BLOCK CHAIN РЕВОЛЮЦИЯ

ДОКЛАДЧИК: РУСЛАН АХМЕРОВ

СЕНТЯБРЬ 2017

СОДЕРЖАНИЕ

ЧАСТЬ I
ИСТОРИЯ

ЗАДАЧА ВИЗАНТИЙСКИХ ГЕНЕРАЛОВ

Византия. Ночь перед великим сражением с противником. Византийская армия состоит из ***n*** легионов, каждым из которых командует свой генерал. Также, у армии есть главнокомандующий, которому подчиняются генералы.

В то же самое время, империя находится в упадке, и любой из генералов и даже главнокомандующий могут быть предателями Византии, заинтересованными в её поражении.

Ночью каждый из генералов получает от предводителя приказ о варианте действий в 10 часов утра (время одинаковое для всех и известно заранее), а именно: «атаковать противника» или «отступать».

Если все они отдадут приказ о нападении, то город падет (**благоприятный исход**); согласованное отступление считается условно **нейтральным исходом**. **Наихудший исход** – при котором какая-то часть армий атакует город, а какая-то отступит

Принять общее решение они могут лишь обмениваясь сообщениями друг с другом через вестовых.

Как организовать систему коммуникаций, чтобы военачальники **всегда** приходили к согласию, тем самым синхронно атаковав или отступав, не взирая на попытки предателей сорвать все планы?

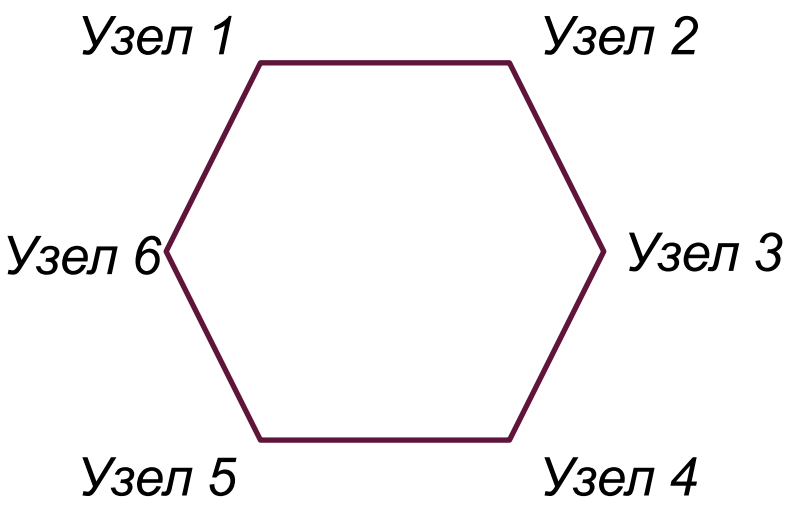
РЕТРОСПЕКТИВА БЛОКЧЕНА

- 1982 – опубликовано математически строгое решение задачи о византийских генералах
- 1989 – Дэвид Чаум создает концепт «неоспоримой подписи» (undeniable signature), основанный на использовании криптографических методов для решения проблемы двойной траты;
- 2005 – Ник Сабо описывает систему BitGold, комбинирующую криптографические методы и архитектуру распределенных баз данных;
- 2008 – под коллективным псевдонимом Сатоши Накамото опубликована и детально описана система Bitcoin;
- 2009 – появление первого биткоина;
- 2011 – зафиксирован паритет BTC и USD; появляется первая альтернативная криптовалюта Litecoin;
- 2013 – цена BTC сравнялась с ценой унции золота;
- 2014 – оборот сети Биткоин превысил оборот Western Union;
- 2017 – Стоимость Биткоина превышает **$5 тыс.** (BTC+BCC)

ЧАСТЬ II
МЕХАНИЗМ

РАСПРЕДЕЛЕННЫЙ РЕЕСТР

В основе блокчейна лежит технология **распределенного реестра.**



Каждый узел:

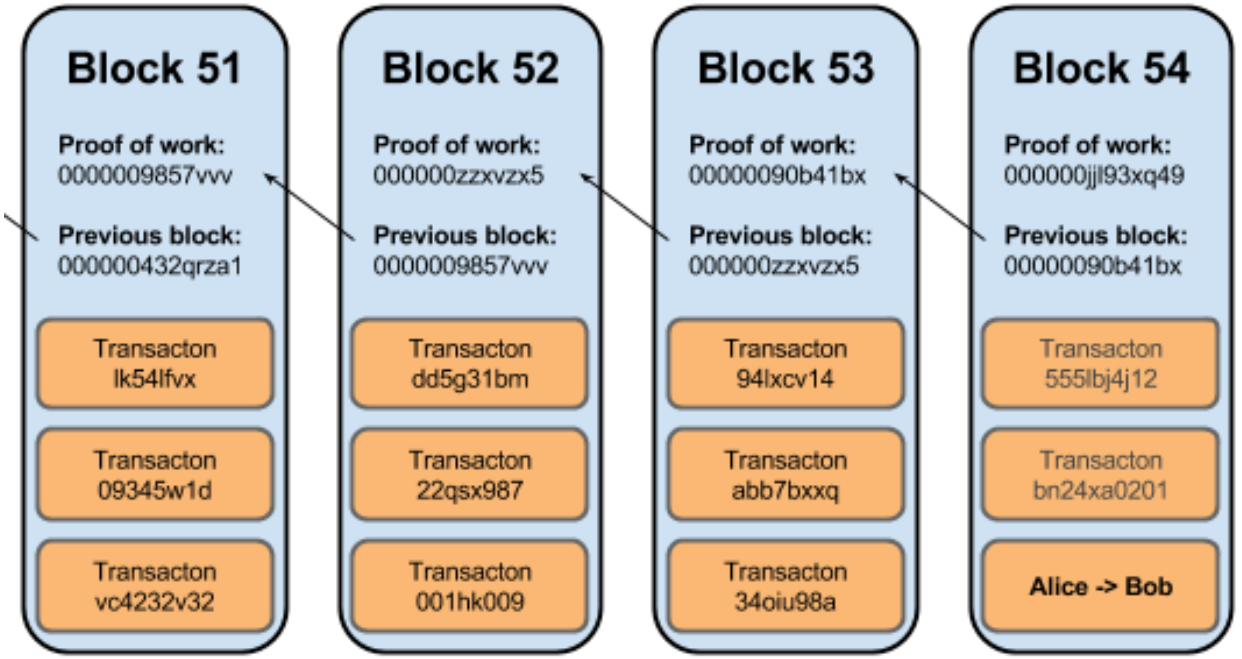
1. Имеет копию всех данных реестра
2. Использует одну и ту же хэш-функцию, чтобы верифицировать данные, полученные от других узлов
3. Независим от других

ВЕРИФИКАЦИЯ ДАННЫХ И КОНСЕНСУС

Все данные, вносимые в реестр, постоянно верифицируются на предмет фальсификации

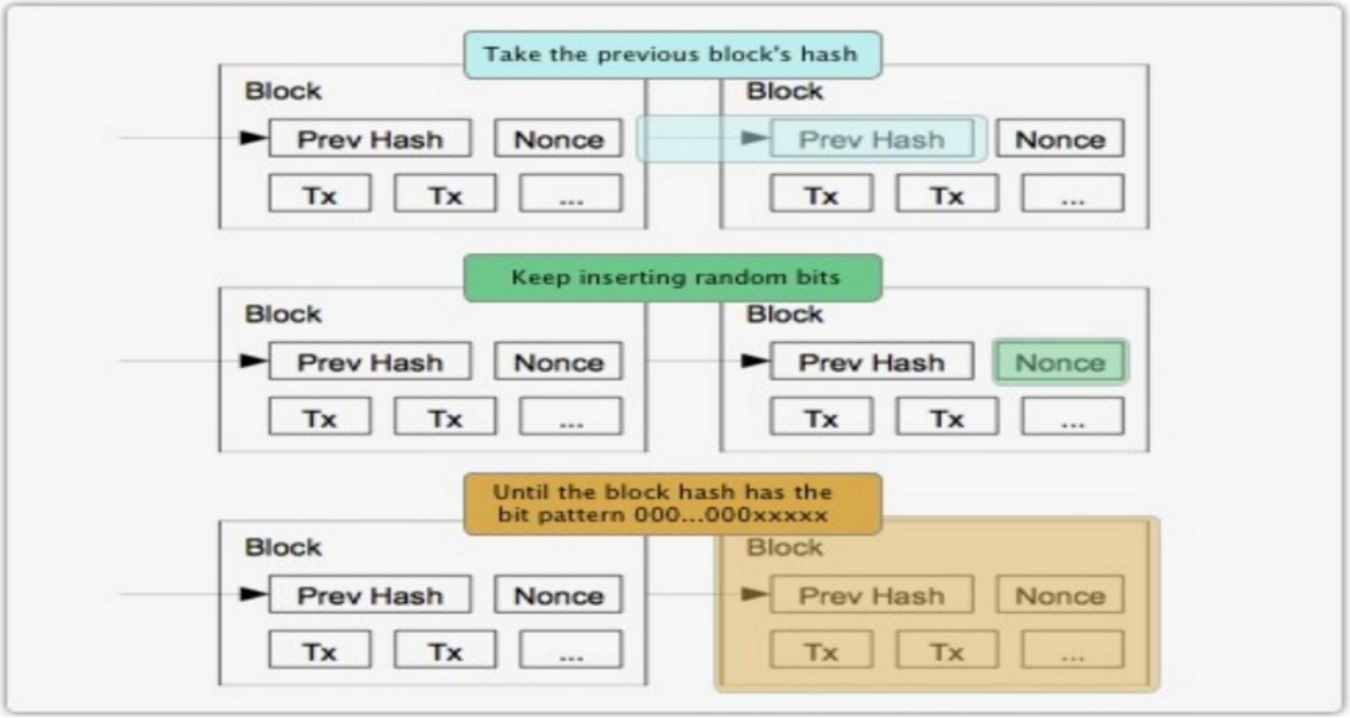
Достижение консенсуса (согласия) навсегда запечатывает данные внутри блока, который становится последним блоком в блокчейне

Каждый блок хранит информацию о предыдущем блоке, хэш каждой строки данных (транзакции) в блоке, а также доказательство работы (proof of work)



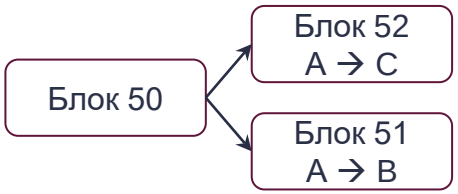
ТРАНЗАКЦИОННЫЙ МЕХАНИЗМ: ПРИМЕР БИТКОИНА

- Биткоин использует proof of work алгоритм для верификации транзакций, собранных в один блок
- Proof of work – информация, произведенная с затратой компутационных ресурсов и удовлетворяющая определенным условиям
- Задача proof of work алгоритма биткоина – найти такое число x, чтобы его хэш-функция, вкупе с рядом других параметров (точка старта, системная строка и пр.) была равна 0

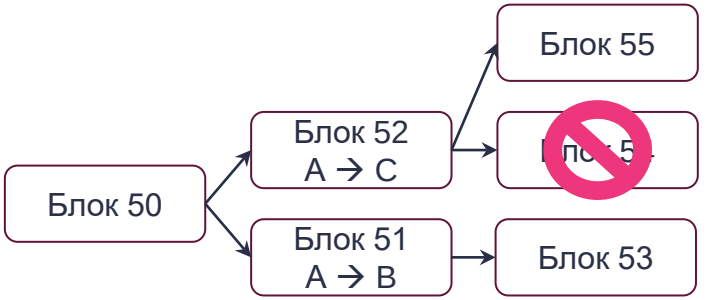


ФОРМИРОВАНИЕ БЛОКЧЕЙНА

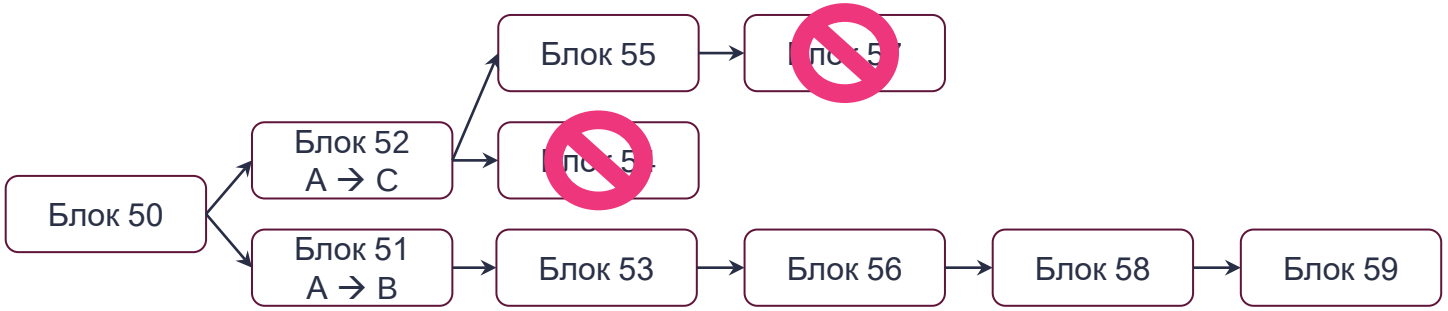
Создание блока – случайный процесс, могут возникать форки



Правильная цепочка – самая длинная



Вероятность форка экспоненциально уменьшается с длиной

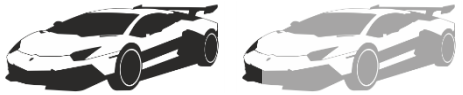


ЧАСТЬ III
БЛОКЧЕЙН СЕГОДНЯ

ИНВЕСТИРОВАТЬ В КРИПТОВАЛЮТЫ НУЖНО ВЧЕРА

Вы уже упустили: **$100, вложенных на ICO стоят:**

NXT **+364345%** **$364,4 тыс.**

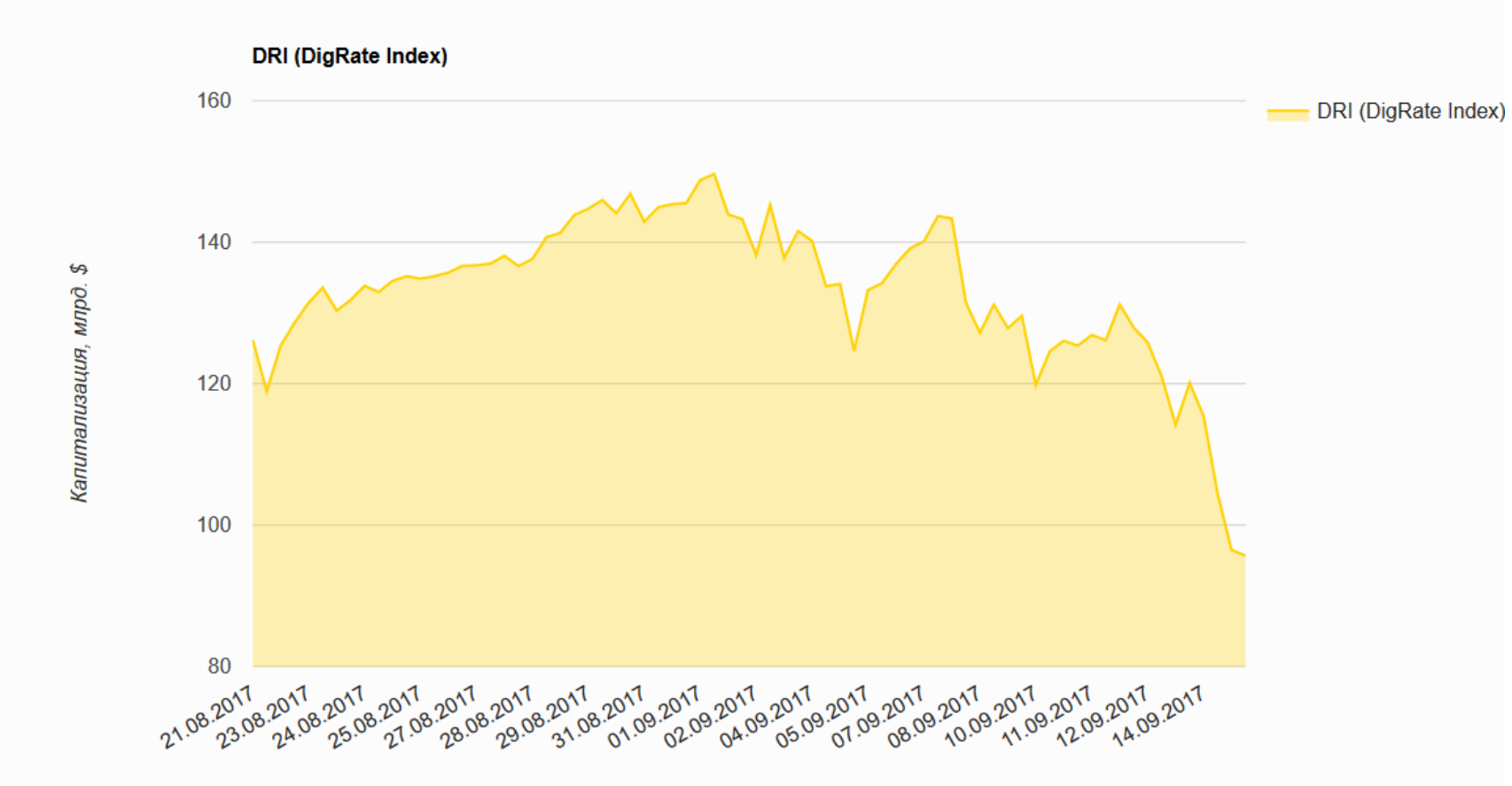


IOTA **+110541%** **$110,6 тыс.**

Ethereum **+78238%** **$78,3 тыс.**

КАПИТАЛИЗАЦИЯ ВСЕХ КРИПТОВАЛЮТ

$95,94 млрд*



*** Это ВВП Анголы, 72% ВВП Казахстана и 7,5% ВВП Росси**

Источник: DigRate

КАПИТАЛИЗАЦИЯ ОТДЕЛЬНЫХ КРИПТОВАЛЮТ

Топ 10 валют по капитализации

#	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	$57,933,924,197	$3496.81
2	Ethereum	ETH	$22,531,104,528	$238.09
3	Bitcoin Cash	BCH	$6,785,649,832	$409.20
4	Ripple	XRP	$6,642,227,042	$0.173228
5	Litecoin	LTC	$2,486,908,443	$46.97
6	Dash	DASH	$1,982,823,250	$262.31
7	NEM	XEM	$1,794,249,000	$0.199361
8	Monero	XMR	$1,374,911,591	$91.14
9	IOTA	MIOTA	$1,301,223,204	$0.468145
10	OmiseGO	OMG	$936,482,982	$9.53

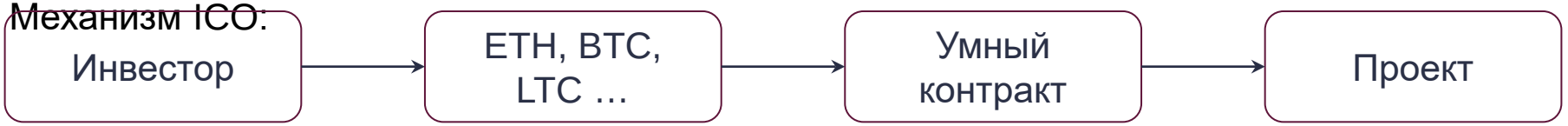
Интересные факты

- На coinmarketcap.com сейчас более 1100 криптовалют и токенов
- В свои лучшие времена *(сегодня явно не его день)* биткоин имел капитализацию более $80 млрд, в то время как глобальная капитализация криптовалют достигла более $145 млрд
- Наименьшая известная капитализация - $130 у Xenixcoin *(не знаю, что за фигня)*
- Официально самый бесполезный токен – UET (Useless Ethereum Token), в пике достигал капитализации $240 тыс., при этом не предлагая вообще ничего своим инвесторам

Источник: Coinmarketcap.com

ICO КАК НОВЫЙ ФЕНОМЕН В ФИНАНСИРОВАНИИ СТАРТАПОВ

- ICO – initial coin offering (как IPO, только размещение не акций, а токенов)
- Не требует вовлечения банков, регистрации где-либо, не имеет требований к продукту, бизнес-модели итд.
- Основные параметры проекта, выходящего на ICO:
  - Наличие идеи (редко – работающего прототипа);
  - Наличие Whitepaper – документа, объясняющего перспективы рынка, продукта, проекта;
  - Наличие команды, иногда внешних советников;
  - ~~Наличие бизнес-плана;~~
  - БОЛЬШЕ НИЧЕГО НЕТ! ЭТИ СУМАСШЕДШИЕ ИНВЕСТОРЫ ИНВЕСТИРУЮТ ВО ВСЕ ПОДРЯД!
- Механизм ICO:



УМНЫЕ КОНТРАКТЫ (1/3)

- **Умный контракт** (или smart contract) – алгоритм, созданный для конкретной задачи, целью которой является заключение и исполнение контрактов в блокчейне
- История создания:
  - Первая идея была предложения Ником Сабо в 1994 году, однако практические реализации стали возможны только после появления блокчейна в 2008 году;
  - Первые принципы были заложены в протоколе биткоина, однако в клиентском ПО они так и не были реализованы, не обладали полнотой по Тьюрингу, и вообще на практике не использовались;
  - Далее начали появляться идеи создания протоколов более высокого уровня (включая полноценные смарт-контракты) поверх протокола биткоина, по аналогии с тем, как поверх TCP/IP также используется ряд протоколов;
  - В 2013 году создатель журнала Bitcoin Magazine Виталик Бутерин пришел к выводу, что биткоин слишком глупый для умных контрактов, и решил создать свой протокол ~~с блэкджеком и шлюхами~~ – Ethereum. который бы стал полноценно совместимым с использованием умных контрактов
- **Основной принцип**: код есть закон (code is law)

УМНЫЕ КОНТРАКТЫ (2/3)

- **Пример работы контракта:**

1. Участник 1 хочет купить дом у участника 2;
2. Они заключают умный контракт;
3. Участник 1 посылает нужную сумму в умный контракт
4. Участник 2 передает права на дом в умный контракт
5. Умный контракт автоматически передает участнику 2 деньги, а участнику 1 права на дом

УМНЫЕ КОНТРАКТЫ (3/4)

Ethereum блокчейн:

- State - Состояние системы в заданный момент времени
- На ноутбуке State меняется с каждым тактом процессора
- В EVM - с каждой добавленной в блок транзакцией

Аналогии

- Ethereum Virtual Machine - компьютер
- Смарт-контракт - программа, которую можно запустить с определенными параметрами
- Адрес контракта - местонахождение программы
- Тогда транзакция к контракту является командой вида “Запустить программу лежащую по адресу X с параметрами p_1, p_2, …, p_n”

Майнинг:

- Взять последний блок, State которого считать валидным
- Запустить EVM, используя этот State
- Взять из пула неподтвержденных транзакций, исполнить их в EVM и сохранить новый State
- Подобрать nonce, чтобы хеш блока удовлетворял условию сети
- Отправить блок в сеть

Аналогии

- Убедиться, что родитель нового блока является самым новым блоком в цепи
- Убедиться, что хеш блока удовлетворяет требованиям сети
- Запустить EVM из состояния последнего блока и убедиться, что исполнение транзакций из нового блока приводит к корректному состоянию
- Добавить блок в цепь

Источник: Алексей Башлыков, Сооснователь EtherionLab

УМНЫЕ КОНТРАКТЫ (4/4)

```
pragma solidity ^0.4.0;

contract Coin {
    // The keyword "public" makes those variables
    // readable from outside.
    address public minter;
    mapping (address => uint) public balances;

    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        Sent(msg.sender, receiver, amount);
    }
}
```

Solidity:

- Тьюринг-полный
- Статически типизированный
- Похож на JavaScript

Простейший алгоритм выпуска новой криптовалюты на Solidity*

** я в нем ничего не понимаю*

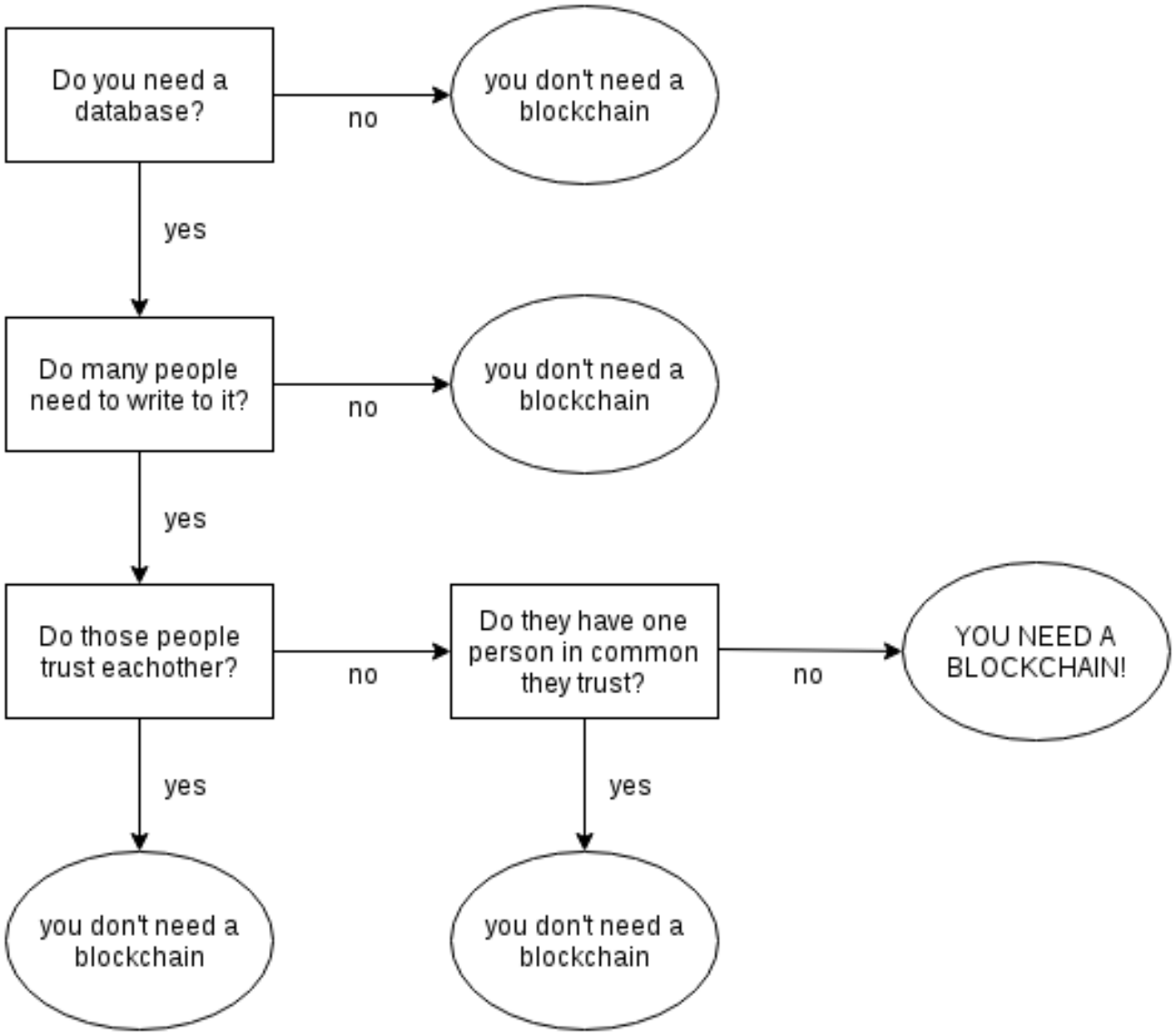
ЧАСТЬ IV

БУДУЩЕЕ БЛОКЧЕЙН

ПРИМЕНЕНИЕ БЛОКЧЕЙН

- Исключить «человеческий фактор» при взаимодействии участников системы
- Устранить недоверие между участниками взаимодействия
- Обеспечить автоматическое выполнение описанных в смарт контракте обязательств каждого участника взаимодействия (code is law)
- Исключить возможность централизации

НУЖЕН ЛИ ВАМ БЛОКЧЕЙН?



ЧТО ЖЕ БУДЕТ ДАЛЬШЕ?

Никто не знает, что будет завтра! Не слушайте никого, кто вам говорит, что знает! А теперь я вам скажу:

- Криптовалюты продолжат расти в количестве, стоимости и разнообразности применений
- ICO останется
- Укрепится множество разных механизмов валидации и функционирования блокчейна: proof of stake, proof of burn и пр.
- Развитие «полезного» майнинга
- Применение блокчейна без создания криптовалют в различных проектах -