**„EU peníze školám“**

**Projekt DIGIT – digitalizace výuky na ISŠTE Sokolov**

**reg. č. CZ.1.07/1.5.00/34.0496**

|  |  |
| --- | --- |
| **III/2 Inovace a zkvalitnění výuky prostřednictvím ICT** | **VY\_32\_INOVACE\_18\_2\_03** |
| **Název vzdělávacího materiálu** | Virtuální měna - bitcoin |
| **Jméno autora** | Mgr. Miloslav Mládek |
| **Tematická oblast** | Zaměstnanci, trh, daňová soustava, národní hospodářství |
| **Vzdělávací obor** | 23-45-M/01 Dopravní prostředky |
| **Předmět** | Ekonomika |
| **Ročník** | 3., 4. |
| **Rozvíjené klíčové kompetence** | Kompetence k učení   * poznává smysl a cíl učení, má pozitivní vztah k učení, posoudí vlastní pokrok  a určí překážky či problémy bránící učení, naplánuje si, jakým způsobem by mohl své učení zdokonalit, kriticky zhodnotí výsledky svého učení a diskutuje o nich.   Kompetence komunikativní   * využívá informační a komunikační prostředky a technologie pro kvalitní a účinnou komunikaci s okolním světem.   Kompetence pracovní   * používá bezpečně a účinně materiály, nástroje a vybavení, dodržuje vymezená pravidla, plní povinnosti a závazky, adaptuje se na změněné nebo nové pracovní podmínky. |
| **Průřezové téma** | Občan v demokratické společnosti - naučí žáka orientovat se v masových médiích, využívat je jako zdroj informací. |
| **Časový harmonogram** | 1 vyučovací hodina |
| **Použitá literatura a zdroje** | Wikipedie: Otevřená encyklopedie: Bitcoin [online]. c2013 [citováno 9. 9. 2013]. Dostupný z WWW:  <http://cs.wikipedia.org/w/  index.php?title=Bitcoin&oldid=11011665>  Bitcoinman.cz [online]. [cit. 2013-09-09]. Dostupné z: http://bitcoinman.cz. |
| **Pomůcky a prostředky** | PC, internet |
| **Anotace** | Virtuální měna, bitcoin |
| **Způsob využití výukového materiálu ve výuce** | Výklad, samostatná práce |
| **Datum (období) vytvoření vzdělávacího materiálu** | Září 2013 |

*Tento výukový materiál je plně v souladu s Autorským zákonem (jsou zde dodržována všechna autorská práva). Pokud není uvedeno jinak, autorem textů   
a obrázků je Ing. Miloslav Mládek.*

**Výklad**

Bitcoin - virtuální open-source peněžní měna

* plně decentralizovaná - nemá žádnou centrální autoritu, žádnou centrální banku; vytváření mincí i potvrzování transakcí zajišťují jednotliví členové Bitcoin sítě, kolektivně;
* žádný prostředník - peníze se posílají přímo a ihned, bez prostředníků, bank, kreditních společností;
* celosvětová - lze je okamžitě poslat na druhý konec světa úplně stejně jako kamarádovi, který sedí vedle vás;
* neprolomitelná - princip Bitcoin sítě je zajištěn kryptografií a silným šifrováním;
* transakční poplatky neexistují nebo jsou extrémně nízké - transakce je potvrzena v řádu minut (zdarma nebo za tisícinu jednoho Bitcoinu);
* (pseudo)anonymní - všechny transakce i prostředky v peněžence jsou definovány pomocí adres (řetězec 34 znaků), žádné osobní údaje;
* přímá komunikace bez prostředníka (P2P) - uživatelé spolu komunikují přímo pomocí internetu, bez prostředníků;
* směnitelnost - Bitcoiny lze bez problémů směnit za jakoukoli jinou světovou měnu;
* otevřený kód - projekt má zcela veřejné a otevřené zdrojové kódy (každý může zkontrolovat přesné vnitřní fungování).

**Minéři** - potvrzují transakce; pro transakce, které čekají na potvrzení, se snaží najít takovou kombinaci, aby se její hash (výstup algoritmu pro převod vstupních dat do relativně malého čísla; z hashe je prakticky nemožné rekonstruovat původní text zprávy) vešel pod nějaký stanovený limit.

**Koncoví uživatelé** - lidé, kteří si za pomoci peněženky posílají peníze.

**Těžba (mining)** - proces, kdy počítačový hardware provádí matematické výpočty a potvrzuje transakce v bitcoin síti; postupně bude vytěženo přesně 21 milionů bitcoinů; těžba je distribuovaný systém shody, který se používá k potvrzení uskutečněných transakcí.

**Blok** - těžaři bitcoin sítě se snaží najít řešení matematického problému (potvrzování transakcí a zvyšování bezpečnosti); pokud miner úspěšně najde řešení, vytvoří tím nový blok, za který mu náleží odměna (potvrzené transakce se ukládají do bloků - zřetězené bloky se nazývají blockchain).

**Peněženka (wallet)** - ekvivalent běžné peněženky; ukazuje celkový počet bitcoinů, které zůstavají na adresách uživatelů; peněženka umožňuje poslat definované množství bitcoinů jinému uživateli na předem známou adresu.

**Mining pooly** - nalezení bloku je náhodný proces, pro malé minéry je výdělek velice nepředvídatelný, proto se minéři sdružují do tzv. mining poolů a zkoušejí štěstí společně - pokud některý z nich nalezne blok, odměna se rozdělí mezi všechny minéry (hlavní výhodou je větší předvídatelnost).

Na princip fungování mining poolu přišel český programátor Marek Palatinus.

V prvopočátcích se pro těžbu bitcoinů používaly klasické počítače, dnes se používají nejčastěji výkonné grafické karty, objevily se také specializované firmy, které se vyvinuly jednoúčelové čipy, které umí jednu věc, ale jsou extrémně rychlé a výkonné.

**Samostatná práce**

1. Proč je virtuální měna označována jako kryptoměna?
2. Za pomoci internetu najděte informaci o tom, jak se aktuálně vyvíjí kurz bitcoin a eura (např. http://bitcoinity.org/markets/mtgox/EUR).
3. Vysvětlete, co znamená následující zápis: 1BTC = 170741.91 CZK.
4. Najděte na internetu informace o organizaci Bitcoin Foundation. Jaký je její význam?
5. Proč bude vytěženo pouze 21 milionů BTC?
6. Jaká je nejmenší možná jednotka bitcoinu?
7. Odpovídá obchodování s bitcoiny pravidlům fair trade?