Mining (Těžba kryptoměn)

Mining je proces, který nahrazuje roli banky v decentralizovaných systémech. Zatímco v bance o platnosti transakce rozhoduje centrální autorita, v síti Bitcoin tuto práci vykonávají tisíce nezávislých počítačů – **těžařů** (minerů).

Těžaři za svou práci (poskytnutí výpočetního výkonu a elektřiny) získávají odměnu v podobě nově vzniklých mincí a poplatků od uživatelů.

Jak těžba funguje: Proof of Work (PoW)

Většina těžitelných kryptoměn využívá algoritmus **Proof of Work** (Důkaz prací). Celý proces lze přirovnat k obří celosvětové digitální loterii:

```
1. **Sběr transakcí:** Těžaři shromažďují nové transakce od uživatelů do tzv. kandidátského bloku.
2. **Hledání řešení (Hashing):** Těžaři se snaží najít specifické číslo (**nonce**), které po přidání k datům bloku a prohnání hashovací funkcí (u Bitcoinu [[sha-256|SHA-256]]) vygeneruje výsledek (hash), který začíná určitým počtem nul.
3. **Obtížnost:** Síť automaticky upravuje "obtížnost" (kolik nul musí být na začátku). Čím více těžařů je v síti, tím je těžší řešení najít.
4. **Vítěz bere vše:** První těžař, který najde platný hash, ohlásí výsledek ostatním. Ti ho během zlomku sekundy ověří a blok se přidá do blockchainu. Vítěz získá odměnu.
```

Hardware pro těžbu

S rostoucí obtížností se měnil i hardware, který je k těžbě potřeba:

- **CPU (Procesor):** V začátcích Bitcoinu (2009) stačil běžný domácí počítač.
- **GPU (Grafická karta):** Později se přešlo na grafické karty, které jsou mnohem efektivnější v paralelních výpočtech.
- **ASIC (Application-Specific Integrated Circuit):** Dnes se Bitcoin těží výhradně na těchto speciálních čipech navržených pro jediný účel – počítat SHA-256 extrémní rychlostí.

Typ hardwaru	Efektivita	Vhodné pro
CPU	Velmi nízká	Experimenty s novými měnami.
GPU	Střední	Ethereum (dříve), Monero, Dogecoin.
ASIC	Extrémní	Bitcoin, Litecoin.

Těžební pooly (Mining Pools)

Pravděpodobnost, že jeden těžař s jedním strojem najde blok v obrovské konkurenci, je dnes téměř nulová. Proto se těžaři sdružují do **poolů**.

- Pool kombinuje výkon všech připojených uživatelů.
- Když pool najde blok, odměna se rozdělí mezi všechny členy podle toho, kolik výkonu poskytli.

Kritika a energetická náročnost

Těžba pomocí Proof of Work je často kritizována za svou energetickou náročnost. Obrovský výpočetní výkon slouží k zabezpečení sítě, ale spotřebovává elektřinu srovnatelnou se spotřebou menších států.

- **Reakce:** Některé kryptoměny (např. Ethereum v roce 2022) přešly na model **Proof of Stake (PoS)**, který těžbu zcela odstraňuje a nahrazuje ji „zástavou“ mincí, což snižuje spotřebu energie o 99 %.

Související pojmy: Bitcoin, Blockchain, SHA-256, Proof of Work, Proof of Stake, ASIC, Hashování.