X4NOVA

TECHNISCHES WHITEPAPER 0.14

Private Werte. Offene Möglichkeiten.

Proof of Work, selbstbestimmte Zahlungen und überprüfbare digitale Nachweise.

VALUE PAY PROOF

Money. Proof. Freedom.

---

22. November 2026 · Nativer Coin X4N · Öffentliches Testnetz

Technischer Projektstand für Betreiber, Entwickler und Integrationspartner. Enthält die geprüften Lab-Funktionen, das Rust-Ausführungsnetz und die offenen Voraussetzungen für ein Mainnet.

Projektkontakt: info@x4nova.com

DAS DOKUMENT

Eine gemeinsame Richtung.

Mining, Privatsphäre und zügige Nutzung werden zusammen gedacht. Diese Fassung verbindet das Produktziel mit den Grenzen und Prüfungen, die zu einem belastbaren Netzwerk gehören.

KAPITEL 01 Leitbild und Prioritäten

KAPITEL 02 Drei Funktionen, ein zusammenhängendes Produkt

KAPITEL 03 Rules are Law

KAPITEL 04 Eine eigene Architektur auf prüfbaren Grundlagen

KAPITEL 05 Privatsphäre als Produktanforderung

KAPITEL 06 Konsens, Bestätigungen und konkurrierende Blöcke

KAPITEL 07 Ein einzelner Miner und ein stillstehendes Netz

KAPITEL 08 Mining und faire gemeinsame Vergütung

KAPITEL 09 Wie der Pool Mining-Aktivität misst

KAPITEL 10 Geldmenge und nachvollziehbare Emission

KAPITEL 11 Das Gleichgewicht von Sicherheit und Nutzung

KAPITEL 12 Gebühren senken durch effiziente Nutzung

KAPITEL 13 Zügig bezahlen, Sicherheit sichtbar halten

KAPITEL 14 Wallet, Sicherung und Kontozugriff

KAPITEL 15 Zahlungsfunktionen für Menschen und Anwendungen

KAPITEL 16 Digitale Nachweise, die unabhängig prüfbar bleiben

KAPITEL 17 Programmierbare Funktionen mit begrenzten Kosten

KAPITEL 18 Was eine kleine Fullnode tragen kann

KAPITEL 19 Skalierung ohne versteckte Gegenrechnung

KAPITEL 20 Sicherheitsziele und Freigabekriterien

KAPITEL 21 Entwicklung nach überprüfbaren Etappen

KAPITEL 22 Versionen, Regeln und ehrliche Produktkommunikation

KAPITEL 23 Vom ersten Miner zum offenen Netzwerk

KAPITEL 24 Welche Regeln Rust heute prüft

KAPITEL 25 Wie sich die Regeln ändern können

KAPITEL 26 Ein- und Auszahlungen an einer Börse

KAPITEL 27 Unterlagen für eine mögliche Handelszulassung

KAPITEL 28 Energieverbrauch und Risiken belegen

REFERENZEN Primärquellen

Leitbild und Prioritäten

X4NOVA verbindet VALUE, PAY und PROOF: Werte selbst halten, direkt bezahlen und digitale Informationen überprüfbar verankern.

Der native Coin heißt X4N. Das Projekt entwickelt eine eigene Layer-1 mit Proof of Work. Mining ist ein bewusster Bestandteil: Teilnehmer sollen gültige Rechenarbeit beitragen und die dafür vorgesehenen Belohnungen verdienen können. Die geplante Geldordnung verzichtet auf Premine und gesonderte Gründer-Ausgaben.

X4NOVA Beacon (X4BCN) ist ein separater Community-Token auf Solana. Der Besitz von Beacon vermittelt weder X4N-Miningrechte noch einen Anspruch auf native Coins im LabNet oder in einem späteren Mainnet.

Die Produktziele stehen in einem gemeinsamen Verhältnis. Zahlungen sollen im Alltag verständlich und zügig sein; private Informationen sollen geschützt bleiben; das Prüfen der Regeln soll für unabhängige Teilnehmer möglich sein. Höhere Geschwindigkeit darf nicht durch versteckte Verwahrung oder das Überspringen von Prüfungen erkauft werden.

- Selbstbestimmung: Schlüssel und Freigabe bleiben beim Nutzer.
- Privatsphäre: Schutz der Zahlungsdaten wird als Protokollaufgabe behandelt.
- Zugänglichkeit: Mining und unabhängige Prüfung sollen mit vertretbaren Ressourcen möglich sein.
- Nachvollziehbarkeit: Geldmenge, Gebühren, Bestätigungen und Entwicklungsstand sind prüfbar.

> Diese Fassung beschreibt vorhandene Lab-Funktionen und die geplante Weiterentwicklung. Standardmäßig private Zahlungen und eine allgemeine Smart-Contract-Plattform bleiben Entwicklungsziele. Der öffentliche Testpool bietet PPLNS und Solo mit einer lokalen Empfangsadresse an. Das Konto ist optional. Das LabNet ist zurücksetzbar; seine Bestände werden nicht in ein späteres Mainnet übernommen.

Drei Funktionen, ein zusammenhängendes Produkt

Eine Wallet soll Besitz, Nutzung und Nachweise verständlich zusammenführen, ohne die Bedeutung der einzelnen Vorgänge zu vermischen.

VALUE · Werte selbst verwahren

Nutzer erzeugen Schlüssel lokal, empfangen X4N und sichern die Wiederherstellung selbst. Eine Übersicht trennt bestätigte, unbestätigte und noch unreife Mining-Belohnungen. Geplant sind vollständige Adressrotation, Coin-Control, zusätzliche Wiederherstellungstests und später Mehrparteienfreigaben. Ein Onlinekonto soll die Verfügung über die Coins nicht ersetzen.

PAY · Zahlungen mit klarer Freigabe

Vor einer Zahlung zeigt die Wallet Empfänger, Betrag, Wechselgeld und Gebühr. Signieren und Veröffentlichen bleiben getrennte Schritte. Zahlungsanforderungen mit QR-Code, verständliche Statusanzeigen und eine Händler-Schnittstelle gehören zur nächsten Produktstufe. Ausbleibende Bestätigungen und Reorganisationen müssen sichtbar bleiben.

PROOF · Daten unabhängig prüfen

Eine Datei wird lokal gehasht. Eine bestätigte Verankerung und eine exportierte Nachweisdatei ermöglichen die spätere Prüfung der Bindung an die Blockchain. Denkbare Anwendungen sind Dokumentversionen, veröffentlichte Software und vereinbarte Freigaben. Die Originaldatei bleibt beim Nutzer; der Nachweis allein erklärt nicht, wem ein Inhalt rechtlich gehört.

> Eine Zahlungsbestätigung, eine Kontonotiz und ein Blockchain-Nachweis sind unterschiedliche Dinge. Die Oberfläche muss diesen Unterschied in jedem Schritt erkennbar machen.

Rules are Law

Jede Fullnode entscheidet selbst anhand derselben veröffentlichten Regeln, welche Blöcke sie annimmt. Mehr geleistete Arbeit entscheidet zwischen gültigen Zweigen.

Ein Coin für Geld und Gebühren

X4N ist der native Coin für selbst gehaltenes Guthaben, Zahlungen und Mining. Bitcoin dient als Beispiel für diese monetäre Rolle. Es gibt weder eine Kursbindung noch einen versprochenen Marktwert. Bei einer Zahlung kann die Wallet den Eingang im Mempool sofort anzeigen. Die erste Bestätigung folgt mit dem nächsten einschließenden Block. Weitere Bestätigungen erhöhen die kumulierte Arbeit hinter der Zahlung.

```
Maximaler nativer Blockerlös = Blocksubvention + Summe der Gebühren aller enthaltenen Zahlungen
```

Im isolierten Versuch zahlten 1.218 signierte Zahlungen je 500 Atome. Die Coinbase erhielt 50,00609000 X4N aus 50 X4N Subvention und 0,00609000 X4N Gebühren. Nur die Subvention vergrößert die Geldmenge. Der Pool verteilt den tatsächlich beanspruchten Erlös nach dem gewählten Verfahren.

Verträge und eigene Tokens

Eine einfache X4N-Zahlung benötigt keinen Smart Contract. Ein Vertrag kann später Anwendungsrechte oder Tokenbestände führen. Die Identität eines Tokens ergibt sich aus Netzkennung und Vertragsadresse. Ein Tokenname oder -symbol gewährt keine Befugnis, native X4N zu erzeugen. Im Ausführungsversuch wurden 75 Einheiten eines ERC-20-Vertrags übertragen. [20]

Die vorgeschlagene Vertragsstufe erfordert ein für alle Validatoren verbindliches Ausführungsergebnis, begrenztes Gas und eine eindeutige Bindung von nativem Wert an das Vertragsguthaben. Eine isolierte Gebührenvariante schreibt auch die tatsächlich berechnete Basisgebühr dem angegebenen Miner im Ausführungszustand gut. Dieselben Gebühren dürfen nicht zusätzlich als native Coinbase-Ausgabe erscheinen.

> Jede X4N-Fullnode erzwingt Geldmenge, Halving-Zyklus und Blockzeitziel selbst. Tokens, Pools und Abstimmungen haben dafür keine Änderungsfunktion. Wer andere Geldregeln in seine Software schreibt, erzeugt ab der ersten Regelverletzung einen inkompatiblen Zweig. Die bisherigen Fullnodes verwerfen diesen Block unabhängig von seiner Rechenarbeit. [1]

Eine eigene Architektur auf prüfbaren Grundlagen

Proof of Work, ein UTXO-Zahlungsmodell und programmierbare Bedingungen lassen sich als getrennte Bausteine betrachten.

Proof of Work legt fest, welche nachprüfbare Rechenarbeit für Blöcke erforderlich ist und wie konkurrierende gültige Historien gewichtet werden. Das Transaktionsmodell legt fest, welche Werte ausgegeben werden können. Die Programmierebene bestimmt zusätzliche Ausgabebedingungen. Die Wahl von Mining erzwingt daher weder eine allgemeine Vertragsmaschine noch deren Verzicht. [1, 3]

Die vorhandene Lab-Codebasis verwendet Bitcoin-Core-Grundlagen für UTXOs und Validierung, kombiniert mit einer experimentellen RandomX-Anpassung. Bitcoin Core v32.1 und RandomX v1.2.3 sind als Ausgangsversionen festgehalten. Das ist eine neue experimentelle Konsenskombination; die Sicherheitsgeschichte eines Upstream-Projekts überträgt sich dadurch nicht vollständig auf X4NOVA. [2]

Für Programme verfolgt X4NOVA eine EVM-Schicht in Rust. Ein eigenes Entwicklungsnetz erprobt bereits signierte Transaktionen und Vertragsausführung. Die Einbindung der Ausführungsregeln in die native Blockvalidierung ist offen. Das UTXO-Modell trägt weiterhin die Zahlungen. [3]

- Gemeinsame Regeln müssen auf allen prüfenden Clients deterministisch zum selben Ergebnis führen.
- Neue Funktionen brauchen begrenzte Rechen-, Speicher- und Datenkosten.
- Bestehende Wallets und Nachweise benötigen nachvollziehbare Versions- und Migrationsregeln.

> Die Eigenleistung soll in verlässlich verbundenen Funktionen und einer guten Nutzererfahrung liegen. Neue Kryptografie oder ein neu erfundener Konsensmechanismus sind kein Selbstzweck.

Privatsphäre als Produktanforderung

Das Ziel ist ein Zahlungsmittel, das nicht automatisch die finanzielle Geschichte seiner Nutzer offenlegt.

Der heutige Lab-Stand bietet noch keine anonymen Zahlungen. Beträge und Transaktionsbeziehungen sind für prüfende Teilnehmer nachvollziehbar. Das verbundene Teamkonto erhält öffentliche Wallet-Daten. Die Verschlüsselung einer Wallet-Datei schützt gespeicherte Schlüssel; sie verbirgt keine Zahlungsdaten auf der Blockchain.

Das Zielbild betrachtet drei Ebenen: Welche Informationen enthält eine Transaktion? Welche Verbindungen verraten Übertragung und Abfrage? Welche Daten sammeln Wallet, Konto und zusätzliche Dienste? Ein Schutz auf nur einer Ebene reicht für ein umfassendes Privatsphäreversprechen nicht aus.

Schutzziel	Zu untersuchende Richtung
Empfänger schwer verknüpfbar machen	Einmalige Empfangsziele und geeignete Scan-Verfahren
Beträge und Zahlungsbeziehungen schützen	Geprüfte vertrauliche Transaktionen und kryptografische Nachweise
Verknüpfung durch Zusatzdienste begrenzen	Datenarme Nutzung und klare Grenzen für Konto- und Abfragedaten
Freiwillige Offenlegung ermöglichen	Gezielt prüfbare Belege mit begrenztem Informationsumfang

Stealth-Adressen und RingCT zeigen unterschiedliche Bestandteile eines bestehenden Privacy-Ansatzes. Sie sind Referenzen für die Bewertung, keine bereits integrierten X4NOVA-Funktionen. Vollständige Betragsverschleierung, korrekte Geldmengenkontrolle, Backup und Scan-Leistung müssen zusammen funktionieren. [5, 6]

> Ein konkretes Privacy-Verfahren wird erst nach Bedrohungsmodell, Kompatibilitätsprüfung und unabhängiger Sicherheitsbewertung festgelegt. Absolute Anonymität wird nicht zugesagt. Zahlungsdaten und freiwillig veröffentlichte Proofs benötigen getrennte Freigaben.

Konsens, Bestätigungen und konkurrierende Blöcke

Jeder gültige Block muss dieselben Regeln erfüllen. Mehr Rechenarbeit macht ungültige Transaktionen nicht gültig.

Prüfende Teilnehmer kontrollieren unter anderem Arbeitsnachweis, Vorgänger, Transaktionen, Signaturen, zulässige Ausgaben und Coinbase-Budget. Unter konkurrierenden gültigen Zweigen zählt die größte kumulierte Proof-of-Work. Ein größerer Blockzähler allein genügt bei unterschiedlichen Schwierigkeitsgraden nicht. [1]

Wenn zwei Miner gleichzeitig erfolgreich sind

Zwei gültige Blöcke können denselben Vorgänger haben. Zunächst können verschiedene Teilnehmer auf unterschiedlichen Spitzen weiterarbeiten. Bei gleicher kumulierter Arbeit besteht die Konkurrenz fort; zusätzliche Arbeit kann den Gleichstand auflösen. Die Coinbase eines ausgeschiedenen Blocks ist in der aktiven Kette nicht ausgebbar. Seine Belohnung wird nicht automatisch halbiert oder zusätzlich ausgeschüttet.

Eine Reorganisation kann bestätigte Zahlungen wieder unbestätigt machen oder eine konkurrierende Ausgabe durchsetzen. Wallet und Nachweisprüfung müssen deshalb den aktuellen Kettenstatus erneut bewerten können. Eine Anzeige darf Erfolg beim Einsenden eines Blocks nicht mit endgültiger Abrechnung gleichsetzen.

Von Block 384 bis einschließlich 671 verwendet die Alpha ASERT mit zwei Stunden Halbwertszeit. Block 672 setzt das Target auf 0x1f08bcf6, rund 7.500 RandomX-Versuche pro Fund. Ab Block 816 misst jede Node alle 144 Blöcke den Zeitunterschied zwischen dem Elternblock und seinem 144 Blöcke älteren Vorfahren. Das Ziel sind zwölf Stunden pro Fenster. Die neue Zielschwelle entspricht der alten multipliziert mit der gemessenen Zeit und geteilt durch zwölf Stunden. Die Zeit geht mit mindestens drei und höchstens 48 Stunden ein. Die Node rundet ganzzahlig ab, begrenzt das Ergebnis auf den erlaubten Wertebereich und kodiert es als kompaktes Target. [12, 21]

> PoW-Sicherheit hängt auch von Umfang und Verteilung der ehrlich eingesetzten Rechenleistung ab. Ein neues kleines Netz erhält nicht automatisch die Angriffskosten von Bitcoin.

Ein einzelner Miner und ein stillstehendes Netz

Difficulty regelt die erforderliche Arbeit für den nächsten Block. Das Halving regelt die maximal neu erzeugten X4N je Blockhöhe. Dieselbe Person kann allein minen, beide Regeln gelten weiterhin.

Wenn ein einziger Miner 30 Tage lang alle gültigen Blöcke findet und das Netz im Fünf-Minuten-Mittel läuft, ergeben sich im Mittel 8.640 Blöcke. In der ersten Ära sind das 432.000 neue X4N. Die Minerzahl wird im Konsens nirgendwo gezählt. Tritt ein zweiter gleich schneller Miner bei, teilen sich beide langfristig die Chancen auf die Blockfunde.

Im öffentlichen Testnetz lagen zwischen den Blöcken 614 und 615 über drei Stunden. Bei Block 616 verlangte das Ziel statistisch rund 86 Hashversuche, bei Block 634 bereits rund 143. Die 20 Blöcke von 615 bis 634 erschienen innerhalb von 89 Sekunden. Im Pool werden außerdem Shares gezählt. Eine Share belegt geleistete Arbeit und erfüllt nur manchmal auch das schwierigere Blockziel.

Was nach einer langen Pause geschieht

Die frühere ASERT-Regel erzeugte nach 30 Tagen Stillstand bei Rückkehr eines Miners mit 25 Hashes pro Sekunde im Median 8.604 Blöcke in der ersten Stunde. Für die Fensterregel hängt die Rückkehr vom Zeitpunkt der Pause ab. In je 32 Läufen ergaben sich am Fensteranfang 10,5, in der Mitte 12 und am Fensterende 45 Blöcke im Median. Am Fensterende waren es maximal 65.

Bitcoin korrigiert die Schwierigkeit alle 2.016 Blöcke mit einer auf Faktor vier begrenzten Änderung. Die native X4N-Fensterregel ergab nach der Pause im Median 12 Blöcke in der ersten Stunde, je nach Lauf 6 bis 52. Nach einem plötzlichen Verlust von 90 Prozent der Hashrate wurden am ersten Tag im Median 35 Blöcke gefunden. Am letzten Simulationstag waren es 286 bei einem Soll von 288. [21]

> Die ausgelieferte Berechnung ergab bei dauerhaft stabiler Hashrate im Modell rund 302 Sekunden je Block. Bei einem fortlaufenden Wechsel zwischen 25 und 50 Hashes pro Sekunde an jeder Fenstergrenze waren es 377 Sekunden. Die Messung umfasst die letzten 16 Fenster je Lauf. Öffentliche Live-Messwerte nutzen Header-Zeitstempel und nennen die Stichprobengröße.

Mining und faire gemeinsame Vergütung

Kleine und große Miner sollen nach tatsächlich nachgewiesener Arbeit teilnehmen können.

RandomX nutzt CPUs und speicherintensive Berechnungen. Das begrenzt angestrebte Hardwarevorteile, garantiert aber keine dauerhafte ASIC-Resistenz. Bitcoin-SHA-256d-ASICs sind nicht kompatibel; X4NOVA benötigt seinen angepassten Miner. [2]

Die Alpha 0.4 bietet PPLNS für gemeinsames Mining und Solo für eigene Blockfunde. PPLNS verteilt den Erlös nach den letzten bis zu 4.096 gültigen Shares beim Blockfund, einschließlich des Finder-Shares. Die gespeicherte Schwierigkeit bestimmt das Gewicht jeder Arbeit. Gemeldete Hashzahlen dienen nicht als Zahlungsbeweis.

Die Gebühr beträgt 1 % bei PPLNS und 1,5 % bei Solo. Vom nativen Budget aus Subvention und Transaktionsgebühren wird zuerst die Poolgebühr abgezogen. Ganzzahlige Quotienten und größte Bruchreste verteilen den verbleibenden Betrag atomgenau; Gleichstände werden deterministisch nach Konto und Adresse aufgelöst.

Pool-Wallet und Auszahlung

Neue Pool-Blöcke zahlen an die eigene verschlüsselte Pool-Wallet. Gutschriften werden erst nach nativer Coinbase-Reife auszahlbar. Automatische Auszahlungen erfolgen alle zwei Stunden ab der Kontogrenze, standardmäßig 1 X4N und einstellbar ab 0,1 X4N. Die Poolgebühr finanziert die Transaktionsgebühr. Während dieses Vorgangs verwaltet der Betreiber die Pool-Guthaben.

- Reorganisationen korrigieren Guthaben; Schulden werden über alle Adressen eines Kontos verrechnet.
- Reservierungen und signierte Transaktionsdaten werden vor der Veröffentlichung dauerhaft gespeichert.
- Wiederholungen verwenden dieselbe Transaktion und werden mit der aktiven Kette abgeglichen.

> Gemeinsames Mining verteilt Glücksrisiko. Ertrag hängt weiterhin von gültiger Arbeit, Difficulty, Blockfunden und Betriebskosten ab. Alpha-Testbestände erlauben keine Euro-Ertragsprognose.

Wie der Pool Mining-Aktivität misst

Die öffentliche Übersicht macht sichtbar, wer gerade verbunden ist und welche Worker zuletzt gültige Arbeit eingereicht haben.

Verbindung und Beitrag

Der Pool zählt jeden angemeldeten Worker einmal, auch bei mehreren gleichzeitigen Verbindungen. Ein neuer Worker erscheint bei der nächsten Aktualisierung. Als beitragend zählt jeder Worker mit mindestens einem geprüften Share in den letzten 900 Sekunden. Ein getrennter Worker bleibt bis zum Ablauf dieses Fensters sichtbar. Eine Person kann mehrere Worker betreiben.

Geschätzte Hashrate

Für jeden akzeptierten Share mit Zielwert T fließt die erwartete Arbeit 2^256 / (T + 1) ein. Die Summe geteilt durch 900 Sekunden ergibt die angezeigte Hashrate in H/s. Ein Worker kann verbunden sein und 0 H/s anzeigen, bis der erste Share eintrifft. Bei wenigen Shares schwankt der Schätzwert stark.

Öffentliche Messwerte

Die Poolseite zeigt einen pseudonymen Alias, Verbindungszustand, Modus, Sharezahl, Hashrate und Zeitpunkt des letzten Shares im Fenster. Rig-Namen, Wallet-Adressen, IP-Adressen und Zugangskennungen bleiben außerhalb der Liste. Der Alias kann über mehrere Messungen wiedererkannt werden.

> Beispiel: Ein Worker trennt sich um 12:00 Uhr unmittelbar nach einem gültigen Share. Andere Miner können seinen Beitrag noch bis 12:15 Uhr in der Übersicht sehen. Für die Vergütung gelten die eigenen Regeln des gewählten Poolmodus.

Geldmenge und nachvollziehbare Emission

Die bestehende Emissionsregel bleibt die Grundlage. Sie wird nicht heimlich an Strompreise oder den Coin-Kurs angepasst.

Eigenschaft	Bestehende Lab-Regel und Entwurfsgrundlage
Kleinste Einheit	1 X4N = 100.000.000 Atome
Genesis	0 X4N ausgebbare Subvention
Erste Belohnungsepoche	50 X4N für Höhe 1 bis 420.000
Halbierung	Alle 420.000 belohnten Blöcke; erstmals ab Höhe 420.001
Obergrenze	41.999.999,9538 X4N durch Ganzzahlrundung
Premine	0 %; keine gesonderte Gründer-Coinbase

```
R(0) = 0
R(h) = 5.000.000.000 >> floor((h – 1) / 420.000), für h ≥ 1; Einheit: Atome
```

Die theoretische Summe beträgt 4.199.999.995.380.000 Atome. Nicht beanspruchte Belohnungen, verlorene Schlüssel und unbrauchbare Ausgaben können die tatsächlich verfügbare Menge verringern. Transaktionsgebühren sind eine Übertragung bestehender Werte und keine zusätzliche Emission.

Eine Epoche dauert bei durchschnittlich 300 Sekunden je Block rund 3,99 Jahre. Alle Fullnodes berechnen die zulässige Subvention aus der Höhe. Gebühren dürfen nur aus tatsächlich ausgegebenen Eingängen stammen. Auch die Stimmen aller Miner zusammen schaffen keinen zusätzlichen Atom.

> In der ausgelieferten LabNet-Version 0.4.3 wurden sämtliche 13.860.000 Höhen mit positiver Subvention nachgerechnet. Der letzte Block dieser Folge zahlt einen Atom. Ab Höhe 13.860.001 besteht der maximal zulässige Blockerlös ausschließlich aus den enthaltenen Transaktionsgebühren.

Das Gleichgewicht von Sicherheit und Nutzung

Miner-Vergütung, Transaktionskosten und Ressourcengrenzen müssen zusammen bewertet werden.

```
Blockerlös = zulässige Subvention + enthaltene Transaktionsgebühren
Erwarteter Miner-Anteil ≈ Anteil an gültiger Arbeit × verfügbares Erlösbudget
```

Die zweite Beziehung ist ein vereinfachter Erwartungswert. Glück, stale Blöcke, Poolregeln und Gebühren verändern tatsächliche Zahlungen. Der wirtschaftliche Ertrag hängt zusätzlich vom Coin-Wert und individuellen Strom-, Geräte- und Betriebskosten ab. Eine große Zahl ausgezahlter Coins allein bedeutet keinen hohen Verdienst.

Die Difficulty soll die mittlere Blockproduktion bei wechselnder Rechenleistung stabilisieren. Sie garantiert weder einen Euro-Gewinn noch eine bestimmte Stromrechnung. Eine neue Coin-Ausgabe automatisch an gemeldete Kosten zu binden wäre zudem manipulierbar und würde die veröffentlichte Geldordnung verändern.

Mit sinkender Subvention wächst die Bedeutung echter Nachfrage nach Blockplatz und der daraus entstehenden Gebühren. Eine hohe Sicherheitsfinanzierung, ein harter Geldmengendeckel und praktisch kostenlose beliebige Nutzung lassen sich nicht gleichzeitig garantieren. X4NOVA muss Nutzung effizient bündeln und die langfristige Tragfähigkeit mit Szenarien prüfen.

Szenario	Was zu bewerten ist
Wenig Nachfrage	Reicht das Erlösbudget für ausreichende verteilte Arbeit?
Hohe Nachfrage	Wie wachsen Wartezeit, Gebühren und Ressourcenbedarf?
Hashrate fällt stark	Wie schnell stabilisiert die Difficulty die Blockabstände?
Subvention halbiert sich	Wie reagieren Teilnahme, Konzentration und Gebührenanteil?

> Die wirtschaftlichen Szenarien dienen der Gestaltung, nicht einer Ertrags- oder Kursprognose. Ein öffentliches Netz wird erst vertretbar, wenn seine Finanzierung und sein Angriffsszenario nachvollziehbar bewertet wurden.

Gebühren senken durch effiziente Nutzung

Das Ziel sind vorhersehbare, angemessene Kosten je nützlicher Handlung und ein tragfähiges Gesamtbudget für Miner.

Die Wallet soll vor der Freigabe eine verständliche Gebührenschätzung aus Größe, Ressourcenbedarf und gewünschter Bestätigungspriorität anzeigen. X4N-Betrag und gegebenenfalls eine separat gekennzeichnete Kursumrechnung dürfen nicht vermischt werden. Eine feste Euro-Gebühr ist keine Eigenschaft des aktuellen Konsenses.

- Zahlungen bündeln, wenn Nutzer mehrere Empfänger gemeinsam bedienen möchten.
- Digitale Nachweise über Merkle-Bäume bündeln, statt jede Datei einzeln zu verankern.
- Nur notwendige Nachweisdaten aufnehmen; keine vollständigen Dokumente in der Chain speichern.
- Rechen- und Datengrenzen für zusätzliche Funktionen vor deren Einführung festlegen.
- Sehr kleine Auszahlungen und UTXO-Zusammenführung bewusst gestalten; Privatsphäre bleibt Teil dieser Entscheidung.

Beispiel für gebündelte Nachweise

Angenommen, eine Verankerung kostet insgesamt 0,01 X4N und bündelt 1.000 Nachweise. Der reine Verankerungsanteil wäre rechnerisch 0,00001 X4N je Nachweis, bevor Zusatzkosten berücksichtigt werden. Der Zahlenwert ist eine Illustration und keine aktuelle Gebühr oder zugesagte Preisstufe. Jeder Nutzer benötigt zusätzlich seinen eigenen Merkle-Pfad und die Daten zur Verifikation. [8]

Mit der Bündelung können geringere Kosten je Nachweis und weiter bezahlter Blockplatz zusammenpassen. Der Miner erhält jedoch insgesamt nur die tatsächlich entrichteten Gebühren. Bündelung garantiert daher kein bestimmtes Sicherheitsbudget. Eine günstige Einzelhandlung braucht langfristig ausreichend reale Gesamtnutzung.

> Der aktuelle lokale Lab-Signer begrenzt eine Transaktionsgebühr auf 10.000 Atome. Das ist eine Schutzgrenze des Prototyps, keine Preisgarantie und keine bereits erprobte Gebührenpolitik für ein öffentliches Netz.

Zügig bezahlen, Sicherheit sichtbar halten

Geschwindigkeit wird aus Nutzersicht und aus Sicht der Konsenssicherheit getrennt gemessen.

Status	Bedeutung für den Nutzer
Erstellt und signiert	Die lokale Freigabe ist erfolgt; noch keine Kettenaufnahme.
Übertragen und gesehen	Teilnehmer kennen die Zahlung; noch keine Bestätigung.
In einem Block	Die Zahlung ist in der aktuellen aktiven Kette enthalten.
Weitere Bestätigungen	Zusätzliche Arbeit erhöht die Absicherung gegen Reorganisationen.

Eine schnelle Rückmeldung darf keine endgültige Zahlung vortäuschen. Empfänger sollen die notwendige Absicherung nach Betrag und Risiko wählen können. Ein Händlerhinweis, dass eine Transaktion gesehen wurde, ist ein anderer Zustand als eine ausreichende Anzahl von Bestätigungen.

Das feste Ziel beträgt 300 Sekunden. Einzelne Blöcke können in Sekunden oder erst nach deutlich mehr als fünf Minuten eintreffen. Ab Block 672 bestimmt das 144-Blöcke-Fenster die erforderliche Arbeit. Die Wallet zeigt die bisher erreichte Zahl von Bestätigungen.

Ein Miner muss 100 Blöcke Reife abwarten, bevor seine Coinbase ausgegeben werden darf. Bei Zieltempo entspricht das rund acht Stunden und zwanzig Minuten. Die Zeit auf der Uhr allein macht eine Coinbase nicht ausgebbar.

Zahlungskanäle können später schnelle wiederholte Übertragungen außerhalb einzelner Hauptkettenblöcke ermöglichen. Dafür braucht es verfügbare Liquidität, korrekte Schließungsregeln und getestete Wiederherstellung. Lightning dient als Referenz; ein kompatibles X4NOVA-Verfahren ist noch nicht vorhanden. [9]

> Vor belastbaren Messungen werden weder eine garantierte Sekundenzahl bis zur sicheren Zahlung noch eine feste Transaktionsrate pro Sekunde zugesagt.

Wallet, Sicherung und Kontozugriff

Das Konto hilft beim Zugang. Die lokale Wallet entscheidet über die Verfügung über Werte.

Die Wallet erzeugt lokal 24 BIP39-Wörter aus 256 Bit Zufall. Eine optionale Zusatzpassphrase, oft 25. Wort genannt, wird exakt mit Großschreibung und Leerzeichen abgeleitet. Jede andere Passphrase führt zu einer anderen Wallet. Das verschlüsselte Backup sichert sie mit. Die aktuellen Schlüsselpfade verwenden BIP32/BIP86; Empfang und Wechselgeld sind im Prototyp noch begrenzt. Signaturen basieren auf secp256k1 und Schnorr; Transaktionen verwenden Taproot-Keypath-Ausgaben. Die vollständige Adressrotation und Wiederherstellung über viele Empfangsadressen sind weitere Entwicklungsaufgaben. [10]

Das lokale Backup verwendet AES-256-GCM und eine passwortbasierte Schlüsselableitung mit PBKDF2-HMAC-SHA256, 600.000 Durchläufen, zufälligem Salt und frischer IV. Ein vergessenes lokales Passwort kann nicht durch ein Website-Passwort ersetzt werden. Die separat gesicherte Wiederherstellungsphrase ist dafür entscheidend.

Das Teamkonto kann öffentliche Wallet-Daten und daraus gelesene Bestände anzeigen. Es erhält keine Seed-Phrase für das normale lokale Signieren. Zwei-Faktor-Anmeldung schützt den Kontozugang; die Wallet-Verschlüsselung schützt lokale Schlüssel. Diese Mechanismen erfüllen verschiedene Aufgaben und machen die aktuelle Transaktionshistorie nicht anonym.

- Vor dem Signieren Empfänger, Betrag, Wechselgeld und Gebühr anzeigen und prüfen.
- Nach Inaktivität lokale Schlüssel sperren; Kontozustand und Schlüsselfreigabe getrennt halten.
- Bestätigte, wartende und unreife Beträge getrennt anzeigen.
- Backups und Wiederherstellung auf unterstützten Geräten mit festen Testvektoren überprüfen.

> Eine spätere Privacy-Architektur kann zusätzliche Schlüssel und andere Scan- oder Wiederherstellungsregeln benötigen. Die heutigen 24 Wörter allein sind kein Nachweis, dass eine solche Migration schon möglich ist. Echte Bitcoin-Seeds werden im Lab nicht wiederverwendet.

Zahlungsfunktionen für Menschen und Anwendungen

Eine gute Zahlung endet nicht bei der Signatur: Sie muss angefordert, verstanden, bestätigt und bei Fehlern erklärt werden können.

Vorhanden sind lokal signierte Lab-Zahlungen mit gesonderter Veröffentlichung und Bestandsanzeige aus geprüften Transaktionsdaten. Die nächste Produktstufe soll Zahlungsanforderungen mit Betrag, Ablaufzeit und optionalem Zweck unterstützen. QR-Codes und teilbare Anfragen sollen Tippfehler verringern, ersetzen aber nicht die Prüfung des Empfängers.

Händler und wiederkehrende Abläufe

Eine geplante Händler-Schnittstelle soll Zahlungseingänge nachvollziehbar einer Anfrage zuordnen. Meldungen benötigen eine eindeutige Kennung, wiederholbare Zustellung ohne doppelte Buchung und Behandlung von Reorganisationen. Ein angezeigter Kurs ist eine zusätzliche Information mit eigener Quelle und Zeitangabe; der native Transfer bleibt in X4N.

Wiederkehrende Anfragen können später Rechnungsabläufe vereinfachen. Automatische Abbuchungen aus einer selbstverwahrten Wallet entstehen dadurch nicht. Jede Delegation von Ausgaberechten müsste ausdrücklich begrenzt, widerrufbar und technisch geprüft sein.

Freigaben mit mehreren Beteiligten

Mehrparteienfreigaben und zeitabhängige Bedingungen sind geplante Kandidaten, etwa für gemeinsame Budgets oder eine Zahlung nach vereinbarter Zustimmung. Ein kryptografisch erfüllter Vertrag entscheidet nicht automatisch, ob eine reale Leistung gut erbracht wurde. Für solche Fälle braucht es definierte Beteiligte, Fristen und einen Umgang mit Streitfällen.

> Zahlungsanforderungen, Händler-Schnittstelle und zusätzliche Freigabemodelle sind geplante Funktionen. Ihr Umfang wird erst nach Protokoll- und Wallet-Tests als verfügbar ausgewiesen.

Digitale Nachweise, die unabhängig prüfbar bleiben

PROOF verbindet lokale Datenintegrität mit einer nachprüfbaren Aufnahme in die Blockchain.

Im aktuellen Lab wird die Datei lokal mit SHA-256 gehasht. Der Proof-Ausgang enthält ein 38-Byte-Payload: Kennung X4NP, Formatversion, Hash-Verfahren und den 32-Byte-Datei-Hash. Die vollständige Datei wird nicht veröffentlicht. Ein exportierter Nachweis enthält Netzwerkkennung, Hash, Transaktion, Block und einen nativen Merkle-Beweis.

Eine Prüfung muss sowohl die Übereinstimmung mit der lokalen Datei als auch die Aufnahme der Transaktion und den aktuellen Kettenstatus bewerten. Ein im Konto gespeicherter Hash ohne Verankerung bleibt ausdrücklich ein Eintrag außerhalb der Blockchain. Ein späterer Zweigwechsel kann Bestätigungen verändern.

Einzelbelege für ein Dateibündel

Der Browser bündelt bis zu 256 Dateien mit zusammen höchstens 100 MiB. Pro Datei erzeugt er lokal einen zufälligen Salt mit 32 Bytes. Blatt, innerer Knoten und Wurzel werden mit getrennten Präfixen gehasht. Die Blattposition und die Anzahl der Dateien sind gebunden. Ein Einzelbeleg enthält den eigenen Salt und die benötigten Geschwisterhashes. [8]

Was der Prüfer bestätigen kann

Mit Originaldatei, Einzelbeleg und einem unabhängig bezogenen Wurzelhash lässt sich die Zugehörigkeit lokal prüfen. Für einen Zeitnachweis muss die Wurzel in einer bestätigten Transaktion stehen. Die Wallet-API prüft den gebundenen Wert, den nativen Merkle-Beweis und den Status des Blocks auf der aktiven Kette. Ein exportierter Beleg ist eine Momentaufnahme.

> Ein Nachweis belegt die geprüfte Bindung bestimmter Daten an eine Verankerung. Er beweist allein weder Urheberschaft noch Eigentum oder einen exakt zertifizierten Erstellungszeitpunkt. Originaldatei, Nachweis und gegebenenfalls Salt müssen erhalten bleiben.

Programmierbare Funktionen mit begrenzten Kosten

Mehr Funktionalität soll einen nachvollziehbaren Nutzen bringen und auf normalen Prüfrechnern beherrschbar bleiben.

Die erste Richtung sind verständliche Zahlungsbedingungen: mehrere Freigaben, Zeitbedingungen, definierte Rückfallpfade und die Verknüpfung von Zahlungen mit ausdrücklich freigegebenen Nachweisen. Solche Abläufe können einen praktischen Mehrwert schaffen, ohne bereits eine beliebige allgemeine Programmausführung zu versprechen.

Im getrennten Entwicklungsnetz führt revm signierte EVM-Transaktionen aus. Die native Zahlungs-Alpha prüft weiterhin UTXOs. Eine verbindliche Vertragsausführung für alle Teilnehmer verlangt identische Zustandsübergänge, begrenzten Gasverbrauch und Regeln zum Verwerfen fehlerhafter Blöcke. [3]

Ein erweitertes UTXO-Modell ist eine alternative Forschungsrichtung für ausdrucksstärkere Bedingungen. Seine Verbindung mit vertraulichen Zahlungen müsste gesondert entworfen werden. Die bloße Wahl von UTXOs liefert weder vollständige Anonymität noch automatisch Ethereum-Kompatibilität. [4]

- Ein Fehler darf keine neue Coin-Ausgabe außerhalb der Emissionsregel ermöglichen.
- Jede zusätzliche Prüfung benötigt ein dokumentiertes Ressourcenbudget.
- Wallets müssen Bedingungen verständlich erklären, statt unbekannten Code blind freizugeben.
- Verträge dürfen nur die Daten offenlegen, deren Veröffentlichung zum gewählten Modell gehört.

> Ein Token-Vertrag wurde im separaten Entwicklungsnetz ausgeführt. Vor einem öffentlichen Einsatz müssen unabhängige Nodes dieselben Zustandswurzeln erzwingen. Brücken zwischen öffentlichen Netzwerken bleiben Forschung.

Was eine kleine Fullnode tragen kann

Der feste Zielabstand beträgt 300 Sekunden im langfristigen Durchschnitt. Für den Start empfehlen wir einen Prüfkandidaten von höchstens 250.000 serialisierten Byte einschließlich Header, Coinbase und Witness.

Blockdaten	Rohdaten pro Jahr bei Volllast	Status
250.000 Byte	26,28 GB	Startkandidat im Versuch
1 MB	105,12 GB	Beide Zahlungsprofile im Lab zulässig
2 MB	210,24 GB	Beide Profile über dem aktiven Gewichtslimit
4 MB	420,48 GB	Beide Profile über dem aktiven Gewichtslimit
8 MB	840,96 GB	Beide Profile über dem aktiven Gewichtslimit

Gerechnet sind 365 Tage und durchschnittlich 105.120 Blöcke. Ein GB bezeichnet eine Milliarde Byte. Bei 25 Prozent Füllung wären es im Startkandidaten 6,57 GB Rohblöcke pro Jahr. Datenbanken, Indizes, Betriebsreserve und Vertragszustand benötigen zusätzlichen Speicher. Pruning kann ältere Rohblöcke nach der Prüfung entfernen. Der aktuelle Zustand bleibt erforderlich.

Das heutige LabNet prüft höchstens 4.000.000 Gewichtseinheiten. Gewicht ist dreimal die Größe ohne Witness plus die gesamte serialisierte Größe. Im Versuch passten 1.218 Zahlungen mit zwei Ausgängen oder 309 mit jeweils 16 Ausgängen in das kleinere Budget. Die beiden Arbeitsprofile beanspruchen unterschiedliche Rechenzeit und erzeugen unterschiedlich viele neue Ausgänge.

Zwei lokale Fullnodes der Version 0.4.3 prüften einen Block mit 249.952 Byte in rund 120 Millisekunden bis zur Bestätigung durch den zweiten Prozess. Der Neuaufbau mit Pruning ergab denselben UTXO-Zustand.

> Vor der Festlegung des Größenlimits fehlen Langzeitmessungen zur Löschung alter Blockdateien sowie Versuche auf schwächeren Geräten und Heimanschlüssen.

Skalierung ohne versteckte Gegenrechnung

Ein günstiger Transfer darf nicht durch unbegrenzt wachsende Prüf- und Speicheranforderungen für alle anderen bezahlt werden.

Zu messen sind Transaktionsgröße, Zeit für Signatur- und Privacy-Prüfungen, Beweisgrößen, Speicherwachstum sowie das Verhalten unter Spitzenlast. Die reine Zahl erzeugter Testtransaktionen ist kein vollständiger Leistungsnachweis. Hardware, Datensatz, Auslastung und Messmethode müssen bei Benchmarks genannt werden.

Zunächst werden unnötige Daten vermieden, Nachweise gebündelt und die Verarbeitung bestehender Formate verbessert. Eine Vergrößerung von Blöcken oder Verkürzung der Blockzeit muss zusammen mit Verteilungsverzögerung und Teilnahmebedingungen bewertet werden. Ein Teil dieser Werkzeuge existiert bereits in anderen Protokollen und ist keine neue X4NOVA-Erfindung.

Compact Block Relay ist eine Referenz für effizientere Blockübertragung. Eine Übernahme bewährter Verfahren muss zum veränderten Arbeitsnachweis und Transaktionsformat passen und erneut gemessen werden. Geschwindigkeit entsteht nicht nur aus kleineren Zeitwerten, sondern auch aus weniger unnötiger Übertragung und zuverlässiger Validierung. [11]

- Schwache und starke Prüfrechner in denselben reproduzierbaren Tests berücksichtigen.
- Normallast, Lastspitzen und absichtliche Überlastung getrennt messen.
- Privacy-Prüfungen, Wallet-Suche und Wiederherstellung als Teil der Leistung erfassen.
- Wachstum und Wartungskosten über längere Zeit statt nur kurze Spitzenwerte bewerten.

> Zahlungskanäle oder zusätzliche Ausführungsebenen verschieben Aufgaben und Risiken. Liquidität, Datenverfügbarkeit, Rückzugsmöglichkeiten und zusätzliche Gebühren müssen im jeweiligen Modell ausdrücklich benannt werden.

Sicherheitsziele und Freigabekriterien

Öffentliche Freigabe folgt überprüfbaren Ergebnissen, nicht einer schönen Oberfläche oder einer festen Marketingfrist.

Im LabNet kann jeder eine Fullnode ab Genesis starten. Sie importiert Rohblöcke und prüft neue Blöcke aus dem öffentlichen HTTPS-Datenstrom lokal. Nach einem Neustart stimmten auf Höhe 611 Blockhash und Prüfsumme aller unverbrauchten Transaktionsausgänge auf drei Instanzen überein. Eine einzelne Datenquelle kann eine stärkere Kette zurückhalten. Für das Mainnet braucht es unabhängige Peers.

Bereich	Nachweis vor einer öffentlichen Freigabe
Konsens	Ungültige Arbeit und Signaturen, Grenzhöhen, Partitionen und tiefe Reorganisationen geprüft
Mining und Difficulty	Hashratewechsel, Zeitstempelangriffe, Jobwechsel und Belohnungsgrenzen untersucht
Wallet	Wiederherstellung, Adresssuche, Freigabeprüfung und Update-Verhalten unabhängig bewertet
Privatsphäre	Bedrohungsmodell, Inflationskontrolle, Metadaten und kryptografische Prüfung dokumentiert
Releases	Nachvollziehbare Quellstände, reproduzierbare Builds und signierte Veröffentlichungen

Die Windows-Wallet der Reihe 0.4 wird mit SHA-256-Prüfsummen verteilt. Gast-Miner verbinden sich per Stratum-TLS mit einer LabNet-Auszahlungsadresse und optionalem Rig-Namen. Freigegebene Teamkonten mit verifizierter E-Mail und Zwei-Faktor-Anmeldung können zusätzlich einzeln widerrufbare Worker-Tokens mit zwölf Stunden Laufzeit erstellen. Der öffentliche Explorer zeigt bestätigte Auszahlungen mit Betrag und Empfangsadresse. Shares verbleiben im Pooljournal.

> Testbestände haben keinen zugesagten Wert. Ein öffentliches Mainnet, ein Verkauf oder eine Börsenlistung wird mit diesem Whitepaper nicht angekündigt. Eine Einführung zusätzlicher Produkte benötigt neben technischen Prüfungen ihre jeweilige rechtliche Bewertung.

Entwicklung nach überprüfbaren Etappen

Der Funktionsumfang wächst in Schritten. Ein Ziel wird erst dann als vorhanden bezeichnet, wenn seine Abnahme bestanden ist.

Etappe	Ergebnis und Abnahme
Lab-Grundlage · vorhanden	Eigene Testkette, lokal prüfende Fullnode, Wallet, CPU-Miner, Zahlungen und Proof-Export
Alltagstaugliche Wallet · geplant	Adressrotation, vollständige Wiederherstellung, Zahlungsanfragen und verständliche Fehlerzustände
Gemeinsames Mining · im Lab vorhanden	PPLNS, Solo, veröffentlichte Gebühren, Pool-Wallet, Auszahlungshistorie, Worker-Verwaltung und Reorg-Abrechnung
Privacy-Protokoll · Forschung	Ausgewähltes, unabhängig bewertetes Verfahren samt Wallet-, Nachweis- und Migrationsmodell
Leistung und Gebühren · Forschung	Vergleich von Blockzielen, Ressourcenbudgets und Nachfrage-/Sicherheits-Szenarien
Programmierbare Anwendungen · Entwicklungsnetz	EVM-Belege vorhanden. Als Nächstes unabhängige Durchsetzung der Zustandsregeln prüfen.
Öffentliche Freigabe · offen	Audits, reproduzierbare Veröffentlichungen und bestandene Langzeittests

Die Kombination aus Mining, Privatsphäre und schneller Nutzung ist das Entwicklungsziel. Der Ablauf kann sich durch Prüfergebnisse ändern. Insbesondere eine andere Transaktionskryptografie kann neue Wallet-Formate und einen getrennten Netzstart erfordern. Bestehende Lab-Bestände werden nicht als Vorteil in ein neues öffentliches Netz übertragen.

Für jeden Schritt werden ein konkreter Nutzen, prüfbare Kriterien und bekannte Grenzen dokumentiert. Eine Verschiebung ist sinnvoller als eine Funktion mit unzutreffendem Sicherheits- oder Datenschutzversprechen zu veröffentlichen. Es gibt deshalb keine garantierten Mainnet-Termine in dieser Fassung.

Versionen, Regeln und ehrliche Produktkommunikation

Ein öffentliches Regelwerk soll es Nutzern ermöglichen, Veränderungen zu verstehen und eigene Entscheidungen zu treffen.

Die Bezeichnungen vorhanden, geplant und Forschung haben eine feste Bedeutung. Vorhanden meint eine im beschriebenen Lab-Umfang nutzbare Funktion. Geplant meint einen konkret beschriebenen nächsten Baustein ohne Verfügbarkeitszusage. Forschung meint eine offene technische oder wirtschaftliche Entscheidung, deren Eignung erst belegt werden muss.

Die Geldordnung und das Blockzeitziel sind für X4N festgelegt. Technische Erweiterungen wie neue Transaktionsformate benötigen eine veröffentlichte Spezifikation, reproduzierbare Testvektoren, eine beschriebene Aktivierung und Angaben zu bestehenden Wallets. Jeder Betreiber prüft die Software seiner Node.

Ein neues Whitepaper allein ändert keine laufenden Konsensregeln. Diese Version bestätigt PoW als Richtung und erweitert die Produktziele. PPLNS, Solo und die Fensterkorrektur ab Höhe 672 gehören zur Alpha. Vertrauliche Zahlungen und eine allgemeine Vertragsmaschine bleiben Entwicklungsziele. Die bestehenden Lab-Grenzen bleiben ausdrücklich erkennbar.

Was künftig veröffentlicht werden soll

- Versionierte Protokoll- und Dateiformate mit Lizenz- und Quellhinweisen.
- Messberichte mit Voraussetzungen, beobachteten Grenzen und nachvollziehbaren Ergebnissen.
- Änderungsbeschreibungen für Nutzer, Miner und Entwickler.
- Sicherheitsmeldungen und korrigierte Releases ohne rückwirkende Umdeutung alter Ergebnisse.

> Das Ziel ist eine eigene, klar erkennbare X4NOVA-Erfahrung. Der Nutzen entsteht aus überprüfbaren Funktionen; eine pauschale Überlegenheit gegenüber Bitcoin, Ethereum oder Privacy-Protokollen wird nicht behauptet.

Vom ersten Miner zum offenen Netzwerk

Ein Miner kann die erste gültige Historie aufbauen. Erst unabhängige Teilnehmer verteilen die Kontrolle über die verfügbare Rechenleistung.

Was beim Ausscheiden des ersten Miners geschieht

In einem separaten Abnahmelauf begann ein Miner allein. Zwei weitere Prozesse synchronisierten sich ab Genesis. Während der erste offline war, entstanden die Blöcke 2 und 3. Nach seiner Rückkehr erreichte er dieselbe Spitze. Eine Wallet erkannte nach der Wiederherstellung aus einer älteren Sicherung die bestätigte Zahlung von 1,25000000 Test-X4N. Alle drei Prozesse gehörten demselben Betreiber.

Jede Full Node prüft unter anderem Arbeitsnachweis, zulässige Ausgabe und Signaturen. Bei zwei zeitnahen gültigen Funden können Nodes vorübergehend verschiedene Spitzen sehen. Sie folgen der gültigen Kette mit der meisten kumulierten Arbeit. Nur die Belohnung im aktiven Zweig zählt. Ein Pool verteilt seinen tatsächlichen Ertrag nach seinen veröffentlichten Regeln.

Abnahme durch unabhängige Betreiber

- Eigene Schlüssel lokal erzeugen, ab Genesis synchronisieren und Höhe, Spitzenhash und kumulierte Arbeit vergleichen.
- Den ersten Miner abschalten, mit eigener Hardware weiterarbeiten und nach dem Wiederanschluss eine Zahlung und ihren Bestätigungsstand prüfen.
- Blocklaufzeiten, verwaiste Blöcke und Konzentration der beobachtbaren Hashrate über einen angegebenen Zeitraum veröffentlichen. Pool-Adressen allein identifizieren keine unabhängigen Menschen.

> Der feste Arbeitsschlüssel im privaten Versuch und die geringe öffentliche Beteiligung erlauben keine belastbare Aussage über die Angriffskosten eines späteren Mainnets.

Welche Regeln Rust heute prüft

Das Zahlungsnetz und das getrennte Rust-Entwicklungsnetz beantworten verschiedene Fragen. Ihr jeweiliger Nachweis lässt sich einzeln wiederholen.

Prüfung	Beobachtbarer Stand
Native Zahlungen	Die C++-Full-Node auf Core-Basis prüft UTXOs, Skripte, Signaturen, Coinbase-Reife und Blocksubvention.
Rust-Prüfer	Prüft Arbeit, Ziel und Geldregeln vor der Vertragsausführung. Der Hash des gesamten UTXO-Bestands stimmt auf zwei Testhistorien mit Core überein. Ein Zweigwechsel verwirft den alten Zustand. Skripte und Zweigauswahl prüft weiterhin Core.
Vertragsausführung	Alloy dekodiert signierte Typ-2-Transaktionen. revm führt sie nach Shanghai-Regeln aus. Das Testlimit beträgt zehn Millionen Gas pro Block bei fünf Millionen Zielgas.
Testbelege	Ein Testvertrag lieferte einen Transaktionsbeleg und eine überprüfte Verankerung des zuvor berechneten Zustands. Native Wallet und Vertragskonto haben getrennte Salden.

Ein nativer Atom entspricht im Versuch zehn Milliarden Ausführungseinheiten. Guthaben gelangt nur in eine Richtung in die Testausführung. Native Gebühren und Ausführungsgas fallen getrennt an. Ein späterer Rücktransfer benötigt eigene Regeln gegen Doppelgutschriften.

> Vor einem gemeinsamen Netz müssen auch andere Nodes ungültige Ausführungswurzeln verwerfen, nach einem Zweigwechsel denselben Zustand herstellen und die gesamte Geldmenge unabhängig prüfen. Ein nativer X4N hat keine ERC-20-Vertragsadresse.

Wie sich die Regeln ändern können

Betreiber wählen die Software, deren Regeln sie anwenden. Ein zusätzlicher Node, ein Website-Konto oder eine Poolmitgliedschaft verleiht kein Stimmrecht im Konsens.

Jeder kann einen Änderungsvorschlag einreichen. Er beschreibt Motivation, präzise Kodierung und Gültigkeitsregeln, Auswirkungen auf bestehende Wallets, Aktivierung und reproduzierbare Positiv- und Negativbeispiele. Autoren veröffentlichen Entwurf und Quelländerung mit einer Version. Betreiber können sie in einem getrennten Netz erproben und selbst über das Update entscheiden.

Bei inkompatiblen Regeln können zwei gültige Historien nach unterschiedlichen Regelwerken entstehen. Vor einer Aktivierung brauchen Nutzer und Börsen eindeutige Netzwerkkennungen, Angaben zur Wiederverwendbarkeit signierter Transaktionen und ein Verfahren für unterbrochene Ein- und Auszahlungen. Ein Betreiber kann die eigene Software auswählen, anderen Nodes jedoch keine neuen Ausgaberegeln aufzwingen.

Die Grenze zwischen einer Erweiterung und einer Abspaltung

Der Vorschlag für ein kürzeres Blockintervall ist geschlossen. Die X4N-Regeln schreiben 300 Sekunden Zielabstand, 420.000 belohnte Blöcke je Halbierung und die ganzzahlige Emission vor. Fremder Quellcode kann kopiert und verändert werden. Eine daraus entstehende Kette mit anderen Geldregeln ist ein Fork. Bestehende Fullnodes verwerfen Blöcke, sobald diese ihre Regeln verletzen. Bis dahin können beide dieselbe Historie teilen.

Eine Community-Abstimmung kann beispielsweise einen Vorschlag zum Speicherbudget bewerten. Er braucht Messdaten, eine veröffentlichte Softwareversion und eine vorab bekannte Aktivierungshöhe. Das Stimmenverhältnis aktiviert keine Regel. Eine Hashrate-Mehrheit kann gültige Zahlungen verzögern oder umordnen. Sie kann weder Eigentümersignaturen ersetzen noch die zulässige Coinbase erhöhen. Diese Unterscheidung folgt aus den Abschnitten 5, 6 und 11 des Bitcoin-Whitepapers. [1]

Ein- und Auszahlungen an einer Börse

X4N ist als nativer Coin einer eigenen Chain entworfen. Ein Integrator braucht eine prüfende Node, eine kompatible Wallet und eine belastbare Entscheidung darüber, wann eine Einzahlung gutgeschrieben wird.

Liefergegenstand	Abnahmekriterium vor echtem Handel
Netzidentität	Versionierter Quellstand, Genesis, Adressformat, Netzwerkparameter und nachvollziehbarer Build. Lab- und Mainnet-Adressen eindeutig unterscheiden.
Einzahlung	Eigene Node vollständig synchronisieren. Einzahlungs-Ausgänge anhand von Transaktions-ID und Ausgangsindex eindeutig buchen. Bei Zweigwechsel Bestätigungen zurücknehmen und dieselbe Einzahlung nie doppelt gutschreiben.
Auszahlung	Acht Dezimalstellen in ganzen Atomen rechnen. Signieren, Gebühr und Wechselgeld prüfen, übertragen und Bestätigung überwachen. Wiederholte Anfragen dürfen keine zweite Auszahlung erzeugen.
Unterbrechung	Bei abweichender Spitze, geringer Arbeit oder langen Blockpausen Buchungen anhalten. Nach erneutem Abgleich kontrolliert fortsetzen. Wiederherstellung mit gesicherter Wallet und eigener Node vorführen.

Eine feste Bestätigungszahl liefert bei unbekannter externer Hashrate keine verlässliche Verlustgrenze. Betreiber müssen Arbeit, beobachtete Reorganisationen und Einzahlungsbetrag zusammen bewerten. Ein belastbarer Mainnet-Empfehlungswert steht aus.

> Für eine Bewerbung fehlen unter anderem öffentliche Netzwerkhistorie, unabhängige Prüfberichte und ein freigegebenes Mainnet-Release. Preise, Handelsvolumen, Partner und Zulassungstermine sind offen.

Unterlagen für eine mögliche Handelszulassung

Diese Fassung erläutert die Technik des zurücksetzbaren Testnetzes. Für eine Zulassung in der EU ist vorab zu klären, wie der Vermögenswert einzuordnen ist und wer rechtlich für den Antrag einsteht.

Bei Anwendbarkeit von MiCA-Titel II führen Artikel 6 und Anhang I unter anderem Angaben zu Antragsteller und gegebenenfalls Emittent und Plattform, Projekt und Finanzierung, Angebot oder Zulassung, Merkmalen und Rechten, Technologie, Risiken und Umweltwirkungen auf. Hinzu kommen die vorgeschriebenen Hinweise, die Erklärung des Leitungsorgans, eine verständliche Zusammenfassung und das Datum. Die rechtlichen Erklärungen stehen aus. [13]

Die Behandlung automatisch erzeugter Mining-Belohnungen in Artikel 4 betrifft Angebote. Eine beabsichtigte Zulassung zum Handel ist gesondert nach Artikeln 4 und 5 zu prüfen. Artikel 8 verlangt im anwendbaren Fall die Notifizierung samt Erläuterung der Einordnung mindestens 20 Arbeitstage vor Veröffentlichung. Die verantwortliche Stelle muss Veröffentlichung und spätere wesentliche Änderungen nachvollziehbar führen. [13]

Die vorgeschriebene maschinenlesbare Fassung nutzt XHTML mit Inline XBRL nach dem anwendbaren EU-Muster. Die ESMA stellt Taxonomie und Hinweise bereit. Die Projekt-PDF dient dem technischen Austausch. [14]

Unabhängig davon prüft jede Plattform selbst

Coinbase fragt nach Projekt, Quellcode und einer Unterschrift unter seine Vereinbarung. Binance verlangt einen direkten Antrag des Gründers oder eines Kernteammitglieds. Kraken nimmt auch Vorabprojekte über sein Formular an. Crypto.com verlangt bereits erfolgte rechtliche und sicherheitstechnische Prüfungen. Fragen gehen an info@x4nova.com. [16–19]

Energieverbrauch und Risiken belegen

Die Blockzeit ist kein Stromzähler. Verbrauch und Sicherheit hängen unter anderem von Anzahl, Leistung und Auslastung der tatsächlich beteiligten Miner ab.

Für den Testbericht sollen Teilnehmer Zeitraum, Gerätemodell, gemessene Wirkleistung über die gesamte Laufzeit, Betriebsstunden und erzielte Arbeit erfassen. Messungen an der Steckdose schließen den Systemverbrauch ein. Leerlaufwerte werden zusätzlich ausgewiesen. Energie in kWh ergibt sich aus mittlerer Leistung in kW mal Laufzeit in Stunden.

Eine Schätzung für ein offenes Netz braucht zusätzlich Angaben zur Abdeckung der Stichprobe, zu Gerätetypen und zur Quelle regionaler Strom- und Emissionsfaktoren. Gemessene Werte, extrapolierte Anteile und Unsicherheitsbereiche müssen erkennbar bleiben. Für ein X4N-Mainnet liegen keine Verbrauchs- oder Emissionsdaten vor. Die einschlägigen Nachhaltigkeitsindikatoren richten sich nach der delegierten Verordnung (EU) 2025/422. [15]

Risiko	Konkrete Folge
Geringe verteilte Arbeit	Bestätigte Zahlungen können bei einer gültigen Reorganisation aus der bevorzugten Historie fallen.
Verlust oder Offenlegung von Schlüsseln	Selbst verwahrte Bestände können unzugänglich werden oder durch Dritte ausgegeben werden.
Öffentliche Transaktionshistorie	Beträge und Verknüpfungen lassen sich auswerten. Eine frische Adresse allein sichert keine Anonymität.
Liquidität und Entwicklung	Handel, Werterhalt, Einlösung und Fertigstellung späterer Funktionen sind ungewiss. Testbestände verfallen bei Rücksetzung.

Primärquellen.

Referenzen für die beschriebenen Grundlagen. Ein Verweis bedeutet keine bereits erfolgte X4NOVA-Integration. Recherchestand: 22. November 2026.

[1] Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf

[2] RandomX: Algorithmus und Design
https://github.com/tevador/RandomX

[3] Ethereum: Ethereum Virtual Machine
https://ethereum.org/developers/docs/evm/

[4] Ergo: Extended UTXO
https://docs.ergoplatform.com/dev/protocol/eutxo/

[5] Monero: Stealth Addresses
https://www.getmonero.org/resources/moneropedia/stealthaddress.html

[6] Monero: RingCT
https://www.getmonero.org/resources/moneropedia/ringCT.html

[7] Meni Rosenfeld: Analysis of Bitcoin Pooled Mining Reward Systems
https://arxiv.org/abs/1112.4980

[8] OpenTimestamps: Nachweis- und Timestamp-Prinzip
https://opentimestamps.org/

[9] Lightning BOLT: Protokollgrundlagen
https://github.com/lightning/bolts/blob/master/00-introduction.md

[10] Bitcoin BIPs: Wallet- und Signaturstandards
https://github.com/bitcoin/bips

Protokoll und Zulassung

[11] BIP152: Compact Block Relay

https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki

[12] Bitcoin Cash Node: ASERT-Spezifikation

https://bitcoin-cash-node.gitlab.io/bchn-sw/bitcoincash-upgrade-specifications/2020-11-15-asert/

[13] MiCA, Titel II und Anhang I

https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[14] EU-Muster und maschinenlesbares Whitepaper-Format

https://eur-lex.europa.eu/eli/reg_impl/2024/2984/oj

[15] EU-Indikatoren zu Klima und Umwelt

https://eur-lex.europa.eu/eli/reg_del/2025/422/oj

[16] Coinbase Listing Application

https://www.coinbase.com/listings/apply

[17] Binance Listing Application Guidelines

https://www.binance.com/en/support/announcement/detail/305c55a531004eb094b838ba7740c98a

[18] Kraken Asset Listings

https://www.kraken.com/get-listed

[19] Crypto.com Listing Application

https://crypto.com/listing

[20] ERC-20 Token Standard

https://eips.ethereum.org/EIPS/eip-20

[21] Bitcoin Developer Guide · Block Chain und Proof of Work

https://developer.bitcoin.org/devguide/block_chain.html