Blockchain CheatSheet - Panoramica

Tempo di Lettura: 5 min

Indice

§ Fondamenti

§ Panoramica della Tecnologia Blockchain

§ Questioni Chiave e Risoluzioni 08/2024

§ Fondamenti

Blockchain: Un Database Distribuito Peer-to-Peer

- **Definizione**: La blockchain è una tecnologia di database distribuito peer-to-peer in cui ogni macchina (peer) funge da nodo-blocco.
- **Meccanismo**: Ogni blocco è collegato al successivo tramite un hash crittografico; la fine di un blocco contiene la chiave per l'inizio del blocco successivo.
- **Aspetto di Scopo**: Ogni tecnologia blockchain deve adattarsi all'applicazione specifica per cui è destinata. La criptovaluta è solo una delle applicazioni che possono utilizzare i protocolli blockchain.

Fiducia e Immutabilità

- **Nessuna Fiducia Necessaria**: Le caratteristiche dei blocchi e la proprietà sono registrate nella storia immutabile della catena (libri mastro).
- **Controllo del Consenso**: Il consenso è sempre controllato da ogni blocco nella catena attraverso il Proof of Work o il Proof of Stake.

Sicurezza e Efficienza Senza Precedenti

- **Verifica della Proprietà**: Questo risolve la verifica e lo scambio di proprietà in modo sicuro senza un intermediario.
- **Velocità**: I tempi di trasferimento dei dati sono significativamente più rapidi, quasi istantanei, il che è utile per gli scambi di mercato e i trasferimenti di proprietà.
- **Caratteristiche Fondamentali**: Sicurezza, velocità e verifica della proprietà sono le principali caratteristiche che rendono la blockchain cruciale per i servizi economici.

Anti-Falsificazione

- **Verifica dei Libri Mastro**: La blockchain risolve la falsificazione controllando i libri mastro delle blockchain.

Potenziale Disruptivo

- **Applicazioni**: Le applicazioni pratiche delle blockchain sono molteplici: votazione tramite token unici, sicurezza IoT, miglioramenti dell'ecosistema medico, dichiarazioni

finanziarie, convalide di processi sicuri, trasparenza delle transazioni per la governance, passaporti, costi delle transazioni e altro ancora.

---

§ Panoramica della Tecnologia Blockchain

Funzione di Hashing

- Una funzione di hashing crea un "fingerprint" degli elementi del blocco in modo dinamico, utilizzato come chiave per collegare i blocchi.

Approfondimenti

Blockchain Cheat Sheet - Hashing

Sistema Chiave Privata/Pubblica

- **Relazione**: La chiave privata e la chiave pubblica sono matematicamente correlate.
- **Facile da Risalire**: Chiave Privata => Chiave Pubblica
- **Difficile da Risalire**: Chiave Pubblica => Chiave Privata

Approfondimenti

Blockchain Cheat Sheet - Crittografia & Firme

Indirizzo Pubblico

- **Relazione con la Chiave Pubblica**: L'indirizzo pubblico è correlato alla chiave pubblica.
- **Derivazione**: Può essere la chiave pubblica stessa o un valore derivato dalla chiave pubblica utilizzando una funzione.

Algoritmi di Firma Digitale (DSA)

- **Prova di Proprietà**: DSA prova chi è il proprietario della chiave privata.
- **Verifica senza Rivelazione**: Permettono la verifica della firma senza rivelare la chiave privata.

Approfondimenti

Meccanica delle Transazioni

Concetto UTXO: Il sistema opera con il Concetto di UTXO (output di transazione non speso), che rappresenta il valore che il blocco possiede e stabilisce le unità non spese e spendibili.

1. **Inizio**: Inizia il processo di transazione.
2. **Verifica degli UTXO non spesi**: Controlla gli UTXO disponibili.
3. **Genera Chiavi (Mittente)**: Il mittente genera una nuova coppia di chiavi privata e pubblica.
4. **Genera Chiavi (Destinatario)**: Il destinatario (Jenna) genera una nuova coppia di chiavi privata e pubblica.
5. **Crea Transazione**: Crea una transazione per inviare 7 unità a Jenna e 3 unità al mittente come resto.
6. **Firma Transazione**: Il mittente firma la transazione con la propria chiave privata.
7. **Broadcast della Transazione alla Rete**: La transazione firmata viene broadcast alla rete blockchain.
8. **Validazione della Transazione**: I nodi della rete verificano e convalidano la transazione.
9. **Aggiornamento della Blockchain**: La blockchain viene aggiornata con la nuova transazione.
10. **Nuovo UTXO**: Il mittente ha un nuovo UTXO di 3 unità, mentre il vecchio UTXO ora è privo di valore.
11. **Fine**: Fine del processo di transazione.

Crittografia

- **Parte Integrante dell'Ecosistema**: La crittografia fluisce all'interno della struttura dell'ecosistema.
- **Utilizzo**: Viene utilizzata per generare chiavi private e memorizzare dati criptati nel blocco.

Approfondimenti

Blockchain Cheat Sheet - Crittografia & Firme

Meccanismo di Consenso

- **Metodi Diversi**: Ci sono diversi modi per ottenere consenso, come:
  - **Proof-of-Work (PoW)**: I miner risolvono problemi complessi per convalidare le transazioni.
  - **Proof-of-Stake (PoS)**: I principali detentori di token creano consenso, poiché hanno il maggiore interesse nella validazione delle transazioni corrette.

Approfondimenti

Blockchain Cheat Sheet - Consenso

Incentivi

- **Scopo**: Gli incentivi sono progettati per incoraggiare la partecipazione al sistema.
- **Sistemi Proof-of-Work**: Nei sistemi PoW, le ricompense vengono date a coloro che contribuiscono al benessere del sistema, ad esempio convalidando le transazioni.
- **Ricompense**: Queste ricompense hanno tipicamente un certo valore e motivano i partecipanti a mantenere la rete.

---

§ Questioni Chiave e Risoluzioni 08/2024

Questioni Chiave Risolte:

1. **Come può la tecnologia blockchain superare le velocità di transazione tradizionali?**
   - La blockchain può elaborare le transazioni più rapidamente rispetto ai metodi tradizionali grazie alla sua natura decentralizzata e agli algoritmi di consenso avanzati.
2. **Perché utilizzare database di grandi dimensioni in una blockchain?**
   - I database di grandi dimensioni garantiscono ridondanza, sicurezza e disponibilità dei dati attraverso la rete.
3. **Come possiamo ottenere l'interoperabilità tra diverse catene?**
   - L'interoperabilità tra catene può essere ottenuta attraverso protocolli e tecnologie che consentono la comunicazione e le transazioni tra diverse blockchain.

Questioni Chiave Non Ancora Risolte:

1. **Privacy:**
   - La privacy rimane una questione irrisolta, poiché migliorare la trasparenza spesso richiede di sacrificare un certo livello di privacy.
2. **Verifica del Mondo Reale:**

- Come possiamo verificare elementi del mondo reale con la blockchain, ad esempio utilizzando tag RFID? Questa è ancora una domanda aperta.

3. **Immutabilità e Forks:**
    - Aggiornare l'immutabilità di una catena può creare fork, portando a nuove tecnologie blockchain e frammentando ulteriormente l'ecosistema.
4. **Governance:**
    - Se queste tecnologie diventano ampiamente diffuse, gli algoritmi dovranno essere aggiornati per rimanere al passo con i cambiamenti sociali. Ottenere consenso per questi cambiamenti sostanziali sarà molto difficile.
5. **Regolamentazioni:**
    - Mancano regolamentazioni a causa della natura dirompente di queste tecnologie. Sono necessarie nuove leggi per regolamentare efficacemente questo campo.

La tecnologia blockchain consente alle persone nei mercati emergenti di monetizzare i prodotti in modi senza precedenti, guidando una crescita significativa accedendo alle finanze moderne e superando vincoli precedenti. Questo aumento del capitale umano beneficia sia i mercati emergenti che quelli sviluppati, portando a progressi inaspettati e impattanti.

Suggerimenti per il Prossimo Passo

Blockchain CheatSheet - La Visione

Autore: Kenneth Boldrini