-rai1



DigiTech.news

dgi.io/2021/07/16/digitech



Cybersecurity360

dgi.io/2021/09/29/cybersecurity360



Studio Paolo Gaeta

dgi.io/2021/09/28/studio-paolo-gaeta



CryptoWeek

Tutti i venerdì alle 18:00



Iniziativa settimanale, ogni venerdì alle 18:00 in live streaming su YouTube, Facebook e LinkedIn, successivamente disponibile su tutte le piattaforme di podcast, l'evento prevede una prima parte in cui Ferdinando M. Ametrano commenta le più rilevanti notizie del mondo Bitcoin e Blockchain. A seguire sono previsti gli interventi di eventuali ospiti di rilievo; infine, spazio alle domande dal pubblico.

Tutte le puntate sono disponibili alla pagina dgi.io/cryptoweek.

Bitcoin & Blockchain - Workshop

14 - 15 dicembre 2021



Bitcoin combina in maniera inedita e creativa elementi di crittografia, teoria monetaria ed economica, sistemi distribuiti e teoria dei giochi: Bitcoin è un esperimento arduo che potrebbe ancora fallire, ma culturalmente fondato e tecnologicamente robusto. Per approfondire questi temi, DGI offre un programma di formazione in due giornate rivolto a chi vuole approfondire Bitcoin e la sua tecnologia blockchain.

La prossima sessione di formazione è pianificata per il 28 e 29 settembre 2021.

Maggiori informazioni su contenuti, quota di partecipazione e modalità di iscrizione disponibili alla pagina dgi.io/workshop.

Presentazione del report trimestrale

6 ottobre 2021



Il report 2021-Q3 è stato presentato in anteprima il 6 ottobre, in web streaming. I fatti più rilevanti del trimestre sono stati commentati dal nostro direttore scientifico Ferdinando M. Ametrano. Al termine dell'evento pubblico è seguito un dibattito riservato ad invito tra esponenti del mondo politico, finanziario, industriale, accademico, consulenziale e giornalistico. È possibile consultare il report e rivedere l'evento di presentazione alla pagina dgi.io/reports. La prossima edizione del report trimestrale 2021-Q4 è prevista per gennaio 2022.

Crypto Asset Lab Conference

4 - 5 novembre 2021



Si terrà in web streaming il 4 e 5 novembre la terza edizione della conferenza organizzata dal Crypto Asset Lab, *joint venture* tra il nostro Istituto e l'Università di Milano-Bicocca, e dalla Commissione Europea (Direzione Generale *Joint Research Centre*). Nota anche come CAL2021, la conferenza vanta un eccellente *program committee* che selezionato le proposte di 40 lavori scientifici provenienti da tre diversi continenti in materia di investimenti, economia e regolamentazione per Bitcoin e cryptoasset.

Per partecipare come uditori alla conferenza è richiesta la registrazione gratuita.

Maggiori informazioni disponibili visitando cryptoassetlab.diseade.unimib.it/calconf.

Autori



Ferdinando M. Ametrano

ferdinando@dgi.io

Alessandro Di Stefano

distefanoalessandro90@gmail.com



Lucia Mandelli

lucia@dgi.io

Michele Mandelli

michele@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

 dgi.io

 info@dgi.io

 [@DigitalGoldInst](https://twitter.com/DigitalGoldInst)

 [@DigitalGoldInstitute](https://facebook.com/DigitalGoldInstitute)

 [@DigitalGoldInstitute](https://linkedin.com/company/DigitalGoldInstitute)

 [@dginst](https://discord.com/invite/dginst)

 [@DigitalGoldInstitute](https://youtube.com/DigitalGoldInstitute)