Bitcoin (Decentralizovaná digitální měna)

Bitcoin (zkratka **BTC**) je digitální platidlo založené na technologii blockchainu. Funguje jako otevřený software, který nikdo nevlastní a nikdo jej nemůže centrálně vypnout nebo ovlivnit. Bitcoin bývá často označován jako „digitální zlato“ díky své omezené zásobě a odolnosti vůči cenzuře.

Jak Bitcoin funguje?

Bitcoin není fyzická mince, ale záznam v digitální účetní knize (blockchainu). Tato kniha je sdílena mezi tisíci počítači (uzly) po celém světě.

1. Transakce a digitální podpisy

Když pošlete Bitcoin, vytvoříte zprávu, kterou podepíšete svým soukromým klíčem pomocí digitálního podpisu. Ostatní v síti mohou pomocí vašeho veřejného klíče ověřit, že transakce je pravá, aniž by znali vaše heslo.

2. Těžba (Mining) a SHA-256

Nové transakce jsou seskupovány do bloků. Aby byl blok přidán do historie, musí těžaři vyřešit složitou matematickou hádanku založenou na algoritmu SHA-256. Tento proces se nazývá **Proof of Work** (Důkaz prací).

- Těžař, který hádanku vyřeší jako první, získá odměnu v podobě nově vytvořených bitcoinů.
- Tento proces zabezpečuje síť – útočník by musel mít větší výpočetní výkon než zbytek sítě dohromady, aby mohl historii přepsat.

Klíčové vlastnosti Bitcoinu

Vlastnost	Popis
Decentralizace	Neexistuje žádná centrální banka. Pravidla sítě vynucuje software.
Konečná zásoba	Celkový počet bitcoinů je omezen na **21 milionů**. To brání inflaci.
Transparentnost	Každá transakce v historii je veřejně dohledatelná v blockchainu.
Pseudonymita	Účty nejsou vázány na jména, ale na adresy (řetězce znaků).
Dělitelnost	Jeden bitcoin lze rozdělit až na 8 desetinných míst. Nejmenší jednotka (0,00000001 BTC) se nazývá **Satoshi**.

Halving (Půlení odměny)

Zhruba každé čtyři roky dochází k události zvané **Halving**. Odměna pro těžaře za nový blok se sníží na polovinu. Tím se zpomaluje tempo vzniku nových mincí, dokud nebude kolem roku 2140 vytěžen poslední bitcoin.

Bezpečnost a uchovávání

Jelikož u Bitcoinu neexistuje tlačítko „zapomenuté heslo“, bezpečnost závisí na uživateli:

- **Horké peněženky (Hot Wallets):** Aplikace v mobilu nebo PC připojené k internetu. Pohodlné, ale méně bezpečné.
- **Hardwarové peněženky (Cold Storage):** Speciální zařízení (např. Trezor, Ledger), která drží soukromé klíče offline. Jsou nejbezpečnější ochranou před hackery.

Kritika a výzvy

- **Volatilita:** Cena Bitcoinu se může prudce měnit v řádu desítek procent během krátké doby.
- **Spotřeba energie:** Těžba vyžaduje obrovské množství elektřiny, což vyvolává ekologické debaty.
- **Rychlost:** Základní síť zvládne jen cca 7 transakcí za sekundu (pro srovnání: Visa zvládne tisíce). Tento problém řeší nadstavby jako **Lightning Network**.

Související pojmy: Blockchain, SHA-256, Digitální podpis, Kryptoměna, Satoshi Nakamoto, Mining, Lightning Network.