DANP

DUAL AUTHENTICATION NODE PROTOCOL

TECHNICAL WHITE PAPER

Working Draft v0.2 | November 2026

Research-stage design document. Not a production security certification, investment offering or promise of future token delivery.

Contents

01. Executive overview

02. Design goals and trust model

03. Node A: transaction execution

04. Node B: independent authentication

05. Witness participation, consensus and finality

06. Native coin and ledger accounting

07. Wallets, authorization and recovery

08. DASP: autonomous agent settlement

09. Sentinel and Red Team AI

10. Throughput, latency and scalability

11. Persistence and fault recovery

12. Threat model and open security work

13. Institutional and public applications

14. Infrastructure, governance and rollout

15. Development status and publication note

01. Executive overview

DANP (Dual Authentication Node Protocol) is a proposed standalone Layer-1 public blockchain. Its design separates transaction execution from independent authentication and adds a witness/finality mechanism. The long-term aim is secure, auditable settlement for individuals, institutions and automated agents. The protocol is in research and prototype development; none of its security or throughput objectives should be read as demonstrated production guarantees.

02. Design goals and trust model

DANP seeks to minimize unilateral authority over finalized transactions. Node A, Node B and witness participants have distinct responsibilities, but decentralization depends on independent operators, validator membership rules, secure key management and a fully specified consensus algorithm. No single AI service or privileged wallet should be able to alter consensus or rewrite finalized state.

03. Node A: transaction execution

Node A is the proposed execution and block-production role. It receives authenticated transactions, checks balances, nonces, fees and transaction validity, constructs candidate blocks and proposes deterministic state transitions. Node A cannot independently declare finality. Block production, scheduling, resource limits and leader replacement remain subjects for specification.

04. Node B: independent authentication

Node B is intended to independently verify the proposed block, transaction signatures, policy requirements and state transition. Its approval is a separate control from Node A execution. An independently operated validator set, rather than one permanent centrally controlled Node B, is required to meet stronger fault-tolerance goals.

05. Witness participation, consensus and finality

A witness/finality layer is planned to resolve Node A/Node B disagreements and avoid unilateral chain stoppage. Proposed controls include signed votes, quorum certificates, locking, timeout handling and validator rotation. However, the exact quorum thresholds, Byzantine fault assumptions, view-change procedure, equivocation handling and finality rules have not been formalized into a verified BFT protocol. A complete specification and independent proof/review are prerequisites for production.

06. Native coin and ledger accounting

The proposed native asset is DANP, with a planned genesis supply of 10,000,000,000 DANP on one public chain. Public and institutional users hold the same native asset. The final genesis allocation, validator rewards, fee mechanics, supply controls, address format and state model are not finalized. This technical paper deliberately excludes presale prices, fundraising targets and offering terms.

07. Wallets, authorization and recovery

The roadmap includes desktop, Android and iOS wallets, cryptographic transaction signing, replay protection, nonce management, multisignature and threshold approval. Institutional users may optionally use hardware security modules, role-based permissions and spending policies. A cryptographically protected Node A recovery block and threshold-based recovery procedure are proposed; exact recovery governance and attack-resistance remain to be designed and audited.

08. DASP: autonomous agent settlement

DANP Agent Settlement Protocol (DASP) is a proposed payment layer for AI agents and machine-to-machine commerce. It envisions verifiable agent identities, owner-constrained wallets, policy-based spending limits, conditional/escrow payments, proof-of-service receipts, request/result hashes, auditable settlement and micropayment channels. Agents cannot override human-defined authorization limits, bypass consensus or independently move protected funds.

09. Sentinel and Red Team AI

DANP Sentinel is proposed as a defensive observer for network telemetry, authentication failures, anomalous transaction sequences, policy-bypass attempts and infrastructure health. A separate Red Team AI would attack isolated test environments and new builds. Neither system should hold signing keys for user funds, finalize blocks, rewrite chain history or change consensus rules. Automated findings require independent verification.

10. Throughput, latency and scalability

DANP targets fast settlement without sacrificing safety. Proposed techniques include transaction batching, efficient verification, controlled concurrency, network-aware block propagation and future payment channels. Earlier local computational benchmarks are not end-to-end network throughput or finality measurements. Production claims require geographically distributed testing, realistic workload mixes, storage durability and adversarial load measurements.

11. Persistence and fault recovery

The experimental roadmap has tested signed commitments, ledger replay, checksummed journals, snapshots, simulated interrupted writes, validator restart and signed equivocation evidence exchange. Production storage needs atomic write-ahead logging, rollback resistance, verified checkpoints, independent backups, crash/power-cut testing and formal state-machine invariants. A checksum alone is not a defense against an attacker with disk-write access.

12. Threat model and open security work

Priority threats include double-signing, equivocation, validator collusion, compromised keys, replay, denial of service, network partitions, forged certificates, software supply-chain compromise, rollback and governance capture. Required work includes authenticated peer networking, secure validator identity and key rotation, BFT view changes, anti-censorship and liveness analysis, fuzzing, formal methods and independent audits.

13. Institutional and public applications

DANP is intended for public payments and asset transfers, institutional settlement, policy-constrained treasury operations and agent payments. Institutional-grade wallet controls are optional account-layer capabilities, not a privileged coin class. Any regulatory, privacy, custody and interoperability requirements must be addressed per deployment and jurisdiction.

14. Infrastructure, governance and rollout

The long-term vision includes independent DANP infrastructure and operator-managed servers, with resilient multi-site operation. Before launch, DANP needs transparent validator governance, protocol upgrade rules, incident response, monitoring, disaster recovery, testnet participation, security disclosures and operational service targets. Concentration of validator authority must be measured and mitigated.

15. Development status and publication note

The DANP prototypes have passed selected automated local tests through Stage 43, including four-process signed evidence relay and journal recovery experiments. These tests do not constitute a production blockchain, independent audit, certified BFT finality, real-funds safety or guaranteed mainnet delivery. This document is a technical working draft, not a securities offering memorandum, token purchase agreement or investment solicitation. Financial and presale documents will be separate.