КРИПТОВАЛУТИ И ДЕЦЕНТРАЛИЗИРАНИ ВАЛУТИ

Владислав Драмалиев
Директор, Фондация „Битхоуп“
Мениджър маркетинг и общество, æternity

Contents

1. Предходна лекция
2. Типове криптовалути
    I. Децентрализирани криптовалути
        a. Консенсусни механизми / хешинг функции
    II. Централизирани криптовалути
    III. „Второ ниво“ криптовалути / Токени **[дискусия]**

Предходна лекция

- Криптография и хеширане?
- Асиметрична криптография?
- Дигитални подписи?
- Хеш функция?
- Merkle Trees?
- Какво копаят „копачите“?

Въпрос 1 – Хешират ли нодовете блоковете локално?

Отговор: Да. Проверяват дали подписите са валидни, за всяка трансакция.

Въпрос 2 – Къде се намира списъкът с транзакциите?

Отговор: При всеки node. Почти напълно идентичен.

Предходна лекция

1. Криптография и хеширане -> двупосочно | еднопосочно
2. Асиметрична криптография -> два шифъра – ключ и ключалка – публичен/частен
3. Дигитални подписи -> подписване на TXs | осигуряват 100% сигурност на информацията
4. Хеш функция -> Bitcoin - SHA256 | Идентификация и верификация
5. Merkle Trees -> Непроменяемост на TXs | Root Hash – част от „заглавието“ на блока
6. Копачите -> „Ниска стойност“ на хеша | Proof-of-Work | **Hashcash PoW**

КОНСЕНСУС

Криптовалути

- Използват криптография, за да постигнат консенсус

Основни видове криптовалути:

I. Децентрализирани криптовалути

II. Частни криптовалути

III. „Второ ниво“ криптовалути (токени) **[дискусия]**

I. Децентрализирани криптовалути

- Най-интересният сегмент
- Функционират посредством собствен блокчейн
- „Копаят“ се публично
- Различават се по своята функционалност
- Основна причина за това:

1) Протокол
2) Консенсусен механизъм – Proof-of-… (какво)
3) Криптографска [хеш] функция (как)

I. Децентрализирани криптовалути
Proof-of-...

Съществуват много консенсусни механизми:

- Proof-of-Work (PoW)
- Proof-of-Stake (PoS)
- Leased Proof of Stake (LPoS)
- Delegated Proof of Stake (DPoS)
- Proof of Importance (PoI)
- Proof of Activity (PoA)
- Proof of Burn (PoB)
- Proof of Capacity (PoC)
- Proof of Elapsed Time (PoET) („централизирана“)

I. Децентрализирани криптовалути
Proof-of-Work (PoW)

Първият дистрибутиран консенсусен механизъм

Характеристики:

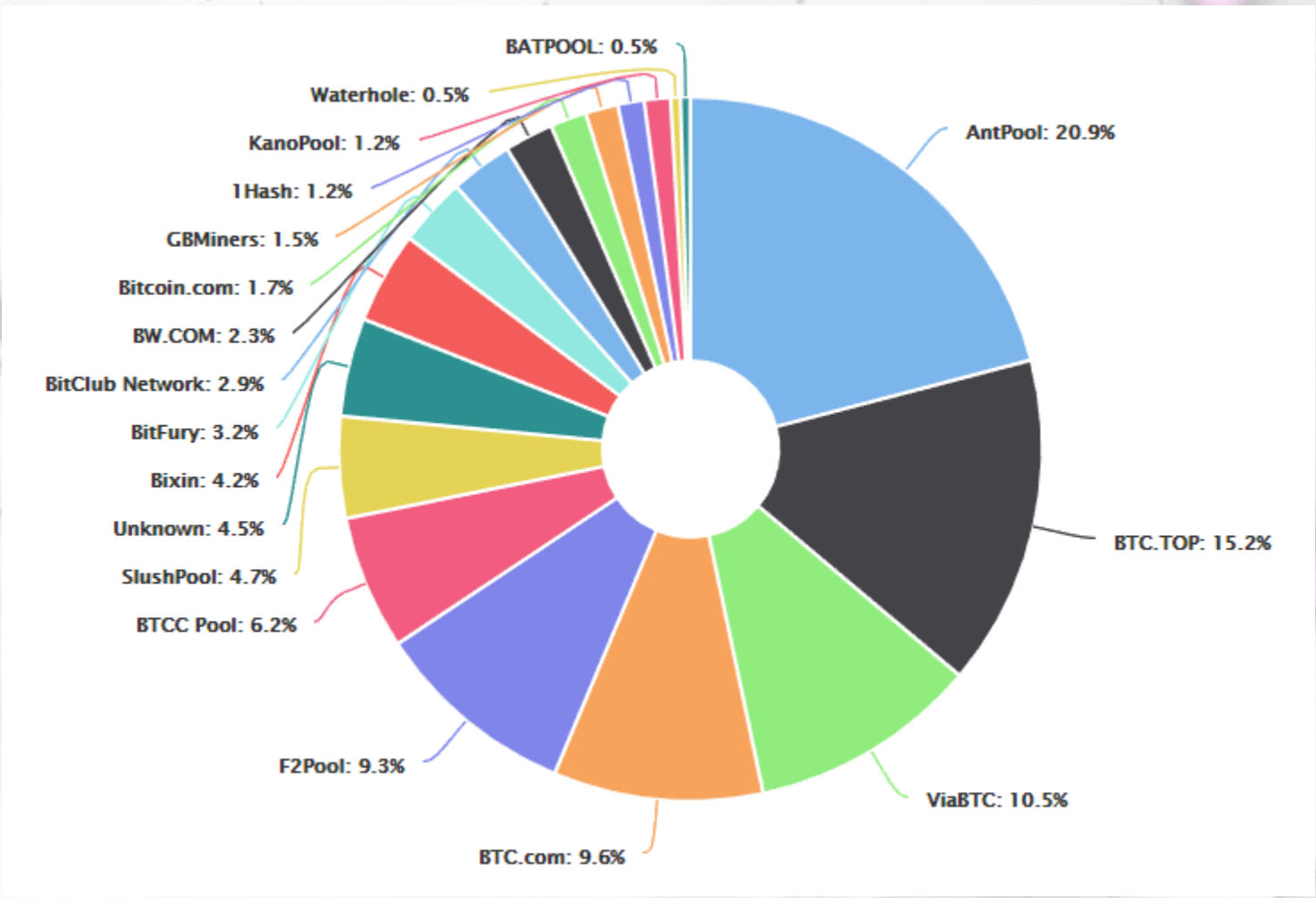
- Изисква компютърна мощност
- Търси се хеш с определена „големина“
- „Изчислително скъп“
- Екстремно повтораям
- Атаки – огромно количество компютърна мощност
- Енергийно интензивен

I. Децентрализирани криптовалути
Proof-of-Work (PoW)

Различните PoW криптовалути използват различни хешинг функции

- Bitcoin – SHA256
- Bitcoin Cash – SHA256 (fork)
- Ethereum – Ethash
- Litecoin – Scrypt
- Monero – CryptoNight
- Zcash – Equihash
- Dash – X11
- Vertcoin – Lyra2rev2
- æternity – Cuckoo Cycle

I. Децентрализирани криптовалути
Proof-of-Work (PoW)



I. Децентрализирани криптовалути
Proof-of-Work (PoW) - Ethash

Ethereum

- Основна причина за използването му – централизация на SHA256 майнинга
- Без ASIC (Application Specific Integrated Circuit)
- Използва „твърдопаметен“ (memory-hard) хеш алгоритъм

„Колко бързо компютърът ви може да мести информация“

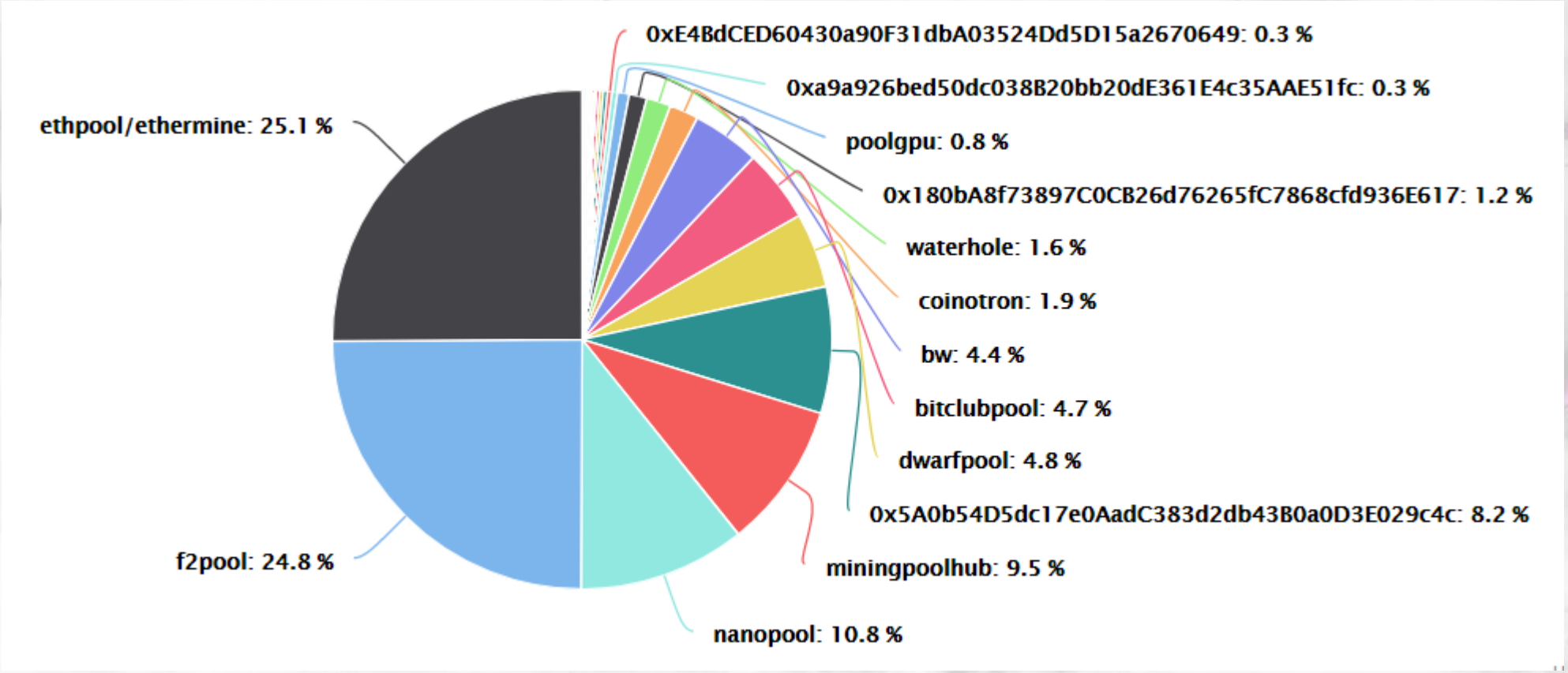
VS

„Колко бързо може да извършва изчислителни операции“

- Повишаване на ефективността зависи от GPU индустрията
- По-добра RAM памет

I. Децентрализирани криптовалути

Proof-of-Work (PoW) - Ethash



I. Децентрализирани криптовалути

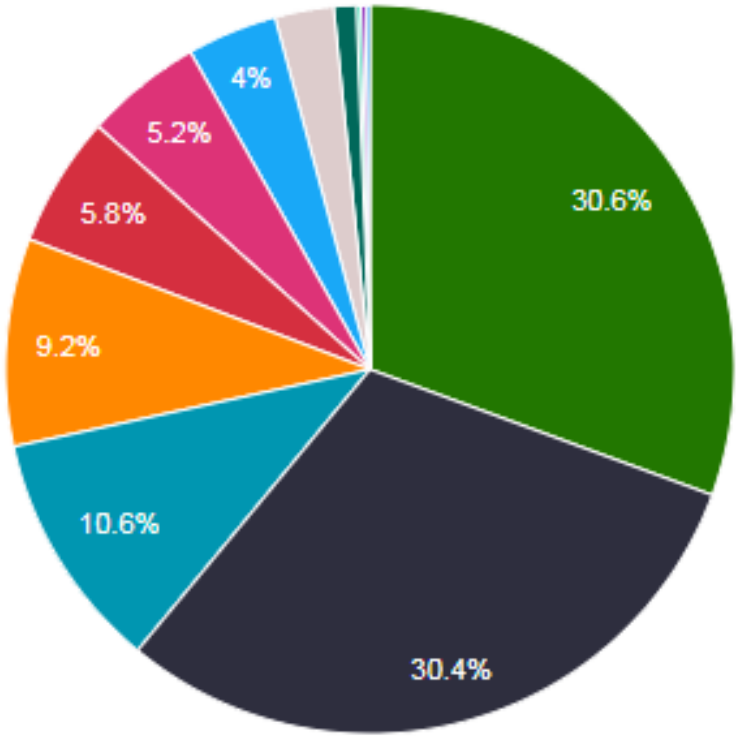
Proof-of-Work (PoW) – Scrypt ["ess crypt“]

Litecoin

- Базирана на парола, ключоизвличаща функция (вариация на хеш)
- Голямо количество RAM
- Използва се за първи път от Tenebrix през 2011
- Използва се и от Dogecoin
- През 2014 е създаден първият ASIC
- През 2016 – InnoSilicone – 14nm | 1.5 вата/мегахеш-секунда

I. Децентрализирани криптовалути

Proof-of-Work (PoW) – Scrypt ["ess crypt“]



F2Pool	~ 7,996 GH/s
Antpool	~ 7,944 GH/s
ViaBTC	~ 2,770 GH/s
LitecoinPool.org	~ 2,404 GH/s
BW.com	~ 1,516 GH/s
LTC.top	~ 1,359 GH/s
BTCChina	~ 1,045 GH/s
TBDice.org	~ 679 GH/s
ProHashing	~ 261 GH/s
Give Me Coins	~ 52 GH/s
Coinotron	~ 52 GH/s
Batpool	~ 52 GH/s
Total	~ 26,132 GH/s

I. Децентрализирани криптовалути

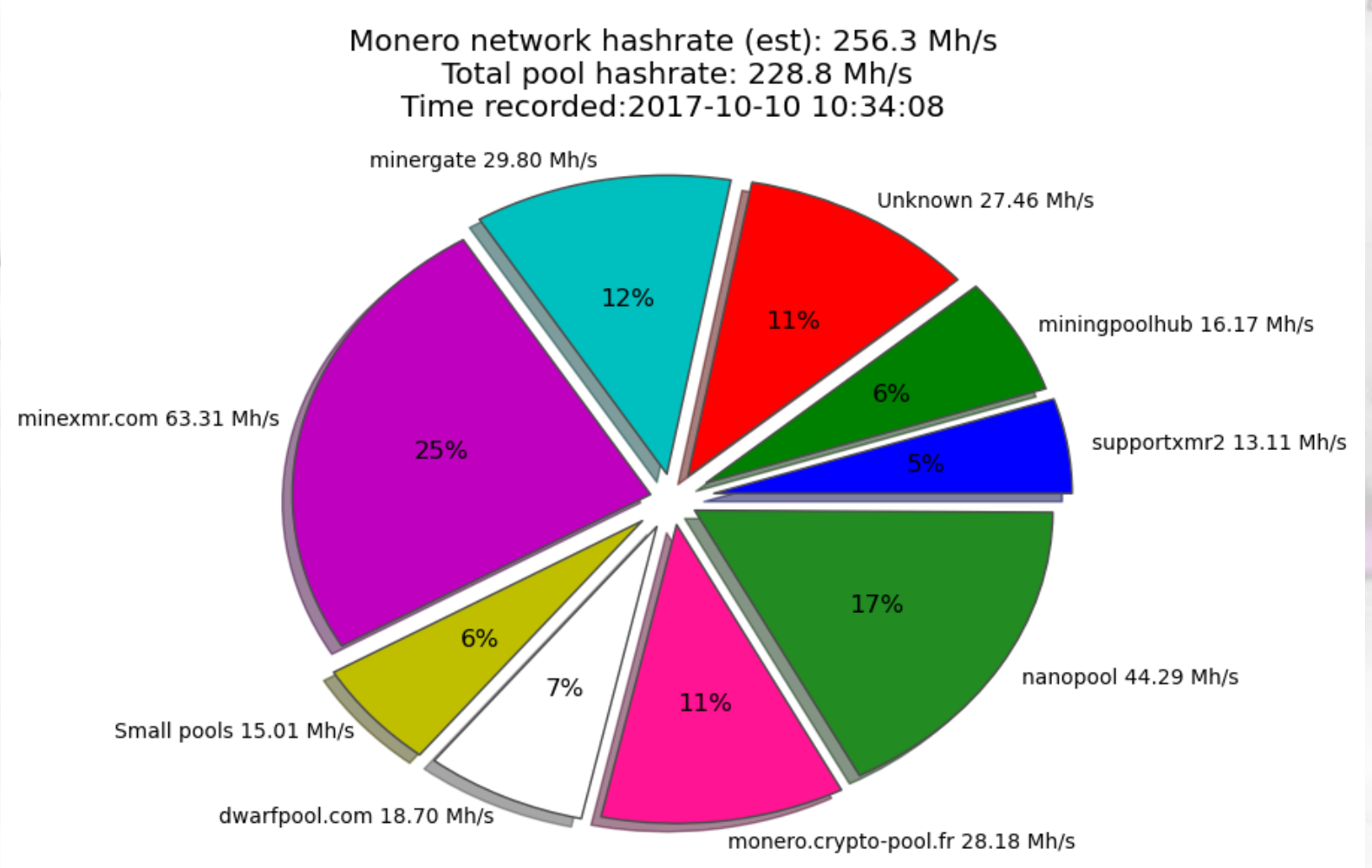
Proof-of-Work (PoW) – CryptoNight

Monero

- Благодарение на CryptoNight - почти анонимен блокчейн
- Не може да се проследяват транзакции
- Начална точка, крайна точка и точна сума – не могат да се определят
- Не може да се определи кой точно е подписал трансакцията
- RAM-интензивна
- Използва CPU и GPU като защита срещу ASIC и видео карти
- Не е ясно колко добре се справя с botnets

I. Децентрализирани криптовалути

Proof-of-Work (PoW) – CryptoNight



I. Децентрализирани криптовалути
Proof-of-Work (PoW) – Equihash

Zcash

- Позволява постигане на високо ниво на анонимност на TXs
- Базиран на проблем в компютърната наука/теорията на възможностите: *Парадоксът на рожденитe дни*
  - Колко хора са необходими, за да има 50% шанс за съвпадение в рождените им дни?
  - Колко хора са необходими за 99.9%?
- Асиметричен, твърдопаметен алгоритъм
- Изисква RAM
- Предотвратява създаването на ASIC
- Позволява „лека“ верификация – може да се използва в Ethereum Smart Contracts

I. Децентрализирани криптовалути
Proof-of-Work (PoW) – X11 Algorithm

DASH

- Използва 11 хешинг функции
- Анонимност
- „Лек“ за копаене (30% по-хладни машини)
- Ефективен от към електроенергия
- Щадящ към хардуера
- Може да се копае с CPU и GPU
- ASIC може да се избегне кратко- и средно-срочно
- Botnet застрашен
- 2-Tier
  - Нови блокове – копачи (45%)
  - PrivateSend, InstantSend, и управление – masternodes (45%)
  - 10% в бюджета

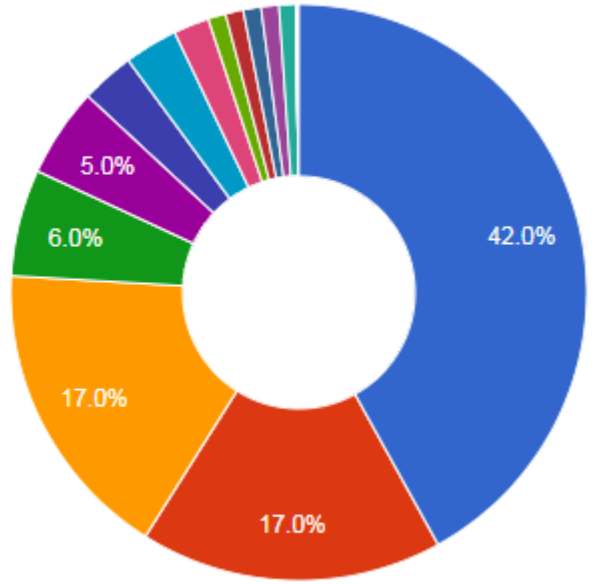
I. Децентрализирани криптовалути

Proof-of-Work (PoW) – X11 Algorithm

Hashrate Distribution

Rank	Pool/Miner		Last 100	Last 1000
1	XvhExSNNr97U1...	↑	42 %	38.5 %
2	cybtc	↑	17 %	12.1 %
3	Coinmine.pl	↑	17 %	12.7 %
4	Coinotron	↓	6 %	9.0 %
5	XssjzLKgsfATY...	→	5 %	5.4 %
6	Mining Pool Hub	↓	3 %	5.7 %
7	XxHS6RDp1Kfmt...	→	3 %	3.4 %
8	All others	↓	2 %	3.6 %
9	Xoyn4Xxugx5K6...	→	1 %	2.0 %

Extraction Share for last 100 Blocks



Orphans Chart expand

I. Децентрализирани криптовалути
Proof-of-Work (PoW) – Lyra2RE

Vertcoin

- Първоначално - Scrypt-Adaptive-N -> ASIC
- Ключоизвличаща функция (Litecoin)
- Включва 6 хеш функции
- Предотвратява ASIC и Multipool копаене
- Ориентирана към GPUs
- Позволява “споделено копаене“ (merged mining)

I. Децентрализирани криптовалути

Proof-of-Work (PoW) – Lyra2RE

Pool	Address	Blocks	Network share	Status
coinotron	VuPp8H4W3g1dmwGg6pe41D2Khw8JvfEznn	833	59.84%	Upgraded 100.00%
miningpoolhub	VqspNKCc3ufsUSJb6Vq2TcEVX1Wn9EdHjP	312	22.41%	Upgraded 100.00%
p2pool	p2pool	95	6.82%	Upgraded 100.00%
unknown	VrnVLcJ7tNCSjMcSmG5p31XQowCLqqvG2F	67	4.81%	Upgraded 100.00%
unknown	VstrmuCHXK7TdZZmguKJZALXRPW7Uu8znC	25	1.80%	Upgraded 100.00%
unknown	Vo51JbXVik36LjA4auqAqgivcj2KhkaBah	24	1.72%	Upgraded 100.00%
unknown	VbnKqcsnXUYn6iPgZc7qb6fXVKd4i3UWM3	15	1.08%	Upgraded 100.00%
unknown	VtQLAsHCJNaHc9E4Vt3Eod6RrTvur1X3yA	5	0.36%	Upgraded 100.00%
unknown	VqPsxd2QKA8Rr3jXeCVZ4UeRFBLs5hiN5T	4	0.29%	Upgraded 100.00%
unknown	Vr4opqKSmoATcFzk6nqAN4htxheMSPtNXJ	4	0.29%	Upgraded 100.00%
verters	Vo38hozyX4UmodmGqfwxGCtXBiZKMsUkie	3	0.22%	Upgraded 100.00%
unknown	VkE3N4HcYfHWAAUi3fbWhY5kjmhUov8e1t	3	0.22%	Upgraded 100.00%
unknown	VoSRdKDc3DUUPBVXpXxxoRmCz2oorsTfiw	1	0.07%	Upgraded 100.00%
unknown	VcB3N8bmgzX2p85CKzExSRVKqe5UrNNw5A	1	0.07%	Upgraded 100.00%

I. Децентрализирани криптовалути
Proof-of-Work (PoW) – Cuckoo Cycle

æternity

- Да се избегнат ASICs
- Първият „графико-теоритичен“ (graph-theoretic) PoW
- Произволен, глобален достъп до RAM за четене и писане
- Ниска консумация на енергия - „студени“ машини
- Прилича на Equihash
- NVIDIA GTX 1080/1070
- DRAM – последователен достъп
- Стимулира създаването на RAM с по-бърз „произволен достъп“
- Още по-енергийно ефективна RAM

I. Децентрализирани криптовалути
Proof-of-Stake (PoS)

Вторият най-разпространен консенсусен механизъм

- Копаенето се извършва на база „залог“ (“forging”)
- Няма награда от блока, само транзакционни такси
- Копачите се избират произволно спрямо:
  - Ниска стойност на хеша
  - Размер на залога
  - (допълнително) възраст на койните на залога (мин 30 дена, макс 90)

- Ethereum (някой ден, Casper)
- NXT – SHA256
- Synereo AMP
- Peercoin – SHA256

I. Децентрализирани криптовалути

Proof-of-Stake (PoS) – Ethash

Ethereum - Защо преминава към PoS?

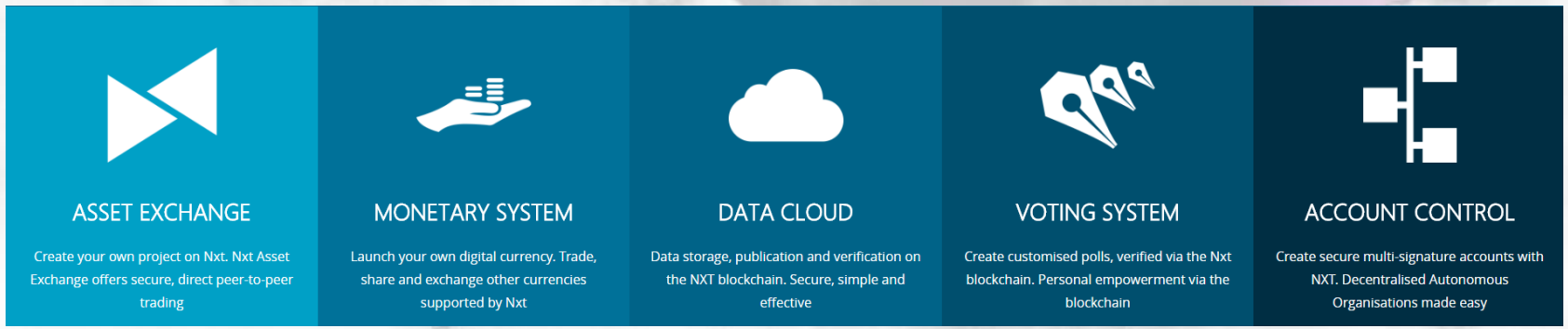
- По-високо ниво на сигурност
- Намален риск от централизация (няма “икономика на размера“)
- Енергийна ефективност
- Може да доведе до прекратяване на инфлацията в системата
- Може да предотврати създаването на картели (Игрова теория)
- Организирането на 51% атаки може да доведе огромни загуби

ДЕТАЙЛИ

I. Децентрализирани криптовалути
Proof-of-Stake (PoS) – SHA256

NXT

- Обсъждана в доклад на Европейския орган за ценни книжа и пазари (ESMA)
- Произволно се избира следващия „копач“
- Количеството койни не се променя
- След 1 ден (1440 потвърждения) – започва „forging”
- Blockchain as a Service (BaaS)
- Заплашена от 51% атаки в момента
- Българско участие



I. Децентрализирани криптовалути
Proof-of-Stake (PoS)

Synero

- NFX Guild избират Synero вместо Ethereum
- JVM (не Python), scalable, fully distributed
- Децентрализирана икономика
- Дигитална самоличност
- Социална мрежа

“Бъдещето на създаването, публикуването и разпространението на съдържание“

I. Децентрализирани криптовалути
Proof-of-Stake (PoS) – SHA256

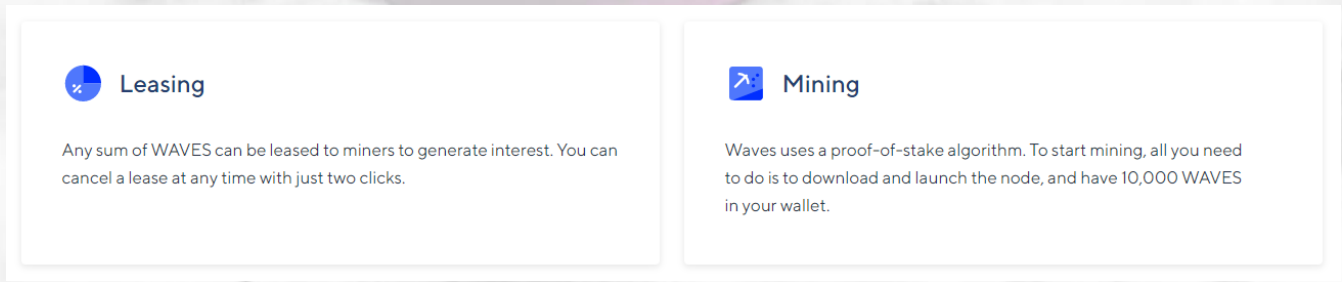
Peercoin

- Голяма част от кода на Биткойн
- PoS и PoW
- Два вида блокове – PoS & PoW
- PoS – „възраст на блоковете“ (coin age)
- PoW – като при Биткойн, но трудността се изчислява при всеки блок
- Ниска инфлация – 1% на година, но безкрайно (2 милиарда)
- Транзакционните такси се определят на протоколно ниво - фиксирани
- Транзакционните такси се унищожават
- Hard Fork – промяна на размера на таксата

I. Децентрализирани криптовалути
Leased Proof-of-Stake (LPoS)

Вариация на PoS

- Малките „залози“ (stakes) може и да не намерят блок с години
- Както при PoW – с една машина и solo mining – нищожен шанс
- Залозите могат да се насочват към node
- Имитира се функцията на pools в PoW
- Заложените койни се притежават от потребителя
- Интегрирана децентрализирана борса
- Може да създавате ваша криптовалута
- Платформа за ICO-та



I. Децентрализирани криптовалути
Delegated Proof-of-Stake (DPoS)

Вариация на LPoS

- Потребителите притежаващи койни ги използват, за да изберат nodes
- Списък с nodes, които могат да залагат и да създават блокове
- Според някой:
  - Най-ефективният
  - Най-бързият
  - Най-децентрализирания
  - Най-гъвкавия консенсусен механизъм

I. Децентрализирани криптовалути
Delegated Proof-of-Stake (DPoS)

BitShares

- 100 000 TPS
- Децентрализирана борса
- Ценово-стабилни криптовалути
- За корпоративни клиенти
- Създаване на токени
- Паричен резерв от 8м долара | от трансакции | 77k USD на месец | работници
- Списък със „свидетели“ (witnesses) | генериращи блокове nodes
- Списък с „делегати“ (delegates) | предлагащи промени на основни параметри

I. Децентрализирани криптовалути
Proof-of-Importance (PoI)

NEM

- Не е важно само да притежаваш койни
- Трябва да се използват – колко транзакции има определен адрес? | оборот
- Трябват най-малко 10к XEM за да се участва в „жътвата“ (harvesting)
- Баланс | Репутация | Брой трансакции
- Репутационна система - Eigentrust++
- Балансите могат да се делегират
- NCDawareRank network centrality measure – за постигане на консенсус
- Има централен компонент, който не е open-source | NEM Infrastructure Server (NIS)
- В момента се пише на C++ (Catapult) | ще бъде open-source

I. Децентрализирани криптовалути
Proof-of-Activity (PoA)

Основна цел: да предотврати „трагедията на общините“ в Биткойн

- Липсата на награда за блок в Биткойн е притеснителна
- Може да доведе до „унищожителен собствен интерес“
- “Selfish Mining”
- Към PoW трябва да се добави и PoS
- Търсят се „ниски хешове“, но не се добавят трансакции в блокове | шаблони
- При намиране на хеш – PoS
- Произволно се избира група от валидатори, които подписват блока
- Колкото по-голям баланс – толкова по-голям шанс да си валидатор
- Транзакционните такси се споделят между копачи и валидатори

I. Децентрализирани криптовалути
Proof-of-Activity (PoA) - BLAKE256 [SHA-3]

Decred

- Хешинг алгоритъмът се счита за по-сигурен
- Самофинансираща се система с интегриран механизъм за управление
- По-балансирана – Копачи VS Потребители – от Биткойн
- Има конституция
- Сложна система на управление (гласуване и избиране на делегати) – Decred Assembly, Admission Council, Attrition Council
- За да се участва в PoS трябва да закупи „билет“ (или билети) чрез заключване на определен брой койни
- „Билетите“ се активират след 28 дни (може повече, може по-малко)
- Използват се „залагане“ и „гласуване“
- В някакъв момент ще се въведе Proof-of-Assembly (PoA)

I. Децентрализирани криптовалути
Proof-of-Burn (PoB)

Какво се гори и как?

- Криптовалута се изпраща към „заключен адрес“
- Колкото повече „изгаряш“ толкова по-голям шанс има да бъдеш избран за „копач“
- С времето – статута ти се губи
- Прилича на PoW (купуват се машини, стойността/производителността им намалява)
- Може да се гори конкретна валута или биткойн

I. Децентрализирани криптовалути
Proof-of-Burn (PoB)

Slimcoin

- Базиран на Peercoin
- Не е много активен (направо е умрял)
- PoW, PoS, PoB
- Пазарна капитализация – 41 биткойна :D

Counterparty

- “ICO” базирано на PoB
- Изпращат се биткойни към заключен Биткойн адрес
- XCP в замяна

I. Децентрализирани криптовалути
Proof-of-Capacity (PoC)

Какъв капацитет?

- Вариациите в изчислителната мощност може да са големи (CPU)
- Не е така при пространството
- Свободно дисково пространство - съхранява се информация
- Колкото повече свободна памет/дисково пространство – толкова по-голям шанс да „копаеш“
- Вариации – Proof-of-Storage | Proof-of-Space

I. Децентрализирани криптовалути
Proof-of-Capacity (PoC)

Permacoin

- Архивиране на информация на харддиска
- Застрашен от „облака“ | обвързване на частния ключ
- Bandwidth/latency защита срещу „облачно копаене“

Filecoin

- Proof-of-Replication (информацията е репликирана някъде | без сваляне)
- Proof-of-Spacetime (постоянни проверки на информацията)
- Децентрализирана система за хостинг на файлове/информация
- Пазар за дисково пространство
- Баланс между копия на информация, скорост на достъп, цена
- ICO: 257m USD

I. Децентрализирани криптовалути
Proof-of-Elapsed Time (PoET)

Решение на Intel (централизирано)

- Изисква използване на trusted execution environments (TEE)
- Защитена зона в централния процесор
- Изисква специализиран хардуер на Intel
- "trust-maximizing„ НЕ “trustless”

I. Децентрализирани криптовалути
Заключение

- Огромно разнообразие от консенсусни механизми
- Разнообразие от криптографски функции
- Подобряват определени характеристики НО,
- Влошават други

- Основни цели:
  - Избягване на „централизация“ [на копаене]
  - Намаляване на електропотреблението

- Децентрализираните криптовалути – не толкова „децентрализирани“ (все още)

I. Децентрализирани криптовалути

Определяне на нивото на „децентрализация“

[ЛИНК]

I. Децентрализирани криптовалути

Определяне на нивото на „децентрализация“

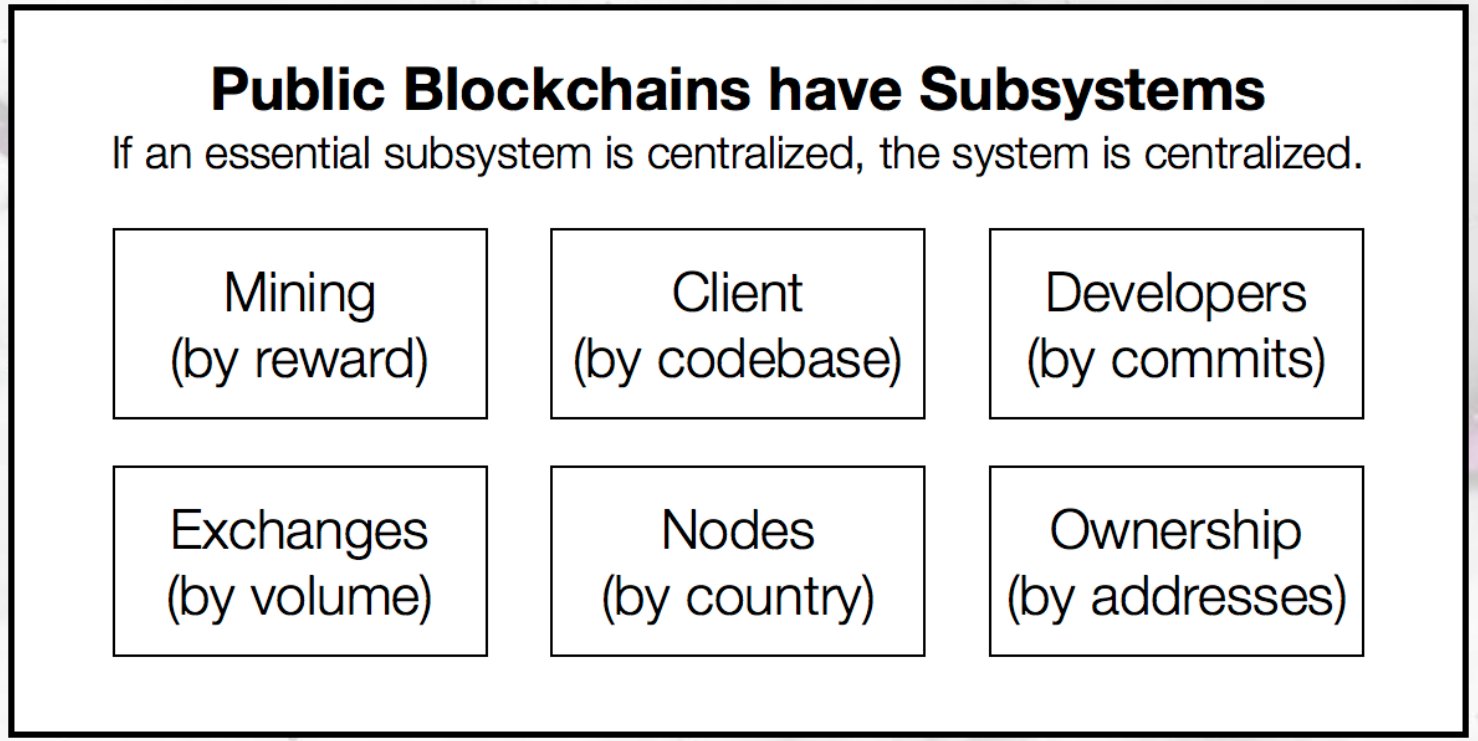
Според Виталик Бутерин:

- Централизация на архитектурата (копаене)
- Политическа централизация (разработка)
- Логическа централизация (много копачи, един собственик)

I. Децентрализирани криптовалути

Определяне на нивото на „децентрализация“

Коефициент на децентрализация – Балажи Сринивасан



II. Частни криптовалути

Съществували са централизирани криптовалути

- DigiCash (1998)
- Open Transaction

Liberty Reserve (2006)

- Артър Буковски
- Много успешна
- Име, мейл, дата на раждане
- Без лимит в размер на трансакцията
- Стабилен курс – USD/EUR
- 17 държави / 1м потребителя
- 2013 – the end – 20 години

II. Частни криптовалути

Ripple

Децентрализирана или централизирана?

Характеристики:

- Open-source
- Peer-to-peer разплащателна мрежа
- Същата криптография като Bitcoin
- Всеки може да има node
- Всяка валута може да се изпраща
- Вградена борса
- Потвърждения за секунди
- Няма сваляне на “blockchain”
- Няма PoW – Consensus

II. Частни криптовалути

Ripple

Децентрализирана или централизирана?

Характеристики:

- Не се копае
- Компанията определя количеството койни
- За сега има лимит – 100 милиарда
- При всяка трансакция – „изгаряне на XRP”
- Продават софтуер на банки и финансови институции

II. Частни криптовалути

Blockchain

- Отворени
  - Публични (Internet)
  - Без-позволение –> Bitcoin, Ethereum, Zcash, Dash, Litecoin
  - Технологични изисквания

- Затворени
  - Частни (Ethernet)
  - Само с позволение -> Hyperledger Fabric, Proof of concepts by EEA & R3
  - Специфични изисквания (платежоспособен, лицензиран, може ли да изпълни договорни задължения)
  - КОНТРОЛ!

III. „Второ ниво“ Криптовалути | Токени

Какво представляват?

- Нямат собствен блокчейн
- Не се използват за „такси“/”газ“ в основния чейн
- Могат да бъдат ограничени или неограничени
- Всеки може да си създаде такива

Популярни проекти

- Ethereum – ERC20
- Counterparty
- Waves

ДИСКУСИЯ

Какво е ICO?

Кой е инвестирал в ICO?

Кое ICO?

Защо точно това ICO?

vlad@aeternity.com

www.aeternity.com