

PBC

PRIVACY BANK CHAIN

P B C

«Private money that works for you.»

Первый блокчейн, объединяющий конфиденциальность Monero с настоящими встроенными банковскими инструментами — и с устойчивостью к квантовым атакам.

Без смарт-контрактов. Без оракулов. Без кастодиального хранения. Без tail emission.
Только проверяемый детерминированный C++ и строго конечная эмиссия.

Срочные вклады 2 Рынок облигаций on-chain 2 Наследование без доверия 2
Гибридная постквантовая защита

Дилемма, которую никто не решил

КОНФИДЕНЦИАЛЬНОСТЬ ИЛИ ДОХОДНОСТЬ — ПРИХОДИЛОСЬ ВЫБИРАТЬ

Monero решил задачу конфиденциальности. Ваши монеты невидимы, неотслеживаемы, взаимозаменяемы. Но, попав в кошелёк... они просто спят. Ни доходности, ни сбережений, ни передачи по наследству. Просто цифровая наличность, и не более того.

DeFi (Ethereum и его клоны) предлагает вклады, доходность и страхование — но каждая транзакция, каждый баланс, каждая позиция публичны. Всё это держится на смарт-контрактах: коде, который можно взломать, изменить и контролировать админскими ключами. За 2023-2024 годы через уязвимости контрактов было похищено более 2 млрд долларов.

Выбор, который навязывали до сих пор

- **A — Конфиденциальность (Monero)** — ваши монеты защищены, но неподвижны.
- **B — Доходность (DeFi)** — ваши монеты работают, но на вас смотрят все.

Privacy Bank Chain снимает эту дилемму. Все финансовые инструменты закодированы прямо в протоколе, на C++, и проверяются консенсусом в каждом блоке. Никакой виртуальной машины, никакого второго уровня, никакого размещённого фронтенда, никакого стороннего хранения средств.

Как это работает — в одном предложении

Вы вносите монеты, они приносят доход, и никто не знает, что это вы.

Известно СКОЛЬКО. Никогда не известно КТО.

Гибридная прозрачность — подход, которого раньше не было

Суммы финансовых операций публичны — они нужны консенсусу, чтобы вычислять веса и распределять вознаграждения с точностью до монеты. Но личности остаются скрыты за кольцевыми подписями и скрытыми адресами CryptoNote.

Наблюдатель видит, что «кто-то внёс 10 000 PBC на 1 год». Он не может ни определить кошелёк, ни связать этот вклад с будущим выводом или запросом вознаграждения. Это строго лучше, чем вся DeFi, где публичны И суммы, И личности.

	Переводы	Суммы операций	Личность
Monero	Приватные (RingCT)	—	—
DeFi Ethereum	Нет	Публичные	Публичная
PBC	Приватные (RingCT)	Публичные (по замыслу)	Приватная (кольцевая подпись)

Функции, которые меняют правила игры

Каждая из них встроена в протокол, написана на C++ и проверяется консенсусом — и уже покрыта автоматическими наборами тестов (вклады, запросы вознаграждений, наследование, рынок, постквантовая часть: сотни успешных проверок).

01 Срочные вклады с реальной доходностью

Заблокируйте свои PBC на срок от 30 дней до 1 года и получайте доход, финансируемый денежной эмиссией, а не долгом. Пять уровней срока с растущим множителем, который вознаграждает терпение.

- **Вознаграждения по запросу:** вы забираете доход тогда, когда захотите. Никаких массовых выплат в coinbase, никакого раздувания блоков, никакого исключения мелких вкладчиков.
- **Защита от дробления по построению:** вес линейен (сумма × множитель срока). Разбить крупный вклад на мелкие никогда не выгоднее.
- **Без комиссии за открытие:** при открытии вклада взимается только стандартная сетевая комиссия.
- **Тело вклада заблокировано до срока:** капитал обездвижен на уровне консенсуса (выход UTXO заблокирован до наступления срока), тогда как вознаграждения можно забирать в любой момент.
- **Досрочный выход:** продайте вклад на вторичном рынке по назначенной вами цене (функция 06) — ноль окошек, ноль посредников, без штрафа.

02 Перераспределение комиссий — реальный доход

Комиссии с каждой транзакции сети делятся на две равные половины: **50 % майнерам, 50 % вкладчикам**, последним — через второй независимый глобальный индекс. Чем активнее сеть, тем выше ваша доходность. Это доход от реальной экономической активности, а не замаскированная инфляция.

- **Раздел, навязанный консенсусом:** доля майнера вычисляется при построении coinbase и перепроверяется при валидации каждого блока. Ни один майнер не может присвоить себе больше своей половины.
- **Двойной источник дохода:** Deposit Pool (эмиссия) + Fee Pool (сетевые комиссии), забираются одновременно.
- **Благотворный круг для майнеров:** доходность привлекает вкладчиков, они блокируют предложение, что структурно поддерживает курс монеты, которую они майнят.
- **Самонастраивающиеся комиссии:** нижний порог комиссии сети автоматически растёт вместе с долей заблокированных сбережений (до ×2). Чем шире принимается PBC, тем больше платит Fee Pool — по построению.

03 Антидампный вестинг вознаграждений за майнинг

Каждое блочное вознаграждение майнера делится на 4 выхода с поэтапной разблокировкой: ~24 ч, ~30 дн., ~60 дн. и ~90 дн. Продать всё сразу в день добычи невозможно — давление продавцов сглаживается, а курс стабилизируется. Вестинг навязан консенсусом прямо на coinbase: никакое пуловое ПО не может его обойти.

04 Страховой фонд, автоматическая дефляция — и конечная эмиссия

1 % каждого блока пополняет Insurance Pool. Встроенная страховочная сетка, поддерживающая доходность в периоды низкой активности — автоматическая, с потолком, без управления и голосований.

Потолок фонда — 184 467 PBC, ровно 1 % максимальной эмиссии. Весь излишек безвозвратно сжигается в каждом блоке консенсусом: детерминированная дефляция, без ручного сжигания, без решений команды, без админских ключей.

- **Контраст с Monero:** Monero и форки CryptoNote выпускают монеты бесконечно (вечная tail emission). У PBC строго конечная эмиссия — 18 446 744 PBC, ни монетой больше — И она сжигает свои излишки. Контраст полный.
- **Устойчивость по замыслу:** когда свыше 60 % оборотного предложения заблокировано во вкладах, стабилизатор (Locked Supply Multiplier) автоматически сглаживает распределение, чтобы сохранить ликвидность сети — доходность остаётся здоровой и никогда не становится рефлексивной.

05 Наследование без доверия — «Dead Man's Switch»

Впервые в блокчейне с конфиденциальностью. Назначьте наследника; если с вами что-то случится, он подаёт запрос on-chain — и если вы не подаёте признаков жизни 18 месяцев, ваши средства, включая действующие вклады и ликвидный баланс, автоматически передаются ему консенсусом.

- **Ноль доверенных третьих лиц:** ни нотариуса, ни адвоката, ни суда. Только консенсус.
- **Срок, высеченный в протоколе:** срок в 18 месяцев — правило консенсуса, одинаковое для всех; наследник не может ни ускорить его, ни изменить настройку.
- **Вы сохраняете полный контроль:** любая операция, подписанная вашим ключом траты (новый вклад, вывод, перенастройка наследования), отменяет текущий запрос. А отозвать назначение можно в любой момент одной транзакцией.
- **Автоматическое завещание:** ваш кошелёк автоматически поддерживает заранее подписанное «завещание» на ликвидный баланс, переподписывая его при каждом изменении баланса — и сохраняет его on-chain, чтобы оно пережило всё.
- **Заблокировано консенсусом:** консенсусная блокировка делает досрочное исполнение завещания невозможным — до наступления срока вся сеть его отклоняет.
- **Конфиденциально:** и личность владельца (кольцевая подпись), и личность наследника (скрытый адрес) остаются скрытыми. Видно, что наследование существует, но никогда — кого оно касается.
- **Надёжно:** состояние детерминированно восстанавливается после любой реорганизации цепи.

06 Рынок облигаций on-chain — ваши вклады это облигации

Срочный вклад PBC экономически представляет собой частную облигацию на предъявителя: тело, срок погашения, доходность. PBC делает его свободно обращающейся ценной бумагой — это первый встроенный рынок облигаций в блокчейне с конфиденциальностью уровня Monero. Нужна ликвидность до срока? Уступите свой вклад покупателю полностью on-chain, без доверенных третьих лиц и без штрафа.

Покупатель обездвиживает сумму покупки в залоговой блокировке (collateral lock) — ровно так же, как вклад обездвиживает своё тело. Затем перевод происходит атомарно, в одном блоке: вклад переходит покупателю, оплата уходит продавцу. Всё или ничего.

И главное: ничего не конфискуется, никакая комиссия не удерживается. Там, где банк навязывает штраф за выход, PBC оставляет вас суверенным: вы назначаете цену, продаёте тогда, когда решите, и тому, кто хочет купить. Решает рынок — свободно, а не посредник.

- **Защита от начала до конца:** добровольная отмена покупателем, автоматическое истечение блокировок с возвратом залога, перевод, проверяемый против блокировки, и полное восстановление при реорганизации цепи.
- **Свободная цена:** уступайте вклад выше или ниже тела — в зависимости от того, насколько срочно вам нужна ликвидность. Решение за вами.

07 Гибридная постквантовая защита — встроена с самого запуска

Решающее преимущество. У Monero, Zcash и всех нынешних форков CryptoNote нет ни квантовой устойчивости, ни даже краткосрочного плана. Достаточно мощный квантовый компьютер однажды сможет взломать их подписи и деанонимизировать всю их историю.

PBC содержит гибридную защиту: к классическим механизмам (Ed25519) параллельно добавлены постквантовые примитивы, стандартизованные NIST.

- **Подписи:** ML-DSA-65 (Dilithium, NIST FIPS 204). Начиная с хардфорка активации любая авторизация вывода вклада или рыночного платежа требует этой сопутствующей подписи в дополнение к классической.
- **Обмен ключами для скрытых адресов:** ML-KEM-768 (Kyber, NIST FIPS 203) в сочетании с классическим ECDH через выведение HKDF, с адресами v2, фиксирующими постквантовые ключи.
- **Два слоя, одна гарантия:** если завтра падёт Ed25519, устоит постквантовая часть; если уязвимость затронет Dilithium, устоит классическая. Безопасность гарантирована, пока держится хотя бы один из двух слоёв. PBC стал бы первым блокчейном с конфиденциальностью уровня Monero, имеющим гибридную квантовую устойчивость и в подписях, и в обмене ключами.

08 Полноценный банк у вас дома — WebUI

Все эти функции управляются из входящего в комплект локального веб-интерфейса, подключённого исключительно к вашему собственному узлу: панель управления, вклады и запросы вознаграждений в один клик, оповещения о наследовании в реальном времени, встроенный рынок облигаций. Ноль облака, ноль аккаунтов, ноль кастодиального хранения — ваши ключи никогда не покидают вашу машину.

Безопасность: без компромиссов

БЕЗ ВИРТУАЛЬНОЙ МАШИНЫ • БЕЗ КАСТОДИАЛЬНОГО ХРАНЕНИЯ • БЕЗ АДМИНСКИХ КЛЮЧЕЙ

Нет смарт-контрактов = нет взломов

Каждая функция скомпилирована на C++ и проверяется консенсусом. Ни виртуальной машины, ни интерпретируемого байткода, ни расширяемой поверхности атаки. Код фиксирован, поддаётся аудиту и одинаков на каждом узле.

Нет стороннего хранения = нет фишинга

PBC используется через локальный CLI- или RPC-кошелёк. Никакого стороннего хранения средств, никакого размещённого фронтенда для взлома, никаких ключей в памяти браузера. Ваши ключи никогда не покидают вашу машину. (Опциональный локальный интерфейс управления подключается только к вашему собственному узлу.)

Платёжеспособность, доказанная математически

Механизм глобального индекса по построению гарантирует, что сумма всех доступных к получению вознаграждений никогда не превысит баланс соответствующего пула: сумма вознаграждений за период = точное изменение пула. Даже если бы все вкладчики обратились одновременно, система осталась бы платёжеспособной. Никакая фиксированная ставка никогда не обещается: любая фиксированная ставка создавала бы неявный долг, который цепь не может гарантировать.

Фонд разработки, прозрачный по построению

Ключ просмотра фонда разработки опубликован в исходном коде: любой может постоянно проверять каждое поступление в фонд. 2 % на блок, ни больше ни меньше — проверяется всеми узлами, видно всем.

Децентрализованный майнинг на CPU, совместимый с пулами

Майнинг RandomX v2 (вариант gx/pbc), только на CPU и с устойчивостью к ASIC. Совместим с любым существующим Stratum-пулом без каких-либо доработок: майнеры видят лишь стандартную структуру coinbase. Все финансовые функции — это операции кошелька.

Токеномика

БЕЗ ПРЕМАЙНА • БЕЗ ICO • БЕЗ ЗАРЕЗЕРВИРОВАННЫХ ТОКЕНОВ

Без премайна. Без ICO. Без зарезервированных токенов. Строго конечная эмиссия в 18 446 744 PBC. Каждый блок распределяется так:

Распределение блока	Доля	Назначение
Майнеры	91 % от R + 50 % комиссий	4 выхода с вестингом (антидамп)
Фонд разработки	2 % от R	Поддержка проекта (доступен для аудита всем)
Fee Pool	3,5 % от R + 50 % комиссий	Доход от сетевых комиссий
Deposit Pool	2,5 % от R	Доход по срочным вкладам
Insurance Pool	1 % от R	Страховочная сетка + дефляция (сжигание)

Параметр	Значение
Алгоритм	RandomX v2 — вариант rx/pbc (только CPU, анти-ASIC)
Время блока	1 минута (1 440 блоков/день)
Период распределения	~1 день (1 440 блоков)
Максимальная эмиссия	18 446 744 PBC — нулевая tail emission
Награда на генезисе (R)	~4,40 PBC/блок (плавное снижение)
Уровни вклада	30 / 90 / 180 / 270 / 365 дней
Множители срока	1,0× — 1,3× — 1,6× — 1,8× — 2,0×
Минимальный вклад	10 PBC
Активных вкладов на адрес	не более 10
Досрочный выход	Вторичный рынок (свободная цена)
Срок наследования	18 месяцев (консенсус)
Префикс адреса	«Pbc...»
Конфиденциальность	CryptoNote (RingCT, кольцевые подписи, скрытые адреса) + гибридная PQS

Стратегия «Mine & Deposit»

PBC спроектирован так, чтобы майнинг и вклады складывались. Вы майните PBC, затем вносите их во вклад ради дополнительного дохода — два источника дохода при одном и том же капитале оборудования. Первые вкладчики механически получают самую высокую доходность: пирог (6 % каждого блока + 50 % комиссий) на старте делится между немногими.

Прогноз доходности

ИЛЛЮСТРАТИВНЫЕ ЦИФРЫ — НЕ ОБЕЩАНИЕ ДОХОДНОСТИ

Иллюстративные цифры, рассчитанные по параметрам протокола (блок в 1 минуту) и линейной модели весов.

Исходные допущения

Параметр	Значение
Хешрейт сети	15 MH/s
Мощность AMD Ryzen 9 9950X	~23 KH/s (RandomX v2)
Эквивалент сети	~652 машины 9950X
Темп блоков	1 минута (1 440 блоков/день)
Награда на генезисе (R)	~4,40 PBC/блок
Дневная эмиссия	~6 333 PBC/день
Максимальная эмиссия	18 446 744 PBC
Майнинг через пулы	~80 % хешрейта

Доход от майнинга

91 % каждого блочного вознаграждения достаётся майнерам (с вестингом в 4 этапа), то есть ~5 763 PBC/день, распределяемых пропорционально мощности, — к чему добавляется половина всех сетевых комиссий:

Конфигурация	В день	В месяц	В год
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

Примечание: доход в PBC, без учёта фиатной стоимости и без учёта доли сетевых комиссий. При удвоении сложности доход на машину уменьшается вдвое.

Доходность вкладов

Доходность зависит от суммарного веса вкладчиков: чем их больше, тем сильнее делится пирог. Deposit Pool и Fee Pool вместе получают 6 % каждого блока (~380 PBC/день) плюс 50 % сетевых комиссий. Три сценария для одного вклада в 10 000 PBC на 365 дней (множитель 2,0×):

Сценарий	Deposit Pool	Fee Pool	Итого/год	APY
Early Bird (~50 вкладчиков)	~11 860 PBC	~16 750 PBC	~28 610 PBC	~286 %
Рост (~500)	~1 460 PBC	~2 060 PBC	~3 520 PBC	~35 %
Зрелость (~2 000)	~460 PBC	~650 PBC	~1 110 PBC	~11 %

Почему Early Bird так высок?

Когда вкладчиков мало, дневной поток делится между очень немногими. Такая высокая доходность быстро привлекает новых вкладчиков, из-за чего APY естественно сходится к последующим сценариям. Система дышит: уход вкладчиков по окончании срока снова поднимает APY у тех, кто остался.

Симуляции — три профиля вкладчика

Три конкретных примера при неизменных условиях сети на всём сроке вклада. Во всех случаях тело вклада возвращается на 100 % в срок — доход добавляется сверху, и забрать его можно в любой момент, не трогая вклад, в том числе после окончания срока.

Профиль	Early Bird (~50)	Рост (~500)	Зрелость (~2 000)
Осторожный — 1 000 PBC / 90 дн. (×1,3)	~460 PBC (+46 %)	~56 PBC (+5,6 %)	~18 PBC (+1,8 %)
Сбалансированный — 5 000 PBC / 180 дн. (×1,6)	~5 640 PBC (+113 %)	~695 PBC (+13,9 %)	~220 PBC (+4,4 %)
С убеждением — 10 000 PBC / 365 дн. (×2,0)	~28 610 PBC (+286 %)	~3 520 PBC (+35 %)	~1 110 PBC (+11 %)

- **Рефлекс раннего вкладчика:** 1 000 PBC, заблокированные на 3 месяца в фазе запуска, могут принести ~460 PBC дохода — почти половину капитала за 90 дней.
- **Ноль потерянного капитала:** доход забирается когда угодно, тело вклада возвращается полностью в срок — а тем временем вклад остаётся продаваемым на рынке облигаций.
- **Честное прочтение:** доход в PBC, без учёта динамики курса; проценты рассчитаны на реальный срок вклада, а не приведены к году.

Комбинированная стратегия: Mine + Deposit

Суммарный доход = майнинг + доход по вкладам (на 10 000 внесённых PBC). В сравнении с одним лишь майнингом:

С 1 × 9950X (майнинг ~3 225 PBC/год)

Сценарий	Майнинг	Вклады	Итого	vs только майнинг
Early Bird	3 225 PBC	28 610 PBC	31 835 PBC	× 9,9
Рост	3 225 PBC	3 520 PBC	6 745 PBC	× 2,1
Зрелость	3 225 PBC	1 110 PBC	4 335 PBC	× 1,3

С 10 × 9950X (майнинг ~32 250 PBC/год)

Сценарий	Майнинг	Вклады	Итого	vs только майнинг
Early Bird	32 250 PBC	28 610 PBC	60 860 PBC	× 1,9
Рост	32 250 PBC	3 520 PBC	35 770 PBC	× 1,1
Зрелость	32 250 PBC	1 110 PBC	33 360 PBC	× 1,03

Никакой фиксированной ставки — индекс, а не обещание

Ваше вознаграждение = вес × (текущий индекс – индекс входа). Индекс только растёт; уже накопленный доход никогда не уменьшается. Показанный APY — это ретроспективный расчёт, который колеблется от периода к периоду, как одометр, который никогда не крутится назад.

Предупреждение — Иллюстративные оценки, ни в коем случае не обещание доходности. Реальная доходность зависит от числа участников, объёма транзакций, хешрейта сети и курса PBC. Итоговые параметры будут зафиксированы до генезис-блока и могут отличаться от этих значений.

РВС на фоне существующих решений

СРАВНЕНИЕ ФУНКЦИЯ ЗА ФУНКЦИЕЙ

	РВС	Monero	DeFi Ethereum
Конфиденциальность переводов	Полная (RingCT)	Полная	Нет
Конфиденциальность личности	Кольцевые подписи	Кольцевые подписи	Публичная
Денежная эмиссия	Конечная (18,45 млн) + сжигание	Бесконечная (tail emission)	Переменная
Встроенные срочные вклады	Да (5 уровней)	Нет	Да (контракт)
Реальная доходность	Эмиссия + комиссии	Нет	Переменная (риск)
Наследование on-chain	Да (1-е в приватной цепи)	Нет	Нет
Рынок облигаций (передаваемые вклады)	Да (атомарно)	Нет	Частично
Постквантовая устойчивость	Гибридная, встроенная	Нет	Нет
Автоматическая дефляция	Да (сжигание страховки)	Нет	Переменная
Доказательство платёжеспособности	Формальное	—	Нет
Зависимость от оракулов	Нет	Нет	Критическая
Риск смарт-контракта	Нулевой	Нулевой	Высокий
Майнинг на CPU (RandomX v2)	Да	Да	Нет (PoS)

Для кого создан PBC?

ЧЕТЫРЕ ПРОФИЛЯ, ОДНА ЦЕПЬ

Долгосрочные держатели

Ваши монеты ничего не делают? Внесите их во вклад. Доход реальный, а не спекулятивный, и ваша конфиденциальность остаётся нетронутой.

Майнеры

Майнинг на CPU по RandomX v2, совместим со всеми Stratum-пулами. 91 % блока майнеру плюс половина комиссий с каждой транзакции сети, с антидампovým вестингом, поддерживающим курс. Майните, затем вносите во вклад: двойной доход.

Те, кому важна приватность

Полноценные переводы CryptoNote (RingCT, скрытые адреса). Никакого KYC, никаких следов, никаких сторонних кошельков — и защита, рассчитанная на квантовую эпоху.

Те, кто планирует будущее

Наследование без доверия передаёт ваши средства без нотариуса, без суда и без раскрытия вашей личности. Вторичный рынок в любой момент даёт ликвидный выход.

Коротко

Конфиденциальность Monero + доходность DeFi + конечная эмиссия + наследование без доверия + квантовая устойчивость.

Без оракулов. Без кастодиального хранения. Без админских ключей. Только криптография и математика.

Чего не объединяет ни один другой блокчейн

В ЧЁМ РАЗНИЦА РВС

- **Встроенные срочные вклады** — сберегательный продукт с реальной доходностью в самом сердце консенсуса, в цепи, приватной как Monero. Такого ещё не было.
- **Встроенное перераспределение комиссий** — сетевые комиссии делятся 50/50 между майнерами и вкладчиками: доход от реальной активности, а не от инфляции.
- **Встроенный рынок облигаций** — каждый вклад это частная облигация на предъявителя, которую можно перепродать до срока атомарным переводом on-chain, без посредников и без комиссии; либо выйти немедленно с 2 %, уходящими в страховой фонд. Вы остаётесь суверенны.
- **Встроенное наследование без доверия** — впервые в блокчейне с конфиденциальностью: автоматическая передача ваших средств без нотариуса, без суда и без раскрытия личности — под замком консенсуса.
- **Гибридная постквантовая устойчивость** — ML-DSA-65 + ML-KEM-768 там, где у Monero, Zcash и всех форков CryptoNote нет ровно ничего.
- **Запрограммированная редкость без управления** — строго конечная эмиссия и излишек страхового фонда, сжигаемый консенсусом, там, где Monero и форки CryptoNote выпускают монеты бесконечно.
- **Нулевая поверхность атаки** — ни смарт-контрактов, ни оракулов, ни кастодиального хранения: ровно та поверхность, которая стоила DeFi миллиарды, устранена по построению.
- **Доказанная платёжеспособность, полная приватность** — гарантирована математически, а не обещана; суммы публичны, личности скрыты на каждом шаге.

PRIVACY BANK CHAIN

«Private money that works for you.»