A Bitcoinon túl…

Egyéb kriptopénzek

Bura Pál

2014-05-30

Egyéb kriptopénzek

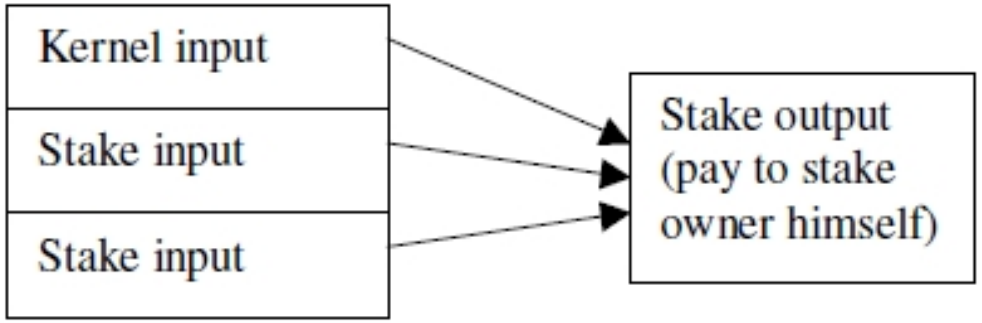
- Bitcoin óta rengeteg új kriptopénz keletkezett
- https://coinmarketcap.com
- 306 coin
- Teljes market cap: $ 8,455,623,627
- Ebből Bitcoin: $ 7,799,026,350
- Jelenlegi három legnagyobb:
  - Bitcoin
  - Litecoin
  - Peercoin

Peercoin

- 2012.08.12.
- Sunny King
- Proof-of-work és proof-of-stake hibrid
- Coin age
  - A 10 PPC-t kap B-től és azt 50 napig magánál tartja
  - = > coinage = 500
- Leghosszabb lánc a legnagyobb teljes elhasznált coin age alapján

Peercoin

- Proof-of-stake hamisítása is nehéz
- Két féle blokk
  - Proof-of-work
  - Proof-of-stake
- Coinbase analógiájára coinstake
- Kernelnek bizonyos feltételt kell teljesítenie
- Hashelés korlátos tartományon , így kis számítási teljesítmény
- Coinstake generálás valószínűsége ~ felhalmozott coinage



Peercoin

- Checkpointing
  - Bitcoin esetében nem folyamatos
  - Első 2010-ben
- Checkpointig bezárólag a blokklánc be van fagyasztva
- Naponta többször
- Fix beépített infláció

Litecoin

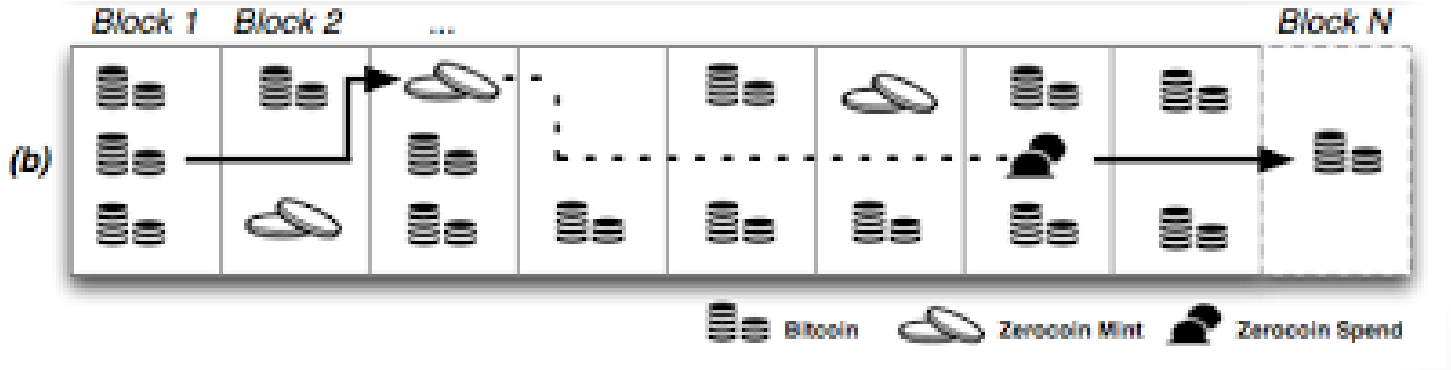
- 2011.10.07.
- Charles Lee
- Silver to Bitcoin’s gold
- 4-szer gyorsabb blokkgenerálás (2.5 perc)
- 84 millió LTC
- SHA-256 helyett Scrypt
- SHA-256: algoritmus párhuzamosítással felgyorsítható => ASIC
- Scyrpt: számítás szerializáltabb
  - Inkább gyors RAM kell, mint pusztán számítási teljesítmény => PC grafikus kártyákkal
- Tranzakciós sebesség nagyobb

Mastercoin

- Nincs saját blokkklánca
- Bitcoin meglévő láncát használja
  - Már legelejétől hatalmas számítási teljesítmény védte
- Alkalmazás réteg a Bitcoin fölé
  - HTTP és TCP/IP
- Nem bányászással keletkeztek, hanem támogatásszerző folyamattal
- 619478.6 MSC
- Előnye a sok általa bevezethető funkció
  - Bets – Fogadás egy árucikkről, shortolható és longolható
  - Savings account - Letéti számla kezelése
- https://github.com/mastercoin-MSC/spec

Zerocoin

- Magasabb szintű anonimitás
- Bitcoin esetében data mining használatával meghatározható, hogy egyes címek kihez tartoznak
- Laundry
- http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf



Összehasonlítás

	Bitcoin	Litecoin	Peercoin
Megjelenés	2009.01.03.	2011.10.07.	2012.08.12.
Egység	BTC	LTC	PPC
Érték	**$ 569.75**	**$ 11.51**	**$ 2.43**
Piaci tőke	**$ 7,301,453,362**	**$ 330,028,477**	**$ 52,019,113**
Kibányászott készlet	12,815,250 BTC	28,679,204 LTC	21,428,108 PPC
Teljes pénzkészlet	21 millió	84 millió	korlátlan
Legkisebb egység	0.00000001 (satoshi)	0.00000001 (spark)	0.00000001
Hash algoritmus	SHA-256	Scrypt	SHA-256
Bányászás	proof-of-work	proof-of-work	proof-of-work és proof-of-stake hibrid
Jutalom	kezdetben 50 BTC blokkonként 4 évente feleződik	kezdetben 50 LTC blokkonként 4 évente feleződik	proof-of-work: feleződik proof-of-stake: évi 1%
Nehézség hangolása	2016 blokkonként 14 nap	2016 blokkonként 3.5 nap	bányászok száma alapján folyamatos
Tranzakciós díj	nincs	nincs	0.001 PPC

A Bitcoinon túl…

Egyéb kriptopénzek

Bura Pál

2014-05-30