CuanticChain: Un Blockchain Securizat Post-Cuantic cu Consens Proof-of-Quantum-Work (PoQW)

Rezumat

CuanticChain este o blockchain de nouă generație, conceput pentru a rămâne sigur în era calculatoarelor cuantice. Utilizează criptografie post-cuantică (PQC) pentru semnături și introduce Proof-of-Quantum-Work (PoQW), un mecanism de consens care integrează sarcini de calcul cuantic în validarea blocurilor. Acest model de consens hibrid permite participarea atât a minerilor cuantici, cât și a celor clasici, prioritizând securitatea împotriva adversarilor cuantici.

1. Introducere

Odată cu apariția calculatoarelor cuantice, primitivele criptografice clasice precum ECDSA și RSA devin vulnerabile la algoritmul lui Shor. Blockchain-urile care se bazează exclusiv pe aceste algoritme riscă să devină nesigure. CuanticChain abordează această problemă prin:

- Adoptarea schemelor de semnătură post-cuantice bazate pe rețele de tip lattice (Dilithium).

- Înlocuirea Proof-of-Work cu Proof-of-Quantum-Work, un mecanism ce solicită calcule cuantice în procesul de validare a blocurilor.

Această abordare întărește securitatea împotriva atacurilor cuantice și stimulează dezvoltarea și utilizarea resurselor de calcul cuantic.

2. Prezentare generală a arhitecturii

2.1 Structura nodului

Nodurile CuanticChain sunt implementate în Rust, organizate în module independente:

- **crates/crypto** – Implementarea funcțiilor hash (Blake3), generarea adreselor, codificarea datelor și primitivele PQC (Dilithium).

- **crates/node** – Logica principală a blockchain-ului: rețea P2P, stocare, model UTXO, mempool, minerit, API RPC, portofel.

- **configs/** – Configurații pentru mainnet și testnet.

- **genesis/** – Definițiile blocului genesis.

- **docker/** – Configurații pentru implementare.

2.2 Rețea

Un strat peer-to-peer personalizat asigură propagarea descentralizată a blocurilor și tranzacțiilor. Endpoint-urile RPC permit interacțiunea cu nodurile prin HTTP/JSON.

2.3 Stocare

Starea blockchain-ului este menținută folosind modelul UTXO, care oferă simplitate și securitate ridicată în validarea tranzacțiilor.

3. Consens: Proof-of-Quantum-Work (PoQW)

3.1 Structura provocării

Fiecare bloc necesită rezolvarea unei provocări PoQW, definită prin:

- **header_preimage_hash** – Hash Blake3 al antetului blocului (fără semnături/proof).

- **difficulty** – Dificultatea opțională PoW clasică pentru fallback.

- **circuit_id** – ID-ul sarcinii de calcul cuantic (ex. Random Circuit Sampling, Trapdoor Claw-Free functions).

- **salt** – Separare de domeniu pentru prevenirea coliziunilor între provocări.

3.2 Structura transcriptului

Proverul returnează un transcript ce conține:

- **circuit_id** – Trebuie să corespundă provocării.

- **prover_id** – Identificatorul nodului/validatorului.

- **y_bytes** – Rezultatul principal al calculului cuantic.

- **aux** – Date suplimentare specifice protocolului (commitment-uri, semnături).

- **verifier_hint** – Date opționale pentru verificare.

- **timestamp_ms** – Timpul execuției.

3.3 Verificare

- Se verifică consistența `circuit_id`.

- Se verifică semnătura post-cuantică pe `(chal_hash || y_bytes)` folosind Dilithium.

- Opțional: teste statistice pentru validarea entropiei/coliziunilor în `y_bytes`.

3.4 Suport hibrid

Nodurile fără hardware cuantic pot apela un prover extern prin HTTP, permițând participarea extinsă.

4. Securitate post-cuantică

4.1 Schema de semnătură

CuanticChain folosește **Dilithium**, o schemă bazată pe rețele lattice, recomandată de NIST, rezistentă la atacuri cuantice.

4.2 Funcția hash

Blake3 este utilizată pentru hashing datorită vitezei, paralelismului și rezistenței la atacuri criptanalitice cunoscute.

4.3 Securitatea consensului

Mecanismul PoQW leagă producția de blocuri de probleme computaționale considerate dificile chiar și pentru adversarii cuantici fără resurse cuantice suficiente.

5. Tokenomics

Parametrii economici pot fi configurați, dar designul suportă:

- Recompense de bloc pentru soluțiile PoQW valide.

- Taxe de tranzacție ca stimulent pentru validatori.

- Recompense diferențiate pentru contribuții cuantice vs clasice.

6. Implementare

6.1 Mainnet

Configurația în `configs/mainnet.toml` și blocul genesis în `genesis/mainnet.genesis.json`.

6.2 Testnet

Disponibil în `configs/testnet.toml` cu un genesis separat.

6.3 Infrastructură

- Scripturile Docker și docker-compose permit implementarea rapidă.

- Fișierele systemd permit rularea persistentă a nodurilor.

7. Plan de dezvoltare

- **Faza 1**: Lansare cu consens PoQW/PoW hibrid.

- **Faza 2**: Integrarea unor provocări cuantice avansate (ex. QAOA, boson sampling).

- **Faza 3**: Introducerea zk-PoQW pentru dovezi cuantice cu păstrarea confidențialității.

- **Faza 4**: Interoperabilitate cross-chain cu alte blockchain-uri securizate PQC.

8. Concluzie

CuanticChain este un protocol blockchain orientat spre viitor, conceput să reziste amenințărilor calculatoarelor cuantice. Prin integrarea Proof-of-Quantum-Work și a criptografiei post-cuantice, oferă securitate imediată și pe termen lung, stimulând inovația în calculul cuantic descentralizat.

Referințe

1. Proiectul NIST pentru Criptografie Post-Cuantica: https://csrc.nist.gov/projects/post-quantum-cryptography

2. Funcția hash Blake3: https://blake3.io/

3. Avantajul Computațional Cuantic: https://www.nature.com/articles/s41586-019-1666-5