

**Digital  
Gold  
Institute**

*Scarcity in the Digital Realm*

N. **09**



**REPORT TRIMESTRALE**

**2021 Q2**



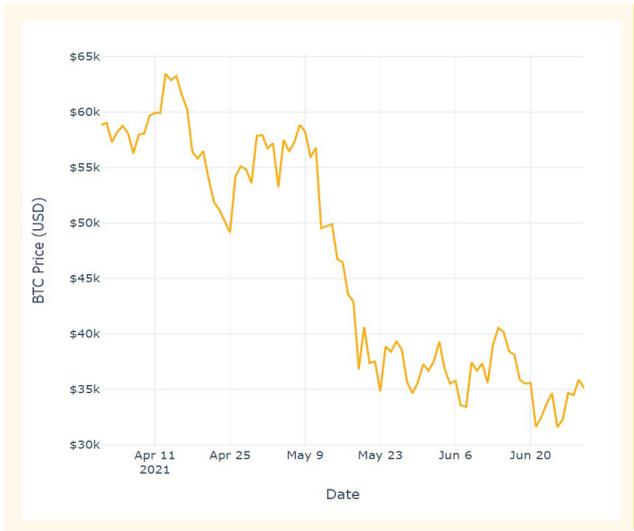
**Deloitte.**

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

© 2021 DIGITAL GOLD INSTITUTE

# E

## ditoriale



Il secondo trimestre del 2021 ha visto Bitcoin segnare il nuovo record assoluto di prezzo e poi ritracciare significativamente, ma in misura limitata rispetto ai *drawdown* visti in passato. Abbiamo avuto la quotazione di Coinbase, ad una valorizzazione paragonabile a quella dei principali istituti bancari mondiali, Bitcoin ha ottenuto corso legale in El Salvador, tutte le banche di investimento americane offrono accesso all'investimento in Bitcoin. Anche la messa al bando del mining e delle criptovalute in Cina è stata assorbita dal mercato e dall'ecosistema con relativa facilità. In que-

sto quadro di forte crescita e significativa maturazione, tutti i regolatori stanno tentando di mettere a fuoco il fenomeno, in un clima preoccupato per utilizzi criminali e sostenibilità ambientale. In realtà le preoccupazioni sono spesso sproporzionate e, come auspicato anche dal Presidente di Consob Paolo Savona, su questi temi è essenziale formazione ed educazione: il Digital Gold Institute è lieto di poter contribuire, forte anche del sostegno economico ed industriale di CheckSig, la nostra capogruppo.

Il primo contributo è proprio il report che avete tra le mani (o sul vostro schermo): rappresenta uno sforzo di sintesi informativa e di giudizio per aiutare i nostri lettori a seguire l'ecosistema Bitcoin, *crypto-asset* e *blockchain*. Non perdetevi il video di presentazione associato: [youtu.be/RP3Pd0aKous](https://youtu.be/RP3Pd0aKous).

In questo numero Paolo Mazzocchi presenta una approfondita analisi dei processi di custodia per bitcoin e crypto-asset: un aspetto tanto frainteso quanto cruciale per abilitare l'operatività di tutta l'industria di servizi finanziari in questo ambito. Seguono le nostre analisi e segnalazioni secondo le usuali categorie: mercato, ecosistema, regolazione e tecnologia.

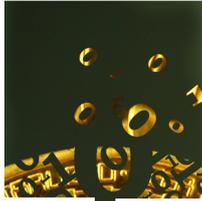
Il numero si chiude con la presentazione delle iniziative che caratterizzano la vita del nostro istituto: dal programma di formazione ([dgi.io/workshop](https://dgi.io/workshop)), riproposto almeno trimestralmente ma erogabile anche a richiesta e su misura ([dgi.io/training](https://dgi.io/training)), alla rassegna stampa settimanale CryptoWeek ([dgi.io/cryptoweek](https://dgi.io/cryptoweek)), ai diversi webinar che vengono annunciati sulla nostra pagina dedicata agli eventi ([dgi.io/events](https://dgi.io/events)) e spesso fruibili anche in differita grazie ai video online.

Infine, la terza conferenza del Crypto Asset Lab ([cryptoassetlab.diseade.unimib.it/calconf](https://cryptoassetlab.diseade.unimib.it/calconf)) prevista per il 4 e 5 Novembre, organizzata assieme all'Università Milano-Bicocca ed alla direzione generale *Joint Research Center* della Commissione Europea. Si tratta del principale evento accademico e scientifico del settore in Europa, ma quest'anno darà spazio anche alla presentazione di applicazioni nell'industria finanziaria e dei servizi.

Buona estate e buon Bitcoin a tutti.

# coinbase





# INDICE

## Opinion

|                               |   |
|-------------------------------|---|
| La custodia sicura di Bitcoin | 7 |
|-------------------------------|---|

## Mercato

|                   |    |
|-------------------|----|
| Bitcoin           | 18 |
| Alt-coin          | 22 |
| Correlazione      | 23 |
| Futures e opzioni | 25 |

## Ecosistema

|   |    |
|---|----|
| Borse di scambio  | 28 |
| Influenze sul mercato                                   | 29 |
| Il caso El Salvador: Bitcoin come moneta a corso legale | 30 |
| Bitcoin e servizi finanziari                            | 32 |
| I digital asset nel mondo finanziario europeo           | 32 |
| Ransomware: il caso Colonial Pipeline                   | 33 |
| Criptovalute e attività criminali                       | 34 |
| NFT: un trend sostenibile?                              | 35 |

## Regolazione

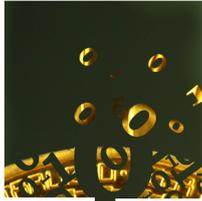
|   |    |
|---|----|
| Central Bank Digital Currency: Banca Centrale Europea | 38 |
| I regolatori: il contesto globale                     | 38 |
| I regolatori: Consob e Banca d'Italia                 | 39 |

## Tecnologia

|  |    |
|--|----|
| Protocollo Bitcoin: luce verde per Taproot | 42 |
| Mining: la migrazione dell'hashrate        | 43 |
| Mining: sostenibilità ambientale           | 44 |
| Il declino della blockchain                | 45 |

## Vita dell'Istituto

|  |    |
|--|----|
| Cryptocurrency Open Patent Alliance                    | 48 |
| Bitcoin e criptovalute: instant-book de Il Sole 24 ore | 48 |
| Webinar  | 49 |
| Presenza sui media                                     | 50 |
| CryptoWeek   | 52 |
| Bitcoin & Blockchain - Workshop                        | 52 |
| Presentazione del report trimestrale                   | 53 |
| Crypto Asset Lab Conference                            | 53 |



## La custodia sicura di Bitcoin

di Paolo Mazzocchi, CheckSig Operating Officer

La custodia sicura di Bitcoin si ottiene curando sia aspetti strettamente tecnologici, sia aspetti funzionali e di processo. È inevitabile che la comprensione dei

primi sia in qualche modo preliminare per poter comprendere gli ultimi: il lettore dovrà quindi avere una attitudine curiosa, metodica e paziente per cogliere i diversi passaggi qui affrontati. Le considerazioni che seguono si applicano in linea di massima con pochi adattamenti anche ai numerosi *crypto-asset* che sono venuti dopo Bitcoin, avendo questi mutuato la maggioranza delle scelte tecnologiche architettoniche.

La sicurezza di Bitcoin è basata su un libro mastro, chiamato *blockchain*, dove sono registrate tutte le transazioni ed i criteri con cui possono essere trasferiti i Bitcoin esistenti. La sicurezza delle singole transazioni è affidata, invece, alla crittografia asimmetrica, basata su una coppia di chiavi: una *pubblica* ed una *privata* o *segreta*. Le due chiavi sono matematicamente collegate e svolgono un ruolo complementare in un protocollo

di firma digitale: la chiave privata è utilizzata per generare firme digitali, la chiave pubblica è utilizzata da chiunque per verificare la genuinità delle firme digitali prodotte dalla corrispondente chiave privata. La chiave pubblica deriva dalla chiave privata ma la chiave privata non può essere derivata dalla chiave pubblica.

Esistono, poi, anche gli *indirizzi*: un indirizzo deriva da una chiave pubblica ma la chiave pubblica non può essere derivata dall'indirizzo. Insomma, la derivazione procede dalla chiave privata verso la pubblica per arrivare poi all'indirizzo ma non può essere percorsa in senso inverso. La chiave privata è cruciale perché permette la spesa dei Bitcoin associati all'indirizzo corrispondente. È possibile generare arbitrariamente chiavi private e le loro corrispondenti chiavi pubbliche e indirizzi, senza dover chiedere alcun tipo di autorizzazione. Anche per questo, Bitcoin è un bene al portatore: se si perde una chiave privata, i Bitcoin associati sono persi per sempre e nessuno, tantomeno una autorità centrale, può recuperarli.



Paolo Mazzocchi



Bitcoin Address



SHARE

19GBnmEGSpC3hJQExJwQfDAVSEx6agN9X1

Private Key (Wallet Import Format)



SECRET

5KXSFRN5BR1tLV7ro8qtBVGrciBq3nYJjNhMiHjKDCh3pxXynTV

Immaginiamo che Alice voglia trasferire dei Bitcoin da un suo indirizzo verso un indirizzo controllato da Bob. Alice dovrà (i) comporre un messaggio transazionale che include la quantità di Bitcoin che vuole trasferire, la sua chiave pubblica e l'indirizzo di Bob, (ii) firmare con la sua chiave privata questo messaggio che sarà poi inoltrato alla rete Bitcoin. Tutti i nodi della rete Bitcoin, avendo accesso alla chiave pubblica di Alice, potranno indipendentemente verificare che



(i) la quantità di Bitcoin che Alice vuole trasferire è realmente associata al suo indirizzo: l'indirizzo deriva infatti dalla chiave pubblica e sulla *blockchain* (il registro pubblico delle transazioni) si può verificare quanti Bitcoin sono associati ad un certo indirizzo; (ii) la firma del messaggio transazionale è valida e quindi il messaggio non è stato modificato ed è stato firmato proprio con la chiave privata associata all'indirizzo da cui si vogliono trasferire i Bitcoin. A questo

punto, un qualunque nodo della rete può aggiornare la *blockchain* con questa nuova transazione. Tutti sapranno che quel quantitativo di Bitcoin non è più associato all'indirizzo controllato da Alice, ma è stato trasferito all'indirizzo controllato da Bob: solo la chiave privata di Bob potrà trasferire ulteriormente i Bitcoin in questione.

Siccome il registro transazionale *blockchain* è pubblico, per motivi di *privacy* (e anche di sicurezza) è opportuno utilizzare un indirizzo diverso, e quindi una coppia chiave privata/pubblica diversa, per ogni transazione. Per gestire la molteplicità di indirizzi e chiavi si utilizzano soluzioni genericamente chiamate *wallet*: si tratta usualmente di un *software* che utilizza un seme (quasi sempre nella forma di una frase composta da diverse parole, nei diversi standard BIP39 o *Electrum*) da tenere segreto e da cui deriva un albero di chiavi (incluse le chiavi private) e indirizzi associati secondo lo standard noto come BIP32.

Quando le componenti segrete di un *wallet* non sono mai state esposte su Internet si parla di *cold wallet*. Quando lo sono, ad esempio su un server che deve firmare in automatico delle transazioni, si parla invece di *hot wallet*.

I *software wallet* sono talvolta rafforzati da componenti *hardware* (*Hardware Security Module*) che difendono le informazioni segrete all'interno di un *secure element*:

le chiavi private sono utilizzate per firmare le transazioni, ma non lasciano mai il *secure element*, non vengono viste direttamente dal *software* e non possono quindi essere copiate o trafugate. Gli *hardware wallet*, se usati correttamente, sono per definizione *cold wallet*.



Soluzioni mirate alla sicurezza nella conservazione delle chiavi private possono talvolta ritorcersi contro chi detiene Bitcoin. Un uso tecnicamente ingenuo può rendere l'accesso alle chiavi private improvvisamente impossibile allo stesso "legittimo proprietario", che dimentica un seme, un PIN, o perde un dispositivo *hardware*. Inoltre, il passaggio generazionale diventa impossibile se il defunto non ha documentato la sua prassi di sicurezza; ma documentarla avrebbe rappresentato un rischio operativo perché avrebbe consentito ad altri di appropriarsi dei Bitcoin.

Per questo spesso si preferisce affidare il controllo dei Bitcoin ad una molteplicità di attori diversi, con schemi *multi-firma m-di-n* (in inglese *m-of-n multi-sig*):  $m$  di  $n$  chiavi private devono firmare la transazione. Ad esempio, il caso 1-di-2 è analogo ad un conto bancario tradizionale cointestato a firma disgiunta, mentre il caso 2-di-2 è analogo ad un conto cointestato a firma congiunta. Usualmente, si evitano le configurazioni 1-di- $n$ , perché rendono l'accesso ad un singolo *wallet* su  $n$  sufficiente per trafugare i Bitcoin, vanificando il rafforzamento che si vuole ottenere coinvolgendo più attori nel controllo dei Bitcoin.

Anche se difese dal *secure element* di un dispositivo *hardware*, le componenti private di un *wallet* (o il dispositivo *hardware* medesimo) restano a rischio furto,

perdita, smarrimento, guasto. Per limitare questi rischi, le configurazioni di sicurezza più avanzate prevedono schemi multi-firma con ridondanze: ad esempio, in un 2-di-3 la perdita di uno dei tre *wallet* non comporta la perdita dei Bitcoin associati, che sono trasferibili con i due *wallet* rimanenti. Allo stesso tempo, non c'è un singolo attore che controlla i Bitcoin.

Si parla spesso anche di approcci *multi-party computation* come alternativa al multi-firma. In questo caso i Bitcoin sono spendibili da una singola chiave, che viene suddivisa in  $n$  componenti ma può essere ricostruita con solo  $m$  componenti. Apparentemente l'approccio sembra simile ad un *multi-firma m-di-n*, ma in realtà al momento della firma viene ricostituita l'unica chiave che, se trafugata in quel momento, consente il furto dei Bitcoin. Inoltre, mentre in una configurazione 2-di-3 multi-firma si riconoscono sempre, dalle chiavi specificamente utilizzate, i due attori che hanno firmato

la transazione, in un 2-di-3 *multi-party* non è possibile sapere quali dei tre attori siano stati coinvolti nella firma che avviene sempre con l'unica chiave ricostruita. L'approccio *multi-party*, noto da decenni come *Shamir secret sharing*, è da sempre considerato meno sicuro del multi-firma per i due motivi appena esposti: la debolezza di una unica chiave e l'impossibilità di verificare chi ha contribuito a ricostruirla. La recente popolarità di approcci *multi-party computation* è dovuta alla mancanza di supporto multi-firma per molti *crypto-asset* tecnologicamente immaturi (ad esempio Ether); purtroppo, operatori tecnologicamente ambigui la usano irresponsabilmente anche per Bitcoin, sebbene sia subottimale dal punto di vista della sicurezza e dell'*audit*.

“

Soluzioni mirate alla sicurezza nella conservazione delle chiavi private possono talvolta ritorcersi contro chi detiene Bitcoin.

”





*Il fai-da-te sulla sicurezza diventa rapidamente pericoloso perché tecnicamente complesso e operativamente pericoloso.*



In ambito *crypto-asset*, il fai-da-te sulla sicurezza diventa rapidamente pericoloso perché tecnicamente complesso e operativamente pericoloso. Chi possiede pochi gioielli li tiene usualmente in casa: potremmo dire che questo comportamento è

analogo a custodire i propri Bitcoin con un *software wallet* a firma singola gestito personalmente; quando i gioielli fossero tanti si preferisce di solito una cassaforte o meglio ancora una cassetta di sicurezza: questo è l'equivalente di un *hardware wallet* o di una configurazione multi-firma; invece, quando si possedessero lingotti d'oro, allora ci si rivolge a servizi di custodia professionale: lo stesso vale per i *crypto-asset*.

Eppure, in ambito Bitcoin si sente spesso la frase “*not your keys, not your coins*” per sottolineare che la gestione diretta delle chiavi private è l'unica garanzia di possesso reale, che il controllo è l'unica forma di possesso. Si parla di sovranità finanziaria (“*financial sovereignty*”) e si incita ognuno ad essere la sua propria banca (“*be your own bank*”). Queste osservazioni

radicali sono pertinenti e condivisibili, specialmente in alcune situazioni o momenti della storia: se si fugge da regimi dittatoriali come quello cinese, nordcoreano o venezuelano, è cruciale la possibilità di attraversare il confine avendo semplicemente memorizzato le dodici parole che costituiscono un seme *BIP39*, un po' come facevano gli ebrei che tentavano di scappare da Hitler e nascondevano pochi gioielli nella biancheria intima che indossavano. In regimi più liberali questi rischi esiziali non ci sono e i rischi associati alla custodia fai-da-te diventano più rilevanti: non solo per l'imperizia tecnica che può portare alla perdita dei beni, ma per il rischio di aggressione legato a tentativi di furto e, non da ultimo, per la difficoltà di trasferire i Bitcoin nel passaggio generazionale ereditario. La risposta definitiva ai *Bitcoiner* più radicali la fornisce Pieter Wuille, oggi probabilmente il più rilevante sviluppatore del protocollo Bitcoin: “*Proprietà e controllo non sono la*

*stessa cosa. Non intendo solo in senso legale: sarei sorpreso se molta gente ritenesse che il possesso di qualcosa sia necessariamente collegato al suo controllo*”.

Servizi di custodia professionale non prevedono che il possessore dei Bitcoin debba gestire chiavi private e lo liberano da qualsiasi responsabilità operativa. Questo approccio risolve i problemi di passaggio generazionale, in quanto il dossier di custodia entra a pieno titolo nell'asse ereditario. Servizi di custodia

professionale sono inoltre essenziali per gli investitori istituzionali che, per ragioni regolamentari, non possono detenere direttamente i loro beni.



Le soluzioni di custodia sono usualmente a più livelli, con ogni livello configurato in multi-firma: *hot wallet* più *cold wallet* è la soluzione a maggior diffusione. La maggioranza dei Bitcoin è detenuta nel *cold wallet*, una parte minoritaria nell'*hot wallet*: quest'ultimo è utilizzato solo per velocizzare e facilitare il prelievo di Bitcoin da parte dell'utente finale. Si stanno però diffondendo soluzioni *cold wallet* più *frozen wallet* che privilegiano la sicurezza a scapito di una liquidità istantanea. È infatti inevitabile che una maggiore sicurezza renda il processo di prelievo meno fluido; viceversa, la facilità di prelievo può essere ottenuta solo con standard di sicurezza più rilassati.

Le soluzioni di custodia professionali possono essere valutate con diversi criteri. Essendo un settore di mercato molto giovane è generalmente ancora caratterizzato da tratti di immaturità.

Ad esempio, paradossalmente, il criterio più rilevante per valutare la qualità di un servizio di custodia è oggi trascurato dalla quasi totalità degli operatori di mercato: la prova delle riserve detenute (*proof-of-reserve*).

Si tratta di fornire una prova periodica di non aver perso il controllo dei beni in custodia. Se, infatti, gli scandali degli ultimi anni hanno coinvolto borse di scambio che hanno perso i *crypto-asset* gestiti sulle loro piattaforme, è facile immaginare che gli scandali dei prossimi anni potranno coinvolgere custodi professionali che hanno già perso o perderanno, accidentalmente o per malversazione, i beni a loro affidati, senza che nessuno se ne accorga tempestivamente.

Un altro criterio è la trasparenza del processo di custodia. Molte aziende lo tengono segreto, citando ragioni di sicurezza, ma in ambito crittografico la *security-by-obscurity* (sicurezza tramite oscurità) è unanimemente condannata da tutti gli esperti in quanto intrinsecamente insicura. Infatti, uno schema crittografico che non regga lo scrutinio pubblico degli esperti non può essere considerato affidabile. In un certo senso si può dire che se un servizio di custodia non fornisce elementi di trasparenza sul processo, è perché se ne vergogna.



Abbiamo già accennato perché sia opportuno diffidare di schemi *multi-party computation* utilizzati dai custodi che offrono servizi per diversi *crypto-asset*. Questi schemi rendono più fragile proprio la custodia di quel Bitcoin che, leader di mercato indiscusso per volumi scambiati e capitalizzazione, reclama il titolo di oro digitale, promette una maggiore durabilità nel tempo e si candida ad essere il bene di rifugio del XXI secolo. E che quindi meriterebbe processi di custodia e sicurezza senza compromessi.

Gli ultimi mesi hanno invece visto un deciso rafforzamento per quanto riguarda altri due criteri di valutazione: le coperture assicurative e le attestazioni SOC.



“

*Il custode è l'assicuratore ultimo che, solo, può fornire garanzie per il livello di sicurezza più profondo.*

”

A fine 2019 le coperture assicurative sui processi di custodia erano rarissime; oggi sono diffuse tra tutti gli operatori qualificati. Le coperture riguardano sempre e solo il livello *hot* in soluzioni *hot+cold* o il livello *cold* in soluzioni *cold+frozen*. È il custode, infatti, l'assicuratore ultimo che, solo, può fornire garanzie per il livello di sicurezza più profondo. A titolo comparativo, anche nella custodia di oro fisico a livello istituzionale (Fort Knox, Bank of England) non è il contenuto del caveau blindato ad essere assicurato, ma i trasferimenti da e verso quel caveau. Analogamente in ambito *crypto-asset*, un assicuratore terzo rispetto al custode assicurerà solo il livello più esposto, dove vengono conservati una frazione marginale dei beni.

Come per le garanzie assicurative, a fine 2019 tra i fornitori dei servizi di custodia si registrava l'assenza sostanziale di attestazioni SOC. Emesse da primarie società di consulenza, queste attestazioni documentano l'adeguatezza, sicurezza, robustezza e resilienza dei processi operativi del custode. Oggi sono molto più diffuse, sia le attestazioni SOC 1 relative agli aspetti tecnici e di processo, sia quelle SOC 2 relative agli aspetti di organizzazione interna; entrambe sono poi disponibili sia nella versione *Type 1* relativa ad una osservazione puntuale nel tempo, sia nella versione *Type 2* relativa ad una osservazione continuativa. Le attestazioni SOC rappresentano oggi l'indispensabile evidenza che un *crypto-custodian* accetta di sottoporsi ad un audit esterno.

Nel mondo finanziario tradizionale è consolidato il concetto di terzietà nella custodia dei titoli e dei beni, di solito svolto dalle cosiddette banche depositarie. Inoltre, è ormai acquisita la consapevolezza regolamentare che non è opportuno un custode svolga anche attività di scambio o intermediazione. Purtroppo in ambito *crypto-asset* questo conflitto di interessi è spesso presente: le borse di scambio svolgono un ruolo ancora dominante anche nel segmento dei servizi di custodia. Il regolatore non è ancora intervenuto in questo ambito, sia per mancanza di comprensione tecnica sia per la (non troppo nascosta) speranza di poter evitare la legittimazione del fenomeno *crypto-asset*.

Le cose sembrano però essere finalmente cambiate negli Stati Uniti, almeno dall'ultimo trimestre 2020. L'*Office of the Comptroller of the Currency*, l'ufficio indipendente del Tesoro che regola e supervisiona le banche, ha autorizzato tutte le banche ad erogare servizi di custodia per *crypto-asset* ed ha persino attribuito la licenza bancaria ad un *crypto-custodian*. Sembra purtroppo difficile che l'Europa possa recuperare il divario, con grave danno per l'industria europea del settore, visto l'atteggiamento conservatore sia del dibattito politico-culturale sia di quello genuinamente regolamentare.



Se si guarda agli Stati Uniti, si può cogliere un'altra tendenza caratterizzante la custodia di *crypto-asset*: il ricorso da parte del mondo finanziario tradizionale

a startup specializzate. Bitcoin è digitale come le azioni Facebook o i Titoli di Stato italiani, ma non si è mai sentito che qualcuno abbia rubato il 3% dei titoli azionari di una azienda o dei titoli obbligazionari di uno stato. Questo perché i titoli sono nominativamente intestati, mentre Bitcoin non lo è, essendo un bene al portatore, simile all'equivalente digitale dell'oro. Ma chi volesse rubare oro fisico avrebbe significative difficoltà logistiche, legate al trasporto e conservazione di quanto sottratto a Fort Knox o Bank of England; l'oro digitale, invece, è leggerissimo e



le sue transazioni, i suoi trasferimenti, sono irreversibili. Insomma Bitcoin ed i *crypto-asset* hanno caratteristiche straordinariamente diverse da quelle dei beni usualmente custoditi dalle banche depositarie o difesi dalla pratiche di *cyber-security* degli istituti finanziari tradizionali. Sono necessarie competenze specifiche che il mondo finanziario non ha. Infatti, dopo aver aperto ai suoi utenti la possibilità di investire in Bitcoin e affini, PayPal ha acquisito Curv, società di custodia israeliana. La più antica banca depositaria statunitense, Bank of New York Mellon, ha investito in Fireblocks, ai cui servizi intende ricorrere per offrire *crypto-custody* ai suoi clienti.

Al momento in cui scriviamo, il gestore di fondi Galaxy Digital sta considerando l'acquisizione di BitGo, altro *crypto-custodian*.

Concludendo, molta strada è stata fatta nel percorso di maturazione degli standard di sicurezza: lo sviluppo di soluzioni di custodia professionale ne rappresentano l'apice.

Come abbiamo visto, il processo di custodia si qualifica fundamentalmente sugli aspetti tecnici, ma

deve sapersi sposare con rilevanti aspetti amministrativi, assicurativi, e regolamentari. Molta strada resta ancora da fare, specialmente in Europa, per sviluppare un quadro regolamentare adeguato. Ed è ancora rara la cultura tecnologica che permetta di discriminare tra soluzioni di custodia approssimative e quelle che, invece, sono l'implementazione efficace delle migliori prassi. E già si intravedono all'orizzonte sviluppi innovativi di tecniche crittografiche che potranno rendere la custodia ancora più sicura. Ci sarà modo di parlarne e scriverne in futuro.

“ Sono necessarie competenze specifiche che il mondo finanziario non ha. ”



BNY MELLON

## Taking the pulse of digital assets in financial services

**Antonio Senatore**, Deloitte EMEA Blockchain Lab Lead and Global Blockchain CTO

Invariably, any technology that shows early promise comes with hype. Yet in the digital assets and cryptocurrency space, developments over the last few months would seem to suggest this area is moving towards the mainstream.

Almost 90 per cent of the world's central banks are looking at introducing digital currencies. In June, El Salvador became the first country to accept Bitcoin as legal tender. Citi declared that it is looking into cryptocurrency markets, specifically citing customer demand as the driver. This year also saw non-fungible tokens, or NFTs, come into the spotlight offering a powerful new means to represent digital property.

This all suggests positive momentum, but it is also important to acknowledge the volatile and unpredictable nature of the crypto market. In May, Tesla said it would no longer accept payment in Bitcoin, although CEO Elon Musk subsequently clarified that the car maker would resume Bitcoin transactions when the environmental cost of mining the coins reduces. China's recent crackdown on Bitcoin mining has led to its price plummeting. We must also recognize the skepticism that exists around this much-hyped area. But what are the key highlights about the industry evolution?

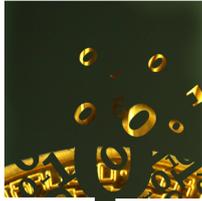
- **Investments in digital assets:** 'Announcements' and 'plans' make for positive press coverage, but the question to ask is whether financial services organizations are committing real investment to this area. From our work with large global banking and financial services clients, we know many have been experimenting with digital assets for several years. However, the transition from research and experimentation into strategic intent, investment and execution can be harder to discern. One of the indicators of real strategic intent can be inferred by observing marketplace M&A activity; Paypal's recent acquisition of digital asset custody specialist Curv is one relevant example of this. As the examples show, there are clearly some players at the forefront that are putting real investment into crypto. Another factor to consider is whether large institutional and corporate clients are asking their financial services advisors about what services they offer in the digital assets space. Our sense is that changing customer demand is triggering a lot of the activity. It is likely some of the banks are reacting to this change in behaviour out of a sense of not wanting to lose customers if they don't offer crypto products and services.
- **Regulation:** On the other hand, there is no question that regulators are making their voices heard in the digital assets space. Earlier this year, the European Commission proposed Markets in Crypto-Assets (MiCA), a regulation to help regulate currently out-of-scope crypto-assets and their service providers in the EU and provide a single licensing regime across all member states by 2024. This proposed framework will bring into scope other cryptocurrencies, security tokens and stablecoins that are not caught by existing regulation.
- **Tokenization:** The last key highlight is tokenization - representing a financial asset like an equity or share as a digital token - Unlike traditional settlements that can take up to three days to reconcile, buying or selling the token on a blockchain network facilitates near real-time reconciliation. This acceleration of value transfer can transform financial markets infrastructure.



# FinTech Talks 2021 | 6<sup>th</sup> edition

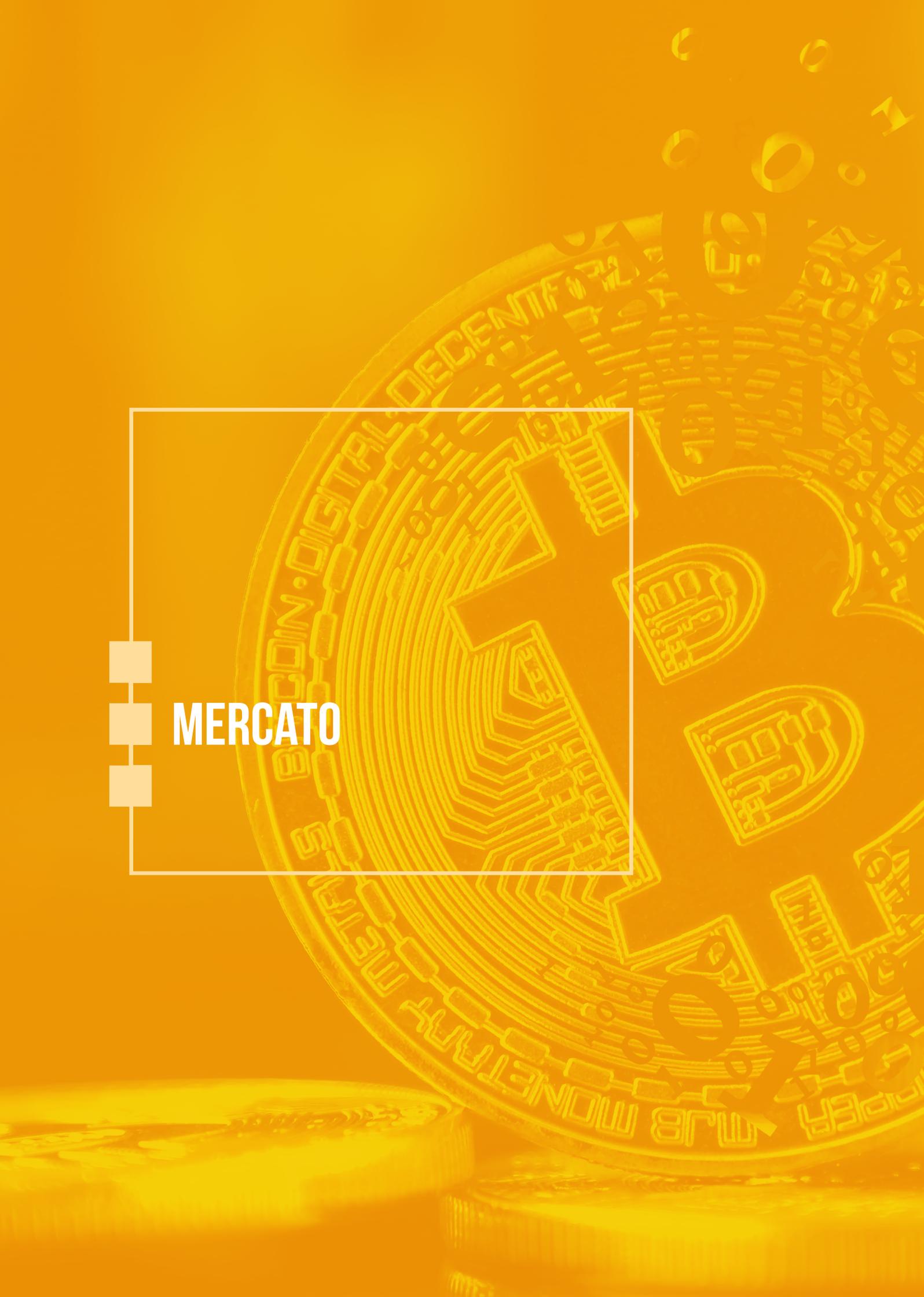
Discover the future of FinTech and the new ideas in the FSI world

**SAVE THE DATE OCTOBER 7<sup>th</sup> 2021**





# MERCATO



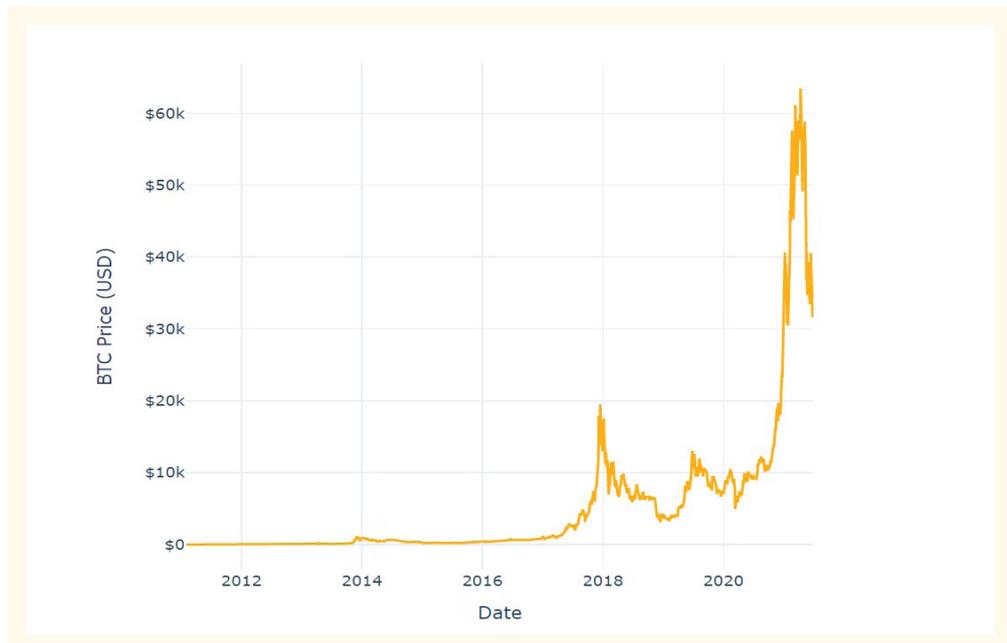
## Bitcoin

Il secondo trimestre è stato decisamente diverso rispetto al primo trimestre dell'anno. Bitcoin è passato in poche settimane dal record storico di oltre 63mila dollari ad una quotazione in area 30mila per poi chiudere il trimestre a circa 35mila, segnando una delle peggiori performance trimestrali degli ultimi anni, con una perdita del 40%.



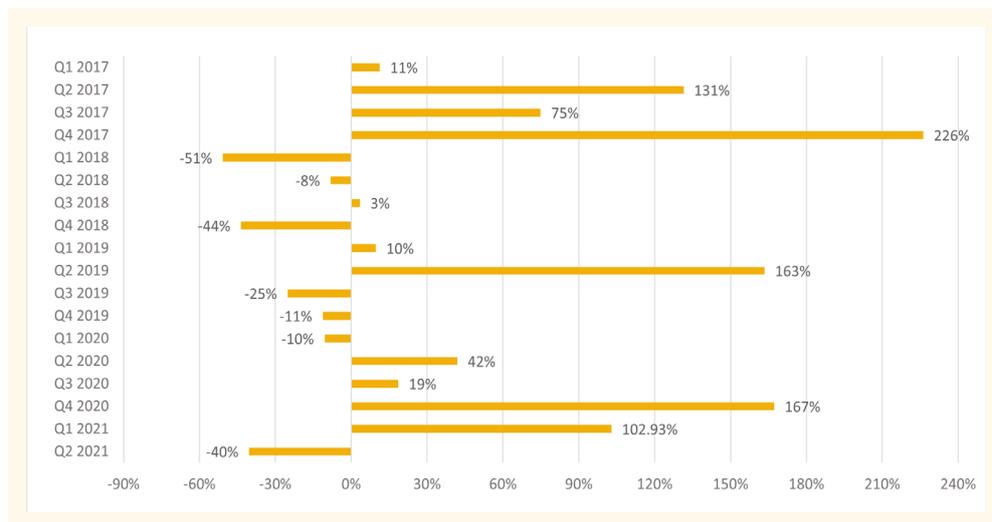
Valore di Bitcoin in USD, secondo trimestre 2021

La correzione dei corsi è estremamente marcata, tipica della crescita a strappi di Bitcoin: significativi bull run che portano a nuovi all-time high del prezzo, per poi ritracciare significativamente, ma consolidando il valore sempre e comunque a livelli sostanzialmente più alti di quelli visto in precedenza.



Valore di Bitcoin in USD

Questo è stato il primo trimestre negativo dopo una sequenza di ben quattro trimestri positivi; per questo, rispetto alle quotazioni di 12 mesi fa l'apprezzamento di valore resta comunque eccezionale, essendo il prezzo di Bitcoin sostanzialmente triplicato nell'ultimo anno.

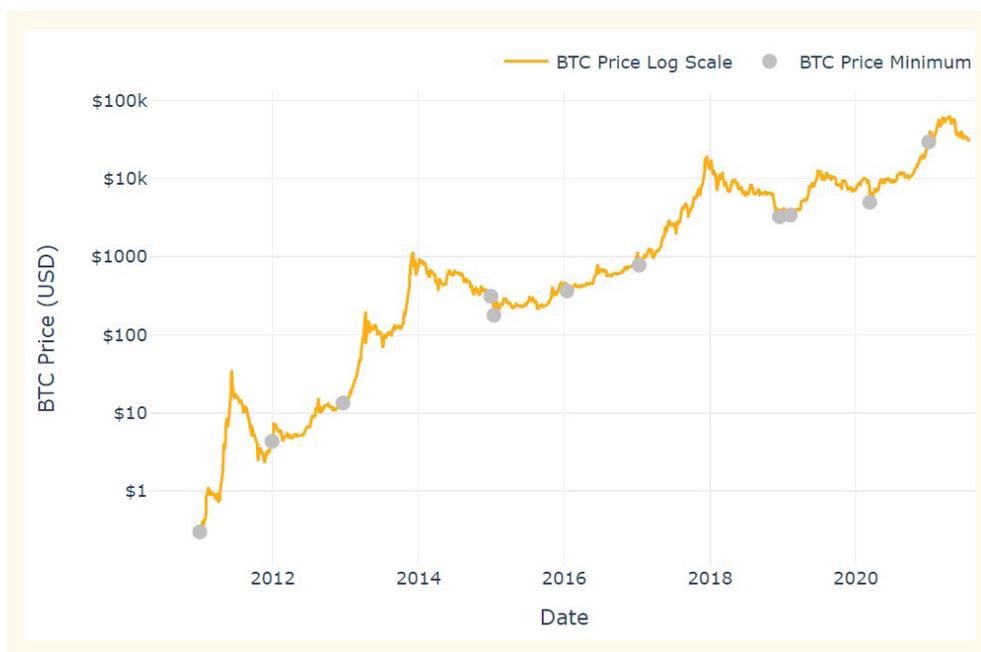


Performance trimestrale di Bitcoin

Anche la performance da inizio anno resta comunque positiva, segnando quasi un +20% di apprezzamento.

| DATA               | PREZZO              | PERFORMANCE ANNUALE |
|--------------------|---------------------|---------------------|
| 31 Dec 2011        | 5.00 \$             | 1,566.67 %          |
| 31 Dec 2012        | 13.59 \$            | 171.80 %            |
| 31 Dec 2013        | 754.01 \$           | 5,448.27 %          |
| 31 Dec 2014        | 320.19 \$           | -58.49 %            |
| 31 Dec 2015        | 430.57 \$           | 37.02 %             |
| 31 Dec 2016        | 963.74 \$           | 121.89 %            |
| 31 Dec 2017        | 14,156.40 \$        | 1,318.01 %          |
| 31 Dec 2018        | 3,742.70 \$         | -72.60 %            |
| 31 Dec 2019        | 7,193.60 \$         | 87.16 %             |
| 31 Dec 2020        | 28,968.31 \$        | 302.33 %            |
| <b>30 Jun 2021</b> | <b>35,086.59 \$</b> | <b>19.40 %</b>      |

Il 25 giugno ha segnato il punto più basso del trimestre a 31mila dollari; in ogni caso, il minimo dell'anno resta la quotazione del primo gennaio come si vede nel grafico del prezzo Bitcoin in scala logaritmica. Questo grafico è particolarmente significativo perché mostra la crescita sostanzialmente esponenziale del prezzo e la conseguente crescita anche dei minimi per anno. I valori minimi per anno sono certamente meno eccitanti rispetto all'euforia dei record di prezzo, ma dicono di una linea di tenuta forte che può contestualizzare una volatilità sicuramente significativa, ma non spaventosa.



Valore di Bitcoin in USD

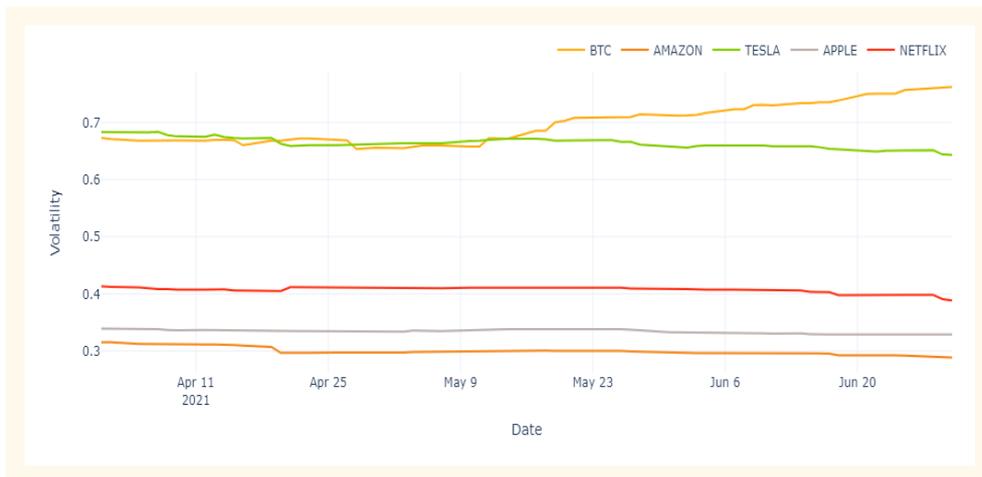
Anzi, l'evidenza è che il mercato Bitcoin sia significativamente maturato rispetto agli anni scorsi. Come mostrato nella tabella dedicata ai drawdown, cioè ai record negativi da massimo a minimo successivo, quest'ultimo targato 2021 è stato (finora) del 50%: significativamente più contenuto rispetto ai precedenti del 2011 (-93%), del 2015 (-85%) e del 2018 (-83%). Questa evoluzione si spiega facilmente con l'ingresso nel mercato Bitcoin di investitori istituzionali, che non vendono in preda al panico, entrano con orizzonti di medio-lungo periodo e, soprattutto, hanno la freddezza di acquistare quando i corsi crollano.

| ALL-TIME HIGH DATE | ALL-TIME HIGH VALUE | DRAWDOWN DATE | DRAWDOWN VALUE | DRAWDOWN PERCENTAGE |
|--------------------|---------------------|---------------|----------------|---------------------|
| 10 Jun 2011        | 35.00 \$            | 21 Nov 2011   | 2.29 \$        | -93 %               |
| 4 Dec 2013         | 1,151.00 \$         | 14 Jan 2015   | 178.10 \$      | -85 %               |
| 16 Dec 2017        | 19,497.40 \$        | 15 Dec 2018   | 3,236.76 \$    | -83 %               |
| 13 Apr 2021        | 63,445.64 \$        | 25 Jun 2021   | 31,604.13 \$   | -50 %               |

Per completezza riportiamo anche le peggiori perdite giornaliere del 2021: sebbene enfatizzate dall'informazione generalista, non rientrano nella lista delle peggiori di sempre. Nessuna delle giornate di mercato del 2021 entra nella classifica delle peggiori giornate del mercato Bitcoin, a conferma di un regime di volatilità meno estremo rispetto al passato.

| DATE (2021) | RETURN   | DATE (ALL-TIME) | RETURN   |
|-------------|----------|-----------------|----------|
| 19 May      | -14.18 % | 12 April 2011   | -61.37 % |
| 21 January  | -13.13 % | 12 March 2020   | -37.17 % |
| 12 May      | -12.78 % | 12 June 2011    | -28.60 % |
| 21 June     | -11.21 % | 18 October 2011 | -25.66 % |
| 23 February | -9.60 %  | 2 May 2013      | -24.52 % |

Peraltro, in finanza il rendimento è sempre la remunerazione di rischi: impossibile sfuggire a quella che rappresenta una legge di natura nel mondo degli investimenti. Come da noi ripetutamente spiegato, Bitcoin ha una volatilità sostanzialmente in linea con quella dei best performing asset dell'ultimo decennio: Tesla, Amazon, Apple e Netflix).



Volatilità di Amazon, Apple, Bitcoin, Netflix e Tesla su una finestra mobile di 90 giorni

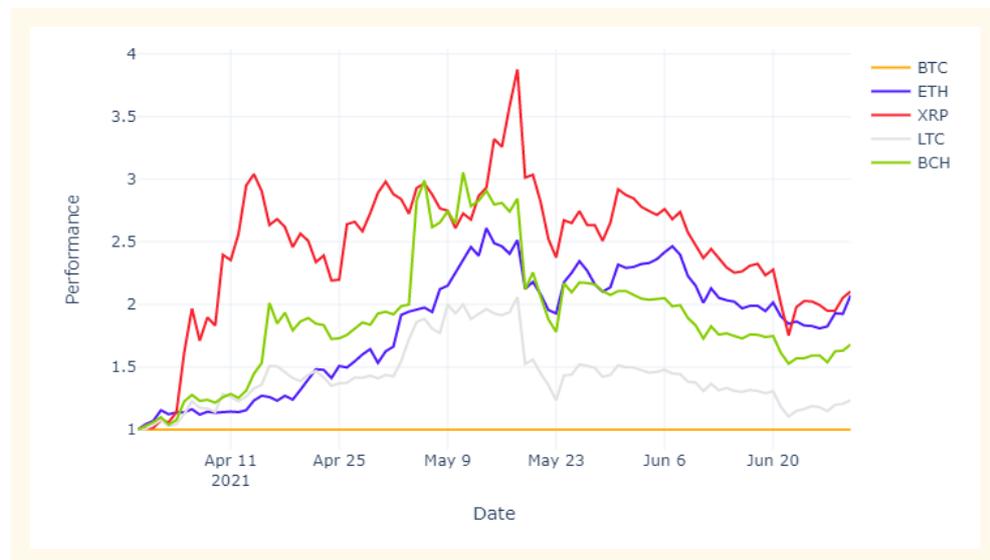
## Alt-coin

Il trimestre negativo per Bitcoin ha influenzato anche le alt-coin, le criptovalute alternative a Bitcoin.

Dopo un avvio molto promettente caratterizzato da grandi rialzi e record storici nelle quotazioni, i prezzi hanno subito un brusco crollo che ha in gran parte annullato i guadagni registrati nel trimestre.

Nonostante ciò, le performance rimangono superiori a quelle fatte registrare nello stesso periodo da Bitcoin. In figura sono riportati i rendimenti espressi in Bitcoin: cioè quanto avrebbe reso un Bitcoin investito ad inizio periodo in ognuno degli altcoin considerati.

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



Rendimenti alt-coin denominati in Bitcoin, secondo trimestre 2021

Estendendo però l'intervallo di osservazione oltre il trimestre e guardando guardando gli ultimi 12 mesi, è soltanto Ether ad aver performato meglio di Bitcoin.



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

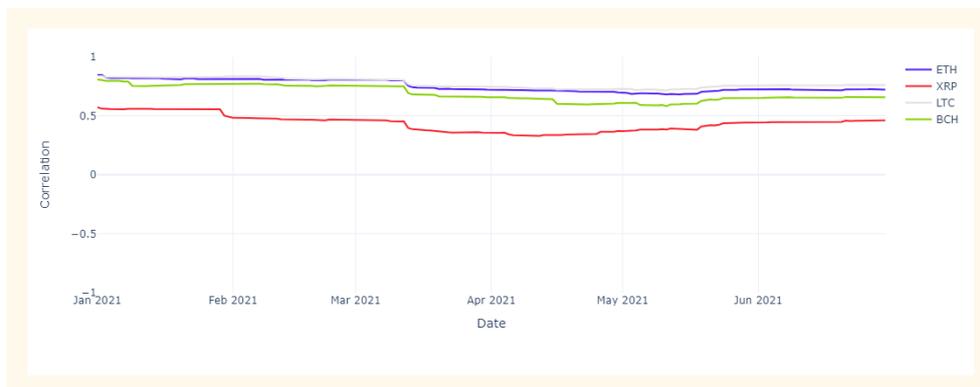
Sarebbe d'altro canto miope concentrarsi sui dati degli ultimi mesi per concludere che le alt-coin siano davvero in grado davvero di competere con Bitcoin: negli ultimi tre anni nessuna ha reso più di Bitcoin.



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

## Correlazione

Il motivo per cui non è facile offrire un'alternativa valida a Bitcoin è dovuto a un dato oggettivo: tutti i *crypto-asset* seguono l'andamento di Bitcoin come si vede dai grafici riportati sotto. Se è vero che la diversificazione in ambito di investimenti è un'operazione virtuosa, aggiungere un *cryptoasset* oltre a Bitcoin non va in questa direzione.

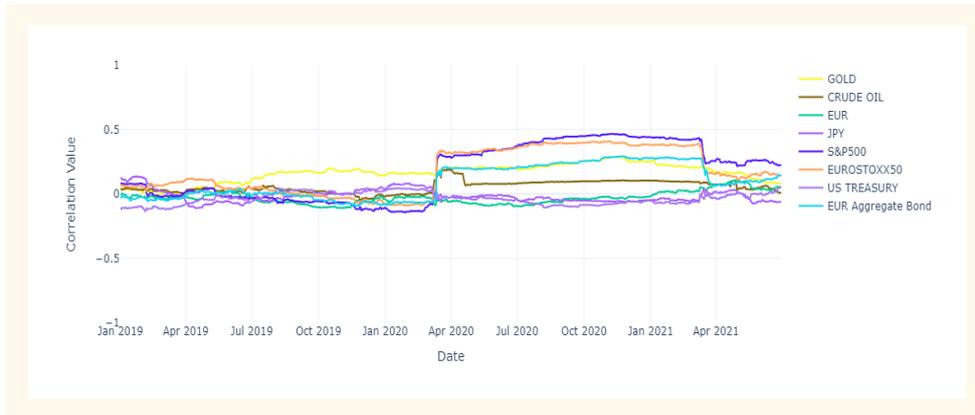


Correlazione ETH, XRP, LTC, BCH con BTC su una finestra temporale di un anno

Tutt'altro discorso è invece la correlazione di Bitcoin e i vari *crypto-asset* con le altre *asset class*. Come si può dedurre dai numeri riportati nella matrice riportata sotto, i valori di correlazione tra Bitcoin e le *altre asset class* (commodity, currency, equity, volatility e bond) hanno valori sempre molto contenuti, mostrando una sostanziale assenza di correlazione.



Restringendo la finestra di osservazione a un anno si nota come con l'uscita dall'intervallo considerato del 12 marzo 2020 i valori tornano ad allinearsi ai numeri pre-covid.



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

## Futures e opzioni

Come sempre concludiamo le analisi di mercato del trimestre guardando ai derivati del Chicago Mercantile Exchange (CME). I futures scambiati nel Q2 sono in lieve flessione rispetto al Q1 che aveva segnato, ricordiamolo, il record assoluto di volumi. Il trend complessivo resta comunque molto positivo, come confermato dalla crescita dei volumi in opzioni. CME resta sempre indietro rispetto ad alcune borse non regolate, ma per queste ultime non ci sono garanzie sulla veridicità dei volumi dichiarati, tantomeno su affidabilità, correttezza e solvibilità. Per questo CME è di gran lunga preferito dagli operatori finanziari tradizionali e rappresenta, a nostro avviso, il mercato di riferimento.



Volumi futures CME Group Inc.



Volumi opzioni CME Group Inc.

# 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)**





# ECOSISTEMA



## Borse di scambio



Brian Armstrong

«L'ho letto per la prima volta durante le feste di Natale: non ho smesso di pensarci per i sei mesi successivi. La maggior parte dei miei amici pensava che Bitcoin fosse un'invenzione bizzarra, ma qualcosa nella pancia mi suggeriva che, invece, era importante». Queste le parole di Brian Armstrong, amministratore delegato di Coinbase, mentre ricordava quei giorni di fine 2008, quando il white paper di Satoshi Nakamoto era stato appena rilasciato. A quasi 13 anni di distanza molta acqua è passata sotto i ponti e il percorso di questo imprenditore, che ha fondato l'exchange nel 2012, è arrivato fino alla quotazione della società a Wall Street il 14 aprile. A inizio anno la valutazione di Coinbase sfiorava i 50 miliardi di dollari e, complici le ottime performance di Bitcoin nel primo trimestre, gli analisti si erano spinti a ipotizzare una quotazione a 100 miliardi di dollari. Il giorno del debutto, il primo per un player legato al mondo crypto, il valore di mercato è stato di 85 miliardi di dollari.

coinbase

Oltre alla rilevanza di questa notizia per il settore, l'occasione si è rivelata utile anche per comparare la capitalizzazione di Coinbase con quello di soggetti istituzionali bancari. Se è infatti vero che la società di Armstrong ha visto scendere il proprio valore di mercato subito dopo il debutto in Borsa intorno ai 60/65 miliardi di dollari per chiudere il Q2 a 45 miliardi, d'altra parte queste cifre la pongono comunque all'interno della top 10 delle principali banche europee per capitalizzazione.

Anche Kraken guarda alla quotazione, messa in programma per il 2022. Come si legge su Bloomberg, il fondatore dell'exchange Jesse Powell ha parlato di una valutazione della società intorno ai 10 miliardi di dollari. Mentre a inizio giugno il valore continuava a scendere, Powell ha pubblicato un tweet in cui dichiarava di avere comprato Bitcoin («Mi sembrava irresponsabile non farlo», ha aggiunto). Non c'è dunque soltanto Musk a utilizzare i social: buona parte dei personaggi pubblici utilizzano i social network per comunicare.

kraken



Jesse Powell

Nel frattempo altri exchange come Gemini e Bitstamp non hanno ancora parlato di quotazione all'orizzonte.

Il secondo semestre 2021 parla anche un po' italiano per quel che riguarda l'ambito exchange. A fine giugno, infatti, la startup Young Platform, fondata nel 2018 da sei studenti di informatica del Politecnico di Torino, ha chiuso un aumento di capitale da 3,5 milioni di euro, per una valutazione aziendale di 18,5 milioni.

Young Platform

## Borse di scambio

[theblockcrypto.com/post/101493/coinbase-direct-listing-what-you-should-expect](https://theblockcrypto.com/post/101493/coinbase-direct-listing-what-you-should-expect)  
[washingtonpost.com/business/2021/04/14/coinbase-ipo-crypto-bitcoin](https://washingtonpost.com/business/2021/04/14/coinbase-ipo-crypto-bitcoin)  
[forbes.it/2021/04/13/coinbase-quota-borsa-storia-fondatore-brian-armstrong](https://forbes.it/2021/04/13/coinbase-quota-borsa-storia-fondatore-brian-armstrong)  
[statista.com/statistics/382818/leading-banks-in-europe-by-market-capitalization](https://statista.com/statistics/382818/leading-banks-in-europe-by-market-capitalization)  
[bloomberg.com/news/articles/2021-06-17/kraken-ceo-says-crypto-exchange-could-go-public-in-12-18-months](https://bloomberg.com/news/articles/2021-06-17/kraken-ceo-says-crypto-exchange-could-go-public-in-12-18-months)  
[twitter.com/jespow/status/1402522405906509826](https://twitter.com/jespow/status/1402522405906509826)  
[startupitalia.eu/158541-20210628-round-di-serie-a-da-35-milioni-di-euro-per-young-platform](https://startupitalia.eu/158541-20210628-round-di-serie-a-da-35-milioni-di-euro-per-young-platform)  
[theblockcrypto.com/post/109766/uk-fca-bans-crypto-exchange-binance](https://theblockcrypto.com/post/109766/uk-fca-bans-crypto-exchange-binance)  
[theblockcrypto.com/linked/106654/crypto-exchange-volume-2-trillion-may-highest-history](https://theblockcrypto.com/linked/106654/crypto-exchange-volume-2-trillion-may-highest-history)

Continua invece il maltempo su Binance, exchange che già nel primo trimestre aveva scelto di impiegare esperti del mondo istituzionale per migliorare la propria reputazione e la relazione con i regolatori. A fine giugno la Financial Conduct Authority della Gran Bretagna, la Consob d'Oltremarica, ha ordinato alla società di bloccare tutte le operazioni entro la fine del mese.

Per chiudere l'analisi del secondo trimestre per le borse di scambio, rilevanti i dati sugli scambi complessivi: in maggio è stato record storico con 2 trilioni di dollari a livello mondiale.



## Influenze sul mercato

Anche nel secondo trimestre del 2021 c'è spazio per analizzare le uscite social dei più importanti influencer del mondo cypto. Perfino la stampa generalista ha inseguito i tweet di Elon Musk che, dopo l'annuncio dell'investimento da 1,5 miliardi di dollari di Tesla in Bitcoin, ha fatto poi marcia indietro sempre con un cinguettio nel quale si rammaricava dell'impronta troppo gravosa della criptomoneta sull'ambiente. D'altra parte il Q2 è stato caratterizzato anche dalle performance senza precedenti di Dogecoin, spinte dallo stesso Elon Musk con una campagna social che, in un mercato tradizionale, rischierebbe le accuse di aggraffaggio. L'esposizione mediatica del Ceo di SpaceX gli ha assicurato anche l'attenzione da parte di Anonymus, che a inizio giugno ha pubblicato un video in cui si scaglia contro l'imprenditore con minacce neanche troppo velate.



Elon Musk

Un altro personaggio pubblico che utilizza il megafono di Twitter per comunicare è Micheal Saylor, amministratore delegato di MicroStrategy, società informatica quotata al Nasdaq, che ha investito buona parte della propria tesoreria in Bitcoin, dando un segnale su una possibile strada soprattutto al mondo delle aziende. Invitato

al Parallel Summit 2021, Saylor ha dichiarato quanto segue in merito a Bitcoin: «Non credo esista nessun altro asset dove ogni persona intelligente in grado di capirlo decide di fare tutto il possibile per renderlo più prezioso». In un altro tweet è tornato sulla questione dicendo che «tutti stanno aumentando il valore dei vostri Bitcoin».

Ma non c'è soltanto Twitter. Nel Q2 anche YouTube è diventato un megafono per Bitcoin se si va a guardare l'effetto avuto dal video in cui l'investitore e miliardario Paul Tudor Jones ha dichiarato il proprio amore. Il suo «I like Bitcoin. Cash is trash.» ha dato una spinta alle performance della criptovaluta. Come ha spiegato, il beneficio che garantisce un investimento in Bitcoin si apprezza ancor di più in

“  
I like Bitcoin.  
Cash is trash.”

un momento come quello attuale, inflattivo a causa dell'immissione di liquidità da parte delle banche centrali alle prese con gli effetti della crisi pandemica.



Paul Tudor Jones

## Influenze sul mercato

[youtu.be/UG07x3aN3b0](https://youtu.be/UG07x3aN3b0)

[twitter.com/michael\\_saylor/status/1408414572441214986](https://twitter.com/michael_saylor/status/1408414572441214986)

[twitter.com/DigitalChamber/status/1405693685505794054](https://twitter.com/DigitalChamber/status/1405693685505794054)

[twitter.com/michael\\_saylor/status/1405676137221705737](https://twitter.com/michael_saylor/status/1405676137221705737)

[cnbc.com/2021/06/14/paul-tudor-jones-says-bet-heavily-on-every-inflation-trade-if-fed-keeps-ignoring-higher-prices.html](https://cnbc.com/2021/06/14/paul-tudor-jones-says-bet-heavily-on-every-inflation-trade-if-fed-keeps-ignoring-higher-prices.html)

[coindesk.com/consensus-ray-dalio-i-have-some-bitcoin](https://coindesk.com/consensus-ray-dalio-i-have-some-bitcoin)

Proseguendo nel mondo degli influencer crypto il Q2 assegna un posto di rilievo anche a Ray Dalio, nome di rilievo nel mondo hedge fund, il quale ha dichiarato di aver “qualche Bitcoin”; così come a George Soros, uno dei volti simbolo del capitalismo, che avrebbe investito in Bitcoin come si legge sulla stampa di settore; c'è infine da citare le mosse di Ricardo Salinas, proprietario della banca messicana Banco Azteca che potrebbe iniziare ad accettare Bitcoin. La dichiarazione è arrivata poche settimane dopo l'approvazione della Bitcoin law in El Salvador.

## Il caso El Salvador

### Bitcoin come moneta a corso legale

Tra le notizie che mescolano colore e sostanza, c'è senz'altro la novità che arriva da El Salvador. Il minuscolo paese centro americano, che non ha una valuta nazionale, affiancherà al dollaro americano il Bitcoin da settembre. Si tratta del primo caso al mondo in cui uno stato sovrano decide di trasformare la criptovaluta in una valuta legale. Il 9 giugno il presidente Nayib Bukele, classe 1981, ha annunciato con un tweet l'approvazione storica della Bitcoin Law per 62 voti su 84. In un post di qualche giorno prima il capo di stato spiegava che, data la capitalizzazione di mercato di Bitcoin a 680 miliardi di dollari, se l'1% di questo valore venisse investito in El Salvador questo farebbe crescere il prodotto interno lordo del 25%.



Nayib Bukele

Più che gli investimenti, il tema chiave è in realtà quello delle rimesse dall'estero: in una economia basata fondamentalmente sui flussi economici (circa 6 miliardi di dollari, oltre il 20% del prodotto interno lordo) proveniente dai lavoratori emigrati, la possibilità di trasferire questo valore utilizzando Bitcoin consentirebbe di ridurre i costi degli intermediari ed inciterebbe al risparmio. L'introduzione del Bitcoin come valuta legale non significa, infatti, che questa verrà utilizzata per le compere di tutti i giorni. Le prospettive sono altre: gli investimenti dei cittadini, invece che in dollari, potrebbero essere convertiti (o mantenuti) in una moneta con performance che crescono anno dopo anno.

Nella partita di El Salvador ha giocato un ruolo decisivo Jack Mallers, amministratore delegato di Zap (app che consente i pagamenti in Bitcoin). Il suo è senz'altro uno dei nomi che hanno spinto di più per far sì che il paese adottasse una strada pionieristica in materia di istituzionalizzazione del mondo crypto. Il suo tweet che celebra l'approvazione della legge recita così: “Un piccolo passo per Bitcoin, un grande salto per l'umanità.”. In chiusura di trimestre Mallers è stato invitato in diverse trasmissioni USA per commentare questa novità.



Jack Mallers

Restano comunque incertezze legate, per esempio, alla scarsa copertura del digitale nel paese centroamericano: secondo uno studio di Microsoft e della Interamerican Development Bank, El Salvador sarebbe il secondo stato con la più bassa penetrazione di internet dell'America Latina (nelle zone rurali solo il 10% ha accesso alla rete). Da parte sua, l'app Zap pensa di poter ingolosire i risparmiatori con 30 dollari di welcome bonus.

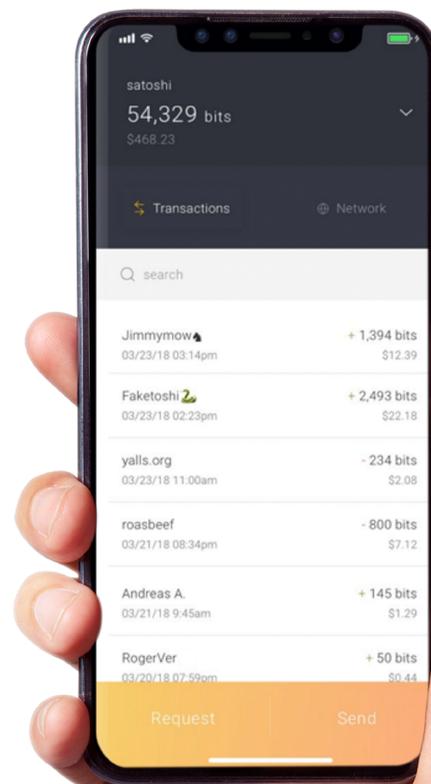
“

*Un piccolo passo per Bitcoin,  
un grande salto per l'umanità.*

”

I commenti da parte delle istituzioni finanziarie non si sono fatti attendere. Il Fondo Monetario Internazionale ha commentato attraverso Gerry Rice, direttore della comunicazione: «L'adozione del Bitcoin come moneta

a corso legale solleva una serie di questioni macroeconomiche, finanziarie e legali che richiedono un'analisi molto attenta. Stiamo seguendo da vicino gli sviluppi e continueremo la nostra consultazione con le autorità». Allo stesso modo la Banca Mondiale ha rifiutato la richiesta di aiuto di El Salvador per implementare Bitcoin nel proprio sistema valutario.



L'app ZAP

## Il caso El Salvador: Bitcoin come moneta a corso legale

[twitter.com/nayibbukele/status/1402507224916836352](https://twitter.com/nayibbukele/status/1402507224916836352)

[twitter.com/nayibbukele/status/1401335885497524226](https://twitter.com/nayibbukele/status/1401335885497524226)

[bbc.com/news/world-latin-america-57373058](https://bbc.com/news/world-latin-america-57373058)

[twitter.com/jackmallers/status/1402500978662952964](https://twitter.com/jackmallers/status/1402500978662952964)

[youtube.com/watch?v=4tLo74533xc](https://youtube.com/watch?v=4tLo74533xc)

[bbc.com/news/business-57507386](https://bbc.com/news/business-57507386)

## Bitcoin e servizi finanziari

Nel Q2 la notizia da segnalare per quel che riguarda i servizi finanziari è quella di un sondaggio di Intertrust Group secondo il quale un Hedge Fund su sei (ne sono stati intervistati 100) sarebbe intenzionato a investire oltre il 10% delle proprie risorse in crypto entro i prossimi cinque anni. Come sempre i numeri vengono interpretati a seconda delle fazioni: per i critici, infatti, il fatto che cinque su sei ancora non si espongano in questo settore varrebbe come conferma del proprio scetticismo.



D'altra parte è in situazioni simili che si nota la lungimiranza di alcuni attori istituzionali d'Oltreoceano: Goldman Sachs, BBVA, Morgan Stanley, State Street, Standard Chartered e JP Morgan sono soltanto alcuni dei nomi di peso che

hanno aperto le porte a servizi finanziari di brokeraggio o custody legati al mondo crypto. La distanza tra quanto accade negli Stati Uniti e il Vecchio Continente è ancora più evidente se si paragonano queste scelte alle posizioni di soggetti europei come HSBC, il cui amministratore delegato ha dichiarato che Bitcoin «non fa per noi».

Per il capitolo custodian il Q2 si è chiuso con importanti operazioni. Galaxy Digital ha acquisito per 1,2 miliardi di dollari BitGo, il più autorevole custodian operante sul mercato, che in precedenza era stato lungamente corteggiato da PayPal; c'è stato movimento anche in Europa, con il round Serie B da 50 milioni di dollari di Copper.co e il Serie A di Finoa a 22 milioni di dollari. Infine, segnaliamo che l'italiana CheckSig ha ottenuto le attestazioni SOC 1 e SOC 2 da Deloitte.



## I digital asset nel mondo finanziario europeo di Andrea Cattaneo

Andrea Cattaneo, General Manager Italy e Head of Italy, Switzerland & Iberia di BNP Paribas Securities Services, è intervenuto alla presentazione del nostro report trimestrale: "Il mondo degli asset digitali è un ambito di grande interesse per tutte le



Andrea Cattaneo

istituzioni finanziarie che oggi tuttavia sconta differenti tipologie di asset, un track record relativamente breve, un contesto normativo ancora in divenire e difficoltà a comprendere e misurare i rischi, anche reputazionali. Rispetto al mercato statunitense, il sistema finanziario europeo e ancor più quello italiano sono oggi in una fase di cauta esplorazione, focalizzata soprattutto su servizi ancillari. Ci si attende tuttavia un significativo cambio di passo con l'approvazione del regolamento europeo MiCA (Markets in Crypto-assets)."

Il suo intervento integrale è disponibile nel video completo della presentazione del report trimestrale: [youtu.be/RP3Pd0aKous](https://youtu.be/RP3Pd0aKous)

## Bitcoin e servizi finanziari

[blockworks.co/survey-1-in-6-hedge-funds-plan-to-invest-in-crypto-in-5-years](https://blockworks.co/survey-1-in-6-hedge-funds-plan-to-invest-in-crypto-in-5-years)  
[itpro.co.uk/technology/cryptocurrencies/359648/hsbc-not-into-Bitcoin-says-ceo](https://itpro.co.uk/technology/cryptocurrencies/359648/hsbc-not-into-Bitcoin-says-ceo)  
[coindesk.com/galaxy-digital-to-buy-bitgo-for-about-1-2-billion-in-stock-cash](https://coindesk.com/galaxy-digital-to-buy-bitgo-for-about-1-2-billion-in-stock-cash)  
[copper.co/insights/crypto-scaleup-copper-co-secures-50-million-series-b-investment-co-led-by-dawn-capital-and-target-global](https://copper.co/insights/crypto-scaleup-copper-co-secures-50-million-series-b-investment-co-led-by-dawn-capital-and-target-global)  
[checksig.io/news](https://checksig.io/news)

## Ransomware

### Il caso Colonial Pipeline

Pochi anni dopo WannaCry, si torna a parlare di ransomware, ovvero di un virus che cifra i dati di una rete di computer, chiedendo un riscatto in criptovalute per lo sblocco. A inizio maggio gli Stati Uniti hanno lanciato l'allarme dopo che la Colonial Pipeline, ovvero uno dei più grandi oleodotti del paese che alimenta città come New York e Atlanta, è caduta vittima di un attacco hacker con pochi precedenti. Questi software malevoli devono il loro nome proprio al ransom, ovvero al riscatto che occorre pagare per risolvere la situazione. All'epoca di WannaCry – migliaia di computer colpiti in 150 paesi giro di una manciata di ore – il riscatto richiesto dai criminali era stato di appena 130mila dollari a fronte dell'utilizzo di quattro zero day vulnerability, bug del sistema operativo Windows, del valore di mercato di alcuni milioni di dollari. Circostanze che hanno reso evidente quanto, pochi anni fa, l'obiettivo del ransomware non fosse tanto il riscatto, quanto invece lo spionaggio industriale.



Il caso della Colonial Pipeline spalanca le porte su un'evoluzione del ransomware verso una logica di ransomware as a service (raas). Se le aziende tradizionali si avvantaggiano del software as a service (saas) come piattaforma esterna, con conseguente risparmio in termini di investimenti, i criminali informatici dispongono a loro volta di strumenti analoghi in grado di creare ingenti danni su vasta scala. Nel caso USA i criminali hanno richiesto un riscatto di quasi 64 Bitcoin (del valore di oltre 4 milioni di dollari in quei giorni di fuoco), somma che l'FBI è poi riuscita a recuperare in un secondo momento visto che i criminali avevano utilizzato un wallet Bitcoin in cloud, ingenuità clamorosa per hacker informatici che dovrebbero essere sofisticati. Una storia a lieto fine che però ha scosso le stesse istituzioni della società, con l'amministratore delegato della società Joseph Blount che ha giustificato la scelta di pagare il riscatto per riattivare l'attività dell'oleodotto. «Ho deciso di pagare e di mantenere le informazioni il più riservate possibile - ha detto Blount - È stata la decisione più difficile che ho preso nei miei 39 anni nell'industria energetica». Oltre all'esigenza di migliorare la preparazione di aziende e cittadini alla sicurezza informatica, questa vicenda arricchisce anche il quadro sui nemici che abbiamo di fronte. Il rocambolesco esito del bottino recuperato dall'FBI a colpo concluso conferma come la trasparenza blockchain favorisca gli investigatori e, almeno in questo caso, svela quanto questi criminali informatici non siano i più astuti su piazza. Nel mucchio, infatti, ci sono anche parecchi teppistelli. Sono le armi che hanno, non loro, a doverci preoccupare.



Joseph Blount

### Ransomware: il caso Colonial Pipeline

[techcrunch.com/2019/05/12/wannacry-two-years-on](https://techcrunch.com/2019/05/12/wannacry-two-years-on)

[zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business](https://zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business)

## Criptovalute e attività criminali

A seguito dell'attacco ransomware alla Colonial Pipeline si è tornati anche a parlare del presunto legame tra Bitcoin e la criminalità. Se è infatti vero che c'è stata una richiesta di pagamento del riscatto in criptovalute, questo non significa che simili attività siano così diffuse come si vuole far credere per screditare Bitcoin. Come spiega il report annuale di Chainalysis, che fotografa l'ecosistema blockchain dal punto di vista criminale, "la criminalità legata alla criptovaluta sta diminuendo: rimane una piccola parte dell'economia complessiva delle criptovalute ed è relativamente inferiore alla quantità di fondi illeciti coinvolti nella finanza tradizionale". In numeri, l'ordine di grandezza parla della quota illecita delle attività allo 0,34% nel 2020 (pari a circa 10 miliardi di dollari).

“

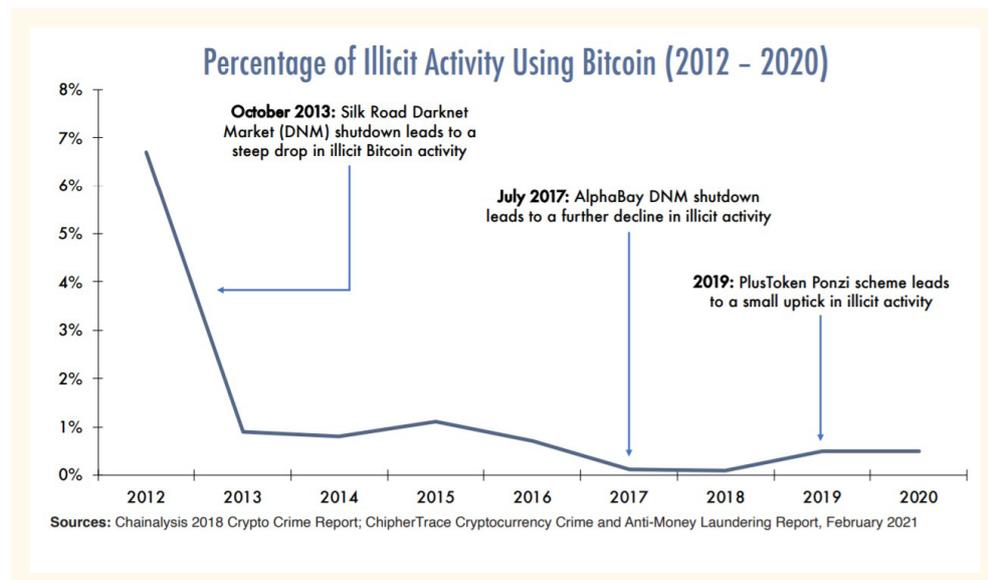
*La criminalità legata alla criptovaluta sta diminuendo.*

”

I dati in questione sono quelli che hanno in mano le forze dell'ordine che si occupano di crimine informatico e che, visti i numeri, non hanno elementi per dire che Bitcoin offra un terreno fertile per il crimine. A rafforzare questa visione c'è anche il dato pubblicato nel National risk assessment of money laundering 2020 voluto dal Governo inglese: i cryptoasset sono classificati a rischio medio (in crescita rispetto all'edizione precedente), ma restano comunque più sicuri rispetto all'intero sistema bancario tradizionale. Nonostante questo, resiste ancora la visione del mondo crypto associato al crimine: Janet Yellen, segretario al Tesoro degli Stati Uniti, e Christine Lagarde, presidente della Banca Centrale Europea, hanno allertato paesi e risparmiatori sull'uso criminoso di Bitcoin, che può spingersi, secondo le loro informazioni, addirittura fino al finanziamento di organizzazioni terroristiche.

Non tutto il mondo istituzionale tuona contro e vede solo i rischi del mondo crypto. Ad esempio Michael Morrell, ex direttore della CIA, ha firmato un'analisi dalla quale emerge che "l'uso di Bitcoin in attività illecite è relativamente limitato". Se si guarda al periodo tra il 2017 e il 2020 la percentuale di operazioni criminali effettuate via crypto hanno riguardato meno dell'1% dei volumi totali scambiati con questa modalità. Sempre Morrell aggiunge che, a differenza delle truffe della finanza tradizionale, nel caso dei Bitcoin la tracciabilità dei movimenti è garantita e funge da deterrente.

Non tutto il mondo istituzionale tuona contro e vede solo i rischi del mondo crypto.



## Criptovalute e attività criminali

[finance.yahoo.com/news/jerome-powell-dismisses-cryptocurrencies-speculative-163949463.html](https://finance.yahoo.com/news/jerome-powell-dismisses-cryptocurrencies-speculative-163949463.html)  
[we-wealth.com/news/fintech/blockchain/bitcoin-e-il-paradiso-dei-criminali-finanziari-i-neri-suggeriscono-il-contrario](https://we-wealth.com/news/fintech/blockchain/bitcoin-e-il-paradiso-dei-criminali-finanziari-i-neri-suggeriscono-il-contrario)  
[cnbc.com/2021/04/12/bitcoin-kraken-ceo-jesse-powell-warns-of-cryptocurrency-crackdown.html](https://cnbc.com/2021/04/12/bitcoin-kraken-ceo-jesse-powell-warns-of-cryptocurrency-crackdown.html)  
[cryptoforinnovation.org/resources/Analysis\\_of\\_Bitcoin\\_in\\_Illicit\\_Finance.pdf](https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf)

## NFT

### Un trend sostenibile?

Il primo trimestre del 2021 ha segnato una fiammata per gli NFT, i Non-Fungible Token che si sono guadagnati anche l'attenzione della stampa generalista.

La vendita di un'opera dell'artista digitale americano Beeple per quasi 70 milioni di dollari all'asta è sembrata per molti la prima di una lunga serie. Il Q2 del 2021, a parte qualche notizia di colore come quella sull'NFT del meme Disaster Girl venduto per mezzo milione di dollari, non ha visto grossi fuochi d'artificio. Sul sito nonfungible.com sono disponibili i grafici che confermano quanto nel secondo trimestre dell'anno i dollari scambiati sul mercato NFT siano scesi dal picco di maggio. Preannunciato

come un nuovo trend in ascesa, questo strumento ha aperto le porte a nuova forma di collezionismo. Vedremo se si tratta di un trend duraturo e sostenibile.



Love is in the Air - Banksy

In questo scenario case d'asta con secoli di storia alle spalle come la britannica Sotheby's ha compiuto un passo importante con la vendita di un diamante a Hong Kong, pagato in criptovalute (non è chiaro se in Bitcoin o Ether, entrambe accettate dalla società) per un valore complessivo di 12,3 milioni di dollari; questa notizia è arrivata qualche mese dopo l'iniziativa simile, sempre in casa Sotheby's, che ha riguardato il capolavoro dello street artist Banksy "Love is in the air".

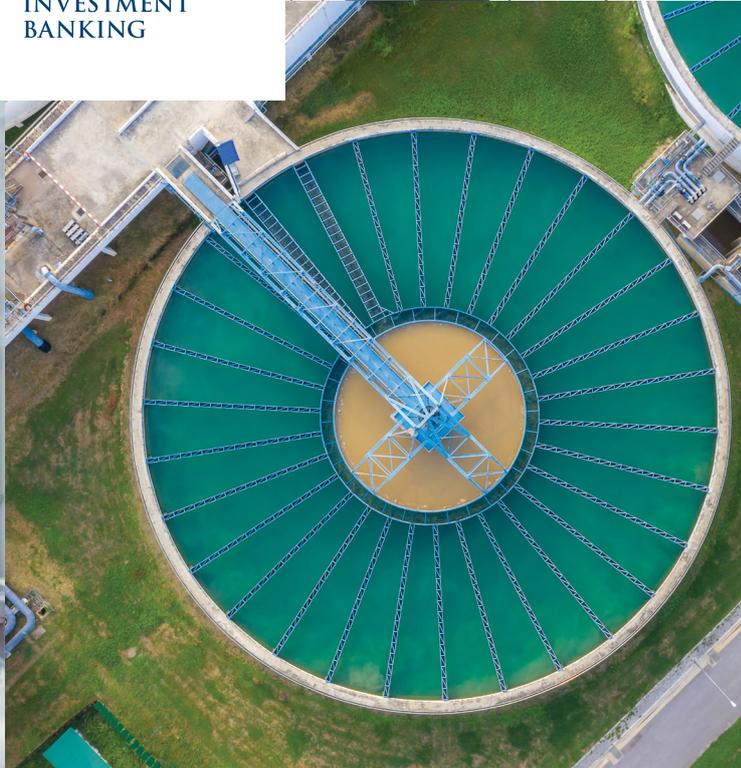
“  
Abbiamo riscontrato un crescente interesse tra i collezionisti verso opzioni di pagamento più semplici per concludere affari con Sotheby's.  
”

Sotheby's

A spingere la casa d'aste ad accettare pagamenti in criptovalute è proprio la volontà di ampliare la propria clientela. «Abbiamo riscontrato un crescente interesse tra i collezionisti verso opzioni di pagamento più semplici per concludere affari con Sotheby's», ha dichiarato Stefan Pepe, Chief Technology Officer del gruppo.

### NFT: un trend globale

[nytimes.com/2021/04/29/arts/disaster-girl-meme-nft.html](https://nytimes.com/2021/04/29/arts/disaster-girl-meme-nft.html)  
[nonfungible.com/market/history](https://nonfungible.com/market/history)  
[theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq](https://theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq)  
[coindesk.com/sothebys-sells-rare-diamond-for-12-3m-in-crypto](https://coindesk.com/sothebys-sells-rare-diamond-for-12-3m-in-crypto)



**IMI** | CORPORATE & INVESTMENT BANKING

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](http://imi.intesasanpaolo.com)



# REGOLAZIONE



## Central Bank Digital Currency

### Banca Centrale Europea

Nel campo della Central Bank Digital Currency continua il lavoro incessante a livello globale, con diversi istituti centrali al lavoro su una valuta digitale. Da notare



Christine Lagarde

la Banca Centrale Svizzera che si è sfilata, dichiarando di non essere interessata. Sul fronte della Banca Centrale Europea ci sono passi avanti sul cantiere euro digitale. «Sono passati nove mesi da quando abbiamo pubblicato il nostro rapporto sull'euro digitale – ha spiegato la presidente della BCE, Christine Lagarde - In questo lasso di tempo abbiamo condotto ulteriori analisi, chiesto il contributo di cittadini e professionisti e condotto alcuni esperimenti, con risultati incoraggianti. Tutto questo ci ha portato a decidere di fare un passo avanti e avviare il progetto dell'euro digitale. 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, ovvero quella della banca centrale». Sul tema evidenziamo anche l'intervento di Fabio Panetta, membro della BCE e guida della task force sull'euro digitale: «Ci impegneremo con il Parlamento europeo e altri decisori e li

informeremo regolarmente sui nostri risultati. Anche i cittadini, i commercianti e l'industria dei pagamenti saranno coinvolti».

## I regolatori

### Il contesto globale

Il contesto globale dal punto di vista dei regolatori vede un trimestre segnato dal brusco stop cinese, che ha bloccato qualsiasi forma di movimento crypto. A stabilirlo è stata la People's Bank of China, la cui posizione sembra essere condivisa anche dal governo messicano. Il ministro delle finanze, Arturo Herrera, ha infatti dichiarato che le criptovalute non diventeranno mai



Arturo Herrera

valuta legale, come accaduto invece un po' più a sud, a El Salvador. La decisione del Messico è arrivata poco dopo l'annuncio di Solinas, numero 1 di Banco Azteca, di aprire alle criptovalute.

Continuano i lavori della Financial Action Task Force (FATF), gruppo sovranazionale creato per contrastare il riciclaggio e il finanziamento del terrorismo. Da questo tavolo è infatti arrivato un aggiornamento alle linee guida che, però, ancora peccano di un difetto strutturale. Si vogliono infatti ancora applicare ai crypto-asset gli standard del mondo tradizionale, col rischio non soltanto di risultare inefficaci, ma anche di spingere fuori mercato gli operatori che tentano di muoversi in adeguatezza regolamentare, alimentando di conseguenza lo scenario da Far West.



## Central Bank Digital Currency: Banca Centrale Europea

[coindesk.com/swiss-national-bank-has-no-plans-for-a-digital-currency-report](https://coindesk.com/swiss-national-bank-has-no-plans-for-a-digital-currency-report)  
[www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html](https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html)

## I regolatori

### Consob e Banca d'Italia

La notizia del trimestre per quanto riguarda i regolatori in Italia è la presa di posizione pubblica e netta da parte di Banca d'Italia e Consob sui crypto-asset. Con un comunicato stampa congiunto rilasciato il 28 aprile entrambe avvertono e “richiamano l'attenzione della collettività, e in particolare dei piccoli risparmiatori, sugli elevati rischi connessi con l'operatività in crypto-attività (crypto-asset) che possono comportare la perdita integrale delle somme di denaro utilizzate”.

Il problema di fondo tuttavia sta però in un'altra parte del comunicato, quando i regolatori dicono che “in assenza di un quadro regolamentare di riferimento, l'operatività in crypto-attività presenta rischi di diversa natura”. A questo punto la memoria deve tornare al 2014, quando era stata la stessa Autorità Bancaria Europea a dissuadere i singoli paesi dall'autorizzare Bitcoin fin tanto che non fosse stato introdotto un framework legale. È evidente che in tutti questi anni, complici anche il fumo negli occhi delle alt-coin e shit-coin che si sono diffusi come funghi, alla fine si sia preferito marginalizzare Bitcoin invece di inquadralo dal punto di vista legale.

Il comunicato stampa chiude con una frase che suona come sentenza di condanna: “Anche l'adesione a offerte di prodotti finanziari correlati a crypto-attività, quali ad esempio i cd. digital token, è un investimento altamente rischioso, tanto più qualora, come spesso riscontrato, le offerte siano effettuate da operatori abusivi, non autorizzati, non regolati e non vigilati da alcuna Autorità”.



Paolo Savona

Lato Consob, l'intervento del presidente Paolo Savona all'incontro annuale con il mercato finanziario è stato eloquente perché ha mostrato le ampie resistenze che ancora in Italia vi sono contro Bitcoin, buttato nel calderone dei cryptoasset senza distinzioni. Come ha spiegato Savona «l'informatica finanziaria è una lampada prodigiosa dalla quale è uscito il Genio. Le autorità non riusciranno a riportarlo dentro, perché esso agisce nella sfera

immateriale controllabile solo cambiando protocollo di scambio delle informazioni, ossia frammentando l'unità del mercato mondiale e così riducendo il saggio di competitività internazionale». Nel suo intervento si è inoltre spinto a prefigurare uno scenario da mutui subprime per l'ecosistema crypto con un effetto a valanga sul mercato.

“  
L'informatica finanziaria è una  
lampada prodigiosa dalla quale è  
uscito il Genio.  
”

### I regolatori: il contesto globale, Consob e Banca d'Italia

[nasdaq.com/articles/mexicos-finance-minister-confirms-cryptos-are-banned-from-financial-system-2021-06-28](https://nasdaq.com/articles/mexicos-finance-minister-confirms-cryptos-are-banned-from-financial-system-2021-06-28)  
[jdsupra.com/legalnews/fatf-releases-proposed-updates-to-5409624](https://jdsupra.com/legalnews/fatf-releases-proposed-updates-to-5409624)  
[www.bancaditalia.it/media/comunicati/documenti/2021-01/CS\\_Congiunto\\_BI\\_CONSOB\\_cryptoasset.pdf](https://www.bancaditalia.it/media/comunicati/documenti/2021-01/CS_Congiunto_BI_CONSOB_cryptoasset.pdf)  
[youtube.com/watch?v=quog0hRclSg&](https://youtube.com/watch?v=quog0hRclSg&)

# DA OLTRE 50 ANNI INVESTIAMO SUL FUTURO.



I nostri private banker: Marco, Paola, Sandro, Nevia, Sergio.

Il valore di un solido domani è frutto delle scelte di oggi.

Per questo Fideuram, la prima Private Bank in Italia e leader in Europa, conosce appieno l'importanza di essere vicini ai clienti nei momenti che contano, attraverso una consulenza esclusiva fondata su fiducia, solidità ed esperienza.



# TECNOLOGIA



## Protocollo Bitcoin

### Luce verde per Taproot

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*, 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 per l'approvazione di *SegWit*, il precedente aggiornamento protocollare: si era trattato nel 2015-2017 di un processo estremamente contenzioso e che ha dato vita all'*hard fork* di Bitcoin Cash (se 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).

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 presenteremo approfondimenti in tal senso.

### Protocollo Bitcoin: luce verde per Taproot

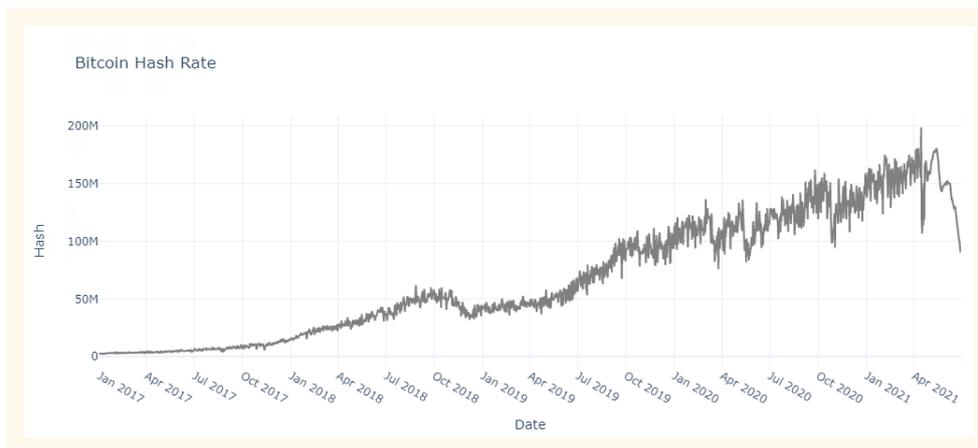
[coindesk.com/locked-in-bitcoin-taproot-upgrade-gets-activation-mandate](https://coindesk.com/locked-in-bitcoin-taproot-upgrade-gets-activation-mandate)  
[bitcoinmagazine.com/technical/taproot-locks-in](https://bitcoinmagazine.com/technical/taproot-locks-in)  
[bitcoinmagazine.com/technical/taproot-activates-massive-upgrade](https://bitcoinmagazine.com/technical/taproot-activates-massive-upgrade)  
[river.com/learn/what-is-taproot](https://river.com/learn/what-is-taproot)  
[bitcoinops.org/en/topics/taproot](https://bitcoinops.org/en/topics/taproot)

## Mining

### La migrazione dell'hashrate

La notizia che ha sconvolto il settore mining è esplosa a fine giugno, con la scelta della Cina di vietarlo. Il gigante asiatico era da tempo riconosciuto come il principale paese in cui si svolgeva questa attività cruciale per l'ecosistema e, tra le novità provenienti da Pechino, si è aggiunta anche quella del blocco di tutte le transazioni crypto. Secondo alcuni osservatori la scelta avrebbe potuto essere stata ispirata dal presunto inquinamento provocato da Bitcoin: dal momento che Pechino sta seguendo la propria strada verso la sostenibilità, al Partito deve essere sembrato indiscutibile l'inserimento della criptomoneta nella lista nera.

Nel frattempo si sono già candidati altri paesi vicini, come il Kazakistan, pronti ad accogliere le mining farm orfane della Cina. Nelle ore decisive per il mining, su Twitter c'è stato chi ha addirittura fotografato il crollo delle attività con i server incasottati proprio come durante un trasloco. Resta ancora da capire dove si indirizzerà il settore che, finora, aveva visto il dominio cinese (con gli USA che inseguivano). Tra le conseguenze del divieto segnaliamo la scelta di Bitmain, principale produttore di hardware dedicato al mining, di bloccare le vendite di nuovi dispositivi, per evitare la concorrenza con l'usato che sta inondando il mercato.



A fine giugno si è continuato a registrare il crollo dell'hashrate, ovvero della potenza computazionale. La stretta cinese ha avuto impatti su tutte le aziende coinvolte nel settore; ad esempio, BTC China, uno dei principali exchange del paese, si è vista costretta ad abbandonare qualsiasi velleità di business nel paese. Discorso analogo anche per l'azienda cinese Huobi, impegnata sia nel trading sia nel mining. E le conseguenze non potevano non arrivare a cascata anche sugli immensi bacini idroelettrici che hanno finora garantito prosperità al settore in Cina e che oggi lamentano una perdita di profittabilità.

Di fronte a questo scenario gli esperti si sono subito esercitati con le previsioni: si puntano gli occhi sul Nord America, dove ci si aspetta un aumento delle attività di mining ora che la Cina ha alzato i muri. Prendiamo dunque a prestito un'espressione di Nic Carter, che su Coindesk ha dichiarato "the hashrate migration is real".

### Mining: la migrazione dell'hashrate

[www.theglobeandmail.com/business/international-business/article-bitcoin-falls-almost-10-in-wake-of-chinas-deepening-crackdown-on](http://www.theglobeandmail.com/business/international-business/article-bitcoin-falls-almost-10-in-wake-of-chinas-deepening-crackdown-on)

[twitter.com/bigmagicdao/status/1406181039265902592](https://twitter.com/bigmagicdao/status/1406181039265902592)

[decrypt.co/74343/bitmain-suspends-sales-bitcoin-mining-machine-amid-china-crackdown](https://decrypt.co/74343/bitmain-suspends-sales-bitcoin-mining-machine-amid-china-crackdown)

[coindesk.com/Bitcoin-unpacking-hashrate-nic-cart-migration](https://coindesk.com/Bitcoin-unpacking-hashrate-nic-cart-migration)

[smp.com/tech/policy/article/3138618/btcchina-countrys-first-bitcoin-exchange-gives-cryptocurrency-amid](https://smp.com/tech/policy/article/3138618/btcchina-countrys-first-bitcoin-exchange-gives-cryptocurrency-amid)

## Mining

### Sostenibilità ambientale

Quando il 13 maggio Elon Musk ha pubblicato un tweet in cui spiegava le ragioni del dietro front sui pagamenti in Bitcoin per gli acquisti di Tesla, si è tornati a parlare

dell'impatto ambientale dell'ecosistema crypto, sempre più spesso accusato di inquinare tanto quanto interi paesi. Se è vero che il mining (nella fattispecie l'hashrate, ovvero la potenza di calcolo combinata totale utilizzata per estrarre le monete) ha una carbon footprint misurabile e misurata, è opportuno analizzare anche i passi avanti che il settore ha fatto, soprattutto in un'ottica di ricerca delle fonti sostenibili. Stando al Cambridge Center for Alternative Finance – fonte di riferimento in questo caso – nel 2019 il 73% del consumo di energia di Bitcoin sarebbe stato a emissioni zero, dal momento che la maggior parte del mining – che avviene in Cina – utilizza l'energia idroelettrica. Trattandosi di un'attività sparsa in tutto il mondo i numeri sono sempre ballerini, ma anche le stime più caute lasciano intendere che una buona fetta dei consumi provenga da fonti rinnovabili. In altre parole, non è certo l'ambito Bitcoin quello che, in percentuale, inquina di più al mondo.



Circa 150 terawattora è il costo in termini di energia richiesto ogni anno da Bitcoin. Si parla dello 0,69% del consumo complessivo globale. Una delle future terre promesse per la sostenibilità crypto potrebbe essere localizzata in Cina, precisamente nelle regioni di Sichuan e di Yunnan: qui lo spreco di energia idroelettrica pulita è enorme e questa offerta di energia non ha ancora incontrato una domanda adeguata. In uno studio dell'Harvard Business Review si sottolinea che «queste regioni molto probabilmente rappresentano la



**Elon Musk** @elonmusk

Tesla & Bitcoin

Tesla has suspended vehicle purchases using Bitcoin. We are concerned about rapidly increasing use of fossil fuels for Bitcoin mining and transactions, especially coal, which has the worst emissions of any fuel.

Cryptocurrency is a good idea on many levels and we believe it has a promising future, but this cannot come at great cost to the environment.

Tesla will not be selling any Bitcoin and we intend to use it for transactions as soon as mining transitions to more sustainable energy. We are also looking at other cryptocurrencies that use <1% of Bitcoin's energy/transaction.

12:06 AM · May 13, 2021 · Twitter for iPhone

77.3K Retweets 50.2K Quote Tweets 506.2K Likes

**Elon Musk** @elonmusk · May 13  
Replying to @elonmusk  
Energy usage trend over past few months is insane [cbeci.org](https://www.cbeci.org)

24.3K 12.7K 90.4K

## Mining: sostenibilità ambientale

[twitter.com/elonmusk/status/1392602041025843203](https://twitter.com/elonmusk/status/1392602041025843203)  
[we-wealth.com/news/fintech/blockchain/bitcoin-e-davvero-lindustria-piu-energivora-e-inquinante-del-pianeta](https://we-wealth.com/news/fintech/blockchain/bitcoin-e-davvero-lindustria-piu-energivora-e-inquinante-del-pianeta)  
[businessinsider.in/cryptocurrency/news/what-is-the-crypto-climate-accord/articleshow/83946286.cms](https://businessinsider.in/cryptocurrency/news/what-is-the-crypto-climate-accord/articleshow/83946286.cms)  
[hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume](https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume)

più grande risorsa energetica bloccata del pianeta, e non è un caso che siano diventate il cuore del mining cinese, responsabili di quasi il 10% dell'estrazione globale di Bitcoin nella stagione secca e del 50% nella stagione umida».

A dimostrazione che c'è interesse per venire incontro a un Bitcoin che sia più green possibile è stato lanciato il Crypto Climate Accord, un'iniziativa che ricalca gli Accordi sul Clima di Parigi: l'obiettivo dichiarato e ambizioso è arrivare alla neutralità carbonica entro il 2030. Il dibattito sull'inquinamento di Bitcoin, ca va sans dire, può essere affrontato in maniera costruttiva soltanto se si accetta il fatto che Bitcoin abbia una ragione di esistere.

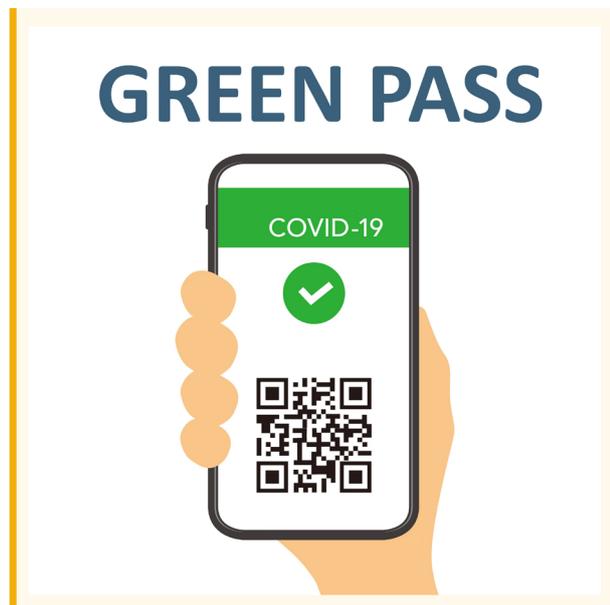


## Il declino della blockchain

Nulla di davvero rilevante da segnalare dal fronte blockchain come tecnologia utilizzata per attività non monetarie. Il Green Pass su blockchain in cantiere a New York, di cui vi avevamo già parlato nel report del Q1, è finito in un nulla di fatto. Ma siccome ci sono sempre attori velleitari pronti a lanciarsi sulle applicazioni inverosimili, l'idea è stata raccolta "vicino casa nostra", a San Marino; pronti ad essere smentiti dai fatti, ma per ora sembra comunque che la significatività dell'iniziativa si confermi trascurabile.

Anche le applicazioni blockchain per la finanza sono ormai tramontate quasi del tutto. Un colpo di coda è rappresentato dall'emissione di un bond blockchain della Banca Europea per gli investimenti, ma non è chiaro in che modo l'infrastruttura blockchain venga davvero utilizzata. Le prime evidenze sembrano confermare il solito approccio di marketing senza sostanza reale.

Infine, JPMorgan, DBS, e Temasek hanno realizzato un consorzio per migliorare i pagamenti cross border, ma non è dato di sapere a cosa serva tecnicamente la blockchain che dichiarano di usare.



## Il declino della blockchain

[fortuneita.com/2021/06/30/san-marino-un-green-pass-basato-su-blockchain](https://fortuneita.com/2021/06/30/san-marino-un-green-pass-basato-su-blockchain)

[eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain](https://eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain)

[fintechnews.sg/50633/payments/dbs-j-p-morgan-and-temasek-to-develop-a-blockchain-based-interbank-payments-platform](https://fintechnews.sg/50633/payments/dbs-j-p-morgan-and-temasek-to-develop-a-blockchain-based-interbank-payments-platform)

# 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://checksig.io)**

 **CheckSig**  
TRANSPARENT BITCOIN CUSTODY



# VITA DELL'ISTITUTO



## Cryptocurrency Open Patent Alliance

Il Digital Gold Institute è diventato membro della Cryptocurrency Open Patent Alliance (COPA).

COPA è un consorzio senza scopo di lucro di persone e aziende, formato per incoraggiare l'adozione e il progresso delle tecnologie legate allo sviluppo delle criptovalute e rimuovere i brevetti come ostacolo alla crescita e all'innovazione.



In particolare, i membri di COPA mettono insieme i loro brevetti di cripto-tecnologia per formare una libreria condivisa: si impegnano a non usare i brevetti cripto-tecnologici contro nessuno, fatta eccezione per motivi difensivi, rendendo la libreria condivisa liberamente disponibile per tutti.

Questa importante scelta pone DGI in compagnia dei leader di mercato: Blockstream, CheckSig, Coinbase, Kraken, MicroStrategy e Square.



## Bitcoin e Criptovalute

### Instant-book de Il Sole 24 ore

DGI ha contribuito attivamente alla guida "Bitcoin e Criptovalute", *instant-book* de Il Sole 24 Ore, uscito in edicola l'11 maggio 2021.



A cura di Francesco Avella, la guida affronta in modo sistematico i principali risvolti dell'adozione delle criptovalute nella realtà quotidiana e fornisce gli strumenti per una migliore conoscenza e comprensione del fenomeno affinché i professionisti possano adeguatamente supportare privati e imprese, ciascuno per le proprie competenze, cogliendone soprattutto le implicazioni giuridiche e fiscali, oltre che economiche e finanziarie.

Il volume contiene l'opinione "Hayek, l'oro Digitale Bitcoin e l'euro Digitale di Bce" a cura del direttore scientifico DGI Ferdinando M. Ametrano e l'intervento "La custodia sicura di Bitcoin" di Paolo Mazzocchi, direttore esecutivo DGI e Chief Operating Officer di CheckSig.

L'instant-book è acquistabile solo online, nello store shopping24 de Il Sole 24 Ore. E' disponibile sia in formato cartaceo che in formato PDF.

### Link utili

[opencrypto.org/members](https://opencrypto.org/members)

[dgi.io/2021/05/11/il-sole-24-ore](https://dgi.io/2021/05/11/il-sole-24-ore)

[www.shopping24.ilsole24ore.com/sh4/collateral/products/libri-r.jsp?productId=prod2650197](https://www.shopping24.ilsole24ore.com/sh4/collateral/products/libri-r.jsp?productId=prod2650197)



## 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.

### Linklaters

[dgi.io/2021/06/25/linklaters](https://dgi.io/2021/06/25/linklaters)

Linklaters

### Fuori TG – TG3

[dgi.io/2021/06/16/fuoritg-tg3](https://dgi.io/2021/06/16/fuoritg-tg3)

TG3

### Class CNBC

[dgi.io/2021/06/05/class-cnbc](https://dgi.io/2021/06/05/class-cnbc)



### Radio Televisione Svizzera

[dgi.io/2021/06/07/rsi](https://dgi.io/2021/06/07/rsi)



### Il Sole 24 Ore

[dgi.io/2021/06/06/il-sole-24-ore](https://dgi.io/2021/06/06/il-sole-24-ore)



### Rai Radio1

[dgi.io/2021/05/20/rairadio1](https://dgi.io/2021/05/20/rairadio1)



**We Wealth**

dgi.io/2021/06/04/we-wealth  
 dgi.io/2021/05/24/we-wealth  
 dgi.io/2021/05/14/we-wealth  
 dgi.io/2021/04/17/we-wealth

**Il Foglio**

dgi.io/2021/04/28/il-foglio

IL FOGLIO

**AdnKronos**

dgi.io/2021/04/27/adnkronos  
 dgi.io/2021/04/26/adnkronos  
 dgi.io/2021/03/29/adnkronos

**Il Post**

dgi.io/2021/04/23/il-post

**StartupItalia!**

dgi.io/2021/04/22/smartmoney

**Rai News24**

dgi.io/2021/04/21/rai-news

**Le Iene**

dgi.io/2021/04/19/le-iene

**Agenda Digitale**

dgi.io/2021/04/18/agenda-digitale



## CryptoWeek

Tutti i venerdì alle 18:00

**CryptoWeek**  
il venerdì alle 18:00  
LIVE STREAMING  
[www.dgi.io/cryptoweek](http://www.dgi.io/cryptoweek)

con **Ferdinando M. Ametrano**  
direttore scientifico Digital Gold Institute

Sponsored by:  
**CheckSig**  
TRANSPARENT BITCOIN CUSTODY

Digital Gold Institute  
Scarcity in the Digital Realm

[www.dgi.io](http://www.dgi.io) #cryptoweek

Successo di ascolti e di interesse, la CryptoWeek è confermata per tutta l'estate.

Iniziativa settimanale, ogni venerdì alle 18 in live streaming su YouTube e 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](http://dgi.io/cryptoweek).

## Bitcoin & Blockchain - Workshop

28 - 29 settembre 2021

**Bitcoin & Blockchain**  
28-29 settembre 9:00-18:00  
ONLINE WORKSHOP  
[www.dgi.io/workshop](http://www.dgi.io/workshop)

Partners:  
**CheckSig** **Deloitte.**  
TRANSPARENT BITCOIN CUSTODY

Digital Gold Institute  
Scarcity in the Digital Realm

[www.dgi.io](http://www.dgi.io) #DGIWORKSHOP

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](http://dgi.io/workshop).

## Presentazione del report trimestrale

6 ottobre 2021

Presentazione trimestrale  
**Report 2021-Q3**  
 6 ottobre 17:30-19:00  
 LIVE STREAMING  
[www.dgi.io/reports](http://www.dgi.io/reports)

Partners:

CheckSig  
TRANSPARENT BITCOIN CUSTODY

Deloitte

[www.dgi.io](http://www.dgi.io) #DGIREPORT2021Q3

Il report 2021-Q2 è stato presentato in anteprima il 14 luglio, in web streaming. I fatti più rilevanti del trimestre sono stati commentati dal nostro direttore scientifico Ferdinando M. Ametrano; Andrea Cattaneo (General Manager Italy e Head of Italy, Switzerland & Iberia di BNP Paribas Securities Services) ha invece curato un approfondimento sugli asset digitali. Al termine dell'evento pubblico è seguito un dibattito riservato tra esponenti del mondo politico, finanziario, industriale, accademico, consulenziale e giornalistico. Maggiori dettagli alla pagina [dgi.io/reports](http://dgi.io/reports).

Il prossimo evento di presentazione del report trimestrale 2021-Q3 si terrà il 6 ottobre.

## Crypto Asset Lab Conference

4 - 5 novembre 2021

Crypto Asset Lab  
 European Commission  
 UNIVERSITÀ DEGLI STUDI MILANO BICOCCA  
 Digital Gold Institute  
 Scarcity in the Digital Realm

WEB STREAMING ON  
 November 4-5

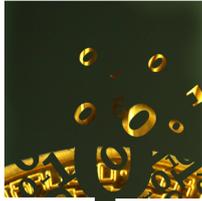
**3rd Crypto Asset Lab Conference · CAL2021**

Investments, Economics, and Regulation  
 for Bitcoin and Crypto Assets.

CheckSig  
TRANSPARENT BITCOIN CUSTODY  
 Gold Sponsor

CAL2021 è 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*).

La conferenza vanta un eccellente *program committee* che valuta la proposta di lavori scientifici in materia di investimenti, economia e regolamentazione per Bitcoin e crypto-asset. La partecipazione è gratuita: si rivolge principalmente a ricercatori, docenti, professionisti, aziende ed istituzioni; sono benvenuti anche studenti e semplici interessati. Maggiori informazioni disponibili visitando [cryptoassetlab.diseade.unimib.it/calconf](http://cryptoassetlab.diseade.unimib.it/calconf).



## Autori



**Ferdinando M. Ametrano**

ferdinando@dgi.io

**Alessandro Di Stefano**

distefanoalessandro90@gmail.com

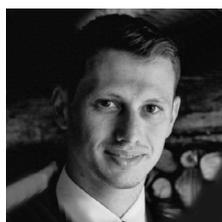


**Lucia Mandelli**

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](https://dgi.io)

 [info@dgi.io](mailto:info@dgi.io)

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

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

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

 [@dginst](https://github.com/dginst)

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