Mainnet Whitepaper

Its own encrypted network on top of the internet: own domains, own mail, own browser. What is built, what runs and what is still missing.

• Beta · no external audit · 2 nodes

English translation. The German version (mainnet-whitepaper.pdf) is binding.

CONTENTS

01 **Summary** 3
Mainnet on one page – and the honest status

02 **The problem** 4
Names, metadata, trust – and why tools alone are not enough

03 **What Mainnet is** 5
Overlay network, roles, extensions, programs

04 **Architecture** 7
Eight layers from transport to operation, and how mature each is

05 **Names and the registry log** 9
Merkle log, checkpoints, witnesses – and what is still missing

06 **Anonymity: what Mainnet can and cannot do** 11
Tor by default, high security, no mix network, honest comparison

07 **Encryption** 13
Methods per purpose, post-quantum where possible, key hierarchy

08 **Mail, chat and hosting** 15
What you do in Mainnet – and how far along it is

09 **Distributed storage** 17
k of n: encrypt first, then split – still mirrored today

10 **Running a node** 18
Who runs a node, what it stores, what runs today

11 **Domains and points** 19
500 points = 1 year, bitcoin, review, reserve, free launch offer

12 **Security and testing** 21
Tests, internal reviews, real Tor tests – no external audit

13 **Limits and risks** 22
What you should know before trusting Mainnet

14 **Roadmap** 23
What comes next – in order, without invented dates

15 **Glossary** 24
Terms from beta to X-Wing

Every statement in this document belongs to one of four maturity levels: **code complete**, **tested locally**, **tested for real** (real Tor network) and **in operation**. Anything that is only a goal is labelled as a goal.

CHAPTER 1

Summary

Mainnet is its own network on top of the internet: own domains such as `shop.de` or `atelier.cp77`, own mail, own browser. By default everything runs over Tor. Mail, chat and private files are encrypted end to end on your device; the key exchange is post-quantum hybrid, users' signatures are still classical. Who owns which name is recorded in a public log that can only grow and that every node checks for itself.

● Built and tested locally

- Node `mainnetd` with built-in Tor
- Mail, chat, contacts, tunnels
- Hosting as `.site` (WebAssembly)
- Splitting k of n, high security
- Mainnet Browser, Studio, search

◐ Running today

- Portal cypherpunk2077.com with onion mirror
- Registry log, checkpoint 13, 3 cosignatures
- Signed heartbeat in the log
- 2 nodes, both run by the operator

○ Not yet

- Signed release to download
- Independent witnesses
- Splitting in operation
- Mix network
- Purchase with real bitcoin
- External audit

28
Rust crates

2,215
of 2,215 tests green in the last full run (28 Oct; not repeated since)

158
port checks over Tor, no open port

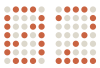
0
external audits so far

What Mainnet wants to do better

- **Names without gatekeepers.** Any extension, one price for all (€4.99 a year), no premium names. Well-known brands only for their owners.
- **Encryption by default.** Content is encrypted on the device. The registry cannot read users' mail, chats or private files because it never receives the keys.
- **Verifiable allocation.** Every approval, renewal and suspension is recorded in the public log, suspensions with a reason code. Goal: a node accepts nothing from the registry that it cannot check itself. Today the node checks signatures and consistency; the witnesses are still run by the operator.
- **Everything in one program.** Names, sites, mail, chat, files and search instead of separate tools you have to put together yourself.

HONEST STATUS

Mainnet is a **beta**. Today **two nodes** are running, **both run by the operator**, plus three launch witnesses, also run by the operator. There is **no signed release** for outsiders to download yet. A **mix network**, in which nodes collect, mix and forward other people's traffic, **does not exist**. There is no external audit. The goals are largely reached at the code level, not yet in real operation.



CHAPTER 2

The problem

The internet works. But using it reveals more than necessary, and anyone who wants a name in it depends on a few organisations.

1. Names belong to a few

Domain extensions are managed by a small number of organisations. Good names have been taken for years or are resold at high prices; some extensions cost many times more than others. Whoever controls an extension can suspend or redirect a name – often without users being able to verify it.

2. Metadata reveals more than content

Even when a connection is encrypted, it remains visible who talks to whom, when, how often and how much. DNS queries show the provider which sites someone visits. Cookies and trackers link visits across many sites into a profile.

3. Trust in many strangers

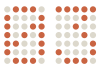
HTTPS relies on hundreds of certificate authorities, and each of them can issue a certificate for any domain. Transparency logs (Certificate Transparency) make mistakes visible – after the fact. Mail depends on providers who can read content, and on phone numbers.

4. Good tools, but separate

Tor protects the path very well, but it has no memorable names (an onion address has 56 characters), no mail and no simple hosting. Encrypted messengers solve chat, not sites. Anyone who wants everything combines many programs and easily makes mistakes along the way.

WHAT MAINNET DOES ABOUT IT

- its own namespace with a public, verifiable log instead of a chain of trusted authorities,
- Tor as the default transport, plus measures against learning from timing and volume,
- end-to-end encryption in mail, chat and files, with keys only on the user's side,
- one program for everything: node, browser, mail, chat, hosting.



CHAPTER 3

What Mainnet is

Mainnet is an **overlay network**: it runs over the internet but has its own names, its own encryption rules and its own browser. Every user runs a node. Names are allocated in one place; the network is operated in a distributed way.

Central allocation, distributed operation

cypherpunk2077.com is only the registry: it allocates and reviews names, keeps the registry log and distributes the programs. It hosts no websites. Other people's content is only present on the registry's machines in encrypted form – as mail envelopes and file pieces on the two launch nodes, which the registry cannot open.

Sites, mailboxes and files live with their owners and on users' nodes. A node keeps a copy of the log and resolves names itself. If cypherpunk2077.com fails, existing sites keep working; there are then no new approvals or suspensions (chapter 13).

Roles

ROLE	WHO	WHAT
User	anyone	browses, writes mail and chats; their node runs in the background
Owner	whoever holds a domain	keeps the domain's key and hosts the site (PC, VPS, Raspberry Pi)
Node	every running `mainnetd`	finds other nodes, stores encrypted pieces, serves its own sites
Post office	node with role `mailbox`	holds encrypted mail envelopes until the recipient collects them
Indexer	goal: independent nodes; today one (empty) indexer on the operator's VPS	build the search index of approved sites
Witness	independent third parties (goal)	cosign checkpoints of the log and refuse forks
Registry	cypherpunk2077.com	reviews and allocates names, suspends under the terms of use, signs releases

Own extensions

Any extension of 2 to 20 letters is possible: `.com`, `.de`, `.net`, `.org`, `.cp77` and new ones such as `.atelier`. The namespace is separate from the old internet: `shop.de` in Mainnet is not the same site as `shop.de` on the internet. To avoid confusion, the Mainnet Browser shows the badge ◆ **Mainnet** on every Mainnet site and keeps Mainnet and the old internet in separate profiles. Reserved are, among others, `.onion`, `.local`, `.test` and file extensions.

Programs

PROGRAM	TASK	STATUS
`mainnetd`	the node (Rust): network, Tor, log mirror, mail, storage, hosting, local API	built, tested, 2 nodes in operation
Mainnet Browser	browser on Qt WebEngine with badge, separate profiles, mail, chat, Studio	built (Windows), tested locally
`mainnet`	command line: keys, domains, publishing, mail	built, tested
App	Android with light node (iOS planned)	built, never started on a device
SDK, Studio	build and publish a site as one `.site` file	built, tested locally

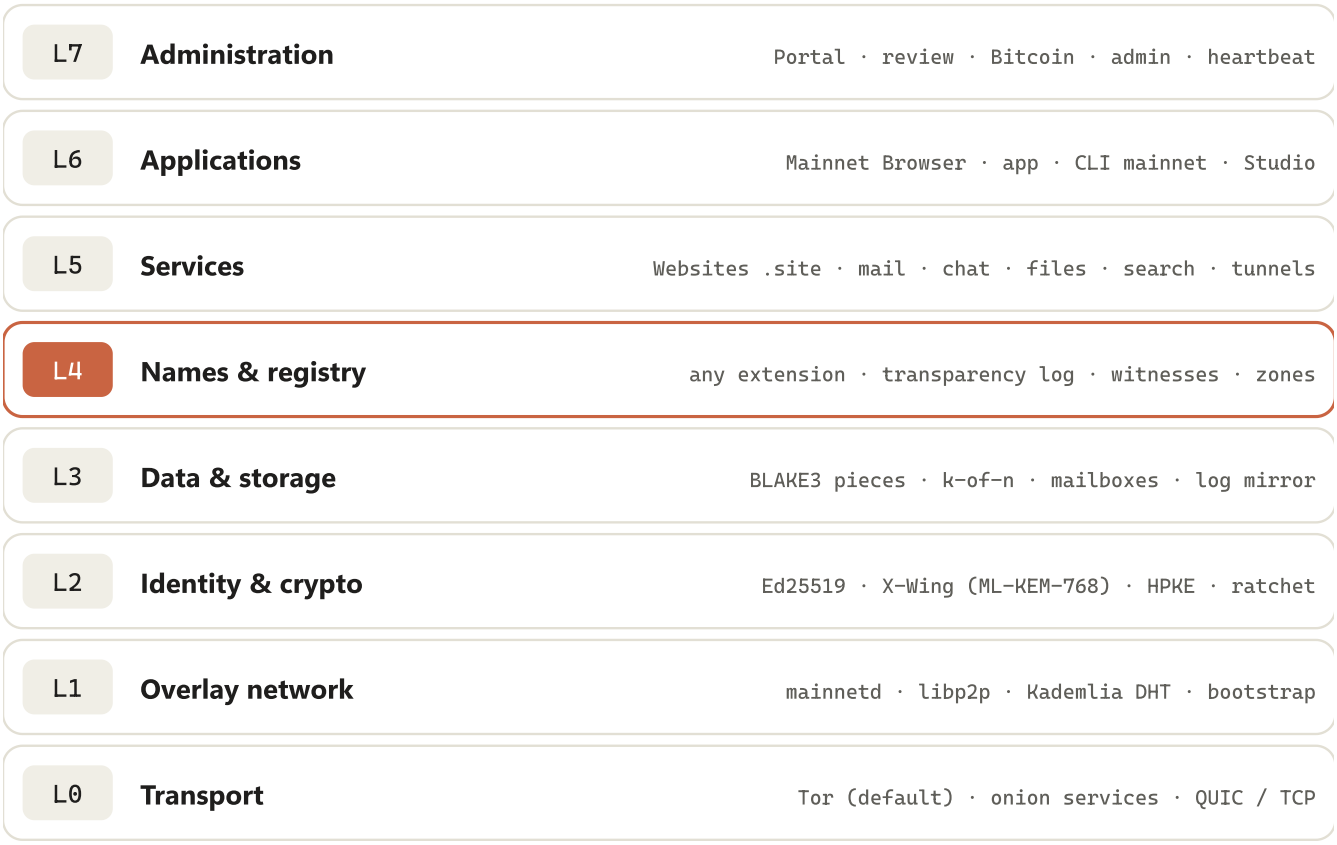
Mainnet and the old internet compared

TOPIC	OLD INTERNET	MAINNET
Names	many taken, prices per extension	fresh namespace, €4.99 a year for every extension
Login	password, cookies	one key on your device
Encryption	transport yes, content rarely	transport and content (mail, chat, private files)
Allocation	hard to verify	public log, every node checks
Speed	fast	slower over Tor; “Fast” mode available
Maturity	decades in use	beta, no external audit
Access	any browser	own program needed; no release yet

CHAPTER 4

Architecture

Mainnet is built in eight layers. Each layer has a clear task and only uses the layers below. That way each one can be checked and replaced on its own.



Each layer only uses the ones below it. Highlighted: L4, the own naming system with a public log.

Figure 1. Layers L0 to L7. L0 is the transport, L7 the operation by the registry.

The layers in brief

- **L0 Transport.** The default is Tor, embedded through Arti (the Rust implementation of Tor). In “Fast” mode connections go directly over QUIC or TCP.
- **L1 Overlay network.** `mainnetd` based on libp2p: Kademlia DHT for discovery, a signed bootstrap list for entry, limits against overload.
- **L2 Identity and crypto.** One key instead of a password; subkeys for mail, chat and devices. Details in chapter 7.
- **L3 Data and storage.** Content as BLAKE3-addressed pieces, distributed storage k of n, mailbox storage, local copy of the log.
- **L4 Names and registry.** The own naming system with transparency log, witnesses and zones signed by the owner (chapter 5).
- **L5 Services.** Websites, mail for every domain, chat, files, search, tunnels (chapter 8).

- **L6 Applications.** Browser, app, command line, Studio.
- **L7 Administration.** Portal, review, payment in bitcoin, admin panel, heartbeat, tripwires.

Maturity per component

For software, "done" means four different things. The table shows how far along each component is.

COMPONENT	CODE	LOCAL	REAL	LIVE	NOTE
Node mainnetd, Anonymous mode	●	●	●	◐	default since 28 Oct; the entry node on the VPS deliberately runs directly
Hidden hosting (onion)	●	●	●	◐	real tests on 2 days; in operation the PC node's descriptor upload sometimes fails
Registry log + witnesses	●	●	●	◐	running, checkpoint 13; the 3 witnesses are run by the operator
End-to-end mail	●	●	○	◐	both nodes are post offices; no outside users yet
Chat, contacts	●	●	○	○	1:1 and groups of up to 256
Hosting .site, Studio	●	●	◐	○	server logic as WebAssembly; no user's site yet
High-security mode	●	●	◐	○	3 real runs; cover traffic never tested against the real network
Splitting k of n	●	●	○	○	with 2 nodes data is mirrored
Search	●	●	○	○	indexer has no documents, not connected in the portal
Tunnels	●	●	○	○	preview
Bridges (obfs4, Snowflake)	●	●	◐	○	not yet passed through to Tor in the node
Mainnet Browser	●	●	○	○	built, only as a ZIP, unsigned
Android app	◐	◐	○	○	never started on a device; iOS not built
Bitcoin purchase, admin panel	●	●	○	○	only in the test network (regtest)
Signed release, updates	●	●	○	○	draft exists, not signed, not published
Mix network	○	○	○	○	not built (chapter 6)

● yes ◐ partly ○ no **Local** = automated tests on one computer **Real** = over the real Tor network

Live = running on the 2 nodes

CHAPTER 5

Names and the registry log

The registry decides who gets a name. But every decision is recorded publicly in a log that can only grow, and every node checks it for itself. Later changes become visible as soon as independent witnesses check; today the witnesses are still run by the operator.

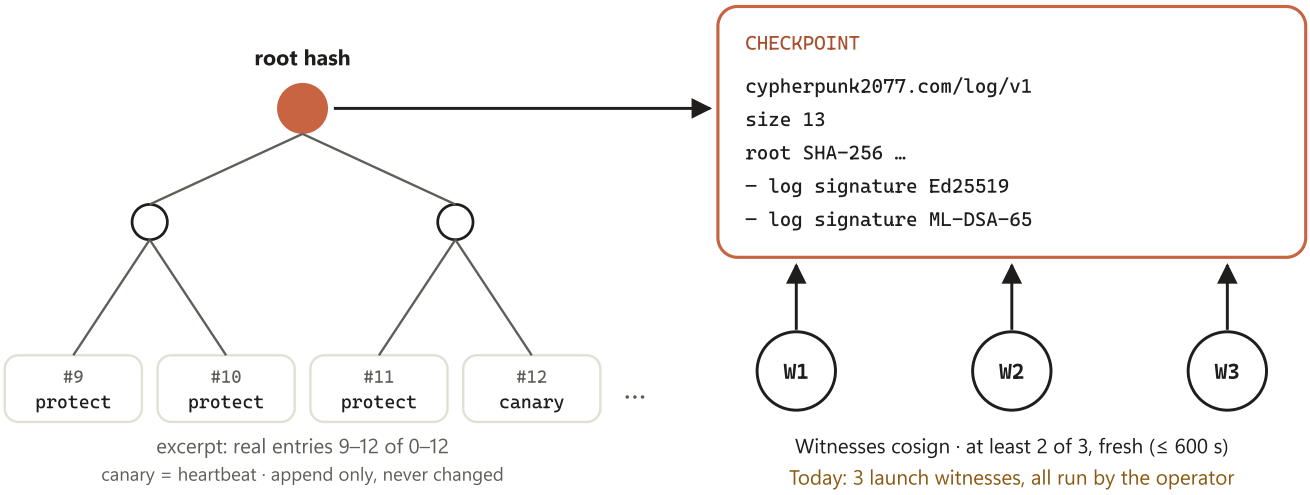


Figure 2. Entries form a Merkle tree. A checkpoint records size and root and is signed twice. Witnesses cosign; nodes only accept checkpoints with at least two fresh cosignatures.

How it works

1. **Entries.** Every approval (`register`), renewal (`renew`), transfer, suspension (`suspend`, `revoke`) and every heartbeat is an entry. Suspensions carry a public reason code.
2. **Merkle tree.** The entries form a hash tree following Certificate Transparency (RFC 9162, C2SP tlog). A later state must contain the earlier one; a short consistency proof shows this.
3. **Checkpoint.** Size, root hash and time are signed twice with the log key: **Ed25519 and ML-DSA-65** (post-quantum), both required.
4. **Witnesses.** Independent witnesses cosign every checkpoint that is consistent with the previous one. They refuse a fork (two different states of the same size) and store it as evidence that anyone can verify.
5. **Nodes.** Every node mirrors the log and accepts a checkpoint only with both log signatures and at least **2 of 3** witness cosignatures that differ from the checkpoint by at most 600 seconds. It resolves names from this copy – without a DNS query. The browser only shows "◆ verified" if the checkpoint is at most 24 hours old.

What runs today

The log has been in operation since 29 Oct 2026. As of 30 Oct 2026: **checkpoint 13**, published at `cypherpunk2077.com/log/v1/checkpoint`, with 3 cosignatures; 6 domains; entry 12 is the operator's first signed heartbeat.

LIMIT TODAY

- The three witnesses are **launch witnesses run by the operator**. Their cosignatures prove nothing to third parties yet. Towards the operator – or someone who takes over the operator's computer – the log is today **verifiable, but not tamper-proof**.
- Today the witnesses only check consistency, not the content of entries (the check is built but not yet switched on).
- The admin double signature per entry is not yet in the public log; nodes trust the log key alone.
- Witness cosignatures are Ed25519 only, so not post-quantum secure.

Goal: at least three independent witnesses in different countries, content checks switched on, admin signature checked by nodes and witnesses. Only then is "tamper-proof" an honest statement.

Why not a mining blockchain?

A blockchain with proof of work (mining) only protects if computing power is widely distributed; a small network tips over as soon as an attacker controls more than half. In a registry with an operator, the operator decides who gets a name anyway. A transparency log with independent witnesses does more here: an entry is in a signed checkpoint after about a minute at most, without the power consumption of mining, and anyone can check it. (The approval itself is reviewed by the operator by hand, within 24 to 48 hours.) The "validators" are the witnesses. The same pattern secures the web's certificates today (Certificate Transparency) and signed software (Sigstore).

Zones and certificates

What lives under a domain (site, mailbox, onion address) is signed by the owner with their own key. That key is created on the owner's device; the registry never receives it. Instead of certificate authorities there are domain certificates derived from log and zone, plus a transfer lock, and transfers only with signatures of both the old and the new owner.

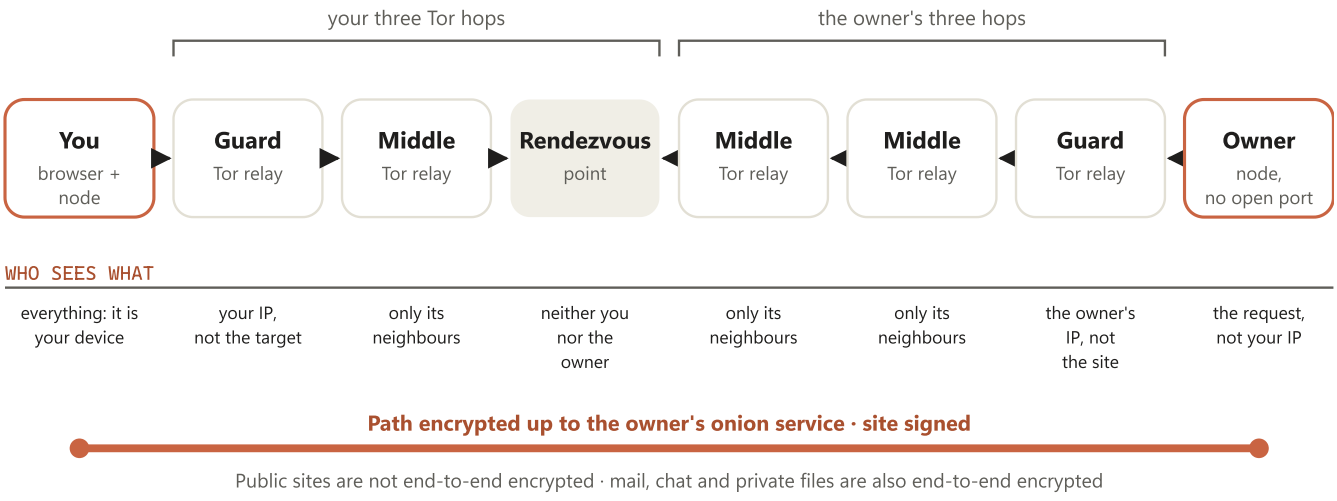
CHAPTER 6

Anonymity: what Mainnet can and cannot do

Mainnet is built on Tor. It inherits Tor's strength – location and address are protected against ordinary observers – and its weakness: someone who watches both ends for a long time can correlate them by timing and volume. Mainnet makes that harder; it does not prevent it.

Three levels

LEVEL	WHAT HAPPENS	COST	STATUS
Fast	direct connections over QUIC/TCP; the other side sees your IP	fastest	one click away
Anonymous (default)	everything over Tor; hidden hosting through onion services, without a listening port	slower; a few minutes after start until reachable	tested for real on 2 days
High security (beta)	strengthens what Anonymous already has (vanguards "lite", fine size buckets, multipath from 1 MiB over 3 circuits, mail delayed 2 min on average): full vanguards, coarse size buckets, multipath always over 4 circuits, mail 10 min on average; adds decoys and fetch cover traffic	about 45 MiB a day, battery, mail 10 min later on average, fetching 1.5 to 2.5 times slower	3 real runs; so far only on the PC




```
STEP 0 · NAME → ADDRESS
Your node resolves shop.de from its own verified copy of the registry log. No DNS query.
```

In "Fast" mode your node connects directly; the other side then sees your IP address.

Figure 3. A request to a hidden-hosted site travels over several Tor relays. No single relay knows both you and the site.

What has been tested for real

- Hidden hosting with the complete node over the real Tor network on two days: on 27 Oct 2026 3 of 4 runs passed in Anonymous mode, on 28 Oct 2026 6 of 7 (Anonymous) and 3 of 3 (high security).
- In all **158 port checks** the owner's computer had no listening port outside 127.0.0.1 and no UDP endpoint.
- Restart with the same onion address. First fetch 5 to 88 seconds after start. After a restart on 28 Oct 8 to 190 seconds; on 27 Oct the site was once unreachable for more than 10 minutes after a restart and once only reachable after 6.7 minutes.
- Multipath: 3 MiB over 3 or 4 separate Tor circuits. Before a fix this worked in only 4 of 9 first attempts, afterwards 2 of 2.

What Mainnet cannot do

> NO MIX NETWORK
>
> In a mix network, mix nodes collect packets from many users, delay them randomly, shuffle their order and forward them – over several layers. **Mainnet does not have this.** Mainnet nodes do not collect or mix other people's traffic; only in "Fast" mode do they relay encrypted traffic for nodes behind NAT (role `relay`), without delay and without mixing. Only the sender's **own outgoing mail** is mixed (random Poisson delay, on average 2 or 10 minutes, plus decoys). Forwarding over several hops is done by Tor – without collecting and without delay per hop.

- **A very strong observer** who watches your network and the destination at the same time for a long period can correlate connections by timing and volume. Size buckets, multipath and cover traffic make this harder, not impossible.
- **Mainnet's own anonymity set is close to zero today:** two nodes, one operator, no outside users. The large crowd comes from Tor alone.
- **Size buckets** still reveal the order of magnitude; tunnels and device pairing are not padded.
- **Cover traffic** (timed decoys, fetch cover traffic) has never been tested against the real network; high security is off on the production nodes.
- **Bridges** (obfs4, Snowflake) are built but not yet passed through to Tor in the node.
- The **entry node** on the operator's VPS deliberately runs directly, with a visible IP. The onion entrance of the second node has not yet been shown to be reachable in operation.
- Mainnet does not protect against malware on your device or against your own mistakes (for example real names in a mail).

Comparison with Tor, Loopix and Nym

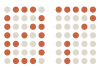
PROPERTY	TOR	LOOPIX (RESEARCH)	NYM	MAINNET TODAY
several hops	3 (onion: 6)	mix layers	3 mix layers	via Tor
collect and delay per hop	no	yes (Poisson)	yes	own outgoing mail only
cover traffic	hardly (padding only)	loop and drop	yes	high security, not tested for real
uniform packet size	cells	yes	Sphinx	size buckets

PROPERTY	TOR	LOOPIX (RESEARCH)	NYM	MAINNET TODAY
latency	low	seconds	seconds	low (mail: minutes)
anonymity set	millions	–	small	Tor's

Against a global observer, Loopix and Nym are stronger by design. Mainnet's advantage is low latency for sites and Tor's large user base.

GOAL

A real mix layer – packets of equal size, delay per hop, cover traffic – would be a new protocol with its own specification and its own audit. It only works with many independent mix nodes. Mainnet therefore lists it as a goal, not as a property.



CHAPTER 7

Encryption

Mainnet does not invent its own cryptography. It uses reviewed methods and libraries and applies them so that content is encrypted on the device. Where possible today, the methods are post-quantum hybrid: classical and post-quantum at the same time, so that breaking one of them alone is not enough.

Methods per purpose

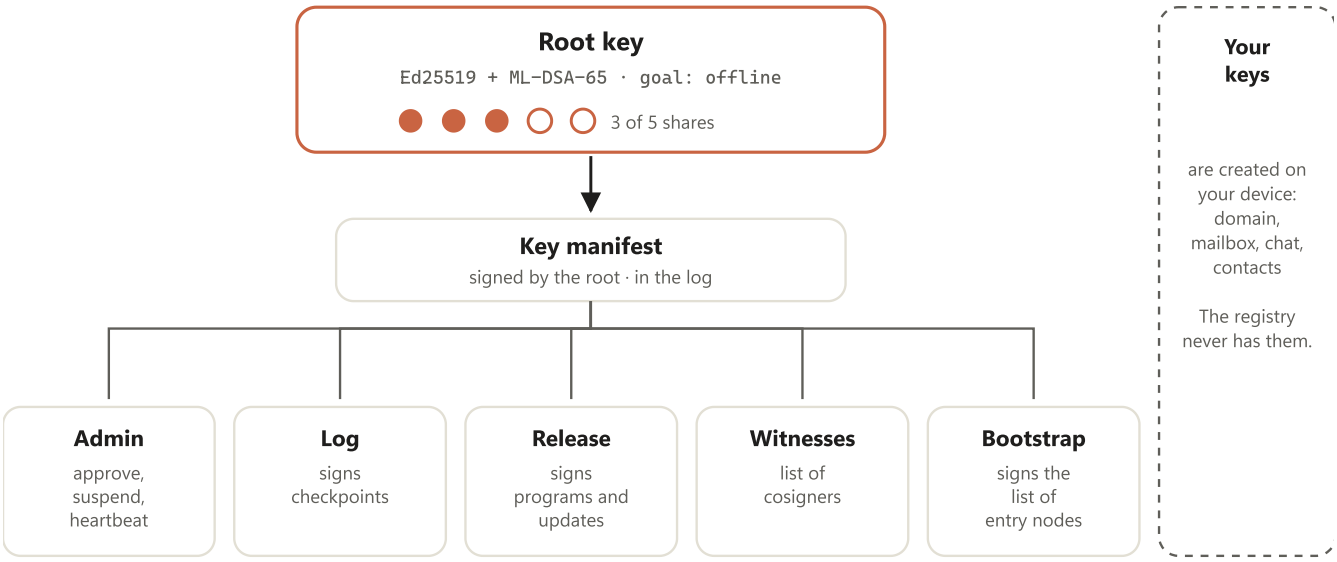
PURPOSE	METHOD	POST-QUANTUM
Mail, chat start, file keys	HPKE (RFC 9180) with **X-Wing** (X25519 + ML-KEM-768), HKDF-SHA256, ChaCha20-Poly1305	yes, hybrid
Chat history	Double Ratchet with an X-Wing step; groups of up to 256 with sender keys	yes, hybrid
Private files	XChaCha20-Poly1305 in segments; the key is only in the link	symmetric, 256 bit
Node to node (QUIC and TCP, also over Tor)	TLS 1.3 with X25519MLKEM768, tried first	yes, hybrid
Node to node (fallback over TCP)	Noise with X25519; can be switched off with `nur_post_quanten`	no
Tor path	methods of the Tor Project (Arti)	no (comes from Tor)
Log checkpoints	Ed25519 **and** ML-DSA-65 (FIPS 204), both required	yes
Root, admin, release	dual keys Ed25519 + ML-DSA-65	yes

PURPOSE	METHOD	POST-QUANTUM
Witness cosignatures	Ed25519 (C2SP tlog-cosignature)	no
Bootstrap list	Ed25519	no
Identity, zones, sites	Ed25519	no (planned for mn2)
Local vault	XChaCha20-Poly1305; key via Argon2id (256 MiB, t = 3) or the operating system's keychain	symmetric
Content addresses, checksums	BLAKE3, SHA-256	yes

WHAT "ENCRYPTED" MEANS HERE

- **Mail, chat and private files** are encrypted end to end: readable only by sender and recipient.
- **Public sites** are public and signed by their owner, not end-to-end encrypted – anyone may read them. What is protected is the path (hybrid TLS 1.3 and Tor) and authenticity (signature).
- The **portal cypherpunk2077.com** is an ordinary website with HTTPS and an onion mirror. Visitors there do not get Mainnet's protection.

Key hierarchy



Today all 5 root shares, the release key and the password file are on the operator's PC. Goal: separate, offline.

Figure 4. The root key is split into 5 shares, 3 of which are needed. It is meant to be kept offline; today it is still on the operator's PC. It only signs the key manifest, which names all other operating keys. Users' keys are separate from this.

- **Root:** dual key, split into 5 shares (Shamir, 3 of 5); signs manifests only.
- **Admin:** approve, suspend, heartbeat. Login to the panel with admin file and PIN; every action double-signed (today in a separate public file, not yet in the log); suspensions are recorded in the log with a reason code.
- **Log:** signs checkpoints. **Witnesses:** listed in the manifest with their keys.

- **Release:** signs programs and updates. A node installs an update only after asking, only over Tor and only if signature and checksum match.
- **User keys** are created on the user's device. Buying a domain buys only the approval; the key belongs to the buyer alone.

> LIMIT TODAY
>
> At launch, all five root shares, the release key and the password file are on the same computer of the operator. Root, admin, log and witnesses are therefore only as secure as that one computer today. Goal: shares and release key in separate places, offline signing.

CHAPTER 8

Mail, chat and hosting

Every domain comes with mail and a site. On top come chat, contacts, files, search and tunnels. Everything runs over the same node and the same keys.

Mail

- Every domain has mail; the mailbox is a key. `postmaster@` receives, among other things, the expiry reminders.
- Post offices only hold **encrypted envelopes** until the recipient collects them (the role is off by default and can be switched on voluntarily; then 1 GiB, kept for at most 90 days). The recipient appears there only as a blinded daily identifier.
- Against spam: a small proof of work for senders the recipient does not know; the recipient sets its size.
- Mail to ordinary internet addresses is a draft: only for explicitly approved users, via a separate server, never with forged senders. **Not built.**

Status: code complete, tested locally between nodes, with mixing and decoys. Both production nodes have the post-office role switched on. Not yet tested over the real Tor network between two computers.

Chat and contacts

- 1:1 and groups of up to 256 members, Double Ratchet with X-Wing.
- Contacts via a contact code, safety number or QR code; verification with a shared secret (SPAKE2). If a verified contact's key changes, Mainnet stops sending and asks.

Status: code complete, tested locally with three nodes. Not in the real network; the construction is to be reviewed externally.

Hosting: a site as one file

- The SDK packs a folder – pages, images and server logic – into **one `.site` file** (default up to 20 MiB, at most 200 MiB). Server logic runs as WebAssembly in the node; Rust, C/C++ and Go are supported, other languages experimental.
- Everyone hosts their own site: on a PC, VPS or Raspberry Pi. The default is **hidden** through an onion service; “host directly” is faster but shows the IP.
- Publish with the deploy key file or in the browser's **Studio**: editor with live preview, publishing after confirmation.

Status: code complete, tested locally, disposable hidden sites served over the real Tor network. No user's site on the network yet.

Search

Search only finds approved Mainnet sites. Goal: indexers are run only by independent nodes, not by the registry. Today one (empty) indexer runs on the operator's VPS. Queries always go over Tor. **Honestly:** the indexer sees the search terms – it is not end-to-end search. Today no indexer is connected in the portal.

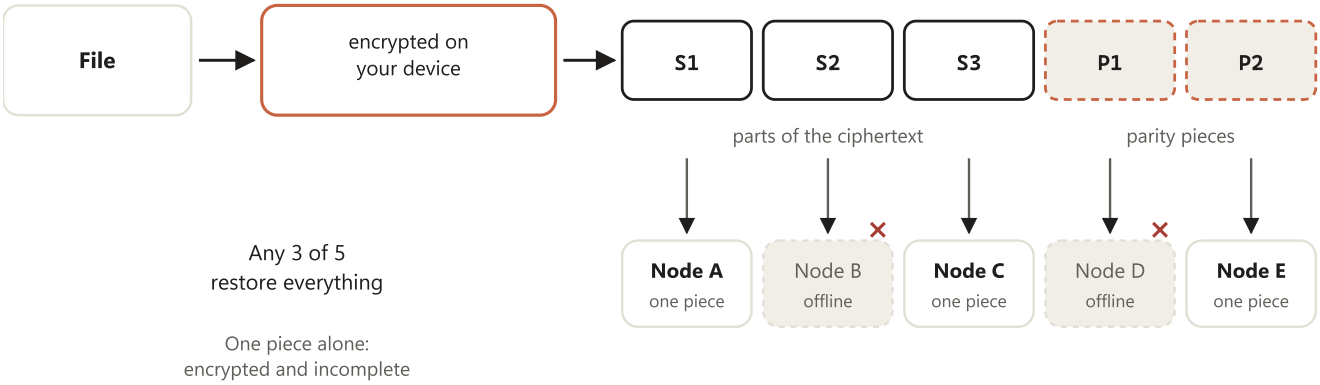
Tunnels

Make SSH, a game server or a local web app reachable over Mainnet, as a port on 127.0.0.1, only with permission per peer. Status: preview, tested locally.

CHAPTER 9

Distributed storage

Private files and mail are split into pieces after encryption and spread over different nodes. A single node then only holds an encrypted, incomplete piece. Reassembly and decryption happen only on the user's device.



IN OPERATION TODAY · 2 NODES

Mirrored instead of split: each node holds a complete, encrypted copy.

From 3 storage providers data is split 2 of 3, from 5 fully 3 of 5.
The program does not check whether the nodes are independent.

Figure 5. Top: the method for files (3 of 5): two nodes may fail. Bottom: the state in operation with two nodes.

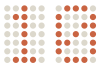
Method

- Encrypt first, then split: a systematic Reed-Solomon erasure code over GF(2^{16}). The first k pieces are parts of the ciphertext, the rest are parity pieces.
- **Files 3 of 5**, **mail 2 of 3**: any k pieces are enough.
- Each piece has a BLAKE3 address and a checksum. The result is checked against the identifier of the whole ciphertext; forged pieces are detected. At most 256 combinations are tried so that forgeries cannot cause heavy computation.
- Each storage node receives at most one piece of a file.

IN OPERATION TODAY

- With **two** storage nodes data is **mirrored** (1 of 2): each node holds a complete, encrypted copy. That gives resilience, but not the protection of splitting.
- Mail goes as a whole encrypted envelope to both post offices; 2 of 3 needs at least three post offices.
- Splitting over the real Tor network has never run. Providers are only searched among connected nodes.
- Both nodes belong to the same operator today.

Goal: splitting switches on without changing the program: for files from three storage providers as 2 of 3, from five fully as 3 of 5; for mail from three post offices. The program does not check whether the nodes are really independent – splitting only helps with nodes that do not belong to the operator.



CHAPTER 10

Running a node

Mainnet lives through its nodes. Every user has one; whoever wants to contribute more keeps it running and switches on roles such as post office or storage.

Roles of a node

ROLE	TASK	DEFAULT
`dht`	help find other nodes and records	on
`relay`	in “Fast” mode relay encrypted traffic for nodes behind NAT (no mixing)	on, can be switched off
`store`	hold encrypted pieces of private files	off; can be switched on voluntarily (desktops donate no storage by default)
`mailbox`	post office for encrypted mail envelopes	off; can be switched on voluntarily, then 1 GiB, kept for at most 90 days
`search`	indexer for search	off
`cache`	cache sites you have viewed yourself	on, 2 GB, can be switched off

A node only stores encrypted pieces and envelopes it cannot open, plus its own sites and the cache of sites visited by its user. Every role can be switched off. In the default Anonymous mode the node opens no listening port outside 127.0.0.1 (only the local API listens there); it only makes outgoing connections to Tor.

In operation today

- **Node 1 (VPS):** entry point for new nodes, post office, storage, (empty) indexer. Deliberately runs directly with a public IP and additionally has an onion entrance.
- **Node 2 (operator's PC):** post office and storage, only over Tor. Its onion entrance sometimes reports failed descriptor uploads; reachability from outside has not been shown yet.
- The VPS hosting provider filters a large share of Tor exits (about 80 %). Nodes therefore fetch log and bootstrap list via the portal's onion mirror first.

WANTED

For splitting, independent witnesses and a real anonymity set, Mainnet needs nodes run by many different people, in different networks and countries. As soon as the first signed release is published, anyone can start a node. There is a separate package with instructions for witnesses.

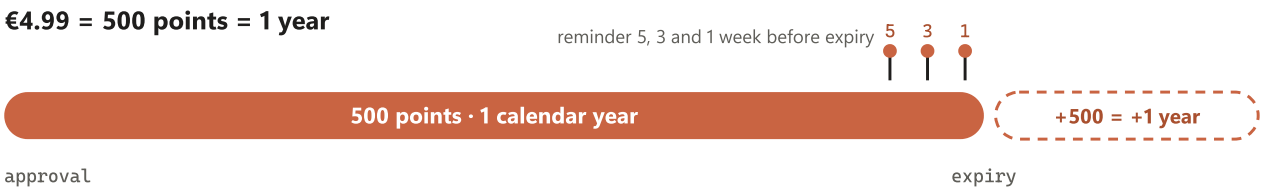
DECIDED, NOT BUILT

Points for node operators (decision of 30 Oct 2026): from 2027, at most 250 points per domain, only as a discount on one's own domain, not paid out. Proven contribution is rewarded – spot checks whether stored pieces are really present, with a warm-up period (the Storj pattern). The hard part remains measuring contribution without monitoring users, and excluding fake nodes. There is no mining and no reward in a cryptocurrency. It will only be advertised once it is built.

CHAPTER 11

Domains and points

A domain costs €4.99 a year – the same for every extension, with no premium names. Payment is in bitcoin; accounting is in points.



500	1,000	250	≤ 10 y.
1 year €4.99 in bitcoin	2 years also at once	about ½ year minimum for a new domain	anything above is refunded

Paid too much or too little? It is converted into points (±1 % counts as exact).

The public log only shows the expiry date – no amounts, no people.

Figure 6. 500 points keep a domain for exactly one calendar year. Top-ups are possible at any time; reminders go out 5, 3 and 1 week before expiry.

Rules

- **€4.99 = 500 points = exactly one year** (same day, same time UTC). The first approval lasts one year, then 500 points extend it by another year each – or more at once.
- **Bitcoin** via a self-hosted BTCPay server; every invoice has its own address and a unique amount.

- **Different amounts** are converted into points: too little gives less, too much gives more time (±1 % counts as exact). Minimum for a new domain is 250 points, for a renewal 10. Anything beyond 10 years is refunded. Points are credited after review, within 24 to 48 hours.
- Points belong to exactly one domain; they cannot be transferred or paid out.
- **Public** is only the expiry date in the log – no amounts and no people. Bitcoin payments themselves are public in the bitcoin blockchain.
- Reminders go to the domain's `postmaster@`, without payment links (phishing protection). Top-ups only through the browser, the command line or the purchase chat.

Review before approval

The operator approves every domain by hand. The review covers **name, brand and payment, not content**. Content is assessed after a report against the terms of use; suspensions are recorded in the log with a reason code, and appeals are possible.

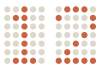
- **Well-known brands and companies** are given only to whoever proves that the name is theirs: via a **DNS TXT record** in the company's real internet domain, which only its owner can set (decided on 30 Oct 2026). A company has priority only if its domain or brand is older than the Mainnet entry. The proof shows control over the domain, not trademark rights. **The automatic proof is not built yet**; until then the operator checks by hand.
- **Generic words** such as “shop” or “insurance” get no priority through the DNS proof. Common words are available at most **once per person**.
- **Operator's reserve:** the operator holds back some sought-after generic names. The list will be **published before advertising starts** and contains no third-party brands. From 2027 these names are allocated by a **verifiable lottery** at the normal price, by 31 Dec 2027 at the latest; participants in the lottery deposit €4.99.
- **The operator's launch domains**, public in the log: `mainnet.com`, `cypherpunk2077.com`, `cypherpunk2077.de`, `test.net`, `shop.com`, `revaultstudio.com`. A trademark check for `shop.com` is still pending. The labels `mainnet` and `cypherpunk2077` are also protected.

TODAY

Purchase chat, BTCPay and admin panel are built and tested in the test network (bitcoin regtest), but **not yet in operation**. No purchase with real bitcoin has taken place yet. The operator approved the six launch domains free of charge; this is recorded publicly in the log with a reason code.

DECIDED ON 30 OCT 2026, NOT YET IN OPERATION

- **Free launch offer:** registrations received by 31 Dec 2026 are free; late ones are approved by 31 Jan 2027. At most 300 approvals per day, at most 3 domains per person, a queue of up to 3,000, with a daily lottery if demand is high. Term 1 year, after that the 500-point logic applies. The log records the public reason code “free of charge by the operator”. Today the admin panel allows at most 10 free approvals per 24 hours without an additional root approval; implementation of the offer is under way.
- **Points for node operators** from 2027, at most 250 points per domain (chapter 10).
- **Marketplace** at first only as a showcase of sites' business cards: no trading, no payment, no escrow.



CHAPTER 12

Security and testing

Mainnet is tested a lot, but so far only by its own developers. There is no external audit yet. Until then Mainnet is a beta and unreviewed.

2,215
of 2,215 tests green (28 Oct 2026)

106
property tests for parsers of untrusted input

14
fuzzing targets, 10 min each, ≈ 20 million inputs

3
internal reviews, all critical and high findings fixed

What is checked

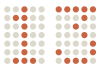
- **Automated tests** for every crate, end-to-end tests with several nodes in one process, a test network in Docker with 6 nodes, log service, witnesses and bitcoin regtest.
- **Robustness:** property tests over all parsers; fuzzing found one bug, which is fixed.
- **Real Tor tests** on two days (chapter 6).
- **Mandatory checks before launch** (go/no-go): secret scan over everything that is published, portal check over Tor (602 of 604 on 29 Oct; the two red ones concerned the log, which did not exist yet), server hardening without errors.
- **Updates** only signed, only over Tor and only after asking; tampered files are rejected (tested, never run with a real release).

Protective features

- **Tripwires:** real-looking decoys on the registry's servers; touching one raises an alarm. They are running; alarms currently only go to the log.
- **Self-test "Am I protected?"** in the browser (built into the app, but the app has never been started on a device): leaks around Tor, clock, version.
- **Heartbeat:** the operator is meant to sign a heartbeat into the log regularly; the first one has been there since 29 Oct 2026 (entry 12); if it is missing, the programs warn after 14 or 30 days. This never automatically grants anyone else any rights.
- **Data minimisation:** no cookies, no trackers, no IP logs in the portal, visitors counted only as daily totals. This is a pledge that cannot be verified from outside – over Tor it is not needed.

> NO EXTERNAL AUDIT
>
> A package for a security firm is ready but has not been commissioned. Internal reviews and many tests do not replace an independent review. We especially want reviewed: chat construction (Double Ratchet with X-Wing), registry log and witnesses, Tor integration, update path.

Please report security issues as described in `cypherpunk2077.com/.well-known/security.txt`, over Tor if you like. Honest research is welcome.



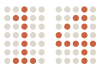
CHAPTER 13

Limits and risks

This chapter collects what Mainnet does not provide today – as completely as possible, even where points are already stated in other chapters.

1. **Beta without external audit.** Bugs are likely; anyone whose safety depends on it should not rely on Mainnet alone today.
2. **Two nodes, one operator.** Mainnet's own layer has no anonymity set yet; splitting does not take effect.
3. **Witnesses run by the operator.** The log is verifiable but not yet tamper-proof towards the operator. The admin double signature is not yet in the log, and the brake against mass suspensions only works in the admin panel, not in the protocol.
4. **Keys in one place.** Root shares, release key and password file are on one computer at launch.
5. **No mix network.** Against a very strong observer of both ends, Mainnet helps only to a limited degree.
6. **No release yet.** The programs are built but neither signed nor published; the existing release draft is out of date. There is no installer and no code-signing certificate yet; Windows will warn at first.
7. **Entry only with a ready-made configuration.** The root fingerprint and the bootstrap key are not yet built into the program. A fresh node finds neither the network nor the names without a supplied configuration.
8. **Much only tested locally.** Mail and chat have never run between two computers over the real Tor network, nor has splitting. Cover traffic has never been tested against the real network. Search is not connected in the portal.
9. **Android app never started.** The app is built but has never run on a device; iOS is not built.
10. **Bridges missing in the node.** obfs4 and Snowflake are built but not yet passed through to Tor in the node. Where Tor is blocked, Mainnet does not get through today.
11. **Classical signatures.** Users, zones, sites, the bootstrap list and witnesses sign with Ed25519 only, so not post-quantum secure.
12. **Search sees search terms.** The indexer learns what is searched for – not who is searching.
13. **Purchase chat in an ordinary browser.** Whoever opens the purchase chat in an ordinary browser trusts the code the site delivers. Safest are `mainnet chat` or the Mainnet Browser; the web-chat fallback is only classically encrypted.
14. **Central allocation.** The operator can suspend domains – on purpose, under the terms of use and publicly in the log. Mainnet is meant to keep running against attackers, not against its legitimate operator.
15. **Registry outage.** Without a running log service there are no checkpoints, approvals or suspensions. After 24 hours nodes show names as “unverified”; existing sites keep resolving. An emergency kit for restarting is built but not yet in operation.
16. **Limits of Tor.** Tor is slower than direct connections, can be blocked, and after start it takes a few minutes until a hidden site is reachable.
17. **Network filters.** The hosting provider of the entry node filters many Tor exits; Mainnet falls back to onion addresses.
18. **Legal.** No legal entity in Germany, the operator's company is based abroad, no imprint; the legal and tax review is still pending.

19. **Bitcoin.** Payments are public in the bitcoin blockchain; the exchange rate fluctuates.
20. **Your device.** Malware, an unencrypted computer or a shared key defeat any protection.
21. **Browser base.** The Mainnet Browser is built on Qt WebEngine (Chromium) and must adopt its security updates promptly.



CHAPTER 14

Roadmap

The order is fixed, the dates are not. A step only counts as done once it runs in real operation.

`today · 30 Oct 2026`

Beta online

- Portal with onion mirror
- Registry log, checkpoint 13
- Heartbeat
- 2 nodes run by the operator

`next steps`

First release

- Node and browser signed for download
- Release key offline
- Admin panel and bitcoin purchase
- Daily emergency backup

`then`

Becoming independent

- ≥ 3 independent witnesses
- Nodes run by others; from 5, splitting takes effect
- Installer, Android app on devices
- Bridges in the node

`goal`

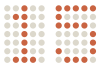
Reviewed and stronger

- External audit
- Post-quantum signatures for users and witnesses (mn2)
- Research: mix layer

Decided, not yet built

- Free launch offer: received by 31 Dec 2026, approved by 31 Jan 2027 (chapter 11).
- Proof for company domains via DNS TXT; reserve list and lottery from 2027.
- Points for node operators from 2027, at most 250 points per domain.
- Marketplace at first as a showcase.
- Mail to ordinary internet addresses for approved users (draft).

The operator decided these points on 30 Oct 2026 (outgoing mail on 29 Oct); they are not yet built or in operation. Until then they are not properties of Mainnet.



CHAPTER 15

Glossary

Beta	In operation, but unfinished and without an external audit.
BLAKE3, SHA-256	Hash functions: a short fingerprint of any data.
Bootstrap list	Signed list of entry nodes through which a new node finds the network.
Checkpoint	Signed state of the registry log: size, root hash, time.
Cover traffic	Extra traffic without payload so that real traffic does not stand out.
Decoy	An encrypted message without content that looks like a real one; makes learning from timing and volume harder.
Double Ratchet	Method for chats that derives new keys for every message.
Ed25519	Classical signature method; fast, not post-quantum secure.
Guard	First Tor hop; sees the IP address but not the destination.
Heartbeat	Entry regularly signed by the operator in the log; if it is missing, the programs warn.
HPKE	Standard (RFC 9180) for encrypting data to a public key.
k of n	Split data into n pieces, any k of which are enough to restore it (Reed-Solomon).
Merkle tree	Hash tree that gives short proofs that an entry is in the log and that the log has only grown.
Mix network	Network of mix nodes that collect, delay and forward packets from many users in shuffled order. Not present in Mainnet.
ML-KEM-768, ML-DSA-65	NIST post-quantum methods for key exchange (FIPS 203) and signatures (FIPS 204).
Multipath	Sending parts of a transfer over separate Tor circuits.
Node (`mainnetd`)	The program that carries the network on every computer.
Onion service	A service reachable over Tor whose location is protected by Tor.
Points	Unit of domain lifetime: 500 points = one year = €4.99.
Post office	Node that holds encrypted mail envelopes until the recipient collects them.
Post-quantum hybrid	Classical and post-quantum method at the same time; protected as long as one of the two methods is not broken.
Registry	cypherpunk2077.com: allocates and reviews names, runs the log, distributes the programs.
`.site`	One file containing a whole website including server logic as WebAssembly.
Tripwire	Decoy on the registry's servers; touching it raises an alarm.
Vanguards	Fixed Tor relays near an onion service against attacks that try to find its guard.
Witness	Independent party that cosigns checkpoints and refuses forks.
X-Wing	Hybrid key exchange made of X25519 and ML-KEM-768.

About this document. Mainnet Whitepaper, version 0.1, beta, as of 30 October 2026. It describes the state of the project on that day and will be updated with the project; older versions are then superseded. The terms of use at cypherpunk2077.com/regeln are binding for using Mainnet; the German version of this whitepaper is binding over this translation. This document does not promise features, dates or security and is not investment advice. Checksums of the PDF files are published at cypherpunk2077.com/whitepaper. Please report security issues as described in cypherpunk2077.com/.well-known/security.txt.