

Mining & Sha256



 Valerio Vaccaro

Spazio 21

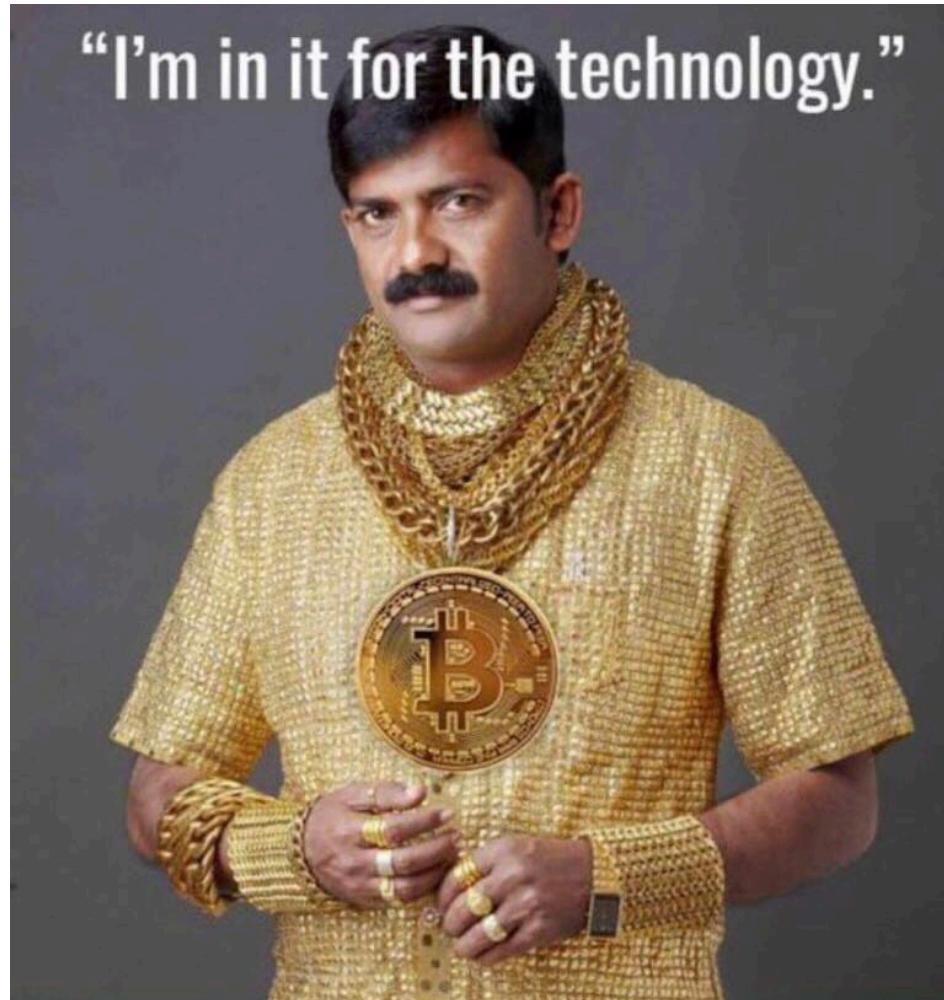
 2025-10-24

- 💻 Sviluppatore Bitcoin ed Esperto Hardware
- 🔥 Contributore a progetti Bitcoin open source
- ⚠ Appassionato di hardware fai-da-te (DIY)
- ₿ Ingegnere Bitcoin e Liquid presso Blockstream

 <https://www.linkedin.com/in/valeriovaccaro/>

 <https://github.com/valerio-vaccaro/>

Meme



Licenza

Questa presentazione è distribuita sotto la licenza Creative Commons [CC BY-SA 4.0](#).

Le immagini utilizzate in questa presentazione sono proprietà dei rispettivi autori e sono incluse solo a fini educativi e illustrativi.

May this presentation inspire you to become more self-sovereign!

Sommario

-  Scopo del mining Bitcoin
-  Come funziona il processo di mining
-  Ottimizzazioni e hardware
-  Costi e ricompense
-  Solo mining vs Pool mining
-  Stima dell'hashrate
-  HAN SOLOminer e NerdMiner



Scopo del Mining

Il mining di Bitcoin è un processo **fondamentale** del protocollo che serve a:

- **Proporre un ordine** tra le transazioni nella mempool
- **Selezionare un sottoinsieme** per creare un nuovo blocco
- **Aggiornare lo stato** della blockchain

Il mining è progettato per essere **decentralizzato e casuale**, evitando una gestione centralizzata delle transazioni.



🚫 Censura

Un ente centrale potrebbe bloccare alcune transazioni, ma con miner decentralizzati le transazioni hanno più possibilità di essere incluse.

⌚ Timestamping

Fornisce un ordine temporale sicuro e condiviso, non dipendente da un'autorità centrale, ma dal consenso tra miner e nodi.



Doppia Spesa

Senza un miner corrompibile, è difficile riscrivere la storia o favorire una transazione a scapito di un'altra.

Processo passo per passo:

1.  **Selezione transazioni:** Il miner sceglie dalla mempool, privilegiando fee più alte
2.  **Costruzione Coinbase:** Crea transazione speciale per il premio (3,125 BTC + fee)
3.  **Merkle Root:** Organizza transazioni in struttura ad albero e calcolo della radice
4.  **Header del Blocco:** Costruisce prototipo con timestamp, hash precedente, Merkle Root, difficoltà, nonce
5.  **Puzzle Crittografico:** Applica SHA-256 e verifica zeri iniziali



Puzzle Crittografico

Il miner applica l'algoritmo SHA-256 all'header e verifica se il risultato rispetta la difficoltà (visivamente minore => ha un certo numero di zeri)

Se valido:

- Blocco trovato!
- Trasmissione alla rete
- Ricompensa ottenuta

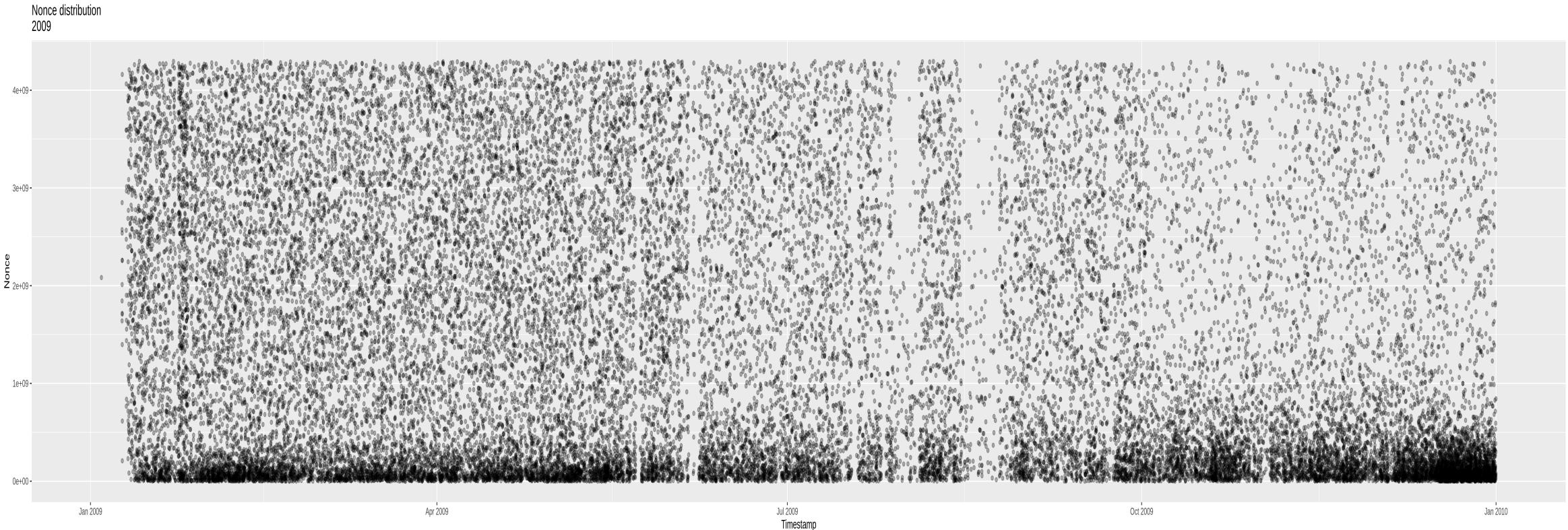
Se non valido:

- Modifica il nonce
- Ripete il calcolo
- Lavoro di forza bruta

Nessuna scorciatoia: Grazie alle proprietà di SHA-256

Puzzle Crittografico: nonce

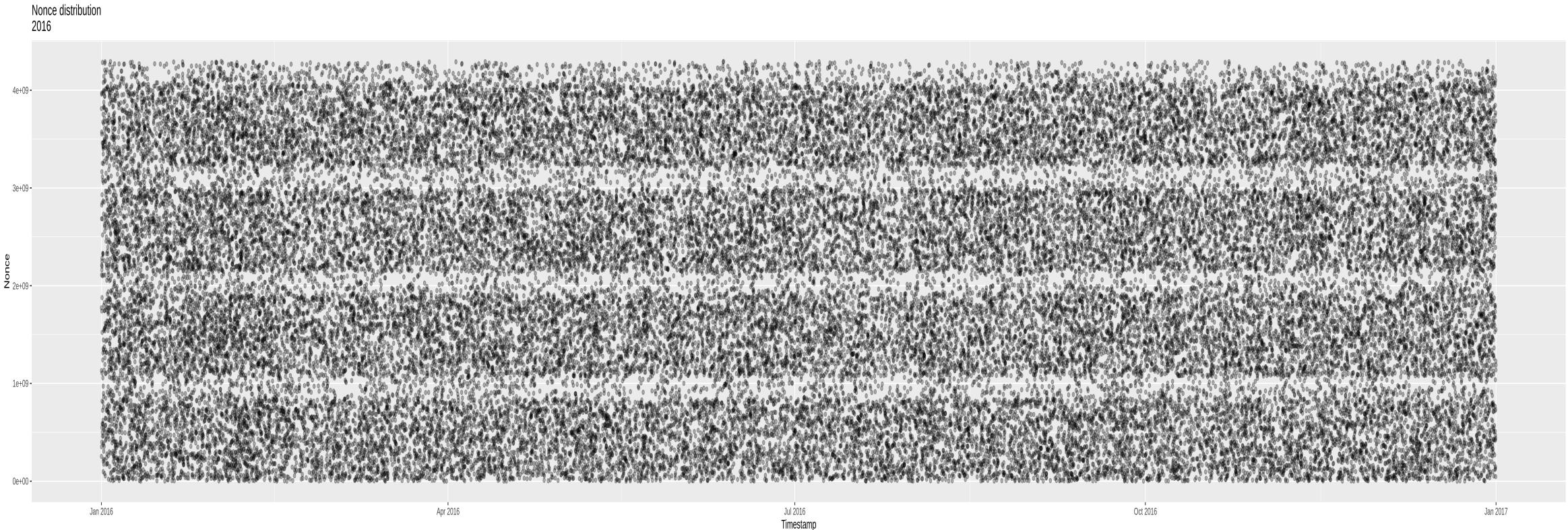
Il nonce nel 2009



Fonte: btcillustrated.com

🔒 Puzzle Crittografico: nonce 🚀🚀

Il nonce nel 2016



Fonte: btcillustrated.com



Puzzle Crittografico: quando il nonce non basta



Se il nonce non basta posso:

- modificare altri dati nell'**header** di un blocco
 - ad esempio il **timestamp**
- aggiungere informazioni alla **coinbase**
 - posso usare input come una campo **extra-nonce** (posso avvantaggiarmi di non ricalcolare tutto il merkle root)
- posso **cambiare transazioni**, o il loro ordine



Ottimizzazioni

Per velocizzare il processo:

- ⚡ **Primo SHA-256:** Calcolato sui primi 64 byte dell'header (immutabili)
- ⚡ **Iterazione:** Solo sul resto, cambiando il nonce
- 🏭 **Specializzazione:** Hardware ASIC che eseguono miliardi di tentativi al secondo

Hardware Evolution:

- 💻 **CPU:** Primi anni
- 🎮 **GPU:** Miglioramento significativo
- 🏭 **ASIC:** Specializzati per SHA-256, massima efficienza

Processo di Validazione

Quando un miner trova una soluzione, trasmette il blocco completo alla rete. I nodi validano:

Validazioni:

- Hash dell'header (un solo SHA-256)
- Correttezza informazioni blocco
- Riproducibilità Merkle Root

Sicurezza:

- Premio spendibile dopo **100 conferme**
- Circa **16 ore** di attesa
- Garantisce stabilità

Teoria dei giochi



Costi e Ricompense



Costi:

- ⚡ **Corrente elettrica:** Variabile principale
- 🏭 **Hardware ASIC:** Costosi e a vita breve
- 🚒 **Infrastrutture:** Raffreddamento, installazione, manutenzione



Ricompense:

- 🏆 **Premio fisso:** 3,125 BTC (dimezzato nel 2024)
- 💰 **Fee variabili:** Delle transazioni selezionate



Rischi:

- Blocco non valido = risorse sprecate
- Blocco "orfanato" = perdite se altro miner vince



Solo Mining vs Pool Mining

🎯 Solo Mining:

- Miner lavora da solo
- Se trova blocco = tutto il premio
- Probabilità bassissima (secoli con un ASIC)

E le solo pool?

💰 Pool Mining:

- Protocollo Stratum
- Collaborazione tra miner
- Divisione proporzionale del premio



Processo:

1. **Template:** Pool fornisce coinbase, Merkle path o root, ecc.
2. **Share:** Miner inviano tentativi inferiori ad una certa difficoltà (diversa da quella necessaria per chiudere un blocco)
3. **Premio:** Diviso proporzionalmente alle share inviate



In una Pool:

- Conta share ricevute per unità di tempo
- Moltiplicate per difficoltà delle share
- Stima perturbabile dalla fortuna

Globale:

- Usa difficoltà di Bitcoin
- Tempo medio tra blocchi (~10 minuti)
- Media affidabile, oscillazioni normali



Il mining è **competitivo**:

Obiettivi:

- Massimizzare tempo di attività
- Ammortizzare costi fissi
- ROI lungo e incerto

Limitazioni:

- Usi spot poco pratici
- Costi iniziali richiedono continuità
- Competizione globale

Si cercano fonti di energia stabili ed economiche, difficilmente saranno fonti green.



Programma di Dimezzamento:

- **Ogni 210.000 blocchi (~4 anni)**
- **Ricompensa dimezzata**
- **2024: 3,125 BTC per blocco**
- **2140: Ultimo Bitcoin emesso**

Impatto:

- **Riduzione inflazione Bitcoin**
- **Aumento importanza delle fee**
- **Crescita difficoltà mining**



HAN SOLOminer e NerdMiner

HAN SOLOminer è un "gioco" che spiega il mining collegandosi a una pool con Stratum.

Da questo prototipo è derivato **NerdMiner**.

⚠ La difficoltà di Bitcoin è tale che i NerdMiner **non mineranno mai un blocco** (e non lo farà nemmeno un milione di NerdMiner).



Hardware Supportato NerdMiner

Hardware	Descrizione
LILYGO T-Display S3	Display touch con ESP32-S3
ESP32-WROOM-32	Modulo ESP32 standard
ESP32-Devkit1	Development board
LILYGO T-QT pro	Display compatto
LILYGO T-Display 1.14	Display 1.14"
LILYGO T-Display S3 AMOLED	Display AMOLED
LILYGO T-Dongle S3	Dongle USB-C
ESP32-2432S028R	Display 2.8"
ESP32-cam	Con camera
M5-StampS3	Stamp compatto



Obiettivi Educativi

Cosa Imparerai:

- **Comprendere** del processo di mining
- **Funzionamento** proof-of-work
- **Economia** del mining
- **Hardware** e ottimizzazioni
- **Esperienza pratica** con NerdMiner



Metodo Semplice:

1. **Vai su:** flasher.bitronics.store
2. **Seleziona:** il device, la board corretta e l'ultima versione
3. **Clicca:** Start flashing
4. **Fatto:** Il firmware viene installato automaticamente

Vantaggi:

- **Nessuna installazione** di software
- **Processo automatico** via browser
- **Supporto multipli hardware**



Installazione NerdMiner

- **Configura il WiFi**

- Alla prima accensione, il device crea una rete WiFi:

NerdMiner-AP

- Collegati con il tuo telefono/computer e vai su:

192.168.4.1

- **Personalizzazione**

- Da menu web puoi inserire:

- Il nome e la password della tua WiFi domestica
 - Il tuo indirizzo Bitcoin (per ricevere le eventuali ricompense)
 - La mining pool da utilizzare
 - Altri parametri

- **Salva e Riavvia**



Installazione NerdMiner

DASHBOARD

[Dashboard](#)

[Settings](#)

Your Best Difficulty [?](#)



935.71

935.713

Network Difficulty

146.72T

146,716,052,770,107.5

Network Hash Rate

1.0 ZH/s

Block Height

920368

Weight: 398,201

Name

Session ID

Hash Rate

Session Best Difficulty

Uptime

Last Seen

▼ worker

2 Sessions

570.0 KH/s

33.13

265d2a0e

351.9 KH/s

33.13

1.5 days

56.0 seconds

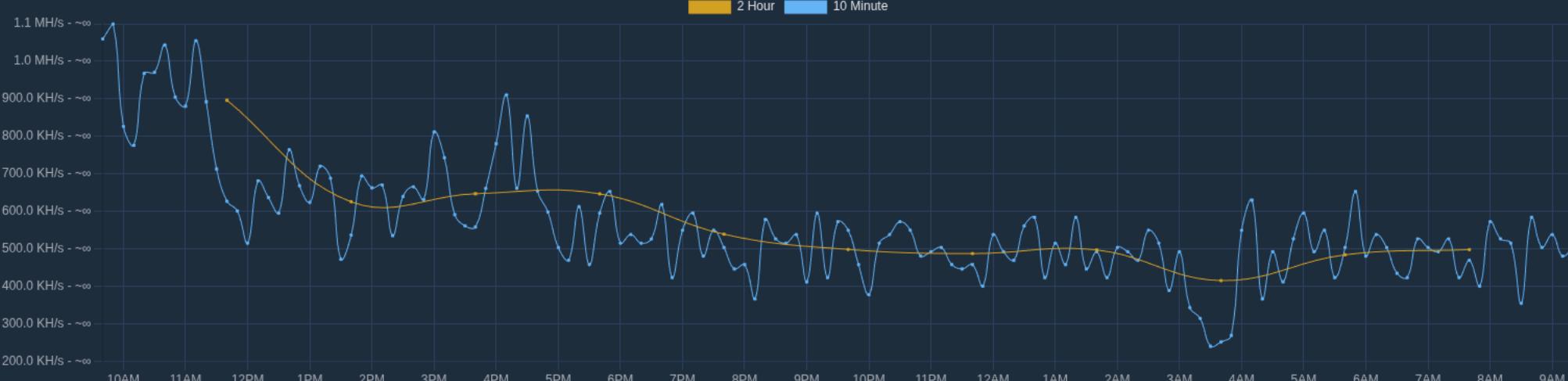
b0408524

218.0 KH/s

0.87

5.7 hours

Just now





Demo NerdMiner



- **Connessione** a pool reale
- **Visualizzazione** hashrate
- **Comprensione** del processo
- **Monitoraggio** performance



Bitaxe e similari

- **Bitaxe**: progetto open source per realizzare un ASIC miner compatto e autocostruibile
 - Basato su chip come **BM1397** o **BM1366**
 - **Basso consumo** compatibile con ambienti casalinghi e di test
 - **Economico** rispetto agli ASIC industriali
 - Interfaccie grafiche di monitoraggio
 - **Hashrate** ridotto
 - Firmware open source (ad es. bitaxe.org)

Questi dispositivi sono utili **per imparare**, sperimentare e vedere come funziona il mining **ma...**



Home Mining: Non Conviene! ⚠

L'home mining, oggi, è utile **solo per studio o per sperimentazione tecnica**.

I **costi** dei device e dell'energia sono alti

L'**hashrate** dei device è abbastanza basso (hashrate globale continua a crescere)



Bibliografia

- officinebitcoin.it/lezioni/mining
- officinebitcoin.it/lezioni/hansol
- [NerdMiner GitHub](#)
- [DIY Flasher](#)
- Bitcoin Whitepaper - Satoshi Nakamoto

Domande





Progetto Satoshi Spritz

- Federazione di gruppi locali di Bitcoiner
- Eventi gratuiti e privacy oriented
- BITCOIN ONLY
- Satoshi Spritz Connect online settimanale
- Orientato all'apprendimento della self-sovereign
- Tutte le settimane un evento online -> Satoshi Spritz Connect

<https://satoshispritz.it>

<https://t.me/SatoshiSpritzConnect>

฿ Officine Bitcoin

- Comunità Italiana di Bitcoiners, totalmente gratuita
- BITCOIN ONLY
- Focus su educazione e sviluppo di progetti
- Progetti:
 - Sviluppo nodi Bitcoin
 - Uso di Hardware Wallet
 - Filosofia open source
 - Installazione di Debian
 - ... e molto altro

<https://officinebitcoin.it>

