



Natura e rilevanza delle contabilità decentralizzate

Antonio Simeone

LUISS Bitcoin Lab (Discover Bitcoin)

LUISS Quantum & AI Lab

LUISS  Search

Discover Bitcoin

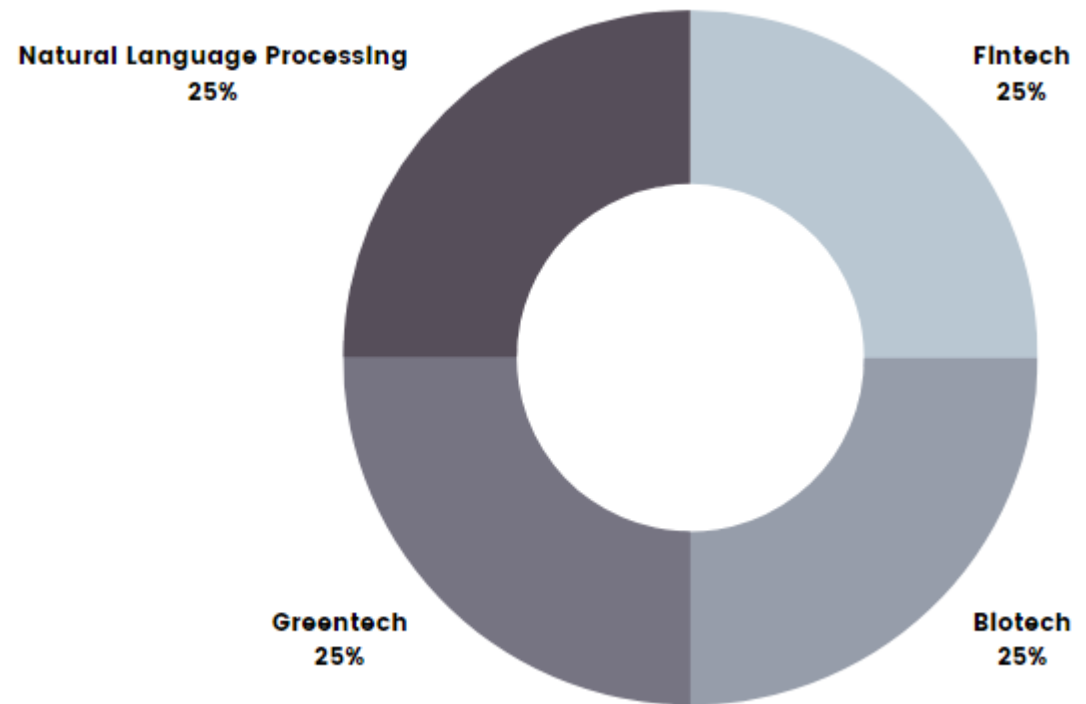
discover 

Home
Our Team
Cryptos
Bitcoin Database
Related Sites
Partners

OUR TEAM

Discover Bitcoin is a project born from the collaboration and passion of different coming together into a great team.

Founders
Academic Committee
Associates



Blockchain Decentralizzate

Come dovrebbero essere

- La decentralizzazione della blockchain si riferisce alla distribuzione del potere e dell'autorità attraverso una rete di computer o nodi che mantengono e convalidano collettivamente una blockchain.
- Nei sistemi centralizzati tradizionali, **un'autorità centrale o un intermediario facilita e verifica le transazioni.**
- Al contrario, la tecnologia blockchain decentralizzata mira a eliminare la necessità di un'autorità centrale, consentendo a più partecipanti di mantenere il sistema collettivamente.
- Per spiegarlo in maniera semplice, è come se la validazione di un pagamento fra due persone avvenisse con la comunicazione istantanea ad un gruppo di individui, anziché tramite una banca centrale
- In una rete blockchain decentralizzata, **ogni nodo ha una copia dell'intera blockchain e partecipa al meccanismo di consenso per convalidare e verificare le transazioni.**
- Questo meccanismo di consenso garantisce l'accordo tra i nodi sulla validità e sull'ordine delle transazioni, promuovendo la fiducia e la sicurezza all'interno della rete.

Tipi di Decentralizzazione nella blockchain

- **Architectural Decentralization:**

Decentralizzazione geografica dei nodi, aumentando la resilienza contro attacchi esterni o possibili interruzioni improvvise della rete

- **Governance Decentralization:**

Decentralizzazione decisionale dei nodi, evitando una singola autorità centrale che prenda tutte le decisioni (DAO)

- **Data Decentralization:**

Distribuzione e archiviazione dei dati su più nodi, impedendo il fallimento della rete a causa del malfunzionamento di un nodo

- **Functional Decentralization:**

Distribuzione dei compiti (mining, validazione, smart contract) attraverso la rete, favorendo un sistema più robusto

- **Incentive Decentralization:**

Distribuzione di ricompense fra i partecipanti alla rete per migliorare la sicurezza della blockchain

Vantaggi della decentralizzazione Blockchain

- **Sicurezza:** Senza un singolo punto di fallimento, **le reti decentralizzate sono più resilienti agli attacchi e ai tentativi di censura. Poiché i dati sono distribuiti su più nodi**, diventa difficile per attori malevoli manipolare o compromettere il sistema.
- **Trasparenza:** La natura decentralizzata della blockchain permette la trasparenza poiché **chiunque nella rete può visualizzare la cronologia delle transazioni e verificarne l'integrità**. Questa trasparenza può favorire la fiducia tra i partecipanti.
- **Assenza di fiducia:** La decentralizzazione riduce la necessità di fiducia tra i partecipanti, poiché il meccanismo di consenso garantisce l'accuratezza e la validità delle transazioni. I partecipanti possono fare **affidamento sui protocolli matematici della blockchain e sui contratti intelligenti anziché sulla fiducia in un'autorità centrale**.
- **Proprietà e controllo:** Eliminando gli intermediari, **la decentralizzazione consente alle persone di avere diretta proprietà e controllo sui propri beni e dati**. Fornisce maggiore autonomia e riduce la dipendenza dalle istituzioni centralizzate.

[Svantaggi della decentralizzazione Blockchain

- **Scalabilità:**

Tempi di elaborazione delle transazioni più lenti all'aumentare delle dimensioni della rete .

- **Governance e Decision Making:**

Possibili disaccordi fra i partecipanti alla rete, che possono portare a fork (Bitcoin Cash nel 2017 e soprattutto Ethereum)

- **Sicurezza della Rete:**

Possibili attacchi del 51%, in cui un'entità o un gruppo ottiene il controllo della maggior parte del potere computazionale della rete (Mining)

- **Esperienza Utente e Responsabilità:**

Gli utenti devono gestire da soli le chiavi dei propri wallet con potenziali rischi come la perdita di fondi nel caso di smarrimento e furto

- **Sfide Regolatorie:**

Mancanza di un organo centrale legislativo, rendendo difficile il rispetto delle normative, facilitando eventuali attività illecite

- **Consumo di Energia:**

Elevato consumo di energia, soprattutto da parte di blockchain proof-of-work, sollevando preoccupazioni sulla sostenibilità ambientale

- **Aggiornamenti e Cambiamenti di Protocollo:**

Difficoltà nell'implementazione di eventuali modifiche o aggiornamenti per la richiesta di consenso da parte dei partecipanti alla rete

{ Impatto Decentralizzazione Blockchain

- **Disintermediazione:**

Eliminazione di intermediari come banche, clearinghouse o broker, non richiedendo costi ulteriori ed evitando ritardi dovuti ad errori umani

- **Maggiore controllo da parte degli Individui:**

Più controllo sui propri dati, migliore gestione delle identità digitali, e quindi della propria privacy personale

- **Aumento della Trasparenza e della Fiducia:**

Aiuto nel contrasto ad attività illecite come frodi e corruzione grazie alla visibilità delle informazioni trascritte sul registro

- **Migliorata Sicurezza e Resilienza:**

Miglioramento della sicurezza grazie alla parallelizzazione del controllo su più nodi, garantendo l'operabilità anche in caso di fallimento di alcuni

- **Sistemi Finanziari Inclusivi:**

Possibilità di maggiore democratizzazione dei sistemi finanziari grazie alla finanza decentralizzata (DeFi), aiutando le popolazioni svantaggiate in termini economici

- **Decisioni Democratiche:**

Governance più distribuita, ovvero meno accentrato del potere in mani di pochi, rendendo le decisioni più democratiche

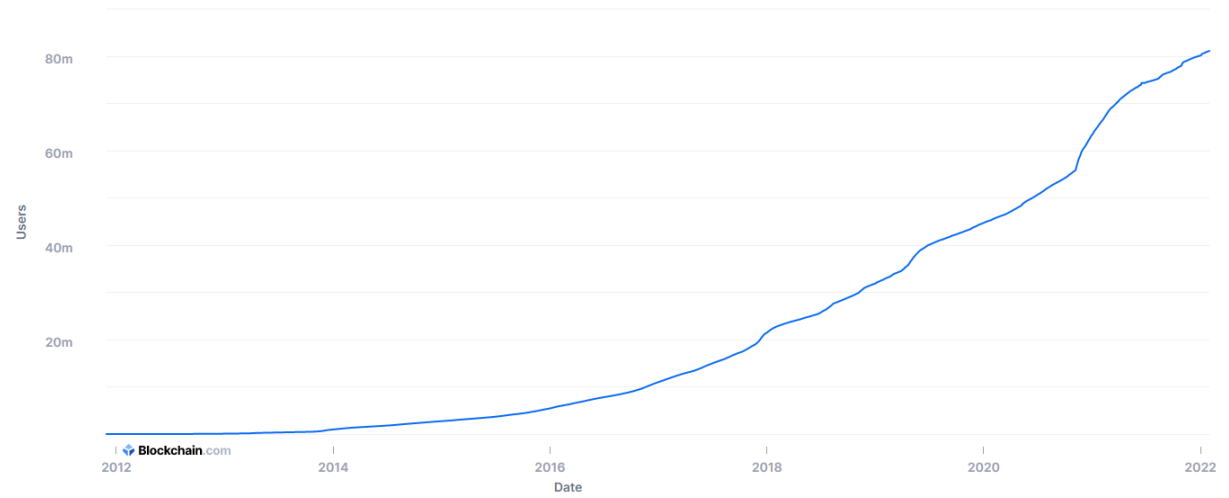
- **Accessibilità Globale e Interoperabilità:**

Maggiore accessibilità a livello globale grazie alla tecnologia, promuovendo l'interoperabilità tra sistemi diversi e favorendo la collaborazione internazionale.

Tutto molto bello ma...

Blockchain.com Wallets

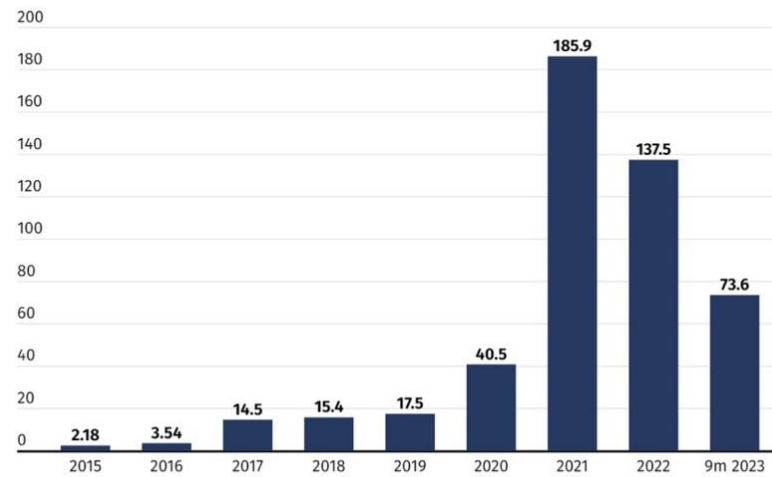
The total number of unique Blockchain.com wallets created.



F
M

Total number of downloads of the 21 largest crypto wallets worldwide from January 2015 to September 2023

(in millions)

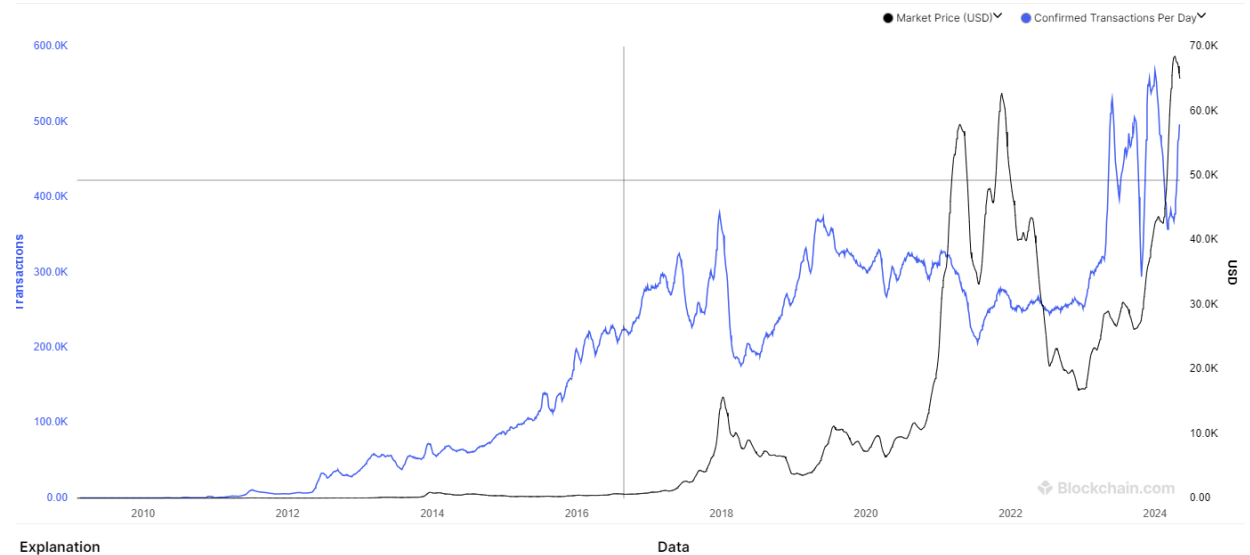


Sources: AppMagic; CryptoSlate, Statista

Confirmed Transactions Per Day

The total number of confirmed transactions per day.

Scales: Linear, 30D Average, Type: Line, Colors: Blue, Black, Camera, 1M, 3M, 6M, 1Y, 3Y, All



Explanation

Data



Blockchain Analysis of the Bitcoin Market

Igor Makarov & Antoinette Schoar

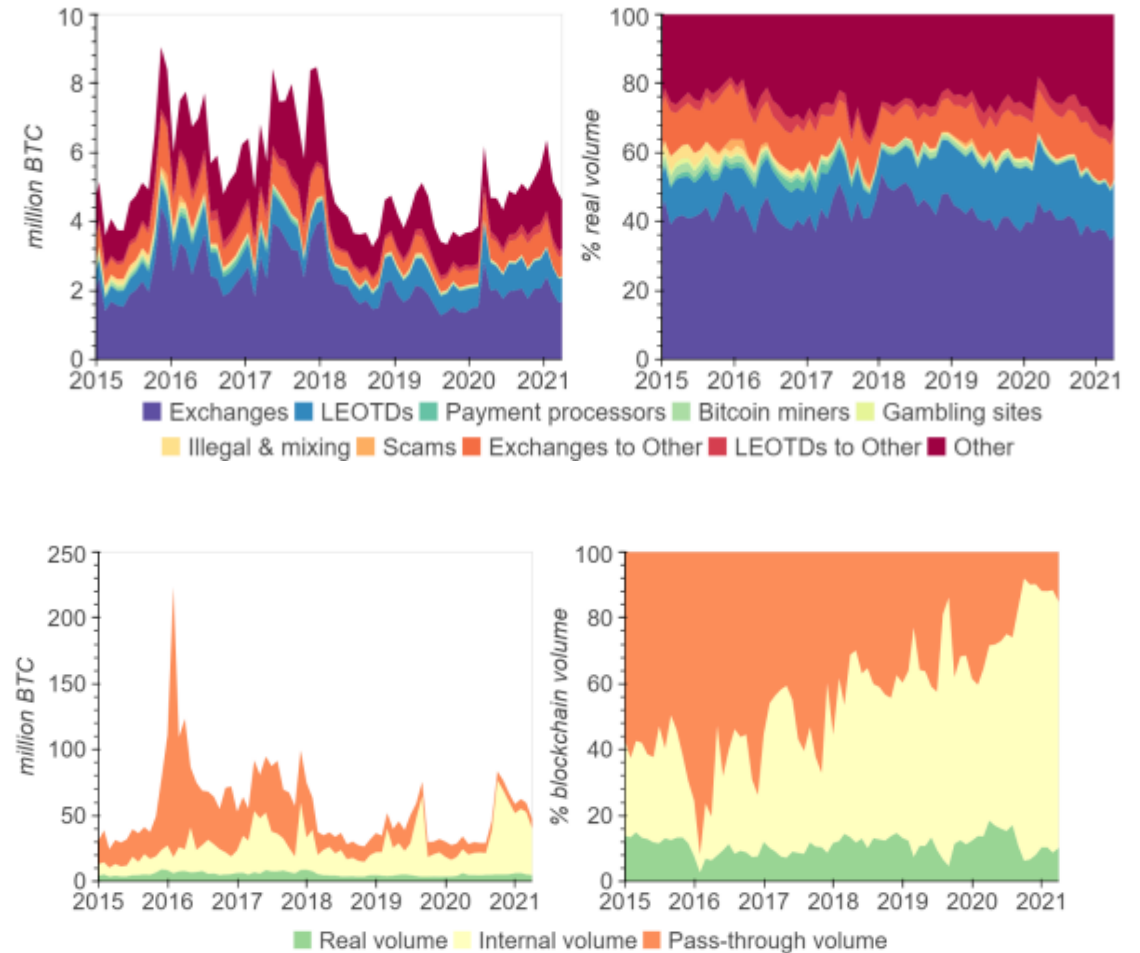
WORKING PAPER 29396

DOI 10.3386/w29396

ISSUE DATE October 2021

In this paper, we provide detailed analyses of the Bitcoin network and its main participants. We build a novel database using a large number of public and proprietary sources to link Bitcoin addresses to real entities and develop an extensive suite of algorithms to extract information about the behavior of the main market participants. We conduct three major pieces of analysis of the Bitcoin eco-system. First, we analyze the transaction volume and network structure of the main participants on the blockchain. Second, we document the concentration and regional composition of the miners which are the backbone of the verification protocol and ensure the integrity of the blockchain ledger. Finally, we analyze the ownership concentration of the largest holders of Bitcoin.

- Il 90% dei volumi della blockchain non è correlato ad attività che hanno una reale funzione economica. **E le transazioni reali? Sono solo 5 per ogni minuto.**
- Si può notare, dal grafico, che **90%, deriva da due attività che non hanno una reale funzione economica.** La prima attività è semplicemente il modo attraverso il quale vengono elaborate le transazioni bitcoin.
- La seconda, sono le transazioni inviate tra i wallet dallo stesso utente che tenta di offuscare la propria identità, una tattica comune per chi cerca l'anonimato. La strategia volta a impedire la tracciabilità dei fondi.
- **Del restante 10% del volume, quello che i ricercatori chiamano "volume reale", domina il trading.**
- **Le transazioni tra borse e trading desk rappresentano circa il 75% del volume totale.**
- Quindi, solo in pochissimi casi, in percentuale al totale, il bitcoin sembrerebbe comportarsi da vera e propria valuta.



E la decentralizzazione?

I primi 10.000 conti bitcoin contengono 5 milioni di bitcoin, l'equivalente di circa 350 miliardi di dollari al cambio attuale. Quindi, **solo lo 0,01% dei possessori di bitcoin controlla il 27%** dei 19 milioni di bitcoin in circolazione.

Il rischio sistemico è molto alto e in caso di aumento di prezzo la disuguaglianza tra questo piccolo gruppo di investitori e i più piccoli si farebbe sempre più vistosa.

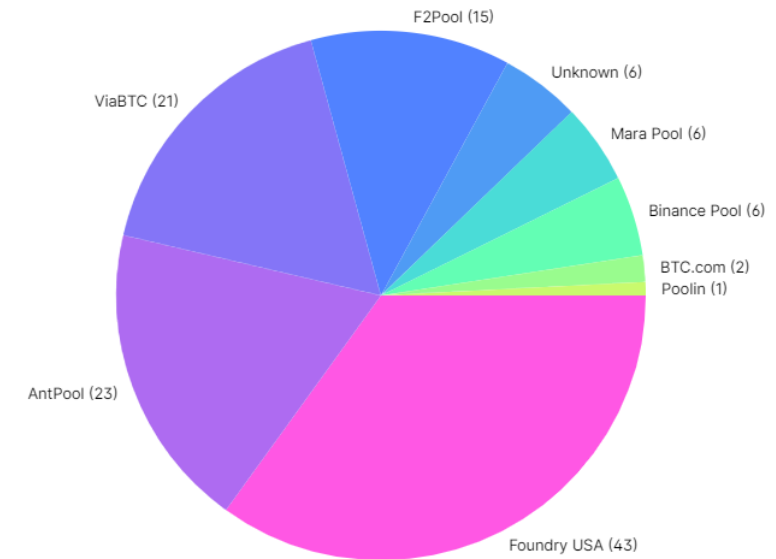
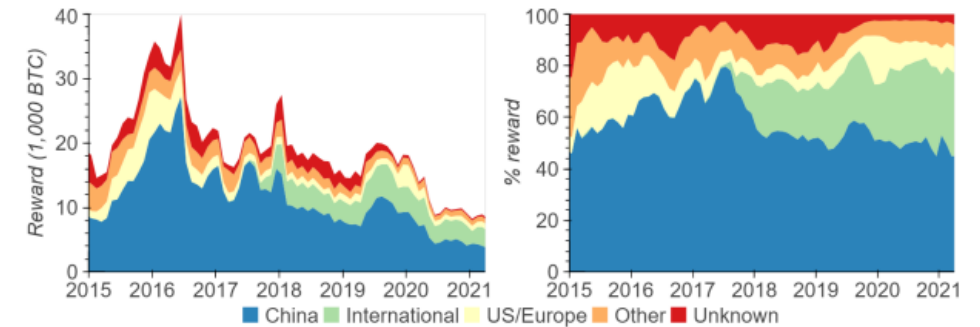
Con il **51% o più del controllo del mining è possibile attaccare la blockchain del bitcoin**, la più decentralizzata e sicura tra le tante.

Ma è davvero così? **Sicura e soprattutto decentralizzata?**

Forse no. Perché non solo un piccolo gruppo controlla diversi milioni di bitcoin ma anche **un ristretto numero di miner, circa 50, controlla di fatto la blockchain**.

I miners, i soggetti deputati alla validazione delle transazioni sulla blockchain e che vengono remunerati in bitcoin, risultano essere molto più concentrati – e spesso facenti parte della stessa regione - rispetto a quanto si possa immaginare.

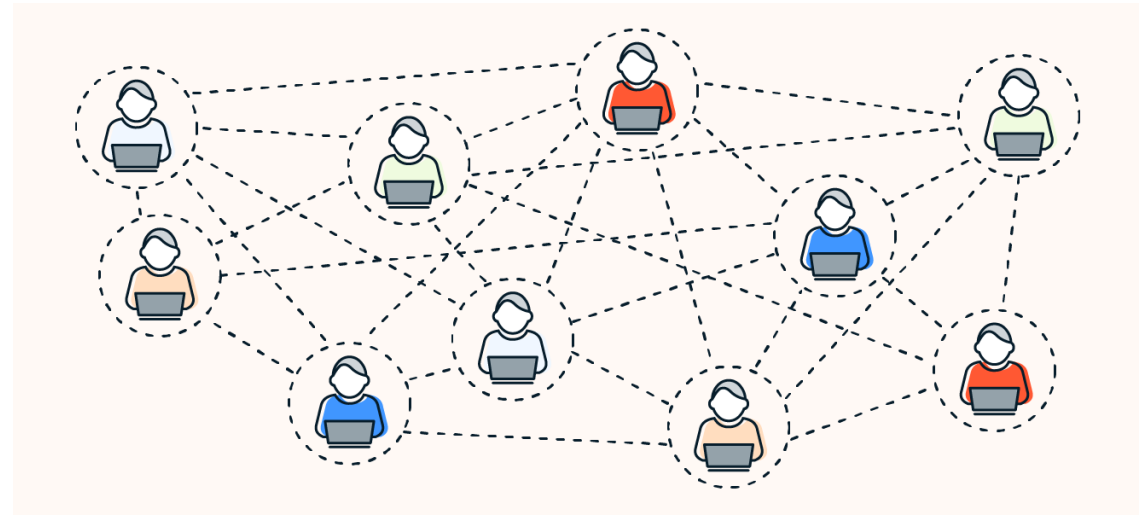
Infatti, sempre secondo gli autori dello studio (Antoinette Schoar della MIT Sloan School of Management e Igor Makarov della London School of Economics), **il 10% dei miners più grandi controlla il 90% del mining, e solo lo 0.1%, circa 50 miners, controlla quasi il 50% dell'intera blockchain del bitcoin**.



Dao

Decentralized Autonomous Organization

- 1. Un'organizzazione autonoma decentralizzata (DAO) è fondamentalmente un fondo comune decentralizzato. In una DAO hai il controllo sulle risorse raccolte dall'organizzazione in base al numero di token di governance che possiedi.
- 2. In una DAO, **possedere token di governance ti dà la possibilità di proporre e votare nuove regole. Queste vengono quindi eseguite automaticamente tramite i famosi smart contract.** Non c'è alcun CEO che passa ordini ai dirigenti su tutta la linea, la DAO si basa solo su contratti intelligenti per svolgere il lavoro (Code is Law).
- 3. Il concetto di DAO è stato ideato per la prima volta nel 2015 da un team chiamato Slock.it.
- 4. Le persone – investendo ETH in Slock.it – avrebbero ricevuto un token rappresentativo del proprio investimento iniziale. L'importo del token sarebbe stato proporzionale al proprio investimento in ETH, rispetto agli ETH totali nel fondo.



Ethereum Dao Hack

- 5. “The DAO” è stato il primo fondo in assoluto decentralizzato, autonomo e gestito dalla community. L’euforia ha portato a un corposo investimento nel giro di poche settimane: 12 Milioni di Ether (\$150M nel Giugno 2016).
- 6. Ma il 17 giugno 2016, all’improvviso, gli ETH iniziarono ad essere rapidamente prosciugati dallo smart contract di “TheDAO” a una velocità di 100 ETH al secondo.
- **Il contratto aveva una vulnerabilità e l’hacker la stava sfruttando.**
- 7. Un progetto che avrebbe dovuto annunciare senza problemi una nuova era di **ingegneria finanziaria decentralizzata** aveva iniziato a perdere milioni di dollari al minuto.



{ Code is Law?

- 8. Le uniche opzioni rimaste erano: **non fare nulla o hard fork.**
- 9. I sostenitori del “codice è legge” avevano ragione: **in che modo un hard fork sarebbe stato diverso dalle procedure tradizionale di una banca centrale come i “salvataggi”?** L'intervento degli sviluppatori centrali nella politica monetaria di Ethereum ha preoccupato molti **puristi della blockchain.**
- 10. Alla fine, dopo un controverso voto della community a cui hanno partecipato solo il 5,5% degli utenti interessati, **ha vinto l'opzione hard fork.**
- 11. Quindi, **il sacrificio dell'immutabilità della blockchain.**



The Ethereum Classic Declaration of Independence

Ethereum Classic

Learn ▾ Play

Ethereum Classic Blog

The Ethereum Classic Declaration of Independence

August 13, 2016 [Ethereum Classic](#)

Announcements, Development, Education, Hard Forks, Teams

The content on this website is user-generated and solely for informational purposes. Do not interpret any content as an endorsement of any product or service. There's "no official anything" in Ethereum Classic. Always do your own research, and remember: don't trust, verify!

Let it be known to the entire world that on July 20th, 2016, at block 1,920,000, we as a community of sovereign individuals stood united by a common vision to continue the original Ethereum blockchain that is truly *free from censorship, fraud or third party interference*. In realizing, that the blockchain represents absolute truth, we stand by it, supporting its immutability and its future. We do not make this declaration lightly, or without forethought to the consequences of our actions.

Looking Back

It should be stated with great gratitude, that we acknowledge the creation of the Ethereum blockchain platform by the Ethereum Foundation and its founding developers. It certainly can be said without objection, that without their hard work and dedication that we as a community would not be, where we are today.

From its inception, the Ethereum blockchain was presented as a decentralized platform for "applications that run exactly as programmed without any chance of fraud, censorship, or third-party interference" [1]. It provided a place for the free association of ideas and applications from across the globe without fear of discrimination, while also providing pseudonymity. In this decentralized platform, many of us saw great promise.

Crediamo:

- *in una blockchain decentralizzata, resistente alla censura e senza autorizzazioni.*
- *nella visione originale di Ethereum come un computer mondiale che non può essere spento, che esegue contratti intelligenti irreversibili.*
- *in un sistema in cui i fork sono possibili solo quando si correggono vulnerabilità, bug a livello di protocollo o si forniscono aggiornamenti delle funzionalità.*
- *nell'intento originale di costruire e mantenere una piattaforma di sviluppo resistente alla censura, trustless e immutabile.*

Bitcoin Obituaries

Bitcoin has died 477 times

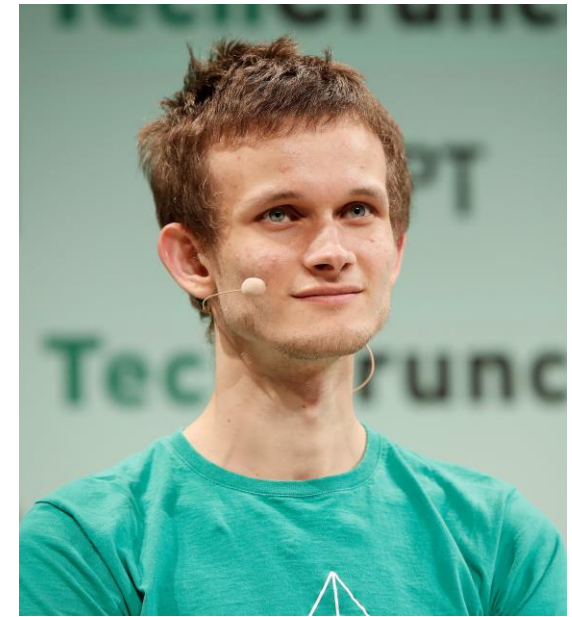
Satoshi Nakamoto
Born: Unknown

**Creator(s) of Bitcoin
Cryptocurrency**

- Pseudonym; true identity has not been verified or revealed
- Authored the Bitcoin whitepaper
- Designed first blockchain database







PRINCIPLE OF THE DAY

Larry Fink Says Tokens Are
“The Next Generation For
Markets”

**EVOLVE
OR DIE.**

@RAYDALIO