Credits (CRDT) — Technical Whitepaper

Version 1.0 (draft)

Date 2026-02-04

Base Credits Core / CRDT

> **Purpose of this document.** This whitepaper describes the design and vision of **Credits (CRDT)**: a PoW blockchain based on Bitcoin Core with its own identity, tuned parameters, and a roadmap for “Projects” (funding/impact) and advanced capabilities (tokens and smart contracts) planned for later phases.

Table of contents

1. Executive summary

Credits (CRDT) is a Layer-1 digital money network inspired by *sci-fi / cyberpunk* aesthetics and narrative, where the concept of *credits* is used as a universal currency. CRDT is a **Blockchain Crypto-currency**, preserves the **UTXO** model and a conservative validation approach, and defines a clearly separate network identity.

Main features

- **SHA256d PoW (ASIC-friendly)**: security based on hashrate and specialized mining.
- **Faster confirmations**: 5 min block target and retarget every 120 blocks (10h).
- **Own identity**: separate network (magic bytes, ports, bech32 HRP) and independent branding.
- **Projects in the wallet**: proposals and funding surfaced in the wallet to support research initiatives (medical/AI/technology/urbanism) with real-world impact in mind (e.g., tech ecosystems like Akihabara).
- **Open governance**: public GitHub, PR-based development, and wallet-based prioritization/voting (signature-based MVP; on-chain evolution planned).
- **Tokens, smart contracts and asset APIs (roadmap)**: planned integration of tokens and smart contracts (via native L1 tokens or an EVM sidechain/L2) and APIs for creation/management of new assets.

In addition, CRDT defines an ecosystem vision where funding and coordination of projects (medical, AI, urbanism, technology culture, etc.) is displayed and operated from the wallet via proposals and voting, with open development on GitHub.

Note: "Ethereum-like" tokens and smart contracts are planned for later phases, prioritizing a stable, secure and production-operable L1 first.

2. Vision, narrative and goals

2.1 Inspiration and branding

The **Credits** brand is grounded in sci-fi/cyberpunk imagery, where *credits* function as a global medium of exchange. CRDT aims to capture that identity on top of a proven technical base (Bitcoin Core), avoiding unnecessary complexity in consensus.

2.2 Impact objective ("Projects")

The network aims to become an open infrastructure that, beyond serving as digital money, enables:

- **Funding** for projects (medical, AI, science/technology, urbanism).
- **Transparency**: proposals visible from the wallet, traceability of contributions and outcomes.
- **Open governance**: public repository; PR-driven improvements; wallet-based voting and prioritization.

2.3 Design principles

Principle	What it means in CRDT
Security first	Conservative consensus (UTXO + Script), explicit and auditable changes, minimizing attack surface.
Independent network	Separate network identity: magic bytes, ports, bech32 HRP, datadir and branding.
Operability	Reproducible releases, stable Linux nodes, monitoring and deployment documentation.
Extensibility	Clear roadmap for Projects, APIs and (later) tokens and smart contracts.

3. L1 technical specification (CRDT)

> **Note.** The parameters described here reflect the current state of the project code. For values not explicitly modified, CRDT inherits Bitcoin Core behavior.

3.1 Consensus model

- **Model**: Proof of Work (PoW)
- **Algorithm**: SHA256d (ASIC-friendly)
- **State model**: UTXO
- **Validation**: Script / Taproot (per inherited Bitcoin Core rules)

3.2 Block target and retarget

- **Target**: `nPowTargetSpacing = 5 minutes`
- **Adjustment interval**: `120 blocks`
- **Target window**: `10 hours`

Operational implications:

- Faster confirmations than 10 min blocks.
- More frequent retarget: reacts faster to hashrate changes, but can be more sensitive when early hashrate is low.
- Recommendation: conservative confirmation policies for integrations (exchanges/bridges) in early stages.

3.3 Network identity

Item	Value
Ticker	`CRDT`
Magic bytes / message start	`0x43 0x52 0x44 0x54`
P2P mainnet	`29444`
RPC mainnet	`29442`
bech32 HRP (mainnet)	`crdt`

3.4 Addresses and formats

CRDT supports typical Bitcoin Core formats, with a distinct identity (bech32 HRP and base58 prefixes).

3.5 Genesis block

Phrase (timestamp):

```
JapanTimes 2026/02/03 Where will Japan's democracy go from here? Some predict that the ruling coalition of the Liberal Democratic Party and the Japan Innovation Party could gain momentum and win a majority in the Lower House of the parliament.
```

To support the long genesis phrase, the maximum coinbase `scriptSig` limit was increased at the consensus level.

4. Economics and issuance

4.1 Block subsidy and halvings

CRDT inherits Bitcoin Core's subsidy schedule:

- **Initial subsidy**: 50 CRDT (genesis uses `50 * COIN`).
- **Halving**: every `210,000` blocks (mainnet).

Important implication: with 5 min blocks, a halving occurs approximately every ~2 years (not ~4). This accelerates issuance "per unit of time" compared to Bitcoin, although the asymptotic supply remains in the ballpark of the classic schedule.

> **Future decision:** if the goal is to keep halvings at ~4 years, the halving interval (in blocks) must be adjusted. It should be decided early to avoid late economic changes.

4.2 Fees

Transaction fees follow the inherited Bitcoin Core model: they are paid in CRDT and awarded to the miner of the block that confirms the transaction.

5. Security and operations

5.1 Early risks (bootstrap)

In early stages, the biggest risk is low hashrate (reorgs, 51%, oscillations). Mitigations:

- Mining bootstrap (allied pools/miners).
- Reference nodes and monitoring.
- Conservative confirmation recommendations for integrations.
- Seeds/fixed seeds to improve connectivity.

5.2 Privacy

CRDT inherits the UTXO model: privacy depends on wallet practices (avoid address reuse, coin control). Taproot reduces information leakage, but the network is not “anonymous” by default.

6. Projects in the wallet: proposals, voting and funding

6.1 Goal

Integrate a **Projects** tab in the wallet to:

- Display proposals and progress (milestones, budget, outcomes).
- Fund projects transparently.
- Vote on development priorities and new features (via the GitHub process).
- Supply Tech projects or districts (Akihabara, Oosaka, SanFrancisco) of Economics and tokenized

6.2 MVP: signed feed + signature-based voting

Proposals (verifiable chain): a JSON catalog (HTTPS/IPFS) signed cryptographically by a known set of public keys.

Votes: users sign a message from the wallet; the backend counts votes (with anti-spam measures) and publishes results.

> **MVP advantage:** no consensus changes required, enables fast UX iteration, and avoids on-chain spam.

6.3 On-chain evolution

Options (to be specified later): on-chain commits with rate limits, voting with timelocked UTXOs, or mechanisms with explicit cost (burn vote).

6.4 Funding models

- **Voluntary donations** (no consensus changes).
- **Foundation/Multisig** (transparency and auditing; social governance).
- **Coinbase treasury** (share of subsidy/pre-mining shares): Supply projects to economy resources.

7. Tokens and smart contracts (roadmap)

7.1 Bitcoin-style smart contracts (already available)

CRDT (by inheriting Bitcoin Core) supports conservative contracts based on Script/Taproot:

- Multisig and complex policies (Taproot).
- Timelocks: CLTV/CSV.
- Hashlocks/HTLCs (swaps/channels).

This enables conditional payments, escrow, swaps and channels, but does not replace an EVM-like VM.

7.2 Tokens: three paths

Path	What it is	Advantages	Cost/Risks
1) Native L1 tokens	Multi-asset UTXO (outputs with `asset_id` + `amount`)	Consensus-native and verifiable; first-class UX	Deep changes in Core/wallet/RPC/DB; economic and fee design
2) Parallel EVM chain	EVM sidechain/L2 with a bridge (CRDT ↔ wCRDT)	Ethereum tooling; ERC tokens; configurable speed	Bridge is critical (initially federated); added operational complexity
3) Overlay + indexer	Interpreted tokens (OP_RETURN/commits) outside consensus	Fast, minimal consensus risk	Not “native”; depends on specific indexers/wallets

8. APIs and integrator stack

8.1 Node RPC

Future extensions for assets and Projects (if integrated into the node stack), while keeping compatibility and security.

8.2 Public API (REST) + indexer

Gateway service for an explorer, project feed, voting and web/mobile endpoints.

8.3 SDKs

SDKs for signing/verification, lightweight wallet creation and (future) bridging to an EVM chain.

9. Roadmap

Phase 1 — Base infrastructure

- Reproducible builds (Windows/Linux) and packaging.
- Linux nodes + seeds/fixed seeds.
- Basic explorer + network status API.
- Operations guides (systemd, hardening, backups).

Phase 2 — Projects in the wallet (MVP)

- Projects tab with a signed feed.
- Signature-based message voting.
- Transparency panel (funds, milestones, outcomes).

Phase 3 — Tokens and smart contracts

- Select a path (native L1 tokens vs. EVM sidechain vs. overlay).
- Implementation + audit + public testnet.

Phase 4 — SDK & Collaboration in Chain (Core)

- Provide a SDK to operate and integrate new models of interact between different networks
- Everyone will be capable to modify if the consensus agree any part of this chain and core

10. Glossary

Term	Short definition
UTXO	Model where “unspent outputs” represent state and balances.
PoW	Proof of work; security based on hashrate and energy cost.
SHA256d	Double SHA-256; the PoW algorithm used by Bitcoin.
Retarget	Difficulty adjustment to keep the target block time.
Taproot	Upgrade improving script privacy/expressiveness and efficiency.
EVM	Ethereum Virtual Machine for executing smart contracts.
Bridge	Cross-chain bridge for moving value (lock/mint and burn/unlock).
wCRDT	Wrapped CRDT on an EVM chain, represented 1:1 with CRDT locked on L1.

11. Appendices (current parameters)

11.1 Main parameters

Parameter	Value
Ticker	`CRDT`
nPowTargetSpacing	`5 min`

Parameter	Value
DifficultyAdjustmentInterval	`120 blocks`
nPowTargetTimespan	`10 hours`
P2P mainnet	`29444`
RPC mainnet	`29442`
bech32 HRP (mainnet)	`crdt`

12. References

- S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”.
- Bitcoin Core documentation (consensus, Script, Taproot/BIPs).
- V. Buterin, “Ethereum Whitepaper”.

From Japan whit love ありがとうございます。