САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

#ЛекторийМинОбрНауки
9 февраля 2018 г.

Blockchain: криптовалюты и не только

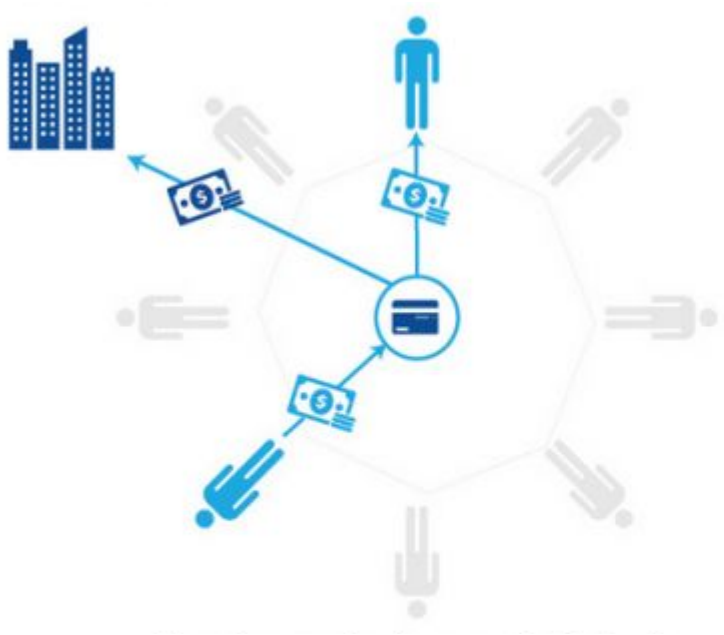
Кузнецов Андрей, к.т.н., доцент кафедры
геоинформатики и информационной безопасности

Содержание

- Банки, транзакции, … Потребность в изменениях
- Блокчейн. История развития
- Криптовалюта. Биткоин. Хеш-функция
- Структура блока. Растущая сложность вычислений
- Майнинг. Как зарабатывать на криптовалюте?
- Proof-of-Work (Доказательство работы)
- Форк
- Проект Ethereum
- Умные контракты как новое применение blockchain
- Что дальше?.. Интернет вещей, распределенные хранилища, …
- P.S…

Как сейчас производятся денежные операции?

- Централизованная система
- Есть 3-и лица, выступающие гарантом выполнения операций
- Центробанк хранит всю информацию о транзакциях
- Постоянно растущая сложность в обеспечении безопасности такой системы
- Транзакции могут быть отменены
- Наличие комиссии за проведение операций (даже незначительных)
- Время выполнения транзакций достигает нескольких дней
- Комиссия за конвертацию валют

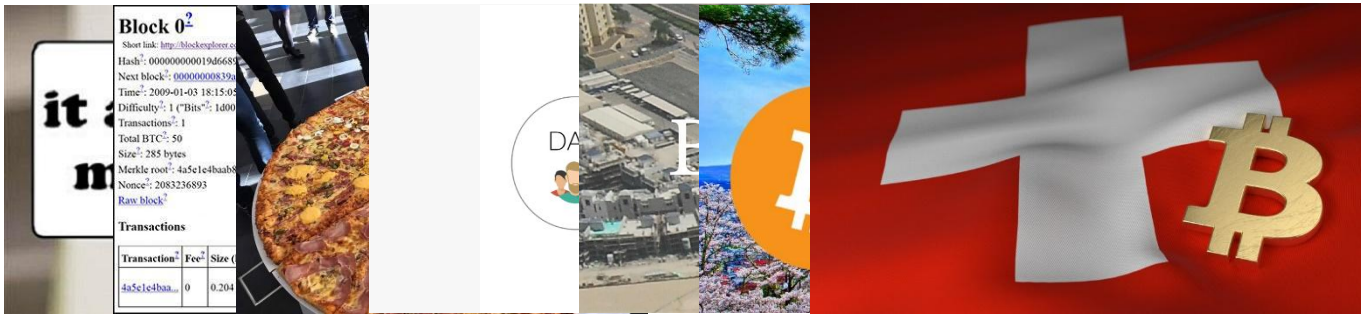


Альтернатива…

- Децентрализованная система
- Все транзакции авторизованы
- Информация о транзакциях доступна всем узлам сети
- Незначительное время выполнения транзакций (~10 минут)
- Транзакции необратимы (двойная трата денег невозможна)
- Отсутствие комиссии за конвертацию валют
- Высокая безопасность (каждый участник сети выступает в роли гаранта)

Немного истории

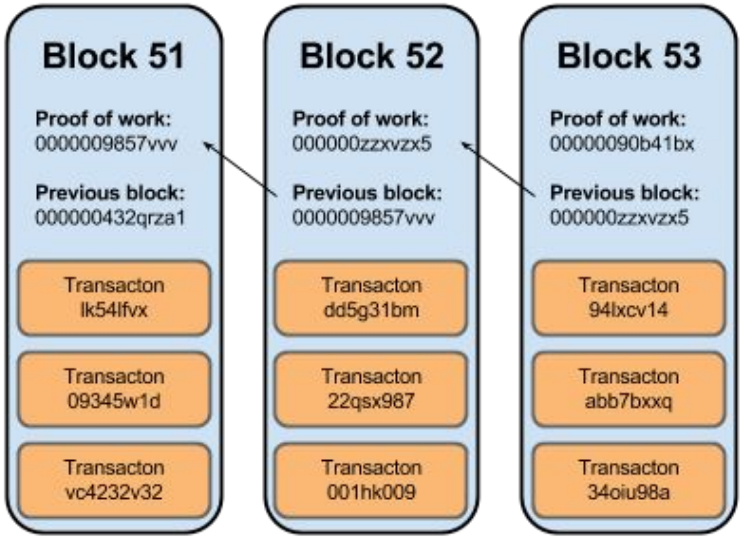
31 октября 2008 – Публикация статьи Сатоши Накамото о биткоинах и блокчейне
3 января 2009 – Первый созданный блок «Genesis block»
22 мая 2010 – Первая покупка посредством биткоинов (2 пиццы за 10000 биткоинов) в размере 25$ (да-да, тогда он стоил столько ☺)
Декабрь 2013 – Виталик Бутерин запускает Ethereum и появляются умные контракты (smart contract)
Май 2016 – Создание Децентрализованной Автономной Организации (ДАО) – рекорд краудфандинга в 150 млн.$
Декабрь 2016 – Анонсирование программы Dubai Blockchain Strategy
Апрель 2017 – Криптовалюты официально признаны в Японии
Январь 2018 – Швейцария начинает сбор налогов посредством биткоинов



Что такое блокчейн?

- Связанный посредством хеш-значений список
- Допускается только добавление блоков
- Новые блоки добавляются в конец списка
- Для изменения блока в цепи потребовалось бы изменить все последующие блоки
- Неэффективен в сравнении с реляционными СУБД

Не столько **технология (алгоритм)**, сколько **новая парадигма** информационного обмена



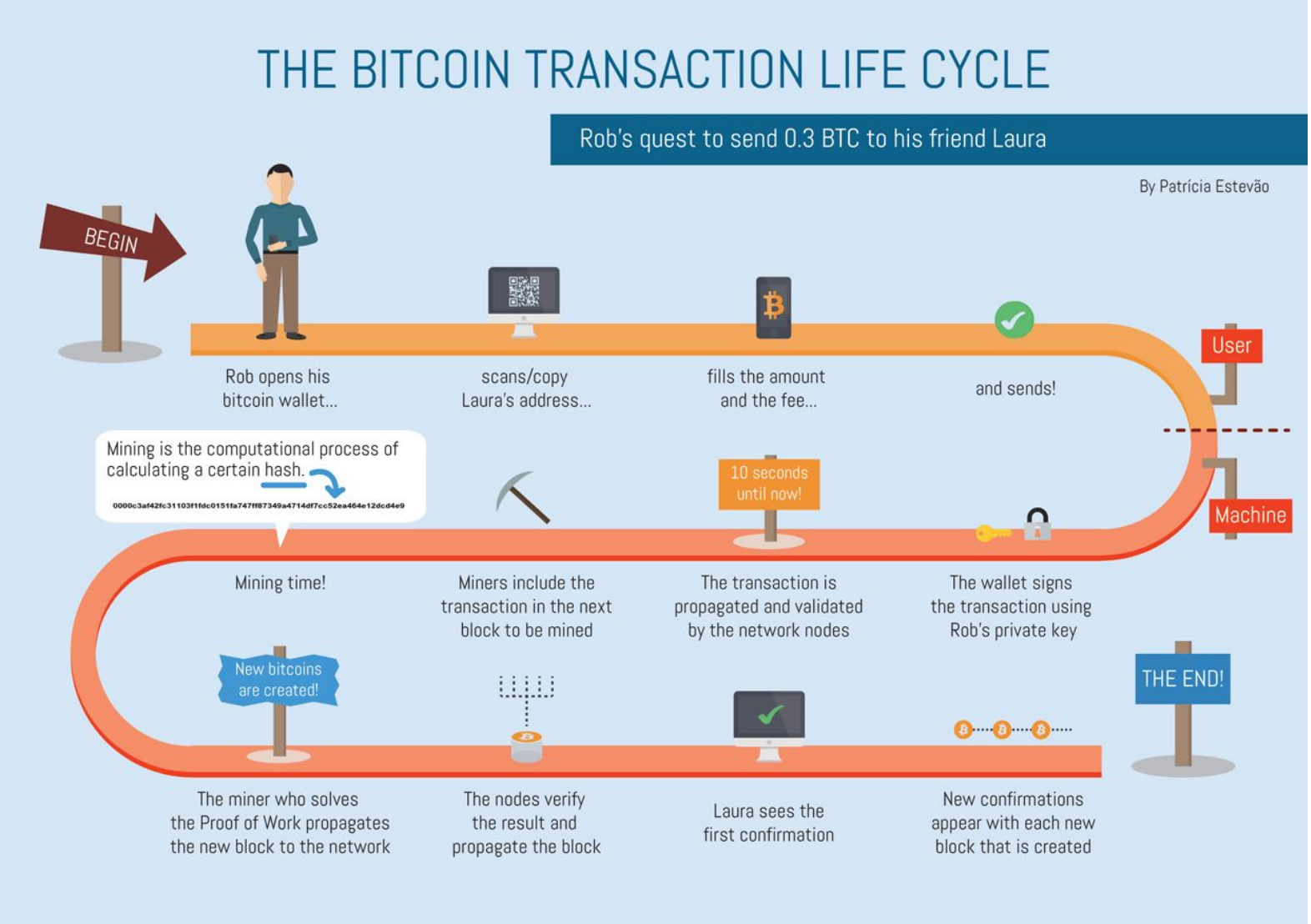
На перекрестке:

1) Теории игр
2) Криптографии
3) Сетевого взаимодействия и распределенной передачи данных
4) Экономики

Блокчейн как распределенное хранилище транзакций. Криптовалюты

- Блок содержит список транзакций
- Информация о блоках распространяется по всей сети
- Распространение производится по P2P протоколу (пиринговая сеть)
- *Майнер* – участник сети, создающий блоки
- Майнеры добавляют транзакции в новые блоки
- Майнеры выполняют дополнительный объём работ
- Все узлы сети могут проверить корректность блоков и транзакций
- Достижение консенсуса в сети является одной из важнейших задач

Выполнение транзакции «на пальцах»

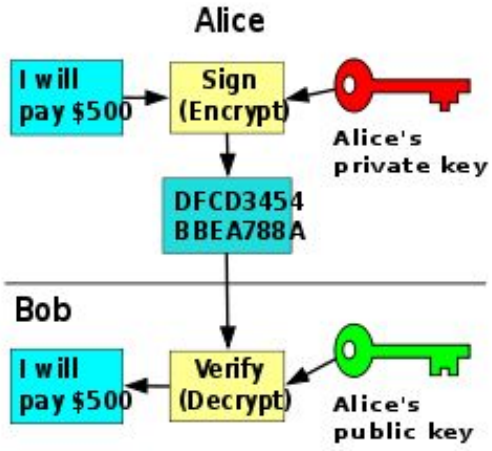


Хеш-функция – основа блокчейн и биткоин

Хеш-функция — однонаправленная функция, преобразующая входные данные любой длины в массив байтов фиксированной длины

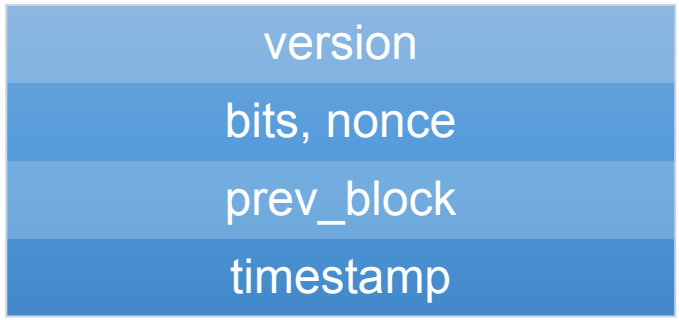
SHA-256 (Secure Hash Algorithm)
- дайджесты сообщений
- эмиссия криптовалюты
- цифровая подпись

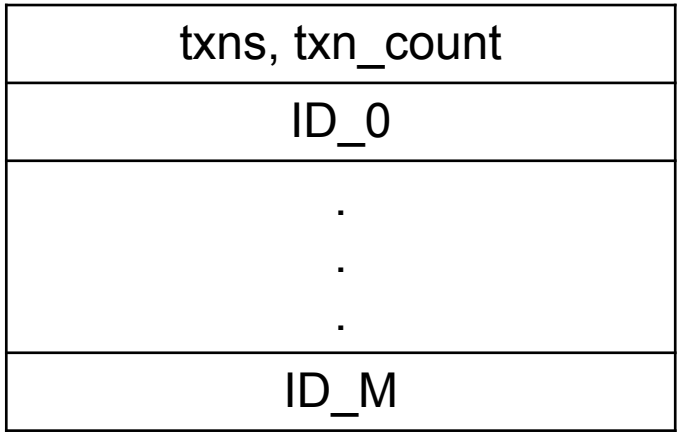
Асимметричное шифрование
- публичный ключ (public key) – ДЛЯ ВСЕХ
- приватный ключ (private key) – ДЛЯ СЕБЯ



Структура блока

- ***version*** – версия блока
- ***bits*** — характеристика сложности создания блока
- ***nonce*** — значение, необходимое для создания блока
- ***prev_block*** — хеш предыдущего блока
- **timestamp** — дата и время создания блока
- ***merkle_root*** — хеш всех транзакций в блоке
- ***txn_count*, *txns*** — число транзакций в блоке и их список





Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

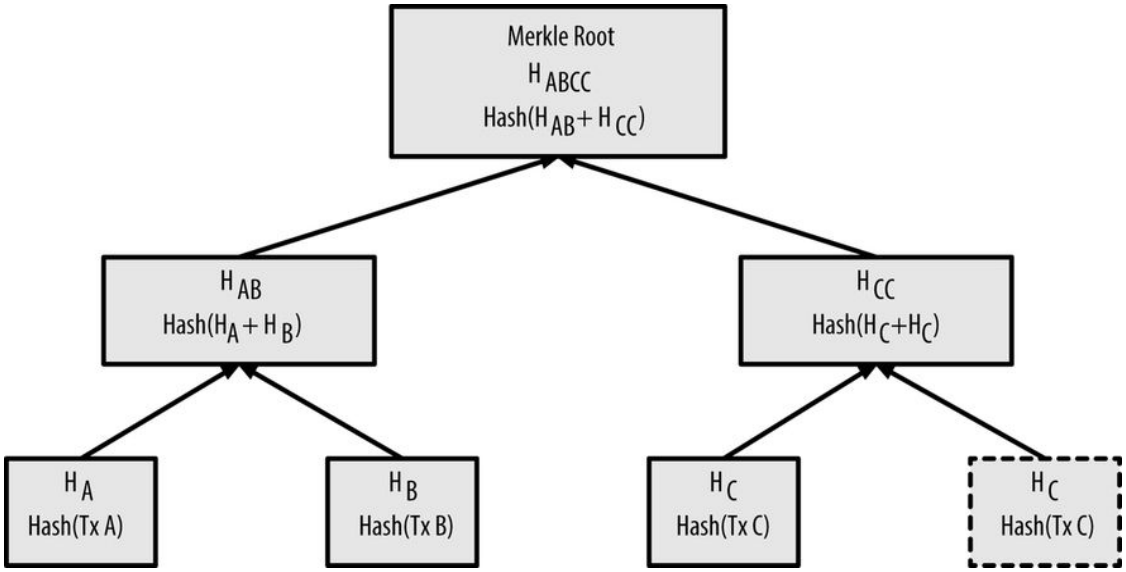
Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

Дерево Меркла — бинарное дерево хешей

1. Сначала считаются хеши всех транзакций в блоке
   H_A = SHA256(SHA256(A))
2. считаются хэши от суммы хешей транзакций
   H_AB = SHA256(SHA256(H_A + H_B))
3. Точно также считаем хэши от суммы получившихся хешей
   H_ABCD = SHA256(SHA256(H_AB + H_CD))



Задача майнера – быстрее других подобрать **nonce** путем перебора всех значений, пока **hash** максимально не приблизится к **target**

Награда за блок
+
fees от транзакций

Структура блока. Difficulty, bits, target,…

Рассмотрим блок **#414793**

Difficulty	199,312,067,531.24
Bits	403014710
Hash	00000000000000000530216a17ab1e11502720c784975dc7618f8408df6f7c77

Bits = 403014710 = **0x18058436**
0x18 – экспонента
0x058436 – мантисса

target = **0x058436** * 2^(8 * **0x18** - 3)

difficulty = max_target / target,
max_target = 0x1d00ffff (в формате bits)

Структура блока. Difficulty, bits, target,…

Рассмотрим блок **#414793**

Difficulty	199,312,067,531.24
Bits	403014710
Hash	00000000000000000530216a17ab1e11502720c784975dc7618f8408df6f7c77

difficulty = 199,312,067,531.24

или

log2(199,312,067,531) + 32 = **69**.53 бит

Hash = **0000 0000 0000 0000 0**530 216a 17ab 1e11 5027 20c7 8497 5dc7 618f 8408 df6f 7c77

17 нулей * 4 бита = 68 бит, 5 = **0**101 => +1 бит = **69** бит

Сложность создания блока в GH/s:

2^69.53 / 10 min = 1,420,000,000

Майнинг. Пример создания нового блока

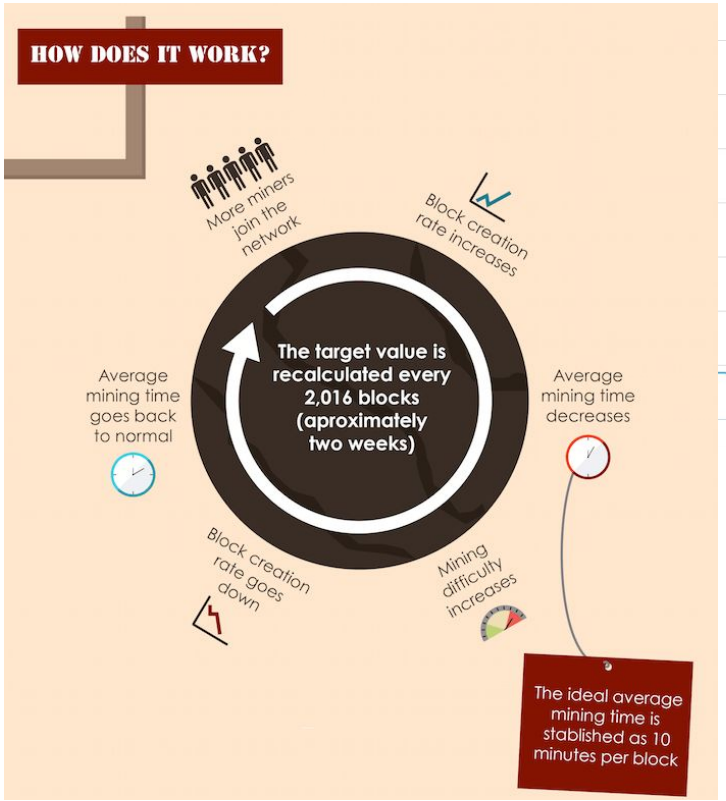
Вход: хеш всех транзакций (корень Меркла) + хеш прошлого блока

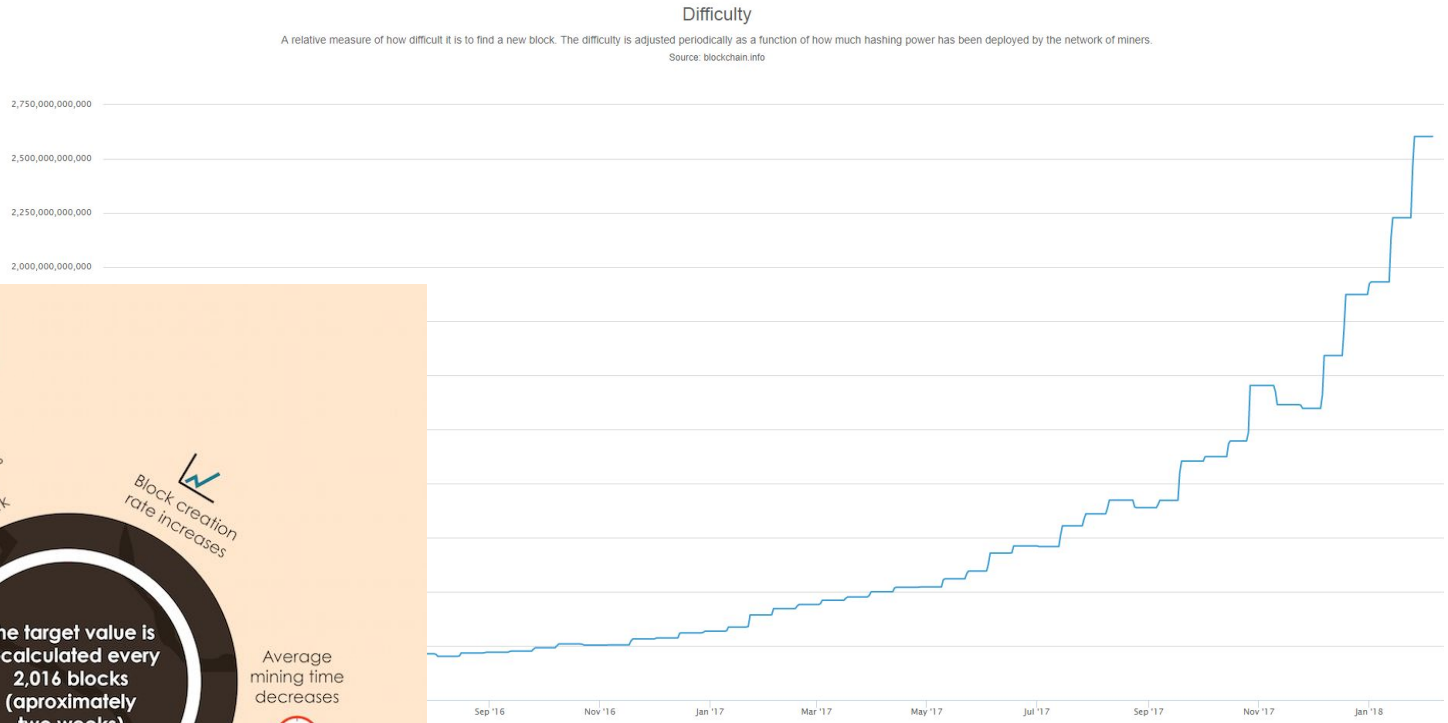
Процесс майнинга – подбор nonce:

- Difficulty = 1 – ищем такой хеш, чтобы в начале был «0» (nonce=20)
- Difficulty = 2 – ищем такой хеш, чтобы в начале был «00» (nonce=120)
- Difficulty = 4 – ищем такой хеш, чтобы в начале был «0000» (nonce=69817)
- …

Nonce	Difficulty (No of Leading zeros)	Input String	Nonce + Input String	Hash (Nonce + Input String)
1	1	Корень Меркла + Хеш прошлого блока	nonce + Корень Меркла + Хеш прошлого блока	6F29B70C30D2D63D7E8E66B194B325B764CD877A18BE7820F846528FC9F794C3
2	1			6A09C54D2C1A20BF4B07640B30DE767D570BAEC9B08F49FA18BEB031AD0F929B
3	1			B353EBEE89E451E8DC727DEEE8E62230B31DA3C412D283FC870BD213FAFBF5DD
19	1			F1BCBAFC0D57311A2B378BADE60B0A63F5FE9FDB3080B391825A1F9243D61B58
20	1			078423E6BD6B3FD42F8331CD2DCDB4715F9AC388BEB2EA8C2E210CD755573575
21	2			1AC7B2D12CADD66B84D37A219EAEDB1B6E91966A5E31CBF99D82863E63C54158
22	2			1D46F3EAE2D007ABC4C73D956B3DFEB5C2F22482F7CED53F03B9142BBC071A53
120	2			0019F2E6CA6D807C8F05CC0AE3F7FD5998E0535008A1856CC33FFA685EEE06B0
69815	4			2A4E837151DB9C019FFC3F1017F99BC81EE4204C3FACAB8C0268ED169D3325F0
69816	4			7139E644610C99695442701C7E5DFDA74CE4A4BB2CCB7E2E7DE5CF1B9CFFC06C
69817	4			0000E095FFAAEC18CFE399D18A2E226E71378096D9132106EDD84370A06CDDA7

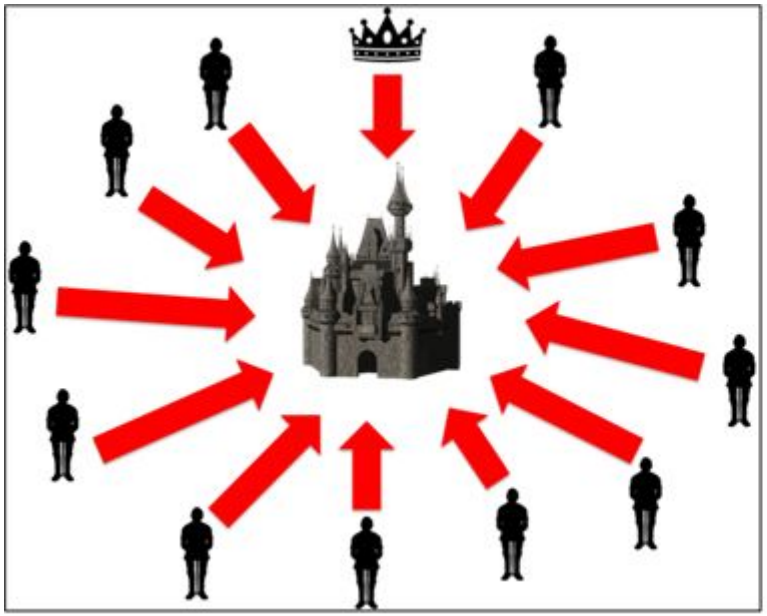
Сложность в наши дни и ее регуляция



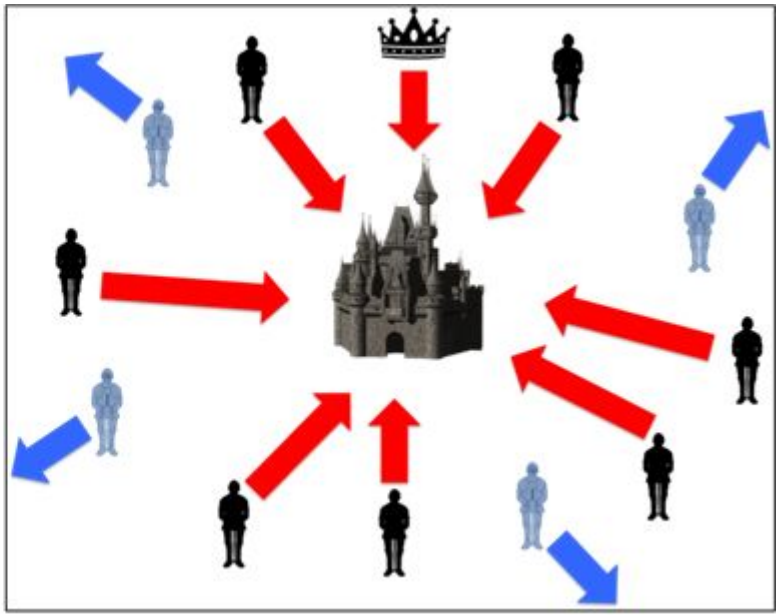


Зависимость сложности создания блока от времени (2016-2018 г.г.)
https://blockchain.info/

Алгоритм достижения консенсуса. Проблема Византийских генералов



Координированная атака
ПОБЕДА



Некоординированная атака
ПОРАЖЕНИЕ

Алгоритм достижения консенсуса. Proof-of-Work

Proof-of-Work — алгоритм защиты распределенных систем от угроз (DoS-атаки, спам-рассылки и т.д.), суть которого сводится к двум основным пунктам:

- необходимость выполнения определенной достаточно сложной и длительной задачи;
- возможность быстро и легко проверить результат.

C. Dwork, M. Naor «Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology», 1992

В **1997** году Адам Бэк запустил проект **Hashcash (**защита от спама). Задача формулировалась следующим образом: «Найти такое значение x, что хеш SHA(x) содержал бы N старших нулевых бит».

Цель – обеспечить способность узла сети проверить, что блок в цепи создан корректно. По сути – проверка вычисленного **Hash**

Алгоритм достижения консенсуса. Proof-of-Stake

Альтернатива – появилась в криптовалюте PPCoin (PeerCoin) в 2012 г.

Идея – использовать «долю» (stake) в качестве ресурса, который определяет, какой именно узел получает право создания следующего блока.

Поиск хеша аналогичен Proof-of-Work

- Сложность распределяется между узлами пропорционально их балансу
- Больше шансов создать следующий блок имеет узел с большим балансом

Итого:
- небольшие требования к вычислительным ресурсам
- не стоит вопрос «потраченных впустую» мощностей

Алгоритм достижения консенсуса. Proof-of-Stake

Плюсы:

- Для проведения атаки требуются значительные средства, что делает ее нецелесообразной с финансовой точки зрения
- Если в распоряжении атакующего имеется большое количество денег, он сам пострадает от атаки, поскольку это нарушит устойчивость криптовалюты.

Минусы (опасения):

- Дает дополнительную мотивацию к накоплению средств в одних руках, что может негативно сказаться на децентрализации сети.
- Если образуется небольшая группа, которая соберет у себя достаточно большие средства, она сможет навязывать свои правила работы сети остальным участникам.

И другие …

- Proof-of-Activity — гибридная схема, совмещающая PoW и PoS
- Proof-of-Burn — «сжигание» происходит путем отправки монет на такой адрес, с которого гарантированно нельзя их потратить
- Proof-of-Capacity — реализация популярной идеи «мегабайты как ресурсы»
- Proof-of-Storage – выделенное место используется всеми участниками как совместное облачное хранилище
- …

Модель	Производительность
Radeon RX Vega 56	36 MH/s
GeForce 1080 Ti	31 MH/s
Radeon R9 390X 8Gb	31 MH/s
GeForce GTX 1070 FE	27 MH/s
RX 480	24 MH/s

NVIDIA GeForce GTX 1080 Ti

AMD Radeon R9 390X 8Gb

ПО для майнера:
Bitcoin Mine, BTCMiner, CGMiner, BFGMiner, …

https://whattomine.com/coins/

http://jkcrypto.com/coin-to-mine-with-nvidia-gtx-1080-ti/

Форк в сети

Форк (англ. fork — ответвление) — использование исходного кода программного проекта в качестве старта для другого

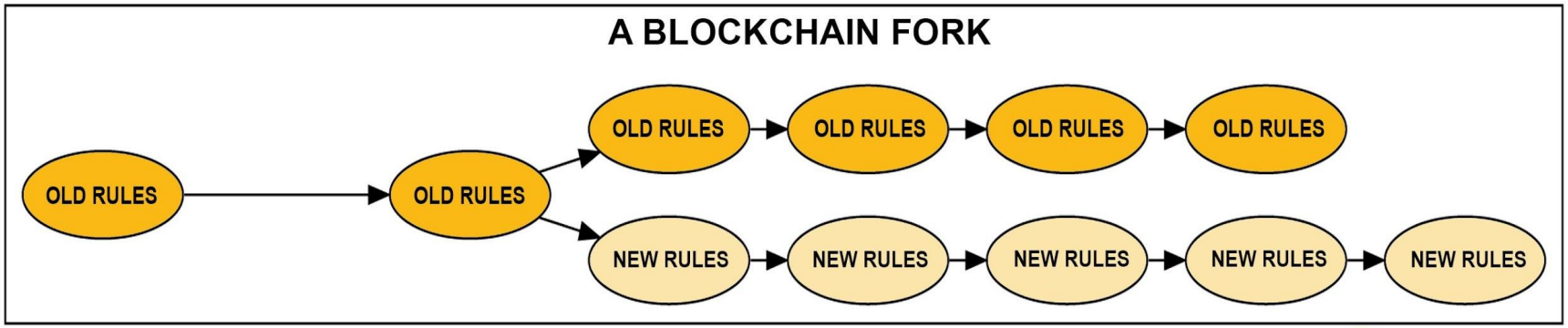
Цель

- увеличение размера блока
- увеличение пропускной способности
- снижение комиссии
- …

Приводит к появлению новых валют

Ethereum, Litecoin, Zcoin, …

На форке можно заработать!



Другие криптовалюты…

Валюта	Капитализация
Ethereum	$44 млрд
Bitcoin Cash	$23 млрд
IOTA	$11 млрд
Ripple	$9 млрд
Litecoin	$8 млрд
Dash	$6 млрд

https://www.rbc.ru/money/11/12/2017/5a212a1e9a79473b35558cb4

зарождение идеи Ethereum

Ethereum не только валюта!

Платформа для построения систем на основе блокчейна:

- уникальные сервисы
- прозрачны для проведения транзакций любого рода
- смарт-контракты
- пользователи сами могут создавать свою валюту
- гибкость платформы
- оперативное выполнение операций (20-30 секунд)
- высокая продуктивность майнинга

форк Ethereum,
появление Ethereum Classic

Ethereum vs Bitcoin

Bitcoin	Ethereum
Время генерации блока	
10 минут	15 секунд
Доход за блок	
↓ в 3 раза каждые 4 года	Неизменен
Майнинг	
Большие вычислительные ресурсы (нужен пул)	Можно добывать самостоятельно (пул не нужен)
Распределение средств	
Большая часть у создателей	Половина будет добыта через 5 лет
Код системы	
–	Математическая модель системы

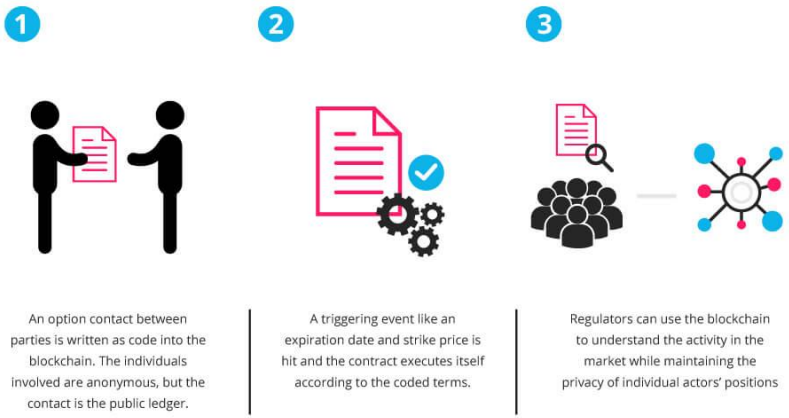
Смарт-контракт. Что это?

Смарт-контракт — компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн.

Смарт-контракты содержат:

- информацию об обязательствах сторон
- информацию о санкциях за их нарушение
- автоматически обеспечивают выполнение всех условий договора

Blockgeeks



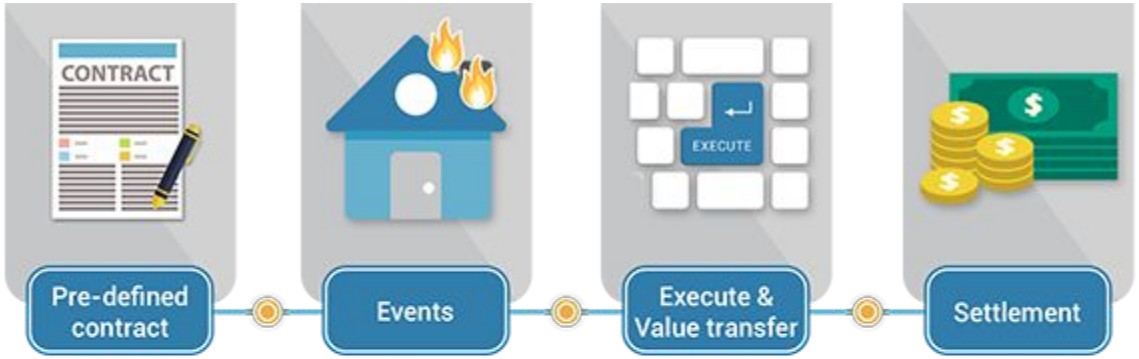
solidity

Смарт-контракт. Пример

1. Создается исполняемый фрагмент кода
2. Фрагмент кода подписывается приватным ключом
3. Подписанный фрагмент помещается в блок
4. У контракта появляется внешний адрес
5. Пользователь может обратиться по адресу к контракту и вызвать его метод
6. Контракт исполняется при соблюдении заложенных в него условий

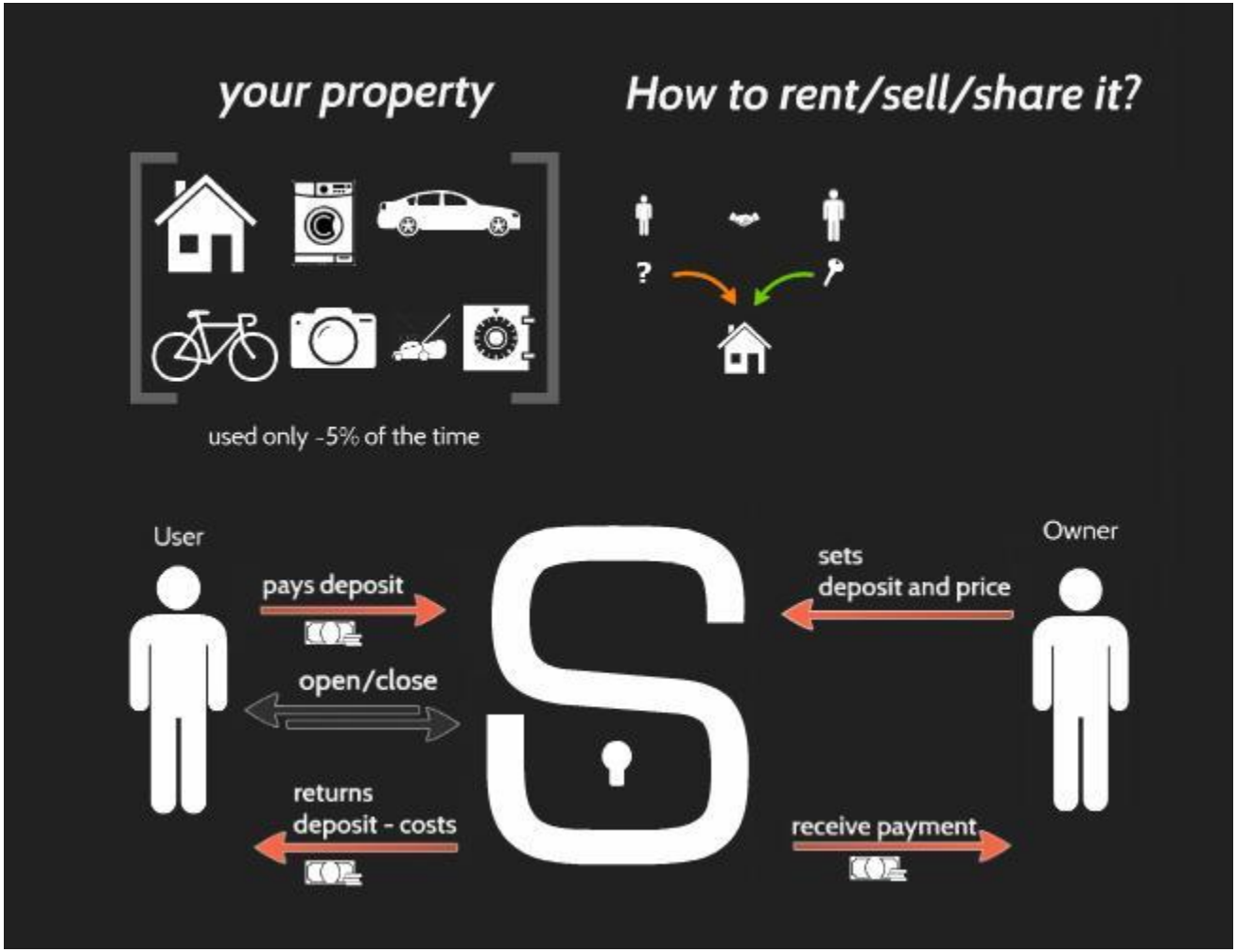
```
pragma solidity ^0.4.0;
contract Counter {
    int private count = 0;
    function incrementCounter() public {
        count += 1;
    }
    function decrementCounter() public {
        count -= 1;
    }
    function getCount() public constant returns
(int) {
        return count;
    }
}
```

Страхование



- Terms of the policy are agreed by all counterparties
- These are hard coded into the smart contract and cannot be chan-ged without all parties knowing
- Event triggers insurance policy execution
- The smart contract policy is automatically executed based on the pre-agreed terms
- Payout / other settlement completed instantly and efficiently

Операции с недвижимостью (slock.it)



Интернет вещей

Применение смарт-контрактов. Реалии

Блокчейн в России 02 февраля

«Газпром нефть» завершил пилот проект по испол блокчейн для Ин

Новая схема лучше подходит д централизованных технологий и небезопасным.

Минфин и Центроб положения законо финансовых актив

Законопроект был опублико как предпринимательскую д виды цифрового финансово электронной форме.

«Легенда о Сатоши Накамото»: криптографическая картина-головоломка разгадана спустя три года

НОВОСТИ 06.02.2018

Пожелавший остаться неизвестным программист расшифровал секретный код биткоин-кошелька, который криптограф Роб Майерс еще в 2015 году поместил в картину TORCHED H34R7S, впоследствии получившую название «Легенда о Сатоши Накамото». В качестве награды за свои усилия неназванный герой получил 4,87 BTC, пишет Motherboard.

YTI>
@coin_artist

The painting is a #puzzle, there is 4.87 #bitcoin concealed by this image. Happy #EasterEgg i.imgur.com/OSpEZtA.jpg

17:08 - 3 апр. 2015 г.

611 447 человек(а) говорят об этом

ный интеллект на менить мир

Earth Partners объявили о рименения искусственного интеллекта и партнерства является создание ной инфраструктуры. Об этом сообщает

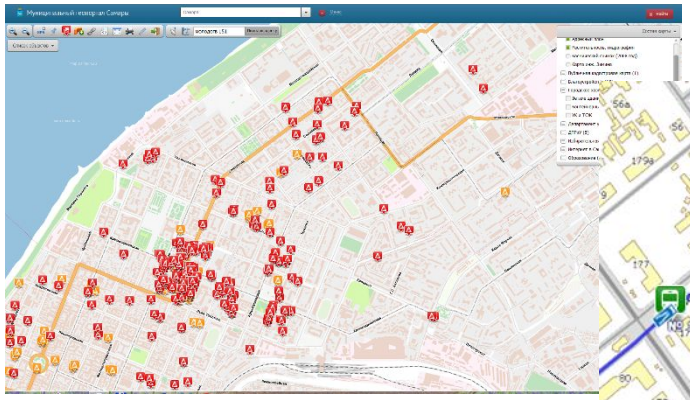
ва SingularityNET Дэвид Хэнсон.

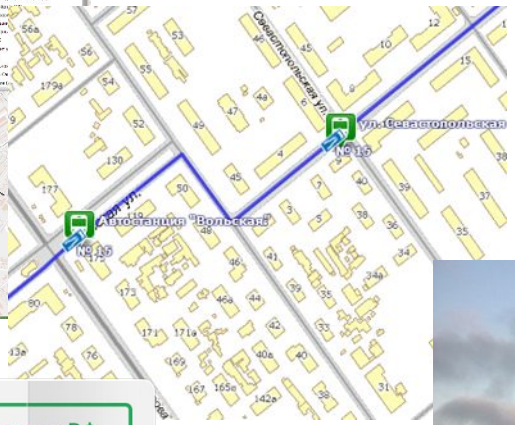
енением ии

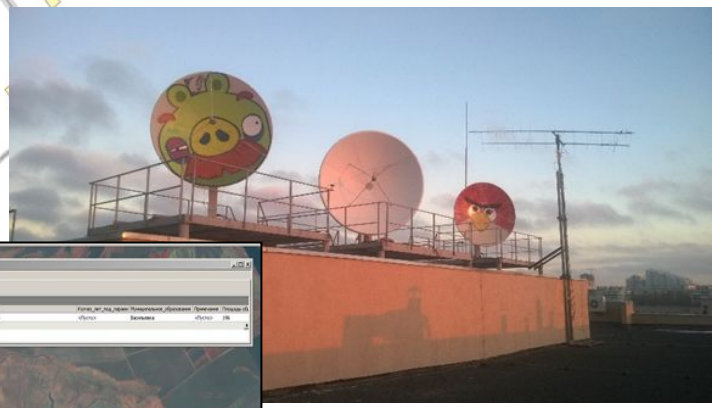
пищного кредитования (АИЖК) и строительстве жилья с компаний.

ым регионом реализации действии Росреестра и долевого строительства". Взнос езервирования и списания

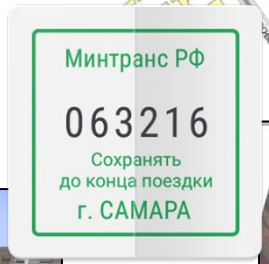
Кафедра геоинформатики и информационной безопасности Самарского университета

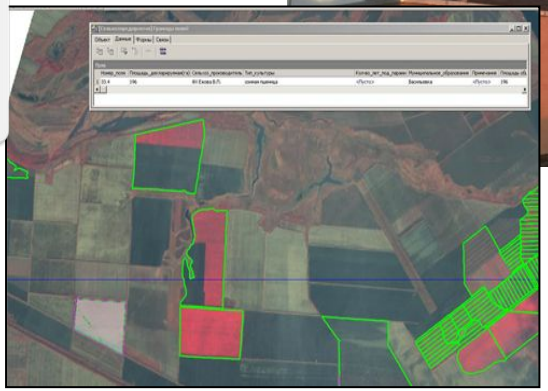






Volga CTF





САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

БЛАГОДАРЮ ЗА ВНИМАНИЕ

ул. Московское шоссе, д. 34, г. Самара, 443086
Тел.: +7 (846) 335-18-26 , факс: +7 (846) 335-18-36
Сайт: www.ssau.ru, e-mail: ssau@ssau.ru