Modcoin: A Peer-to-Peer Electronic Cash System

Dual-Engine Proof-of-Work Design Proposal

Version 0.1 · 5 November 2026 · Design proposal

Abstract. Modcoin is proposed as an independent Proof-of-Work Layer-1 with a maximum supply of 42,000,000 MOD, a shared UTXO ledger, two separately accounted 21,000,000 MOD issuance pools, and authenticated peer networking. The design goal is that compromise of either mining engine alone must not be sufficient to rewrite settled transaction history. This is a security objective requiring a formal consensus design and evidence; it is not established merely by using two source-code lineages or alternating block slots. No mainnet, production wallet, DEM settlement, or $MONEY issuance currently exists.

1. Goals and Non-Goals

- One native currency and one canonical UTXO ledger.
- Two independently budgeted PoW issuance engines, each capped at 21 million MOD.
- PGP-based peer identity proof bound to an encrypted session.
- Settlement policy that resists a single-engine rewrite, with explicit liveness behavior.
- A future DEM for supported Modcoin ecosystem assets.
- A proposed AUD/USD-denominated $MONEY design whose issuance and fiat rails are not live.

Modcoin does not inherit Bitcoin or DigiByte network hashpower, security, user balances, or transaction history. Copying code does not create those properties.

2. Monetary Policy

Proposed maximum supply: 42,000,000 MOD, divided into an issuance cap of 21,000,000 MOD for each engine. Every validating node must enforce both caps and their combined limit through consensus state, including subsidy and any future issuance mechanism. Unclaimed or rounded-away rewards should remain unissued rather than be reallocated without an explicit rule.

A candidate subsidy model is 2.5 MOD per engine block, halving every 4,200,000 blocks of that engine. The geometric series has a theoretical maximum of 21,000,000 MOD per engine before integer rounding. This is a candidate parameter, not an adopted rule. The design must define coin precision, rounding, genesis allocation, fees, subsidy validation, and behavior at zero subsidy.

3. Proposed Dual-Engine Chain

The target average interval is 15 seconds. A proposed strict alternating schedule gives each engine a 30-second target and approximately 120 blocks per hour, for about 240 total blocks per hour. Those are statistical targets. Alternation risks chain-wide stoppage if either engine cannot produce its required block. A fallback rule cannot silently let one compromised engine control settlement; any liveness escape must state what security property is weakened and how users are protected.

Engine	Issuance Cap	Candidate Work	Difficulty Lineage
Bitcoin-derived	21,000,000 MOD	SHA-256d	Bitcoin-style retargeting
DigiByte-derived	21,000,000 MOD	SHA-256d, Scrypt, Skein, Qubit, Odocrypt	MultiShield-derived; new-chain validation required

DigiByte’s candidate algorithm list includes SHA-256d, creating overlap with the Bitcoin-derived engine. The protocol must define algorithm-domain separation, valid engine/algorithm schedules, work normalization, difficulty bounds, and how the same physical hashpower is treated. “Five algorithms” and an adjustment algorithm are separate concepts: MultiShield adjusts difficulty; it is not a mining algorithm.

4. Fork Choice and Settlement

A single scalar chainwork measure is insufficient unless it has a defined security interpretation across all eligible algorithms and enforces both engines' contribution. A viable specification must define:

1. Consensus validity and per-engine block eligibility.
2. Engine-specific difficulty adjustment and minimum/maximum retarget constraints.
3. Fork-choice ordering for branches with uneven or missing engine contributions.
4. A settlement/finality rule that requires independently validated contributions from both engines over a stated window.
5. Reorganization bounds, checkpoint governance if any, and recovery behavior after partitions or software upgrades.
6. How nodes reject forged, replayed, stale, or incorrectly attributed work.

The protocol must be modeled against adaptive hashpower, rented mining, algorithm overlap, network partitions, eclipse attacks, time manipulation, and one-engine compromise. "Both engines contribute" must be measured mathematically; counting blocks alone is not proof of security.

5. Shared UTXO Ledger

Both issuance engines would create native MOD outputs in one ledger. All full nodes must apply identical transaction, script, signature, subsidy, and supply validation rules, irrespective of which engine mined a block. Wallet balances are derived from unspent outputs, not an editable account balance. Native address encoding, script versions, signature algorithms, dust rules, fee policy, mempool behavior, and transaction malleability protections remain to be specified and tested.

6. Peer Authentication and Networking

PGP Proof of Possession can authenticate that a peer controls a signing key when it signs a fresh challenge. The signed challenge should include nonces from both peers, protocol version, both public-key fingerprints, a connection/session binding, and expiration. The authenticated exchange should run inside a reviewed encrypted transport. Key discovery, revocation, rotation, bootstrap peers, privacy, rate limiting, and anonymous-node policy need documented rules.

Peer authentication does not prove honesty, prevent Sybil identities, validate blocks, or protect a compromised endpoint. Consensus validation remains authoritative.

7. DEM — Decentralized Exchange Mechanism

The proposed Decentralized Exchange Mechanism (DEM) is intended to facilitate non-custodial exchange among supported native assets. A signed order is only an expression of intent; it does not itself lock funds, guarantee atomic execution, validate another chain, or settle trades. DEM needs a fully specified matching/market protocol, escrow or atomic-swap construction, cancellation and timeout paths, fee model, failure recovery, market abuse controls, and independent audits before handling value.

BTC-on-Modcoin or DGB-on-Modcoin would be distinct Modcoin-native representations unless a secure verification and redemption mechanism is implemented. They are not native BTC or DGB merely because of their labels.

8. Proposed $MONEY AUD/USD Units

$MONEY is a proposed pair of AUD- and USD-denominated digital units intended for use within DEM. The concept contemplates acquiring AUD units with AUD fiat and USD units with USD fiat, trading between them, and using them for DEM markets. No issuer, reserve, fiat gateway, redemption promise, peg, or token contract is currently established by this proposal.

Before launch, the project would need to decide who issues and redeems each unit, the legal claims held by users, reserve custody and reconciliation, insolvency treatment, audit/attestation cadence, payment partners, consumer disclosures, access controls, AML/CTF responsibilities, and whether the instrument and service require authorisations

in each market. A “decentralized” label does not settle those questions.

9. Security Model and AI-Era Threat Framing

The project aims to make automated attacks more costly and easier to detect through conservative consensus validation, peer authentication, rate/resource controls, signed releases, reproducible builds, independent review, and monitored public infrastructure. AI can increase attack scale and speed, but it does not by itself break sound cryptographic primitives. Practical risks include compromised keys, exploitable implementation bugs, hashpower concentration, social engineering, software supply-chain compromise, denial of service, and unsafe upgrade coordination.

The design objective is: compromising one mining engine should not be sufficient to rewrite confirmed Modcoin transaction history. The phrase “confirmed” must be tied to a precisely specified settlement condition. No security claim should be published as achieved until adversarial analysis and independent audits support it.

10. Wallets and Applications

Desktop, browser extension, Android, and iOS wallets are planned. Production wallet releases require finalized transaction/address formats, secure key generation and storage, encrypted backup and recovery, safe transaction review/signing, node connectivity, network identity verification, update signing, and incident response. UI mockups or shells are not wallets and must not display fictitious balances or accept real funds.

11. Launch Gates

1) Freeze consensus specification and independent review of both source lineages.
2) Implement deterministic validation and tests for every engine, reward cap, replay boundary, and fork case.
3) Model chainwork, finality, liveness, partitions, and single-engine compromise.
4) Run public testnet with diverse miners, nodes, pools, and signed releases.
5) Complete third-party security audits and fix findings before mainnet.
6) Build explorer and node directory from independently verified node data.
7) Complete wallet audit and recovery drills.
8) Complete legal and operational review before DEM or fiat-backed $MONEY.

12. Current Status

The initial supplied file was a static landing page. The subsequently supplied v0.2.0 archive contains a Go testnet node, persistent prototype UTXO chain, command-line wallet, local dashboard, and PGP-authenticated TLS peer prototype. It does not integrate Bitcoin Core or DigiByte Core; its DigiByte-derived engine is Scrypt-only, proof targets are fixed and trivial, and its local reorganization lock is not global finality. A v0.3.0 wallet-dashboard source draft adds local send/receive and transaction-history screens but has not been compiled. No mainnet, production wallet, public chain data, DEM settlement, or real-funds use is claimed.

References

• DigiByte Core source repository — verify the exact upstream release and active consensus rules used for any fork.

• Bitcoin Core source repository — verify the exact upstream release and active consensus rules used for any fork.

• ASIC INFO 225: Digital assets — financial products and services — legal classification depends on the product and activities; obtain current qualified advice.

This document defines a proposed architecture and open engineering requirements. It is not proof that a production network exists. Consensus, finality, and production software remain under development.