Relazione Corso Crittografica
La Blockchain

Alessio Bifulco
Matricola: 0000990143

31 luglio 2024

Indice

Capitolo 1

Introduzione

1.1 Definizione della Blockchain

La *blockchain* è una tecnologia di registro distribuito (Distributed Ledger Technology, DLT) che consente la registrazione sicura, trasparente e immutabile delle transazioni e dei dati. Il termine "blockchain" deriva dalla combinazione delle parole "block" e "chain", riflettendo la struttura della tecnologia stessa: una catena di blocchi contenenti dati.

Una caratteristica fondamentale della blockchain è la sua natura decentralizzata. Anziché essere gestita da un'unica entità centrale, la blockchain opera su una rete distribuita di nodi, ciascuno dei quali mantiene una copia del registro completo. Questa decentralizzazione riduce il rischio di singoli punti di guasto e aumenta la resistenza agli attacchi e alle manipolazioni.

La blockchain utilizza tecniche avanzate di crittografia per garantire la sicurezza dei dati. Le transazioni sono firmate digitalmente dagli utenti, utilizzando chiavi private che autenticano l'identità del mittente e impediscono alterazioni non autorizzate. Inoltre, le funzioni di hash crittografico vengono utilizzate per creare impronte digitali uniche di ogni blocco, rendendo praticamente impossibile modificare i dati senza alterare tutti i blocchi successivi nella catena.

In sintesi, la blockchain rappresenta un innovativo paradigma tecnologico che consente la creazione di registri digitali sicuri, trasparenti e resistenti alle manomissioni, aprendo la strada a una vasta gamma di applicazioni in settori come la finanza, la supply chain, la sanità e molti altri.

1.2 Storia della Blockchain e delle Criptovalute

La storia della blockchain e delle criptovalute inizia negli anni '90 con i primi tentativi di creare valute digitali sicure. Un pioniere in questo campo fu David Chaum, che sviluppò ecash, un sistema di pagamento elettronico anonimo.

Nel 2008, una persona o un gruppo sotto lo pseudonimo di Satoshi Nakamoto pubblicò il whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System". Questo documento descriveva un sistema di pagamento digitale basato su una rete peer-to-peer e introduceva il concetto di blockchain come soluzione al problema del double-spending, ovvero la possibilità di spendere la stessa unità monetaria più di una volta.

Nel gennaio 2009, Nakamoto lanciò la rete Bitcoin, minando il primo blocco, noto come "Genesis Block". Il codice sorgente di Bitcoin fu rilasciato come software open-source, permettendo a chiunque di partecipare al network e contribuire allo sviluppo del progetto.

Bitcoin guadagnò gradualmente popolarità, attirando l'attenzione di sviluppatori, investitori e appassionati di tecnologia. La sua architettura decentralizzata e l'uso della crittografia per garantire la sicurezza delle transazioni rappresentavano una rottura radicale con i tradizionali sistemi finanziari centralizzati.

Nel 2015, Vitalik Buterin lanciò Ethereum, una piattaforma blockchain che estendeva le capacità di Bitcoin permettendo l'esecuzione di "smart contracts", ovvero contratti intelligenti che eseguono automaticamente i termini di un accordo quando le condizioni prestabilite sono soddisfatte. Ethereum introdusse anche il concetto di token, che potevano rappresentare asset diversi dalla valuta, ampliando notevolmente le possibili applicazioni della tecnologia blockchain.

Negli anni successivi, numerosi altri progetti blockchain furono sviluppati, ciascuno con le proprie caratteristiche e casi d'uso. Tra questi si possono citare Ripple, Litecoin, Cardano e Binance Smart Chain. Questi progetti contribuirono a diversificare l'ecosistema delle criptovalute e a esplorare nuove applicazioni della blockchain in settori come la finanza, la gestione della supply chain e la sanità.

Oggi, la blockchain e le criptovalute sono oggetto di crescente interesse da parte delle istituzioni finanziarie, delle aziende e dei governi, che ne riconoscono il potenziale per trasformare vari aspetti dell'economia e della società.

Capitolo 2

Struttura della Blockchain

2.1 Come Funziona la Blockchain?

Il funzionamento della blockchain può essere compreso analizzando i seguenti elementi chiave:

2.1.1 Blocchi e Catene

La blockchain è composta da una serie di blocchi collegati in una sequenza lineare. Ogni blocco contiene un insieme di transazioni e altre informazioni rilevanti, come un timestamp e un *hash* del blocco precedente. L'hash è una funzione crittografica che crea una rappresentazione univoca dei dati nel blocco. Grazie all'hash, ogni blocco è collegato al precedente, formando una catena continua di blocchi.

2.1.2 Transazioni

Una transazione è una registrazione di un trasferimento di valore o di dati tra due o più parti. Le transazioni vengono create dagli utenti della rete e trasmesse ai nodi della blockchain. Ogni transazione deve essere firmata digitalmente dal mittente utilizzando una chiave privata, che garantisce l'autenticità e l'integrità della transazione.

2.1.3 Raccolta delle Transazioni in Blocchi

I nodi della rete raccolgono le transazioni trasmesse e le raggruppano in blocchi. Prima che un blocco possa essere aggiunto alla blockchain, deve essere validato attraverso un processo di consenso. Il metodo di consenso più

comune è il *Proof of Work* (PoW), ma esistono anche altri metodi come il *Proof of Stake* (PoS).

2.1.4 Validazione dei Blocchi

Nel *Proof of Work*, i nodi della rete, chiamati *miner*, competono per risolvere un complesso problema matematico che richiede una significativa potenza di calcolo. Il primo miner che risolve il problema ottiene il diritto di aggiungere il blocco alla blockchain e riceve una ricompensa sotto forma di criptovaluta. Nel *Proof of Stake*, i validatori vengono selezionati in base alla quantità di criptovaluta che possiedono e sono disposti a "mettere in gioco" come garanzia.

2.1.5 Aggiunta del Blocco alla Blockchain

Una volta che un blocco è stato validato, viene aggiunto alla blockchain e diventa parte permanente del registro distribuito. Ogni nodo della rete aggiorna la propria copia della blockchain per riflettere l'aggiunta del nuovo blocco. Poiché ogni blocco contiene l'hash del blocco precedente, qualsiasi tentativo di alterare un blocco precedente richiederebbe la modifica di tutti i blocchi successivi, rendendo tale operazione estremamente difficile e costosa.

2.1.6 Immutabilità e Sicurezza

L'immutabilità della blockchain è garantita dalla struttura della catena di blocchi e dall'uso delle funzioni hash crittografiche. Una volta che un blocco è stato aggiunto alla blockchain, non può essere modificato senza alterare l'intera catena di blocchi, il che richiederebbe una quantità enorme di potenza di calcolo. Questo rende la blockchain estremamente sicura e resistente alle manipolazioni.

2.1.7 Decentralizzazione

La blockchain opera su una rete decentralizzata di nodi, ciascuno dei quali mantiene una copia completa del registro. Questa decentralizzazione elimina la necessità di un'autorità centrale di fiducia e riduce il rischio di singoli punti di guasto. Ogni nodo nella rete partecipa al processo di consenso e contribuisce alla sicurezza e alla trasparenza della blockchain.

In sintesi, il funzionamento della blockchain si basa su una combinazione di crittografia, decentralizzazione e meccanismi di consenso per garantire la sicurezza, l'integrità e la trasparenza delle transazioni e dei dati registrati.

2.2 Blockchain Pubblica vs Blockchain Privata

Le blockchain possono essere classificate in due categorie principali: blockchain pubbliche e blockchain private. Entrambi i tipi utilizzano la tecnologia di registro distribuito per garantire la sicurezza e l'integrità delle transazioni, ma differiscono per quanto riguarda l'accesso, la gestione e l'uso.

2.2.1 Blockchain Pubblica

Una *blockchain pubblica* è una rete aperta a chiunque voglia partecipare. Le caratteristiche principali di una blockchain pubblica sono:

- **Decentralizzazione**: Le blockchain pubbliche sono completamente decentralizzate e non sono controllate da un'entità centrale. Tutti i partecipanti nella rete hanno uguali diritti di accesso e partecipazione.
- **Accessibilità**: Chiunque può unirsi alla rete, leggere, scrivere e verificare le transazioni senza bisogno di autorizzazioni. Questo aumenta la trasparenza e la fiducia tra i partecipanti.
- **Consenso**: Le blockchain pubbliche utilizzano algoritmi di consenso come il *Proof of Work* (PoW) o il *Proof of Stake* (PoS) per validare le transazioni. Questi algoritmi richiedono un considerevole impegno computazionale, rendendo le reti pubbliche sicure ma anche energeticamente costose.
- **Immutabilità**: Una volta che un blocco è stato aggiunto alla blockchain, diventa molto difficile modificarlo senza la collaborazione della maggioranza dei partecipanti alla rete, garantendo così l'integrità del registro.
- **Trasparenza**: Tutte le transazioni sulla blockchain sono visibili pubblicamente, garantendo un elevato livello di trasparenza e rendendo più difficile la frode e la manipolazione dei dati.

Esempi di blockchain pubbliche includono Bitcoin ed Ethereum, che consentono a chiunque di partecipare alla rete e contribuire al processo di consenso.

2.2.2 Blockchain Privata

Una *blockchain privata*, d'altra parte, è una rete chiusa in cui l'accesso è ristretto a un gruppo selezionato di partecipanti. Le caratteristiche principali di una blockchain privata sono:

- **Centralizzazione Parziale**: Le blockchain private sono solitamente gestite da un'entità centrale o da un consorzio di organizzazioni che controllano l'accesso e la gestione della rete.
- **Accesso Limitato**: Solo i partecipanti autorizzati possono leggere, scrivere e verificare le transazioni. Questo rende le blockchain private più adatte per le applicazioni aziendali dove la privacy e il controllo degli accessi sono cruciali.
- **Consenso**: Le blockchain private utilizzano meccanismi di consenso più efficienti dal punto di vista energetico, come il *Proof of Authority* (PoA) o il *Practical Byzantine Fault Tolerance* (PBFT). Questi algoritmi non richiedono un impegno computazionale elevato e possono elaborare le transazioni più velocemente.
- **Immutabilità**: Sebbene le blockchain private offrano un elevato livello di sicurezza, l'entità centrale o il consorzio di gestione possono, in teoria, modificare la blockchain se tutti i partecipanti concordano.
- **Riservatezza**: Le transazioni su una blockchain privata non sono visibili al pubblico, garantendo un livello più alto di riservatezza per le informazioni sensibili.

Esempi di blockchain private includono Hyperledger Fabric e R3 Corda, che sono progettate per essere utilizzate in contesti aziendali dove la sicurezza e la privacy dei dati sono essenziali.

2.2.3 Confronto tra Blockchain Pubbliche e Private

In conclusione, la scelta tra una blockchain pubblica e una blockchain privata dipende dalle esigenze specifiche dell'applicazione. Le blockchain pubbliche sono ideali per applicazioni che richiedono trasparenza e decentralizzazione, mentre le blockchain private sono più adatte per contesti aziendali dove la riservatezza e il controllo degli accessi sono cruciali.

Caratteristica	**Blockchain Pubblica**	**Blockchain Privata**
Accesso	Aperto a tutti	Limitato a partecipanti autorizzati
Controllo	Decentralizzato	Centralizzato parzialmente
Trasparenza	Alta	Limitata
Consenso	PoW, PoS	PoA, PBFT
Efficienza Energetica	Bassa	Alta
Sicurezza	Alta	Alta, ma dipende dal controllo centrale
Esempi	Bitcoin, Ethereum	Hyperledger Fabric, R3 Corda

Tabella 2.1: Confronto tra Blockchain Pubbliche e Private

Capitolo 3

Crittografia nella Blockchain

3.1 Hashing: SHA-256 e altre Funzioni Hash

La crittografia è uno dei pilastri fondamentali della tecnologia blockchain. Tra le tecniche crittografiche più importanti utilizzate nella blockchain vi è l'hashing, un processo che trasforma un input di lunghezza arbitraria in un output di lunghezza fissa, noto come hash o digest. Le funzioni hash garantiscono l'integrità, la sicurezza e la trasparenza delle transazioni nella blockchain.

3.1.1 SHA-256

SHA-256 (Secure Hash Algorithm 256-bit) è una delle funzioni hash più utilizzate nelle blockchain. Fa parte della famiglia di algoritmi SHA-2, progettati dalla National Security Agency (NSA) degli Stati Uniti. SHA-256 prende un input e lo trasforma in un output di 256 bit (32 byte). Le principali caratteristiche di SHA-256 includono:

- **Deterministicità**: Per un dato input, SHA-256 produce sempre lo stesso hash.
- **Velocità**: SHA-256 è progettato per essere computazionalmente efficiente, consentendo la rapida generazione di hash.
- **Pre-image Resistance**: È computazionalmente impraticabile risalire all'input originale a partire dall'hash generato.
- **Resistenza alle Collisioni**: È estremamente improbabile che due input distinti producano lo stesso hash.

- **Sensibilità alle Modifiche**: Anche una minima variazione nell'input produce un hash completamente diverso.

SHA-256 è utilizzato per molteplici scopi nella blockchain, inclusi la creazione di indirizzi di portafoglio, la generazione di impronte digitali di blocchi e transazioni, e la proof of work nel mining di criptovalute come Bitcoin.

3.1.2 Funzionamento di SHA-256

Il processo di hashing con SHA-256 può essere suddiviso in vari passaggi:

1. **Preprocessing**: L'input viene suddiviso in blocchi di 512 bit. Se l'ultimo blocco è inferiore a 512 bit, viene riempito con padding.

2. **Hash Computation**: L'algoritmo utilizza una serie di operazioni logiche e bitwise su questi blocchi, passando attraverso vari round di trasformazioni. Il risultato finale è un hash di 256 bit.

3.1.3 Altre Funzioni Hash

Oltre a SHA-256, esistono altre funzioni hash utilizzate nelle blockchain e in altre applicazioni crittografiche:

SHA-3

SHA-3 è l'ultima aggiunta alla famiglia degli algoritmi SHA ed è basato su una struttura completamente diversa chiamata Keccak. È considerato altamente sicuro ed è stato progettato per resistere agli attacchi crittografici moderni.

RIPEMD-160

RIPEMD-160 è un'altra funzione hash utilizzata nelle criptovalute, in particolare per la generazione degli indirizzi Bitcoin. RIPEMD-160 produce un hash di 160 bit, risultando in indirizzi più compatti rispetto a SHA-256.

BLAKE2

BLAKE2 è una funzione hash altamente efficiente progettata per essere più veloce di MD5, SHA-1 e SHA-256, mantenendo un elevato livello di sicurezza. È utilizzata in varie applicazioni, incluse alcune implementazioni blockchain.

Argon2

Argon2 è una funzione di hashing progettata specificamente per l'hashing delle password. È il vincitore del concorso Password Hashing Competition (PHC) ed è utilizzata in contesti dove è richiesta una protezione elevata contro attacchi di forza bruta.

3.1.4 Applicazioni dell'Hashing nella Blockchain

L'hashing viene utilizzato in vari modi all'interno delle blockchain:

- **Creazione degli Indirizzi**: Gli indirizzi di portafoglio sono generati attraverso l'hashing delle chiavi pubbliche con funzioni hash come SHA-256 e RIPEMD-160.
- **Proof of Work**: Nel mining, i miner devono trovare un nonce che, quando hashato con i dati del blocco, produce un hash che soddisfa una certa condizione (ad esempio, un numero di zeri iniziali).
- **Integrità dei Dati**: Gli hash vengono utilizzati per verificare l'integrità dei dati nei blocchi. Ogni blocco contiene l'hash del blocco precedente, creando una catena di blocchi interdipendenti.
- **Merkle Trees**: Gli alberi di Merkle utilizzano l'hashing per creare una struttura dati che consente la verifica efficiente e sicura delle transazioni.

In sintesi, l'hashing è una componente fondamentale della tecnologia blockchain, garantendo la sicurezza, l'integrità e l'efficienza delle operazioni e delle transazioni.

3.2 Merkle Trees e la Verifica dei Dati

I Merkle Trees, o alberi di Merkle, sono una struttura dati utilizzata nelle blockchain per garantire l'integrità e la verifica efficiente delle transazioni. Prendono il nome dal loro inventore, Ralph Merkle, che li ha introdotti nel 1979. I Merkle Trees sono fondamentali per il funzionamento della blockchain, poiché consentono di verificare l'integrità di un gran numero di dati in modo rapido e sicuro.

3.2.1 Struttura dei Merkle Trees

Un Merkle Tree è un albero binario in cui ogni foglia dell'albero rappresenta l'hash di un singolo blocco di dati, come una transazione. I nodi non foglia (nodi intermedi) contengono l'hash concatenato dei loro nodi figli. Il nodo radice, noto come *Merkle Root*, contiene l'hash complessivo dell'intero albero e rappresenta una sorta di "impronta digitale" di tutti i dati sottostanti.

- **Foglie (Leaf Nodes)**: Ogni foglia rappresenta l'hash di una transazione o di un blocco di dati.
- **Nodi Intermedi (Intermediate Nodes)**: Ogni nodo intermedio rappresenta l'hash concatenato dei suoi nodi figli.
- **Radice (Root Node)**: Il nodo radice contiene l'hash complessivo dell'intero albero.

[width=0.7]merkle$_t ree.png$

Figura 3.1: Struttura di un Merkle Tree

3.2.2 Costruzione di un Merkle Tree

La costruzione di un Merkle Tree avviene attraverso i seguenti passaggi:

1. **Hash delle Transazioni**: Ogni transazione viene hashata utilizzando una funzione hash crittografica come SHA-256.
2. **Creazione dei Nodi Intermedi**: Gli hash delle transazioni vengono poi raggruppati in coppie e concatenati. L'hash risultante diventa un nodo intermedio.
3. **Ripetizione del Processo**: Questo processo viene ripetuto fino a quando si arriva alla radice dell'albero, il Merkle Root.

3.2.3 Verifica dei Dati con i Merkle Trees

I Merkle Trees permettono una verifica efficiente e sicura dei dati. La verifica dell'integrità dei dati in un Merkle Tree può essere fatta con pochi passaggi, rendendo questo processo estremamente efficiente anche per grandi quantità di dati.

Verifica di una Transazione

Per verificare che una transazione specifica sia inclusa in un blocco, è necessario fornire una *Merkle Proof*. Una Merkle Proof è una serie di hash che consente di ricostruire il Merkle Root, partendo dall'hash della transazione e risalendo attraverso l'albero.

1. **Hash della Transazione**: Si parte dall'hash della transazione da verificare.
2. **Concatenazione degli Hash**: Si concatenano gli hash con i corrispondenti nodi fratelli forniti nella Merkle Proof.
3. **Calcolo del Merkle Root**: Si ripete il processo fino a ricostruire il Merkle Root.
4. **Confronto dei Merkle Root**: Il Merkle Root ricostruito viene confrontato con il Merkle Root del blocco. Se coincidono, la transazione è verificata.

Efficienza della Verifica

La verifica dei dati con i Merkle Trees è molto efficiente poiché richiede solo il calcolo e la comparazione di un numero limitato di hash. Questo è particolarmente utile nelle blockchain, dove la quantità di transazioni può essere molto elevata.

3.2.4 Applicazioni dei Merkle Trees nella Blockchain

I Merkle Trees trovano molteplici applicazioni nella blockchain:

- **Verifica delle Transazioni**: Consentono di verificare rapidamente e in modo sicuro che una transazione specifica sia inclusa in un blocco.
- **Integrità dei Dati**: Garantire che i dati nel blocco non siano stati alterati.
- **Blockchain Light Clients**: I nodi leggeri (light clients) possono verificare le transazioni senza dover scaricare l'intera blockchain, utilizzando le Merkle Proofs.
- **Sicurezza dei Contratti Intelligenti**: Utilizzati per garantire l'integrità dei dati nei contratti intelligenti.

In sintesi, i Merkle Trees sono una componente essenziale della tecnologia blockchain, fornendo un metodo efficiente e sicuro per verificare l'integrità delle transazioni e dei dati.

Capitolo 4

Wallet

4.1 Cosa Sono i Wallet e Dove Vengono Archiviate le Criptovalute?

Nell'ambito delle criptovalute e della tecnologia blockchain, i *wallet* (portafogli) sono cruciali. Un wallet è un software o dispositivo hardware che consente agli utenti di gestire le proprie criptovalute. I wallet non memorizzano fisicamente le criptovalute, ma contengono le chiavi crittografiche necessarie per accedere, gestire e trasferire le criptovalute registrate sulla blockchain.

4.1.1 Funzionamento dei Wallet

Le criptovalute sono archiviate sulla blockchain, un registro distribuito che registra tutte le transazioni effettuate. Un wallet contiene una coppia di chiavi crittografiche:

- **Chiave Privata**: Una stringa di caratteri alfanumerici che deve rimanere segreta. Consente al proprietario del wallet di firmare digitalmente le transazioni e accedere ai fondi associati. La perdita della chiave privata comporta la perdita irreversibile dell'accesso alle criptovalute.
- **Chiave Pubblica**: Derivata dalla chiave privata attraverso funzioni crittografiche. Può essere condivisa con altri utenti e viene utilizzata per ricevere fondi.

4.2 Crittografia delle Chiavi Private e Pubbliche

La sicurezza delle transazioni e delle criptovalute nella blockchain si basa sulla crittografia asimmetrica, che utilizza coppie di chiavi: una chiave privata e una chiave pubblica. Queste chiavi svolgono ruoli fondamentali nella protezione dei dati e nella verifica delle transazioni.

4.2.1 Chiavi Private

La chiave privata è una stringa di numeri e lettere generata casualmente, che deve rimanere segreta. Consente di firmare digitalmente le transazioni, garantendo l'autenticità e l'integrità dei dati. La perdita o il furto della chiave privata comporta la perdita irrevocabile dell'accesso alle criptovalute associate.

Generazione delle Chiavi Private

La generazione delle chiavi private deve essere effettuata in modo sicuro per evitare vulnerabilità. Le chiavi private possono essere generate utilizzando algoritmi crittografici come ECDSA (Elliptic Curve Digital Signature Algorithm) su curve ellittiche.

```
5J3mBbAH58CERwQPwAayBrRWzwZjWJcQnuSpMMWT7pM8WlrgLVN
```

4.2.2 Chiavi Pubbliche

La chiave pubblica è derivata dalla chiave privata attraverso un processo crittografico unidirezionale, solitamente utilizzando algoritmi di curve ellittiche. La chiave pubblica può essere condivisa liberamente e viene utilizzata per verificare la firma digitale delle transazioni e per ricevere fondi.

Derivazione delle Chiavi Pubbliche

La chiave pubblica viene generata applicando un algoritmo crittografico alla chiave privata. Per esempio, nell'algoritmo ECDSA, la chiave pubblica è un punto su una curva ellittica generato dalla moltiplicazione della chiave privata per un punto base predefinito sulla curva.

```
04bfcabedb42d9e1839df9516378ac2b2cfd1f4c3bc3fa7d7f2a2c1b5a9c657e
```

4.2.3 Firma Digitale

La firma digitale utilizza la crittografia asimmetrica per garantire l'autenticità e l'integrità delle transazioni. Quando un utente desidera inviare una criptovaluta, crea una transazione e la firma con la propria chiave privata. La firma digitale serve come prova che la transazione è stata autorizzata dal proprietario della chiave privata.

Processo di Firma Digitale

Il processo di firma digitale coinvolge diversi passaggi:

1. **Hashing della Transazione**: La transazione viene hashata utilizzando una funzione hash crittografica come SHA-256.
2. **Creazione della Firma**: L'hash della transazione viene criptato con la chiave privata dell'utente, generando la firma digitale.
3. **Invio della Transazione**: La transazione firmata viene inviata alla rete blockchain per la verifica.

4.2.4 Verifica della Firma Digitale

Quando una transazione firmata viene ricevuta dalla rete, i nodi della blockchain verificano la firma digitale utilizzando la chiave pubblica del mittente. Questo processo assicura che la transazione non sia stata alterata e che sia stata effettivamente autorizzata dal proprietario della chiave privata.

Processo di Verifica

Il processo di verifica della firma digitale comprende vari passaggi:

1. **Hashing della Transazione**: La transazione viene nuovamente hashata utilizzando la stessa funzione hash.
2. **Decrittazione della Firma**: La firma digitale viene decrittata utilizzando la chiave pubblica del mittente, producendo l'hash originale della transazione.
3. **Confronto degli Hash**: L'hash della transazione calcolato viene confrontato con l'hash decrittato dalla firma. Se coincidono, la firma è valida e la transazione è verificata.

4.2.5 Sicurezza delle Chiavi Crittografiche

La sicurezza delle chiavi crittografiche è di fondamentale importanza per proteggere le criptovalute. Alcune misure di sicurezza includono:

- **Archiviazione Sicura**: Conservare le chiavi private in luoghi sicuri, come hardware wallet o paper wallet, per proteggerle da furti o accessi non autorizzati.
- **Backup**: Creare copie di backup delle chiavi private e conservarle in luoghi separati e sicuri.
- **Criptazione**: Utilizzare password forti e crittografare i file contenenti le chiavi private.
- **Aggiornamenti Software**: Mantenere aggiornato il software del wallet per proteggersi da vulnerabilità conosciute.

In conclusione, la crittografia delle chiavi private e pubbliche è essenziale per garantire la sicurezza e l'integrità delle transazioni sulla blockchain. L'uso corretto di queste chiavi consente agli utenti di gestire le proprie criptovalute in modo sicuro e affidabile.

4.3 Tipi di Wallet

Esistono diversi tipi di wallet per la gestione delle criptovalute, ciascuno con caratteristiche specifiche che rispondono a diverse esigenze di sicurezza e usabilità. I principali tipi di wallet includono hardware wallet, software wallet, hosted wallet e non-custodial wallet.

4.3.1 Hardware Wallet

Gli *hardware wallet* sono dispositivi fisici progettati specificamente per la conservazione sicura delle chiavi private. Questi dispositivi mantengono le chiavi private offline, riducendo significativamente il rischio di attacchi informatici. Gli hardware wallet offrono un livello elevato di sicurezza poiché richiedono l'interazione fisica per autorizzare le transazioni.

- **Sicurezza**: Le chiavi private non lasciano mai il dispositivo, rendendole immuni a malware e hacking.

- **Usabilità**: La maggior parte degli hardware wallet è dotata di schermi e pulsanti per confermare le transazioni, offrendo un'interfaccia user-friendly.
- **Esempi**: Alcuni esempi popolari di hardware wallet includono Trezor, Ledger Nano S e Ledger Nano X.

4.3.2 Software Wallet

I *software wallet* sono applicazioni che possono essere installate su computer desktop, laptop, smartphone o tablet. Esistono diversi tipi di software wallet, ciascuno con caratteristiche uniche.

Desktop Wallet

I desktop wallet sono programmi software installati su un computer desktop o laptop. Offrono un buon equilibrio tra sicurezza e usabilità, ma sono vulnerabili a malware e attacchi informatici.

- **Sicurezza**: Meno sicuri rispetto agli hardware wallet poiché sono connessi a internet.
- **Usabilità**: Offrono un'interfaccia completa per la gestione delle criptovalute.
- **Esempi**: Electrum, Exodus e Bitcoin Core sono alcuni esempi di desktop wallet.

Mobile Wallet

I mobile wallet sono applicazioni installate su dispositivi mobili come smartphone e tablet. Sono molto pratici per l'uso quotidiano e consentono pagamenti rapidi e facili.

- **Sicurezza**: Possono essere meno sicuri rispetto ai desktop wallet a causa della vulnerabilità dei dispositivi mobili a furti e malware.
- **Usabilità**: Ideali per pagamenti in mobilità e facili da usare.
- **Esempi**: Mycelium, Trust Wallet e Coinomi sono esempi di mobile wallet.

Online Wallet (Web Wallet)

Gli online wallet sono accessibili tramite un browser web. Offrono grande comodità, ma sono meno sicuri poiché le chiavi private sono spesso gestite da terze parti.

- **Sicurezza**: Dipendono dalla sicurezza del server del fornitore di servizi. Possono essere vulnerabili ad hacking e attacchi di phishing.
- **Usabilità**: Molto convenienti e facili da usare da qualsiasi dispositivo con accesso a internet.
- **Esempi**: Blockchain.com, Coinbase e Binance sono esempi di web wallet.

4.3.3 Hosted Wallet

I *hosted wallet* sono wallet le cui chiavi private sono gestite da una terza parte, solitamente un exchange di criptovalute o un fornitore di servizi. Gli utenti accedono ai propri fondi tramite un account online.

- **Sicurezza**: La sicurezza dipende dalla fiducia nel fornitore del servizio. Gli utenti sono vulnerabili ad attacchi al server del fornitore.
- **Usabilità**: Molto semplici da usare, con funzionalità aggiuntive come l'exchange di criptovalute direttamente nel wallet.
- **Esempi**: Coinbase, Kraken e Bitstamp sono esempi di provider di hosted wallet.

4.3.4 Non-Custodial Wallet

I *non-custodial wallet* sono wallet in cui gli utenti mantengono il controllo esclusivo delle loro chiavi private. Questo tipo di wallet offre maggiore sicurezza e controllo, ma richiede agli utenti di gestire e proteggere le proprie chiavi private.

- **Sicurezza**: Gli utenti sono responsabili della sicurezza delle loro chiavi private. Se gestiti correttamente, possono offrire un alto livello di sicurezza.
- **Usabilità**: Possono essere meno convenienti per gli utenti non esperti, poiché richiedono una gestione attenta delle chiavi private.

- **Esempi**: Electrum, MetaMask e MyEtherWallet sono esempi di non-custodial wallet.

In sintesi, la scelta del tipo di wallet dipende dalle esigenze specifiche dell'utente in termini di sicurezza, usabilità e controllo. Ogni tipo di wallet ha i suoi vantaggi e svantaggi, e la scelta giusta varia a seconda delle circostanze individuali.

Capitolo 5

Transazioni

5.1 Processo di una Transazione su Blockchain

Una transazione su blockchain rappresenta il trasferimento di criptovalute da un indirizzo di portafoglio a un altro. Il processo di una transazione su blockchain può essere suddiviso in diversi passaggi, ciascuno dei quali garantisce la sicurezza, l'integrità e la trasparenza della transazione.

5.1.1 Creazione della Transazione

Il primo passo nel processo di una transazione è la sua creazione da parte dell'utente che desidera inviare criptovalute. L'utente specifica l'indirizzo del destinatario, l'importo da trasferire e, in alcuni casi, una commissione per incentivare i miner a includere la transazione nel blocco successivo.

- **Indirizzo del Destinatario**: Una stringa univoca derivata dalla chiave pubblica del destinatario, utilizzata per ricevere i fondi.
- **Importo**: La quantità di criptovaluta che l'utente desidera trasferire.
- **Commissione**: Un piccolo importo pagato ai miner per elaborare la transazione.

5.1.2 Firma della Transazione

Una volta creata la transazione, l'utente la firma digitalmente utilizzando la propria chiave privata. La firma digitale autentica la transazione, dimostrando che è stata autorizzata dal legittimo proprietario dei fondi. Questo passaggio è fondamentale per garantire la sicurezza della transazione.

5.1.3 Trasmissione della Transazione alla Rete

La transazione firmata viene quindi trasmessa alla rete blockchain. I nodi della rete ricevono la transazione e la propagano ad altri nodi, assicurando che tutti i partecipanti della rete siano a conoscenza della nuova transazione.

5.1.4 Verifica della Transazione

I nodi della rete verificano la validità della transazione. Questo processo di verifica include:

- **Integrità della Firma**: Controllo della validità della firma digitale per assicurarsi che la transazione sia stata effettivamente autorizzata dal proprietario della chiave privata.
- **Disponibilità dei Fondi**: Verifica che il mittente disponga dei fondi sufficienti per completare la transazione.
- **Doppia Spesa**: Assicurarsi che i fondi non siano stati spesi in una transazione precedente non ancora confermata.

5.1.5 Inclusione della Transazione in un Blocco

Una volta verificata, la transazione viene raccolta insieme ad altre transazioni in attesa di essere incluse nel blocco successivo. I miner (o validatori, a seconda del consenso utilizzato) competono per risolvere un problema crittografico che consentirà loro di aggiungere il blocco alla blockchain.

5.1.6 Conferma della Transazione

Quando un miner risolve il problema crittografico, crea un nuovo blocco contenente la transazione verificata e lo aggiunge alla blockchain. Questo processo è noto come *mining* nel contesto del *Proof of Work* (PoW). Una volta aggiunto il blocco, la transazione è considerata confermata.

5.1.7 Propagazione del Blocco nella Rete

Il nuovo blocco viene propagato a tutti i nodi della rete, che aggiornano le loro copie della blockchain per riflettere l'inclusione del nuovo blocco. Ogni nodo verifica nuovamente il blocco e le transazioni in esso contenute per assicurarsi che siano valide.

5.1.8 Stato della Transazione

La transazione può avere diversi stati durante il suo ciclo di vita:

- **Inviata**: La transazione è stata creata e trasmessa alla rete, ma non ancora confermata.
- **Non Confermata**: La transazione è in attesa di essere inclusa in un blocco.
- **Confermata**: La transazione è stata inclusa in un blocco e aggiunta alla blockchain.
- **Finalizzata**: Dopo diverse conferme (tipicamente 6 o più), la transazione è considerata irreversibile e finalizzata.

5.1.9 Esempio di Transazione Bitcoin

```
{
    "txid": "4b8e0e2f2b72e90a76414719772d240446da4cbbfd1dcdf7a44e9db8bcd20e1f",
    "inputs": [
        {
            "previous_output": "3c1e95690c5fbeb762768bf8d9d2d8b5eebc9d383b0d92c3
            "script_sig": "3045022100b4a7b6e94cfd49c674f38f9b6c1e8a09c6c13e5d5ef
        }
    ],
    "outputs": [
        {
            "value": 0.015,
            "script_pub_key": "76a91489abcdefabbaabbaabbaabbaabbaabbaabbaabba88a
        },
        {
            "value": 0.009,
            "script_pub_key": "76a9140123456789abcdef0123456789abcdef01234567898
        }
    ]
}
```

In questo esempio, una transazione Bitcoin include l'ID della transazione, gli input (che rappresentano le fonti dei fondi), e gli output (che rappresentano i destinatari e gli importi).

5.2 Firma Digitale e Crittografia delle Transazioni

La firma digitale e la crittografia delle transazioni sono fondamentali per garantire la sicurezza e l'integrità delle operazioni su una blockchain. Questi meccanismi permettono di autenticare l'identità del mittente, proteggere i dati delle transazioni e assicurare che le transazioni non siano state alterate.

5.2.1 Firma Digitale

Una firma digitale è un valore crittografico che viene calcolato utilizzando una chiave privata e che autentica un messaggio o un documento digitale. Nelle blockchain, le firme digitali garantiscono che solo il proprietario legittimo di una chiave privata possa autorizzare una transazione.

Processo di Firma Digitale

Il processo di firma digitale di una transazione coinvolge diversi passaggi:

1. **Hashing della Transazione**: La transazione viene prima hashata utilizzando una funzione di hash crittografica, come SHA-256. Questo produce un hash della transazione, che rappresenta un'impronta digitale univoca della stessa.

2. **Creazione della Firma**: L'hash della transazione viene criptato utilizzando la chiave privata del mittente, producendo la firma digitale. Questa firma è unica per quella specifica transazione e può essere verificata utilizzando la chiave pubblica del mittente.

3. **Invio della Transazione**: La transazione firmata viene quindi inviata alla rete blockchain per la verifica e l'inclusione in un blocco.

Verifica della Firma Digitale

I nodi della rete blockchain verificano la firma digitale per garantire che la transazione sia autentica e non sia stata alterata. Il processo di verifica coinvolge i seguenti passaggi:

1. **Hashing della Transazione**: La transazione viene nuovamente hashata per ottenere l'hash originale.

2. **Decrittazione della Firma**: La firma digitale viene decrittata utilizzando la chiave pubblica del mittente per ottenere l'hash firmato.

3. **Confronto degli Hash**: L'hash ottenuto dalla decrittazione della firma viene confrontato con l'hash originale della transazione. Se i due hash coincidono, la firma è valida e la transazione è considerata autentica.

5.2.2 Crittografia delle Transazioni

La crittografia delle transazioni garantisce che i dati delle transazioni siano protetti da accessi non autorizzati e alterazioni. La crittografia viene utilizzata per proteggere le chiavi private e per firmare digitalmente le transazioni.

Crittografia Asimmetrica

La crittografia asimmetrica, o a chiave pubblica, è il meccanismo principale utilizzato per la sicurezza delle transazioni su blockchain. Essa coinvolge l'uso di una coppia di chiavi: una chiave privata (segreta) e una chiave pubblica (condivisa).

- **Chiave Privata**: Utilizzata per firmare digitalmente le transazioni. Deve essere mantenuta segreta e protetta.
- **Chiave Pubblica**: Utilizzata per verificare la firma digitale. Può essere condivisa liberamente senza compromettere la sicurezza.

Esempio di Firma Digitale

Supponiamo che Alice voglia inviare una transazione a Bob. Ecco come funziona il processo:

1. **Alice crea una transazione** indicando l'indirizzo di Bob e l'importo da trasferire.
2. **Alice hash la transazione** utilizzando SHA-256, ottenendo un hash univoco della transazione.
3. **Alice firma l'hash della transazione** con la sua chiave privata, creando la firma digitale.
4. **Alice trasmette la transazione firmata** alla rete blockchain.
5. **I nodi della rete verificano la firma** utilizzando la chiave pubblica di Alice. Decrittano la firma per ottenere l'hash e confrontano questo hash con quello calcolato dalla transazione. Se coincidono, la transazione è considerata valida.

5.2.3 Sicurezza delle Chiavi Crittografiche

La protezione delle chiavi crittografiche è essenziale per mantenere la sicurezza delle transazioni. Alcune pratiche di sicurezza includono:

- **Backup Sicuri**: Creare copie di backup delle chiavi private e conservarle in luoghi sicuri, come hardware wallet o supporti fisici protetti.
- **Criptazione**: Utilizzare password robuste e crittografare i file contenenti le chiavi private.
- **Utilizzo di Multi-Signature**: Configurare wallet multi-firma che richiedono l'approvazione di più chiavi private per autorizzare una transazione.
- **Aggiornamenti Software**: Mantenere aggiornato il software del wallet per proteggersi da vulnerabilità conosciute.

In sintesi, la firma digitale e la crittografia delle transazioni sono elementi cruciali che garantiscono la sicurezza, l'autenticità e l'integrità delle operazioni su blockchain. Questi meccanismi proteggono gli utenti da frodi e accessi non autorizzati, assicurando che le transazioni siano condotte in modo sicuro e trasparente.

Capitolo 6

Mining

6.1 Come Vengono Confermate le Transazioni?

Il processo di conferma delle transazioni su una blockchain avviene principalmente attraverso il *mining*. Il mining è il processo mediante il quale le transazioni vengono verificate e aggiunte al registro pubblico distribuito (la blockchain). Questo processo coinvolge vari passaggi e richiede l'uso di algoritmi crittografici per garantire la sicurezza e l'integrità delle transazioni.

6.1.1 Il Ruolo dei Miner

I *miner* sono nodi speciali nella rete blockchain che verificano le transazioni e creano nuovi blocchi. Per il loro lavoro, i miner sono ricompensati con nuove criptovalute e commissioni di transazione.

6.1.2 Processo di Mining

Il processo di mining può essere suddiviso nelle seguenti fasi:

1. Raccolta delle Transazioni

I miner raccolgono le transazioni non confermate e le raggruppano in un blocco candidato, verificando le firme digitali e l'adeguatezza dei fondi.

2. Creazione di un Blocco

Il miner crea un blocco che contiene le transazioni verificate, un *timestamp*, l'hash del blocco precedente e un *nonce*.

3. Risoluzione del Problema Crittografico (Proof of Work)

Il miner deve trovare un nonce che, combinato con il blocco candidato e passato attraverso una funzione hash (es. SHA-256), soddisfi una specifica condizione (es. un certo numero di zeri iniziali).

4. Verifica della Soluzione

Quando un miner trova un nonce valido, trasmette il nuovo blocco alla rete. Gli altri nodi verificano l'hash e la validità del blocco. Se il blocco è valido, viene aggiunto alla blockchain.

5. Aggiunta del Blocco alla Blockchain

Una volta verificato, il nuovo blocco viene aggiunto alla blockchain, e le transazioni contenute in esso sono considerate confermate.

6. Ricompensa del Miner

Il miner che trova la soluzione valida riceve una ricompensa sotto forma di nuove criptovalute (ricompensa di blocco) e commissioni di transazione.

6.1.3 Altri Meccanismi di Consenso

Oltre al Proof of Work, esistono altri meccanismi di consenso utilizzati nelle blockchain:

Proof of Stake (PoS)

In Proof of Stake, i validatori sono scelti in base alla quantità di criptovalute che possiedono e mettono in gioco (stake). Questo meccanismo è meno dispendioso in termini di energia rispetto al PoW.

Delegated Proof of Stake (DPoS)

In Delegated Proof of Stake, i possessori di criptovalute votano per eleggere un piccolo numero di delegati che convalidano le transazioni e creano blocchi.

Proof of Authority (PoA)

In Proof of Authority, un numero limitato di validatori di fiducia è responsabile della convalida delle transazioni e della creazione di blocchi. Questo meccanismo è utilizzato in blockchain private e consorzi.

6.1.4 Importanza del Mining nella Sicurezza della Blockchain

Il mining garantisce la sicurezza della blockchain. Attraverso il mining, le transazioni sono verificate e registrate in modo immutabile, rendendo estremamente difficile alterare i dati storici senza controllare la maggior parte della potenza computazionale della rete.

In sintesi, il mining è un processo complesso e dispendioso in termini di risorse che garantisce la sicurezza, l'integrità e la trasparenza delle transazioni su una blockchain.

6.2 Algoritmi Crittografici nel Mining: Proof of Work (PoW) e Proof of Stake (PoS)

Il mining su blockchain utilizza vari algoritmi crittografici per raggiungere il consenso sulla validità delle transazioni e per aggiungere nuovi blocchi alla catena. I due algoritmi più comuni sono *Proof of Work* (PoW) e *Proof of Stake* (PoS). Ciascuno di essi ha caratteristiche e meccanismi distinti che influenzano la sicurezza, l'efficienza e la decentralizzazione della rete.

6.2.1 Proof of Work (PoW)

Proof of Work è il primo algoritmo di consenso utilizzato nelle blockchain, introdotto da Bitcoin. PoW richiede che i miner competano per risolvere complessi problemi matematici che richiedono una significativa potenza computazionale. Il processo di PoW può essere suddiviso nei seguenti passaggi:

Funzionamento di Proof of Work

1. **Raccolta delle Transazioni**: I miner raccolgono transazioni non confermate e le raggruppano in un blocco candidato.

2. **Creazione del Blocco**: Il miner prepara il blocco includendo l'hash del blocco precedente, un timestamp, le transazioni verificate e un nonce.

3. **Risoluzione del Problema Crittografico**: I miner devono trovare un nonce che, quando combinato con il blocco candidato e passato attraverso una funzione hash (ad esempio SHA-256), produce un hash

che soddisfa una specifica condizione di difficoltà (solitamente un certo numero di zeri iniziali).

4. **Verifica del Blocco**: Una volta trovato il nonce corretto, il miner trasmette il blocco alla rete. Gli altri nodi verificano la validità del blocco e, se valido, viene aggiunto alla blockchain.

5. **Ricompensa del Miner**: Il miner riceve una ricompensa sotto forma di nuove criptovalute e commissioni di transazione.

Vantaggi di Proof of Work

- **Sicurezza**: PoW è altamente sicuro grazie all'elevata potenza computazionale richiesta per risolvere i problemi crittografici.
- **Decentralizzazione**: PoW incentiva la partecipazione di un gran numero di miner, promuovendo la decentralizzazione della rete.

Svantaggi di Proof of Work

- **Consumo Energetico**: PoW richiede una quantità significativa di energia elettrica, rendendolo meno sostenibile dal punto di vista ambientale.
- **Scalabilità**: PoW può essere lento e inefficiente per l'elaborazione di un elevato numero di transazioni.

6.2.2 Proof of Stake (PoS)

Proof of Stake è un algoritmo di consenso alternativo progettato per essere più efficiente dal punto di vista energetico rispetto a PoW. In PoS, i validatori vengono scelti per creare nuovi blocchi in base alla quantità di criptovaluta che possiedono e mettono in gioco (stake). Il processo di PoS può essere descritto come segue:

Funzionamento di Proof of Stake

1. **Selezione dei Validatori**: I validatori vengono scelti in modo deterministico in base alla quantità di criptovaluta che possiedono. Più criptovaluta possiede un validatore, maggiore è la probabilità di essere scelto per creare il prossimo blocco.

2. **Creazione del Blocco**: Il validatore selezionato crea un nuovo blocco contenente le transazioni verificate e lo aggiunge alla blockchain.

3. **Verifica del Blocco**: Gli altri validatori della rete verificano la validità del blocco creato. Se il blocco è valido, viene aggiunto alla blockchain.

4. **Ricompensa del Validatore**: Il validatore riceve una ricompensa sotto forma di commissioni di transazione.

Vantaggi di Proof of Stake

- **Efficienza Energetica**: PoS consuma molta meno energia rispetto a PoW, poiché non richiede il mining competitivo basato sulla potenza computazionale.
- **Scalabilità**: PoS può essere più veloce e scalabile, rendendolo adatto per reti con un elevato numero di transazioni.

Svantaggi di Proof of Stake

- **Centralizzazione**: PoS può portare a una maggiore centralizzazione, poiché i validatori più ricchi hanno maggiori probabilità di essere selezionati per creare nuovi blocchi.
- **Problemi di Sicurezza**: PoS può essere vulnerabile a specifici attacchi, come l'attacco Nothing-at-Stake, dove i validatori possono tentare di creare blocchi su più catene concorrenti.

6.2.3 Confronto tra Proof of Work e Proof of Stake

Caratteristica	**Proof of Work (PoW)**	**Proof of Stake (PoS)**
Consumo Energetico	Alto	Basso
Sicurezza	Molto Alto	Alto
Efficienza	Medio/Basso	Alto
Scalabilità	Limitata	Elevata
Decentralizzazione	Alta	Media
Incentivi	Ricompensa di Blocco + Commissioni	Commissioni

Tabella 6.1: Confronto tra Proof of Work e Proof of Stake

In sintesi, sia Proof of Work che Proof of Stake offrono soluzioni uniche per raggiungere il consenso su una blockchain. Mentre PoW è noto per la sua sicurezza robusta e la decentralizzazione, PoS è apprezzato per la sua efficienza energetica e scalabilità. La scelta tra i due algoritmi dipende dalle esigenze specifiche della rete blockchain e dagli obiettivi del progetto.

6.2.4 Proof of Authority (PoA)

Proof of Authority è un algoritmo di consenso in cui un numero limitato di validatori di fiducia è responsabile della convalida delle transazioni e della creazione di blocchi. Questo meccanismo è spesso utilizzato in blockchain private e consorzi.

Funzionamento di Proof of Authority

- **Selezione dei Validatori**: I validatori sono entità predefinite e di fiducia.
- **Creazione del Blocco**: I validatori creano e verificano i blocchi.
- **Incentivi**: I validatori possono ricevere compensi per la loro attività.

Vantaggi di Proof of Authority

- **Efficienza**: PoA è molto efficiente in termini di velocità e capacità di elaborazione delle transazioni.
- **Sicurezza**: Poiché i validatori sono entità di fiducia, c'è una maggiore sicurezza contro attacchi malevoli.

Svantaggi di Proof of Authority

- **Centralizzazione**: PoA è altamente centralizzato, con la fiducia concentrata in poche entità.
- **Scalabilità Limitata**: La scalabilità può essere limitata dalla capacità dei validatori di fiducia.

6.2.5 Confronto tra gli Algoritmi di Consenso

In conclusione, diversi algoritmi di consenso offrono varie soluzioni ai problemi di sicurezza, efficienza e scalabilità nelle blockchain. La scelta del giusto algoritmo dipende dalle esigenze specifiche della rete e dagli obiettivi del progetto.

Caratteristica	**PoW**	**PoS**	**DPoS**	**PoA**
Consumo Energetico	Alto	Basso	Basso	Basso
Sicurezza	Alta	Alta	Media	Alta
Efficienza	Media	Alta	Molto Alta	Molto Alta
Scalabilità	Limitata	Elevata	Molto Elevata	Elevata
Decentralizzazione	Alta	Media	Media	Bassa
Esempi	Bitcoin	Ethereum 2.0	EOS	VeChain

Tabella 6.2: Confronto tra diversi algoritmi di consenso

Capitolo 7

Sicurezza

7.1 Attacchi alla Blockchain

Nonostante la blockchain sia progettata per essere sicura e resistente alle manomissioni, esistono vari tipi di attacchi che possono comprometterne l'integrità. Alcuni degli attacchi più noti includono il 51% attack, il Sybil attack e altri.

7.1.1 51% Attack

Il *51% attack* si verifica quando un'entità o un gruppo controlla oltre il 50% della potenza di hashing (PoW) o delle criptovalute in stake (PoS). Con tale controllo, l'attaccante può:

- **Doppia Spesa**: Spendere la stessa criptovaluta più di una volta.
- **Interrompere le Transazioni**: Impedire la conferma di nuove transazioni.
- **Modificare l'Ordine delle Transazioni**: Cambiare l'ordine delle transazioni nei blocchi.
- **Escludere o Modificare Blocchi**: Escludere o modificare blocchi creati da altri miner o validatori.

Questo attacco è improbabile su grandi blockchain come Bitcoin ed Ethereum, ma rappresenta una minaccia per blockchain più piccole.

7.1.2 Sybil Attack

Il *Sybil attack* avviene quando un singolo attaccante crea molteplici identità false sulla rete. Questo attacco può:

- **Controllo del Consenso**: Influenzare le decisioni di consenso.
- **Denial of Service**: Sovraccaricare la rete, degradandone le prestazioni.
- **Manipolazione dei Dati**: Alterare la registrazione delle transazioni.

Per mitigare i Sybil attack, molte blockchain implementano meccanismi come PoW, PoS o altri metodi di verifica dell'identità.

7.1.3 Double Spending Attack

Il *double spending attack* tenta di spendere la stessa unità di criptovaluta più di una volta.

- **Race Attack**: Due transazioni vengono inviate in rapida successione, sperando che una venga confermata prima dell'altra.
- **Finney Attack**: Un nodo di mining pre-mina un blocco con una transazione fraudolenta e lo rilascia al momento opportuno.

7.1.4 Eclipse Attack

L'*eclipse attack* isola un nodo specifico dalla rete, monopolizzandone tutte le connessioni.

- **Isolamento del Nodo**: L'attaccante blocca le connessioni legittime al nodo bersaglio.
- **Manipolazione delle Transazioni**: Il nodo isolato può essere indotto a confermare transazioni fraudolente.

7.1.5 DDoS Attack

Il *Distributed Denial of Service (DDoS) attack* mira a sovraccaricare la rete blockchain con traffico dannoso, rallentandone o bloccandone il funzionamento.

- **Sovraccarico della Rete**: L'attaccante invia un'enorme quantità di richieste alla rete blockchain.
- **Interruzione dei Servizi**: Rende la rete blockchain inaccessibile per i legittimi utenti.

7.1.6 Phishing Attack

Il *phishing attack* cerca di ingannare gli utenti per ottenere le loro chiavi private o altre informazioni sensibili.

- **Email Falsificate**: Gli attaccanti inviano email che sembrano provenire da fonti legittime.
- **Siti Web Falsi**: Creano siti web che imitano quelli di wallet o exchange legittimi.

7.1.7 Social Engineering Attack

Il *social engineering attack* sfrutta la manipolazione psicologica per ottenere informazioni sensibili dagli utenti.

- **Truffe Telefoniche**: Gli attaccanti fingono di essere rappresentanti di supporto.
- **Falsi Profili sui Social Media**: Fingono di essere figure autorevoli nel settore delle criptovalute.

7.2 Meccanismi di Sicurezza nella Blockchain

Per contrastare questi attacchi, la blockchain implementa vari meccanismi di sicurezza:

7.2.1 Meccanismi di Consenso

- **Proof of Work (PoW)**: Richiede significative risorse computazionali per confermare le transazioni.
- **Proof of Stake (PoS)**: Seleziona i validatori in base alla quantità di criptovalute possedute.

7.2.2 Crittografia

- **Hashing**: Utilizza funzioni hash per garantire l'integrità dei dati.
- **Crittografia Asimmetrica**: Protegge le chiavi private e verifica le firme digitali.

7.2.3 Decentralizzazione

La natura decentralizzata della blockchain rende difficile per un singolo attaccante compromettere l'intera rete.

7.2.4 Autenticazione e Autorizzazione

- **Multi-Signature Wallets**: Richiedono più firme per autorizzare una transazione.
- **Autenticazione a Due Fattori (2FA)**: Aggiunge un ulteriore livello di sicurezza.

In sintesi, la blockchain implementa una serie di meccanismi di sicurezza per proteggere contro vari attacchi. Tuttavia, è fondamentale che gli utenti adottino buone pratiche di sicurezza per proteggere le proprie risorse.

Capitolo 8

Conclusioni

8.1 Riflessioni Finali

La tecnologia blockchain rappresenta una rivoluzione nel modo in cui gestiamo e verifichiamo le transazioni digitali. Con le sue caratteristiche di decentralizzazione, immutabilità, trasparenza e sicurezza, la blockchain offre soluzioni innovative per una vasta gamma di applicazioni, dai pagamenti digitali alla gestione della supply chain, dall'industria finanziaria alla sanità.

Nonostante i numerosi vantaggi, la blockchain presenta anche delle sfide significative. Queste includono il consumo energetico elevato associato ad alcuni algoritmi di consenso come il Proof of Work, la scalabilità delle reti blockchain e le questioni legali e regolatorie relative all'adozione della tecnologia blockchain in settori regolamentati.

Un'altra sfida importante è rappresentata dalla sicurezza. Sebbene la blockchain sia intrinsecamente sicura, non è immune da attacchi. La comunità deve continuare a sviluppare e implementare meccanismi di sicurezza avanzati per proteggere le reti blockchain dagli attacchi e garantire la fiducia degli utenti.

Gli smart contracts, come componente fondamentale della tecnologia blockchain, offrono ulteriori opportunità per automatizzare e migliorare i processi aziendali. Tuttavia, è essenziale affrontare le sfide legate alla scrittura e alla verifica del codice degli smart contracts per evitare vulnerabilità e garantire il corretto funzionamento dei contratti.

In conclusione, la blockchain ha il potenziale per trasformare molteplici settori, offrendo soluzioni più sicure, efficienti e trasparenti. La chiave per il successo futuro della blockchain risiede nella continua innovazione tecnologica, nella collaborazione tra stakeholder e nella creazione di un quadro

normativo che supporti l'adozione e lo sviluppo responsabile della tecnologia blockchain.

Capitolo 9

Fonti

Le seguenti fonti sono state utilizzate per la preparazione di questa relazione:

- https://www.polito.it/sites/default/files/2022-12/Cripto.pdf
- http://www.mat.uniroma3.it/users/pedicini/slides/gvu2018-slides.pdf
- https://docenti.unimc.it/paolo.sernani/teaching/2023/28227/files/08-introduzione-alle-blockchain-17-11-2023-e-24-11-2023