PBC

PRIVACY BANK CHAIN

P B C

« Private money that works for you. »

La première blockchain qui marie la confidentialité de Monero à de véritables outils bancaires natifs — et résistants au quantique.

Sans smart contracts. Sans oracles. Sans custody. Sans tail emission.
Rien que du C++ vérifiable, déterministe, à offre strictement finie.

Dépôts à terme 2 Marché obligataire on-chain 2 Héritage trustless 2 Post-quantique hybride

Document de présentation — 2026

Le dilemme que personne n'avait résolu

CONFIDENTIALITÉ OU RENDEMENT — IL FALLAIT CHOISIR

Monero a résolu la confidentialité. Vos coins sont invisibles, intraçables, fongibles. Mais une fois dans votre wallet… ils dorment. Pas de rendement, pas d'épargne, pas de transmission. Du cash numérique, rien de plus.

La DeFi (Ethereum & clones) offre dépôts, yield et assurance — mais chaque transaction, chaque solde, chaque position est public. Le tout repose sur des smart contracts : du code piratable, modifiable, contrôlable par des clés admin. Plus de 2 milliards de dollars ont été volés via des failles de contrats en 2023-2024.

> **Le choix imposé jusqu'ici**
>
> - **A — La confidentialité (Monero)** — vos coins sont protégés, mais inertes.
> - **B — Le rendement (DeFi)** — vos coins travaillent, mais tout le monde vous regarde.

Privacy Bank Chain élimine ce dilemme. Tous les outils financiers sont codés directement dans le protocole, en C++, validés par consensus à chaque bloc. Pas de machine virtuelle, pas de couche 2, pas de frontend hébergé, aucune custody tierce.

Comment ça marche, en une phrase

> **Vous déposez des coins, ils génèrent du rendement, et personne ne sait que c'est vous.**
>
> On sait COMBIEN. On ne sait jamais QUI.

La transparence hybride — une approche inédite

Les montants des opérations financières sont publics — le consensus en a besoin pour calculer les poids et distribuer les récompenses au coin près. Mais les identités restent masquées derrière les ring signatures et les adresses furtives de CryptoNote.

Un observateur voit « quelqu'un a déposé 10 000 PBC pour 1 an ». Il ne peut ni identifier le wallet, ni relier ce dépôt à un futur retrait ou à une réclamation. C'est strictement supérieur à toute la DeFi, où montants ET identités sont entièrement publics.

	Transferts	Montants des opérations	Identité
Monero	Privés (RingCT)	—	—
DeFi Ethereum	Aucune	Publics	Publique
PBC	Privés (RingCT)	Publics (honnête)	Privée (ring sig)

Les fonctionnalités qui changent la donne

Chacune est native, codée en C++, vérifiée par consensus — et déjà couverte par des suites de tests automatisés (dépôts, claims, héritage, marketplace, post-quantique : des centaines de vérifications passées).

01 Dépôts à terme à rendement réel

Verrouillez vos PBC de 30 jours à 1 an et percevez un rendement financé par l'émission monétaire — pas par de la dette. Cinq paliers de durée, avec un multiplicateur croissant qui récompense la patience.

- **Récompenses « claim-based »** : vous réclamez vos gains quand vous voulez. Aucun paiement coinbase massif, aucun gonflement des blocs, aucune exclusion des petits déposants.
- **Anti-split par construction** : le poids est linéaire (montant × multiplicateur de durée). Découper un gros dépôt en petits ne rapporte jamais plus.
- **Sans frais de création** : seul le frais réseau standard s'applique à l'ouverture d'un dépôt.
- **Principal verrouillé jusqu'à l'échéance** : le capital est immobilisé au niveau du consensus (sortie UTXO verrouillée jusqu'à maturité), tandis que les récompenses restent réclamables à tout moment.
- Sortie avant terme : cédez votre dépôt sur le marché secondaire au prix que vous fixez (fonctionnalité 06) — zéro guichet, zéro intermédiaire, aucune pénalité.

02 Redistribution des frais — du yield réel

Les frais de chaque transaction du réseau se partagent en deux moitiés égales : **50 % pour les mineurs, 50 % pour les déposants**, ces derniers via un second index global indépendant. Plus le réseau est actif, plus votre rendement grimpe. C'est du rendement issu d'une activité économique réelle, pas de l'inflation déguisée.

- **Un partage imposé par le consensus** : la part du mineur est calculée à la construction de la coinbase et revérifiée à la validation de chaque bloc. Aucun mineur ne peut s'attribuer plus que sa moitié.
- **Double source de revenus** : Deposit Pool (émission) + Fee Pool (frais réseau), réclamés au même moment.
- **Cercle vertueux pour les mineurs** : le yield attire les épargnants, qui verrouillent du supply, ce qui soutient structurellement le cours de la monnaie qu'ils minent.
- **Frais auto-ajustés** : le plancher de frais du réseau s'élève automatiquement avec la part d'épargne verrouillée (jusqu'à ×2). Plus PBC est adopté, plus le Fee Pool rémunère — par construction.

03 Vesting anti-dump des récompenses de minage

Chaque récompense de bloc d'un mineur est fractionnée en 4 sorties à déverrouillage échelonné : ~24 h, ~30 j, ~60 j et ~90 j. Impossible de tout vendre d'un coup le jour du minage — la pression vendeuse est lissée et le cours stabilisé. Le vesting est imposé par le consensus, directement sur la coinbase : aucun logiciel de pool ne peut le contourner.

04 Fonds d'assurance, déflation automatique — et offre finie

1 % de chaque bloc alimente un Insurance Pool. Un filet de sécurité natif qui soutient les rendements en période de faible activité — automatique, plafonné, sans gouvernance ni vote.

Le plafond du fonds est fixé à 184 467 PBC — exactement 1 % de l'offre maximale. Tout excédent est définitivement brûlé, à chaque bloc, par le consensus : une déflation déterministe, sans burn manuel, sans décision d'équipe, sans clés d'admin.

- **Le contraste avec Monero** : Monero et les forks CryptoNote émettent à l'infini (tail emission perpétuelle). PBC a une offre strictement finie — 18 446 744 PBC, pas un de plus — ET brûle ses excédents. Le contraste est total.
- **Stabilité par conception** : au-delà de 60 % de l'offre circulante verrouillée en dépôts, un stabilisateur (Locked Supply Multiplier) amortit automatiquement la distribution pour préserver la liquidité du réseau — les rendements restent sains, jamais réflexifs.

05 Héritage trustless — le « Dead Man's Switch »

Une première sur une blockchain à confidentialité. Désignez un héritier ; s'il vous arrive quelque chose, il dépose une demande on-chain — et si vous ne donnez plus aucun signe de vie pendant 18 mois, vos fonds, y compris vos dépôts en cours et votre solde liquide, lui sont transférés automatiquement par le consensus.

- **Zéro tiers de confiance** : pas de notaire, pas d'avocat, pas de tribunal. Juste du consensus.
- **Un délai gravé dans le protocole** : le délai de 18 mois est une règle de consensus, identique pour tous — l'héritier ne peut jamais l'accélérer ni modifier la configuration.
- **Vous gardez le contrôle total** : toute opération signée de votre clé de dépense (nouveau dépôt, retrait, reconfiguration de l'héritage) annule la demande en cours. Et vous pouvez résilier la désignation à tout instant, d'une seule transaction.
- **Testament automatique** : votre wallet entretient automatiquement un « testament » pré-signé couvrant votre solde liquide, re-signé dès que votre solde évolue — et sauvegardé on-chain pour survivre à tout.
- **Verrouillé par le consensus** : un verrou de consensus rend toute exécution prématurée du testament impossible — avant l'échéance, le réseau entier la rejette.
- **Confidentiel** : l'identité du propriétaire (ring signature) comme celle de l'héritier (adresse furtive) restent masquées. On voit qu'un héritage existe, jamais qui est concerné.
- **Robuste** : état reconstruit déterministiquement après toute réorganisation de chaîne.

06 Marché obligataire on-chain — vos dépôts sont des obligations

Un dépôt à terme PBC, c'est économiquement une obligation privée au porteur : un principal, une échéance, un rendement. PBC en fait un titre librement négociable — le premier marché obligataire natif sur une chaîne à confidentialité de type Monero. Besoin de liquidité avant terme ? Cédez votre dépôt à un acheteur, entièrement on-chain, sans tiers de confiance et sans pénalité.

L'acheteur immobilise le montant d'achat dans un verrou (collateral lock), exactement comme un dépôt immobilise son principal. Le transfert est ensuite atomique, dans un seul bloc : le dépôt passe à l'acheteur, le paiement va au vendeur. Tout ou rien.

Et surtout : aucune somme confisquée, aucune commission prélevée. Là où une banque impose sa pénalité de sortie, PBC vous laisse souverain : vous fixez votre prix, vous vendez quand vous le décidez, à qui veut acheter. C'est le marché qui décide — librement — pas un intermédiaire.

- **Sécurisé de bout en bout** : annulation volontaire de l'acheteur, expiration automatique des verrous avec restitution du collatéral, transfert validé contre le verrou, et restauration intégrale en cas de réorganisation de chaîne.
- **Prix libre** : cédez votre dépôt au-dessus ou en-dessous du principal selon l'urgence de votre besoin de liquidité — c'est vous qui arbitrez.

07 Résistance post-quantique hybride — native dès le lancement

L'avantage décisif. Monero, Zcash et tous les forks CryptoNote actuels n'ont aucune résistance quantique, ni même de plan à court terme. Un ordinateur quantique suffisamment puissant pourrait un jour casser leurs signatures et dé-anonymiser tout leur historique.

PBC intègre une protection hybride : aux mécanismes classiques (Ed25519) viennent s'ajouter, en parallèle, des primitives post-quantiques normalisées par le NIST.

- **Signatures** : ML-DSA-65 (Dilithium, NIST FIPS 204). Dès le hard fork d'activation, toute autorisation de retrait de dépôt ou de paiement de marché exige cette co-signature en plus de la signature classique.
- **Échange de clés furtives** : ML-KEM-768 (Kyber, NIST FIPS 203) combiné à l'ECDH classique par dérivation HKDF, avec des adresses v2 engageant les clés post-quantiques.
- **Deux couches, une garantie** : si Ed25519 tombe demain, le post-quantique tient ; si une faille touche Dilithium, le classique tient. La sécurité est garantie tant que l'une des deux couches résiste. PBC serait la première blockchain à confidentialité de type Monero avec résistance quantique hybride sur les signatures ET l'échange de clés.

08 Une banque complète, chez vous — la WebUI

Toutes ces fonctionnalités se pilotent depuis une interface web locale incluse, connectée exclusivement à votre propre nœud : tableau de bord, dépôts et réclamations en un clic, alertes d'héritage en temps réel, marché obligataire intégré. Zéro cloud, zéro compte, zéro custody — vos clés ne quittent jamais votre machine.

Sécurité : zéro compromis

PAS DE VM · PAS DE CUSTODY · PAS DE CLÉS D'ADMIN

Pas de smart contracts = pas de hacks

Chaque fonctionnalité est compilée en C++ et validée par le consensus. Pas de VM, pas de bytecode interprété, pas de surface d'attaque extensible. Le code est fixe, auditable, identique sur chaque nœud.

Pas de custody tierce = pas de phishing

PBC s'utilise via un wallet CLI ou RPC en local. Aucune custody tierce, aucun frontend hébergé à pirater, aucune clé en mémoire de navigateur. Vos clés ne quittent jamais votre machine. (Une interface de gestion locale optionnelle se connecte uniquement à votre propre nœud.)

Solvabilité prouvée mathématiquement

Le mécanisme d'index global garantit par construction que la somme de toutes les récompenses réclamables ne peut jamais dépasser le solde du pool concerné — somme des récompenses par période = variation exacte du pool. Même si tous les déposants réclamaient en même temps, le système resterait solvable. Aucun taux fixe n'est jamais promis : tout taux fixe créerait une dette implicite que la chaîne ne peut garantir.

Fonds de développement transparent par construction

La clé de vue du fonds de développement est publiée dans le code source : chacun peut auditer chaque entrée du fonds, en permanence. 2 % par bloc, ni plus, ni moins — vérifié par tous les nœuds, visible par tous.

Minage CPU décentralisé, compatible pools

Minage RandomX v2 (variante rx/pbc), CPU-only et résistant aux ASIC. Compatible avec n'importe quel pool Stratum existant, sans aucune modification : les mineurs ne voient que la structure coinbase standard. Toutes les fonctionnalités financières sont des opérations wallet.

Tokenomics

PAS DE PREMINE • PAS D'ICO • PAS DE TOKENS RÉSERVÉS

Pas de premine. Pas d'ICO. Pas de tokens réservés. Une offre strictement finie de 18 446 744 PBC. Chaque bloc se répartit ainsi :

Allocation par bloc	Part	Destination
Mineurs	91 % de R + 50 % des frais	4 sorties vestées (anti-dump)
Fonds de développement	2 % de R	Soutien du projet (auditable par tous)
Fee Pool	3,5 % de R + 50 % des frais	Rendement des frais réseau
Deposit Pool	2,5 % de R	Rendement des dépôts à terme
Insurance Pool	1 % de R	Filet de sécurité + déflation (burn)

Paramètre	Valeur
Algorithme	RandomX v2 — variante rx/pbc (CPU-only, anti-ASIC)
Temps de bloc	1 minute (1 440 blocs/jour)
Période de distribution	~1 jour (1 440 blocs)
Offre maximale	18 446 744 PBC — zéro tail emission
Récompense au genesis (R)	~4,40 PBC/bloc (décroissance douce)
Paliers de dépôt	30 / 90 / 180 / 270 / 365 jours
Multiplicateurs de durée	1,0× — 1,3× — 1,6× — 1,8× — 2,0×
Dépôt minimum	10 PBC
Dépôts actifs par adresse	10 maximum
Sortie avant échéance	Marché secondaire (prix libre)
Délai d'héritage	18 mois (consensus)
Préfixe d'adresse	« Pbc… »
Confidentialité	CryptoNote (RingCT, ring sig, stealth) + PQC hybride

> **Stratégie « Mine & Deposit »**
>
> PBC est conçu pour que minage et dépôts se composent. Vous minez des PBC, puis vous les déposez pour générer un rendement supplémentaire — une double source de revenus avec le même capital matériel. Les premiers déposants captent mécaniquement les rendements les plus élevés : le gâteau (6 % de chaque bloc + 50 % des frais) se partage entre peu de monde au démarrage.

Projections de rentabilité

CHIFFRES ILLUSTRATIFS — PAS UNE PROMESSE DE RENDEMENT

Chiffres illustratifs, calculés sur les paramètres du protocole (bloc de 1 minute) et le modèle de poids linéaire.

Hypothèses de calcul

Paramètre	Valeur
Hashrate réseau	15 MH/s
Puissance AMD Ryzen 9 9950X	~23 KH/s (RandomX v2)
Équivalent réseau	~652 machines 9950X
Rythme de bloc	1 minute (1 440 blocs/jour)
Récompense au genesis (R)	~4,40 PBC/bloc
Émission journalière	~6 333 PBC/jour
Offre maximale	18 446 744 PBC
Minage via pools	~80 % du hashrate

Revenus de minage

91 % de chaque récompense de bloc revient aux mineurs (avec vesting 4 paliers), soit ~5 763 PBC/jour à répartir au prorata de la puissance — auxquels s'ajoute la moitié des frais réseau :

Configuration	Par jour	Par mois	Par an
1 × 9950X (23 KH/s)	~8,8 PBC	~265 PBC	~3 225 PBC
3 × 9950X (69 KH/s)	~26,5 PBC	~795 PBC	~9 675 PBC
5 × 9950X (115 KH/s)	~44,2 PBC	~1 325 PBC	~16 125 PBC
10 × 9950X (230 KH/s)	~88,4 PBC	~2 650 PBC	~32 250 PBC

Note : revenus en PBC, hors valeur fiat et hors part des frais réseau. Si la difficulté double, le revenu par machine est divisé par deux.

Rendement des dépôts

Le rendement dépend du poids total des déposants : plus ils sont nombreux, plus le gâteau se partage. Deposit Pool et Fee Pool reçoivent ensemble 6 % de chaque bloc (~380 PBC/jour) plus 50 % des frais réseau. Trois scénarios pour un dépôt unique de 10 000 PBC sur 365 jours (multiplicateur 2,0×) :

Scénario	Deposit Pool	Fee Pool	Total/an	APY
Early Bird (~50 déposants)	~11 860 PBC	~16 750 PBC	~28 610 PBC	~286 %
Croissance (~500)	~1 460 PBC	~2 060 PBC	~3 520 PBC	~35 %
Mature (~2 000)	~460 PBC	~650 PBC	~1 110 PBC	~11 %

> **Pourquoi le Early Bird est si élevé ?**
>
> Avec peu de déposants, le flux quotidien se partage entre très peu de monde. Ces rendements élevés attirent vite de nouveaux déposants, ce qui fait naturellement converger l'APY vers les scénarios suivants. Le système respire : des départs à maturité font remonter l'APY des fidèles.

Simulations — trois profils d'épargnants

Trois exemples concrets, à conditions de réseau constantes sur la durée du dépôt. Dans tous les cas, le principal est restitué à 100 % à l'échéance — les gains s'y ajoutent, et vous pouvez les réclamer à tout moment, sans toucher au dépôt, y compris après l'échéance.

Profil	Early Bird (~50)	Croissance (~500)	Mature (~2 000)
Prudent — 1 000 PBC / 90 j (×1,3)	~460 PBC (+46 %)	~56 PBC (+5,6 %)	~18 PBC (+1,8 %)
Équilibré — 5 000 PBC / 180 j (×1,6)	~5 640 PBC (+113 %)	~695 PBC (+13,9 %)	~220 PBC (+4,4 %)
Conviction — 10 000 PBC / 365 j (×2,0)	~28 610 PBC (+286 %)	~3 520 PBC (+35 %)	~1 110 PBC (+11 %)

- **Le réflexe early bird** : 1 000 PBC bloqués 3 mois en phase de lancement peuvent générer ~460 PBC de gains — près de la moitié du capital, en 90 jours.
- **Zéro capital sacrifié** : les gains se réclament quand vous voulez, le principal revient intégralement à l'échéance — et entre-temps, votre dépôt reste cessible sur le marché obligataire.
- **Lecture honnête** : gains en PBC, hors évolution du cours ; pourcentages calculés sur la durée réelle du dépôt, pas annualisés.

Stratégie combinée : Mine + Deposit

Revenu total = minage + rendement des dépôts (sur 10 000 PBC déposés). Comparé au minage seul :

Avec 1 × 9950X (minage ~3 225 PBC/an)

Scénario	Minage	Dépôts	Total	vs minage seul
Early Bird	3 225 PBC	28 610 PBC	31 835 PBC	× 9,9
Croissance	3 225 PBC	3 520 PBC	6 745 PBC	× 2,1
Mature	3 225 PBC	1 110 PBC	4 335 PBC	× 1,3

Avec 10 × 9950X (minage ~32 250 PBC/an)

Scénario	Minage	Dépôts	Total	vs minage seul
Early Bird	32 250 PBC	28 610 PBC	60 860 PBC	× 1,9
Croissance	32 250 PBC	3 520 PBC	35 770 PBC	× 1,1
Mature	32 250 PBC	1 110 PBC	33 360 PBC	× 1,03

Pas de taux fixe — un index, pas une promesse

Votre récompense = poids × (index actuel − index d'entrée). L'index ne fait que monter ; vos gains acquis ne diminuent jamais. L'APY affiché est un calcul rétroactif, qui fluctue période après période — comme un compteur kilométrique qui ne recule jamais.

Avertissement — Estimations illustratives, en aucun cas une promesse de rendement. Le rendement réel dépend du nombre de participants, du volume de transactions, du hashrate réseau et du cours du PBC. Les paramètres finaux seront figés avant le bloc genesis et peuvent différer de ces valeurs.

PBC face à l'existant

COMPARATIF FONCTIONNALITÉ PAR FONCTIONNALITÉ

	PBC	Monero	DeFi Ethereum
Confidentialité transferts	**Totale (RingCT)**	Totale	Aucune
Confidentialité identité	**Ring signatures**	Ring signatures	Publique
Offre monétaire	**Finie (18,45 M) + burn**	Infinie (tail emission)	Variable
Dépôts à terme natifs	**Oui (5 paliers)**	Non	Oui (contrat)
Rendement réel	**Émission + frais**	Non	Variable (risque)
Héritage on-chain	**Oui (1re sur chaîne privée)**	Non	Non
Marché obligataire (dépôts cessibles)	**Oui (atomique)**	Non	Partiel
Résistance post-quantique	**Hybride native**	Non	Non
Déflation automatique	**Oui (burn assurance)**	Non	Variable
Preuve de solvabilité	**Formelle**	—	Non
Dépendance oracle	**Aucune**	Aucune	Critique
Risque smart contract	**Zéro**	Zéro	Élevé
Minage CPU (RandomX v2)	**Oui**	Oui	Non (PoS)

Pour qui est PBC ?

QUATRE PROFILS, UNE SEULE CHAÎNE

Les holders long terme

Vos coins ne font rien ? Déposez-les. Le rendement est réel, pas spéculatif, et votre confidentialité reste intacte.

Les mineurs

Minage CPU RandomX v2, compatible tous pools Stratum. 91 % du bloc pour le mineur, plus la moitié des frais de chaque transaction du réseau, avec un vesting anti-dump qui soutient le cours. Minez puis déposez : double revenu.

Les utilisateurs soucieux de leur vie privée

Transferts CryptoNote complets (RingCT, adresses furtives). Aucun KYC, aucune trace, aucun wallet tiers — et une protection qui anticipe l'ère quantique.

Ceux qui planifient l'avenir

L'héritage trustless transmet vos fonds sans notaire, sans tribunal et sans révéler votre identité. Le marché secondaire vous offre une porte de sortie liquide à tout moment.

En résumé

La confidentialité de Monero + le rendement de la DeFi + une offre finie + l'héritage trustless + la résistance quantique.

Sans oracle. Sans custody. Sans admin keys. Juste de la cryptographie et des mathématiques.

Ce qu'aucune autre blockchain ne réunit

LA DIFFÉRENCE PBC

- **Dépôts à terme intégrés** — un produit d'épargne à rendement réel, au cœur du consensus, sur une chaîne aussi privée que Monero. Inédit.
- **Redistribution des frais intégrée** — les frais du réseau se partagent 50/50 entre mineurs et déposants : du yield issu de l'activité réelle, pas de l'inflation.
- **Marché obligataire intégré** — chaque dépôt est une obligation privée au porteur, revendable avant l'échéance par transfert atomique on-chain, sans tiers ni commission ; ou sortez immédiatement contre 2 % reversés à l'assurance. Vous restez souverain.
- **Héritage trustless intégré** — une première sur une blockchain à confidentialité : transmission automatique de vos fonds, sans notaire, sans tribunal, sans révéler votre identité — verrouillée par le consensus.
- **Résistance post-quantique hybride** — ML-DSA-65 + ML-KEM-768, là où Monero, Zcash et tous les forks CryptoNote n'ont strictement rien.
- **Rareté programmée sans gouvernance** — offre strictement finie et surplus du fonds d'assurance brûlé par le consensus, là où Monero et les forks CryptoNote émettent à l'infini.
- **Zéro surface d'attaque** — pas de smart contracts, pas d'oracle, pas de custody : exactement la surface qui a coûté des milliards à la DeFi, supprimée par construction.
- **Solvabilité prouvée, vie privée totale** — mathématiquement garantie, jamais promise ; montants publics, identités masquées à chaque étape.

PRIVACY BANK CHAIN

« Private money that works for you. »