блокчейн и Пари

клас 5

20 септември 2018 г

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?

- Тъй като много дизайнерски характеристики са предшестващи биткойн, какво беше новото 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

Общ преглед на клас 5

• Входящи и изходящи транзакции

• Неизразходвани изходни транзакции

(UTXO) • Скриптов език

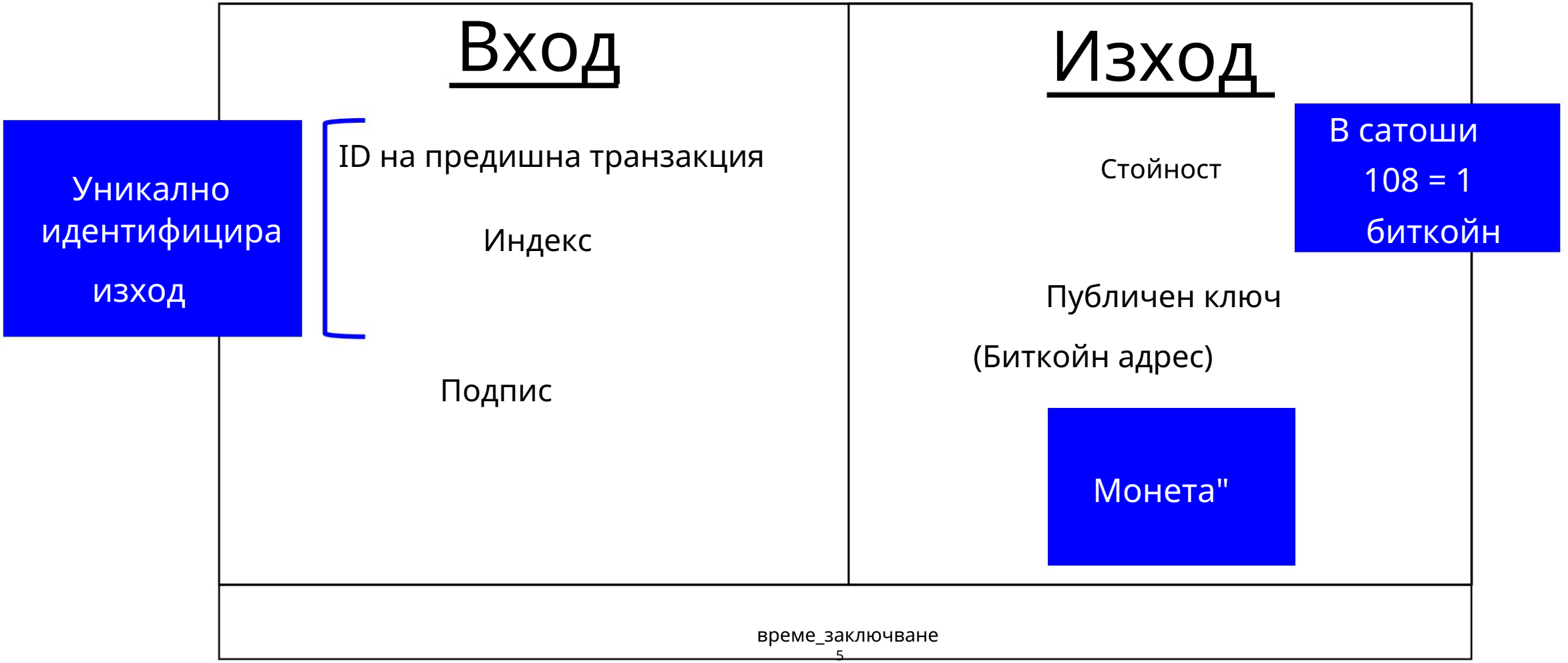
• Блокчейн дизайн – обединяване на всичко •

Академичното родословие на Биткойн

• Кой е Сатоши Накамото?

• Изводи

Формат на транзакцията

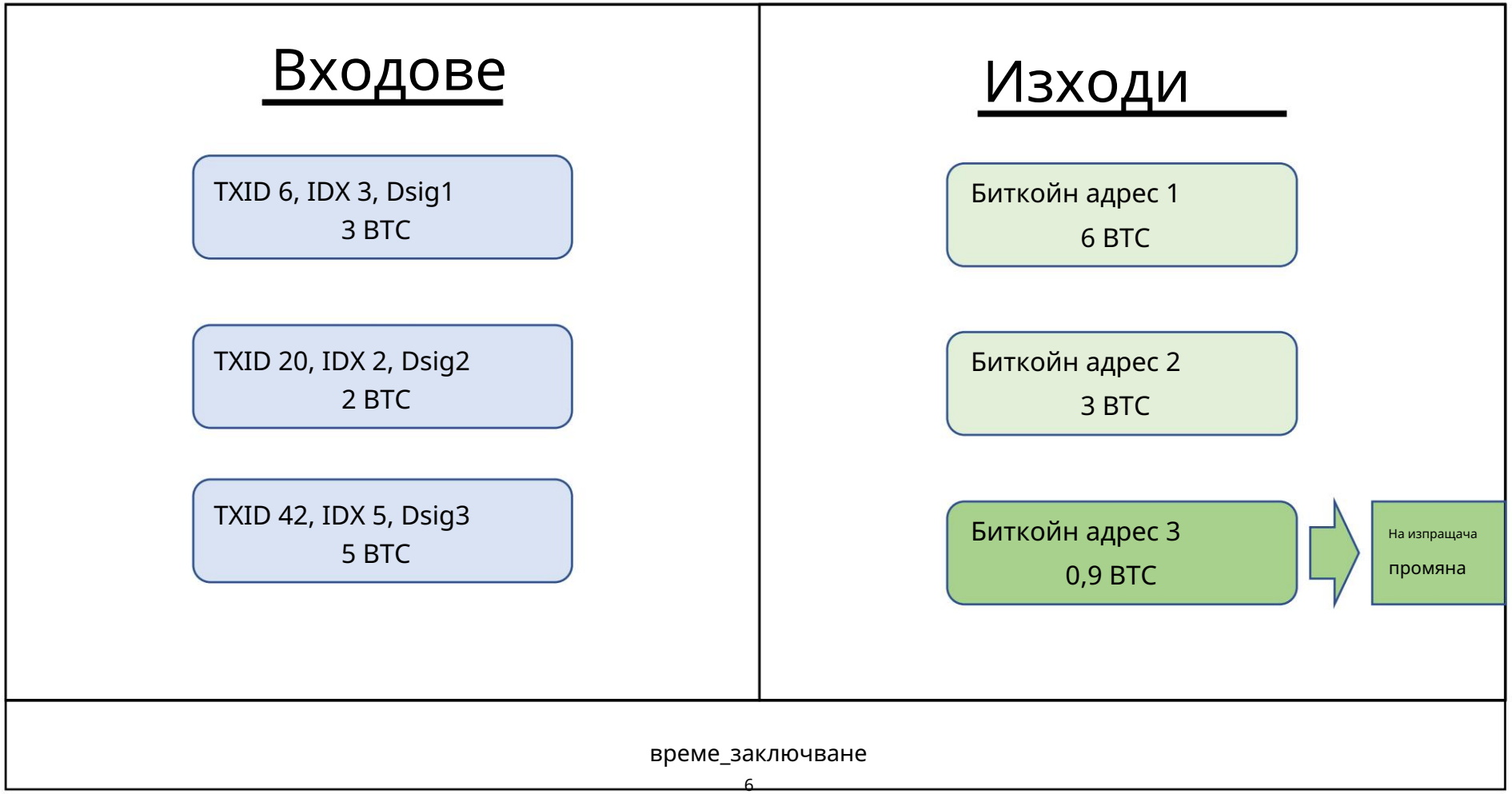


Формат на транзакцията

Множество входове и изходи

Входове > Изходи

Входове – Изходи = Такси



Транзакция на Coinbase

Награда за решаване на доказателство за работа

- Само въвеждане е наградата за блок Coinbase
- Награда наполовина (1/2s) на всеки 210 000 блока • В момента 12,5 биткойна на блок • Първоначално 50 биткойна на блок
- Изходът не може да се използва като вход за транзакция до още 100 блока
- Записана като първа транзакция в Merkle Tree
- Може да включва 100 байта произволни данни
  - Използва се за допълнителен Nonce
  - Включен блок Genesis Заглавие от Financial Times:

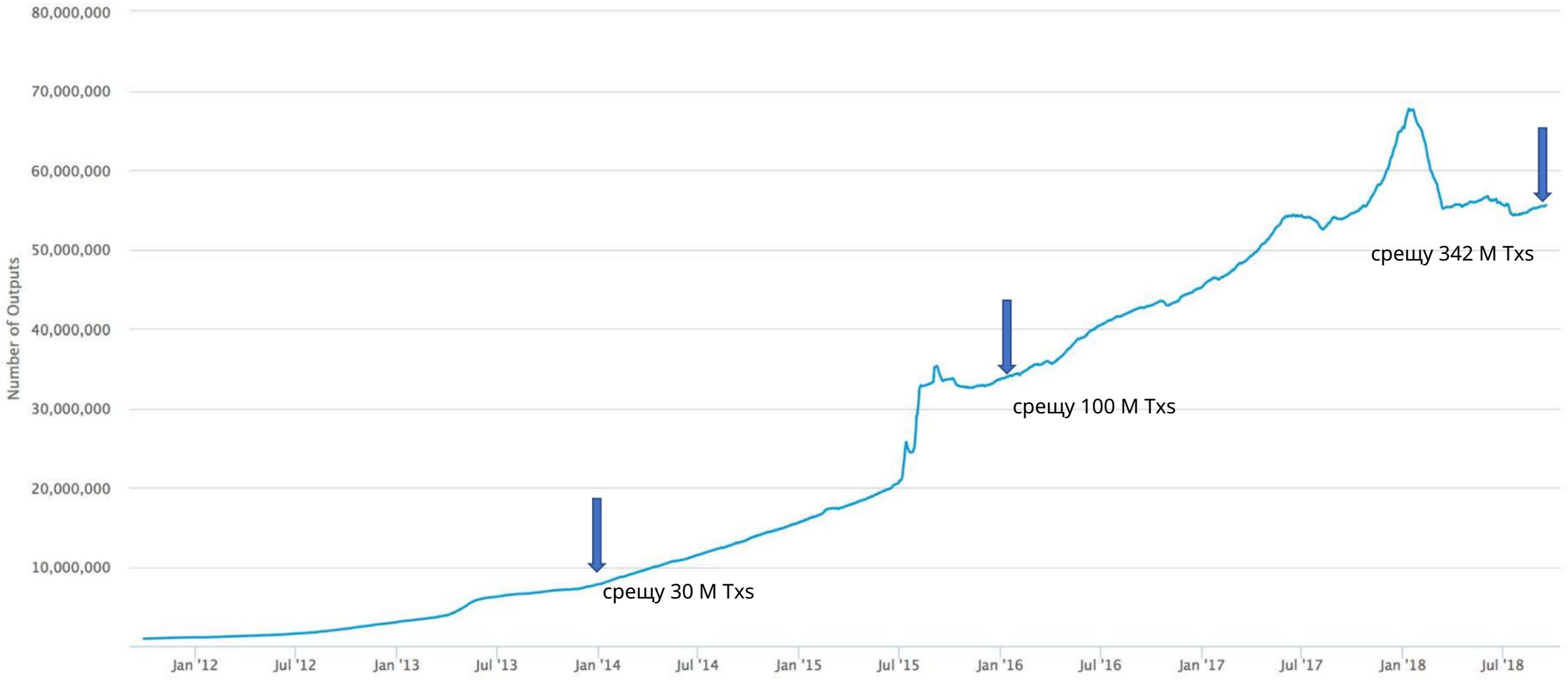
„Таймс 03/Януари 2009 г. Канцлерът е на прага на втория спасителен план за банките“

Задаване на неизразходван резултат от транзакция (UTXO).

Резултати от биткойн транзакции, които не са изразходвани в даден момент

- Съдържа всички текущо неизразходвани резултати от транзакции
- Ускорява процеса на валидиране на транзакция
- Съхранява се с помощта на база данни LevelDB в Bitcoin Core, наречена „chainstate“

Задаване на неизразходван резултат от транзакция (UTXO).



Източник: Blockchain.com – 17.09.18

биткойн скрипт

Програмен код, използван за транзакции

- Базиран на стек код, без цикли (не е пълен с Turing)

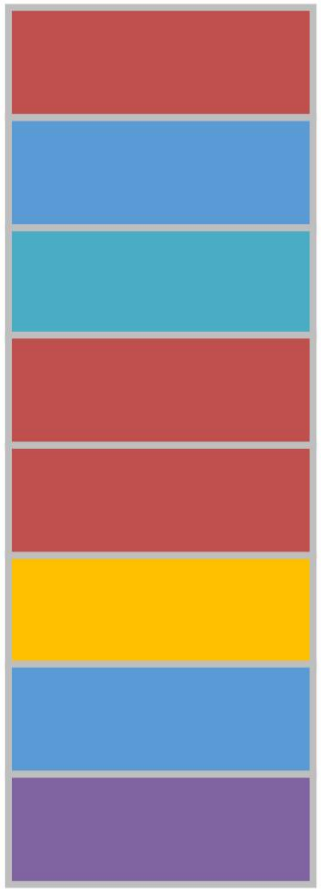
- Осигурява гъвкав набор от инструкции за валидиране на транзакция и
  Удостоверяване на подписа

- Най-често срещаните типове скриптове в
  UTXO: • Транзакция, изпратена до хеш на биткойн адрес – „Pay-to-
  PubkeyHash“ (81%) • Транзакция, изпратена до хеш на условен скрипт – „Pay-to-
  ScriptHash“ (18%) • Транзакция предмет на множество подписи – „M of N
  Multisig“ (0,7%) • Транзакция, изпратена до биткойн адрес – „Pay-to-Pubkey“ (0,1%)
  (Източник: Перес-Сола, Делгадо-Сегура и др.)

Блокчейн технология

регистрационен файл

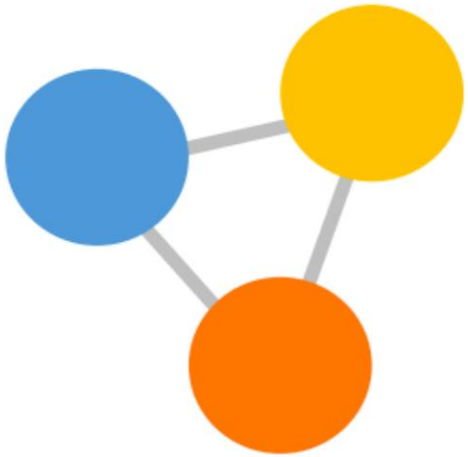
само за добавяне с клеймо за време



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

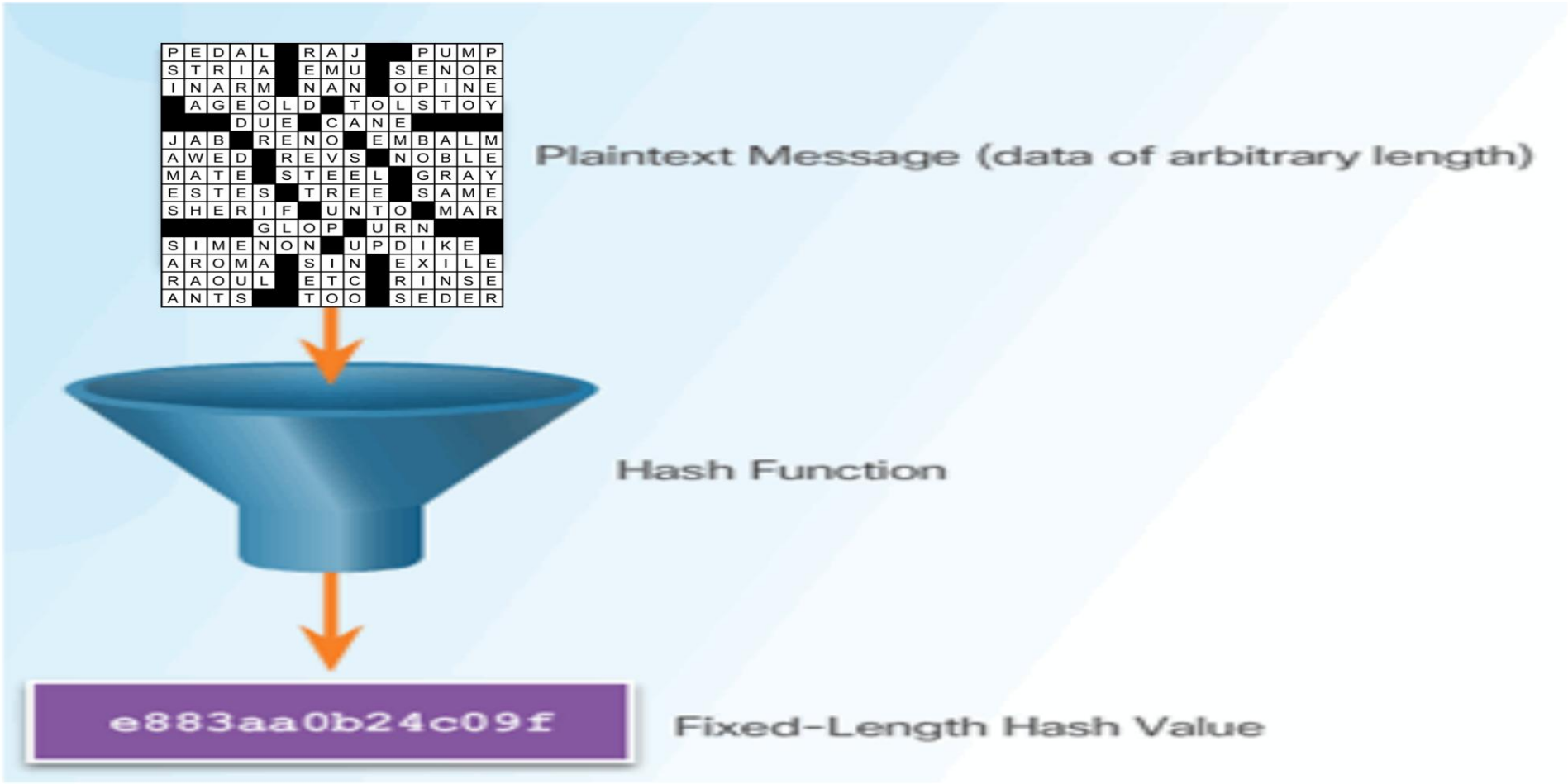
• Без разрешение

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

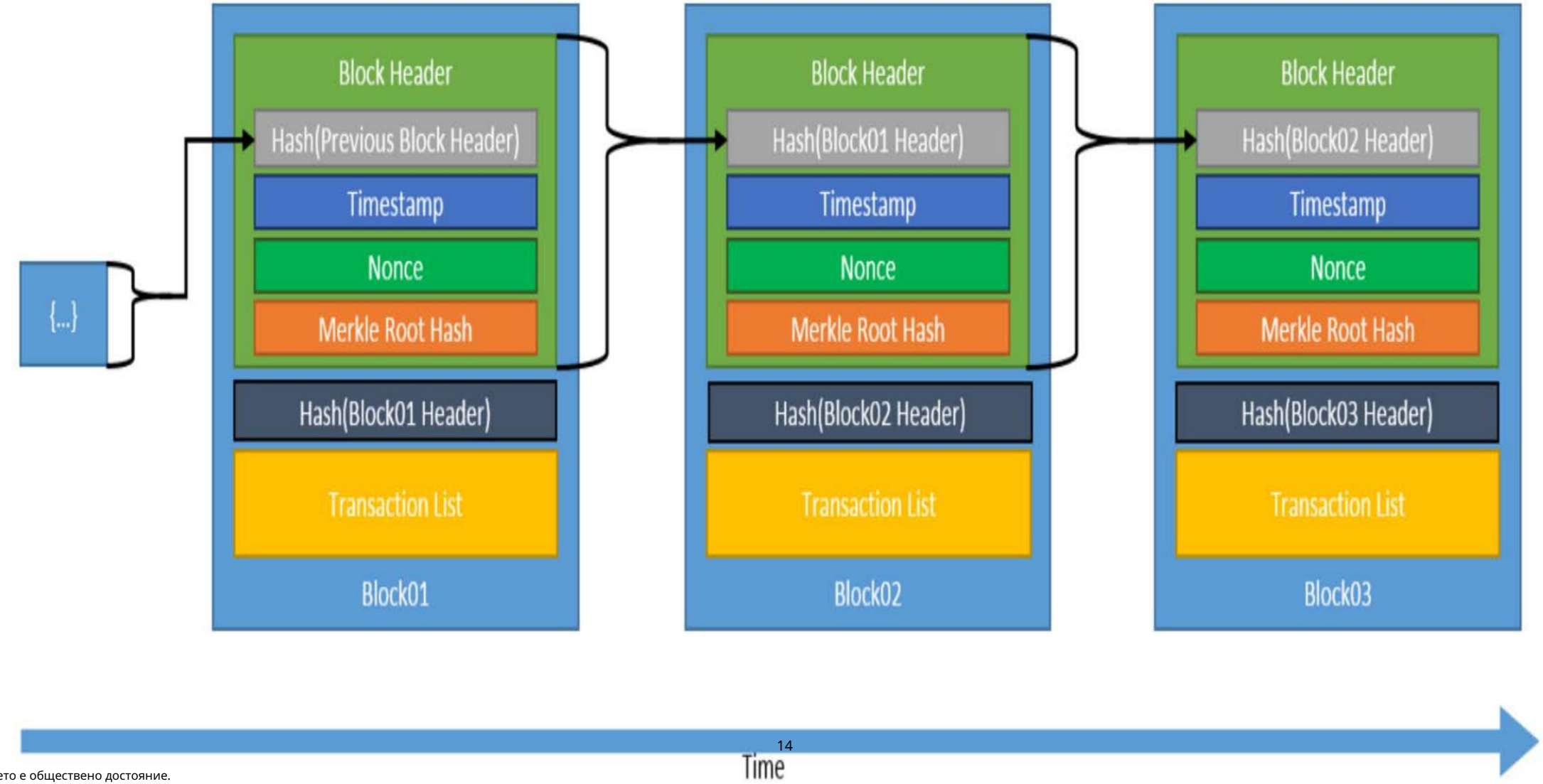
Криптографски хеш функции

Еднопосочна компресия на данни

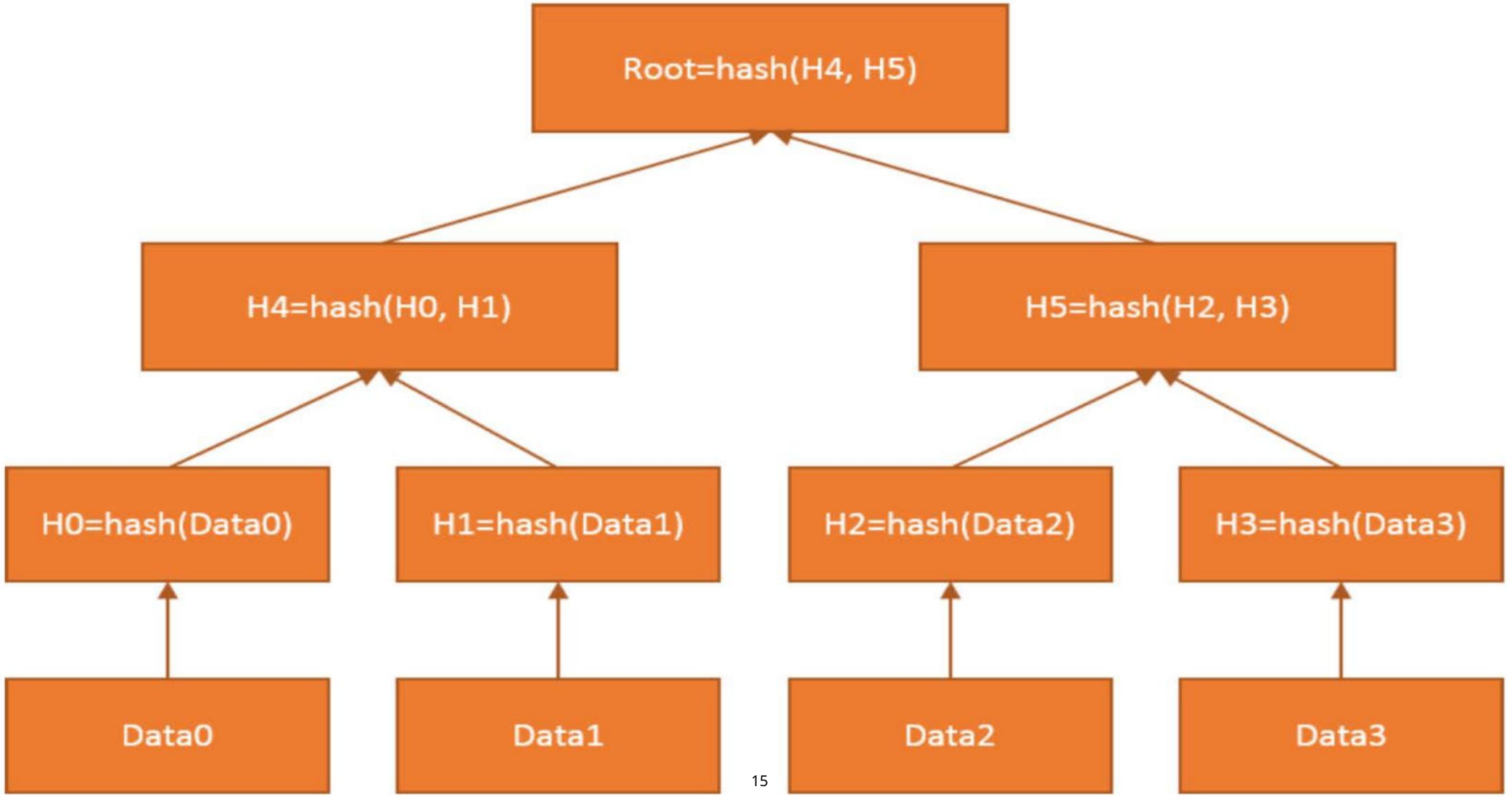


Ангажимент за данни

Дневник само за добавяне с клеймо за време - Blockchain



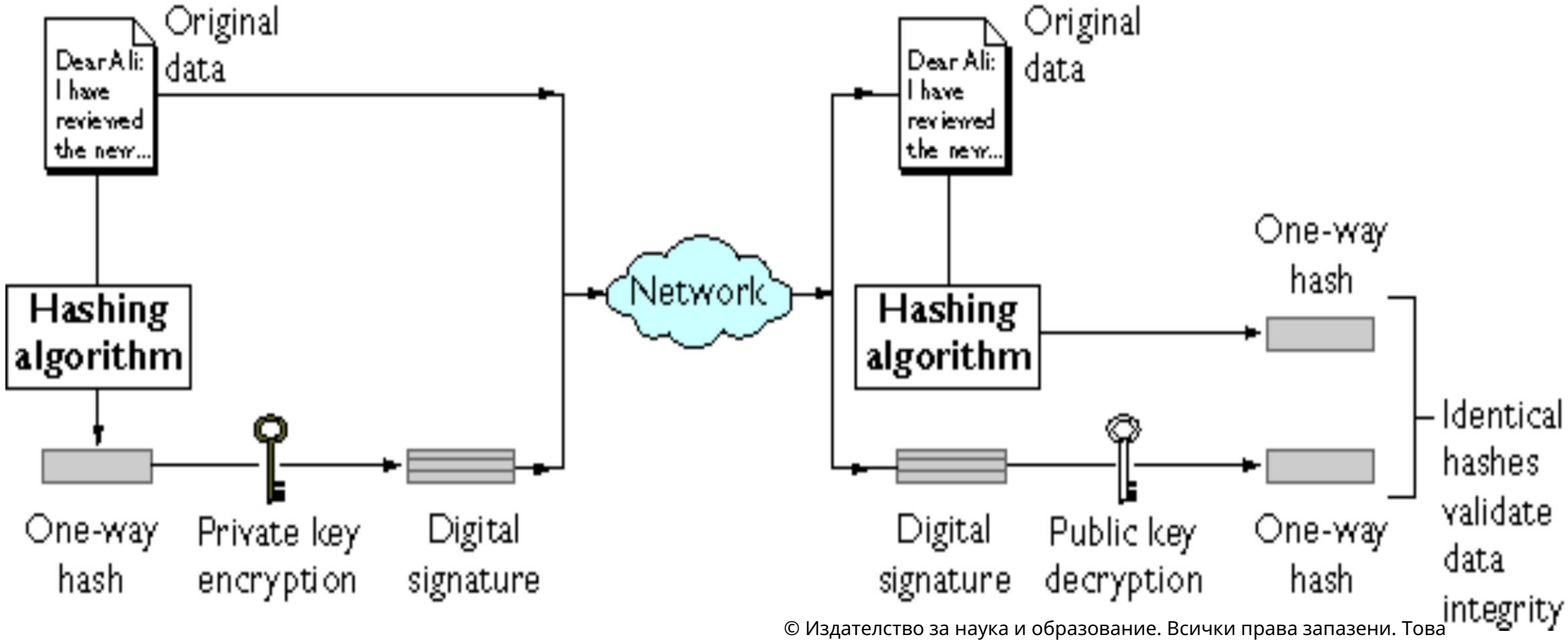
Merkle Tree – Двоично дърво с данни с хешове



Асиметрична криптография и цифрови подписи

Защита срещу подправяне и представяне под чужда самоличност

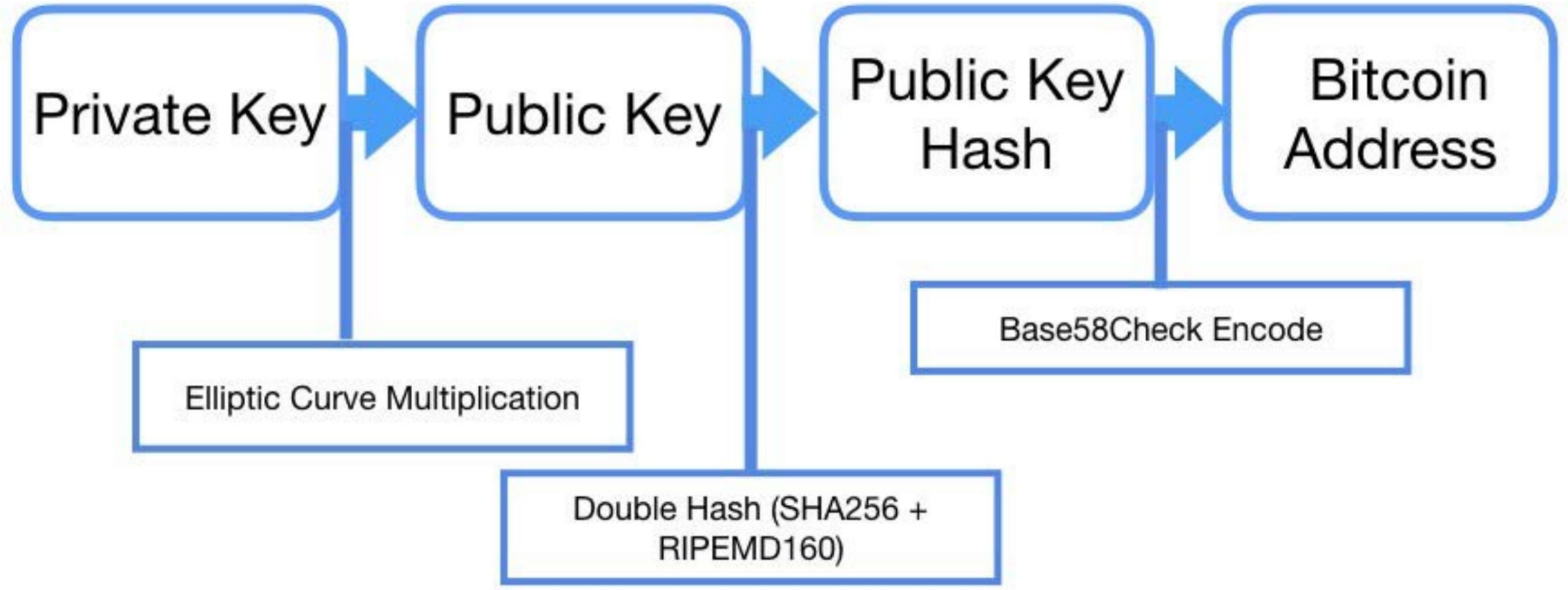
Цифров подпис с хеш



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

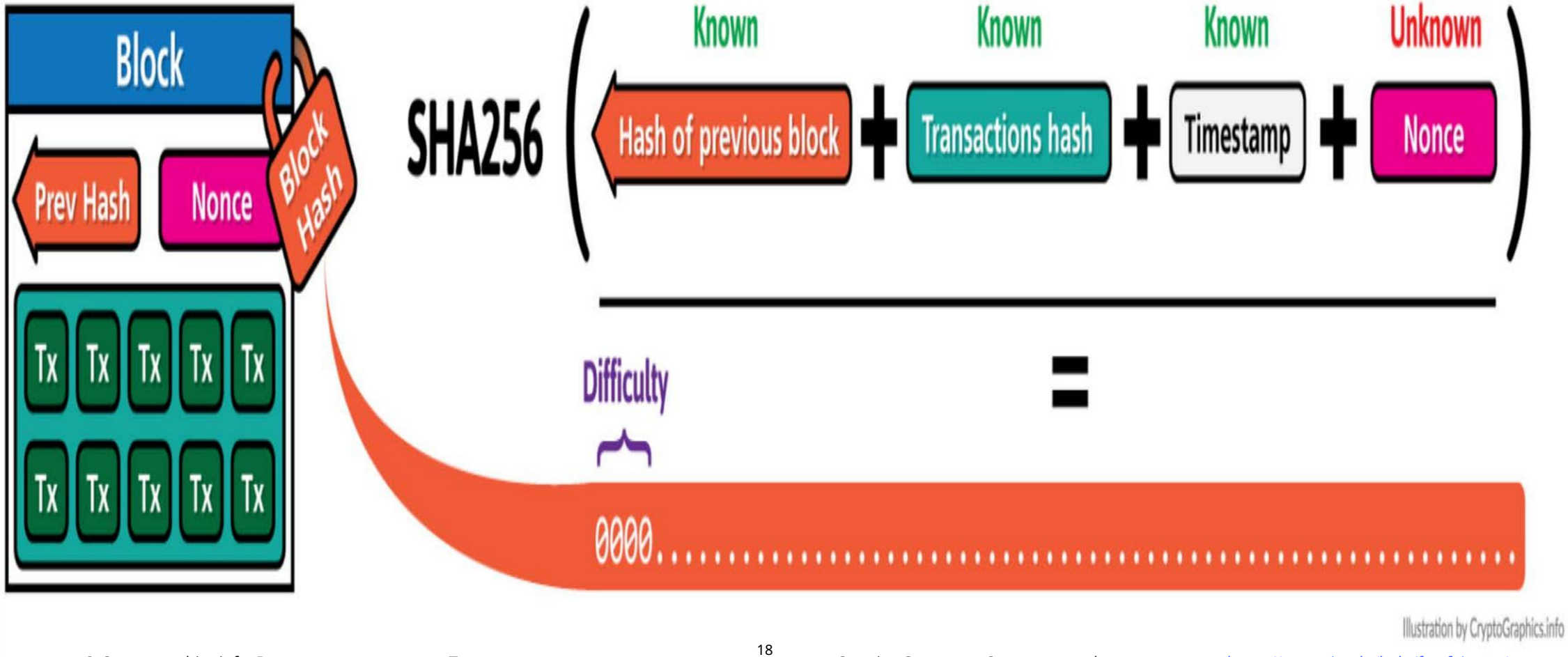
Биткойн адрес

Определя се от – но не идентичен с – Публичен ключ



Блокчейн – доказателство за работа

Верижно доказателство за работа за разпределен мрежов консенсус и времево клеймо



Родна валута

Система за икономически стимули

- Биткойн – BTC

  • Награда, създадена чрез транзакция на Coinbase във всеки блок • Обща „парична политика“ предварително зададена в Bitcoin Core • Награда наполовина (1/2s) на всеки 210 000 блока • В момента 17,3 милиона BTC; ограничаване на 21 милиона BTC през 2140 г. • Пазарен механизъм за такси за транзакции, също предвиден в софтуера

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

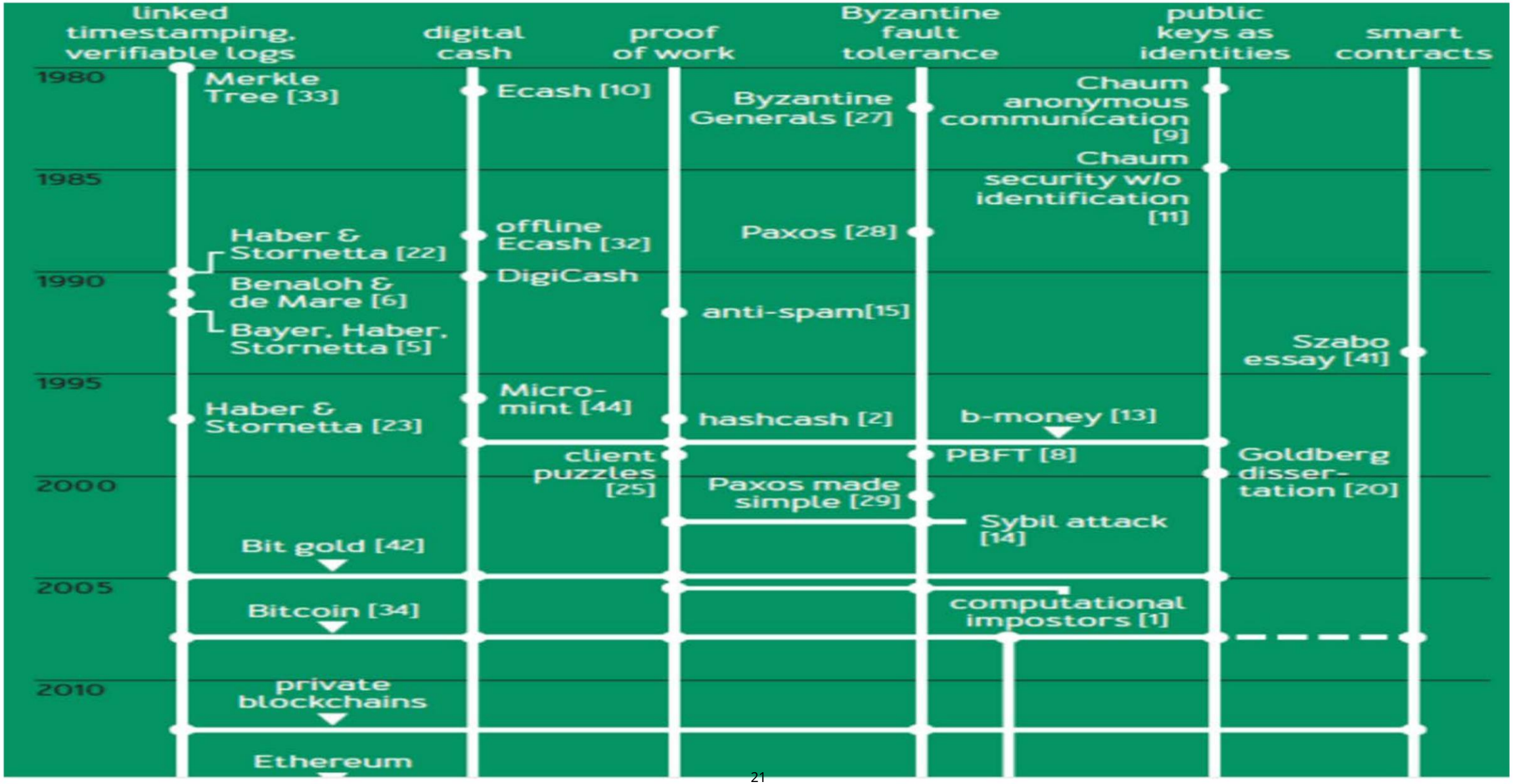
• Копачи – Извършва доказателство за работа и създава нови блокове – Не е необходимо да сте а
Пълен възел

• Оператори на майнинг пул

• Портфейли – съхранявайте, преглеждайте, изпращайте и получавайте транзакции и създавайте двойки ключове

• Mempool – Съвкупност от непотвърдени (все още валидирани) транзакции

Хронологията на идеите в Биткойн на Нараянан и Кларк



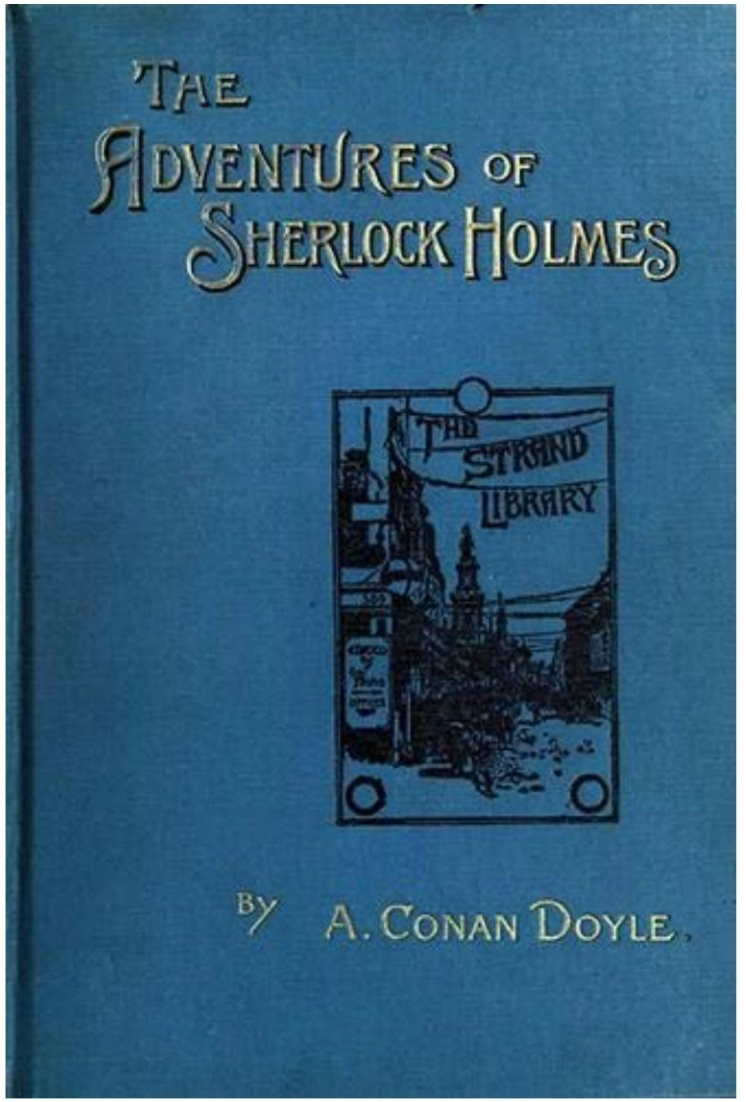
Кой е Сатоши Накамото?

Резултати от ad hoc анкета на студенти

Група, ръководена от Хал Фини
Ник Сабо

Крейг Райт
Дориан Накамото

Държавен актьор - Правителство на САЩ (NSA) или друго



Клас 6 (9/25): Учебни въпроси

- Какво представляват интелигентните договори? Как се сравняват с традиционните договори? Какво представляват токените?

- Какво представляват платформите за интелигентни договори като Ethereum? Какво като цяло ги отличава от Bitcoin?

- Какво представляват децентрализираните приложения (DApps)? Каква е била употребата и защо нито едно DApps все още не е получило широк потребител осиновяване?

6 клас (9/25): четения

Задължително

• Камара за цифрови технологии „Интелигентни договори: 12 случая на използване за бизнеса и извън него“
Търговия

• „Състояние на Dapps: 5 наблюдения от данни за употреба“ McCann •

„Конкуренти на Ethereum: Ръководство за алтернативните платформи за интелигентни договори“
Blockonomi

По избор

• „Интелигентни договори: градивни елементи за цифрови пазари“ Szabo •

„Интелигентен договор от следващо поколение и децентрализирана платформа за приложения“
Ethereum

• „Блокчейн технологията като регулаторна технология“ De Filippi & Hassan

Гост-лектор – Лари Лесиг

• Харвардски професор по право и лидерство. •
Основател на Stanford Law's Center for Internet and Society. •
Сътрудник на съдията Антонин Скалия и на съдията от Апелативния съд Ричард Познър.
• Наградите включват наградата за свобода на Фондацията за свободен софтуер, наградата Fastcase 50 и определянето на един от 50-те най-добри визионери на Scientific American.

„Код и други закони на киберпространството“

• Код/архитектура – физически или технически ограничения
• Пазар – икономически сили
• Закон – изрични мандати от правителството
• Норми – социални конвенции

Изводи

• Биткойн на Накамото ни донесе технологията Blockchain

• Блокчейн технологията е част от дългата история на Money & Ledgers

• Неговите дизайнерски характеристики също могат да бъдат поставени в историята на технологиите • Регистрационни файлове само за добавяне (блокове) с клеймо за време • Криптографски хеш функции и цифрови подписи • Мрежов консенсус

• Ключова иновация – децентрализиран верижен консенсусен протокол

• Адресира „Разходите за доверие“

• Осигурява Peer-to-Peer алтернатива за пари, книги и изчисления

15.S12 Блокчейн и пари

Есен 2018г