

Механизмы обеспечения качества данных и справедливого взаимодействия при распределенном конфиденциальном инфообмене

Сергей Вельц svelts@technoscore.ru

ООО КБ ТехноСкор, МГТУ им. Н. Э. Баумана

5 июня 2025

Обмен историями рассрочек (BNPL) в реальном времени

Позволяет обмениваться данными по шифрованным номерам телефонов и по идентификаторам устройств в онлайн режиме.

Цель: защита от мошенников, вычисление признаков для скоринговых моделей, чтобы принимать решения по выдаче кредитов.

История: Изначально для BNPL. Ввод в эксплуатацию осень 2023. В реестре отечественного ПО Минцифры.

Гарантии:

- 1 Распределенное хранение данных.
- 2 Конфиденциальность: никто кроме запрашивающего не знает однозначно субъекта.
- 3 Балансировка запросов/ответов (механизм репутации)
- 4 Журналирование сделок.
- 5 (доп.) Защита от синтетических данных и функции контроля качества данных.

В основе - k-анонимность, криптопротоколы private membership test, oblivious transfer поверх ECC и написанные на Rust.

Доверие и немного теории игр.

Definition

Доверие - это вера в то, что другой участник не будет действовать против ваших интересов.

Возникает при **повторяющихся** играх с **смешанным** интересом ¹, т.е. должна быть взаимная ценность от взаимодействия в настоящем и будущем. ²

- 1 Угроза исключения из игры и упущенной выгоды.
- 2 Угроза штрафа за нарушение.
- 3 Угроза штрафа за выход из игры?

Советую книгу: *Томас Шеллинг, "Стратегия конфликта" (1960).*

Знаем ли мы функцию полезности другой стороны? см. bayesian games, inverse reinforcement learning.

¹Игры со смешанным интересом - это что-то среднее между антагонистическими играми и кооперативными играми. Пример: игры дилемма заключенного или битва полов.

²Есть еще институциональное доверие, которое обеспечивается правилами и законами, но это не наш случай.

- 1 **Honest** - честно и точно выполняет протокол.
- 2 **Honest but curious (semi-honest)** - честный, но любопытный. Выполняет протокол, но пытается узнать больше. Например, кеширует запросы. ← Координатор КРаб.
- 3 **Coward adversary** - "трусливый" противник. Выполняет протокол, только если нарушение будет обнаружено. ← Участники КРаб.
- 4 **Malicious** - злонамеренный. Не выполняет протокол, пытается обмануть других участников ⇒ токенизация.

Доп.: crash/fail-stop³. threshold adversary and Sybil attacks.

³Например, выкачал все данные других участников и отключился.

Модели доверия

- 1 Пропорция полученной и предоставленной полезности.
Например, торренты или КРАБ.

$$Reputation = \frac{Received\ nonempty}{Answer\ nonempty}$$

- 1 Затухание
 - 2 Качество данных
 - 3 Проведение ретро тестов и т.д.
- 2 Байесовское доверие.
 - 3 Децентрализованные механизмы: proof of work, proof of state, proof of authority, proof of space, proof of time, proof of burn и т.д.

Криптографические механизмы: commitment schemes, zero-knowledge proof (ZKP), ЭЦП, распределенные реестры.

Контрмеры: штрафы нарушителей(читеров).

Обеспечение качества данных

Чего мы хотим от данных? Полнота, точность, актуальность, достоверность. darkgreen **Причины проблем:** ошибки человеческие, технические ошибки, злой умысел.

Данные вне системы vs. данные внутри системы

Механизмы контроля:

- 1 **Контрольные суммы и временные метки на Координаторе**
- 2 **Валидация данных на входе**
- 3 **Отчет риск-офицера** - анализ рисков и аномалий в данных.
- 4 **Отчет о качестве данных в базе** - регулярные проверки и отчеты о состоянии данных.
- 5 **Механизм диспутов между участниками**
- 6 **Зависимость от качества своих данных**
- 7 **Тестовые закупки после интеграции**

- 1 Обеспечение качества данных в условиях, когда их не видишь - сложная задача. Важно дать нужные инструменты и тщательно тестировать!
- 2 Необходимо использовать распределенные механизмы доверия и репутации, иначе участники друг друга обманывают.
- 3 Более слабая модель безопасности компенсируется техническими и организационными мерами.

На рынке есть спрос на новые решения. С банками напрямую тяжело, с их дочерними финтехами проще.