# Blockchain

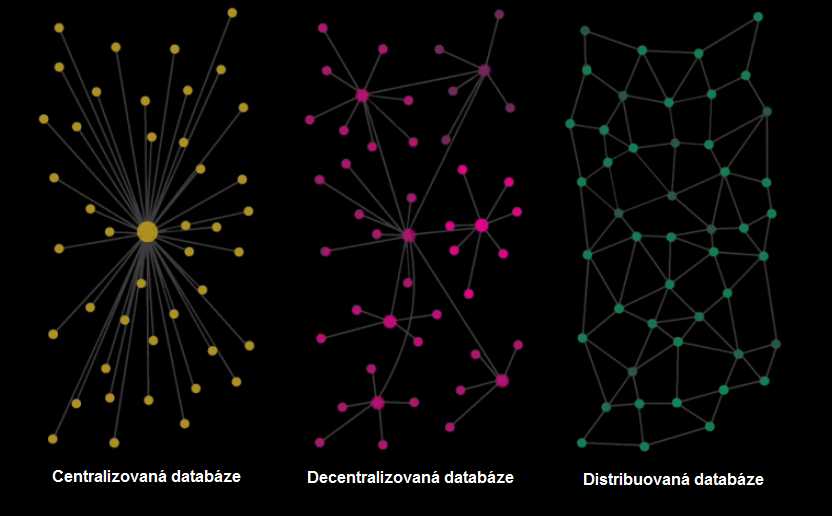
* Systém pro uchovávání dat
* Podobnost s databází

|  |  |
| --- | --- |
| Tradiční databáze | Blockchain |
| Centralizovaná | Decentralizovaný |
| Administrátor | Peer to peer |
| Relační data | Real-time data |
| CRUD operace | Pouze vkládání dat |
| Autentizace a Autorizace | Kryptografické mechanismy v každém bloku |
| Master-slave / Master-master | Replikace v každém bloku |

* Vznikl již v 80. letech, ale reálné využití nalezl až díky Bitcoinové síti v roce 2008

## Výhody Blockchainu

* **Decentralizace**
  + Síť neřídí jedna hlavní organizace, ale samotní uživatelé
* **Rychlost**
  + Přímý přístup do blockchainu bez zdržujících prostředníků
* **Distribuovanost**
  + Každý uzel v síti má přístup k databázi a její celé historii
* **Transparentnost**
  + Kdokoliv si může zobrazit jakoukoliv transakci
* **Bezpečnost**
  + Šifrování dat v každém bloku pomocí algoritmů SHA-2 a SHA-3
* **Imutabilita**
  + Data uložená do blockchainu nemůžou být změněny nebo smazány



## Využití blockchainu

1. Finanční sektor

Transparentnost a důvěryhodnost blockchainu umožňuje rozvoj takzvaných chytrých kontraktů (smart contracts), kdy si jednotliví uživatelé posílají platby a zboží přímo mezi sebou (peer to peer), bez asistence právníků, bank, úřadů a dalších prostředníků. O plnění podmínek kontraktu se stará technologie. Což znamená zrychlení, zefektivnění a zlevnění. Blockchainové technologie pracující s kryptoměnami zároveň výrazně zrychlují a zlevňují platby do zahraničí.

1. Zdravotnictví

Poskytovatelé zdravotní péče mohou využít blockchain k bezpečnému ukládání lékařských záznamů svých pacientů. Když je lékařský záznam vytvořen a podepsán, může být zapsán do blockchainu, což pacientům poskytuje důkaz a jistotu, že záznam nelze změnit. Tyto osobní zdravotní záznamy by mohly být zakódovány a uloženy na blockchainu pomocí soukromého klíče, takže jsou přístupné pouze určitým jednotlivcům, čímž je zajištěno soukromí, snadná manipulace a komunikace mezi doktory a institucemi.

Je možné představit si to jako centrální databázi pacientů, kterou si ale na rozdíl od té naší nemůže nikdo „jen tak“ listovat. Vždy je k tomu potřeba nějaký vstup od pacienta nebo jeho blízkých.

1. Úřady

Pokud jste někdy strávili čas na místním úřadu ohledně záznamu majetku, budete vědět, že proces zaznamenávání vlastnických práv je obtížný a neefektivní. Dnes musí být dokumenty fyzicky doručeny vládnímu zaměstnanci na místním úřadu, kde jsou ručně zadány do centrální databáze kraje a veřejného indexu. V případě sporu o majetek musí být nároky na majetek sladěny s veřejným indexem.

Tento proces není jen nákladný a časově náročný - je také protkán lidskou chybou, kde každá nepřesnost způsobuje, že sledování vlastnictví nemovitosti je méně efektivní. Blockchain má potenciál eliminovat potřebu skenování dokumentů a sledování fyzických souborů v místním úřadu. Pokud je vlastnictví nemovitosti uloženo a ověřeno na blockchainu, mohou vlastníci věřit, že jejich záznam je přesný a trvalý.

1. Hlasovací systémy

Hlasování s blockchainem přináší potenciál k eliminaci volebních podvodů a zvýšení účasti voličů, jak bylo testováno ve volbách v Západní Virginii v listopadu 2018. Každý hlas by byl uložen jako blok na blockchainu, takže by bylo téměř nemožné s ním manipulovat. Protokol blockchain by také udržoval průhlednost ve volebním procesu, snížil by počet zaměstnanců potřebných k provedení voleb a poskytoval by úředníkům okamžité výsledky. Jednoduše řečeno, vše by bylo transparentnější a jednodušší. Proč toho nevyužít?

1. Trh s uměním

Na trhu působí blockchainové kartotéky uměleckých děl, jako třeba americká Artory, která shromažďuje ověřené informace o původu a historii díla a kupcům přitom zaručuje anonymitu. S tou už začala spolupracovat třeba významná aukční síň Christie’s. Příkladem byla listopadová aukce sbírky amerického investora Barneyho Ebswortha (kolekce se rozprodala za 318 milionů dolarů, tedy asi 7,2 miliardy korun), kdy se veškeré transakce evidovaly v Artory.

Společnost De Beers, největší producent diamantů na světě, začala využívat blockchain k ověření autenticity původu těchto drahokamů. Snaží se tak vyhnout obchodování s „krvavými diamanty“ z oblastí Afriky ovládaných různými gerilami, které takto financují svá válečná tažení. Další velcí světoví producenti diamantů a výrobci šperků využívají coby garanta autenticity blockchainovou technologii TrustChain od IBM.

1. Automobilový průmysl

Průkopníkem v aplikaci blockchainu do automobilů je firma Porsche. Ta nyní testuje odemykání a zamykání vozu pomocí mobilní aplikace propojené s blockchainem. Majitel může přes aplikaci na stanovenou dobu propůjčit digitální klíčky od auta jiné osobě. Třeba dalšímu členu rodiny, jenž si vůz potřebuje půjčit, mechanikovi, který ho má odvézt do servisu, nebo doručovateli, který má uložit do kufru auta balíček.

**Umělá inteligence v systémech autonomního řízení se orientuje podle obrovského množství cloudových dat**. Pokud by měla centrální databáze výpadek, může to mít na [samořiditelná auta](https://www.csas.cz/cs/firmy/articles/samoriditelna-auta-spasa-nebo-cesta-do-pekel) a [jiné autonomně řízené dopravní prostředky](https://www.csas.cz/cs/firmy/articles/budoucnost-letecke-prepravy-2), které se zrovna pohybují s lidskou posádkou, katastrofální následky. Decentralizovaný blockchain by toto riziko odstranil. Zároveň by takovou databázi nemohli ovládnout hackeři. A v neposlední řadě by tak bylo možné lépe ověřovat správnost dat, která jednotlivé autonomně řízené dopravní prostředky sbírají o svém okolí a předejít tak chybám a nehodám.

## Typy blockchainů

1. Veřejný

Většina dnešních blockchainů je veřejná. To znamená, že se k nim může připojit kdokoli a všichni účastníci sítě mohou vidět sdílenou distribuovanou účetní knihu a podílet se na ověřování transakcí. Tento typ blockchainu je obvykle postaven na konsensuálním mechanismu proof-of-work (PoW), takže účastníky sítě lze nazývat těžaři. Pod veřejným blockchainem si můžeme představit například Bitcoin nebo Ethereum.

Stejně jako všechno, i blockchainy mají své výhody a nevýhody. U veřejného blockchainu je výhodou decentralizace, takže jej nikdo neovládá, transparentnost, všechny transakce jsou viditelné, je velmi odolný vůči cenzuře a je přístupný, může se k němu připojit kdokoli. Mezi nevýhody patří energetická neefektivita kvůli PoW a sledovatelnost transakcí, i když jsou účastníci anonymní, transakce jsou dohledatelné.

1. Soukromý

Tento typ sítě je pouze na pozvání. Existuje tedy centrální subjekt, který kontroluje, kdo se může k síti připojit. Zároveň mohou být účastníkům přiděleny role a řídicí subjekt může upravovat, mazat nebo rušit transakce. Mezi nejznámější sítě patří Morpheus (blockchain pro logistiku a dodavatelské řetězce) nebo Patientory (aplikace pro lékařské dodavatelské řetězce na platformě Ethereum).

Mezi výhody patří jednoznačně větší bezpečnost, protože díky kontrolám je méně účastníků s nekalými úmysly. Také větší škálovatelnost, změny jsou snadněji proveditelné, vyšší propustnost, kdy jsou transakce rychlejší, a větší důvěryhodnost díky omezenému přístupu a lepší identifikaci. Na druhou stranu tyto blockchainy nejsou dostatečně centralizované a mezi nevýhody patří skutečnost, že provozovatel může transakce měnit.

1. Hybridní

Hybridní blockchain je jedinečný typ technologie blockchainu, která spojuje součásti veřejného i soukromého blockchainu nebo se snaží využít ideální část veřejných i soukromých blockchainových řešení. Transakce a záznamy v hybridním blockchainu jsou soukromé, ale lze je ověřit, pokud jsou s tím spojeny, například povolením přístupu prostřednictvím chytré smlouvy. Soukromé informace jsou uchovávány v síti, ale stále je lze ověřit.

Ačkoli soukromý subjekt může vlastnit hybridní blockchain, nemůže měnit transakce. Hybridní blockchain umožňuje organizacím založit soukromý systém založený na oprávnění vedle veřejného systému bez oprávnění, což jim umožňuje spravovat, kdo má přístup ke konkrétním datům uloženým v blockchainu a která data budou zveřejněna.

1. Sidechain

Špičkové blockchainy jako Bitcoin a Ethereum historicky trpěly nedostatečnou škálovatelností. Existuje tolik platforem s téměř nesčetnými případy použití, ale odesílání kryptografických aktiv v řetězci často nutí uživatele, aby si vybrali mezi časem a náklady. Naštěstí ve vývoji existuje řešení škálovatelnosti zvané blockchain sidechain. Nyní se podívejme na definici sidechainu a důležitost této technologie.

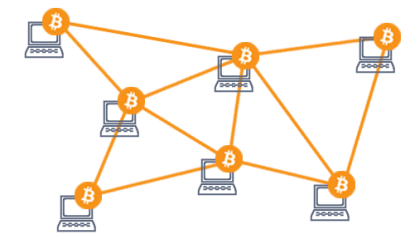
Sidechain se skládá z blockchainové sítě vázané na hlavní řetězec. Použijme Bitcoin jako příklad.

Pokud někdo chce využít sidechain připojený k bitcoinovému protokolu, musí uzamknout určité množství BTC odesláním na výstupní adresu na sidechainu. Po krátké době jsou nyní zaslané prostředky k dispozici na vedlejším řetězci.

## Pod kapotou bitcoinu

Jak tedy ten známý bitcoin funguje a jak souvisí s blockchainem? Velká globální účetní kniha ověřená kryptografií by bylo asi to nejjednodušší vysvětlení. Pojďme si to ale rozvést.

Bitcoinová síť má několik druhů účastníků. Prvním z nich jsou lidé provozující bitcoinové uzly (anglicky “bitcoin nodes”). Dále jsou zde těžaři (anglicky “bitcoin miners”) a v neposlední řadě tu jsou uživatelé, kteří bitcoin používají pro placení.



### Uzly

Již zmíněná účetní kniha je uložená právě v uzlech. Úkolem bitcoinových uzlů je zajišťovat komunikaci a zapisovat transakce. Uzly umožňují těžařům dělat svoji práci. Musí se kolektivně shodovat na pohybech účetní knihy (anglicky se kolektivní shodě říká “consensus”).

***Těžba bitcoinu znamená spolupráci mezi těžaři a provozovateli uzlů, kteří společně udržují bitcoinovou síť bezpečnou.***

Zmiňovaný uzel si můžete na svém počítači spustit i vy. Se správným hardwarem to je ve skutečnosti velmi jednoduchý proces.

### Peněženky

Mají za úkol „přelouskat“ blockchain a uživateli dát srozumitelné informace. Jednoduše od nich můžete očekávat to, co byste očekávali od peněženky ve vaší kapse nebo od vašeho bankovního účtu. Peněženka zobrazí váš aktuální zůstatek a také historii plateb. Díky peněžence můžete také vytvořit novou transakci a odeslat vaši kryptoměnu na jinou adresu.

Existují dva druhy peněženek, **softwarové a hardwarové**. Jak názvy napovídají, softwarová peněženka nabízí řešení v podobě programu v počítači nebo chytrém telefonu, zatímco hardwarová je fyzicky hmatatelné zařízení.

### Transakce

Zastánci kryptoměn tvrdí, že bitcoin a další coiny nahradí v budoucnu běžné měny. Mohou kryptoměny nahradit českou korunu, euro nebo americký dolar? Bylo by to vůbec technicky možné?

Již dnes není žádný problém odeslat své BTC (nebo jeho část) druhé osobě. Vše, co k tomu potřebujete, je mít nastavenou kryptoměnovou peněženku (nebo alespoň privátní a veřejný klíč). Pokud budete chtít odeslat své BTC kamarádovi, učiníte následující:

1) Vypíšete adresu peněženky vašeho kamaráda, případně naskenujete QR kód s jeho adresou.

2) Zvolíte množství BTC, které chcete odeslat.

3) Kryptograficky transakci podepíšete.

Když vezmeme v potaz, že třetí krok za vás řeší kryptoměnové burzy či peněženky, tak v porovnání s běžným bankovním účtem se náročnost provedení transakce z pohledu běžného uživatele nijak neliší. Naopak je postup v některých ohledech jednodušší.

Například pokud budete chtít poslat peníze do Číny, bude potřeba vyplňovat spoustu údajů o příjemci peněz. Navíc transakce přijde na účet zpravidla až za několik pracovních dní. Kryptoměny jsou v tomto ohledu “user-friendly” neboli jejich použití je snazší pro běžného uživatele. Díky novým technologiím jako je Lightning Network proběhne transakce doslova jen během několika vteřin.

### Blockchain a Bitcoin

To, čemu říkáme blockchain, je právě již zmiňovaná účetní kniha (anglicky “ledger”). Výraz “blockchain” je tak složen ze dvou anglických slov “block” (v překladu “blok”) a “chain” (v překladu “řetěz” nebo také “svázat”). Co to tedy je?

Představte si, že jste bankéř v roce 1980. Žádné počítače k dispozici nejsou, jenom papír a tužka. Vynalezli jste novou měnu zvanou Bitcoin (zkráceně BTC) a jako správný bankéř potřebujete udržovat pořádek v tom, kdo má kolik peněz na účtu.

Na prázdný papír budete zapisovat transakce, dokud nebude papír plný. Třeba Bob poslal Alici 0,2 BTC, Alice poslala Honzovi 0,1 BTC a tak dále. Poté, co se tento papír naplní, připíšete číslo stránky, nicméně nejen té současné, ale i předchozí, z toho důvodu, aby bylo bezesporu jasné, jak jdou stránky v účetní knize po sobě. Na závěr stránku podepíšete a založíte ji do účetní knihy.

Jedné takové stránce v účetní knize říkáme blok. První stránka v této účetní knize se nazývá “genesis block” a každá další stránka je schopna pojmout až 1 MB (dat) transakcí.

Pokud na druhé stránce je explicitně zmíněna stránka první, vytváříme tak vztah, kdy první stránka se váže na druhou stránku, následně druhá stránka třetí, třetí na čtvrtou a tak dále. **Blockchain je vlastně hromada stránek popsaných transakcemi v účetní knize s jasně daným postupem, jak vkládat jednotlivé stránky za sebe.**