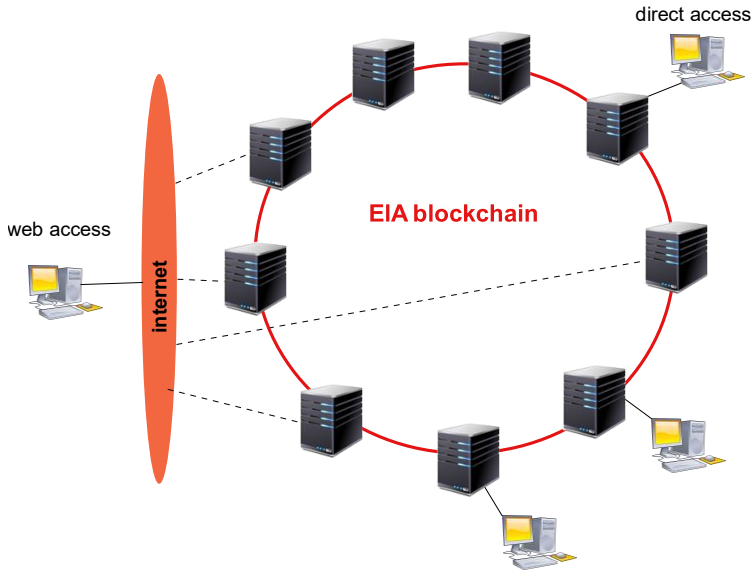
ELA Blockchain Services

Blockchain v průmyslu

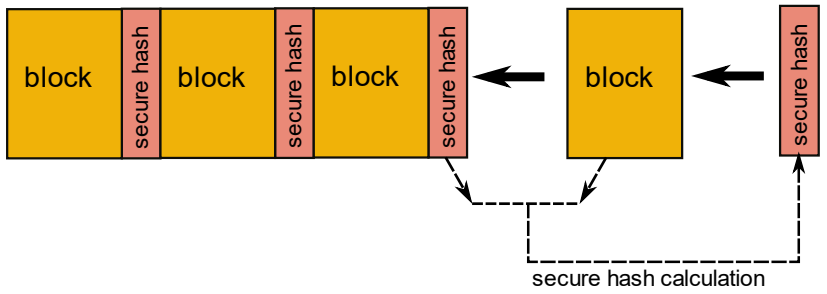
Co je blockchain

Blockchain je nezničitelná a nezfalšovatelná databáze.
Kombinuje dva základní technické principy. První z nich jej činí nezničitelným, druhý nezfalšovatelným.

Distributed Ledger Technology,
nezničitelná databáze



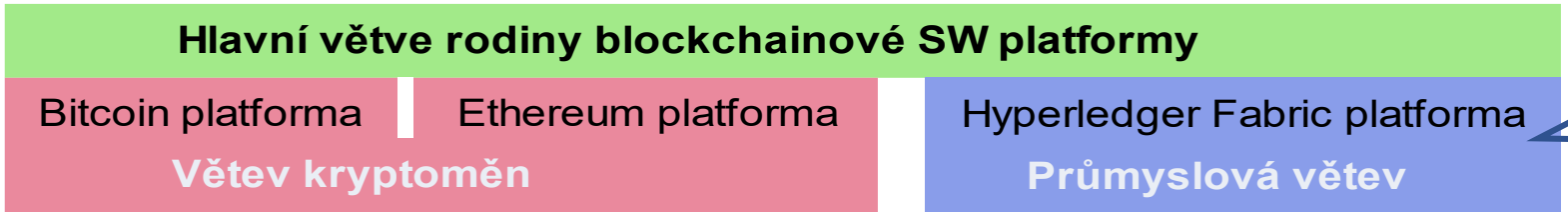
Sekvenční blockchainový soubor,
nezfalšovatelná databáze



oproti standardní databázi omezená počet operací:
čtení, zápis, ~~modifikace~~, ~~mazání~~

Průmyslový blockchain, jak ho chápe EBS

1. **průmyslová technologie**:



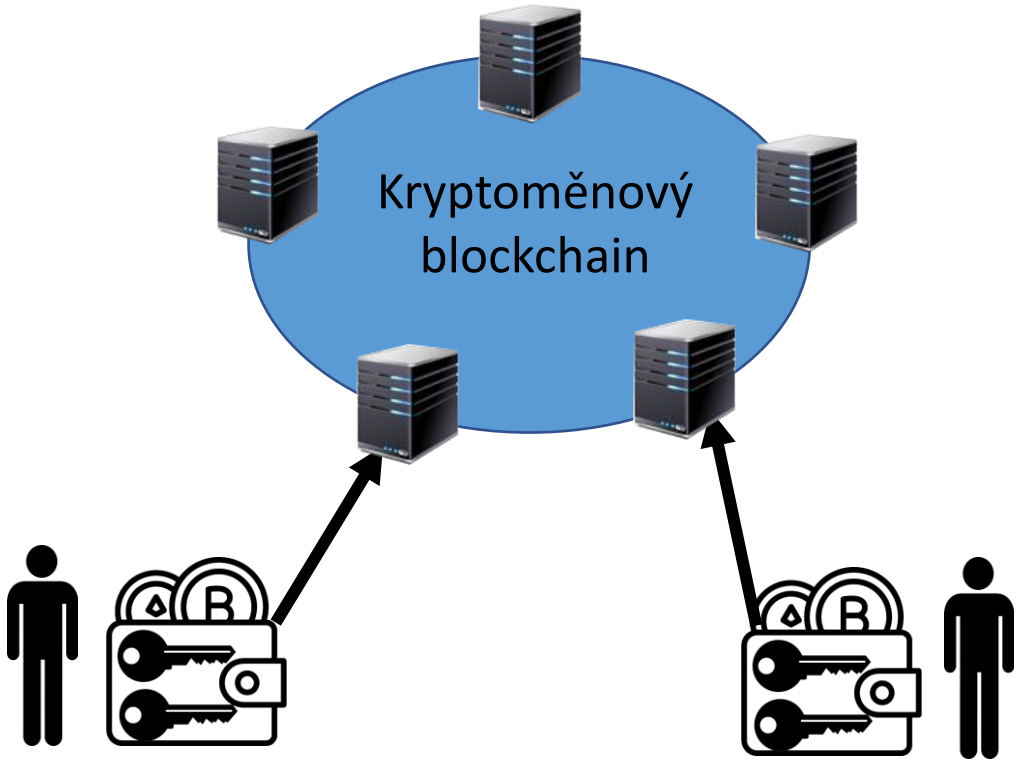
Hyperledger Fabric je velký open-source projekt, s účastí 17 tisíc vývojářů, podporovaý IBM

2. **blockchain konsorciálního typu**:

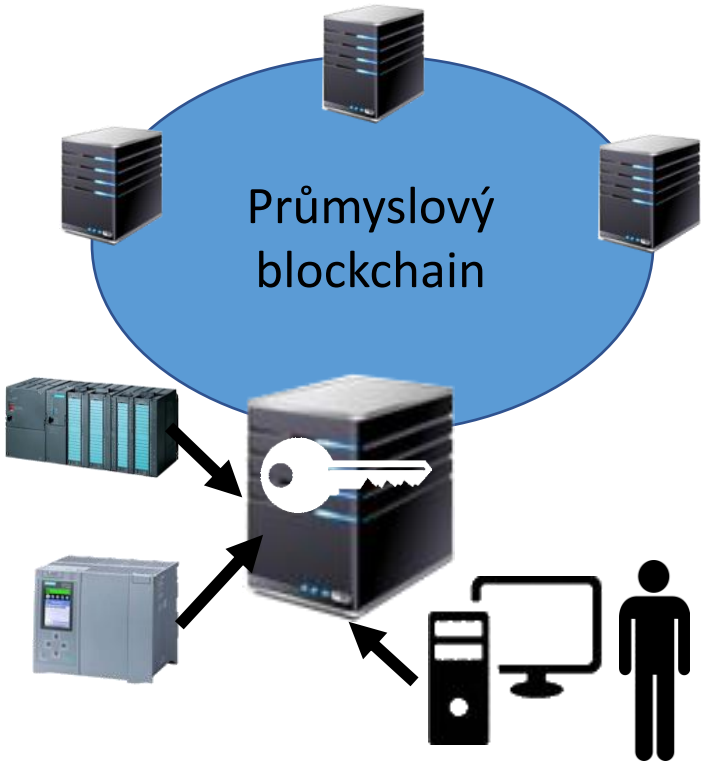
typ blockchainu	veřejný	privátní	konsorciální
typické aplikace	kryptoměny	kyb. bezpečnost	veřejná autorita
majitelé nodů	anonymní	jeden vlastník	uzavřená skupina
přístup a operace	bez povolení	s povolením /povoluje vlastník	řízeno pravidly konsorcia, která jsou vložena do blockchainu
rychlost transakcí	nízká	vysoká	vysoká

Pravidla konsorcia (členství, členská práva, změny v blockchainu) jsou uložena přímo v blockchainu jako software policies **nelze je porušit ani obejít**

Přístup k blockchainu



přímý přístup
přes jakýkoliv node

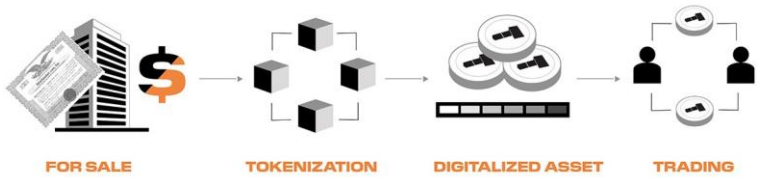


hierarchicky
uspořádaná
přístupová práva na
nodu organizace

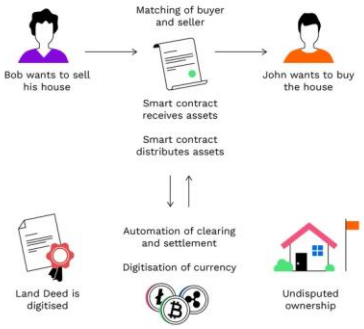
Tokeny a smart kontrakty

Kryptoměny

Kryptoměnový token



jednoduchý smart contract



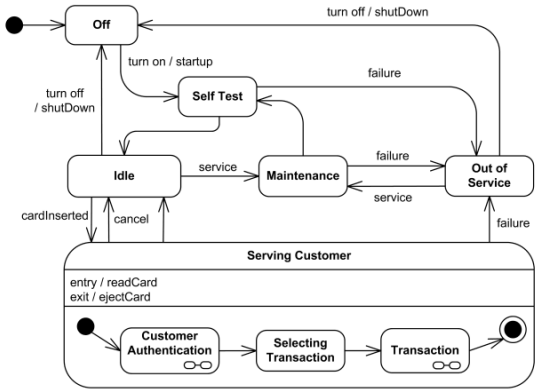
Průmyslový blockchain

advanced token

JSON

- strukturovaný modulární digitální objekt
- může reprezentovat virtuální dvojče skutečného objektu

konečný automat



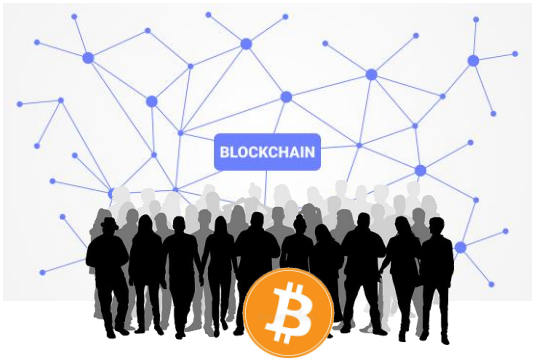
- může představovat mnohem složitější proces než smart kontrakt
- programuje se v GO (strukturovaný typovaný jazyk vycházející z C)

Blockchain jako distribuovaná autorita

Původní účel blockchainu:
náhrada databáze transakcí v bance nezničitelnou a nezfalšovatelnou blockchainovou databází

bankovní databáze se záznamy transakcí

nahrazena



nezničitelná a bezfalšovatelná blockchainová databáze

centrální autorita banky

nahrazena

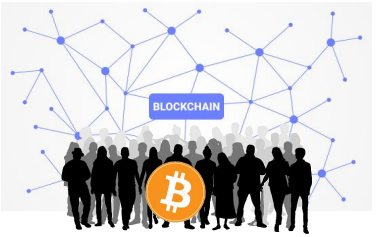
distribuovaná autorita

Blockchain sám o sobě není autoritou !
Je technickým prostředkem, který umí sdružit množství dílčích a ne vždy důvěryhodných autorit majitelů nodů (= kopií databáze) do využitelné necentrální autority za podmínek:

- **dílčí autority jsou nezávislé**
- **v každém okamžiku je mezi nimi část důvěryhodných**
- **existuje důvěryhodný ověřitelný proces přidání nového bloku**

Podmínky 1 a 2

Veřejný blockchain – využívá důsledků teorie pravděpodobnosti



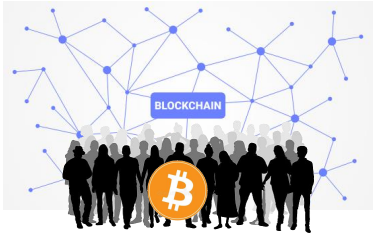
1. Nezávislost nodů
   - využívá vlastností náhodného výběru: anonymita
2. Část účastníků je důvěryhodná
   - vyplývá ze zákona velkých čísel: rozložení poctivců a zločinců je stejné jako v populaci

Princip veřejného blockchainu zaručuje splnění těchto podmínek při dostatečném počtu nodů

Konsorciální blockchain – malý počet nodů, nelze využít teorie pravděpodobnosti

1. Nezávislost nodů
   - nezávislost správy nodu (žádná centrální správa, nelze zvenčí vypnout, nebo upravit SW)
2. Důvěryhodnost účastníků
   - členy konsorcia je nutné motivovat k loajalitě ke konsorciu i uživatelům

3. Proces přidání nového bloku



Kryptoměnový blockchain – vychází z teorie her

postup:

- výběr nodu, který transakci zpracuje a nový blok rozešle (Block Proposer Selection)
  - algoritmus založený na „ekonomické obtížnosti“ – PoW (Bitcoin), PoS (Ethereum)
- sestavení, rozeslání bloku a potvrzení jeho validity všemi nody v síti (consensus algorithm)
  - Nakamotův algoritmus - je přijat je blok, podporovaný většinou výpočetního výkonu sítě

Průmyslový blockchain – deterministický

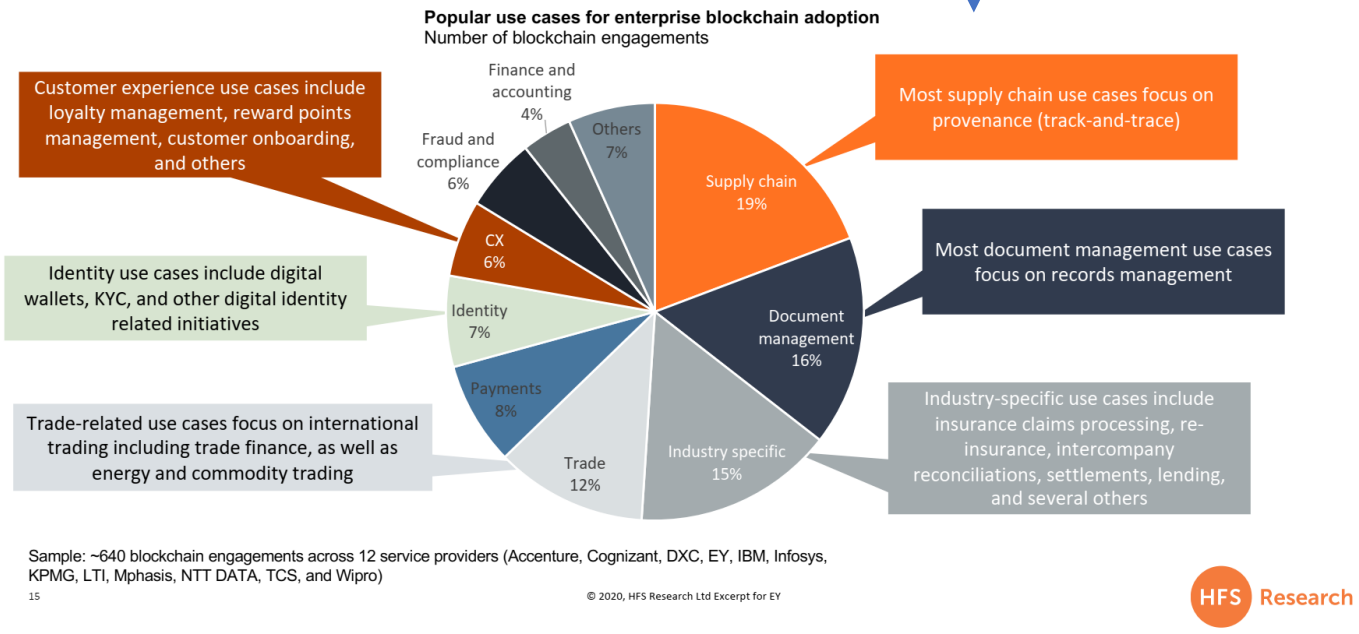
proces má čtyři fáze

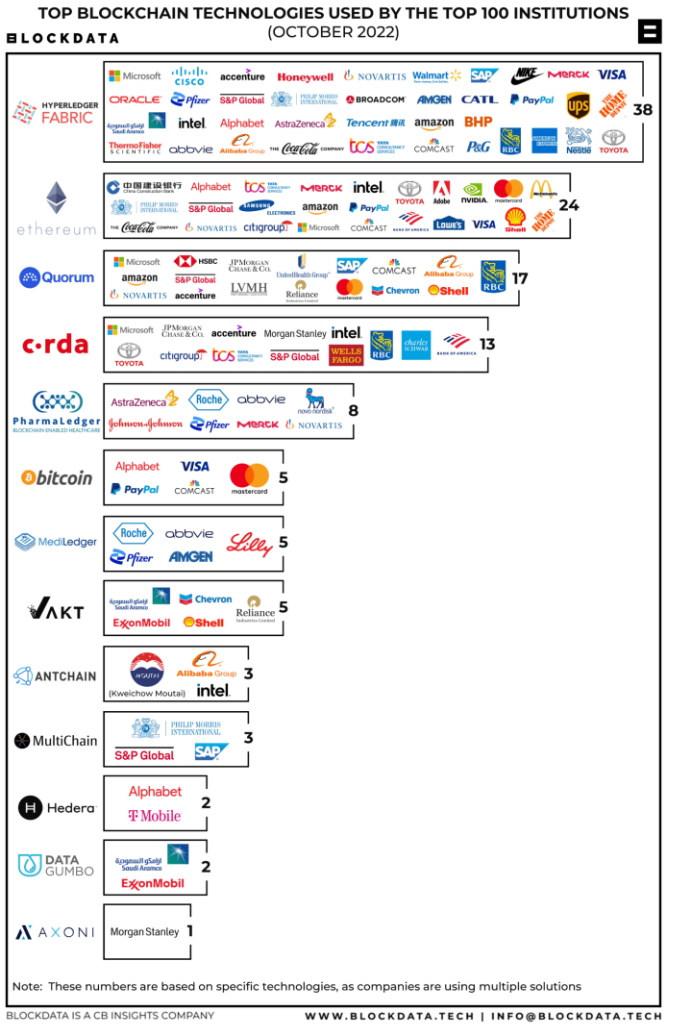
- výběr nodu, sestavení bloku, rozeslání bloku
  - každou část provádí jiná skupina nodů
- potvrzení validity bloku – deterministické algoritmy
  BFT (Byzantine Fault Tolerance), PBFT (Practical Byzantine Fault Tolerance)

Blockchain v průmyslu a službách

pořadí blockchainových platforem v roce 2022

aplikace blockchainu v průmyslu a službách





Využití blockchainu

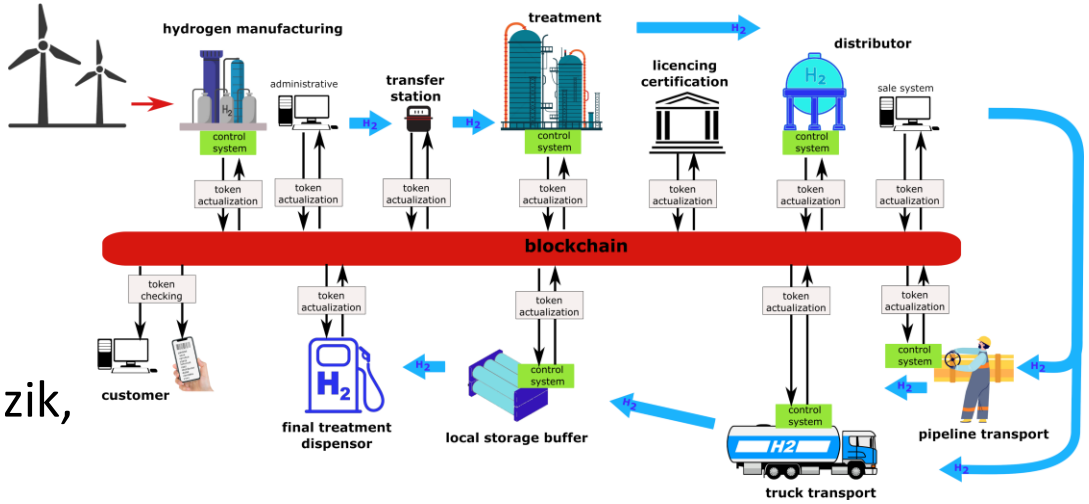
Blockchain je nástroj pro snižování míry rizika

kryptoměny – snížení rizika investice do fiat měn
NFT – snížení rizika falšování registrace aktiv

zde blockchain umožňuje vytvořit investiční produkty s nižší mírou rizika (b2c)

průmysl
snížení rizika falšování značky
snížení rizika administrativních chyb či zločinu
(b2b)

v průmyslu existují nástroje pro snižování těchto rizik,
blockchain umožňuje jen snižování nákladů



neúspěch projektu TradeLens společnosti MAERSK

Budoucnost blockchain v průmyslu

Blockchain umožní ošetřit komplexní rizika, která teprve vznikají v souvislosti s nasazením AI

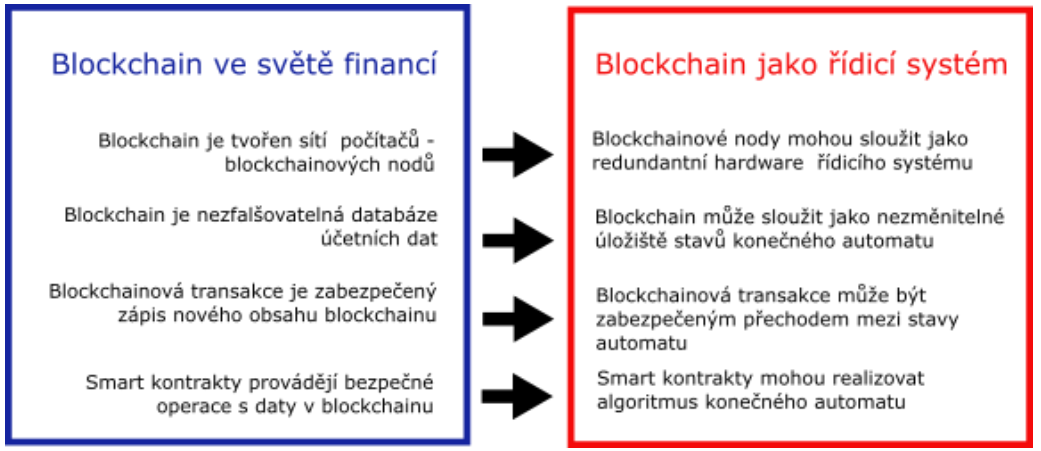
sofistikované napadení napříč několika vrstvami výrobního a distribučního procesu – obchodní, datovou, výrobní, logistickou.. s využitím AI a deep fakes

Blockchain nemusí být jen databáze, umožňuje vytvořit fail-safe a kyberneticky bezpečný řídicí systém spojuje dvě ochrany, které se dosud řeší odlišnými nespolupracujícími systémy:

- provozní bezpečnost (fail-safe, fault-tolerant)
- kybernetická bezpečnost

- patentová přihláška ELA Blockchain Services

takový systém bude nezbytný proti komplexním útokům



Děkuji za pozornost

Otto Havle, COB / CEO
havle@elachain.cz
https://www.linkedin.com/in/otto-havle-b1046616/

ELA Blockchain Services webová stránka (CZ + E)
https://www.elachain.cz/
Základní informace o firmě a ElA blockchainu

NABRE (Národní Blockchainový Registr)
https://www.nabre.cz/
Platforma pro blockchainové aplikace

Náš akcionář: **Elektrotechnická asociace České republiky**
www.electroindustry.cz