Distribuované transakce, blockchain

Paralelní a distribuované systémy, přednáška 11

Tomáš Urbanec

Katedra informatiky PřF UPOL

11.12.2024

Co nás čeká?

1. Distribuované transakce
   - Motivace
   - Jedno-, dvou- a třífázový commit
2. Blockchain
   - Motivace a základy
   - Problémy a možná řešení
   - Bezpečnost
   - Bitcoin a Ethereum (příště)

Distribuované transakce

Distribuované transakce

Základy

- Transakce, která zahrnuje více uzlů v DS.
- Mezibankovní převod (různé systémy),
- zápis do více různých DB (i lokálně),
- ...,
- obecná změna více úložišť/systémů.
- Zaměříme se na distribuovaný commit.
  - $\approx$ Závěrečná fáze distribuované transakce.
    - Skutečné provedení změn na všech uzlech.
    - Musí být provedeno buď všude, nebo nikde.

Jednofázový commit

Distribuované transakce

- Naivní řešení.
- Procesy: koordinátor a následovnící.
- Koordinátor pošle všem následovníkům instrukci.
- Hotovo . . .
- . . . ale co když
  - uzel nejede?
  - zpráva nedojde?
  - uzel neumí reagovat dle požadavků?
  - . . .
- (tabule)

Dvoufázový commit

Distribuované transakce

- Rozumné řešení.
- Procesy: koordinátor a následovnící
- Koordinátor pošle všem VOTE_REQUEST.
  - Uzel je připraven → reaguje VOTE_COMMIT.
  - Uzel není připraven → reaguje VOTE_ABORT.
- Kooridnátor dostal zpět
  - všechny VOTE_COMMIT → GLOBAL_COMMIT.
  - alespoň jeden VOTE_ABORT → GLOBAL_ABORT.
- Uzel dostal GLOBAL_COMMIT → provede commit.
- (tabule)

Dvoufázový commit

Distribuované transakce

- Problémy?
  1. Koordinátor vypadne (následovník v READY)
  2. Následovník vypadne (koordinátor ve WAIT)
- Řešení:
  1. čekání na zotavení koordinátora, nebo domluva s ostatními.
  2. koordinátor čeká, nebo ABORT.
- Nejpoužívanější varianta.
- Např. PostgreSQL
  - PREPARE TRANSACTION,
  - COMMIT/ROLLBACK PREPARED.
  - Neplést s (klasickými) transakcemi.

Třífázový commit

Distribuované transakce

- Řeší problémy dvoufázového commitu.
  1. Ze žádného stavu nelze volit rovnou COMMIT nebo ABORT.
  2. Neexistuje stav, kde neznáme výsledek a lze přejít do COMMIT.
- Nový (mezi)stav PRECOMMIT a zpráva PREPARE-COMMIT.
- (tabule)
- Problémy?
  1. Kordinátor vypadne (následovník READY nebo PRECOMMIT)
  2. Následovník vypadne (koordinátor v PRECOMMIT)
- Řešení:
  1. čekání na zotavení koordinátora, nebo domluva s ostatními (většina READY $\rightarrow$ ABORT).
  2. koordinátor čeká, pak COMMIT (vyžaduje zotavení u následovníka)

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

Changelog