

Блокчейн и криптовалюты

Что такое блокчейн?

Причины популярности криптовалют

Что происходит со стоимостью криптовалют?

Какие способы заработка существуют?

Что такое криптовалюта?

- Просто нули и единички?
- Денежный суррогат?
- Электронные ценные бумаги?
- Пирамида или пузырь?
- Способ совершения незаконных сделок?
- Активы, неподконтрольные государству?

Что такое криптовалюта?

Распределенный журнал записей о том, кто кому дал сколько «монеток»



Как это работает? Биткоин-транзакции

Он-лайн магазин Боба, принимает криптовалюту в качестве оплаты. У Алисы есть биткоины и она хочет оплатить ими покупку в этом магазине.

КОШЕЛЬКИ И АДРЕСА

На компьютерах Алисы и Боба установлены биткоин-кошельки

Кошельки реализуют доступ к множеству биткоин-адресов

СОЗДАНИЕ НОВОГО АДРЕСА

Каждому адресу соответствует свой баланс биткоинов

Адрес - это строка, состоящая из букв и цифр, например
14zdTEDmFQZ
ZRQcWz1K5GTc
hcT6HmKFKD

ПОДТВЕРЖДЕНИЕ ПЛАТЕЖА

Криптосистема с открытым ключом

Когда Боб создает новый адрес, фактически он создает пару криптографических ключей. Новый биткоин-адрес Боба представляет собой уникальный открытый ключ, а соответствующий ему закрытый ключ сохраняется в файле кошелька. Открытый ключ позволяет кому угодно убедиться в том, что сообщение, подписанное закрытым ключем Боба достоверно и действительно принадлежит Бобу.

С помощью Биткоин-клиента Алиса переводит деньги за покупку на адрес Боба

ЗАКРЫТЫЙ КЛЮЧ

Кошелек Алисы содержит закрытые ключи для каждого из ее адресов. Биткоин-клиент подписывает новую транзакцию закрытым ключом того адреса, с которого Алиса передает монеты

ОТКРЫТЫЙ КЛЮЧ

Любой пользователь сети может с помощью открытого ключа, которым является адрес отправителя, проверить подлинность транзакции.

И хотя Биткоин-адрес удобно представлять себе как банковский счет, он работает немного по-другому. Пользователи могут создавать сколько угодно таких адресов. Вообще, для сохранения анонимности рекомендуется создавать новый адрес для каждой транзакции.

ПРОВЕРКА ТРАНЗАКЦИИ

Гарри, Гарт и Гленн занимаются Биткоин-майнингом

Их компьютеры собирают транзакции в "блок транзакций"

Компьютеры майнеров вычисляют криптографическую хэш-функцию

Хэширование

Хэширование - это преобразование набора данных в строку из букв и цифр фиксированной длины. Результат таких преобразований называют хэш-суммой или хэшем. Любое изменение исходных данных изменяет их хэш. Практически невозможно предсказать, какие нужны исходные данные для создания специфического хэша

Майнеры вычисляют новые хэши, основанные на комбинации предыдущего хэша, нового блока транзакций и случайного кода

Хэш-сумма + Соль = Новый хэш

Корень всего зла ???

Вычисление хэшей не является сложным процессом, но есть условие - хэш блока должен содержать заданное число нулей в начале.

Корень всего зла → 0000 0000 0000 ...

Соль

Для создания разных хэшей из одних и тех же данных используется "Соль" (Nonce). Соль - это произвольное число, которое добавляется к данным перед хэшированием. Изменение этого числа приводит к кардинальному изменению хэш-суммы

Майнеры не знают, какая "соль" даст хэш, удовлетворяющий условию.

Поэтому они генерируют множество хэшей, используя разные значения "соли", пока случайно не появится подходящий хэш.

| | | |
|------------------|---|-------------------|
| Корень всего зла | → | 6d0a 1899 086a... |
| Корень всего зла | → | 4b6c 6be4 6dde... |
| Корень всего зло | → | b8db 7ee9 8392... |

Самая первая транзакция в блоке называется coinbase-транзакция. Она не имеет входов и зачисляет майнеру, нашедшему подходящий хэш, вознаграждение в 25 монет за создание данного блока.

ТРАНЗАКЦИЯ ПОДТВЕРЖДЕНА

Каждый блок, в том числе и тот, который хранит транзакцию от Алисы к Бобу, содержит заголовок и список транзакций. В заголовке есть хэш предыдущего блока. Со временем появится новый блок, в котором будет хэш блока с транзакцией Алиса-Боб. Поэтому модифицировать данные транзакции невозможно.

Экспертные комментарии в статье подготовил Сергей Гурасов

Что в блоках?

<https://blockchaindemo.io/>



Преимущества блокчейна

- Прозрачность
- Децентрализованность
- Анонимность
- Равноправие
- Безопасность



Лицо блокчейна — Bitcoin



Роли в системе Bitcoin



Майнеры создают Биткоины, используя компьютеры для решения математических функций. Этот же процесс также подтверждает предыдущие транзакции в системе.



Обмен Биткоином позволяет производить торги с традиционными валютами, давая «не-майнерам» путь на рынок, а также как способ обналичить Биткоин



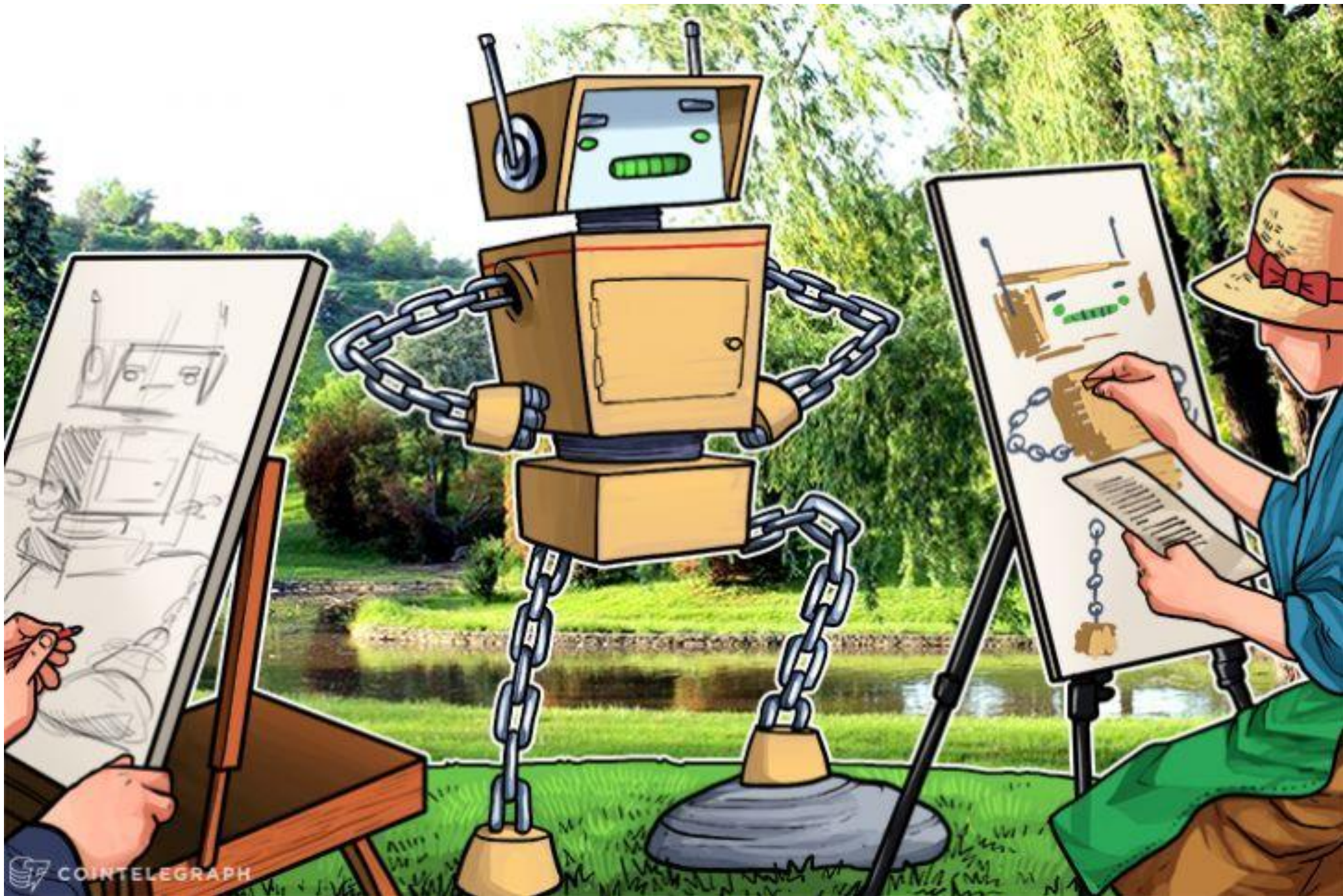
Пользователь скачивает Биткоин кошелек, работа которого немного напоминает e-mail адрес, обеспечивающий возможность хранить и принимать электронные деньги. Биткоины можно отправлять от одного кошелька к другому, используя браузер или мобильное приложение.

Создание кошелька для бизнеса не отличается от создания кошелька обычного пользователя, кроме возможности использовать кнопку оплаты Биткоинами на сайте. Для упрощения и ускорения оплаты клиентами, могут использоваться QR-коды



АЛТКОИНЫ





Борьба с банковской системой



Ethereum и умные контракты

Ethereum («Эфириум»)

Платформа для создания **децентрализованных** онлайн-сервисов на базе **блокчейна** работающих при помощи **умных контрактов**.



Виталик
Бутерин



Smart Contract

Умный контракт — электронный алгоритм, описывающий набор условий, выполнение которых влечет за собой некоторые события в реальном мире или цифровых системах.

Для реализации умных контрактов требуется **децентрализованная среда**, полностью исключая человеческий фактор, а для возможности использования в умном контракте передачи стоимости требуется **криптовалюта**.

Smart Contract

1



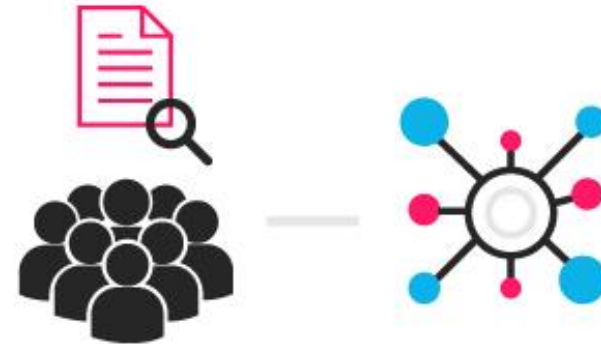
An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is the public ledger.

2



A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3

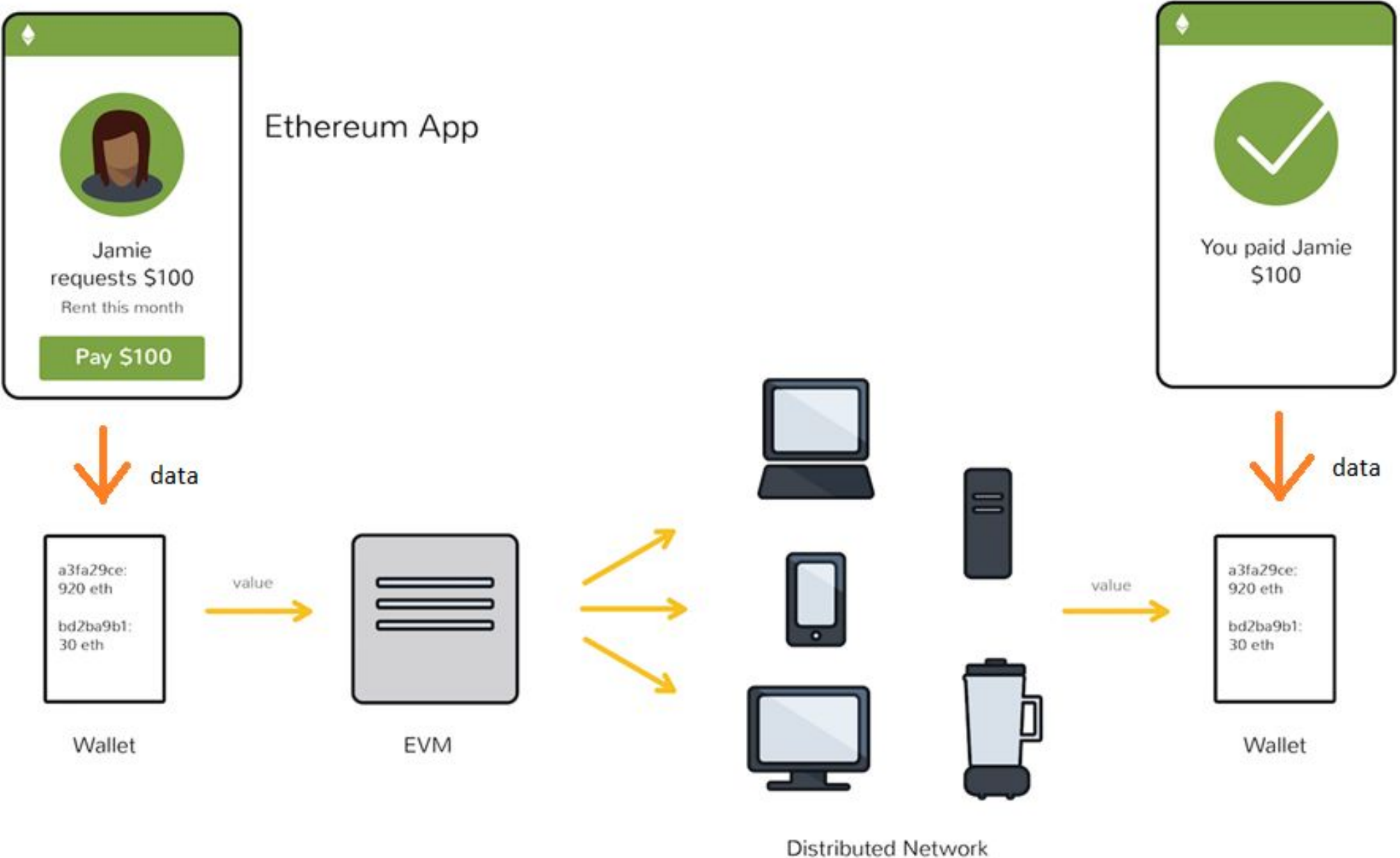


Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

Децентрализованная среда — EVM

Виртуальная машина Ethereum (Ethereum Virtual Machine) имеет своей целью **обеспечение безопасности (неизменности и неотвратимости) операций и выполнении кода компьютерами по всему миру.**

Децентрализованная среда — EVM



Не просто криптовалюта, но «криптотопливо»

Ether — внутренняя валюта и топливо Ethereum.

Поскольку контракт выполняется на тысячах «Полных узлов» (Full Nodes) Ethereum — **вычисления (выполнение команд контракта) стоят денег**. Если вы не снабдите ваш код небольшим количеством эфира — EVM не будет работать на вас. Это количество можно назвать «стоимостью сделки» на платформе Ethereum. Средней сложности новый контракт обойдется менее чем в 0.05 эфира (примерно \$15).

Что всё это значит для
программиста?

Давайте взглянем на контракт «СМЕРТНОГО»

```
contract mortal {  
    /* Define variable owner of the type address*/  
    address owner;  
  
    /* this function is executed at initialization and sets the owner of  
function mortal() { owner = msg.sender; }  
  
    /* Function to recover the funds on the contract */  
function kill() { if (msg.sender == owner) selfdestruct(owner); }  
}
```

Контракт «смертного, который умеет приветствовать»

```
contract greeter is mortal {  
    /* define variable greeting of the type string */  
    string greeting;  
  
    /* this runs when the contract is executed */  
    function greeter(string _greeting) public {  
        greeting = _greeting;  
    }  
  
    /* main function */  
    function greet() constant returns (string) {  
        return greeting;  
    }  
}
```

**место юриста,
составляющего контракт
для обеспечения условий
сделки**

А в будущем:

| | | |
|------------|------------------|------------|
| вахтера | сотрудника банка | модератора |
| коллектора | сотрудника биржи | надзорника |
| клерка ЖКХ | чиновника | избиркома |
| пристава | | ... |

С чего начать, если хочешь программировать на Solidity?

- Читайте примеры умных контрактов;
- Выберите фреймворк разработки (Truffle, OpenZeppelin, Solium);
- Выберите среду для написания кода (VS Code, Remix, IntelliJ IDEA);
- Выберите приложение-провайдер для взаимодействия с блокчейном (geth, Parity, Metamask);
- Используйте тестовые блокчейны с бесплатной инфраструктурой (testRPC, Ropstan) для тестирования ваших контрактов;
- Приготовьтесь к сложностям, которые свойственны молодым

С чего начать знакомство с умными контрактами?

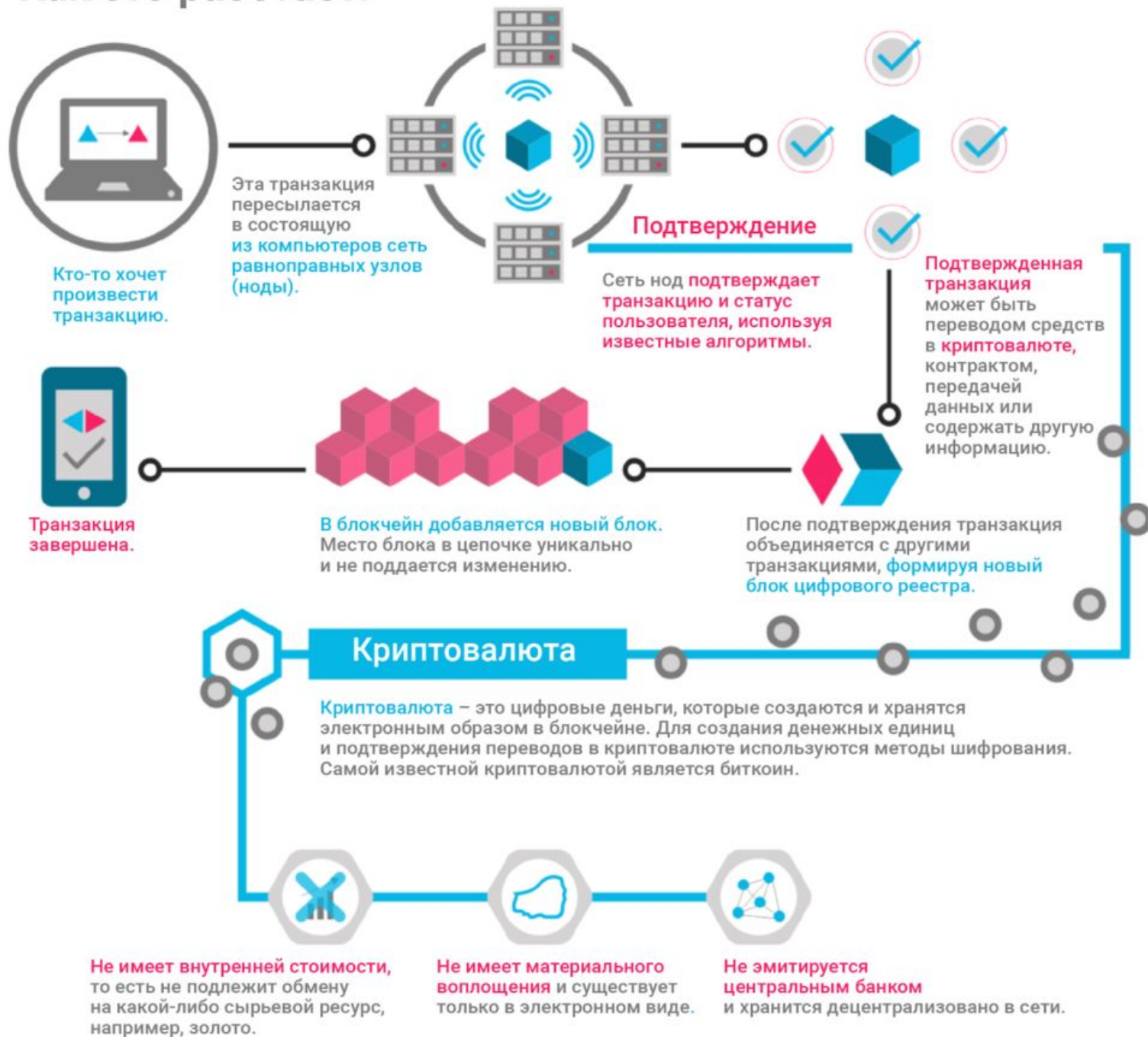
- <https://www.ethereum.org/greeter>
- <http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html>
- <http://solidity.readthedocs.io/en/develop/solidity-by-example.html>

Спасибо за внимание!

<http://nlo-mir.ru/tech/52864-kak-ustroen-blokchejn.html>

Backup slides

Как это работает:



Какие способы заработка существуют?

- Майнинг
- Инвестиции в криптовалюты
- Инвестиции в блокчейн-проекты (ICO)
- Торговля на рынке криптовалют
- Участие в блокчейн-проектах

Майнинг

Создание узла-участника сети, генерирующего новые блоки в цепочке. Фактически такие узлы обеспечивают децентрализованную инфраструктуру, за что и получают вознаграждение.



Майнинг



Инвестиции в криптовалюты



Что происходит со стоимостью криптовалют?

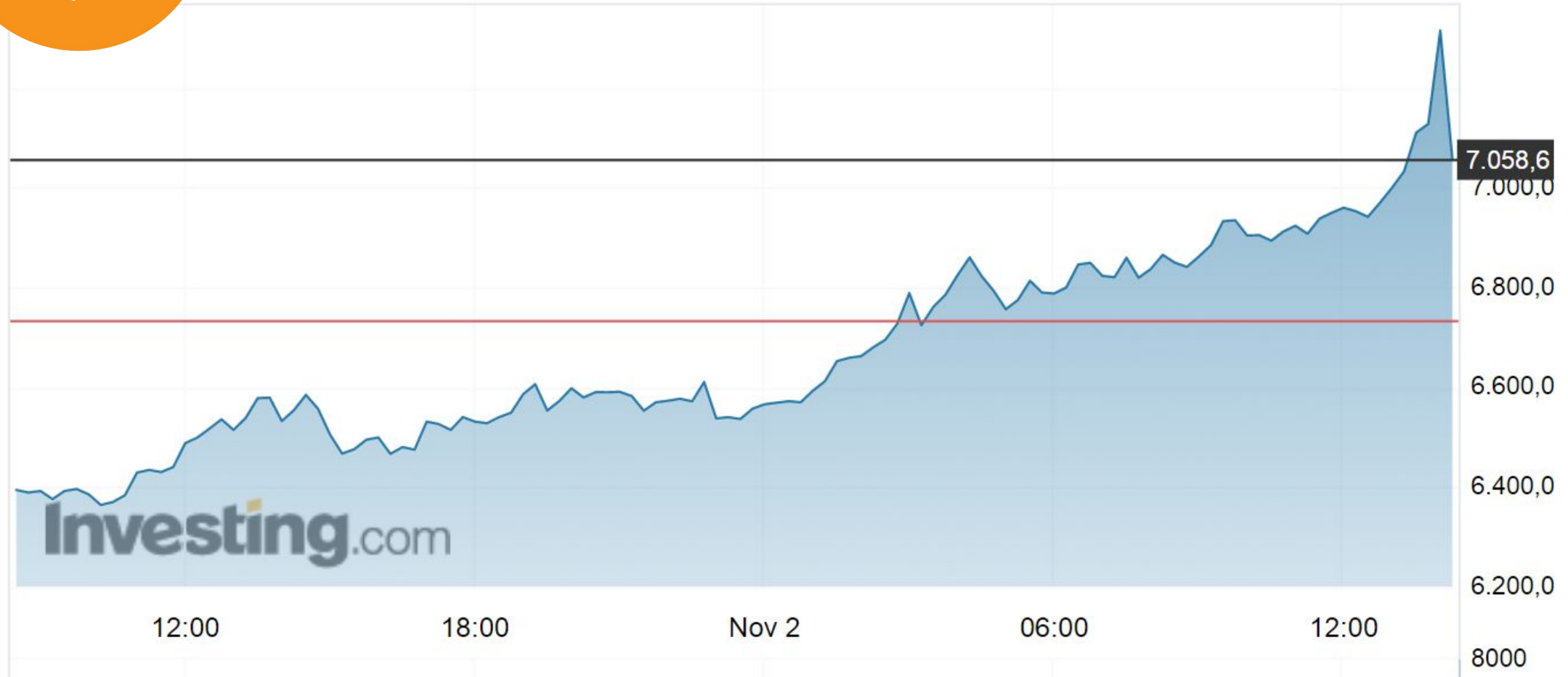


x 10000 =





Что происходит со стоимостью криптовалют?

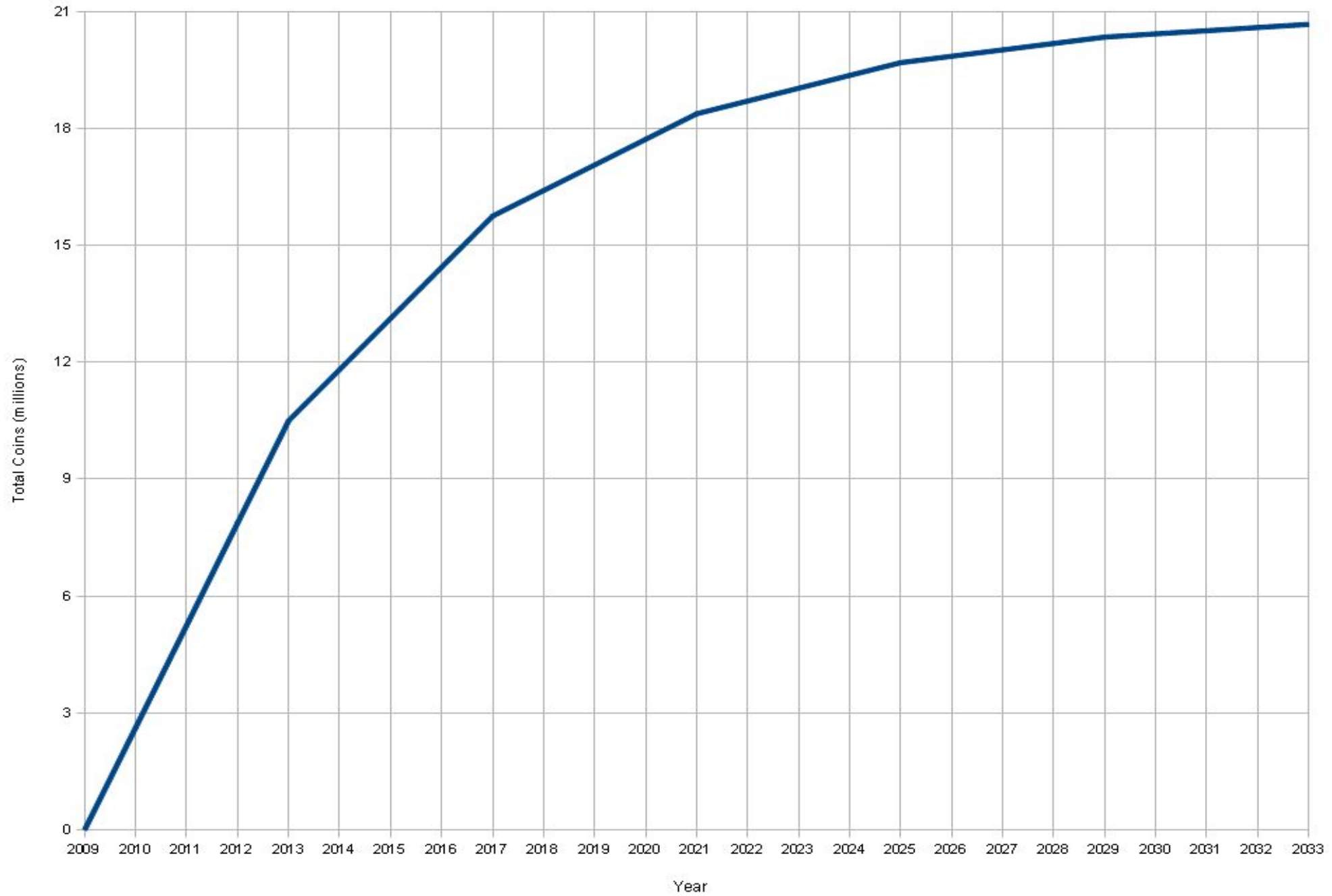




А за год?



Total Bitcoins over time



Инвестиции в блокчейн-проекты (ICO)



Что такое ICO?

- Предложение изначального капитала
- Новый вид крауд-фандинга
- Способ инвестировать в стартапы
- Новая «монета», которая может выстрелить или не выстрелить



Законно или незаконно?

В России статус пока не определен.

- Майнить можно
- Принимать в качестве платы за услуги нельзя
- Покупать можно
- Обменивать... не стоит

К концу года обещан регулирующий законопроект



Как войти на рынок?

- Нужно понять, что такое и как работает блокчейн, майнинг, альткоины, ICO и решить, верите ли вы, что эти технологии перспективны;
- Вход не менее \$1000;
- Не следует рисковать более чем 10% своих сбережений;
- Если вы хотите майнить — подробно изучите технологические вопросы;
- Если вы хотите инвестировать — тщательно выбирайте способ покупки, технологию и личный кошелёк;
- Если вы хотите торговать — тщательно выбирайте биржу и пару.