Технические основы блокчейн-технологий и криптовалют

Всеволод Пелипас

ООО «СоларЛаб»

Кафедра ИС ИИТиУТС СевГУ

План

- Что такое блокчейн и зачем он нужен?
- Как это работает:
  - Основы криптографии
    - Хеш-функции
    - Асимметричная криптография
    - Цифровые подписи
  - Блоки и цепочки блоков
- Платформы:
  - Bitcoin и его сайдчейны
  - Ethereum
    - Global Computer, DApp и Smart Contract'ы
  - Пару слов о том, что в этой области делаем вы в СоларЛаб

Что такое блокчейн?

Земельные реестры

Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury

Проверка дипломов и сертификатов учебных заведений

Holberton School to Authenticate Its Academic Certificates With the Bitcoin Blockchain

The New Software Engineering School Now the World's First School to Deliver Secure Academic Certificates Within the Bitcoin Blockchain

Голосование

Blocktchain Technologies Corp. To Bring Blockchain Voting to New York Libertarian Party

Биржевая торговля

Nasdaq shares hands-on experience of capital markets and blockchains

Здраво-охранение

Blockchain Provider Gem Pursues Expansion Into Health Care Sector

Microsoft

Страхование

Lloyd's Sees Blockchain's Potential For Insurance Markets

Прогнозы

Augur Bets on Bright Future for Blockchain Prediction Markets

Защита от кибератак

Что такое блокчейн?

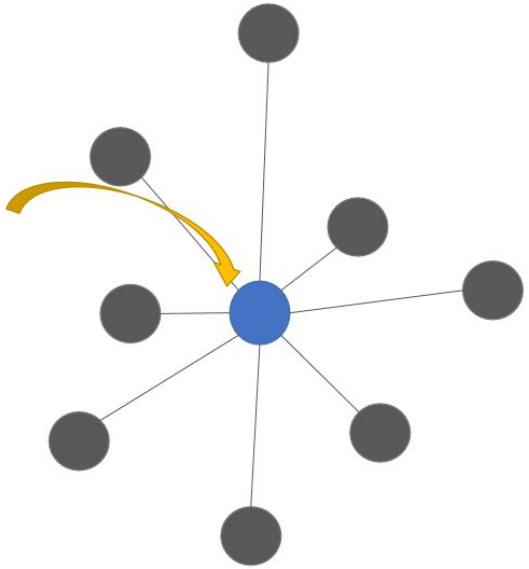
- Криптовалюты? Не только и не столько.
- По сути, блокчейн – это способ организации распределенной БД со специфичными характеристиками:
  - Безопасность (Secure)
    - базируется на криптографическом подтверждении действий узлов;
  - Разделяемость данных (Shared)
    - Данные хранятся на всех узлах сети параллельно;
  - Распределенность логики (Distributed)
    - Каждый узел сети может независимо валидировать приходящие данные;
  - Авторитетность (Authoritative)
    - Иммутабельные записи, нет возможности удалить или редактировать.
- Больше RegTech чем FinTech.

Безопасный распределенный реестр с общим доступом

- Подтверждается с помощью шифрования
  - Используется проверенная и надежная технология подписей с открытыми и закрытыми ключами. Эта технология позволяет создавать в Blockchain транзакции, защищенные от мошенничества, и устанавливать общее доверие без единого центра доверия (**trustless**).
- Общий доступ
  - Ценность технологии Blockchain прямо пропорциональна количеству использующих ее организаций и компаний. Даже в условиях жесточайшей конкурентной борьбы соперникам выгодно вместе участвовать в развертывании этой общей распределенной базы данных
- Распределенная архитектура
  - Существует множество реплик базы данных Blockchain. Фактически, чем больше реплик, тем выше достоверность данных.
- Распределенный реестр
  - К базе данных предоставляется доступ на чтение и однократную запись, поэтому в ней навсегда фиксируются все транзакции.

Централизация и децентрализация

- Одна точка управления
- Одна точка отказа
- Одна точка доверия
- Одна точка атаки
- Система с одним узким местом



napster

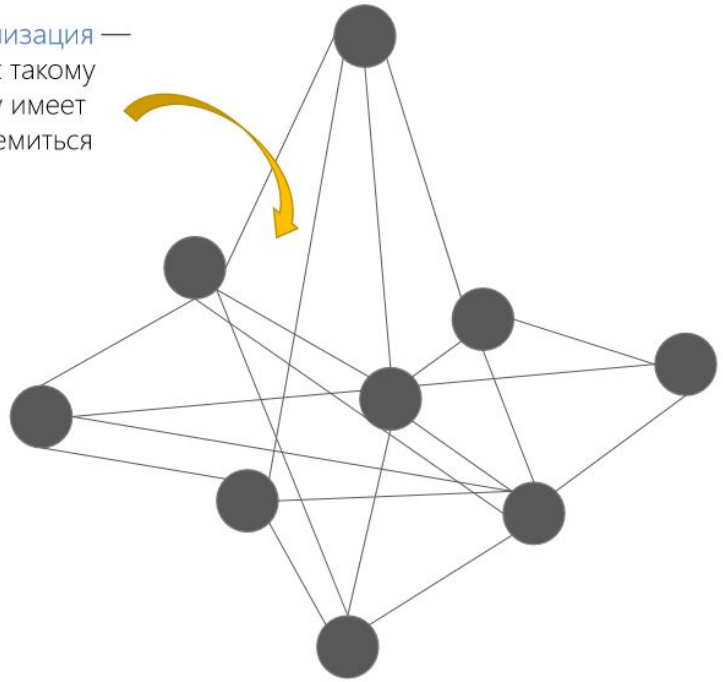
Распределенная централизованная структура

BitTorrent™

Распределенная децентрализованная структура

Децентрализация — пожалуй, к такому устройству имеет смысл стремиться

- Не используется центр управления
- Используется согласие равноправных участников



Отсутствие доверия (Trustlessness)

- **Отсутствие доверия (Trustless)** означает, что стороны, не доверяющие друг другу, могут сотрудничать, не привлекая при этом доверенную третью сторону или центр
- Весь финансовый мир до блокчейна был основан на привлечении доверенных третьих сторон – банки, платежные системы, ЦБ, Swift.
- Nick Szabo в 1998 г. предложил идею отказа от доверенной третьей стороны, заменив ее криптографической защитой передаваемых данных.
- Возникающие проблемы:
  - Кто ведет журнал транзакций?
  - Кто решает, какие транзакции имеют силу? (*проблема двойного расходования*)
  - Как добиться согласия (консенсуса) в децентрализованной сети?
- Первая практическая реализация ответов – **Bitcoin**.

Bitcoin

- Bitcoin Whitepaper - https://bitcoin.org/bitcoin.pdf
- Сочетание:
  - p2p-технологии (BitTorrent DHT) для распределенной работы;
  - Асимметричная криптография для безопасности
  - **Proof of Work для бездоверительной работы.**
- Сама идея цепочки блоков данных (блокчейна) появилась в академической среде еще в 90е.
- В 2008 году Сатоши Накамото в Bitcoin Whitepaper предложил решение проблемы **двойного расходования** через Proof of Work.

Технологические основы

- Вспоминаем основы асимметричной криптографии:
  - Хеш-функции
  - Асимметричная криптография
  - Цифровые подписи
- Блокчейн
- Proof of Work
- Транзакционная информация

Хеш-функции

- Детерминированное преобразование данных произвольного размера (входные данные) в данные фиксированного размера (хеш-суммы).
- Хеш-суммы невозможно спрогнозировать на основе входных данных без фактического выполнения хеш-функции.
- Хеш-суммы также нельзя преобразовать обратно во входные данные.
- Хеш-суммы не содержат сведений о входных данных.
- В идеале хеш-функция при изменении одного бита входных данных зеркально отражает каждый бит выходных данных с вероятностью в 0,5.
- Bitcoin использует SHA-256 (256-битные хеш-суммы)

SHA-256 примеры

- **С**олярлаб -> c24bedffee49b8c9bc8d0e372de9c6256692ec33da8a163791b8f39e4526768d
- **с**олярлаб -> 464342543d5180be2be0645ca0b28059c70a0281fb62cef6f3c03063d3228a8f
- солар лаб -> 5f468a088b422d30a38c9e03c44b88b0c8e4ce7da6fd1c8814f5fe3250a9bcb4
- Можно использовать хеш для контроля **изменения** данных.

Шифрование с использованием открытого ключа

Как отправлять секретные сообщения по проводной сети, если за тобой следит старуха Шапокляк?

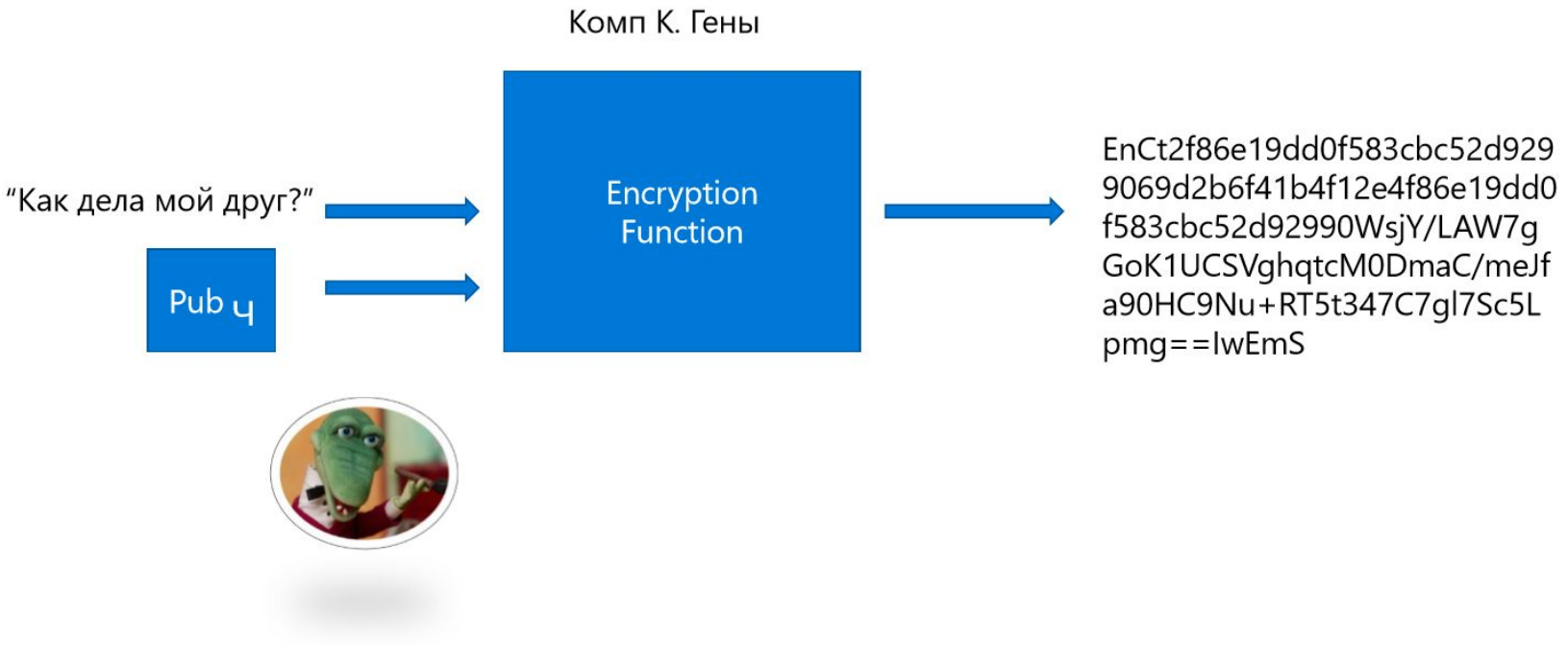
Шифрование с использованием открытого ключа

- Все базируется на “keypairs”, состоящих из открытого и закрытого ключа.
- Открытый ключ создается на основе закрытого.
- Открытые ключи не содержат сведений о закрытом ключе.
- Данные, зашифрованные с использованием открытого ключа, можно расшифровать с помощью закрытого ключа, и наоборот.

Шифрование с использованием открытого ключа

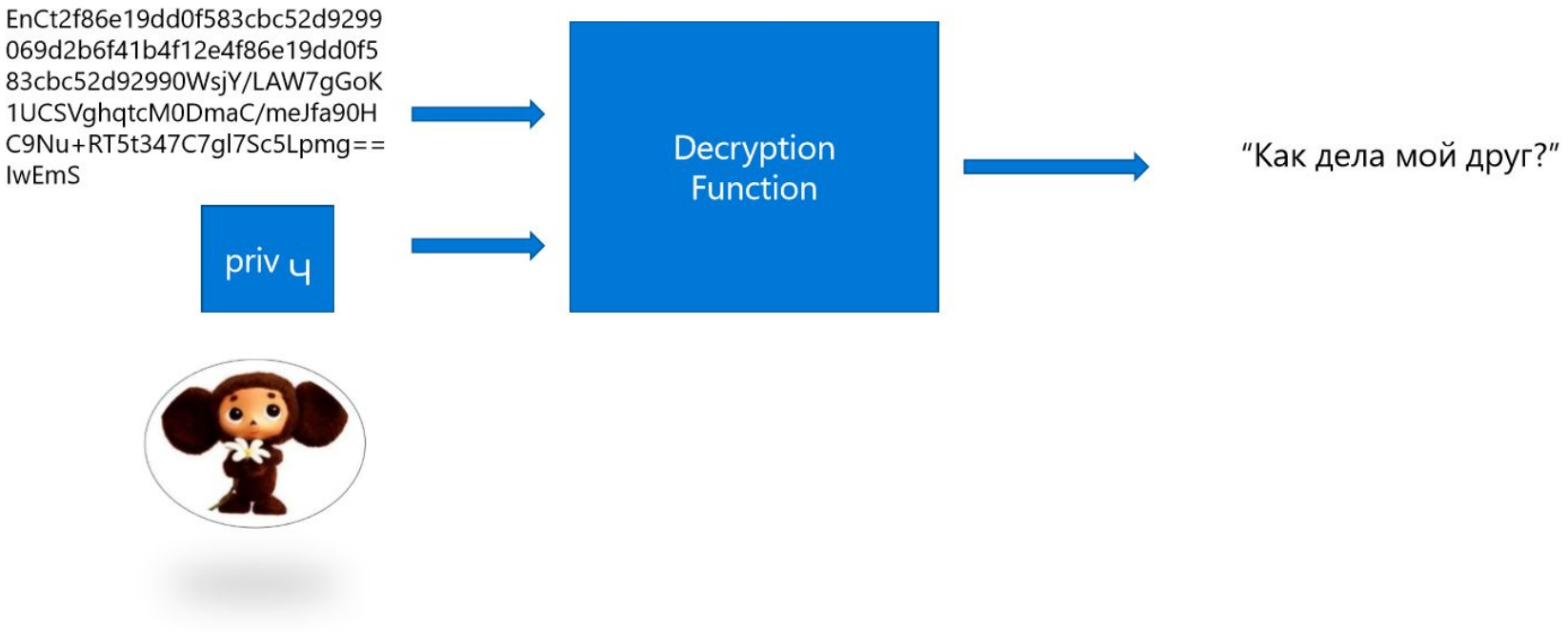
Как отправлять секретные сообщения по проводной сети, если за тобой следит Шапокляк?

Шифрование с использованием открытого ключа

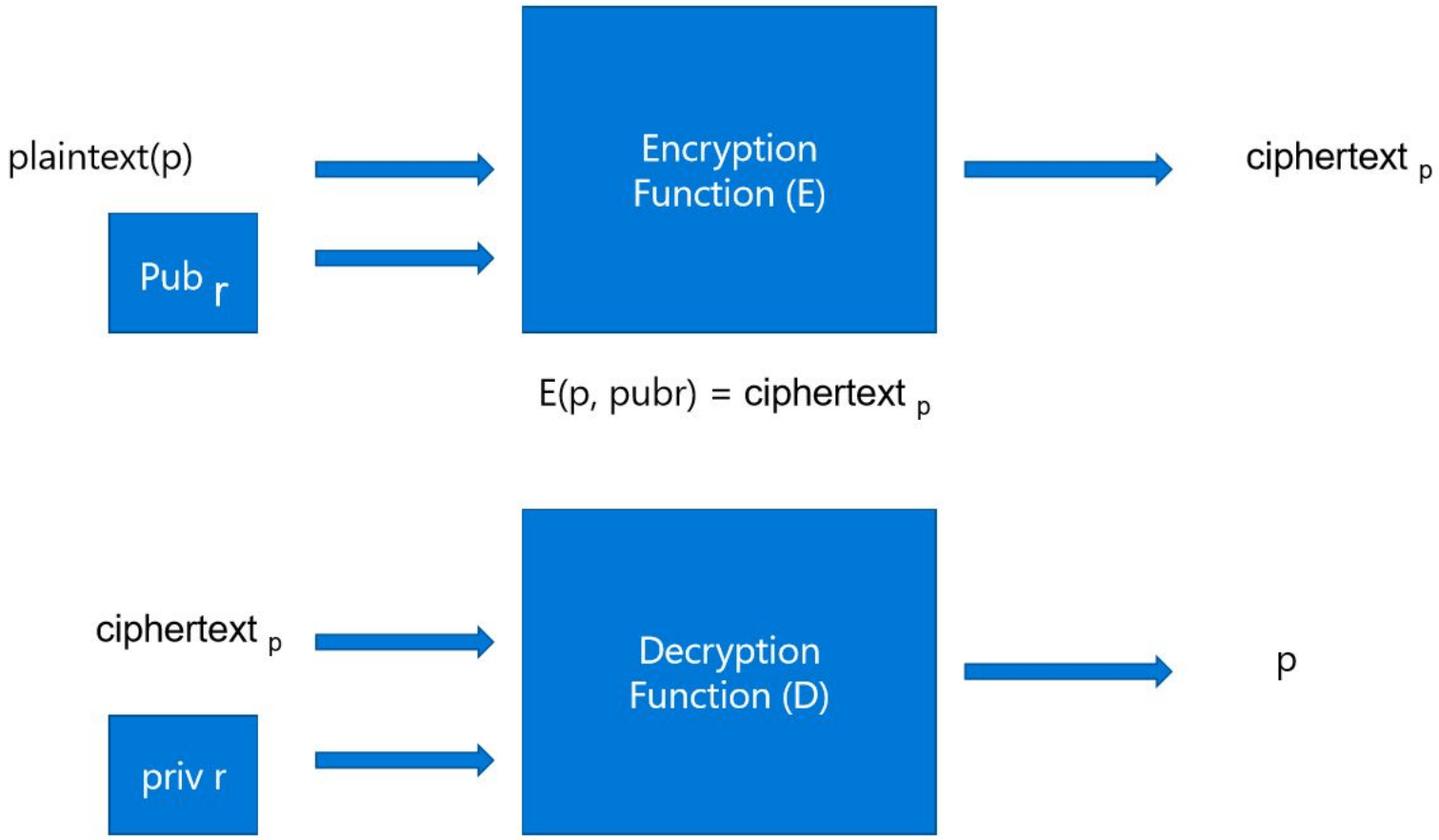


Шифрование с использованием открытого ключа

Шифрование с использованием открытого ключа



Другими словами



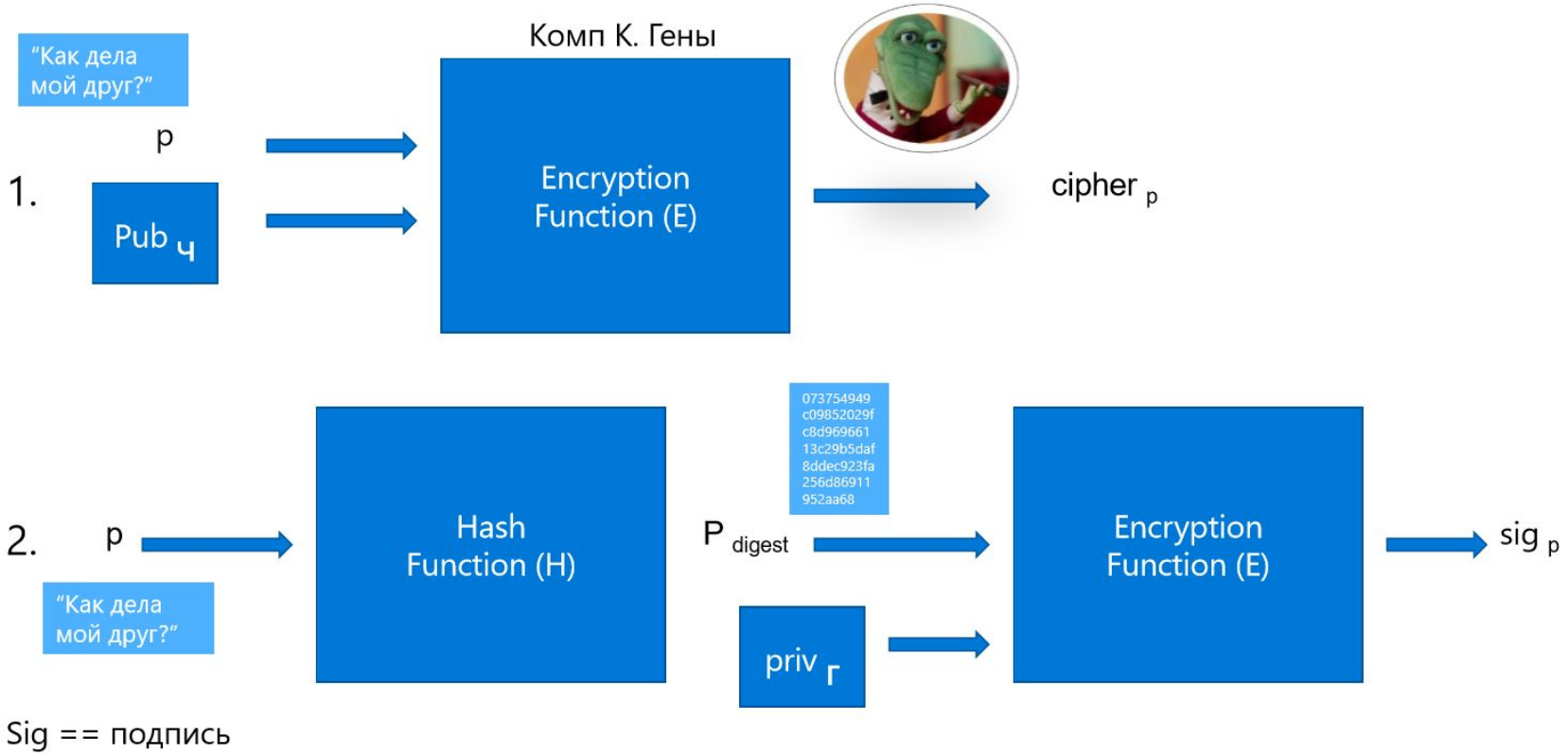
Цифровые подписи

Как отправлять секретные сообщения по проводной сети и при этом быть уверенным, что Шапокляк их никак не изменило?

Электронная подпись

- Объединение алгоритмов хеширования и шифрования с использованием открытого ключа.
- Подтвердить, что содержание полученного сообщения не изменилось с момента его отправки.
- Подтвердить, что полученное якобы от Гены сообщение действительно было отправлено Геной, а не другим крокодилом.

Создание подписи

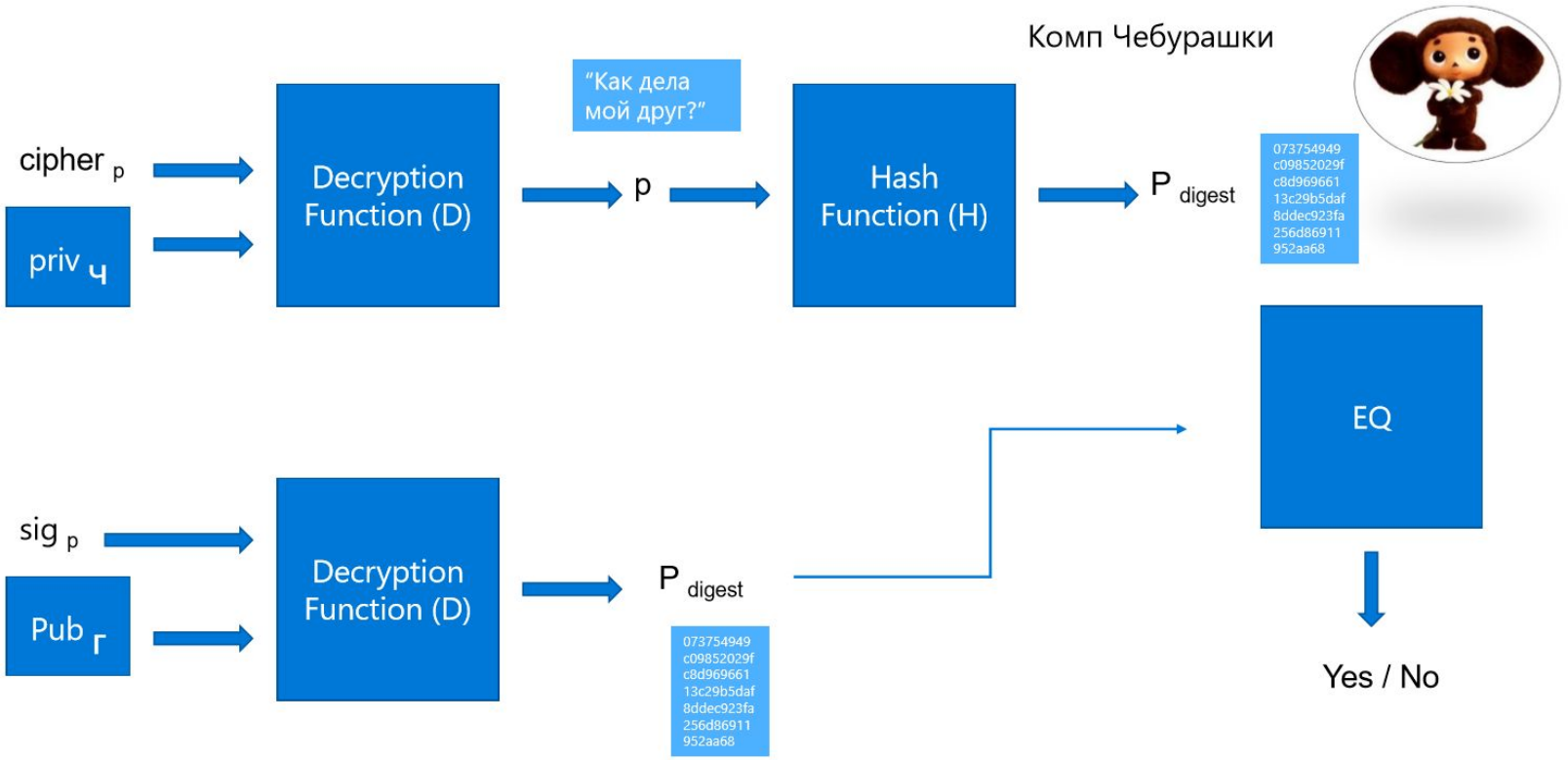


Sig == подпись

Сообщение для Чебурашки

Электронная подпись

Расшифровка и проверка подлинности



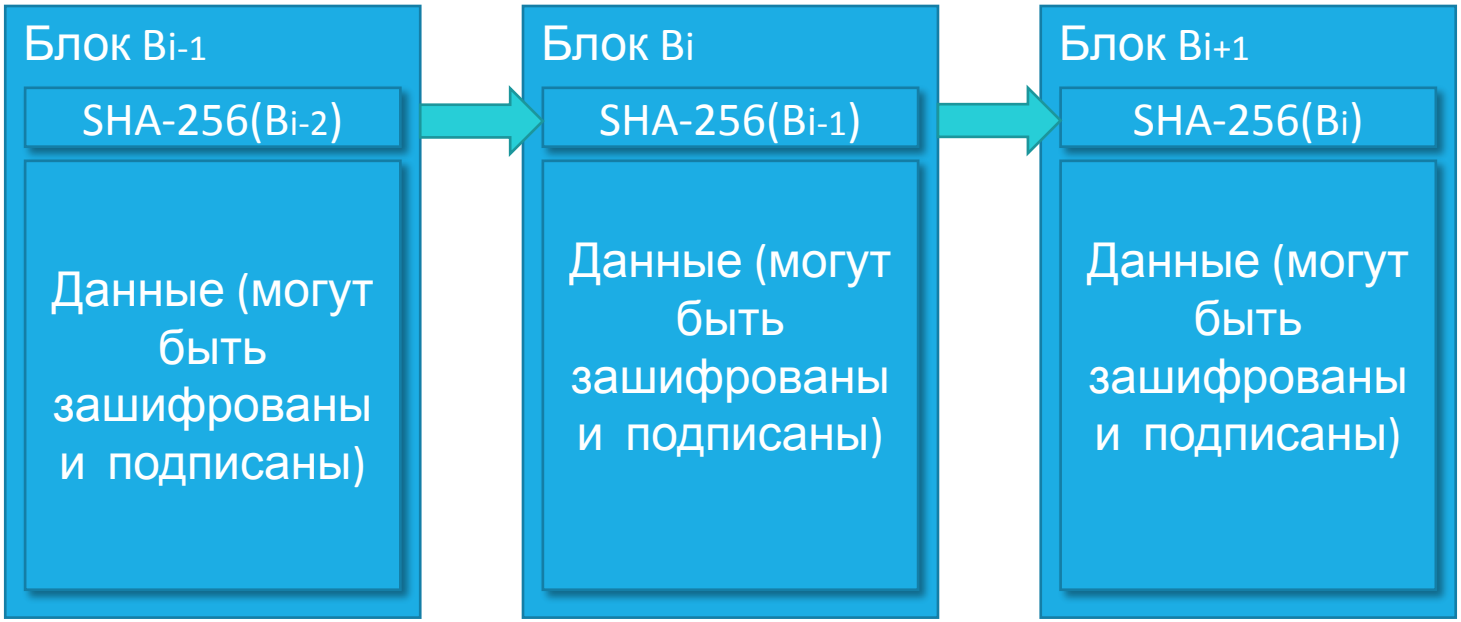
Попытка взлома подписанного сообщения?

1. Шапокляк изменяет открытый текст с «<3» на «:(»
2. Если Чебурашка применяет шифрование для подписи и хеширование для открытого текста, они не будут совпадать.

Попытка взлома подписанного сообщения?

1. Шапокляк изменяет открытый текст с «<3» на «:(» и подпись sig p на sig p, используя собственный закрытый ключ.
2. Если Чебурашка пытается зашифровать подпись, используя открытый ключ Гены, то расшифровку выполнить не удастся, так как подпись зашифрована с помощью закрытого ключа Шапокляк.

Блокчейн – цепочка блоков



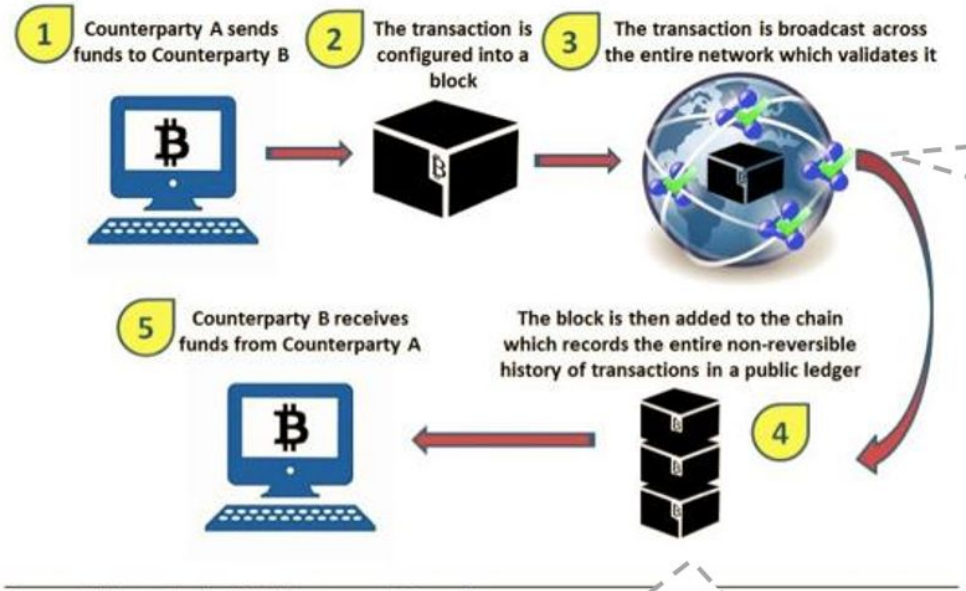
- Решает проблему контроля изменений.
- Распределенный иммутабельный реестр данных.
- Не решает проблему доверия (кто строит цепь?)

Блокчейн в Биткойне

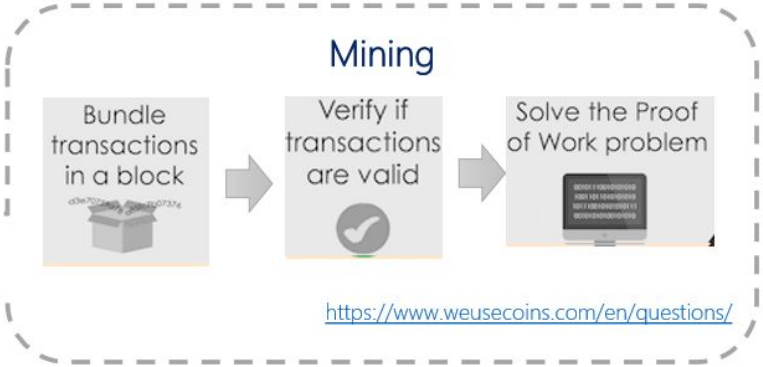
- Blockchain — это общедоступная распределенная база данных (реестр) транзакций, защищенных с помощью шифрования.
- В этом реестре хранится вся история транзакций каждой заданной системы.
  - Она является общей для всех участников каждой заданной системы.
  - Нет какой-либо одной точки доверия или одной точки отказа.
  - Транзакции являются общедоступными, но сохраняется конфиденциальность.
  - Мошенничество сразу же становится очевидным.
- Основное нововведение Bitcoin: целостность такого распределенного реестра поддерживается и обеспечивается **«майнерами»**, которые проводят аудит и архивацию транзакций за вознаграждение.

Блокчейн в Биткойне

Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin

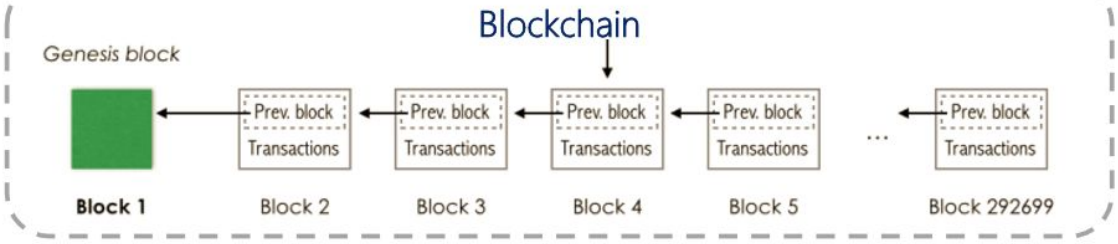


Source: Goldman Sachs Global Investment Research.



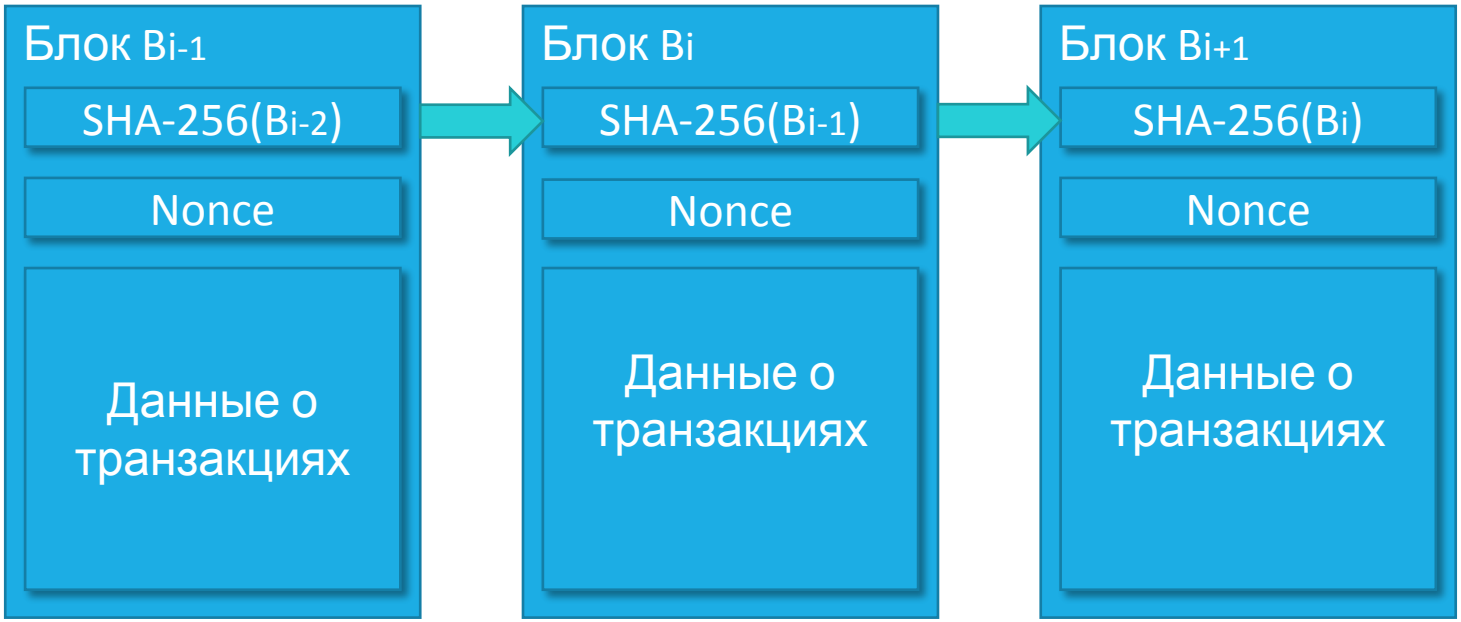
https://www.weusecoins.com/en/questions/

Blockchain
Декодированные данные



https://digitalcoinlobby.wordpress.com/

Блокчейн в Биткойне: Nonce и Proof of Work

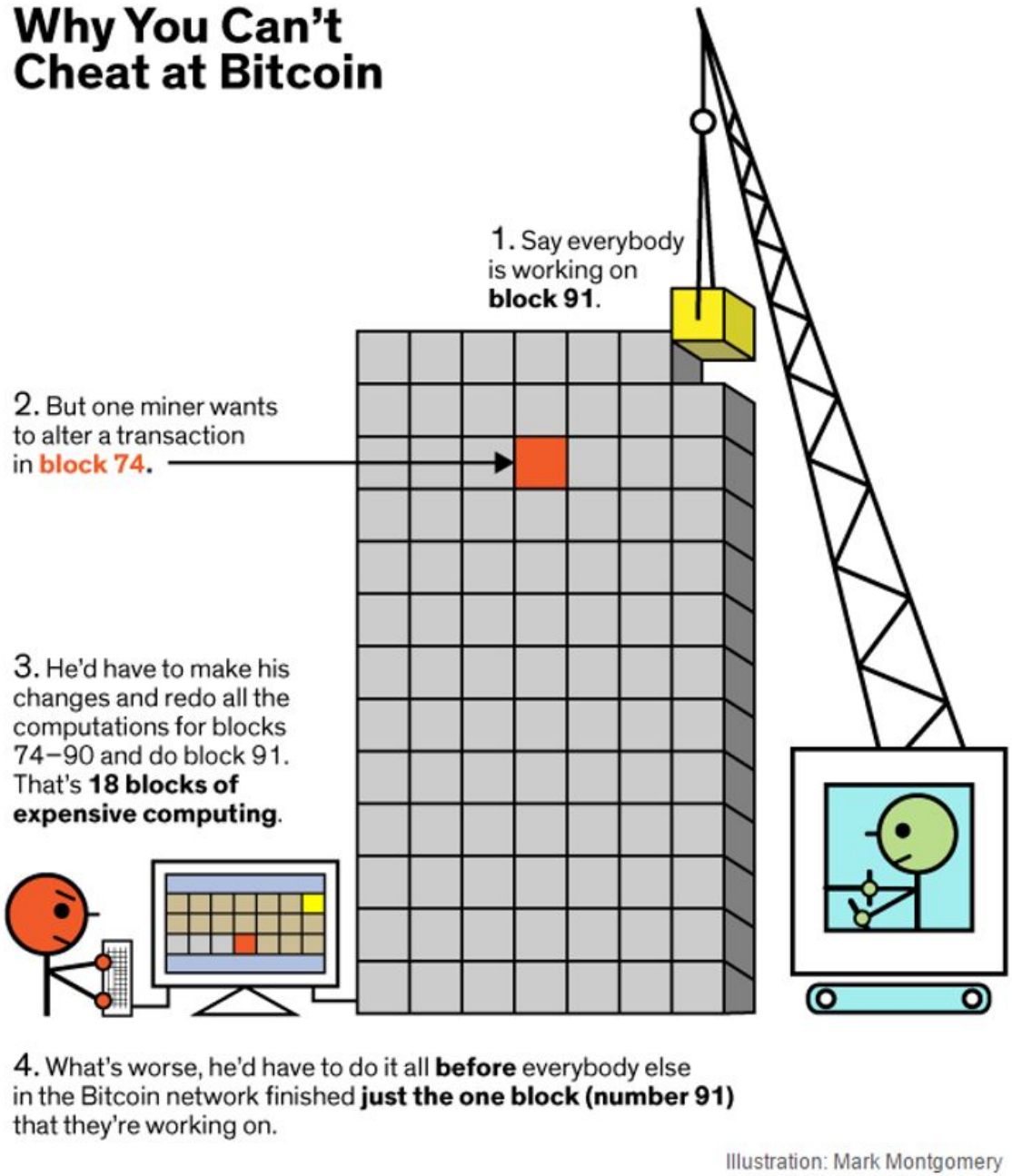


- Nonce – случайное число, которое подбирается так, чтобы значение хеша стало необычным (начинается с N нулей, где N задает сложность майнинга)
- Nonce пошагово приращивается и хеш пересчитывается, пока не найдем нужное значение. После этого блок публикуется в чейн.

Блокчейн в Биткойне

- Каждый новый блок рассчитывается майнером на базе текущего последнего, таким образом транзакции «закапываются» все глубже.
- Если приходит новый блок до нахождения Nonce, процесс надо начинать заново.
- Из-за лагов или других причин может оказаться, что более одного узла все же сгенерировали разные версии одного и того же блока. Это создает ветвление (fork) чейна.
  - При этом система считает истинной ту ветку, которая длиннее (на базе которой сгенерили большее число блоков.
  - Транзакции из проигравшей ветке откатываются и включаются в новые блоки.
- Обычно 6 уровней «закапывания» блока достаточно – для гарантии подтверждения транзакции (средства, пришедшие по таким транзакциям уже можно тратить).

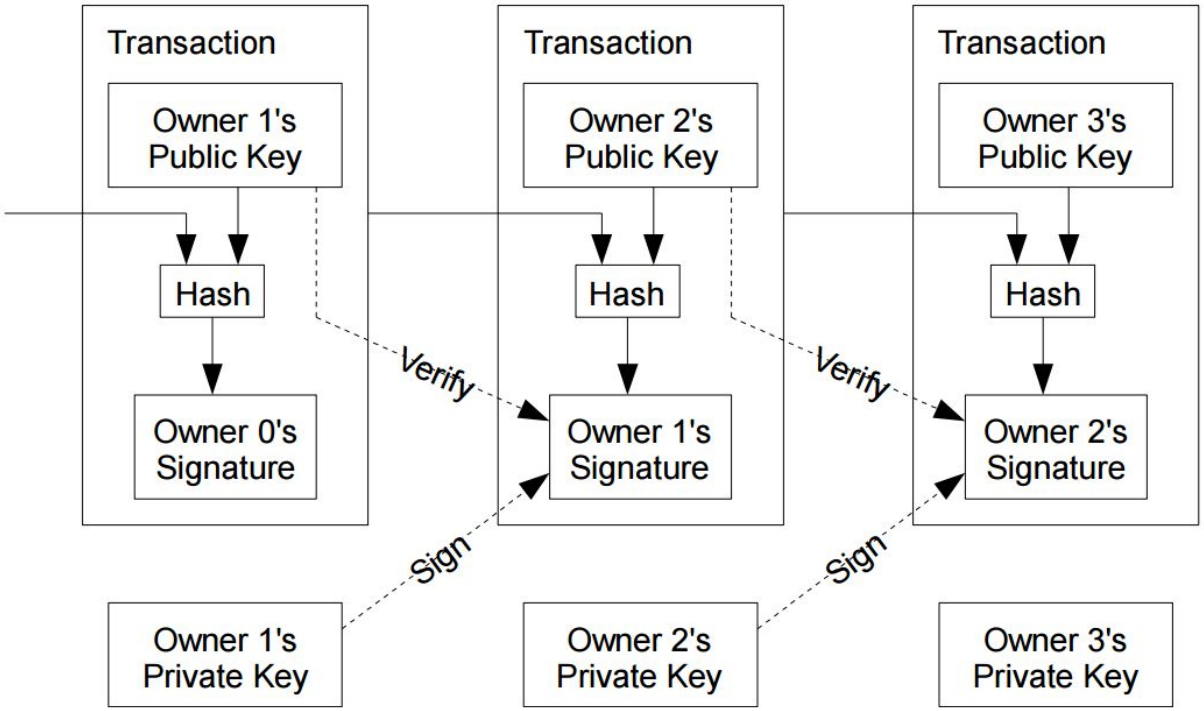
Как PoW защищает от фрода



Проблемы PoW и альтернативы

- Proof of Work – ресурсоемкая операция по свой сути, что требует «жечь» огромное количество вычислительных ресурсов и энергии.
- Альтернативы:
  - **Proof of Authority** – старое доброе доверие ☺️
  - **Proof of Stake** – идея в том, что если у тебя есть определенное количество криптовалюты, тебе не выгодно нарушать правила, содействуя обвалу этой валюты
  - Вариации **BFT**-алгоритма – есть ряд допущенных к майнингу узлов, и даже если до 1/3 из них скомпрометированы, алгоритм гарантирует целостность данных.
  - Активно ищутся другие варианты.
    - Такая экзотика как Proof of Disk Space – идея замены подтверждения ресурсов процессора ресурсами дисковой системы.

Транзакционные данные

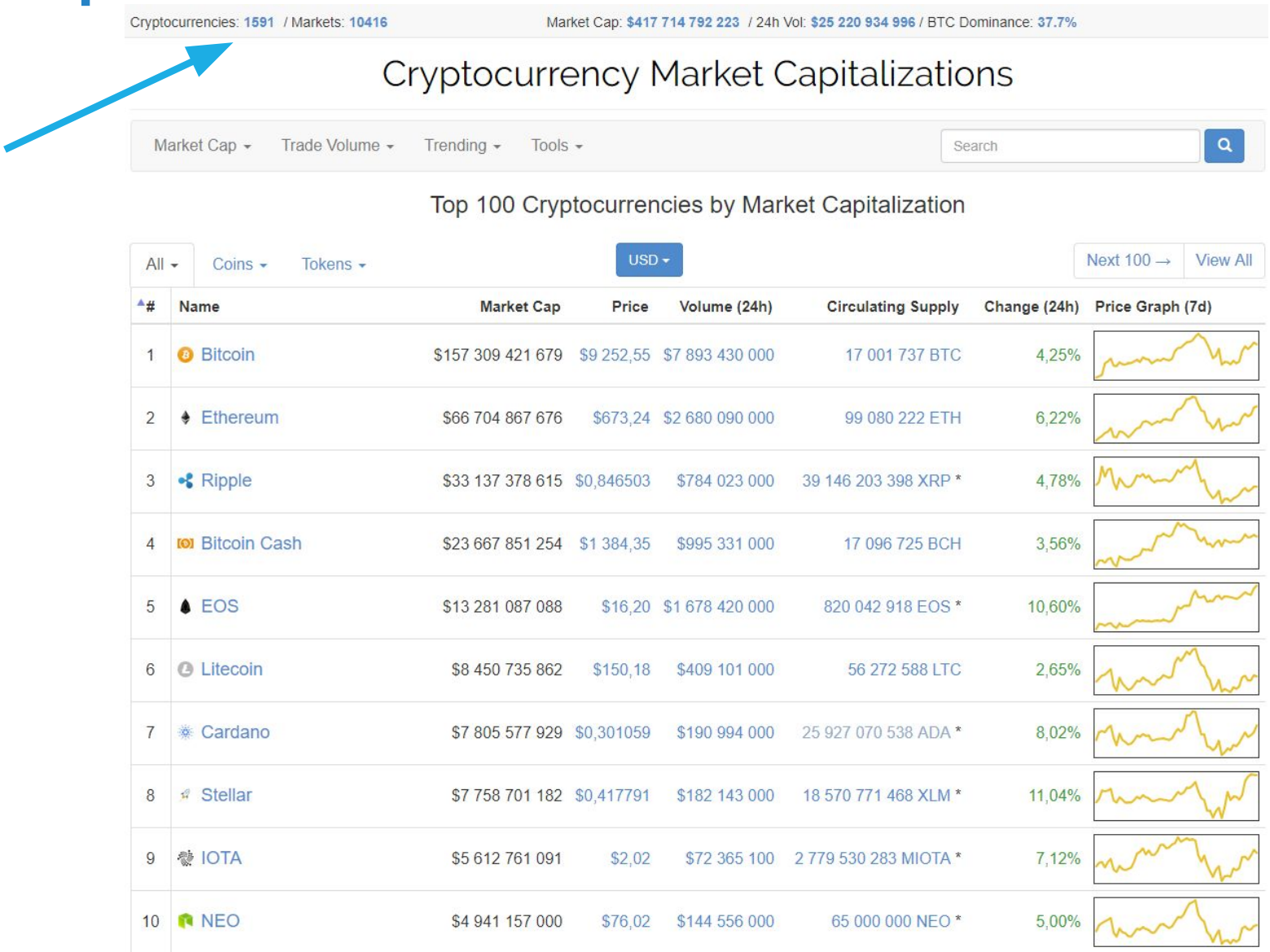


- Транзакции связаны в цепь – каждая транзакция базируется на другой
- Первая транзакция в каждом блоке – особая, создает монету-вознаграждение для майнера.
- Для уменьшения объема транзакционной информации старые транзакции могут «засушиваться» (pruning) – свертываться в хеш-дерево (дерево Меркла, Merkle tree)

Эволюция блокчейна

- “Blockchain 1.0“ – Bitcoin и сайдчейны.
- “Blockchain 1.5“ – Multichain.
- “Blockchain 2.0” – Ethereum
  - Глобальный компьютер
  - Смарт-контракты и децентрализованные приложения
  - Оракулы
- “Blockchain 3.0” – ???
  - Все пытаются им себя объявить ☺️
  - Решение проблем скорости, масштабируемости, пропускной способности и стоимости.

Криптовалюты



Cryptocurrencies: 1591 / Markets: 10416 Market Cap: $417 714 792 223 / 24h Vol: $25 220 934 996 / BTC Dominance: 37.7%

Cryptocurrency Market Capitalizations

Market Cap ▾ Trade Volume ▾ Trending ▾ Tools ▾ Search

Top 100 Cryptocurrencies by Market Capitalization

All ▾ Coins ▾ Tokens ▾ USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$157 309 421 679	$9 252,55	$7 893 430 000	17 001 737 BTC	4,25%	
2	Ethereum	$66 704 867 676	$673,24	$2 680 090 000	99 080 222 ETH	6,22%	
3	Ripple	$33 137 378 615	$0,846503	$784 023 000	39 146 203 398 XRP *	4,78%	
4	Bitcoin Cash	$23 667 851 254	$1 384,35	$995 331 000	17 096 725 BCH	3,56%	
5	EOS	$13 281 087 088	$16,20	$1 678 420 000	820 042 918 EOS *	10,60%	
6	Litecoin	$8 450 735 862	$150,18	$409 101 000	56 272 588 LTC	2,65%	
7	Cardano	$7 805 577 929	$0,301059	$190 994 000	25 927 070 538 ADA *	8,02%	
8	Stellar	$7 758 701 182	$0,417791	$182 143 000	18 570 771 468 XLM *	11,04%	
9	IOTA	$5 612 761 091	$2,02	$72 365 100	2 779 530 283 MIOTA *	7,12%	
10	NEO	$4 941 157 000	$76,02	$144 556 000	65 000 000 NEO *	5,00%	

Ethereum

- Основана в 2013, вышла на краудфандинг в 2015
- Своя реализация блокчейна
  - PoW+PoS
  - Валюта Ether (ETH)
- Распределение кода через блокчейн
  - Глобальный компьютер (Ethereum VM)
  - Смарт-контракты и распределенные приложения
    - Понятие смарт-контракта
    - Пример смарт-контракта - https://www.ethereum.org/crowdsale
- Оракулы – источники внешних событий

Multichain

- Базируется на Bitcoin Core, во многом совместима с протоколами Bitcoin.
- Основная особенность - оптимизация под консорциумы (закрытые блокчейны)
  - Множество сетей (чейнов) для одной ноды
  - Управление разрешениями (permissions)
  - Кастомные активы (assets) в транзакциях
  - Потоки данных (immutable key-value storage)
  - PoA-майнинг – размениваем бездоверительность на скорость.

Платформа Федерация

- Организация безопасного обмена данными между организациями без единого центра доверия.
- Распределенное хранилище данных на базе потоков Multichain.
- Поверх блокчейна – ГОСТовское шифрование, обеспечивающее защиту данных от НСД.
- Сценарий - аккредитация