QNS — Quantum Neural Security

Whitepaper v2.0

Date: 2026-02-05
Version: 2.0.0

Table of Contents

1. Introduction

QNS (Quantum Neural Security) is a next-generation blockchain combining:

- **Neural AI** — BlockchainBrain for adaptive network optimization
- **10-cluster DAG** — GHOSTDAG ordering for maximum throughput
- **Post-quantum cryptography** — Dilithium3, Kyber1024 for quantum attack protection
- **Multi-VM architecture** — EVM, TVM and QVM for maximum compatibility
- **200,000+ TPS** — thanks to BlockSTM parallel execution

Key Metrics

Parameter	Value
TPS Target	200,000+
Block Time	1-2 sec
Finality	~3 sec

Parameter	Value
Validators	171 (3-tier)
DAG Clusters	10
QVM Opcodes	180+

2. Architecture

2.1 Block Structure

```
pub struct BlockHeader {
    // Basic fields
    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,

    // Validation (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,

    // Neural fields
    pub neural_activation: i128,
    pub neural_learning_rate: i128,
    pub neural_plasticity: i128,

    // DAG structure (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 Transaction Types

Type	ID	Description
Legacy	0	Pre-EIP-2718
AccessList	1	EIP-2930
EIP1559	2	Fee market
Transfer	3	Simple transfer
ContractDeployment	4	Contract deploy
ContractCall	5	Contract call
CrossShard	6	Cross-shard
Staking	7	Staking
Governance	8	Voting
NeuralProposal	9	Neural optimization

---

3. Consensus

Algorithm: Tendermint BFT (3-phase)

```
MECHANISM:
├─ Propose Phase      (waiting for leader proposal)
├─ Prevote Phase      (first voting round - 2/3+)
├─ Precommit Phase    (final voting round - 2/3+)
└─ Commit Phase       (block committed)
```

Consensus Phases

Phase	Purpose	Exit Condition
Propose	Wait for block from leader	Valid block received or timeout
Prevote	First voting	2/3+1 prevotes
Precommit	Final voting	2/3+1 precommits
Commit	Finalization	Automatic transition

Parameters

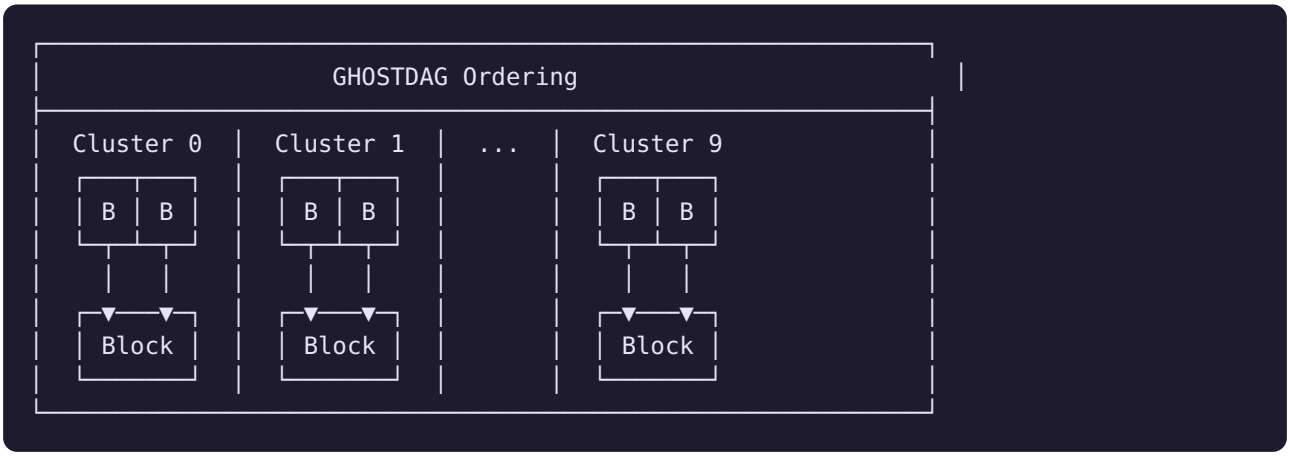
```
propose_timeout: 3 seconds
prevote_timeout: 2 seconds
precommit_timeout: 2 seconds
finality: ~3 seconds
```

---

4. Neural DAG with GHOSTDAG

4.1 Structure

QNS uses a 10-cluster Neural DAG with GHOSTDAG ordering:



4.2 GHOSTDAG Algorithm

- **Blue set selection**: Determining "honest" blocks
- **Blue score**: Metric for ordering
- **K-cluster parameter**: k=10 for optimal performance

4.3 DAG Parameters

Parameter	Value
Clusters	10
Maximum depth	60 (2^60 shards)
Parallel blocks per shard	10

5. Cryptography

5.1 Post-Quantum Algorithms

Algorithm	Purpose	Key Size	Signature Size	NIST Level
Dilithium3	Signatures	1952 bytes	3293 bytes	L5 (192-bit)
Kyber1024	Key Encapsulation	1568 bytes	1568 bytes	L5
SPHINCS+	Backup signatures	Variable	Variable	L5

5.2 Hybrid Signatures

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

Cryptography modes:
- `Classical` — DEPRECATED, Ed25519 only
- `Hybrid` — Ed25519 + Dilithium3 (for validators)
- `QuantumOnly` — Dilithium3 only (DEFAULT)

5.3 Hash Functions

Function	Usage	Quantum-resistant
BLAKE3	Blocks, state, consensus	Yes
Keccak256	EVM compatibility	No

---

6. Virtual Machines

6.1 Multi-VM Architecture

VM	Description	Workchain ID	Address Format
QVM	Quantum VM (native DeFi)	0	`quant...`
EVM	Ethereum VM (revm 14)	1	`0x...`
TVM	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 Primitives

7.1 AMM / Swaps

4 pool types:

Type	Formula	Use Case
Constant Product	x × y = k	Volatile pairs
Stable Swap	D curve (Newton)	Stablecoins
Concentrated Liquidity	Tick-based	Capital efficient
Weighted Pool	Π(B_i^w_i)	Multi-asset

7.2 Flash Loans

- **Fee:** 0.09% (9 BPS)
- **Requirement:** Repayment in same block
- **Protection:** Reentrancy guard per (borrower, asset)
- **Max per block:** 1000 loans

7.3 Lending

- **Model:** Compound-style

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

7.4 Oracle

- **TWAP window:** 30 minutes
- **Min observations:** 10
- **Max deviation:** 5% from TWAP

---

8. Validators

8.1 Three-Tier System

Tier	Minimum	Reward	Max Validators
Execution	10,000 QNS	1.0x	300
Neural	50,000 QNS	1.5x	150
Verification	100,000 QNS	2.0x	63

Total: Up to 513 validators (300+150+63)

8.2 Lifecycle

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

8.3 Slashing (Graduated Penalties)

Level	Violation	Penalty	Jail
Light	Downtime	0.1%	1 hour
Medium	Equivocation	5%	24 hours
Critical	DoubleVote	33%	7 days
Critical	CoordinatedAttack	100%	Permanent

Unbonding period: 7 days

---

9. BlockchainBrain AI

9.1 Components

Component	Purpose
`brain.rs`	BlockchainBrain — ML for optimization
`prediction.rs`	Gas, load, risk, MEV prediction
`learning.rs`	Hebbian, STDP, reinforcement learning
`memory.rs`	Sensory, working, episodic, semantic
`consciousness.rs`	Global Workspace Theory
`reasoning.rs`	Rule engine, causal graph
`attention.rs`	Multi-head self-attention
`meta_learning.rs`	Adaptive learning rates
`controller.rs`	Closed-loop network control

9.2 Determinism

100% deterministic computations:
- `NeuralScalar = I64F64` (128-bit fixed-point)
- Polynomial approximations (no exp/sin/cos)
- `BTreeMap/BTreeSet` (deterministic order)
- `NeuralRng` seeded from block hash

9.3 MEV Protection

- **Commit-Reveal:** two-phase protection
- **AI Detection:** sandwich attack prediction
- **Slippage protection:** Default 100 bps (1%)

---

10. Bridges

10.1 Supported Networks (10+)

Network	Type	Status
Ethereum	BLS aggregation	Production
Bitcoin	SPV light client	Production
BSC	EVM compatible	Production
Polygon	Checkpoint-based	Production

Network	Type	Status
TON	Cell-based proof	Production
Arbitrum	Optimistic	Active
Optimism	Optimistic	Active
Avalanche	Subnet	Active
Solana	Wormhole	Planned
XCM/IBC	Polkadot/Cosmos	Active

10.2 Mechanism

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

---

11. Tokenomics

11.1 Block Rewards

```
INITIAL_BLOCK_REWARD = 2 QNS
HALVING_PERIOD = 315,360,000 blocks (~10 years)

Distribution:
├─ 40% → Block Producer
├─ 40% → Attesters Pool
├─ 10% → Skynet Neural Fund
└─ 10% → Treasury/Faucet
```

11.2 Fees

```
├─ 50% → Validators (60% producer, 40% attesters)
├─ 25% → Burn (deflation)
└─ 25% → Treasury
```

---

12. Performance

12.1 Test Results

Test	TPS	Success
TPS Measurement	**293,983**	99.90%
Network Partition	2,417,397	100%

Test	TPS	Success
Byzantine Validators	562,870	100%
Neural Learning	15,749	95.40%
Cross-Shard	7,432,693	99.94%
Combined Chaos	**10,739**	**93.93%**

12.2 Key Findings

1. **Performance:**
   - Maximum TPS: ~294,000
   - Realistic TPS under chaos: ~10,700
   - P99 latency: < 2ms

2. **Security:**
   - 100% Byzantine attack detection
   - 100% slashing of malicious validators
   - BFT works at < 33% Byzantine

3. **Reliability:**
   - 99.94% cross-shard message delivery
   - Automatic recovery after partitions
   - No memory leaks

Conclusion

QNS represents a fully integrated Neural AI blockchain with:
- 200,000+ TPS potential throughput
- Post-quantum cryptographic protection
- 10-cluster GHOSTDAG DAG
- Up to 513 validators in 3-tier system (300+150+63)
- 180+ native QVM opcodes
- BlockchainBrain AI for adaptive optimization

QNS — Quantum Neural Security
Document Updated: 2026-02-05