



В L ∞ M T E C H

конфиденциальные вычисления

О КОМПАНИИ

 bloomtech.ru

МЫ — РОССИЙСКАЯ КОМПАНИЯ, ОСНОВАННАЯ В МОСКВЕ В 2021

Разрабатываем решения для банковской сферы, изучаем и развиваем технологии совместных конфиденциальных вычислений и их практические приложения в Fintech.

Капитализируем hands-on опыт в искусственном интеллекте, больших данных и криптографии, умеем внедрять сложные продукты в крупнейшие компании и государственные структуры Российской Федерации.

Bloomtech — независимая коммерческая компания, не аффилированная ни с одной кредитной организацией

Наша цель — честное, взаимовыгодное сотрудничество участников между собой и нами



МЕЖБАНКОВСКИЙ СКОРИНГ

Скоринговая инфраструктура позволяет банкам вычислять агрегированные метрики по клиентам, например, доход или среднемесячный остаток по счетам, не обмениваясь данными друг с другом и не консолидируя их у третьих сторон.

АГРЕГИРОВАНИЕ ФИНАНСОВЫХ ДАННЫХ

Слагаемые x_i, y_i, z_i сохраняются в секрете

ПРИМЕНЕНИЯ:

- 1 Кредитный скоринг, BNPL, POS
- 2 Доход для ПДН/РТИ
- 3 AML/КУС

ПРЕИМУЩЕСТВА:

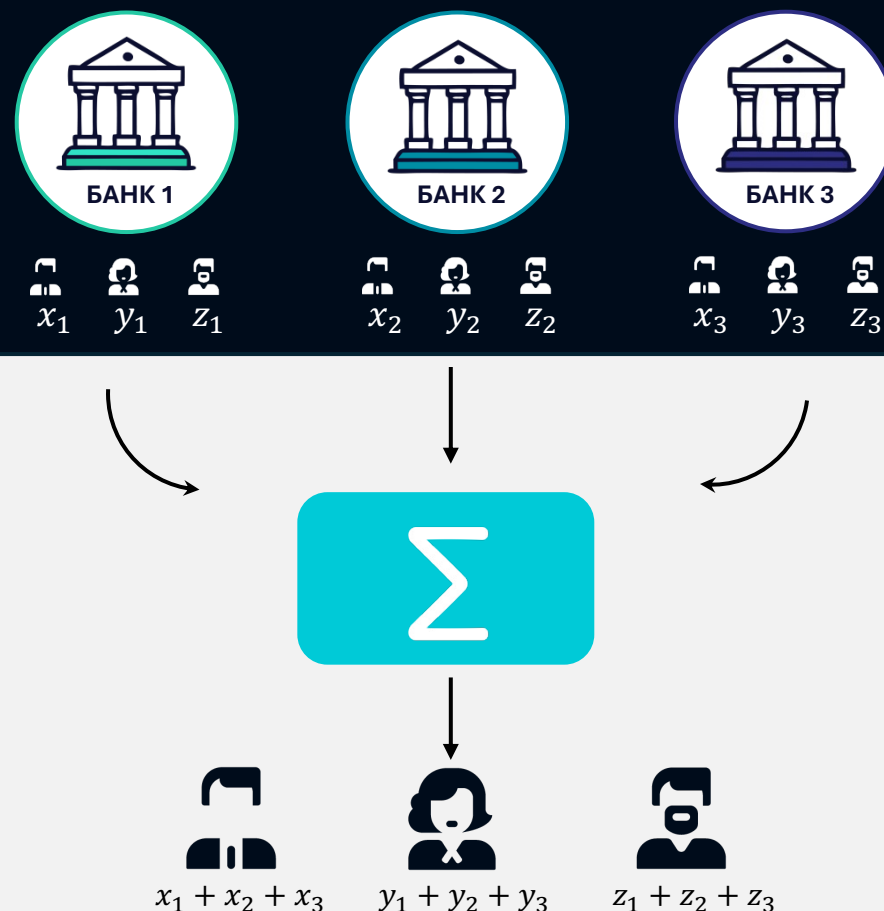
- Банки не обмениваются собственными данными
- Банки не передают данные третьей стороне
- Высокий хит-рейт (более 50%)

9 банков

подключены к системе

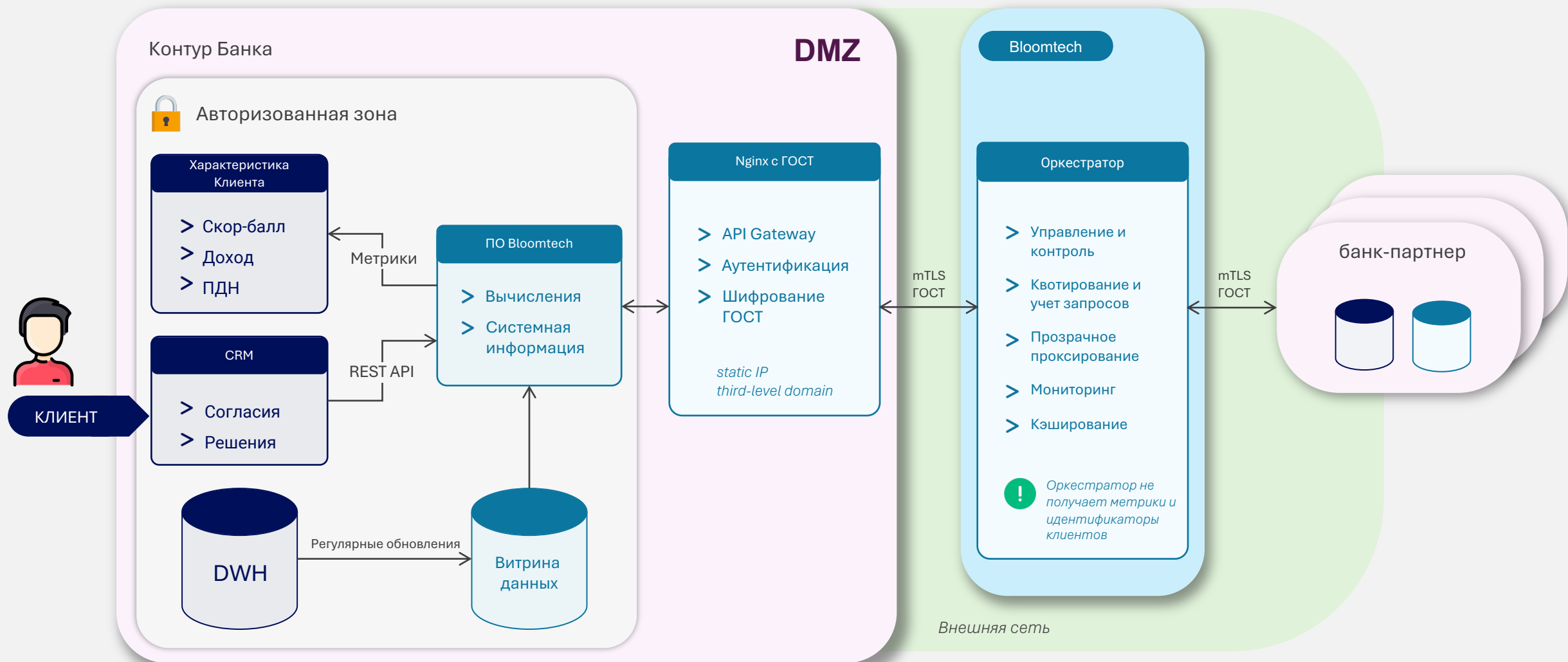
> 10 банков

сейчас в работе
(из топ-30 розничных)



АРХИТЕКТУРА ПЛАТФОРМЫ

Децентрализация



ИНЖЕНЕРНЫЕ ОГРАНИЧЕНИЯ

Полностью децентрализованные MPC-системы сложно внедрять и поддерживать. Если участников сравнительно много (больше трех), такая архитектура подходит только для простых операций (сложение, агрегация, простые статистики). Более сложные вычисления требуют других архитектур (федерализация).

1 Внедрение – долго и дорого (часто очень дорого) для участника системы;

2 Эксплуатация – не все участники готовы предоставить ресурсы и экспертизу;

3 Сложность – даже простая операция требует множество взаимодействий;

масштабируемость



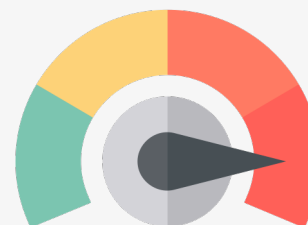
участников много
(банков в РФ > 300)

SLA



~ 1 секунда на ответ

эффективность



сложение ~7 операций
умножение ~15 операций

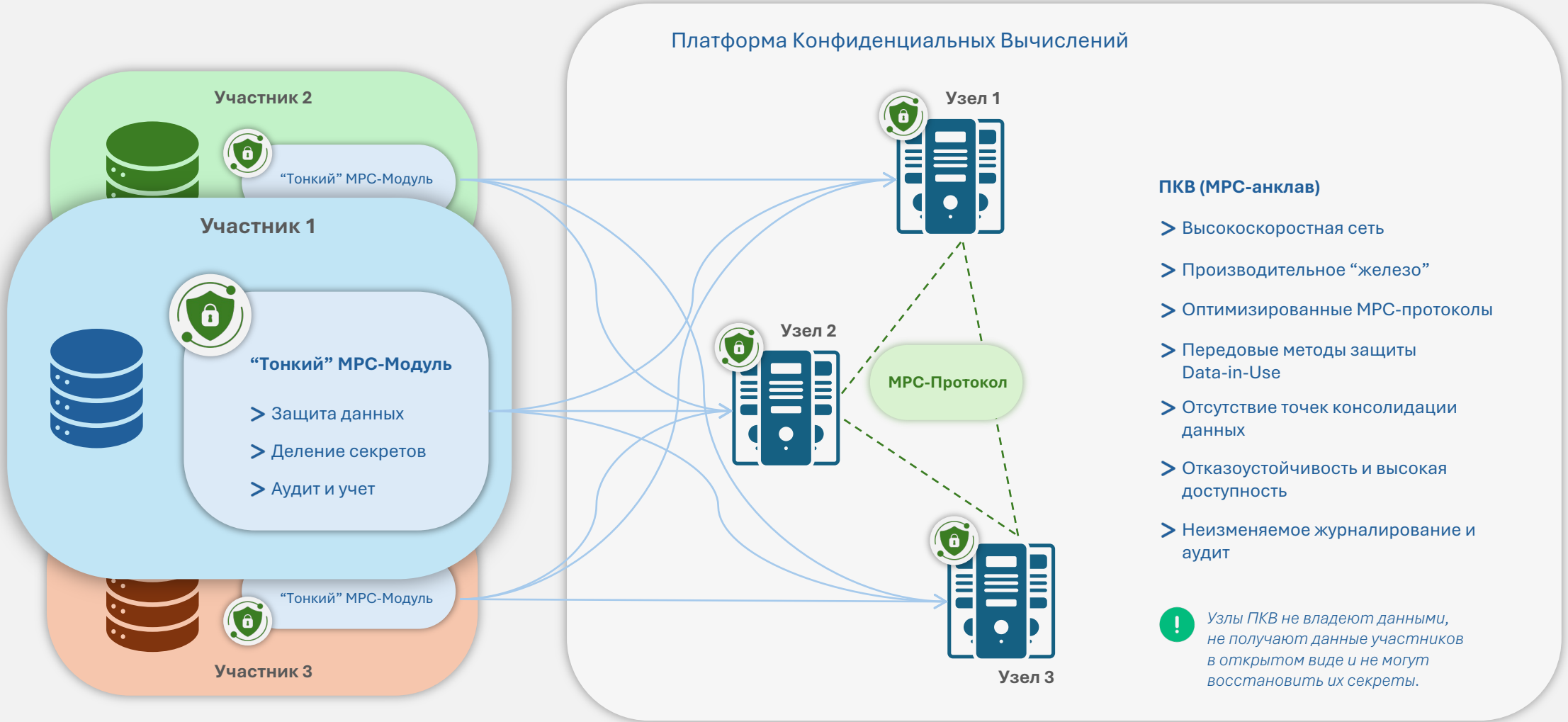
сеть



в худшем случае
связь всех со всеми

РАСПРЕДЕЛЕННЫЙ АНКЛАВ

Делегирование вычислений



В ЧЕМ РАЗНИЦА



децентрализация



абсолютный контроль

вычисления проводятся со всеми участниками сразу или не проводятся вообще



исключительная модель угроз

нарушение конфиденциальности возможно только при сговоре всех участников одновременно



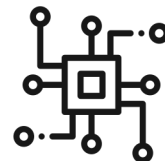
сложность внедрения

каждый участник выделяет оборудование, устанавливает и настраивает полный пакет программного обеспечения



сложность эксплуатации

процесс останавливается при сбое любого участника, производительность системы определяется по "самому медленному" участнику



распределенный анклава



надежность и производительность

работоспособность и производительность системы зависит от самых надежных и мощных узлов анклава



внедрение и эксплуатация

сложное и требовательное к ресурсам программное обеспечение устанавливается только на узлы анклава



распространение ПАК

узел анклава – программно-аппаратный комплекс с предустановленным ПО



гибкая модель угроз

узлы анклава – распределенная сеть доверия, сговор узлов запрещен (вероятность сговора тем ниже, чем больше узлов в системе)



СПАСИБО!
