# Blockchain CheatSheet - La Visione

**Tempo di lettura: 9 Min**

---

## Indice

- Il Meccanismo del Fork
- Lezioni

## § Blockchain Private

- Applicazioni Speciali

## § Caratteristiche della Visione Blockchain

- Rischi delle Criptovalute

# § Bitcoin

## Panoramica

Una base di dati distribuita peer-to-peer come un libro mastro pubblico che dimostra la proprietà.
Nessuna necessità di fiducia: le caratteristiche dei blocchi e la proprietà sono mantenute nella cronologia immutabile della catena (libri).
Sicurezza ed efficienza tramite una solida crittografia e la rete di computer più potente.
I miner offrono sicurezza tramite un sistema di ricompensa.

## Hashing

I blocchi della blockchain di Bitcoin sono naturalmente riempiti di dati ogni 10 minuti, una pratica stabilita dal 2009.

**Specifiche della catena**:

- Ogni ultima riga (Hash) di un blocco è un hash SHA-256 dei dati del blocco.
- Questo hash diventa la prima riga del blocco successivo.
- Se modifichi un blocco, anche il suo hash SHA-256 cambia.
- Questa modifica interrompe la catena, poiché la prima riga del blocco successivo non corrisponde più.

## Mining nel Proof of Work

- **Scopo**: Garantire l'immutabilità della blockchain.
- **Come si fa**: Si aggiungono nonce (numeri usati una sola volta) alla fine dell'hash di ogni blocco per trovare un hash con un certo numero di zeri all'inizio, che valida il blocco.
- **Perché**: Il sistema richiede una prova che è stata fatta del lavoro. Trovare un hash con un certo numero di zeri all'inizio è difficile e richiede molti tentativi, dimostrando che è stato fatto lavoro.
- **Sicurezza**: Questo processo rende difficile per qualcuno modificare i dati senza rifare tutto il lavoro computazionale, rafforzando così la sicurezza della blockchain.

# § Ethereum e Blockchain di Nuova Generazione

**Evoluzione e miglioramento della blockchain di Bitcoin**

Oggi Ethereum è considerata una delle tecnologie principali per le applicazioni commerciali. Mantiene tutte le funzioni di Bitcoin e consente di integrare piccole applicazioni all'interno dei blocchi. Questo permette di costruire un sistema informatico decentralizzato utilizzando la struttura della blockchain. Inoltre, amplia l'ambito dei dati utilizzabili sulla blockchain e migliora, con la tecnologia degli Smart Contracts, le capacità delle transazioni.

**Alcune dimensioni**:

- **Wei**: Moltiplicatore $10^0$
- **Szabo**: Moltiplicatore $10^{12}$
- **Finney**: Moltiplicatore $10^{15}$
- **Ether**: Moltiplicatore $10^{18}$

## Concetto di Smart Contracts

- **Aggiornamenti di stato programmabili**
  - Può aggiungere qualsiasi funzionalità desiderata.
- **Può consentire l'accesso e la distribuzione di fondi basati su condizioni stabilite**
- **Può creare, trasferire e modificare beni digitali**
- **Interagisce con altri contratti per creare applicazioni robuste e interoperabili**
- **Base per l'Internet del valore**

## App Decentralizzate (dApps)

Come già detto, Ethereum e altre blockchain di nuova generazione consentono lo sviluppo di App Decentralizzate (dApps). Queste app utilizzano tecnologie come gli Smart Contracts per la logica dell'applicazione, IPFS o Swarm per la memorizzazione dei dati, Ethereum Name Service (**ENS**) per la denominazione decentralizzata e Whisper per la comunicazione decentralizzata tra app.

**Spiegazione**

- **Ethereum e Blockchain di Nuova Generazione**: Queste piattaforme supportano lo sviluppo di dApps e permettono soluzioni innovative e decentralizzate.
- **Smart Contracts**: Utilizzati per implementare la logica e le regole delle dApps.
- **IPFS o Swarm**: Soluzioni di memorizzazione decentralizzate per il salvataggio e il recupero dei dati.
- **Ethereum Name Service (ENS)**: Fornisce un DNS decentralizzato per nomi leggibili.
- **Whisper**: Un protocollo per la comunicazione decentralizzata che consente una comunicazione sicura tra le dApps.

**Contesto**

- **App Decentralizzate (dApps)**: Applicazioni che funzionano su una rete decentralizzata e utilizzano la tecnologia blockchain per garantire sicurezza, trasparenza e affidabilità.

> In definitiva, è saggio considerare Ethereum come la prima idea rivoluzionaria e brillante che ha portato alla creazione dello strato fondamentale per l'Internet del valore e delle applicazioni decentralizzate.

---

# § Memorizzazione

## Tipi di Conto

**Conti Gestiti Esternamente (EOA)**

- Conti gestiti da persone
- Sistema di chiavi pubbliche e private per gestire le transazioni

**Conti Contrattuali**

- Conti con codice incorporato che vengono gestiti dopo la creazione
- Possono contenere e trasferire BTC, ETH o altri token
- Non modificabili tranne che dal codice incorporato

## Wallet

**Definizione**: Uno strumento che consiste in uno o più conti utilizzati per memorizzare e trasferire BTC, ETH o altri token.

**Multisig**: Divide le tue chiavi per aumentare la sicurezza richiedendo più firme per approvare una transazione.

---

# § Criptovalute

**Prima Generazione/Oro 2.0**:

- **Bitcoin (BTC)**: La blockchain madre è limitata, così come **Litecoin (LTC)**.

**Tokens per Calcoli Distribuiti**:

- **Ethereum (ETH)**: Rivoluziona l'industria permettendo piccole applicazioni sul sistema blockchain. Altri progetti in questa categoria sono **Tezos (XTZ)**, **EOS** e **DFinity**.

## Tokens

*Contrariamente alle monete che hanno blockchain dedicate, i tokens esistono e dipendono dalla blockchain specifica su cui sono creati.*

**Utility Tokens**:

- Utilizzati con asset blockchain programmabili, come **Storj**, **Golem (GNT)**, **Sia (SC)** e **FileCoin**.

**Security Tokens**:

- Rappresentano azioni, obbligazioni o altri beni, consentendo l'uso dei token per tali scopi.

**Fungible Tokens**:

- **ERC-20 Token della Blockchain Ethereum**: Un protocollo che lega qualcosa a un token specifico che viene referenziato come asset sulla blockchain Ethereum.

**Non-Fungible Tokens (NFTs)**:

- **ERC-721 Token della Blockchain Ethereum**: Un protocollo che assegna valore a un nuovo token unico, come avviene con le opere d'arte.

**Stablecoins**:

- **Collateralizzati da Fiat**: Indicizzati sul valore di valute fiat come **EURC** o **USDT**.
- **Krypto-Fiat-Nazionali**: Come **Eurocoin** o **Fedcoin**.
- **Collateralizzati da Attivi Fisici**: Come **Digix Gold (DGX)** o **Swiss Real Coin (SRC)**.
- **Non-Collateralizzati**: Come **Basecoin**.

Questi, per le menti più imprenditoriali, potrebbero alla fine rappresentare il futuro dei contratti intelligenti e dell'economia digitale. In questo senso, è importante avere un quadro generale del fenomeno della criptovaluta e del suo impatto sulla finanza globale.

---

# § Gas

## Il Problema

Il termine **Gas** si riferisce al costo per eseguire operazioni sulla blockchain, simile alle commissioni di transazione nelle blockchain di Bitcoin. I miner vengono ricompensati per gestire la potenza di calcolo delle applicazioni in relazione alla quantità di gas utilizzata.

## Soluzione

**Gas** è un'unità di misura per determinare il costo computazionale delle operazioni. È simile alle commissioni di transazione e premia i miner per il loro lavoro.

## Analogia

Un pedale del gas difettoso in un'auto potrebbe essere pericoloso con gas illimitato. Questo è il principio della blockchain: limita l'uso delle applicazioni tramite il costo del gas che si è disposti a spendere.

---

# § The DAO (Organizzazione Autonoma Decentralizzata)

Un DAO (Decentralized Autonomous Organization) è un'organizzazione costruita tramite smart contracts, finanziata da investitori che ricevono token per votare. In quel periodo, i token DAO rappresentavano una parte significativa del valore di mercato di Ethereum e venivano considerati come titoli all'interno di una struttura aziendale.

## Un Problema Sorge

È stato scoperto un difetto che permetteva prelievi illimitati senza una corretta contabilità, svuotando le riserve. Questo è stato un grande problema.

## Danni e Patrimonio

I contratti smart del DAO sono stati hackati in due tentativi, di cui uno ha prelevato il 30% e l'altro il 70% del valore del progetto. Fortunatamente, il contratto smart era codificato con un periodo di liquidazione di 28 giorni.

## La Soluzione

La comunità ha deciso di effettuare un Hard Fork della blockchain per evitare questo incidente e restituire i token agli originali proprietari sotto il nome di **Ethereum Classic (ETC)**.

## Il Meccanismo del Fork

Un Soft Fork è un aggiornamento che introduce nuove regole compatibili con le versioni precedenti, simile agli aggiornamenti di Windows che supportano nuove funzionalità mentre le applicazioni più vecchie continuano a funzionare. Al contrario, un Hard Fork richiede un aggiornamento del sistema per implementare nuove funzionalità non compatibili con le versioni precedenti, come nel caso dell'Hard Fork sulla blockchain di Ethereum.

**Soft Fork**

- Modifiche di sistema minori
- Retrocompatibile
- I nodi non devono essere aggiornati per raggiungere il consenso

**Hard Fork**

- Modifiche di software significative
- Non retrocompatibile
- I nodi devono aderire alle nuove regole di consenso

## Lezioni

- Non tutti i contratti sono intelligenti; la loro efficienza dipende dalla loro implementazione.
- Un contratto una volta implementato non può essere facilmente corretto.
- Se un contratto è difettoso, può compromettere l'immutabilità della blockchain.

---

# § Blockchain Private

La blockchain esiste in due forme, e il caso d'uso è cruciale:

- **Pubblica**: Poiché non ci fidiamo dei nodi, abbiamo bisogno di un gruppo pubblico per validare le transazioni per la sicurezza.
- **Privata**: Possiamo limitare la blockchain a settori specifici per ottimizzare alcune aree.

## Applicazioni Speciali

L'uso delle proprietà della blockchain per garantire dati, ad esempio nei contratti bancari tra parti. Con la crittografia dei contratti su un sistema blockchain, l'accesso ai dati è concesso solo alle parti coinvolte e alle autorità di regolamentazione. Questo garantisce un sistema sicuro, efficiente, immutabile e non contestabile. Inoltre, i protocolli di smart contract possono razionalizzare e interrompere documenti amministrativi, portando a notevoli risparmi sui costi.

# § Caratteristiche della Visione Blockchain

- **Transazioni Sicure, Efficienti, Immutabili e Non Contestabili**
  - Le transazioni sono sicure, efficienti e non possono essere modificate o contestate una volta confermate.
- **Riduzione di Molti Intermediari**
  - La tecnologia blockchain riduce o elimina la necessità di intermediari.
- **Un Mondo con Costi di Transazione Quasi Nulli Crea Nuovi Asset**
  - Costi di transazione estremamente bassi possono portare alla creazione di nuovi tipi di asset.
- **Fiducia nella Rete Anziché nella Banca Centrale**
  - La fiducia è nel network decentralizzato anziché nelle banche centrali. Tuttavia, le banche centrali potrebbero introdurre le proprie criptovalute.
- **Tokenizzazione di Quasi Tutti gli Asset**
  - Quasi tutti gli asset possono essere tokenizzati, facilitando il commercio e la gestione.
- **Inclusione Finanziaria per i Non Bancarizzati**
  - La blockchain può offrire servizi finanziari a coloro che non hanno accesso alla banca tradizionale.

## Rischi delle Criptovalute

- **Tecnologia Complessa da Comprendere**
  - La complessità della tecnologia delle criptovalute può essere un ostacolo per l'adozione e la comprensione diffusa.
- **Il Far West degli ICO e degli Investitori in Cerca di Soldi**
  - Gli Initial Coin Offerings (ICO) possono essere rischiosi, poiché mancano di regolamentazione, il che può portare a frodi e investimenti mal informati.
- **Volatilità Estrema**
  - Le criptovalute sono note per la loro alta volatilità dei prezzi, il che può comportare rischi finanziari significativi.
- **Rischio Normativo**
  - L'ambiente legale e normativo per le criptovalute è incerto e può cambiare rapidamente, influenzando il loro valore e utilità.
- **Discussione sul Privacy**
  - C'è una discussione continua e preoccupazioni sui problemi di privacy associati all'uso delle criptovalute, inclusi i compromessi tra trasparenza e anonimato.

## Azioni Consigliate

### Blockchain CheatSheet - Crittografia & Firme

---

**Autore**: Kenneth Boldrini

4o mini