Marco Dal Prà (m_dalpra)

CRIPTOVALUTE: COSA SONO LE POOL?

13 January 2018

Di recente sono riuscito ad avere tra le mani alcune "macchine" costruite appositamente per vidimare i pagamenti che avvengono nel mondo delle criptovalute come Bitcoin, Ethereum o altre, ma prima di pubblicare i risultati dei test, devo spiegare qualche concetto che sta a monte. Con questo articolo spiegherò come e perché alcuni siti internet offrono servizi dedicati a chi vuole intraprendere questa attività, che nel gergo è chiamata mining.

Premessa

Le criptovalute hanno scatenato una nuova sfida sia tra gli sviluppatori di Hardware che di Software, con soluzioni sempre più sofisticate quanto originali per risolvere un tipo di problemi che fino a qualche anno fa non erano nemmeno immaginabili.
Questo articolo riguarda le criptovalute nelle quali per convalidare i pagamenti che si scambiano gli utenti sono richieste apparecchiature Hardware, perché si deve dimostrare che dietro alla convalida c'è stato un lavoro impegnativo. E' quella che nel gergo si chiama **Proof of Work (POW)** cioè prova di lavoro.
Le persone che svolgono questo lavoro, per il quale sono necessari investimenti in "macchinari", nel nel gergo sono chiamati **miners**, cioè minatori, perché il lavoro che svolgono è tutt'altro che semplice ma anche perché vengono premiati con criptovalute di nuovo conio.

E' cioè un mestiere analogo a chi scava per riuscire a trovare un minerale prezioso.
Segnalo comunque che non tutte le criptovalute utilizzano la tecnica della Proof of Work per convalidare le operazioni; altre ad esempio usano la Proof of Stake, per la quale c'è comunque dietro un investimento, che sta in un elevato numero di criptomonete che devono essere "immobilizzate" nel software preposto alle convalide (tecnologia dei Masternode).

Cosa fanno i minatori

Nel mondo delle criptovalute con il termine "minatori" o "miners" si intendono quelle persone o aziende che si dotano di apparecchiature elettroniche destinate esclusivamente a confermare la correttezza delle operazioni di pagamento di una specifica criptovaluta, come ad esempio Bitcoin, Ethereum, Dash, Litecoin, ecc.
Coloro che fanno "mining" sono in pratica i responsabili della sicurezza delle transazioni, ma a differenza delle banche, non possiedono nulla: possono solamente vidimare le nuove transazioni che vengono richieste dagli utenti; il minatore cioè non può dirottare una criptovaluta su un altro conto (in particolare... sul suo!), perché altrimenti verrebbe escluso dal database condiviso della moneta alla quale partecipa (la blockchain), in quanto la sua operazione non risponde alle regole

del protocollo e verrebbe scartata da tutti gli altri partecipanti.
Il minatore ha inoltre tutto l'interesse di completare i suoi "compiti" più velocemente possibile, perché **si trova in competizione con gli altri minatori** che operano sulla stessa criptovaluta (che sono anche migliaia).
I minatori, infine, vengono ricompensati del loro compito con la criptovaluta sulla quale stanno vidimando le operazioni, la quale viene assegnata sulla base di un programma prestabilito dai creatori del software.
I minatori talvolta sono persone improvvisate che assemblano componenti nel garage di casa, ma altre volte **sono aziende con investimenti da milioni di dollari in Hardware e Capannoni Industriali**.

Dave Carlson, CEO di giga-watt.com

Calcoli alla base

Le apparecchiature elettroniche di cui si dota il minatore, come accennato, servono per "confermare" le transazioni che si scambiano gli utenti (potremmo paragonarle a dei bonifici all'interno della stessa banca); in particolare il minatore una volta verificate che sono corrette, le carica nel registro pubblico della rispettiva criptovaluta (la Blockchain).
Per fare questa operazione è necessario raggruppare gli ultimi pagamenti in un "blocco" e calcolarne l'HASH, una sorta di firma elettronica.
L'Hash è una operazione crittografica che serve per calcolare l'impronta digitale di un file, ed è congegnato in modo che modificando anche solo un bit il calcolo dell'Hash dà un risultato completamente diverso. Serve appunto per verificare che un documento non sia stato alterato.
Questa procedura sfrutta algoritmi consolidati.

UN ESEMPIO
Nella criptovaluta Bitcoin le operazioni vengono "vidimate" dai minatori

```
con l'algoritmo SHA-256, che genera una sequenza di 256 bit
0x e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

E' lo stesso algoritmo che sta alla base del procedimento che usano le "chiavette"
per la Firma Elettronica, ad esempio quelle che forniscono alle aziende
le Camere di Commercio.
```

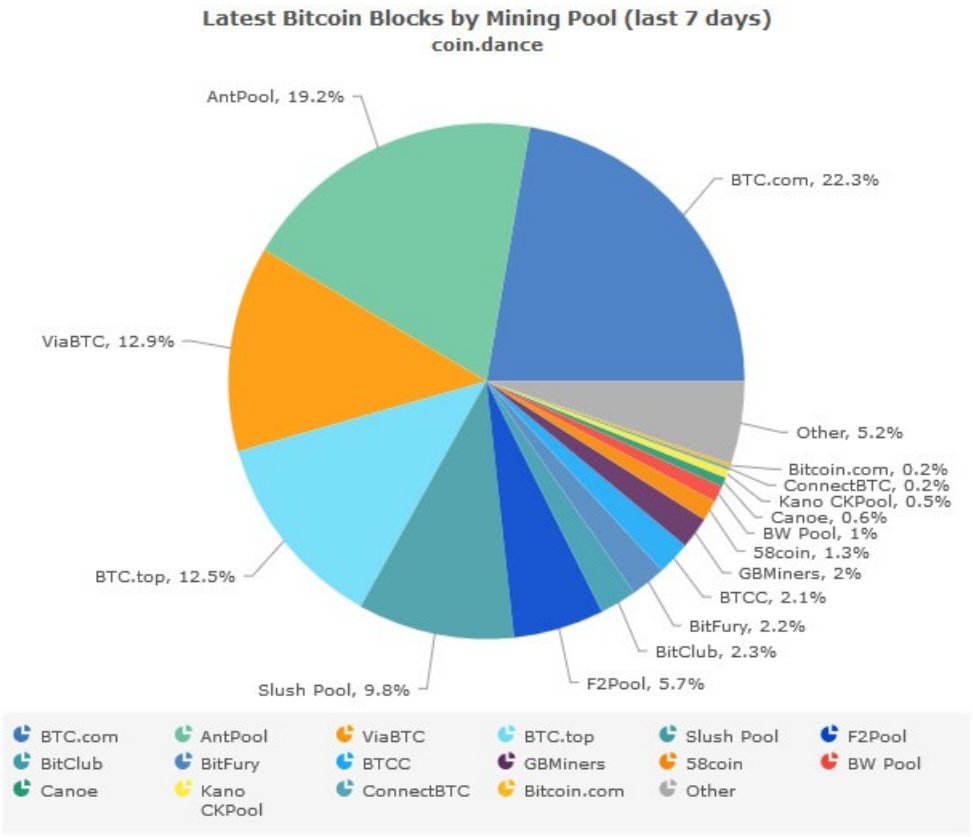
Ma chi concepisce il software che sta alla base delle criptovalute non si accontenta di qualunque firma, ma richiede che la firma presenti determinate caratteristiche, come ad esempio iniziare con una sequenza di zeri.
Questo significa che se la firma non va bene il minatore deve ricominciare il calcolo da capo fino a che non trova la firma corretta.
Questa operazione richiede **migliaia di tentativi**, e solo riuscendo a farla per tempo il minatore prenderà la "ricompensa" sul blocco confermato (nel gergo "Reward").
Diversamente avrà fatto del lavoro per niente.

Sempre più veloce

Come detto in precedenza, i minatori sono in competizione tra loro perché fanno a gara su chi per primo conferma le ultime transazioni, o meglio, su chi per primo riesce a confermare un blocco e lo aggiunge in coda alla Blockchain.
Per aumentare le probabilità di convalidare i blocchi e prendere la relativa "ricompensa" il minatore ha essenzialmente due strade :

1. Aumentare il numero di apparati/processori che fanno i calcoli, oppure
2. Mettersi in gruppo con altri minatori dividendosi poi la ricompensa (lavoro in POOL).

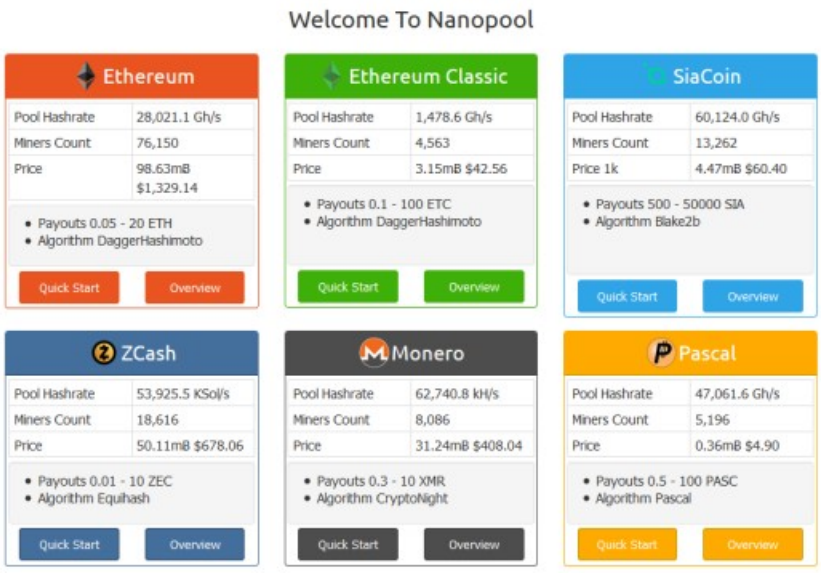
La prima opzione **richiede investimenti importanti**, in quanto sono necessarie ulteriori costose apparecchiature, spazi, impianti elettrici e forniture dei energia elettrica. Come ho spiegato in un precedente articolo, infatti, queste macchine sono piuttosto energivore LINK QUI .
La seconda è il motivo di questo articolo e la vedremo qui a seguire.
Come si può vedere dal grafico sottostante, che riguarda i blocchi confermati nella criptovaluta Bitcoin, è evidente che la maggior parte dei minatori lavora in pool; i valori percentuali si riferiscono a quanti blocchi ciascuna pool ha confermato nell'ultima settimana (settimana n. 2 del 2018).



https://coin.dance/ Bitcoin thisweek

Cosa sono le POOL

Una pool di minatori, nel gergo "Mining Pool", è un sito internet (solitamente di una azienda) che si prefigge di mettere assieme più minatori possibili per aumentare la probabilità di indovinare/ confermare un blocco.

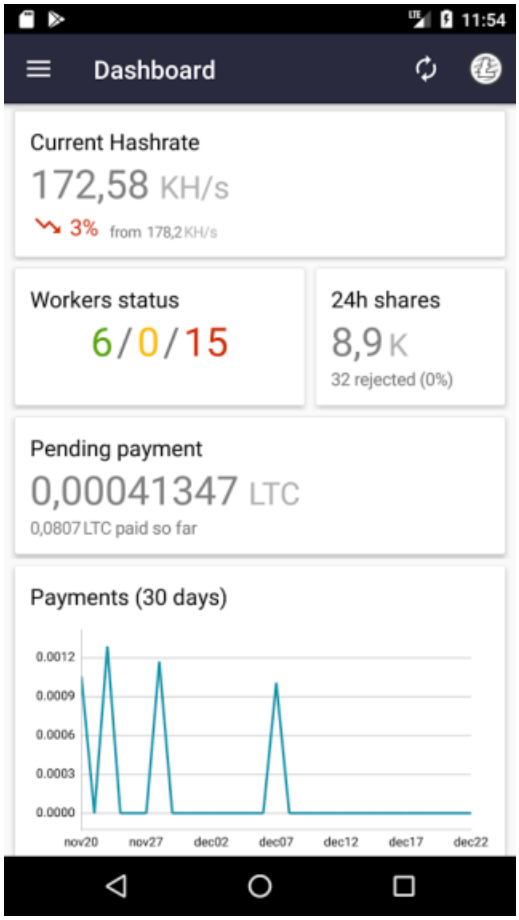


Sito web Nanopool.org

Le mining Pool sono in concorrenza tra loro e solitamente si contendono i minatori per queste caratteristiche :

- costo delle commissioni che trattengono per il proprio funzionamento (nel gergo "Fee")
- resa giornaliera, fornita sulla base dei MegaHash/secondo delle proprie apparecchiature,
- costanza nel funzionamento senza guasti,
- rapidità nei pagamenti (in bitcoin o altre criptovalute),
- qualità del sito con tutte le informazioni ed i software per unirsi alla Pool.

Per chi vuole fare il minatore le Pool sono un punto di riferimento perchè evitano al minatore di tenere anche un PC acceso H24 con la copia costantemente aggiornata di tutto il database delle criptovaluta (la blockchain), cioè quello che nel gergo è chiamato **Full Node**.
La Pool inoltre **garantisce al minatore una rendita piuttosto costante** indipendentemente se le sue macchine "azzeccano" o meno i calcoli, perchè comunque la ricompensa è divisa tra tutti i partecipanti.
Inoltre, alcune come Antpool mettono a disposizione una APP per cellulare per verificare il funzionamento delle proprie macchine a livello di rendimento "economico"; altre si affidano a pagine Web.



Antpool_APP.png

Le mining pool sono parecchie decine, direi più di un centinaio.
Alcune di famose sono **Niceshash, Antpool, Nanopool, VIABtc**.

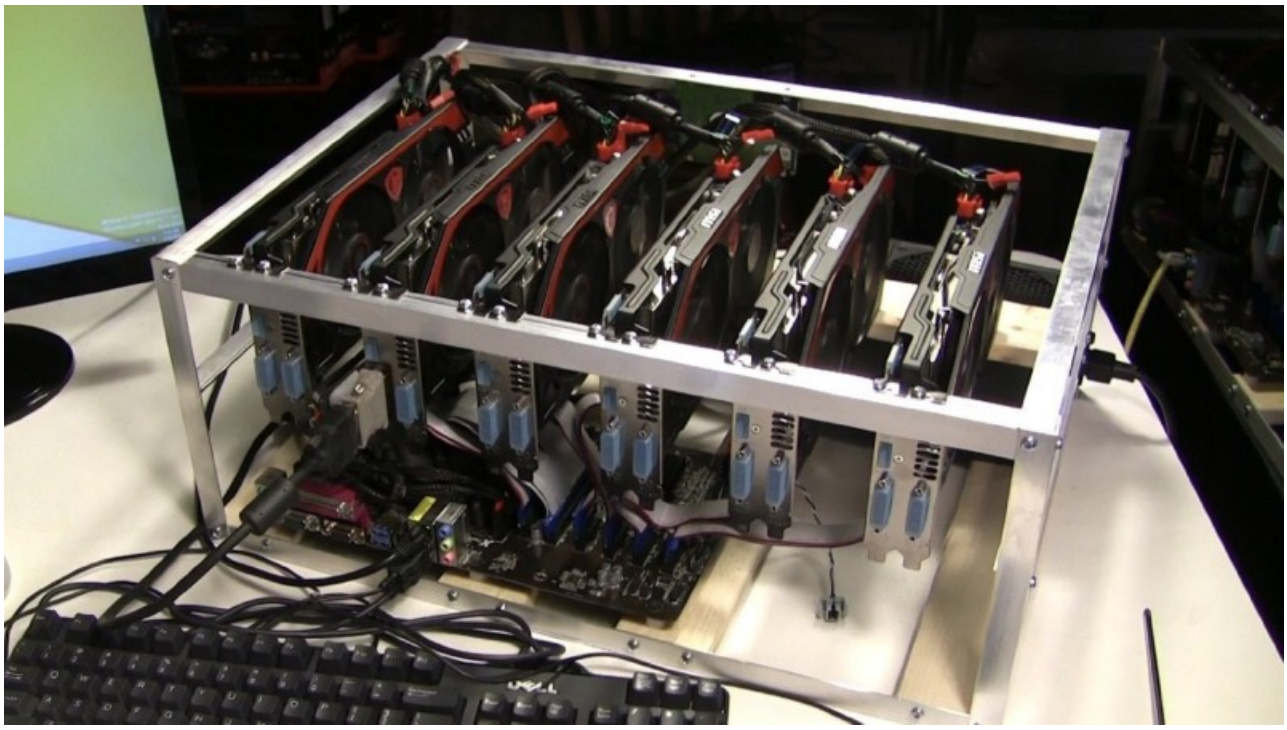
Come Funziona una POOL ?

In linea di massima una POOL ha dei PC in ciascuno dei quali gira il software di una criptovaluta, con archiviata la copia della rispettiva Blockchain.
Quando una pool raccoglie un numero sufficiente di transazioni richieste da parte degli utenti di una specifica criptovaluta, il PC della pool invia ai propri minatori i "compiti per casa", cioè i dati con i quali bisogna cercare di "indovinare" l'hash.
Con Bitcoin, ad esempio, questa operazione viene fatta ogni 10 minuti, con Litecoin ogni 2,5 minuti, con Ethereum circa ogni 30 secondi.
I dati non sono molto ingombranti, ma anzi sono pacchetti molto piccoli, nell'ordine di qualche centinaio di Byte.
Quando un dispositivo riesce nell'intento di trovare un Hash corretto, lo invia alla propria Pool che a sua volta lo fa vedere a tutti i nodi della rete di quella criptovaluta. Se nessun altro è riuscito a farlo così velocemente, il blocco di transazioni confermato con l'Hash viene inviato a tutti i nodi e

la Pool incassa la Reward per il compito svolto.
Nel momento in cui scrivo, una pool che riesce a confermare un blocco Bitcoin incassa 12,5 bitcoin; con Ethereum, incassa 3 ether.
Alcune Pool, come ad esempio Nanopool, gestiscono solo poche criptovalute, inoltre con queste pool il minatore **deve decidere a priori quale criptovaluta minare**, installando un determinato software; una decisione non semplice perché poi il valore della criptovaluta potrebbe scendere per ragioni di mercato, costringendo il minatore ad interventi continui di cambiamento del software o delle configurazioni.
Altre pool invece **gestiscono decine di criptovalute**, come ad esempio mining-dutch.nl o Nicehash, e poi provvedono loro **ora per ora** a valutare quale valuta sia più conveniente minare in quel momento.

Come scegliere ?

Chi decide di intraprendere l'attività di minatore deve prima di tutto scegliere **se iniziare con macchine ASIC**, prestanti ma costose, e con tempi di consegna lunghissimi (3-4 mesi), **oppure con le GPU**, più economiche ma che dal 2017 sono diventate di non facile reperibilità proprio a causa dei minatori.
In ogni caso, prima di acquistare una GeForce GTX 1080 Ti o altro prodotto equivalente, consiglio di consultare i siti che calcolano i rendimenti, come ad esempio https://whattomine.com/coins .
Qui inserendo semplicemente il numero di GPU che si hanno, si possono vedere la resa giornaliera ed il conseguente ammortamento della spesa.
Attenzione a non scegliere algoritmi che minano valute di nicchia, che poi potrebbero crashare dal punto di vista finanziario; necessario quindi controllare l'andamento storico della critpovaluta su coinmarketcap.com .
Ricordo comunque che per le macchine di mining basate su GPU **non serve un PC prestante**; un processore i3 con 4GB di Ram ed un Hard Disk SSD da 128GB sono più che sufficienti. Solitamente anche vecchi processori si adattano bene.
Piuttosto è necessario investire sul telaio e sugli alimentatori.



Ethereum "Mining RigL"

Ricordo infine che le **macchine ASIC invece**, come ad esempio Bitmaiin o Innosilicon, non hanno bisogno di un PC locale per funzionare, in quanto colloquiano direttamente con la Pool.

Configurazione

Una volta scelto l'hardware, si dovrà procedere alla configurazione; in internet e soprattutto su Youtube si trovano moltissime guide a riguardo, con indicazioni utili sia sulle parti Hardware che software

L'attività di configurazione che cambia notevolmente tra chip ASIC e GPU.
Negli ASIC la configurazione è molto semplice, dato che è sufficiente indicare l'indirizzo della POOL alla quale ci si è registrati (oppure l'indirizzo del wallet nel quale la Pool effettuerà i pagamenti).
Per le GPU la cosa è molto più complessa perchè si devono installare software piuttosto "amatoriali" che poi si dovranno configurare tramite opzioni a riga di comando; mettere in conto che si dovrà perdere parecchio tempo per trovare il giusto compromesso tra rendimento e crash del PC.
Suggerisco infine di evitare di ricorrere all'Overclocking delle GPU, perché non si adatta a macchine che stanno accese 24 Ore su 24 per 365 giorni all'anno.

LINK UTILI

L'algoritmo di Hashing SHA-256 su Wikipedia

La convenienza economica di minare con le GPU aggiornata in tempo reale LINK QUI

La convenienza economica di minare con gli ASIC aggiornata in tempo reale LINK QUI

Mining Pool

Qui alcune delle Pool piuttosto famose, che ho avuto l'opportunità di visionare :
https://www.nicehash.com/
https://www.antpool.com/
https://nanopool.org/
https://pool.viabtc.com/

Qui una classifica con tantissime Pool, filtrabile a seconda dei servizi erogati :
https://www.cryptocompare.com/mining/#/pools