

Whitepaper

ForeMetric.ai

Содержание

Глава 1. Что такое ForeMetric: позиционирование, субстрат, честный статус

Глава 2. Проблема и почему сейчас

Глава 3. Решение: Insights-as-a-Service и слои приложения

Глава 4. Фаза 1: TMA-фундамент

Глава 5. Регистрационный контракт и proof-wire

Глава 6. Криптографический слой и приватность

Глава 7. Фаза 2: native app и confidential computing

Глава 8. Фаза 3: децентрализация и federated learning

Глава 9. Токеномика \$HSIG: real yield и иммутабельный расчёт

Глава 10. Конкуренция и рвы

Глава 11. Roadmap, гейты, команда, финансирование, реестр рисков

Приложение А. Глоссарий

Приложение В. Инфраструктурные стоимости по фазам

Приложение С. Приоритетные B2B-сценарии: кто и за что платит

Приложение D. Регистрационный контракт Фазы 1 простыми словами

О СТАТУСАХ И ПРАВИЛАХ ЧТЕНИЯ

Как читать статус-теги:

[PLANNED PHASE 2] / [PLANNED PHASE 3] — проектируется, не реализовано;

[PLANNED PHASE 2 EXPERIMENT — untested, unpriced] — экспериментальный режим Фазы 2: не тестировался, цена не подтверждена;

[PLANNED, not live] — спроектировано, не запущено;

[DESIGN — NOT DEPLOYED] — спецификация контракта до деплоя;

[PLANNED, POST-TGE, no committed date] — после TGE, без даты;

[DESIGN — ILLUSTRATIVE RATIOS] — проектные пропорции, не измеренные;

[PHASE 1 PILOT OFFER] — то, что валидируется сейчас;

[PHASE 1 PILOT OFFER — not yet signed] — валидируемое предложение; ни один пилотный контракт не подписан.

[PROPOSED — NOT AGREED] — предложенное решение или патч вне канона: ожидает подтверждения (ACK) владельцев, не является обязательством.

Три правила чтения документа:

1. Календарных обещаний нет. Переходы между фазами определяют метрические гейты (11.1); все даты в тексте — планировочные оценки с честными статусами, а не обязательства.
2. Суммы, ставки и примеры выплат — иллюстрации. Реальные значения калибруются первыми платными запросами; архитектурные обязательства — пропорции, фиксированные до деплоя.
3. Юридические оценки не проводились. Документ описывает механику и не является юридическим заключением, предложением ценных бумаг или предложением токенов.

КАРТА ЧТЕНИЯ ПО РОЛЯМ

Если вы пользователь.

Что вы делаете: открываете мини-приложение Telegram, подключаете TON-кошелёк и включаете только те сигналы, которые хотите отдавать, — каждый отдельным согласием ; при желании приглашаете друзей, строго на один уровень .

Из чего складывается доход: дневная ставка за включённые сигналы плюс 10% валовой выручки от вклада прямых приглашённых. До TGE баланс — запись IOU-леджера, конвертируемая по курсу, опубликованному до запуска Фазы 1 и неизменяемому после.

Что вы контролируете: включение и выключение каждого сигнала;
срок действия каждого разрешения Signal Passport;
удаление своих данных — уничтожением ключа burn_keys, после которого данные не восстанавливаются.

Что важно знать до включения: доход зависит от платежей покупателей,
а не от эмиссии токенов; разовых бонусов за подключение, серию дней или тапы нет
вывести IOU до TGE нельзя.

Если вы бизнес — покупатель ответов.

Что вы покупаете:

в Фазе 1 — когортные отчёты о вовлечённости (пилотное предложение);

в Фазе 2 — ответы на ваши вопросы через B2B Terminal,
проверенные срезы профилей Signal Passport,
миссии и задачи федеративного обучения.

Чего вы не получаете никогда: сырые векторы, записи об отдельных людях и любую выгрузку данных — экспортного эндпоинта не существует по построению, а не по политике .

Как вы платите: в USDT/TON,

со Фазы 2 каждый платёж делит смарт контракт Revenue Splitter : 80/10/10 .

пилотные платежи Фазы 1 проходят вне контракта и учитываются в IOU-леджере .

Что вы можете проверить: аттестацию защищённых машин и воркеров COCOON —

тем ли кодом и на том ли оборудовании посчитан ваш отчёт .

Если вы инвестор или фонд.

С чего начать: честные статусы , затем гейты и «что нас опровергнет» , затем юнит-экономика платежа, три контура роста без эмиссии (3.7) и честные пределы дизайна, риски.

Ключевые обязательства канона: фиксированный supply без mint , каждая выплата обеспечена выручкой — funded, never minted; переходы между фазами — только прописанные гейты, а не календарь, условия ликвидности публикуются до снапшота TGE .

Расширенная редакция с evidence-реестром, открытыми вопросами дизайна и инфраструктурными стоимостями предоставляется квалифицированным инвесторам в закрытом Data Room по запросу. Запросы — через foremetric.ai.

ТЕЗИС ДЛЯ ИНВЕСТОРА

Что построено. ForeMetric — инфраструктура поведенческих данных с защитой приватности: протокол превращает согласованные сигналы смартфона в доход для людей, которые их производят, и в верифицированные предиктивные инсайты для бизнеса. Покупатель никогда не получает данные — только агрегированный ответ с минимальной когортой 50; экспортного эндпоинта не существует по построению. 80% каждого платежа возвращается источникам сигнала, 10% — одноуровневому рефереру, 10% — казне.

Почему сейчас. Post-cookie дефицит intent-данных оставил покупателей с бюджетом без supply (тест Criteo: до 60% потери таргетинга в протестированном сценарии). Премия за верифицированного человека уже торгуется: Reddit раскрыл \$203M агрегированного лицензирования данных, ручная разметка стоит \$30-50 в час. Confidential computing дошёл до commodity-цен, а Telegram Mini Apps дают consent- и payout-рельсу без трения онбординга. Четыре линии сходятся одновременно — развёртка в 2.4.

Как зарабатываем. B2B-клиенты платят за ответы, а не за данные: когортные отчёты \$1-5K в Фазе 1 [PHASE 1 PILOT OFFER — not yet signed], предиктивные инсайты и верифицированные срезы Signal Passport в Фазе 2, задачи брендов Missions с prepaid-эскроу. Начальный обслуживаемый сегмент — \$25M в год (bottom-up оценка с допущениями, 2.4); якорь масштаба проблемы — рынок дата-брокеража \$278B, построенный на поведении людей без их согласия и без компенсаций.

Где рост. Топливо роста — выручка, а не эмиссия: функции mint() в контракте не существует. Три контура: пожизненная 10% реферальная доля с первого оплаченного пилота; C2C-петля Signal Passport, где каждый опубликованный QR-код — бесплатный билборд протокола [PLANNED PHASE 2]; Oracle-ретеншен, умножающий LTV каждого привлечённого. Контур 1 живёт с первого платного пилота, контуры 2-3 гейтуются доказательством спроса Фазы 1. Полная механика и границы честности — 3.7.

Что уже существует. Публичный прототип foremetric.ai (данные помечены как симулированные), задеплоенный Rust/Axum-бэкенд с PostgreSQL IOU-леджером, Identity Vault на TON Testnet. Ближайшие фальсифицируемые события: закрытая альфа до 500 инвайтов в декабре 2026 с гейтом Day-7 retention $\geq 20\%$; первый платный пилот \$1-5K. Ни один клиент ещё не заплатил — это честный статус, а не слабость позиции: именно его и измеряют гейты.

Что опровергнет позицию. Пять фальсификаторов (11.1): ретеншен-контур, B2B-спрос, компенсационный контур, юнит-экономика аттестованного compute, дифференциация. Каждый привязан к измеримому гейту — фонд проверяет позицию по данным, а не по вере в команду.

Расширенная редакция. Версия с evidence-реестром, открытыми вопросами дизайна и инфраструктурными стоимостями предоставляется квалифицированным инвесторам в закрытом Data Room по запросу через foremetric.ai.

ГЛАВА 1. ЧТО ТАКОЕ FOREMETRIC

1.1 Определение

ForeMetric — инфраструктура поведенческих данных с защитой приватности: протокол, который превращает поведенческие сигналы смартфона в доход для людей, которые их производят, и в верифицированные предиктивные инсайты для бизнеса — без передачи сырых данных кому-либо. Мы строим на TON и стандартной инфраструктуре: стек приватности и confidential computing (AMD SEV-SNP, Intel TDX / COCOON, Qdrant, OpenDP)

относится к инфраструктуре Фазы 2 [PLANNED PHASE 2]; собственный блокчейн, собственную базу данных или собственную фундаментальную модель мы не создаём.

Три стороны одной цепи ценности:

- **пользователи** (consent-опт-ин, доход от сигнала),
- **B2B-клиенты** (ответы на бизнес-вопросы, а не датасеты),
- **AI-лаборатории** (верифицированный человеческий ground-truth против Model Collapse — Фаза 3).

Чем ForeMetric не является. Четыре отрицания на первой странице — чтобы скептик не собирал их по всему тексту; развёрнутые отрицания архитектуры :

Мы не про маркетплейс данных и не витрина «купить базу» — экспортного эндпоинта для сырых векторов не существует по построению, а не по политике.

Не схема с печатью токенов — функции **mint()** в контракте нет; supply фиксирован — 1 000 000 000 \$HSIG при деплое; всё, что получают пользователи, оплачено покупателями.

Не финансовая пирамида — реферальная система строго **одноуровневая**: ровно 10% валовой выручки за вклад прямого приглашённого, второго уровня и дерева нет .

Не новая инфраструктура с нуля — TON, AMD SEV-SNP, Intel TDX / COCOON, Qdrant, OpenDP: мы строим слой доверия поверх стандартного . хорошо зарекомендовавшего себя стека.

1.2 Инсайт, а не датасет

ForeMetric не продаёт данные. Мы продаём ответы на бизнес-вопросы, вычисленные поверх зашифрованных поведенческих векторов внутри аппаратно-аттестованных анклавов (Фаза 2) [PLANNED PHASE 2], с гарантиями дифференциальной приватности на каждом выходе. Клиент получает отчёт: размер когорты, ритм активности, тайминг, кросс-интенты, предиктивные метрики — не CSV, не датасет, не профиль, не персональные данные; исключает ли это ответственность контроллера по GDPR — вопрос

юрконсультации, но проект рассчитывает при реализации отвечать самым строгим нормам по защите приватности и не раскрытии перс.данных своих пользователей.

Экономический факт протокола: 80% gross-выручки каждого B2B-платежа возвращается пользователям, чьи сигналы произвели инсайт; 10% — реферерам (один уровень); 10% — казне. Если у контрибьютора нет реферера, реферальный срез уходит в казну (эффективно 80/20).

Правило зашивается в байткод Revenue Splitter при деплое на mainnet и неизменяемо, сегодня Revenue Splitter — спецификация, не задеплоен.

1.3 Субстрат и слои приложения

ForeMetric — инфраструктура с прикладными слоями, которые активируются последовательно, на одном субстрате:

согласованный сбор →

зашифрованное хранение →

аттестованная обработка (Фаза 2) →

агрегированные ответы без передачи сырых данных.

Четыре слоя приложения, каждый — отдельный продукт на общей рельсе:

B2B Terminal — витрина для бизнеса. Маркетинговая или продуктовая команда платит за ответ на свой вопрос («в какие часы когорта пользователей финтеха наиболее близка к кредитной заявке?»), а не за датасет.

Фаза 1 — когортные отчёты, собираемые командой вручную с раскрытием модели доверия [PHASE 1 PILOT OFFER];

Фаза 2 — аттестованные запросы обычным языком с криптографическим доказательством того, где и как считалось.

Signal Passport — слой, который превращает поведенческий профиль человека в актив: им можно делиться по своим правилам и на своих условиях.

Два режима:

- **B2B** — банк, страховщик, HR-сервис или программа лояльности запрашивает верифицированный срез профиля через явный грант пользователя и платит за каждый запрос; бизнес получает ответ-пригодность (score), а не персональные данные.

- **C2C** — создатель публикует публичный профиль; подписчики платят за вопросы о его реальном поведении («ты действительно тренируешься 5 раз в неделю?», «какой у тебя ритм сна в поездках?»); ответ вычисляется из верифицированного профиля, создатель получает 80% платежа.
Рынок верифицированной аутентичности вместо заявительных слов.

Оба режима — [PLANNED PHASE 2] (режим untested, unpriced — прил. D).

Oracle — личный предиктивный помощник: приложение говорит пользователю не «что было», а «что будет» — пик фокуса сегодня, тренд качества сна, лучшее окно для тренировки завтра. Главный ретеншен-крюк: причина открывать приложение ежедневно, не связанная с балансом [PLANNED PHASE 2].

B2B Missions — бренды ставят задачи реального мира («100K шагов за 14 дней», «посети локацию X») с полным бюджетом наград, внесённым заранее в смарт-контракт; выполнение проверяется сигналами устройства, а не селфи и самозаявлениями; награда

высвобождается автоматически. Для бренда — оплата за доказанное действие, для пользователя — деньги за реальные действия без бюрократии [PLANNED PHASE 2].

Инфраструктурный тезис: после того как субстрат доказан (спрос, ретеншен, аттестация), он открывается внешним разработчикам — персональные AI-агенты и цифровые двойники, запрашивающие поведенческую историю пользователя через наш API с его явного согласия на каждый запрос. Мы не строим эти приложения сейчас; они расширяют тот же субстрат. Начинаем с самого узкого wedge — когортный отчёт \$1-5K — чтобы валидировать спрос до масштабирования любого слоя.

1.4 Три фазы доверия

Доверие в ForeMetric — не обещание, а фаза, у которой есть измеримый гейт входа.

Фаза 1 (сейчас): trusted-operator с раскрытием. DataKey хранится серверно под AWS KMS с аудит-трейлом; tamper-evidence спроектирована как on-chain content-hash батчей (механизм — daily Merkle anchoring [PLANNED, not live]); до запуска anchoring целостность обеспечивается ACID-транзакциями и аудит-логами.

Оператор теоретически может прочитать данные; аппаратная аттестация расшифровки появляется в Фазе 2.

Фаза 2: hardware-attested confidential computing. Расшифровка только внутри зашифрованной памяти AMD SEV-SNP VM; отчётность генерируется в COCOON Intel TDX с независимо верифицируемой аттестацией.

Фаза 3: full decentralization. TON Storage как единственный слой хранения, COCOON как дефолтный compute, децентрализованная аттестация, federated learning.

Переходы между фазами происходят по метрикам (ретеншен, MRR, стабильность аттестации), никогда по календарю; календарные окна — планировочные оценки. Если гейт не пройден — фаза продолжается, и это не провал, а дисциплина.

1.5 Статус на октябрь 2026

Live сегодня: публичный интерактивный прототип foremetric.ai (симулированные данные, помеченные как симулированные); задеплоенный Rust/Axum-бэкенд с PostgreSQL IOU-ledgerом; контракт Identity Vault на TON Testnet.

В разработке: DoH/DoT DNS-сервер (hickory-dns); инфраструктура Daily Merkle Drop [PLANNED, not live]; фронтенд TMA — интеграция регистрационного контракта не завершена и заблокирована финальной ревизией и готовностью бэкенда (детали и рельса альфы — 11.2 и 11.5); текущая тестовая среда и живой API работают на прежней (легаси) схеме регистрации.

Proposed, не Frozen и не задеплоено: общий регистрационный контракт. Freeze-кандидат зафиксирован; дайджест спецификации пересчитывается при любом изменении контракта до фриза; полный текст и conformance-матрица — в закрытом Data Room по запросу. Это спецификация и conformance-тулинг, не верифицированный пользовательский registration-флоу.

Не начато по дизайну: native app, TEE-деплой, TGE, автоматические on-chain выплаты, Signal Passport, Missions, Oracle, FL — всё гейтуется доказательством спроса Фазы 1.

Коммерческий статус: закрытая альфа до 500 инвайтов планируется на декабрь 2026 с гейтом Day-7 retention $\geq 20\%$. Первый платный пилот \$1-5K [PHASE 1 PILOT OFFER — not yet signed] — валидируемая гипотеза Фазы 1. Пилоты Фазы 1 по дизайну — founder-operated, disclosed trusted-operator; методология отчётов — Приложение С.

1.6 Инварианты, которые не меняются ни в одной фазе

1. Никакой продажи сырых датасетов: экспортного эндпоинта векторов не существует.
2. Граница COCOON: воркеры получают только текст запроса и анонимизированные агрегаты — никогда DataKey, сырые векторы, идентичность. COCOON — compute-only, никогда storage.

3. Single-level referral: 10% прямого реферала, навсегда; никаких вторых уровней и командных бонусов.
4. Никакой необеспеченной эмиссии: в проекте токен-контракта `mint()` отсутствует; при деплое на TGE фиксируется неизменяемый байткод и фиксированный supply 1B \$HSIG; каждая выплата обеспечена реальной B2B-выручкой через DEX-buyback [PLANNED, POST-TGE, no committed date]. Единственное проектируемое исключение — миссии под 100% prepaid-эскроу спонсора [PLANNED PHASE 2].
5. Crypto-shredding: `burn_keys()` уничтожает DataKey практически моментально (~5 секунд, TON block finality); GDPR Article 17 требует стирания «без неоправданной задержки»; целевые задержки нашего каскада удаления приведены в 6.3.
6. Message Metadata не существует ни в одном артефакте; CI валит любую сборку со ссылкой на legacy-категории.
7. Границы фаз: модели доверия Фазы 1 и Фазы 2 не эквивалентны; Фаза 1 — disclosed trusted-operator.

ГЛАВА 2. ПРОБЛЕМА И ПОЧЕМУ СЕЙЧАС

2.1 Синтетическая энтропия: Model Collapse

AI-модели деградируют, когда обучаются на собственном синтетическом выходе. Shumailov et al. (Nature, 2024) показали прогрессивную деградацию — потерю хвостов распределений и миноритарных мод — при рекурсивном обучении моделей на сгенерированных ими же данных. Прогнозы указывают на растущую долю синтетического контента в вебе; мы сознательно не приводим конкретный процент как факт: оценки расходятся по методологиям. Практическое следствие для покупателей данных: верифицированный человеческий сигнал становится самым дефицитным входом цифровой экономики. Каждое следующее поколение моделей повышает премию за не-синтетический поведенческий ground-truth.

2.2 Деградация supply intent-данных

Рекламный и fintech-acquisition стек десятилетиями строился на пассивном трекинге: third-party cookies, device fingerprinting, мобильные идентификаторы до ATT. 2024-2025 годы закрыли эту эпоху. Тест Criteo (июнь 2024) показал среднее падение выручки пабlishеров на 60% в протестированном сценарии замены cookies; сворачивание планов полной депрекации third-party cookies оставило рынку дорогой и деградировавший статус-кво. Intent-данные — сигнал «что этот человек сделает дальше» — не стали менее ценными для покупателя. Они стали менее доступными и менее легальными. Consumer-fintech команды аквизиции, ведущие кампании внутри Telegram, потеряли таргетинг-сигнал, который их стеки производили раньше.

2.3 Эрозия ценности: источник не получает ничего

Экономика поведенческих данных уже существует и велика: рынок data-brokerage \$278B (2024, Grand View Research); глобальные рекламные расходы \$1T+, из них ~73% digital (GroupM, декабрь 2024); рынок AI training datasets \$3.2B (2025, Grand View Research). В каждом из этих потоков человек, породивший исходный сигнал, не получает ничего: ни согласия, ни доли, ни resource. Брокеры продают профили, собранные из поведения, которое люди не соглашались продавать; платформы монетизируют attention-граф как инвентарь; AI-лаборатории лицензируют агрегированные корпуса, чья provenance-цепочка заканчивается соскрёбанным личным контентом.

Эти рынки пересекаются, и складывать их нельзя. Мы приводим их как контекст размера проблемы, а не как оценку нашего рынка: собственная bottom-up оценка обслуживаемого сегмента — в 2.4, и она сознательно консервативна.

Премия за верифицированного человека уже priced in: Reddit раскрыл \$203M агрегированного лицензирования данных (SEC Form S-1); человеческая разметка продаётся по \$30-50 в час. Рынок платит за человеческий сигнал — он просто платит всем, кроме людей.

Источники рыночных цифр :

[Shumailov et al. — AI model collapse, Nature \(2024\).](#)

[Grand View Research — Data Broker Market Report.](#)

[Grand View Research — AI Training Dataset Market.](#)

[WPP Media \(GroupM\) — This Year Next Year, декабрь 2024.](#)

[Reddit, Inc. — форма S-1, SEC EDGAR.](#)

[TechCrunch — о лицензировании данных Reddit.](#)

2.4 Почему сейчас: четыре сходящиеся линии

Demand-side. Post-cookie деградация intent-данных оставила покупателей с бюджетом и без supply (Criteo: 60% в протестированном сценарии).

Price-side. Верифицированные человеческие данные уже торгуются с премией (Reddit \$203M; разметка \$30-50/час) — бюджетная строка существует и измерима.

Tech-side. Confidential computing дошёл до commodity-цен: AMD SEV-SNP bare-metal и COCOON Intel TDX воркеры делают режим «расшифровка только внутри аттестованной памяти» подъёмным для стартапа [PLANNED PHASE 2].

Distribution-side. Telegram Mini Apps дают дистрибуцию внутри Telegram с wallet-anchored идентичностью с первой сессии — consent- и payout-рельса на TON без трения онбординга.

Bottom-up оценка обслуживаемого рынка начального сегмента, помеченная как допущение: ~500 достижимых consumer-fintech и retail команд аквизиции в первый год × допущенные \$50K/год = \$25M. Сознательно консервативно: считаем только wedge, достижимый через Telegram-native кампании, а не весь брокеражный рынок в \$278B.

2.5 Честные границы проблемной рамки

Цифры выше доказывают три вещи: бюджетная строка на человеческий поведенческий сигнал существует; supply согласованных intent-данных деградировал; люди, производящие сигнал, не получают ничего. Они не доказывают: что конкретный

покупатель заплатит \$1-5K за наш конкретный отчёт; что per-contributor доход будет осмысленным на масштабе альфы; что Model Collapse создаёт покупательскую срочность к конкретной дате. Это гипотезы Фазы 1, и закрытая альфа декабря 2026 с гейтом Day-7 retention $\geq 20\%$ и первым платным пилотом — способ их проверить.

ГЛАВА 3. РЕШЕНИЕ: INSIGHTS-AS-A-SERVICE И СЛОИ ПРИЛОЖЕНИЯ

3.1 Пайплайн от сигнала до ответа

Пять стадий, каждая со своей фазовой границей.

1. Consented-сбор. Пользователь opt-in через Telegram Mini App (**Фаза 1**) или native app (Фаза 2) и тумблерами выбирает категории сигналов.

Скоуп Фазы 1 жёстко ограничен: TMA session events (open/close timestamps, navigation patterns, signal toggle interactions) плюс опциональные DNS intent-сигналы при ручной конфигурации — и ничего сверх этого.

Фаза 2 добавляет мультимодальный on-device сбор: инерциальные сенсоры, теги галереи, ambient audio labels, Wi-Fi контекст [PLANNED PHASE 2].

2. Векторизация.

Фаза 1: серверная векторизация session-телеметрии под disclosed trusted-operator моделью.

Фаза 2: векторизация на устройстве в Rust Core; сырые сенсорные данные никогда не покидают телефон — наружу уходит только зашифрованный вектор [PLANNED PHASE2].

3. Зашифрованное хранение.

Фаза 1: AWS S3 под disclosed trusted-operator с KMS-аудит-трейлом; целостность

сегодня — ACID-транзакции леджера и аудит-логи; on-chain content-hash tamper-evidence спроектирована и не live [PLANNED, not live].

Фаза 2: гибрид S3 hot-tier (<30 дней) + TON Storage cold-tier (>30 дней).

Фаза 3: только TON Storage.

COCOON — compute-only, никогда слой хранения, ни в одной фазе.

4. Обработка.

Фаза 1: PostgreSQL-агрегации, founder-operated отчёты, без аппаратной аттестации, с явным раскрытием модели доверия.

Фаза 2: трансляция natural-language запроса внутри AMD SEV-SNP confidential VM (local-first Phi-3-mini), cohort search по зашифрованным Qdrant-векторам, дифференциальная приватность на выходе, генерация отчёта внутри COCOON Intel TDX с client-verifiable аттестацией [PLANNED PHASE 2].

Фаза 3: federated learning задачи на COCOON-воркерах [PLANNED PHASE 3].

5. Ответ и выплата. Покупатель получает отчёт-ответ; 80% gross-выручки платежа маршрутизируется контрибьюторам через Revenue Splitter (с TGE; в Фазе 1 сплиттер не задеплоен — механика контрибьюторской доли пилотных платежей до TGE); 10% — рефереру (один уровень); 10% — казне; при отсутствии реферера реферальный срез уходит в казну (эффективно 80/20).

3.2 Граница: ответ, а не датасет

Клиент получает: размер когорты, ритм активности, тайминг, кросс-интент паттерны, предиктивные метрики и (в Фазе 2) аттестационный отчёт о вычислении.

Клиент никогда не получает: сырые векторы; индивидуальные профили; экспортный эндпоинт (он не существует по построению);

Message Metadata (не существует ни в одном артефакте протокола).

Гарантии на выходе [PLANNED PHASE 2]: дифференциальная приватность $\epsilon=x.0$ на B2B-выходах; минимальная отчётная когорта — 50 пользователей; запрос ниже порога

возвращает агрегированный отказ, а не ослабленный ответ с меньшим шумом.

В Фазе 1 выходы — founder-operated агрегаты без формальной DP-механики; формальная DP появляется в Фазе 2.

Клиент не получает персональных данных и профилей. Оценка того, исключает ли это ответственность контроллера по GDPR, требует юрконсультации; мы утверждаем только архитектурный факт — экспортного эндпоинта персональных данных не существует по построению. Приватность здесь — свойство архитектуры, а не комплаенс-слой поверх продажи данных.

3.3 Слои приложения, активируемые последовательно

B2B Terminal. Витрина протокола для бизнеса: место, где маркетинговая команда покупает ответ на свой вопрос, а не данные. Два контура запросов, оба aggregate-only. Первый — отчёт по всему массиву активной панели: ритм активности, тайминг, переходы между категориями; это продукт пилотов Фазы 1 — пока панель мала, узкие сегменты статистически нечестны.

Второй — запрос по ограниченной выборке: сегмент по категориям сигналов, гео-кластерам (geohash-6), временным окнам и кросс-интентам — включается по мере роста плотности сигналов.

В обоих контурах действует жёсткий минимум отчётной когорты 50: запрос ниже порога возвращает агрегированный отказ, а не ослабленный ответ с меньшим шумом.

Фаза 1 — founder-operated, disclosed trusted-operator [PHASE 1 PILOT OFFER];

Фаза 2 — аттестованные natural-language запросы: покупатель пишет вопрос обычным языком, протокол исполняет его внутри анклавов и возвращает отчёт с предиктивными метриками, TDX-quote и формальными DP-гарантиями [PLANNED PHASE 2].

Полный путь запроса — 7.6; кто и за что платит — Приложение С.

Signal Passport. Слой, который превращает поведенческий профиль человека в актив: делиться им можно по своим правилам и на своих условиях.

Два вектора с общей базой: грант — подписанный Ed25519-объект ~112 байт

{grantee, category-scope, TTL, nonce};

три уровня отзыва (грант, категория, глобальный burn); журнал выдач и отзывов, видимый пользователю.

B2B-вектор — верифицированный срез вместо заявительных данных: банк, страховщик, HR-сервис или программа лояльности запрашивает category-bounded срез профиля; совпадение вычисляется в аттестованном анклав над зашифрованными данными; бизнес получает ответ-пригодность (score), не профиль и не сырые записи; 80% платежа уходит пользователю.

Экономика вектора — регулярные андеррайтинговые и комплаенс-бюджеты: контрактная цена за запрос и повторяемость покупок; поведенческий сигнал точнее заявительного — люди переоценивают свою дисциплину, датчики и анализ поведенческого следа пользователя — нет.

C2C-вектор: Creator-Led Distribution и рынок верифицированной аутентичности.

Signal Passport в C2C-режиме — это не просто утилита, это инструмент вирального захвата аудитории через лидеров мнений (Creator-Led Distribution), работающий по модели «нового типа донатов» и выступающий «Троянским конём» для масс-маркета. Создатель (блогер, селебрити, эксперт) публикует QR-код своего верифицированного профиля с тумблерами категорий. Его аудитория сканирует код и платит микро-платежи за вопросы к его реальному поведенческому следу («Действительно ли ты тренируешься 5 раз в неделю?», «Какой у тебя реальный ритм сна?»). Ответ вычисляется в анклав из верифицированного профиля — только по открытым категориям и только в агрегированной форме, без сырых записей; 80% платежа уходит создателю, далее стандартный сплит 10/10 [PLANNED PHASE 2 EXPERIMENT — untested, unpriced].

Виральная петля (K-factor > 1):

Фанат приходит за ответом от кумира (платный запрос).

Фанат видит работающую экономику и генерирует свой собственный QR-код, чтобы монетизировать свою аудиторию.

Каждый опубликованный в соцсетях QR-код становится **бесплатным билбордом ForeMetric.**

Инвестиционный смысл и экономика: плательщик — физлицо, чек микро, цену задаёт создатель. Мы получаем потребительский охват (B2C) без затрат на пользовательский маркетинг. Аудиторию приводят сами создатели, мотивированные прямым доходом от B2C-микро-транзакций, которые обеспечиваются архитектурой (80% сплит), а не эмиссией. Каждый опубликованный QR — бесплатный канал привлечения: протокол не выкупает трафик. B2B несёт выручку, C2C несёт аудиторию — механика грантов и граница анклава у векторов общие. Пошаговая механика и экономика обоих режимов — 7.8.

Oracle. Личный предиктивный помощник: приложение говорит пользователю не «что было», а «что будет». Утренний брифинг из коротких предсказаний и советов дня: «фокус-пик сегодня 14:00–16:00», «качество сна трендит вниз третью неделю, окно восстановления до 23:00», «лучшее окно для тренировки завтра 7:00–8:30».

Почему он знает больше самого пользователя: персональная on-device модель видит регулярности, которые внимание не фиксирует, — корреляции DNS-интентов с временем суток, ритма сессий со сном, мобильности с покупками; когортный базис добавляет сравнение «как такой ритм развивается у похожих людей», прошедшее дифференциальную приватность и порог когорты 50. Каждое предсказание несёт калиброванную уверенность и цитаты — какие категории сигналов и какой когортный базис внесли вклад; предсказание без цитат не рендерится: это свойство кода, а не политика. Oracle category-bounded: медицинские диагнозы и юридические выводы вне его поверхности по построению. Чем больше людей на рельсе, тем выше достоверность предсказаний для каждого — сетевой эффект, встроенный в продукт; главный ретеншен-крюк протокола: причина открывать приложение ежедневно, не связанная с балансом.

Дни использования конвертируются и в точность персональной модели, и в плотность сигнала для B2B-запросов [PLANNED PHASE 2]. Механика и границы — 7.7.

B2B Missions. Бренды коммисионируют задачи реального мира с деньгами, заранее внесёнными в prepaid-эскроу: «100K шагов за 14 дней», «посети локацию X и верифицируй». Миссия начинается с бюджета: смарт-контракт держит 100% наград с момента публикации — ни бренд, ни протокол не могут их изъять или перенаправить. Выполнение проверяется сигналами устройства — шаги инерциальными сенсорами и PoB-подписью, локация geohash-достижением, правдоподобность темпоральной проверкой, — а не селфи и самозаявлениями; награда высвобождается контрактом по верификации, неиспользованный остаток возвращается спонсору. Для бренда это оплата доказанного действия, для пользователя — доля токенов за реальные действия без бюрократии. Миссии — единственное проектируемое исключение из правила «никакой необеспеченной эмиссии»: каждый токен награды покрыт деньгами спонсора в эскроу — funded, never minted [PLANNED PHASE 2]. Механика — 7.9.

Правило активации: каждый слой включается только после того, как предыдущий доказал спрос метрическим гейтом (Глава 11). Слои не запускаются «на всякий случай» — сначала рельса доказывает, что за ответы платят, и только затем каждый слой расширяет обе стороны протокола: приток людей (Oracle как ежедневная личная ценность, Missions как деньги за действия, C2C-Passport как заработок создателей и виральный двигатель) и приток выручки (Terminal, B2B-гранты, миссии, открытый API).

Слои — это то, ради чего пользователи приходят и остаются и за что бизнес платит; субстрат — то, что делает это возможным без продажи данных, сам фундамент проекта.

3.4 Инфраструктурный тезис

После того как субстрат доказан — спрос, ретеншен, верифицируемая аттестация — он открывается внешним разработчикам: персональные AI-агенты и цифровые двойники, запрашивающие поведенческую историю пользователя через наш API с его явного согласия на каждый запрос. Мы не строим эти приложения сейчас и не обещаем их в

roadmap-датах: они расширяют тот же субстрат, ту же enclave-границу и ту же экономику 80%.

Как это устроено экономически. Сторонний проект не покупает «доступ к данным» — такого товара не существует ни в одной фазе. Он оплачивает каждый конкретный запрос, и платёж проходит по смарт-контракту через Revenue Splitter: 80% суммы уходит людям, чьи сигналы дали вклад в ответ, 10% — их реферерам, 10% — казне протокола. Механика едина для всех: неважно, кто задал вопрос — наш B2B-терминал, бренд или чужое приложение, — источник сигнала получает свою долю всегда. Платёжная рельса TON делает модель рабочей даже для небольших сумм и потока мелких запросов: комиссия не съедает экономику запроса.

Пример. Команда строит персонального AI-планировщика дня. Чтобы он по-настоящему понимал ритм человека, нужны годы поведенческой истории, а собирать их с нуля — дорого, долго и юридически рискованно. Вместо этого разработчик подключается к ForeMetric API: пользователь видит запрос, даёт согласие на конкретный тип доступа, приложение получает ответ, а пользователь получает свою долю с каждого запроса. Сторонний продукт выходит на рынок за недели, а не годы; ForeMetric для поведенческих данных становится тем, чем Twilio стал для коммуникаций и Cloudflare для доставки контента — слоем, который арендуют, а не строят.

Отсюда позиционирование: ForeMetric — инфраструктура сначала, продукт вторым. Wedge Фазы 1 валидирует рельсу; рельса несёт экосистему; экосистема создаёт несколько потоков выручки, которые обеспечивают токен-экономику реальным доходом, а не эмиссией. Маховик замыкается на внешних разработчиках: каждый новый внешний сервис увеличивает спрос на сигналы, растут выплаты пользователям, растёт причина подключаться, плотность сигналов растёт, качество ответов растёт — и экосистема притягивает следующий сервис. Экономика открытого API и его границы — Приложение C.5.

3.5 Реферальная система: один уровень, один контракт, двигатель роста

Реферал в ForeMetric — протокольный контур роста, а не маркетинговая программа:

связь «пригласивший ↔ приглашённый» фиксируется регистрационным контрактом как отношение 1:1 и никогда не становится деревом. Реферер получает 10% валовой выручки, атрибутированной прямому приглашённому, — навсегда.

Второго уровня, рангов и командных бонусов нет структурно: Revenue Splitter не содержит типов данных, способных отслеживать second-degree связи .

Контрактная связь и активация. Реферальное намерение записывается при первой успешной регистрации — окно закрывается перманентно в этот момент.

Начисления активируются только после `wallet_verified=true`; до этого интерфейс показывает «реферал записан — активация после верификации кошелька».

Не MLM. Доход участника зависит от выручки, которую принёс его прямой приглашённый, а не от притока новых участников: источник доходности — B2B-спрос и бюджеты миссий, а не взносы входа. Юридически и экономически это revenue-sharing протокол, не пирамида; правило зашивается в байткод при деплое и после деплоя не может быть изменено.

Двигатель роста Фазы 1. Acquisition в Telegram идёт через deep-links с префиксом `ref_<code>`: коды — 4-60 URL-safe ASCII символов, гарантированно помещающиеся в 64-символьный start-параметр Telegram .

Вознаграждение за рост выплачивается только из реальной выручки, поэтому виральный контур самофинансируем с первого оплаченного пилота и масштабируется вместе со спросом, а не вместе с маркетинговыми расходами: каждая приглашённая когорта снижает предельную стоимость привлечения следующей. Это расчётный двигатель вирального роста Фазы 1 — без рекламного бюджета и без структуры MLM.

Матрица конфликтов. Тот же реферальный кандидат при свежем ключе даёт 200 по-ор; другой кандидат после закрытия окна — 409 REFERRAL_CONFLICT; отсутствие кандидата

сохраняет состояние; конфликты не являются echo-кодами.

Это строки матрицы регистрационного контракта (Proposed, freeze-кандидат); полная семантика — 5.3, математика сплита — 9.3.

3.6 Экономическое замыкание решения

Пайплайн замыкается в простую петлю: бизнес платит за ответ → ответ вычисляется поверх согласованных сигналов → 80% gross платежа возвращается источникам сигнала → источники сигнала получают причину продолжать opt-in и расширять consent → качество и плотность сигналов растут → ответы становятся точнее → бизнес платит больше. Полная токеномика петли — в Главе 9; детали и ограничения Фазы 1 — в Главе 4; криптографический контур, делающий петлю проверяемой, — в Главе 6.

3.7 Рост без эмиссии: три контура и ответ на возражение фонда

Возражение, которое формулирует почти каждый крипто-фонд: «Без раздач токенов нет бесплатного вирального топлива, которым обычно разгоняют крипто-проекты. Рост будет медленным и честным. Готов ли фонд ждать?» Настоящий раздел отвечает на него прямо. Топливо роста у ForeMetric — не эмиссия, а выручка: функции mint() в контракте не существует, поэтому проект не может купить показной рост, даже если захочет, — и мы считаем это проектной фичей, а не ограничением. Эмиссия оплачивает клик, выручка оплачивает мотивацию: клик умирает вместе с кампанией, мотивация растёт вместе с протоколом. Рост без эмиссии — не «медленнее, зато честнее»: он дешевле по природе, потому что издержка привлечения встроена в каждый платёж, и прочнее, потому что мотивация участника привязана к потоку, а не к разовому событию.

Контур 1 — реферальный (Фаза 1, с первого оплаченного пилота; механика — 3.5). Deep-link с префиксом ref_<code>, запись связи «пригласивший ↔ приглашённый» при первой регистрации — окно закрывается навсегда, — и 10% валовой выручки прямого приглашённого — навсегда. Экономическое отличие от bounty-раздач: разовый бонус оплачивает факт клика и прекращает действовать вместе с кампанией; реферальная доля

оплачивает поток выручки и дорожает вместе с протоколом. Приглашающий строит не «команду» (уровень ровно один — дерево структурно невозможно), а портфель пожизненных потоков, каждый из которых растёт с ростом B2B-спроса. Мотивация, привязанная к потоку, а не к событию, не распадается со временем — виральный коэффициент копится, а не сгорает. Наглядный калькулятор реферальной доходности доступен на сайте протокола.

Контур 2 — креаторский (Фаза 2, Signal Passport C2C — 3.3, 7.8). Создатель публикует QR-код верифицированного профиля; аудитория сканирует его и платит за вопросы к его реальному поведенческому следу; 80% платежа уходит создателю [PLANNED PHASE 2 EXPERIMENT — untested, unpriced]. Петля: фанат приходит за ответом → видит выплату 80% → генерирует собственный QR → его аудитория видит QR → цикл повторяется. Каждый опубликованный код — бесплатный билборд протокола; каждая выплата — публичное доказательство работающей экономики. CAC протокола в этой петле равен нулю: дистрибуцию покупают сами участники, потому что монетизируют её лично. Если в контур заходит медийная величина, её QR делает для протокола то, что для веба сделала кнопка «Поделиться»: превращает внимание в дистрибуцию [PLANNED PHASE 2].

Контур 3 — ретеншен-мультипликатор (Oracle — 3.3, 7.7). Oracle не приводит пользователей — он умножает ценность каждого приведённого: ежедневная личная польза, не связанная с балансом, конвертирует привлечённого пользователя в долгоживущий источник сигнала и реферальных потоков. В терминах фонда: контуры 1 и 2 снижают CAC, контур 3 поднимает LTV; вместе они управляют единственным соотношением, по которому фонд судит рост, — LTV/CAC .

Экономика сравнения. Эмиссионный разгон: протокол платит за привлечение разводнением; пользователь приходит за раздачей, а не за продуктом; после окончания раздач retention падает к нулю, и DAU повторяет кривую «пик на TGE — обвал после». Это покупка метрики, а не рост. Реферально-креаторский разгон: издержка привлечения встроена в unit-economics каждого платежа — 10% реферального среза плюс 80%

пользователю означает, что 90% каждого платежа уходит участникам рынка; это структура биржи, а не SaaS. Бюджет на рост возникает только вместе с выручкой и не может опередить её: он не сжигает runway и не создаёт понзи-хвост. Скорость роста становится функцией реального B2B-спроса: каждый платёж увеличивает выплаты → выплаты увеличивают мотивацию звать → приглашения увеличивают плотность сигналов → плотность улучшает ответы → ответы увеличивают выручку. Рост и выручка — одна петля (3.6), а не две несвязанные траектории.

Бенчмарки. Реферальная программа PayPal (бонусы \$10-20 за нового пользователя) в 1999-2000 держала базу на темпах до 7-10% в день и стоила дешевле любого платного канала привлечения (Eric Jackson, The PayPal Wars, 2002). Крупнейшие DeFi-протоколы набрали аудиторию без рекламных бюджетов: участников приводил доход, который платила сама механика ликвидности. ForeMetric применяет тот же принцип к поведенческим данным: доход, который платит экономика каждого B2B-платежа, — единственное виральное топливо, не требующее mint().

Ответ на «готов ли я ждать». Фонду не нужно ждать на вере: контуры наблюдаемы, а фальсификаторы названы (10.7, 11.1). Если реферальный контур не даёт динамики, это видно в измеряемых метриках — K-фактор реферального контура, доля опубликованных QR, Day-7/Day-30 retention — и проект итерирует механику, не имея при этом возможности купить показной рост: mint() не существует. Если контуры работают, они разгоняются от первых же пилотных платежей: каждый платёж создаёт выплаты, каждая выплата — видимый кейс для следующего приглашения. Эмиссия в этой картине не ускорила бы рост, а скрыла бы его отсутствие: квартал красивого DAU ценой разводнения навсегда. Для фонда отсутствие mint() — не минус, а защита от главного способа сжечь токен-экономику до проверки спроса.

Границы честности. Реферальный контур живёт с первого оплаченного пилота Фазы 1, но выплаты до TGE — записи IOU-леджера, а не он-чейн транзакции (9.6); контрактная гарантия сплита включается деплоем Revenue Splitter [PLANNED, POST-TGE, no committed

date]. Креаторский и ретеншен-контур — [PLANNED PHASE 2] и гейтуются доказательством спроса Фазы 1 (11.1). K-factor > 1 для C2C-петли — проектная гипотеза, а не измеренный факт: у режима нет цены и нет подтверждённого спроса (7.8). Холодный старт остаётся риском: до первых платежей цикл не крутится — гейт альфы декабря 2026 и есть честная проверка стартового плеча.

ГЛАВА 4. ФАЗА 1: ТМА-ФУНДАМЕНТ

4.1 Почему сначала Telegram Mini App

Фаза 1 сознательно не строит дорогую часть протокола. Её задача — доказать три вещи минимальной ценой: что люди дают осознанный consent на сбор поведенческих сигналов; что они возвращаются (ретеншен); что бизнес платит за агрегированный ответ. Telegram Mini App даёт для этого три рельсы сразу: дистрибуцию внутри Telegram без установки отдельного приложения, кошелек-anchored идентичность с первой сессии через TON Connect, и платёжную рельсу TON на будущее. Инфраструктурный принцип фазы: сначала дешёвая проверка спроса, затем капитальные затраты на attested-контур. Обратный порядок — строить TEE до доказательства спроса — мы считаем ошибкой распределения runway.

4.2 Точный скоуп сигналов Фазы 1

Собирается ровно две категории и ничего сверх:

TMA session events: open/close timestamps, navigation patterns внутри мини-аппа, взаимодействия с тумблерами сигналов.

DNS intent-сигналы (опционально, только при ручной конфигурации пользователем): категории доменов верхнего уровня из DNS-запросов, прошедших через наш DoH/DoT-сервер.

Не собирается в Фазе 1 и не собирается никогда без явного тумблера Фазы 2: геолокация, галерея, аудио, Wi-Fi окружение, содержимое переписок, история браузера вне ТМА, поисковые запросы как таковые. Legasy-категории старого позиционирования («Browsing

History», «Search Queries», «App Usage», «Location History», «Message Metadata») удалены из протокола: Message Metadata не существует ни в одном артефакте, а CI валит любую сборку, ссылающуюся на legacy-имена. Честное название категории важнее маркетингового: пользователь видит в UI ровно то, что собирается.

4.3 Онбординг и UX

Целевой онбординг — до 30 секунд: открытие ТМА из Telegram, экран consent с тумблерами категорий, подключение TON-кошелька (zero gas для пользователя, без seed-фраз в нашем контуре), дашборд с баланс-тикером. Баланс Фазы 1 — pre-token IOU-кредиты в PostgreSQL-леджере с ACID-гарантиями против double-crediting; конвертация 1:1 в \$HSIG на TGE [PLANNED, POST-TGE, no committed date]. Экран сигналов показывает текущую ставку и активные тумблеры; реферальный экран — одну ссылку, один уровень, 10% навсегда, с явной пометкой, что активация реферала произойдёт только после wallet-верификации (Глава 5).

4.4 DNS-щит и его границы

DNS-канал построен как privacy-щит, а не как инструмент наблюдения: трафик идёт только по DoH/DoT; сервер видит категории доменов, не содержимое страниц; сырые логи не сохраняются сверх окна агрегации; пользователь может выключить канал одним тумблером в любой момент. Классификация двухуровневая: Tier 1 — детерминированный Trie-словарь категорий; Tier 2 сегодня — детерминированный keyword-эвристика вместо модельного API. Серверный TinyBERT-классификатор — [PLANNED, not live]; запуск ждёт размеченных данных. Границы канала формулируются явно: категории, не страницы; частотность и время суток, не keystrokes; отключаемость без последствий для базовой ставки.

Платформы DNS-канала Фазы 1. Ручная конфигурация доступна на Android (Private DNS, DoT) и десктопе; отдельное iOS-приложение-компаньон для DoH отклонено для Фазы 1: Network Extension entitlements такого профиля — практически гарантированный риск отказа App Review, а установка профиля .mobileconfig/MDM ломает гейт онбординга до 30 секунд (4.3). Пользователи iOS в Фазе 1 остаются на базовой ставке событий сессии ТМА

без потери согласия и баланса; автоконфигурация DNS-канала входит с нативным приложением Фазы 2. Принятие DNS-канала в Фазе 1 — допущение дизайна, а не обязательство протокола: фактический уровень принятия канала калибрует экономику сигналов Фазы 2 и не меняет скоуп Фазы 1.

4.5 Хранение и tamper-evidence Фазы 1

Векторы и агрегаты Фазы 1 хранятся в AWS S3 под disclosed trusted-operator моделью: DataKey серверный, под AWS KMS с аудит-трейлом каждого доступа. Тампер-evidence спроектирована как on-chain content-hash каждого батча, фиксируемый в daily Merkle-транзакции; [PLANNED, not live]. До её запуска целостность обеспечивается ACID-транзакциями и KMS-аудит-логами. Ограничение фазы: оператор теоретически может прочесть данные; криптографическое исключение такой возможности появляется только с Фазой 2 (Глава 6-7). Ограничение раскрыто в privacy-политике и UI-баннере.

4.6 Антифрод как детерминированные правила

Антифрод Фазы 1 — три детерминированных правила, без ML: верификация initData HMAC от Telegram; per-user rate limits на начисления; проверка темпоральной равномерности сессий ($CoV < 0.1$ отклоняет скриптованный трафик). Никакой «AI-модели антифрода» в Фазе 1 нет. Proof-of-Behavior (1D-CNN по инерциальным сигналам) — [PLANNED PHASE 2], с целевым FPR $\leq 2\%$ на attested-human holdout как гейтом фазы, а не как текущим свойством (бюджет FNR — открытый вопрос).

4.7 Экономика сигналов Фазы 1

Видимые ставки Фазы 1 [DESIGN — ILLUSTRATIVE RATIOS]: базовая 5.0 \$HSIG/день (в IOU-эквиваленте) за session-события и +3.0/день за включённый DNS-канал. Полный стек ставок (location +1.5, Wi-Fi +1.0, shopping +0.67, app patterns +0.33, visual +4.0, ambient +4.0, cap 19.5/день) — экономика Фазы 2: пропорции проектные, не измеренные, калибруются по реальной B2B-выручке на запуске Фазы 2. Начисления — pull-модель с ACID-транзакциями леджера; реферальные 10% начисляются в учёт, но активируются только после wallet_verified=true. Ни одна цифра дохода пользователя не обещается в

маркетинге: конкретные суммы станут известны только после первых реальных B2B-платежей.

4.8 Что Фаза 1 доказывает и чего не доказывает

Доказывает: consent-UX работает (опт-ин конверсия); ретеншен (гейт Day-7 $\geq 20\%$ на когорте до 500 инвайтов, декабрь 2026); бизнес платит (первый пилот \$1-5K, на момент написания не подписан — это и есть валидируемая гипотеза); wallet-рельса и IOU-ledger держат нагрузку без double-crediting.

Не доказывает и не должна доказывать: аппаратно-аттестованную обработку (появляется в Фазе 2); осмысленный per-contributor доход на масштабе; токеномику в бою; мультимодальную плотность сигналов. Альфа, не прошедшая гейт, не запускает Фазу 2 автоматически: переходы gated by metrics, never by calendar.

4.9 Операционная дисциплина фазы

Фаза 1 живёт на одном VPS-классе хостинга плюс object storage: PostgreSQL IOU-ledger, Ахум API, DNS-сервер и отчётный пайплайн совмещены без отдельной оркестрации — операционная поверхность фазы сознательно минимальна. B2B-отчёты Фазы 1 с первого пилота собираются founder-operated: агрегации из PostgreSQL плюс нарратив, с явным раскрытием покупателю модели доверия и отсутствия аттестации. Стоимость фазы доминируется S3-хранением и эгрессом, а не compute — и это осознанный выбор: дорогая часть (SEV-SNP bare-metal, COCOON-воркеры) включается только после того, как пилот доказал спрос.

4.10 Freeze Фазы 1: что зафиксировано и как вносится изменение

Фаза 1 заморожена в следующем составе до прохождения гейта Фаза 1 → Фаза 2 (11.1): (1) сигналы — события сессии TMA и опциональный DNS-канал с ручной конфигурацией (4.2), иных категорий в Фазе 1 нет; (2) модель доверия — disclosed trusted-operator (4.5), отчёты founder-operated (4.9),

аппаратная аттестация в Фазе 1 не обещается; (3) антифрод — три детерминированных правила без ML (4.6), Proof-of-Behavior — Фаза 2; (4) рельса регистрации — выбор продукта между вариантом А (легаси-рельса регистрации) и вариантом В (реализация регистрационного контракта): оба варианта не меняют скоуп Фазы 1, и при выборе А альфа не называется реализацией контракта (11.5); (5) токеномика — IOU-леджер PostgreSQL с ACID-гарантиями, видимые ставки с тегом [DESIGN — ILLUSTRATIVE RATIOS] (4.7), без сжиганий, разовых бонусов и тарификации Oracle (9.6, 9.7); (6) слои — Oracle, Signal Passport, Missions и открытый API в Фазе 1 не строятся и не обещаются (3.3, 11.2).

Правило изменения: любой новый механизм, предлагаемый в Фазу 1, сначала вносится в реестр открытых вопросов дизайна с владельцем и статусом [PROPOSED — NOT AGREED] и попадает в основной текст только после явного решения продукта и архитектора ядра, версионной ревизией с changelog. Правки Фазы 1 «на лету» не допускаются; найденные противоречия решаются приоритетом настоящего раздела, а не расширением скоупа.

ГЛАВА 5. РЕГИСТРАЦИОННЫЙ КОНТРАКТ И PROOF-WIRE

5.1 Назначение и честный статус

Регистрационный контракт ForeMetric — это HTTP+TON proof-wire спецификация, которая связывает три сущности: субъекта (user_hash пути), Telegram-идентичность (initData) и TON-кошелёк (ton_proof), с семантикой рефералов и идемпотентности, проверяемой обеими сторонами. Текущее состояние: Proposed, не Frozen и не задеплоен. Freeze-кандидат зафиксирован; дайджест спецификации пересчитывается при любом изменении

контракта до фриза; полный текст спецификации и conformance-матрица — в закрытом Data Room по запросу. Это спецификация и conformance-тулинг; live registration-флоу появляется после фриза и деплоя.

5.2 Три операции и bearer-модель

Контракт определяет ровно три операции в фиксированном порядке: challenge (выдача ton_proof challenge с привязкой к профилю окружения), register (создание субъекта из верифицированного initData с опциональным реферальным кандидатом), wallet link (привязка кошелька через ton_proof). Единственный bearer-credential сессии — EdDSA JWT с $TTL \leq 24$ часов, sub = path user_hash; сессионные cookie не являются bearer-токенами и не дублируют авторизацию. JWT подписывается сервером, верифицируется Stateless-промежутком; отзыв не предусмотрен по дизайну короткого TTL — принятое ограничение.

5.3 Реферальная семантика: шесть строк матрицы

Реферальное окно закрывается перманентно в момент первой успешной регистрации субъекта. Матрица из шести строк зафиксирована в спецификации и определяет поведение без двусмысленностей: тот же реферальный кандидат X при свежем ключе даёт 200 no-op (состояние сохранено); другой кандидат Y после закрытия окна даёт 409 REFERRAL_CONFLICT; отсутствие кандидата сохраняет текущее состояние; конфликты не являются echo-кодами успешной операции. Код ответа 422/REFERRAL_INVALID удалён из спецификации как избыточный. Поле referral_intent_recorded означает «намерение записано», а не «реферал активирован»: активация начислений происходит только после wallet_verified=true (Глава 9). Сгенерированные реферальные коды — 4-60 URL-safe ASCII символов, так что префикс ref_<code> гарантированно помещается в 64-символьный start-параметр Telegram.

5.4 Идемпотентность и кардинальность кошелька

Идемпотентный ключ равенства исключает сырые proof-байты (они уникальны на попытку), но включает: операцию, wallet claim, proof-presence mode и точный реферальный кандидат либо его явное отсутствие. Единственный retryable конфликт —

IDEMPOTENCY_IN_PROGRESS с заголовком Retry-After; все прочие 409 терминальны и типизированы. Кардинальность кошелька — иммутабельная биекция 1:1 с двумя направленными 409: WALLET_ALREADY_LINKED (субъект уже имеет кошелёк) и WALLET_ALREADY_BOUND (кошелёк уже принадлежит другому субъекту).

Неверифицированный wallet claim не создаёт ни binding, ни reservation, ни lock: атомарность обеспечивается DB-unique ограничением, а не check-then-write гонкой. public_key в proof трактуется как недоверенный equality-hint: верификатор дважды ре-выводит ключ из walletStateInit, и расхождение отклоняется.

5.5 Proof-wire: AppDomain, timestamp, caps, CORS

AppDomain определяется нормативно: это hostname из поля url манифеста JSON, а не origin TMA и не хост, обслуживающий файл манифеста; сравнение exact-match.

Замороженные профили окружения: production — foremetric.ai, TON mainnet (-239); staging и development — staging.foremetric.ai, testnet (-3), workchain 0. localhost в замороженной матрице отсутствует. Эмпирический кейс Tonkeeper (browser extension v26.6.1), который отказывает в подключении при несовпадении page origin с manifest url, зафиксирован как наблюдаемое основание для выделенного staging-хоста.

proof.timestamp — проверенное неотрицательное целое в JSON-токене: кавычки, float и coerced-значения отклоняются на границе контракта.

Caps (жёсткие границы тел запросов): 12 288 / 24 576 / 16 384 байта для challenge / register / wallet-link; init_data ≤ 8 192 символов; walletStateInit ≤ 8 192 base64 / 6 144 декодированных байт; domain ≤ 128 UTF-8 байт; signature ровно 64 байта; payload ровно 32 байта; реферальный кандидат — непустая строка в пределах bound, заданного OpenAPI-схемой.

Тайминговые окна контракта: challenge живёт 300 секунд; максимальный возраст proof — 900 секунд; максимальный возраст init_data — 3600 секунд; допуск clock-skew — 30 секунд. Порядок проверок фиксирован: consumed-state → expiry → proof-freshness.

CORS: allow- и expose-наборы зафиксированы так, чтобы браузер мог прочитать код и детали ошибки без утечки внутренних трейсов; инварианты wire-строк зафиксированы в

freeze-кандидате (статус Proposed, не Frozen) и меняются только явной ревизией с АСК владельцев.

5.6 Evidence-статус и стандарт freeze-grade

Реестр доказательств контракта и окружений ведётся: полные статусы, артефакты и provenance-цепочки предоставляются квалифицированным инвесторам в закрытом Data Room.

Стандарт freeze-grade принят как производственный: hook-emitted verbatim safe envelope на источнике (без seed/ключей, точные runtime-типы, версии кошелька и приложения, полный 40-значный SHA, deployment ID, capture timestamp); immutable binding деплоя, при котором timestamps не могут предшествовать коммиту provenance; adapter equality assertion поле-в-поле до redaction; версионированная JSON Schema на реальном движке с negative-probe resistance; Markdown/JSON parity, при которой расхождение валит CI. Владение: архитектор — reusable mapper/evidence слой; фронтенд — интеграция, деплой, пересъёмка; бэкэнд — DTO/verifier согласование.

Governance-правило: реклассификация evidence-пунктов из pre-freeze в post-freeze происходит только явной ревизией контракта с АСК именованных владельцев — никогда неявно через relabel или merge. Все перечисленные ограничения зафиксированы как производственный стандарт, к которому проект возвращается после альфы.

5.7 Что контракт намеренно не делает

Контракт не проводит on-chain регистрационную транзакцию в Фазе 1 (zero gas для пользователя); не содержит токен-операций и не ссылается на Revenue Splitter; не заменяет Identity Vault (отдельный контракт на TON Testnet, хранящий обе зашифрованные копии DataKey — Blob A/B — и указатели на зашифрованные поведенческие blob'ы); не реализует миграцию кошельков (Phase 2, после wallet_verified и аттестации). Его единственная работа — сделать связку «субъект ↔ Telegram ↔ кошелёк ↔ реферальное намерение» проверяемой обеими сторонами до того, как протокол начнёт начислять ценность.

ГЛАВА 6. КРИПТОГРАФИЧЕСКИЙ СЛОЙ И ПРИВАТНОСТЬ

6.1 Модель угроз и границы доверия по фазам

ForeMetric проектирует криптографию против четырёх противников: злоумышленный покупатель (пытается извлечь профиль или сырые векторы из ответа); скомпрометированный облачный провайдер (читает память и диски вне анклава); будущий принудительный запрос (изъятие хранилища постфактум); внутренний оператор (insider-доступ к ключам). Граница фазы: защита от внутреннего оператора в Фазе 1 не обеспечивается криптографией — она обеспечивается раскрытием, аудит-трейлом и tamper-evidence. Полная криптографическая нейтрализация оператора появляется только с Фазой 2, когда расшифровка становится возможной исключительно внутри аттестованной памяти.

6.2 DataKey и dual-encryption

Единица защиты — per-user 256-битный AES DataKey, шифрующий все поведенческие чанки пользователя (AES-256-GCM, 96-битный случайный nonce на чанк, AAD = {user_id_hash, timestamp_utc_seconds, chunk_seq_num} — аутентифицирует метаданные без шифрования, закрывая переупорядочивание чанков и подмену timestamp). DataKey никогда не хранится в открытом виде и никогда не комбинируется XOR-схемами: он шифруется дважды, в две независимые копии внутри Identity Vault.

Blob A — DataKey под публичный ключ TON-кошелька пользователя (Ed25519): это даёт пользователю независимую криптографическую возможность расшифровать собственные данные вне протокола — основу data-portability и суверенитета; копия пользователя восстанавливается через seed phrase навсегда, независимо от протокола, оператора и блокчейна. Blob B — DataKey под ключ вычислительной стороны: в Фазе 1 это серверный ключ вычислительной стороны под AWS KMS с envelope-шифрованием и аудит-трейлом каждого обращения (модель trusted-operator, раскрытая пользователю); в Фазе 2 — VM-bound ключ, сгенерированный внутри аттестованной AMD SEV-SNP VM и никогда не

покидающий зашифрованную RAM. Миграция Фазы 1→2 — фоновая пере-шифровка каждого Blob B без действия пользователя.

Две копии решают центральное противоречие privacy-систем: пользователь должен мочь восстановить свои данные вечно (иначе compute держит единственную копию и становится точкой принуждения), и compute должен мочь расшифровывать векторы при запросах (иначе данные бесполезны). Две копии одного ключа в двух разных доменах доверия — ответ. Вычислительный сервер никогда не видит Blob A; пользователь не обязан быть онлайн, чтобы его данные обработали.

Ни в одной фазе не существует точки, где оба ключа и открытый DataKey встречаются вне аттестованного контура.

6.3 Crypto-shredding и SLA удаления

Удаление реализовано как уничтожение ключа, а не стирание данных: `burn_keys()` обнуляет Blob A и Blob B в Identity Vault и стирает DataKey из Secure Enclave / StrongBox. После finality блока TON (~5 секунд) весь шифротекст пользователя — в S3, TON Storage или резервных копиях — становится вычислительно невозстановимым шумом для любой стороны: оператора, облачного провайдера, TON-валидаторов, физического атакующего с серверами. Резервная копия шифротекста без ключа — резервная копия шума. Целевая задержка необратимости — порядка 5 секунд (finality блока TON для фиксации события уничтожения); регуляторная планка GDPR Article 17 — стирание «без неоправданной задержки», и мы проектируем удаление как уничтожение ключей: необратимость на уровне секунд, далее каскад по производным записям (таблица ниже — целевые показатели дизайна). Запрос на удаление проходит workflow с подтверждением пользователю и on-chain фиксацией события shredding, чтобы факт удаления был аудируем так же, как факт хранения.

Событие	Задержка
Уничтожение DataKey, обнуление Blob A/B	T+0 ... T+5 с (TON finality)
Инвализация Qdrant-индекса tombstone-сообщением (Фаза 2)	T+5 мин
Удаление balance- и session-записей PostgreSQL	T+30 мин
Анонимизация DNS-логов (user_hash → криптографический random)	T+24 ч

Строка Qdrant применима с Фазы 2 (индекс появляется только в ней); в Фазе 1 каскад — DataKey → записи PostgreSQL → DNS-логи.

Регуляторная планка GDPR Article 17 — стирание «без неоправданной задержки»; целевые задержки каскада — в таблице выше; фактическая необратимость PII — 5 секунд (finality блока TON). Шифротекст может физически оставаться на узлах хранения: по GDPR Recital 26 данные, не относимые к идентифицируемому лицу, вне периметра персональных данных, а AES-256-GCM без ключа вычислительно неотличим от случайных байт. Это не лазейка, а следствие: мы уничтожаем точку смысла, а не байты по всем репликам — классическая нерешаемая задача распределённого удаления здесь обходится архитектурно.

6.4 Дифференциальная приватность на выходах

Индивидуальное удаление защищает прошлое; дифференциальная приватность защищает настоящее — ответы, выдаваемые пока пользователь активен. Каждый B2B-выход Фазы 2 [PLANNED PHASE 2] проходит шумовой контур OpenDP: Rényi DP при $\epsilon=4.0$ на когортах от 50 пользователей. Жёсткий минимум когорты — 50: запрос ниже порога возвращает агрегированный отказ, а не ослабленный ответ с меньшим шумом; отказ честнее приближённой цифры, которая де-анонимизируется. Бюджет приватности — отслеживаемый ресурс: центральный privacy accountant ведёт кумулятивную экспозицию по клиенту и семейству запросов и автоматически отклоняет запросы сверх порога. Бюджеты приватности — параметры контракта с покупателем, а не скрытые константы:

они указываются в аттестационном отчёте Фазы 2 вместе с результатом вычисления. Federated Learning (Глава 8) работает под более строгим бюджетом — Gaussian DP $\epsilon=1.0$ с клиппированием градиентов на устройстве: градиентная обновка может нести регулярности одного пользователя сильнее, чем агрегат отчёта.

6.5 Граница COCOON: правило двух входов

COCOON Intel TDX воркеры выполняют инференс и генерацию отчётов, но получают ровно два входа: (а) текст запроса покупателя и (б) анонимизированные агрегированные статистики, подготовленные внутри SEV-SNP VM. Они никогда не получают DataKey, сырые векторы, идентичности пользователей или историю запросов других покупателей.

COCOON — compute-only: он не хранит векторы, не хранит ключи и не является слоем хранения ни в одной фазе (хранение — S3 hot-tier и TON Storage, Глава 7-8).

Аттестационный отчёт воркера прикладывается к отчёту покупателя, и покупатель может независимо верифицировать TDX-quote: доверие к вычислению не требует доверия к нам.

6.6 Tamper-evidence и аудит

Три независимых контура обнаружения модификаций: (1) спроектированный on-chain content-hash каждого батча (механизм — daily Merkle-anchoring, [PLANNED, not live]): после запуска любая тихая правка математически обнаружима; до запуска целостность обеспечивается ACID-транзакциями и аудит-логами; (2) KMS аудит-трейл каждого обращения к серверной копии DataKey в Фазе 1; (3) client-verifiable attestation в Фазе 2 и децентрализованный реестр аттестаций в Фазе 3.

6.7 Hard limits, обеспечиваемые архитектурой

Ограничения, нарушение которых требует переписывать компоненты и выпускать новый бинарник, а не менять конфигурацию: фоновый сбор 100Hz+ на iOS невозможен (Resource Governor переключает на 1Hz hardware-DSP режим); Message Metadata не существует (API-поверхности нет физически); сырые векторы не экспортируются (export-эндпоинта нет по построению); COCOON-воркеры не получают DataKey и сырые векторы (task builder принимает только {nl_query, aggregate_stats} — передача вектора есть compile-time type

error); продажа сырых датасетов исключена (B2B-эндпоинт возвращает только аттестованные ответы); FL без явного opt-in невозможен (маршрутизация задач — только на кошельки с флагом FL_CONSENT; статус флага как свойства байткода — вопрос спеки); ручные выплаты невозможны (Revenue Splitter иммутабелен, admin-ключа нет).

Протокольные запреты, которые не отключаются ни одной настройкой и ни одной фазой: не собирается и не хранится содержимое переписок; не собираются keystrokes; DNS-канал видит категории доменов, а не содержимое страниц; сырые сенсорные данные Фазы 2 не покидают устройство (наружу уходит только зашифрованный вектор); экспортного эндпоинта векторов не существует по построению; категории Message Metadata удалены из протокола навсегда, и CI валит любую сборку, ссылающуюся на legacy-имена («Browsing History», «Search Queries», «App Usage», «Location History»). Эти запреты — не политика приватности, которую можно переписать решением менеджмента, а свойства кода и пайплайна.

6.8 Что криптография не решает

Перечень границ: в Фазе 1 оператор теоретически может прочитать данные — риск снижается раскрытием, аудитом и тампер-очевидностью, но не исчезает; паттерны метаданных (частотность, ритм) несут информацию даже без содержимого — поэтому агрегация и DP-пороги применяются к выходам, а не только к payload; криптография не защищает от принуждения пользователя к consent и от социальной инженерии тумблеров — поэтому consent-UX проектируется с явными названиями категорий и обратимостью; и никакая аттестация не компенсирует баг в нашем собственном коде — поэтому регистрационный контракт и proof-wire вынесены в проверяемую спецификацию с conformance-кейсами (Глава 5), а freeze-grade evidence-стандарт требует negative-probe тестов валидатора. Приватность в ForeMetric — это сумма криптографии, проверяемых контрактов и раскрытых ограничений, и третье мы ценим не меньше первых двух.

6.9 Выбор алгоритмов

Назначение	Алгоритм	Обоснование
Симметричное шифрование	AES-256-GCM	Аппаратное ускорение на всех целевых устройствах (ARMv8 Crypto Extensions, AES-NI); AEAD-конструкция даёт конфиденциальность и целостность одной операцией; реализация — Rust crate ring с автодетектом CPU
Обмен ключами	X25519 (Curve25519 ECDHE)	32-байтные ключи, константное время по построению (иммунитет к timing side-channel), отсутствие патентных ограничений
Подписи	Ed25519	64-байтные подписи, верификация <15 мкс; то же поле Curve25519, что и X25519 — одна криптобиблиотека на JWT, Signal Passport-гранты, epoch-аттестацию устройств и TON-аутентификацию
Хеширование	SHA-256	user_hash, Merkle-деревья, каноникализация DNS-доменов, content-hash anchoring; нативный хеш TON — критично для кросс-совместимости Identity Vault
Пост-квантовая защита	Kyber-768 (ML-KEM-768, FIPS 203)	Только Фаза 3, гибрид KEM: SharedSecret = SHA-256(Kyber // X25519); отложена осознанно — практического квантового атакующего в 2026-2028 нет, а цена раннего ввода +15 МБ бинарника и сложный FFI

6.10 Минимизация данных по построению

Каждый сигнал редуцируется в момент захвата, и ни один слой не реконструирует то, что предыдущий отбросил: GPS → geohash-6 (~1 км) сразу, точные координаты не существуют ни в одном хранилище и логе; Wi-Fi BSSID → SHA-256(BSSID)[0:8], сырая строка отбрасывается после хеширования; аудио → только классификационные метки SoundAnalysis на аппаратном DSP, PCM-буфер не создаётся в software-слое вообще; галерея → thumbnail 200×200 → top-5 тегов MobileCLIP, thumbnail освобождается после инференса, оригинал фото не читается; DNS → категория, доменная строка отбрасывается сразу после классификации; Telegram user_id → односторонний SHA-256 user_hash

(псевдонимизация; обратное отображение не существует по построению). Фундамент — односторонняя векторизация: телеметрия становится feature-вектором, и feature-вектор никогда не становится телеметрией снова.

ГЛАВА 7. ФАЗА 2: NATIVE APP И CONFIDENTIAL COMPUTING

7.1 Почему native, и почему Rust Core + Flutter shell

Telegram Mini App физически не может нести Фазу 2: WebView не даёт фонового выполнения, доступа к инерциальным сенсорам на нужной частоте, hardware DSP-пайплайнов и гарантированного жизненного цикла процессов. Фаза 2 — это native приложение с жёстким разделением ответственности: Rust Core владеет всем, что касается данных и криптографии (сбор, векторизация, шифрование, Secure Enclave/StrongBox, epoch-аттестация, upload-очереди), Flutter shell владеет только UI и навигацией через FFI-границу. Причина разделения не эстетическая: memory-safety и константное время криптографических операций нам нужны как свойство языка, а не как дисциплина code review; при этом скорость итерации UI остаётся flutter-овской. FFI-поверхность минимальна и типизирована: UI не видит сырых буферов сенсоров вообще.

7.2 On-device векторизация и zeroing

Локальная модель на 2-секундных окнах инерциальных сигналов выдаёт 12-компонентный вектор признаков; модальные блоки (DNS-категории, временные ритмы, lifestyle-теги, ambient-метки, app-паттерны) комбинируются в канонический 128-мерный поведенческий вектор на 30-минутном окне. Сырые буферы затираются явно (zeroing), а не полагаются на сборщик мусора: наружу уходит только зашифрованный embedding плюс метаданные категории и epoch-подпись. Ни один слой сервера не имеет API, принимающего сырые компоненты. Частоты сбора регулируются Resource Governor с пятью состояниями (норма, battery-saver, thermal, background-restricted, suspended): при деградации состояния Governor снижает sampling rate детерминированно, а не «на глаз», и пользователь видит текущее состояние в UI сигналов. Каждое устройство несёт epoch-

key аттестацию: Ed25519 ключ эпохи, ротация по epoch, регистрация эпох в on-chain реестре — сервер принимает векторы только от устройств с валидной цепочкой эпохи, что делает налив бот-ферм дорогостоящим, а не тривиальным.

7.3 Proof-of-Behavior и персональная on-device модель

Proof-of-Behavior (PoB) — 1D-CNN по инерциальным последовательностям, отличающая человеческую микро-моторику от скриптованной и эмулированной активности. Целевые метрики приёмки: $FPR \leq 2\%$ (бюджет FNR); устойчивое держание $FPR \leq 2\%$ в течение 90 дней — гейт уже Фазы 3. PoB работает на устройстве и выдаёт score-подпись эпохи, а не сырые акселерометрические треки: сервер видит подпись и агрегат, не видит трек. Персональная on-device модель пользователя компилируется на устройстве из его собственной истории (ритмы, фокус-окна, кросс-интенты); она никогда не покидает устройство и является вычислительной основой Oracle; в агрегированном виде её паттерны сопоставимы с когортными, но сама модель — собственность пользователя в его Secure Enclave (закрепление термина в спеке).

7.4 Hybrid TEE: два анклава, две работы

Фаза 2 использует не один анклав, а пару с разными ролями. AMD SEV-SNP confidential VM — application layer: внутри зашифрованной памяти происходят трансляция natural-language запроса (local-first Phi-3-mini), cohort search по зашифрованному Qdrant-индексу и применение дифференциальной приватности. COCOON Intel TDX воркеры — report boundary: генерация финального отчёта и аттестационного пакета. Граница COCOON подчиняется правилу двух входов: текст запроса и анонимизированные агрегированные статистики; DataKey, сырые векторы и идентичности не передаются никогда, и передача вектора в task builder есть compile-time type error, а не политика. Аттестация client-verifiable: покупатель отчёта получает TDX-quote и SEV-SNP measurement и может независимо проверить, что вычисление прошло в том коде, который зафиксирован в реестре версий.

7.5 Хранение Фазы 2 и Master HashmapE

Горячий слой (<30 дней) — S3 с быстрым доступом для cohort search; холодный слой (>30 дней) — TON Storage с децентрализованной репликацией шифротекста. COCOON не является слоем хранения ни здесь, ни где-либо ещё. Реестр указателей на пользовательские vault'ы консолидируется в Master Contract на TON HashmapE: per-user Identity Vaults Фазы 1 остаются корнем совместимости, а Master HashmapE даёт масштабируемый онбординг и атомарные обновления указателей без миграции данных пользователей (асимптотика). Указатели — не данные: сам шифротекст лежит в S3/TON Storage, в цепочке только хеши и blob-ссылки.

7.6 End-to-end B2B pipeline

Полный путь запроса Фазы 2: покупатель отправляет natural-language вопрос → Domain Query Router декомпозирует его на доменные подзапросы (fintech, retail, mobility, media) с бюджетом приватности на каждый → подзапросы исполняются внутри SEV-SNP VM: cohort search по зашифрованным embedding'ам, фильтрация минимальной когортой 50, шум OpenDP $\epsilon=4.0$ → агрегаты передаются в COCOON TDX по правилу двух входов → генерируется отчёт с предиктивными метриками и аттестационным пакетом → покупатель верифицирует quote → Revenue Splitter маршрутизирует 80% gross платежа контрибьюторам когорты, 10% рефереру (или казне при его отсутствии), 10% казне. Ни на одном шаге покупатель не получает вектор, профиль или экспорт; ни на одном шаге оператор не видит открытый запрос вне аттестованной памяти.

7.7 Oracle: механика и citation contract

Oracle — это личный предиктивный слой протокола и главный ретеншен-крюк: причина открывать ForeMetric каждый день, не связанная с балансом. Тикер баланса отвечает на вопрос «сколько мне заплатили»; Oracle отвечает на вопрос «что со мной происходит и что будет дальше» — а этот вопрос человек задаёт себе каждое утро. Продукт строится так, чтобы ответ был ценнее, чем у любого трекара: трекары показывают прошлое, Oracle — рассчитанное будущее.

Что видит пользователь. Утренний брифинг: короткие предсказания и советы о собственном дне — «фокус-пик сегодня в 14:00», «качество сна трендит вниз третью неделю — окно восстановления сегодня до 23:00», «лучшее окно для тренировки завтра 7:00–8:30», «окно для поездки на следующей неделе». Каждое предсказание несёт уровень уверенности; уверенность ниже порога показывается честно, а не скрывается. Это принципиальное отличие от статистики о прошлом, которую показывает любое фитнес-приложение: Oracle выдаёт утверждение о будущем с обоснованием.

Как это работает: две опоры. Первая — персональная модель, которая обучается на самом устройстве из истории самого пользователя: ритмы активности, окна фокуса, паттерны сна, покупок и перемещений (7.3). Она никогда не покидает телефон — ни целиком, ни частями; на сервере нет API, который мог бы её принять. Вторая — когортные паттерны: обобщённые закономерности по всем участникам протокола, прошедшие дифференциальную приватность и минимальный порог когорты 50. Предсказание рождается на пересечении: «ваш ритм» × «как такой ритм развивается у похожих людей». Отсюда прямая зависимость качества от масштаба: чем больше участников на рельсе, тем плотнее когортный базис и тем выше достоверность предсказаний для каждого — сетевой эффект достоверности, встроенный в продукт с первого дня.

Citation contract — обязательство честности. Каждое предсказание обязано цитировать источники: какие категории сигналов внесли вклад, на каком когортном базисе построено сравнение, с какой калиброванной уверенностью. Предсказание без цитат не рендерится — это свойство кода, а не политика: поверхность рендеринга физически не принимает объект без поля цитирования. Пользователь раскрывает карточку предсказания и видит, на чём оно стоит; «чёрных ящиков» в Oracle нет по построению.

Границы и роль. Oracle category-bounded: медицинские диагнозы и юридические выводы вне его поверхности по построению, а не по дисклеймеру — он не лечит и не консультирует по праву; он замечает паттерны и называет окна для действий. Роль в протоколе двусторонняя: пользователю — ежедневная ценность без ежедневного вмешательства в приватность (всё вычисление локально, плюс обезличенные когорты); протоколу — ретеншен: чем дольше человек в системе, тем точнее его персональная

модель и тем плотнее его сигнал для B2B-запросов. Дни использования конвертируются и в ценность для человека, и в его доход. Статус: [PLANNED PHASE 2]; форматы брифинга и порог отображаемой уверенности — открытые вопросы дизайна.

7.8 Signal Passport: гранты, B2B-срезы и C2C-режим

Signal Passport — слой, который превращает верифицированный поведенческий профиль человека в актив: им можно делиться по своим правилам, им можно зарабатывать, и его можно в любой момент закрыть. Ключевая идея: люди десятилетиями «делятся» данными о себе бесплатно и не по своей воле — Signal Passport делает акт «поделиться» осознанным, ограниченным и оплачиваемым. Слой работает в двух режимах — B2B и C2C, — и в обоих наружу уходят ответы, а не записи.

Единица доступа — грант. Грант — подписанный Ed25519-объект размером ~112 байт: {grantee — кому выдан; category-score — какие категории профиля открывает; TTL — на какой срок; nonce — одноразовый номер, исключающий повторное использование; подпись пользователя}. Грант нельзя подделать и нельзя переиспользовать после истечения срока. Отзыв работает на трёх уровнях: конкретный грант, целая категория, глобальный burn — уничтожение DataKey, после которого весь профиль необратимо превращается в шум (crypto-shredding, Глава 6). Каждая выдача и каждый отзыв фиксируются и видны пользователю в журнале доступа: доступ не бывает незаметным.

B2B-режим: верифицированный срез вместо покупки данных. Кому это нужно: банку — предскоринг клиента; страховщику — реальный риск-профиль вместо анкетного; HR-сервису — проверка «живого» резюме; программе лояльности — честный уровень активности участника. Шаги: (1) бизнес формулирует запрос на срез — какие категории, на какой срок, с какой оплатой за запрос; (2) пользователь получает предложение в приложении и видит список категорий, срок, вознаграждение и то, как бизнес будет использовать ответ; (3) по согласию выдаётся грант — ровно на выбранные категории и срок; (4) запрос исполняется внутри аттестованного анклава: совпадение профиля с критериями бизнеса вычисляется над зашифрованными данными; (5) бизнес получает ответ-пригодность (score), а не профиль и не сырые записи; (6) 80% платежа уходит

пользователю автоматически. Почему бизнес платит: поведенческий сигнал точнее заявительного — люди переоценивают свою дисциплину, датчики — нет; при этом архитектура не передаёт бизнесу персональные данные, выводя его из-под роли контролера по GDPR (архитектурный факт; юридическая оценка — юрконсультация).

C2C-режим: монетизация верифицированного «я». Второй режим делает Signal Passport потребительским продуктом: за вопрос платит не бизнес, а живой подписчик — создателю, за которым он следует. Проблема, которую режим решает: рынок инфлюенс-маркетинга держится на словах — блогер заявляет «я живу спортом», «я пользуюсь этим банком», «я правда так тренируюсь», — и подписчик не может это проверить. Signal Passport вводит рынок верифицированной аутентичности: за ответы создателя ручается протокол, а не обещание.

Как работает C2C, по шагам: (1) пользователь включает публичный профиль и тумблерами выбирает категории, на которые разрешает вопросы — например, спортивную дисциплину, ритм сна, покупательские интенции, путешествия; (2) приложение генерирует QR-код и ссылку — сам QR не содержит данных, только указатель на грант-политику пользователя; (3) создатель публикует QR в своём канале, соцсетях, на стриме; (4) подписчик сканирует и платит за вопрос (цены задаёт создатель; платёж в TON) — например: «ты действительно тренируешься 5 раз в неделю?», «какой у тебя реальный ритм сна в поездках?», «действительно ли ты пользуешься банком, который рекламируешь?»; (5) вопрос уходит в аттестованный анклав, ответ вычисляется из верифицированного профиля — только по открытым категориям и только в агрегированной форме, без сырых записей; (6) 80% платежа автоматически уходит создателю, далее стандартный сплит: 10% рефереру, 10% казне.

Почему это важно для протокола. Верификация: Proof-of-Behavior подтверждает, что сигналы создателя произведены живым человеком, а не скриптом, — «честность» становится проверяемым свойством, за которое платят. Рост: каждый опубликованный QR — бесплатный канал привлечения — подписчики сканируют, видят работающую экономику и подключаются сами; создатели приводят аудиторию, а не мы выкупаем трафик. Спрос: экспертам, тренерам, амбассадорам брендов режим даёт новый источник

дохода из уже существующей аудитории — без продажи данных, потому что наружу уходят ответы, а не записи.

Честный статус: [PLANNED PHASE 2]; оба режима — untested, unpriced. Готовность подписчиков платить за вопросы создателя, структура ценообразования (цена за вопрос, подписка, тарифные сетки) и правила матчинга категорий — открытые вопросы дизайна. Механика гранта, уровни отзыва и границы анклава наследуются из B2B-режима без изменений.

7.9 Missions: prepaid-эскроу без эмиссии

Missions — слой, который соединяет бренды и людей через задачи реального мира с доказуемым выполнением. Проблема, которую слой решает: весь рынок промо-активностей — челленджи, программы лояльности, инфлюенс-задания — подтверждает выполнение словами: селфи, чек, кнопка «я сделал». Накрутка в таком контуре — не исключение, а норма: бюджеты сгорают, реальные действия не происходят, и бренд платит за видимость активности, а не за активность.

Как работает. (1) Бренд формулирует миссию — «100K шагов за 14 дней», «посети локацию X в течение недели», «используй продукт 7 дней подряд» — и заранее вносит полный бюджет наград в prepaid-эскроу: смарт-контракт держит деньги с момента публикации, и ни бренд, ни протокол не могут их изъять или перенаправить. (2) Миссия появляется в приложении у пользователей, чей профиль ей соответствует; участие добровольно, как и любой сигнал. (3) Выполнение проверяется сигналами устройства: шаги — инерциальными сенсорами и PoB-подписью, посещение локации — geohash-достижением, правдоподобность — темпоральной проверкой; селфи и самозаявления в контуре проверки не существуют. (4) Смарт-контракт видит верифицированное выполнение и высвобождает награду — без менеджера, согласований и риска неоплаты: деньги уже в эскроу. (5) Неиспользованный остаток возвращается спонсору.

Почему платит бизнес и почему приходят пользователи. Для бренда миссия — оплата за доказанное действие: платёж происходит только за выполнения, подтверждённые сигналами, а не за отчёт о кампании. Фрод отсекается архитектурно: скриптованные шаги

не проходят Proof-of-Behavior, выдуманные визиты — гео-проверку, «пачками» набитые дни — темпоральную правдоподобность. Это первый промо-канал, где конверсия измерима на уровне каждого выполнения, а не декларируется площадкой. Для пользователя — деньги за реальные действия без бюрократии: не нужно ничего доказывать людям, всё уже доказано сигналами, и награда приходит автоматически.

Безопасность для токеномики — по построению. Миссии — единственное проектируемое исключение из правила «никакой необеспеченной эмиссии» (инвариант 1.6), и оно не нарушает правило, а выполняет его: каждый токен награды заранее покрыт деньгами спонсора, уже лежащими в эскроу, — эмиссии без покрытия не существует. Статус: [PLANNED PHASE 2]; каталог миссий, матчинг по профилю и антифрод-пороги — открытые вопросы дизайна.

7.10 Что Фаза 2 не меняет

Инварианты Главы 1.6 переносятся без изменений: нет экспортного эндпоинта; COCOON compute-only; single-level referral; нет mint(); crypto-shredding ~5 секунд; Message Metadata не существует; границы фаз сохраняются — Фаза 2 делает оператора криптографически нейтрализованным, но не делает протокол децентрализованным: децентрализация хранения, compute по умолчанию и federated learning — Фаза 3 (Глава 8). Переход в Фазу 2 гейтуется: B2B MRR $\geq$ \$3K/месяц устойчиво плюс обеспеченный runway (11.4) и верифицируемая end-to-end аттестация; календарь не является гейтом.

ГЛАВА 8. ФАЗА 3: ДЕЦЕНТРАЛИЗАЦИЯ И FEDERATED LEARNING

8.1 Три перехода, а не переписывание

Фаза 3 — не новая система, а смена дефолтов в трёх местах: где хранится шифротекст, где выполняется compute и кто верифицирует аттестацию. ForeMetric переходит из роли инфраструктурного оператора в роль протокольного слоя: наши серверы становятся одним из многих участников, теряя привилегию, но не функцию. Ни один из переходов не меняет модель ключей и не ослабляет hard limits Главы 6: децентрализация хранения не означает доступности данных провайдерам — они держат шарды шума.

8.2 Хранение: только TON Storage

Горячий и холодный слои сходятся в один: весь шифротекст — S3 выводится из эксплуатации — живёт на TON Storage провайдерах с шардированием и диверсификацией провайдеров на каждый blob. Retrieval оплачивается из протокольной экономики, а не из доверия к одному вендору. Модель ключей не меняется: blob остаётся AES-256-GCM под per-user DataKey, провайдер хранения не имеет ни ключа, ни второй копии Blob B, ни контекста user_hash сверх указателя. Децентрализация хранения решает цензуру и single-point-of-failure, но не приватность — приватность по-прежнему обеспечивает криптография.

8.3 Compute: COCOON как дефолт

Все вычислительные нагрузки — трансляция запросов, cohort search, генерация отчётов, FL-агрегация — выполняются на COCOON-воркерах (Intel TDX и SEV-SNP). Наши собственные AMD SEV-SNP bare-metal сервера Фазы 2 перепрофилируются в COCOON worker-ноды (SEV-SNP-бэкенд COCOON — cohort search и FL-агрегация; report boundary остаётся за TDX-воркерами): оператор теряет эксклюзивность, но не нагрузку. Сторонние операторы присоединяются с hardware-аттестацией и экономическим обеспечением (stake/slash за аттестационное мошенничество); маршрутизация задач идёт по совпадению code measurement из версионного реестра, а не по доверию к имени оператора. Правило двух входов становится протокольным свойством: типизированный worker API принимает только {nl_query, aggregate_stats} или {fl_task, clipped_update} — передача вектора или DataKey воркеру есть compile-time type error на стороне любого честного клиента и slash-событие на стороне нечестного.

8.4 Децентрализованная аттестация

Аттестация перестаёт быть доверием к одному вендору и к одному оператору: TDX-quote и SEV-SNP measurement каждого вычисления проверяются независимыми верификаторами (другими воркерами, верификаторами со стороны покупателя) против

on-chain реестра code measurements. Отчёт несёт кворум подписей верификаторов, и покупатель может проверить кворум сам. Обновления реестра — подписанные релизы с notice-периодом и ротацией measurements; скомпрометированный measurement отзывается по пути, аналогичному epoch-revocation: отзыв фиксируется в цепочке, задачи на старый measurement отклоняются с момента finality.

8.5 Federated learning: верифицированный ground-truth без передачи данных

AI-лаборатории публикуют FL-задачи с предоплаченным бюджетом по той же escrow-дисциплине, что и Missions. Маршрутизация: только кошельки с флагом FL_CONSENT — контракт не маршрутизирует задачи на кошельки без флага; статус флага как свойства байткода — вопрос спеки. Task payload содержит инициализатор модельной дельты и критерии выборки (категории, форма когорты) и никогда — данные других пользователей. На устройстве шаг обучения выполняется поверх персональной on-device модели пользователя и локального feature store; градиенты клиппируются per-sample и шумятся Gaussian-механизмом при $\epsilon=1.0$; обновки подписываются epoch-ключом с PoB-доказательством живости человека. Агрегация обновлений происходит внутри TDX-контура: агрегатор видит сумму, не вклады. Оплата — за принятую обновку после quality-гейта на held-out валидации внутри анклава; Sybil-сопротивление обеспечивается связкой PoB + epoch-аттестация + rate-limit задач на кошелёк. Лаборатория получает глобальную дельту модели и аттестационный пакет происхождения: верифицированный человеческий ground-truth без единого переданного примера.

8.6 Пост-квантовая граница и честный threat model

Kyber-768 (ML-KEM-768, FIPS 203) активируется в Фазе 3 как hybrid KEM: $\text{SharedSecret} = \text{SHA-256}(\text{Kyber_shared} \parallel \text{X25519_shared})$ — компрометация одного примитива не компрометирует сессию. Граница: угроза harvest-now-decrypt-later направлена не на сессии, а на хранящиеся Blob A/B, обёрнутые в классические публичные ключи. Поэтому Фаза 3 включает key re-wrap кампанию: Blob'ы пере-оборачиваются в hybrid-KEM конверт

в фоновом режиме без действия пользователя; до её завершения остаётся остаточное окно экспозиции архивных копий. Payload-шифрование остаётся AES-256-GCM: граница Гровера для 256-битного ключа оставляет симметрию вне практического квантового риска, и пост-квантовые усилия сосредоточены там, где риск реален, — на key wrap и handshake.

8.7 Гейты Фазы 3 и перенос инвариантов

Вход в Фазу 3 гейтуется четырьмя условиями: 5 000 opted-in FL-пользователей; B2B MRR > \$10K устойчиво в течение 3 месяцев; PoB FPR $\leq 2\%$ устойчиво в течение 90 дней; аттестационный трек-рекорд без инцидентов. Гейт не пройден — Фаза 2 продолжает работать и зарабатывать: децентрализация не является дедлайном и не является условием выживания протокола. Инварианты Главы 1.6 и hard limits Главы 6.7 переносятся в Фазу 3 без изменений. Токеномика не приобретает новой эмиссии: вознаграждение воркеров и верификаторов формируется из бюджетов задач и среза казны протокола, никогда из mint() [DESIGN — NOT DEPLOYED]. Полная токеномика, включая механику splitter'a и pre-TGE IOU, — Глава 9.

ГЛАВА 9. ТОКЕНОМИКА \$HSIG: REAL YIELD И ИММУТАБЕЛЬНЫЙ РАСЧЁТ

Статус главы: [DESIGN — NOT DEPLOYED]. Токен-контракт и Revenue Splitter не реализованы и не задеплоены; на TON Testnet жив только Identity Vault; ни одной committed-даты TGE.

9.1 Зачем протоколу токен

\$HSIG — не спекулятивный emission-токен и не субсидия роста. Это расчётный актив протокола: единица, в которой пользователи получают долю B2B-выручки, рефереры — сетевой доход, а экономика протокола становится видимой on-chain. Ответ на очевидный вопрос «почему не платить стейблкоинами напрямую»: стейблкоин-выплаты закрыли бы сторону пользователя, но не создали бы общего экономического слоя между четырьмя сторонами протокола — контрибьюторами, реферерами, покупателями и казной. Токен с

фиксированным supply даёт сети собственный расчётный актив: рост B2B-спроса создаёт спрос на тот же актив, который получают пользователи, без выпуска новой единицы.

Токен не подменяет выручку — он является учётом и рельсой выручки: делает утверждение «80% каждого платежа возвращается людям, породившим данные» исполняемым кодом, а не обещанием.

9.2 Спецификация и целостность supply

\$HSIG — jetton стандарта TEP-74 на TON. Спецификация (Proposed, контрактный слой не задеплоен; live сегодня только Identity Vault на Testnet):

Supply: 1 000 000 000 токенов, фиксирован при деплое, не расширяем.

Decimals: 9 (TBD — конвенция TON, не утверждённое решение ForeMetric).

Mint: в проекте контракта функции mint() нет; при деплое фиксируется байткод, после которого ни голосование, ни admin-ключ, ни казна, ни «аварийный процесс» не увеличит supply: no-mint — контрактный инвариант, а не маркетинговое утверждение.

Admin override: отсутствует. Нет owner-ключей с mint-полномочиями, нет emergency-pause хуков в сплиттере, нет функций модификации supply.

Запрещённые механики вознаграждения — каждая потребовала бы несуществующий mint: connect-wallet бонусы, daily login, streak-бонусы, tap-to-earn гранты, лидерборд-множители, многоуровневые реферальные эмиссии, ретро-аирдропы без revenue-обеспечения, инфляция «под валидаторов». Санкционированные источники токенов: B2B-платежи через buyback; prepaid sponsor-эскроу миссий; pre-TGE IOU-конверсия по фиксированному курсу; гранты казны с явной пометкой treasury spend. Всё остальное потребовало бы несуществующий mint.

9.3 Revenue Splitter: 80/10/10 и правило 80/20

Revenue Splitter — иммутабельный TVM-контракт в центре токеномики; не реализован и не задеплоен (на TON Testnet жив только Identity Vault); каждый B2B-платёж проходит через него. Распределение на платёж: 80% контрибьюторам когорты пропорционально

весам вклада; 10% реферерам (прямой реферер каждого контрибьютора, из той же транзакции); 10% казне протокола (инфраструктура, аудиты, юридический комплаенс).

Правило отсутствия реферера: если у контрибьютора нет записанного реферера, реферальные 10% уходят в казну — эффективный сплит 80/20. Невостребованный срез никогда не сжигается и не перераспределяется другим пользователям. Правило зашивается в байткод при деплое на mainnet; будучи иммутабельным, оно не может быть добавлено или изменено позже.

Реферальная система строго одноуровневая: реферер получает ровно 10% валовой выручки, атрибутированной прямому приглашённому, навсегда. Второго уровня, командных бонусов, рангов и бинарных деревьев нет структурно: сплиттер не содержит типов данных, способных отслеживать second-degree связи. 80% пользователя никогда не уменьшаются на 10% реферера — доли вычисляются независимо в одном settlement-событии. Юридически и экономически ForeMetric — revenue-sharing протокол, не пирамида: источник доходности — B2B-спрос, а не покупки токена новыми участниками.

Админ-обхода нет: ни emergency withdrawal, ни перенаправления пользовательских долей, ни founder-правок сплита после роста сообщества. Аудит до mainnet-депоя; после депоя поведение фиксировано навсегда.

9.4 Real yield через buyback

Платёж покупателя приходит в стейблкоине (USDT на TON). Протокол конвертирует пользовательскую долю в \$HSIG через DEX-buyback с TWAP-защитой [PLANNED, POST-TGE, no committed date] и распределяет купленные токены когорте. Связь прямая: B2B-спрос создаёт рыночное давление покупки, которое финансирует выплату. Пользователи зарабатывают не потому, что токен инфлирует, а потому, что бизнес заплатил за ответ и протокол купил \$HSIG для расчёта этого ответа. Если инсайты никто не покупает — real yield отсутствует; это честно по построению.

Механика на платёж, пошагово: (1) клиент платит стейблкоином; (2) сплиттер инициирует buyback 80% через роутер DeDust/Ston.fi с $\text{min_amount_out} = \text{floor}(\text{oracle_price} \times 0.99)$, где oracle_price — 30-минутный TWAP из on-chain фидов (защита от sandwich и flash-

манипуляций на тонких парах); на платежах, крупных относительно глубины пула, исполнение растягивается во времени — пользователь получает токены с короткой задержкой расчёта, а не худшую цену; (3) купленные токены распределяются когорте по весам; (4) реферальные доли уходят реферерам; (5) доля казны — зачисляется в казну. Bounce-обработка асинхронной цепочки TON явна: при bounce свопа контракт держит USDT, эмитит `swap_failed` и повторяет свап до трёх раз с корректировкой `slippage`; после исчерпания ретраев средства остаются в контракте с флагом на `manual resolution multisig` — потери on-chain активов нет ни при каком числе ретраев.

9.5 Атрибуция вклада

Сложнейшая часть честных выплат — определить, чьи данные породили ответ. ForeMetric использует когортную атрибуцию, а не перепродажу профилей. На каждый запрос settlement-система фиксирует: `query id`, хеш `query plan`, когортный фильтр, порог минимальной когорты, корни входных батчей, множество псевдонимных `user_hash` контрибьюторов, веса вклада, параметры DP, хеш отчёта, сумму платежа и ссылку settlement-транзакции.

Веса зависят от категорий сигналов, использованных запросом, и качества вклада: mortgage-запрос тяжелее весит DNS-интент и `location context`; mobility-запрос — инерционные сигналы; fraud-запрос дисконтирует сессии с высоким `P_bot` — Proof-of-Behavior умножает вклад на $(1 - P_bot)$, масштабируя подозрительные сессии к нулю вместо бана. B2B-клиент никогда не видит список контрибьюторов; settlement видит только псевдонимное множество, необходимое для распределения; публичные `proof`'ы раскрывают агрегированную корректность, не личности. Формула выплат одинакова для всех и не содержит серверных множителей, невидимых пользователю: $\text{веса} = \text{категории сигналов, использованных запросом, плюс качество вклада} (PoB \times (1 - P_bot))$.

9.6 Pre-TGE накопление, TGE и дисциплина раскрытия

\$HSIG не существует on-chain до TGE. Пользователи Фазы 1 накапливают IOU-балансы в PostgreSQL-леджере с ACID-гарантиями; дизайн — ежедневная анкеровка Merkle Root к

TON Testnet [PLANNED, not live]. Правила периода накопления: баланс виден в реальном времени через тикер (rate_per_hour + 2-минутный TTL-guardrail); курс конверсии IOU→\$HSIG фиксируется и публикуется до запуска Фазы 1 и неизменяем после публикации; на TGE весь накопленный баланс конвертируется 1:1 в claimable \$HSIG одним snapshot Merkle Drop на Mainnet [PLANNED, POST-TGE, no committed date]; частичных выводов, ранних выходов и вторичного рынка IOU нет. UI говорит прямо: баланс pre-TGE, конвертируется по объявленному курсу, до TGE не выводится, в момент снапшота claimable целиком.

Шестимесячный лок — продукт, а не ограничение: к моменту открытия выводов одновременно выполняются три условия — протокол держит шесть месяцев B2B-ценных данных (реальный спрос за токеном на листинге), Day-7 ретеншен доказан инвесторам, тысячи пользователей держат claimable-балансы и создают claim-driven интерес к покупке. Лок строит актив до монетизации.

TGE происходит одновременно с запуском Фазы 2: снапшот финального IOU-лидjera коммитится on-chain; claim-контракт открывает выводы по Merkle Proof через Mini App с проверкой неповторности; ликвидность размещается на DeDust и Ston.fi; с этого момента сплиттер работает на каждом B2B-платеже. Рамка запуска: community-distributed at TGE; распределение пропорционально фактическому вкладу данных Фазы 1. Токен инвесторам не продаётся.

Vesting и раскрытия: командные и contributor-токены размещаются в отдельном vesting-контракте (не в сплиттере: байткод распределения выручки остаётся минимальным — меньше аудит-поверхность); условия вестинга закреплены в спецификации (отдельный vesting-контракт) и публикуются до TGE. Community-награды не несут лока сверх периода накопления: claimed-токены ликвидны. Механика launch-ликвидности (аллокация, LP-локапы, router-ограничения) — операционное решение момента TGE, публикуется в token launch disclosure. Любые локи, применяемые к community-наградам, раскрываются до распределения, никогда ретроактивно: ретро-изменения обещанных аллокаций архитектурно исключены иммутабельностью.

9.7 Потоки токенов: источники и стоки

При отсутствии mint каждый \$HSIG у пользователя имеет одно из двух происхождений: TGE Merkle Drop (конверсия IOU-снапшота) или DEX-buyback, финансируемый B2B-платежом либо prepaid-эскроу спонсора миссии. Сток — 0.1% burn на P2P-переводах: постоянное малое дефляционное давление; при этом распределения Revenue Splitter от burn освобождены — выплаты пользователей никогда им не уменьшаются. Sponsor-миссии — единственное проектируемое исключение из «никакой новой токеновой стоимости»: награды миссий на 100% покрыты prepaid-эскроу спонсора — funded, never minted. Итоговая петля: B2B-спрос покупает токен с рынка → токен доходит до пользователей → P2P-переводы сжигают малую часть → следующий платёж покупает снова. Circulating supply отвечает на реальную коммерческую активность в обе стороны. Обращения к Oracle не тарифицируются токенами: инференс брифинга выполняется на устройстве, когортный базис доставляется обезличенным агрегатом через дифференциальную приватность (7.7).

Правило стоимости: бесплатность Oracle — следствие архитектуры, а не обещание. Пер-запросных серверных вычислений нет: брифинг считает устройство пользователя, когортный базис доставляется амортизированным батчем, дорогие B2B-совпадения в анклавах оплачивает покупатель через Revenue Splitter (9.3). Если будущая реализация Фазы 2 потребует серверных вычислений на один запрос (например, TEE-инференс по требованию), вопрос тарификации возвращается на стол решений как новый открытый вопрос дизайна — до этого сжигание \$HSIG за Oracle не предусмотрено.

9.8 Юнит-экономика одного платежа

Финтех-клиент платит \$10 000 за предиктивный когортный отчёт. \$8 000 уходят в buyback-бюджет: сплиттер исполняет TWAP-защищённые покупки \$HSIG и распределяет купленное когорте по весам вклада. \$1 000 — реферерам контрибьюторов; у контрибьюторов без реферера их срезы уходят в казну. \$1 000 — казне протокола. Эти \$8 000 не напечатаны: они конвертированы в рыночный спрос на \$HSIG в момент расчёта. Петля «инсайт → доход» замыкается внутри одного settlement-цикла.

9.9 Риски и честные пределы дизайна

Чего токеномика не защищает и что мы не обещаем. Глубина ликвидности не гарантирована архитектурой: при нулевой B2B-выручке buyback нулевой; у токена нет инфляционного «пола» — его ценность отражает фактический спрос на инсайты ForeMetric; ответ протокола — не token engineering, а B2B go-to-market Фазы 1. Ранняя концентрация: тяжёлые контрибьюторы pre-TGE держат пропорционально больше на снапшоте — это задуманное распределение по вкладу, но оно же означает повышенное sell-давление на TGE; контрвесы — claim-driven интерес и условия ликвидности, публикуемые в launch disclosure до снапшота. DEX execution risk: TWAP защищает от манипуляций, но не от тонкой ликвидности; крупные платежи рассчитываются во времени, не мгновенно. Регуляторная позиция: \$HSIG позиционируется как utility-токен весь жизненный цикл; community-distributed модель выбрана именно чтобы избежать признаков инвестиционного инструмента; это design intent, не юридическая гарантия — jurisdiction-анализ продолжается. Языковая дисциплина: интерфейс показывает оценки \$HSIG/день и исторические ставки, но не обещает фиксированный фиатный доход; все pre-TGE балансы описываются как IOU, не ликвидные токены. Масштабирование цифр: все абсолютные величины главы — ставки, чеки, доходы — иллюстративные пропорции, калибруемые по реальной B2B-выручке на запуске Фазы 2; архитектурные обязательства — это сплит-пропорции, фиксированный supply, механика buyback и иммутабельность всех трёх.

\$HSIG спроектирован скучным в лучшем смысле: фиксированный supply, нет mint, revenue-backed выплаты, одноуровневый реферал, ежедневный Merkle-settlement, никакой печати токенов под видом дохода пользователей. Если спрос на инсайты существует — токен его отражает. Если нет — токен не спрячет провал за инфляцией.

9.10 Чего токен не обещает

Четыре прямых не-обещания — по одному на каждое ожидание, с которым приходят к токену. Каждое следует из механик этой главы, а не добавлено дисклеймером.

Цены. Buyback выполняется при каждом B2B-платеже, но его объём пропорционален выручке. Рост цены не гарантирован и не обещается: у токена нет инфляционного «пола» и нет поддержки курса, кроме реального спроса на инсайты (9.4, 9.9).

Дохода. Доход пользователей — доля B2B-платежей покупателей, а не эмиссия: при малом спросе доход мал, и токены не выпускаются, чтобы это компенсировать (9.1, 9.7).

Рынка и сроков. Листинг, глубина ликвидности и календарные сроки не обещаются: TGE совпадает с запуском Фазы 2 и определяется гейтами, а не датой; условия ликвидности публикуются до снапшота (9.6, 11.1).

Вывода до TGE. Баланс до запуска токена — запись IOU-леджера: вывести, продать или передать её нельзя; частичных выводов и вторичного рынка IOU нет (9.6).

ГЛАВА 10. КОНКУРЕНЦИЯ И РВЫ

10.1 Почему сравниваем по свойствам, а не по лейблам

Рынок «данных с приватностью» полон маркетинговых клеймов: «user-owned data», «privacy-first», «decentralized». Клейма непроверяемы, поэтому мы сравниваем архитектуру по шести свойствам, каждое из которых дилидженс может проверить за один день: чтением privacy-политики, наличием export-эндпоинта, байткодом сплиттера, аттестационным отчётом, структурой выплат. Таблица ниже — не позиционирование, а чек-лист; любая строка, где ForeMetric не соответствует собственному утверждению на дату проверки, является нашим провалом, а не нюансом.

10.2 Шесть проверяемых свойств

Свойство	Что проверяет дилидженс	ForeMetric
Consent-архитектура	Opt-in на уровне протокола, per-category тумблеры, обратимость без последствий	Тумблеры категорий в TMA/native app; отзыв = burn_keys или отключение канала; Message Metadata не существует
Происхождение данных	Пассивный мобильный сигнал против экспортов, скрейпинга, активных задач	Phase 1: TMA session events + опциональный DNS; Phase 2: мультимодальный on-device сбор
Граница покупателя	Существует ли export-эндпоинт; применяются ли DP-пороги	Export-эндпоинта нет по построению; $\epsilon=4.0$, min cohort 50, агрегированный отказ ниже порога [PLANNED PHASE 2]; в Фазе 1 — aggregate-only без DP-механики
Компенсация	Из чего платят: эмиссия, разовые гонорары или доля выручки	80% gross каждого платежа через иммутабельный сплиттер; no mint; эмиссия отсутствует
Доверие к compute	Верифицируема ли обработка третьей стороной	Phase 2: SEV-SNP + COCOON TDX, client-verifiable quotes; правило двух входов
Ретеншен источника	Есть ли ежедневная личная польза вне баланса	Oracle + баланс-тикер + Signal Passport C2C; ретеншен не покупается эмиссией

10.3 Ландшафт: пять категорий и одна не-категория

Data brokers (LiveRamp, Acxiom, брокеражный длинный хвост): спрос и инфраструктура есть, consent-архитектуры и компенсации нет; \$278B рынок построен на поведении, которое люди не соглашались продавать. Мы не конкурируем с ними за покупателей, мы конкурируем за источник: их supply-модель юридически и репутационно хрупнет быстрее, чем наша вырастет.

Consented panels (Prolific, UserTesting): consent честный, но сбор активный (опросы, задачи), выборка смещена к профессиональным респондентам, компенсация разовая и не связана с последующей выручкой. Пассивной мобильной плотности сигнала и токенового settlement-контура нет.

DePIN data-сети (Grass и подобные): доказали, что крипто-settlement пассивного вклада работает на масштабе — и одновременно показали предел: их сигнал (прокси-трафик, bandwidth) не является согласованным поведенческим инсайтом, а выплаты не привязаны к выручке за конкретный покупательский запрос. Когда сетевые стимулы ослабевают, ретеншен источника исчезает.

Data DAOs и personal data vaults (Vana, Ocean): валидируют нарратив «личные данные как актив пользователя» — это важная для нас валидация категории (см. 10.4).

Annotation marketplaces (Scale, Surge): доказывают цену верифицированного человеческого труда (\$30-50/час) — но это активный труд, а не пассивный сигнал, и компенсация не масштабируется после сдачи задачи.

Confidential-computing маркетплейсы (generic TEE-провайдеры): имеют аттестованный compute, но не имеют ни согласованного data-актива, ни дистрибуции, ни settlement-контура. Они — поставщики нам, а не конкуренты: COCOON-воркеры ровно такого рода.

10.4 Честное чтение Vana

Vana — ближайший идеологический сосед, и мы относимся к ней серьёзно. Что она валидирует: рынок принимает идею пользовательской собственности на данные; Data DAO-структуры и contribution-награды работают как нарратив привлечения; «личные данные для обучения AI» продаются как категория. Где архитектуры расходятся по проверяемым осям: origin — Vana строится преимущественно вокруг веб-кошелька и пользовательских экспортов (Takeout-файлы, подключённые аккаунты), то есть вокруг данных, которые пользователь уже отдал кому-то другому; мы строим вокруг пассивного мобильного сигнала, который рождается на устройстве и не покидает его в сыром виде. Что получает покупатель — Vana лицензирует пулы данных для обучения моделей: покупатель в конечном счёте получает данные; наш покупатель получает ответ и не может

получить данные, потому что export-эндпоинта не существует. Компенсация — награды Vana привязаны к вкладу в DAO и токен-инсентивам; наша — к каждому конкретному B2B-платежу через иммутабельный сплиттер, и это различие проверяется чтением байткода, а не whitepaper. Ретеншен — у Vana нет ежедневного личного utility-слоя (Oracle-класса), который держал бы источник онлайн между продажами. Мы не утверждаем, что Vana «не работает»; мы утверждаем, что её контур и наш контур решают разные задачи, и наш — про непрерывный пассивный сигнал с непрерывной же выплатой.

10.5 Контур, который никто не замыкает

Каждый игрок ландшафта замыкает часть контура: брокеры — спрос и инфраструктуру без consent; панели — consent без пассивного масштаба; DePIN — пассивный масштаб и крипто-settlement без согласованного поведенческого сигнала и без aggregate-only границы; data DAOs — нарратив собственности без мобильной плотности и аттестованного compute; annotation — цену верифицированного человека без пассивности; TEE-маркетплейсы — compute без актива и дистрибуции. Утверждение ForeMetric не в том, что мы изобрели каждый узел, а в том, что мы замыкаем все шесть свойств в одном контуре: согласованный мобильный сбор → зашифрованное хранение → аттестованный compute → aggregate-only ответ → иммутабельный revenue-share settlement → ежедневный личный utility, держащий источник онлайн. Ценность контура сверх суммы узлов — в том, что каждый пройденный цикл делает следующий дешевле: история сигнала длиннее, когорты плотнее, аттестационный трек-рекорд длиннее, реферальная дистрибуция шире.

10.6 Рвы: что дорожает со временем

Un-backdateable data asset. Продольная согласованная поведенческая история накапливается только в реальном времени: конкурент, стартовавший в 2028-м, не может купить, соскрести или догенерировать когорты 2026-2027 годов.

Наш актив не воспроизводится капиталом — только временем и согласием людей.

Иммутабельный settlement-контур.

Доверие «пользователи реально получают 80%» проверяемо on-chain постфактум:

каждая settlement-транзакция с query id, корнями батчей, весами и DP-параметрами — публичный аудиторский след. Копировать можно пропорции; нельзя скопировать накопленный аудиторский трек-рекорд без прохождения того же времени.

Дорогая цепочка аттестации. Freeze-grade evidence-стандарт (hook-emitted envelope, immutable build binding, negative-probe валидатор, conformance-кейсы регистрационного контракта, открытая спецификация) — инженерный капитал в кварталы работы, который к тому же работает как trust-моат: наша проверяемость публична, и её цена воспроизводства для конкурента включает не только код, но и репутационную ставку.

Самофинансируемый сетевой эффект (Anti-Ponzi Flywheel). Большинство DePIN и Data-сетей распадаются, когда заканчивается эмиссионное топливо: майнеры и пользователи уходят, как только падает доходность от печати токенов. Ров ForeMetric — в смене парадигмы удержания и роста, где маховик не требует постоянного инфляционного «подлива» для поддержания оборотов.

Привлечение (Acquisition) обеспечивается не эмиссией, а реальной B2B-выручкой (через одноуровневый 10% реферальный сплит) и C2C-создателями, которые приводят аудиторию через QR-коды Signal Passport, превращая верифицированный профиль в актив. Удержание (Retention) обеспечивается слоем Oracle — персональным предиктивным ассистентом, дающим ежедневную ценность (утренние брифинги, окна фокуса, тренды здоровья) вне зависимости от баланса.

Пользователь остается в приложении, потому что Oracle полезен ему лично; приводит друзей, потому что рефералка платит живые деньги от B2B-сектора; монетизирует аудиторию, потому что C2C-Паспорт превращает его профиль в актив. Telegram-native онбординг до 30 секунд держит конверсию, а каждая новая когорта снижает предельную стоимость привлечения следующей без рекламного бюджета.

Это устойчивая бизнес-модель, упакованная в крипто-рельсу. Полная механика трёх контуров роста и ответ на возражение об «отсутствии эмиссионного топлива» — 3.7.

10.7 Фальсификаторы позиции

Позиция честна только тогда, когда названы наблюдения, которые её убивают:

Ретеншен-контур ложен, если Day-7 retention альфы ниже 20% и не поднимается после включения Oracle/Passport-экспериментов: без ежедневной причины вернуться источник гаснет, и контур распадается на разовые панели.

B2B-спрос ложен, если первые 3-5 paid-пилотов не конвертируются в повторные покупки и MRR не достигает \$3K/месяц к гейту Фазы 2: тогда «инсайт, а не датасет» не является покупной ценностью.

Компенсационный контур ложен, если при реальных ценах начисления ниже порога, при котором пользователи держат тумблеры включёнными (отток consent-ов растёт): 80% от малого числа всё ещё мало.

Юнит-экономика аттестованного compute ложна, если стоимость аттестации и TEE-инференса на запрос превышает валовую маржу при реалистичных размерах когорты: тогда Фаза 2 экономически не включается.

Дифференциация схлопывается до скорости исполнения, если Vana или крупный брокер запускает мобильный пассивный consented-сбор с revenue-share: тогда наш моат — время и трек-рекорд, а не уникальность идеи, и мы должны выиграть исполнением, а не нарративом.

Каждый фальсификатор привязан к измеримому гейту Главы 11.

ГЛАВА 11. ROADMAP, ГЕЙТЫ, КОМАНДА, ФИНАНСИРОВАНИЕ, РЕЕСТР РИСКОВ

11.1 Roadmap с метрическими гейтами

ForeMetric не публикует календарных дат запуска фаз — это дисциплина, а не скромность. Переходы между фазами гейтуются метриками; если гейт не пройден, фаза продолжается, и это не провал, а корректная работа дисциплины капитала. Три гейта, каждый с явным условием входа в следующую фазу и явным условием остановки. Календарные окна

(включая декабрь 2026 для закрытой альфы) — планировочные оценки; гейты — метрические:

Гейт Фазы 1 → Фаза 2:

Closed alpha: 500 инвайтов, декабрь 2026.

Day-7 retention $\geq 20\%$ на когорте инвайтов.

Первый платный B2B-пилот \$1-5K подписан и выполнен.

B2B MRR $\geq$ \$3K/месяц устойчиво в течение 3 месяцев.

End-to-end аттестация SEV-SNP + COCOON TDX верифицируема третьей стороной.

Обеспеченный runway 12+ месяцев после входа в Фазу 2 (11.4).

Если гейт не пройден — Фаза 1 продолжается с расширенной валидацией, раунд не расходуется на инфраструктуру, для которой нет спроса.

Гейт Фазы 2 → Фаза 3:

5 000 opted-in FL-пользователей (активный флаг FL_CONSENT).

B2B MRR $>$ \$10K устойчиво 3 месяца.

Proof-of-Behavior FPR $\leq 2\%$ устойчиво 90 дней.

Аттестационный трек-рекорд без инцидентов.

Гейт TGE:

TGE совпадает с запуском Фазы 2, не раньше.

Условия ликвидности публикуются в token launch disclosure до снапшота.

Шестимесячный период накопления pre-TGE встроен в продукт; на TGE весь накопленный баланс конвертируется 1:1 и claimable.

Никаких «Q1 2027», «конец года» или «в течение 18 месяцев» как обещаний.

Календарные обещания вне обязательств проекта: единственная форма обязательства — метрический гейт.

Что нас опровергнет. Гейты выше фиксируют, когда мы двигаемся дальше. Здесь — противоположное: при каких наблюдениях мы признаём неправоту и переделываем

продукт, не расходуя капитал следующей фазы. Заранее названные фальсификаторы — та же дисциплина, что и гейты, только в обратную сторону.

Ретеншен-контур ложен, если Day-7 retention альфы ниже 20% и не поднимается после включения Oracle/Passport-экспериментов: без ежедневной причины вернуться источник гаснет, и контур распадается на разовые панели.

B2B-спрос ложен, если первые 3-5 paid-пилотов не конвертируются в повторные покупки и MRR не достигает \$3K/месяц к гейту Фазы 2: тогда «инсайт, а не датасет» не является покупной ценностью.

Компенсационный контур ложен, если при реальных ценах начисления ниже порога, при котором пользователи держат тумблеры включёнными (отток consent-ов растёт): 80% от малого числа всё ещё мало.

Юнит-экономика аттестованного compute ложна, если стоимость аттестации и TEE-инференса на запрос превышает валовую маржу при реалистичных размерах когорт: тогда Фаза 2 экономически не включается.

Дифференциация схлопывается до скорости исполнения, если Vana или крупный брокер запускает мобильный пассивный consented-сбор с revenue-share: тогда наш моат — время и трек-рекорд, а не уникальность идеи, и мы должны выиграть исполнением, а не нарративом.

Каждый фальсификатор привязан к измеримому гейту Главы 11; проект, который не готов умереть на собственном гейте, не имеет позиции, а имеет надежду.

11.2 Честное состояние на октябрь 2026

Live сегодня:

Публичный симулированный прототип foremetric.ai (симулированные данные, помечены).

Задеплоенный Rust/Axum бэкенд с PostgreSQL IOU-ledgerом.

Identity Vault смарт-контракт на TON Testnet (верифицируемо в эксплорере).

В разработке:

Фронтенд ТМА: интеграция регистрационного контракта (Proposed) не завершена и заблокирована финальной ревизией и готовностью бэкенда — текущая тестовая среда и живой API работают на прежней (легаси) схеме регистрации; выбор рельсы декабрьской альфы — решение продукта (см. 11.5).

DoH/DoT DNS-сервер (hickory-dns).

Инфраструктура Daily Merkle Drop [PLANNED, not live].

Фикстуры init_data HMAC (в работе; материал — после фриза контракта).

Реестр доказательств ведётся; статусы и артефакты — в закрытом Data Room по запросу.

Не начато:

Native app, TEE-деплой, TGE, автоматические on-chain выплаты, Signal Passport, Missions, Oracle, FL — всё гейтуется доказательством спроса.

Коммерческий статус:

Закрытая альфа до 500 инвайтов — декабрь 2026, гейт Day-7 $\geq 20\%$.

Первый платный пилот \$1-5K — валидируемая гипотеза [PHASE 1 PILOT OFFER — not yet signed].

11.3 Команда

Четыре ко-фаундера, распределённые по четырём странам. Проект ведётся с начала 2026 года.

Sergey Chernyshov (Россия) — Founder, Product Owner. Full-time с начала 2026.

Продуктовая архитектура, fundraising, GTM и первые B2B-продажи (нетворк и прямой outreach), критический путь альфы. Финальные решения.

Thao Dinh (Вьетнам) — Lead Core Architect. В команде с августа 2026. Владеет: reusable mapper/evidence слой, Phase 2 specs, регистрационный контракт, TEE design.

Mohammad Ayaz (Пакистан) — Frontend Lead. ТМА автор; подготовил evidence совместимости четырёх кошельков с TON Connect. В команде с июня 2026. Владеет:

TMA alpha (декабрь 2026, 500 инвайтов, Day-7 $\geq$ 20%), frontend-интеграция mapper, деплой и пересъёмка evidence.

Prashant Rahulkar (Индия) — Backend Lead. В команде вскоре после Mohammad.

Владеет: Axum backend, PostgreSQL IOU-леджер, Tolk контракты, backend DTO/verifier согласование.

Доли основателей подлежат вестингу по соглашению каждого основателя. Токен-аллокации (\$HSIG) отделены от equity компании: аллокации протокола — по графику вестинга токенов, планируются к исполнению on-chain, не через капстол.

11.4 Стратегия финансирования

Условия финансирования — цель раунда, структура, use of funds и runway — в публичной редакции не раскрываются: материал предоставляется квалифицированным инвесторам в закрытом Data Room по запросу (полная редакция настоящего документа). Запросы — через foremetric.ai.

Единственное публичное обязательство капитала — гейт Фазы 2 «обеспеченный runway 12+ месяцев» (11.1).

11.5 Реестр рисков

Риск	Вероятность	Impact	Владелец	Митигация
Альфа не проходит гейт Day-7 $\geq$ 20%	Medium	High	фронтенд	Итеративный UX-testing; Oracle/Passport эксперименты как ретеншен-крюки (прототипные проверки гипотез, не запуск слоёв Фазы 2); если гейт не пройден — Фаза 1 продолжается, Фаза 2 не активируется
Первый B2B-пилот не подписан	Medium	High	Sergey	Outreach wave активен; если спрос не валидируется — pivot wedge, не

				инфраструктура
ТЕЕ-инференс дороже маржи	Medium	High	архитектура	Pilot pricing \$1-5K калибруется по реальной стоимости; если юнит-экономика не сходится — pivot на off-chain aggregation с раскрытием
Регуляторная реклассификация \$HSIG	Low	High	Sergey	Community-distributed модель; utility-позиционирование; jurisdiction-анализ продолжается; если реклассификация — pivot на off-chain settlement
Конкурент (Vana, брокер) запускает мобильный passive consented сбор	Low	High	Все	Моат — время и трек-рекорд; выигрываем исполнением, не нарративом
Model Collapse не создаёт покупательской срочности	Medium	Medium	Sergey	Pivot на post-cookie деградацию intent-данных (Criteo 60%); Model Collapse — нарратив, не триггер
Per-contributor доход ниже порога удержания тумблеров	Medium	High	фронтенд	Honest disclosure в UI; если отток consent растёт — pivot pricing, не инфраструктура
Интеграция криптографического контракта в клиент не завершена к декабрьской альфе	High	Medium	продукт / бэкенд	Выбор скоупа за продуктом: (А) альфа на прежней (легаси) рельсе — валидирует ретеншен и consent-гипотезу, а не криптографический контракт; (В) ожидание финальной ревизии контракта и её реализация. Ретеншен-гипотеза не блокируется.

Правило реестра: каждый риск имеет владельца и митигацию; риски без митигации — это не риски, это надежды. Реестр пересматривается quarterly; новые риски добавляются с владельцами и митигациями, не как наблюдения.

11.6 Заключение

ForeMetric — инфраструктура поведенческих данных с защитой приватности, которая превращает согласованный мобильный сигнал в доход для людей и верифицированные инсайты для бизнеса. Мы не продаём данные, мы продаём ответы. Мы не обещаем доход, мы строим контур, где доход — следствие реальной B2B-выручки. Мы не обещаем децентрализацию, мы строим её фазами с метрическими гейтами.

Этот документ — спецификация, а не маркетинг: каждое утверждение сформулировано так, чтобы его можно было проверить — кодом, контрактом, аттестационным отчётом или settlement-транзакцией.

Мы строим ForeMetric как инфраструктуру, которая переживёт нас: иммутабельные контракты, проверяемые спецификации, честные раскрытия ограничений. Если проект получится — он создаст новый стандарт того, как поведенческие данные могут быть этичными и прибыльными одновременно. Если проект не получится — он завершится честно, с проверяемым следом того, что было построено и что не сработало.

В этом точка.

ПРИЛОЖЕНИЕ А. ГЛОССАРИЙ

TMA — Telegram Mini App: точка входа и consent-рельса Фазы 1.

IOU-ledger — PostgreSQL-ledger pre-token балансов Фазы 1 с ACID-гарантиями; конвертируется 1:1 в \$HSIG на TGE.

DataKey — per-user 256-битный AES-ключ, шифрующий поведенческие blob'ы; существует только в двух зашифрованных копиях.

Blob A / Blob B — копии DataKey: под публичный ключ TON-кошелька пользователя / под ключ вычислительной стороны (KMS в Фазе 1, VM-bound в Фазе 2).

burn_keys() / crypto-shredding — уничтожение DataKey как механизм удаления: шифротекст становится шумом за ~5 секунд.

ϵ (эпсилон) — бюджет дифференциальной приватности: 4.0 на B2B-выходах, 1.0 на FL-обновках.

Min cohort 50 — жёсткий порог: запрос ниже порога возвращает агрегированный отказ, не ослабленный ответ.

SEV-SNP / TDX / COCOON — AMD confidential VM (application layer) / технология Intel TDX-воркеров / сеть COCOON TDX-воркеров: report boundary в Фазе 2, децентрализованный дефолт в Фазе 3.

Attestation quote / measurement — подписанное hardware-доказательство исполнения кода / хеш кода, против которого проверяется quote.

Правило двух входов — COCOON принимает только {текст запроса, анонимизированные агрегаты}; DataKey и сырые векторы — compile-time type error.

PoB (Proof-of-Behavior) — 1D-CNN по инерциальным сигналам: подпись человеческой моторики, гейт $FPR \leq 2\%$ (бюджет FNR).

Персональная on-device модель пользователя — компилируется на устройстве из собственной истории пользователя; основа Oracle; никогда не покидает устройство (закрепление термина в спеке).

Oracle — персональный предиктивный слой с citation contract [PLANNED PHASE 2].

Signal Passport — подписанный грант доступа (~112 байт) к category-bounded спрезу профиля; B2B- и C2C-режимы [PLANNED PHASE 2].

Missions — брендовые задачи с prepaid-эскроу и signal-verified выполнением [PLANNED PHASE 2].

Revenue Splitter — иммутабельный TVM-контракт: 80/10/10 от gross; 80/20 при отсутствии реферера; без admin-ключа.

TGE / Merkle Drop — генерация токена / снапшот-конверсия IOU 1:1 в claimable \$HSIG [PLANNED, POST-TGE, no committed date].

Epoch key — Ed25519 ключ эпохи устройства; ротация и on-chain реестр эпох как анти-бот рельса.

Resource Governor — пять состояний регулирования sampling rate на устройстве.

Domain Query Router — декомпозиция NL-запроса на доменные подзапросы с бюджетом приватности.

Master HashmapE — TON-реестр указателей на vault'ы Фазы 2; указатели, не данные.

Trusted-operator — модель доверия Фазы 1 с явным раскрытием: оператор теоретически может прочитать данные.

Insights-as-a-Service — продуктовая граница: покупатель получает ответ, никогда датасет.

ПРИЛОЖЕНИЕ В. ИНФРАСТРУКТУРНЫЕ СТОИМОСТИ ПО ФАЗАМ

Месячные цифры калибруются по реальным инвойсам и меняются с регионом хостинга.

Ниже — структура и доминанты затрат по фазам:

Фаза 1: один VPS-класс хостинга (Axum API, PostgreSQL IOU-ledger, DNS-сервер, отчётный пайплайн) + object storage S3. Доминанта — хранение и эгресс, не compute. TON Testnet — без gas-затрат пользователя.

Фаза 2: AMD SEV-SNP bare-metal аренда (application layer) + COCOON TDX-воркеры (report boundary) + Qdrant-индекс зашифрованных embedding'ов + S3 hot + TON Storage cold. Доминанта — confidential compute и индекс; юнит-экономика на запрос калибруется первыми пилотами и является фальсификатором позиции (Глава 10.7).

Фаза 3: собственные SEV-SNP ноды перепрофилируются в COCOON-воркеры (SEV-SNP-класс); расходы смещаются в task-бюджеты и срез казны; вознаграждение воркеров формируется из бюджетов задач и казны, новой эмиссии нет [DESIGN — NOT DEPLOYED].

Правило: любая инфраструктурная позиция включается только после того, как предыдущий гейт доказал спрос; дорогие позиции (SEV-SNP, COCOON) не арендуются «на вырост».

ПРИЛОЖЕНИЕ С. ПРИОРИТЕТНЫЕ B2B-СЦЕНАРИИ: КТО И ЗА ЧТО ПЛАТИТ

Статус: [PHASE 1 PILOT OFFER — not yet signed]. На октябрь 2026 пилотных контрактов ещё не подписано (11.2). Сценарии ниже — целевые гипотезы для первых платных пилотов \$1-5K; каждый сформулирован проверяемо: кто платит, за какой ответ, что покупатель не получает никогда и что опровергает гипотезу (фальсификаторы — 10.7).

С.1 Фундамент: инфраструктура поведения в пяти слоях. ForeMetric —

инфраструктурный проект (1.1, 3.4): сначала строится рельса, затем на ней работают все продуктовые слои — B2B-терминал, Signal Passport, Oracle, миссии (3.3). Рельса — это пять слоёв: согласованный сбор поведенческих сигналов; векторизация поведения (Фаза 1 — серверная, Фаза 2 — на устройстве, сырые данные не покидают телефон, 7.2); шифрование двухключевой схемой DataKey, при которой ни оператор, ни облако не расшифровывают данные по отдельности (5.7, 6.2); распределённое хранение (Фаза 2 — S3 hot-tier + TON Storage cold-tier, Фаза 3 — только TON Storage, 8.2); аттестованная обработка в аппаратных анклавах COCOON (7.4).

Выход фундамента — предиктивный инсайт: статистически обоснованное утверждение о будущем событии, которое уже предсказуемо на когортных данных, — тайминг спроса, окно активности, кросс-интенты (1.2). Ключевое свойство фундамента — сетевой эффект достоверности: чем больше участников на рельсе, тем плотнее когорты и тем выше статистическая устойчивость закономерностей и точность предиктивных метрик; при малой панели честный ответ — «данных недостаточно», а не догадка. В Фазе 1 фундамент существует в сокращённом виде — серверная векторизация, хранение у оператора, вычисление без TEE; границы этого сокращения раскрыты в С.3, полный контур собирается в Фазах 2-3.

С.2 Что продаётся всегда: ответ, а не данные и не доступ к людям. Клиент покупает когортный ответ: агрегат по группе не меньше 50 человек. Клиент никогда не получает: сырые векторы, индивидуальные профили, экспортный эндпоинт, Message Metadata (3.2). «Достучаться» до когорты через ForeMetric нельзя: клиент не может написать нашим

пользователям, загрузить их в свой рекламный кабинет или отфильтровать по ним свою базу. Инсайт используется для настройки собственных каналов покупателя — времени показа рекламы, состава оффера, географии закупки. Это покупка исследования рынка, а не таргетинга.

С.3 Фаза 1 — когортный отчёт из TMA-телеметрии [PHASE 1 PILOT OFFER]. Продукт: когортный отчёт \$1-5K из TMA-телеметрии: размер когорты, ритм активности, тайминг, кросс-интент паттерны (3.2); founder-operated, disclosed trusted-operator (3.3). Сигналы Фазы 1: сессии мини-приложения; категории DNS-доменов тех, кто включил DNS-щит, — сервер видит категории, не содержимое (4.4).

Пример вопроса: «Когда и какие категории финансовых продуктов исследует когорта панели за последние 14 дней?» Структура ответа (иллюстрация): размер когорты; распределение активности по часам и дням недели; топ исследуемых категорий; частые переходы между категориями (например, кредитные калькуляторы → страхование).

Кто платит: продуктовые и маркетинговые команды потребительских сервисов — финтех, ритейл, маркетплейсы, — которым нужна честная карта спроса и тайминга аудитории Telegram. Что покупатель делает с ответом: переносит закупку собственной рекламы на пиковые окна, меняет состав креативов и оффера. Людей он не получает.

Граница честности: панель альфы мала (до 500 участников), DNS-щит включают не все; поэтому первый продукт — широкие срезы по всей активной панели, а не узкие сегменты; Phase 1 — aggregate-only без формальной DP-механики (DP-гарантии — Фаза 2); вычисление на стороне оператора без TEE (TEE-аттестация отчётов — Фаза 2); доля пользователей (80%) в платежах пилота до деплоя Revenue Splitter начисляется кандидат-механикой IOU — открытый вопрос дизайна.

С.4 Фаза 2 — TEE, нативное приложение и предиктивные инсайты [PLANNED PHASE 2].

Богаче сигналы: векторизация поведения на устройстве — сырые сенсорные данные не покидают телефон (7.2); сенсоры нативного приложения, гео-кластеры; когорты могут быть уже (порог 50 сохраняется).

ИИ в анклавах: вычисление проходит в COCOON TEE — модели находят закономерности в зашифрованных векторах, обобщают поведение когорт и выдают отчёт с предиктивными

метриками; отчёт несёт TDX-quote и формальные DP-гарантии (7.6). Аттестованные natural-language запросы: полный путь 7.6 — вопрос покупателя декомпозируется роутером, подзапросы исполняются внутри анклавов, покупатель верифицирует quote. Точность предиктивных метрик растёт с плотностью когорт (C.1): чем больше пользователей на рельсе, тем устойчивее закономерности и тем выше уверенность, которую отчёт может честно заявить.

Пример вопроса: «Какие категории исследует когорта за 14 дней перед крупной покупкой и в какие часы она активна?»

Signal Passport B2B: category-bounded срезы профиля по явному гранту пользователя (7.8); совпадение вычисляется в анклав, пользователь получает свою долю платежа. Здесь «достучаться» до пользователя становится впервые возможно — через его явное согласие и с выплатой ему, а не через наблюдение. B2B Missions: бренды коммисионируют signal-verified задачи из prepaid-эскроу (7.9). Цены сценариев Фазы 2 не установлены: режим Passport — untested, unpriced.

С.5 Открытый API: когда данные запрашивают сторонние проекты [PLANNED PHASE 2].

Когда субстрат доказан, рельса открывается внешним разработчикам (3.4): сторонние проекты — персональные AI-агенты, цифровые двойники, сервисы и исследовательские команды — решают через ForeMetric собственные задачи, не строя сбор, приватность и аттестацию с нуля.

Механика: запрос стороннего проекта проходит те же правила рельсы — анклав, минимальная когорта 50, aggregate-only выход, аттестация отчёта; запрос персональной истории конкретного пользователя — только через его явный per-query грант (Signal Passport, 7.8). Оплата: каждый запрос оплачивается по смарт-контракту; платёж проходит через Revenue Splitter (9.3) — 80% пользователям, чьи сигналы дали вклад в ответ, по весам вклада (9.5), 10% реферерам, 10% казне протокола. Сторонний проект платит за ответ на свой вопрос, а не за данные: экспортного эндпоинта не существует по построению (3.2).

Статус: механика и тарифы открытого API не установлены; в Фазе 1 доступ не продаётся — панель мала и TEE-контур не запущен.

С.6 Сводная таблица.

Сценарий	Кто платит	Что получает	Что не получает никогда	Фаза
Когортный отчёт (Engagement Intelligence)	продукт/маркетинг финтеха и ритейла	агрегат: ритмы, тайминг, категории	людей, данные, экспорт	1
Аттестованный NL-запрос	аналитики и маркетинг	агрегат + TDX-quote + предиктивные метрики	то же	2
Passport B2B-грант	банки, страховщики, HR-сервисы	совпадение по гранту пользователя	доступ без гранта, сырые данные	2
B2B Missions	бренды	signal-verified выполнение задач	непроверенный self-report	2
Запрос через открытый API	сторонние проекты и разработчики	агрегированный ответ на свой вопрос	людей, данные, экспорт	2

С.7 Проверка гипотезы (10.7). Гипотеза: маркетинговые команды готовы платить \$1-5K за агрегированный когортный ответ из Telegram-родной панели. Проверка: первые 3-5 paid-пилотов Фазы 1. Опровержение: пилоты не конвертируются в повторные покупки и MRR не достигает \$3K/месяц к гейту Фазы 2 — тогда «инсайт, а не датасет» не является покупной ценностью, и продукт пересматривается.

ПРИЛОЖЕНИЕ D. РЕГИСТРАЦИОННЫЙ КОНТРАКТ ФАЗЫ 1 ПРОСТЫМИ СЛОВАМИ

Приложение и сервер Фазы 1 проектируются под один общий контракт регистрации.

Ниже — его правила простыми словами: без кода и wire-форматов, но дословно по матрице интеграционных кейсов контракта (статусы — 1.5, 11.2).

Статус: [DESIGN — NOT DEPLOYED] — Proposed, freeze-кандидат, на согласовании команды; полный текст спецификации и матрица кейсов — в закрытом Data Room по запросу.

Правило	Что значит
Единственный токен доступа	Подписанный JWT (EdDSA) со сроком 24 часа. Других способов войти нет. Адрес кошелька паролем не служит.
Кошелёк привязывается один раз и навсегда	Один кошелёк — один аккаунт, и наоборот. Привязку нельзя тихо заменить. Если кошелёк уже занят другим аккаунтом или у аккаунта уже другой кошелёк, сервер отвечает типизированной ошибкой 409 — это две разные ошибки, по одной на каждое направление конфликта.
Пригласивший определяется один раз	Окно для реферальной связи закрывается навсегда при первой успешной регистрации. Повторный запрос с тем же пригласившим — ответ 200, ничего не меняется; с другим пригласившим — ответ 409. Если ссылку не передали, ранее установленная связь сохраняется.
Домен приложения	Берётся из адреса манифеста мини-приложения (hostname) и сравнивается точным совпадением: foremetric.ai для основной сети, staging.foremetric.ai для тестовой, workchain 0. Адреса localhost в утверждённой матрице нет.
Время в доказательстве владения кошельком	Передаётся целым числом в JSON, а не строкой.
Реферальные коды	Коды, которые создаёт сервер, не длиннее 60 символов и безопасны для адресной строки.
Реферальный доход	Начинает работать только после подтверждения кошелька.

Полная техническая документация — evidence-реестр со статусами PR, открытые вопросы дизайна, детали спецификаций контрактов — предоставляется фондам и техническим партнёрам в закрытом Data Room по запросу.