# Preface

Original (ZH): 前言

SAT20协议白皮书
SAT20协议
概述
SAT20是一个"聪本位(Satoshi Standard)"的BTC原生资产发行和流通协议，其核心特征是
资产绑定聪，跟随聪自由流动。 聪网是BTC主网的原生扩展协议，基于闪电通道+平行BTC
网络，其存在的目的就是为了拓展BTC主网原生资产的流动性。聪网是SAT20落地的样本。

Translation (EN) – Preface (partial draft):

SAT20 Protocol Whitepaper
SAT20 Protocol – Overview
SAT20 is a “Satoshi Standard” native Bitcoin asset issuance and circulation protocol. Its core characteristic is that every asset is cryptographically bound to individual satoshis (sats) and therefore inherits the sat’s ownership and transfer path, allowing assets to move freely wherever the sat goes.

SatoshiNet ("聪网") is a native extension layer for the Bitcoin mainnet, constructed with Lightning channels plus a parallel Bitcoin network. Its purpose is to expand the liquidity and usability of native Bitcoin assets. SatoshiNet serves as the first concrete implementation (reference network) of the SAT20 protocol.

Key characteristics of SatoshiNet:

1. A native Layer-2 expansion network for Bitcoin.
2. No bridges: built on Lightning channels (channel-based security, no external custodians).
3. No new token: all assets originate from Bitcoin mainnet.
4. Shared consensus assumptions: same addresses, same fee unit (sats), same underlying asset semantics.
5. Faster block production and lower fees than L1.
6. Supports smart contract capabilities (via extended opcodes and parallel execution environment).

Asset Circulation Protocol (STP – Satoshi Transcending Protocol)
The SAT20 asset circulation ("transcending") protocol defines how sat-linked assets traverse between the Bitcoin mainnet and the native extension environment using Lightning channel mechanics.

Features of the Satoshi Transcending Protocol:

1. Bitcoin-Native Security: Inherits the RSMC (Revocable Sequence Maturity Contract) construction of Lightning channels; final custody and security are anchored to the Bitcoin mainnet—users retain unilateral withdrawal capability.
2. Full Asset Coverage: Supports prevailing Bitcoin-native asset standards such as Ordinals, Runes, BRC20, ORDX, etc.
3. Dynamic Lightning Channel Technology: Channels can splice in/out capacity and restructure UTXO composition.
4. Minimal Atomic Interface Primitives:
5. Cross-Chain Extensibility: Designed for future interoperability with other chains that can honor the atomic semantic set.

Asset Issuance Protocol (ORDX)
The SAT20 asset issuance layer (ORDX) is an enhanced variant of the Ordinals approach. Issued artifacts are called Sat Assets (SAT20 ASSETS). Each asset is bound 1:1 to a sat and thus inherits the satoshi’s immutable and indivisible properties:

1. A sat cannot be destroyed; therefore the bound asset is non-burnable by design.
2. Data bound to a sat is immutable; post-issuance mutation is disallowed, preserving provenance integrity.
3. Wherever the sat travels (L1 or L2 environments), the asset travels with it—no wrapping or synthetic representations.
4. Ownership of the sat equals ownership of the asset; transferring the sat atomically transfers the asset.
5. The inherent non-fungible ordering uniqueness of sats (ordinal position) imparts semi-fungible (SFT) characteristics to aggregated asset sets.
6. A sat can bind arbitrary structured data—even smart contract references—yielding programmable asset semantics.

Vision
“One sat, one universe.” Enable every individual to directly benefit from the expressive and economic potential of the Bitcoin network.

Background (Rationale)
Sats, as the atomic monetary unit of Bitcoin, carry deep semantic weight. If the broader Bitcoin ecosystem trend is toward richer native asset layers, then a truly “Satoshi-centric” issuance and circulation standard is an inevitable evolutionary milestone.

Motivations:

1. Native Fit: Binding assets to sats is the most natural Bitcoin-native issuance paradigm. Only the mint (inscription / binding) phase touches the L1 ledger; subsequent transfers or L2 mobility do not require additional L1 writes—minimizing chain bloat while maintaining cryptographic anchoring. Users retain direct mainnet-enforced custody throughout.
2. Forward Compatibility: Regardless of how Bitcoin scaling or execution layers evolve (e.g., future covenant-based constructs, BitVM, or additional opcode activations), sat-bound assets remain portable without synthetic wrapping. If a new L2 emerges, the sat (and thus its asset) can traverse there permissionlessly.
3. Mission of Expansion: Even prior to universal availability of fully native smart-contract-enabled Bitcoin layers, exploring a sat-centric expansion network (SatoshiNet) accelerates liquidity, experimentation, and user empowerment—fulfilling SAT20’s mandate.

In summary, the SAT20 sat-asset paradigm is a logically emergent construct in Bitcoin’s evolutionary arc; it unlocks the latent potential of the smallest denomination while reinforcing the uniqueness of Bitcoin-native asset provenance.

TODO: Translate this paragraph.

# SatoshiNet (聪网)

## Introduction

SatoshiNet is a Bitcoin-native expansion Layer-2 network composed of (a) Lightning Network channels (RSMC-based) and (b) a parallel Bitcoin-style chain. It preserves Bitcoin semantics while extending throughput, programmability, and multi-asset expressiveness.

It is “native” because of four core properties:

1. All assets on SatoshiNet originate from Bitcoin mainnet (no synthetic wrapped IOUs; no new inflationary governance token).
2. Security inheritance: Assets are effectively locked inside mainnet Lightning channels whose enforceability is guaranteed by Bitcoin L1 consensus.
3. User self-custody: At all times a user can unilaterally close channels and reclaim funds on L1 without third‑party permission.
4. Consensus symmetry: Same addressing principles, sat-based fee unit, and UTXO mental model.

SatoshiNet intentionally evolves Lightning in a different direction: retaining RSMC while omitting HTLC routing complexity, and pairing channels with a parallel ledger that records channel state transitions (auditable, append-only, UTXO-structured). With activation of additional opcodes (e.g. OP\_CAT) it approaches a Turing-complete scripting surface, enabling competitive smart-contract capabilities akin to other programmable ecosystems.

Differences vs Bitcoin mainnet:

1. Consensus: Proof of Stake (network-level ordering) while anchoring settlement guarantees to L1.
2. Block interval: ~12 seconds target.
3. Base fee: 10 sats per transaction (subject to future adjustment).
4. Enhanced UTXO schema: Explicit multi-asset representation within extended outputs.
5. Programmability: Optional activation of expanded opcodes enabling higher-level contract templates.

SatoshiNet functions as a staging ground for innovations difficult or slow to activate on L1 (bigger blocks, opcode experimentation, higher frequency settlement batching, etc.) while preserving a cryptographic peg via channels.

## Native Character (原生性)

Because Bitcoin L1 is intentionally conservative (limited script, no general-purpose VM), L2 solutions must avoid assumptions that L1 verifies arbitrary off-chain state. Traditional Lightning + HTLC architecture restricts asset types (pure BTC). SatoshiNet rethinks channel semantics by replacing HTLC routing with a parallel authenticated chain for: (a) state attestation, (b) asset metadata propagation, (c) multi-asset UTXO tracking.

Advantages over classic Lightning:

* Dynamic Channels: Channels become a \*set\* of UTXOs, supporting splicing-in/out and granular capacity reshaping.
* Native Asset Support: Ordinals, ORDX, BRC20, Runes and future sat-bound standards share the same channel plumbing.
* Lightweight Module Design: Channel core can compile to WASM, enabling browser-based light clients.
* Retained Security: RSMC revocation + penalty mechanics remain intact—guaranteeing user unilateral exit and punishment for stale state broadcasts.

Inheritance benefits:

* Asset provenance anchored on L1.
* Same addresses and fee denomination reduce cognitive friction.
* UTXO continuity: Familiar operational model for tooling and audits.

## Security (安全性)

Security derives from layered assurances:

1. L1 Enforcement: RSMC Lightning channels inherit Bitcoin’s hashpower finality for custody and dispute resolution.
2. Deterministic State Base: Parallel chain codebase (BTCD-derived) prevents double-spends of channel-reflected assets.
3. Provenance Conservation: Every sat and sat-bound asset originates on L1—precluding arbitrary mint/burn inflation vectors.
4. Economic Alignment: POS stake + slashing/penalty incentives discourage collusion or censorship at the ordering layer.

So long as Bitcoin L1 consensus remains uncompromised, every sat within SatoshiNet remains reclaimable by its legitimate owner.

## Proof of Stake Layer (POS)

A POS ordering layer maximizes throughput and lowers latency/fees while leaving ultimate escrow and dispute safety to mainnet. Validators stake Pearl (planned governance / service utility token) to participate. Because final custody resides in Lightning channels, decentralization pressure is lower than for a standalone L1, allowing efficiency gains without disproportionate trust tradeoffs.

Economic notes:

* Lower hardware demands vs PoW.
* Channel-backed exit reduces systemic stake attack surface.
* Fee + liquidity pool revenue share can subsidize infrastructure.

## Enhanced UTXO (增强型UTXO)

On L1, UTXOs principally encode sat balances. Upon “transcending” (channel ascent) into SatoshiNet, augmented outputs (enUTXO) embed:

* Sat balance
* Bound asset descriptors (protocol / ticker / ordinal binding / metadata)
* Optional contract script references
  This enables streamlined validation, provenance queries, historical tracing, and multi-asset atomic operations.

## Smart Contracts (智能合约)

Two tiers:

1. Template Contracts: Curated opcode sequences embedded at protocol layer for common primitives (escrow, swaps, staking, multi-asset settlement).
2. Extended Script / VM (via opcode activation e.g. OP\_CAT + potential higher-level scripting harness) enabling near Turing-complete logic.

## Liquidity Pools (流动池)

Global liquidity pools amortize channel capacity adjustments (splicing) and reduce fragmentation. A Foundation-maintained base pool supplies baseline depth; third parties may deploy specialized pools (e.g. stable sat asset pairs, ordinal-backed derivatives). Fees reward liquidity provision while keeping end-user routing costs low.

## Foundation (基金会)

A non-profit entity catalyzing ecosystem buildout.
Responsibilities:

1. Core protocol R&D.
2. Network infrastructure bootstrapping (indexers, routing relays, reference wallets).
3. Grants for open-source SAT20/SatoshiNet tools.
4. Education & outreach.
   Revenue Sources:
5. Donations.
6. Share of core services (mining/order flow aggregation, base liquidity pools) with declining percentage over maturity phases.
   Organizational Units: Executive Board, Engineering, Operations, Community & Education.
   Governance Principles: Progressive decentralization, transparency, on-chain reporting.

Note: The SatoshiNet Foundation is independent from SAT20Labs (no hierarchical control); suggestions herein are reference recommendations.

# Economic Model (经济模型)

Primary revenue conduits:

* Transaction packaging fees (base network fees, 10 sats initial target).
* Liquidity pool ingress/egress service spreads.
* Ancillary protocol service fees (future: indexing, attestation markets, data retrieval microfees).

Phased network growth assumptions (illustrative):

1. Bootstrap Phase: 0 → 1k daily tx.
2. Expansion Phase: 1k → 100k daily tx / ≥10 active asset classes.
3. Maturity Phase: 100k → 10M daily tx / ≥100 active tickers.
4. Exponential Phase: 10M+ daily tx / broad BTC asset saturation.

Validator (Mining Analog) Economics:

* Stake-target distribution encourages broad participation (e.g. Pearl lock ratios adjusting with volume).
* Revenue = (packaged tx \* fee) – foundation share – core service data fee.

Liquidity Pool Yield Illustration (Exponential Phase):

* Assume 1% of volume triggers exit fees; exit formula = base fee (e.g. 5,000 sats) + 1% notional.
* Potential gross annualized yield modeled at high volume could approach mid/high teens % before foundation share adjustments.

Dynamic Adjustments:

1. Foundation Share: Declines from 20% early to low single digits (1–5%).
2. Base Fee: May decrease (e.g. from 10 sats toward 1 sat) as Pearl stake / usage scale improves security-per-cost.

# Evolution (不断进化)

SatoshiNet is intentionally iterative—integrating channel throughput acceleration (instant block emission when mempool saturates), adaptive block size experiments (e.g. scaling toward 16MB with adequate decentralization metrics), opcode activation pipelines, and multi-chain interoperability bridges (anchored through sat custody rather than synthetic wrappers).

Potential throughput with modern hardware/networking: O(10k) TPS sustained for microtransactions under optimistic uplink conditions.

Vision: Serve as a neutral connectivity substrate linking Bitcoin-native value to external execution environments without compromising sat provenance.

# Use Cases & Scenario Concepts (场景)

## SatSwap (SATSWAP)

First DEX on SatoshiNet focused on high-efficiency sat-asset swaps (ordinal NFTs, semi-fungible sat baskets, sat-bound tokens).

## Stablecoins (稳定币)

Sat-bound denominations reduce capital lock in high-value BTC for microsettlement; stable units circulate while underlying sat channels enforce withdrawal safety.

## Micropayments (微支付)

Low per-tx fees + channel settlement efficiency → ideal for AI inference tolling, content streaming, pay-per-compute.

## DePIN (去中心化物理基础设施)

Legacy smartphones (multi-core, modest RAM) can operate lightweight channel/indexer clients—forming a mesh that indexes sat-asset ownership and provides distributed storage / SVM execution for small rewards.

# SAT20 Asset Circulation Protocol (资产流通协议 STP)

## Overview

Defines how sat-bound assets ascend (lock on L1 / unlock on L2), traverse (swap / re-bind across channels), and descend (settle back to L1) while preserving unilateral user control.

Core Concepts:

1. Lock / Unlock: Channel-mediated custody shift between latent (locked) and spendable (unlocked) states on L2.
2. Transcend (Ascend/Descend): Automatic state reflection ensuring L2 asset sets mirror locked channel sats.
3. Sat Swap: Reallocation and re-binding of sat+asset packages across multi-UTXO channel architectures.
4. RSMC Safety: Revocable commitments guarantee stale state penalties.
5. Dynamic Capacity: Splicing modifies channel UTXO composition without full close/reopen cost.
6. Multi-Protocol Support: Ordinals, ORDX, Runes, BRC20, etc.

## Protocol Flow Highlights

* User-initiated operations (principle of user primacy); remote service nodes act as deterministic responders.
* L2 neutrality: Any chain supporting atomic interface primitives can host unlocked sats.

### Open Channel

Standard Lightning open with immediate generation of initial commitment tx. Simultaneously an Ascend event reflects asset presence in SatoshiNet enUTXO ledger.

### Close Channel

Two modes:

1. Cooperative Close (lowest latency / immediate spendability after confirmation).
2. Force Close (broadcast latest commitment; funds reclaimable after CSV delay, e.g. 144 blocks).
   Concurrent Descend finalizes asset reconciliation (L2 representations collapse back strictly into locked channel outputs).

### Unlock / Lock

* Unlock: Emit L2 spendable UTXO from channel allocation.
* Lock: Re-absorb L2 spendable UTXO into channel (capacity permitting) for future multi-hop or splicing operations.

### Splicing

* Splice-In: Inject additional UTXOs (including heterogeneous sat-asset sets) expanding channel capacity.
* Splice-Out: Extract subset outputs to external addresses (triggers Descend logic for parity). Ascend/Descend invariants enforce 1:1 sat/asset accounting.

## Sat Swapping (聪交换)

Enables re-binding sat-bound assets across distinct UTXO partitions for routing efficiency, consolidation, or liquidity reshaping—without synthetic wrapping or trust bridges.

## Dynamic Channels

Represented as flexible UTXO sets:

1. Multi-UTXO membership.
2. Arbitrary add/remove operations.
3. Granular size adjustments enabling capital-efficient partial reallocations.

## Full Asset Support & Compatibility

Any UTXO-centric issuance model with deterministic binding (Ordinals, ORDX, Runes, BRC20) is supportable. For non-UTXO smart-contract chains, a compatibility layer could emulate atomic primitives, provided unilateral user exits remain enforceable.

# ORDX Asset Issuance Protocol (资产发行协议 ORDX)

## Introduction

ORDX is an enhanced Bitcoin-native issuance layer producing SAT20 Assets: sat-bound immutable objects spanning fungible, semi-fungible, and non-fungible semantics (SFT spectrum).

### Core Sat-Inherited Properties

1. Non-destructibility → Asset permanence.
2. Immutable embedded data → Provenance stability.
3. Co-location with sat trajectory → Native portability across L1/L2.
4. Ownership = sat custody → Atomic transfer semantics.
5. Ordered individuality → Semi-fungible grouping potential.
6. Arbitrary data binding → Programmable extensions (contracts, metadata, logic handles).

### Foundational Capabilities

1. Sat identification & tracking.
2. Data inscription / retrieval on sats.

### Principles

1. Uniqueness by birth order (ordinal index as immutable ID).
2. Conservation via ledger balancing (no sat burn semantics acknowledged by SAT20).

## Supporting Services

* Naming Service (DNS-like human-readable mapping for sats).
* Data Service (read public / owner-write interface; future micro-metered reads).
* Pay / Execution Service (WASM-executed modules paying sat-denominated microfees; revenue share between node operators and code publishers).

## Protocol Activation

Validation testnet activation at height 827,307; mainnet target activation at 845,000 (example timeline).

## Command Set (v1)

Two primary instructions:

* deploy
* mint
  Transfer unnecessary because asset motion equals sat transfer.

### Deploy Fields

p: protocol ("ordx")
op: deploy
tick: ticker (3 or 5–16 chars; 4-char reserved for BRC-20)
lim: per-mint cap (default 10,000; special sat-bound tokens default 1)
n: tokens per sat (default 1, max 65,535 v2)
selfmint: issuer-reserved ratio (two decimals)
max: total cap (64-bit int)
block: start-end activation heights (start-end)
attr: sat attribute filters (e.g. rar=uncommon;trz=8)
des: description text

Validation rules include uniqueness, block offset safety margin (≥1000 blocks before start if specified), attribute filtering syntax correctness.

### Attributes

* rar: rarity (common, uncommon, rare, epic, legendary, mythic)
* trz: trailing zeros count in sat index (e.g. trz=8)
* Future: extensible custom attributes.

### Mint Fields

p: ordx
op: mint
tick: ticker
amt: amount (≤ lim)
sat: specific sat index satisfying attr filters

Mint validation enforces protocol, op correctness, ticker existence, limits (lim, selfmint ratio \* max, overall max), block window inclusion, attribute satisfaction.

## Protocol v2.0 Enhancements

Objectives: streamline L2 circulation alignment, simplify issuance flows.
Upgrades:

* Data encoding migration from witness inscription to OP\_RETURN layout.
* New control types: Destroy (CT\_DESTROY) and Swap (CT\_SWAP) enabling irreversibly burning an inscription or reassigning to another sat.
  Format: OP\_RETURN | MAGIC\_NUMBER(OP\_16) | CT\_TYPE(OP\_4/OP\_5) | CONTENT

Exploratory Features (Not Final):

* stake / unstake issuance gating (non sat-bound variant) requiring channel presence.

## Sat Numbering (聪的编码)

SAT20 employs strict sequential numbering from genesis (first sat index = 0) with no gaps, rejecting destruction semantics recognized by some Ordinals interpretations. Differences vs Ordinals:

1. Ordinals acknowledges sat burn (yielding gaps); SAT20 treats sats as conserved.
2. Some theoretical ordinal indices predate actual issuance supply due to historical under-claimed coinbase rewards; SAT20 aligns numbering strictly with realized supply chronology.

SAT20 remains compatible with Ordinals NFTs functionally because inscriptions are sat-bound assets.

## Inscription (铭刻)

Supported data binding methods (current + future):

1. UTXO embedding (e.g. SRC20-style)
2. SegWit witness (Ordinals-style)
3. OP\_RETURN (Runes-style)
   Strategy: maximize security alignment; present approach follows Ordinals witness method with future multi-mode support.

## Issuance Modes

Three principal configuration archetypes:

1. Project-Controlled (max + selfmint specified; optionally block window) → centralized mint authority (e.g. stablecoins).
2. Partially Controlled (selfmint < 100%, enforced block window; fairness window + community participation).
3. Fair Launch (block window required; optional max; mandatory ≥1000 block gap post deploy confirmation).
4. Unrestricted (no selfmint / optional max / no block window) — external constraints define eventual scarcity.

## Sat Objects (聪对象)

Conceptualizes each sat as a scarce, owner-attributed, programmable digital object (contrasting with infinitely replicable traditional digital files). Properties: scarcity, uniqueness, ownership clarity, programmability. This substrate underpins value-network primitives and innovation surfaces for composable sat-bound logic / assets.

## Naming Service (名字服务)

Goals: human-readable mapping, collision-resistant uniqueness, sat-bound ownership inheritance.
Rules:

1. First registration wins.
2. UTF-8, case-insensitive, lowercased canonical storage.
3. No spaces, punctuation excluded (dot-separated names treated as full literals).
4. Length ≥3 bytes; 4-byte reserved for BRC20 tickers; 1–2 byte permanently system-reserved (anti-squatting).

Compositions via @ syntax (e.g. alice@sat20) require dual-signature authorization—forming contractual name unions (organization-like semantics).

Compatibility plan: Passive read of existing ecosystems (.btc, .x, etc.) while maintaining namespace separation.

Monopoly Resources & Royalties: Name ownership conveys exclusive ticker deploy rights; protocol can levy configurable royalty percentages automatically distributed to resource owners.

## D-Indexer

Interconnected indexers form a decentralized overlay network enabling:

* Redundant sat/asset state discovery
* Mobile/light client verification
* Distributed storage for metadata & execution logs
  Serves as critical reliability + censorship resistance layer.

# Token Classes & Examples

## Fungible Tokens (FT)

Each coin bound to a sat; examples:
"Pearl" (fair mint window defined by block range) — experimental meme / zero intrinsic promise.
Rare sat gating examples (e.g. uncommon rarity or trailing zero patterns) producing ultra-scarce tokens (1 sat = 1 token enforced by attribute filter).

## NFTs

Ticker-managed collections unify indexing and allow attribute-based conditional mint (height windows, rarity enforcement, sat composition metadata). Evolutionary NFTs possible via dynamic underlying sat composition updates.

## SFT (Semi-Fungible Tokens)

Emergent from sat uniqueness + data layering. Examples:

* Pizza: Visual composition varies with sat rarity counts inside aggregate.
* Denominated Stable Units: Multiple face-value sets each sat-bound for atomic micropayment utility.
* RWA Fractionalization: Building → ticker; rooms → NFTs; subdivided fractional sat-bundles for liquidity.
* Game Equipment: Attribute mutability through sat attribute swaps.

## DID

Decentralized identifiers anchored by naming service; uniqueness, persistence, cryptographic verifiability, and sat-custody enforced ownership (immutability via sat non-destructibility).

## DeIP (Decentralized Intellectual Property)

Framework for inscribing works directly onto sats; usage-based micro-compensation; permissionless publication; cryptographic authorship provenance.

# Roadmap (路线图)

1. ORDX Issuance Protocol: 1H 2024 baseline complete.
2. Transcending Protocol: Target functional completion Q1 2025.
3. SatoshiNet Launch: Q2 2025 mainnet target (BTCD-derived chain + channel integration).
4. SatSwap DEX: Coordinated launch with SatoshiNet Q2 2025.
5. Progressive Open Source:
6. Community Governance Exploration: Pearl as potential governance primitive (proposals, voting) post open-sourcing.

# API (接口)

(Planned) Public endpoints for: asset indexing, channel state proofs, inscription metadata, name resolution, swap routing quotes.

# Donations (捐赠)

Support development through voluntary contributions. Address: bc1ppejz29yxpz66yzkaxh6dek8pzsm8aajne6p4qak0xhxphkwzqnmsw45sur
Funds: maintenance, infrastructure, roadmap acceleration.

# About (关于)

We are a technically focused, Bitcoin-ecosystem-oriented team building open, sat-native protocols. No official token issuance; community-driven asset deployments are independent. Commitment: maintain SAT20 neutrality, provide technical guidance aligned with protocol principles, and expand sat utility.

# Links (链接)

* GitHub
* Twitter
* Website

# Disclaimer

This English translation is provided for informational purposes. In case of ambiguity, original Chinese text (above) prevails until a formally ratified bilingual canonical release is published.