Blockchain

ORIGINI, FUNZIONAMENTO E APPLICAZIONI

Authori

MARCO PIGNATONE

DANILO GIUDICE

Data

9 MARZO 2023

Try Pitch

Agenda

Introduzione

- Premessa storica dei registri
- Struttura dei registri
- Rischi dei centralizzati

Parte 1: DLT & Blockchain

- Definizione
- Come funziona
- Tipologie

Parte 2: La Blockchain

- Cos'è
- Come funziona
- I blocchi
- Sicurezza
- Applicazioni
- I fork

Introduzione

L'ORIGINE DELLA BLOCKCHAIN

"La Blockchain costituirà per le transazioni ciò che Internet ha costituito per l’informazione"

Ginni Rometty, CEO di IBM

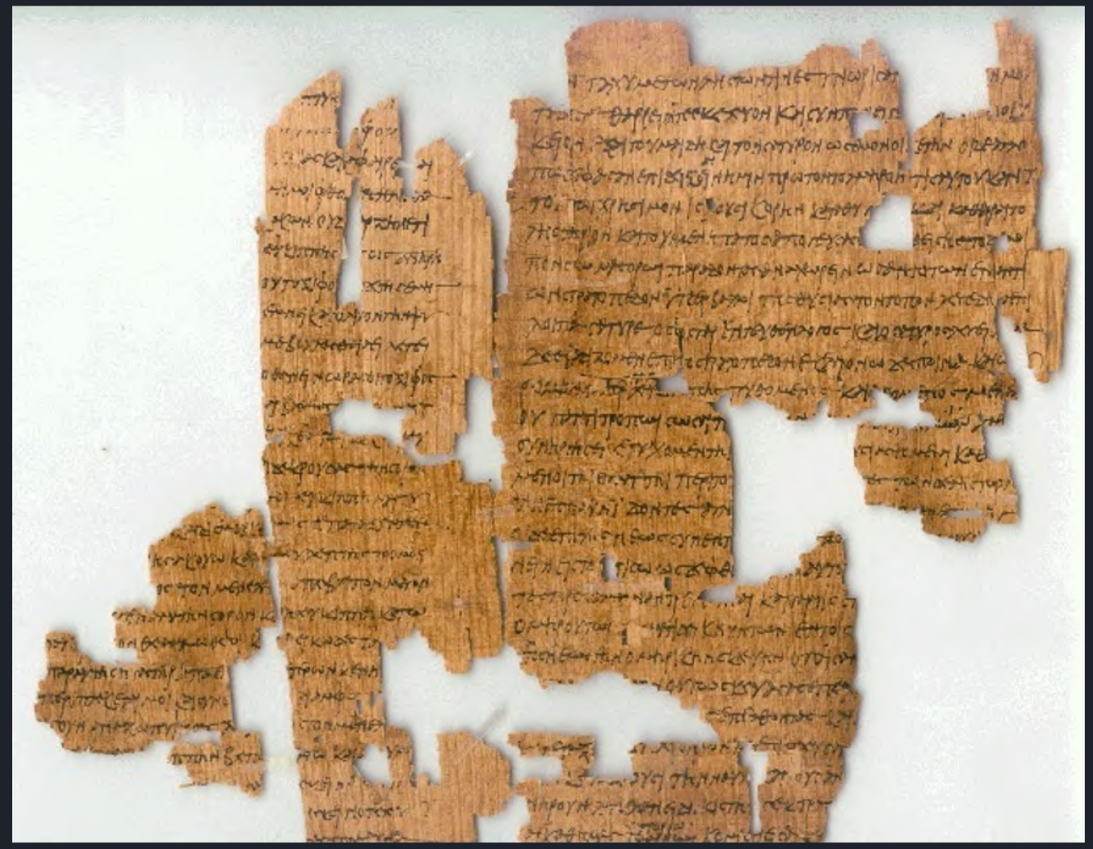
Try Pitch

Introduzione - 1

Quando parliamo di blockchain dobbiamo tenere a mente che essa non è una innovazione in senso stretto.

Blockchain, infatti, è solamente un registro ("ledger"), un libro mastro, ed esiste da secoli.

È una nuova e tecnologicamente avanzata versione di un qualcosa che esiste da migliaia di anni: più che una innovazione è una evoluzione dei classici sistemi di registrazione.



Try Pitch

Introduzione - 2

Le Pietre Rai, ad esempio, possono essere considerate una forma primitiva di registro distribuito, esse erano antiche tavolette di pietra utilizzate dalle tribù del Pacifico nell'isola di Yap, per registrare informazioni sulla storia, sulla genealogia e sulla proprietà della terra.

Ogni tribù aveva le proprie pietre rai, che venivano passate di generazione in generazione e utilizzate come registro permanente.

Try Pitch

Introduzione - 3

In generale un registro viene utilizzato per:

- dimostrare la proprietà di un asset (ad es. i catasti o gli inventari) o di una semplice transazione tra due soggetti (ad es. compravendita di un immobile);
- confermare l’identità delle persone (ad es. l'anagrafe dei cittadini o il registro delle imprese)
- definire uno status (ad es. registrazione dei matrimoni)

Try Pitch

Introduzione - 4

TIPOLOGIE DI REGISTRI

Centralizzato

Un unico nodo elaborativo (Server) che fornisce servizi ed informazioni agli altri nodi della rete (Client)

Decentralizzato

Più nodi elaborativi (Server) che forniscono servizi ed informazioni agli altri nodi della rete (Client)

Distribuito

Tutti i nodi sono uguali, contengono le medesime informazioni e forniscono i medesimi servizi agli altri nodi

Try Pitch

Introduzione - 5

RISCHI E LIMITI DEI REGISTRI CENTRALIZZATI

- Affidabilità dipendente dal funzionamento del sistema centrale (ad es. in caso di guasto si blocca l'operatività di tutti gli utenti)

- La scalabilità determinata dalle performance del sistema centrale che deve essere modificato o sostituito qualora le esigenze degli utenti aumentassero

Try Pitch

DLT & Blockchain

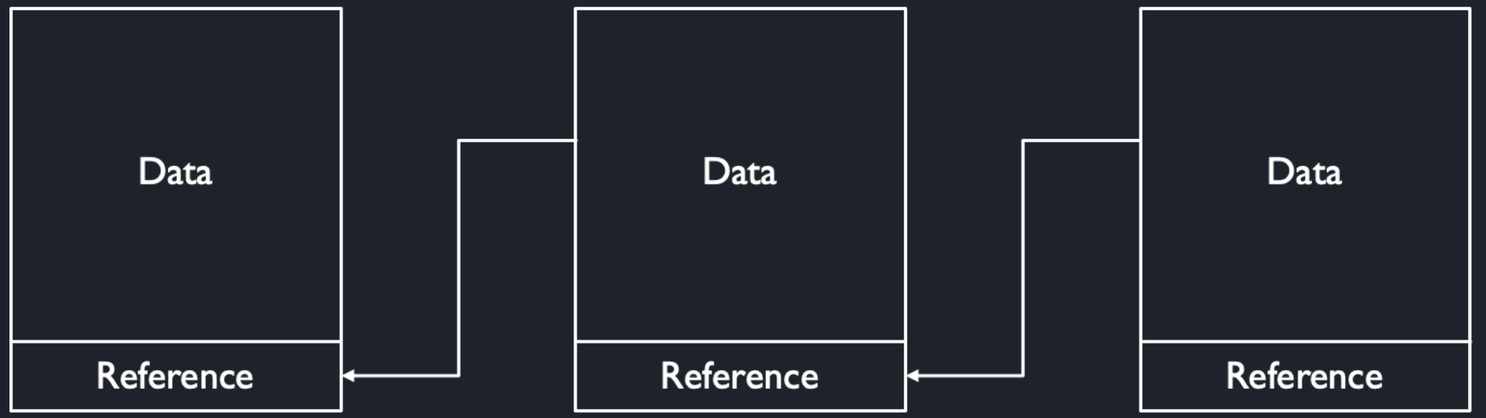
DEFINIZIONI E TIPOLOGIE

Try Pitch

DLT & Blockchain - 1

DEFINIZIONE DI BLOCKCHAIN

La Blockchain è un sistema **distribuito** che consente di registrare informazioni in modo **sicuro, trasparente e immutabile** grazie ad una struttura a blocchi concatenati e attraverso una **rete decentralizzata**.

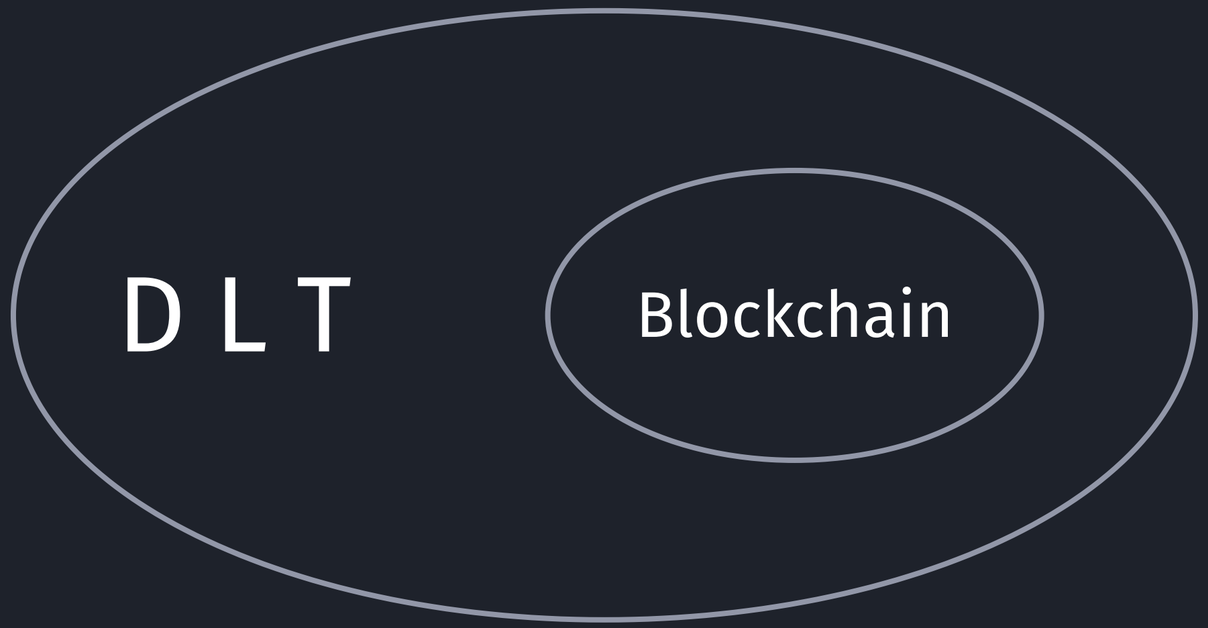


Try Pitch

DLT & Blockchain - 2

La Blockchain è innanzitutto un Registro Distribuito, anzi un **Distributed Ledger Technology (DLT)**

Tutte le Blockchain sono DLT, ma non tutti i DLT sono blockchain



Try Pitch

DLT & Blockchain - 3

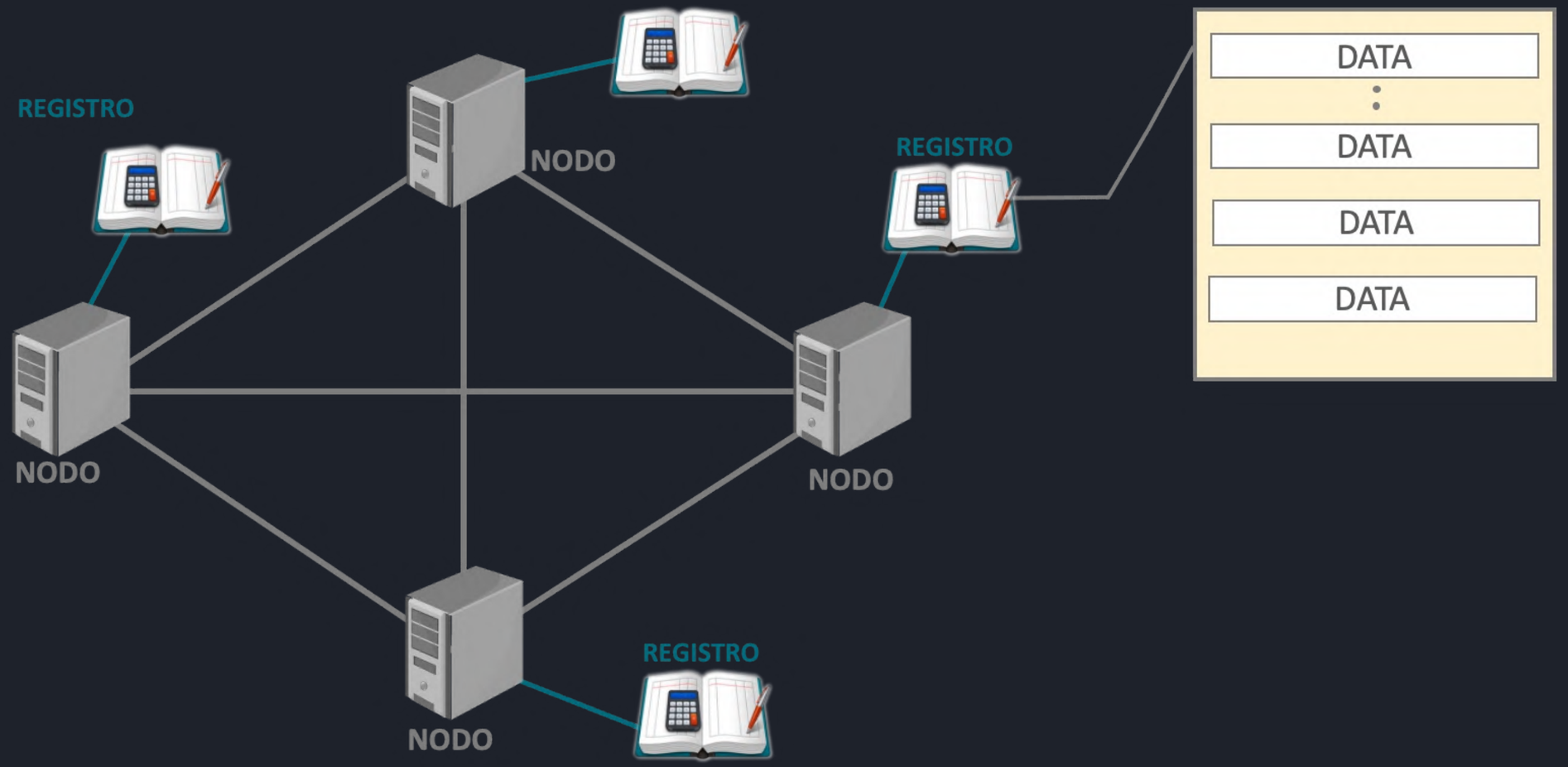
Definizione di DLT:

Sono registri caratterizzati dalla rubrica sincronizzata nel registro in diversi punti chiamati nodi che si comportano come fossero sistemi indipendenti collegati tra loro da una rete di comunicazione in cui ciascun nodo gestisce la propria copia del registro mantenuta allineata a tutte le altre.

Try Pitch

DLT & Blockchain - 4

Come funziona un registro distribuito



Try Pitch

DLT & Blockchain - 5

Criteri di distinzione dei DLT:

- Tipologia di rete
- Ruolo dei validatori
- Meccanismi di consenso
- Struttura del registro

Try Pitch

DLT & Blockchain - 6

1. Tipologie di rete:

- **Pubbliche:** sono accessibili a chiunque e non richiedono alcuna autorizzazione per accedere alla rete. Qualsiasi persona può diventare un nodo della rete, effettuare transazioni e partecipare alla verifica dei blocchi.
- **Private**: sono accessibili solo a un gruppo di utenti autorizzati e gestiti da una singola organizzazione o entità. I nodi della rete sono controllati e autorizzati dall'organizzazione, il che le rende meno decentralizzate rispetto alle Blockchain pubbliche.
- **Ibride**: sono una combinazione di Blockchain pubbliche e private, utilizzate per creare reti ibride con caratteristiche e regole personalizzate per diversi scopi.

Try Pitch

DLT & Blockchain - 7

2. Ruolo dei validatori:

- **Permissionless:** tutti gli attori possono accedere ai dati e hanno anche la possibilità di partecipare alla validazione delle transazioni senza alcuna autorizzazione

- **Permissioned**: soltanto alcuni attori esplicitamente autorizzati possono svolgere l'attività di validazione.: sono accessibili a chiunque e non richiedono alcuna autorizzazione per accedere alla rete.

Try Pitch

DLT & Blockchain - 8

3. Meccanismi di consenso:

- **Semplici**: in questi casi quando un nodo propone l’aggiunta di una transazione ne viene verificata la validità e si vota semplicemente a maggioranza sull’opportunità di aggiungerlo al registro

- **Complessi**: questi sono normalmente implementati in reti permissionless con l’obiettivo di evitare che soggetti malevoli possano creare identità fittizie e quindi modificare il registro. I principali sono:

- **Proof of Work** (PoW): è l'algoritmo di consenso utilizzato da Bitcoin e da molte altre criptovalute. Il PoW richiede che i nodi della rete risolvano complessi problemi matematici per validare le transazioni e creare nuovi blocchi. Ciò richiede una grande quantità di potenza di calcolo elettronico, noto come "mining".
- **Proof of Stake** (PoS): è un algoritmo di consenso che funziona in modo simile al PoW, ma invece di richiedere la risoluzione di complessi problemi matematici, richiede che i nodi della rete blocchino un certo numero di token o criptovaluta per dimostrare il loro interesse nella validazione delle transazioni.

Try Pitch

DLT & Blockchain - 8

PROOF OF WORK

- Il nodo che riuscirà a risolvere il problema matematico (**estrazione del blocco**) avrà il diritto di validare il blocco con la presentazione della **Proof of Work** che è anche la prova della soluzione al problema matematico.
  •Per questo impegno e per questo risultato, il nodo viene appunto remunerato con una unità o parte di unità di valore che dipende dalla tipologia di blockchain.
- Va poi aggiunto che nelle blockchain i nodi non sono “pubblici”, ovvero non si conoscono fra loro e il **Proof of Work** rappresenta anche il modo per costruire un rapporto di “fiducia” basato sulla concreta collaborazione alla soluzione delle prove che devono essere validate.

PROOF OF STAKE

- L’algoritmo PoS stabilisce che per minare blocchi è necessario possedere e bloccare più o meno grandi quantità di criptovaluta (definito staking, o “mettere in gioco” più informalmente).Più grande è la quantità di criptovalute posseduti da un utente, maggiori sono le probabilità che non stia violando il sistema.
- I blocchi nel meccanismo PoS, non vengono estratti, ma coniati. I partecipanti che possiedono una partecipazione significativa nei sistemi Proof of Stake vengono selezionati su base pseudocasuale per coniare i blocchi e aggiungerli alla blockchain.

DLT & Blockchain - 9

4. Struttura del registro:

- **Ledger**: le informazioni sono validate e registrate a livello di singola transazione proprio come avviene nei registri cartacei;

- **Blockchain**: più transazioni vengono raccolte all'interno di un blocco che viene validato e registrato a livello aggregato e che viene concatenato al precedente tramite crittografia;

- **Tangle**: una particolare tipologia di registro con una struttura basata su grafici di anticiclici diretti in cui le transazioni vengono processate in parallelo e non in modo sequenziale come nei precedenti

Try Pitch

La Blockchain

DEFINIZIONE E FUNZIONAMENTO

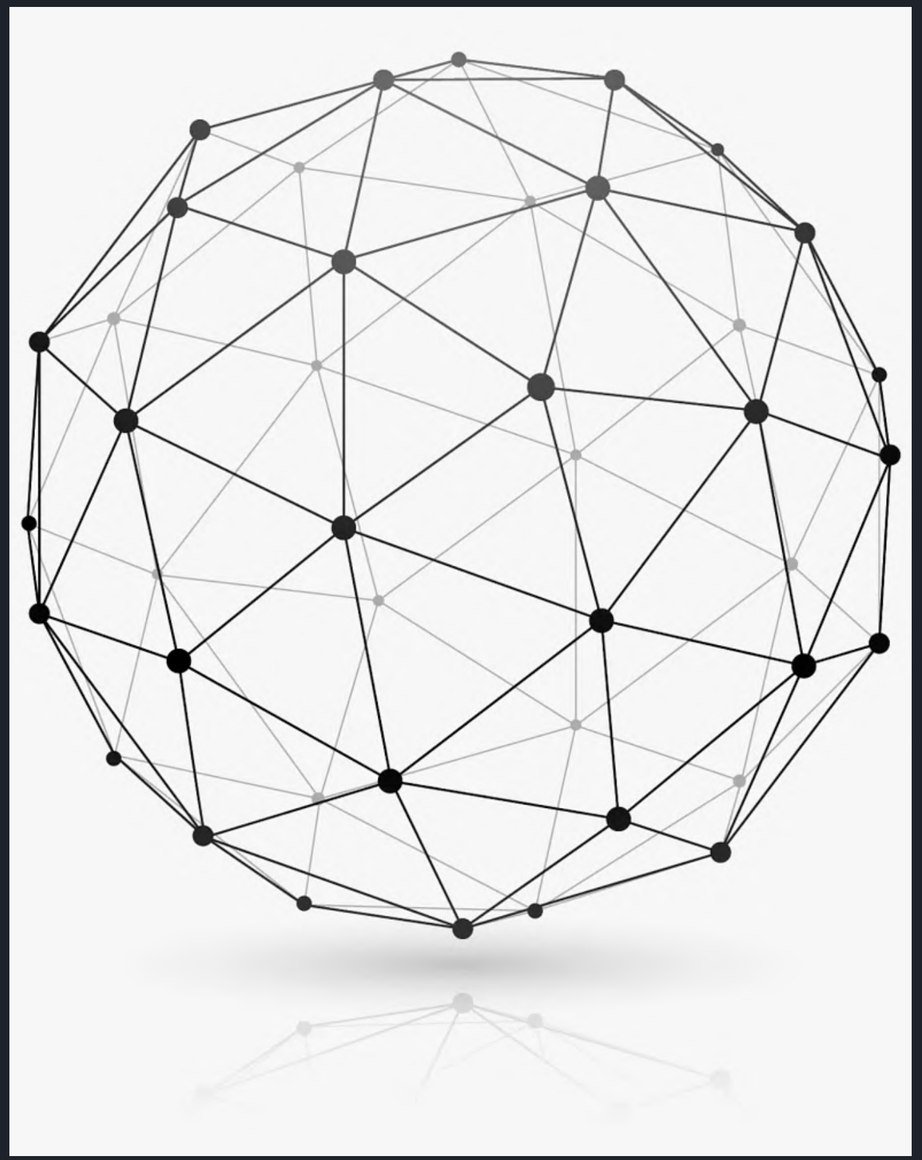
Try Pitch

La Blockchain - 1

COSA È

La Blockchain basa il suo funzionamento su un registro, distribuito attraverso gli attori del suo network (**Nodi**), ognuno dei quali possiede una copia di questo registro.

Questa "**catena di blocchi**" rappresenta la totalità delle informazioni scambiate tra i Nodi. Ogni blocco della catena contiene le informazioni (**transazioni**) scambiate tra i nodi, che devono essere verificate e approvate da tutti, attraverso **algoritmi di crittografia complessi**.



Try Pitch

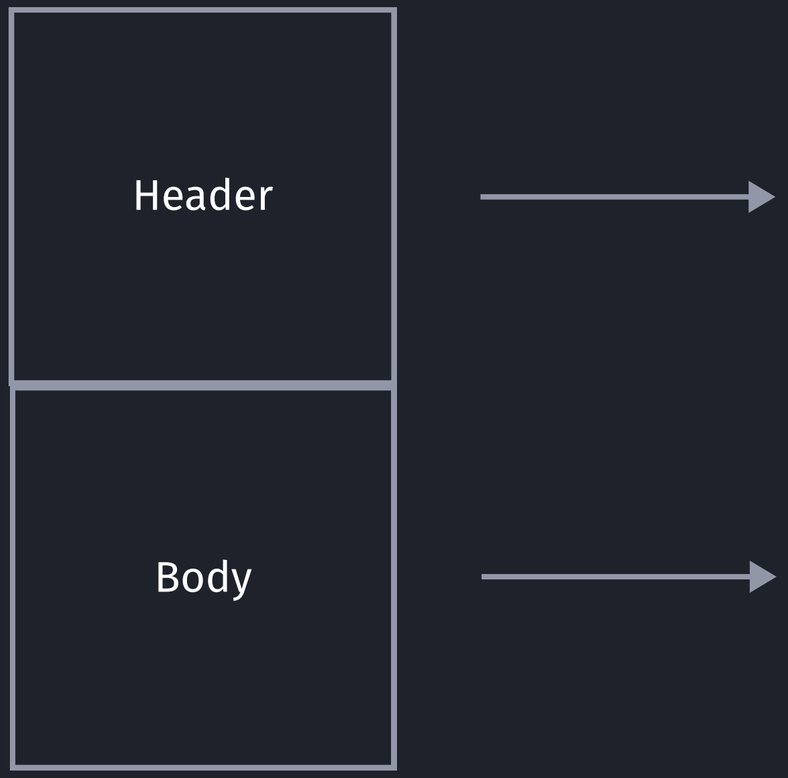
La Blockchain - 2

COSA E' E COME FUNZIONA

Try Pitch

La Blockchain - 3

Il Contenuto del blocco:



- Numero del blocco
- Codice hash del blocco
- Codice hash del blocco precedente
- Timestamp
- Totale delle coin movimentate
- Dimensione del blocco in Kb

- Tutte le transazioni contenute nel blocco

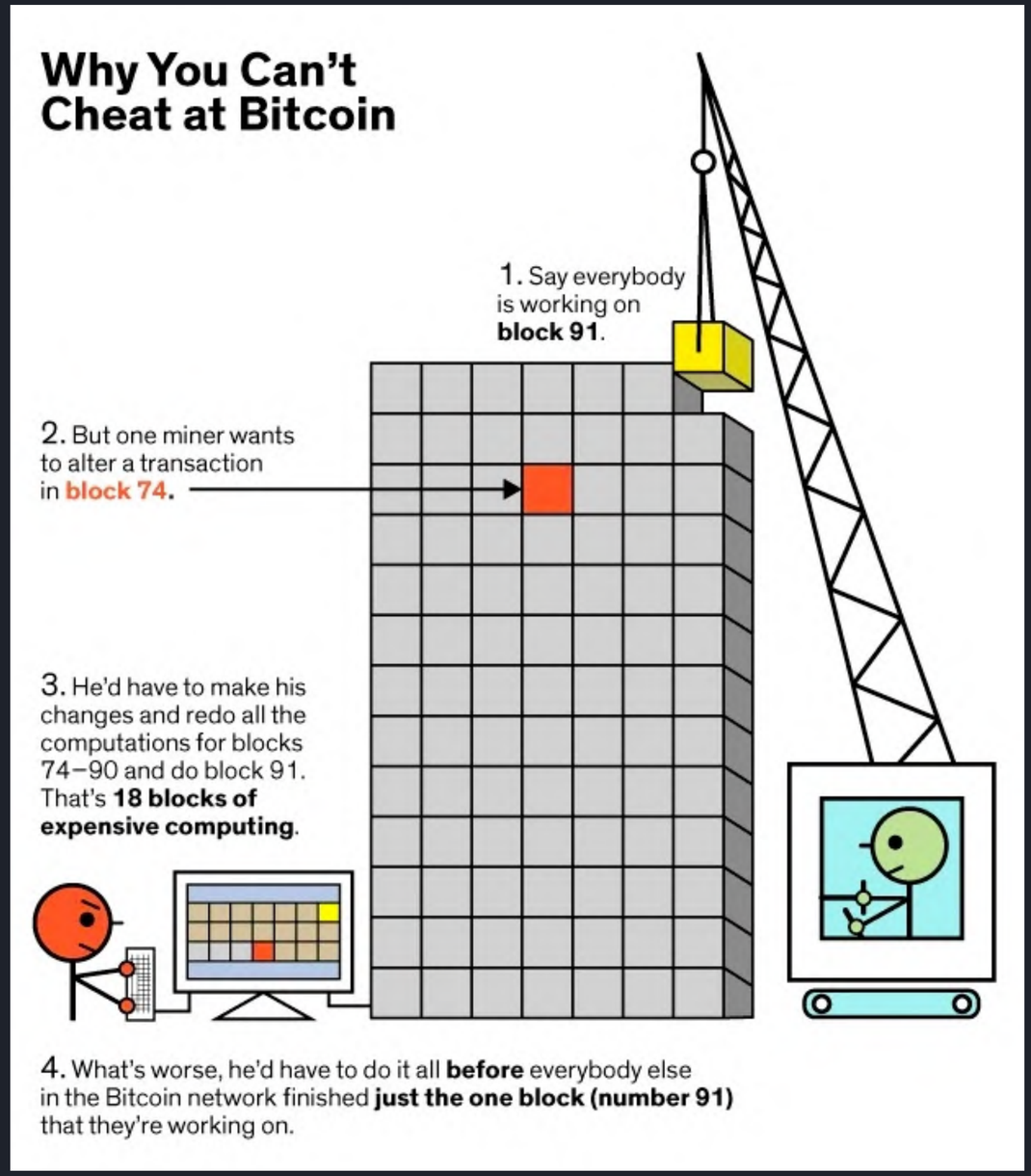
Try Pitch

La Blockchain - 4

COME FUNZIONA

Ogni transazione approvata viene quindi aggiunta al blocco successivo, costituendo una catena di informazioni collegate tra loro e distribuite per poter essere incontrovertibili.

Ogni blocco è quindi legato al precedente e necessita dell'approvazione di tutti i nodi per essere modificato.
Più si andrà avanti con la validazione dei blocchi maggiore sarà il lavoro necessario a modificare un blocco passato: questo significa **immutabilità del dato.**



Try Pitch

La Blockchain - 5

Caratteristiche comuni:

- **Disintermediazione**: le piattaforme consentono di gestire le transazioni senza intermediari, ossia senza la presenza di enti centrali fidati
- **Decentralizzazione**: le informazioni sono registrate distribuendole tra più nodi per garantire sicurezza informatica e resilienza dei sistemi
- **Immutabilità del registro**: una volta scritti sul registro, i danti non possono essere modificati senza il consenso della rete
- **Trasparenza del registro**: il contenuto del registro è aperto e visibile a tutti
- **Tracciabilità dei trasferimenti**: ciascun elemento rappresentato sul registro è tracciabile e se ne può risalire all'esatta provenienza
- **Programmabilità dei trasferimenti**: possibilità di programmare determinate azioni che vengono effettuate al verificarsi di certe condizioni
- **Digitalizzazione**: rappresentazione dei dati ed eventualmente anche degli asset fisici in formato digitale

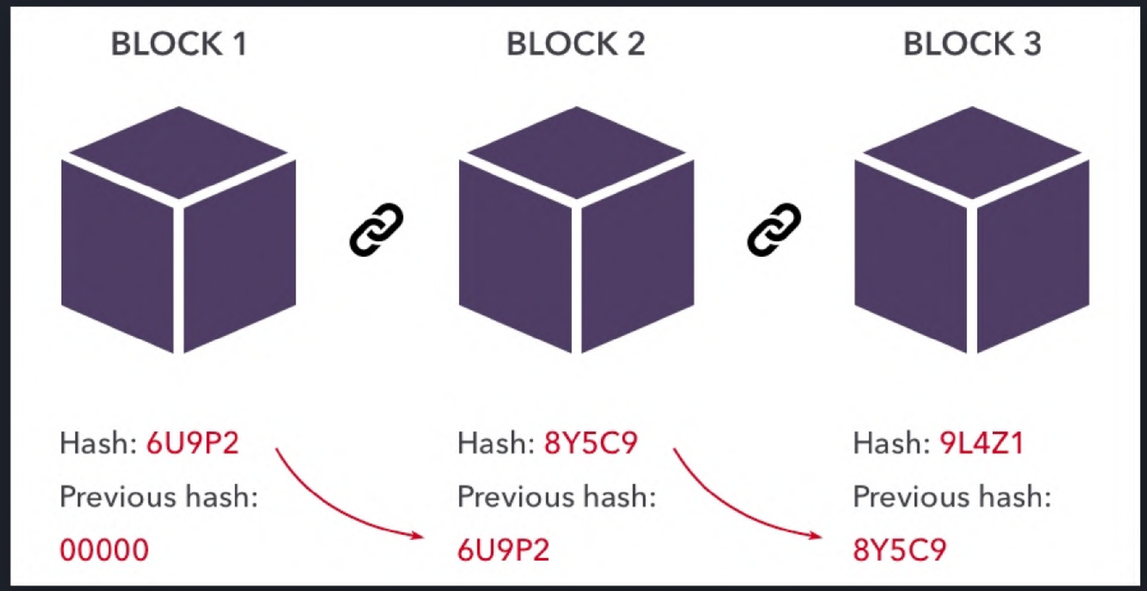
Try Pitch

La Blockchain - 6

APPLICAZIONI DELLA BLOCKCHAIN

Ecco un elenco delle possibili applicazioni della tecnologia Blockchain:

- Criptovalute
- Gestione delle identità
- Tracciabilità e rintracciabilità
- Gestione dei diritti d'autore
- Votazione elettronica
- Contratti intelligenti
- Salute

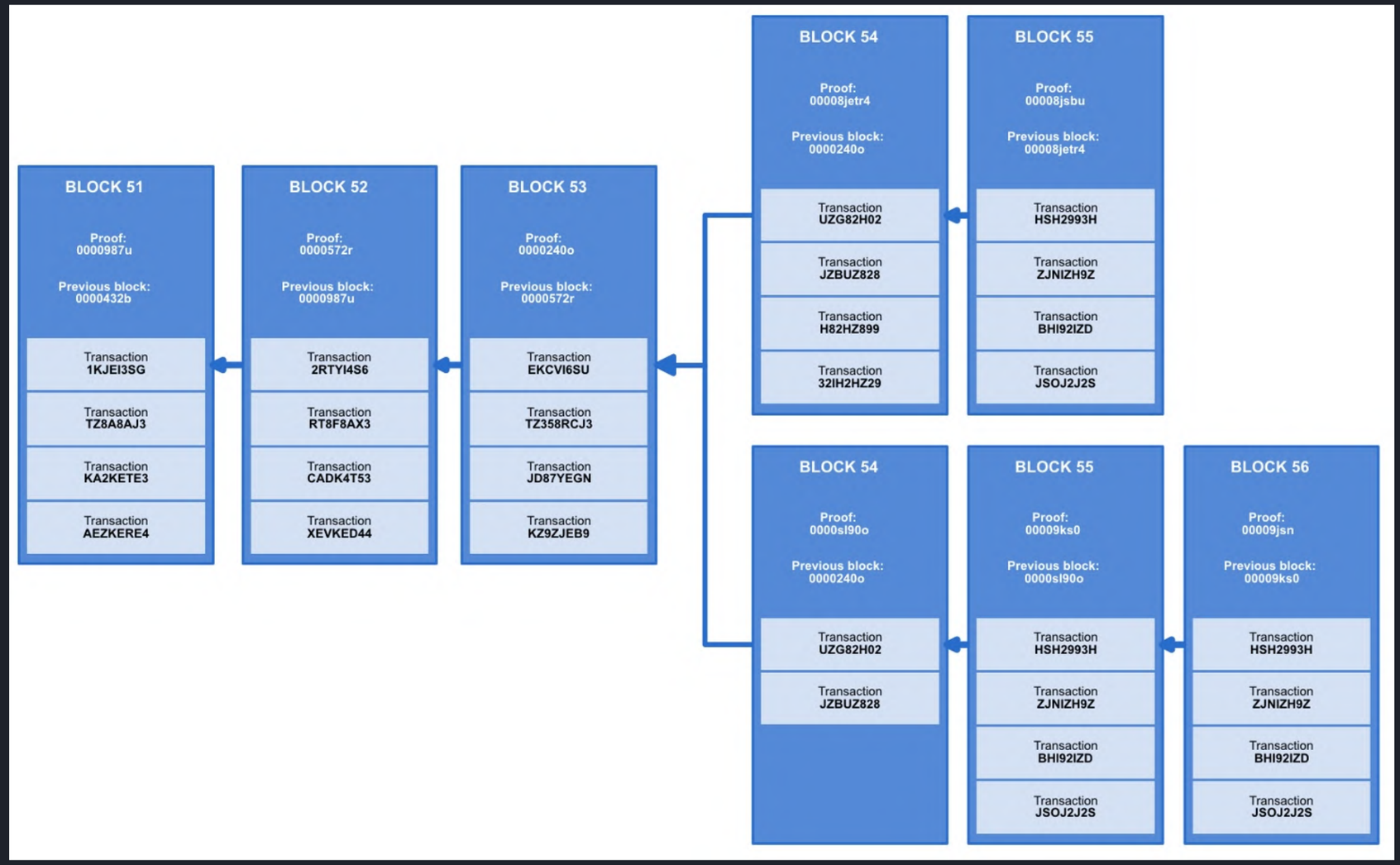


Catena di Blocchi e hash che li lega

Try Pitch

La Blockchain - 7

I FORK



Try Pitch

Bitcoin

ORIGINI, FUNZIONAMENTO E APPLICAZIONI

Authors

MARCO PIGNATONE

DANILO GIUDICE

Date

TODAY'S DATE

Try Pitch

Agenda

Introduzione: Le origini di Bitcoin

Parte 1: Cos'è e come funziona

Parte 2: POW e mining

Parte 3: Bitcoin green

Parte 4: Bitcoin è morto

Introduzione

LE ORIGINI DI BITCOIN

"Se non mi credete o non lo capite, non ho tempo per cercare di convincervi, mi dispiace".

- Satoshi Nakamoto

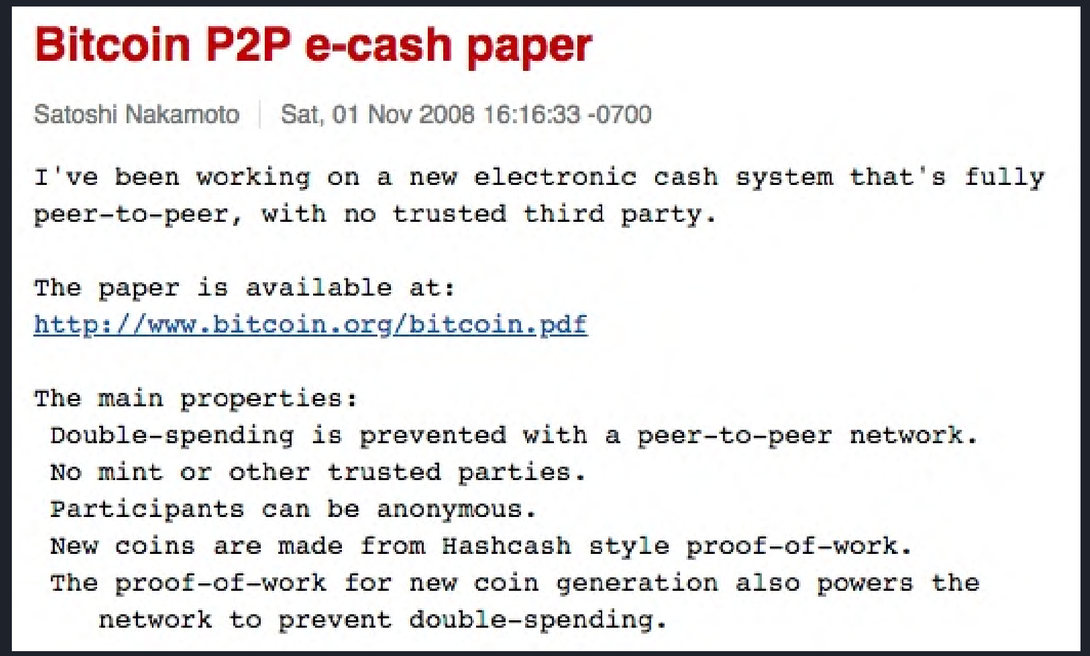
Try Pitch

Storia dell'origine di Bitcoin

SATOSHI NAKAMOTO

Nel 2008, un gruppo o una singola persona con lo pseudonimo di Nakamoto, ha espresso tramite mailing list la volontà di creare un sistema di pagamento digitale decentralizzato ed indipendente.

Nel 2009 ha rilasciato il codice sorgente di Bitcoin e ha avviato la sua rete, che ha permesso agli utenti di effettuare transazioni in modo sicuro e anonimo senza la necessità di intermediari.



Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

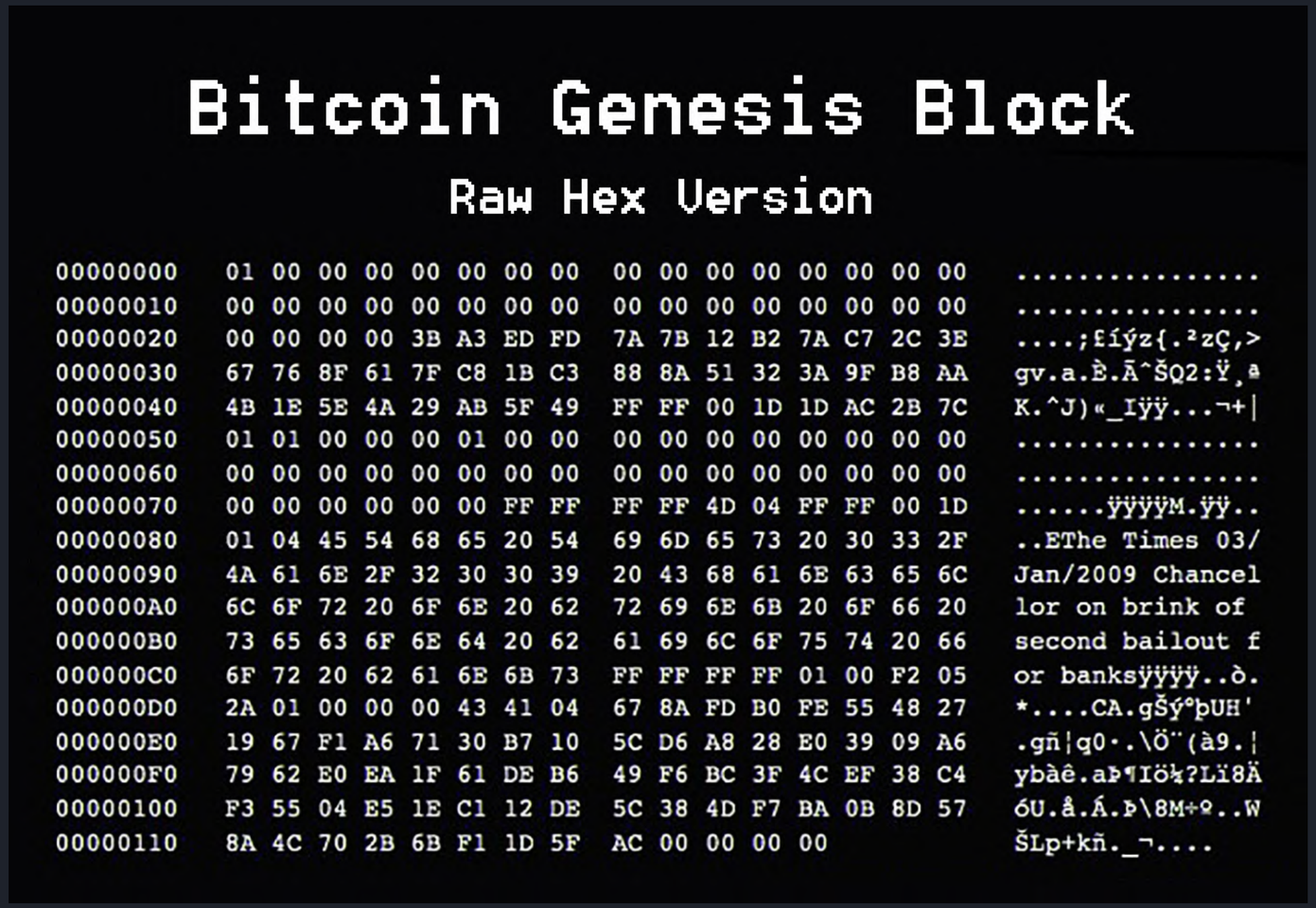
The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Try Pitch

Bitcoin Genesis Block

Raw Hex Version



```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00           ŠLp+kñ._¬....
```

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

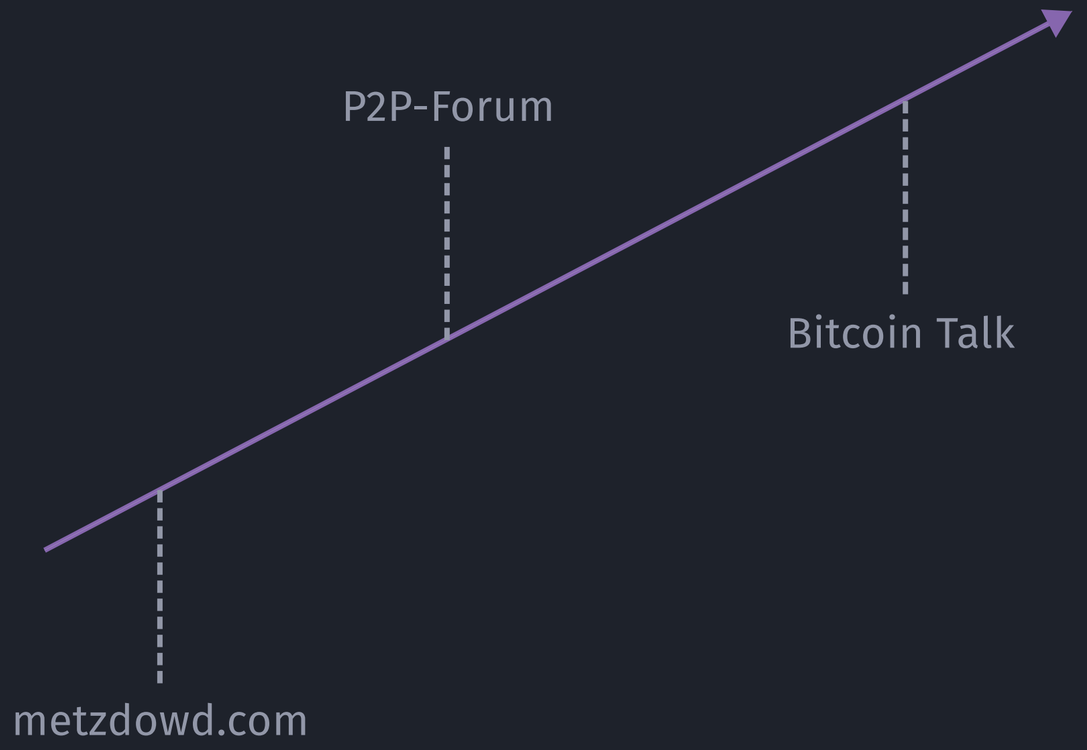
Try Pitch

Storia dell'origine di Bitcoin

SATOSHI NAKAMOTO

La storia di Satoshi Nakamoto, è avvolta nel mistero: non ha mai rivelato la propria vera identità ed è rimasto completamente anonimo durante tutto il processo di creazione di Bitcoin, che ha gestito lavorando con una comunità di sviluppatori e utenti della rete tramite la mailing list di **metzdowd.com**

Successivamente la community si è spostata dapprima su **P2P-Forum** per finire con la creazione di **Bitcoin Talk**, oggi principale forum di discussione legato alla comunità Bitcoin.



Try Pitch

Storia dell'origine di Bitcoin

SATOSHI NAKAMOTO

Nel 2011, dopo due anni di lavoro sul progetto Bitcoin, Nakamoto ha annunciato la propria uscita dal progetto senza fornire una motivazione specifica. Da allora, non è piu apparso online, spingendo la community alle piu disparate tesi sulla sua identità.

Nonostante la sua (o loro) identità rimanga un mistero, la creazione di Bitcoin e la tecnologia Blockchain, hanno avuto un impatto significativo sul mondo della finanza e della tecnologia, e ha aperto la strada a molte innovazioni e sviluppi futuri.

Try Pitch

Come funziona Bitcoin

IL WHITEPAPER

Una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un'entità ad un'altra senza passare tramite un'istituzione finanziaria. Le firme digitali offrono una soluzione parziale al problema, ma i benefici principali sono persi se una terza persona di fiducia è ancora richiesta per prevenire la doppia spesa. Proponiamo una soluzione al problema della doppia spesa mediante l'utilizzo di una rete peer-to-peer. La rete stampa un marcatore temporale sulle transazioni facendo hashing sulle stesse e incatenandole in una catena di proof-of-work basata sugli hash, formando una registrazione che non può essere modificata senza rifare la proof-of-work. La catena più lunga non solo serve come prova della sequenza di eventi ai quali si è assistito, ma anche come prova che essa proviene dal gruppo più grande di potenza CPU. Fintanto che la maggior parte della potenza CPU è controllata da nodi che non cooperano per attaccare la rete, questi genereranno la catena più lunga e supereranno gli utenti malintenzionati. La rete stessa richiede una struttura minimale. I messaggi sono trasmessi su base best effort, e i nodi possono lasciare e ricongiungersi con la rete a loro piacimento, accettando la catena proof-of-work più lunga come prova di quello che è avvenuto mentre erano non erano presenti.

Try Pitch

Come funziona Bitcoin

LE TECNOLOGIE DI CUI FA USO BITCOIN

- **Blockchain:** Bitcoin utilizza la tecnologia Blockchain per creare un registro distribuito, sicuro e permanente di tutte le transazioni effettuate sulla rete.
- **Crittografia ECDSA:** Bitcoin utilizza algoritmi di crittografia per garantire la sicurezza delle transazioni e la protezione delle chiavi private degli utenti come la Crittografia Asimmetrica (ECDSA).
- **Protocollo peer-to-peer (P2P):** Bitcoin utilizza un protocollo P2P per consentire agli utenti di connettersi alla rete Bitcoin e di effettuare transazioni in modo diretto e sicuro senza la necessità di intermediari.
- **Algoritmo di Consenso (PoW):** Bitcoin utilizza l'algoritmo di consenso Proof-of-Work per validare e confermare le transazioni sulla rete. Questo processo richiede che gli utenti risolvano problemi matematici complessi, utilizzando una grande quantità di potenza di calcolo.
- **Modello di Sviluppo (Open Source):** Bitcoin basa il suo modello di sviluppo sull'Open Source, dove il codice sorgente del software è pubblico ed accessibile a chiunque voglia verificarne il funzionamento o proporne delle modifiche.

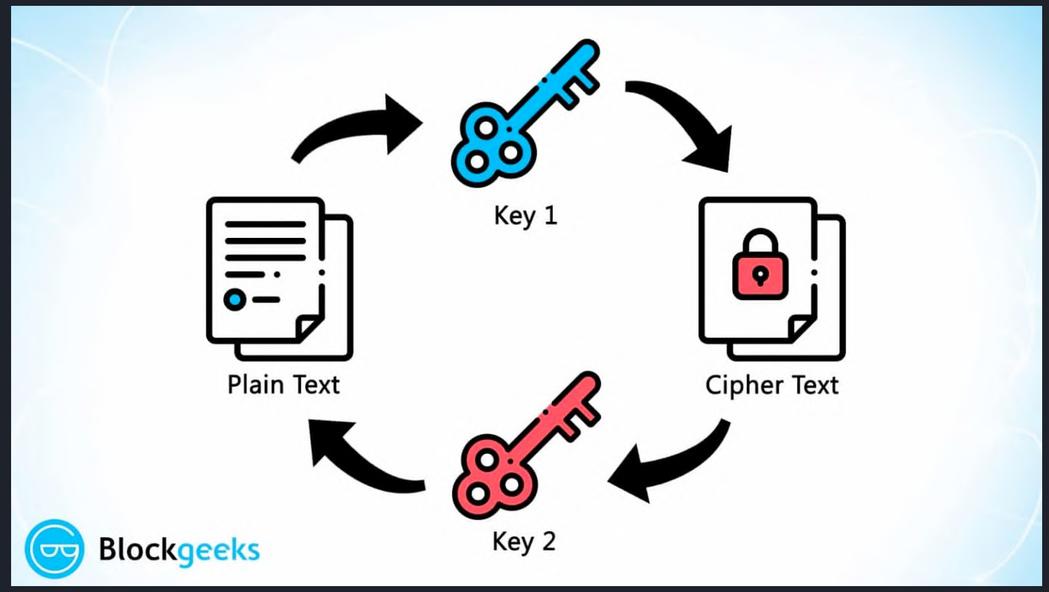
Try Pitch

Crittografia ECDSA

ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

La crittografia **ECDSA** è un algoritmo di firma digitale utilizzato da Bitcoin per garantire la sicurezza delle transazioni e la protezione delle chiavi private degli utenti.

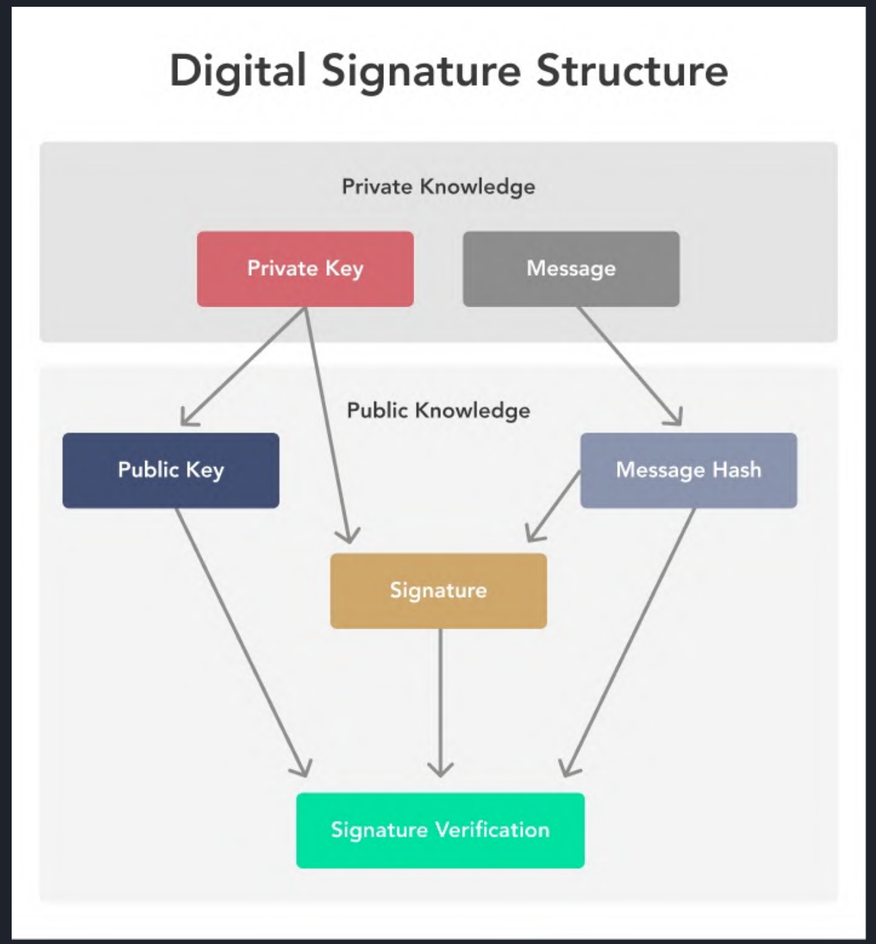
Essa è una **crittografia a chiave pubblica**, che si basa sull'utilizzo di due chiavi diverse, una **chiave pubblica** e una **chiave privata**, per crittografare e decrittografare le informazioni.



Try Pitch

Crittografia ECDSA

FIRME DIGITALI, CHIAVI PUBBLICHE & PRIVATE



L'ECDSA utilizza la crittografia a curva ellittica per generare le chiavi e le firme digitali.

Per utilizzare questo metodo, ogni utente crea due "chiavi": una **chiave pubblica** che può essere condivisa liberamente e una **chiave privata** che deve essere tenuta segreta.

Quando un utente vuole inviare una transazione, usa la sua chiave privata per "firmare" la transazione, come "sigillo" che garantisce l'autenticità della transazione e l'identità dell'utente che l'ha inviata. Gli altri utenti possono quindi verificare la firma utilizzando la chiave pubblica dell'utente, confermando che la transazione è stata effettivamente inviata da quella persona e che non è stata manipolata.

Try Pitch

Come avviene una transazione

Try Pitch

Crittografia ECDSA | FIRME DIGITALI, CHIAVI PUBBLICHE & PRIVATE

La chiave pubblica è come una serratura che può essere vista e usata da chiunque per ricevere denaro quell'utente.

La chiave privata, invece, è come una chiave che sblocca la serratura e permette all'utente di inviare denaro ad altri utenti.

Quando un utente invia una transazione, deve utilizzare la sua chiave privata per "sbloccare" la serratura della sua chiave pubblica e firmare la transazione. Questa firma funziona come una sorta di "timbro di approvazione" che garantisce l'autenticità e l'integrità della transazione.

Gli altri utenti sulla rete possono quindi utilizzare la chiave pubblica dell'utente per "bloccare" la serratura e verificare la firma.
In questo modo, la chiave pubblica funziona come una serratura che può essere aperta solo dalla chiave privata corrispondente, garantendo che solo l'utente autorizzato possa inviare denaro e che le transazioni siano sicure e protette.
In sintesi, possiamo pensare alla crittografia ECDSA come a una serratura e una chiave, in cui la chiave pubblica funziona come una serratura che può essere sbloccata solo dalla chiave privata corrispondente, garantendo la sicurezza delle transazioni sulla rete Bitcoin.

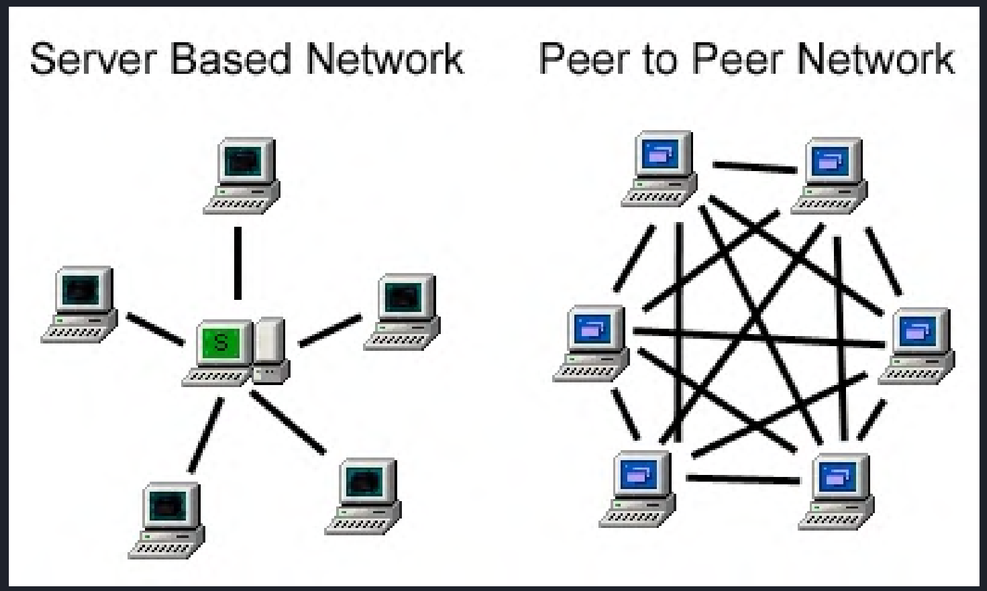
Try Pitch

Protocollo P2P

COME FUNZIONA

Il protocollo P2P (Peer-to-Peer) consente agli utenti di connettersi e interagire direttamente sulla rete Bitcoin, senza intermediari o autorità centrali.

- La rete Bitcoin è decentralizzata, in cui ogni nodo ha le stesse funzioni e responsabilità.
- I nodi si connettono tra loro attraverso il protocollo Internet e si scambiano informazioni e transazioni sulla rete.
- Le transazioni sono convalidate e confermate sulla rete in modo distribuito e sicuro, senza la necessità di una autorità centrale.
- La decentralizzazione e la distribuzione del protocollo P2P rendono la rete Bitcoin sicura, resistente alle interruzioni e indipendente dalle autorità centrali.



Try Pitch

Proof-Of-Work

ALGORITMO DI CONSENSO

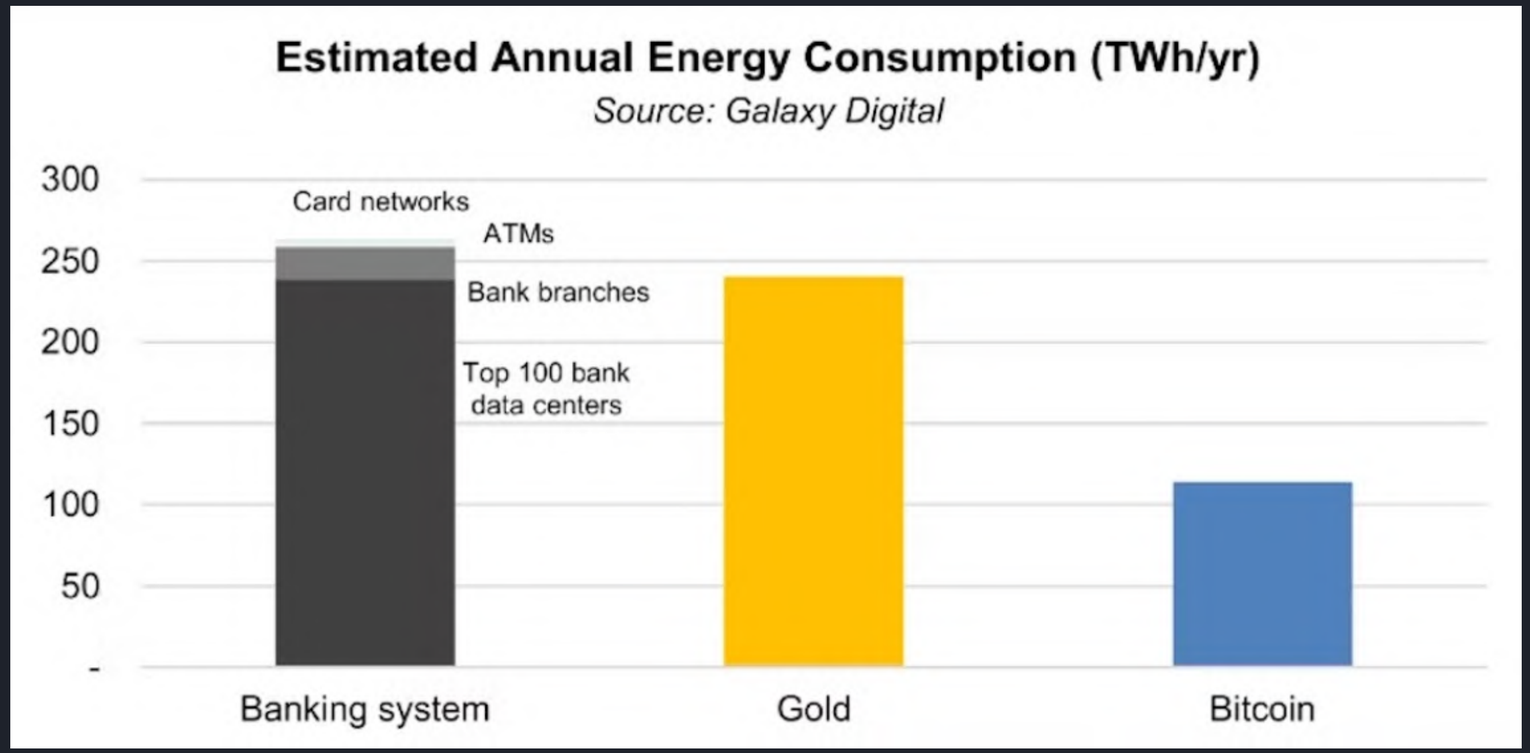
Quando due nodi si scambiano un'informazione un terzo nodo, chiamato **Miners**, si occuperà di validarla. Per farlo dovrà risolvere complessi calcoli matematici con l'ausilio di elaboratori molto potenti. Questa è la "**Proof of Work**" che premierà il nodo che riuscirà a risolvere questi calcoli nel minor tempo possibile aggiudicandosi il conio di nuova moneta.

Potete immaginare questi calcoli come la risoluzione di un rompicapo, come il cubo di rubik in una competizione: **il primo a risolverlo potrà validare il blocco di transazioni e aggiudicarsi la ricompensa.**

Try Pitch

Bitcoin green

Quanto consuma davvero Bitcoin?



Try Pitch

Bitcoin è morto

“Why Bitcoin can’t be a currency” – The Underground Economist | $0.23

By JORDAN TUWINER Last updated on February 4, 2021 at 11:36 No Comments

> *Negative feedback loops like this are basically homeostasis. In nature, positive feedback loops like exist with Bitcoin are lethal; the only thing that’s even kept Bitcoin alive this long is its novelty. Either it will remain a novelty forever or it will transition from novelty status to dead faster than you can blink.*

Try Pitch