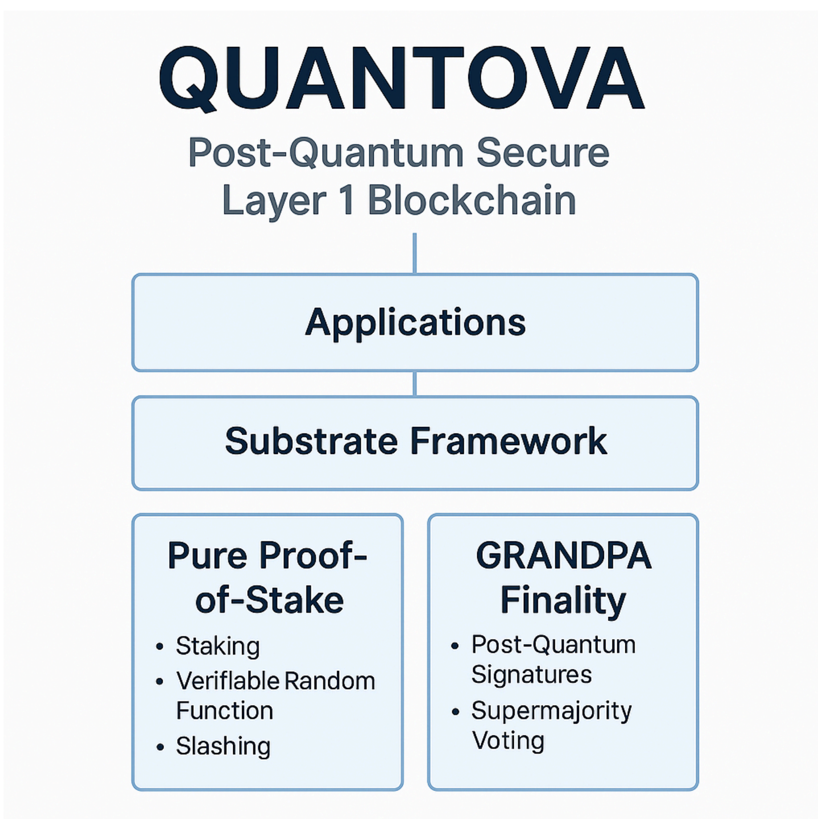
Quantova Network: Consensus Mechanism Report

1. Executive Summary

The Quantova Network is a next-generation Layer 1 blockchain designed to address the imminent security challenges posed by quantum computing. At its core, Quantova adopts a Pure Proof-of-Stake (PoS) consensus mechanism enhanced by GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) for deterministic finality. Built on the modular and extensible Substrate framework, Quantova achieves a high level of security, scalability, and sustainability. This document provides an in-depth technical and conceptual analysis of the Quantova consensus protocol, validator operations, fault tolerance mechanisms, security assumptions, and its integration with post-quantum cryptographic primitives.

The goal of this report is to enable transparent understanding, effective auditing, and seamless developer onboarding by detailing how consensus is achieved and maintained on Quantova.



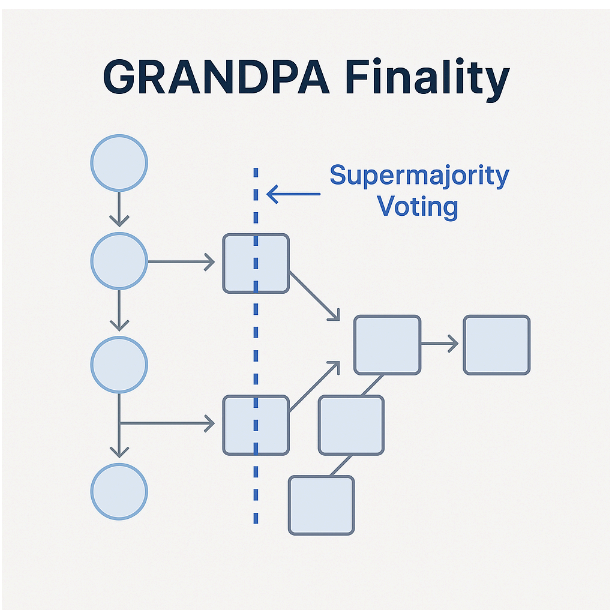
2. Consensus Mechanism Overview

2.1 Consensus Model

Quantova uses a Pure Proof-of-Stake (PoS) model where validators are chosen based on their stake in the network. This selection is probabilistic but influenced by Verifiable Random Functions (VRFs), ensuring fairness and unpredictability. The system is designed to be energy-efficient, scalable, and secure.

2.2 Finality Gadget: GRANDPA

Quantova implements GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) for finalizing blocks. Unlike traditional PoS chains that conflate block production and finality, GRANDPA decouples them, allowing blocks to be produced rapidly while a separate voting process ensures deterministic finality.



.

2.3 Key Design Goals

- **Security**: Ensure robust protection against both classical and quantum threats.
- **Scalability**: Enable high throughput via batch verification and efficient networking.
- **Decentralization**: Enable fair validator participation through PoS and community governance.
- **EVM Compatibility** – Supports Ethereum-style signatures, allowing developers to use tools like MetaMask, Remix, Hardhat, and Web3.js.

3. Consensus Protocol Details

3.1 Type

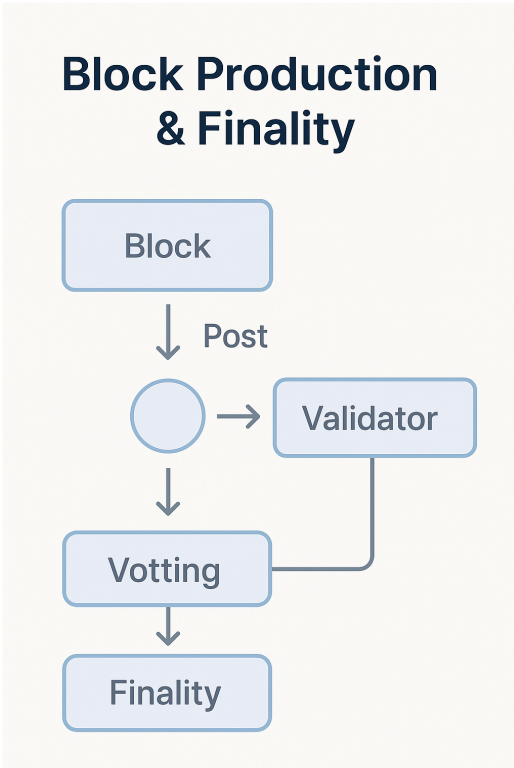
- **Base Model**: Pure Proof-of-Stake (PoS)
- **Finality Mechanism**: GRANDPA
- **Validator Selection**: Weighted by stake, randomized via VRFs

3.2 Finality

- **Mechanism**: GRANDPA supermajority voting
- **Determinism**: Once finalized, blocks are immutable
- **Recursive Guarantee**: Finalizing block B finalizes all its ancestors

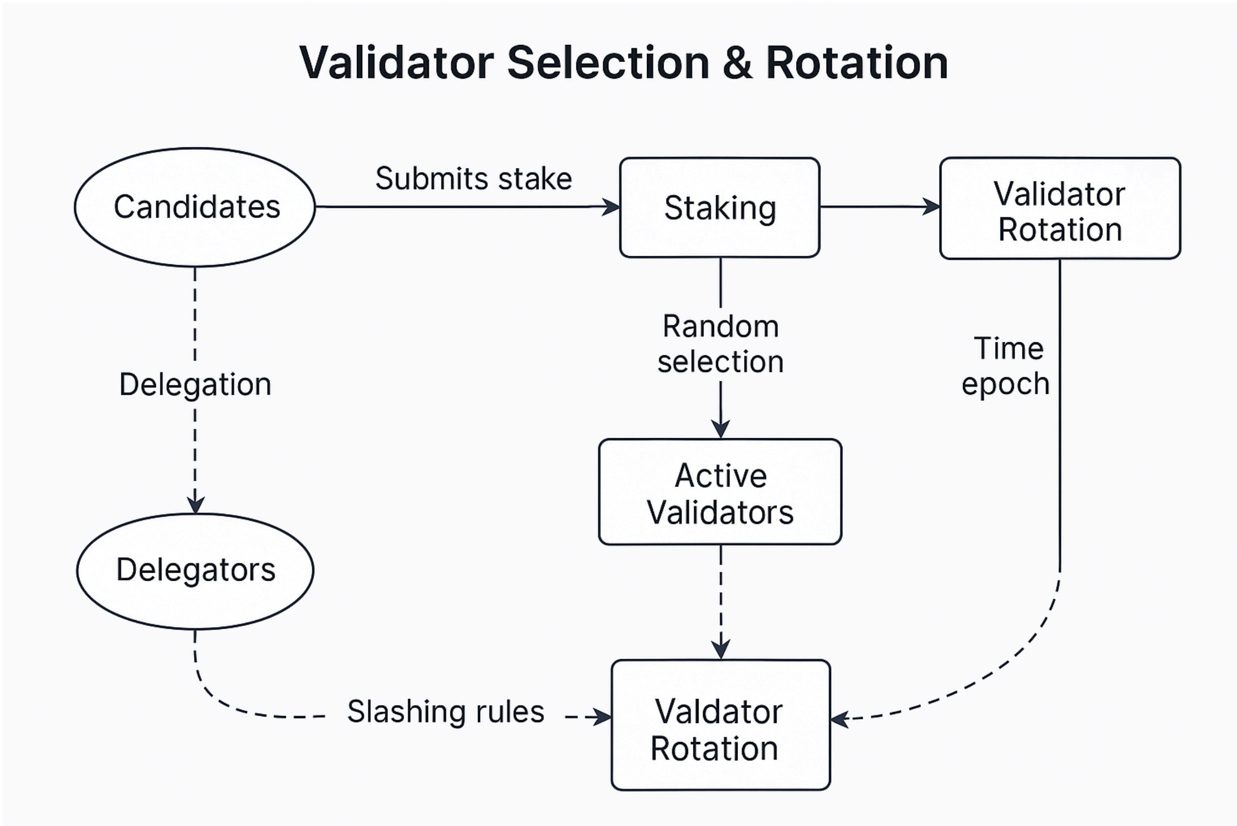
3.3 Block Production

- **Interval**: Fast, optimized for low-latency. Chain creates a block every 3 seconds.
- **Signatures**: Each block signed by the validator



3.4 Validator Rotation and Randomness

- **Selection**: Achieved using VRFs
- **Rotation**: Dynamically updated based on staking and randomness
- **Slashing Conditions**: Validators can be penalized for malicious behavior such as double-signing or prolonged downtime



3.5 Staking and Delegation

- **Minimum Stake**: Required to stake the fix QTOV tokens(eg 1000) to become a validator of the network.

- **Nominators:** Delegate stake to validators and earn rewards.

4. Validator and Node Participation

4.1 Eligibility

- Anyone with sufficient QTOV tokens can become a validator
- Must run a full node using Substrate-based node software
- **Hardware Requirements(Recommended)**
    - **CPU**: Multi-core processors
    - **RAM**: Minimum **16GB RAM**
    - **Storage**: SSD with at least **1TB capacity**
    - **Bandwidth**: High-speed internet connection with **low latency**

4.2 Validator Duties

- Block proposal and validation
- Participation in GRANDPA voting
- Maintaining node uptime and performance

4.3 Incentives

- **Rewards**: Transaction fees, block rewards, treasury incentives
- **Penalties**: Slashing of stake for malicious actions

4.4 Agreement Process

- Validators reach consensus by voting on blockchains they consider valid
- Blocks gain finality upon reaching a 2/3+ supermajority under GRANDPA

4.5 Setup

Compilation:

```
# Clone the repository

git clone https://github.com/Quantova/Quantova.git

cd Quantova
```

Build the node in release mode:

```
cargo build --release
```

Running a Node:

Local Development Network:

```
./target/release/quantova-node build-spec --disable-default-bootnode
--chain=local --raw > ./specs/local/customSpecRaw.json
```

Testnet:

```
./target/release/quantova-node build-spec --disable-default-bootnode
--chain=testnet --raw > ./specs/testnet/customSpecRaw.json
```

Mainnet:

```
./target/release/quantova-node build-spec --disable-default-bootnode
--chain=quantova-node --raw > ./specs/mainnet/customSpecRaw.json
```

Insert Consensus Keys (For Validators)

Insert AURA Key (Block Production)

```
./target/release/quantova-node key insert --base-path /tmp/node01 \

  --chain ./specs/customSpecRaw.json \

  --scheme Sr25519 \

  --suri <key> \

  --password-interactive \

  --key-type aura
```

Insert GRANDPA Key (Finality)

```
./target/release/quantova-node key insert --base-path /tmp/node01 \
  --chain ./specs/customSpecRaw.json \
  --scheme Ed25519 \
  --suri <key> \
  --password-interactive \
  --key-type gran
```

Start Validator Nodes

1.First Validator Node:

```
./target/release/quantova-node \
  --base-path /tmp/node01 \
  --chain ./specs/customSpecRaw.json \
  --port 30333 \
  --rpc-port 9945 \
  --validator \
  --rpc-methods Unsafe \
  --name MyNode01
```

Additional Validator Node

```
./target/release/quantova-node \
  --base-path /tmp/node02 \
  --chain ./specs/customSpecRaw.json \
  --port 30334 \
  --rpc-port 9946 \
  --validator \
```

```
  --rpc-methods Unsafe \
  --name MyNode02 \
  --bootnodes /ip4/127.0.0.1/tcp/30333/p2p/<node-key>
```

Run a Full Node (Non-Validator)

```
./target/release/quantova-node \
  --base-path /tmp/fullnode01 \
  --chain ./specs/customSpecRaw.json \
  --port 30335 \
  --rpc-port 9947 \
  --name FullNode01 \
  --bootnodes /ip4/127.0.0.1/tcp/30333/p2p/<node-key>
```

---

5. Security Assumptions

5.1 Honest Majority

- **GRANDPA** requires < 1/3 of validators to be malicious for safety to hold
- Assumes economic disincentive for attack (stake loss)

5.2 Resistance to Common Attacks

- **Sybil Attacks**: Inhibited by staking requirements
- **Censorship**: Mitigated by randomized validator selection
- **Reorganizations**: Prevented after finality through GRANDPA

---

6. Liveness and Fault Tolerance

6.1 Validator Downtime

- Validators can be temporarily or permanently removed based on activity
- Inactivity leads to missed rewards and potential slashing

6.2 Network Partitions

- GRANDPA finality halts until ≥2/3 validators reconnect
- No fork can finalize under 2/3 supermajority condition

6.3 Recovery

- Automatic recovery once validator quorum re-established
- Finality resumes and unfinalized blocks can be reverted if needed

7. Upgradability

- Built on Substrate, allowing runtime upgrades without hard forks

---

8. Observations and Network Metrics

8.1 Metrics

- Validator counts: Will be able to add that after proper testnet and mainnet release.
- **Block Propagation Time:**
  - **Description:** The average time taken for a newly created block to propagate across the network and reach the majority of validators.
  - **Importance:** Lower propagation times indicate efficient networking and contribute to shorter finality times, improving user experience and validator coordination.

    - Average Block Propagation Time: 1.5 seconds

    - Best Case: 0.8 seconds

    - Worst Case: 3.2 seconds

- **Block Production Interval:**
  - **Description:** Average and targeted intervals at which blocks are produced.
  - **Importance:** Indicates network efficiency and reliability. Consistency in block intervals demonstrates network stability.

    - Target Block Time: 3 seconds

    - Actual Average Block Time: 3.1 seconds

- **Finality Rate (Time to Finality):**

- **Description:** Time taken from block production until GRANDPA finalizes the block irreversibly.
- **Importance:** Critical for transaction settlement guarantees. A shorter finality rate indicates rapid transaction certainty, essential for financial and high-security applications.

  - Average Finality Time: 9 seconds (3 blocks)

  - Fastest Finality Time Observed: 6 seconds (2 blocks)

8.2 Sources for Metrics

- QuantovaScan
- Internal telemetry tools: prometheus and grafana

---

9. Codebase References

9.1 GitHub Repository

- Quantova GitHub

9.2 Mapping Theory to Code

Concept	Code Module
Validator Selection	BABE, staking pallet
Block Finality	GRANDPA

Slashing	staking/slash.rs
Chain node	Node

---

10. Summary and Conclusion

Quantova Network's consensus protocol represents a modern and forward-looking approach to blockchain governance and security. By integrating quantum-resistant cryptographic algorithms, using a deterministic finality protocol (GRANDPA), and operating under an energy-efficient Pure PoS model, Quantova ensures long-term viability against both classical and emerging threats.

Strengths:

- Quantum-safe security architecture
- Deterministic finality and rapid confirmation
- Scalable and upgradable via Substrate
- Fair validator selection with enforced slashing

Trade-offs:

- PoS systems rely on proper economic incentive design
- GRANDPA requires >2/3 quorum for finality, making partial network outages disruptive
- Currently lacks delegation support

Open Questions:

- How will governance evolve in response to community expansion?
- What thresholds should govern protocol parameter changes?

For more technical details and community discussion, refer to:

- Quantova Documentation
- Quantova Explorer
- Quantova GitHub