блокчейн и Пари

клас 4

18 септември 2018 г

Клас 4 (9/18): Учебни въпроси

- Какъв е проблемът с византийските генерали? Как доказателството за работа и копаене в биткойн се справят с това? По-общо как се справя блокчейн технологията?

- Какви други протоколи за консенсус има? Какви са някои от компромисите на алтернативните консенсусни алгоритми – доказателство за работа, доказателство за залог и т.н.?

- Как работят икономическите стимули в блокчейн технологията, за да поддържате децентрализирани регистри и избягвате двойно харчене? Какви са стимулите на консенсусните протоколи и майнинга? (Преместено от 20 септември)

4 клас (9/18): четения

- „Доклад от Женева“, глава 1 (страници 1 – 7); Кейси, Крейн, Генслер, Джонсън и Нарула
- „Преглед на технологията на блокчейн“ NIST (страници 23 - 32, раздели 3 и 4)
- „Проблемът с византийските генерали“ Лампорт, Шостак и Пийз (382-387)
- „Кратко ръководство за консенсусните протоколи“ CoinDesk

Общ преглед на клас 4

- Преглед на дизайна на блокчейн

- Консенсус чрез доказателство за работа
- Копаене на биткойни • Родна валута

- Мрежа

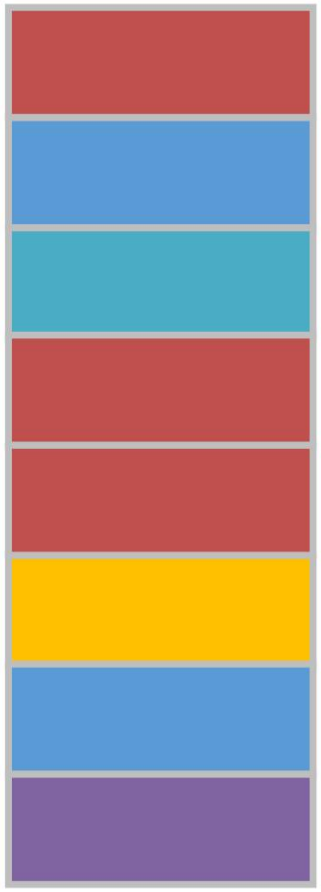
- Други консенсусни протоколи

- Изводи

Преглед - Блокчейн технология

регистрационен файл

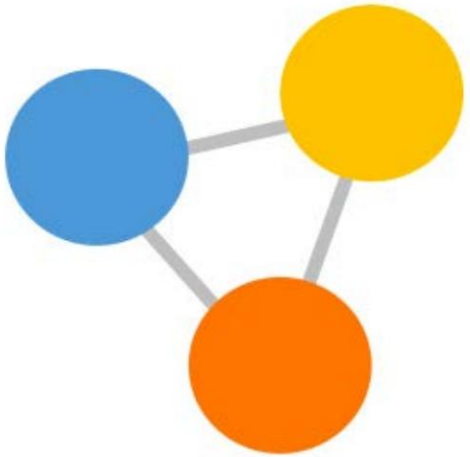
само за добавяне с клеймо за време



подлежаща на одит база данни

Защитено чрез криптография • Хеш функции за устойчивост на фалшифициране и цялост • Цифрови подписи за съгласие Консенсус за съгласие

мрежов консенсусен протокол



Адресира „цената на доверието“

(Проблем с византийските генерали) • Разрешено

• Без разрешение

Биткойн – Технически характеристики

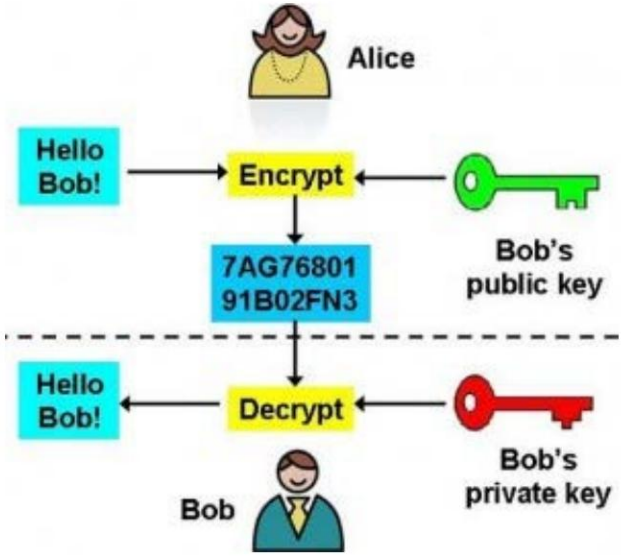
- Криптография и регистрационни файлове с времево клеймо
  - Криптографски хеш функции •
  - Регистрационни файлове само за добавяне (блокове) с клеймо за време • Заглавки на блокове
  - и Merkle дървета • Асиметрична криптография и цифрови подписи • Адреси
- Децентрализиран мрежов консенсус
  - Доказателство за
  - работа • Родна валута
  - Мрежа
- Скрипт за транзакции и UTXO
  - Входове и изходи на транзакция •
  - Задаване на неизразходван изход на транзакция
  - (UTXO) • Скриптов език

Криптография:

Комуникации в присъствието на противници

Scytale Cipher
Древни времена

Машина Енигма 1920 -
Втората световна война



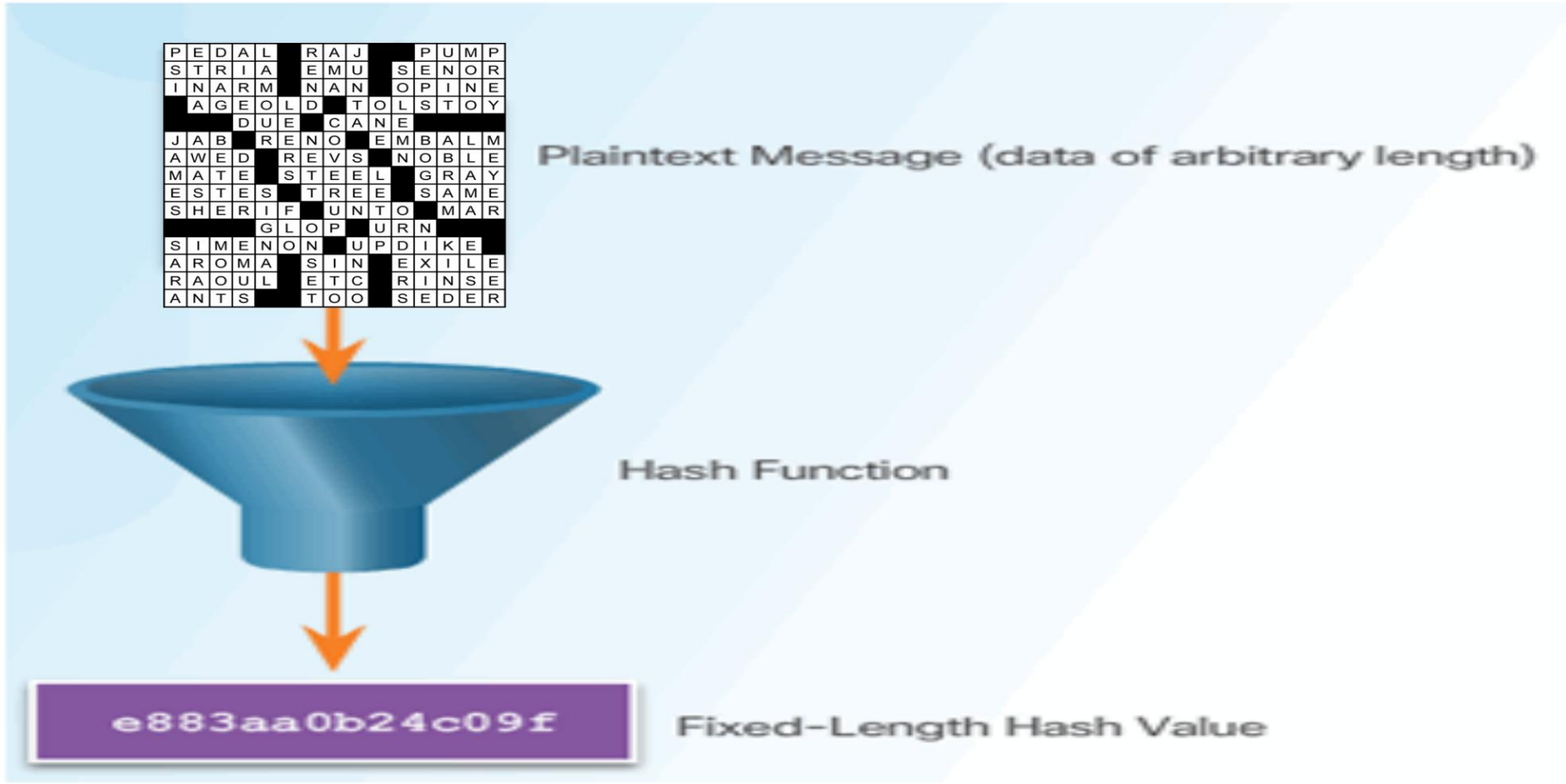
Асиметрична криптография от 1976 до днес

Изображение от ЦРУ и е публично достояние чрез Wikimedia Commons.

Изображението е обществено достояние чрез Wikipedia.

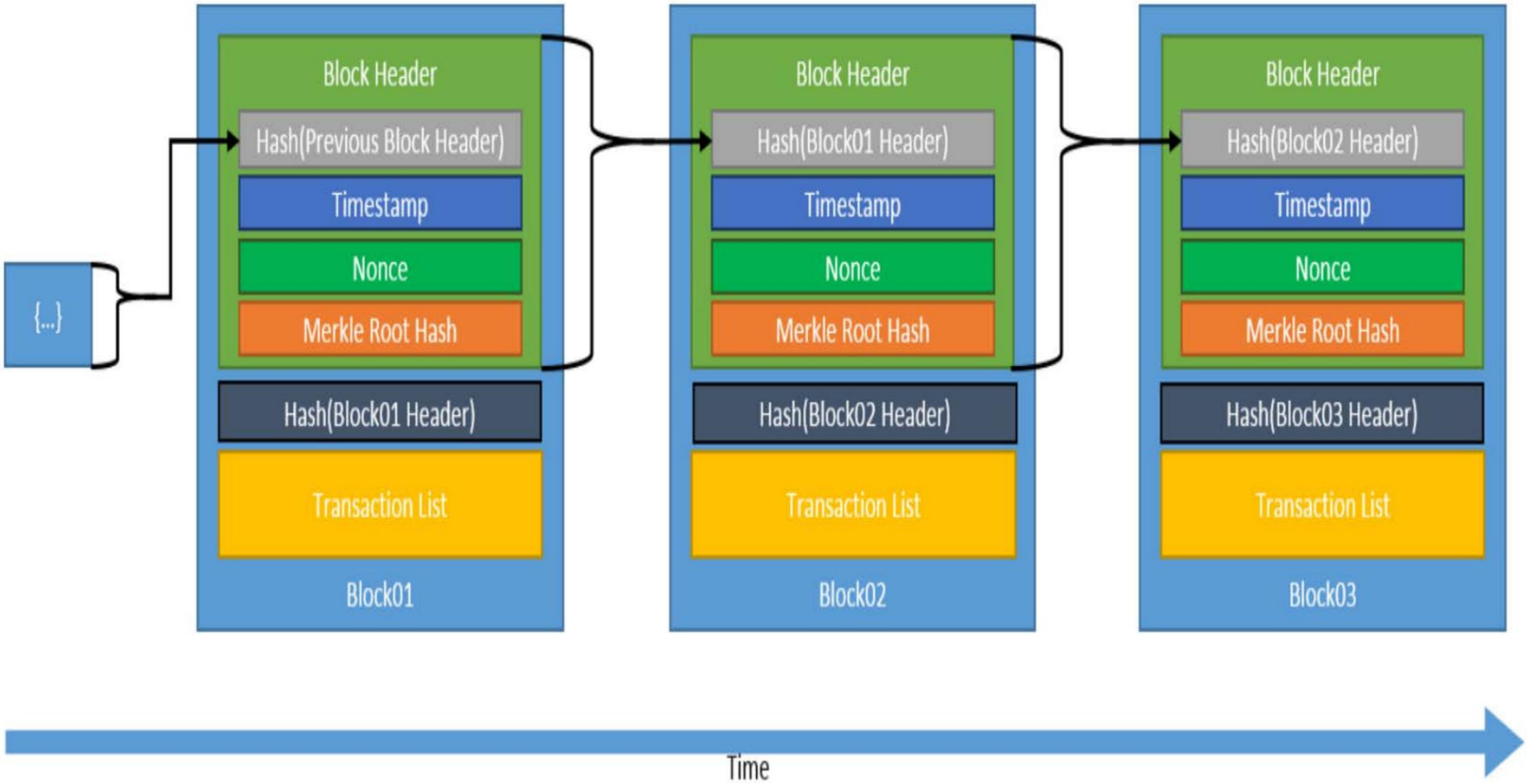
Криптографски хеш функции

Еднопосочна компресия на данни

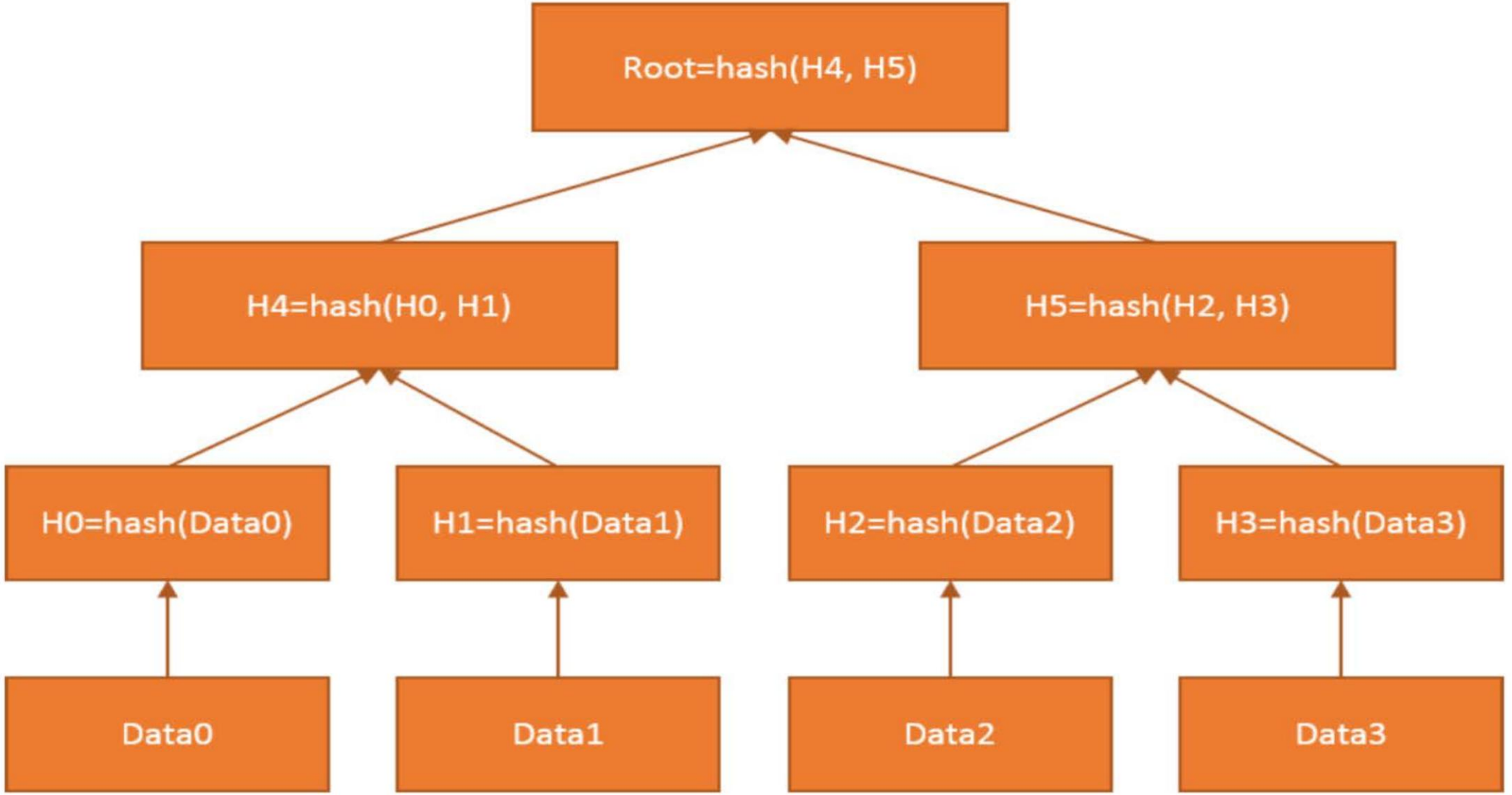


Ангажимент за данни

Дневник само за добавяне с клеймо за време - Blockchain



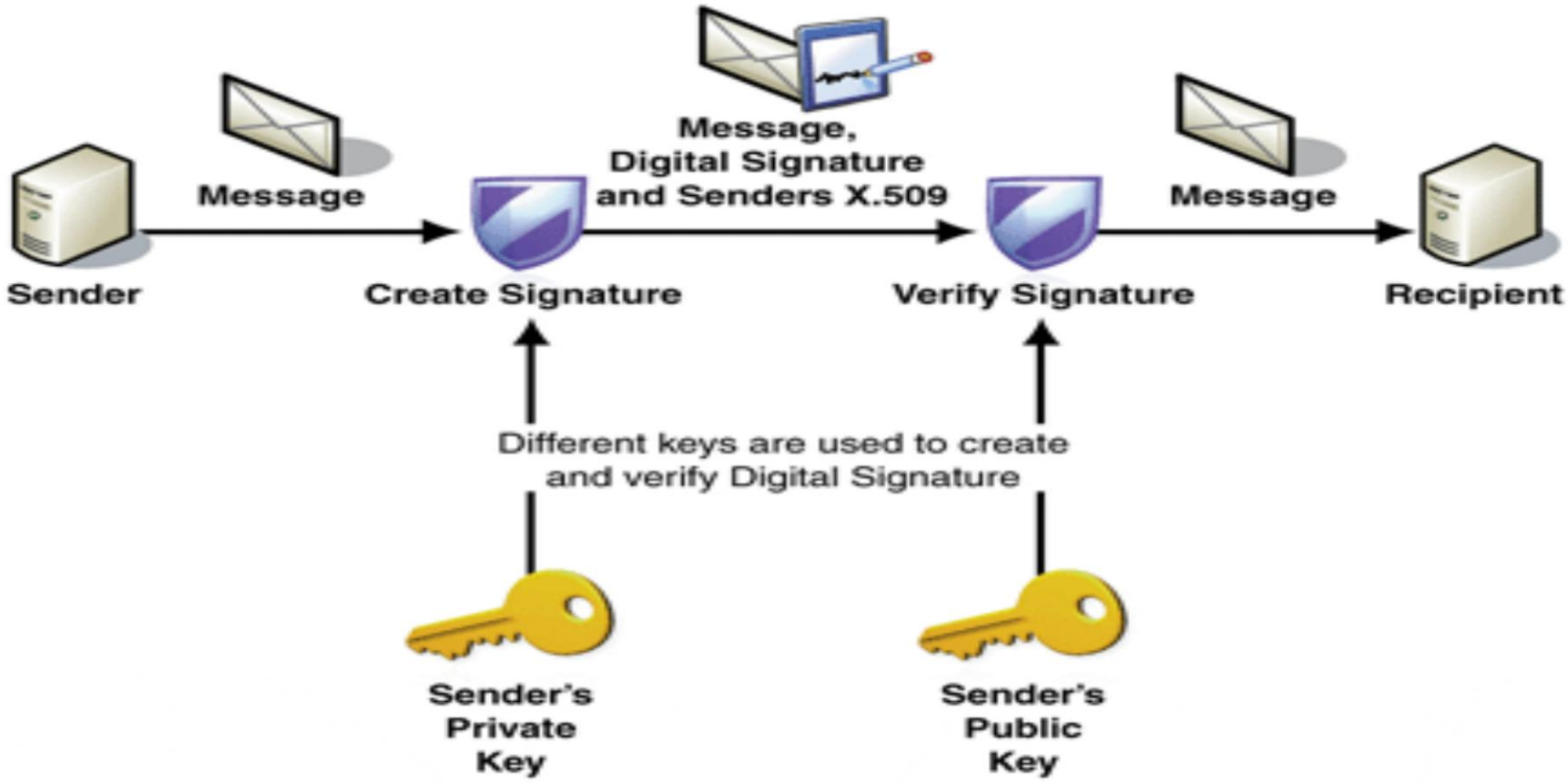
Merkle Tree – Двоично дърво с данни с хешове



Асиметрична криптография и цифрови подписи

Защита срещу подправяне и представяне под чужда самоличност

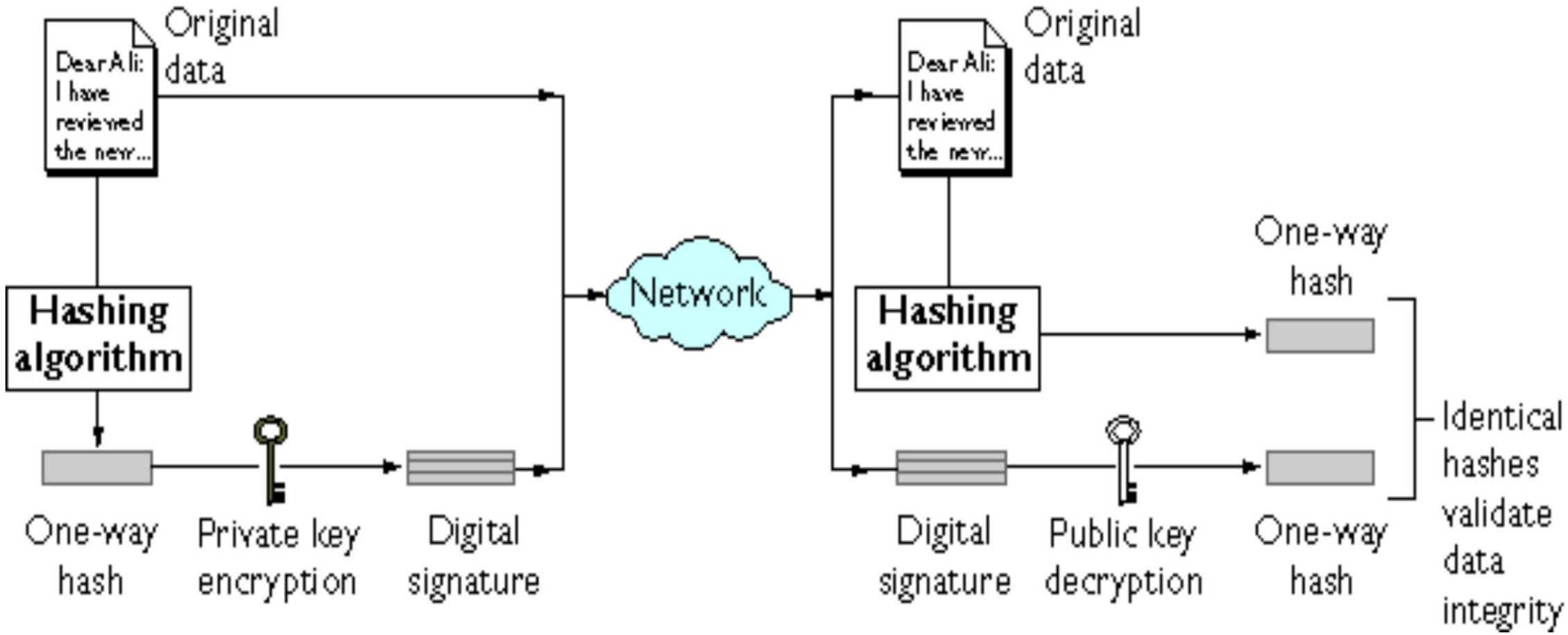
Цифров подпис без хеш



Асиметрична криптография и цифрови подписи

Защита срещу подправяне и представяне под чужда самоличност

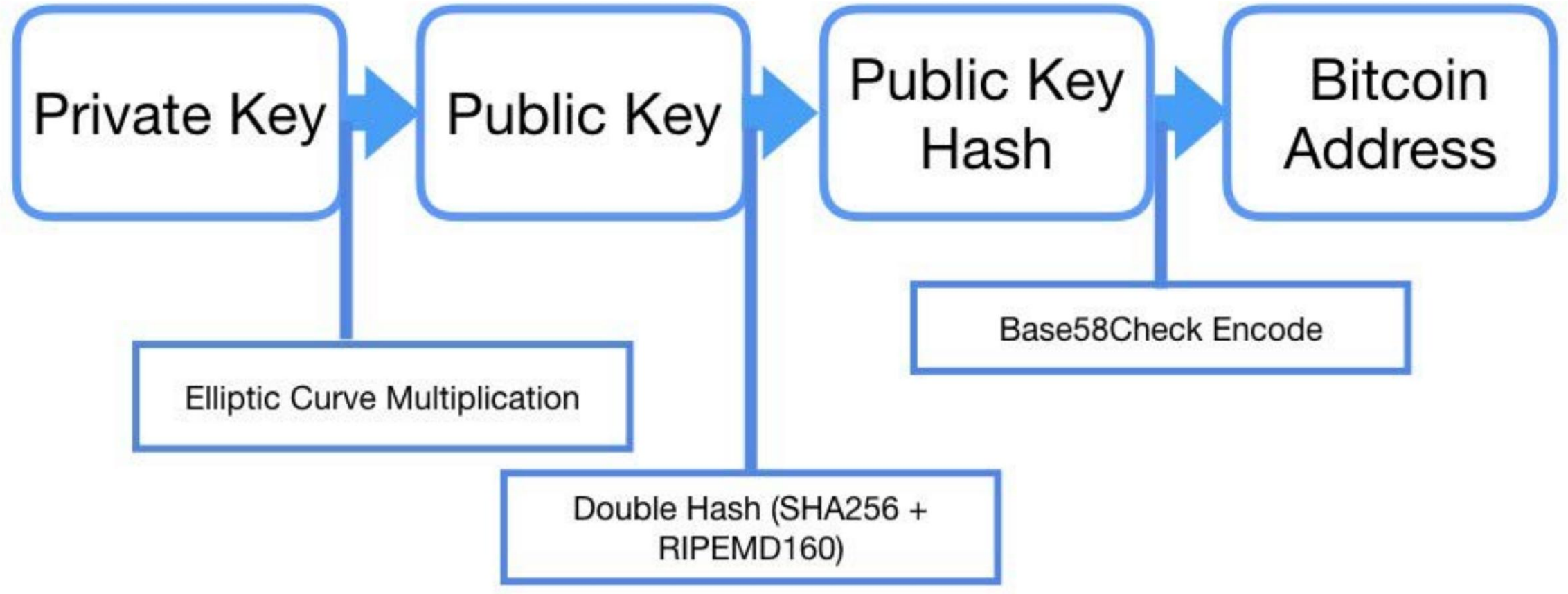
Цифров подпис с хеш



Shyam Nandan Kumar и др. Преглед на мрежовата сигурност и криптографията.

Биткойн адрес

Определя се от – но не идентичен с – Публичен ключ



Децентрализирани мрежи

Проблемът с византийските генерали

Атака!

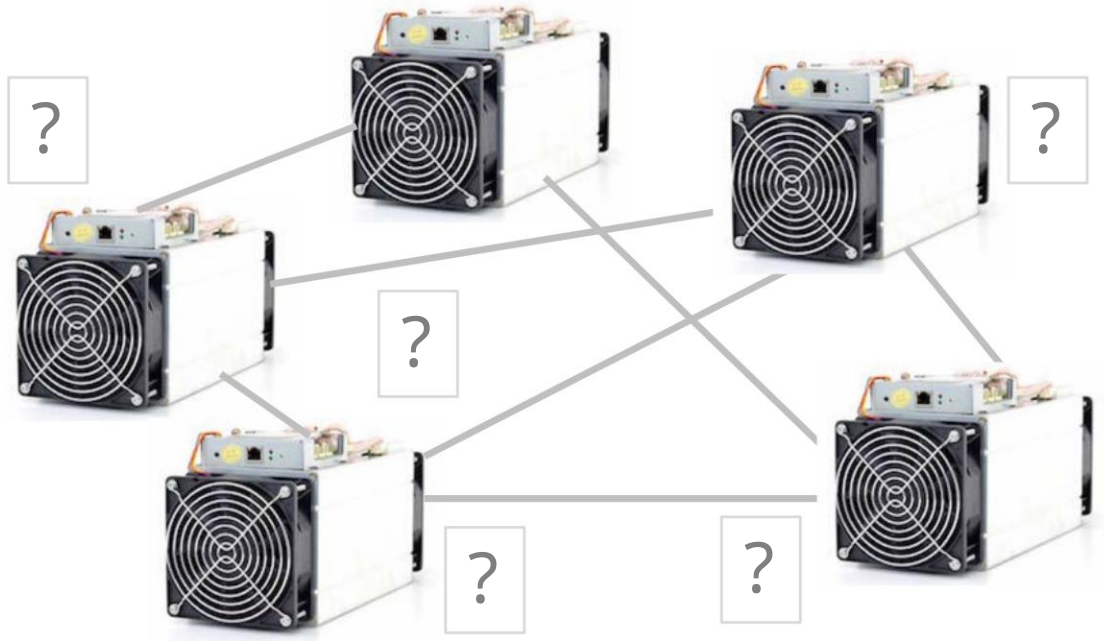
Атака!

Отстъпление

Отстъпление

Атака!

Блокови вериги без разрешение - Неизвестни участници

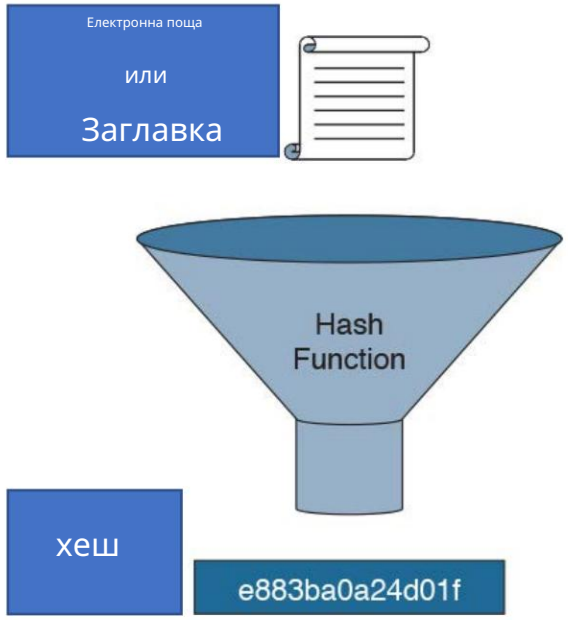


Сигурност, базирана на: • Консенсусен протокол & • Местна валута

Hashcash – доказателство за работа (Adam Back, 1997)

Предложено за справяне с имейл спам и атаки за отказ на услуга

• Изисква изчислителна работа за намиране на хеш в предварително определен диапазон

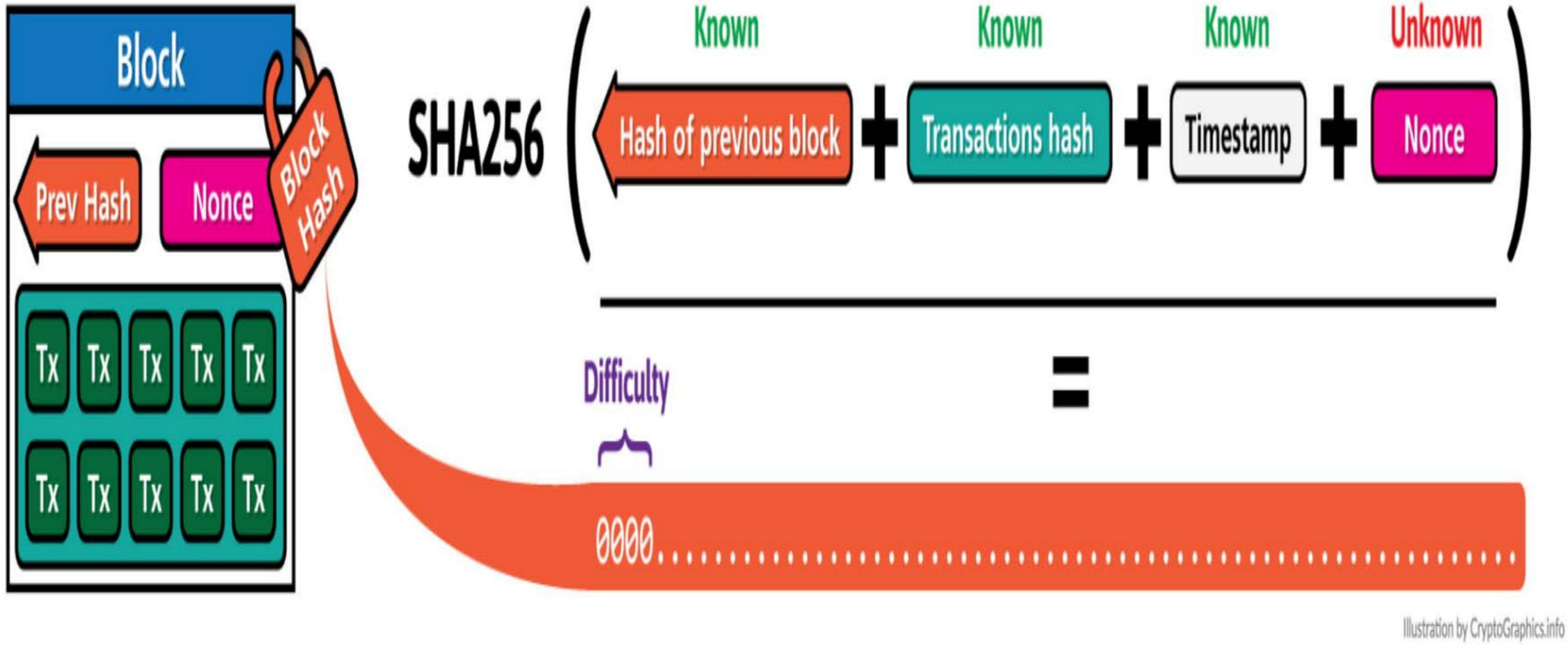


• Трудност, определена от броя на водещите нули в хеш изхода •

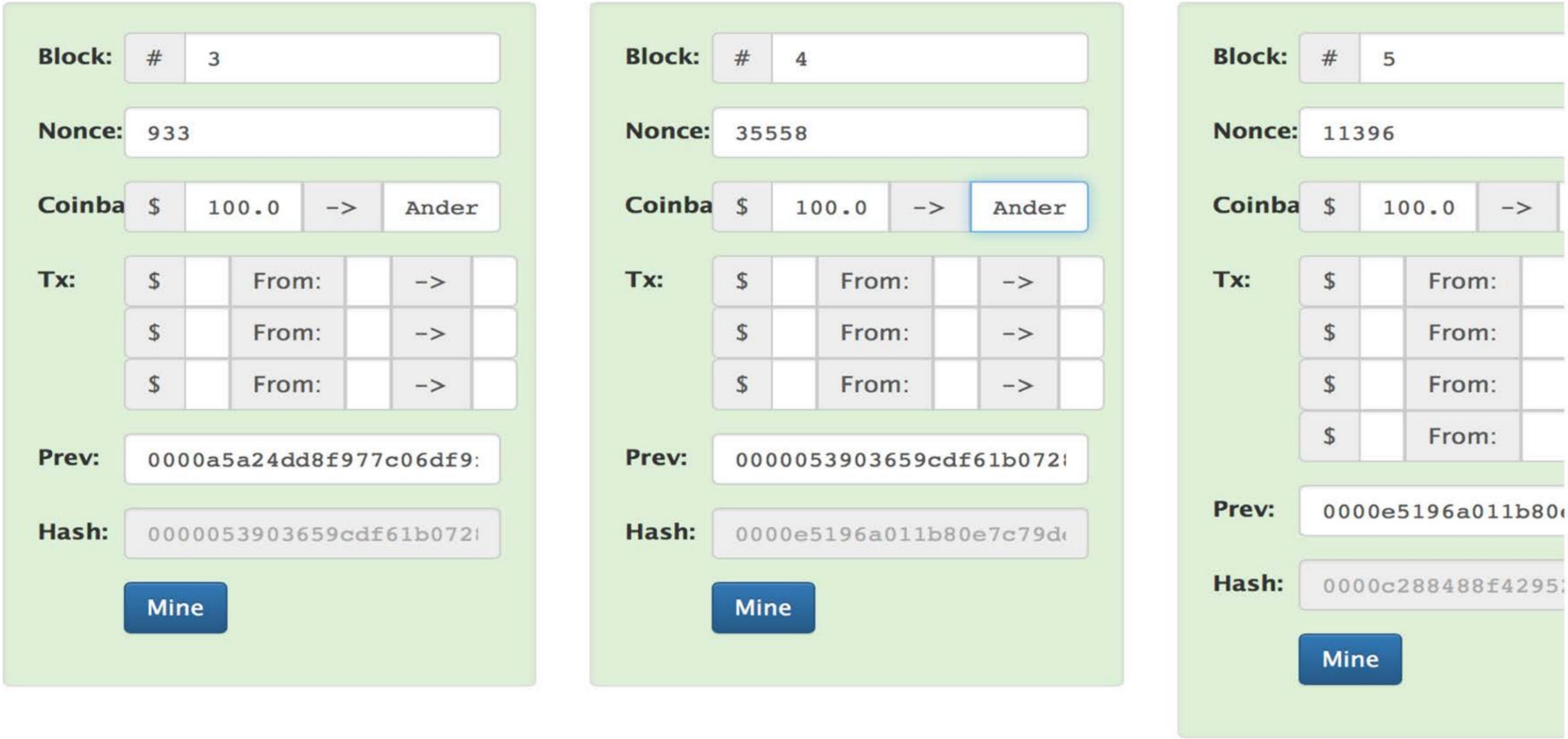
Доказателството за работа може да бъде ефективно проверено 15

Блокчейн – доказателство за работа

Иновация – Верижно доказателство за работа за разпределен мрежов консенсус и маркиране на време

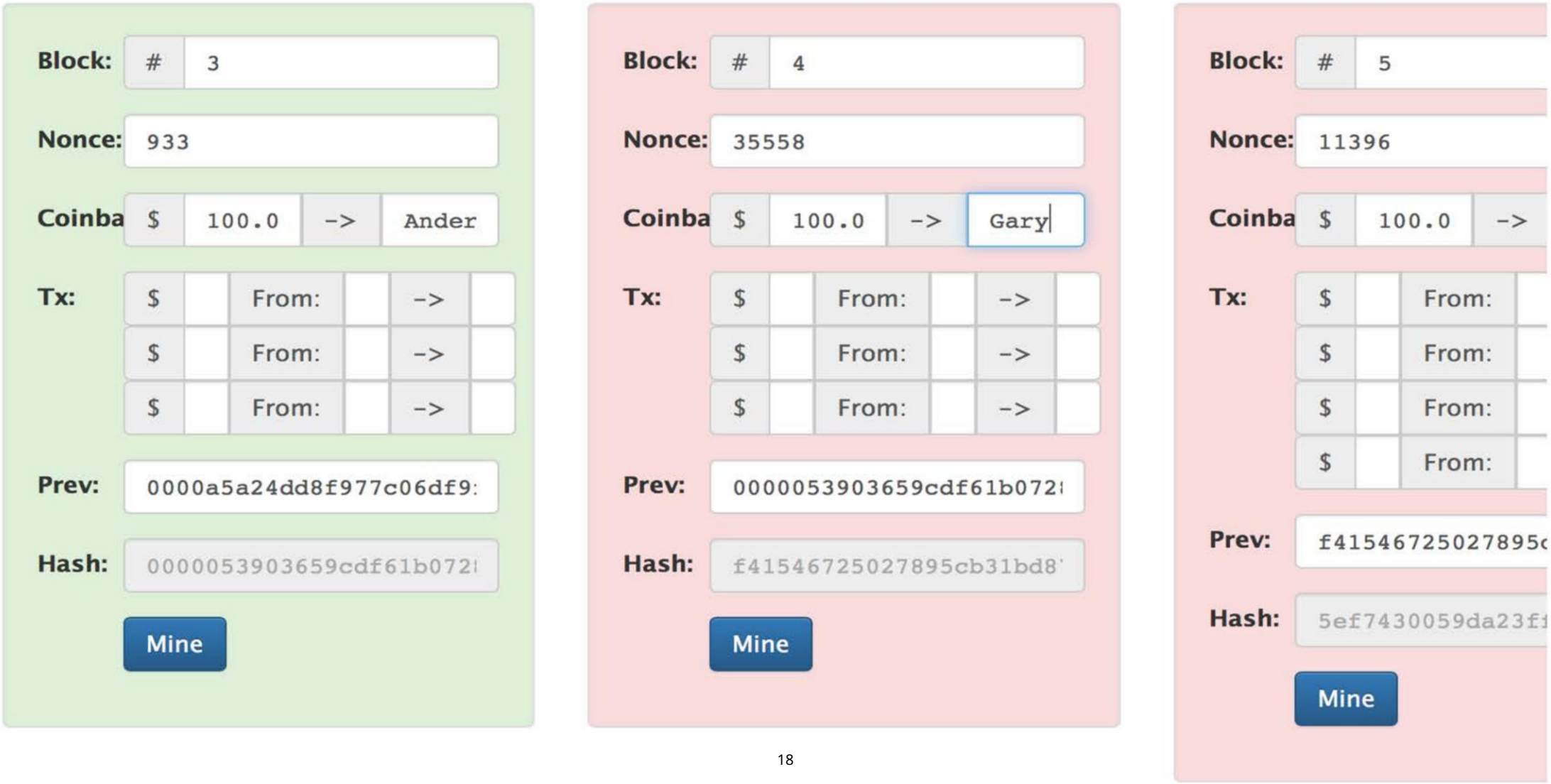


Блокчейн – доказателство за работа



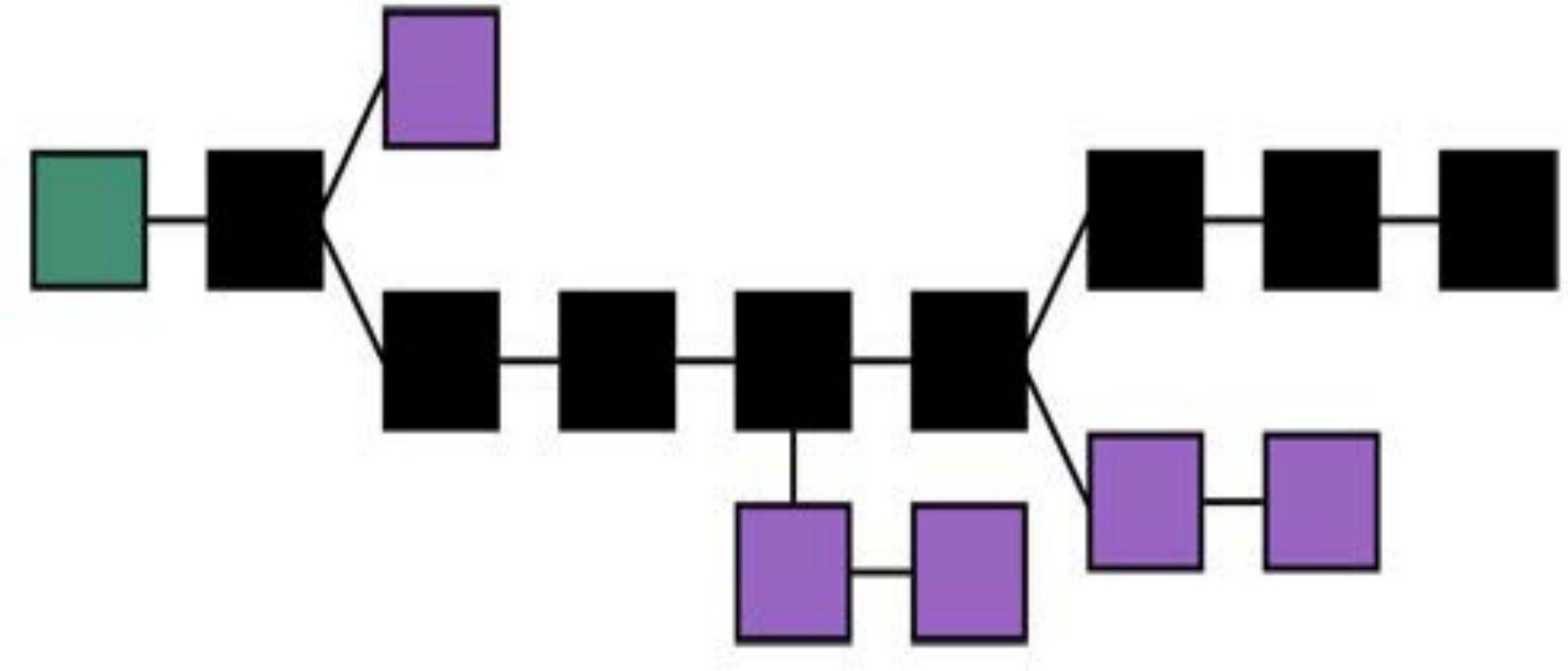
Изображение от Anders Brownworth. Използва се с разрешение.

Блокчейн – доказателство за работа



Изображение от Anders Brownworth. Използва се с разрешение.

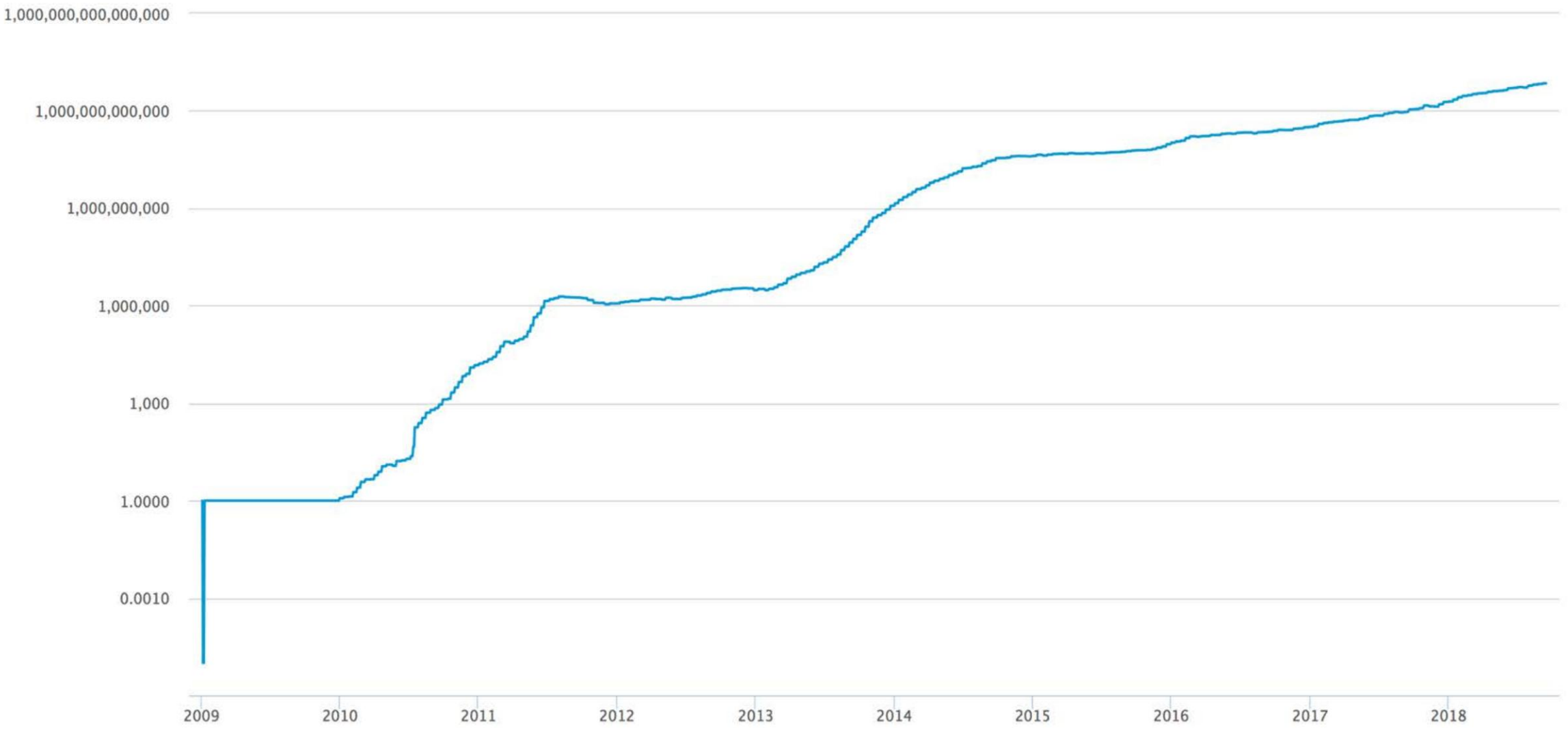
Blockchain – Consensus поддържа най-дългата верига



Биткойн доказателство за трудна работа

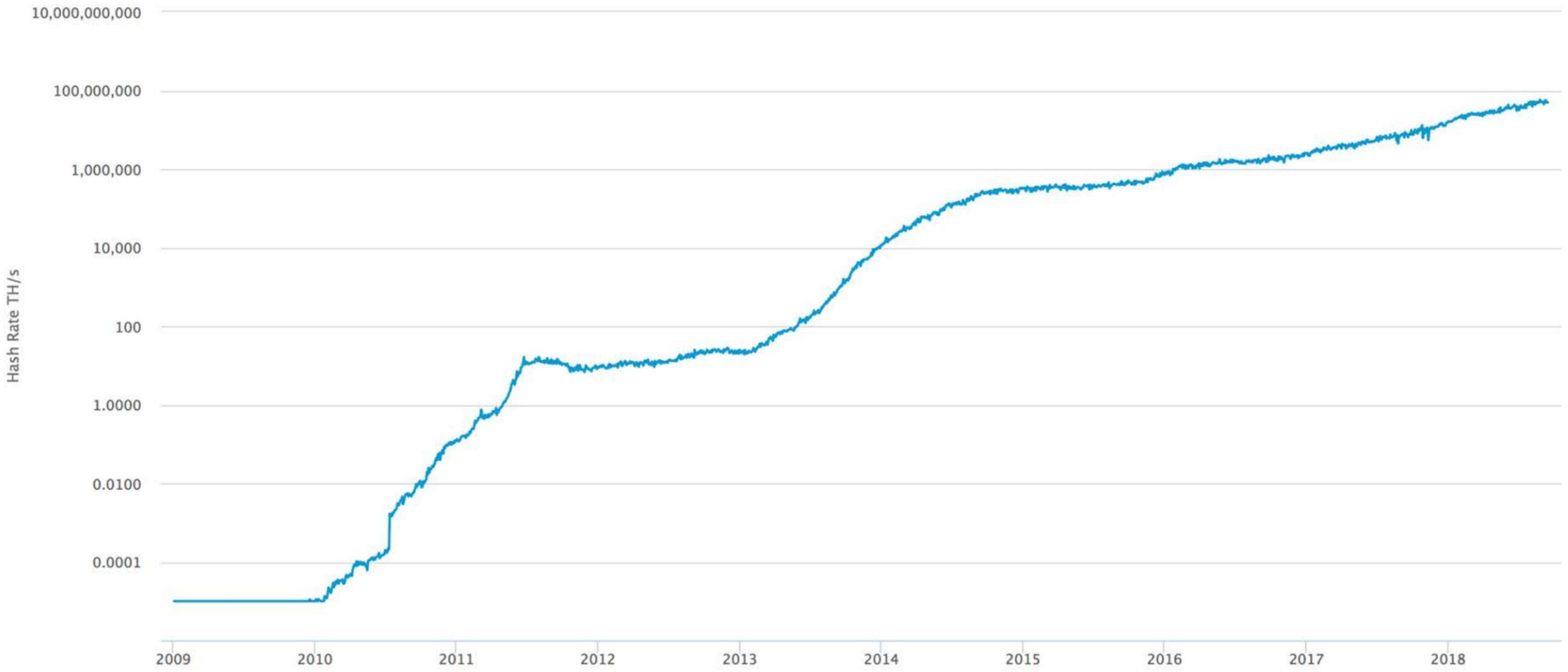
- Цели 10 минути средно време за генериране на блок
- Определя се от броя на водещите нули. Хеш изходът изисква за решаване на доказателство за работа
- Коригира се на всеки 2016 блока - приблизително на всеки две седмици
- В момента > 18 водещи нули (от 64 шестнадесетични знака)
- Блок 541974 (9/18/18) - 18 водещи нули
  000000000000000001104a863046dfbad1a294112881566962 3ff93c2a3945f
- Genesis Block (1/3/09) – 10 водещи нули, но са необходими само 8
  000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Трудност при копаене на биткойни



Източник: Blockchain.com

Хеш-рейт на биткойн мрежата



Източник: Blockchain.com

Еволюция на копаене на биткойни

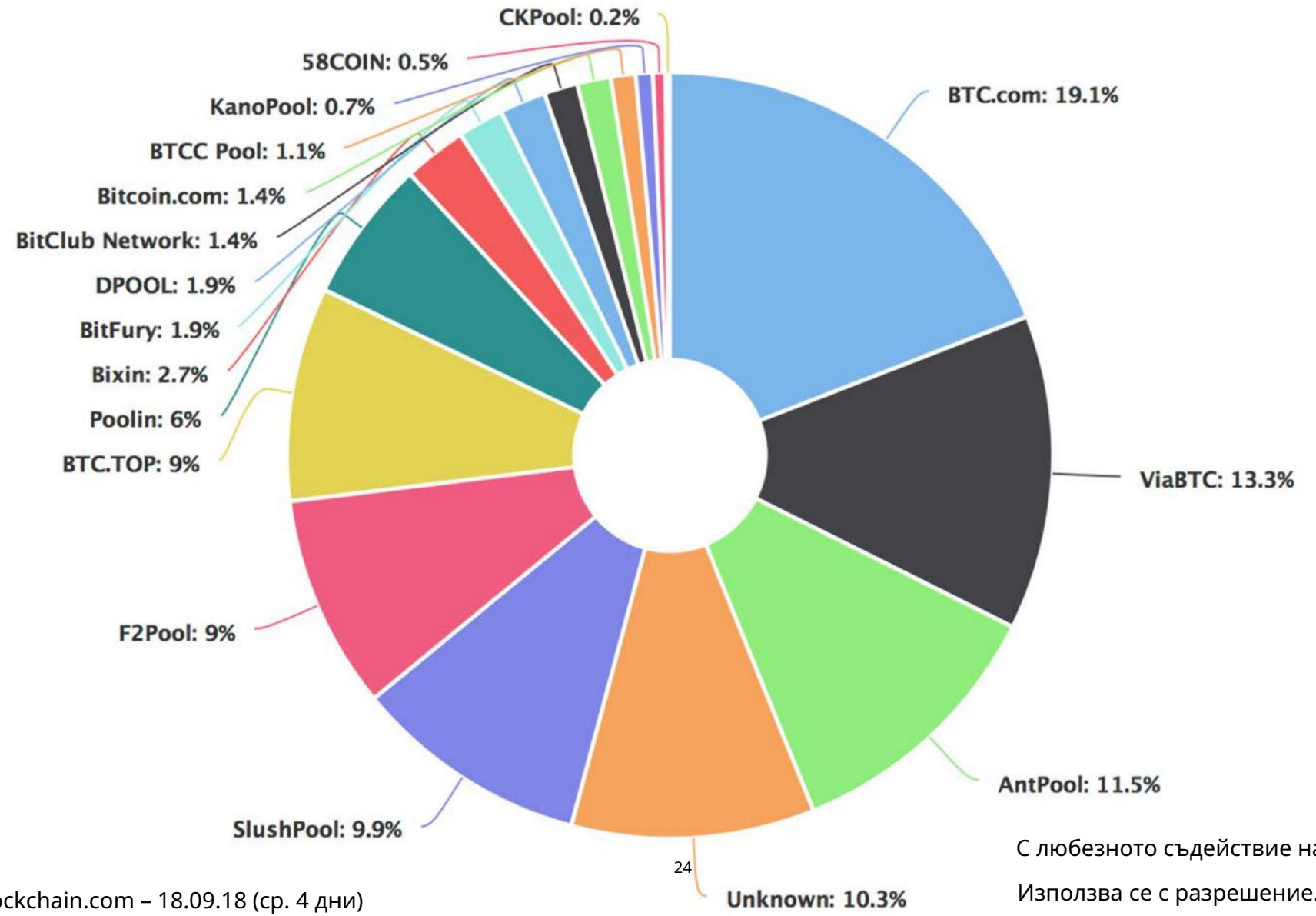
Централни процесори
(CPU) 2009 – 2010 г
2 - 20 MH/S

Графични процесори
(GPU) 2010 – 2013 г
20 - 300 MH/S

Специфична интегрална схема за приложение
(ASIC) 2013 – 2018 г
4 – 16 TH/S

Модерна минна фабрика

Разпределение на хешрейта за копаене на биткойни



Източник: Blockchain.com – 18.09.18 (ср. 4 дни)

Родна валута

Система за икономически стимули

„Паричните политики“ се различават значително

• Биткойн - BTC •

Създаден чрез транзакция на Coinbase във всеки блок • Предварително зададена „Парична политика“ в Bitcoin Core • Създаване първоначално 50 биткойна на блок • Награда наполовина (1/2s) на всеки 210 000 блока • В момента създадени 12,5 BTC на блок – следователно „инфлация“ ' 4,1% • В момента 17,3 милиона BTC; ограничение до 21 милиона BTC през 2040 г. • Пазарен механизъм за такси за транзакции също е предвиден в Bitcoin Core •

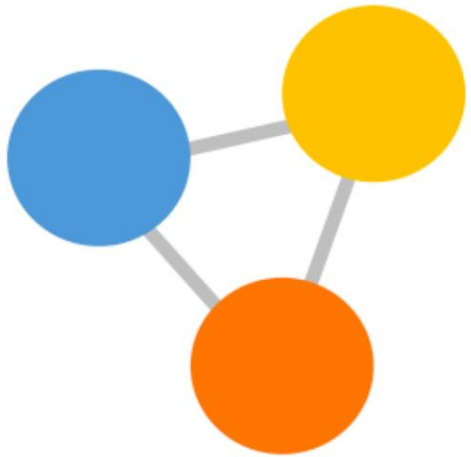
Ethereum • В момента 3 ETH на блок – следователно „инфлация“ 7,4% • Скорошно предложение за намаляване на 2 ETH на блок през 11/18 • Такси платени в газ (109 газ на ETH) за изчисление се кредитират на миньорите

мрежа

- Пълни възли – Съхранявайте пълния блокчейн и можете да валидирате всички транзакции
- Подрязване на възли – Отрязване на транзакции след валидиране и остаряване
- Леки възли – възли за опростена проверка на плащанията (SPV) – Магазин
  Само заглавки на блокчейн
- Копачи – Извършва доказателство за работа и създава нови блокове – Не е необходимо да сте а
  Пълен възел
- Оператори на майнинг пул
- Портфейли – съхранявайте, преглеждайте, изпращайте и получавайте транзакции и създавайте двойки ключове
- Mempool – Съвкупност от непотвърдени (все още валидирани) транзакции

Алтернативни консенсусни протоколи

Обикновено произволен или делегиран избор на възли за валидиране на следващия блок • Може да има добавен механизъм за потвърждаване на работата на валидаторите на блокове



Рандомизираният избор може да се основава на: • Доказателство за залог – залог в местна валута

• Доказателство за дейност - Хибрид на POW и POS

• Доказателство за изгаряне – Валидирането идва с изгаряне на монети

• Доказателство за капацитет (съхранение или пространство) – въз основа на хардуерно пространство

Делегираният избор може да се основава на многослойна система от възли

Основните блокчейн приложения без разрешение все още използват доказателство за работа – въпреки че: • DASH е хибрид на POW с многостепенна система от „Masternodes“

• NEO използва делегиран протокол на „Професионални възли“

Клас 5 (9/20): Учебни въпроси

- Как Биткойн записва транзакции? Какво е неизразходван изход от транзакция (UTXO)? Какъв е скрипт кодът, вграден във всяка биткойн транзакция и колко гъвкав език за програмиране е той? (Преместено от 18 септември)

- Тъй като много функции на дизайна – криптография с публичен ключ, хеш функции, регистрационни файлове с времеви печат само за добавяне, цифрови пари и доказателство за работа – съществуват преди биткойн, каква беше новата иновация на Сантоши Накамото?

- Кой е Сатоши Накамото? (Само се шегувам малко.)

5 клас (9/20): четения

- „Академичното родословие на биткойн“ Нараянан и Кларк
- „Осъзнаване на криптоикономиката“ CoinDesk

Изводи

Прегледани характеристики на дизайна на

биткойн • Регистрационни файлове само за добавяне

(блокове) с клеймо за време • Защитени чрез криптографски хеш функции и цифрови

Подписи

Децентрализиран мрежов консенсус

• Консенсус чрез доказателство за работа •

Родна валута • Мрежа

Регистъри на транзакции

• Входящи и изходни данни за транзакции

• Комплект неизразходвани изходни данни за

транзакции (UTXO) • Скриптов език

15.S12 Блокчейн и пари

Есен 2018г

15.S12 Блокчейн и пари

Есен 2018г