Intro

Ciao a tutti...

Salto intro su blockchain

Come usare blockchain per videogiochi

Come storage

- Ownership indipendente
- Cross compatibility

Come esecuzione

- Trasparenza (e.g. loot boxes)
- Controllo esecuzione + assegnazione premi (citare tesi)

Perchè livello 1 non va bene?

- Latenza innata (anche per loot box)
- Fee alte per contratti complessi

Layer 2

Spiegazione generica

State channels

Apertura

- Depositare fondi + firma

Utilizzo

- Transazione valida se segue regole + firmata da TUTTI

Chiusura

1. Un utente manda transazione a smart contract
2. Challenge period (transazioni più nuove)

Problema computazioni off-chain (scacchi)

Sidechains

- Blockchain indipendenti ma generate da una livello 1
- Protocolli ad hoc
- No garanzie del livello 1

Rollup

- Molte transazioni eseguite in blockchain livello 2 e poi batchate su livello 1
- La blockchain di livello 2 è più piccola e può usare consensus più veloce
- Fee L1 splittate su tutte le transazioni di una batch

Rollup ottimistici

- Assumption transazioni valide (L1 smart contract NON necessita verification)
- Challenge period (problema uscita)

Interazione L2 - L1

- Sequencer manda: state Merkle root old, state Merkle root new, sommario transazioni (fee alte), Merkle root transazioni

Fraud proofs

- Single round
- Multi round (vogliamo verificare che il codice di esecuzione fornita e quello eseguito siano uguali)

ZK rollups

- Interazione simile a optimistic rollups, ma mandano ZK proof anzichè tutte le transazioni
- Intuizione ZK proof (da ri-esecuzione transazioni ==> eseguire sistema di equazioni matematiche)
- Risolto problema challenge period e fee alte
- Scalabili (batch), L1 fee basse (split), on-L2-chain, ancorati a L1

Starknet

Generalità

- Ethereum based + Cairo per smart contract

Account abstraction

- Tutto è un contratto
- La private key non può modificare lo stato direttamente, ma solo invocare contratti
- Più flessibilità, più user friendly
- Contract account interface

Transaction journey

1. Creazione transazione
2. Ricezione node
3. Verifica + esecuzione + creazione blocco sequencer
4. Generazione ZK proof prover
5. Accettazione Ethereum L1

Salto setup e Cairo, vediamo subito il progetto

Loot boxes

Perchè on-chain

Gioco d'azzardo (intermittent rewards)

Percentuali non rispettate (fairness)

Content creator per hype

Demo

Come deployare smart contract

Storage + `buyLootBox` + `viewBalance`

Python client

starknet_py

- FullNode (read)
- Account (crea transazioni)
- Contract (handle per invocare contratti)

Polling loop