Омский научный семинар
«Современные проблемы радиофизики и радиотехники»

Блокчейн (Blockchain) или технология надежного распределенного хранения достоверных данных
Часть 1

Докладчик: Инна Леонидовна Бондарева
Компания «ТАРГЕТТА» (г.Москва)

г.Омск, 24 декабря 2016 г

OPEN INNOVATION MARKETPLACE. OIMP
INTERNATIONAL ASSOCIATION
OF SCIENCE PARKS AND AREAS. IASP
MOSCOW 2016

Инновационные решения и технологии в сфере распределенных реестров на базе технологий блокчейна
Видео

Сбербанк Технологии

BLOCKCHAIN REVOLUTION

- Blockchain — **distributed ledger** representing a network consensus of every transaction that has ever occured....

- World Wide Web
- World Wide Ledger

Don Tapscott

BLOCKCHAIN ECOSYSTEM

- Blockchain is a peer-to-peer distributed ledger technology for a new generation of transactional applications that establishes trust, accountability and transparency while streamlining business processes.

Hyperledger.org

СЕТЕВАЯ ЭВОЛЮЦИЯ. ИЛИ РЕВОЛЮЦИЯ?

- Before 2005:

Closed and centralized IoT networks

- Today:

Open acess IoT networks, **centralized cloud**

- 2025 and beyond:

Open acess IoT networks **distributed cloud**

Report IBM: «Device democracy. Saving the future of the IoT» page 9

От закрытых к открытым сетям

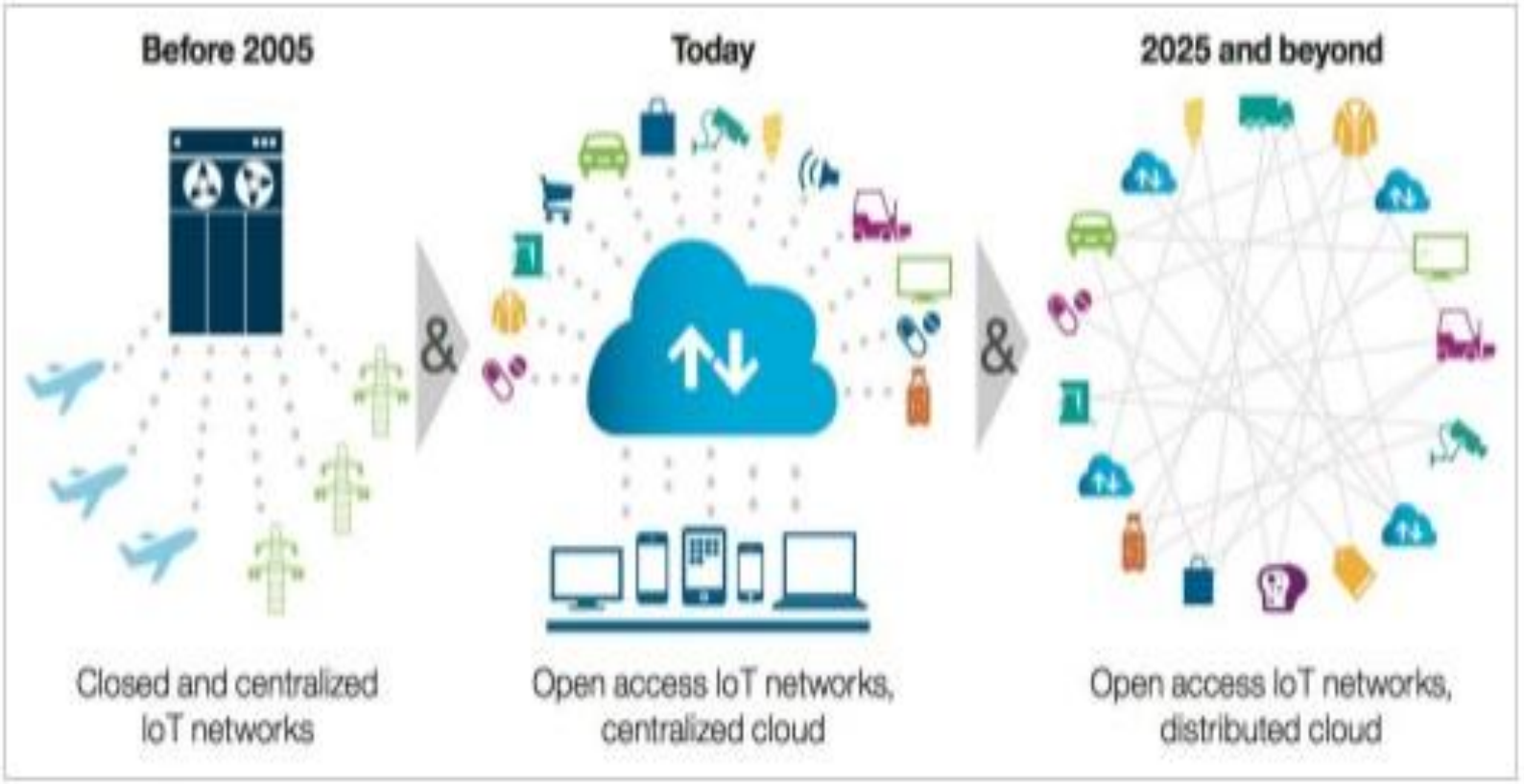


Иллюстрация реорганизации сети в зависимости от современных потребностей, отчет IBM "Device democracy. Saving the future of the Internet of Things" стр. 9

Одноранговая сеть + консенсус

Решение задачи византийский генералов: БЛОКЧЕЙН:

Задача византийских генералов — в криптологии задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть злоумышленниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов.

Лесли Лампорт, 1982 г.

Achieving trust in the digital age.

TRUST:

1. «Rather than dressing for success, corporations can undress for success...»

2. From the netwirk and even from objects on the network

3. Data is becoming a new asset class

Don Tapscott

70% всех инвестиций в Силиконовой долине - Блокчейн

- Блокчейн и Сбербанк технологии:

а. документооборот

б. система обмена финансовыми документами

в. факторинг

г. доверенности

д. закладные

е. внутрибанковские взаиморасчеты

СТРУКТУРА БЛОКЧЕЙНА

1. Blockchain – цепочка блоков данных, где каждый блок связан с предыдущим.

   Блок содержит в себе набор записей.

   Новые блоки всегда добавляются строго в конец цепочки.

2. Принципы: распределенность, открытость, защищенность.

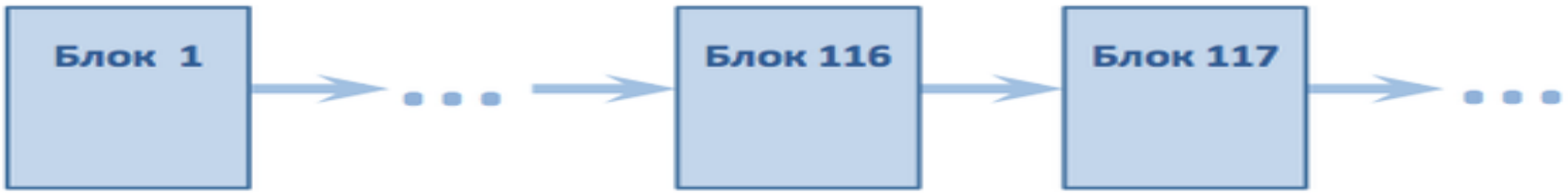
3. Копии данных или части данных блокчейн хранятся на всех компьютерах пользователей блокчейн.

4. Равноправность. Каждый отвечает сам за себя.

5. Каждый новый пользователь укрепляет систему.

6. Блоки и содержимое — открыты для всех.

7. Шифрование



Открытость и достоверность блокчейн

любой может увидеть, что у кого-то есть миллион.

У кого конкретно он есть – этот любой узнать не может, пока владелец миллиона не даст ему **специальный ключ**, тем самым подтверждая, что миллион есть именно у него

КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ

- Ключ - алгоритм хэш-функции,

например такой:
11731619542357098500868790785326998466564056403945758400791312963993 5

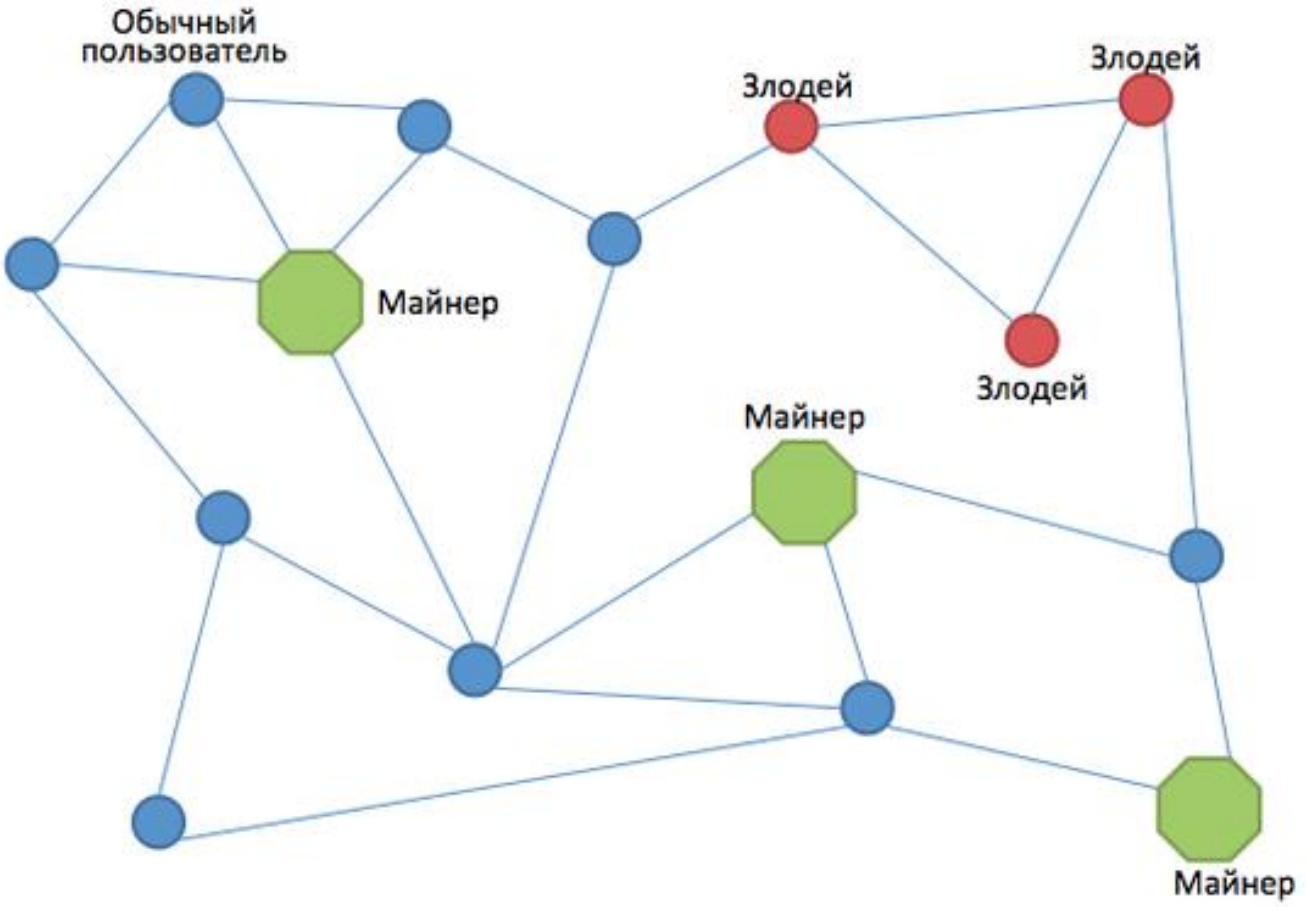
- Свойства ключа:

а. Обладая ключом, нельзя узнать исходный набор данных

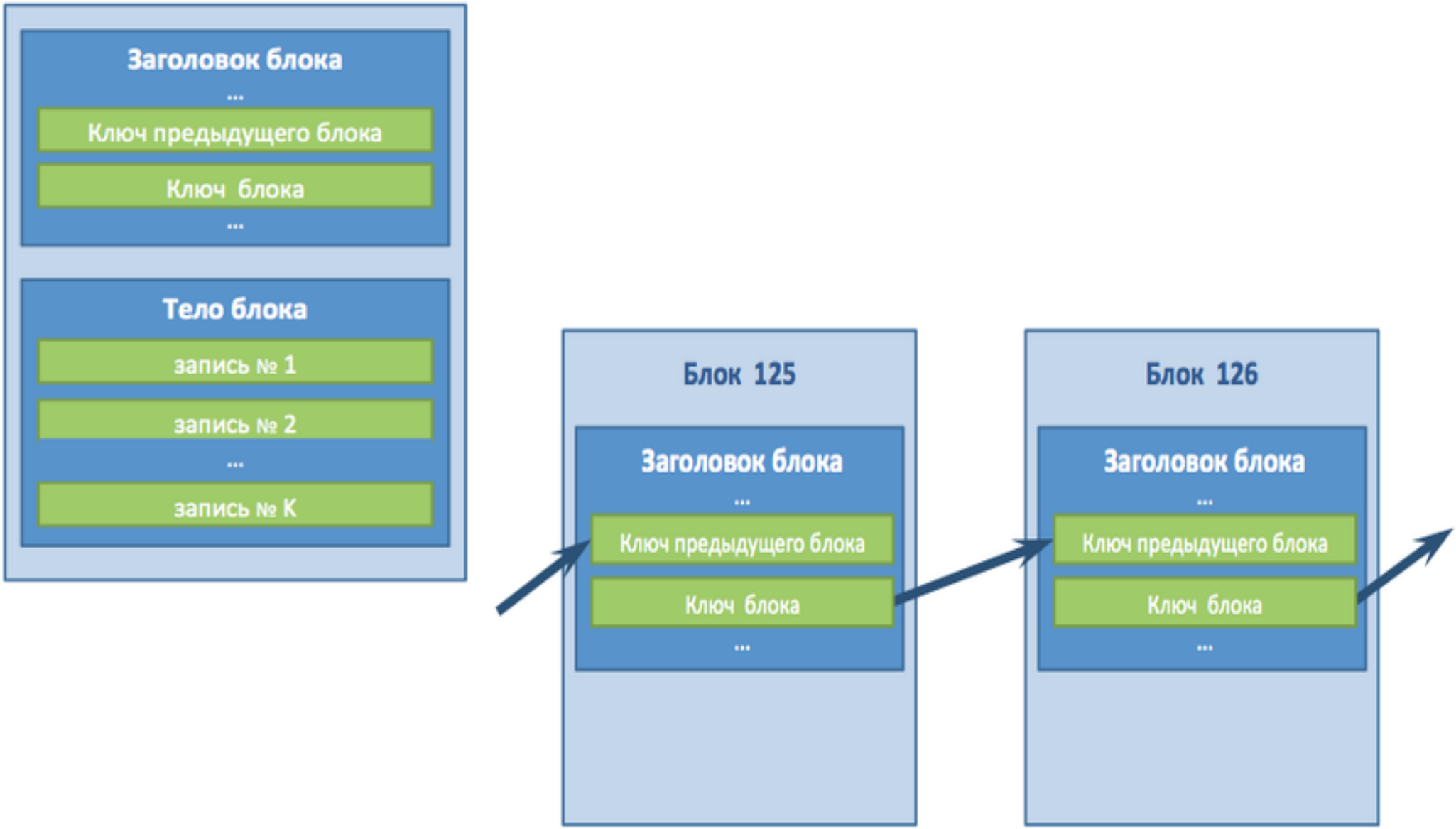
б. Найти другой набор данных, дающий такой же ключ, практически нереально

в. При изменении исходных данных ключ полностью меняется

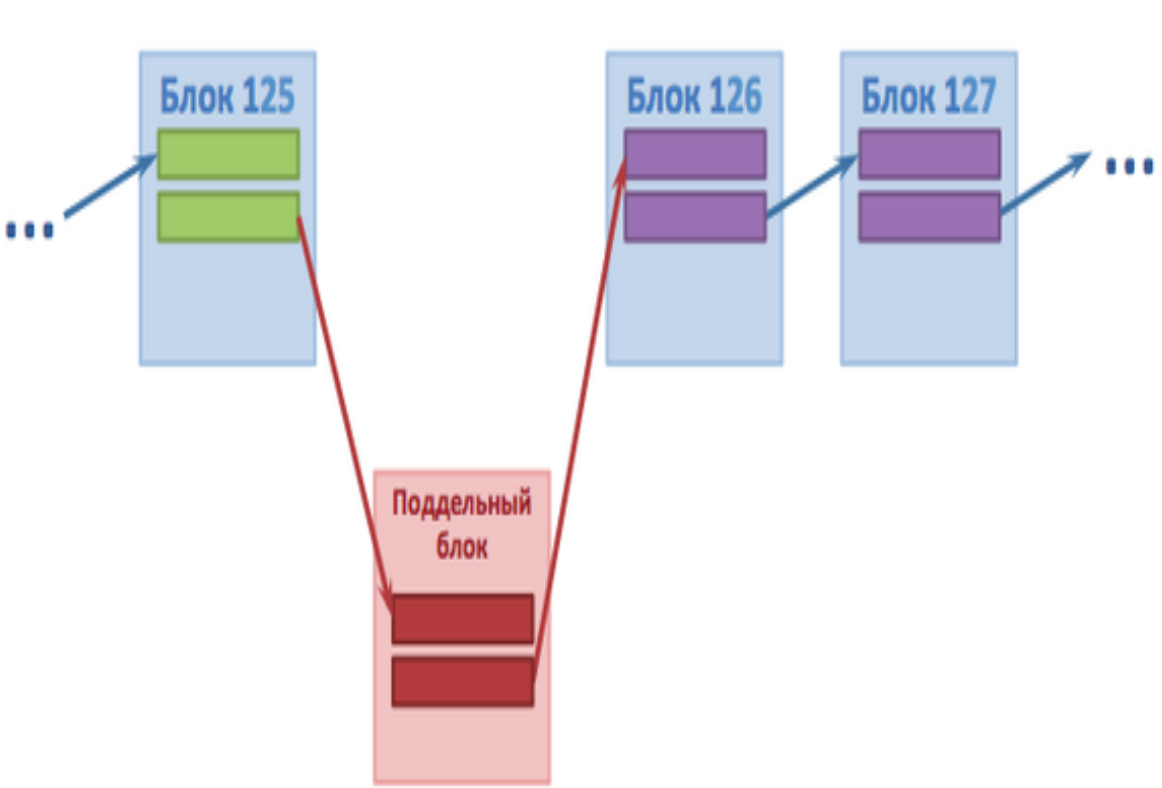
Структура сети. Майнеры



СТРУКТУРА БЛОКА



Поддельный блок и записи



Умные контракты

Реализация интерфейса:

- Человек — машина — человек
- Машина — машина
- Человек — человек

- Среда разработки:

- hyperledger.org

- ethereum

Блокчейн. Часть 2

- ВОПРОС: Какое применение технологии распределенных реестров Вы видите?

- ОТВЕТ: 31 декабря в 11-30!

ЛИТЕРАТУРА

- Blockchain revolution.

Don Topscott

- OIMP. IASP. Video.
- Сергей Лоншаков. Эксурс по блокчейн технологии
- Форум «Открытые инновации 2016». Сессия «Основы Блокчейн»