ホワイトペーパー

Noticoin のプロトコル、発行、ウォレットのプライバシー、地図のノートと採掘。

技術仕様 · 1.0.0

Noticoin は RandomX のプルーフ・オブ・ワークと供給上限を備え、ウォレットに地図を統合したネットワークです。本仕様書は、コンセンサス、取引のプライバシー、ピンの公開形式、有料ノートの配信、オペレーター登録簿、基金の会計、マイニングプールを解説します。表ではコンセンサスとアプリの設定を区別します。時間と発行量の図にはモデルの前提を示します。

01 コンセンサスとネットワーク ID

02 プルーフ・オブ・ワークとブロック検証

03 供給量とブロック補助金

04 承認と使用可能条件

05 ウォレットと取引のプライバシー

06 地図レコードの形式とライフサイクル

07 オペレーター登録簿と更新期間

08 地図の記録とノート配信

09 手数料と基金

10 採掘とプールの精算

11 検証と公開条件

12 実装と運用ガイド

01

コンセンサスとネットワーク ID

Noticoin は Monero v0.18.5.4 を基にします。目標ブロック間隔は 45 秒で、ブロック 1 からバージョン 16 の RandomX を検証します。バージョン 17 は高さ 160 で有効になります。P2P ハンドシェイクがネットワーク ID を検証し、各ネットワークは固有のジェネシス、ポート、アドレス接頭辞を持ちます。

新規ノードは設定とジェネシスからネットワークを識別します。Levin のハンドシェイクは 16 バイトのネットワーク ID を照合します。アドレス接頭辞は標準アドレス、統合アドレス、サブアドレスを区別します。支払いの検証に使う前に、高さゼロのブロックを定義と照合できます。regtest のデータは隔離し、支払いサービスでは明示的に有効化します。

ネットワーク	P2P	RPC	ZMQ	アドレス接頭辞
mainnet	19080	19081	19082	111 / 112 / 113
testnet	29080	29081	29082	114 / 115 / 116
stagenet	39080	39081	39082	117 / 118 / 119

標準 / 統合 / サブアドレス

Mainnet

ジェネシスハッシュ

`2784467d7c909874668b9f0accf533c63f77aad79a3b72bfc5b23ca09e3cb614`

P2P ネットワーク ID

`305639f9810544e48197a8f69a0a6d19`

Testnet

ジェネシスハッシュ

`e2c8d4803df588a35e8289d2f939f3521ec92c43d4e8e453d05585917c205a90`

P2P ネットワーク ID

`3946c278a80142618044dfa92619e1e7`

Stagenet

ジェネシスハッシュ

`090c1b22ef96a0d7e05d7ec6321ad3f61d4f36c90cce2ce573e3c4be19f8daef`

P2P ネットワーク ID

`0205f90fad5c4d41a8ad3bf27b9c1f06`

02

プルーフ・オブ・ワークとブロック検証

ノードは親ブロック、メジャーバージョン、時刻、作業量証明、取引、採掘者報酬を検証します。競合する分岐は累積難易度で比較します。RandomX はチェーン由来のシードでブロックのハッシュ入力を処理します。初期シードはジェネシスハッシュです。既定のシード期間は 2,048 ブロックで、64 ブロックの遅延があります。

高さ	メジャーバージョン	適用先
0	1	Genesis
1	16	RandomX · CLSAG · Bulletproofs+
160	17	6 ブロック

難易度調整では 40 ブロック遅らせた履歴を最大 1,920 件使います。タイムスタンプを整列し、十分な件数があれば両端を切り詰めます。対象区間の累積作業量に目標間隔を掛け、経過秒数で割って切り上げます。経過秒数の下限は 1 で、履歴が 1 件以下なら難易度は 1 です。ブロック時刻の検証には別途 160 ブロックの窓と 2 時間の未来上限があります。

パラメーター	値
RandomX の期間 / 遅延	2,048 / 64 ブロック
難易度の窓 / 遅延 / 切り詰め	1,920 / 40 / 160 ブロック
時刻の窓 / 未来時刻の上限	160 ブロック / 2 h

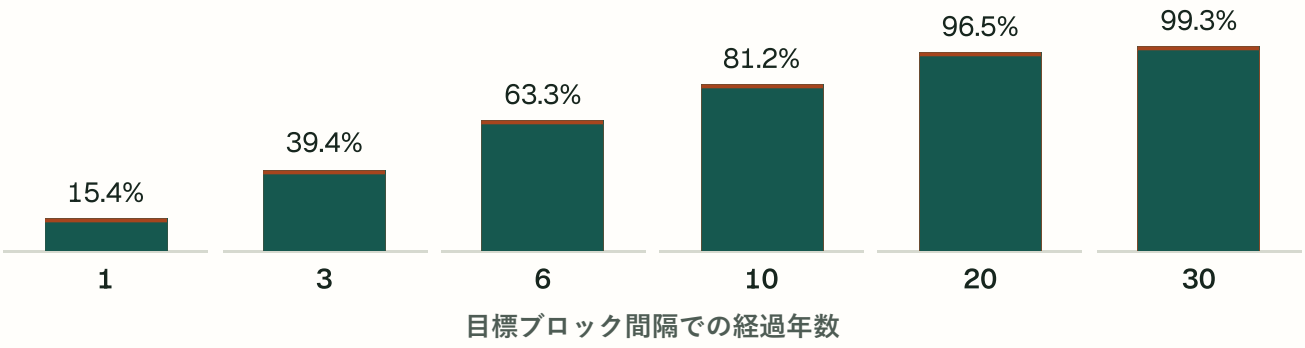
03

供給量とブロック補助金

供給上限は 3 億 8,200 万 Noticoin で、小数点以下 9 桁です。ジェネシスの 17.592186044 Noticoin は使用不能な出力です。上限到達後、採掘者へのオンチェーンの報酬は取引手数料です。

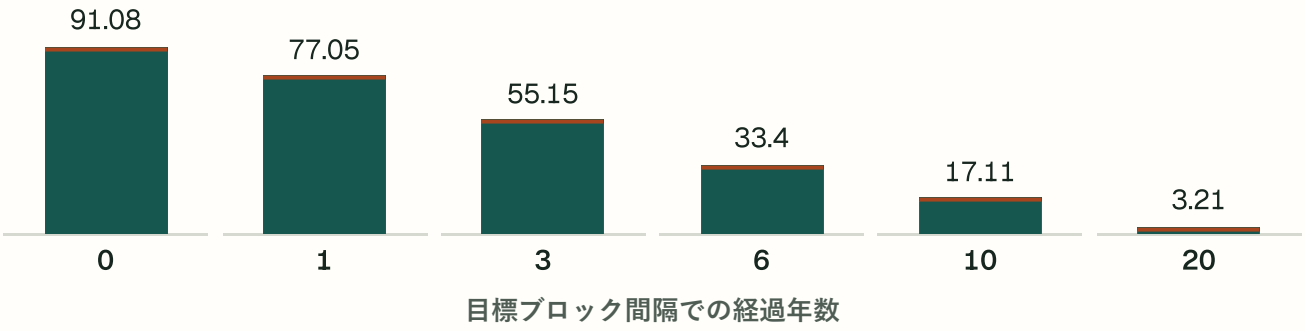
S はジェネシス出力を含む累計発行最小単位です。補助金は上限でゼロとなり、それ以前は ceil((3820000000000000000 − S) / 4194304) です。ジェネシスの次のブロックの通常補助金は手数料を除き 91.075893023 Noticoin です。有効基準重量とその 2 倍の間で補助金が減額されます。手数料計算には発行と独立した 0.3 Noticoin の下限基準があります。

発行上限に対する累積発行割合



1 ブロック 45 秒、年 365.25 日とした目安です。ブロック重量の減額と最小単位の丸めを省略した近似値です。

時間経過に伴うブロック補助金のモデル



単位はブロックあたりの Noticoin で、取引手数料、重量による減額、最小単位の丸めを除きます。

04

承認と使用可能条件

高さ 160 以降、通常の出力は 6 承認で使用できます。採掘報酬は 160 ブロックで成熟します。ノートの自動配信は 3 承認と有効な鍵の分割片を検証します。待ち時間は取引の収録、ブロック発見、チェーンの再編成で変動します。

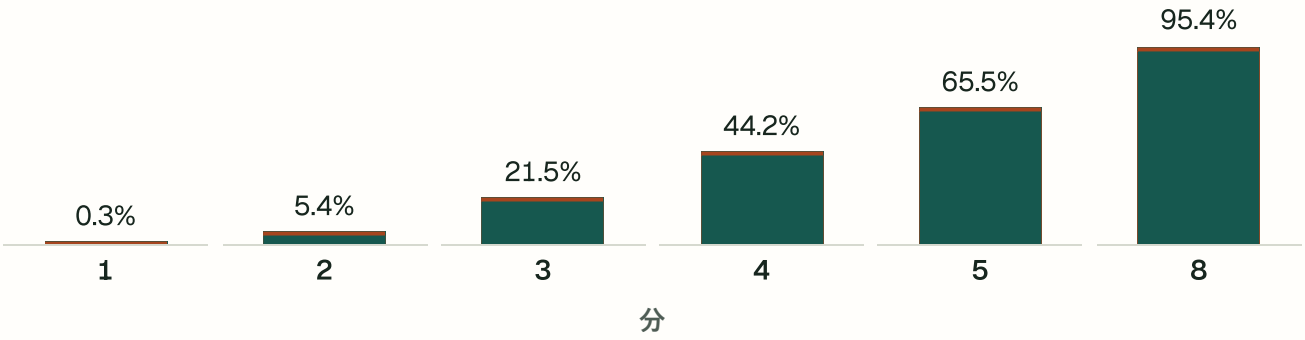
取引を含むブロックが 1 承認目です。メモリプール内は 0 承認です。バージョン 17 より前の通常出力の年齢条件は 27 ブロックでした。高さ規則はブロック数で計算します。この推定は最初に到着するブロックへの収録を仮定し、混雑、難易度変化、再編成を含みません。

承認数ごとの目標時間



目標ブロック間隔の 45 秒に基づく目安です。

6 ブロック到着の確率モデル



ポアソン到着モデルでは発見が独立し、平均が 45 秒で一定と仮定します。横軸の時刻までに 6 ブロック以上到着する確率を示します。

05

ウォレットと取引のプライバシー

RingCT が金額を秘匿し、ワンタイム出力がブロックチェーン上の受取先アドレスを隠します。相手ごとにサブアドレスを作成できます。

ウォレットは秘密ビューキーで出力を検出し、スペンドキーで支出に署名します。チェーンには出力鍵、入力リング、キーイメージ、コミットメント、証明が記録されます。通常の RingCT 入力のリングは実入力 1 件とデコイ 15 件からなります。CLSAG は署名権限を証明し、キーイメージは二重支出を防ぎます。Bulletproofs+ は金額の範囲を検証します。手数料と取引重量は公開されます。

受取用途を分ける場合はサブアドレスを使います。復元フレーズと、非公開ピン・購入に必要なローカル地図プロファイルは別々に保管します。チェーンの観測者は取引の時刻と構造を確認できます。ピアやサービスが接続メタデータの一部を把握する場合があります。

フィールド	適用先
RingCT	秘匿額のコミットメント
CLSAG	連結可能なリングによる承認
Bulletproofs+	金額が範囲内にあることの証明
公開取引データ	手数料、重量、構造、時刻

06

地図レコードの形式とライフサイクル

チェーンへの記録を有効にすると、ウォレットは署名済みの 118 バイトを tx_extra の nonce に格納します。署名対象は 0 から 53 バイトです。地図は公開や取り下げを適用する前に署名と 3 承認を検証します。公開レコードはピン ID と作成者の鍵を記録します。期限、タイトル、座標、暗号文は地図サービスが管理します。無料公開や取り下げでは自分のウォレットへ最小単位を送金し、ネットワーク手数料を負担します。

バイト位置	フィールド	値
0–4	マジックとバージョン	4e544d5001
5	操作	1 · ピンを公開する 2 · 取り下げ
6–21	区切りなしのピン UUID	16 B
22–53	作成者の Ed25519 公開鍵	32 B
54–117	Ed25519 署名	64 B

公開ノートでは AES-256-GCM を使い、暗号文と読み取り鍵を公開します。共有ピンは受取人向けに SHA-256 を使う RSA-OAEP で包むまで送信者のウォレットに保存します。受取側はローカルで開きます。Atlas は地図タイルとノートを別に扱います。

07

オペレーター登録簿と更新期間

オペレーターは署名済み取引にネットワーク、有効期限の高さ、Ed25519 ID、RSA-3072 暗号鍵、HTTPS エンドポイントを記録します。ノードは期間境界の 6 ブロック前までの正規チェーンから名簿を求めます。手数料順、同額なら署名 ID の昇順です。暗号鍵と URL の重複を排除します。名簿には 3 件以上が必要で、配信には過半数を使います。

パラメーター	公開ネットワーク	Regtest
更新期間	40	10
登録の最大有効期間	240	30
名簿の基準深さ	6	6
高さ 200 前 / 以降の名簿上限	3 / 10	3 / 10

購入には掲載ブロック時の名簿を使い、新しい名簿は今後の掲載に適用します。処理中の購入には古い分割片が必要です。選出は登録とチェーン上の位置を証明します。運営者の独立性と鍵管理は別の運用上の前提です。元の運営者が十分に応答しないと配信が滞ることがあります。

`get_note_operator_roster · NOTI_NOTE_REGISTRY=1`

08

地図の記録とノート配信

作成者のウォレットは、メモを AES-256-GCM で暗号化してから地図サーバーに送信します。

地図サーバーは暗号化されたメモの本文を保存します。ブロックチェーンにはメモの公開と支払い取引が記録されます。

有料版の価格と 1 〜 100 部の上限は販売者が設定します。ウォレットは各部に固有の販売者サブアドレスを作り、署名済みの販売条件を公開します。購入者が予約して指定先へ支払うと、オペレーターは支払い証明、注文との対応、3 承認を照合し、購入者向けに暗号化した分割片を返します。購入側が AES 鍵を復元します。配信機能が有効なら販売側は公開後にオフラインにできます。

有料ノートの配信手順

署名済みの販売条件	1 部を予約	支払いを検証	鍵の分割片を配信	端末で復号

販売後は 24 時間の取得期間があります。読めるコピーを端末に保存すると、削除するまで購入済みノートから開けます。売り切れや期限切れの掲載は公開地図から消えます。システムは配信手順を管理します。開封した読者は内容を保存または共有できます。

09

手数料と基金

掲載料は専用基金ウォレットのサブアドレスで受け取ります。ブリッジがデーモンとウォレットの識別情報、高さ、受取額を確認します。サイトはスナップショットから残高、使用可能額、6 承認以降の履歴を表示します。取引ハッシュをエクスプローラーへつなぎ、支出額や用途も掲載できます。個別の入金額や送信者アドレスは基金レポートの対象外です。採掘者へのネットワーク手数料は別に計算します。

操作別の料金

操作	値	受取先
公開ピン、7 日、標準アイコン	ネットワーク手数料	採掘者
有料ノート、7 日	0.2 Noticoin	基金
30 日間の掲載	0.6 Noticoin	基金
ダイヤモンドアイコン	0.1 Noticoin	基金
秘密のメモ	作成者が設定	作成者
寄付を受け付けるピン	送信者が設定	作成者

掲載料とアイコン料金をまとめて基金に支払います。送信者が別途負担するネットワーク手数料はマイナーが受け取ります。

10

採掘とプールの精算

両 Stratum モードは RandomX を使います。共同採掘では直近 128 シェアの作業量に応じて報酬を配分し、ソロ報酬は採掘者が直接受け取ります。プールのハッシュレートは直近 10 分の承認済みシェアから推定します。ネットワークの値は難易度を目標ブロック間隔で割って推定します。個人統計の取得には完全なアドレスが必要です。

Stratum ジョブにはハッシュ用データ、シードハッシュ、高さ、シェア目標、ジョブ ID が含まれます。シェアはシェア目標を満たします。ブロック候補はネットワーク難易度も満たし、デーモンへ送られます。共同採掘の台帳は正規ブロック候補に結びつく直近 128 シェアの配分を保存します。160 ブロック後に報酬が成熟すると、手数料を差し引いて支払います。ソロでは提出者のアドレス宛に採掘取引を作ります。

ダッシュボードは直近 600 秒の承認済み作業量を使い、起動直後は対象時間が短くなります。30 秒ごとに両方式の推定とネットワーク難易度を計測し、プロセス内に最大 240 件を保持します。再起動するとグラフの計測値が消えます。台帳は別に永続化します。公開画面は集計を表示し、個別照会には完全なアドレスが必要です。

パラメーター	値
PPLNS	128
ハッシュレート集計時間	600 s
グラフの計測間隔と最大件数	30 s · 240
報酬の成熟期間	160 ブロック

11

検証と公開条件

記録された開発試験では実際のデーモンとウォレットを隔離データで動かしました。固定難易度の regtest で取引や会計状態の変化を再現できます。公開時は独立したピア、持続的な採掘、ネットワーク中断からの復旧も確認します。

確認項目	記録済みの検証範囲
コンセンサスとネットワーク ID	3 ネットワークのジェネシスと最初の RandomX ブロックを隔離環境で確認
承認と使用可能条件	有効化後の送金中継、ピアでの可視性、6 承認での使用
地図レコードの形式とライフサイクル	作成者による撤下、有料配信と部数制限、直接寄付と基金への入金
採掘とプールの精算	Shared・Solo のブロック受理、台帳の再起動、支払い確認

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

公開準備

12

実装と運用ガイド

Windows CLI パッケージには START-NODE.cmd が含まれます。ノードを起動し、チェーンの識別情報を確かめ、同期後に残高を確認します。管理用 RPC は信頼できるインターフェースに限定します。ネットワークごとにデータとウォレットファイルを分けます。配布物のチェックサムを確認し、復元フレーズはウォレットファイルと別に保管します。

公開時は各支払いコンポーネントに対象ネットワークを設定し、高さゼロのハッシュを照合します。ウォレット RPC は認証付きでループバックに置きます。地図に必要な場合だけ、範囲を絞ったブリッジを HTTPS で公開します。受取用ウォレットと請求データを一緒に保管します。運営者の鍵を守り、未処理の取得期間が終わるまで元の分割片を利用可能にします。試験と公開サービスのデータを分離します。

コンポーネント	運用インターフェース
Daemon RPC	チェーン ID、高さ、採掘テンプレート `get_info`, `get_block_header_by_height`, `get_block_template`
Wallet RPC	残高、アドレス、支払い証明 `get_balance`, `get_address`, `check_tx_proof`
オペレーター登録簿と更新期間	署名 ID と配信鍵を含む期間名簿 `get_note_operator_roster`
Bridge	限定された支払い照合とサブアドレス割り当て
Pool HTTP	集計統計とアドレス指定の POST 照会 `GET /api/stats · POST /api/miner`

- ネットワーク定義 (/assets/noticoin-network.json)
- デスクトップウォレットガイド (/ja/guide.html) · ノードを起動する (/ja/guide-node.html) · CLI とウォレット RPC (/ja/guide-cli.html)
- 地図とピン (/ja/map.html) · 支払い (/ja/payments.html) · Noticoin のプライバシー (/ja/privacy.html)
- マイニングとプール (/ja/mining.html) · 基金報告 (/ja/fund.html)