Whitepaper

Noticoin-Protokoll, Emission, Wallet-Privatsphäre, Kartennotizen und Mining.

Technische Spezifikation · 1.0.0

Noticoin ist ein RandomX-Proof-of-Work-Netz mit begrenzter Geldmenge und integrierter Wallet-Karte. Die Spezifikation beschreibt Konsens, Transaktionsschutz, das Publikationsformat von Pins, die Zustellung bezahlter Notizen, das Betreiberregister, den Fonds und den Mining-Pool. Die Tabellen unterscheiden Konsensparameter und Anwendungseinstellungen. Die Diagramme nennen ihre Modellannahmen.

01 Konsens und Netzwerkidentität

02 Proof of Work und Blockvalidierung

03 Geldmenge und Blocksubvention

04 Bestätigungen und Verfügbarkeit

05 Wallet- und Transaktionsschutz

06 Format und Lebenszyklus der Kartenmarkierung

07 Betreiberregister und Epochen

08 Karteneinträge und Auslieferung

09 Gebühren und Fonds

10 Mining und Pool-Abrechnung

11 Verifikation und Freigabekriterien

12 Implementierung und Betriebsanleitungen

01

Konsens und Netzwerkidentität

Noticoin basiert auf Monero v0.18.5.4. Die Soll-Blockzeit beträgt 45 Sekunden. RandomX gilt ab Block 1 mit Version 16, Version 17 ab Höhe 160. Der P2P-Handshake prüft die Netzwerk-ID. Die Netze haben eigene Genesis-Hashes, Ports und Adresspräfixe.

Ein frischer Knoten bestimmt die Netzwerkidentität aus Konfiguration und Genesis. Beim Levin-Handshake wird die 16 Byte lange Netzwerk-ID geprüft. Adresspräfixe unterscheiden Standardadressen, integrierte Adressen und Unteradressen. Betreiber vergleichen Block null mit dem Manifest, bevor sie einen Knoten zur Zahlungsprüfung einsetzen. Zahlungsdienste müssen isolierten Regtest ausdrücklich freigeben.

Netzwerk	P2P	RPC	ZMQ	Adresspräfixe
mainnet	19080	19081	19082	111 / 112 / 113
testnet	29080	29081	29082	114 / 115 / 116
stagenet	39080	39081	39082	117 / 118 / 119

Standard / integriert / Unteradresse

Mainnet	**Genesis-Hash**	`2784467d7c909874668b9f0accf533c63f77aad79a3b72bfc5b23ca09e3cb614`
	P2P-Netzwerk-ID	`305639f9810544e48197a8f69a0a6d19`
Testnet	**Genesis-Hash**	`e2c8d4803df588a35e8289d2f939f3521ec92c43d4e8e453d05585917c205a90`
	P2P-Netzwerk-ID	`3946c278a80142618044dfa92619e1e7`
Stagenet	**Genesis-Hash**	`090c1b22ef96a0d7e05d7ec6321ad3f61d4f36c90cce2ce573e3c4be19f8daef`
	P2P-Netzwerk-ID	`0205f90fad5c4d41a8ad3bf27b9c1f06`

02

Proof of Work und Blockvalidierung

Knoten prüfen Vorgänger, Hauptversion, Zeitstempel, Proof of Work, Transaktionen und Miner-Auszahlung. Konkurrierende Zweige werden anhand ihrer kumulierten Schwierigkeit verglichen. RandomX hasht den vorgesehenen Blockdatensatz mit einem aus der Kette abgeleiteten Seed. Der erste Seed ist der Genesis-Hash. Standardepochen umfassen 2.048 Blöcke mit 64 Blöcken Verzögerung.

Höhe	Hauptversion	Geltungsbereich
0	1	Genesis
1	16	RandomX · CLSAG · Bulletproofs+
160	17	6 Blöcke

Die Anpassung nutzt nach 40 Blöcken Verzögerung bis zu 1.920 Einträge. Zeitstempel werden sortiert und bei ausreichender Stichprobe an den Rändern beschnitten. Die Schwierigkeit ist die aufgerundete kumulierte Arbeit mal Sollzeit geteilt durch die verstrichenen Sekunden, mindestens eine Sekunde. Bei höchstens einem Eintrag ergibt sich eins. Die Zeitstempelregel nutzt separat 160 Blöcke und ein Zukunftslimit von zwei Stunden.

Parameter	Wert
RandomX-Epoche / Verzögerung	2.048 / 64 Blöcke
Schwierigkeitsfenster / Verzögerung / Beschnitt	1.920 / 40 / 160 Blöcke
Zeitfenster / Zukunftslimit	160 Blöcke / 2 h

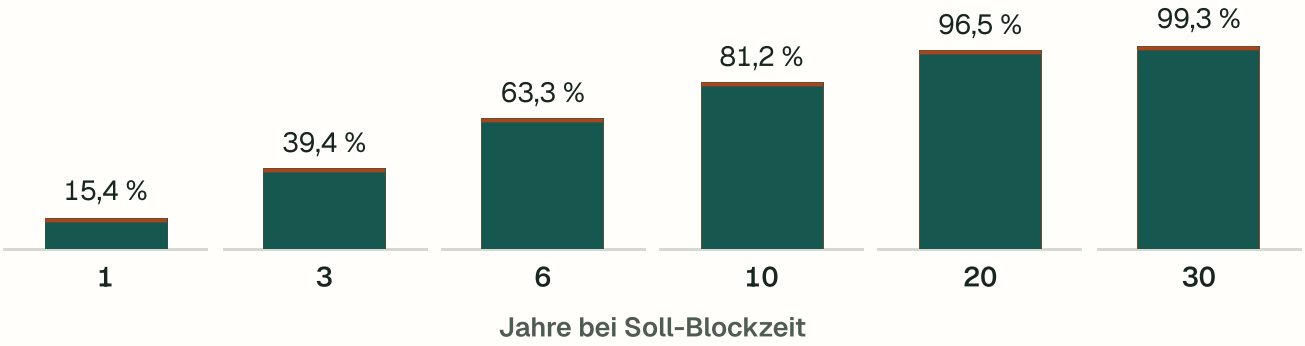
03

Geldmenge und Blocksubvention

Das Limit beträgt 382 Millionen Noticoin mit neun Dezimalstellen. Der Genesis zählt 17,592186044 Noticoin als nicht ausgebbaren Output. Nach Erreichen des Limits bestehen die On-Chain-Einnahmen der Miner aus Transaktionsgebühren.

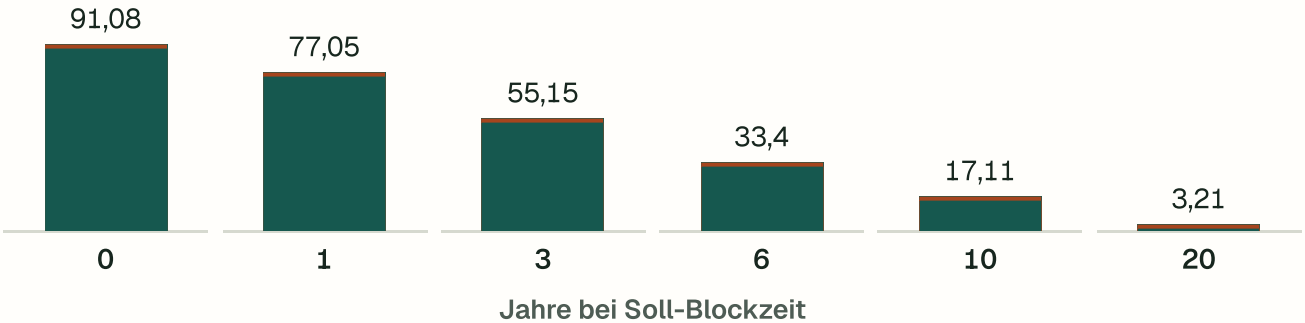
S bezeichnet kumuliert ausgegebene atomare Einheiten einschließlich Genesis. Die ungekürzte Subvention ist am Limit null und sonst ceil((382000000000000000 − S) / 4194304). Der erste Block nach Genesis zahlt bei vollem Gewichtsspielraum 91,075893023 Noticoin vor Gebühren. Zwischen Referenzgewicht und dem Doppelten senkt der Gewichtsabzug die Subvention. Für Gebühren gilt ein separater Mindest-Referenzwert von 0,3 Noticoin.

Kumulierte Emission als Anteil am Limit



Modell mit 45 Sekunden pro Block und 365,25 Tagen pro Jahr. Die volle Subvention wird ohne Gewichtsabzüge und atomare Rundung angenähert.

Modellierte Blocksubvention



Noticoin pro Block vor Gebühren, Gewichtsabzug und atomarer Rundung.

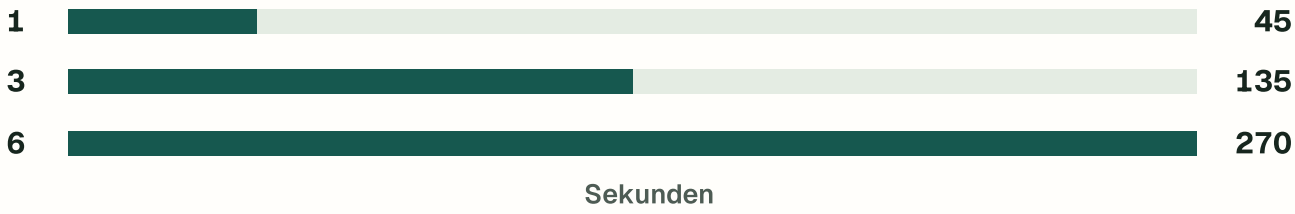
04

Bestätigungen und Verfügbarkeit

Ab Höhe 160 sind reguläre Outputs nach sechs Bestätigungen ausgebbar. Mining-Ausgaben reifen nach 160 Blöcken. Die automatische Notizauslieferung prüft drei Bestätigungen und gültige Schlüsselanteile. Die tatsächliche Wartezeit hängt von Aufnahme, Blockfunden und Reorganisationen ab.

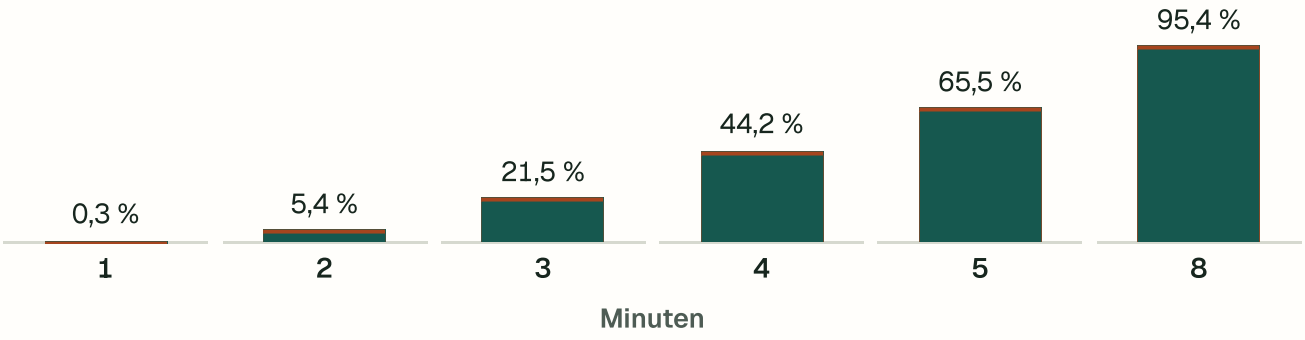
Der aufnehmende Block zählt als erste Bestätigung. Eine Transaktion im Mempool hat null Bestätigungen. Vor Version 17 beträgt das reguläre Konsensalter 27 Blöcke. Die Höhenregel zählt Blöcke. Die Schätzungen setzen die Aufnahme im ersten eintreffenden Block voraus und lassen Staus, Schwierigkeitsänderungen und Reorganisationen außen vor.

Sollzeit nach Bestätigungszahl



Schätzung anhand von 45 Sekunden Soll-Blockzeit.

Modellwahrscheinlichkeit für sechs Blöcke



Das Poisson-Modell setzt unabhängige Funde mit konstantem Mittelwert von 45 Sekunden voraus. Angezeigt wird die Wahrscheinlichkeit für mindestens sechs Blöcke bis zur jeweiligen Zeit.

05

Wallet- und Transaktionsschutz

RingCT verbirgt Beträge, Einmalausgänge verbergen die Empfängeradresse auf der Blockchain. Für verschiedene Kontakte kannst du eigene Subadressen erstellen.

Das Wallet scannt Outputs mit dem privaten View-Key und signiert Ausgaben mit dem Spend-Key. Die Kette speichert Output-Keys, Ringe, Key Images, Commitments und Beweise. Ein regulärer RingCT-Input nutzt einen echten Ringteilnehmer und fünfzehn Decoys. CLSAG belegt die Berechtigung, ein Key Image verhindert Doppelausgaben. Bulletproofs+ prüft Betragsbereiche. Gebühr und Transaktionsgewicht bleiben öffentlich sichtbar.

Eigene Subadressen trennen Empfangskontexte. Sichere die Wiederherstellungsphrase und das lokale Kartenprofil für private Pins oder Käufe separat. Beobachter sehen Zeitpunkt und Aufbau von Transaktionen. Peers und Dienste können Verbindungsmetadaten sehen.

Feld	Geltungsbereich
RingCT	Vertrauliche Betrags-Commitments
CLSAG	Verknüpfbarer Ringnachweis
Bulletproofs+	Beweis für gültige Betragsbereiche
Öffentliche Transaktionsdaten	Gebühr, Gewicht, Struktur und Zeitpunkt

06

Format und Lebenszyklus der Kartenmarkierung

Mit aktivierten Chain-Ankern legt das Wallet einen signierten 118-Byte-Record im tx_extra-Nonce ab. Die Signatur deckt Bytes 0 bis 53 ab. Der Kartendienst prüft sie und drei Bestätigungen vor Veröffentlichung oder Rücknahme. Der öffentliche Record bindet Pin-ID und Autorenschlüssel. Ablaufdatum, Titel, Koordinaten und Chiffretext verwaltet der Kartendienst. Eine kostenlose Veröffentlichung oder Rücknahme sendet eine atomare Einheit zurück ans Autoren-Wallet und kostet die Netzwerkgebühr.

Byte-Offsets	Feld	Wert
0–4	Formatkennung und Version	`4e544d5001`
5	Aktion	1 · Markierung veröffentlichen 2 · Rücknahme
6–21	Pin-UUID ohne Trennzeichen	16 B
22–53	Öffentlicher Ed25519-Autorenschlüssel	32 B
54–117	Ed25519-Signatur	64 B

Öffentliche Notizen nutzen AES-256-GCM und veröffentlichen den Leseschlüssel mit dem Chiffretext. Geteilte Pins bleiben im Sender-Wallet bis zur Verpackung für einen Empfänger per RSA-OAEP und SHA-256. Das Empfänger-Wallet öffnet das Paket lokal. Atlas trennt Kartenkacheln vom Notizspeicher.

07

Betreiberregister und Epochen

Betreiber melden Netz, Ablaufhöhe, Ed25519-Identität, RSA-3072-Schlüssel und HTTPS-Endpunkt in einem signierten Record. Der Knoten ermittelt die Liste aus kanonischen Blöcken bis sechs Blöcke vor der Epochengrenze. Er sortiert nach Gebühr, anschließend aufsteigend nach Signaturidentität, dedupliziert Schlüssel und URLs und benötigt mindestens drei Einträge. Eine strikte Mehrheit genügt für die Auslieferung.

Parameter	Öffentliche Netze	Regtest
Epochenlänge	40	10
Maximale Registrierungsdauer	240	30
Tiefe der Grenze	6	6
Listengrenze vor / ab Höhe 200	3 / 10	3 / 10

Käufe verwenden die Liste des Publikationsblocks. Neue Listen gelten für künftige Publikationen. Für offene Käufe müssen alte Anteile erreichbar bleiben. Die Auswahl belegt Registrierung und Chain-Position. Unabhängigkeit und sichere Schlüsselverwahrung sind Betriebsannahmen. Bei zu wenigen erreichbaren Mitgliedern kann die Auslieferung stocken.

`get_note_operator_roster · NOTI_NOTE_REGISTRY=1`

08

Karteneinträge und Auslieferung

Das Wallet des Autors verschlüsselt die Notiz mit AES-256-GCM, bevor es sie an den Kartenserver sendet.

Der Kartenserver speichert den verschlüsselten Text der Notiz. Die Blockchain hält ihre Veröffentlichung und die Zahlungstransaktion fest.

Für eine bezahlte Auflage legt der Verkäufer Preis und 1 bis 100 Exemplare fest. Je Exemplar entsteht eine eigene Verkäufer-Unteradresse in einem signierten Angebot. Käufer reservieren und bezahlen diese Adresse. Betreiber prüfen Zahlungsnachweis, Bestellbindung und drei Bestätigungen und verschlüsseln die Anteile für den Käufer. Dessen Wallet rekonstruiert den AES-Schlüssel. Bei aktivierter Zustellung kann der Verkäufer offline sein.

Ablauf der bezahlten Notizauslieferung

Signiertes Angebot	Exemplar reservieren	Zahlung prüfen	Schlüsselanteile zustellen	Lokal entschlüsseln

Der Dienst bietet 24 Stunden Abrufzeit ab Verkauf. Eine lokal archivierte lesbare Kopie kann bis zu ihrer Löschung in den Käufen geöffnet werden. Ausverkaufte oder abgelaufene Einträge verschwinden von der öffentlichen Karte. Das System steuert die Zustellung. Leser können geöffneten Inhalt speichern oder weitergeben.

09

Gebühren und Fonds

Veröffentlichungsgebühren gehen an eine Unteradresse des Fonds-Wallets. Die Bridge prüft Knoten- und Wallet-Identität, Höhe und empfangenen Betrag. Die Website zeigt Guthaben, verfügbares Guthaben und Vorgänge ab sechs Bestätigungen aus Snapshots. Transaktions-Hashes führen zum Explorer, Ausgaben können Betrag und Zweck veröffentlichen. Einzelne Zahlungseingänge und Zahleradressen bleiben außerhalb des Berichts. Miner-Gebühren werden separat berechnet.

Gebühren je Aktion

Aktion	Wert	Empfänger
Öffentlicher Pin, 7 Tage, Standardsymbol	Netzwerkgebühr	Miner
Bezahlte Notiz, 7 Tage	0,2 Noticoin	Fonds
Veröffentlichung für 30 Tage	0,6 Noticoin	Fonds
Diamantsymbol	0,1 Noticoin	Fonds
Geheime Notiz	Vom Autor festgelegt	Autor
Markierungen mit Spendenfunktion	Vom Absender gewählt	Autor

Veröffentlichung und Symbol werden gemeinsam an den Fonds bezahlt. Der Sender zahlt die Netzwerkgebühr zusätzlich, die der Miner erhält.

10

Mining und Pool-Abrechnung

Beide Stratum-Modi nutzen RandomX. Gemeinsames Mining verteilt berechtigte Belohnungen nach Arbeit in den letzten 128 Shares. Ein Solo-Block zahlt direkt an den Miner. Die Pool-Hashrate nutzt zehn Minuten akzeptierter Shares. Die Netzwerk-Hashrate wird aus Schwierigkeit und Soll-Blockzeit geschätzt. Einzelwerte erfordern die vollständige Adresse.

Ein Stratum-Job enthält Hashing-Blob, Seed-Hash, Höhe, Share-Ziel und Job-ID. Ein Share erfüllt das Share-Ziel. Ein Blockkandidat erfüllt zusätzlich die Netzwerkschwierigkeit und wird dem Knoten übergeben. Das Ledger bindet die Aufteilung der letzten 128 Shares an den kanonischen Kandidaten. Nach 160 Blöcken Reife wird mit Gebührenabzug ausgezahlt. Solo zahlt der Knoten an die angegebene Miner-Adresse.

Das Dashboard schätzt die Hashrate aus 600 Sekunden angenommener Arbeit, beim Start aus einem kürzeren Zeitfenster. Alle 30 Sekunden erfasst es beide Poolraten und die Netzwerkschwierigkeit und hält bis zu 240 Werte pro Prozess. Ein Neustart löscht die Grafikwerte. Das Ledger bleibt erhalten. Die öffentliche Ansicht zeigt Summen, die Einzelsuche benötigt die volle Adresse.

Parameter	Wert
PPLNS	128
Hashrate-Fenster	600 s
Grafikintervall und maximale Messwerte	30 s · 240
Reife der Belohnung	160 Blöcke

11

Verifikation und Freigabekriterien

Die protokollierten Entwicklungsläufe verwenden echte Binaries und isolierte Daten. Regtest mit fester Schwierigkeit reproduziert Zahlungs- und Abrechnungsabläufe. Der öffentliche Betrieb erfordert zusätzlich unabhängige Peers, dauerhaftes Mining und Wiederanlauf nach Netzunterbrechungen.

Prüfung	Erfasste Abdeckung
Konsens und Netzwerkidentität	Genesis und erster RandomX-Block aller drei Netze in isolierten Läufen
Bestätigungen und Verfügbarkeit	Relay, Peer-Sichtbarkeit und Ausgabe nach sechs Bestätigungen nach Aktivierung
Format und Lebenszyklus der Kartenmarkierung	Rücknahme durch den Autor, bezahlte Zustellung und Auflage, direkte Spende und Fondseingang
Mining und Pool-Abrechnung	Akzeptierte Shared- und Solo-Blöcke, Ledger-Neustart und bestätigte Auszahlung

`verify-first-blocks.mjs` · `verify-economy.mjs` · `verify-note-registry.mjs` · `verify-offline-release.mjs` · `pool/tests/integration.mjs`

Startvorbereitung

12

Implementierung und Betriebsanleitungen

Das Windows-CLI-Paket enthält START-NODE.cmd. Starte den Knoten, prüfe die Netzwerkidentität und warte vor der Kontostandsprüfung auf die Synchronisierung. Binde Verwaltungs-RPC an eine vertrauenswürdige Schnittstelle. Nutze getrennte Daten und Wallet-Dateien je Netz. Prüfe die Paket-Prüfsumme und sichere die Wiederherstellungsphrase separat.

Im Betrieb wird für jede Zahlungskomponente das erwartete Netz eingestellt und der Hash bei Höhe null verglichen. Authentifiziertes Wallet RPC bleibt auf Loopback. Nur die begrenzte Bridge ist bei Bedarf über HTTPS erreichbar. Empfangs-Wallet und Rechnungsdaten werden zusammen gesichert. Betreiberschlüssel werden geschützt und benötigte Anteile bleiben erreichbar. Test- und Produktivdaten liegen getrennt.

Komponente	Betriebsschnittstellen
Daemon RPC	Chain-Identität, Höhe und Blockvorlagen `get_info, get_block_header_by_height, get_block_template`
Wallet RPC	Guthaben, Adresse und Zahlungsnachweis `get_balance, get_address, check_tx_proof`
Betreiberregister und Epochen	Epochenliste mit Signaturidentitäten und Auslieferungsschlüsseln `get_note_operator_roster`
Bridge	Begrenzte Zahlungsprüfung und Zuteilung von Unteradressen
Pool HTTP	Gesamtstatistik und POST-Adressabfrage `GET /api/stats · POST /api/miner`

- Netzwerkmanifest (/assets/noticoin-network.json)
- Desktop-Wallet-Anleitung (/de/guide.html) · Einen Knoten starten (/de/guide-node.html) · CLI und Wallet RPC (/de/guide-cli.html)
- Karte und Markierungen (/de/map.html) · Zahlungen (/de/payments.html) · Datenschutz bei Noticoin (/de/privacy.html)
- Mining und Pool (/de/mining.html) · Fondsbericht (/de/fund.html)