

A decorative graphic in the top right corner of the slide, consisting of a grid of blue squares of varying shades, arranged in a pattern that tapers off towards the right edge.

Hyperledger

Блокчейн-фреймворк для бизнеса

Александр Земцов, Научно-технический центр IBM
28 февраля 2017

Блокчейн сегодня

Блокчейн сегодня

- ✓ Блокчейн – молодая технология, интерес к которой постоянно растет
- ✓ Согласно исследованиям основная часть интересующихся технологией компаний готова внедрить ее после 2018 года
- ✓ Для внедрения блокчейн недостаточно одной организации: требуется экосистема
- ✓ Кроме финансовых учреждений технологией интересуются и государственные организации
- ✓ Блокчейн принесет на рынок новые модели взаимодействия между компаниями без участия регуляторов

Реализации технологии блокчейн сегодня

Bitcoin

- ✓ Старейшая реализация технологии блокчейн
- ✓ Крупнейшая блокчейн-сеть
- ✓ Bitcoin принимается более, чем в 100.000 магазинов



Ethereum

- ✓ Имеет свою криптовалюту Ether
- ✓ Поддерживает смарт-контракты



Ripple

- ✓ Ориентирована на обмен денежными средствами
- ✓ Имеет свою криптовалюту XRP



Hyperledger

- ✓ Поддерживается крупными технологическими и финансовыми компаниями
- ✓ Не поддерживает криптовалюту
- ✓ Ориентирована на бизнес-задачи



Как блокчейн может помочь бизнесу

Увеличение скорости

Блокчейн сильно сокращает время выполнения транзакций, а также урегулирования споров

1

2

3

Уменьшение стоимости

Сокращаются расходы на поддержку инфраструктуры за счет автоматизации процессов

Сокращение рисков

Уменьшаются риски сговора, фальсификации данных, а также случайного удаления информации

Проект Hyperledger

Проект Hyperledger

- ✓ Основан в декабре 2015 года
- ✓ Самый быстрорастущий проект Linux Foundation
- ✓ Цель проекта – создание транзакционных систем нового поколения
- ✓ Развивает проекты с открытым исходным кодом
- ✓ Поддерживается технологическими компаниями, финансовыми учреждениями, банками (в том числе, российскими участниками)



Premier members of Hyperledger



General members of Hyperledger



Проекты в рамках Hyperledger

Fabric



Iroha

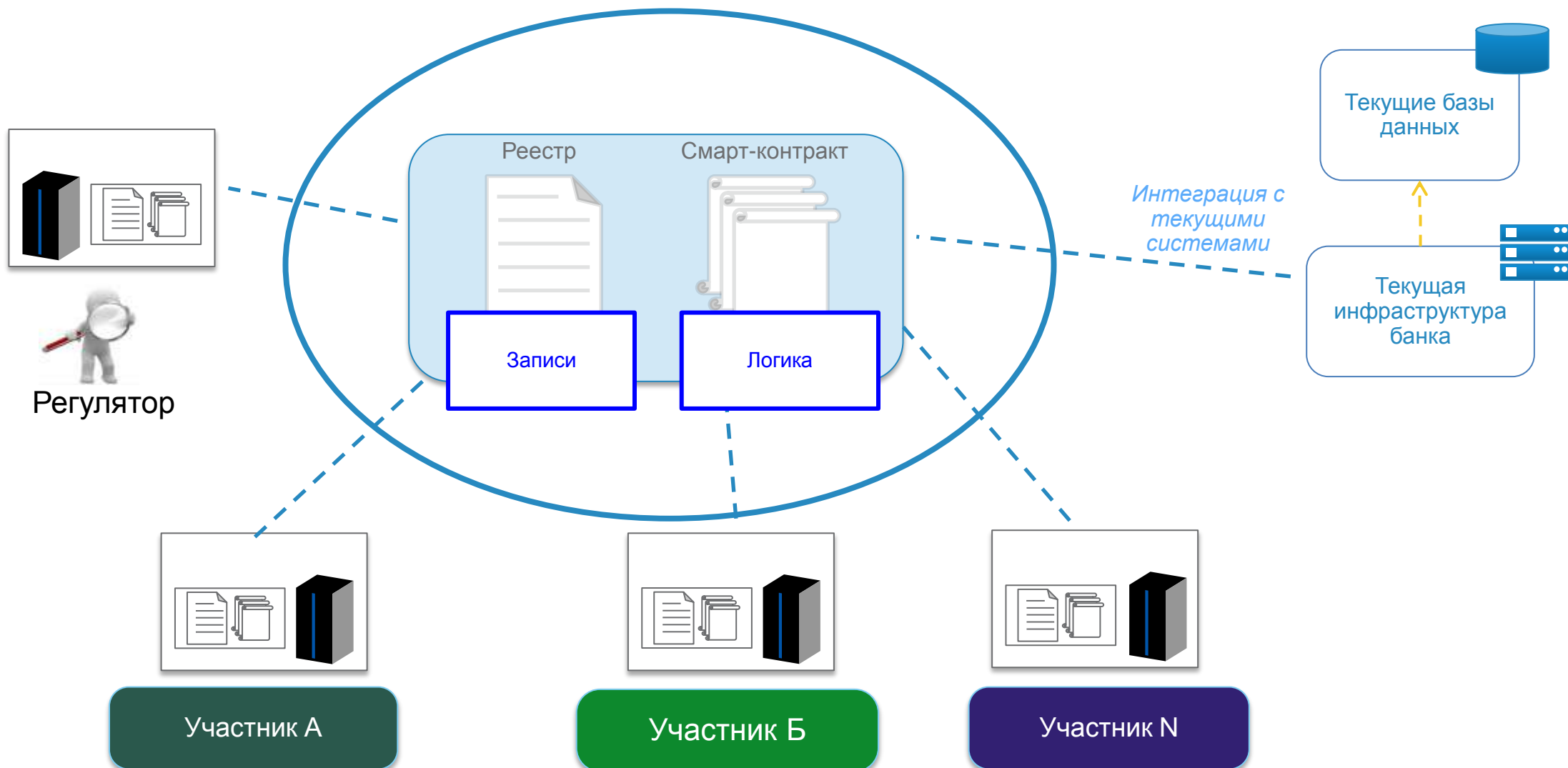


Sawtooth Lake

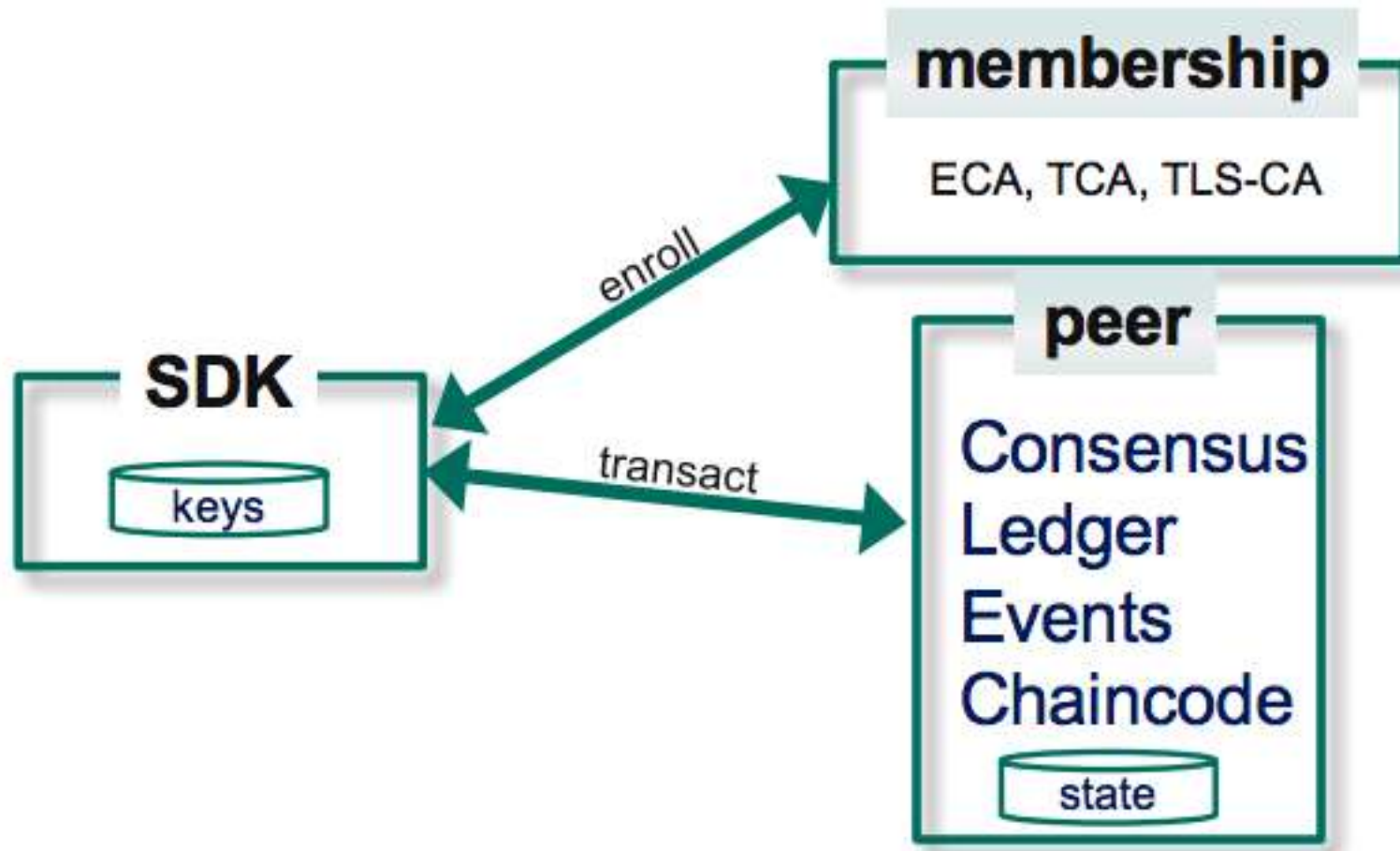


Fabric

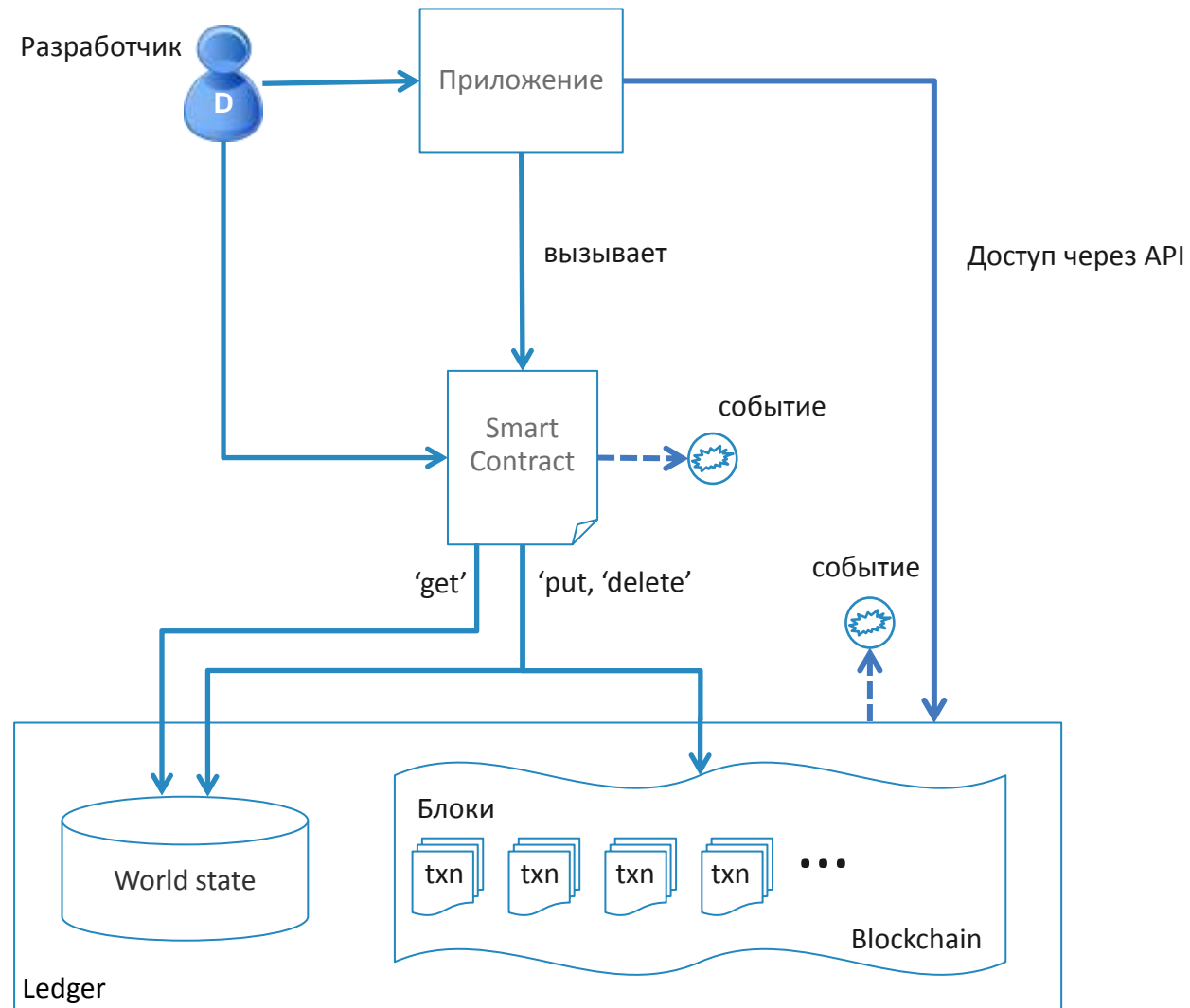
Взаимодействие участников сети



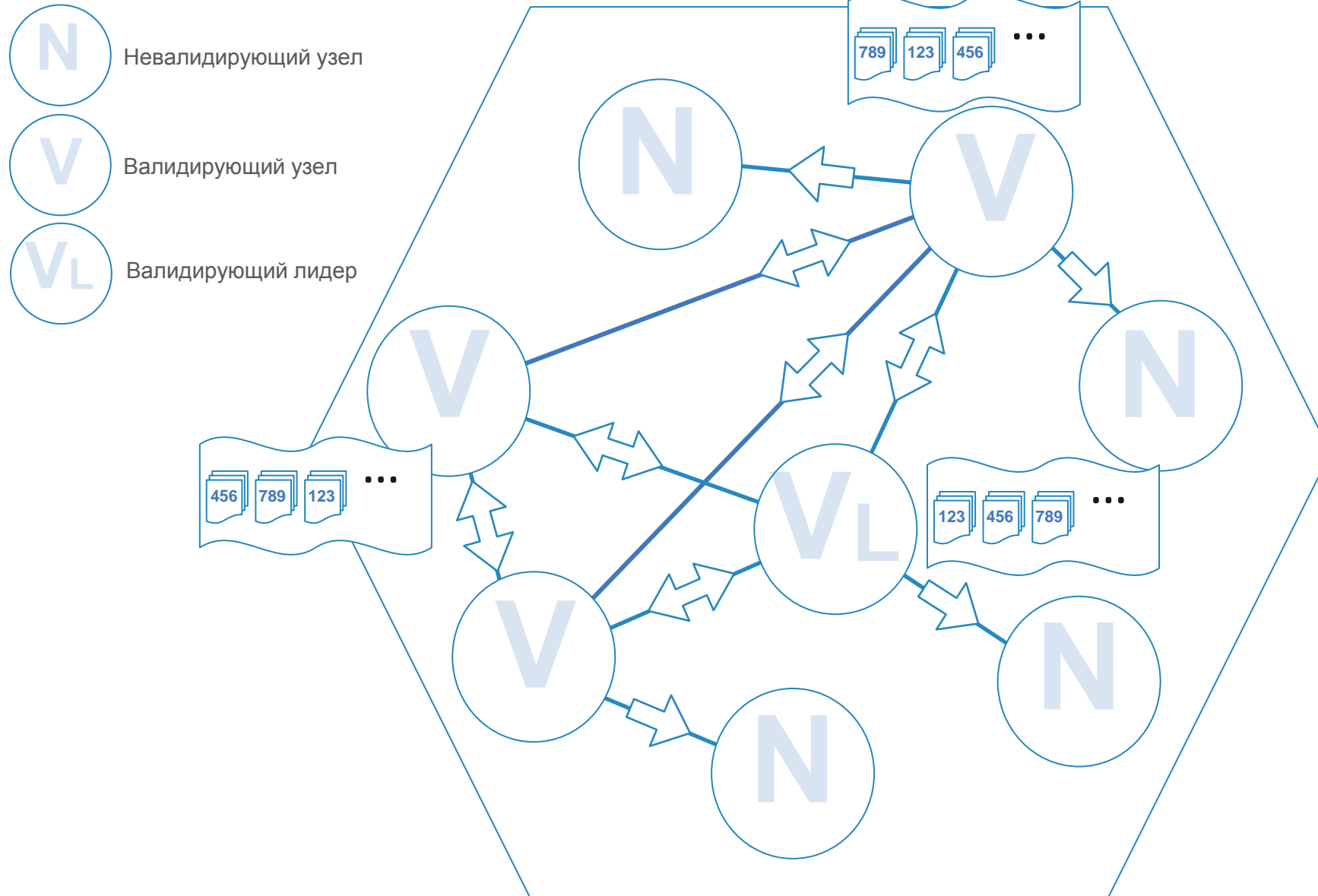
Архитектура Fabric v.0.6



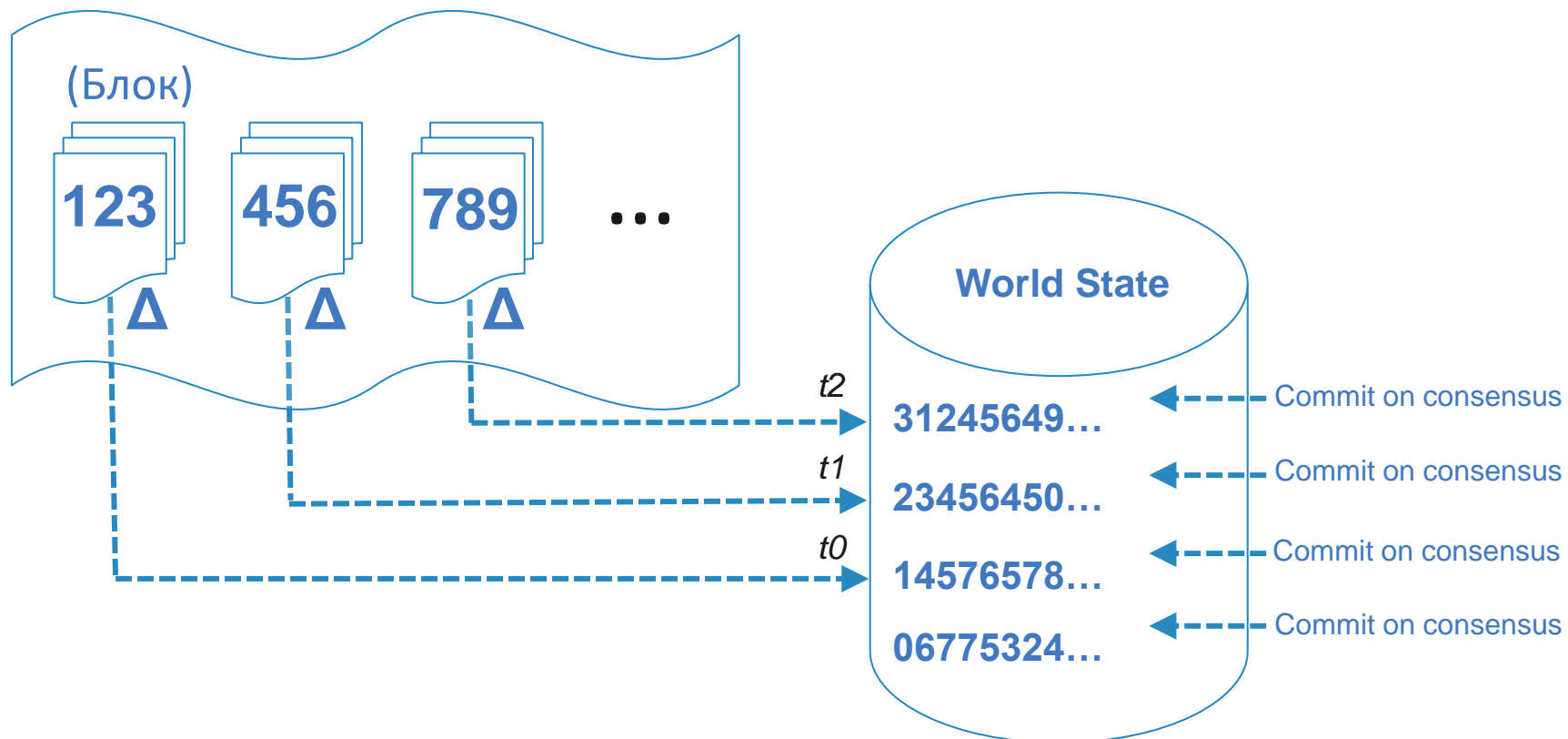
Работа приложений с блокчейн-сетью



PBFT-консенсус



Запись результата



Δ = Хэш изменений

Fabric v.1.0

Что изменится в версии 1.0

✓ Fabric 0.6

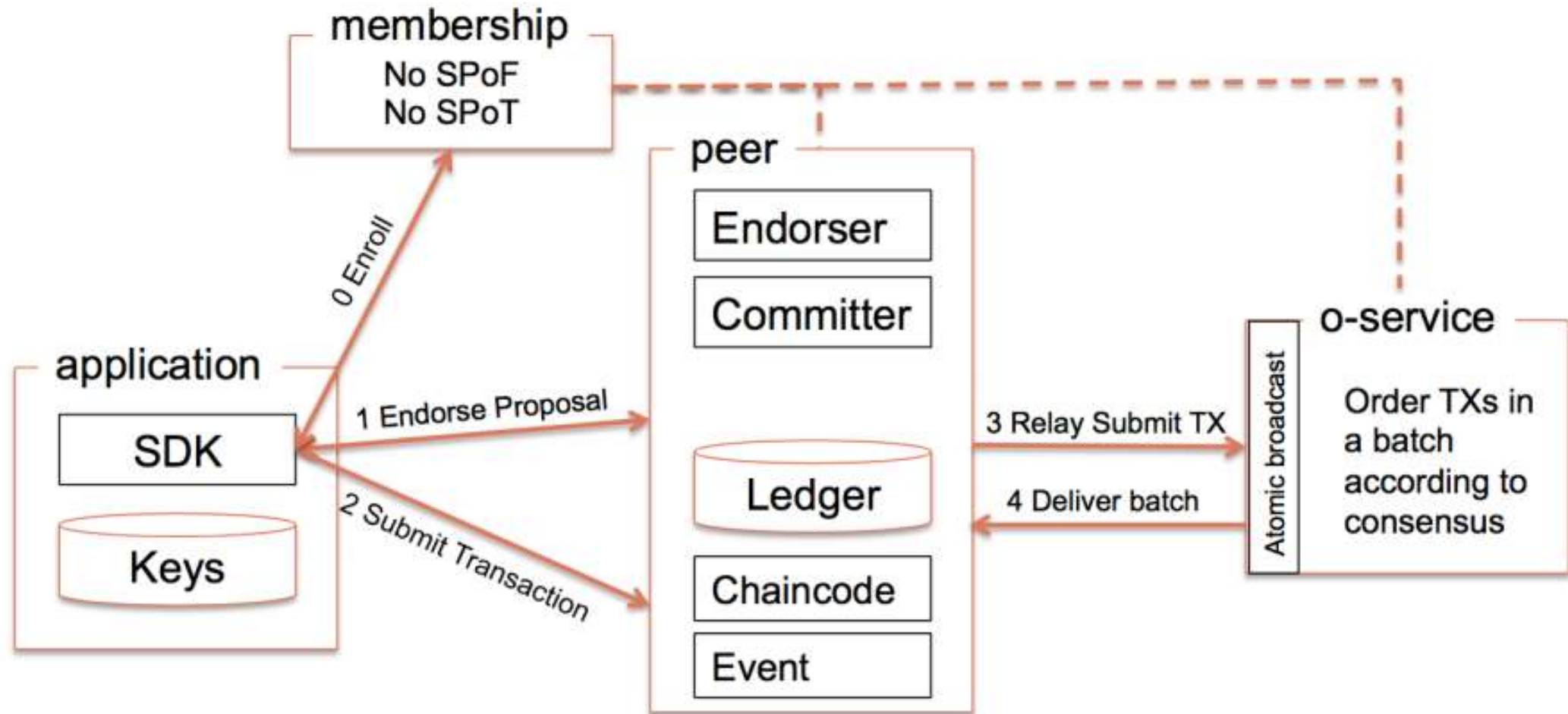
- Выполнение смарт-контрактов и подтверждение транзакций происходит на всех узлах сети
- Затруднено разделение прав доступа к информации
- Хранение полной копии реестра на всех узлах затрудняет масштабируемость сети

✓ Fabric 1.0

- Выполнение смарт-контрактов и подтверждение транзакций разделено между разными узлами сети
- Локальное состояние данных хранится только на тех узлах, к которым эти данные относятся
- Разделение ролей узлов в сети улучшает масштабируемость и безопасность



Архитектура Fabric v.1.0



Роли в Fabric 1.0

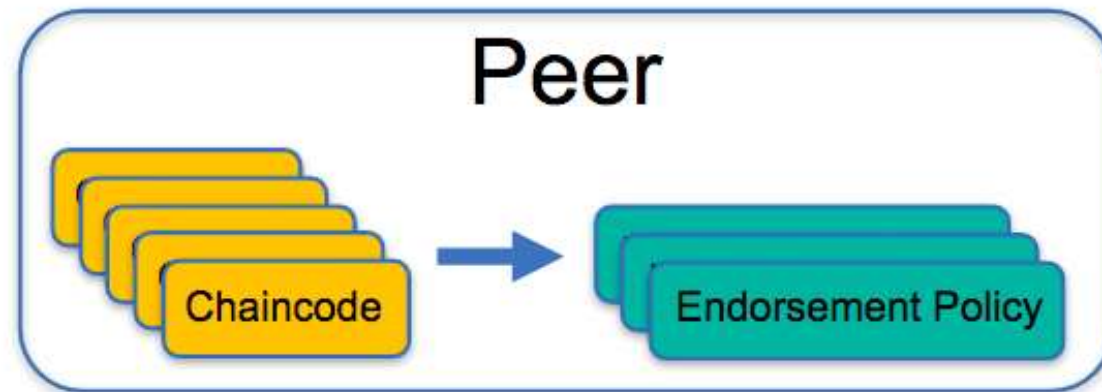
- ✓ **Peer.** Отправляет запросы на выполнение транзакций, поддерживает цепочку транзакций и версию локальных данных.
- ✓ **Endorsing peer.** Получает транзакцию для одобрения. Отвечает одобрением или запретом транзакции.
- ✓ **Ordering peer.** Подтверждает включение транзакции (или пакета транзакций) в реестр, сообщает результат всем остальным узлам в сети



Политика смарт-контрактов

Политика одобрения описывает, кем именно должен быть одобрен смарт-контракт. Транзакция считается одобренной только в том случае, если она была одобрена согласно политики смарт-контракта.

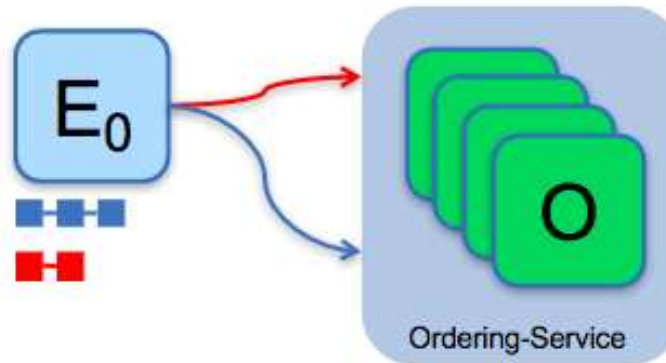
- ✓ Узлы могут быть частью нескольких политик
- ✓ Политика смарт-контракта (чейнкода) определяется при его размещении в блокчейне



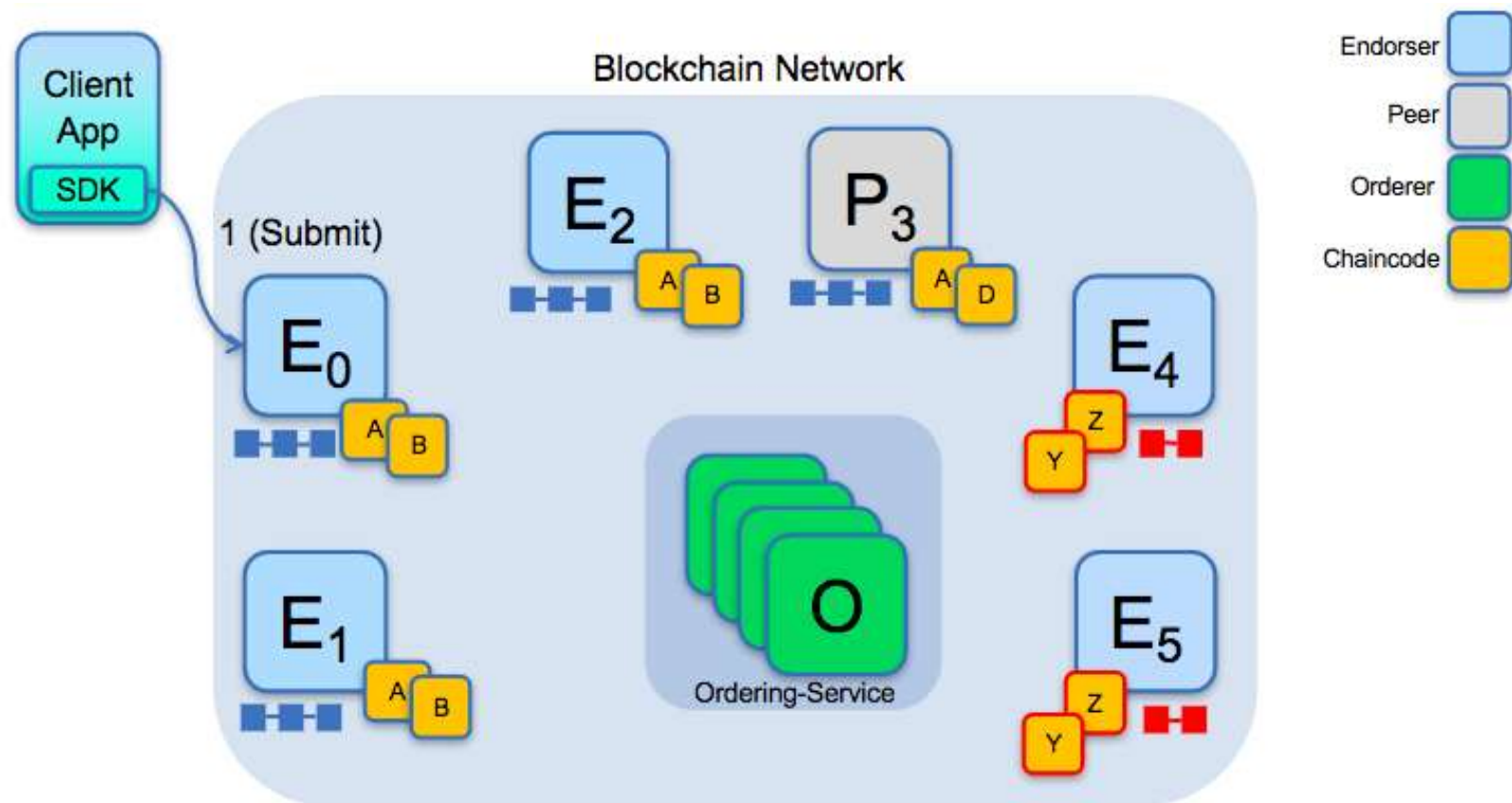
Каналы

Все узлы общаются с ordering service через каналы.

- ✓ **Повышается безопасность**
 - Смарт-контракты размещаются на определенные узлы
- ✓ **Сообщения опраляются в отдельные каналы**
 - Хранение реестра зависит от канала и узла
- ✓ **Узлы могут быть соединены с несколькими каналами**



Новая версия консенсуса



Приложение отправляет запрос на выполнение транзакции для смарт-контракта A на узел E0.
Политика одобрения: E0, E1 и E2 должны подписать транзакцию. Остальные узлы не являются частью политики.

База данных в Fabric

- ✓ В базах данных, хранящих пары ключ-значение, таких как RocksDB или LevelDB, содержимое может быть запрошено только по ключу.
 - Не отвечают требованиям написания смарт-контрактов, аудита, отчетности.
- ✓ В документо-ориентированных базах данных, таких как CouchDB, содержимое представлено в формате JSON, они полностью запрашиваемы.
 - Отвечает большей части требований написания смарт-контрактов, аудита и простых отчетов
 - Для более глубокой отчетности и аналитики, реплицируются в платформы анализа данных, такие как Spark
 - Модель данных «ID/документ» совместима со смарт-контрактами, использующими модель «ключ/значение». Поэтому при хранении данных в формате JSON переписывания кода не требуется
- ✓ Базы данных SQL также возможны, но требуют более сложного уровня реляционных преобразований, таких как управление схемами



Спасибо

Q&A