Boing Network — Security Standards

> ***Purpose:*** *Top-tier security across protocol, network, application, and operational layers.*
> ***References:*** *BOING-BLOCKCHAIN-DESIGN-PLAN.md, DEVELOPMENT-AND-ENHANCEMENTS.md (appendix: cryptographic verification)*

Table of Contents

---

1. Protocol-Level Security

1.1 Consensus (HotStuff BFT + PoS)

Measure	Description	Status
Byzantine Fault Tolerance	Network operates correctly with up to 1/3 malicious validators	✓ HotStuff
PoS + Slashing	Validators stake BOING; malicious behavior penalized	✓ Implemented
VRF Leader Selection	Unpredictable, unbiased leader election	Design / Roadmap
Equivocation Detection	Double-signing detected and slashed	✓ Consensus

1.2 Cryptography

Measure	Description	Status
Audited Primitives	Ed25519 signatures, BLAKE3 hashing	✓ In use
Secure Key Management	HD wallets, multi-sig for critical ops	Roadmap
Post-Quantum	Investigate quantum-resistant algorithms for long-term integrity	Research target

1.3 Smart Contract Security (Rust VM)

Measure	Description	Status
Memory Safety	Rust prevents buffer overflows, null derefs	✓ Core in Rust
Formal Verification	Mathematical proof for critical contracts (staking, DeFi, automation)	Roadmap
Continuous Audits	Independent audits of core protocol and contracts	Roadmap

1.4 State Management (Verkle Trees)

Measure	Description	Status
Data Integrity	Verkle trees for compact proofs; smaller, verifiable state	✓ Sparse Merkle
Stateless Clients	More participants can validate without full state	✓ Proof APIs

---

2. Network-Level Security

2.1 P2P Layer

Measure	Description	Status
Decentralized Bootstrapping	DHT + gossip-first; bootnode rotation	Roadmap
Encrypted Transport	Noise + TLS over TCP (libp2p)	✓ libp2p
DDoS Resistance	HTTP RPC rate limits (`RateLimitConfig`); P2P **per-IP connection cap** (`--max-connections-per-ip`); gossip payload signature verification before mempool	✓ See RUNBOOK.md §8.1, TECHNICAL-SPECIFICATION.md §12.3
Gossip integrity	Signed tx gossip (`SignedTransaction`); invalid signatures dropped	✓ `boing-node` P2P ingest
Sybil / Eclipse Mitigation	Reputation, stake requirements, diverse connections; partial relief via per-IP connection limits	Partial / roadmap

2.2 Client Diversity

Measure	Description
Multiple Implementations	Encourage independent clients (different languages/teams)
Rationale	Single client bug cannot compromise entire network

---

3. Application-Level Security

3.1 Boing SDK

Measure	Description
Secure Defaults	Guide developers toward secure patterns
Integrated Security Tools	Static analysis, vulnerability scanning, testing
Human-Readable Signing	Users understand what they authorize

3.2 Decentralized Automation

Measure	Description	Status
ZKPs / Fraud Proofs	Verify off-chain execution	Design in DEVELOPMENT-AND-ENHANCEMENTS (appendix)
Decentralized Oracles	External data via decentralized oracle networks	Roadmap
Executor Incentives & Slashing	Economic alignment for honest execution	✓ ExecutorIncentive

3.3 User-Facing Security

Measure	Description
Account Abstraction	Smart-contract wallets; MFA, limits, spending policies
Social Recovery	Recovery without single seed phrase; guardians, time locks

---

4. Operational Security & Governance

4.1 Audits & Bug Bounties

Measure	Description
Continuous Audits	Multiple independent firms; core protocol and new features
Bug Bounty Program	Generous rewards for responsible disclosure
Scope	Consensus, execution, automation, bridges

4.2 Governance

Measure	Description	Status
Phased Upgrades	Proposal → Cooling → Execution	✓ boing-governance
Community Vetting	Security-critical changes reviewed by community	
No Central Control	Parameter and upgrade control decentralized	

4.3 Transparency & Incident Response

Measure	Description
Transparency	Public security posture, audit reports, incidents
Incident Response Plan	Clear, tested process for vulnerabilities and attacks
Communication	Fast, accurate disclosure to users and ecosystem

---

5. Security Contacts

Channel	Use
Security advisories	GitHub Security Advisories — for responsible disclosure of vulnerabilities
Bug bounty	*TBD — program to be announced with incentivized testnet*
Incident response	See RUNBOOK.md §6; severity-driven communication

For vulnerabilities: Please report via GitHub Security Advisories. Do not open public issues for security-sensitive findings.

Security Checklist

- [ ] VRF/VDF for leader selection
- [ ] Post-quantum cryptography research
- [ ] Formal verification for critical contracts
- [ ] Continuous external audits
- [ ] Bug bounty program
- [x] DDoS resistance (RPC rate limits, mempool per-sender cap)
- [ ] Sybil/eclipse mitigation in P2P
- [ ] SDK security tools (static analysis, scanning)
- [x] Incident response runbook (RUNBOOK §6)

Boing Network — Authentic. Decentralized. Optimal. Sustainable.