блокчейн и Пари

клас 6

25 септември 2018 г

Общ преглед на клас 6

- Преглед на курсови проекти
- Интелигентни договори
- Блокчейн дизайн с интелигентни договори
- DApps и Token Sales
- Правни въпроси на интелигентните договори
- Изводи

Изисквания

- Участие в клас 30%

- Две индивидуални писмени оценки (15% x 2) 30%
  - Критично бизнес разсъждение относно темата на класа
  - Предстои преди класа: 1- ви до 10-ти клас; 2- ри до 23-ти клас

- Групова изследователска работа 40%
  - Сериозни усилия по случай на употреба • Организирайте групи (3 или 4) до 8-ми клас (10/2) • Изберете област за случаи на употреба до 12-ти клас (10/18) • Теми извън финансите с предварително одобрение

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

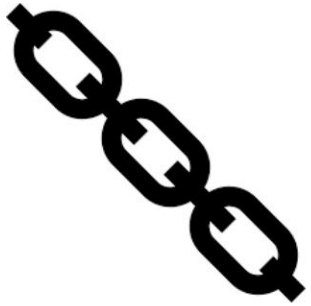
По избор

• „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

Интелигентни договори



• „Набор от обещания,

• посочени в цифров вид,

• включително протоколи

• в рамките на които страните изпълняват тези обещания.“

Ник Сабо, 1996 г

Въпреки това ....

• Интелигентните договори може да не са „умни“

• Интелигентните договори може да не са „Договори“

Биткойн – Технически характеристики

Ethereum?

- Криптография и регистрационни файлове с времево клеймо — да
  - Криптографски хеш функции • Регистрационни файлове само за добавяне с времеви печат (блокове) • Заглавки на блокове и Merkle дървета • Асиметрична криптография и цифрови подписи • Адреси — ✓ ✓ ✓ ✓ ✓
- Децентрализиран мрежов консенсус — да
  - Доказателство за работа • Na9ve валута • Мрежа — ✓ ✓ ✓
- Transac9on скрипт и UTXO — Не
  - Входове и изходи на Transac9on • Комплект неизразходван изход на Transac9on (UTXO) • Скриптов език — Преходи на състоянието Базиран на акаунт 7 езика

Bitcoin срещу Ethereum Design

• Основател: Сатоши Накамото	Ваталик Бутерин
• Генезис: януари 2009 г. • Код:	юли 2015 г
Non Turing (Сценарий)	Turing Complete (солидност, Serpent, LLL или Mutan)
• Ledger: UTXO – транзакция • Merkle Trees: транзакции	Държава - Въз основа на сметка 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

Bitcoin срещу Ethereum Design

• 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

Платформи за интелигентни договори

• Ethereum (2015) - $22 милиарда текуща пазарна стойност

• EOS (2018) - $5 милиарда – завършено $4,2 милиарда годишно ICO през юли • NEO (2016) – $1,1 милиарда - Китай; делегиран BFT; поддържа по-широк диапазон от код • Ethereum Classic (2016) – $1,1 b - Създаден от хард форка 'DAO' • LISK (2016) – $360 m - код в Java; използва странични вериги • Stratis (2017) - $150 млн

Случаи на потенциална употреба на интелигентен договор

Дигитална търговска камара (16/12)

- Цифрова идентичност
- Ценни книжа
- Деривати
- Ипотеки
- Верига за доставки
- Клинични изпитвания

Записи

Търговско финансиране

Финансови данни

Заглавие на земя

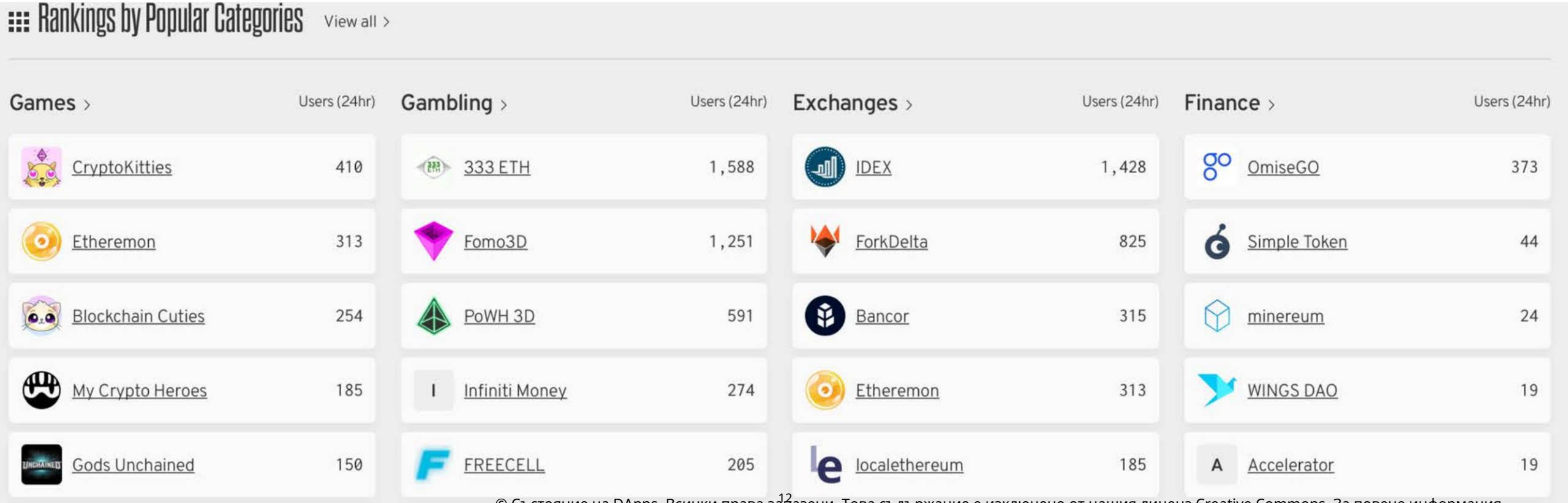
Автомобилна застраховка

Изследване на рака

Децентрализирани приложения (dApps)

• Приложенията се изпълняват в децентрализирана блокчейн мрежа •

Обикновено имат роден токен и се изпълняват като интелигентен договор върху Платформа



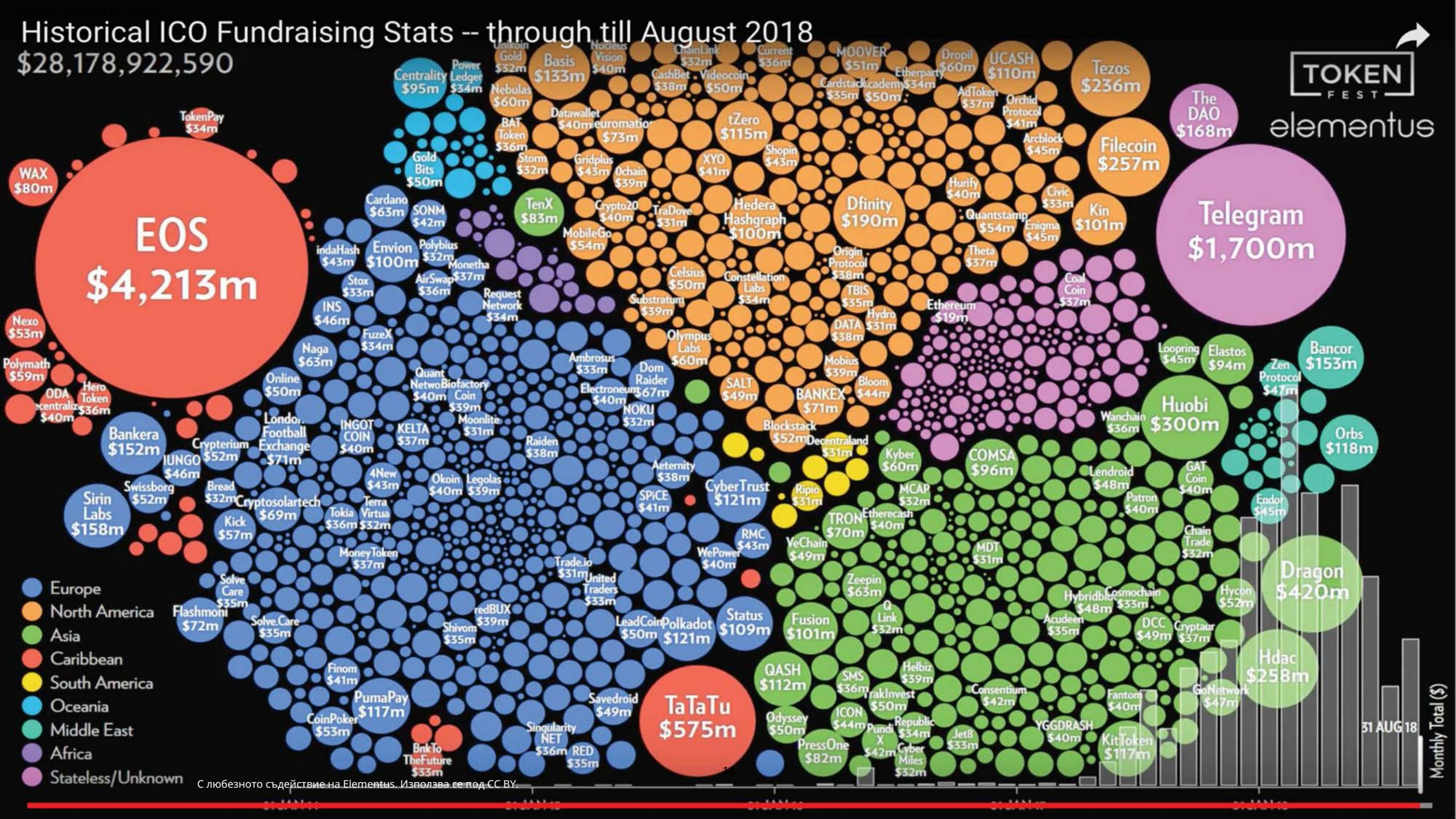
Източник: State of the Dapps (9/18) вижте https://ocw.mit.edu/help/faq-fair-use/

Първоначални предложения за монети –

Групово финансиране за Инвестиции и потребление

• Постъпления, използвани за изграждане на мрежи

• Токените обикновено се издават преди да бъдат функционални • Разработката, макар и с отворен код, е до голяма степен централизирана • Организаторите си разпределят „предварителните” токени • Токените са заменими и прехвърляеми • Оскъдността се насърчава с предварително зададена „Парична политика” • Купувачите очакват печалби чрез поскъпване



Правни въпроси – интелигентни договори

Гост-лектор – Лари Лесиг

• Харвардски професор по право и лидерство •
Основател на Станфордския юридически център за интернет и
общество • Служител на правосъдието Антонин Скалия и на съдия от апелативния съд Ричард
Познър • Многобройни награди, включително наградата за свобода на Фондацията за свободен софтуер, Fastca
50 награда и е обявен за един от Топ 50 визионери на Scientific American

• Автор на 8 книги, включително:

„Код и други закони на киберпространството“

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

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 (на, скалируемостта и сигурност? Какви са компромисите от консенсусните актуализации на soAware, управление и така наречените „хард форкове“?

- Какво може да работи в момента – приложения от слой 2, нулево знание доказателства, алтернативни алгоритми за консенсус – да се направи, за да се отговори на текущите търговски предизвикателства?

7 клас (9/27): четения

Задължително • Глава 2 „Доклад от Женева“ (страници 9 – 16); Кейси, Крейн, Генслър, Джонсън и Нарула • „Относно скалируемостта на блоковите вериги“ Контролът • „Скорости на трансакция: Как скоростите на криптовалутите се натрупват спрямо Visa или PayPal?,“ Колко.net

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

Незадължително • „Относно шардинга на блокчейни“ Ethereum Wiki • „zkLedger: Защита на поверителността Audi;ng for Distributed Ledgers“ Narula, Vas

Изводи

- P2P парите на Nakamoto

  Ethereum P2P изчисления на Buterin

- Интелигентните договори и DApps осигуряват: •

  Децентрализирано изчисление & •

  Самоизпълняващи се ангажименти

- Продажбите на токени за предложени DApps породиха нова форма на

  Групово финансиране – Първоначално предлагане на монети (ICO)

- Сред 1000-те предложения и оферти, малко DApps все още са спечелили

  Широко приемане от потребителите

- Интелигентните договори и DApps обаче имат реален потенциал да донесат промяна

15.S12 Блокчейн и пари

Есен 2018г