Blockchain

Blockchain je decentralizovaná, distribuovaná a neměnná databáze (účetní kniha), která slouží k zaznamenávání transakcí v síti mnoha počítačů. Hlavní vlastností je, že jakmile jsou data do blockchainu zapsána, je extrémně obtížné je zpětně změnit bez narušení celého řetězce.

Ačkoliv je nejvíce spojován s kryptoměnami (jako Bitcoin), jeho využití sahá od logistiky až po státní správu.

Architektura a princip fungování

Blockchain se skládá ze tří hlavních prvků, které zajišťují jeho bezpečnost:

1. Bloky (Blocks)

Data jsou seskupována do bloků. Každý blok obsahuje:

- **Data:** Informace o transakci (odesílatel, příjemce, částka).
- **Hash:** Unikátní digitální otisk bloku (jako otisk prstu).
- **Hash předchozího bloku:** Toto je klíčový prvek, který vytváří „řetězec“.

2. Hashování (Hashing)

Pokud se v bloku změní jediný bit dat, jeho hash se zcela změní. Protože následující blok obsahuje hash bloku předchozího, jakákoli změna v historii způsobí, že všechny následující bloky se stanou neplatnými.

3. Decentralizace (P2P síť)

Blockchain neběží na jednom serveru, ale je sdílen tisíci počítači (uzly - nodes) po celém světě. Každý uzel má kompletní kopii celé historie. Před přidáním nového bloku se musí síť shodnout na jeho platnosti pomocí mechanismu konsensu.

Mechanismy konsensu (Consensus Models)

Aby mohl být do sítě přidán nový záznam bez centrální autority, musí existovat pravidla:

- **Proof of Work (PoW):** Uzly (těžaři) řeší složité matematické úlohy. Vyžaduje obrovský výpočetní výkon a elektřinu. (Využívá Bitcoin).
- **Proof of Stake (PoS):** O platnosti rozhodují držitelé dané měny. Je energeticky mnohem úspornější. (Využívá Ethereum).

Klíčové vlastnosti

Vlastnost	Popis
Transparentnost	Každý může nahlédnout do historie transakcí (u veřejných blockchainů).
Neměnnost	Data nelze smazat ani upravit bez souhlasu většiny sítě.
Bezpečnost	Díky kryptografii a distribuci je odolný proti útokům i výpadkům.
Eliminace prostředníků	Umožňuje přímý přenos hodnoty (P2P) bez banky nebo notáře.

Typy Blockchainů

- **Veřejné (Public):** Kdokoli se může připojit, číst a zapisovat (např. Bitcoin, Ethereum).
- **Soukromé (Private):** Přístup je řízen jednou organizací (využití v korporacích).
- **Konsorciální:** Spravováno skupinou organizací (např. bankovní konsorcia).

Využití v praxi

- **Kryptoměny:** Digitální peníze bez centrální banky.
- **Chytré kontrakty (Smart Contracts):** Programy, které se automaticky spustí při splnění podmínek (např. automatické vyplacení pojistky při zpoždění letu).
- **Sledování dodavatelského řetězce:** Ověření původu zboží (např. zda je káva skutečně Fair Trade).
- **Digitální identita:** Bezpečné ukládání osobních údajů pod kontrolou uživatele.

Související pojmy: Bitcoin, Ethereum, Hash, P2P, Smart Contract, Cryptography, Decentralization.