Bitcoin, Ethereum a shrnutí

Paralelní a distribuované systémy, přednáška 12

Tomáš Urbanec

Katedra informatiky PřF UPOL

11.12.2024

Co nás čeká?

1. Bitcoin a Ethereum
2. Shrnutí kurzu
3. Zkouška
4. Zpětná vazba

Blockchain

Bitcoin

Základy

- Satoshi Nakamoto (?), 2009
- První úplná implementace DLT.
- Záměr: Alternativa k fiat měnám.
- V blocích jsou generovány BTC.
- Fixní počet BTC: 21 000 000
- $1\,\text{BTC} = 10^8\,\text{Satoshi}$.
- Nejprve odměna 50 BTC v bloku.
- Tzv. Halving každých 210 000 bloků ($\approx$ 4 roky)
- Očekávaný konec 2140 (odměna $<$ 1 Satoshi).
- Cena? google

Bitcoin

Technikálie

- Hashovací funkce: SHA-256
- Podpis transakcí: ECDSA (Elliptic Curve Digital Signature Algorithm)
- Privátní klíč podepisuje transakce, veřejný ověřuje.
- Nový blok každých cca 10 minut.
- Velikost bloku do 1 MB (dnes až 4 MB)
- PoW: Doplnit blok o nonce (číslo), aby hash měl prefix 0^n.
- Délka prefixu (n) nastavitelná $\rightarrow$ úprava obtížnosti.

Ethereum

Základy

- Vitalik Buterin, Gavin Wood, 2015
- Druhá nejvýznamější kryptoměna.
- Záměr: Blockchain může poskytovat více než jen měnu.
- . . . a také z toho sám může těžit.

→ Decentralizované aplikace, smart contracts.

- $1\,\mathrm{ETH} = 10^{18}\,\mathrm{Wei}$
- Nemá limit, ale má jiné nástroje pro omezení inflace (a možnost změn).
- Cena? google

Ethereum

Technikálie

- Hash: Keccak-256 (modifikovaný SHA-3).
- Podpis transakcí: ECDSA.
- Privátní klíč podepisuje transakce, veřejný ověřuje.
- Původně PoW (Ethas), paměťově náročné operace, hledání odpovědi ve velkých datech.
- Eliminovalo specializovaný HW.
- Nyní PoS (od 2022). Snížení spotřeby o 99%.
- Podporuje Smart contracts:
  - Součástí je EVM (Ethereum Virtual Machine).
  - Vlastní bytekód. Turingovsky úplný.
  - Jazyky: Solidity (OOP, C-like), Vyper (Python-like)
  - Kontrakt je nasazen na vlastní adresu.
  - V transakci očekává vstup a platbu.
  - Vykonávání operací vyžaduje „gas“ – uživatel platí validátorům.

Shrnutí

Shrnutí

- Pokrytá témata na webu.
- Spíše jsme klouzali po povrchu.
- Alespoň jednou otevřete knihu Van Steen & Tanenbaum!
- Pokud Vás něco zaujalo, otevřete i doplňkové zdroje.
- Slidy mohou dostat drobných úprav
  - korektura a formualce,
  - ne obsah.
- Na slidech není vše, co bylo řečeno. . .

Zkouška

Otázky

- Rozsah znalostí daný přednáškami a cvičeními.
- Obecný rozhovor – letem světem, hodně skákání mezi tématy.
- Otázky: Státnicové okruhy ve větším detailu.
- Algoritmy pro kritickou sekci. Základní synchronizační primitiva a jejich použití. Prostředky pro synchronizaci vláken. Prostředky pro synchronizaci procesů. Koordinace času v DS. Vzájemné vyloučení v DS. Volba lídra v DS. Shoda v DS. Tolerance chyby v DS. Globální stav v DS. Replikace a konzistence v DS. Chord systém. Blockchain.
- Otázky se často prolínají!
- Vybraný/vylosovaný článek přehledově
  - O čem to je? K čemu to je? Jak to funguje? ...
  - Ne důkazy, ne technikálie, ...
- Detaily na webu.

Zpětná vazba?

Changelog