OPENNUM PROTOCOL

OpenNum Protocol

Bitcoin's Phone Book and Wallet for the AI Era

Version: 1.0
Date: March 2026
Team: OpenNum Team
Website: opennum.org

Abstract

OpenNum is an application-layer identity protocol built on top of the Bitcoin Ordinals indexing system — Bitcoin's phone book and wallet for the AI era. It transforms Ordinal Inscription numbers into permanent, human-readable identity identifiers. Rather than sharing 62-character wallet addresses, users register their inscription number as their OpenNum ID — a short, memorable integer that maps cryptographically to their Bitcoin wallet. The inscription's image serves as their verified on-chain avatar. OpenNum requires no smart contracts, no sidechains, and no changes to the Bitcoin protocol. One number takes you everywhere.

Contents

1. The Problem

Bitcoin wallet addresses are cryptographically secure but humanly unusable. A typical Taproot address looks like this:

```
bc1p8dqa4wjvnt890qmfws83te2v3rxd7zr5uu6vsrk8kqnf3cgwwuqszc3qa5
```

This creates three compounding problems:

- **Poor usability.** Nobody can reliably remember, dictate, or verify a 62-character alphanumeric string. Every transfer requires copy-paste; a single wrong character means permanent asset loss.
- **No identity.** Bitcoin has no native mechanism for linking wallet addresses to human identity. Without identity, a Bitcoin wallet cannot serve as the foundation for social interaction, community building, or trust.
- **Barrier to adoption.** Complex address formats are one of the primary obstacles to Bitcoin's mainstream adoption.

> The best interface is the one that disappears. Bitcoin needs an identity layer that people understand instinctively — a number.

2. The OpenNum Solution

OpenNum leverages a unique property of the Bitcoin Ordinals protocol: every inscription is permanently assigned a sequential integer — its inscription number — at creation time. As of early 2026, over **112 million inscriptions** exist on Bitcoin.

OpenNum makes this simple: **your inscription number is your identity.**

> Think of OpenNum as Bitcoin's phone number system: your inscription number is your number, your wallet is your device, sending to #2025 is like making a call. Nobody needs to remember a 62-character string — they just need your number.

```
// Before:
Send to: bc1p8dqa4wjvnt890qmfws83te2v3rxd7zr5uu...

// Now:
Send to: #2025
```

The inscription number resolves to the wallet currently holding it. The inscription image becomes the holder's avatar. One number carries identity, payment routing, social context, and community membership.

3. Protocol Specification

3.1 Registration

> Why inscriptions, not UTXOs, PubKeys, or Satoshi numbers? UTXOs are destroyed on spending — not persistent; PubKeys can be generated infinitely with no scarcity; Satoshi numbers lack images and content. Inscriptions uniquely combine: globally unique sequential number (scarcity) + embedded image (avatar) + market price (economic anchor) + transfer cost (sybil resistance). No other anchor offers all four.

To register an OpenNum ID, a holder produces a signed registration message:

```
{
  "protocol":           "opennum",
  "version":            "1.0",
  "inscription_number": 2025,
  "inscription_txid":   "abc123...def",   // Bitcoin consensus
  "indexer_ruleset":    "ord-v0.18-mainnet",
  "wallet":             "bc1p...",
  "timestamp":          1735689600,
  "signature":          "H9k2mN...Xp4q"
}
```

The signature uses standard secp256k1 Bitcoin message signing, compatible with all major wallets. This proves wallet ownership — and therefore inscription ownership — without revealing the private key and without any on-chain transaction.

3.2 Validity Rules

A registration is valid if and only if ALL of the following hold:

1. The signing wallet **currently holds** the declared inscription (verifiable via any Ordinals indexer).
2. The cryptographic signature is valid for the declared wallet and canonical message.
3. The timestamp is within the freshness window (recommended: 10 minutes for initial registration).
4. No other currently-valid registration exists for the same inscription number from a different wallet.

3.3 Transfer and Reassignment

When an inscription transfers to a new wallet, the following occurs automatically:

- Previous registration becomes cryptographically invalid (old wallet no longer holds the inscription).
- The inscription number enters **Dormant** state: visible in OpenNum but not mapped to any active identity.
- New holder may register at any time by producing a signed message from the new wallet.
- Until re-registration, the number cannot be used for payments, messaging, or community access.

> This mirrors the real-world model of phone numbers: the number travels with the asset, but identity activation requires the new holder's explicit action.

3.4 Indexer Architecture

OpenNum operates entirely at the application layer. Any party may run an OpenNum indexer. Three functions: (1) **Monitor** Bitcoin blocks for inscription ownership changes. (2) **Validate** incoming registration messages. (3) **Serve** a public REST API resolving numbers to wallets and profile metadata.

Message propagation: In v1.0, registration messages are submitted via HTTP REST API to the reference indexer (POST /api/v1/register). Future versions (v2.0+) will introduce P2P Gossip network propagation without any centralized entry point.

3.5 Number Authority & Deterministic Foundation

Inscription numbers are computed by ord indexer software, not Bitcoin consensus. OpenNum uses a **dual-anchor design**: every registration includes both inscription_number (human-readable) and inscription_txid (Bitcoin consensus primitive). The txid is the GPS coordinate — unforgeable. The number is the street address — human-readable. Together they make OpenNum **numbering-dispute-immune**.

Cursed Inscriptions (#c-1234): ~472,043 inscriptions created before block 824,544 received negative numbers. The Ordinals Jubilee update (Jan 6, 2024) formally rehabilitated them. OpenNum treats cursed inscriptions as first-class citizens: they display as #c-1234 and carry identical registration rights to positive-numbered inscriptions.

> The txid is the GPS coordinate, the number is the door number. Both are essential: the GPS finds the right building, the door number tells your neighbors how to find you.

3.6 Identity State Machine

Every OpenNum number exists in exactly one of four states:

State	Flag	Meaning	API Response
Active	Green	Registered & valid; current holder has signed	Returns wallet address
Dormant	Black	Transferred; old registration void, new holder not registered	Returns dormant status
Cooling	Orange + countdown	Transfer occurred within last 30 days; prompts new holder to activate	Returns days remaining
Flagged	Blue	Previous holder published a transfer declaration	Returns declaration

> The 30-day cooling window gives wallets and integrations sufficient buffer to handle ownership transitions. A cooling number shows a visible orange indicator rather than silently going dormant, reducing missed payments.

3.7 .btc Display Alias

Inscriptions containing SNS domain registration JSON ({"p":"sns","op":"reg","name":"satoshi.btc"}) are automatically read by the OpenNum indexer as a display alias for that inscription number. The number remains the canonical identifier; .btc is a human-friendly display layer. btcmap, unisat domains, and other SNS-compatible systems are also supported.

4. Use Cases

4.1 Simplified Bitcoin Payments

Any OpenNum-compatible wallet resolves a number to the current wallet address before constructing a transaction. The user types **#2025** — the wallet handles resolution invisibly. As intuitive as sending a payment in WeChat.

4.2 On-Chain Social Identity

Every registered OpenNum ID has a public profile: inscription image as avatar, registration timestamp (proving early participation), on-chain holdings visible to all, and verified external social account links.

4.3 Social Media Binding

Users link their OpenNum ID to external platforms (Twitter/X, TikTok, etc.) via mutual verification. Indexers crawl both signals. Once bound, followers can send Bitcoin directly through the creator's social profile.

4.4 Community Membership

Holding a specific inscription series grants access to that community. The inscription is the membership card — on-chain, verifiable by anyone, transferable as a standard Bitcoin transaction.

4.5 Inscription Gifting

Sending an inscription requires only the recipient's OpenNum number. No address copying, no error risk. This dramatically reduces gifting friction and enables viral social behavior.

4.6 Contract Attestation

Two OpenNum holders jointly sign a structured document with their wallet private keys. The combined signature produces a tamper-proof, timestamped attestation proving both parties agreed to the document content at a specific time.

4.7 Wallet Onboarding

Wallet providers can mint low-cost text inscriptions in bulk and gift one to each new user at signup. From day one, the user has a permanent, unique inscription number — their Bitcoin identity number.

5. Competitive Landscape

Feature	ENS (Ethereum)	OpenNum (Bitcoin)
Identifier type	User-chosen text (satoshi.eth)	Sequential integer (#2025)
Blockchain	Ethereum	Bitcoin
Smart contracts required	Yes (ERC-721 + registry)	No
Avatar source	Linked NFT (separate asset)	Inscription image (same asset)
Registration cost	Gas fees + annual renewal	Signature only (zero on-chain cost)
Asset backing	None (name separate from asset)	Yes (inscription is the identity asset)

5.1 Full Competitive Map

OpenNum is the only system targeting **individual users**, **inscription-number-anchored**, with **zero on-chain registration cost**, on Bitcoin.

Feature	ENS	MicroStrategy Orange	BTCO DID	OpenNum
Target users	Individuals (Ethereum)	Enterprise/institutions	Developers	Individual users
Identifier	Text name	W3C DID string	W3C DID string	Sequential integer
Chain	Ethereum	Bitcoin	Bitcoin	Bitcoin
On-chain cost	Gas + annual	Yes (batch tx)	Yes (inscription)	No (signature only)

Feature	ENS	MicroStrategy Orange	BTCO DID	OpenNum
Human-readable	High (satoshi.eth)	Low (DID string)	Low (DID string)	High (#2025)
Built-in avatar	Requires linked NFT	None	None	Inscription image, automatic
AI agent identity	None	None	None	v1.1 native support

6. Open Protocol Principles

OpenNum is designed to be public infrastructure for the Bitcoin ecosystem, not a proprietary platform:

- **Open specification.** Published under MIT license. Any developer may implement it without permission or payment.
- **No rent-seeking.** OpenNum charges no registration, renewal, or transaction fees at the protocol layer.
- **Decentralized indexing.** We run a reference indexer but actively encourage independent indexers. Deterministic validation guarantees convergence.
- **Wallet-neutral.** Open SDK; no affiliation with any specific wallet provider.
- **Inscription-bound, not wallet-bound.** Identity is anchored to the inscription, not the wallet. Wallets are replaceable containers; inscriptions are unique on-chain assets with transfer costs. This provides stronger ownership semantics consistent with the domain name and phone number model.

7. Known Risks and Challenges

7.1 Bitcoin Community Conservatism

A portion of the Bitcoin community opposes Ordinals, viewing inscriptions as unnecessary congestion. OpenNum inherits this controversy. We note: OpenNum adds zero additional on-chain load — registration is a pure off-chain cryptographic operation.

7.2 Network Effects and Cold-Start Strategy

Like all identity systems, OpenNum's value is proportional to adoption. Three cold-start entry points: **(1) BRC-20 holder communities** — tens of thousands already have inscriptions; **(2) OpenClaw AI agent operators** — immediate agent identity need; **(3) Inscription marketplaces** — Magic Eden, OKX can display OpenNum IDs without wallet integration.

7.2.1 Inscriptions as Natural Spam Barrier

Unlike systems requiring engineered rate limits, OpenNum's spam resistance is structural: **registration requires holding an inscription, and inscriptions have real on-chain cost.** Mass spam registration requires mass inscription minting — economically prohibitive. The economic structure is the primary spam defense.

7.3 Indexer Centralization Risk

In the early phase, a single reference indexer handles most queries. Temporary centralization risk. We publish indexer source code from day one and encourage independent instances.

7.4 Inscription Liquidity and ID Stability

High-value inscriptions are frequently traded. The dormant state mechanism handles ownership changes gracefully. Applications must handle dormant IDs without crashing; reference implementations will include dormancy handling patterns.

7.5 Competitive Risk

MicroStrategy's Orange DID addresses enterprise identity on Bitcoin. Wallet providers with large user bases could implement similar functionality. OpenNum's defense: if our standard is adopted as the de facto Bitcoin identity layer, it succeeds even if large players build on top of it rather than competing with it.

8. Roadmap

Phase	Timeline	Deliverables
Phase 1: Foundation	2026 Q1	Protocol v1.0 spec · opennum.org · Whitepaper · GitHub
Phase 2: Explorer	2026 Q2	Web app · Connect wallet · Profile · Send BTC by number
Phase 3: Social	2026 Q3	Messaging · Inscription gifting · Social account binding · Community gating
Phase 4: SDK	2026 Q4	Open source wallet SDK · Third-party wallet integration · Merchant tools
Phase 5: Scale	2027+	Mobile app · Multi-language · Global expansion

9. AI Agent Integration

The rise of self-hosted AI agent frameworks — most notably **OpenClaw**, supporting ~150,000 autonomous agents globally as of early 2026 — introduces a new class of Bitcoin participants: software agents that independently hold wallets and transact without human confirmation on every action.

These agents face an unsolved identity problem that OpenNum is uniquely positioned to address.

9.1 The AI Agent Identity Problem

- *Who is accountable* when an AI agent sends or receives funds?
- *How to verify* whether a counterparty is a legitimate agent operated by a trusted human, vs. a sybil attack or honeypot?
- *How do agents discover* each other's payment addresses without a centralized registry?

- *Can agent reputation* accumulate and persist through infrastructure changes?

9.2 OpenNum as the Agent Trust Anchor

Every AI agent can register under its human operator's inscription number, establishing a cryptographically verifiable chain of accountability — the **Human-Agent Trust Bridge**.

9.3 Protocol Extension: Agent Registration (v1.1)

```
{
  "protocol":     "opennum",
  "version":      "1.1",
  "inscription_number": 2025,
  "wallet":       "bc1p...",           // operator wallet (holds inscription)
  "agent_wallet": "bc1pagent...",      // agent operational wallet
  "agent_role":   "openclaw",          // agent framework identifier
  "agent_label":  "Trading Agent #1",
  "signature":    "H9k2mN...Xp4q"    // signed by operator wallet
}
```

9.4 Human-Agent Trust Bridge: Practical Impact

- **Accountability.** Every agent action traces back to a human holding a real on-chain asset.
- **Reputation portability.** Operators upgrade infrastructure without losing identity; the inscription number and its history are immutable.
- **Discoverability.** Applications enumerate all agent wallets under an inscription number via the OpenNum API.
- **Payment routing.** Both the operator's OpenNum number and registered agent wallets resolve through the same API.

9.5 The Emerging Agent Economy

OpenClaw agents already use Bitcoin Lightning micropayments for compute, APIs, and inter-agent service fees. As the agent economy grows from 150,000 today to potentially millions by 2027, a readable identity layer with accountability chains becomes critical infrastructure.

> "Every AI agent has a human operator. Every inscription holder has a number. OpenNum makes that relationship cryptographically verifiable — and publicly transparent."

9.6 Comparison with Ethereum ERC-8004

Ethereum's ERC-8004 (Trusted Agent) standard launched January 2026 with 24,000+ agents registered. OpenNum v1.1 is the Bitcoin-native equivalent — with key advantages:

Feature	ERC-8004 (Ethereum)	OpenNum v1.1 (Bitcoin)
Chain	Ethereum	Bitcoin
Registration cost	Gas fees (on-chain tx)	Zero on-chain cost (signature only)
Human operator anchor	None (agent identity anonymous)	Mandatory: must hold inscription
Accountability	Low (on-chain address only)	High (traceable to real asset holder)
Asset backing	None	Inscription asset backing
Payment integration	Requires x402 etc.	Native Bitcoin payments, number = payment address

---

10. Extended Applications

10.1 Dormant Inscriptions Reactivated

Hundreds of millions of inscriptions sit dormant in Bitcoin wallets — minted during the 2023 BRC-20 frenzy, never traded. OpenNum fundamentally reframes the value of any inscription: **what matters is not the content, but the permanent integer number.** A "worthless" BRC-20 mint inscription #8,400,221 carries a globally unique, immutable number that can become the holder's permanent Bitcoin identity.

10.2 BRC-20 Community Identity Layer

BRC-20 token communities — ORDI, SATS, MEME holders — lack shared on-chain identity infrastructure. OpenNum provides it. The indexer can enumerate all registered holders of any BRC-20 symbol, making the community cryptographically legible for access gating, community payments, and visual identity.

10.3 On-Demand Identity Creation

Creating a Bitcoin inscription costs a few dollars at current fee rates. Any user can mint a new inscription at any time and immediately have a new OpenNum identity number — without changing their existing wallet. Multiple identities for personal, commercial, and project use, all under the same private key.

10.4 Multi-Number Routing

Number	Role	Use case
#2025	Primary identity	Social profile, public payments, community membership
#88052	Business identity	Merchant payments, invoicing, professional contact
#3,400,120	Project identity	Specific DAO, NFT collection, community event
#29,400,800	Temporary identity	One-time transactions, privacy-preserving payments

11. Conclusion

There are 112 million inscriptions on Bitcoin, and growing. Every one carries a unique, permanent integer — a number that has existed on the most secure distributed ledger in history since the moment it was created. These numbers are already scarce, already on-chain, already held by real people.

OpenNum turns these numbers into what humans have always used to find each other: **a simple, memorable identifier.**

Your inscription number is your Bitcoin identity. It routes payments, represents your on-chain reputation, grants community access, and serves as your verified avatar across the internet. When you transfer it, it goes with you; when you sell it, it enters dormancy waiting for the next holder to activate it — just like a phone number.

The protocol is open. The standard is free. The number is yours.

OpenNum Team · opennum.org · 2026 · MIT License · Open Protocol · Permissionless