DRACHMA (DRM) Whitepaper

Introduction
Drachma is a minimalist proof-of-work cryptocurrency engineered for predictable issuance, transparent accounting, and conservative security assumptions. The protocol follows a Bitcoin-class model with SHA-256d proof-of-work, Schnorr signatures, a UTXO ledger, and straightforward networking. The design prioritizes determinism, reproducibility, and reviewability over novelty while maintaining production-grade operational expectations.

Monetary Policy
- **Max supply:** 42,000,000 DRM
- **Genesis premine:** None; the genesis coinbase is provably unspendable.
- **Block subsidy:** 50 DRM initially, halving every 210,000 blocks.
- **Block interval:** 60 seconds target.
- **Reward maturity:** Coinbase outputs require standard maturity before spending.
- **Fee model:** Transaction fees are collected by miners and are the only reward after subsidy exhaustion.

The subsidy schedule follows integer division at each halving height, and cumulative supply accounting enforces the hard cap through consensus validation. Supply range checks and overflow prevention are part of transaction and block validation.

Consensus Overview
1. **Proof-of-Work:** SHA-256d over the block header. Difficulty retargets every 60 blocks using a 3,600-second target window with ±25% clamp per period. Mainnet disallows minimum-difficulty blocks; testnet permits them when timestamps drift beyond the retarget window.
2. **Blocks:** Contain version, previous hash, Merkle root, timestamp, nBits, nonce, and transactions. Merkle roots duplicate the final leaf for odd layers to preserve deterministic tree construction.
3. **Transactions:** Deterministic serialization with tagged SHA-256 (BIP-340 style) for transaction IDs. Only Schnorr signatures over secp256k1 are valid; no ECDSA fallback exists. Scripts are minimal, non-Turing-complete, and forbid loops and recursion.
4. **Validation:** Nodes verify proof-of-work, header linkage, Merkle consistency, input availability, signature validity, coinbase maturity, fee correctness, and money-range constraints. Blocks failing any rule are rejected deterministically.

Genesis Block
The genesis block includes an unspendable coinbase with a commitment string documenting the chain launch. The Merkle root is derived from this single transaction. The genesis header is mined so its double-SHA-256 hash meets the encoded difficulty target. No special launch or checkpoint logic exists; the chain starts normally from height 0.

Network
Drachma uses TCP-based peer connections with custom magic bytes per network (mainnet/testnet). Peers relay headers, transactions, and blocks respecting fee and size policies. DNS seeds and static seed nodes assist initial bootstrapping; bootstrap.dat import accelerates initial sync without bypassing validation.

Wallet Model
Wallets are local-only HD wallets producing Schnorr keypairs. Seeds are 24-word mnemonics; private material is encrypted on disk using AES-256. The wallet tracks UTXOs, constructs

transactions using fee estimation from mempool policy, and signs inputs with Schnorr.

Security Considerations

- Deterministic serialization and tagged hashing reduce malleability risk.
- Schnorr signatures and constant-time verification mitigate timing leaks.
- Difficulty clamping prevents large oscillations while retaining responsiveness.
- UTXO set updates are atomic per block and reorg-safe through rollback metadata.
- No governance, staking, or admin keys exist; all participants follow the same rules.

Cross-Chain Support (Layer 2)

Cross-chain components operate off-consensus. Proof-based adapters validate external chain headers and Merkle proofs to inform relayers and wallets, but Layer 1 state is never altered by cross-chain messages. Relayers are untrusted; users must verify proofs locally.

Conclusion

Drachma delivers a conservative, auditable proof-of-work system with clear monetary bounds and a minimal feature set. The layered architecture isolates consensus from services and UI, enabling independent review and safe extensibility without compromising core security guarantees.