Blockchain a kryptoměny

Paralelní a distribuované systémy, přednáška 10

Tomáš Urbanec

Katedra informatiky PřF UPOL

9.12.2025

Co nás čeká?

1. Blockchain
   - Motivace a základy
   - Problémy a možná řešení
   - Bezpečnost
   - Bitcoin a Ethereum

Blockchain

Blockchain

Motivace a historie

- DLT (Distributed Ledger Technology) – distribuovaná účetní kniha
- Blockchain – implementace DLT (datové struktury, algoritmy, . . .)
- Myšlenka DLT již v 90. letech.
- Datové strukutry a potřebná kryptografie ještě dříve.
  - Algoritmy shody v DS,
  - Merkelovy stromy,
  - asymetrická kryptografie,
  - . . .
- První (teoretické) digitální měny v 80./90. letech.
  - DigiCash (anonymita, kryptografie),
  - B-money, Bit Gold (bez implementace),
  - . . .
- Bitcoin (2009)
  - první úplná implementace DLT,
  - popularita $\rightarrow$ i pro blockchain

Základy

Blockchain

- Bitcoin, Ethereum, Cardano, Dogecoin, *coin, ...
- Ale nejen kryptoměny:
  - DNS,
  - smart contracts,
  - lékářské záznamy,
  - volby,
  - IoT,
  - ...
- Nejen veřejné:
  - Nějaká míra centralizace, omezení přístupnosti nebo transparentnosti, ...
  - Privátní (centralizovaný),
  - Hybridní (řízený důvěryhodným konsorciem, s autentizací, ...)

Bloky a jejich provázání

Blockchain

- Blockchain – block chain – řetězec (provázaných) bloků
- Blok obsahuje:
  - data (transkace, záznamy, . . . , aplikační věci),
  - timestamp,
  - hash dat (většinou kryptografický),
  - hash předchozího bloku (většinou kryptografický),
  - další (různorodé).
- Bloky provázané do řetězce (dále).
- První blok v řetězci (genesis block) trochu jiný (v čem?).
- Hash dat v bloku:
  - většinou kryptografický (SHA-256, . . .),
  - snadné ověření (důležité),
  - často použit hašový (Merkle) strom (dále).

Bloky a jejich provázání

Blockchain

- Každy blok (kromě genesis) obsahuje hash předchozího bloku.
- Rekurzivní vlastnost.

$\rightarrow$ Předchozí bloky prakticky nelze změnit.

- Při změně bloku n nebude sedět hash v blocích $> n$.

$\rightarrow$ Podvod je snadno detekovatelný.

- Každý uzel může mít vlastní kopii blockchainu.
- Ale stačí shoda na jednom (posledním) bloku.
- Se shodou to není jednoduché (byzantské uzly, velká síť, dále)
- Může exitovat více konkurenčních bloků $\rightarrow$ větve $\rightarrow$ pravděpodobnostní volba $\rightarrow$ eventuální konzistence.

Datové struktury

Blockchain

- Bloky (tabule)
- Merkle tree
  - Ralph Merkle, 1979.
  - Hašový strom (obvykle binární).
  - Obecná datová struktura.
  - Bitcoin, Ethereum, . . . , git, Btrfs, BitTorrent, . . .
  - (tabule)

Vrstvy a jejich problémy

Blockchain

- Které problémy DS blockchain řeší/musí řešit?
- Vrstvy
  1. Infrasturktura (HW).
  2. Síťová vrstva
     - změna uzlů,
     - šíření a ověřování informace.
  3. Datová vrstva (Bloky, transakce)
  4. Shoda (dále).
  5. Aplikační nástavby
     - kryptoměny,
     - „smart contracts“,
     - decentralizované aplikace,
     - ...
- Problémy
  1. Konzistence (CAP teorém $\rightarrow$ AP, ale eventuální C)
  2. Bezpečnost
  3. Anonymita (?)

Shoda, PoW

Blockchain

- Proof of Work
- Vytvoření nového validního bloku vyžaduje velké množství práce.
  1. Zájemce posbírá transakce do bloku.
  2. Sestaví základ bloku.
  3. Musí blok doplnit tak, aby vyřešil nějakou výpočetně náročnou hádanku.
  4. Hádanka ma upravitelnou obtížnost (dle aktuálních možností sítě).
- Kdo to zvládné první, získává odměnu za blok (poplatky, nové prostředky, . . .).
- Ověření validity bloku (výsledku hádanky) musí být triviální.
- Změna bloku = přepočítání všech dalších bloků $\rightarrow$ nereálné.
- Žádná centralizace = výkon je rozdělen mezi účastníky (dále)
- Problémy: spotřeba, pooly, rychlost.
- Např. Bitcoin a délka nulového prefixu hashe.

Shoda, PoS

Blockchain

- Proof of Stake
- Problémy PoW $\rightarrow$ místo práce zástava.
- Vytvoření nového bloku vyžaduje (relativně) velkou zástavu.
  1. Zájemce (validátor) nabídne zástavu (kryptoměnu daného blockchainu).
  2. Systém vybere zájemce
     - podle velikosti zástavy,
     - podle dlouhodobé důveryhodnosti,
     - s prvkem náhody.
  3. Vítěz posbírá transakce do bloku a připojí jej do sítě.
- Ostatní validátoři ověří platnost bloku ($\rightarrow$ odměna).
  - OK: Vítěz získává odměnu za blok (poplatky, nové prostředky).
  - KO: Vítěz ztrácí zástavu, je penalizován v síti, ...
- Podvod vyžaduje mít hodně prostředků $\rightarrow$ útok na sebe sama.
- Jinak odhalení $\rightarrow$ ztráta zástavy a možností.
- Problém: potenciální centralizace bohatsví (a moci).

Shoda, další

Blockchain

- Delegated PoS
  - vždy volena malá skupina validátorů,
  - váha hlasu podle majetku.
- Proof of Authority
  - předvybraná malá důvěryhodná skupina validátorů,
  - centraliazce autority.
- Proof of Elapsed Time
  - nutný důvěryhodný HW,
  - nutný robustní systém práce s časem.
- Practical Byzantine Fault Tolerance
  - založeno na BFT,
  - volby, toleracne byzanstkých uzlů,
  - problém se škálováním.
- ...

Hrozby

Blockchain

- 51% útok – ovládnutí většiny v síti
- Sybil(a) útok – vydávání se za více účastíků
- Eclipse útok – oddělení uzlu
- Chyby v chytrých smlouvách (smart contracts) – zneužití bugu
- Fyzická/linková vrstva – útoky na podpurné vrstvy
- Kryptografie – aktuálně kvantové počítače a SHA-256
- DDoS – přetížení sítě
- Sociální inženýrství – útoky na uživatele obecně

Příklady kryptoměn

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.

Changelog