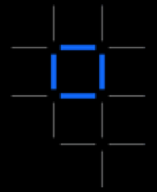


Технологии блокчейн: от науки до бизнеса

Григорий Мальцев, IBM

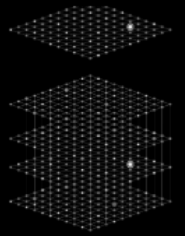
5 in 5

Five innovations that will help change our lives within five years

Watch the replay presentation of the 5 in 5 from the IBM Think conference

Crypto-anchors and blockchain

1



Hackers gonna hack. Until they encounter lattice cryptography.

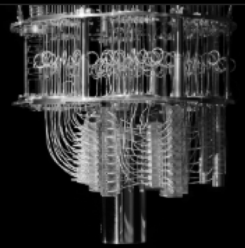
2

Our oceans are dirty. AI-powered robot microscopes may save them.

3

AI bias will explode.
But only the unbiased AI will survive.

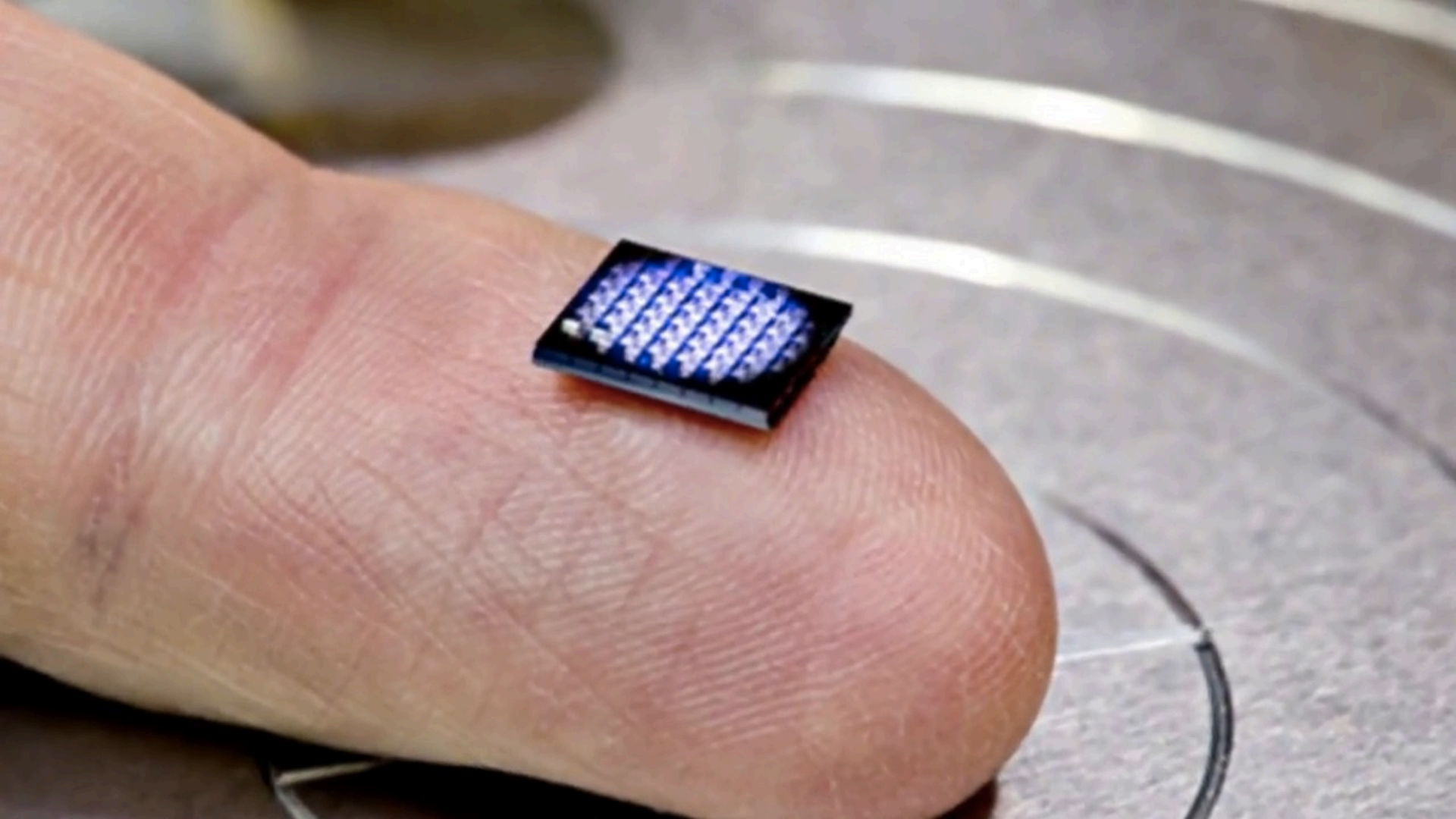
4



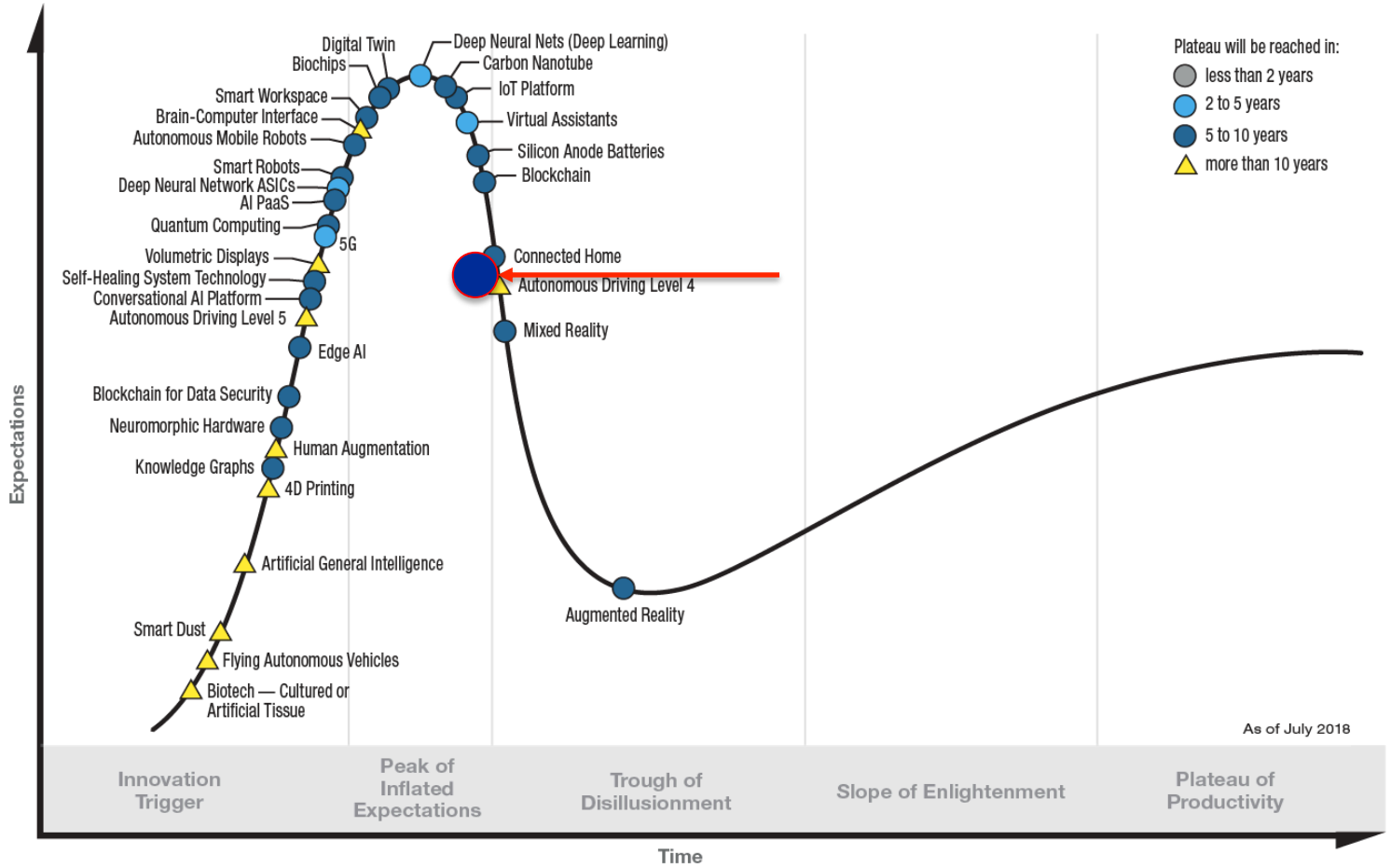
Today, quantum computing is a researcher's playground. In five years, it will be mainstream.

5

http://www.research.ibm.com/5-in-5

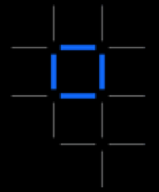


Цикл зрелости технологий



Содержание

- ✓ Что такое блокчейн?
- ✓ Hyperledger Fabric – реализация технологии для бизнеса
- ✓ Сценарии использования
- ✓ Блокчейн в IBM
- ✓ Платформа для блокчейн



Что такое блокчейн?

Открытые и закрытые блокчейны

Открытые блокчейны

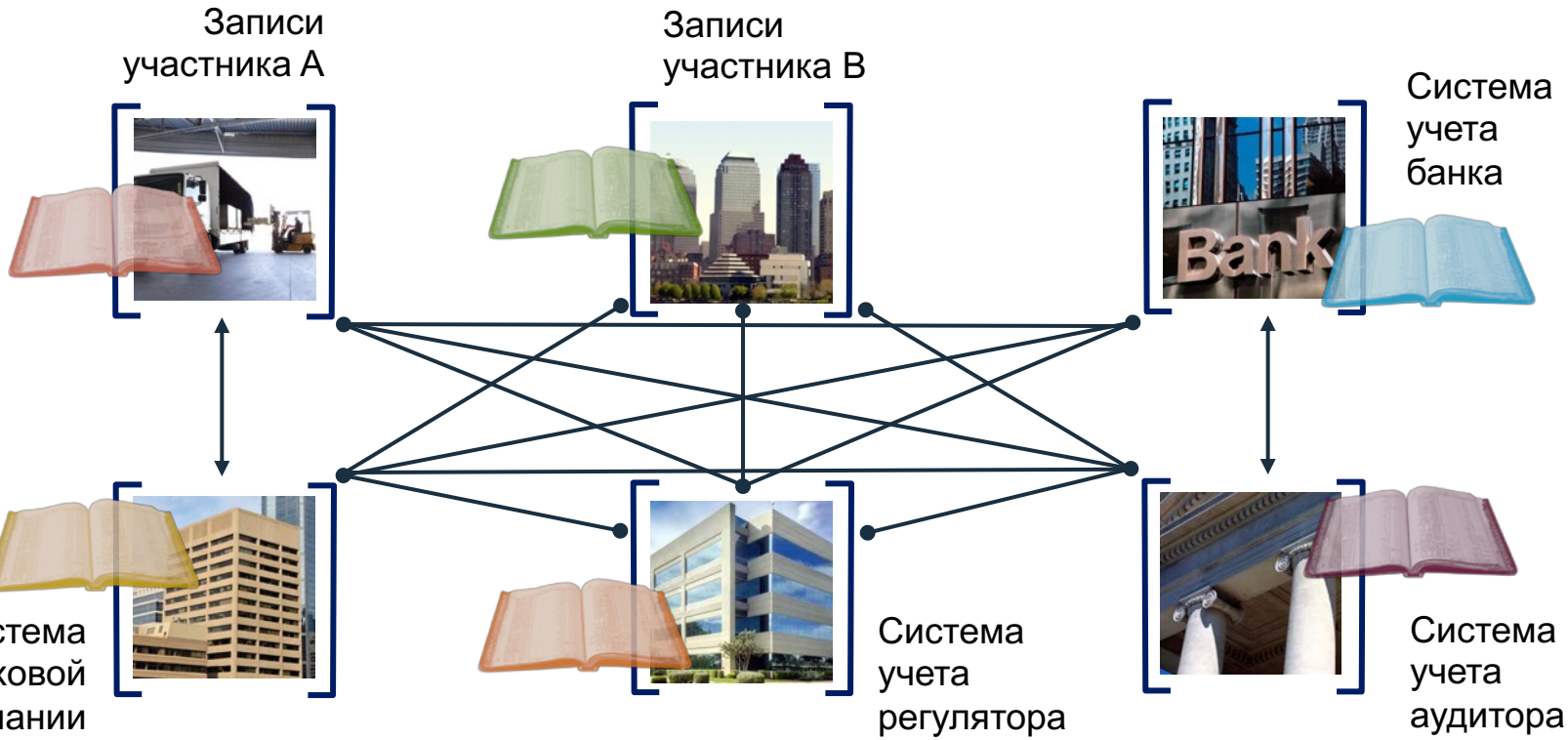
- Например, Bitcoin
- Транзакции видны всем участникам
- Сложно идентифицировать участников

Закрытые блокчейны

- Например, Hyperledger Fabric
- Участники известны, но транзакции засекречены

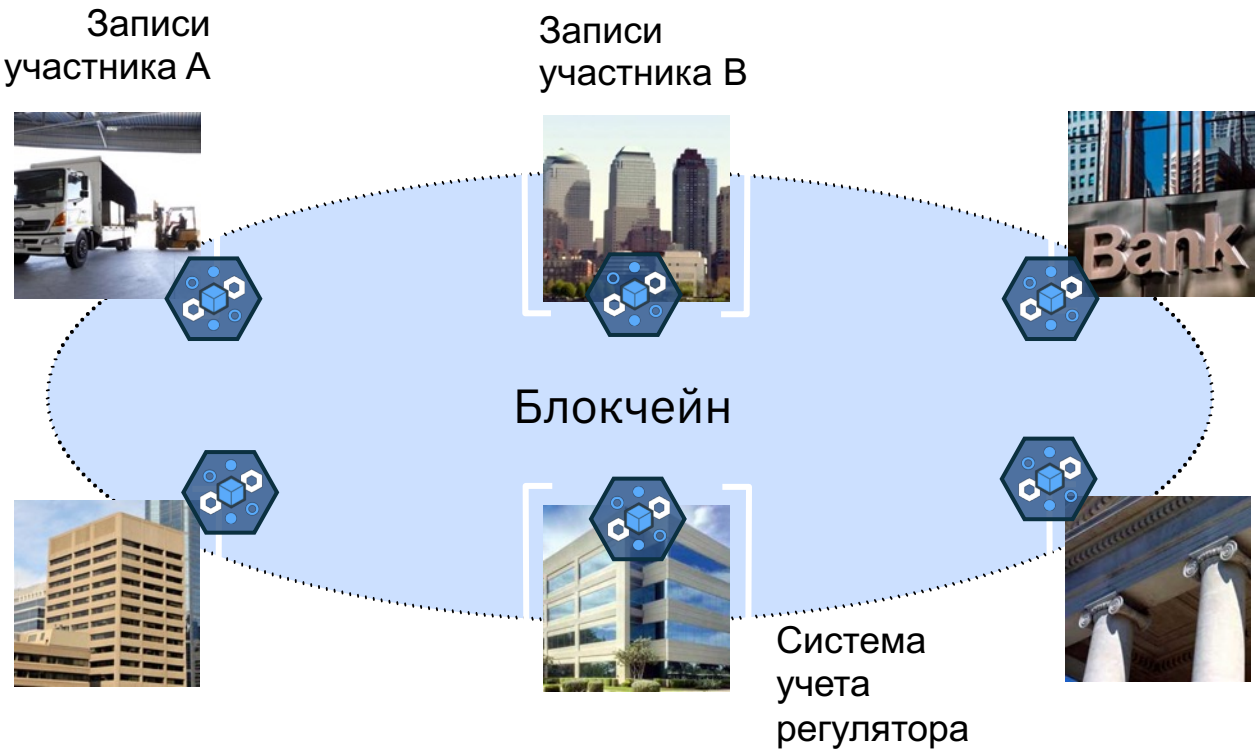
- ✓ Некоторые сценарии требуют анонимность, другие – закрытость.
  - Некоторые могут совмещать в себе эти требования в зависимости от участников
- ✓ К большинству бизнес-сценариев больше походит использование закрытого блокчейна.
  - Участники знают, с кем они проводят транзакции
  - Как правило, транзакции конфиденциальны между вовлеченными участниками
  - Участие в системе контролируется

Проблема бизнес-сетей…



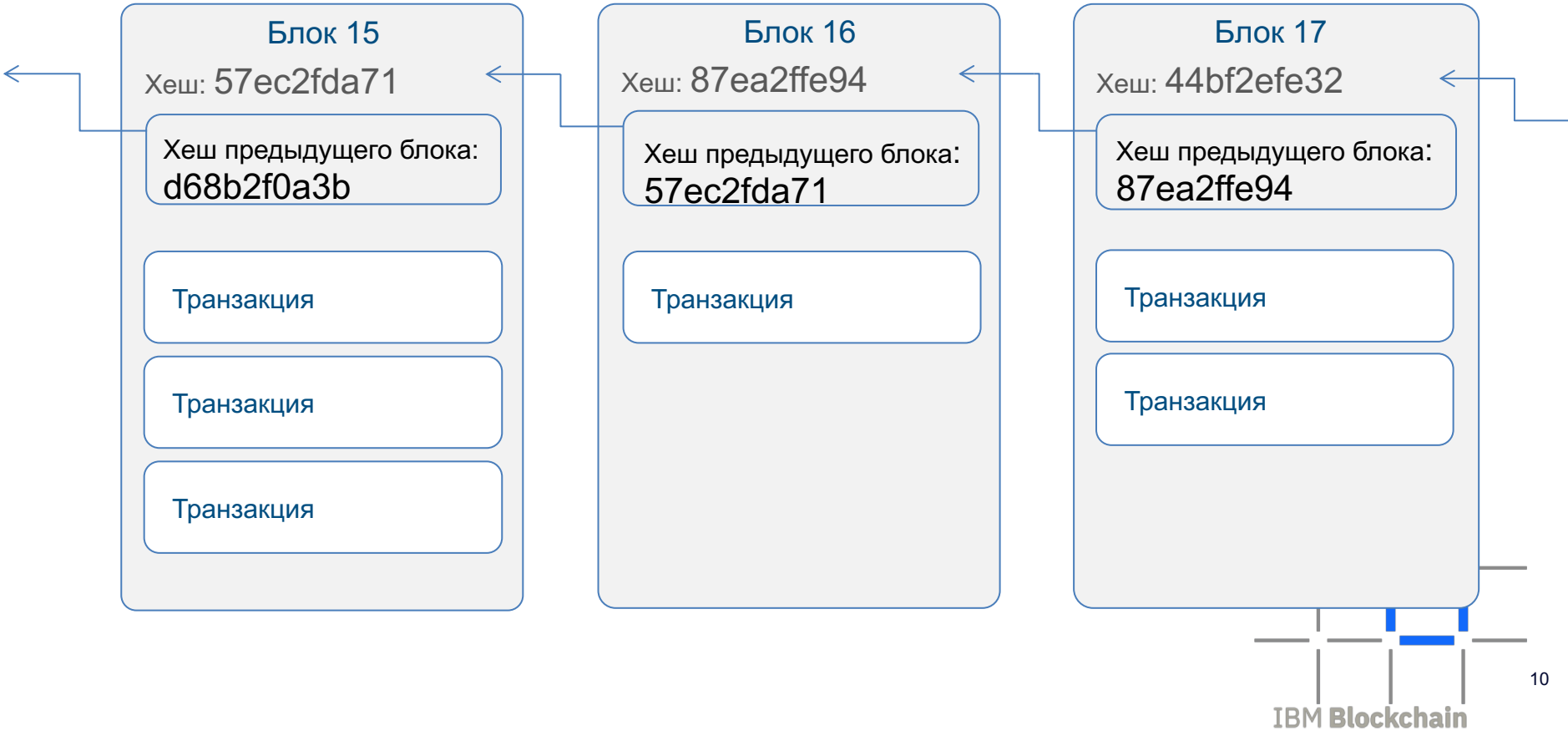
… неэффективно, дорого, уязвимо

Общий распределенный реестр с управлением доступом

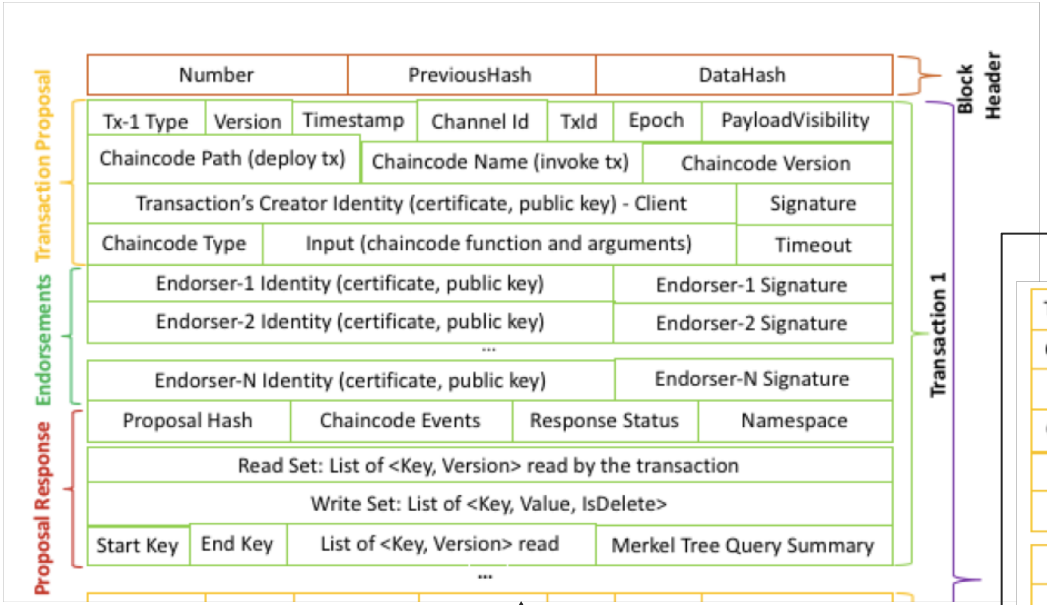


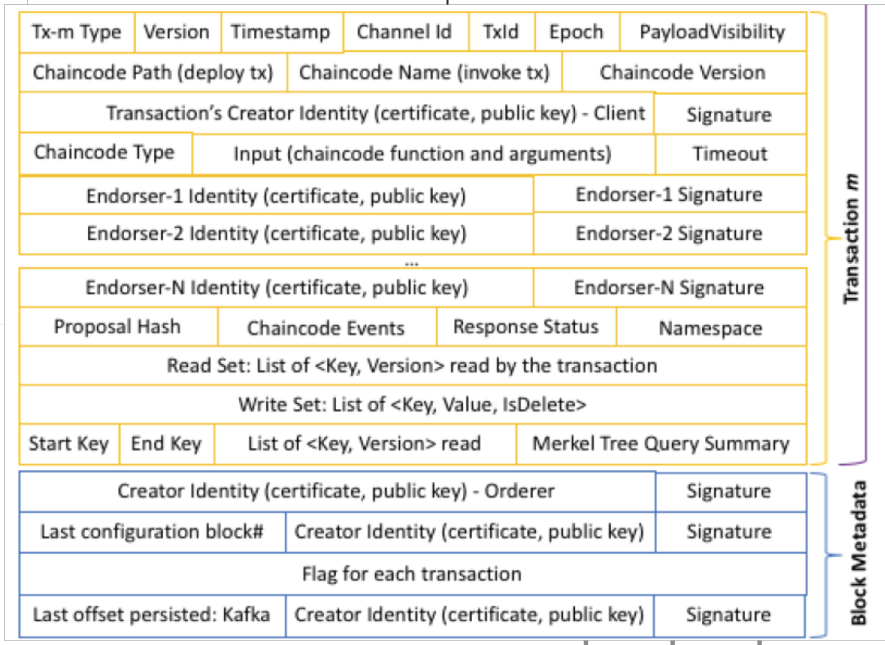
… с консенсусом, достоверностью происхождения, неизменностью, окончательностью

Основа технологии – цепочка блоков



Структура блока на примере HL Fabric v1



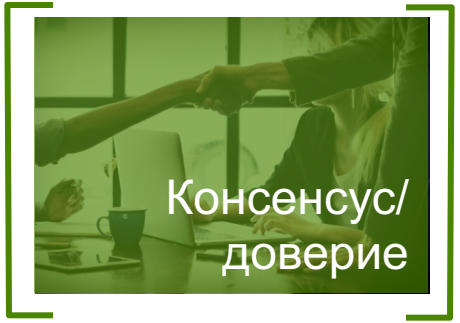


Основные составляющие технологии

Добавление записи в распределенную бизнес-сеть

Коммерческие условия включены в транзакции и выполняются с операциями

Обеспечение надлежащей видимости; Безопасные, аутентифицированные и проверяемые



Стороны сети подтвержают подлинность транзакции

Консенсус – алгоритм одобрения блока транзакций, примеры

Proof of Work

Требует от узлов, формирующих блоки, решения сложных криптографических задач

+ Хорошо работает в открытых сетях.

– Высокое потребление энергии, низкая скорость выполнения транзакций.

Примеры использования: Bitcoin, Ethereum.

Proof of Stake

Требует от узлов, формирующих блоки, наличие внутренней валюты сети.

+ Хорошо работает в открытых сетях.

– Привязка к внутренней валюте сети.

Примеры использования: Nxt, в будущем Ethereum.

Proof of Elapsed Time

Формирование блоков в защищенной программной среде процессора.

+ Высокая эффективность.

– Требует наличие специального расширения в процессоре.

Примеры использования: Hyperledger Sawtooth Lake.

Консенсус – алгоритм одобрения блока транзакций, примеры

Solo / No-ops

Транзакции исполняются без достижения консенсуса.

+ Высокая скорость исполнения транзакций. Подходит для разработки.

– Отсутствие консенсуса может привести к расходящимся цепочкам блоков.

Примеры использования: Hyperledger Fabric.

PBFT-based

Решение задачи о византийских генералах.

+ Высокая эффективность, устойчивость к появлению вредоносных узлов.

– Плохая масштабируемость сети.

Примеры использования: Hyperledger Fabric 0.6.

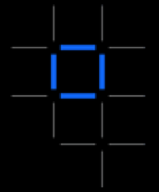
Kafka / Zookeeper

Формирование новых блоков производится в специальном сервисе сети.

+ Высокая эффективность и отказоустойчивость.

– Нет устойчивости к появлению вредоносных узлов.

Примеры использования: Hyperledger Fabric.



Hyperledger Fabric

Hyperledger – это блокчейн-консорциум в Linux Foundation

HYPERLEDGER

THE LINUX FOUNDATION

open source

Hyperledger – сообщество открытой разработки **(Open source)** отраслевых проектов на основе технологии блокчейн.

Потенциал блокчейна *"строительство нового поколения транзакционных приложений, которые устанавливают отношения* ***доверия, подотчетности и прозрачности*** *в их ядро при оптимизации бизнес-процессов и правовых ограничений."*

Hyperledger – это блокчейн-консорциум в Linux Foundation

Проекты Hyperledger

Infrastructure

Technical, Legal, Marketing, Organizational

Ecosystems that accelerate open development and commercial adoption

THE LINUX FOUNDATION

Cloud Foundry | Node.js | **Hyperledger** | Open Container Initiative

Frameworks

Meaningfully differentiated approaches to business blockchain frameworks developed by a growing community of communities

Hyperledger Fabric | Hyperledger Sawtooth | Hyperledger Iroha | Hyperledger Indy | Hyperledger Burrow

Tools

Typically built for one framework, and through common license and community of communities approach, ported to other frameworks

Hyperledger Composer | Hyperledger Cello | Hyperledger Explorer | Hyperledger Quilt

Развитие Hyperlager Fabric

v1.1

- Network administration:
  - Node.js connection profile
- Smart contract:
  - Node.js smart contracts
  - Encryption library
  - Attribute Based Access Control
- Performance & scale:
  - More orderers at scale
  - Parallel txn validation
  - CouchDB indexes
- Events:
  - Per channel vs global
  - Block info minimal events
- Membership services:
  - CSR for secure certificates
- Serviceability:
  - Upgrade from 1.0

v1.2

- Network administration:
  - ACL mechanism per channel
  - Service discovery
- Consensus:
  - Pluggable endorsement and validation
- Smart Contract:
  - Private Data Collections (SideDB)
- Documentation:
  - Improved documentation and tutorials
- Serviceability:
  - Improvements and bug fixes

v1.3

- Network administration:
  - SDK improvements
  - Service Discovery remaining items
- Consensus:
  - State based endorsement
- Smart Contract:
  - Java chaincode
  - Burrow EVM support
  - Private Data remaining items
  - Chaincode query result pagination
- Membership services:
  - Identity Mixer
- Serviceability:
  - Improvements and bug fixes

v1.4

- Network administration:
  - CLI redesign
- Consensus:
  - RAFT Consensus
- Smart Contract:
  - Higher level programing model
- Membership services:
  - Identity Mixer Node.js SDK + revocation
- Serviceability:
  - Operational Metrics for Fabric runtime components
  - Monitor health for Fabric runtime components
  - Improve troubleshooting for Fabric components

** To be 1st LTS!! **

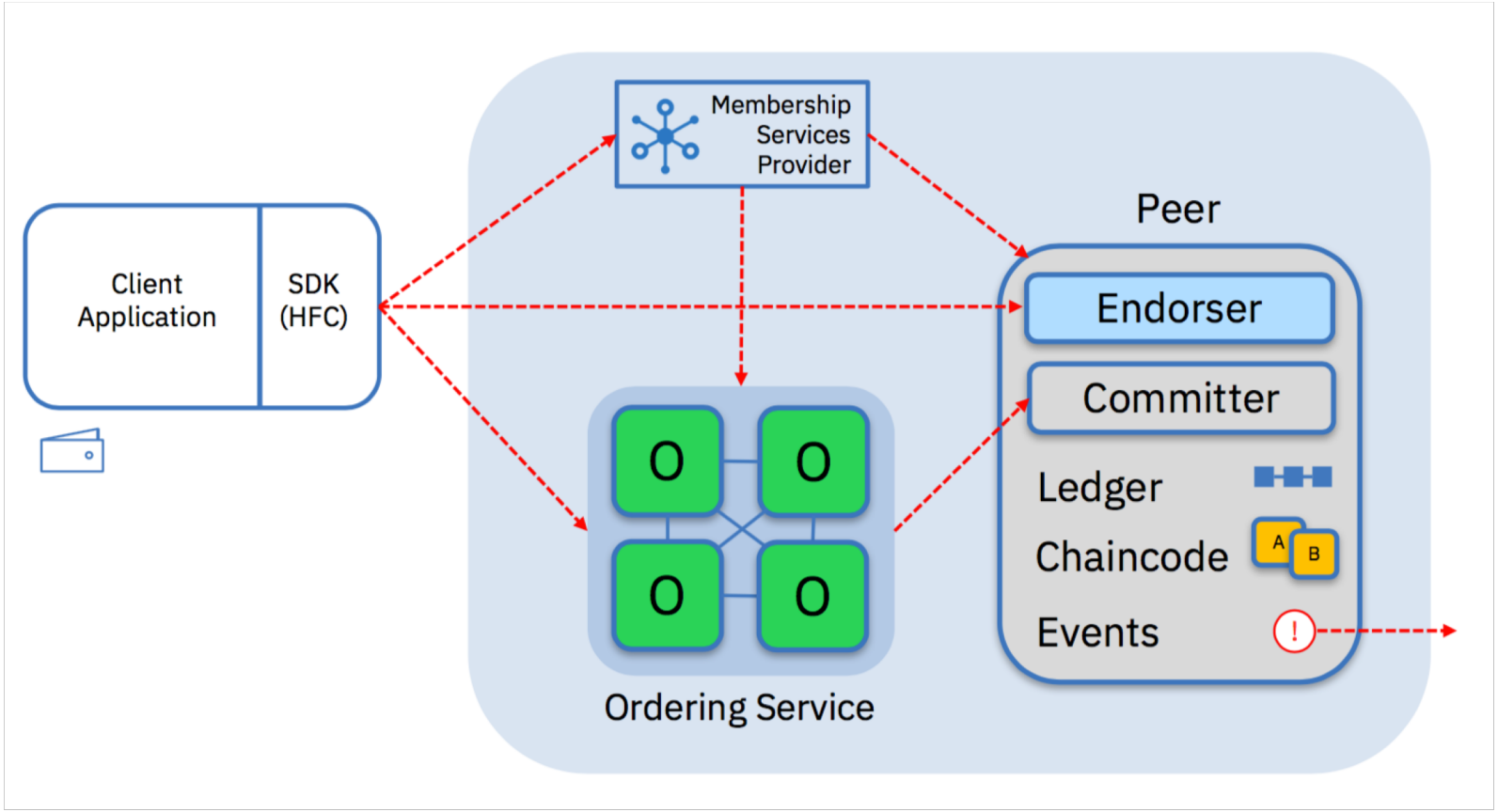
Over 291 developers, 41 companies, over 8,00 change sets!

March 2018 | June 2018 | Oct 2018 | *Dec 2018* (quarterly)*

HYPERLEDGER

* Dates determined by the Hyperledger community, subject to change

Архитектура Hyperledger Fabric



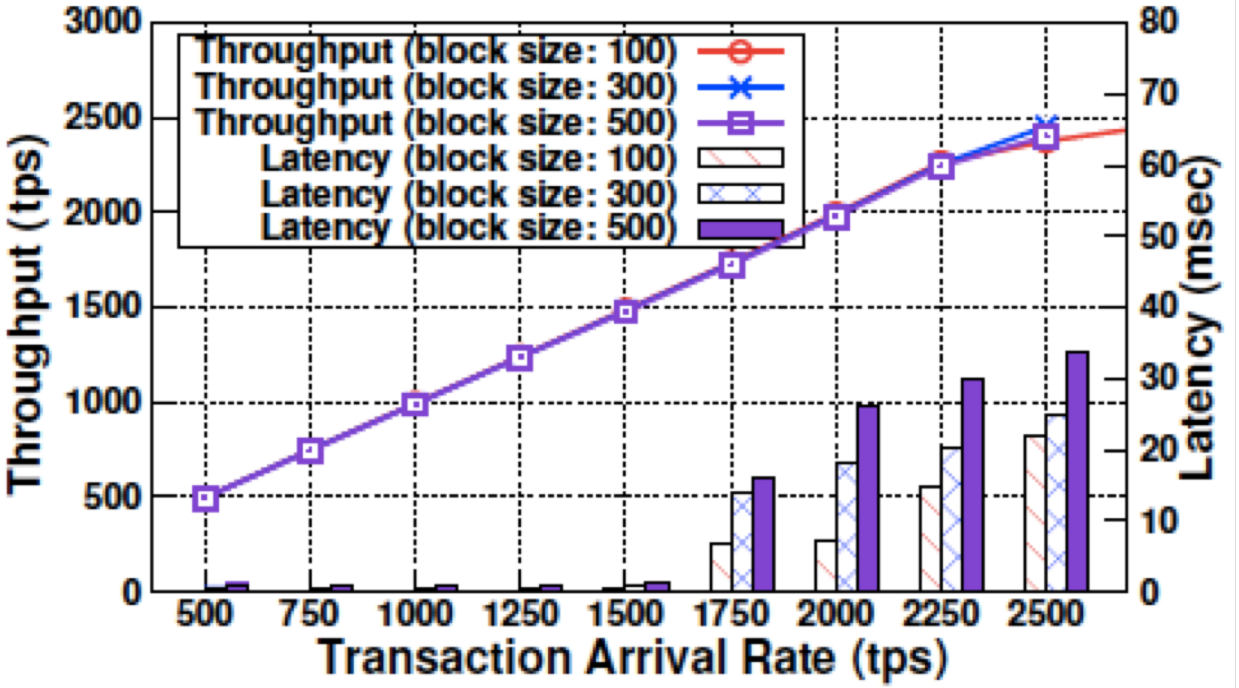
Исследовательская работа по оптимизации Fabric

Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform

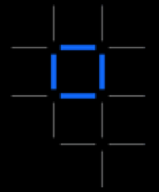
Parth Thakkar*
National Institute of Technology, Trichy, India

Senthil Nathan N
IBM Research Lab, India

Balaji Viswanathan
IBM Research Lab, India



~2500 транзакций в секунду



Сценарии использования

Примеры реализованных проектов – как выбирать сценарий

– Выявить хороший сценарий использования блокчейн не всегда просто!

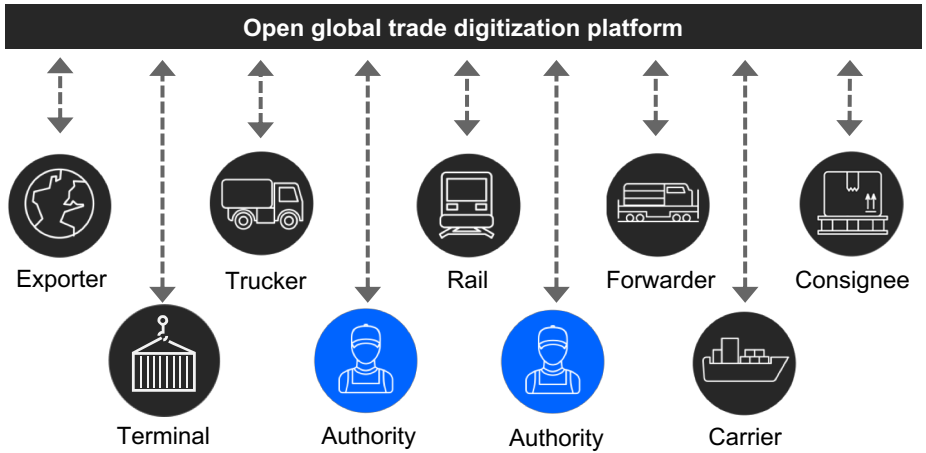
1. Бизнес-проблема, которая будет решена (нельзя решить более зрелыми технологиями)
2. Идентифицируемая бизнес-сеть с участниками, активами и транзакциями
3. Необходимость в доверии к информации
4. Разные компании нуждаются в едином представлении данных
5. Разные компании изменяют данные в рамках одного процесса
6. Участие посредников вносит дополнительную стоимость
7. Взаимодействие между различными участниками занимает слишком долгое время

Пекинский Технологический Институт

Предоставляют решение уровня Blockchain-as-a-service
на базе IBM LinuxONE

«На базе сотрудничества с IBM и внедрению платформы LinuxONE мы получили доступ к передовой технологии для наших студентов и сотрудников.»
- Ганги Дин, декан факультета разработки ПО, Пекинский технологический институт

Maersk



- Совместная платформа **IBM и Maersk;**
- Реализован быстрый, безопасный и эффективный способ обработки процессов документирования;
- Обмен событиями и документами цепочки поставок в реальном времени;
- Устранены задержки, связанные с ошибками в физическом перемещении документов;
- Экономия до 15% (1,8 трлн $ – стоимость мировой торговли год).

Примеры реализованных проектов в разных отраслях

Торговое финансирование

Digital Trade Chain

MIZUHO

NATIXIS TRAFIGURA

Торговые операции

DTCC

CLS Fundamental to FX

JPX

Bolsa Comercio SANTIAGO

Покрытие сложных рисков

AIG

Standard Chartered

Идентификация (KYC)

SECURE KEY

Crédit Mutuel ARKEA

DIACC

Управление частным капиталом

NORTHERN TRUST

BORSA ITALIANA

SBI GROUP SBI証券

Программа лояльности

UnionPay 银联

Обмен данными о здоровье

FDA

Мошенничество/ Compliance Registry

دبي الذكية SMART DUBAI

Распределенная энергия/ Кредиты на выбросы

TenneT

ENERGY BLOCKCHAIN LABS

Цепочка поставок

MÆRSK

PSA The World's Port of Call

Безопасность продуктов питания

Walmart

Driscoll's Only the Finest Berries

Tyson

McLANE

Dole

Kroger

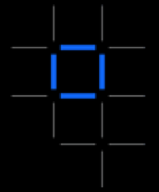
Nestlé

Unilever

gsf golden state foods

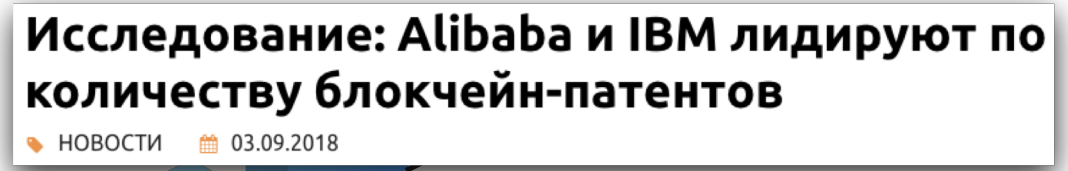
Доказательство происхождения/трекинг

everledger



Блокчейн в IBM

Развития темы блокчейн в IBM



Aug 2017
Анонс IBM Blockchain Platform

Jul 2017
Релиз Hyperledger Fabric v1.0

Feb 2017
Запуск «early program» для Hyperledger Composer в IBM labs

Dec 2016
Число блокчейн-проектов IBM достигает 400

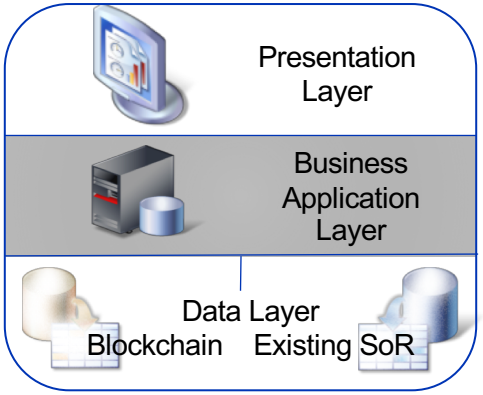
Jun 2016
IBM открывает первые блокчейн-гаражи для клиентов. Релиз HyperLedger Fabric 0.6.

Feb 2016
IBM становится одним из основателей проекта HyperLedger в рамках Linux Foundation. Передача кода и прав интеллектуальной собственности.

Aug 2015
Первый прототип блокчейн технологии для enterprise (Open Blockchain). Первые проекты с клиентами.

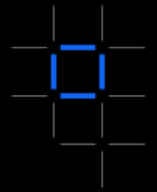
IBM помогает начать работу с Blockchain

- **Обучение в Учебном центре IBM**
  - Курс «Основы технологии Блокчейн» - 2 дня
  - Курс «Основы разработки на Блокчейн» – 2 дня
- **Помощь в подготовке среды для начала использования технологии**
  - Создание макетов решений для возможности использования в рамках исследовательских проектов
  - Установка и базовая настройка программно-аппаратного комплекса для запуска необходимых компонентов решения на Blockchain
  - Определение и выбор компонентов Blockchain для реализации решения
  - Установка и настройка технологических компонентов решения на Blockchain
  - Поиск потенциальных базовых сценариев с целью быстрой реализации простого прототипа



Онлайн ресурсы

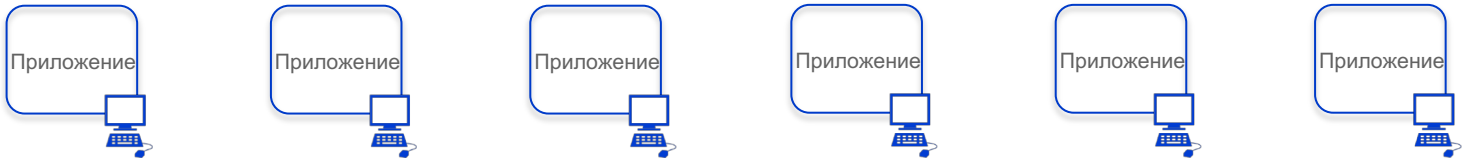
- **Обучение**
  - Основы технологии Блокчейн
    - https://developer.ibm.com/courses/all/blockchain-essentials/
  - Руководство по началу работы с IBM Blockchain для разработчиков
    - https://www.ibm.com/developerworks/ru/library/cl-ibm-blockchain-101-quick-start-guide-for-developers-bluemix-trs/index.html
  - IBM Blockchain для разработчиков
    - https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers
- **IBM Blockchain Platform – «starter plan» бесплатно на 30 дней**
  - https://console.bluemix.net/catalog/services/blockchain
- **Среда для быстрой разработки в Hyperledger Composer с шаблонами и примерами**
  - https://composer-playground.mybluemix.net/



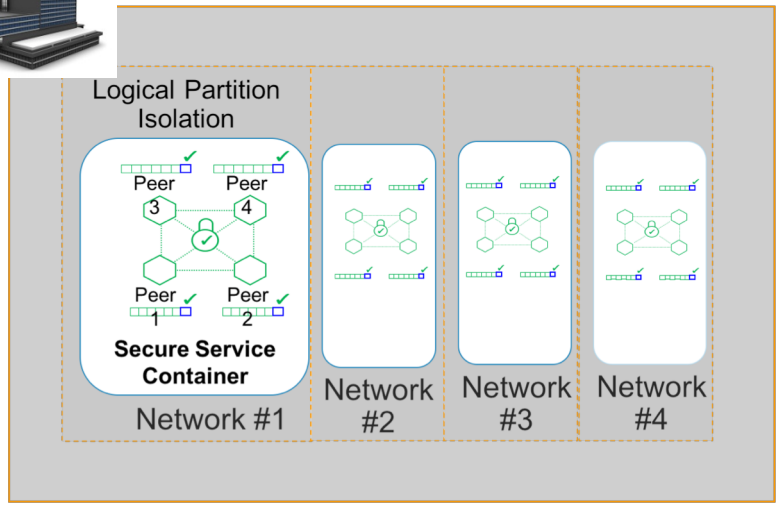
Платформа для блокчейн

Реализация архитектуры решения на основе Blockchain

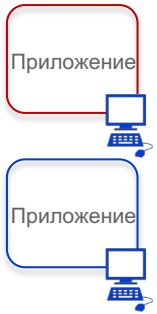
Участники сети Блокчейн



Инфраструктурный провайдер

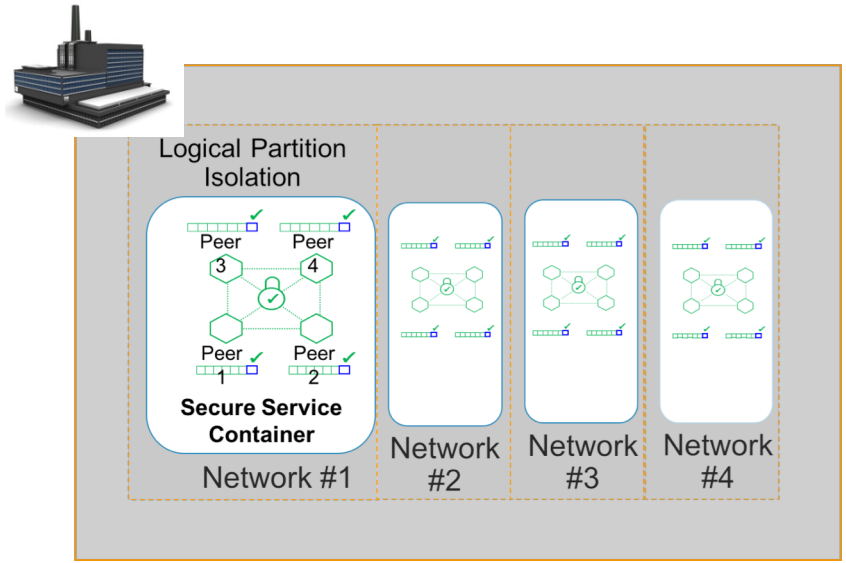


Оператор сети Блокчейн



Требования к провайдеру

- Безопасность и шифрование на различных уровнях
- Возможность выполнять центральное администрирование сетей
- Минимальные сетевые задержки
- Максимальная изоляция ресурсов отдельных блокчейн-сетей
- Практически линейная масштабируемость
- Надежность критичных элементов



Инфраструктура на основе LinuxONE

3 измерения для обеспечения безопасности в сетях Blockchain

- На уровне кода
- На уровне контейнера с критическими узлами
- На уровне физического сервера

Безопасная инфраструктура

Hardware Security Module

Encrypted Storage

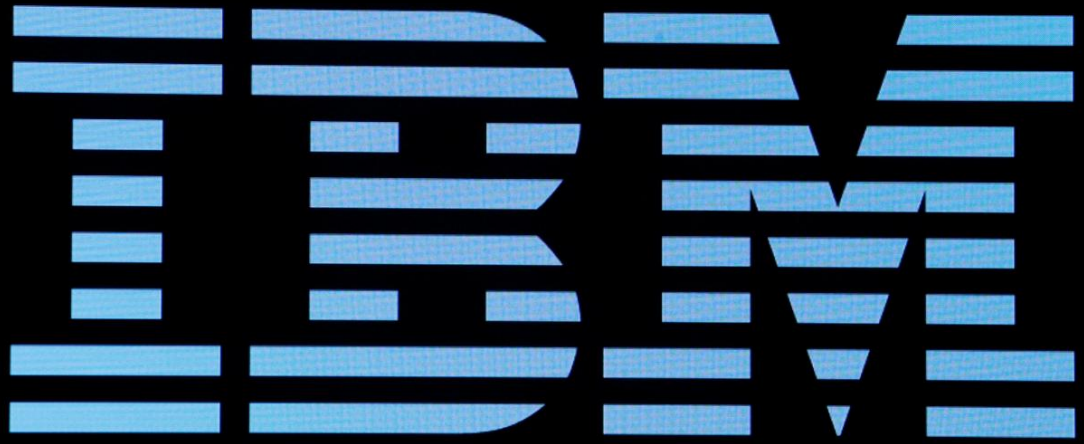
Secure Services Containers

Membership Services

Secure Comms

Consensus

Hyperledger Fabric



IBM Systems Consulting (IBM Russia/CIS)

Contacts:

Ruslan Karpov (ruslan.karpov@ru.ibm.com)

Vladimir Sergienko (v.sergienko@ru.ibm.com)

Grigoriy Maltsev (g.Maltsev@ru.ibm.com)