

Su questo sito utilizziamo cookie tecnici e, previo tuo consenso, cookie di profilazione, nostri e di terze parti, per proporti pubblicità in linea con le tue preferenze. Se vuoi saperne di più o prestare il consenso solo ad alcuni utilizzi [clicca qui](#). Cliccando in un punto qualsiasi dello schermo, effettuando un'azione di scroll o chiudendo questo banner, invece, presti il consenso all'uso di tutti i cookie **OK**



Volete investire in criptovalute? Secondo Michael Casey, guru della blockchain: 'fatelo solo se avete capitali che potete permettervi di perdere'

Matteo Vegetti | 51 MINUTI



Michael Casey. Token Fest

- Business Insider Italia ha intervistato Michael Casey, guru della blockchain, autore del recente libro *La macchina della verità: la blockchain e il futuro di ogni cosa*
- Nell'intervista Casey spiega perché la blockchain può rappresentare la risposta alla crisi di fiducia post-2008 in istituzioni come le banche, o persino i governi
- Secondo l'esperto gli investimenti in criptovalute sono "molto costruttivi", a patto che si investa un capitale che si è disposti a perdere
- [Per leggere un estratto del libro, in esclusiva per i lettori di Business Insider, clicca qui](#)

Guarda Anche



Questi 5 segnali indicano che sei più intelligente della media secondo diversi studi scientifici



L'aereo più lungo e lussuoso al mondo: forme tonde e pavimento in vetro per vedere il panorama



Il gigante con le ali che trasporta i pezzi di altri aerei in tutto il mondo - video



Una fisica smonta il più grande mito sul Triangolo delle Bermude

da Taboola

Più letti Oggi

- 1 11 trucchi degli esperti di finanza per risparmiare un po' di soldi ogni giorno
- 2 In Olanda una messa dura ininterrottamente da 49 giorni per impedire alla polizia di deportare una famiglia di immigrati

Michael Casey, formatore e consulente del Mit Media Lab ed ex giornalista del *Wall Street Journal*, è noto soprattutto per il bestseller *The Age of Cryptocurrency*, a cui segue ora *La macchina della verità* (pubblicato in Italia da **Franco Angeli**), entrambi scritti insieme a Paul Vigna. In questa intervista di Business Insider Italia ha parlato della blockchain come nuovo sistema di fiducia e degli aspetti legati alla sicurezza e alla privacy, consigliando a chiunque sia interessato a investire nell'area delle criptovalute di procedere, ma con prudenza.

Guarda anche



Michael Casey

La macchina della verità (pubblicato in Italia da **Franco Angeli**) presenta la blockchain come una risposta alla crisi di fiducia post-2008 in istituzioni come le banche, o persino i governi. Eppure anche il World Wide Web sembrava così aperto e democratico inizialmente, mentre oggi suscita sfiducia per questioni legate alla privacy e alla raccolta dati. Non esiste il rischio che la blockchain segua un percorso simile?

“È un’ottima domanda. In base ai principi di una blockchain pubblica, quella che noi chiamiamo ‘non autorizzata’ (permissionless), come Bitcoin, Ethereum e molte altre, i nodi che fanno parte del network sono strutturati in modo tale che non esista letteralmente nessuno che abbia in mano il potere. È una struttura profondamente diversa da quella di Internet. Nella blockchain non autorizzata nessuno può fungere da gatekeeper, da guardiano, almeno sul piano del registro.

“In effetti questo non è necessariamente sufficiente per prevenire lo scenario di cui ha parlato; affermare che all’interno di sistemi come Bitcoin o anche Ethereum esista una concentrazione eccessiva di potere è una critica corretta e ragionevole, perché in realtà è solo un piccolo numero di nodi a controllare le attività di mining necessarie per il sistema.

“Per quanto riguarda le blockchain pubbliche, esiste un forte interesse a porre l’enfasi su un modello più

3 Tra yacht, ville sfarzose e auto di lusso, ecco l'impero di Roman Abramovich: così il miliardario russo spende i suoi miliardi

4 Una nuova prova del fuoco per Draghi: salvare l'eurozona senza il Qe

5 In Spagna il socialista Sanchez aumenta gli stipendi minimi del 22%

FinanciaLounge

Contenuti offerti da **FINANCIALOUNGE**

Draghi vede rischi ma rassicura i mercati

L'Europa politicamente divisa sempre più periferia del mondo

Gli indici della paura rientrano, ma attenzione alle illusioni ottiche

Facebook non è più il posto migliore dove lavorare in America

Dal Web



Il Cloud Computing oggi è una scelta obbligata, anche per le PMI italiane

Aruba



La moda è in evoluzione. Rinnova il tuo stile con Imperial.

Imperial



Ecco i vip con cui nessuno vuole lavorare!

Alfemminile



decentralizzato; nella comunità di Bitcoin e altrove è in corso un grande dibattito sulla struttura opportuna per questo modello, ma essenzialmente dovremmo sforzarci di seguire modelli di gestione che non diano troppo potere in mano a un piccolo gruppo di miner.

“Inoltre, dobbiamo incoraggiare la società a dare più input possibili per controllare gli algoritmi prodotti da queste blockchain. Se è solo un piccolo gruppo di sviluppatori a scrivere quegli algoritmi, il potere è concentrato esclusivamente nelle loro mani, perché sono gli unici in grado di farlo.

*“Devono esserci dunque **più programmatori**, ma anche più persone che capiscono la questione e si interessano, che sono in grado di supervisionare quest’area e sviluppare norme. Nel libro sottolineiamo che deve esserci un interesse nei confronti di questo processo da parte dell’intera società, per garantire la varietà degli input sugli stessi algoritmi.*

A proposito delle corporation, nel libro scrivete che “Il modo in cui Uber e naturalmente Facebook, Google e gli altri giganti tecnologici del XXI secolo gestiscono i dati è diventato una questione critica”. Quali meccanismi di tutela ci offre invece la blockchain?

*“Ci sono molte ragioni che hanno portato a una situazione di questo tipo; una è che non abbiamo a disposizione il framework giusto per gli scambi tra pari (peer-to-peer) su Internet, perché non ci fidiamo gli uni degli altri. Così abbiamo dovuto affidarci a questi ‘intermediari fidati’ perché gestissero gli scambi tra di noi, e in questo senso i dati sono una valuta, una preziosa fonte di informazioni. È diventato necessario creare queste **entità centralizzate, che hanno finito per acquisire sempre più potere**. Essenzialmente dobbiamo capire come effettuare transazioni tra di noi senza questi intermediari.”*



Scopri GLC Coupé con ecoincentivo Mercedes-Benz.

Mercedes-Benz

Contenuti Sponsorizzati da Taboola

MICHAEL J. CASEY, PAUL VIGNA

LA MACCHINA DELLA VERITÀ

LA BLOCKCHAIN E IL FUTURO
DI OGNI COSA



Sempre sul tema delle blockchain pubbliche, voi scrivete che “la natura decentralizzata di questa tecnologia rende il coordinamento piuttosto difficile” (come ha dimostrato per esempio lo scisma tra Bitcoin e Bitcoin Cash). Sembra che in questo si nasconda un paradosso: non è forse la natura stessa di ogni iniziativa collettiva a rendere indispensabile il ricorso a un gatekeeper, cioè un intermediario fidato?

*“È un'altra buona domanda. Penso che debba sempre esserci **fiducia**, fiducia in un'entità che gestisce il sistema, e che si tenda sempre a un certo livello di **centralizzazione**, perché è così che **si garantisce l'efficienza** e che si possono realizzare profitti.*

*“È utile vedere la questione in termini di strati diversi. Se possiamo fare in modo che lo **strato del registro**, quello che documenta la sequenza di transazioni, sia gestito a un livello completamente **decentralizzato**, tutte le altre fonti di fiducia — l'immissione dei dati, il coordinamento e così via — dovranno avere delle entità che le valutino sulla base di determinati criteri e nelle quali noi dovremo avere fiducia, ma almeno avremo sottratto una certa quantità di potere al gatekeeper.*

“In più questo sistema ci offre un meccanismo per verificare la performance di quelle entità, quelle persone

o quei dispositivi fidati, perché il registro stesso diventa uno strumento che ci permette di tornare indietro nel tempo e di effettuare tale verifica”.

La questione si complica invece per le blockchain private. Perché?

*“La blockchain pubblica di per sé impedisce che esista un gatekeeper centralizzato, quindi offre già una certa protezione. Le blockchain **private** invece sono ‘autorizzate’ (permissioned), nel senso che **ogni nodo del network esiste perché è autorizzato da qualcun altro**; all’interno di queste blockchain c’è già una certa concentrazione di potere, perché l’autorità di cui sopra è il gatekeeper, il soggetto che decide chi può partecipare o meno.*

*“Tuttavia, se esiste un consorzio di aziende che non hanno interessi in comune, ma semmai interessi variegati, e se esiste un complesso di regole associative che salvaguardano fermamente il raggiungimento del consenso più ampio, è molto difficile immaginare uno scenario in cui il gruppo possa colludere per conquistare il potere. Ci sono dunque dei modi per assicurarsi che il **consorzio in questione sia ampio e variegato**, e che non sia naturalmente propenso a introdurre un controllo più centralizzato.*

“Nessuno ha in mano la soluzione perfetta; c’è molto lavoro da fare per assicurare che non si arrivi a una concentrazione della proprietà del network di validazione che gestisce questi sistemi”.

Passando al tema della sicurezza, voi scrivete che “una delle applicazioni più importanti della blockchain del sistema Bitcoin, al di là delle valute, potrebbe essere proprio la sicurezza”: il fatto che la relativa blockchain non sia stata violata dagli hacker nei suoi nove anni di esistenza dimostrerebbe che è una tecnologia molto affidabile. Ma la natura stessa dei token digitali non comporta più rischi dei token fisici?

“Occorre distinguere fra lo strato del registro, che nel caso di Bitcoin non è mai stato violato dagli hacker, e lo strato applicativo, che non risiede sulla blockchain ma in realtà è un’entità fidata. Gli exchange di criptovalute, e anche i singoli wallet, sono vulnerabili perché sono controllati da esseri umani o dispositivi.

*“Esiste dunque effettivamente **un rischio, ma non riguarda la vulnerabilità del sistema**. La questione è se le persone, o le imprese, o chiunque controlli i bitcoin eserciti **un grado di controllo sufficiente** sulla relativa chiave privata e sull’infrastruttura di accesso alla valuta.*

“Bisogna lavorare sulla sicurezza a quel livello. Forse esiste anche un ruolo da svolgere per un ‘custode’ che

eserciti un certo grado di controllo. Ci sono moltissime cose che possono contribuire a incrementare la sicurezza al livello degli exchange e dei singoli wallet, ma è una questione completamente diversa dalla sicurezza del sistema Bitcoin di per sé, che finora non è mai stato compromesso.”

Quanto alla sicurezza della blockchain come sistema di base, voi spiegate che i computer quantistici sono le uniche macchine che un giorno potrebbero violare il sistema. Che cosa succederà quando saranno effettivamente disponibili?

“In effetti, mentre con i computer di oggi i costi da sostenere per violare il sistema sarebbero proibitivi, con i computer quantistici si tratterebbe di un’operazione immediata. Ma quando li avremo a disposizione scatterà una gara fra chi ha intenzione di usarli a fini di attacco e chi vuole svolgere una funzione di difesa. Esisteranno algoritmi basati sul quantum computing, di conseguenza la sicurezza sarà elevata a un livello quantistico. Ci sono già persone che stanno sviluppando sistemi quantum-proof. È una questione cruciale perché l’intera Internet poggia su sistemi di crittografia di enorme importanza, e saranno tutti messi sotto pressione dall’avvento dei computer quantistici.”

Lei dunque non crede, pensando alla visione mitologica della blockchain, che vedremo manifestarsi un giorno la nemesi di Satoshi Nakamoto (pseudonimo della persona o del gruppo di persone ignote a cui è attribuita la creazione del Bitcoin nel 2009)?

“Quella di cui abbiamo appena parlato è una forma di nemesi, in effetti, ma credo proprio che si troverà una soluzione al problema.”

Nel libro spiegate che altre criptovalute tutelano la privacy meglio del bitcoin; c’è però il rischio che proprio per questo motivo siano usate a fini criminali. Come si può mantenere il giusto equilibrio fra il desiderio di privacy da parte degli utenti comuni, e la necessità di rilevare utilizzi illegali delle criptovalute?

“È una questione fondamentale. Penso che si rivolga un’attenzione eccessiva al rilevamento dei criminali. Non dico che non dovremmo cercare di proteggere il sistema, ma la privacy è davvero importante per garantire la finanziabilità e la funzionalità del sistema. Per moltissime aziende la privacy è un requisito essenziale. Alcuni però finiscono per criminalizzare lo scambio che avviene in sé e per sé, invece di far fronte ai reati effettivamente commessi.

“Personalmente sarei molto contento di avere un sistema che preveda un grado di privacy ancora più elevato, ma abbia la capacità di individuare i criminali usando altri mezzi. È un’area che richiede interventi politici; da parte

mia ci tengo solo ad assicurarmi che si discuta sul tema della privacy.”

E ai nostri lettori, molti dei quali sono interessati alle criptovalute o già attivi in quest’ambito, quali consigli di investimento può dare?

“Non amo dare consigli specifici; non spetta a me, quindi non dico mai di comprare questa o quella criptovaluta.

*“Quello che dico è: se volete investire in quest’ambito, tenete presente che si trova **ancora in una fase sperimentale**. Io sono convinto che questa tecnologia sarà davvero importante in futuro, è per questo che ho scritto il libro; ha una serie di applicazioni enormi, ma c’è ancora **molto lavoro da fare e non sappiamo se funzionerà di sicuro o meno**.*

*“Se investite in questa fase, **investite dunque capitali che potete permettervi di perdere**. Al tempo stesso, cercate di informarvi su quello in cui state investendo. Non riversate assolutamente tutti i risparmi di una vita in quest’area; penso però che mettere in gioco una piccola quantità di capitale che si può rischiare di perdere sia un investimento molto costruttivo”.*

Un tema particolarmente “caldo” nel settore sono le Ico (initial coin offering). Le considera un mezzo efficace per investire e per raccogliere capitali?

“A dire il vero penso che l’utilizzo delle Ico per raccogliere capitali rappresenti il loro vero problema. Lo scopo di una Ico dovrebbe essere quello di proporre un token che possa avere un ruolo trainante nella creazione di un network, come ether per Ethereum, non come mezzo per raccogliere dei soldi.

*“Se questo avviene come esito secondario, va bene, ma il problema è che **tutte le Ico degli ultimi tempi erano essenzialmente veicoli per la raccolta di capitali**, dunque sono state tutte immediatamente soggette a una valutazione da parte della Sec (Securities and Exchange Commission) negli Stati Uniti. Questo ente non le ha raccomandate come veicoli d’investimento sicuri, di conseguenza è stato molto difficile proporle a un ampio mercato.*

*“Per me, **una Ico è un evento di generazione di token volto a creare un nuovo sistema di gestione economica decentralizzata**. La struttura degli utility tokens dev’essere ulteriormente sviluppata, e non sono certo che gli enti di controllo li comprendano a fondo. Ma a prescindere da questo, il punto è che non bisognerebbe focalizzarsi così tanto sulla semplice raccolta di fondi, bensì riflettere sul ruolo del token stesso all’interno del sistema”.*

Dato che ha parlato degli enti di controllo, qual è la sua percezione dell'approccio seguito dai governi nei confronti delle criptovalute e della blockchain?

"L'opinione dei governi su questi temi sta ancora evolvendo. Manca una piena comprensione. Molti enti di controllo stanno iniziando a prenderne atto, ma occorre arrivare a una comprensione più ampia di queste tecnologie e di come si possano rivedere i modelli esistenti di misurazione dell'autorità in questo ambiente.

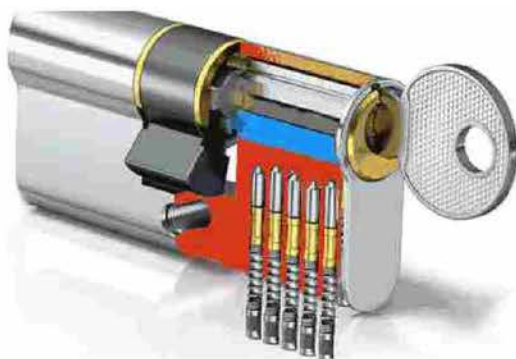
"In ultima analisi però penso che sia importante che si arrivi a una certa regolamentazione. Io non ho idee ultraliberali sotto quest'aspetto, penso però che questi enti debbano assicurarsi che sia mantenuto saldamente l'equilibrio fra privacy e funzionalità; che le startup che producono in quest'area non siano eccessivamente gravate dai requisiti normativi; e che il bisogno di sicurezza sia tutelato. Trovare l'equilibrio giusto è essenziale".

Business Insider Italia

Vuoi ricevere ogni giorno le migliori notizie di Business Insider Italia? Iscriviti gratuitamente alla nostra newsletter

ISCRIVITI

Taboola Feed



Questi geniali sistemi di allarme stanno stravolgendo l'Italia

Expert Market | Sponsorizzato



Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.