Livre blanc

Protocole Noticoin, émission, confidentialité du portefeuille, notes sur la carte et minage.

Spécification technique · 1.0.0

Noticoin est un réseau à preuve de travail RandomX, à offre plafonnée, avec une carte intégrée au portefeuille. Cette spécification décrit le consensus, la confidentialité des transactions, la publication des repères, la remise des notes payantes, le registre des opérateurs, la comptabilité du fonds et le pool. Les tableaux distinguent les paramètres du consensus des réglages applicatifs. Les graphiques présentent des modèles et leurs hypothèses.

01 Consensus et identité réseau

02 Preuve de travail et validation des blocs

03 Offre et subvention des blocs

04 Confirmations et disponibilité

05 Confidentialité du portefeuille

06 Format et cycle de vie des repères

07 Registre et époques des opérateurs

08 Enregistrements et remise des notes

09 Frais et fonds

10 Minage et comptabilité du pool

11 Vérifications et critères de lancement

12 Implémentation et guides

01

Consensus et identité réseau

Noticoin dérive de Monero v0.18.5.4. Il vise des blocs de 45 secondes et vérifie RandomX dès le bloc 1, en version 16. La version 17 s'active au bloc 160. Le P2P vérifie les identifiants réseau. Chaque réseau a son genesis, ses ports et ses préfixes d'adresse.

Un nœud neuf tire l'identité réseau de sa configuration et du genesis. La poignée de main P2P sur Levin vérifie l'identifiant de 16 octets. Les préfixes distinguent adresses standard, intégrées et sous-adresses. Comparez le bloc à la hauteur zéro au manifeste avant de vérifier des paiements. Le regtest utilise des données isolées et exige une activation explicite dans les services de paiement.

Réseau	P2P	RPC	ZMQ	Préfixes d'adresse
mainnet	19080	19081	19082	111 / 112 / 113
testnet	29080	29081	29082	114 / 115 / 116
stagenet	39080	39081	39082	117 / 118 / 119

Standard / intégrée / sous-adresse

Mainnet

Hachage genesis

`2784467d7c909874668b9f0accf533c63f77aad79a3b72bfc5b23ca09e3cb614`

Identifiant réseau P2P

`305639f9810544e48197a8f69a0a6d19`

Testnet

Hachage genesis

`e2c8d4803df588a35e8289d2f939f3521ec92c43d4e8e453d05585917c205a90`

Identifiant réseau P2P

`3946c278a80142618044dfa92619e1e7`

Stagenet

Hachage genesis

`090c1b22ef96a0d7e05d7ec6321ad3f61d4f36c90cce2ce573e3c4be19f8daef`

Identifiant réseau P2P

`0205f90fad5c4d41a8ad3bf27b9c1f06`

02

Preuve de travail et validation des blocs

Les nœuds vérifient le parent, la version majeure, les horodatages, la preuve de travail, les transactions et la récompense. Ils comparent les branches selon leur difficulté cumulée. RandomX hache le bloc de données dédié avec une graine dérivée de la chaîne. La première graine est le hachage genesis. Par défaut, chaque époque couvre 2 048 blocs avec un décalage de 64 blocs.

Hauteur	Version majeure	Portée
0	1	Genesis
1	16	RandomX · CLSAG · Bulletproofs+
160	17	6 Blocs

Le réglage exploite l'historique disponible, limité à 1 920 entrées après un décalage de 40 blocs. Il trie les horodatages et retire les extrêmes quand l'échantillon le permet. La difficulté arrondit au supérieur le travail cumulé multiplié par la cible et divisé par un intervalle minimal d'une seconde. Avec au plus une entrée, elle vaut un. La règle d'horodatage utilise 160 blocs et limite l'avance à deux heures.

Paramètre	Valeur
Époque / décalage RandomX	2048 / 64 Blocs
Fenêtre / décalage / retrait de difficulté	1 920 / 40 / 160 Blocs
Fenêtre d'horodatage / avance maximale	160 Blocs / 2 h

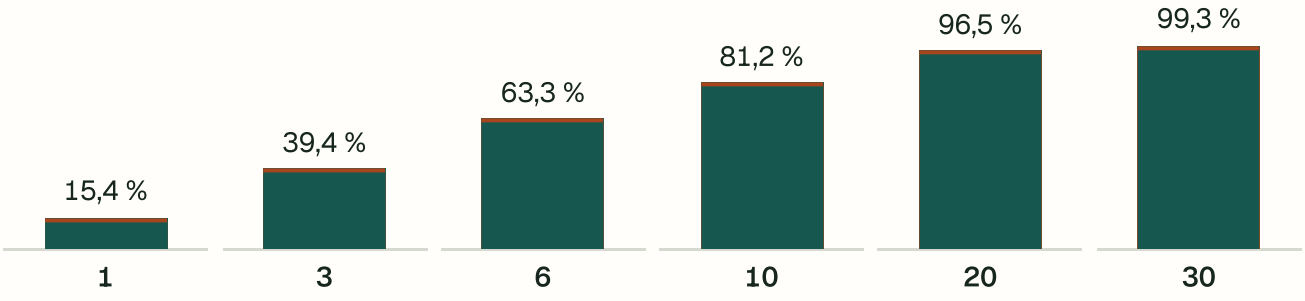
03

Offre et subvention des blocs

Le plafond est de 382 millions de Noticoin avec neuf décimales. Le genesis comptabilise 17,592186044 Noticoin dans une sortie inutilisable. Au plafond, les frais de transaction constituent la rémunération sur chaîne des mineurs.

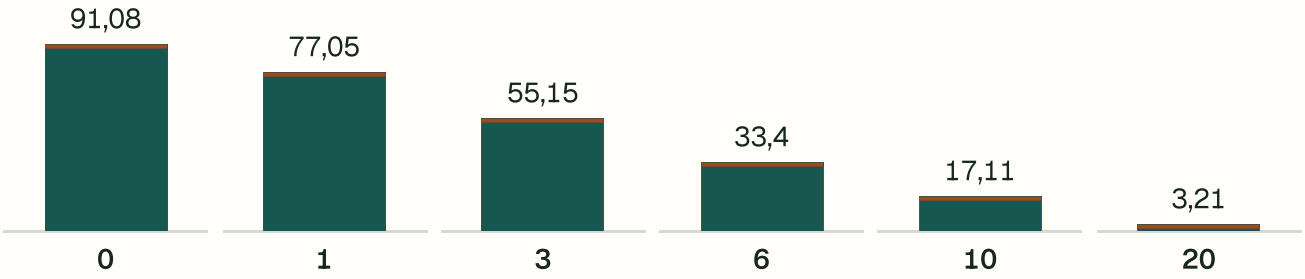
Soit S le total émis en unités atomiques, genesis compris. La subvention sans pénalité vaut zéro au plafond, sinon ceil((3820000000000000000 − S) / 4194304). Le premier bloc après le genesis rapporte 91,075893023 Noticoin avant frais à poids admissible. Entre le poids de référence et son double, la pénalité réduit la subvention. Le calcul des frais utilise une référence minimale distincte de 0,3 Noticoin.

Émission cumulée en part du plafond



Modèle indicatif à 45 secondes par bloc et 365,25 jours par an. Il approxime la subvention entière avant pénalités de poids et arrondi atomique.

Subvention modélisée par bloc



En Noticoin par bloc avant frais, pénalités de poids et arrondi atomique.

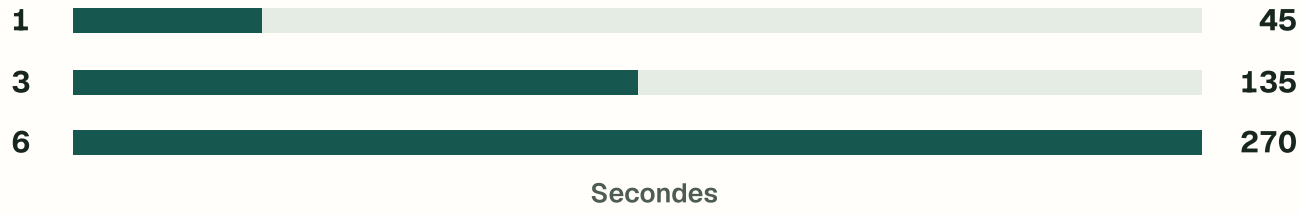
04

Confirmations et disponibilité

Dès la hauteur 160, les sorties ordinaires deviennent dépensables après six confirmations. Les sorties minées mûrissent après 160 blocs. La remise de notes vérifie trois confirmations et les parts de clé. L'attente varie selon l'inclusion, la découverte des blocs et les réorganisations.

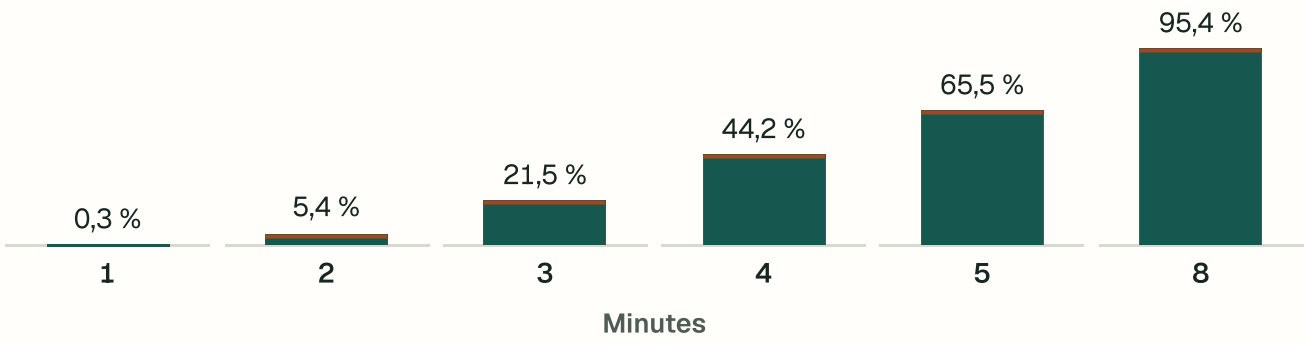
Le bloc d'inclusion vaut première confirmation. Une transaction en mempool a zéro confirmation. Avant la version 17, l'âge de consensus des sorties ordinaires est de 27 blocs. La règle mesure une hauteur, donc des blocs. Les estimations supposent une inclusion au premier bloc et ignorent congestion, changements de difficulté et réorganisations.

Temps cible selon les confirmations



Estimations fondées sur la cible de 45 secondes par bloc.

Probabilité modélisée de six blocs



Le modèle de Poisson suppose des découvertes indépendantes avec une moyenne stable de 45 secondes. Il donne la probabilité d'au moins six blocs avant le temps indiqué.

05

Confidentialité du portefeuille

RingCT masque les montants et les sorties à usage unique masquent l'adresse du destinataire sur la blockchain. Vous pouvez créer des sous-adresses pour différents contacts.

Le portefeuille analyse les sorties avec sa clé privée de vue et signe avec le matériel de dépense. La chaîne enregistre clés de sortie, anneaux, images de clé, engagements et preuves. Un anneau RingCT ordinaire comprend un membre réel et quinze leurres. CLSAG prouve l'autorisation, et l'image de clé empêche la double dépense. Bulletproofs+ vérifie la plage des montants. Les frais et le poids restent publics.

Utilisez des sous-adresses pour séparer les contextes de réception. Sauvegardez la phrase de récupération ainsi que le profil local nécessaire aux repères privés et achats. Les observateurs voient les horaires et la structure des transactions. Les pairs et services peuvent voir certaines métadonnées de connexion.

Champ	Portée
RingCT	Engagements sur les montants confidentiels
CLSAG	Autorisation d'anneau avec liaison
Bulletproofs+	Preuve que les montants sont dans la plage
Données publiques de transaction	Frais, poids, structure et horaire

06

Format et cycle de vie des repères

Avec l'ancrage activé, le portefeuille place un enregistrement signé de 118 octets dans un nonce tx_extra. La signature couvre les octets 0 à 53. La carte vérifie la signature et trois confirmations avant publication ou retrait. Le registre ancre l'identifiant du repère et la clé auteur. Le service gère l'expiration, le titre, les coordonnées et le texte chiffré. La publication gratuite ou le retrait renvoie une unité atomique au portefeuille auteur et paie les frais réseau.

Offsets en octets	Champ	Valeur
0–4	Signature de format et version	`4e544d5001`
5	Action	1 · Publier un repère 2 · Retrait
6–21	UUID du repère sans séparateurs	16 B
22–53	Clé publique Ed25519 de l'auteur	32 B
54–117	Signature Ed25519	64 B

Les notes publiques utilisent AES-256-GCM avec une clé de lecture publiée avec le chiffré. Un repère partagé reste dans le portefeuille avant d'être empaqueté pour un destinataire avec RSA-OAEP et SHA-256. Son portefeuille ouvre le paquet en local. L'Atlas sépare les tuiles des notes. Un nouveau repère laisse les tuiles intactes.

07

Registre et époques des opérateurs

Les opérateurs annoncent réseau, hauteur d’expiration, identité Ed25519, clé de chiffrement RSA-3072 et point d’accès HTTPS dans un enregistrement signé. Le nœud calcule la liste à partir des blocs canoniques jusqu’à six blocs avant la frontière. Il classe les inscriptions par frais puis par identité croissante, déduplique clés et URL et exige au moins trois entrées. La remise exige une majorité stricte.

Paramètre	Réseaux publics	Regtest
Durée de l’époque	40	10
Durée maximale d’inscription	240	30
Profondeur de la limite	6	6
Limite avant / à partir de la hauteur 200	3 / 10	3 / 10

Un achat utilise la liste du bloc de publication. La nouvelle liste s’applique aux publications suivantes. Les anciennes parts doivent rester disponibles pour les achats en cours. La sélection établit l’inscription et sa position sur la chaîne. L’indépendance des opérateurs et la protection des clés restent des conditions d’exploitation. Un quorum indisponible peut bloquer la remise.

`get_note_operator_roster · NOTI_NOTE_REGISTRY=1`

08

Enregistrements et remise des notes

Le portefeuille de l'auteur chiffre la note avec AES-256-GCM avant de l'envoyer au serveur de carte.

Le serveur de carte conserve le texte chiffré de la note. La blockchain enregistre sa publication et la transaction de paiement.

Pour une édition payante, l'auteur fixe le prix et un tirage de 1 à 100. Le portefeuille crée une sous-adresse du vendeur par copie et publie une offre signée. L'acheteur réserve puis paie cette adresse. Les opérateurs vérifient preuve, commande et trois confirmations avant de chiffrer les parts pour l'acheteur. Le portefeuille de ce dernier reconstruit la clé AES. Avec cette remise, le vendeur peut être hors ligne après publication.

Séquence de remise d'une note payante

Offre signée	Réserver une copie	Vérifier le paiement	Remettre les parts	Déchiffrer en local

Le service propose une fenêtre de récupération de 24 heures après la vente. Une copie lisible archivée localement peut être rouverte jusqu'à sa suppression. Un repère épuisé ou expiré disparaît de la carte publique. Le système contrôle la remise. Un lecteur peut enregistrer ou partager le texte après ouverture.

09

Frais et fonds

Les frais de publication vont à une sous-adresse du portefeuille du fonds. Le pont vérifie l'identité du nœud et du portefeuille, la hauteur et le montant reçu. Le site présente soldes et historique à six confirmations. Les relevés relient les hachages à l'explorateur et peuvent publier montants et motifs des dépenses. Les montants entrants individuels et adresses des payeurs restent hors du rapport. Les frais des mineurs sont calculés séparément.

Frais par action

Action	Valeur	Destinataire
Repère public, 7 jours, icône standard	Frais réseau	Mineur
Annonce payante, 7 jours	0,2 Noticoin	Fonds
Publication pendant 30 jours	0,6 Noticoin	Fonds
Icône diamant	0,1 Noticoin	Fonds
Note secrète	Fixé par l'auteur	Auteur
Repères avec dons	Choisi par l'expéditeur	Auteur

La publication et l'icône font l'objet d'un seul paiement au fonds. L'expéditeur paie les frais réseau en supplément, et le mineur les reçoit.

10

Minage et comptabilité du pool

Les deux modes Stratum utilisent RandomX. En commun, la récompense est répartie au prorata du travail des 128 dernières parts. En solo, le bloc paie son mineur. Le hashrate du pool utilise dix minutes de parts acceptées. L'estimation réseau divise la difficulté par le temps de bloc cible. Les statistiques individuelles exigent l'adresse complète.

Une tâche Stratum contient les données à hacher, la graine, la hauteur, la cible de share et son identifiant. Un share satisfait sa cible. Un candidat bloc satisfait aussi la difficulté réseau et part au nœud. Le registre partagé conserve la répartition des 128 dernières parts liée au candidat canonique. Le paiement intervient après 160 blocs de maturité et déduit ses frais. En solo, le nœud construit la récompense pour l'adresse du mineur.

Le tableau de bord utilise le travail accepté sur 600 secondes, avec une période plus courte au démarrage. Il échantillonne les estimations et la difficulté toutes les 30 secondes et garde jusqu'à 240 points par processus. Un redémarrage efface ces points. Le registre des parts et paiements est persistant. Le tableau expose des agrégats et la recherche individuelle exige l'adresse entière.

Paramètre	Valeur
PPLNS	128
Fenêtre de hashrate	600 s
Intervalle et maximum du graphique	30 s · 240
Maturité de la récompense	160 Blocs

11

Vérifications et critères de lancement

Les essais de développement utilisent les binaires réels avec des données isolées. Le regtest à difficulté fixe reproduit les transitions de paiement et de comptabilité. Le déploiement public ajoute des contrôles avec des pairs indépendants, un taux de hachage durable et la reprise après interruption.

Vérification	Couverture enregistrée
Consensus et identité réseau	Genesis et premier bloc RandomX des trois réseaux en essais isolés
Confirmations et disponibilité	Relais, visibilité par le pair et dépense après six confirmations après activation
Format et cycle de vie des repères	Retrait par l'auteur, remise payante et quotas, don direct et reçu du fonds
Minage et comptabilité du pool	Blocs Shared et Solo acceptés, redémarrage du registre et versement confirmé

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

Préparation du lancement

12

Implémentation et guides

Le pack CLI Windows inclut START-NODE.cmd. Lancez le nœud, vérifiez l'identité réseau et attendez la synchronisation avant de contrôler le solde. Réservez le RPC administratif à une interface de confiance. Séparez les données et portefeuilles de chaque réseau. Vérifiez la somme de contrôle et conservez la phrase de récupération à part.

En public, configurez le réseau attendu par composant de paiement et vérifiez le hachage de hauteur zéro. Gardez le RPC du portefeuille authentifié sur loopback. Exposez en HTTPS uniquement le pont limité où la carte en a besoin. Sauvegardez le portefeuille de réception et la base de facturation ensemble. Protégez les clés et gardez accessibles les parts encore nécessaires. Séparez les données de test et les données publiques.

Composant	Interfaces d'exploitation
Daemon RPC	Identité de chaîne, hauteur et modèles de bloc `get_info, get_block_header_by_height, get_block_template`
Wallet RPC	Solde, adresse et preuve de transfert `get_balance, get_address, check_tx_proof`
Registre et époques des opérateurs	Liste d'époque avec identités et clés de remise `get_note_operator_roster`
Bridge	Contrôle limité des paiements et attribution de sous-adresses
Pool HTTP	Statistiques agrégées et recherche POST par adresse `GET /api/stats · POST /api/miner`

- Manifeste réseau (/assets/noticoin-network.json)
- Guide du portefeuille de bureau (/fr/guide.html) · Lancer un nœud (/fr/guide-node.html) · CLI et Wallet RPC (/fr/guide-cli.html)
- Carte et repères (/fr/map.html) · Paiements (/fr/payments.html) · Confidentialité dans Noticoin (/fr/privacy.html)
- Minage et pool (/fr/mining.html) · Rapport du fonds (/fr/fund.html)