

Раздел 1: Executive Summary (Обзор проекта)

1.1. Миссия и Видение

Sovereign Bank — это децентрализованная финансовая экосистема (Web3-Bank), созданная для обеспечения полной финансовой автономии пользователей. Наша миссия — предоставить инструменты для свободного распоряжения капиталом в обход ограничений традиционных банковских систем (TradFi), сохраняя при этом удобство повседневных платежей.

Мы строим мост между миром цифровых активов и реальным сектором экономики, где пользователь является единственным владельцем своих средств.

1.2. Проблематика

Современная финансовая система сталкивается с системными вызовами, которые ограничивают права человека на распоряжение собственностью:

Цензура и блокировки: Банки могут заморозить счет без объяснения причин или по требованию третьих лиц.

Инфляционное давление: В ряде стран национальные валюты стремительно теряют покупательную способность.

Сложность трансграничных переводов: Высокие комиссии и длительные проверки делают международную деятельность фрилансеров и релокантов неэффективной.

1.3. Решение: Sovereign Bank

Проект предлагает инфраструктуру, основанную на некастодиальном хранении (non-custodial). В отличие от обычных банков или централизованных бирж, Sovereign Bank не имеет доступа к ключам пользователя. Все активы хранятся на смарт-контрактах в блокчейне.

Ключевые продукты:

Freedom Card: Карта для быстрой регистрации (Email/Telegram) с лимитом до \$1000, обеспечивающая максимальный уровень приватности.

Resident Card: Полнофункциональная карта с процедурой KYC, предлагающая повышенные лимиты и интеграцию с расширенными финансовыми сервисами.

1.4. Экономическая модель и Инвестиции

Проект базируется на устойчивой модели монетизации, включающей плату за выпуск физических/виртуальных карт и транзакционную комиссию в размере 1%.

Запрос на инвестиции: \$335,000 за 15% доли в проекте.

Целевые показатели: Достижение прибыли в размере \$5–7 млн к концу третьего года работы.

Окупаемость (ROI): Прогнозируемый период возврата инвестиций составляет 18–24 месяца.

1.5. Технологический стек (кратко)

Архитектура Sovereign Bank опирается на смарт-контракты (предпочтительно в сетях Ethereum L2 для минимизации комиссий) и защищенный шлюз для взаимодействия с платежной системой Visa. Это позволяет конвертировать стейблкоины в фиат непосредственно в момент совершения покупки.

Раздел 2: Техническая Архитектура (The Stack)

2.1. Выбор блокчейн-инфраструктуры (L2 Solutions)

Для обеспечения скорости транзакций и низких комиссий (Gas fees), Sovereign Bank строится на базе Ethereum Layer 2 (L2) решений.

Основной выбор: Arbitrum или Polygon (zkEVM).

Обоснование: Эти сети обеспечивают высокую пропускную способность (TPS) и минимальные затраты на подтверждение транзакций, что критически важно для работы микроплатежей по картам.

2.2. Некастодиальная логика (Smart Contract Vaults)

В отличие от кастодиальных систем, где банк владеет ключами, архитектура Sovereign Bank строится на базе индивидуальных смарт-контрактов:

User Vault: Для каждого пользователя разворачивается персональный смарт-контракт-хранилище.

Control: Пользователь подписывает разрешение (Approval) для платежного модуля банка только на использование определенного лимита стейблкоинов

(USDT/USDC/EURC).

Ownership: Приватные ключи от кошелька хранятся только у пользователя (через интерфейс Sovereign App или аппаратные кошельки).

2.3. Протокол взаимодействия с платежной системой Visa

Связующим звеном между блокчейном и фиатным миром выступает Hybrid Payment Gateway:

Authorization (Запрос): В момент свайпа карты в POS-терминале, процессинговый центр (через BIN-партнера) запрашивает подтверждение у бэкенда Sovereign Bank.

Oracle Validation: Бэкенд-оракул проверяет баланс в смарт-контракте пользователя в режиме реального времени.

Instant Swap & Settlement: При наличии средств, система инициирует мгновенную конвертацию (через ликвидность DEX или внутренних маркетмейкеров) и подтверждает транзакцию в Visa.

On-chain Settlement: Списание средств со смарт-контракта происходит асинхронно или через предварительно заблокированную ликвидность, чтобы не заставлять пользователя ждать подтверждения блока в блокчейне.

2.4. Backend и API слой

Стек: Go (Golang) или Node.js для высокопроизводительного API.

База данных: PostgreSQL (для хранения метаданных, истории транзакций и зашифрованных пользовательских настроек).

Безопасность: Использование аппаратных модулей безопасности (HSM) для подписи операционных транзакций на стороне шлюза.

2.5. Специфика архитектуры карт

Freedom Card (Privacy Layer): Техническая реализация через виртуальные prepaid-счета (Prepaid bins). Регистрация через Telegram/Email создает уникальный хеш-идентификатор, который не связывает публичный адрес блокчейна с реальной личностью в открытом виде.

Resident Card (Compliance Layer): Интеграция с KYC-провайдером через API. Данные KYC хранятся в зашифрованном виде (AES-256) в защищенном контуре, соответствующем стандартам PCI DSS.

Раздел 3: Механика Карточных Продуктов Этот раздел описывает логику работы двух типов карт, их лимиты и программные интерфейсы (API), через которые происходит управление активами.

3.1. Freedom Card (Уровень конфиденциальности) Freedom Card спроектирована как входной билет в экосистему для пользователей, ценящих приватность и скорость доступа. **Протокол регистрации:** Создание профиля происходит через OAuth-авторизацию Telegram или подтверждение E-mail. Система генерирует внутренний виртуальный идентификатор (UID), который связан с временным кошельком в системе. **Механика анонимности:** Личные данные пользователя не запрашиваются. С точки зрения блокчейна, транзакции проходят через общий пул ликвидности Sovereign Bank, что затрудняет прямую связь между конкретной покупкой в магазине и публичным адресом кошелька пользователя. **Технические лимиты:** * Максимальный баланс/оборот: \$1,000. **Тип карты:** Виртуальная (с возможностью заказа физической без эмбоссирования имени). **Смарт-контракт:** Используется стандартный контракт с жестко закодированным верхним порогом суммы (Hard Cap).

3.2. Resident Card (Уровень комплаенса и высоких лимитов) Resident Card – это полноценный финансовый инструмент для управления крупными капиталами с полным доступом ко всем банковским функциям. **Интеграция KYC/AML:** Технический стек включает API-интеграцию с провайдером верификации (например, Sumsb или Onfido). Процесс проверки полностью автоматизирован в приложении. **Логика смарт-контракта:** После прохождения KYC, статус пользователя в блокчейне обновляется через специальный оракул. Это «разблокирует» функции смарт-контракта, позволяя устанавливать индивидуальные лимиты и работать с суммами свыше \$1,000. **Преимущество:**

Активы пользователя по-прежнему находятся на его персональном смарт-контракте. Банк не может распоряжаться ими, но предоставляет инфраструктуру для их мгновенной траты.

3.3. Сравнительная таблица механизмов

Характеристика :	Freedom Card	ResidentCard
Идентификация :	Telegram / Email	Полный KYC (ID + Selfie)
Хранение данных:	Минимальные метаданные	Шифрованные данные (AES-256)
Лимит (Hard Cap):	До \$1,000	Настраиваемый (высокий)
Тип кошелька :	Упрощенный (Hot Wallet)	Персональный Vault Smart Contract
Контроль ключей:	Non-custodial	Non-custodial

3.4 Процессинг транзакций (Step-by-Step) Для обоих типов карт механика списания выглядит так: Trigger: Запрос от сети Visa при оплате. Logic Engine: Система проверяет тип карты и текущий лимит в базе данных и на смарт-контракте. Authorization: Если лимиты не превышены и баланс в стейблкоинах достаточен, Ledger (внутренняя книга учета) мгновенно подтверждает транзакцию. Conversion: Внутренний маркетмейкер Sovereign Bank обеспечивает мгновенный обмен USDT/USDC на фиатную валюту (EUR/USD/GBP) для расчёта с Visa.

Раздел 4: Безопасность и Протоколы

В этом разделе описываются многоуровневые меры защиты, которые гарантируют сохранность активов и конфиденциальность данных пользователей Sovereign Bank.

4.1. Реализация Non-Custodial управления

Фундаментальный принцип безопасности Sovereign Bank — отсутствие доступа системы к приватным ключам пользователя.

Управление ключами: Мы используем технологию MPC (Multi-Party Computation) или Account Abstraction (ERC-4337). Это позволяет пользователю иметь удобный доступ к кошельку (например, через биометрию смартфона), но при этом сохранять полный контроль над транзакциями.

Social Recovery: Возможность восстановления доступа к смарт-контракту через доверенных лиц или дополнительные факторы аутентификации без участия централизованного сервера, хранящего ключи.

4.2. Безопасность смарт-контрактов

Смарт-контракт — это ядро банка, поэтому к нему применяются высшие стандарты проверки:

Аудит (Security Audits): Перед запуском в основной сети (Mainnet) все контракты проходят двойной аудит в ведущих компаниях (например, CertiK, OpenZeppelin или Hacken).

Формальная верификация: Математическое доказательство корректности логики контрактов для исключения возможности «логических дыр».

Bug Bounty: Постоянная программа вознаграждения для белых хакеров за обнаружение уязвимостей в коде.

4.3. Защита платежного шлюза и транзакций

Несмотря на то, что активы находятся в блокчейне, взаимодействие с сетью Visa требует защиты на стороне бэкенда:

Hardware Security Modules (HSM): Все операционные подписи, подтверждающие конвертацию стейблкоинов для Visa, генерируются в изолированных аппаратных модулях, недоступных для внешнего взлома.

Лимиты и "Автоматический тормоз": Система риск-менеджмента в реальном времени отслеживает подозрительные паттерны (например, сотни транзакций в секунду) и может временно приостановить работу карточного шлюза (не блокируя при этом средства на самом смарт-контракте в блокчейне).

4.4. Стандарты защиты данных (Compliance & Privacy)

PCI DSS: Наша инфраструктура проектируется в соответствии со стандартом безопасности индустрии платежных карт. Данные о картах никогда не хранятся в открытом виде.

Шифрование AES-256: Для пользователей Resident Card личные данные (KYC) хранятся в зашифрованных базах данных с раздельным доступом (Zero-Knowledge подход к хранению данных там, где это применимо).

Privacy Layer (для Freedom Card): Использование миксеров ликвидности или протоколов конфиденциальности, чтобы покупки в офлайне нельзя было напрямую связать с публичным адресом кошелька в эксплорере блокчейна.

4.5. План аварийного восстановления

Emergency Pause: В коде смарт-контракта предусмотрена функция «паузы» для экстренных случаев (только для взаимодействия с картой), которая может быть активирована мультисигом (Multi-sig) управляющего совета.

Self-Custody Exit: У пользователя всегда остается возможность вывести средства напрямую из смарт-контракта на любой другой кошелек через сторонние интерфейсы (например, Etherscan), даже если приложение Sovereign Bank будет недоступно.

Раздел 5: Токеномика и Экономика системы

Экономическая модель Sovereign Bank (Unit-экономика) построена на сочетании традиционных финтех-доходов и эффективности блокчейн-технологий.

5.1. Основные потоки доходов (Revenue Streams)

Проект монетизируется через три основных канала:

Card Issuance Fee (Плата за выпуск):

Freedom Card: Фиксированная плата за активацию виртуальной или выпуск физической карты. Это покрывает затраты на BIN-партнера и логистику.

Resident Card: Более высокая стоимость выпуска, включающая затраты на расширенный KYC и премиальное обслуживание.

Transaction Fee (Транзакционная комиссия):

Единая комиссия в размере 1% с каждой транзакции (покупки). Это основной источник долгосрочного дохода при масштабировании базы пользователей.

B2B и дополнительные сервисы (Перспектива):

Комиссии за кастомизированные решения для корпоративных клиентов, фриланс-бирж и интеграции с мерчантами.

5.2. Математика транзакции (Пример)

Для понимания устойчивости модели рассмотрим транзакцию на сумму \$1,000:

Списание со смарт-контракта: \$1,010 (сумма покупки + 1% комиссия системы).

Распределение комиссии (\$10):

~\$2-3 (0.2-0.3%): Выплата эквайеру, платежной системе Visa и BIN-спонсору (Interchange fees).

~\$1 (0.1%): Затраты на Gas (сетевой сбор блокчейна L2) и оракулы.

~\$6-7 (0.6-0.7%): Чистая прибыль Sovereign Bank.

5.3. Операционные расходы (Burn Rate)

Инвестиции в размере \$335,000 распределяются следующим образом:

R&D (Разработка): 45% — создание и аудит смарт-контрактов, бэкенд шлюза, мобильное приложение.

Compliance & Legal (Юридическое сопровождение): 20% — получение лицензий (EMI/VASP), партнерства с банками-эмитентами.

Marketing (Маркетинг): 25% — привлечение первых 10,000-50,000 активных пользователей (CAC — Cost per Acquisition).

Operations (Операционка): 10% — поддержка инфраструктуры и команда.

5.4. Прогноз масштабирования

Целевая аудитория: Фрилансеры, релоканты, крипто-энтузиасты.

Точка безубыточности: Достигается при достижении объема транзакций (TPV) в размере \$10-15 млн в месяц.

Прогноз на 3-й год: При достижении базы в 100,000 активных пользователей со средним чеком трат \$1,000/мес, годовая выручка составит более \$12 млн, из которых чистая прибыль составит \$5-7 млн.

5.5. Инвестиционная привлекательность (ROI)

Сумма инвестиций: \$335,000.

Доля инвестора: 15%.

Срок возврата инвестиций: 18–24 месяца.

Мультипликатор: Ожидаемая капитализация компании к 3-му году на основе прибыли — \$25–40 млн, что дает инвестору потенциал роста в 10+ раз от вложенного капитала.

ПОДРОБНО: Эта сумма (\$25–40 млн) не взята с потолка. Она рассчитана на основе стандартного финансового метода P/E (Price-to-Earnings) — отношения цены компании к её чистой прибыли, который применяется для оценки финтех-стартапов.

Вот логика расчета, которую мы заложили:

1. База для расчета (Прибыль) Мы опираемся на наш прогноз из раздела 5.4: к концу 3-го года чистая прибыль проекта составляет \$5–7 млн в год.

2. Выбор мультипликатора (P/E Ratio) Для разных индустрий существуют свои средние коэффициенты (мультипликаторы): Традиционные банки: P/E обычно составляет 8x – 12x. Зрелые IT-компании: P/E около 15x – 20x. Высокотехнологичный Финтех и Web3 (на стадии роста): Мультипликаторы могут достигать 20x – 50x (например, как у Revolut или Stripe на пике). Для нашего расчета я взял очень консервативный и реалистичный коэффициент: от 5x до 8x.

3. Математический расчет Нижняя граница: $\$5\,000\,000$ (прибыль) $\times 5$ (коэффициент) = $\$25\,000\,000$. Верхняя граница: $\$7\,000\,000$ (прибыль) $\times 6$ (коэффициент) $\approx \$42\,000\,000$ (округлили до \$40 млн для презентации, чтобы выглядеть более прагматично).

Почему мы выбрали именно такой низкий коэффициент (5x–8x)? Я специально заложил «заниженный» мультипликатор по трем причинам честно и открыто:

а) Снижение рисков: В крипто-индустрии высокие регуляторные риски, поэтому инвесторы часто дисконтируют (снижают) стоимость компаний по сравнению с классическим финтехом.

в) Доверие: Если мы покажем инвестору оценку в \$100 млн (применив мультипликатор 20x), это может выглядеть как «пузырь». Оценка в \$25–40 млн при прибыли в \$5–7 млн выглядит фундаментально обоснованной и дешевой, что делает предложение «335к за 15%» (при оценке в \$2.2 млн на старте) невероятно выгодным для него (потенциал роста в 15–20 раз).

с) Запас для маневра: Если к 3-му году рынок будет «бычьим» (растущим), реальный мультипликатор может быть 15x, и тогда компания будет стоить уже \$75–100 млн. Мы даем инвестору «приятный сюрприз» в будущем.

Раздел 6: Roadmap Разработки (Технический)

Данный план разбит на ключевые этапы, ориентированные на последовательное снижение технологических и регуляторных рисков.

Этап 1: Формирование ядра и Проектирование (Месяцы 1–3)

Рекрутинг: Найм Technical Co-founder (CTO) и формирование костяка команды (Blockchain engineer, Full-stack developer).

Архитектура: Финализация выбора L2-сети (Arbitrum/Polygon) и проектирование архитектуры смарт-контрактов.

Партнерства: Подписание соглашений с BIN-спонсором и платежным шлюзом (Visa partner).

Результат: Развернутая тестовая среда и техническое задание (Spec) для всех модулей.

Этап 2: Разработка MVP и Альфа-тест (Месяцы 4–7)

Smart Contracts: Написание и первичное тестирование контрактов хранилища (Vaults) в тестовой сети (Testnet).

Gateway: Создание прототипа шлюза для авторизации транзакций.

Mobile App (v0.1): Базовый интерфейс кошелька с возможностью депозита стейблкоинов.

Security: Закрытое альфа-тестирование внутри команды и аудит безопасности

первой версии кода.

Результат: Первая успешная транзакция «крипто-фиат» в закрытой среде.

Этап 3: Запуск Freedom Card и Бета-тест (Месяцы 8–12)

Релиз Freedom Card: Запуск виртуальных карт с регистрацией через Telegram/Email.

Интеграция L2: Полный переход на Layer 2 для минимизации комиссий пользователей.

Маркетинг: Привлечение первых 5,000 пользователей для тестирования под нагрузкой.

Результат: Стабильно работающий продукт с лимитами до \$1,000 в публичном доступе.

Этап 4: Масштабирование и Resident Card (Год 2)

KYC Integration: Полноценное внедрение модуля верификации личности.

Релиз Resident Card: Запуск пластиковых карт с высокими лимитами.

Оптимизация: Внедрение Account Abstraction (ERC-4337) для оплаты газа в стейблкоинах (чтобы пользователю не нужно было иметь на счету нативную валюту сети, например ETH).

Лицензирование: Получение собственных финансовых лицензий (EMI/VASP) для снижения зависимости от партнеров.

Результат: Выход на объем транзакций (TPV) более \$5 млн в месяц.

Этап 5: Экспансия и Экосистема (Год 3)

Global Reach: Выход на рынки Латинской Америки, Юго-Восточной Азии и Африки.

B2B API: Запуск шлюза для сторонних компаний (фриланс-биржи, онлайн-шопы), желающих принимать оплату через Sovereign Bank.

Инвестиционные продукты: Добавление возможности стейкинга и получения доходности прямо из приложения (DeFi-интеграция).

Результат: Достижение чистой прибыли \$5–7 млн в год.

Заключение документа

Этот документ представляет собой полное описание проекта Sovereign Bank.

Мы объединили идеологию суверенных финансов с современными банковскими технологиями. С инвестициями в размере \$335,000 и правильно подобранной технической командой, проект готов стать лидером на рынке Web3-банкинга.