PBC

PRIVACY BANK CHAIN

P B C

“Private money that works for you.”

The first blockchain that pairs Monero-grade privacy with genuine native banking tools — and quantum resistance.

No smart contracts. No oracles. No custody. No tail emission.
Nothing but verifiable, deterministic C++ with a strictly finite supply.

Term deposits 2 **On-chain bond market** 2 **Trustless inheritance** 2 **Hybrid post-quantum**

Presentation document — 2026

The dilemma nobody had solved

PRIVACY OR YIELD — YOU HAD TO CHOOSE

Monero solved privacy. Your coins are invisible, untraceable, fungible. But once they are in your wallet… they sleep. No yield, no savings, no transmission. Digital cash, nothing more.

DeFi (Ethereum and its clones) offers deposits, yield and insurance — but every transaction, every balance, every position is public. All of it rests on smart contracts: code that can be hacked, modified, and controlled by admin keys. More than $2 billion was stolen through contract flaws in 2023–2024.

> **The choice you were forced into until now**
>
> - **A — Privacy (Monero)** — your coins are protected, but inert.
> - **B — Yield (DeFi)** — your coins work, but everyone is watching you.

Privacy Bank Chain eliminates that dilemma. Every financial tool is coded directly into the protocol, in C++, validated by consensus at every block. No virtual machine, no layer 2, no hosted front end, no third-party custody.

How it works, in one sentence

> **You deposit coins, they generate yield, and nobody knows it is you.**
>
> Everyone sees HOW MUCH. Nobody ever sees WHO.

Hybrid transparency — an approach never seen before

The amounts of financial operations are public — consensus needs them in order to compute weights and distribute rewards down to the last coin. But identities remain masked behind CryptoNote ring signatures and stealth addresses.

An observer sees that “someone deposited 10,000 PBC for 1 year”. They can neither identify the wallet, nor link that deposit to a future withdrawal or claim. This is strictly superior to all of DeFi, where amounts AND identities are entirely public.

	Transfers	Operation amounts	Identity
Monero	Private (RingCT)	—	—
DeFi Ethereum	None	Public	Public
PBC	Private (RingCT)	Public (by design)	Private (ring sig.)

The features that change the game

Each one is native, written in C++, verified by consensus — and already covered by automated test suites (deposits, claims, inheritance, marketplace, post-quantum: hundreds of checks passing).

01 Term deposits with real yield

Lock your PBC from 30 days to 1 year and earn a yield funded by monetary emission — not by debt. Five duration tiers, with a rising multiplier that rewards patience.

- **Claim-based rewards**: you claim your gains whenever you want. No massive coinbase payout, no block bloat, no exclusion of small depositors.
- **Anti-split by construction**: weight is linear (amount × duration multiplier). Splitting a large deposit into smaller ones never pays more.
- **No creation fee**: only the standard network fee applies when opening a deposit.
- **Principal locked until maturity**: capital is immobilised at the consensus level (UTXO output locked until maturity), while rewards stay claimable at any time.
- Exit before term: sell your deposit on the secondary market at the price you set (feature 06) — no counter, no middleman, no penalty.

02 Fee redistribution — real yield

The fees on every network transaction are split into two equal halves: **50 % to miners, 50 % to depositors**, the latter through a second independent global index. The busier the network, the higher your yield climbs. This is yield derived from real economic activity, not disguised inflation.

- **A split enforced by consensus**: the miner's share is computed when the coinbase is built and re-verified when each block is validated. No miner can award themselves more than their half.
- **Two revenue streams**: Deposit Pool (emission) + Fee Pool (network fees), claimed at the same moment.
- **A virtuous circle for miners**: yield attracts savers, who lock up supply, which structurally supports the price of the currency they mine.
- **Self-adjusting fees**: the network fee floor rises automatically with the share of locked savings (up to ×2). The more PBC is adopted, the more the Fee Pool pays — by construction.

03 Anti-dump vesting on mining rewards

Every miner block reward is split into 4 outputs with staggered unlocks: ~24 h, ~30 d, ~60 d and ~90 d. Selling everything at once on mining day is impossible — sell pressure is smoothed and the price stabilised. Vesting is enforced by consensus, directly on the coinbase: no pool software can bypass it.

04 Insurance fund, automatic deflation — and a finite supply

1% of every block feeds an Insurance Pool. A native safety net that supports yields in periods of low activity — automatic, capped, with no governance and no vote.

The fund is capped at 184,467 PBC — exactly 1% of maximum supply. Any excess is permanently burned, at every block, by consensus: deterministic deflation, with no manual burn, no team decision, no admin keys.

- **The contrast with Monero**: Monero and the CryptoNote forks emit forever (perpetual tail emission). PBC has a strictly finite supply — 18,446,744 PBC, not one more — AND burns its surplus. The contrast is total.
- **Stability by design**: beyond 60% of circulating supply locked in deposits, a stabiliser (Locked Supply Multiplier) automatically dampens distribution to preserve network liquidity — yields stay healthy, never reflexive.

05 Trustless inheritance — the “Dead Man’s Switch”

A first on a privacy blockchain. Designate an heir; if something happens to you, they file an on-chain request — and if you give no further sign of life for 18 months, your funds, including your active deposits and your liquid balance, are transferred to them automatically by consensus.

- **Zero trusted third party**: no notary, no lawyer, no court. Just consensus.
- **A delay carved into the protocol**: the 18-month delay is a consensus rule, identical for everyone — the heir can never accelerate it nor modify the configuration.
- **You keep total control**: any operation signed with your spend key (new deposit, withdrawal, inheritance reconfiguration) cancels the pending request. And you can revoke the designation at any instant, in a single transaction.
- **Automatic testament**: your wallet automatically maintains a pre-signed “testament” covering your liquid balance, re-signed as soon as your balance changes — and backed up on-chain to survive anything.
- **Locked by consensus**: a consensus lock makes any premature execution of the testament impossible — before the deadline, the entire network rejects it.
- **Confidential**: the owner’s identity (ring signature) and the heir’s (stealth address) both stay masked. One sees that an inheritance exists, never who is concerned.
- **Robust**: state deterministically rebuilt after any chain reorganisation.

06 On-chain bond market — your deposits are bonds

A PBC term deposit is, economically, a private bearer bond: a principal, a maturity, a yield. PBC turns it into a freely tradable security — the first native bond market on a Monero-style privacy chain. Need liquidity before term? Sell your deposit to a buyer, entirely on-chain, with no trusted third party and no penalty.

The buyer immobilises the purchase amount in a collateral lock, exactly as a deposit immobilises its principal. The transfer is then atomic, within a single block: the deposit passes to the buyer, the payment goes to the seller. All or nothing.

And above all: no sum confiscated, no commission taken. Where a bank imposes its exit penalty, PBC leaves you sovereign: you set your price, you sell when you decide, to whoever wants to buy. The market decides — freely — not an intermediary.

- **Secured end to end**: voluntary cancellation by the buyer, automatic lock expiry with collateral returned, transfer validated against the lock, and full restoration in case of chain reorganisation.
- **Free pricing**: sell your deposit above or below principal depending on how urgent your need for liquidity is — the arbitrage is yours.

07 Hybrid post-quantum resistance — native from launch

The decisive advantage. Monero, Zcash and all current CryptoNote forks have no quantum resistance, nor even a short-term plan. A sufficiently powerful quantum computer could one day break their signatures and de-anonymise their entire history.

PBC embeds hybrid protection: alongside the classical mechanisms (Ed25519) run, in parallel, post-quantum primitives standardised by NIST.

- **Signatures**: ML-DSA-65 (Dilithium, NIST FIPS 204). From the activation hard fork onward, any deposit-withdrawal or market-payment authorisation requires this co-signature in addition to the classical signature.
- **Stealth key exchange**: ML-KEM-768 (Kyber, NIST FIPS 203) combined with classical ECDH through HKDF derivation, with v2 addresses committing to the post-quantum keys.
- **Two layers, one guarantee**: if Ed25519 falls tomorrow, post-quantum holds; if a flaw hits Dilithium, the classical layer holds. Security is guaranteed as long as one of the two layers resists. PBC would be the first Monero-style privacy blockchain with hybrid quantum resistance on both signatures AND key exchange.

08 A complete bank, at home — the WebUI

All of these features are driven from an included local web interface, connected exclusively to your own node: dashboard, deposits and claims in one click, real-time inheritance alerts, integrated bond market. Zero cloud, zero account, zero custody — your keys never leave your machine.

Security: zero compromise

NO VM · NO CUSTODY · NO ADMIN KEYS

No smart contracts = no hacks

Every feature is compiled in C++ and validated by consensus. No VM, no interpreted bytecode, no extensible attack surface. The code is fixed, auditable, identical on every node.

No third-party custody = no phishing

PBC is used through a local CLI or RPC wallet. No third-party custody, no hosted front end to hack, no keys in browser memory. Your keys never leave your machine. (An optional local management interface connects only to your own node.)

Solvency proven mathematically

The global index mechanism guarantees by construction that the sum of all claimable rewards can never exceed the balance of the pool concerned — sum of rewards per period = exact variation of the pool. Even if every depositor claimed at the same time, the system would remain solvent. No fixed rate is ever promised: any fixed rate would create an implicit debt the chain cannot guarantee.

A development fund transparent by construction

The view key of the development fund is published in the source code: anyone can audit every inflow to the fund, permanently. 2% per block, no more, no less — verified by every node, visible to all.

Decentralised CPU mining, pool-compatible

RandomX v2 mining (rx/pbc variant), CPU-only and ASIC-resistant. Compatible with any existing Stratum pool, with no modification whatsoever: miners only ever see the standard coinbase structure. All financial features are wallet operations.

Tokenomics

NO PREMINE • NO ICO • NO RESERVED TOKENS

No premine. No ICO. No reserved tokens. A strictly finite supply of 18,446,744 PBC. Every block is split as follows:

Per-block allocation	Share	Destination
Miners	91 % of R + 50 % of fees	4 vested outputs (anti-dump)
Development fund	2% of R	Project support (auditable by all)
Fee Pool	3.5% of R + 50% of fees	Yield from network fees
Deposit Pool	2.5% of R	Yield on term deposits
Insurance Pool	1% of R	Safety net + deflation (burn)

Parameter	Value
Algorithm	RandomX v2 — rx/pbc variant (CPU-only, ASIC-resistant)
Block time	1 minute (1,440 blocks/day)
Distribution period	~1 day (1,440 blocks)
Maximum supply	18,446,744 PBC — zero tail emission
Genesis reward (R)	~4.40 PBC/block (gentle decay)
Deposit tiers	30 / 90 / 180 / 270 / 365 days
Duration multipliers	1.0× — 1.3× — 1.6× — 1.8× — 2.0×
Minimum deposit	10 PBC
Active deposits per address	10 maximum
Exit before maturity	Secondary market (free pricing)
Inheritance delay	18 months (consensus)
Address prefix	“Pbc...”
Privacy	CryptoNote (RingCT, ring sig., stealth) + hybrid PQC

The “Mine & Deposit” strategy

PBC is designed so that mining and deposits compound. You mine PBC, then you deposit it to generate additional yield — two revenue streams from the same hardware capital. Early depositors mechanically capture the highest yields: the pie (6% of every block + 50% of fees) is shared among very few people at launch.

Profitability projections

ILLUSTRATIVE FIGURES — NOT A PROMISE OF RETURN

Illustrative figures, computed on the protocol parameters (1-minute block) and the linear weight model.

Calculation assumptions

Parameter	Value
Network hashrate	15 MH/s
AMD Ryzen 9 9950X power	~23 KH/s (RandomX v2)
Network equivalent	~652 × 9950X machines
Block pace	1 minute (1,440 blocks/day)
Genesis reward (R)	~4.40 PBC/block
Daily emission	~6,333 PBC/day
Maximum supply	18,446,744 PBC
Mining via pools	~80% of hashrate

Mining revenue

91 % of every block reward goes to miners (with 4-tier vesting), i.e. ~5,763 PBC/day to be shared pro rata to hashpower — on top of which comes half of all network fees:

Configuration	Per day	Per month	Per year
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: revenue expressed in PBC, excluding fiat value and excluding the share of network fees. If difficulty doubles, revenue per machine is halved.

Deposit yield

Yield depends on the total weight of depositors: the more of them there are, the more the pie is shared. Together, the Deposit Pool and the Fee Pool receive 6% of every block (~380 PBC/day) plus 50% of network fees. Three scenarios for a single 10,000 PBC deposit over 365 days (2.0× multiplier):

Scenario	Deposit Pool	Fee Pool	Total/year	APY
Early Bird (~50 depositors)	~11,860 PBC	~16,750 PBC	~28,610 PBC	~286%
Growth (~500)	~1,460 PBC	~2,060 PBC	~3,520 PBC	~35%
Mature (~2,000)	~460 PBC	~650 PBC	~1,110 PBC	~11%

> **Why is the Early Bird figure so high?**
>
> With few depositors, the daily flow is shared among very few people. Those high yields quickly attract new depositors, which naturally makes the APY converge toward the later scenarios. The system breathes: departures at maturity push the APY back up for those who stay.

Simulations — three saver profiles

Three concrete examples, at constant network conditions over the duration of the deposit. In every case, the principal is returned in full at maturity — gains come on top, and you can claim them at any moment, without touching the deposit, including after maturity.

Profile	Early Bird (~50)	Growth (~500)	Mature (~2,000)
Cautious — 1,000 PBC / 90 d (×1.3)	~460 PBC (+46%)	~56 PBC (+5.6%)	~18 PBC (+1.8%)
Balanced — 5,000 PBC / 180 d (×1.6)	~5,640 PBC (+113%)	~695 PBC (+13.9%)	~220 PBC (+4.4%)
Conviction — 10,000 PBC / 365 d (×2.0)	~28,610 PBC (+286%)	~3,520 PBC (+35%)	~1,110 PBC (+11%)

- **The early-bird reflex**: 1,000 PBC locked for 3 months in the launch phase can generate ~460 PBC in gains — nearly half the capital, in 90 days.
- **Zero capital sacrificed**: gains are claimed whenever you want, the principal comes back in full at maturity — and in the meantime, your deposit remains tradable on the bond market.
- **An honest reading**: gains in PBC, excluding price movement; percentages computed over the actual duration of the deposit, not annualised.

Combined strategy: Mine + Deposit

Total revenue = mining + deposit yield (on 10,000 PBC deposited). Compared with mining alone:

With 1 × 9950X (mining ~3,225 PBC/year)

Scenario	Mining	Deposits	Total	vs mining alone
Early Bird	3,225 PBC	28,610 PBC	31,835 PBC	× 9.9
Growth	3,225 PBC	3,520 PBC	6,745 PBC	× 2.1
Mature	3,225 PBC	1,110 PBC	4,335 PBC	× 1.3

With 10 × 9950X (mining ~32,250 PBC/year)

Scenario	Mining	Deposits	Total	vs mining alone
Early Bird	32,250 PBC	28,610 PBC	60,860 PBC	× 1.9
Growth	32,250 PBC	3,520 PBC	35,770 PBC	× 1.1
Mature	32,250 PBC	1,110 PBC	33,360 PBC	× 1.03

No fixed rate — an index, not a promise

Your reward = weight × (current index − entry index). The index only ever rises; your accrued gains never shrink. The displayed APY is a backward-looking calculation that fluctuates period after period — like an odometer that never runs backwards.

Disclaimer — Illustrative estimates, in no way a promise of return. Actual yield depends on the number of participants, transaction volume, network hashrate and the PBC price. Final parameters will be frozen before the genesis block and may differ from these values.

PBC against what already exists

FEATURE-BY-FEATURE COMPARISON

	PBC	Monero	DeFi Ethereum
Transfer privacy	**Total (RingCT)**	Total	None
Identity privacy	**Ring signatures**	Ring signatures	Public
Monetary supply	**Finite (18.45 M) + burn**	Infinite (tail emission)	Variable
Native term deposits	**Yes (5 tiers)**	No	Yes (contract)
Real yield	**Emission + fees**	No	Variable (risk)
On-chain inheritance	**Yes (1st on a privacy chain)**	No	No
Bond market (tradable deposits)	**Yes (atomic)**	No	Partial
Post-quantum resistance	**Native hybrid**	No	No
Automatic deflation	**Yes (insurance burn)**	No	Variable
Proof of solvency	**Formal**	—	No
Oracle dependency	**None**	None	Critical
Smart-contract risk	**Zero**	Zero	High
CPU mining (RandomX v2)	**Yes**	Yes	No (PoS)

Who is PBC for?

FOUR PROFILES, ONE CHAIN

Long-term holders

Your coins doing nothing? Deposit them. The yield is real, not speculative, and your privacy stays intact.

Miners

RandomX v2 CPU mining, compatible with all Stratum pools. 91 % of the block for the miner, plus half the fees on every network transaction, with anti-dump vesting that supports the price. Mine, then deposit: double income.

Privacy-conscious users

Full CryptoNote transfers (RingCT, stealth addresses). No KYC, no trace, no third-party wallet — and protection that anticipates the quantum era.

Those planning ahead

Trustless inheritance passes your funds on with no notary, no court and without revealing your identity. The secondary market gives you a liquid exit at any time.

In summary

Monero’s privacy + DeFi’s yield + a finite supply + trustless inheritance + quantum resistance.

No oracle. No custody. No admin keys. Just cryptography and mathematics.

What no other blockchain brings together

THE PBC DIFFERENCE

- **Integrated term deposits** — a real-yield savings product, at the heart of consensus, on a chain as private as Monero. Unprecedented.
- **Integrated fee redistribution** — network fees are split 50/50 between miners and depositors: yield from real activity, not from inflation.
- **Integrated bond market** — every deposit is a private bearer bond, resellable before maturity by an atomic on-chain transfer, with no third party and no commission; or exit immediately against 2% paid to the insurance fund. You stay sovereign.
- **Integrated trustless inheritance** — a first on a privacy blockchain: automatic transmission of your funds, with no notary, no court, without revealing your identity — locked by consensus.
- **Hybrid post-quantum resistance** — ML-DSA-65 + ML-KEM-768, where Monero, Zcash and every CryptoNote fork have strictly nothing.
- **Programmed scarcity without governance** — a strictly finite supply and insurance-fund surplus burned by consensus, where Monero and the CryptoNote forks emit forever.
- **Zero attack surface** — no smart contracts, no oracle, no custody: precisely the surface that has cost DeFi billions, removed by construction.
- **Proven solvency, total privacy** — mathematically guaranteed, never promised; amounts public, identities masked at every step.

PRIVACY BANK CHAIN

“Private money that works for you.”