блокчейн и Пари

клас 7

27 септември 2018 г

Общ преглед на клас 7

- Въпроси за четене и изучаване
- Технически характеристики на блокчейн
- Рамка за сравняване на разходите и компромисите от децентрализацията
- Предизвикателства с блокчейн технологията
- Трилема на Бутерин
- Възможни решения за мащабируемост, ефективност, поверителност и оперативна съвместимост
- Управлението е най-предизвикателно
- Заключение

7 клас (9/27): четения

Задължително • Глава 2 „Доклад от Женева“ (страници 9 – 16); Кейси, Крейн, Генслер, Джонсън и Нарула

• „Относно мащабируемостта на блокчейните“ Контролът • „Скорости на транзакции: Как скоростите на криптовалутите се натрупват до Visa или PayPal?,“

Колко.net

• „Layer 2 / the Lightening Network“ Инициатива за цифрова валута • „Топ 8 монети за поверителност“ Инвестирайте в блокчейн

По избор

• „Относно шардинг блокчейни“ Ethereum Wiki •

„zkLedger: Одит за запазване на поверителността за разпределени счетоводни книги“ Narula , Vasquez & Virza

Клас 7 (9/27): Учебни въпроси

- Колко критични са техническите и търговски предизвикателства – мащабируемост, ефективност, поверителност, сигурност, оперативна съвместимост – на текущата блокчейн технология?

- Какви са възможните компромиси от децентрализацията, скалируемостта и сигурност? Какви са компромисите от консенсусните софтуерни актуализации, управлението и така наречените „хард форкове“?

- Какво може да работи в момента – приложения от слой 2, нулево знание доказателства, алтернативни консенсусни алгоритми – какво да се направи за справяне с текущите търговски предизвикателства?

Блокчейн – 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

- Код на транзакция и счетоводни книги

  • Входове и изходи на транзакции или преходи на състояния •
  Зададени неизразходвани изходни данни на транзакции (UTXO) или
  базирани на акаунт • Скрипт, Solidity или други езици за програмиране 5

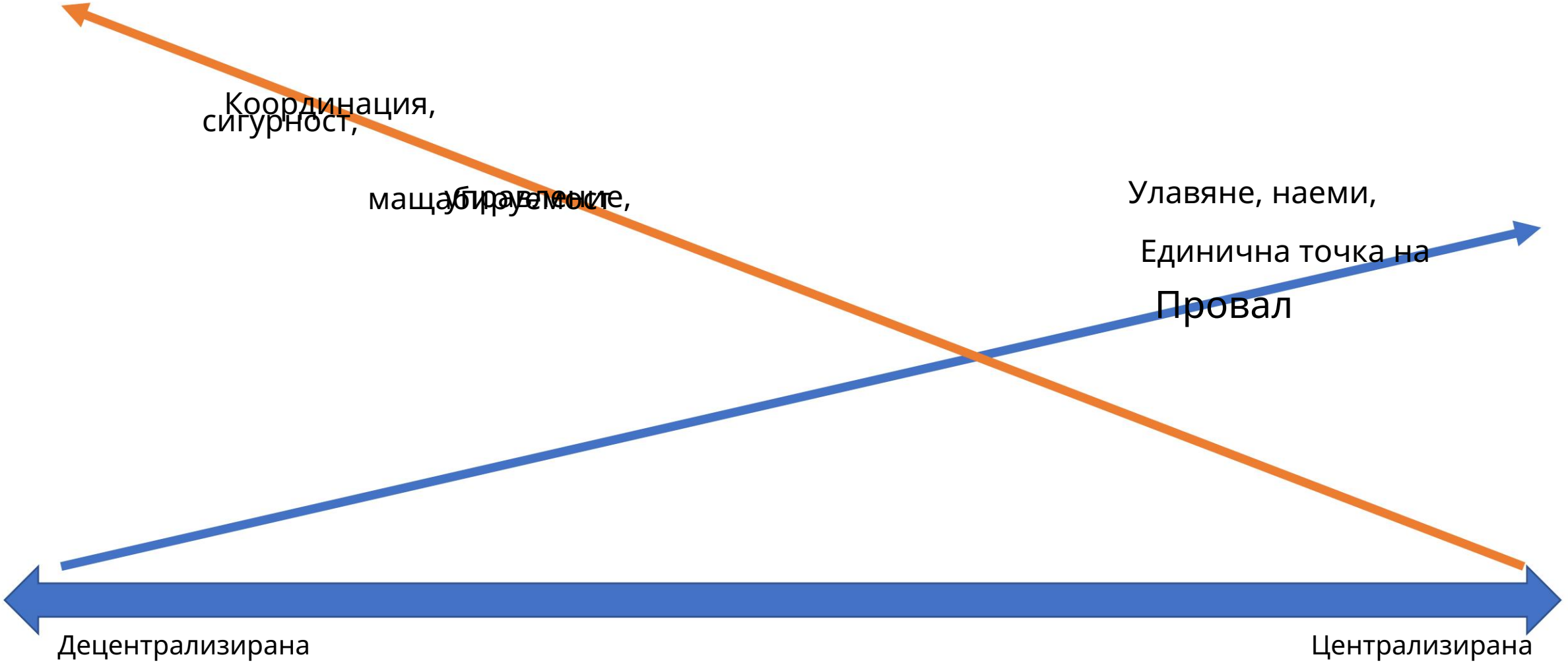
Дизайн на Bitcoin и Ethereum

• Основател: Сатоши Накамото	⟷	Ваталик Бутерин
• Генезис: януари 2009 г	⟷	юли 2015 г
• Код: Non Turing (Скрипт)	⟷	Turing Complete (солидност, Serpent, LLL или Mutan)
• Книга: UTXO – Транзакция	⟷	Държава - Въз основа на сметка
• Merkle Trees: Транзакции	⟷	Транзакции, състояние, съхранение, Разписки (без еднократни)
• Време за блокиране: 10 минути	⟷	14 секунди
• Консенсус: Доказателство за работа	⟷	Доказателство за работа
• Хеш функция: SHA 256	⟷	Ethash

Дизайн на Bitcoin и Ethereum

• Валута: биткойн •	⟷	ETH
Копаене: ASIC • Хешрейт:	⟷	GPU
54 Exahash/S	⟷	260 Terahash/S
• Предварителна продажба: Няма	⟷	ICO и предварително пускане на 72 m ETH
• Награди: 12,5 BTC/блок • Парична	⟷	3 ETH/блок
политика: 1/2s на всеки 210 000 блока (4 години) • Такси: Доброволни	⟷	Коригирано, но промени чрез актуализации (беше 5/блок; предложение до 2)
	⟷	Необходими и базирани на пазара

Рамка за сравняване на разходите и компромисите (Коуз)



Предизвикателства с блокчейн технологията

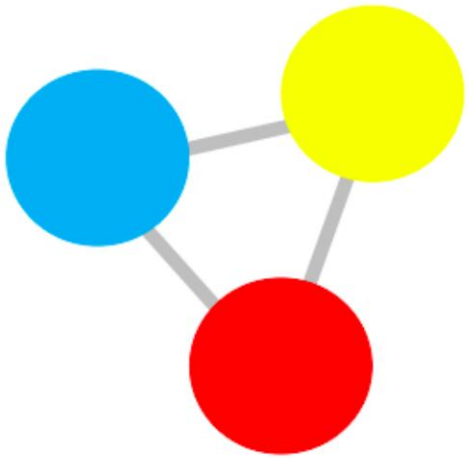
- Производителност, мащабируемост и ефективност
- Поверителност и сигурност
- Оперативна съвместимост
- Управление и колективни действия
- Случаи на търговска употреба
- Обществена политика и правни рамки

9

Трилема на Виталик Бутерин

Децентрализация

Мащабируемост



Сигурност

Производителност, мащабируемост и ефективност

Пропускателна

способност • Bitcoin: 7 – 10 транзакции / сек

• Ethereum: 20 транзакции / сек • Visa: 24

000 / сек • DTCC: до 100 000 / сек

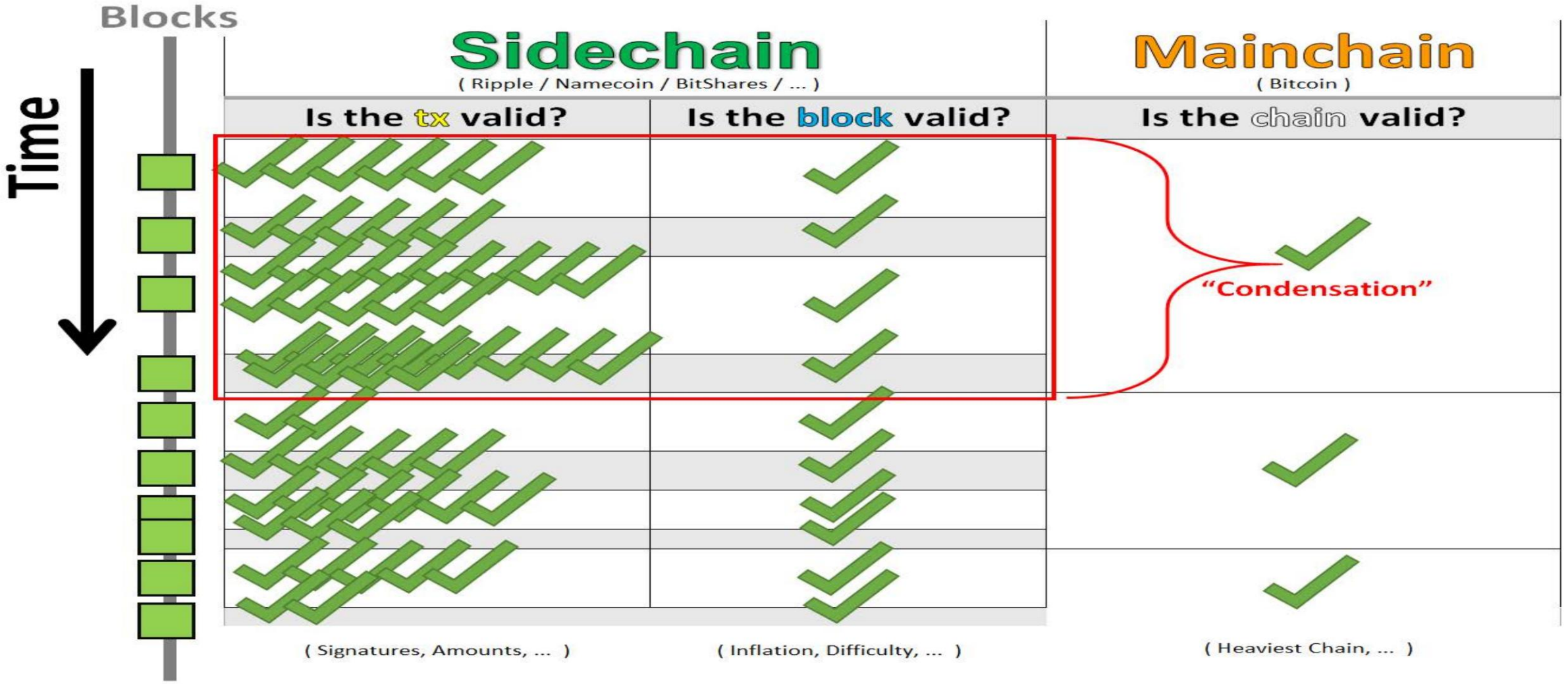
Доказателство за работа Консумация на

енергия • Биткойн: диапазон на прогнозите.

• Digiconomist изчислява 200 милиона Kwh/ден - еквивалентно на потреблението на електроенергия от:

  • 6,8 милиона домове в САЩ, • 0,33% от света, или • Австрия

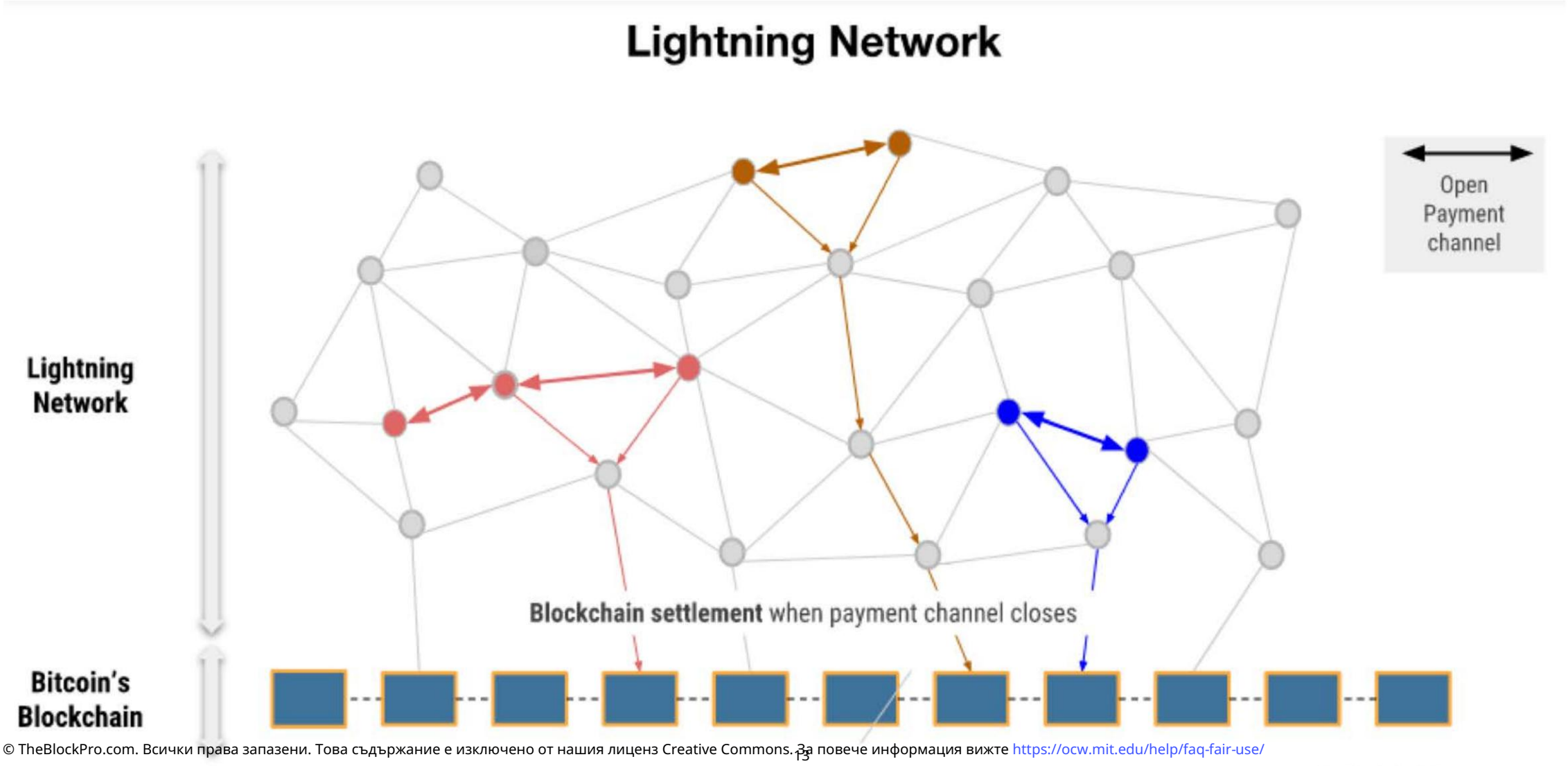
Странични вериги, шардинг, слой 2 и канали за плащане



Изображение от Truthcoin. Използва се с разрешение.

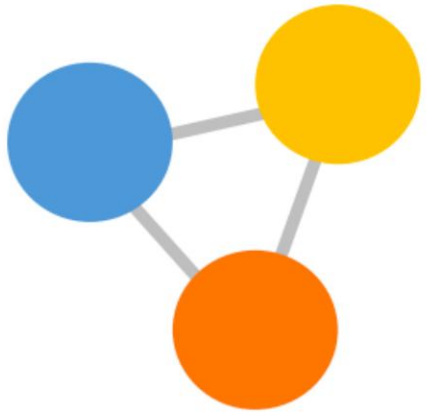
Източник: Truthcoin (11/24/15)

Светкавична мрежа



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



Случайният 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“

Поверителност и сигурност

- Противоречиви напрежения на псевдонимни обръщения
  - Правоприлагащите органи и регулаторите искат повече прозрачност •
    Финансовите институции, регулаторите и някои потребители искат по-малко публична прозрачност

- Притеснения относно неприкосновеността на личния живот Монети и механизми, насърчаващи
  незаконни дейности • Монети: Dash, Monero, Zcash • Механизми: Миксери или чаши

- Предизвикателства пред киберсигурността при съхранение, генериране и съхранение на частни
  ключове • Значителни загуби поради хакове, лошо управление и кражби

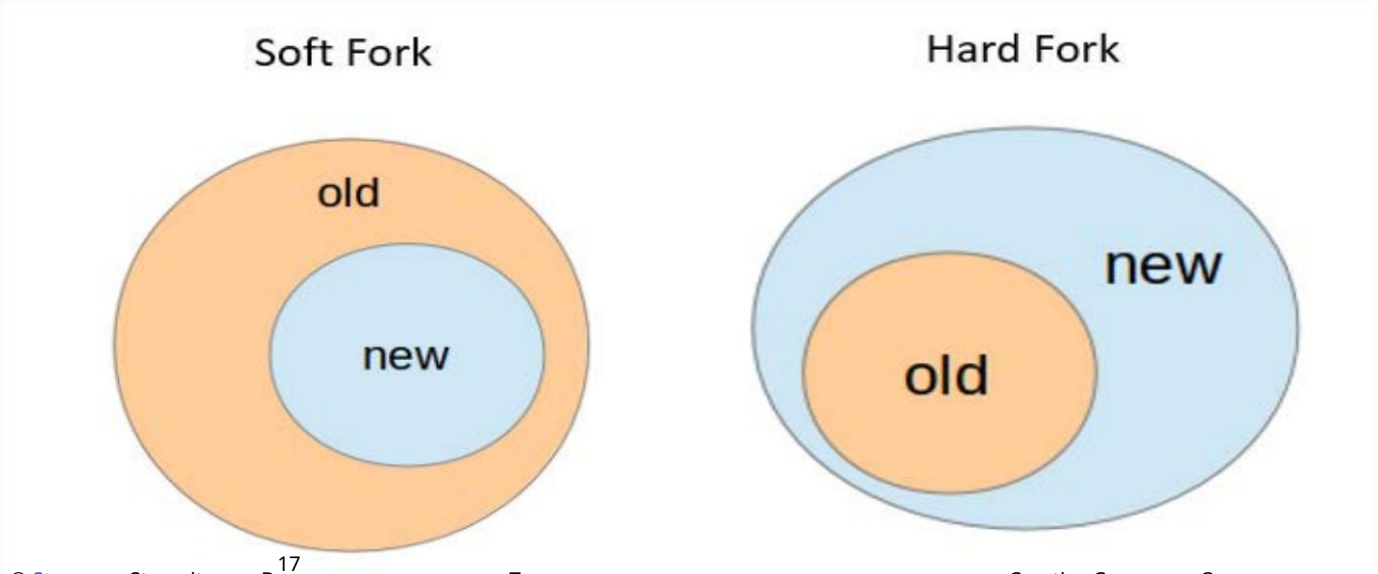
- Възможните решения включват а) Доказателства с нулево знание и б) Ангажименти на Pedersen
  - Криптографски примитиви, които: а) позволяват на някого да докаже, че твърдението е вярно
    без да се разкриват подробностите защо точно това твърдение е вярно и
    б) обвързване с данни (като хеш), но може също така да комбинира ангажименти

Оперативна съвместимост

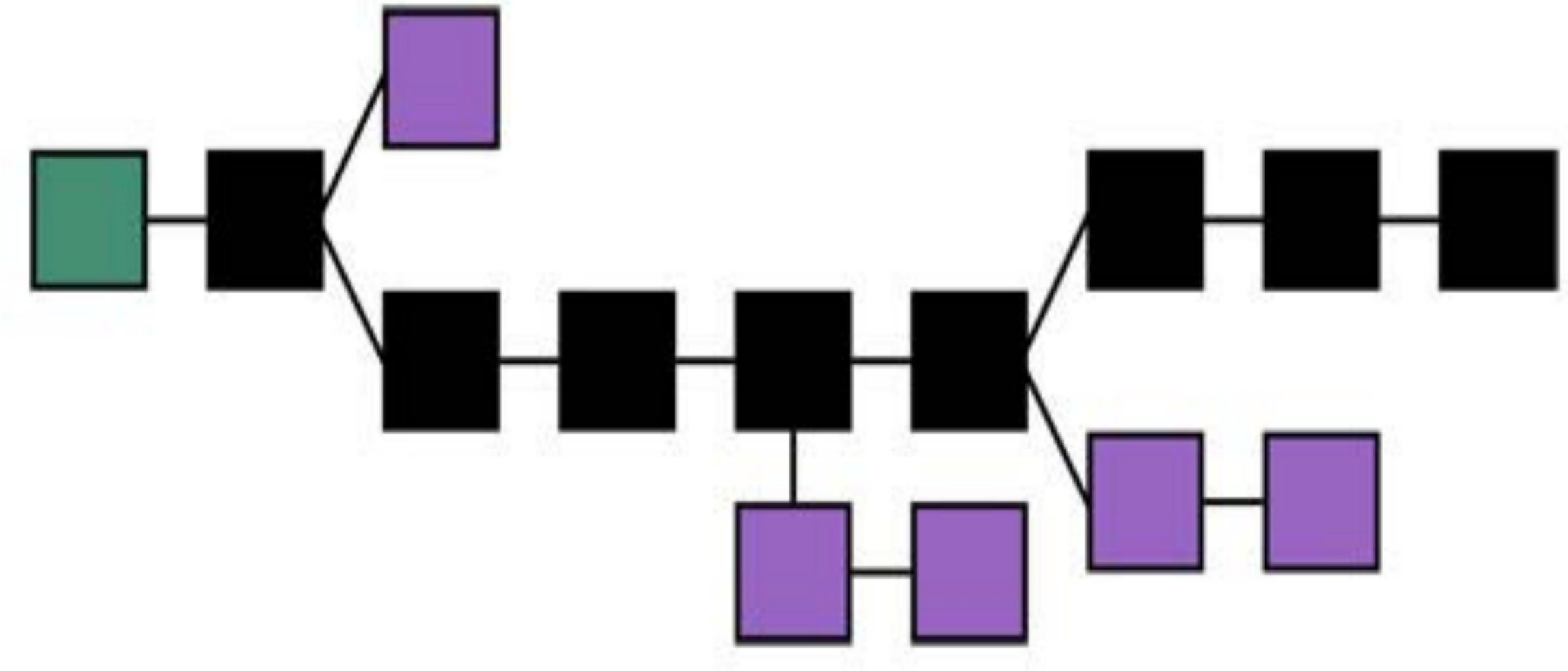
- Свързване на блокчейн приложение с наследени бази данни, инфраструктури, и технологии
- Повишава „разходите за доверие“ при координирането на прехвърлянето на активи и Информация в Blockchain или Across Chains
- Решение може да бъде активирането на децентрализирани механизми (включително Странични вериги или „Слой 0“) за прехвърляне на данни между вериги
- Необходима е много повече работа за постигане на безпроблемно движение между и между новата блокчейн технология и съществуващата технология

Изисква се консенсус за определени софтуерни актуализации

- Актуализации на софтуер с отворен код, които не са назад Съвместим
  - По-старите версии няма да валидират всички нови блокове
  - Подобно на това, ако актуализацията на Excel или Word и Новите файлове не са Съвместим
- Води до „Hard Forks“



Blockchain – Consensus поддържа най-дългата верига



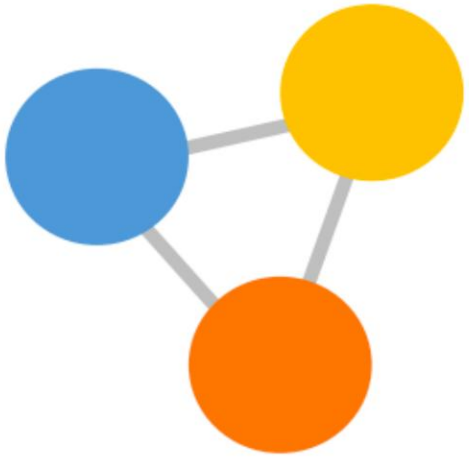
Колективни действия

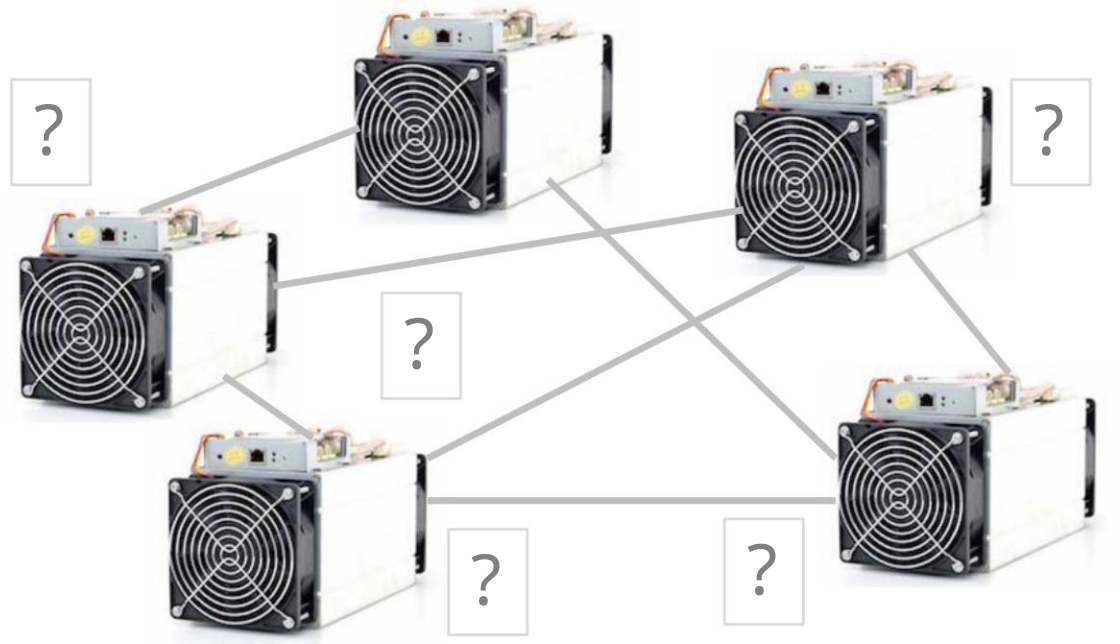
- Блокчейн приложенията извличат стойността си от участието на множество страни в мрежа, осиновяването изисква колективни действия

- Кокошка и яйце: трябват ранни осиновители, за да започнат мрежови ефекти, но пътят към постепенното приемане често не е ясен

Финансовият сектор в момента е в полза

блокови вериги с разрешение срещу блокови вериги без разрешение





• Известен набор от участници • Няма доказателство за работа или копаене • Няма нужда от местна валута
• Технология за разпределена база данни

• Неизвестни участници
• Сигурност, базирана на стимули
• Родна валута
• Крипто-икономика

20

Клас 8 (10/2): Учебни въпроси

- Как ключовите рамки на обществената политика – защита срещу незаконни дейности, осигуряване на финансова стабилност и защита на инвеститорите – са свързани с блокчейн технологията и крипто финансирането?

- Според законите за данъците, банковата тайна, ценните книжа и стоките, какво е значението, ако крипто токените се считат за собственост? Валути? Нещо ценно? Инвестиционен договор? Стока? Каква е същността на "Howey Test" на Върховния съд на САЩ?

- Как „Тестът на патица“ може да насочи мисленето за блокчейн технология и крипто финанси?

8 клас (10/2): четения

- „Криптовалути: Надзор на нови активи в цифровата ера“ Генслер
- „Бъдещето на парите“ Карни
- „Икономисти, спечелили Нобелова награда: Властите ще свалят „чук“ на биткойн“ CNBC

Изводи

- Blockchain осигурява P2P мрежа, но с разходи

- Разходи за децентрализация и компромиси от Permissionless

  Блокчейн трябва да се сравнява с централизирани и разрешени системи

- За мащабируемостта, ефективността и предизвикателствата, свързани с поверителността – рано е, но

  Съществува обещаваща работа по възможните решения – странични вериги, алтернатива

  Консенсусни протоколи и доказателства с нулево знание

- Предизвикателствата на оперативната съвместимост могат да се възползват от децентрализираното

  Механизми през вериги

- Проблемите с управлението и колективните действия, присъщи на Дизайна, могат да приключат

  като най-предизвикателната за решаване 23

15.S12 Блокчейн и пари

Есен 2018г