

# QNS — Quantum Neural Security

## Whitepaper v2.0

Дата: 2026-02-05

Версия: 2.0.0

## Содержание

1. Введение
2. Архитектура
3. Консенсус
4. Neural DAG с GHOSTDAG
5. Криптография
6. Виртуальные машины
7. DeFi примитивы
8. Валидаторы
9. BlockchainBrain AI
10. Мосты
11. Токеномика
12. Производительность

## 1. Введение

QNS (Quantum Neural Security) — это блокчейн следующего поколения, объединяющий:

- **Neural AI** — BlockchainBrain для адаптивной оптимизации сети
- **10-кластерный DAG** — GHOSTDAG упорядочивание для максимальной пропускной способности
- **Post-quantum криптографию** — Dilithium3, Kyber1024 для защиты от квантовых атак
- **Multi-VM архитектуру** — EVM, TVM и QVM для максимальной совместимости
- **200,000+ TPS** — благодаря параллельному выполнению BlockSTM

## Ключевые метрики

| Параметр   | Значение |
|------------|----------|
| TPS Target | 200,000+ |
| Block Time | 1-2 сек  |

| Параметр      | Значение     |
|---------------|--------------|
| Finality      | ~3 сек       |
| Валидаторов   | 171 (3-tier) |
| DAG кластеров | 10           |
| Opcodes QVM   | 180+         |

## 2. Архитектура

### 2.1 Структура блока

```
pub struct BlockHeader {
    // Базовые поля
    pub workchain: i32,
    pub shard: ShardId,
    pub seq_no: u64,
    pub timestamp: u64,
    pub prev_block_hash: Hash,
    pub state_root: Hash,
    pub transactions_root: Hash,

    // Валидация (Tendermint BFT)
    pub proposer: Address,
    pub validator_set_hash: Hash,
    pub proposer_signature: Vec<u8>,

    // EIP-1559
    pub gas_used: u64,
    pub gas_limit: u64,
    pub base_fee: u128,

    // Нейронные поля
    pub neural_activation: i128,
    pub neural_learning_rate: i128,
    pub neural_plasticity: i128,

    // DAG структура (GHOSTDAG)
    pub dag_parents: Vec<Hash>,
    pub dag_children: Vec<Hash>,
    pub cluster_id: u8,

    // Proofs
    pub brain_state_hash: Hash,
    pub neural_proof: NeuralProof,
    pub consensus_proof: ConsensusProof,
}
```

## 2.2 Типы транзакций

| Тип                | ID | Описание          |
|--------------------|----|-------------------|
| Legacy             | 0  | Pre-EIP-2718      |
| AccessList         | 1  | EIP-2930          |
| EIP1559            | 2  | Fee market        |
| Transfer           | 3  | Простой перевод   |
| ContractDeployment | 4  | Deploy контракта  |
| ContractCall       | 5  | Вызов контракта   |
| CrossShard         | 6  | Кросс-шард        |
| Staking            | 7  | Стейкинг          |
| Governance         | 8  | Голосование       |
| NeuralProposal     | 9  | Нейро-оптимизация |

## 3. Консенсус

### Алгоритм: Tendermint BFT (3-фазный)

**МЕХАНИЗМ:**

- └ Propose Phase (ожидание предложения от лидера)
- └ Prevote Phase (первый раунд голосования - 2/3+)
- └ Precommit Phase (второй раунд голосования - 2/3+)
- └ Commit Phase (блок закоммичен)

### Фазы консенсуса

| Фаза      | Назначение                | Условие выхода                        |
|-----------|---------------------------|---------------------------------------|
| Propose   | Ожидание блока от лидера  | Получение валидного блока или timeout |
| Prevote   | Первое голосование        | 2/3+1 prevotes                        |
| Precommit | Окончательное голосование | 2/3+1 precommits                      |
| Commit    | Финализация               | Автоматический переход                |

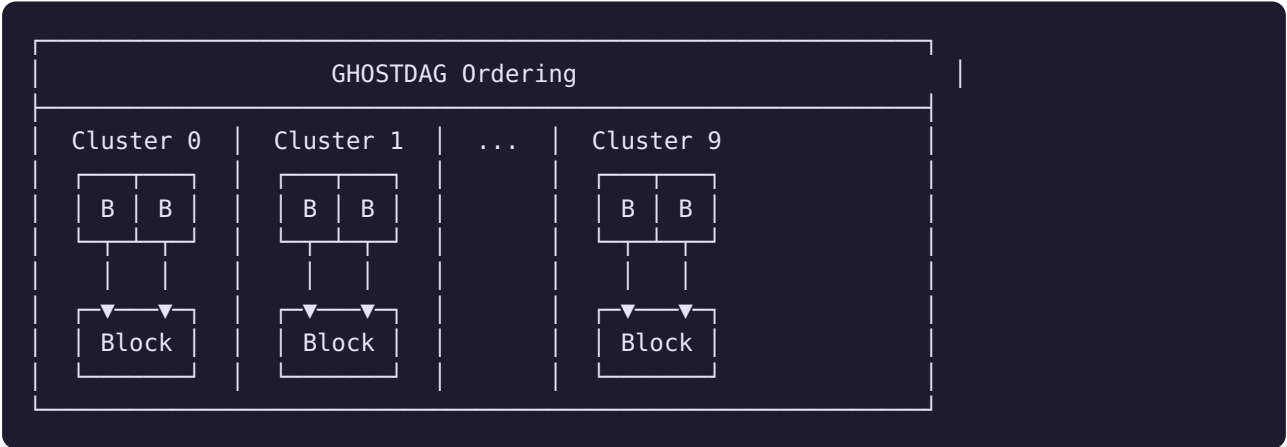
### Параметры

```
propose_timeout: 3 seconds
prevote_timeout: 2 seconds
precommit_timeout: 2 seconds
finality: ~3 seconds
```

## 4. Neural DAG с GHOSTDAG

### 4.1 Структура

QNS использует 10-кластерный Neural DAG с GHOSTDAG упорядочиванием:



### 4.2 GHOSTDAG алгоритм

- **Blue set selection:** Определение "честных" блоков
- **Blue score:** Метрика для упорядочивания
- **K-cluster parameter:** k=10 для оптимальной производительности

### 4.3 Параметры DAG

| Параметр                    | Значение              |
|-----------------------------|-----------------------|
| Кластеров                   | 10                    |
| Максимальная глубина        | 60 ( $2^{60}$ шардов) |
| Параллельных блоков на шард | 10                    |

## 5. Криптография

### 5.1 Post-Quantum алгоритмы

| Алгоритм          | Назначение        | Размер ключа | Размер подписи | Уровень NIST |
|-------------------|-------------------|--------------|----------------|--------------|
| <b>Dilithium3</b> | Подписи           | 1952 bytes   | 3293 bytes     | L5 (192-bit) |
| <b>Kyber1024</b>  | Key Encapsulation | 1568 bytes   | 1568 bytes     | L5           |
| <b>SPHINCS+</b>   | Резервные подписи | Variable     | Variable       | L5           |

## 5.2 Гибридные подписи

```
pub enum UniversalSignature {
    Classical(Ed25519Signature),    // 64 bytes
    Quantum(QuantumSignature),      // 3293 bytes (Dilithium3)
    Hybrid {
        classical: Ed25519Signature,
        quantum: QuantumSignature,
    },                             // 3357 bytes
}
```

### Режимы криптографии:

- **Classical** — DEPRECATED, только Ed25519
- **Hybrid** — Ed25519 + Dilithium3 (для валидаторов)
- **QuantumOnly** — Только Dilithium3 (DEFAULT)

## 5.3 Хеш-функции

| Функция          | Использование               | Квантостойкость |
|------------------|-----------------------------|-----------------|
| <b>BLAKE3</b>    | Блоки, состояние, консенсус | Да              |
| <b>Кеccak256</b> | EVM совместимость           | Нет             |

## 6. Виртуальные машины

### 6.1 Multi-VM архитектура

| VM         | Описание                 | Workchain ID | Формат адреса     |
|------------|--------------------------|--------------|-------------------|
| <b>QVM</b> | Quantum VM (native DeFi) | 0            | quant...          |
| <b>EVM</b> | Ethereum VM (revm 14)    | 1            | 0x...             |
| <b>TVM</b> | TON VM (cells, stack)    | 2            | EQ.../UQ.../0:hex |

### 6.2 QVM Opcodes (180+)

#### EVM-Compatible (92 opcodes)

- Stack: PUSH1-PUSH32, POP, DUP1-DUP16, SWAP1-SWAP16
- Arithmetic: ADD, SUB, MUL, DIV, MOD, EXP
- Memory/Storage: MLOAD, MSTORE, SLOAD, SSTORE

#### QVM Extensions (88+ opcodes)

##### Cross-Shard:

- CROSS\_SHARD\_CALL (100,000 gas)
- ATOMIC\_SWAP (200,000 gas)

### Post-Quantum Crypto:

- PQ\_SIGN\_DILITHIUM (50,000 gas)
- PQ\_VERIFY\_DILITHIUM (10,000 gas)
- PQ\_KYBER\_ENCAP (20,000 gas)

### Zero-Knowledge:

- ZK\_PROVE (500,000+ gas)
- ZK\_VERIFY (50,000 gas)
- MERKLE\_VERIFY (50,000 gas)

### DeFi Native:

- DEFI\_SWAP (30,000 gas)
- ADD\_LIQUIDITY (40,000 gas)
- FLASH\_LOAN (50,000 gas)
- ORACLE\_PRICE (100 gas)
- STAKE/UNSTAKE (100,000 gas)

### Neural:

- NEURAL\_FORWARD (10,000 gas)
- TENSOR\_MATMUL (5,000 gas)
- ATTENTION (25,000 gas)

## 7. DeFi примитивы

### 7.1 АММ / Свопы

#### 4 типа пулов:

| Тип                    | Формула          | Применение        |
|------------------------|------------------|-------------------|
| Constant Product       | $x \times y = k$ | Volatile pairs    |
| Stable Swap            | D curve (Newton) | Stablecoins       |
| Concentrated Liquidity | Tick-based       | Capital efficient |
| Weighted Pool          | $\Pi(B_i^{w_i})$ | Multi-asset       |

### 7.2 Flash Loans

- **Fee:** 0.09% (9 BPS)
- **Requirement:** Погашение в том же блоке
- **Protection:** Reentrancy guard per (borrower, asset)
- **Max per block:** 1000 loans

### 7.3 Lending

- **Модель:** Compound-style

- **Min Collateral Ratio:** 150%
- **Liquidation Threshold:** 125%
- **Liquidation Bonus:** 5%

## 7.4 Oracle

- **TWAP window:** 30 минут
- **Min observations:** 10
- **Max deviation:** 5% от TWAP

# 8. Валидаторы

## 8.1 Трёхуровневая система

| Уровень      | Минимум     | Награда | Макс. валидаторов |
|--------------|-------------|---------|-------------------|
| Execution    | 10,000 QNS  | 1.0x    | 100               |
| Neural       | 50,000 QNS  | 1.5x    | 50                |
| Verification | 100,000 QNS | 2.0x    | 21                |

**Всего:** 171 валидатор

## 8.2 Жизненный цикл

PENDING → ACTIVE → INACTIVE → UNBONDING → EXITED  
 ↘ JAILED ↗

## 8.3 Slashing (Graduated Penalties)

| Уровень  | Нарушение         | Штраф | Тюрьма    |
|----------|-------------------|-------|-----------|
| Light    | Downtime          | 0.1%  | 1 час     |
| Medium   | Equivocation      | 5%    | 24 часа   |
| Critical | DoubleVote        | 33%   | 7 дней    |
| Critical | CoordinatedAttack | 100%  | Permanent |

**Unbonding period:** 7 дней

## 9. BlockchainBrain AI

### 9.1 Компоненты

| Компонент                     | Назначение                            |
|-------------------------------|---------------------------------------|
| <code>brain.rs</code>         | BlockchainBrain — ML для оптимизации  |
| <code>prediction.rs</code>    | Gas, load, risk, MEV prediction       |
| <code>learning.rs</code>      | Hebbian, STDP, reinforcement learning |
| <code>memory.rs</code>        | Sensory, working, episodic, semantic  |
| <code>consciousness.rs</code> | Global Workspace Theory               |
| <code>reasoning.rs</code>     | Rule engine, causal graph             |
| <code>attention.rs</code>     | Multi-head self-attention             |
| <code>meta_learning.rs</code> | Adaptive learning rates               |
| <code>controller.rs</code>    | Closed-loop network control           |

### 9.2 Детерминизм

**100% детерминистичные вычисления:**

- `NeuralScalar = I64F64` (128-bit fixed-point)
- Polynomial approximations (no exp/sin/cos)
- `BTreeMap/BTreeSet` (deterministic order)
- `NeuralRng` seeded from block hash

### 9.3 MEV защита

- **Commit-Reveal:** двухфазная защита
- **AI Detection:** предсказание sandwich атак
- **Slippage protection:** Default 100 bps (1%)

## 10. Мосты

### 10.1 Поддерживаемые сети (10+)

| Сеть     | Тип              | Статус     |
|----------|------------------|------------|
| Ethereum | BLS aggregation  | Production |
| Bitcoin  | SPV light client | Production |
| BSC      | EVM compatible   | Production |
| Polygon  | Checkpoint-based | Production |



| Сеть      | Тип              | Статус     |
|-----------|------------------|------------|
| TON       | Cell-based proof | Production |
| Arbitrum  | Optimistic       | Active     |
| Optimism  | Optimistic       | Active     |
| Avalanche | Subnet           | Active     |
| Solana    | Wormhole         | Planned    |
| XCM/IBC   | Polkadot/Cosmos  | Active     |

## 10.2 Механизм

- **Lock-and-mint:** Lock на source → mint wrapped на QNS
- **Burn-and-release:** Burn wrapped → release на source
- **Security:** Threshold signatures, MPC

## 11. Токеномика

### 11.1 Блочные награды

INITIAL\_BLOCK\_REWARD = 2 QNS  
 HALVING\_PERIOD = 315,360,000 блоков (~10 лет)

Распределение:

- └ 40% → Block Producer
- └ 40% → Attesters Pool
- └ 10% → Skynet Neural Fund
- └ 10% → Treasury/Faucet

### 11.2 Комиссии

- └ 50% → Validators (60% producer, 40% attesters)
- └ 25% → Burn (дефляция)
- └ 25% → Treasury

## 12. Производительность

### 12.1 Результаты тестирования

| Тест              | TPS            | Успех  |
|-------------------|----------------|--------|
| TPS Measurement   | <b>293,983</b> | 99.90% |
| Network Partition | 2,417,397      | 100%   |

| Тест                  | TPS           | Успех         |
|-----------------------|---------------|---------------|
| Byzantine Validators  | 562,870       | 100%          |
| Neural Learning       | 15,749        | 95.40%        |
| Cross-Shard           | 7,432,693     | 99.94%        |
| <b>Combined Chaos</b> | <b>10,739</b> | <b>93.93%</b> |

## 12.2 Ключевые выводы

### 1. Производительность:

- Максимальный TPS: ~294,000
- Реалистичный TPS под хаосом: ~10,700
- P99 latency: < 2ms

### 2. Безопасность:

- 100% детекция Byzantine атак
- 100% slashing злонамеренных валидаторов
- BFT работает при < 33% Byzantine

### 3. Надёжность:

- 99.94% доставка cross-shard сообщений
- Автоматическое восстановление после партиций
- Нет утечек памяти

## Заключение

QNS представляет собой полностью интегрированный Neural AI блокчейн с:

- 200,000+ TPS потенциальной пропускной способностью
- Post-quantum криптографической защитой
- 10-кластерным GHOSTDAG DAG
- 171 валидатором в 3-уровневой системе
- 180+ нативными QVM opcodes
- BlockchainBrain AI для адаптивной оптимизации

## QNS — Quantum Neural Security

Документ обновлён: 2026-02-05