

Партнерский семинар компании «Актив»

13–16 июня 2017, ивент-отель «Конаково Ривер Клуб»

Блокчейн и его защита

Владимир Салькин
Менеджер по продуктам
компании «Актив»



Почему СЕЙЧАС?

1 июля 2016 года

**Создан консорциум по развитию
блокчейна в России**



Открытие
Банк



Тинькофф
Банк



МДМ Банк



QIWI



БИНБАНК

Октябрь 2016 года

Пилот Digital Ecosystem по обмену документами на основе блокчейн



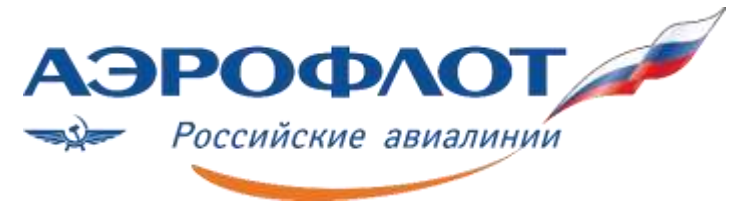
Федеральная
Антимонопольная
Служба



СБЕРБАНК



РУССКИЙ УГОЛЬ



Март 2017 года

**Блокчейн в программе
«Цифровая экономика»
2017–2025 г.**



4 июня 2017 года

**Центробанк заявил
о создании собственной
криптовалюты**



2 июня 2017 года

**В.В. Путин провел
личную встречу
с Виталием Бутериным**



4 июня 2017 года

**Центробанк заявил о
создании собственной
криптовалюты**

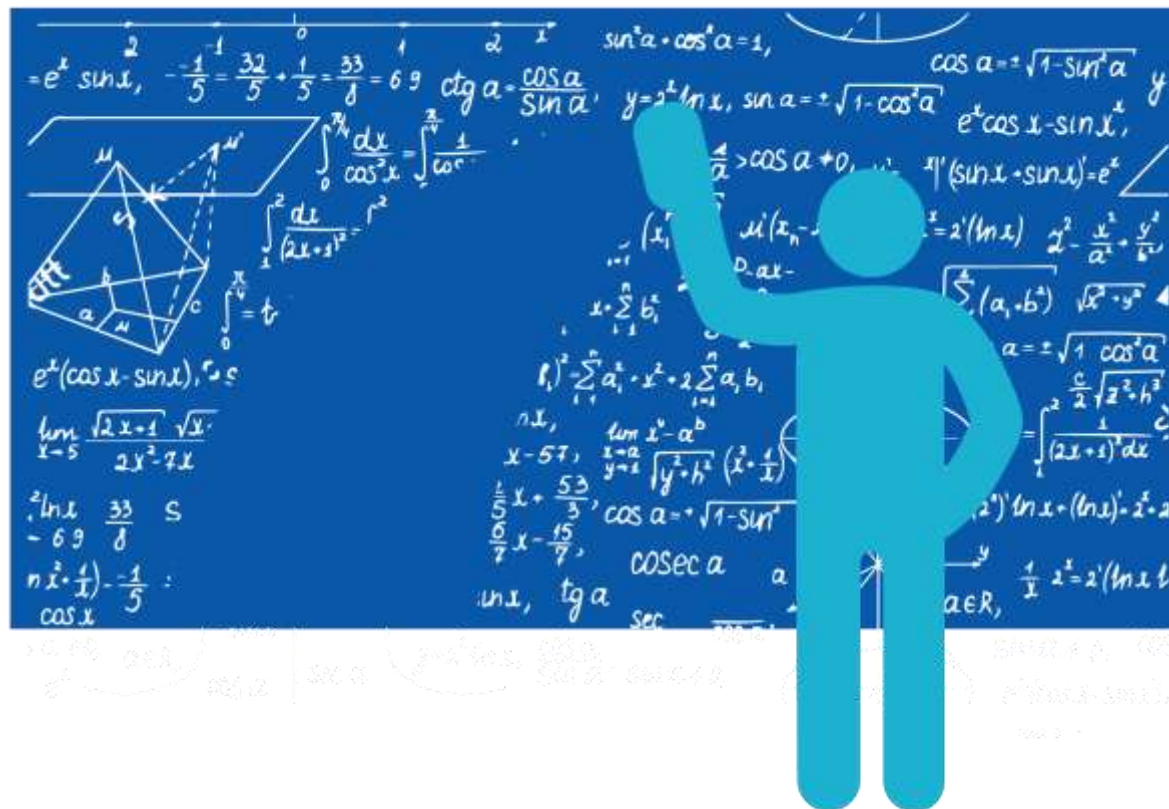


Как работает блокчейн?

Как это работает?

Вася	5 конфет	1 конфета для Пети $5-1=4$ <i>Вася</i>		
Петя	3 конфеты	1 конфета для Васи 1 конфета для Маши $3+2=5$ конфет	4 конфеты для Кати $5-4=1$ <i>Петя</i>	4 конфеты от Маши $1+3=4$
Маша	7 конфет	1 конфета для Пети $7-1=6$ <i>Маша</i>		3 конфеты для Пети $6-3=3$ <i>Маша</i>
Катя	1 конфета		4 конфеты от Пети $1+4=5$	

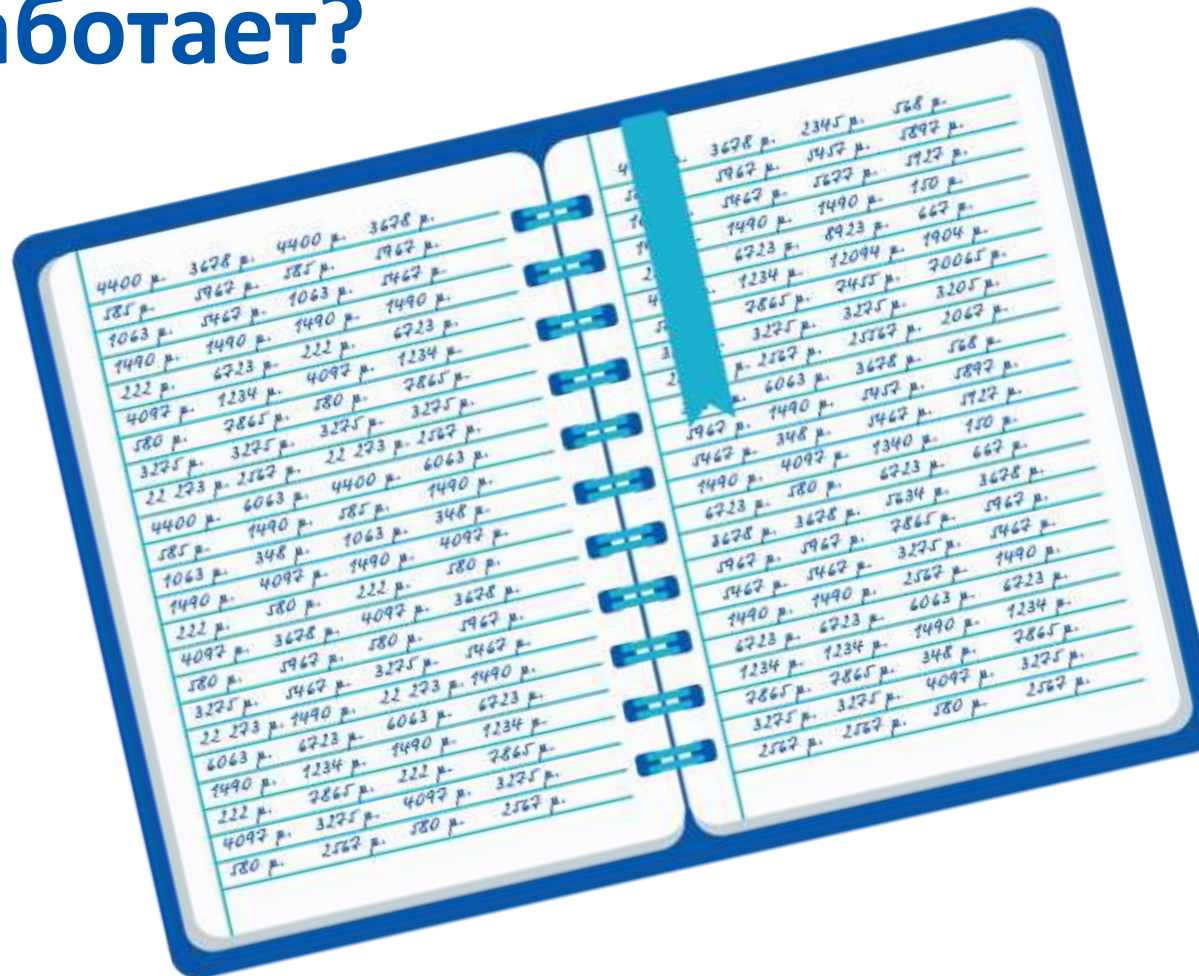
Как это работает?



Как это работает?



Как это работает?



Как это работает?



Заложено на этапе проектирования

- Защита от подделки
- Защита от цензуры
- Защита от отката операций
- Защита от нелегитимной эмиссии
- Защита от непоследовательности
- Защита от простоя

Почему блокчейн не покорил мир?

- Неотказуемость
- Проблема 51%
- Проблема консенсуса
- Проблема выбора
- Скорость работы
- Размер
- **Отсутствие развитой экосистемы**

А что с безопасностью?

Уязвимые реализации (инцидент The DAO)

Вредоносные реализации

Иностранные алгоритмы

Подписывается не вся информация

Уязвимость закрытого ключа

Почему закрытый ключ так важен в блокчейн?

Защита лежит на плечах пользователя

Социальную инженерию НИКТО не отменял

Нет отката операций

Решение проблемы безопасности ключа



Чем помогут токены?



**Неизвлекаемость
закрытого ключа**





Вычисление ЭЦП на борту





Secure Messaging





Защита от удаленного управления





Двухфакторная аутентификация



Вопросы



Контактная информация

Электронная почта:

Личная – sv@rutoken.ru

Общие вопросы – info@rutoken.ru

Отдел продаж – sales@rutoken.ru

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

8-495-925-77-90



