



Mainnet Whitepaper

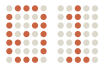
Ein eigenes, verschlüsseltes Netz über dem Internet: eigene Domains, eigene Mail, eigener Browser. Was gebaut ist, was läuft und was noch fehlt.

• Beta • kein externes Audit • 2 Knoten

INHALT

01	Zusammenfassung	3
	Mainnet in einer Seite – und der ehrliche Stand	
02	Das Problem	4
	Namen, Metadaten, Vertrauen – und warum Werkzeuge allein nicht reichen	
03	Was Mainnet ist	5
	Overlay-Netz, Rollen, Endungen, Programme	
04	Architektur	7
	Acht Schichten von Transport bis Betrieb, und wie reif jede ist	
05	Namen und Registry-Log	9
	Merkle-Log, Checkpoints, Zeugen – und was heute noch fehlt	
06	Anonymität: was Mainnet kann und was nicht	11
	Tor als Standard, Hochsicherheit, kein Mix-Netz, ehrlicher Vergleich	
07	Verschlüsselung	14
	Verfahren je Zweck, post-quanten wo möglich, Schlüssel-Hierarchie	
08	Mail, Chat und Hosting	16
	Was man im Mainnet tut – und wie weit es ist	
09	Verteilte Speicherung	17
	k von n: erst verschlüsseln, dann zerstückeln – heute noch gespiegelt	
10	Knoten betreiben	18
	Wer einen Knoten betreibt, was er speichert, was heute läuft	
11	Domains und Punkte	20
	500 Punkte = 1 Jahr, Bitcoin, Prüfung, Reserve, Gratis-Aktion	
12	Sicherheit und Prüfungen	21
	Tests, interne Reviews, echte Tor-Tests – kein externes Audit	
13	Grenzen und Risiken	22
	Was man wissen muss, bevor man Mainnet vertraut	
14	Roadmap	24
	Was als Nächstes kommt – in Reihenfolge, ohne erfundene Termine	
15	Glossar	25
	Begriffe von Attrappe bis Zeuge	

Jede Aussage in diesem Dokument ist einer von vier Reifestufen zugeordnet: **Code fertig**, **lokal getestet**, **echt getestet** (echtes Tor-Netz) und **in Betrieb**. Was nur Ziel ist, steht ausdrücklich als Ziel da.



Zusammenfassung

Mainnet ist ein eigenes Netz über dem Internet: eigene Domains wie `shop.de` oder `atelier.cp77`, eigene Mail, eigener Browser. Standardmäßig läuft alles über Tor. Mail, Chat und private Dateien werden auf deinem Gerät Ende-zu-Ende verschlüsselt; der Schlüsselaustausch ist post-quanten-hybrid, die Signaturen der Nutzer sind noch klassisch. Wem welcher Name gehört, steht in einem öffentlichen Log, das nur wachsen kann und das jeder Knoten selbst nachprüft.

● Gebaut und lokal getestet

- Knoten `mainnetd` mit eingebautem Tor
- Mail, Chat, Kontakte, Tunnel
- Hosting als `.site` (WebAssembly)
- Zerstückeln k von n, Hochsicherheit
- Mainnet Browser, Studio, Suche

● Läuft heute

- Portal cypherpunk2077.com mit Onion-Spiegel
- Registry-Log, Checkpoint 13, 3 Kosignaturen
- Signiertes Lebenszeichen im Log
- 2 Knoten, beide beim Betreiber

○ Noch nicht

- Release zum Download (signiert)
- Unabhängige Zeugen
- Zerstückeln im Betrieb
- Mix-Netz
- Kauf mit echtem Bitcoin
- Externes Audit

28

Rust-Crates

2.215

von 2.215 Tests grün im letzten vollen Lauf (28.10.; seitdem nicht wiederholt)

158

Port-Prüfungen über Tor, kein Port offen

0

externe Audits bisher

Was Mainnet besser machen will

- **Namen ohne Torwächter.** Jede Wunsch-Endung, ein Preis für alle (4,99 € im Jahr), keine Premium-Namen. Bekannte Marken nur für ihre Inhaber.
- **Verschlüsselung als Grundeinstellung.** Inhalte entstehen verschlüsselt auf dem Gerät. Der Verwalter kann Mail, Chats und private Dateien der Nutzer nicht lesen, weil er die Schlüssel nie bekommt.
- **Nachprüfbare Vergabe.** Jede Freischaltung, Verlängerung und Sperre steht im öffentlichen Log, Sperren mit Grund-Code. Ziel: Ein Knoten glaubt dem Verwalter nichts, was er nicht selbst prüfen kann. Heute prüft der Knoten Signaturen und Konsistenz; die Zeugen stehen noch beim Betreiber.
- **Alles in einem Programm.** Namen, Seiten, Mail, Chat, Dateien und Suche statt einzelner Werkzeuge, die man selbst zusammensetzen muss.

EHRLICHER STAND

Mainnet ist eine **Beta**. Heute laufen **zwei Knoten, beide beim Betreiber**, und drei Start-Zeugen, ebenfalls beim Betreiber. Für Außenstehende gibt es noch **kein signiertes Release** zum Herunterladen. Ein **Mix-Netz**, in dem Knoten fremden Verkehr sammeln, mischen und weitergeben, **gibt es nicht**. Ein externes Audit fehlt. Die Ziele sind auf der Code-Ebene weitgehend erreicht, im echten Betrieb noch nicht.



KAPITEL 2

Das Problem

Das Internet funktioniert. Aber wer es benutzt, gibt dabei mehr preis als nötig, und wer darin einen Namen haben will, ist auf wenige Stellen angewiesen.

1. Namen gehören wenigen

Domain-Endungen werden von wenigen Organisationen verwaltet. Gute Namen sind seit Jahren vergeben oder werden teuer weiterverkauft; manche Endungen kosten ein Vielfaches anderer. Wer die Endung kontrolliert, kann einen Namen sperren oder umleiten – oft ohne dass Nutzer es nachprüfen können.

2. Metadaten verraten mehr als Inhalte

Selbst wenn eine Verbindung verschlüsselt ist, bleibt sichtbar, wer wann mit wem spricht, wie oft und wie viel. DNS-Anfragen zeigen dem Anbieter, welche Seiten jemand aufruft. Cookies und Tracker verbinden Besuche über viele Seiten hinweg zu einem Profil.

3. Vertrauen in viele fremde Stellen

HTTPS stützt sich auf Hunderte Zertifizierungsstellen, und jede davon kann für jede Domain ein Zertifikat ausstellen. Transparenz-Logs (Certificate Transparency) machen Fehler sichtbar – erst nachträglich. Mail hängt an Anbietern, die Inhalte lesen können, und an Telefonnummern.

4. Gute Werkzeuge, aber getrennt

Tor schützt den Weg sehr gut, hat aber keine merkbaren Namen (eine Onion-Adresse hat 56 Zeichen), keine Mail und kein einfaches Hosten. Verschlüsselte Messenger lösen Chat, nicht Seiten. Wer alles will, setzt viele Programme zusammen und macht dabei leicht Fehler.

WAS MAINNET DARAUSS MACHT

- ein eigener Namensraum mit öffentlichem, nachprüfbarem Log statt einer Kette von Vertrauensstellen,
- Tor als Standard-Transport, ergänzt um Maßnahmen gegen das Ablesen aus Zeit und Menge,
- Ende-zu-Ende-Verschlüsselung in Mail, Chat und Dateien, mit Schlüsseln nur beim Nutzer,
- ein Programm für alles: Knoten, Browser, Mail, Chat, Hosting.



KAPITEL 3

Was Mainnet ist

Mainnet ist ein **Overlay-Netz**: Es läuft über das Internet, hat aber eigene Namen, eigene Regeln für Verschlüsselung und einen eigenen Browser. Jeder Nutzer betreibt einen Knoten. Vergeben werden die Namen an einer Stelle, betrieben wird das Netz verteilt.

Vergabe zentral, Betrieb verteilt

cypherpunk2077.com ist nur der Verwalter: Es vergibt und prüft Namen, führt das Registry-Log und liefert die Programme aus. Es hostet keine Websites. Fremde Inhalte liegen auf Rechnern des Verwalters höchstens verschlüsselt – als Mail-Umschläge und Datei-Stücke auf den beiden Start-Knoten, die der Verwalter nicht öffnen kann.

Seiten, Postfächer und Dateien liegen bei ihren Inhabern und auf den Knoten der Nutzer. Ein Knoten kennt eine Kopie des Logs und löst Namen selbst auf. Fällt cypherpunk2077.com aus, laufen bestehende Seiten weiter; neue Freischaltungen und Sperren gibt es dann nicht (Kapitel 13).

Rollen

ROLLE	WER	WAS
Nutzer	jeder	surft, schreibt Mail und Chats; sein Knoten läuft im Hintergrund
Inhaber	wer eine Domain hat	hält den Schlüssel der Domain, hostet die Seite selbst (PC, VPS, Raspberry Pi)
Knoten	jedes laufende <code>mainnetd</code>	findet andere Knoten, speichert verschlüsselte Stücke, liefert eigene Seiten aus
Postamt	Knoten mit Rolle <code>mailbox</code>	hält verschlüsselte Mail-Umschläge, bis der Empfänger sie abholt
Indexer	Ziel: unabhängige Knoten; heute ein (leerer) Indexer auf dem VPS des Betreibers	bauen den Suchindex freigeschalteter Seiten
Zeuge	unabhängige Dritte (Ziel)	kosignieren Checkpoints des Logs und lehnen Gabelungen ab
Verwalter	cypherpunk2077.com	prüft und vergibt Namen, sperrt nach den Nutzungsregeln, signiert Releases

Eigene Endungen

Jede Wunsch-Endung mit 2 bis 20 Buchstaben ist möglich: `.com`, `.de`, `.net`, `.org`, `.cp77` und neue wie `.atelier`. Der Namensraum ist vom alten Internet getrennt: `shop.de` im Mainnet ist nicht dieselbe Seite wie `shop.de` im Internet. Damit es keine Verwechslung gibt, zeigt der Mainnet Browser bei jeder Mainnet-Seite das

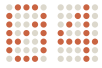
Abzeichen ♦ **Mainnet** und trennt Mainnet und altes Internet in eigene Profile. Reserviert sind unter anderem `.onion`, `.local`, `.test` und Datei-Endungen.

Programme

PROGRAMM	AUFGABE	STAND
<code>mainnetd</code>	der Knoten (Rust): Netz, Tor, Log-Spiegel, Mail, Speicher, Hosting, lokale API	gebaut, getestet, 2 Knoten in Betrieb
Mainnet Browser	Browser auf Qt WebEngine mit Abzeichen, getrennten Profilen, Mail, Chat, Studio	gebaut (Windows), lokal getestet
<code>mainnet</code>	Befehlszeile: Schlüssel, Domains, Veröffentlichen, Mail	gebaut, getestet
App	Android mit Leicht-Knoten (iOS geplant)	gebaut, nie auf einem Gerät gestartet
SDK, Studio	Seiten als eine <code>.site</code> -Datei bauen und veröffentlichen	gebaut, lokal getestet

Mainnet und das alte Internet im Vergleich

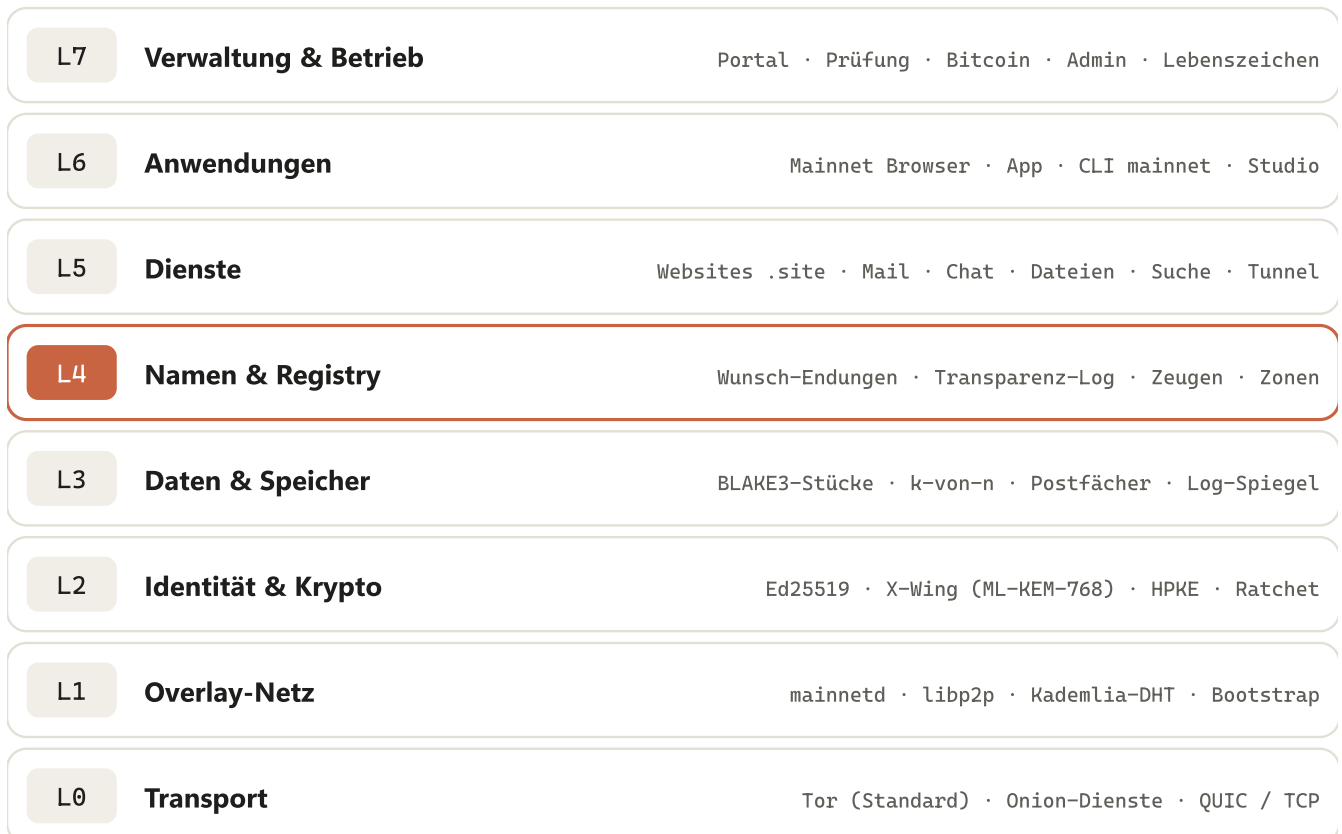
THEMA	ALTES INTERNET	MAINNET
Namen	viele vergeben, Preise je Endung	frischer Namensraum, 4,99 € im Jahr für alle Endungen
Anmelden	Passwort, Cookies	ein Schlüssel auf deinem Gerät
Verschlüsselung	Transport ja, Inhalte selten	Transport und Inhalte (Mail, Chat, private Dateien)
Vergabe	schwer nachprüfbar	öffentliches Log, jeder Knoten prüft
Tempo	schnell	langsamer über Tor; Modus „Schnell“ wählbar
Reife	Jahrzehnte im Einsatz	Beta , ohne externes Audit
Zugang	jeder Browser	eigenes Programm nötig ; noch kein Release



KAPITEL 4

Architektur

Mainnet ist in acht Schichten gebaut. Jede Schicht hat eine klare Aufgabe und nutzt nur die darunter. So lässt sich jede für sich prüfen und austauschen.



Jede Schicht nutzt nur die darunter. Hervorgehoben: L4, das eigene Namenssystem mit öffentlichem Log.

Abbildung 1. Die Schichten L0 bis L7. L0 ist der Transport, L7 der Betrieb durch den Verwalter.

Die Schichten kurz

- **L0 Transport.** Standard ist Tor, eingebettet über Arti (die Rust-Fassung von Tor). Im Modus „Schnell“ gehen Verbindungen direkt über QUIC oder TCP.
- **L1 Overlay-Netz.** `mainnetd` auf Basis von libp2p: Kademlia-DHT zum Finden, eine signierte Bootstrap-Liste zum Einstieg, Grenzen gegen Überlast.
- **L2 Identität und Krypto.** Ein Schlüssel statt Passwort; Unterschlüssel für Mail, Chat und Geräte. Details in Kapitel 7.
- **L3 Daten und Speicher.** Inhalte als BLAKE3-adressierte Stücke, verteilte Speicherung k von n, Postfach-Speicher, lokale Kopie des Logs.
- **L4 Namen und Registry.** Das eigene Namenssystem mit Transparenz-Log, Zeugen und vom Inhaber signierten Zonen (Kapitel 5).
- **L5 Dienste.** Websites, Mail zu jeder Domain, Chat, Dateien, Suche, Tunnel (Kapitel 8).

- **L6 Anwendungen.** Browser, App, Befehlszeile, Studio.
- **L7 Verwaltung und Betrieb.** Portal, Prüfung, Zahlung in Bitcoin, Admin-Panel, Lebenszeichen, Stolperdrähte.

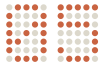
Reifegrad je Baustein

„Fertig“ heißt bei Software viererlei. Die Tabelle zeigt für jeden Baustein, wie weit er ist.

BAUSTEIN	CODE	LOKAL	ECHT	BETRIEB	ANMERKUNG
Knoten mainnetd, Modus Anonym	●	●	●	⦿	Standard seit 28.10.; der Einstiegsknoten auf dem VPS läuft absichtlich direkt
Verborgenes Hosten (Onion)	●	●	●	⦿	echte Tests an 2 Tagen; im Betrieb scheitert der Deskriptor-Upload des PC-Knotens zeitweise
Registry-Log + Zeugen	●	●	●	⦿	läuft, Checkpoint 13; die 3 Zeugen stehen beim Betreiber
Mail Ende-zu-Ende	●	●	○	⦿	beide Knoten sind Postamt; noch keine fremden Nutzer
Chat, Kontakte	●	●	○	○	1:1 und Gruppen bis 256
Hosting .site, Studio	●	●	⦿	○	Server-Logik als WebAssembly; noch keine Seite eines Nutzers
Hochsicherheits-Modus	●	●	⦿	○	3 echte Läufe; Deckverkehr nie gegen das echte Netz
Zerstückeln k von n	●	●	○	○	mit 2 Knoten wird gespiegelt
Suche	●	●	○	○	Indexer ohne Dokumente, im Portal nicht angebunden
Tunnel	●	●	○	○	Vorschau
Brücken (obfs4, Snowflake)	●	●	⦿	○	im Knoten noch nicht an Tor durchgereicht
Mainnet Browser	●	●	○	○	gebaut, nur als ZIP, unsigned
Android-App	⦿	⦿	○	○	nie auf einem Gerät gestartet; iOS nicht gebaut
Kauf mit Bitcoin, Admin-Panel	●	●	○	○	nur im Testnetz (Regtest)
Signiertes Release, Updates	●	●	○	○	Entwurf liegt vor, nicht signiert, nicht veröffentlicht
Mix-Netz	○	○	○	○	nicht gebaut (Kapitel 6)

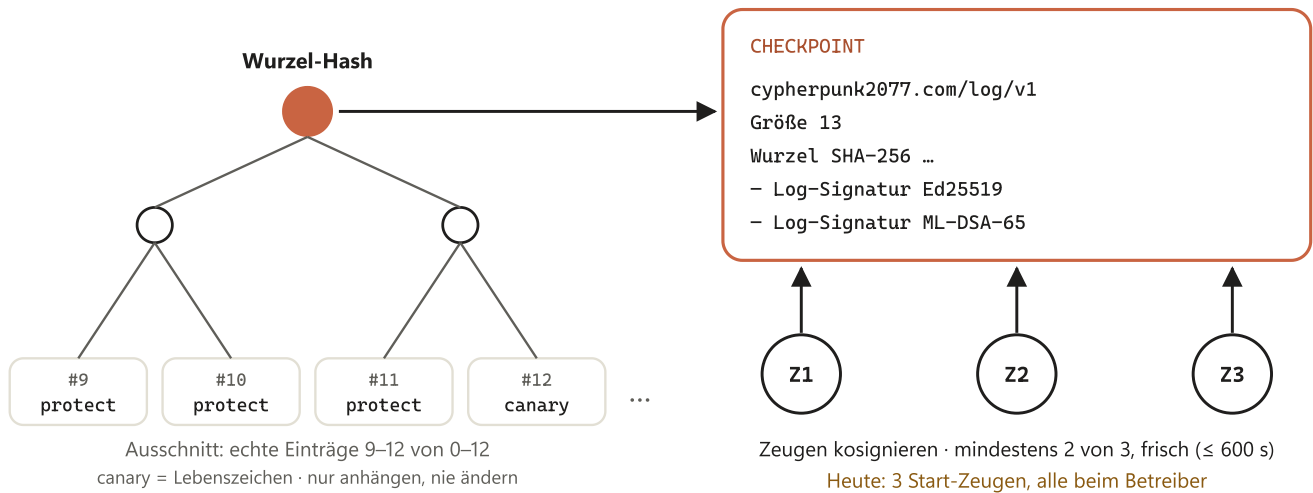
● ja ⦿ teilweise ○ nein **lokal** = automatische Tests auf einem Rechner **echt** = über das echte Tor-Netz

Betrieb = läuft auf den 2 Knoten



Namen und Registry-Log

Wem ein Name gehört, entscheidet der Verwalter. Aber jede Entscheidung wird öffentlich in einem Log festgehalten, das nur wachsen kann, und jeder Knoten prüft es selbst. Nachträgliche Änderungen fallen auf, sobald unabhängige Zeugen prüfen; heute stehen die Zeugen noch beim Betreiber.



JEDER KNOTEN PRÜFT

beide Log-Signaturen + ≥ 2 Zeugen · Konsistenz zum letzten Stand · Gabelung = Beweis für alle

Abbildung 2. Einträge bilden einen Merkle-Baum. Ein Checkpoint hält Größe und Wurzel fest und ist doppelt signiert. Zeugen kosignieren; Knoten akzeptieren nur Checkpoints mit mindestens zwei frischen Kosignaturen.

So funktioniert es

- Einträge.** Jede Freischaltung (**register**), Verlängerung (**renew**), Übertragung, Sperre (**suspend** , **revoke**) und jedes Lebenszeichen ist ein Eintrag. Sperren tragen einen öffentlichen Grund-Code.
- Merkle-Baum.** Die Einträge bilden einen Hash-Baum nach dem Muster von Certificate Transparency (RFC 9162, C2SP tlog). Ein späterer Stand muss den früheren enthalten; das lässt sich mit einem kurzen Konsistenz-Beweis zeigen.
- Checkpoint.** Größe, Wurzel-Hash und Zeit werden mit dem Log-Schlüssel doppelt signiert: **Ed25519** und **ML-DSA-65** (post-quanten), beide Pflicht.
- Zeugen.** Unabhängige Zeugen kosignieren jeden Checkpoint, wenn er zum vorigen passt. Eine Gabelung (zwei verschiedene Stände gleicher Größe) lehnen sie ab und legen sie als Beweis ab, den jeder prüfen kann.
- Knoten.** Jeder Knoten spiegelt das Log und akzeptiert einen Checkpoint nur mit beiden Log-Signaturen und mindestens **2 von 3** Zeugen-Kosignaturen, die höchstens 600 Sekunden vom Checkpoint abweichen. Namen löst er aus dieser Kopie auf – ohne DNS-Anfrage. „♦ geprüft“ zeigt der Browser nur, wenn der Checkpoint höchstens

24 Stunden alt ist.

Was heute läuft

Das Log ist seit dem 29.10.2026 in Betrieb. Stand 30.10.2026: **Checkpoint 13**, veröffentlicht unter cypherpunk2077.com/log/v1/checkpoint, mit 3 Kosignaturen; 6 Domains; Eintrag 12 ist das erste signierte Lebenszeichen des Betreibers.

GRENZE HEUTE

- Die drei Zeugen sind **Start-Zeugen beim Betreiber**. Ihre Kosignaturen beweisen Dritten noch nichts. Gegenüber dem Betreiber – oder jemandem, der seinen Rechner übernimmt – ist das Log heute **nachprüfbar, aber nicht fälschungssicher**.
- Die Zeugen prüfen heute nur die Konsistenz, nicht den Inhalt der Einträge (die Prüfung ist gebaut, aber noch nicht eingeschaltet).
- Die Admin-Doppelsignatur je Eintrag steht noch nicht im öffentlichen Log; Knoten vertrauen allein dem Log-Schlüssel.
- Zeugen-Kosignaturen sind nur Ed25519, also nicht post-quanten-sicher.

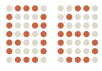
Ziel: mindestens drei unabhängige Zeugen in verschiedenen Ländern, Inhaltsprüfung eingeschaltet, Admin-Signatur von Knoten und Zeugen geprüft. Erst dann ist „fälschungssicher“ eine ehrliche Aussage.

Warum keine Mining-Blockchain?

Eine Blockchain mit Arbeitsnachweis (Mining) schützt nur, wenn die Rechenleistung breit verteilt ist; ein kleines Netz kippt, sobald ein Angreifer mehr als die Hälfte stellt. Bei einer Registry mit Betreiber entscheidet am Ende ohnehin der Betreiber, wer einen Namen bekommt. Ein Transparenz-Log mit unabhängigen Zeugen leistet hier mehr: Ein Eintrag steht nach höchstens etwa einer Minute in einem signierten Checkpoint, ohne den Stromverbrauch des Minings, und jeder kann ihn nachprüfen. (Die Freischaltung selbst prüft der Betreiber von Hand, in 24 bis 48 Stunden.) Die „Prüfer“ sind die Zeugen. Das gleiche Muster sichert heute die Zertifikate des Webs (Certificate Transparency) und signierte Software (Sigstore).

Zonen und Zertifikate

Was unter einer Domain liegt (Seite, Postfach, Onion-Adresse), signiert der Inhaber mit seinem eigenen Schlüssel. Dieser Schlüssel entsteht auf seinem Gerät; der Verwalter bekommt ihn nie. Statt Zertifizierungsstellen gibt es eigene Domain-Zertifikate aus Log und Zone, dazu Übertragungssperre und Übertragung nur mit Signatur von altem und neuem Inhaber.

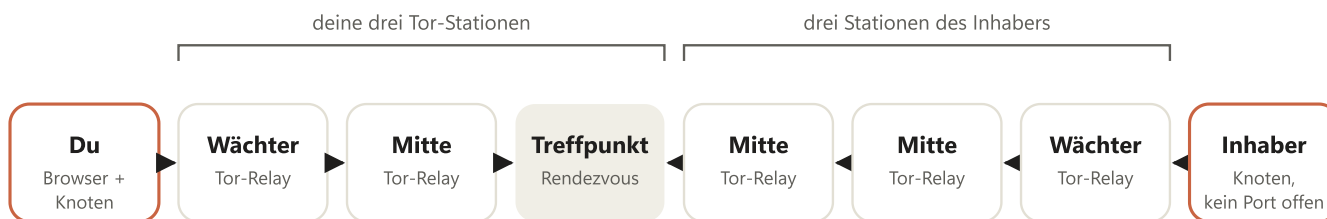


Anonymität: was Mainnet kann und was nicht

Mainnet baut auf Tor auf. Es erbt damit dessen Stärke – Standort und Adresse sind vor normalen Beobachtern geschützt – und dessen Schwäche: Wer beide Enden lange gleichzeitig beobachtet, kann über Zeit und Menge zuordnen. Mainnet erschwert das, verhindert es aber nicht.

Drei Stufen

STUFE	WAS PASSIERT	PREIS	STAND
Schnell	direkte Verbindungen über QUIC/TCP; die Gegenstelle sieht deine IP	am schnellsten	wählbar per Klick
Anonym (Standard)	alles über Tor; verborgenes Hosten über Onion-Dienste, ohne lauschenden Port	langsamer; nach dem Start einige Minuten bis zur Erreichbarkeit	echt getestet an 2 Tagen
Hochsicherheit (Beta)	verstärkt, was Anonym schon hat (Vanguards „leicht“, feine Größenstufen, Mehrweg ab 1 MiB über 3 Kreise, Mail im Mittel 2 min verzögert): Vanguards voll, grobe Größenstufen, Mehrweg immer über 4 Kreise, Mail im Mittel 10 min; neu dazu Attrappen und Abruf-Deckverkehr	rund 45 MiB am Tag, Akku, Mails im Mittel 10 min später, Abruf 1,5- bis 2,5-mal langsamer	3 echte Läufe; bisher nur am PC



WER SIEHT WAS

alles: es ist dein Gerät	deine IP, nicht das Ziel	nur die Nachbarn	weder dich noch den Inhaber	nur die Nachbarn	nur die Nachbarn	IP des Inhabers, nicht die Seite	die Anfrage, nicht deine IP
--------------------------	--------------------------	------------------	-----------------------------	------------------	------------------	----------------------------------	-----------------------------

Weg verschlüsselt bis zum Onion-Dienst des Inhabers · Seite signiert

Öffentliche Seiten sind nicht Ende-zu-Ende verschlüsselt · Mail, Chat, private Dateien zusätzlich Ende-zu-Ende

SCHRITT 0 · NAME → ADRESSE

Dein Knoten löst shop.de aus seiner eigenen, geprüften Kopie des Registry-Logs auf. Keine DNS-Anfrage.

Im Modus „Schnell“ verbindet sich dein Knoten direkt; die Gegenstelle sieht dann deine IP-Adresse.

Abbildung 3. Eine Anfrage zu einer verborgen gehosteten Seite läuft über mehrere Tor-Stationen. Keine einzelne Station kennt zugleich dich und die Seite.

Was echt getestet ist

- Verborgenes Hosten mit dem ganzen Knoten über das echte Tor-Netz an zwei Tagen: am 27.10.2026 im Modus Anonym 3 von 4 Läufen bestanden, am 28.10.2026 6 von 7 (Anonym) und 3 von 3 (Hochsicherheit).
- In allen **158 Port-Prüfungen** hatte der Rechner des Inhabers keinen lauschenden Port außerhalb von 127.0.0.1 und keinen UDP-Endpunkt.
- Neustart mit gleicher Onion-Adresse. Erster Abruf nach dem Start 5 bis 88 Sekunden. Nach einem Neustart am 28.10. 8 bis 190 Sekunden; am 27.10. war die Seite nach einem Neustart einmal über 10 Minuten nicht erreichbar und einmal erst nach 6,7 Minuten.
- Mehrweg: 3 MiB über 3 bzw. 4 getrennte Tor-Kreise. Vor einer Korrektur klappte das nur in 4 von 9 ersten Versuchen, danach 2 von 2.

Was Mainnet nicht kann

KEIN MIX-NETZ

In einem Mix-Netz sammeln Mix-Knoten Pakete vieler Nutzer, verzögern sie zufällig, mischen ihre Reihenfolge und geben sie weiter – über mehrere Schichten. **Das gibt es in Mainnet nicht.** Mainnet-Knoten sammeln und mischen keinen fremden Verkehr; nur im Modus „Schnell“ leiten sie verschlüsselten Verkehr für Knoten hinter NAT weiter (Rolle `relay`), ohne Verzögerung und ohne Mischen. Gemischt wird nur der **eigene Mail-Ausgang** beim Absender (Zufallsverzögerung nach Poisson, im Mittel 2 bzw. 10 Minuten, und Attrappen). Das Weiterleiten über mehrere Stationen macht Tor – ohne Sammeln und ohne Verzögerung je Station.

- **Ein sehr starker Beobachter**, der dein Netz und das Ziel lange gleichzeitig überwacht, kann Verbindungen über Zeit und Menge zuordnen. Größenstufen, Mehrweg und Deckverkehr machen das schwerer, nicht unmöglich.

- **Die eigene Anonymitätsmenge ist heute fast null:** zwei Knoten, ein Betreiber, keine fremden Nutzer. Die große Menge kommt allein von Tor.
- **Größenstufen** verraten weiter die Größenordnung; Tunnel und Gerätekopplung werden nicht aufgefüllt.
- **Deckverkehr** (Attrappen im Takt, Abruf-Deckverkehr) ist nie gegen das echte Netz getestet; auf den Betriebsknoten ist Hochsicherheit aus.
- **Brücken** (obfs4, Snowflake) sind gebaut, im Knoten aber noch nicht an Tor durchgereicht.
- Der **Einstiegsknoten** auf dem VPS des Betreibers läuft absichtlich direkt, mit sichtbarer IP. Der Onion-Eingang des zweiten Knotens ist im Betrieb noch nicht nachweislich erreichbar.
- Mainnet schützt nicht vor Schadsoftware auf deinem Gerät und nicht vor eigenen Fehlern (zum Beispiel echte Namen in einer Mail).

Vergleich mit Tor, Loopix und Nym

EIGENSCHAFT	TOR	LOOPIX (FORSCHUNG)	NYM	MAINNET HEUTE
mehrere Stationen	3 (Onion: 6)	Mix-Schichten	3 Mix-Schichten	über Tor
Sammeln und Verzögern je Station	nein	ja (Poisson)	ja	nur eigener Mail-Ausgang
Deckverkehr	kaum (nur Padding)	Schleife und Leer	ja	Hochsicherheit, nicht echt getestet
gleiche Paketgröße	Zellen	ja	Sphinx	Größenstufen
Wartezeit	niedrig	Sekunden	Sekunden	niedrig (Mail: Minuten)
Anonymitätsmenge	Millionen	–	klein	die von Tor

Gegen einen globalen Beobachter sind Loopix und Nym bauartbedingt stärker. Der Vorteil von Mainnet ist die niedrige Wartezeit für Seiten und die große Nutzermenge von Tor.

ZIEL

Eine echte Mix-Schicht – Pakete gleicher Größe, Verzögerung je Station, Deckverkehr – wäre ein neues Protokoll mit eigener Spezifikation und eigenem Audit. Sie wirkt erst mit vielen unabhängigen Mix-Knoten. Mainnet nennt sie deshalb als Ziel, nicht als Eigenschaft.



KAPITEL 7

Verschlüsselung

Mainnet erfindet keine eigene Kryptografie. Es nutzt geprüfte Verfahren und Bibliotheken und setzt sie so ein, dass Inhalte schon auf dem Gerät verschlüsselt werden. Wo es heute möglich ist, sind die Verfahren post-quanten-hybrid: klassisch und post-quanten zugleich, damit ein Bruch des einen allein nicht reicht.

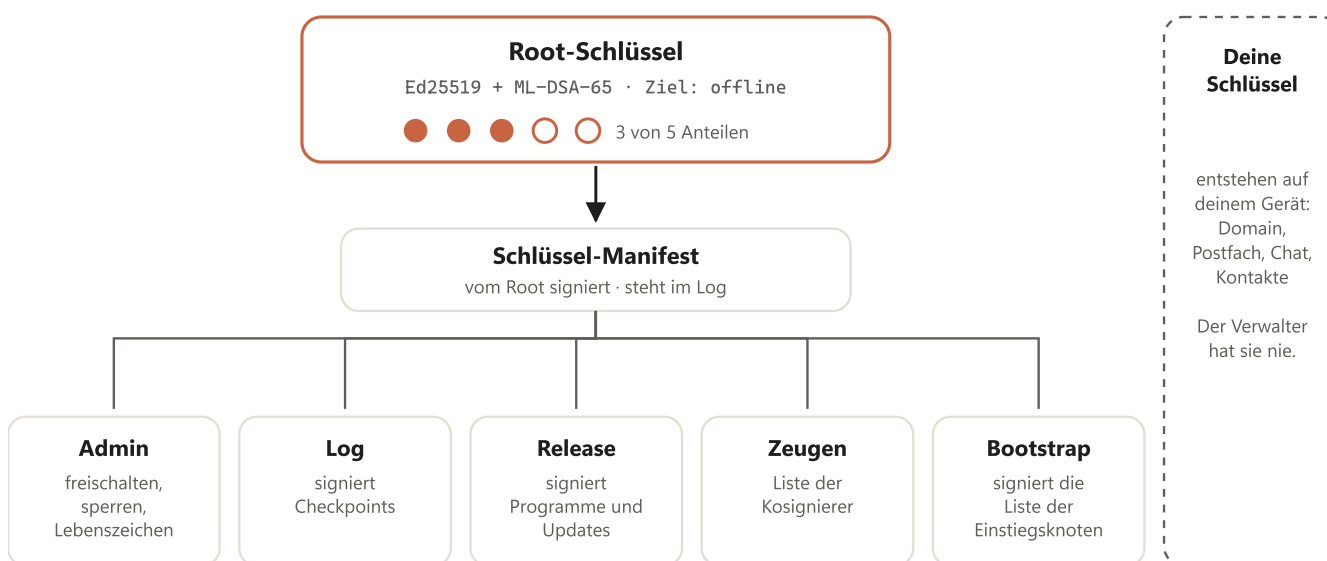
Verfahren je Zweck

ZWECK	VERFAHREN	POST-QUANTEN
Mail, Chat-Start, Datei-Schlüssel	HPKE (RFC 9180) mit X-Wing (X25519 + ML-KEM-768), HKDF-SHA256, ChaCha20-Poly1305	ja, hybrid
Chat-Verlauf	Double Ratchet mit X-Wing-Schritt; Gruppen bis 256 mit Sender-Schlüsseln	ja, hybrid
Private Dateien	XChaCha20-Poly1305 in Segmenten; der Schlüssel steht nur im Link	symmetrisch, 256 Bit
Knoten zu Knoten (QUIC und TCP, auch über Tor)	TLS 1.3 mit X25519MLKEM768, zuerst versucht	ja, hybrid
Knoten zu Knoten (Rückfall über TCP)	Noise mit X25519; abschaltbar mit <code>nur_post_quanten</code>	nein
Tor-Strecke	Verfahren des Tor-Projekts (Arti)	nein (kommt von Tor)
Log-Checkpoints	Ed25519 und ML-DSA-65 (FIPS 204), beide Pflicht	ja
Root, Admin, Release	Doppelschlüssel Ed25519 + ML-DSA-65	ja
Zeugen-Kosignaturen	Ed25519 (C2SP tlog-cosignature)	nein
Bootstrap-Liste	Ed25519	nein
Identität, Zonen, Seiten	Ed25519	nein (geplant für mn2)
Lokaler Tresor	XChaCha20-Poly1305; Schlüssel per Argon2id (256 MiB, t = 3) oder Schlüsselbund des Betriebssystems	symmetrisch
Inhalts-Adressen, Prüfsummen	BLAKE3, SHA-256	ja

WAS „VERSCHLÜSSELT“ HIER HEISST

- **Mail, Chat und private Dateien** sind Ende-zu-Ende verschlüsselt: lesbar nur für Absender und Empfänger.
- **Öffentliche Seiten** sind öffentlich und vom Inhaber signiert, nicht Ende-zu-Ende verschlüsselt – jeder darf sie lesen. Geschützt ist der Weg (TLS 1.3 hybrid und Tor) und die Echtheit (Signatur).
- Das **Portal cypherpunk2077.com** ist eine normale Website mit HTTPS und Onion-Spiegel. Wer es besucht, hat dort keinen Mainnet-Schutz.

Schlüssel-Hierarchie



Heute liegen alle 5 Root-Anteile, Release-Schlüssel und Passwort-Datei auf dem Betreiber-PC. Ziel: getrennt, offline.

Abbildung 4. Der Root-Schlüssel ist in 5 Anteile geteilt, von denen 3 nötig sind. Er soll offline liegen; heute liegt er noch auf dem Betreiber-PC. Er signiert nur das Schlüssel-Manifest, das alle anderen Betriebsschlüssel nennt. Die Schlüssel der Nutzer sind davon getrennt.

- **Root:** Doppelschlüssel, in 5 Anteile geteilt (Shamir, 3 von 5); signiert nur Manifeste.
- **Admin:** freischalten, sperren, Lebenszeichen. Anmeldung im Panel mit Admin-Datei und PIN; jede Aktion doppelt signiert (heute in einer eigenen öffentlichen Datei, noch nicht im Log); Sperren stehen mit Grund-Code im Log.
- **Log:** signiert Checkpoints. **Zeugen:** stehen mit ihren Schlüsseln im Manifest.
- **Release:** signiert Programme und Updates. Ein Knoten installiert ein Update nur nach Rückfrage, nur über Tor und nur, wenn Signatur und Prüfsumme stimmen.
- **Nutzer-Schlüssel** entstehen auf dem Gerät des Nutzers. Wer eine Domain kauft, kauft nur die Freischaltung; den Schlüssel hat er allein.

GRENZE HEUTE

Zum Start liegen alle fünf Root-Anteile, der Release-Schlüssel und die Passwort-Datei auf demselben Rechner des Betreibers. Damit sind Root, Admin, Log und Zeugen heute nur so sicher wie dieser eine Rechner. Ziel: Anteile und Release-Schlüssel an getrennte Orte, Signieren offline.



KAPITEL 8

Mail, Chat und Hosting

Zu jeder Domain gehören Mail und eine Seite. Dazu kommen Chat, Kontakte, Dateien, Suche und Tunnel. Alles läuft über denselben Knoten und dieselben Schlüssel.

Mail

- Jede Domain hat Mail; das Postfach ist ein Schlüssel. `postmaster@` bekommt unter anderem die Ablauf-Erinnerungen.
- Postämter halten nur **verschlüsselte Umschläge**, bis der Empfänger sie abholt (die Rolle ist standardmäßig aus und freiwillig einschaltbar; dann 1 GiB, Aufbewahrung höchstens 90 Tage). Der Empfänger steht dort nur als verblindete Tageskennung.
- Gegen Spam: ein kleiner Arbeitsnachweis für Absender, die der Empfänger nicht kennt; die Höhe legt der Empfänger fest.
- Mail an normale Internet-Adressen ist ein Entwurf: nur für ausdrücklich freigeschaltete Nutzer, über einen eigenen Server, nie mit fremden Absendern. **Nicht gebaut.**

Stand: Code fertig, lokal getestet zwischen Knoten, mit Mischung und Attrappen. Beide Betriebsknoten haben die Rolle Postamt eingeschaltet. Über das echte Tor-Netz zwischen zwei Rechnern noch nicht getestet.

Chat und Kontakte

- 1:1 und Gruppen bis 256 Mitglieder, Double Ratchet mit X-Wing.
- Kontakte über einen Kontakt-Code, Sicherheitsnummer oder QR-Code; Prüfung mit gemeinsamem Geheimnis (SPAKE2). Ändert sich der Schlüssel eines geprüften Kontakts, hält Mainnet das Senden an und fragt nach.

Stand: Code fertig, lokal mit drei Knoten getestet. Nicht im echten Netz; die Konstruktion soll extern geprüft werden.

Hosting: eine Seite als eine Datei

- Das SDK packt einen Ordner – Seiten, Bilder und Server-Logik – in **eine .site -Datei** (Standard bis 20 MiB, höchstens 200 MiB). Server-Logik läuft als WebAssembly im Knoten; Rust, C/C++ und Go sind unterstützt, weitere Sprachen experimentell.
- Jeder hostet selbst: auf PC, VPS oder Raspberry Pi. Standard ist **verborgen** über einen Onion-Dienst; „direkt hosten“ ist schneller, zeigt aber die IP.
- Veröffentlichen mit der Deploy-Schlüsseldatei oder im **Studio** des Browsers: Editor mit Live-Vorschau, Veröffentlichen nach Bestätigung.

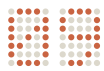
Stand: Code fertig, lokal getestet, verborgene Wegwerf-Seiten über das echte Tor-Netz ausgeliefert. Noch keine Seite eines Nutzers im Netz.

Suche

Die Suche findet nur freigeschaltete Mainnet-Seiten. Ziel: Indexer betreiben nur unabhängige Knoten, nicht der Verwalter. Heute läuft ein (leerer) Indexer auf dem VPS des Betreibers. Anfragen laufen immer über Tor. **Ehrlich:** Der Indexer sieht die Suchbegriffe – es ist keine Ende-zu-Ende-Suche. Heute ist kein Indexer im Portal angebunden.

Tunnel

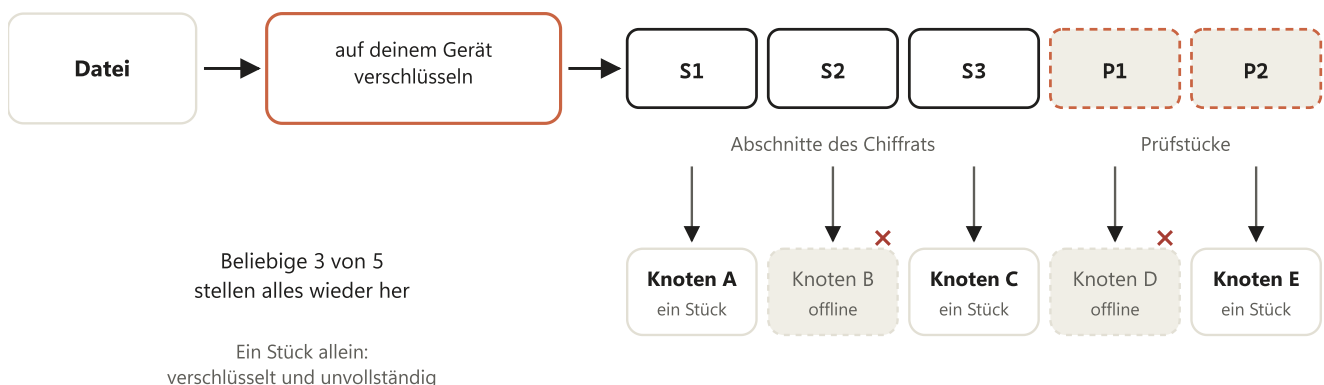
SSH, Spiel-Server oder eine lokale Web-App über Mainnet erreichbar machen, als Port auf 127.0.0.1, nur mit Freigabe je Gegenstelle. Stand: Vorschau, lokal getestet.



KAPITEL 9

Verteilte Speicherung

Private Dateien und Mail werden nach dem Verschlüsseln in Stücke geteilt und auf verschiedene Knoten verteilt. Ein einzelner Knoten hält dann nur ein verschlüsseltes, unvollständiges Stück. Zusammengesetzt und entschlüsselt wird nur auf dem Gerät des Nutzers.



HEUTE IM BETRIEB · 2 KNOTEN

Gespiegelt statt zerstückelt: jeder Knoten hält eine vollständige, verschlüsselte Kopie.

Ab 3 Speicher-Anbietern wird 2 von 3 zerstückelt, ab 5 voll 3 von 5.

Ob die Knoten unabhängig sind, prüft das Programm nicht.

Kopie
verschlüsselt

Kopie
verschlüsselt

Abbildung 5. Oben das Verfahren für Dateien (3 von 5): zwei Knoten dürfen ausfallen. Unten der Stand im Betrieb mit zwei Knoten.

Verfahren

- Erst wird verschlüsselt, dann zerlegt: ein systematischer Reed-Solomon-Löschcode über $GF(2^{16})$. Die ersten k Stücke sind Abschnitte des Chiffrats, die übrigen Prüfstücke.
- **Dateien 3 von 5, Mail 2 von 3:** beliebige k Stücke genügen.

- Jedes Stück hat eine BLAKE3-Adresse und eine Prüfsumme. Das Ergebnis wird gegen die Kennung des ganzen Chiffrats geprüft; gefälschte Stücke fallen auf. Höchstens 256 Kombinationen werden probiert, damit Fälschungen keine Rechenlast erzeugen.
- Jeder Speicher-Knoten erhält höchstens ein Stück einer Datei.

HEUTE IM BETRIEB

- Mit **zwei** Speicher-Knoten wird **gespiegelt** (1 von 2): Jeder Knoten hält eine vollständige, verschlüsselte Kopie. Das bringt Ausfallsicherheit, aber nicht den Schutz durch Zerstückeln.
- Mail geht als ganzer verschlüsselter Umschlag an beide Postämter; 2 von 3 braucht mindestens drei Postämter.
- Zerstückeln über das echte Tor-Netz ist noch nie gelaufen. Anbieter werden nur unter verbundenen Knoten gesucht.
- Beide Knoten gehören heute demselben Betreiber.

Ziel: Das Zerstückeln schaltet sich ohne Änderung am Programm zu: bei Dateien ab drei Speicher-Anbietern als 2 von 3, ab fünf voll als 3 von 5; bei Mail ab drei Postämtern. Ob die Knoten wirklich unabhängig sind, prüft das Programm nicht – es wirkt nur mit Knoten, die nicht dem Betreiber gehören.



KAPITEL 10

Knoten betreiben

Mainnet lebt von seinen Knoten. Jeder Nutzer hat einen; wer mehr beitragen will, lässt ihn dauerhaft laufen und schaltet Rollen wie Postamt oder Speicher ein.

Rollen eines Knotens

ROLLE	AUFGABE	STANDARD
dht	andere Knoten und Einträge finden helfen	an
relay	im Modus „Schnell“ verschlüsselten Verkehr für Knoten hinter NAT weiterleiten (kein Mischen)	an, abschaltbar
store	verschlüsselte Stücke privater Dateien halten	aus; freiwillig einschaltbar (Desktops spenden standardmäßig keinen Speicher)
mailbox	Postamt für verschlüsselte Mail-Umschläge	aus; freiwillig einschaltbar, dann 1 GiB, Aufbewahrung höchstens 90 Tage
search	Indexer für die Suche	aus
cache	selbst angesehene Seiten zwischenspeichern	an, 2 GB, abschaltbar

Ein Knoten speichert nur verschlüsselte Stücke und Umschläge, die er nicht öffnen kann, dazu eigene Seiten und den Zwischenspeicher selbst besuchter Seiten. Jede Rolle lässt sich abschalten. Im Standard-Modus Anonym öffnet der Knoten keinen lauschenden Port außerhalb von 127.0.0.1 (dort lauscht nur die lokale API); er baut nur ausgehende Verbindungen zu Tor auf.

Heute in Betrieb

- **Knoten 1 (VPS):** Einstieg für neue Knoten, Postamt, Speicher, (leerer) Indexer. Läuft absichtlich direkt mit öffentlicher IP und hat zusätzlich einen Onion-Eingang.
- **Knoten 2 (PC des Betreibers):** Postamt und Speicher, nur über Tor. Sein Onion-Eingang meldet zeitweise fehlgeschlagene Deskriptor-Uploads; die Erreichbarkeit von außen ist noch nicht belegt.
- Der Hosting-Anbieter des VPS filtert einen großen Teil der Tor-Ausgänge (rund 80 %). Knoten holen Log und Bootstrap-Liste deshalb zuerst über den Onion-Spiegel des Portals.

GESUCHT

Für Zerstückeln, unabhängige Zeugen und eine echte Anonymitätsmenge braucht Mainnet Knoten bei vielen verschiedenen Menschen, in verschiedenen Netzen und Ländern. Sobald das erste signierte Release veröffentlicht ist, kann jeder einen Knoten starten. Für Zeugen gibt es ein eigenes Paket mit Anleitung.

ENTSCHIEDEN, NICHT GEBAUT

Punkte für Knoten-Betreiber (Entscheidung vom 30.10.2026): ab 2027, höchstens 250 Punkte je Domain, nur als Rabatt auf eine eigene Domain, nicht auszahlfar. Belohnt wird nachgewiesene Leistung – Stichproben, ob gespeicherte Stücke wirklich vorhanden sind, mit Eingewöhnungszeit (Muster Storj). Schwierig bleibt, Leistung zu messen, ohne Nutzer zu überwachen, und erfundene Knoten auszuschließen. Es gibt kein Mining und keine Belohnung in einer Kryptowährung. Beworben wird es erst, wenn es gebaut ist.



KAPITEL 11

Domains und Punkte

Eine Domain kostet 4,99 € im Jahr – in jeder Endung gleich, ohne Premium-Namen. Bezahlt wird mit Bitcoin; gerechnet wird in Punkten.

4,99 € = 500 Punkte = 1 Jahr Laufzeit

Erinnerung 5, 3 und 1 Woche vor Ablauf



500 Punkte · 1 Kalenderjahr

+500 = +1 Jahr

Freischaltung

Ablauf

500

1 Jahr
4,99 € in Bitcoin

1.000

2 Jahre
auch auf einmal

250

etwa ½ Jahr
Untergrenze neue Domain

≤ 10 J.

mehr wird erstattet
statt gutgeschrieben

Zu viel oder zu wenig bezahlt? Es wird in Punkte umgerechnet ($\pm 1\%$ gilt als genau).

Im öffentlichen Log steht nur das Ablaufdatum – keine Beträge, keine Personen.

Abbildung 6. 500 Punkte halten eine Domain genau ein Kalenderjahr. Aufladen geht jederzeit; erinnert wird 5, 3 und 1 Woche vor Ablauf.

Regeln

- **4,99 € = 500 Punkte = genau ein Jahr** (gleicher Tag, gleiche Uhrzeit UTC). Die erste Freischaltung gilt ein Jahr, danach jeweils mit 500 Punkten weiter – oder mehr auf einmal.
- **Bitcoin** über einen selbst betriebenen BTCPay-Server; jede Rechnung hat eine eigene Adresse und einen eindeutigen Betrag.
- **Abweichende Beträge** werden in Punkte umgerechnet: zu wenig ergibt weniger, zu viel mehr Laufzeit ($\pm 1\%$ gilt als genau). Untergrenze für eine neue Domain 250 Punkte, für eine Verlängerung 10. Über 10 Jahre hinaus wird erstattet. Gutgeschrieben wird nach Prüfung, in 24 bis 48 Stunden.
- Punkte gehören zu genau einer Domain; sie sind nicht übertragbar und nicht auszahlbar.
- **Öffentlich** ist nur das Ablaufdatum im Log, keine Beträge und keine Personen. Bitcoin-Zahlungen selbst sind in der Bitcoin-Blockchain öffentlich.
- Erinnerungen gehen an `postmaster@` der Domain, ohne Bezahl-Links (Schutz vor Phishing). Aufladen nur über Browser, Befehlszeile oder den Kauf-Chat.

Prüfung vor der Freischaltung

Jede Domain schaltet der Betreiber von Hand frei. Geprüft werden **Name, Marke und Zahlung, nicht der Inhalt**. Inhalte bewerten wir nach Meldung anhand der Nutzungsregeln; Sperren stehen mit Grund-Code im Log, Einspruch ist möglich.

- **Bekannte Marken und Firmen** bekommt nur, wer nachweist, dass ihm der Name gehört: per **DNS-TXT-Eintrag** in der echten Internet-Domain des Unternehmens, den nur deren Inhaber setzen kann (entschieden am 30.10.2026). Vorrang hat eine Firma nur, wenn ihre Domain oder Marke älter ist als der Mainnet-Eintrag. Der Nachweis zeigt Kontrolle über die Domain, kein Markenrecht. **Der automatische Nachweis ist noch nicht gebaut**; bis dahin prüft der Betreiber von Hand.
- **Allgemeine Wörter** wie „shop“ oder „versicherung“ bekommen keinen Vorrang über den DNS-Nachweis. Häufige Wörter gibt es höchstens **einmal je Person**.
- **Reserve des Betreibers:** Einige begehrte allgemeine Namen hält der Betreiber zurück. Die Liste wird **vor der Werbung veröffentlicht** und enthält keine Marken Dritter. Ab 2027 werden diese Namen per **nachprüfbarem Los** zum Normalpreis vergeben, spätestens bis 31.12.2027; wer am Los teilnimmt, hinterlegt 4,99 € Pfand.
- **Start-Domains des Betreibers**, öffentlich im Log: `mainnet.com`, `cypherpunk2077.com`, `cypherpunk2077.de`, `test.net`, `shop.com`, `revaultstudio.com`. Für `shop.com` steht eine Markenprüfung noch aus. Geschützt sind außerdem die Labels `mainnet` und `cypherpunk2077`.

HEUTE

Kauf-Chat, BTCPay und Admin-Panel sind gebaut und im Testnetz geprüft (Bitcoin-Regtest), aber **noch nicht in Betrieb**. Ein Kauf mit echtem Bitcoin hat noch nicht stattgefunden. Die sechs Start-Domains hat der Betreiber kostenlos freigeschaltet; das steht mit Grund-Code öffentlich im Log.

ENTSCIEDEN AM 30.10.2026, NOCH NICHT IN BETRIEB

- **Gratis-Aktion:** Registrierungen, die bis 31.12.2026 eingehen, sind kostenlos; Nachzügler werden bis 31.01.2027 freigeschaltet. Höchstens 300 Freischaltungen am Tag, höchstens 3 Domains je Person, Warteschlange bis 3.000, bei Andrang tägliches Los. Laufzeit 1 Jahr, danach gilt die 500er-Logik. Im Log steht dafür der öffentliche Grund-Code „vom Betreiber kostenlos“. Heute erlaubt das Admin-Panel ohne zusätzliche Root-Freigabe höchstens 10 kostenlose Freischaltungen je 24 Stunden; die Umsetzung der Aktion läuft.
- **Punkte für Knoten-Betreiber** ab 2027, höchstens 250 Punkte je Domain (Kapitel 10).
- **Marktplatz** zuerst nur als Schaufenster aus Visitenkarten der Seiten: kein Handel, keine Zahlung, keine Treuhand.

**KAPITEL 12**

Sicherheit und Prüfungen

Mainnet wird viel getestet, aber bisher nur von seinen eigenen Entwicklern. Ein externes Audit gibt es noch nicht. Bis dahin ist Mainnet eine Beta und ungeprüft.

2.215

von 2.215 Tests grün
(28.10.2026)

106

Property-Tests für Parser
fremder Eingaben

14

Fuzzing-Ziele, je 10 min, ≈ 20
Mio. Eingaben

3

interne Reviews, alle kritischen
und hohen Funde behoben

Was geprüft wird

- **Automatische Tests** für jedes Crate, Ende-zu-Ende-Tests mit mehreren Knoten im Prozess, ein Testnetz in Docker mit 6 Knoten, Log-Dienst, Zeugen und Bitcoin-Regtest.
- **Robustheit:** Property-Tests über alle Parser; Fuzzing fand einen Fehler, der behoben ist.
- **Echte Tor-Tests** an zwei Tagen (Kapitel 6).
- **Pflicht-Prüfungen vor dem Start** (Go/No-Go): Geheimnis-Suche über alles, was veröffentlicht wird, Portal-Prüfung über Tor (602 von 604 am 29.10.; die zwei roten betrafen das damals noch fehlende Log), Härtung der Server ohne Fehler.
- **Updates** nur signiert, nur über Tor und nur nach Rückfrage; manipulierte Dateien werden abgelehnt (getestet, mit einem echten Release noch nie gelaufen).

Schutz-Funktionen

- **Stolperdrähte:** echt aussehende Köder auf den Servern des Verwalters; jede Berührung löst Alarm aus. Sie laufen; Alarmer gehen heute nur ins Protokoll.
- **Selbsttest „Bin ich geschützt?“** im Browser (in der App gebaut, aber nie auf einem Gerät gestartet): Lecks am Tor vorbei, Uhr, Version.
- **Lebenszeichen:** der Betreiber soll regelmäßig ein Lebenszeichen ins Log signieren; das erste steht seit dem 29.10.2026 darin (Eintrag 12); fehlt es, warnen die Programme nach 14 bzw. 30 Tagen. Es gibt dabei nie automatisch Rechte an jemand anderen.
- **Datensparsamkeit:** keine Cookies, keine Tracker, keine IP-Protokolle im Portal, Besucher nur als Tagessummen gezählt. Das ist ein Versprechen, das sich von außen nicht prüfen lässt – über Tor ist es nicht nötig.

KEIN EXTERNES AUDIT

Ein Paket für eine Sicherheitsfirma liegt bereit, ist aber nicht beauftragt. Interne Reviews und viele Tests ersetzen keine unabhängige Prüfung. Besonders prüfen lassen wollen wir: Chat-Konstruktion (Double Ratchet mit X-Wing), Registry-Log und Zeugen, Tor-Einbindung, Update-Weg.

Sicherheitslücken bitte über cypherpunk2077.com/.well-known/security.txt melden, auf Wunsch über Tor. Ehrliche Forschung ist willkommen.



KAPITEL 13

Grenzen und Risiken

Dieses Kapitel sammelt, was Mainnet heute nicht leistet – möglichst vollständig, auch wenn einzelne Punkte in anderen Kapiteln schon stehen.

1. **Beta ohne externes Audit.** Fehler sind wahrscheinlich; wer Mainnet für Leib und Leben braucht, sollte heute nicht allein darauf setzen.
2. **Zwei Knoten, ein Betreiber.** In der eigenen Schicht gibt es noch keine Anonymitätsmenge; Zerstückeln wirkt nicht.

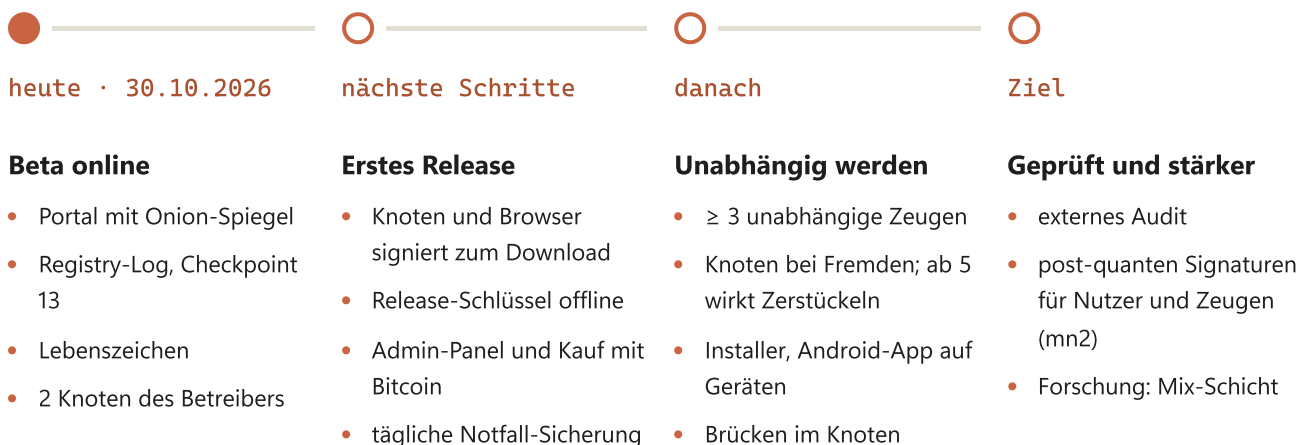
3. **Zeugen beim Betreiber.** Das Log ist nachprüfbar, aber gegenüber dem Betreiber noch nicht fälschungssicher. Die Admin-Doppelsignatur steht noch nicht im Log, und die Bremse gegen Massen-Sperren wirkt nur im Admin-Panel, nicht im Protokoll.
4. **Schlüssel an einem Ort.** Root-Anteile, Release-Schlüssel und Passwort-Datei liegen zum Start auf einem Rechner.
5. **Kein Mix-Netz.** Gegen einen sehr starken Beobachter beider Enden hilft Mainnet nur begrenzt.
6. **Noch kein Release.** Die Programme sind gebaut, aber nicht signiert und nicht veröffentlicht; der vorhandene Release-Entwurf ist veraltet. Es gibt noch keinen Installer und kein Code-Signing-Zertifikat; Windows wird zunächst warnen.
7. **Einstieg nur mit fertiger Konfiguration.** Root-Fingerabdruck und Bootstrap-Schlüssel sind noch nicht ins Programm eingebaut. Ein frischer Knoten findet ohne mitgelieferte Konfiguration weder das Netz noch die Namen.
8. **Vieles nur lokal getestet.** Mail und Chat liefen noch nie zwischen zwei Rechnern über das echte Tor-Netz, Zerstückeln ebenfalls nicht. Deckverkehr ist nie gegen das echte Netz getestet. Die Suche ist im Portal nicht angebunden.
9. **Android-App nie gestartet.** Die App ist gebaut, lief aber noch nie auf einem Gerät; iOS ist nicht gebaut.
10. **Brücken fehlen im Knoten.** obfs4 und Snowflake sind gebaut, aber im Knoten noch nicht an Tor durchgereicht. Wo Tor blockiert ist, kommt Mainnet heute nicht durch.
11. **Signaturen klassisch.** Nutzer, Zonen, Seiten, Bootstrap-Liste und Zeugen signieren nur mit Ed25519, also nicht post-quanten-sicher.
12. **Suche sieht Suchbegriffe.** Der Indexer erfährt, wonach gesucht wird – nicht, wer sucht.
13. **Kauf-Chat im normalen Browser.** Wer den Kauf-Chat in einem normalen Browser öffnet, vertraut dem Code, den die Seite liefert. Am sichersten sind `mainnet chat` oder der Mainnet Browser; der Rückfall im Web-Chat ist nur klassisch verschlüsselt.
14. **Zentrale Vergabe.** Der Betreiber kann Domains sperren – gewollt, nach den Nutzungsregeln und öffentlich im Log. Gegen Angreifer soll Mainnet weiterlaufen; gegen den rechtmäßigen Betreiber nicht.
15. **Ausfall des Verwalters.** Ohne laufenden Log-Dienst entstehen keine Checkpoints, Freischaltungen und Sperren. Nach 24 Stunden zeigen Knoten Namen als „ungeprüft“; bestehende Seiten lösen weiter auf. Ein Notfall-Kit zum Neustart ist gebaut, aber noch nicht in Betrieb.
16. **Grenzen von Tor.** Tor ist langsamer als direkte Verbindungen, kann blockiert werden, und nach dem Start dauert es einige Minuten, bis eine verborgene Seite erreichbar ist.
17. **Netz-Filter.** Der Hosting-Anbieter des Einstiegsknotens filtert viele Tor-Ausgänge; Mainnet weicht auf Onion-Adressen aus.
18. **Recht.** Keine Rechtsform in Deutschland, Sitz der Betreiber-Firma im Ausland, kein Impressum; die rechtliche und steuerliche Prüfung steht aus.
19. **Bitcoin.** Zahlungen sind in der Bitcoin-Blockchain öffentlich; der Kurs schwankt.
20. **Dein Gerät.** Schadsoftware, ein unverschlüsselter Rechner oder ein weitergegebener Schlüssel heben jeden Schutz auf.
21. **Browser-Basis.** Der Mainnet Browser baut auf Qt WebEngine (Chromium) auf und muss dessen Sicherheits-Updates zeitnah übernehmen.



KAPITEL 14

Roadmap

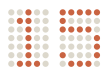
Die Reihenfolge steht fest, die Termine nicht. Jeder Schritt gilt erst als erledigt, wenn er im echten Betrieb läuft.



Entschieden, noch nicht gebaut

- Gratis-Aktion: Eingang bis 31.12.2026, Freischaltung bis 31.01.2027 (Kapitel 11).
- Nachweis für Firmen-Domains per DNS-TXT; Reserve-Liste und Los ab 2027.
- Punkte für Knoten-Betreiber ab 2027, höchstens 250 Punkte je Domain.
- Marktplatz zuerst als Schaufenster.
- Mail an normale Internet-Adressen für freigeschaltete Nutzer (Entwurf).

Diese Punkte hat der Betreiber am 30.10.2026 entschieden (die Mail nach außen am 29.10.); gebaut und in Betrieb sind sie noch nicht. Bis dahin sind sie keine Eigenschaft von Mainnet.



Glossar

Attrappe	Eine verschlüsselte Nachricht ohne Inhalt, die wie eine echte aussieht; erschwert das Ablesen aus Zeit und Menge.
Beta	In Betrieb, aber unfertig und ohne externes Audit.
BLAKE3, SHA-256	Hash-Verfahren: ein kurzer Fingerabdruck beliebiger Daten.
Bootstrap-Liste	Signierte Liste der Einstiegsknoten, über die ein neuer Knoten das Netz findet.
Checkpoint	Signierter Stand des Registry-Logs: Größe, Wurzel-Hash, Zeit.
Deckverkehr	Zusätzlicher Verkehr ohne Nutzinhalte, damit echter Verkehr nicht auffällt.
Double Ratchet	Verfahren für Chats, das für jede Nachricht neue Schlüssel ableitet.
Ed25519	Klassisches Signaturverfahren; schnell, nicht post-quanten-sicher.
HPKE	Standard (RFC 9180), um Daten für einen öffentlichen Schlüssel zu verschlüsseln.
k von n	Daten in n Stücke teilen, von denen beliebige k zum Wiederherstellen genügen (Reed-Solomon).
Knoten (mainnetd)	Das Programm, das auf jedem Rechner das Netz trägt.
Lebenszeichen	Regelmäßig signierter Eintrag des Betreibers im Log; fehlt er, warnen die Programme.
Mehrweg	Teile einer Übertragung über getrennte Tor-Kreise schicken.
Merkle-Baum	Hash-Baum, mit dem sich kurz beweisen lässt, dass ein Eintrag im Log steht und das Log nur gewachsen ist.
Mix-Netz	Netz aus Mix-Knoten, die Pakete vieler Nutzer sammeln, verzögern und gemischt weitergeben. In Mainnet nicht vorhanden.
ML-KEM-768, ML-DSA-65	Post-quanten-Verfahren der NIST für Schlüsselaustausch (FIPS 203) und Signaturen (FIPS 204).
Onion-Dienst	Über Tor erreichbarer Dienst, dessen Standort durch Tor geschützt ist.
Postamt	Knoten, der verschlüsselte Mail-Umschläge hält, bis der Empfänger sie abholt.
Post-quanten-hybrid	Klassisches und post-quanten Verfahren zugleich; geschützt, solange eines der beiden Verfahren nicht gebrochen ist.
Punkte	Laufzeit-Einheit: 500 Punkte = ein Jahr = 4,99 €.
.site	Eine Datei mit einer ganzen Website samt Server-Logik als WebAssembly.
Stolperdraht	Köder auf Servern des Verwalters, dessen Berührung Alarm auslöst.
Vanguards	Feste Tor-Stationen nahe einem Onion-Dienst gegen Angriffe, die seinen Wächter aufspüren wollen.
Verwalter	cypherpunk2077.com: vergibt und prüft Namen, betreibt das Log, liefert Programme aus.
Wächter (Guard)	Erste Tor-Station; sieht die IP-Adresse, aber nicht das Ziel.
X-Wing	Hybrider Schlüsselaustausch aus X25519 und ML-KEM-768.
Zeuge (Witness)	Unabhängige Stelle, die Checkpoints kosigniert und Gabelungen ablehnt.



Über dieses Dokument. Mainnet Whitepaper, Version 0.1, Beta, Stand 30.10.2026. Es beschreibt den Projektstand an diesem Tag und wird mit dem Projekt fortgeschrieben; ältere Fassungen gelten dann nicht mehr. Verbindlich für die Nutzung sind die Nutzungsregeln auf cytherpunk2077.com/regeln. Dieses Dokument ist keine Zusage von Funktionen, Terminen oder Sicherheit und keine Anlageempfehlung. Prüfsummen der PDF-Dateien stehen auf cytherpunk2077.com/whitepaper. Sicherheitslücken bitte nach cytherpunk2077.com/.well-known/security.txt melden.