Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il Management

Analisi e progettazione di una mining pool sostenibile per TurtleCoin

Relatore:
Chiar.mo Prof.
Stefano Ferretti

Presentata da:
Alberto Zini

Sessione II
ANNO ACCADEMICO 2018/2019

A tutti coloro che non reclamano le cose,
ma le ottengono . . .

Indice

Introduzione

La nostra epoca è caratterizzata da forti innovazioni tecnologiche, alcune delle quali rappresentano delle vere e proprie sfide a sistemi esistenti e consolidati.
Degno di nota è l'avvento della tecnologia blockchain e, di conseguenza, l'introduzione del concetto di criptovaluta.
Una criptovaluta è una moneta digitale che può essere scambiata come quella cartacea ma con modalità differenti, basate sulla crittografia.
La crittografia serve a rendere sicure le transazioni e a controllare la creazione di nuove valute.
Diversamente da tutte le monete non digitali, le criptovalute sfuggono a qualsiasi autorità, infatti a coniarle non ci pensa la Zecca dello Stato e non c'è alcuna Banca Centrale che ne controlli il valore, non esiste neppure un intermediario finanziario che ne convalidi le transazioni.
La vera rivoluzione infatti non è tanto nella digitalizzazione dei pagamenti, a cui tutti ormai nell'era di Internet sono abituati, quanto al fatto che questi siano decentralizzati e non convalidati con i sistemi tradizionali.
La prima criptovaluta è stata Bitcoin (con la "B" maiuscola).
Satoshi Nakamoto è l'autore del "white paper" del 2008 sulle criptovalute, ed è considerato da più fonti autorevoli come il creatore del Bitcoin.
Satoshi ha sviluppato il protocollo originale e la tecnologia blockchain che sta alla base del Bitcoin, ma la sua vera identità è tuttora sconosciuta.
Satoshi Nakamoto è solo uno pseudonimo, usato da una persona o, come alcuni pensano, da un gruppo di persone.

Bitcoin nasce con l'intento di rendere più sicure e veloci le transazioni su internet senza necessariamente basarsi sulla fiducia di autorità terze, ma sulla matematica e sulla crittografia. La Banca Centrale viene sostituita da una rete di tipo peer-to-peer a cui tutti possono partecipare. Ogni partecipante della rete è chiamato "nodo". I nodi della rete, attraverso un semplice software open-source, contribuiscono in modo diffuso a convalidare e registrare le transazioni tra due utenti che vogliono scambiarsi unità di quella valuta, garantendone l'anonimato grazie alla crittografia annidata nel sistema.
In realtà mantenere l'anonimato non è facile. Con la nascita di servizi di exchange, che permettono il deposito di valute o la semplice compravendita, può succedere che l'anonimato venga perso. Un'altra possibile causa di perdita di anonimato potrebbe anche essere quella di seguire il blocco contenente la transazione e vedere l'indirizzo del destinatario, provando così a ricostruire l'identità delle parti.
L'attività di validazione e registrazione delle transazioni è detta "mining", in italiano significa "estrarre", un termine che riporta all'attività di estrazione dell'oro da una miniera. I nodi che svolgono tale operazione sono chiamati "miners". Questa attività sfrutta la potenza computazionale dei dispositivi dei nodi ed è remunerata attraverso un sistema preciso di ricompense.
Dopo l'ideazione del Bitcoin sono nati altri progetti di criptovalute.
TurtleCoin è una criptovaluta che nasce da un progetto già esistente, come qualsiasi altra criptovaluta. Questa nello specifico nasce da Monero.
Monero è una criptovaluta che funziona grazie ad un network di utenti.
Le transazioni sono confermate da un consenso distribuito e in seguito registrate in maniera immutabile sulla blockchain. La blockchain è pubblica ma nel caso di Monero(o TurtleCoin) è privato, cioè gli indirizzi, gli ammontari, le destinazioni di tutte le transazioni sono offuscati alle origini per garantirne la privacy.
Nel progetto abbinato alla tesi sono stati testati diversi sistemi per massimizzare l'efficienza energetica e rendere il progetto il più sostenibile possibile.
Si è scelta la mining pool di TurtleCoin, che è formata da una base compu-

tazionale abbastanza potente e, attualmente, rientra tra le top 10 in Italia.
E' importante notare che, per computare una transazione, non ci vuole la potenza di calcolo che ci vorrebbe in Bitcoin, Monero, Ethereum, ecc..
Nella sezione tecnica si vedrà la struttura dell'algoritmo.
Il progetto nasce inoltre come idea "green", ovvero con l'idea di garantire pagamenti digitali veloci rispettando l'ambiente, minimizzando i consumi di elettricità e quindi le emissioni CO2.
Il progetto utilizza, in primo luogo, solo energia prodotta di giorno la quale è completamente fornita da pannelli fotovoltaici installati sopra l'abitazione dove è situata la "base computazionale"; in secondo luogo si produce calore nell'ambiente dove sono situati i "dispositivi da miner" senza bisogno di altro tipo di riscaldamento.
L'ambiente è salvaguardato grazie all'utilizzo di una tecnologia energivora completamente sostenibile.
Si presenterà, infine, un'analisi della sostenibilità e dei costi riguardanti la mining pool del progetto, includendo possibili vantaggi e svantaggi di tale approccio.

Capitolo 1

Cos'è la blockchain

E' difficile classificare la blockchain e ridurla in una unica definizione.
La blockchain può essere letta e presentata da diversi punti di osservazione e da diverse prospettive.
Il termine "blockchain", letteralmente, significa catena di blocchi. Può essere considerata un grande registro digitale in cui le voci sono raggruppate in blocchi concatenati in ordine cronologico.
Si pensi alla blockchain come a un'enorme banca dati condivisa a cui si possono aggiungere man mano nuovi blocchi e a cui tutti possono accedere, ma senza possibilità di modifica.
La sua sicurezza è garantita dalla crittografia.
L'origine della blockchain è piuttosto recente (risale al 2009), e si deve alla mente di Satoshi Nakamoto, il misterioso inventore del Bitcoin.
L'idea rivoluzionaria di Nakamoto comprende un tipo di archiviazione dati in cui tutti possono vedere cosa c'è dentro e assicurarsi che i dati siano reali. Non può essere modificato neanche un singolo bit e, una volta che qualcosa è sulla rete, rimane lì per sempre.
Inizialmente era legata esclusivamente al Bitcoin. Infatti, per un certo tempo è stata identificata con la blockchain Bitcoin, ovvero con la prima blockchain (identificata con la "B" maiuscola).
A questa identificazione si è sovrapposta anche quella con la criptocurrency

bitcoin, che ha portato un po' a "confondere" la blockchain con altri ambiti di innovazione come le digital currency o, in generale, al mondo delle criptovalute, con lo scopo di verificare tutte le transazioni tra gli utenti evitando le frodi.
Forse per quest'ultima ragione la blockchain è stata spesso associata ad un concetto di digital currency alternativa o complementare e di digital payment.
In realtà, la blockchain è un fenomeno assai più ampio e articolato.
La blockchain è una sottofamiglia di tecnologie in cui il registro è strutturato come una catena di blocchi contenenti le transazioni e la cui validazione è affidata, nel caso delle blockchain permissionless o pubbliche, a un meccanismo di consenso distribuito su tutti i nodi della rete o, nel caso delle blockchain permissioned o private, su tutti i nodi che sono autorizzati a partecipare al processo di validazione delle transazioni.
Le principali caratteristiche delle tecnologie blockchain sono: l'immutabilità del registro, la trasparenza, la tracciabilità delle transazioni e la sicurezza basata su tecniche crittografiche.
Dal punto di vista operativo è una alternativa agli archivi centralizzati e permette di gestire l'aggiornamento dei dati con la collaborazione dei partecipanti alla rete e con la possibilità di avere dati condivisi, accessibili, distribuiti presso tutti i partecipanti.
Di fatto, permette una gestione dei dati in termini di verifica e di autorizzazione senza che sia necessaria una autorità centrale.
Per alcuni, la blockchain è la nuova generazione di Internet, o meglio ancora è la Nuova Internet. Si ritiene che possa rappresentare una sorta di Internet delle Transazioni.
Questa definizione tende ad affiancare la blockchain alla Internet of People (o Internet delle persone), che usiamo ogni giorno e che si è a sua volta estesa alla Internet of Things (o Internet delle cose) per arrivare a creare e rappresentare la Internet del Valore sulla base di sette caratteristiche:

1. Decentralizzazione

2. Trasparenza
3. Sicurezza
4. Immutabilità
5. Consenso
6. Responsabilità
7. Programmabilità

La blockchain non ha costi di transazione (è possibile addebitare qualsiasi importo in qualsiasi quantità senza preoccuparsi di terze parti che incidono sui profitti) ma solo costi di infrastruttura.
Per tutte queste caratteristiche, la blockchain si è allargata a diversi ambiti applicativi, rivelando la sua utilità per industrie, banche e altri soggetti operanti in molteplici settori; dal risparmio gestito alle opere d'arte, sino al Made in Italy. Un'altra applicazione molto importante pensata di recente è stata quella del suo utilizzo nel settore agro-alimentare.
Partendo da questi principi, la blockchain è diventata la declinazione in digitale di un nuovo concetto di fiducia al punto che alcuni ritengono che la blockchain possa assumere anche un valore per certi aspetti di tipo "sociale e politico".
In questo caso, la blockchain è da vedere come una piattaforma che consente lo sviluppo e la concretizzazione di una nuova forma di rapporto sociale che, grazie alla partecipazione di tutti, è in grado di garantire a chiunque la possibilità di verificare, controllare, disporre di una totale trasparenza sugli atti e sulle decisioni che vengono registrati in archivi con la caratteristica di essere inalterabili, immodificabili e dunque immuni da corruzione.

1.1 Come funziona la blockchain

Il funzionamento della blockchain non è banale. Chiunque può formare un blocco di dati. Una parte di una transazione avvia il processo di creazione di un blocco. Questo blocco viene verificato e validato dai nodi distribuiti e presenti nella rete e viene così aggiunto alla catena in modo permanente.
Tutte le informazioni sono crittografate, il che rende praticamente impossibile qualsiasi tentativo di frode e falsificazione.
Poiché tutte le transazioni avvengono "peer-to-peer", ovvero nodo a nodo della stessa rete, non sono necessari intermediari.

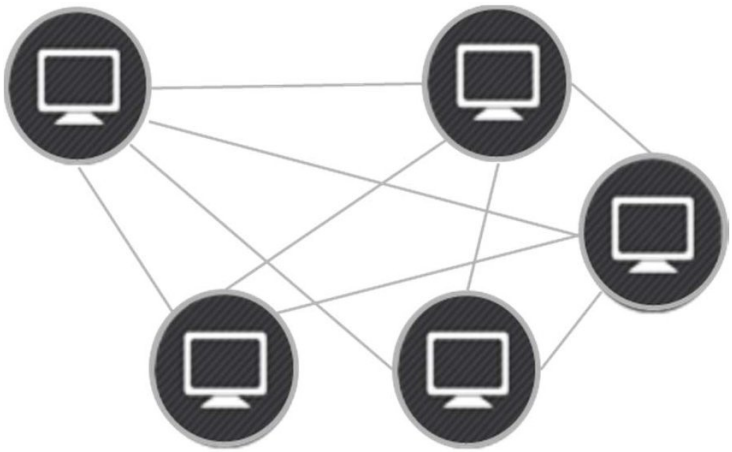


Figura 1.1: Rete p2p. FONTE: https://www.researchgate.net/

Gli ambiti di applicazione della blockchain sono tantissimi, potenzialmente infiniti. Si parte dai trasferimenti in denaro eseguiti con l'ausilio di criptovalute: si tratta di transazioni estremamente sicure e senza addebiti.
Anche gli smart contract sono avvantaggiati dalla blockchain, poiché risultano imparziali e neutrali nei confronti di tutte le parti coinvolte.
In un mondo sempre più esposto ad hacker e violazione della privacy, la blockchain diventa uno strumento essenziale per la verifica delle informazioni.
Ciò che viene aggiunto alla blockchain rimane in modo permanente e immutabile. Questo significa che le identità non possono essere rubate o alterate, poiché nel registro blockchain esiste una sola identità per ogni persona.

La blockchain ha determinate regole su cui basarsi, ma sta a ogni cryptovaluta implementarla secondo le proprie esigenze.
Ci può essere una cryptovaluta che implementa algoritmi più leggeri, e quindi più rapidi nel trasmettere una transazione, di quelli di un'altra cryptovaluta, ma quest'ultima può essere accompagnata da minore sicurezza.
Oppure, semplicemente, potrebbe anche essere che una determinata blockchain supporti gli smart contracts, mentre un'altra no.
Nella realizzazione del progetto sono state valutate varie cryptovalute, ma la scelta è ricaduta su TurtleCoin, per alcune precise considerazioni che si illustreranno in seguito.

1.2 Mining e estrazione di cryptovalute

Il mining (o estrazione) è il metodo utilizzato da molti sistemi di cryptovalute in generale, per estrarre, e quindi creare, monete.
La rete delle cryptovalute memorizza le transazioni all'interno di strutture di dati chiamate "blocchi". Affinchè un blocco possa essere aggiunto alla blockchain, ovvero all'enorme database pubblico contenente tutte le transazioni, è necessario che un elaboratore lo convalidi trovando un particolare codice, che può essere unicamente indovinato a forza di tentativi e algoritmi crittografici basati sulla matematica.
Ogni blocco di transazione, ossia l'insieme di tutte le transazioni avvenute nell'arco di tempo che varia da blockchain a blockchain, è affidato ad un singolo nodo della rete.
Il compito del miner, o del nodo, è quello di installare nelle sue macchine il software necessario per la computazione di funzioni hash; questo software è in grado di calcolare i dati delle transazioni, alle quali viene aggiunto un valore casuale o pseudo casuale detto "nonce"[1].

Questo valore, insieme ai dati del blocco delle transazioni, genera una stringa alfanumerica chiamata "hash". Per calcolare il contenuto di una stringa hash, il minatore necessita di un grande numero di tentativi e calcoli, dunque un vasto numero di nonce.
Nel processo di calcolo viene aggiunto anche l'hash del blocco precedente che, insieme ai dati del blocco di transazioni e al nonce, genera l'hash del blocco attuale.
La caratteristica che rende questo calcolo complesso, ma essenziale per essere reputato corretto dal sistema, è dovuta al fatto che l'hash deve cominciare

[1] In crittografia il termine nonce indica un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico. Un nonce viene utilizzato spesso nei protocolli di autenticazione per assicurare che i dati scambiati nelle vecchie comunicazioni non possano essere riutilizzati in attacchi di tipo replay attack. I nonce sono differenti ogni volta che il codice di risposta del tentativo di autenticazione 401 è presentato. Ogni richiesta di un client ha una sequenza numerica unica, così da rendere virtualmente impossibili attacchi di tipo replay-attack e attacchi a dizionario.

con un numero fisso di zeri.
Quando la stringa viene validata, il blocco di transazioni viene reso a sua volta valido.
L'operazione si conclude con l'estrazione della cryptovaluta su cui sta lavorando il miner e l'aggiornamento del registro blockchain, il libro mastro dei blocchi di transazioni.
L'intero processo permette al sistema di essere estremamente sicuro, poiché i blocchi di transazioni sono legati tra loro dalla condivisione dell'hash; questo permette ad un ipotetico malintenzionato di rinunciare all'alterazione delle transazioni in quanto andrebbe a modificare inevitabilmente anche il suo hash.
Esistono diversi metodi per l'estrazione di cryptovalute: Asic, FPGA, GPU, CPU, Cloud Mining, Pool Mining, ecc.
Ogni giorno la rete per cui si lavora crea un certo numero di ricompense in monete e le distribuisce ai miner online.
Per aumentare la probabilità di riceverle, si ha bisogno di macchine specifiche molto potenti, con una potenza di calcolo maggiore.
Maggiore è la potenza di calcolo, maggiore sarà la probabilità di estrarre e ricevere cryptovalute.
Le prime farm di Asic sono nate in Cina e Singapore nel 2013, con una forte concentrazione nelle centrali idroelettriche e in luoghi con una temperatura adeguata per ridurre il surriscaldamento dei sistemi.
Col passare del tempo sono state acquistate molte di queste macchine facendo crescere la difficoltà dell'algoritmo: nasce così il Pool mining.
Per "difficulty" si intende la misura per determinare la difficoltà del mining. Entrando più nello specifico, è la difficoltà distribuita dal protocollo per la conferma di un blocco della blockchain. Nel caso in cui la difficoltà aumenti, i miner reagiscono iniziando a competere tra loro e aumentando la potenza di calcolo dei sistemi fino a quando non viene trovata la giusta sequenza mediante un blocco ogni fissato periodo di tempo.
La difficulty viene calcolata ogni "n" blocchi, dipende dalla cryptovaluta e,

nel momento in cui si dovessero aggiungere altri miner alla rete, si verificherà un aumento di generazione di nuovi blocchi: il livello di difficoltà verrà ricalcolato e si subirà un rallentamento della produzione di nuovi blocchi.
I miner che non rispettano il livello di difficoltà richiesto verranno incontrovertibilmente esclusi dalla rete, bannandoli per un periodo limitato di tempo; anche per questo motivo, nelle varie mining pool, sono presenti varie porte di rete dove accedervi. Ogni porta è finalizzata per nodi di certe fasce di potenza di calcolo.
Si tratta quindi uno svolgimento che comporta un certo impegno, attraverso il quale si crea gradualmente una nuova valuta.
Tornando al discorso di Pool mining, questo consiste in un gruppo di miner, ognuno dei quali cede una parte delle risorse del proprio hardware al fine di risolvere gli algoritmi e guadagnare monete. Qualora i miners ottenessero ricompense, queste verranno divise in base alla potenza di trasmissione che i componenti della pool hanno ceduto per l'estrazione.
Per chiunque volesse cominciare con l'attività di mining, esiste qualche regola base e qualche consiglio su cui ci si potrà basare.
Innanzitutto, l'attività di mining, in linea generale, non è sostenibile per via degli esagerati consumi energetici, quindi sarà una attività che probabilmente rimarrà in vita ancora per pochi anni.
Nel caso si volesse comunque proseguire in questa impresa, bisognerà trovare l'hardware adeguato e avere contratti di fornitura luce convenienti.
Attualmente il mining è sconsigliato per tutti quelli che pagano una cifra al di sopra di 0.06 Euro al KWh in bolletta. Al valore attuale, anche con il migliore hardware, servirebbero almeno 10 mesi per raggiungere il punto di BEP, ripagandosi l'investimento.
Non è affatto un caso che l'hardware abbia un valore monetario pari a quanto sia performante, ma soprattutto non è un caso che sia proporzionato alla efficienza nell'estrazione di cryptovalute.
Una volta ottenuto l'hardware necessario, occorrerà montarlo su una struttura in grado di supportare e sostenere il sistema multi-gpu (cioè multi-schede

video); in seguito, solo dopo aver trovato una configurazione stabile di partenza del sistema, bisognerà avviare un software di mining a scelta, partecipando ad una Pool mining preferita.
In ogni caso, a meno che non si investa un capitale nell'hardware da miner, l'unica soluzione possibile rimane quella di partecipare ad una mining pool.
Infine, occorrerà lasciare acceso l'hardware più tempo possibile, controllando che esegua correttamente i suoi calcoli senza che avvengano crash indesiderati.

1.3 Cos'è TurtleCoin

TurtleCoin è una cryptovaluta che originariamente nasce da un fork del progetto di Monero, basato sull'algoritmo "CryptoNight".
Inizialmente l'algoritmo utilizzato da TurtleCoin era modificato in modo tale da essere il più leggero possibile, cercando di aiutare i miner a fare in modo che fosse conveniente estrarre questa cryptovaluta.
L'algoritmo era chiamato "CryptoNight Lite" o più semplicemente "CryptoNight Turtle".
Per sintetizzare, CryptoNight Turtle è una modifica dell'algoritmo CryptoNight, semplificando la computazione.
Questa semplificazione è stata ottenuta nei seguenti due modi:

Modifica dell'iterazione E' stato effettuata una riduzione del numero delle iterazioni di quattro volte, da 524,288 iterazioni a 131,072. Questa modifica ha consentito di aumentare il rateo di hash effettuabile dai miner, andando a vantaggio loro e del network per la velocità delle transazioni. Sicuramente è stata effettuata una procedura simile perchè la rete non era sicuramente paragonabile a una rete di cryptovalute che giravano su algoritmo CryptoNight.

Modifica dello scrath pad Anche la modifica dello scratch pad è calata di quattro volte, da 1MB (CN Lite) a 256KB. Poichè si è mirato a rendere il tutto il più veloce possibile, riducendo così il contatore di iterazione, bisognerà essere sicuri che lo scratch pad sia usato effettivamente per prevenire qualche attacco.

A differenza di altri progetti di cryptovalute, attualmente, a livello di funzionalità, non ci sono differenze sostanziali tra questa cryptovaluta ed un'altra. La domanda sorge spontanea: perchè puntare proprio a TurtleCoin e non a progetti analoghi?
TurtleCoin ha un ottimo potenziale, in quanto nasce da un fork di Monero, ovvero una cryptovaluta nella classifica delle migliori 10 come capitalizzazione del mercato. Quindi, come per chi del settore sa, Monero utilizza uno dei

migliori algoritmi preferiti dai miner ed è conosciuto e stimato per stabilità, convenienza e supporto.
Attualmente TurtleCoin è la cryptovaluta più profittevole in assoluto per i miner, sebbene il suo valore odierno sia di circa 0.00003 Euro. E' anche vero che di mese in mese possono nascere Altcoin[1] differenti più profittevoli, ma già da qualche mese risulta la preferita di molti miner.

L'algoritmo così leggero permette ai miner di completare un blocco in media ogni 30 secondi; facendo qualche banale calcolo ci si potrà accorgere che con lo stesso hardware utilizzato per estrarre, ad esempio, una cryptovaluta molto discussa come Ethereum, TurtleCoin è più profittevole di circa il 30% su schede video AMD e di circa il 40% su schede video nVidia.
Una proposta puramente speculativa è di rendere il più utilizzabile possibile questa cryptovaluta per garantirne l'aumento del valore della moneta.
In questo modo un miner riuscirebbe tranquillamente a sostenere tutti i costi relativi all'estrazione della cryptomoneta, garantendo parallelamente una sicurezza sempre maggiore della blockchain. Questo accade quando si utilizza un algoritmo di tipo "Proof of Work" che sarà spiegato a breve nel secondo capitolo.
Si noti che dal momento in cui la cryptovaluta dovesse guadagnare molto valore, la profittabilità calerebbe immediatamente, poichè sicuramente balzerebbe all'occhio di tutti i miner.
Se attualmente si riuscisse ad accumulare una buona somma, sarebbe solo perchè è un periodo negativo per i miner e per le cryptovalute.
Un'ultima osservazione prima di indicare qualche curiosità storica su TurtleCoin, che potrebbe venire alla mente di chiunque segua l'andamento generale di Bitcoin, è quella di pensare alla prossima "bolla speculativa" che potrebbe avvenire nel mondo delle cryptovalute. Proprio in questo caso, se TurtleCoin riuscisse a "cavalcare l'onda", si potrebbe avere un aumento esponenziale del suo valore, in quanto mai prima d'ora è entrata in questa famosa speculazione.

[1]Le Altcoin sono criptovalute alternative create dopo il successo di Bitcoin. Si proiettano come sostituti migliori di Bitcoin.

1.4 Storia di TurtleCoin

TurtleCoin nasce una notte del 9 dicembre 2017, quando due sviluppatori che lavoravano su altri progetti, in mezzo a tanta follia e volatilità del mercato, hanno pensato di progettare una cryptovaluta divertente e ottima per effettuare transazioni veloci (si stimano 20 volte più veloci delle transazioni di Bitcoin o Bitcoin Cash).
Nella loro idea di cryptomoneta c'era l'intenzione di garantire la privacy, avere facilità di estrazione e facilità di utilizzo.
TurtleCoin si focalizza quindi sulla riservatezza, la decentralizzazione, la scalabilità e sulla fungibilità, prendendo queste caratteristiche da Monero.
La community di TurtleCoin è molto attiva e presente su canali ufficiali tramite l'utilizzo del software Discord.
Il canale si struttura per tipologie di discussione da parte dei developers, che forniscono nuove idee, presentano report di bug e fix; inoltre, esiste un canale per l'aiuto generale per qualsiasi tipo di utente.
Le modalità di accesso a TurtleCoin sono svariate: si può acquistare direttamente da vari exchange oppure in poche ore estrarre migliaia di monete.
Il valore attuale di TurtleCoin, attualmente, è di circa 0.00003 Euro.
Una volta acquistati o estratti, è possibile controllare il proprio wallet. Esistono diversi applicativi per ambiente Windows, Apple, Linux e Android ed anche siti di exchange.

1.4.1 Storia di Monero

Monero è una criptovaluta creata nell'aprile del 2014. Si focalizza sulla privacy, la decentralizzazione, la scalabilità e sulla fungibilità.
Il suo primo nome è stato BitMonero, per poi divenire semplicemente Monero che in esperanto significa moneta.
Monero è decentralizzato, cioè è una cryptomoneta digitale sicura utilizzata dagli utenti della rete. Le transazioni sono confermate da consensi distribuiti e dopo registrate in maniera immutabile sulla blockchain. Non vi è alcun bisogno di terze parti per tenere al sicuro i propri Monero.
Monero è privato, cioè utilizza tre differenti tecnologie mirate alla privacy: "ring signatures" (firme ad anello), "ring confidential transactions" (RingCT, transazioni confidenziali ad anello) e "stealth addresses" (indirizzi stealth oscurati di default). Queste tre tecnologie mascherano rispettivamente il mittente, l'ammontare ed il destinatario della transazione.
Gli indirizzi di invio e ricezione, così come l'ammontare della transazione, sono offuscati di default. Le transazioni sulla blockchain di Monero non possono essere collegate ad alcuna identità nel mondo reale.
Tutte le transazioni sulla rete Monero sono private: non c'è alcuna possibilità di effettuare, neanche accidentalmente, una transazione trasparente.
Questa caratteristica è tipica solo di Monero. Non si ha bisogno di dare fiducia a nessuno per mantenere la propria privacy.
Monero è fungible poichè è privato di default. Nessuna unità di questa cryptomoneta può essere inserita in una lista nera da venditori o exchange perché associata a transazioni effettuate in precedenza.
Un esempio pratico: si supponga che la moneta in proprio possesso sia stata usata precedentemente in un attacco ransomware. Il titolare della moneta, se avesse saputo di riceve la moneta "sporca", non l'avrebbe accettata.
Monero è fungibile, pertanto chi lo utilizza non ha bisogno di effettuare questi controlli.
Il supporto tecnico di Monero è molto attivo; infatti per mantenere la migliore decentralizzazione della rete, vengono eseguiti abituali fork del progetto

indicativamente ogni 6 mesi.
Monero gira su un algoritmo computazionale denominato "CryptoNight". Su CryptoNight viene eseguito un fork che prevede un leggero cambiamento dell'algoritmo, aggiornandone il nome in "CryptonightV7", "CryptonightV8", "CryptonightR" (attuale).
Si ritiene che entro poco tempo avverrà un nuovo fork che cambierà completamente l'algoritmo, passando al nuovo "RandomX" che avvantaggerà le CPU dei miners invece che le GPU. Si parla quindi di un hard fork imminente. E' stato effettuato questo cambio estremo di algoritmo per motivi che si analizzeranno in seguito, per separare la rete dei miner possessori e utilizzatori di CPU con gli altri che utilizzano ASIC.
Una domanda che ci si può porre è quella di chiedersi per quale motivo l'algoritmo cambi periodicamente. Come da introduzione, bisogna ricordare che è importante che la rete mantenga il livello massimo di decentralizzazione tra i miner, così da evitare di avvantaggiare qualcuno nello specifico; vengono creati dispositivi ad hoc per quel tipo di algoritmo che permettono di computare operazioni in maniera molto più veloce ed efficiente rispetto ai classici dispositivi dei miner medi. Questi dispositivi si chiamano ASIC; Monero e TurtleCoin nascono con l'idea alla base di "ASIC-Resistant" per contrastare tale hardware.
Gli ASIC non sono altro che dispositivi "embedded"(o circuiti integrati) in grado di svolgere un solo tipo di calcolo ma di svolgerlo in maniera molto rapida.
In realtà sono stati citati solamente gli ASIC, ma più avanti sarà citato anche un altro tipo di dispositivo hardware chiamato "FPGA", il quale permette una quantità di calcolo molto maggiore rispetto una scheda video comune, ma con un consumo elettrico relativamente basso.
Tornando al nuovo algoritmo di Monero, RandomX è un algoritmo completamente nuovo e ancora poco diffuso; l'utilizzo di esso serve a svantaggiare i possessori di ASIC. Si ritiene che questo tipo di algoritmo avvantaggerà le CPU e non più le GPU, quindi si avrà un grosso cambiamento anche a livello

di rete e ci si aspetterà molta instabilità nei primi tempi, rischiando anche forti oscillazioni nel valore della cryptovaluta.

1.4.2 Obiettivi TurtleCoin

Si ripercorrano gli obiettivi di TurtleCoin e quelli già raggiunti.
TurtleCoin nel primo trimestre del 2018 ha raggiunto l'obiettivo prefissato di creare Partnership di mercato, quindi possibile compravendita in diversi mercati.
Nel secondo trimestre del 2018 ha iniziato lo sviluppo di Karai, per semplici smart contracts. Le reti distribuite e senza fiducia hanno usi oltre la valuta. Karai è l'obiettivo per abilitare applicazioni e reti distribuite oltre la blockchain principale.
Nel primo trimestre del 2019 gli sviluppatori di TurtleCoin hanno lanciato servizi di integrazione dei pagamenti divertenti, veloci e facili per gli sviluppatori stessi. Questi servizi sono:

TurtlePay progettato per aiutare gli sviluppatori a integrare i pagamenti TurtleCoin nelle loro applicazioni esistenti, fornendo un set di strumenti di facile utilizzo.

TRTL.services per creare app on-chain in modo facile, divertente e veloce sulla rete TRTL.

Il prossimo obiettivo sarà complesso e tratterà l'uso di smart contracts.
Blocchi di piccole dimensioni aiutano sicuramente il miner, ma per contro, producono una chain enorme. L'obiettivo di TurtleCoin quindi, sarà di produrre blocchi più veloci su una catena più corta. Obiettivo di forte impatto, che richiederà il massimo aiuto per il completamento.
Da pochi giorni a questa parte, TurtleCoin ha rilasciato un grande aggiornamento della blockchain. L'ultima versione contiene un aggiornamento del consenso di rete al blocco 2.000.000 che non consentirà all'output di una transazione di superare 1/4 della fornitura totale (250.000.000.000,00 TRTL). La dimensione dell'ammontare inviabile di TurtleCoin, ora, supporta somme elevate, al contrario di prima che doveva suddividere l'ammontare in numerose transazioni.

Capitolo 2

Problematica mining pool

2.1 Protocollo Stratum

Il "pool mining", come è stato appena introdotto, è un approccio al mining dove più client contribuiscono all'aumento di probabilità di chiudere un blocco e quindi dividersi la ricompensa in accordo con la potenza di calcolo fornita in termini di hashrate. E' molto importante entrare nel dettaglio, il pool mining riduce efficacemente la granularità della ricompensa per la generazione di blocchi, diffondendola nel tempo in modo più uniforme.
Lo Stratum Protocol è essenzialmente l'evoluzione del protocollo "getwork", creato per supportare il pooled mining. In passato, con getwork, l'intestazione del blocco (block header) veniva passata dal server al client, senza alcuna transazione.
L'unico modo per modificare il blocco era attraverso il valore nonce. Il massimo che il client poteva fare era provare tutti i valori nonce richiedendo più lavoro dal server.
Il metodo "getwork" RPC(Remote Procedure Calls) era il metodo più semplice e originale, che costituiva direttamente un'intestazione per il miner.
Dal momento che un'intestazione contiene solo un singolo nonce a 4 Byte valido per circa 4 gigahash, molti miner moderni dovrebbero eseguire dozzine o centinaia di "getwork" al secondo.

I solo-miner, o nodi della rete, possono ancora usare "getwork" su vecchie versioni, ma la maggior parte delle mining pool, oggi, lo scoraggia o non ne consente l'utilizzo.
Un metodo migliorato è il RPC "getblocktemplate". Ciò fornisce al software di mining molte più informazioni, ad esempio le informazioni necessarie per costruire una transazione pagando la pool o il wallet TRTL(nel caso di TurtleCoin) del solo-miner.
Stratum è un protocollo basato su linea che utilizza una socket TCP, con payload[2] codificato come messaggi JSON-RPC.
Il client apre semplicemente la socket TCP e invia richieste al server sotto forma di messaggi formato JSON. Ogni riga ricevuta dal client è di nuovo un frammento JSON-RPC valido, contenente la risposta.
Stratum è un protocollo facile da implementare ed è facile eseguirne il debug, perché entrambe le parti stanno parlando in un formato leggibile.
In aggiunta, JSON è ampiamente supportato su tutte le piattaforme e i miner attuali dispongono già di librerie JSON. Quindi comprimere e decomprimere il messaggio è davvero semplice e conveniente.

[1]Un payload è una routine presente in un virus informatico che ne estende le funzioni oltre l'infezione del sistema. In breve, sono le azioni che il virus esegue dopo aver infettato il sistema. Virus differenti possono avere uno stesso payload. Quindi si intende qualsiasi operazione a tempo determinato, casuale o attivata da un trigger che un virus o worm manda in esecuzione. Questa può essere di distruzione parziale o totale di informazioni. Alcuni virus possono avere più payload. Altri possono non averne e limitarsi a replicarsi da un computer a un altro.

2.1.1 I vantaggi di Stratum

Il protocollo Stratum è una soluzione sull'attuale protocollo HTTP.
HTTP è stato progettato per la navigazione dei siti Web in cui i client richiedono al server contenuti specifici, il che significa che nel mining le comunicazioni HTTP sono guidate dai minatori che richiedono nuovi lavori di mining disponibili per i server della pool.
Quello che succede nella realtà è questo: come accadrebbe se si utilizzasse il protocollo HTTP, i miner o le pool dovrebbero richiedere notizie per quanto riguarda i nuovi lavori di mining. Con il protocollo Stratum, invece, è possibile controllare la comunicazione in modo più efficiente scambiando i ruoli.
Un altro vantaggio e anche una soluzione per "ntime rolling" è che per ogni lavoro ricevuto dal server, un minatore può modificare solo ntime e nonce. Di solito, i miner di grandi dimensioni possono eseguire tutti i possibili valori dei due campi alla ricerca della soluzione. Se un minatore esaurisce le uniche possibilità, dovrà inviare una nuova richiesta.
I miner più nuovi e più veloci rendono questo compito più semplice da eseguire e l'utilizzo della larghezza di banda per una pool aumenterebbe in maniera esponenziale.
Stratum risolve questo problema, concedendo ai miner alcuni campi in più che aumentano seriamente le soluzioni totali possibili di un blocco.
Il terzo vantaggio è Long-Polling: quando le pool entrano in gioco, le persone scoprono che devono decidere tra intervalli di polling brevi (= carico di rete più elevato, rapporto di stallo inferiore) e intervalli che non sovraccaricano la rete ed i server, ma che portino a un rapporto molto più elevato di azioni rifiutate. Il Long-Polling era la risposta.
Il long-polling è un ottimo modo per ottenere aggiornamenti in tempo reale utilizzando tecnologie web standard. Sempre per la stessa ragione di HTTP, le tecnologie web standard creano molta inefficienza poiché i minatori richiedono dati che semplicemente non ci sono e i server devono mantenere tali connessioni per tutto il tempo in cui avviene l'estrazione.

2.1.2 Sicurezza di Stratum

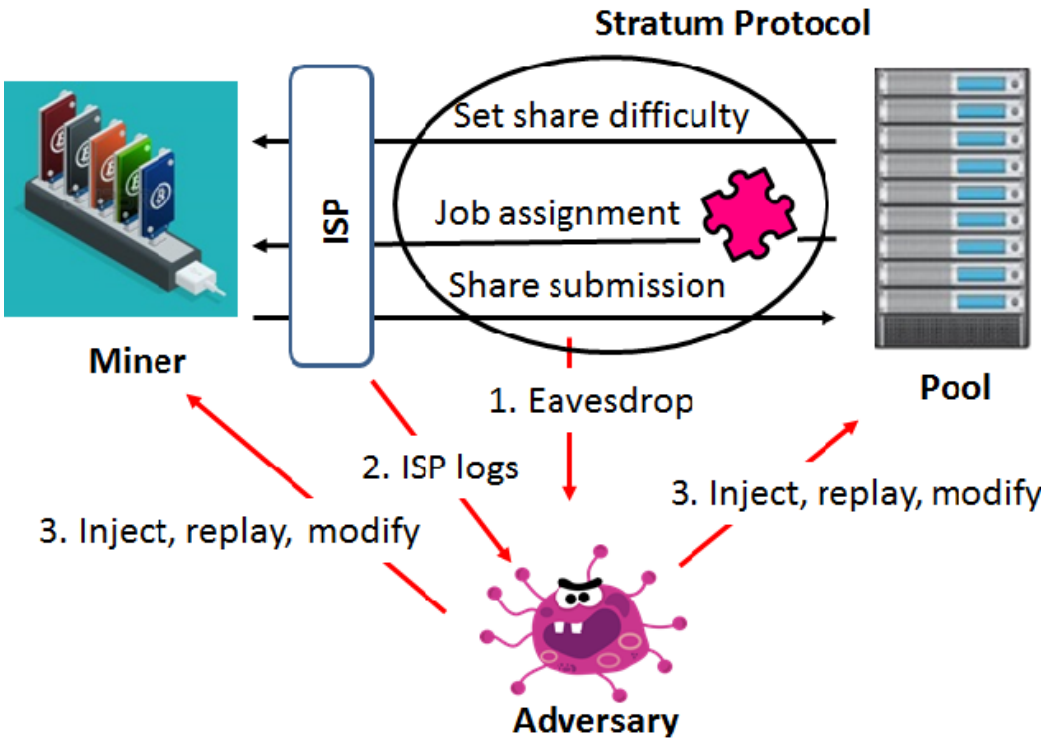


Figura 2.1: Come reagisce il protocollo Stratum agli attaccanti.

Stratum è un protocollo testato anche attraverso attacchi di penetration testing. In particolare, la pool e i miner comunicano tramite il protocollo Stratum, per assegnare lavori e per inviare risultati. Il famoso penetration tester Ruben Recabarren mostra tre tipi di possibili attacchi creando un "modello avversario":

Attacco di Eavesdrop L'eavesdropping è un tipo di attacco in cui un malintenzionato cerca di catturare passivamente i segnali radio decodificando, o cercando di decodificare, i dati trasmessi.

Recupero log ISP Attacco nel recupero di informazioni dai log dell'Internet service provider (ISP in italiano significa fornitore di servizi Internet); nelle telecomunicazioni indica un'organizzazione o un'infrastrut-

tura che offre agli utenti servizi inerenti a Internet, i principali dei quali sono l'accesso al World Wide Web e la posta elettronica.

Interferire e modificare le comunicazioni Stratum dei minatori Attacco piuttosto diffuso, quello di modificare ad esempio l'indirizzo di pagamento di miner o di cambio pool.

Analizzando gli attacchi di cui sopra, Recabarren ha lavorato su due attacchi passivi chiamati: StrapTap, dove l'avversario può catturare e accedere a tutte le informazioni sui pacchetti Stratum e agli ISP Logs, dove l'avversario può solo accedere al tempo del pacchetto.
La soluzione richiesta per ottenere un protocollo Stratum più forte deve considerare:

Sicurezza proteggersi dagli attacchi Stratum ed esser resilienti agli attacchi.

Efficienza la crittografia di tutti i pacchetti Stratum è inefficiente e non sicura.

Adattabilità modifiche minime al protocollo Stratum.

Quindi, eccoci con Bedrock, un'estensione sicura ed efficiente del protocollo Stratum. Essa cerca di impedire agli avversari di dedurre gli hashrates dei miner e di autenticare in modo efficiente i messaggi Stratum. Bedrock ha 3 componenti, ognuno dei quali affronta diverse vulnerabilità Stratum.
Il primo componente autentica e offusca l'assegnazione del lavoro e condivide i messaggi di invio.
Il secondo componente protegge le notifiche di difficoltà di condivisione.
Il terzo componente protegge l'inferenza della pool sulle capacità del miner.

2.2 Proof of work vs Proof of Stake

Cynthia Dwork e Moni Naor avevano inizialmente concepito il PoW nel 1993.
Bitcoin è l'implementazione di PoW (Proof of Work) più famosa e tra poco sarà spiegato il concetto.
Le transazioni nella blockchain Bitcoin sono raggruppate in una pool di memoria chiamata "mempool"; nello stesso momento, ogni 10 minuti, viene creato un blocco. Ogni transazione in mempool necessita di verifica e i "miner" lo eseguono.
Il processo di verifica della transazione si chiama "mining", anche se già ripetuto è giusto ribadire il concetto perchè a breve si entrerà nel nocciolo del funzionamento delle cryptovalute che utilizzano l'algoritmo di "Proof of work".
L'utente Bitcoin che richiede la transazione fornisce i dati della transazione al miner, il quale procede quindi alla verifica di essa.
Tuttavia, per includere la transazione nel blocco successivo, il miner deve conoscere il valore dell'hash crittografico dell'ultimo blocco registrato e nascosto a tutti. Questo valore di hash deve essere referenziato per la creazione di un nuovo blocco.
Per trovare l'hash dell'ultimo blocco, il miner deve provare un numero dopo l'altro con un metodo di calcolo a "forza bruta" e senza competenze particolari per farlo. I miner vengono premiati con una frazione del Bitcoin, il miner di successo è colui che batte tutti gli altri in questa fase e risolve questo enorme enigma matematico usando un'immensa potenza di calcolo.
Dopo aver trovato l'hash dell'ultimo blocco registrato, il miner lo annuncia alla rete per la verifica da parte degli altri nodi e crea un nuovo blocco con le transazioni nella verifica post di mempool.
Il puzzle crittografico risolto dal miner è asimmetrico; questo vuol dire che nel periodo di tempo successivo, i miner restano in attesa di un nuovo blocco da convalidare. A questo punto, i miner trovano il puzzle più semplice in base alla loro potenza e il tempo di generazione del blocco si riduce.

Quindi, il puzzle viene rivisto ogni 14 giorni per renderlo più complesso. Ciò significa che d'ora in poi sarà necessaria una maggiore potenza di calcolo.
Tuttavia, questa elevata sicurezza ha un costo elevato. La potenza di calcolo sempre crescente dei nodi richiede sempre più energia elettrica, ad esempio alla fine del 2018, le operazioni di mining di Bitcoin consumavano più energia in Islanda rispetto al consumo totale di energia domestica del paese.
Il Bitcoin non è supportato da alcun bene tangibile e tale tensione ambientale per una valuta digitale sta attirando una copertura mediatica negativa.
Inoltre, il coinvolgimento di tutti i nodi nel processo di convalida della transazione influisce sulla scalabilità e sulla velocità effettiva della transazione.
Come se non bastasse, è difficile per i singoli miner aggiornare continuamente il loro hardware per risolvere enigmi matematici sempre più complessi e far fronte alla crescente bolletta dell'elettricità.
Ogni nuovo hardware rilasciato dalle varie case produttrici, sarà sempre più performante e meno costoso in termini di energia. Quindi ciò che avviene è una sempre più debole decentralizzazione nel mining, perchè i miner più piccoli si troveranno a competere con grandi piattaforme organizzate con disponibilità liquide sicuramente maggiori.

Tale decentralizzazione sempre più debole va contro il principio fondamen-

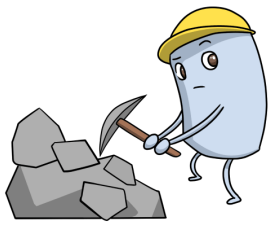


Figura 2.2: PoW - FONTE: korancrypto.com

tale dell'idea per cui è nata la blockchain.
Proprio per questa ragione nascono progetti come TurtleCoin, per mantenere una rete appetibile a tutti, allontanando i produttori di ASIC o di quell'hardware particolare, non alla portata di tutti.
In che cosa differisce l'algoritmo PoS?

Nel caso dell'algoritmo PoS (Proof of Stake), un insieme di nodi decide di puntare le proprie criptovalute per la convalida della transazione. Sono chiamati "stakers". Maggiore è la quantità di puntata e più lunga è la durata della puntata, maggiori sono le possibilità dello staker di ottenere la responsabilità della convalida della transazione.
Tutte le criptovalute in questa rete sono già state create e non esiste mining. Ciò elimina la necessità di risolvere un puzzle crittografico complesso con tutte le consueguenze negative già citate, quindi il continuo aggiornamento dell'hardware e l'aumento dei costi energetici sono stati eliminati.
Il processo di convalida della transazione si chiama "sharding".
Tuttavia non è necessario che l'intera rete sia coinvolta nel processo di convalida della transazione, il che migliora la scalabilità. PoS consente di implementare un'altra soluzione tecnologica chiamata "sharding".
Il concetto originario di gestione di un database, si basa sulla memorizzazione di diverse partizioni dello stesso, in un'istanza del server separata, per una maggiore efficienza; lo sharding della blockchain ha un significato attribuito alla archiviazione di porzioni orizzontali della rete in gruppi separati di nodi. Poiché nessun nodo può vedere l'intera rete, lo sharding non può essere implementato insieme all'algoritmo PoW ed è necessario PoS con staker separati per shard(frammenti) separati.

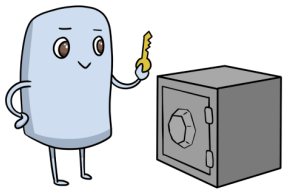


Figura 2.3: PoS - FONTE: korancrypto.com

2.2.1 PoW vs PoS: qual è la migliore?

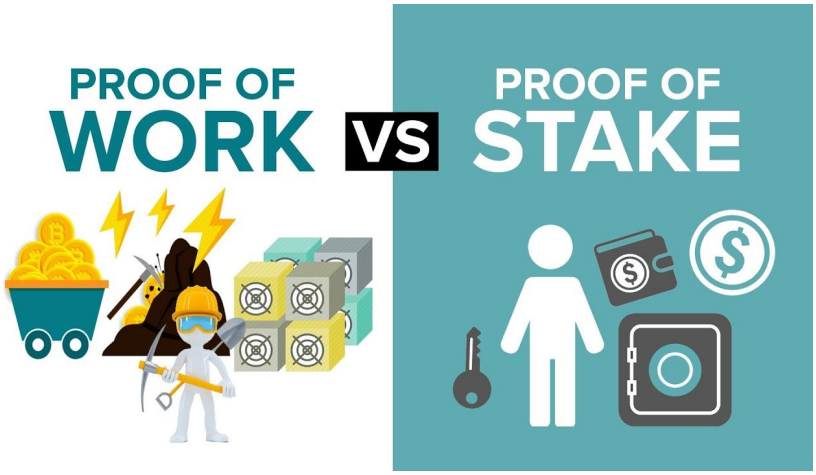


Figura 2.4: Differenze tra due tipi principali di algoritmi: PoW e PoS. - FONTE: itastakers.com

PoW è stato ben testato e utilizzato in molti progetti di criptovalute. Gli attacchi DDoS su una blockchain che utilizza questo algoritmo sono impossibili con la tecnologia informatica odierna; tuttavia, l'elevato costo energetico, l'aumento della tensione per l'ambiente, la copertura mediatica avversa associata, l'aumento della centralizzazione delle operazioni di mining e il basso rendimento delle transazioni lo renderanno probabilmente non sostenibile nel lungo periodo.
Le comunità sono sempre più preoccupate per gli alti costi energetici del mining di Bitcoin e la Cina, in passato, ha tentato vietare tutte queste operazioni. In realtà, in base a una notizia di questo fine 2019, la Cina starebbe tornando a supportare Bitcoin come tecnologia anche per quanto riguarda il mining.
Le idee sono ancora molto confuse, in quanto dei reali progetti con utilizzi pratici sono in netta minoranza rispetto tutti i progetti delle cryptovalute esistenti. Quello che è certo è che la più grande azienda cinese produttrice di ASIC al mondo, ha annunciato di voler divenire la più grande miniera per l'estrazione di Bitcoin.

L'algoritmo PoS fornisce una blockchain più scalabile con un "throughput" (capacità trasmissiva) di transazione più elevato; alcuni progetti l'hanno già adottata, come ad esempio: DASH, NEO, QTUM, ecc.
PoS è meno sicuro dell'algoritmo PoW che è completamente decentralizzato, come nel caso di TurtleCoin. Tuttavia, la rete decentralizzata Bitcoin si sta spostando sempre più verso grosse farm cinesi, a discapito della sicurezza globale. Si vedano per esempio gli attacchi 51%.
Tornando all'algoritmo PoS, è possibile acquistare la maggior parte delle monete nella rete, diventare la falsa scelta e convalidare transazioni sbagliate come parte di un attacco.
Tuttavia, l'economia di mercato ha una valvola di sicurezza naturale per questo, perché il prezzo della moneta aumenterà in modo significativo quando qualcuno cercherà di acquistare un gran quantitativo di monete, rendendo il lavoro degli attaccanti molto più difficile.
È anche possibile che uno staker si trasformi in un attaccante e convalidi transazioni sbagliate. Il progetto Ethereum, come parte della loro prevista transizione al PoS, ha progettato il protocollo "Casper" in cui tali criminali vengono puniti confiscando le loro criptovalute puntate e impedendo loro di non puntare mai più.
Se l'implementazione pianificata di PoS in un protocollo famoso come Ethereum dovesse aver successo, la comunità crittografica sarà probabilmente rassicurata sulla capacità dell'algoritmo PoS di proteggere la rete. Questo però potrebbe rovesciare la medaglia a favore del PoS e solo il tempo dirà quale sarà l'algoritmo di consenso per la blockchain nel futuro.

Capitolo 3

Analisi economica di TurtleCoin

Dopo una accurata introduzione su cos'è e come funziona la blockchain e alla presentazione della nuova cryptovaluta, si passa all'analisi economica della sostenibilità della blockchain di TurtleCoin e della progettazione per la realizzazione di una mining pool, prendendo in considerazione i costi derivanti dal mining.
Lo scopo di questo progetto è verificare la sostenibilità di tale tecnologia, lasciando come principale obiettivo il rispetto per l'ambiente, il basso consumo energetico, quindi il basso rilascio di CO2, e analizzarne l'investimento e il trading di cryptovalute. Questi sono i due modi principali possibili per trarre profitto dalla blockchain, generando utili nel mercato finanziario del Forex.
Per un Trader alle prime armi è utile conoscere la differenza di entrambi all'interno del mondo finanziario.
Nella società odierna, lo scopo di un investitore è quello di accrescere in maniera graduale il proprio patrimonio attraverso il possesso o l'acquisto di strumenti di investimento, come ad esempio un portafoglio di azioni.
Gli investimenti possono avere un orizzonte temporale molto vasto. Questo permette agli investitori di interessarsi al valore a lungo termine non preoccupandosi delle oscillazioni giornaliere del mercato; qualora ci fosse una perdita

di valore, questi trattengono il proprio investimento nell'attesa dell'aumento dei prezzi.
Nel caso in cui si parla di Trader più esperti, è possibile speculare anche intra-day, cioè all'interno di una giornata è possibile comprare e vendere più volte.
Le cryptocurrencies sono mantenute da una comunità di miner che hanno istituito, tramite i loro computer, una partecipazione, validazione ed elaborazione delle transazioni.
E' importante sottolineare e ricordare che questo tipo di moneta è attualmente un'alternativa alle valute tradizionali, perché si usa unicamente online e non viene sottoposta ad alcun controllo da parte di alcuna banca, ma dipende unicamente dalle transazioni che ne determinano il valore.
Ciò che garantisce il corretto funzionamento del sistema TurtleCoin, come per tutte le cryptovalute in generale, è il mining.
Il mining è un'operazione onerosa, in termini economici, se si considerano l'hardware e l'elettricità impiegati.
A tal proposito si riporta quanto calcolato dalla rete Bitcoin, per effettuare una singola transazione in termini energetici.
Una singola transazione in Bitcoin utilizza un quantitativo di elettricità sufficiente ad alimentare 10 case americane, mentre nel suo complesso l'energia consumata dalla cryptovaluta potrebbe soddisfare il fabbisogno di 2,79 milioni di case.
Questo è un dato aggiornato al 4 ottobre 2018. Attualmente la rete Bitcoin ha continuato a crescere ed evolversi molto rapidamente, sia per quanto riguarda l'hardware, sia per quanto riguarda l'efficienza.
Si noti che con lo stesso consumo attuale della blockchain di Bitcoin, si ha un network molto cresciuto.
Purtroppo, in paesi Asiatici o paesi Arabi dove la corrente elettrica costa poco, non viene dato grosso peso al consumo di energia richiesto dalle macchine e nemmeno all'inquinamento, ma ci si concentra esclusivamente sulla potenza che riescono a raggiungere. Questo è l'impatto ambientale di cui si parla e

che bisognerebbe evitare, sfruttando maggiormente energie rinnovabili.

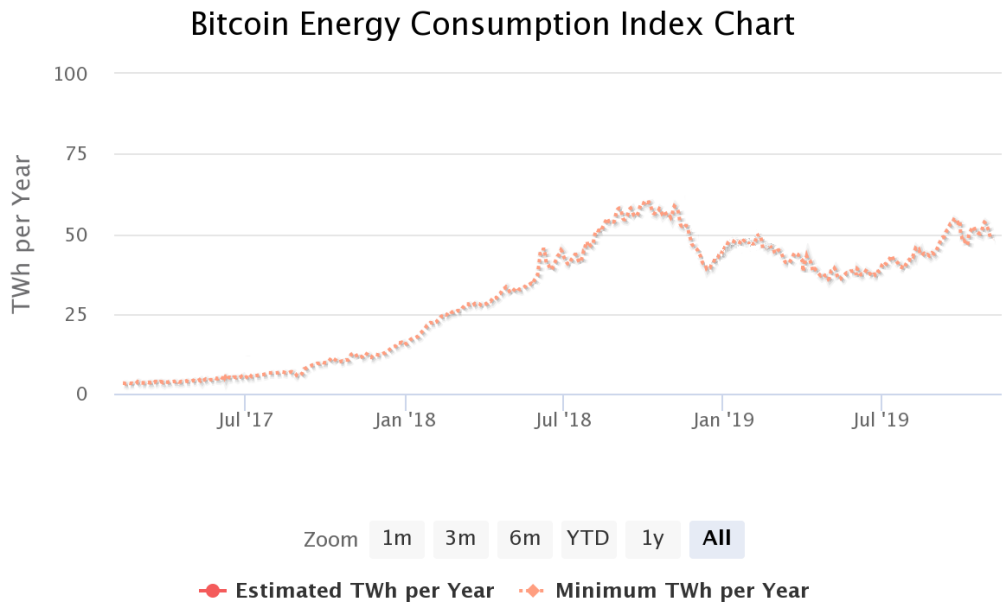


Figura 3.1: Consumo energetico impiegato nel mining di Bitcoin. FONTE: https://digiconomist.net/bitcoin-energy-consumption

Da questa figura si può notare come l'hashrate globale, in essa indicato, sia cresciuto tantissimo negli anni. Nel frattempo, con l'arrivo delle nuove tecnologie hardware, il consumo elettrico è rimasto contenuto.
Un punto forte da considerare è che l'hashrate di Bitcoin ha raggiunto un valore pari a 114 EH/s: la cifra più alta di sempre.
L'hashrate di una criptovaluta è un parametro che indica la quantità di calcoli che il network riesce a compiere in una unità di tempo.
Questo valore può essere anche utilizzato per identificare il livello di competizione fra i miner della criptovaluta per aggiudicarsi le ricompense legate alla generazione di nuovi blocchi.
In altre parole, i miner prevedono che in futuro il prezzo di Bitcoin aumenterà.
Nel grafico sotto riportato vengono evidenziati l'andamento e la crescita della

rete Bitcoin. A breve avverrà l'halving di Bitcoin e, in seguito ad esso, potrebbe calare drasticamente l'hashrate globale, aumentando probabilmente il valore di Bitcoin. Questa è una delle probabili ipotesi per cui il mining potrebbe non durare ancora a lungo.
Con le tecnologie odierne, la prospettiva sarà quella di passare lentamente da algoritmo di tipo PoW (Proof of Work) ad uno di tipo PoS(Proof of Stake).

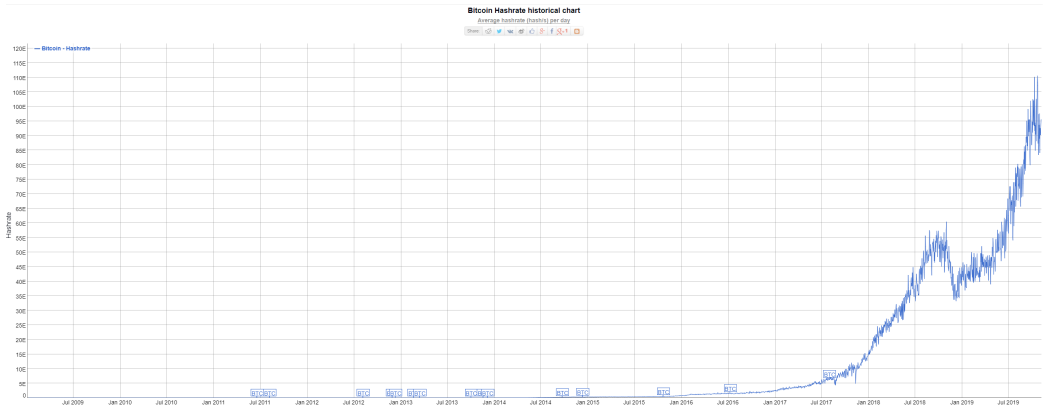


Figura 3.2: Crescita dell'hashrate globale dei miner. FONTE: https://www.blockchain.com/charts/hash-rate

Ma cos'è l'halving? La ricompensa per chi risolve i blocchi della blockchain è quella di ricevere Bitcoin appena coniati. Questo causerebbe l'aumento spropositato di distribuzione della cryptomoneta Bitcoin e un'inflazione che poi finirebbe con l'erodere il valore.
Per questo motivo, ogni 4 anni, secondo le regole stabilite da Nakamoto, avviene il dimezzamento o halving del Bitcoin (comprese tutte quelle altre cryptovalute che nascono da un fork di Bitcoin).
Finora, a partire dalla creazione di Bitcoin nel 2008 sono avvenuti soltanto 2 halving: il primo nel 2012 e il secondo nel 2016. Nel 2016 la ricompensa è passata da 25 a 12,5 Bitcoin e nel 2020 arriverà ad un valore di 6,25 BTC.
Per sostenere tutta questa potenza di calcolo servono computer sempre più potenti e sistemi di condizionamento (ma si vedrà nel capitolo seguente che l'hardware si può ottimizzare di molto!) per evitarne il surriscaldamento.

Per soddisfare le necessità energetiche sono nate le Server Farm, ossia interi campi in cui viene prodotta energia elettrica generata da centrali a carbone che vanno a costituire le cosiddette “farm” o “miniere”.
La larga diffusione delle farm sostenute dalle miniere di carbone, hanno prodotto un sensibile aumento delle emissioni di CO2.
I paesi in cui le farm sono più diffuse, come la Cina, si stanno rivolgendo sempre più ad energie rinnovabili, dall’idroelettrico al fotovoltaico, per essere in linea con le recenti politiche di decarbonizzazione dei processi e essere quindi più appetibili sul mercato.
Recenti studi sull’utilizzo del fotovoltaico hanno evidenziato come esso, in condizioni favorevoli, possa garantire la produzione di energia elettrica a costi inferiori rispetto alle fonti tradizionali. Questa tecnologia potrebbe sia limitare l’inquinamento da CO2 che abbassare il costo delle attività informatiche.

3.1 Ecosostenibilità

Si parla di sostenibilità per indicare una forma di sviluppo economico compatibile con la salvaguardia dell'ambiente e dei beni disponibili per tutelare le generazioni future. Ciò ha dato vita all'economia sostenibile, basata almeno in parte alla cosiddetta economia verde.
La consapevolezza ambientale sta diventando sempre più importante nella società odierna: da questo punto di vista, dunque, vediamo come si può valutare una tecnologia come Blockchain.
Dal punto di vista del supply management si tratterà l'aspetto sul consumo di energia.
In questi ultimi anni è nata una fortissima esigenza di garantire un futuro prospero anche alle generazioni future, visti i numerosi cambiamenti che la società odierna si trova a dover affrontare.
Se prima la sostenibilità era vista come un'opera di miglioramento da adottare, ad oggi si rende necessaria l'adozione di misure drastiche in grado di ridimensionare i comportamenti umani e il funzionamento delle macchine.
In questo senso la blockchain offre un'alternativa molto forte, in quanto sembra essere la risposta ai requisiti del mercato di oggi in termini di semplificazione e sicurezza.
Nelle prossime sezioni verranno spiegate le tecniche per la sostenibilità e le progettazione utilizzate.
La blockchain sta riscuotendo molto successo perché, se prima veniva accostata unicamente alla "bolla del Bitcoin", ora sembra invece avere delle potenzialità che in molti avevano sottovalutato in prima battuta.
Si è iniziato a pensare che potesse rappresentare uno strumento molto efficace non solo per le già citate transazioni finanziarie, ma per tutte quelle applicazioni che richiedevano un immagazzinamento permanente e trasparente del dato.
Ora si pensi alla giornata tipo della maggior parte delle persone. Essa è composta da innumerevoli operazioni come: prelievi in banca, pagamento di bollette, pagamento di merci, rifornimenti e via dicendo.

La cosa che accomuna tutte queste attività è la grande mole di carta e/o altro materiale che ci si ritrova a fine giornata, per la maggior parte inutile e non più consultata.
Una qualsiasi ricevuta passa da essere un tagliando di acquisto ad un rifiuto in poche ore.
Ora si immagini di allargare questo concetto e di rendersi conto di quante tonnellate di rifiuti vengano prodotte a fine giornata senza una reale necessità e, di conseguenza, dell'impatto sull'economia e sull'ambiente.
Ovviamente bisogna considerare tutti questi elementi, non la singola ricevuta o la pubblicità che ci si ritrova nella buchetta, dove ben presto diventa materiale di rifiuto.
La necessità di dover stampare qualcosa di fisico nasce dall'esigenza di dover dimostrare che il possessore della ricevuta sia colui che ha effettuato l'operazione.
Questo meccanismo ha riscontrato numerosi feedback negativi, in quanto la perdita della ricevuta non potrebbe più dimostrare l'effettiva provenienza della merce acquistata.
In questo contesto, la tecnologia blockchain rientra pienamente. Si pensi a quanto crollerebbero velocemente i consumi legati alla carta destinata a diventare uno scontrino per la propria merce.
Come già sta succedendo tra i vari miner, ad ogni transazione i dati sono persistenti e non vi è alcun bisogno di ricevute dopo l'invio monetario da una parte all'altra.
Grazie alle sue caratteristiche costruttive, tale meccanismo assicura un elevato standard di sicurezza dell'infrastruttura.
Le informazioni saranno conservate nel tempo e si avrà la possibilità di accedere nuovamente a questo dato anche in seguito, avendo la certezza che l'originalità e la trasparenza siano sempre garantite.
Si ha così la possibilità di dematerializzare la maggior parte delle informazioni che prima invece passavano tramite carta, riducendo l'impatto ambientale e tutte le attività ad esso correlate.

3.1.1 Gestione "green" delle risorse

Per la gestione delle risorse attualmente in uso per la realizzazione di questa mining pool, si è ricorso allo studio e all'analisi di ognuno dei componenti hardware, per trovare quelli che possano garantire un minor impatto a livello ambientale, determinato dal consumo diretto di energia elettrica.
Ogni componente hardware presente nel sistema del progetto realizzato ha avuto pertanto una sua attenta analisi.
Nell'elenco sottostante saranno mostrate le risorse integrate nel sistema e il loro relativo consumo:

Processore AMD Ryzen 7 - 2700x Questo è un componente hardware molto prestante e anche molto recente che AMD ha concepito sulla propria architettura Zen.

I Ryzen di seconda generazione sono realizzati con un processo migliorato, noto come 12nm[1], che promette maggiori prestazioni ed efficienza rispetto ai 14nm dei primi processori Ryzen di prima generazione. AMD, inoltre, ha modificato l'architettura Zen, ora chiamata Zen+, per supportare frequenze più alte, livelli di boost multi-core più sofisticati e dimensioni superiori per cache e memoria.

Il consumo standard dichiarato da AMD per questo processore è un TDP di 105w, mentre il consumo del fratello minore, il ryzen 7 2700, di solo un TDP di 65w. La differenza è minima ma sostanziale. Quello utilizzato nel sistema ha un miglioramento massimo della frequenza fino a 4.3GHz, mentre quello normale può raggiungere i 4.1GHz.

Inoltre, la CPU del sistema in uso, di fabbrica esce con un dissipatore migliore nativo per i 105w, ma non è tutto. Presto si vedranno le caratteristiche aggiuntive.

La prima modifica è stata quella di portare la CPU scelta al pari del fratello minore, ciò ha ridotto la potenza standard e la frequenza allineandosi a 4.1GHz per 65w.

La scelta del processore è stata rivolta verso questo articolo poichè acquistato a prezzo minore, con una dissipazione di calore migliore.

Secondo e ultimo accorgimento è stato quello di calare ulteriormente il voltaggio di -0.128v, quindi passando da un valore di 1,2v si è passati a 1,0872v, riducendo il consumo da 65w a 50w.
I dati sotto riportati sono le potenze massime, o di picco, che il processore può raggiungere; pertanto il funzionamento a normale regime si può ridurre fino metà della potenza appena dichiarata.
Ammettendo ora che il funzionamento della CPU sia sempre al 100% di carico, nel peggiore dei casi, si otterranno questi valori relativi al consumo:

% uso	Consumo(w)	Giorno(w)	Settimana(w)	Mese(w)	Anno(w)
100	50	1.200	8.400	33.600	403.200

Figura 3.3: Tabella dei consumi inerenti alla CPU.

Dissipatore per CPU Il dissipatore per l'areazione consuma a pieno regime 12w. Dal momento che la CPU lavora alla metà della potenza, è stata impostata la velocità di rotazione della ventola al minimo, quindi circa al 35%. I dati tengono in considerazione quindi un consumo di 5w.

Scheda grafica nVidia 9600 GT La scheda grafica è stata utilizzata solo nella prima fase dove il monitor era essenziale. Questo per "colpa" della CPU scelta che non prevede soluzioni con grafica integrata. Eliminando la scheda video, e quindi anche il monitor, il consumo di elettricità creato dalla nVidia 9600 GT non risulta più un problema.
Il controllo e la gestione vengono effettuati da desktop remoto con il software TeamViewer. Lo stesso discorso vale per mouse, tastiera e qualsiasi altra periferica.

SSD L'SSD, o disco a stato solido, in uso è un SSD "Green" nel vero senso della parola. E' classificato nella lista di drive per lo storage per una

[1]nm = processo produttivo della tecnologia dei semiconduttori.

persistenza dei dati a basso consumo. Il suo consumo dichiarato non raggiunge nemmeno i 5w.

Alimentatore E' stato scelto un alimentatore già acquistato in precedenza e quindi già disponibile, della potenza nominale di 500w. L'efficienza di un alimentatore è definita come il rapporto tra la potenza assorbita e quella a disposizione della macchina. L'efficienza di un gruppo di alimentazione migliora in modo inversamente proporzionale all'energia assorbita dalla presa, a parità di energia in uscita. L'alimentatore scelto ha un differenziale di efficienza che oscilla tra il 75% e l'80%.

In conclusione, considerando un consumo misurato a muro grazie al wattmetro, il consumo dell'intero sistema è pari a 70w. Considerando la sua dispersione di calore, il suo consumo totale è stato di 90w. A questo punto rieseguendo l'analisi dei costi energetici, si avrà:

% uso	Consumo(w)	Giorno(w)	Settimana(w)	Mese(w)	Anno(w)
100	90	2.160	15.120	60.480	725.760

Figura 3.4: Tabella dei consumi inerenti all'intero sistema.

3.1.2 Progettazione delle infrastrutture

Figura 3.5: Pannelli fotovoltaici utilizzati.

Questa è una sezione ricca di dettagli tecnici relativi alle infrastrutture utilizzate per svolgere una mining pool ecosostenibile.
Dopo aver effettuato lo studio e l'analisi del sistema e del suo consumo complessivo, si è dimensionata la struttura minima necessaria per trovare con facilità una soluzione che permettesse la piena sostenibilità del progetto con l'utilizzo di energie rinnovabili.
Andando a recuperare il consumo precedentemente calcolato giornalmente, pari a 2160 Watt nell'arco di una intera giornata, per accumulare una corrente elettrica di 0.216 KWh, è sufficiente una batteria singola da 48 Volt, 14.54 Ah ed una profondità di scarica ad ogni ciclo pari al 50 per cento.
Nella struttura ospitante ci sono 12 pannelli fotovoltaici utilizzati per il pro-

getto. Entrando nel dettaglio, ogni pannello fotovoltaico da 300W e 24V è in silicio monocristallino. Considerando la potenza raggiungibile di 300w ognuno, moltiplicato il numero dei pannelli disponibili, si otterrà una potenza massima di picco di 3600W/h.

Con questa energia è stato possibile anche alimentare alcune schede hardware per il supporto della mining pool. La corrente prodotta in eccesso viene rimbalzata nella rete.

Considerando, per eccesso, una copertura di 12 ore, comprendente la notte e/o il maltempo, servirà un accumulo di 90W (consumo orario del sistema) moltiplicate per le 12 ore di copertura necessaria, ottenendo così 1080 Wh o 1,08 kWh, una potenza molto bassa.

Capitolo 4

Implementazione dell'infrastruttura

In questo capitolo si parlerà delle scelte implementative effettuate nel progetto, da quelle hardware a quelle software, trattando della parte energetica e quindi di sostenibilità, e della parte iniziale di test. Per finire, alcuni approfonimenti relativi alla fase precedente dell'inizio del progetto.
Il primo passo è stato quello di realizzare un fork dal progetto presente nel repository di Github della community di TurtleCoin, dove in esso sono state documentate tutte le configurazioni e API dei servizi necessari.
Il progetto è presente su Github e viene costantemente aggiornato per garantirne il corretto funzionamento, l'introduzione di nuove funzionalità e la correzione di bug riscontrati.
Questa parte infrastrutturale è molto importante perchè determinerà le scelte effettuate per realizzare la mining pool ecosostenibile.
Non solo si parlerà della ecosostenibilità del progetto, ma si affronteranno anche quelle tematiche riguardanti le fonti di energia rinnovabile.
Tuttavia, un problema molto evidente riguarda l'accumulo della carica. Non sono ancora presenti delle batterie sufficientemente evolute rispetto alla tecnologia odierna. Si spera che con l'arrivo delle nuove batterie in grafene, la tecnologia possa progredire ulteriormente.

A questo punto può sorgere spontanea la domanda: "Perchè allora utilizzare un algoritmo di tipo "Proof of Work" quando ci sono ancora tutti questi problemi nel produrre e accumulare energie, mentre già esiste l'algoritmo di tipo "Proof of Stake" che sopprime tutte queste problematiche?".
Come si è già anticipato nei capitoli precedenti, il progetto viene incentrato su TurtleCoin che utilizza un algoritmo PoW, quindi maggiore sicurezza informatica e minor rischio di attacchi. Quello che si proverà a proporre alla community TurtleCoin, sarà creare un ibrido tra PoW e PoS, sfruttando i punti di forza di entrambi gli algoritmi.
Questa è il capitolo giusto per approfondire la progettazione del sistema e del progetto di TurtleCoin su cui gira la piattaforma della mining pool.
La progettazione del sistema è stata strutturata su diversi livelli di analisi.
Una prima analisi riguarderà la scelta legata al sistema operativo utilizzato, effettuando alcune comparazioni con altri. Si valuteranno i vari software e tools compatibili con i servizi del sistema operativo, che risultino migliori per quanto riguarda la stabilità.
Una seconda analisi tratterà l'uso dell'hardware grafico scelto, con motivazioni e test pratici del perchè la scelta sia ricaduta su un dispositivo invece di un altro. Si tratteranno, inoltre, le varie ottimizzazioni adottate.
Il passo più importante è proprio l'ottimizzazione, poichè è la base del progetto che tratterà la sostenibilità. Di fatto, è possibile avere enormi risultati e vantaggi modificando i dispositivi hardware.
La terza analisi si incentrerà sul ruolo del server centrale e dei suoi servizi in esecuzione e delle relative porte di rete in uso.
Per finire saranno mostrate le milestone raggiunte e gli obiettivi futuri per lo sviluppo e il miglioramento del sistema.

4.1 Scelte software per lo sviluppo

La scelta del sistema operativo è molto importante. Esso è la base su cui si avvieranno i servizi della pool, per l'immagazzinamento dei dati nel database Redis e per i diversi servizi collegati e utilizzati attraverso API, quali "TurtleCoin Daemon" e "Turtle-Service" per il completo funzionamento del sistema.
Questi servizi sono principalemente il demone di TurtleCoin, ovvero il servizio relativo ai pagamenti ottenuti dalle ricompense dei blocchi convalidati, il servizio che pagherà ogni miner e il servizio sviluppato in "NodeJS" per l'esecuzione della mining pool.
Per questo progetto è stato scelto di utilizzare il sistema operativo Ubuntu 18.04.3 LTS, una distribuzione stabile di Linux basato su supporto continuato da parte della community. E' importantissimo avere una base solida e stabile dove sviluppare il server.
La scelta su quale sistema operativo usare non è ricaduta su Windows.
Il problema di Windows è che usa un quantitativo eccessivo di servizi totalmente inutili per il progetto, consumando risorse preziose per il server: quantità eccessiva di ram occupata e difficoltà di gestione e installazione dei pacchetti utilizzati.
Occupare risorse significa diminuire le prestazioni. Il sistema è in costante aggiornamento per garantirne sempre la migliore stabilità.
A questo punto si può passare a parlare dei vari software e tools implementati e configurati nella nostra mining pool. Passando un pochino più nel dettaglio, gli elementi essenziali per avviare il progetto sono stati i seguenti:

TurtleCoin Daemon v0.20.0 Nuova versione del demone[1] per la sincronizzazione in background della rete TurtleCoin. Il suo principale obiettivo è quello di sincronizzare i nuovi blocchi convalidati trovati nella rete, rimanendo in ascolto sulla porta 11898. Più avanti si vedrà che non si utilizzerà solo per questo scopo, ma anche per il suo servizio passivo collegato ai pagamenti relativi ai vari wallet tramite API, per

la verifica delle ricompense ottenute per ogni miner collegato alla pool.

NodeJS NodeJS è un runtime JavaScript costruito sul motore JavaScript V8 di Chrome[2]. La configurazione è avvenuta tramite NVM, Node Version Manager. Con questo tool è stato possibile scaricare e configurare facilmente node e NPM, Node Package Manager, permettendo salti di versioni node-npm per trovare le versioni che vanno di pari passo.
La mining pool creata utilizza alcuni moduli node compatibili con versioni meno recenti di node, per questo NVM è stato essenziale. La scelta finale è stata utilizzare, node versione 8 e NPM versione 6.

Redis v5 stable Redis è un archivio di strutture di dati in memoria open source, utilizzato come database e cache. Supporta strutture dati come stringhe, hash, elenchi, set, set ordinati con query di intervallo, bitmap, hyperloglog, indici geospaziali con query di raggio e flussi.
Il servizio gira sulla porta 6379 di default.

libssl E' una libreria SSL[3] richiesta per l'utilizzo di un modulo node, chiamato "node-multi-hashing", per l'utilizzo di alcune funzioni di hashing della cryptovaluta, per cui in seguito permetterà la convalida dei blocchi.

Boost Boost è il gestore delle dipendenze per i moduli nativi basati su CMake.js. E' necessario per il modulo node "cryptoforknote-util".

turtle-service E' un servizio per il pagamento automatico attraverso le API del wallet della pool verso tutti i miner che hanno contribuito nella convalida dei blocchi. Turtle-service è il servizio più vecchio compatibile con wallet legacy, ovvero le prime versioni. Attualmente è disponibile

[1]In informatica, nei sistemi Unix e multitasking, un demone (daemon in inglese) è un programma eseguito in background, cioè senza che sia sotto il controllo diretto dell'utente. Tipicamente fornisce un servizio all'utente. Di solito i demoni hanno nomi che finiscono per "d": per esempio, TurtleCoind.

il servizio "wallet-api", ma non ancora utilizzabile con la mining pool perchè non tutti i componenti sono stati ancora completamente aggiornati. Si ricorda che l'intero progetto è incentrato sulla stabilità, la facilità d'uso e comprensione.

[2]Fonte ufficiale: https://v8.dev/

[3]Fonte: Wikipedia. SSL è un protocollo per la comunicazione sicura attraverso una rete. La porta utilizzata generalmente è la 443. Consiste nella comunicazione tramite il protocollo HTTP all'interno di una connessione criptata, tramite crittografia asimmetrica, dal Transport Layer Security (TLS) o dal suo predecessore, Secure Sockets Layer (SSL).

4.2 Hardware utilizzato

Per l'avvio della mining pool non è necessario avere hardware proprio, però se non si dovessero già avere contatti con altri miner, allora, bisognerà preparare qualche macchina ad hoc per garantirne un funzionamento minimo sin da subito. Il problema di avere poca potenza computazionale iniziale, può voler significare, non trovare blocchi nella rete oppure, convalidarli troppo lentamente da rischiare di perdere quel blocco.
L'hardware ad hoc sarà la base per la mining pool ecosostenibile.
Ora occorre capire quante macchine e dispositi hardware utilizzare.
Sicuramente serve esperienza da miner per avere già qualche idea circa l'hardware da utilizzare. Vediamo a breve come sceglierlo in base alle proprie esigenze.
Per finire, si è optato obbligatoriamente per l'utilizzo di un gruppo di continuità da 750VA per garantire la stabilità del sistema, in modo che rimanga online 24 ore su 24, evitando sbalzi di corrente indesiderati.
Al gruppo di continuità sono stati collegati sia il router, per mantenere sempre una connessione attiva, che il server, per tenere avviati i servizi legati alla mining pool.
Passando ora ai vari dispositivi proposti dal mercato, troviamo tre tipi principali di hardware utilizzabile nel mining, ma non tutti sono utilizzabili con TurtleCoin:

ASIC Con l'acronimo ASIC(Application-Specific Integrated Circuit) si denota un genere di circuiti integrati destinati all'esecuzione di uno specifico tipo di operazioni svolte in maniera velocissima, a differenza di normali CPU destinate ad operazioni più generiche e con prestazioni nettamente inferiori.
Gli ASIC nascono per un determinato tipo di algoritmo.
Si veda come fare per respingere un ASIC dalla rete. Semplicemente tenendo aggiornato l'algoritmo e cambiandolo leggermente. Il cambio algoritmo in realtà non è affatto banale. Monero e TurtleCoin, ad esem-

pio, eseguono hard fork ogni 6 mesi in genere, per scoraggiare sin da subito le case produttrici di ASIC nella produzione e in seguito nella vendita.
Per cambiare e tenere costantemente aggiornato l'algoritmo ci sono grossi team di sviluppo dietro.
Turtlecoin come detto nell'introduzione, è una blockchain ASIC-resistant, pertanto non potremo fare affidamento a questo tipo di dispositivo embedded. Gli ASIC svoglono una quantità massiccia di operazioni al secondo rispetto qualsiasi altra tipologia di hardware, ma sono dispositivi con consumi davvero molto elevati. Non sempre risultano la soluzione pià efficiente.

FPGA In generale, le schede FPGA non sono state progettate principalmente per il settore del mining, ma utilizzate in altri campi per la loro estrema velocità di calcolo essenziale per lo sviluppo di progetti come AI(Artificial Intelligence), ma se programmate correttamente per gli algoritmi di mining, possono raggiungere potenze di calcolo molto elevate su tanti algoritmi.
Solitamente, l'uso intensivo e prolungato della scheda produce un calore che deve essere dissipato in modo efficiente per garantire buone prestazioni e una maggiore durata dell'hardware stesso (durata e prestazioni nel tempo).
Proprio per questo motivo, ci sono tre diverse soluzioni, elencate sotto, e che vanno dal meno dissipante al più refrigerante:

1. Soluzione di raffreddamento ad aria;
2. Soluzione di raffreddamento Water Block;
3. Soluzioni di raffreddamento ad immersione.

La soluzione ad aria è la più efficiente a livello di consumi, ma nella scala refrigerante è all'ultimo posto; potrebbe risultare ottimale per paesi con un clima freddo. Per quanto riguarda la soluzione Water Block

risulta molto efficiente, è un ottimo compromesso tra consumo e raffreddamento delle schede. Per finire, la soluzione migliore rimane quella ad immersione in un fluido dielettrico per isolarne la conducibilità. E' una pratica molto onerosa.

GPU Una GPU(Graphics Processing Unit), o scheda video, è un componente hardware che ha lo scopo di elaborare un segnale video e restituirlo in output all'utente attraverso un monitor. Le schede video da qualche anno sono utilizzate come hardware per estrarre cryptovalute.
Questo è possibile perchè una scheda video è composta da tantissimi processori al suo interno. NVidia, per esempio, utilizza i CUDA core, estremamente efficienti per l'algoritmo "Chukwa[1]" utilizzato da TurtleCoin, mentre AMD viene classificata per "Stream Processors".
Si legga rapidamente la differenza.
I core CUDA e gli Stream Processors sono una delle parti più importanti della GPU e decidono che potenza ha tale GPU. Ci sono algoritmi che vengono digeriti meglio da nVidia e altri da AMD.
In linea di massima dopo numerosi test effettuati su AMD con serie RX 4xx e Rx 5xx, ma soprattutto RX vega xx e su nVidia con serie 9, 10 e 20, si può affermare che AMD ha un prodotto più customizzabile soprattutto a livelli di efficienza. NVidia, invece, ha come pregio che i modelli in commercio sono meglio ottimizzati e ottimizzabili in maniera più semplice.
Va notato che i "core" CUDA non equivalgono ai processori Stream

[1]E' un algoritmo duro di memoria ed è vincitore assoluto della memoria del 2015 Password Hashing Comptetition (PHC). Argon2 o Chukwa, è anche relativamente unico in quanto consente un alto livello di personalizzazione nel modo in cui vengono calcolati gli hash, includendo parametri come: il numero di thread da utilizzare (parallelismo), la lunghezza dell'hash risultante arbitraria, i requisiti di memoria (durezza della memoria), il numero di iterazioni (costo del tempo) e l'uso di Sale. Il Sale o Salt è una sequenza casuale di bit utilizzata assieme ad una password come input a una funzione unidirezionale, di solito una funzione hash, il cui output è conservato al posto della sola password, e può essere usato per autenticare gli utenti.

in termini di potenza e numero. Ciò significa che due schede grafiche con lo stesso numero di core CUDA e processori Stream, aventi le stesse frequenze di memoria e di clock, sicuramente non avranno le stesse prestazioni.
Ciò è dovuto dalla differenza dell'architettura delle due case produttrici.
L'algoritmo Chukwa(o argon2/chukwa) rende molto efficiente entrambi i tipi di scheda in termini di prestazioni e consumi.
Si vedano quindi i modelli scelti e utilizzati per la realizzazione e inizializzazione della mining pool: NVidia 2080, 2080ti, AMD rx-570, rx-580 e rx-vega56.

4.3 Ottimizzazione hardware

Di seguito verranno analizzati i vari modelli di GPU impiegati nel progetto. Questa sezione è particolarmente importante perchè le finalità di questo progetto sono rivolte al mantenimento di una blockchain ecosostenibile, quindi con il minimo rilascio possibile nell'aria di CO2 e utilizzando solo ed esclusivamente energie rinnovabili. Esistono vari tipi di energie rinnovabili per sopperire ai danni causati dal carbone e dai derivati del petrolio.
La scelta del fotovoltaico è nata dalla disponibilità dei già citati 12 pannelli fotovoltaici. L'energia in eccesso viene convertita da un inverter e in seguito immagazzinata in una batteria.
Nella realizzazione del progetto, la prima operazione effettuata è stata quella di analizzare i parametri originali della CPU e di conseguenza calare la frequenza del core del processore, eliminando modalità turbo e passando da una frequenza per core di 3,9GHz con consumo di 95w a 3,7Ghz con un consumo di 65w. In seguito è stata effettuata una operazione di undervolt, ovvero una diminuzione di tensione in ingresso dalla CPU di 0.128mV, ottenendo un consumo di soli 50w.
I dati sopra riportati sono stati utilizzati e registrati come picchi da un wattmetro a muro, ma si evidenzia che comunque il consumo non è costante.
La maggior parte del tempo la CPU non è utilizzata completamente.
I vantaggi ottenuti sono: basso costo per la sua alimentazione in termini monetari e basso riscaldamento del componente con conseguente allungamento della vita dei chip interni.
Esistono anche strumenti di automatizzazione, chiamati di autotune, per le schede grafiche. Essi possono fornire un buon setting di base per coloro che non sono molto pratici, ma non sono invece consigliati per gli esperti, in quanto le configurazioni manuali risultano migliori.
La funzione di autotune di intensità dell'hardware, quando abilitata, è un software che testerà le differenti intensità di lavoro delle schede, una alla volta, tentando di trovare una soluzione con parametri di overclock e undervolt stabili. Una volta trovata tale configurazione, registrerà i valori su un file di

testo e la scheda sarà pronta per l'uso.
Come già detto, esistono due case produttrici principali di hardware di schede video, nVidia e AMD. La più grande differenza che intercorre tra loro è l'architettura su cui si compongono.
NVidia è basata su CUDA core e AMD su Stream Processors. Nelle prossime due sezioni si parlerà anche di questo.
L'approccio che va intrapreso su di esse è molto diverso. Le schede nVidia, specialmente nelle ultime serie rilasciate, hanno una tipologia di overclock e undervolt che agisce su settori molto differenti da AMD. A primo impatto le schede video nVidia parrebbero più ottimizzate di fabbrica di AMD, ma non è necessariamente così. A breve si capirà il motivo.
L'ottimizzazione massima raggiunta per questo progetto di mining pool è stata ottenuta su sistema operativo basata su Linux, specialmente per la maggiore stabilità riscontrata.
Per quanto riguarda, invece, il sistema Windows, si sono riscontrati molti più problemi generali, dalla configurazione dei driver delle schede, alle modifiche software dei voltaggi interni delle schede, ad automatismi per l'autostart del software da mining.
Come nota positiva, c'è da dire che per nVidia si sono riusciti ad ottenere valori leggermente superiori dell'ordine del 3% rispetto Linux, ma a livello di consumo energetico la gestione migliore viene gestita da Linux.
La spiegazione data è stata che Linux non aveva ancora dei driver definitivi per nVidia.
Si passi ora alla parte pratica, con dati e valori più specifici riportati e alle configurazioni utilizzate per la realizzazione del progetto.

4.3.1 AMD

Ecco alcune analisi dei modelli di schede grafiche precedentemente riportate, ma descritti più nel dettaglio.
Ogni scheda AMD modello RX, serie 5xx o vega-xx può essere resa molto più efficiente da come esce originariamente da fabbrica.
Innanzitutto è importante sapere che ogni scheda video, anche se apparentemente uguale come modello e sigla, possiede chip differenti.
I principali chip sulle memorie video usati sono: Samsung, Hynix, Elpida e Micron. Quelli preferiti rimangono in ordine Hynix, Samsung e Micron.
A questo punto vediamo come rendere efficienti tali risorse per l'algoritmo "chukwa" in uso da TurtleCoin.
Il risultato che si vuole ottenere è quello di trovare il punto in cui la GPU renda meglio, in termini di computazione, al minor consumo elettrico assorbito possibile.
Per rendere ciò possibile, si utilizzano tool o sistemi operativi che integrano questi software al loro interno.
Il test effettuato è stato fatto sia per Windows che per Linux su una distribuzione specifica nata proprio per il settore del mining, denominata "HiveOS".
La prima operazione effettuata è stata quella di abbassare la frequenza del core il più possibile, perchè è una delle cause principali di consumo eccessivo.
Questa è una fase molto delicata e potrebbe non essere facile per chi si scontra per la prima volta con questo mondo, basta però prestare attenzione ai valori consigliati e inserire quel range di valori per evitare eventuali rotture o danneggiamenti dei chip o delle memorie video.
Esistono alcuni semplici trucchi sfruttabili per arrivare alla soluzione ottimale in breve tempo. Si vedrà quello più semplice e intuitivo.
La regola fondamentale è non avere mai fretta di raggiungere immediatamente valori estremi; si devono eseguire pochi passi per volta se non si vuole causare un crash della scheda con seguente freeze del sistema operativo.
In tal caso sarà necessario riavviare il sistema forzatamente.
Dopo ogni cambiamento si deve testare semplicemente la modifica; questo

si può fare attraverso un qualsiasi software da mining e iniziare la computazione per la convalida di blocchi. A questo punto si effettua una verifica di quante operazioni hash vengano elaborate dal dispositivo, ma soprattutto si deve controllare che le schede abbiano un funzionamento stabile.
Anche la temperatura dovrà essere un buon segnale di verifica: una temperatura bassa indica sicuramente un buon punto di partenza e l'hardware sarà soggetto a minori rischi di rotture.
Potrebbe accadere che dopo ore di funzionamento si inizi a osservare un calo di prestazioni; questo può essere dovuto alla frequenza non ottimale della memoria.
Ci sono due valutazioni da compiere, la prima è quella di controllare se il software da mining ha rilevato degli errori, in tal caso bisognerà abbassare la frequenza della memoria video; la seconda è che invece potrebbe esserci una frequenza legata al core troppo bassa e quindi bisognerà andare ad aumentare di uno step.
Gli step per l'ottimizzazione per la memoria video sono stati effettuati di 25MHz alla volta, mentre per quanto riguarda la frequenza del core, si possono eseguire step con frequenze minori a scelta dell'utente.
A questo punto è essenziale trovare con quale tensione riesce a funzionare ogni GPU. Questa operazione si chiama operazione di "undervolt" ed è diversa per ogni tipo di scheda.
Per ottenere risultati migliori bisogna modificare ogni stato della scheda e il relativo voltaggio, HiveOS però, aiuta questa parte di processo con una funziona chiamata "Aggressive Undervolt" che permette di abbassare forzatamente il voltaggio dei vari stati.
Da notare che con il sistema Windows sarebbe stata necessaria una modifica manuale, pertanto dato che con HiveOS era immediato, è stato optato per questa rapida scelta, automatica e ottimale.
Per quanto riguarda la velocità di elaborazione, invece, l'overclock della frequenza del core e della memoria è la parte più importante per aumentare le prestazioni.

L'overclock della memoria non aumenta il consumo finale significatamente, mentre aumentare il core significa aumentare la potenza finale esponenzialmente.
I risultati ottenuti dalle schede AMD sopracitate, sono stati:

AMD RX-570 Dati delle tensioni e frequenze:
Range di tensione di funzionamento: 850mV - 900mV.
Range di frequenze di funzionamento del core: 1000MHz - 1100MHz.
Range di frequenze di funzionamento della memoria: 1850MHz 2050MHz.
Consumo energetico stock: circa 300w
Consumo energetico ottimizzato: circa 80w

AMD RX-580 Dati delle tensioni e frequenze:
Range di tensione di funzionamento: 875mV - 910mV.
Range di frequenze di funzionamento del core: 1000MHz - 1100MHz.
Range di frequenze di funzionamento della memoria: 2050MHz - 2250MHz
Consumo energetico stock: circa 300w
Consumo energetico ottimizzato: circa 80w

AMD RX-Vega56 Dati delle tensioni e frequenze:
Range di tensione di funzionamento: 875mV - 900mV.
Range di frequenze di funzionamento del core: 1200MHz - 1300MHz.
Range di frequenze di funzionamento della memoria: 940MHz - 9550MHz.
Consumo energetico stock: circa 300w
Consumo energetico ottimizzato: circa 123w

Si noti che, anche in questo caso, gli step sono stati effettuati di 25mV alla volta fino a raggiungere valori finali più specifici di 10mV.
E' stato un ottimo successo, il consumo raggiunto è davvero minimale. Di conseguenza temperature e rilascio di CO2 sono anch'essi inferiori a quando il funzionamento era stock. Se ogni miner riuscisse ad apportare queste piccole modifiche, si potrebbe ottenere un ottimo risultato globale.
Per riassumere, il risultato delle prestazioni finale è stato:

AMD RX-570 Performance computazionale unitaria:

Stock: 40 KHs

Overclock: 60 KHs

AMD RX-580 Performance computazionale unitaria:

Stock: 40 KHs

Overclock: 64 KHs

AMD RX-Vega56 Performance computazionale unitaria:

Stock: 65 KHs

Overclock: 103 KHs

Si è ottenuta una riduzione netta di più del 70% del consumo elettrico originale da fabbrica e una potenza computazionale tra il 40% e il 55%.
Un ulteriore aggiornamento in queste schede è stato quello di ottimizzare i timing delle memorie VRAM attraverso la modifica del BIOS di default.
I valori di timing determinano la prestazione della scheda nei vari algoritmi per il mining, ma non solo; con un altro tool chiamato "AMDTweak", sono stati modificati ulteriormente altri parametri per ridurre i tempi di risposta delle RAM.
Ecco le statistiche precedentemente descritte, da uno screenshot di HiveOS GUI:

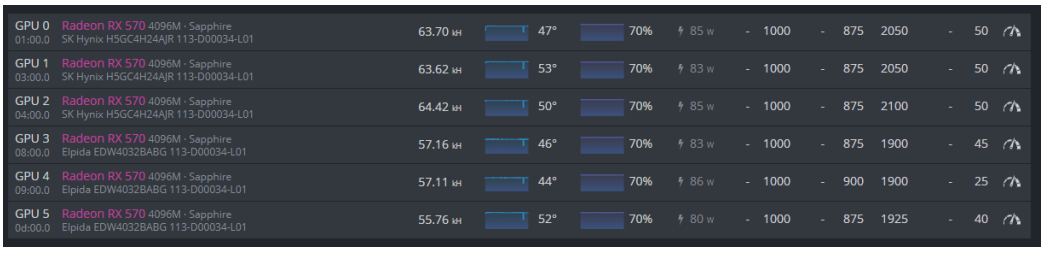


Figura 4.1: Ottimizzazione hardware AMD RX-570.

Per la serie RX-Vega56 il procedimento è simile ma non lo stesso, siccome utilizzano memorie RAM di tipo HMB2(memorie veloci per evitare colli di bottiglia di banda) invece che GDDR5. Per questo tipo di scheda non è

possibile e non è conveniente modificare il BIOS di default, è necessario solamente aumentare la frequenza della memoria e diminuire quella del core. Si può inoltre impostare un limite di potenza che aiuta a evitare sbalzi di corrente. Anche in queste schede sono stati leggermente modificati i timing della memoria da interfaccia HiveOS. Ecco i valori attuali:

Figura 4.2: Ottimizzazione hardware AMD RX-Vega 56.

L'utilizzo di AMD è rivolto principalmente ad un gruppo di persone esperte. Sono schede hardware economiche, alla portata di tutti e qualitativamente parlando sono molto solide.

4.3.2 NVidia

Come per AMD, anche le schede nVidia usate, hanno ricevuto ottimizzazioni, non solo da fabbrica, ma anche manualmente. Il modello utilizzato è nVidia RTX-2080. Il procedimento è simile per quasi tutte le nVidia: non è sufficiente modificare direttamente i voltaggi, ma è sufficiente modificare la frequenza del core e del "power limit", riducendo la potenza massima assorbita da ogni scheda.
I risultati ottenuti dalle schede nVidia sopracitate, sono stati:

NVidia Dati del power limit e frequenze:
Range del power limit di funzionamento: 110% - 125%.
Frequenza di funzionamento del core: -134 MHz.
Frequenza di funzionamento della memoria: 700MHz.
Range del consumo energetico stock: 235w - 250w
Range del consumo energetico ottimizzato: 110w - 125w

Il principio con cui sono stati trovati questi valori è lo stesso che è stato utilizzato per AMD; anche in questo casi gli step sono stati effettuati con step di 25mV alla volta fino a raggiungere valori finali più specifici di 10mV alla volta.
Per riassumere, il risultato delle prestazioni finale è stato:

NVidia RTX-2080 Performance computazionale unitaria:
Stock: 80 KHs
Overclock: 120 KHs

Anche con il modello RTX-2080 c'è stato un risparmio del 60% sull'energia consumata. Stesso discorso valido per le prestazioni raggiunte: si stima all'incirca un 50% in più rispetto a quelle appena uscite da fabbrica.
C'è da sottolineare che nVidia si trova presente nel mercato già più ottimizzata di AMD. Il bios di nVidia però non permette modifiche alle tensioni interne, ma si modifica solo il power limit.
Un grosso vantaggio nell'utilizzare nVidia è la stabilità. Rispetto AMD si

potranno avere molti meno crash non andando mai ad agire sui voltaggi interni. Ecco i valori sopra descritti:

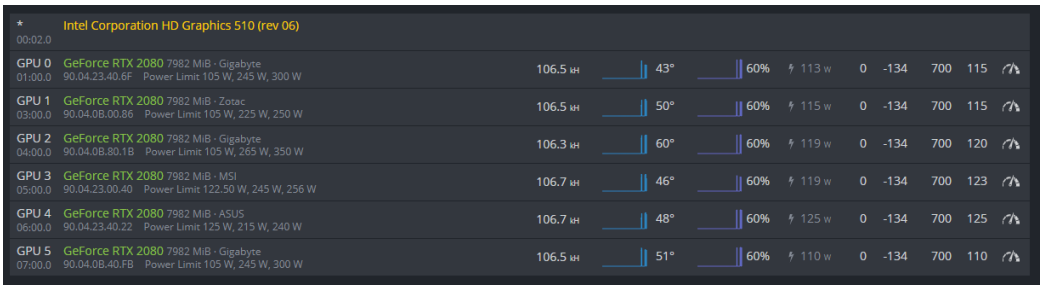


Figura 4.3: Ottimizzazione hardware nVidia RTX-2080.

L'utilizzo di nVidia è fortemente consigliato per persone neofite. Sono schede molto resistenti come per AMD. E' raro che si verifichi qualche malfunzionamento dopo aver trovato una configurazione stabile. La temperatura rimane bassa in quanto sono modelli a 3 ventole.

4.4 Server e gestore dei servizi

Arrivati a questo punto, si passa a descrivere il server che si occupa della gestione dei servizi.
Innanzitutto, il server è stato preparato e gira su piattaforma AMD, con scheda madre che monta il socket AM4 e chipset AMD a320.
La scelta del processore è ricaduta su un Ryzen 7 2700x, una CPU multicore da 8 processori e 16 thread, per favorirne il parallelismo dei processi evitando rallentamenti del sistema.
La memoria RAM utilizzata è DDR4 e ne monta 16GB. La frequenza è lasciata stock a 2400MHz.
Per finire si usa SSD m2 NVMe ad alta efficienza da 500gb, con velocità dichiarate di R/W a 3400/3000MB/s.
La blockchain occupa all'incirca 120gb, per questo motivo la scelta è ricaduta su questa dimensione.
Ecco ora i servizi in esecuzione per il funzionamento della mining pool, avviati all'accensione del server:

Redis Database Database per la registrazione dei vari tipi dati della pool, come miner, blocchi trovati, pagamenti effettuati e da effettuare, varie statistiche sul profitto generato dalla pool e una zona amministratori dove moderare il sito; tutto sincronizzato con il demone di TurtleCoin.

TurtleCoind Non è altro che il demone già visto più volte che permetterà di sincronizzare la rete e di trovare nuovi blocchi. Viene utilizzato anche per il conteggio di cryptomonete accumulate nei vari wallet. Da pochi giorni è stato aggiornato il servizio allineandosi all'aggiornamento rilasciato dalla rete.

Turtle-service Servizio RPC-JSON attraverso l'utilizzo di API per il pagamento automatico per i miner e per il ricevimento delle ricompense dei blocchi. E' il servizio che remunererà ogni miner che ha partecipato alla convalida di ogni blocco.

Avvio Node Pool Avvio della pool attivando le API per i servizi esterni, rimanendo in ascolto sulle porte 5555 dedicate ad un hardware di piccole-medie potenze, come un pc con una buona GPU. La porta 7777, invece, è indicata per hardware assemblati ad hoc multi-schede. La differenza tra le due porte sta nell'avviare i miner con una difficulty più o meno alta in partenza. Se si dovesse tentare di avviare macchine potenti sulla porta 5555, è molto probabile incorrere nel rischio di essere bannati dalla pool per qualche minuto.

Ora che sono stati elencati i principali componenti della mining pool, si può passare a consultare anche l'applicativo web collegato con le API del server e in costante aggiornamento.
Qui è possibile trovare i vari dati relativi alla pool e alle statistiche relative al proprio hardware. Non solo, sono presenti tutte le statistiche globali della rete, è possibile stimare quanto si può produrre con il proprio hardware, è possibile vedere i blocchi convalidati dalla pool e anche controllare i pagamenti in sospeso e quelli già pagati.
Tutte queste informazioni vengono gestite e salvate nel database Redis.

4.5 Piattaforma di test

La fase "zero" del progetto è stata la realizzazione della mining pool su una macchina virtuale in VMware. L'emulazione di VMware è stata supportata da un MacBook Pro abbastanza recente, composto da una CPU intel i7 di settima generazione e quindi di 4 core e 4 thread disponibili.
Il sistema operativo utilizzato è Ubuntu 18.04.3 LTS e le risorse allocate sono: 6 core, 8GB RAM e 150GB di disco.
Per quanto riguarda la dimensione del disco è stata estesa più volte perchè la sincronizzazione della blockchain ha richiesto molto spazio.
Il requisito minimo di RAM invece è di 4GB; infatti al di sotto si sarebbero rischiati rallentamenti e crash durante la sincronizzazione con il demone.
Le principali problematiche riscontrate sono state testate e risolte su questa macchina. Esse hanno riguardato la configurazione della mining pool e della cryptovaluta TurtleCoin che da poco tempo ha eseguito un fork del progetto e subito si è dovuto riallineare la nuova rete con il nuovo algoritmo Chukwa.
Ogni modifica rilevante è stata salvata in uno snapshot, funzionalità di VMware, e sono stati effettuati periodicamente backup su hard disk esterni. In questa fase di test, le principali operazioni effettuate sono state:

- Test delle performance necessarie per mantenere attiva la mining pool. In questa fase è stata verificata la quantità di risorse utilizzate attraverso le statistiche di Ubuntu. Con il comando "top" si possono monitorare i processi attivi e si può mostrare sia la CPU che la RAM in uso. Un altro comando utilizzato è stato "stat" per osservare ulteriori informazioni di sistema e file.

- Test di pool mining: sono stati invitati alcuni nodi a partecipare alla rete. Sono stati invitati dei miner aventi dell'hardware che soddisfacessero i requisiti minimi per partecipare alla rete. Nessun rallentamento e nessun aumento di latenza[1] si sono registrati.

- Creazione del servizio DNS[2] che rimanda all'IP pubblico del router utilizzato. In seguito sono state aperte le porte necessarie per utilizzare i

vari servizi ed è stato fatto il port mapping all'IP e porte del server della pool. Si è dovuto inoltre sfruttare la tecnologia DMZ, per reindirizzare tutte le connessioni al server.

- Test servizi delle API dal web server alla pool, con qualche modifica per aumentare il numero di feature predefinite.

[1]La latenza (o in inglese ping) indica in un sistema di elaborazione dati e/o di telecomunicazioni, l'intervallo di tempo che intercorre fra il momento in cui viene inviato l'input/segnale al sistema e il momento in cui è disponibile il suo output. In altre parole, la latenza non è altro che una misura della velocità di risposta di un sistema.

[2]Fonte Wikipedia: Il DNS(Domain Name System) è un sistema utilizzato per assegnare nomi ai nodi della rete (in inglese: host). Questi nomi sono utilizzabili mediante una traduzione, di solito chiamata risoluzione, al posto degli indirizzi IP originali. Il servizio è realizzato tramite un database distribuito, costituito dai server DNS. Ad ogni dominio o nodo corrisponde un nameserver, che conserva un database con le informazioni di alcuni domini di cui è responsabile e si rivolge ai nodi successivi quando deve trovare informazioni che appartengono ad altri domini.

4.6 Configurazione della rete

In questa sezione si spiega il funzionamento della rete locale e come comunica con la blockchain di TurtleCoin.
La prima operazione è stata quella di verificare il tipo di connessione su banda larga in uso con le relative configurazioni nel pannello del router.
E' necessario che la rete funzioni correttamente, in modo da garantire la stabilità del servizio e una minor latenza possibile; questo perchè è assolutamente consigliato arrivare e computare e convalidare per primi i blocchi.

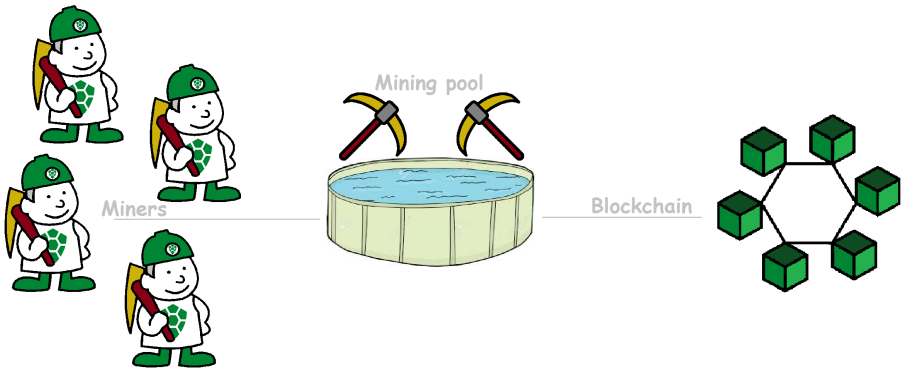


Figura 4.4: Come funziona la rete.

Si supponga, ad esempio, che due nodi arrivino sullo stesso blocco nello stesso momento: il primo nodo che lo riesce a computare e risolvere vuole comunicare l'esito alla blockchain. Dal momento che i blocchi non sono di grandezze paragonabili a quelli di altre blockchain, ma come si è visto TurtleCoin predilige la velocità, per completare un blocco ci vogliono pochi secondi o minuti con grandi quantità di potenza di calcolo.
A questo punto si supponga di avere anche il secondo nodo che dopo poco tempo rispetto al primo nodo, abbia la soluzione del blocco pronta; è importante che il primo nodo abbia una buona latenza perchè, qualora il secondo blocco riuscisse a convalidarlo per primo, otterrebbe lui la ricompensa. Cosa appare al nodo nel momento della risposta da parte della blockchain?

Appare semplicemente che il nodo esiste già e viene abbandonato, perdendo la computazione degli hash fatta sino quel momento.
Una buona mining pool potrebbe anche collegarsi alla rete wireless, ma è altamente sconsigliato per quanto appena detto.
La soluzione scelta, infatti, è stata di realizzare un collegamento LAN diretto dal router, senza passare da alcuno switch.
Dopo qualche test per il controllo della rete al fine di ottenere la migliore performance, è stato deciso di utilizzare un IP statico con priorità alta (impostazione del router in uso), come host del sistema.

4.7 Milestone

Le milestone del progetto sono state di varia natura.
La scelta è ricaduta su un percorso composto da tanti piccoli passi che hanno coinciso con modifiche software e hardware. Software, nel senso di programmazione di nuove funzionalità o aumento delle risorse del sistema in uso. Hardware perchè dopo la fase di test sono stati selezionati i componenti migliori per la gestione del sistema.
Ecco quindi una lista di milestone raggiunte:

Installazione e configurazione VMware In questa fase, l'obiettivo era semplicemente installare la Virtual Machine e configurarla con il sistema operativo.

Installazione sistema e configurazione delle risorse Installazione del sistema Ubuntu 18.04.3 LTS. Inizialmente le risorse allocate non erano sufficienti per il completamento della mining pool. Sono state riviste più volte. La blockchain completa infatti occupa su disco parecchio spazio, nell'ordine di gigabyte.

Installazione dei requisiti di base Installazione di tutti i componenti software e delle varie librerie per l'esecuzione della mining pool.

Configurazione pool In questa fase molto delicata e difficile sono stati inizializzati tutti i componenti e le configurazioni di base per il supporto di TurtleCoin. E' stato difficile perchè da poco TurtleCoin ha effettuato un fork del progetto cambiando algoritmo per i miner, così la difficoltà principale è stata aggiornare tutto perchè fosse compatibile con il resto delle funzioni della pool. Inoltre anche i servizi legati al wallet e al daemon sono stati aggiornati.

Configurazione servizio "turtle-service" "Turtle-service" viene usato per il pagamento automatico tramite RPC-JSON ai miner delle rispettive ricompense per la convalida dei vari blocchi. Il servizio turtle-service

attualmente è stato deprecato per incentivare l'utilizzo dei wallet non legacy, per aumentare la sicurezza. Con la versione attuale della pool però era obbligatorio ancora l'utilizzo di queste API più vecchie.

Creazione della build che ospita il server Sono stati selezionati alcuni componenti hardware per la creazione di una macchina ad hoc per questo servizio di mining pool.

Trasferimento sul nuovo server e configurazione ex-novo Sono state trasferite tutte le informazioni della pool su nuovo server con installazione pulita per evitare bug o eventuali attacchi dall'esterno. Le opzioni preliminari che riguardano la configurazione base del sistema sono state effettuate ex-novo.

Acquisto dominio web e upload website In questa fase del progetto la concentrazione è ricaduta su quale dominio web scegliere per ospitare il servizio web collegato alla pool. E' stato selezionato un piano che supporti fino 800 mila visite al giorno. In seguito è stato effettuato l'upload del sito con le nuove funzionalità e configurazioni aggiornate.

4.8 Obiettivi futuri, idee e innovazioni

Per quanto riguarda le implementazioni future del progetto si prospettano varie idee.
Innanzitutto, si vogliono estendere le funzionalità del sito web e aumentare la sicurezza generale del server. Subito dopo, si cercherà un host online che mantenga il server acceso 24h su 24 per garantirne al meglio l'affidabilità.
A questo punto i servizi sono attivi e le risorse a disposizione sono tante, pertanto il passo successivo sarà creare una nuova pool e cercare di mantenere alta la decentralizzazione delle cryptovalute.
La scelta su qualche cryptovaluta spingere e scegliere, si baserà sul progetto che non sia per sola speculazione basata sui profitti dei miner, ma per innovazione tecnologica.
Tutti questi progetti che saranno avviati saranno incentrati sull'ecosostenibilità e salvaguardia dell'ambiente.
I profitti generati da tali servizi verranno in parte reinvestiti per progetti puramente "green".

Capitolo 5

Funzionamento visuale e user experience

Per "esperienza d'uso" (più nota come User Experience o UX) s'intende ciò che una persona prova quando utilizza un prodotto, un sistema o un servizio.
Il termine User Experience si è diffuso negli ultimi anni in contesti e ambiti disciplinari molti diversi; si intende il concetto di usabilità e di studio dell'esperienza di interazione con le interfacce mediali che appaiono all'utente.
La UX non deve essere confusa con la user interface (UI) di cui è solo una delle componenti, nel nostro caso il website con le statistiche rivolto ai miner.
Questo capitolo è la parte finale del progetto per presentare il reale funzionamento della mining pool.
Si descriveranno le varie sezioni del sito web e delle statistiche di cui è composto; sarà possibile vedere quali macchine, o mining rig, saranno collegate realmente al sistema TurtleCoin tramite la mining pool; per finire si potrà osservare il server realizzato e i componenti in uso.

5.1 Webserver

Il webserver gira su tecnologia “NodeJS”, attualmente è stato ospitato su un server con larghezza di banda elevata e traffico delle visite che risale a un massimo di 800.000 visite giornaliere. Si è optato per un servizio prestazionale per evitare rallentamenti dei servizi API e delle statistiche riportate dal sito.

A prima vista appare la homepage del sito:

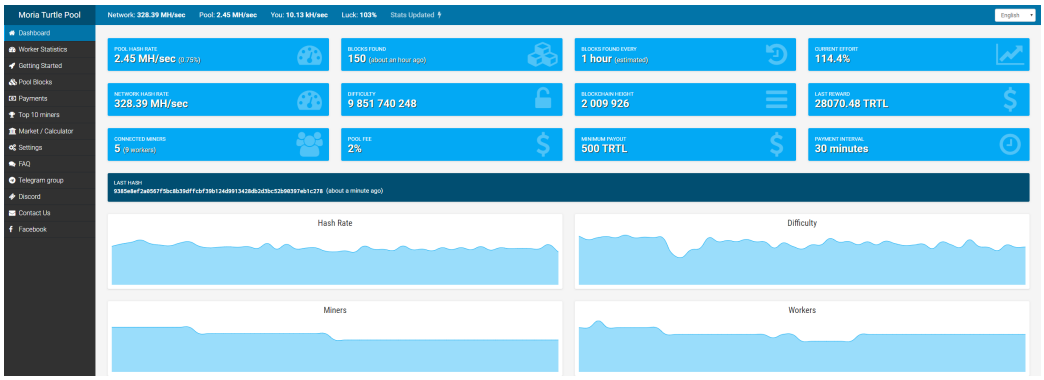


Figura 5.1: Homepage del progetto.

In figura 5.3 sono spiegate tutte le voci e le loro relative funzioni e statistiche. La Homepage è molto importante anche per poter visionare il confronto tra la mining pool realizzata in questo progetto con il network globale.

Con l’aumento di hardware dedicato per la mining pool, crescerà sia il network globale che l’hashrate della pool.

Questi valori sono fondamentali perchè entro fine anno 2019 si avrà un grosso incremento del network di questa pool in quanto sono stati stipulati vari contratti con altri miner, per il 2020.

Nella successiva pagina sarà spiegata la pagina personale relativa ad ogni miner con le relative statistiche del loro hardware in uso.

Come appare la schermata per il miner connesso, dopo aver immesso nella textbox in cima alla pagina, il suo wallet personale.
Come si può vedere ci sono tutti i pagamenti effettuati fino a quel momento, le varie stime per quanto lavoro ha svolto e quanto è stato pagato dalla pool. Nella parte destra si vedono due grafici, il primo è composto dall'andamento del suo hashrate, mentre il secondo dall'ammontare pagato per diversi periodi di tempo, dalla pool.

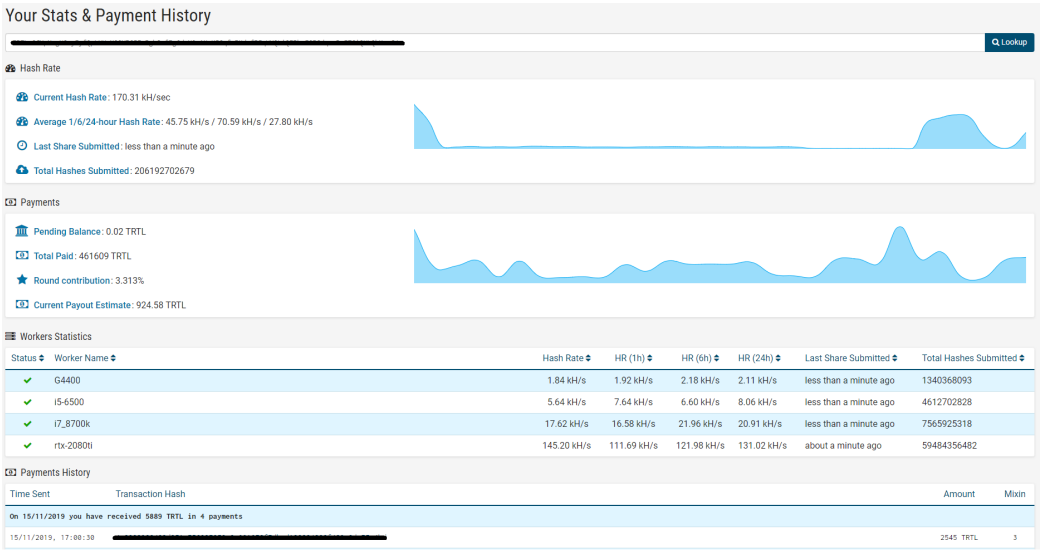
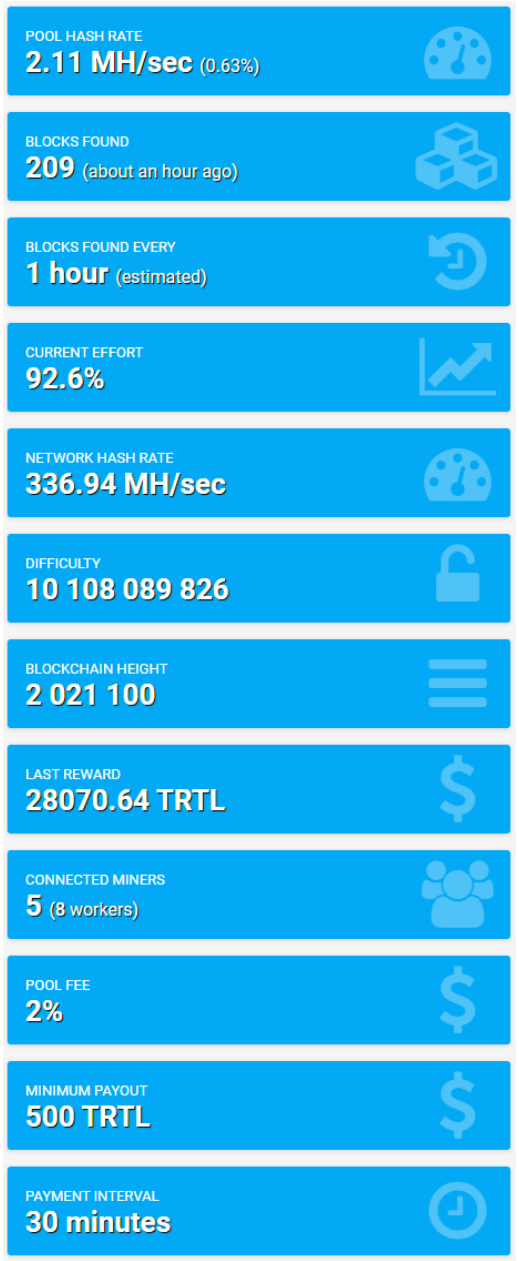


Figura 5.2: Foto esempio delle statistiche relative a un miner.

Come si accennava nella parte di Homepage del sito, saranno spiegate le varie funzionalità e statistiche che formano il Web Server.



POOL HASH RATE
Hashrate attuale della mining pool. Alla destra l'attuale dimensione della pool nella rete globale.

BLOCKS FOUND
Blocchi che la mining pool è riuscita a trovare con l'ausilio del lavoro dei miner.

BLOCKS FOUND EVERY
E' una stima della frequenza dei blocchi trovati. Tanto più è alto l'hasharate della pool, tanto più è facile convalidare e quindi trovare blocchi.

CURRENT EFFORT
Sforzo corrente per la convalida del blocco. Un valore attorno al 100% è il miglior rapporto tra miner connessi e difficoltà del blocco corrente.

NETWORK HASH RATE
Hashrate globale della blockchain di TurtleCoin.

DIFFICULTY
Difficoltà corrente. E' un valore che misura la complessità di un calcolo di una funzione hash. La difficulty è direttamente proporzionale all'hashrate globale dei miner connessi.

BLOCKCHAIN HEIGHT
Altezza del blocco attuale della blockchain convalidato.

LAST REWARD
Ultima ricompensa assegnata alla pool.

CONNECTED MINERS
Numero di miner connessi alla pool e numero di worker posseduti dai miner.

POOL FEE
Percentuale di tasse che trattiene la pool per il lavoro svolto.

MINIMUM PAYOUT
Il pagamento del lavoro svolto viene effettuato una volta superata la soglia dei 500 Turtle.

PAYMENT INTERVAL
Il pagamento viene effettuato ogni 30 minuti se e solo se il miner in questione ha raggiunto il payout minimo.

Figura 5.3: Statistiche dashboard.

In figura 5.4 è possibile studiare e capire come il menù del Web Server sia formato.
Le voci di menù relative al gruppo di Telegram, Discord e Facebook, sono in fase di sviluppo, ma comunque funzionanti.
Esse hanno la funzione di permettere la comunicazione e le varie segnalazioni con il proprietario e gestore della pool.
Inoltre, c'è una community attiva per il confronto diretto per informazioni e/o chiarimenti generali.
Nella sezione FAQ è già possibile trovare qualche soluzione a qualche problematica, per l'aiuto diretto al miner.

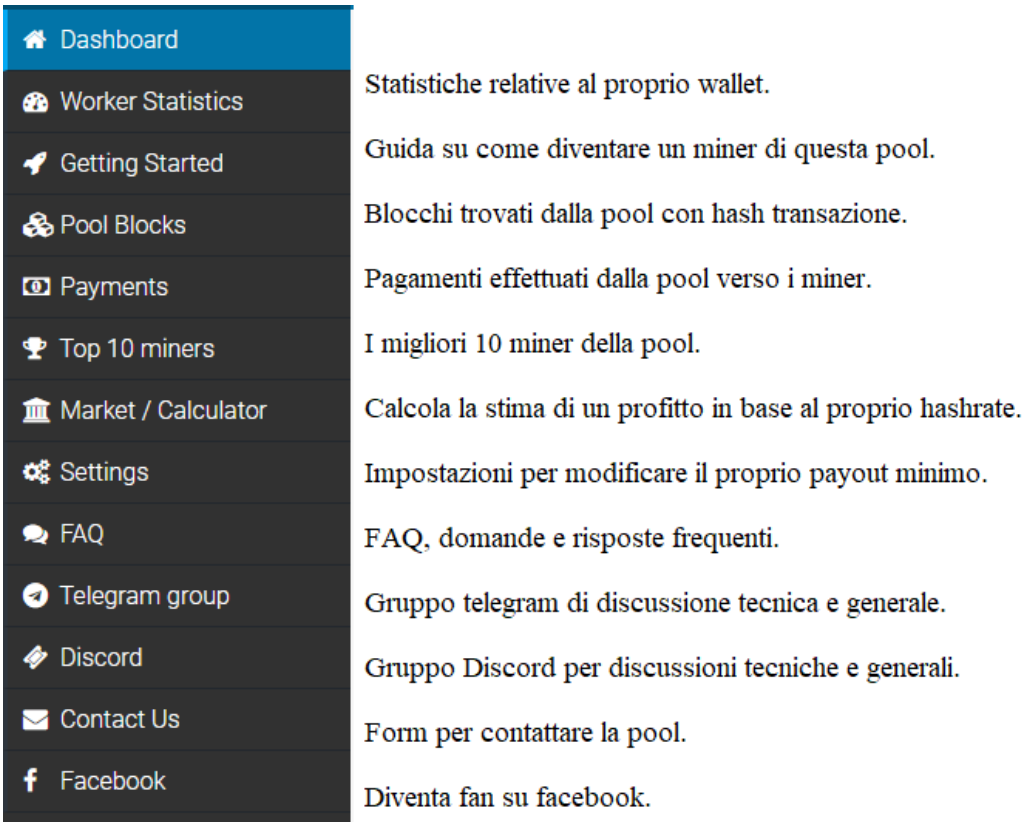


Figura 5.4: Menu del sito.

5.2 Sistema Ubuntu 18.04.3

Questi sono i 4 servizi precedentemente descritti, in esecuzione sul server, di cui Redis in background non visibile:

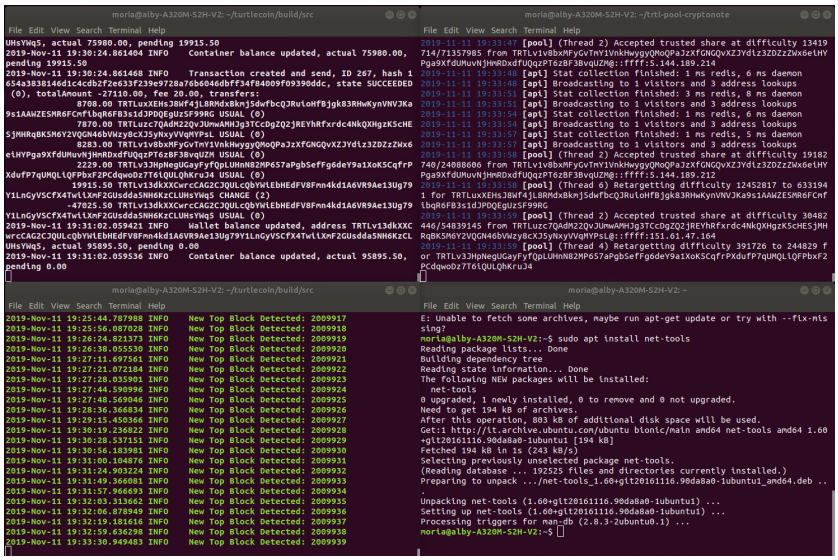


Figura 5.5: Servizi in esecuzione nel server.

Il primo nel riquadro in alto a sinistra utilizza il servizio “turtle-service”. Esso ci permette di effettuare i pagamenti in automatico ai miner.
Le richieste di transazione sono effettuati dal servizio nodeJS che gestisce tutti questi servizi.
Tutte queste operazioni sono visibili concretamente sulla pagina web collegata tramite API al server.
Nel secondo riquadro in alto a destra si avvia il servizio principale.
Questo processo utilizzerà un servizio tramite API di pagamento dei miner (riquadro in alto a sinistra già descritto), registrerà informazioni con il database Redis e si sincronizzerà alla rete tramite il demone di TurtleCoin visibile nel riquadro in basso a sinistra.
L’ultimo riquadro in basso a destra viene utilizzato per controllare aggiornamenti della rete o per aggiornamenti riguardanti la stabilità del sistema Linux.

5.3 Qualche foto del progetto

Questo è il progetto concreto del server per la mining pool realizzata. Come illustrato nella foto 5.6, il server viene alimentato dal suo gruppo di continuità, non si deve spegnere per nessuna ragione.
Il gruppo di continuità alimenta sia il server che il router. Il collegamento tra router e server è diretto per evitare switch ethernet e/o possibili dispositivi intermedi di rete, che potrebbero condizionarne il funzionamento.
Nella foto è visibile anche la scheda grafica che era ancora utilizzata durante la prima fase di test, per mostrare il sistema a video.
Attualmente la GPU è stata rimossa perchè ora la gestione è gestita da remoto.

Figura 5.6: Server e gestore dei servizi, primo piano.

Questo è la stessa foto di quella sopra, solo che la vista è dall'alto.
Da qui è possibile osservare meglio i componenti assemblati, il disco SSD m2, il dissipatore, la ram e l'alimentatore.
Prossimamente sarà coperto da un pannello di plexyglass trasparente, in modo tale che la polvere non rovini l'hardware.

Figura 5.7: Server e gestore dei servizi, primo piano dall'alto.

5.4 Mining rig

Un mining rig non è altro che un PC assemblato che monta i classici componenti di un personal computer, ossia una scheda madre che supporti l'alloggiamento di più schede grafiche, della RAM, uno o più processori, un alimentatore e delle schede video sufficientemente potenti per poter effettuare il mining considerando i consumi di corrente.
Le strutture, o frame, sono degli "open case"; questo serve per permettere ai vari dispositivi video di non surriscaldarsi, mantenendo controllata la temperatura. Questo fa sì che si possa allungare la durata di vita dei componenti. Generalmente queste strutture vengono tenute in luoghi freschi o climatizzati per garantirne il costante funzionamento.
I mining rig possono essere composti anche da dei dispositivi "watchdog", ovvero dei dispositivi "cane da guardia", che possono essere di tipo software o hardware.
La loro principale funzione è quella di resettare il sistema dopo che incorre un crash o malfunzionamento generale di qualche dispositivo.
I watchdog software e hardware compiono la stessa operazione di riavvio.
Nel caso in cui il sistema vada in stato di "freeze", il watchdog software entrerà in "congelamento" come tutto il sistema, smettendo di funzionare; quello hardware, invece, se il sistema dovesse smettere di rispondere, come in caso di "freeze", effettuerà un riavvio forzato hardware della macchina.
Tipicamente, essi sono oggetti che utilizzano il protocollo USB per comunicare con la scheda madre.

5.4.1 AMD

La foto mostra un mining rig che dispone di otto schede video rx-580 da 8gb e una r9-290x. La scheda video r9-290x è stata inserita per aumentare la base computazionale, ma non è stata considerata nel progetto perchè probabilmente sarà solo una scheda provvisoria.
Il consumo della macchina totale è di 700w. Essa è stata realizzata per aumentare il livello di stabilizzazione della mining pool e permettere quella potenza minima che consenta di trovare sempre nuovi blocchi nella rete.

Figura 5.8: Mining rig - AMD rx-580.

5.4.2 nVidia

Per terminare il discorso dei mining rig, si inserisce l'immagine di un altro componente della mining pool per supportare l'intero progetto.
Tale macchina è composta da sei schede video nVidia rtx-2080, con una considerevole forza nel calcolo di questo algoritmo.
Il consumo totale è pari a circa 700w.

Figura 5.9: Mining rig - nVidia rtx-2080.

Conclusioni

La progettazione di questa mining pool per TurtleCoin è stata un progetto molto gratificante che mi ha fatto acquisire davvero tantissime skills riuscendo a migliorare le conoscenze acquisite dal corso di studio.
Da ormai 4 anni lavoro nel settore delle cryptovalute. Sono sempre più affascinato da questa nuova tecnologia emersa da pochi anni, in continua evoluzione.
Attualmente, possiedo varie macchine per il sostegno e lo sviluppo della cryptovaluta TurtleCoin come developer della community.
La motivazione è tanta e anche la voglia di credere in questo progetto.
Sono convinto che una cryptocurrency che riesca a nascere dal nulla nel momento peggiore del mercato delle cryptovalute e che continui a crescere nonostante l'andamento volatile con tutti i trend ribassisti, abbia in background una base solida di sviluppatori che a loro volta credono nel progetto e nella comunità.
La mia opinione è che non passerà molto tempo prima che il network cresca ancora. I miner sono ancora orientati su cryptovalute con capitalizzazione di mercato più alto, nell'ordine di milioni di dollari, credendo che sia la scelta migliore e più conveniente.
Per non parlare della Cina che, addirittura, ignora tutte le cryptovalute che non siano Bitcoin.
Nei prossimi mesi a venire, bisognerà cercare di portare TurtleCoin a un livello successivo, il suo valore monetario è ancora molto basso.
Per questa ragione e per le sue prospettive date dalla sua potenza, trovo che

sia molto conveniente investire una piccola quota nel progetto Turtlecoin.
Per chiunque voglia visionare le statistiche della mining pool realizzata, è possibile visitare il seguente link: http://moriapool.eu/.
Il progetto è in funzione e presto verrà potenziato ulteriormente.
Il progetto di Moriapool, nasce con lo scopo di diventare un gruppo di mining pool, per tutte quelle nuove cryptovalute emergenti e con grande potenziale e profittabilità per i miner.
Gli obiettivi a breve termine saranno quelli di integrare pagamenti online con servizio TurtlePay e portare la mining pool al primo posto in Italia. Entro la fine del 2019 l'obiettivo sarà anche raggiungere il quarto posto, per potenza, in Europa.

Bibliografia

[1] Chris Dannen, Introducing Ethereum and Solidity - Foundations of Cryptocurrency and Blockchain Programming for Beginners, Apress.

[2] Narayanan, Bonneau, Felten, Miller and Goldfeder, Bitcoin and cryptocurrency technologies, Princeton.

[3] Arshdeep Bahga, Vijay Madisetti, Blockchain Applications - A Hands-On Approach.

[4] Sitografia: The Cryptonomist, Bitcoin network, https://cryptonomist.ch/

[5] Sitografia: The Cryptonomist, Mining pool, https://cryptonomist.ch/2019/06/30/come-funziona-mining-pool/

[6] Sitografia: Bioterra, Un'analisi sul grande consumo di energia di Bitcoin, https://www.bioterra.it/analisi-consumo-energia-mining-di-bitcoin/

[7] Sitografia: Cointelegraph, Bitcoin: l'halving, https://it.cointelegraph.com/news/bitcoin-most-dramatic-2020-halving-could-cut-supply-by-63m-a-week

[8] Sitografia: TurtleCoin, Storia e obiettivi di TurtleCoin, https://turtlecoin.lol/

[9] Sitografia: Monero, Storia e caratteristiche di Monero, https://www.getmonero.org/

[10] Sitografia: TurtleCoin Developers, Documentazione TurtleCoin, https://docs.turtlecoin.lol/

[11] Sitografia: Wikipedia, User Experience, https://it.wikipedia.org/wiki/UserExperience/

[12] Sitografia: Punto Energia Shop, Informazioni su pannelli solari e batterie, https://www.puntoenergiashop.it/

[13] Sitografia: Ubuntu, https://ubuntu.com/

[14] Sitografia: Redis, https://redis.io/

[15] Sitografia: VMware, https://www.vmware.com/it.html

[16] Sitografia: NodeJS, https://nodejs.org/it/

[17] Sitografia: NPM, https://www.npmjs.com/

[18] Sitografia: Package NVM, https://www.npmjs.com/package/nvm

[19] Sitografia: Wikipedia, Salt, https://it.wikipedia.org/wiki/Sale_(crittografia)

[20] Sitografia: Cryptounit, Argon2/Chukwa, https://www.cryptunit.com/algo/ArgChukwa