

Blockchain: Kryptografie v akci

Blockchain je distribuovaná, decentralizovaná databáze (nebo také sdílená účetní kniha), která uchovává neustále rostoucí seznam záznamů. Jeho bezpečnost a nezměnitelnost stojí na třech pilířích [kryptografie](#).

1. Hašování a řetězení bloků

Základem blockchainu je **kryptografický hash** (typicky algoritmus **SHA-256**). Každý blok v řetězci obsahuje:

- Data (např. transakce).
- Vlastní hash bloku.
- **Hash předchozího bloku.**

Právě odkaz na hash předchozího bloku vytváří „řetězec“. Pokud by útočník změnil data v jednom bloku, změnil se jeho hash. Tím se přeruší vazba na následující blok a celý zbytek řetězce se stane neplatným.

—

2. Digitální podpisy (Asymetrická kryptografie)

Aby bylo zajištěno, že transakci může vytvořit pouze majitel prostředků, používá blockchain **asymetrickou kryptografii** (často na bázi eliptických křivek - ECDSA).

- **Privátní klíč:** Slouží k „podpisu“ transakce. Je to váš digitální přístup k prostředkům.
 - **Veřejný klíč:** Slouží ostatním uzlům v síti k ověření, že podpis je pravý, aniž by znali váš privátní klíč.
 - **Adresa:** Je odvozena z veřejného klíče a slouží jako „číslo účtu“.
-

3. Merkle Tree (Merkleův strom)

Pro efektivní ověřování velkého množství transakcí v jednom bloku se používá datová struktura zvaná **Merkle Tree**.

- Všechny transakce jsou hašovány v párech, dokud nezbyde jeden jediný výsledný hash - **Merkle Root**.
 - Merkle Root je uložen v hlavičce bloku. To umožňuje lehkému klientovi (např. mobilní peněženke) ověřit, že transakce je součástí bloku, aniž by musel stahovat všechna data celého blockchainu.
-

4. Mechanismus konsenzu (Proof of Work)

V distribuovaném systému (viz [Distribuované systémy](#)) musí všechny uzly souhlasit s tím, který blok je další. V Bitcoinu se k tomu používá **Proof of Work** (PoW).

- Těžaři hledají tzv. **Nonce** – číslo, které po přidání k datům bloku vytvoří hash začínající určitým počtem nul.
- Nalezení takového hashe je matematicky nesmírně obtížné a vyžaduje obrovský výpočetní výkon, ale jeho ověření ostatními je okamžité.

—

5. Smart Contracts (Chytré kontrakty)

Platformy jako Ethereum rozšiřují blockchain o možnost ukládat nejen data, ale i spustitelný kód.

- **Decentralizované aplikace (dApps):** Kód, který běží přesně tak, jak byl naprogramován, bez možnosti cenzury, podvodu nebo zásahu třetí strany.
- Využití v [e-commerce](#): Automatické uvolnění platby dodavateli až po potvrzení doručení zboží dopravcem.

Související články:

- [Základy kryptografie](#)
- [Teorie distribuovaných systémů](#)
- [Budoucnost financí a DeFi](#)

Tagy: it blockchain cryptography sha256 bitcoin ethereum decentralization

From:

<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

<https://www.serviceit.cz/doku.php?id=it:sw:blockchain>

Last update: **2026/01/02 20:09**

