

# Uhlíková stopa technologie Bitcoin

Ondrej Klinovský (xbarto96)

Martin Bartoš (xbarto96)

9.12.2019

# Obsah

.....	1
1 Úvod.....	3
1.1 Zadání.....	3
1.2 Ověření validace modelu.....	3
2 Fakta.....	4
2.1 Termíny.....	4
2.2 Energie.....	5
3 Koncepce modelu.....	6
3.1 Použité metody.....	6
3.2 Obecná koncepce.....	6
3.3 Petriho síť.....	7
4 Experimenty.....	8
4.1 Referenční experiment.....	8
4.2 Experiment 1.....	9
4.3 Experiment 2.....	9
4.4 Experiment 3.....	10
5 Použití programu.....	11
6 Závěr.....	12

# 1 Úvod

Tato práce se zabývá problematikou uhlíkové stopy Bitcoinu. V současnosti existuje asi 1600 kryptoměn.<sup>[1]</sup> My jsme se ale zaměřili výhradně na Bitcoin, který je suveréně nejrozšířenější kryptoměna. Právě proto její dopad na uhlíkovou stopu je podstatně výraznější než u ostatních. Budeme simulovat protokol Bitcoin pomocí jednoduché Petriho sítě. Protokol Bitcoin spočívá v přijímání finančních transakcí, které se sdružují do bloků.

Pro každý blok je potřebné vyřešit matematicky i energeticky náročnou úlohu a to je důvod, proč celý proces Bitcoinu zanechává tak velkou uhlíkovou stopu. Vyřešení této úlohy je odměněné samotnými bitcoiny, víc a víc zařízení se připojují do sítě a tím síť vyžaduje víc energie. Smyslem našich experimentů bude ukázat, jak se mění uhlíková stopa při použití různých zdrojů energie.

## 1.1 Zadání

Zadání této práce spadá do kategorie „Uhlíková stopa informačních technologií“ a my jsme si vybrali problematiku „Uhlíková stopa technologie Bitcoin“.

## 1.2 Ověření validace modelu

Validita referenčního modelu byla ověřena daty z důvěryhodného zdroje.<sup>[3]</sup>

## 2 Fakta

Bitcoin je decentralizovaná digitální měna bez centrální autority (banky) založena na **blockchain** technologii. Je to síť tvořená uživateli a minery (těžaři).

### 2.1 Termíny

- **Blok** – struktura obsahující záznam transakcí (průměrně okolo 2000), nonce a odkaz na předešlý blok
- **Blockchain** – Řetězec bloků, kde změna pořadí bloků je nemožná díky odkazování se na předešlé bloky.
- **Uživatelé** – Lidé, kteří si posílají peníze. Když chce uživatel poslat někomu peníze, vytvoří transakci podepsanou svým soukromým klíčem a pošle tuto informaci do celé sítě. Příjemce tuto informaci obdrží okamžitě, avšak transakce ještě není potvrzena. V průměru se vytvoří asi 3-4 transakce za sekundu.
- **Minerů** – potvrzují transakce v síti. Miner seskupí transakce čekající na potvrzení (do bloku), přidá k nim odkaz na předcházející blok transakcí a tzv. Kryptografickou nonce. **Nonce** musí být menší jako limit, který je daný celou sítí. Nonce musí být menší, nebo rovna tomuto limitu. Limit tedy udává počet nul, kolika musí nonce začínat a vyjadřuje celkovou složitost sítě. Hodnota limitu je nastavena tak, aby minerům trvalo v průměru 10 minut k nalezení nonce. Za každý vypočítaný nonce je přiřazený nový blok od blockchainu, transakce v daném bloku jsou potvrzené a miner, který nonce vypočítal získává odměnu v podobě Bitcoinů.
- **SHA-256** – Kryptografická hashovací funkce, která pro libovolný vstup (např. Soubor), vrátí 256-bitové číslo. Když se dva vstupy budou lišit jen v jednom bitu, výstup bude úplně jiný.
- **Proof-of-work** – Když Bitcoin nemá žádnou centrální autoritu, která by ověřovala transakce, ověřování //TODO
- **Výkon sítě** (Hash rate) – Úlohou zařízení v síti je ověřovat Bitcoin transakce. Ověřování spočívá ve výpočtu matematicky komplikované úlohy. Čím víc práce je vyprodukováno, tím větší důvěra (proof-of-work). Podstatou této úlohy je spočítat hash bloku tak, aby byl menší jako cíl. Výkon sítě udává, kolik hashů (H) dokáže síť vypočítat za jednu sekundu. Dnes je toto číslo velmi velké a proto je tato hodnota udávána v terahash za sekundu (TH/s).

- **Náročnost** – míra, jak náročné je najít hash pro jeden blok, mění se každých 2016 bloků. Náročnost je nastavena tak, aby výpočet hashu bloku trval v průměru 10 minut bez ohledu na celkový výkon sítě.
- **Limit (target)** – 256-bitové číslo, které je sdílené s každým zařízením v síti. Vypočítaný hash bloku musí být menší, nebo rovný tomuto číslu, aby byl blok uznaný. Zjednodušeně řečeno, hash musí začínat určitým počtem nul. Čím menší limit (větší počet počátečních nul), tím vyšší složitost.

## 2.2 Energie

Podle našich zdrojů zaobírajících se energetickou náročností Bitcoinu je 68% těžařů z Asie, 17% z Evropy a 15% ze Severní Ameriky.

V **Asii** se daří hlavně kvůli tomu, že největším producentem je **Čína**, kde náklady na produkci elektrické energie jsou velmi nízké. Zjistili jsme, že hlavním zdrojem elektřiny v této oblasti pro zásobování těžařů je uhlí, které pokrývá **60%** z celkové produkce elektřiny. Navzdory tomu, že uhelné elektrárny produkují mnoho elektřiny za **nízkou cenu**, produkují **nejvíce CO<sub>2</sub>**.

V **Severní Americe** uhelné elektrárny produkují pouze 13% z celkové produkce energie a hlavním zdrojem je ropa (36%) a zemní plyn (30%). Díky těmto zdrojům je produkce elektrické energie šetrnější k životnímu prostředí, hlavně díky zemnímu plynu.

V **Evropě** je produkce elektrické energie nejšetrnější k životnímu prostředí díky obnovitelným zdrojům, které pokrývají přes 32% z celkové produkce. Musíme zahrnout i 25% zastoupení produkce elektřiny z jaderných elektráren. Pro zajímavost můžeme porovnat, že uhelné elektrárny produkují 993g/kWh CO<sub>2</sub> a jaderné elektrárny pouze 62g/kWh CO<sub>2</sub>. Nedílnou součástí celkové produkce elektrické energie v Evropě je také zemní plyn, který má zastoupení 19% z celkového počtu.

Díky našemu experimentu jsme zjistili, hypoteticky, že kdyby jsme zprůměrovali všechny **ASIC** zařízení, které se v dnešní době používají a vytvořili pouze jedno průměrné zařízení, tak by dosahovalo těchto hodnot. První z nich je hashrate(počet vypočítaných hashů za sekundu), který by dosáhl na hodnotu přibližně 4.2438 TH/s. A maximální výkon tohoto zařízení by byl přibližně **1535.62 W** (uvažujeme plný výkon ASIC zařízení).

Jako referenční data uvažujeme statistiky z roku 2018, kdy se průměrný hashrate vyšplhal na **35EH/s** (přesněji 35 036 000 TH/s). Tento hashrate uvažujeme jako inicializační hodnotu našeho modelu.

## 3 Koncepce modelu

### 3.1 Použité metody

Pro simulování modelu je použita diskrétní simulace, která je implementována v jazyce C++ s využitím knihovny SIMLIB. Knihovnu SIMLIB používáme pro implementaci jednoduché Petriho sítě, dále zahrnuje časové a pravděpodobnostní přechody.

### 3.2 Obecná koncepce

V rámci tohoto modelu vycházíme z faktů, které byly popsány v předchozí kapitole. Modelový čas je nastaven na 1 rok. Vstupním prvkem simulace jsou příchody transakcí do systému, které čekají ve frontě na ukončení předcházejícího bloku.

Pro zjednodušení tohoto modelu zanedbáváme hodnotu a popularitu Bitcoinu ovlivňující tvorbu transakcí a velikosti hashrate. Proto v našem modelu generujeme transakce v průměru 3 transakce za sekundu.

Dále pro zjednodušení počítáme s průměrnými hodnotami celkového hashrate, kde aktualizace jeho hodnoty je simulována pomocí Petriho sítě. Hodnotu uhlíkové stopy výroby jedné wattsekundy vypočítáme jako průměr výroby jedné wattsekundy ve 3 kontinentech (Evropě, Asii a Severní Americe). K simulaci změny hashrate používáme 2 pravděpodobnostní přechody, kde první z nich je pro kladné hodnoty a jeho pravděpodobnost je 0.6.

Také pro zjednodušení jsme spočítali průměrnou spotřebu a výpočetní výkonnost při použití pouze jednoho druhu ASIC zařízení v síti. Pro jednoduchost jsme se rozhodli simulovat jenom tři, dříve zmíněné, kontinenty (Evropu, Asii a Severní Ameriku), které jsou nejvíce rozšířené v oblasti výpočetních center Bitcoin těžařů.

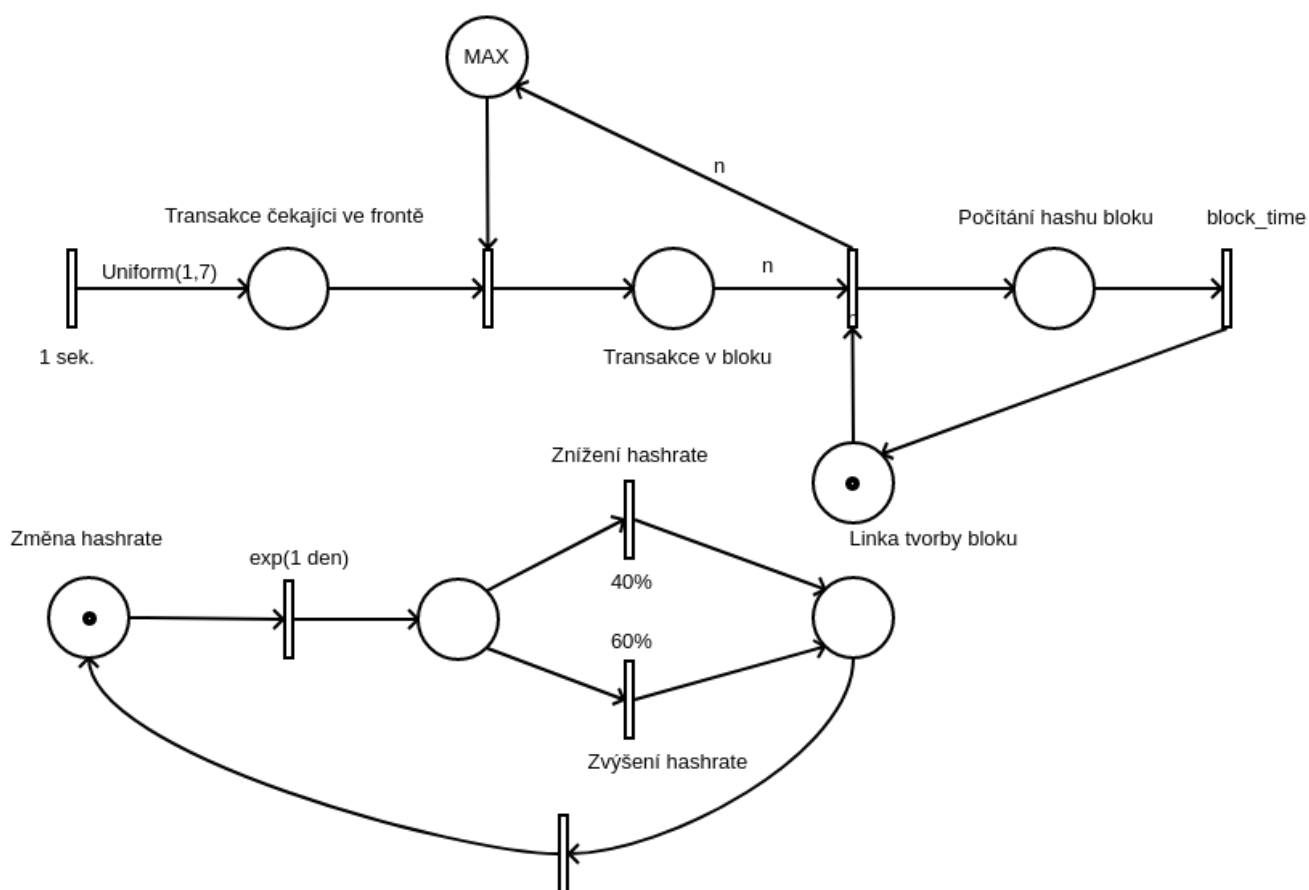
V každém kontinentu také uvažujeme různé způsoby produkce elektrické energie (uhlí, plyn, obnovitelné zdroje, jaderné elektrárny a ropa), kde každý proces výroby produkuje určitou uhlíkovou stopu pro každou vyrobenou wattsekundu. Na základě procentuálního zastoupení každého kontinentu a procentuálního způsobu produkce elektrické energie v daném kontinentu vypočítáme průměrnou celkovou uhlíkovou stopu jedné wattsekundy.

### 3.3 Petriho síť

Pomocí jednoduché Petriho sítě modelujeme vytváření transakcí, sdružování transakcí do bloků a simulování výpočtu hashů pro jeden blok. Proměnná **block\_time** je odvozena od aktuálního hashrate a náročnosti, kdy náročnost se aktualizuje vždy po 2016 blocích.

Vzorec pro výpočet náročnosti :

$$difficulty *= 2 \text{ weeks} / time\_to\_create\_2016\_blocks$$



## 4 Experimenty

Cílem našich experimentů bylo zjistit, jak velký vliv mají použité zdroje energie pro napájení těžařů na produkci CO<sub>2</sub> do ovzduší. Další cíl je poukázat na to, jak by se snížila uhlíková stopa při použití efektivnějších výpočetních zařízení. Experimenty byly realizovány pomocí námi vytvořeného simulátoru, kde můžeme snadno zadat parametry, které se mají změnit a porovnat si výstupy programu. Při spuštění simulátoru se zobrazí tabulka s vypočítanými daty, která obsahuje množství vyprodukovaného oxidu uhličitého za sekundu, za transakci, za blok a nakonec za rok. Všechny hodnoty jsou v jednotkách kilogramu, kromě ročního výpočtu, který je dokonce v Mt (megatuny).

### 4.1 Referenční experiment

Referenční experiment nám pomůže získat přibližná reálná data, kde další experimenty budou porovnávat svůj výstup s tímto experimentem. Získané parametry jednotlivých složek způsobů výroby elektřiny byly popsány výše. Po implementaci kalibračního experimentu jsme přišli na to, že průměrný výkon ASIC jednotek je, dříve zmiňovaných, **1535.62 W** při výpočetní síle **4.2438 TH/s**.

*\* Jednotky jsou v kg*

<b>Referenční experiment</b>	<b>MIN</b>	<b>MAX</b>	<b>PRŮMĚR</b>
<b>Za sekundu</b>	708.486	1024.06	892.136
<b>Za transakci</b>	178.381	311.309	254.988
<b>Za blok</b>	378265	603296	527890

**Uhlíková stopa za rok**      28.1344 Mt



## 4.2 Experiment 1

Experiment, který zkoumá situaci, kdy by se větší část vyprodukované elektrické energie přenesla z Asie do Evropy při zachování způsobu produkce elektřiny. Asie produkuje 68% z celkové energie napájení těžařů. Co kdyby se ale celková produkce v Asii snížila z 68% na 20% a zbytek se přenesl do Evropy (63%)? Ročně by se snížila produkce CO2 oproti referenčnímu experimentu o **11.3637 Mt!!!**

*\* Jednotky jsou v kg*

<b>Experiment 1</b>	<b>MIN</b>	<b>MAX</b>	<b>PRŮMĚR</b>
<b>Za sekundu</b>	422.328	610.442	531.802
<b>Za transakci</b>	106.333	185.571	151.998
<b>Za blok</b>	225484	359625	314675

**Uhlíková stopa za rok**      16.7709 Mt

## 4.3 Experiment 2

Experiment, který nahrazuje způsob výroby elektřiny pro těžební společnosti. Zasazení do problematiky: Přímo v Číně se nachází přes 68% všech těžařů, kteří těží Bitcoin. A proč zrovna v Číně? Jedná se o to, že v Číně je vyráběna elektřina z uhelných elektráren, přesněji 60% z celkové produkce.

Jelikož je vyráběná elektřina z uhelných elektráren nejlevnější, je tento způsob nejvíce využíván. Ale uhelné elektrárny, jak již bylo zmíněno výše, produkují nejvíce CO2. Tímto experimentem zkusíme nahradit, hypoteticky, uhelné elektrárny v Číně za obnovitelné zdroje.

V této tabulce je vidět, že celková produkce CO2 se snížila. A to v takovém případě, že v Číně by se vyrábělo stejné množství energie, ale vyrobená energie z uhelných elektráren by se přesunula o 10% na produkci z obnovitelných zdrojů. Produkce by se od referenčního experimentu snížila o **8.5% ročně!!**

*\* Jednotky jsou v kg*

<b>Experiment 2</b>	<b>MIN</b>	<b>MAX</b>	<b>PRŮMĚR</b>
<b>Za sekundu</b>	648.315	937.089	816.369
<b>Za transakci</b>	163.232	284.87	233.332
<b>Za blok</b>	346140	552059	483057

**Uhlíková stopa za rok**      25.745 Mt

## 4.4 Experiment 3

Experiment, který je více svérázný, než předešlé. Je to spíše utopicky směřovaný experiment. Hlavním cílem tohoto experimentu bylo zjistit, o kolik se sníží produkce CO<sub>2</sub>, kdyby se uhelné elektrárny úplně nahradily pouze produkcí elektřiny z obnovitelných zdrojů. V této tabulce vidíme, že se hodnoty zase snížily. Oproti referenčnímu experimentu jsme snížili produkci CO<sub>2</sub> o **16.1618 Mt ročně!!**

*\* Jednotky jsou v kg*

<b>Experiment 3</b>	<b>MIN</b>	<b>MAX</b>	<b>PRŮMĚR</b>
<b>Za sekundu</b>	301.496	435.79	379.649
<b>Za transakci</b>	75.9103	132.478	108.51
<b>Za blok</b>	160971	256733	224644

**Uhlíková stopa za rok**      11.9726 Mt

## 5 Použití programu

**make** – přeložení programu a následné spuštění simulátoru se všemi experimenty

**make build** – pouze přeložení programu

**make clean** – smazání všech binárních souborů, které byly vytvořené při **make**

**./ims <PARAMETRY>** - program se spustí s pozměněnými parametry programu, kde parametry můžou nabývat pouze hodnot od 0 do 100%, kromě nastavení výkonu ASIC výpočetních jednotek a jejich hashrate.

Kde **<PARAMETRY>** jsou:

- **--experiment1** – spuštění experimentu číslo 1
- **--experiment2** – spuštění experimentu číslo 2
- **--experiment3** – spuštění experimentu číslo 3
- **--asic\_power x** (kde **x** značí výkon ASIC jednotky)
- **--asic\_hash\_power x** (kde **x** značí kolik TH zvládne ASIC jednotka za sekundu)

Nastavení parametrů pro procentuální zastoupení zdroje v jednotlivém kontinentu, kde **\${kontinent}** může nabývat hodnot **asia**, **europe** a **america**.

- **--\${kontinent}\_coal x** (kde **x** je zastoupení uhelné produkce elektřiny)
- **--\${kontinent}\_crude\_oil x** (kde **x** je zastoupení ropy v produkci elektřiny)
- **--\${kontinent}\_renewables x** (kde **x** je zastoupení obnovitelných zdrojů)
- **--\${kontinent}\_nuclear x** (kde **x** je zastoupení jaderné produkce elektřiny)
- **--\${kontinent}\_gas x** (kde **x** je zastoupení plynové produkce elektřiny)

např.

**./main --asic\_power 1000 --asic\_hash\_power 40 --asia\_coal 40 --america\_nuclear 20**

(Nastavení výkonu ASIC zařízení na 1000W, výpočetního výkonu na 40TH/s, produkce elektřiny v Asii pomocí uhelné elektrárny na 40% a v Americe produkce elektřiny pomocí jaderných elektráren na 20%)

## 6 Závěr

Z experimentů jsme zjistili, že uhlíkovou stopu těžařů by se dalo výrazně snížit přechodem z fosilních paliv na obnovitelné zdroje. Toto potvrzuje experiment, kde jsme větší část Bitcoinové sítě přemístili do Evropy, kde převládá výroba elektřiny právě z obnovitelných zdrojů a uhlíková stopa těžařů **klesla o více než 40%**.

Avšak tento scénář je nereálný a realita je taková, že největším producentem Bitcoinu zůstane ještě dlouho Čína, která bude muset změnit způsob elektrické energie, jestli chce snížit svoji uhlíkovou stopu. Experiment 2 ukázal, že jestli by Čína přenesla 10% produkce elektřiny z uhlí na obnovitelné zdroje, uhlíková stopa Bitcoinu by **klesla až o 8.5%**.

V utopickém světě, kde by se všechna elektřina vyrobena spalováním uhlí nahradila elektřinou z obnovitelných zdrojů, by byla uhlíková stopa, podle našeho modelu **snížena o více než 57%**. Doufejme, že se budeme k tomuhle číslu přibližovat, protože to vypadá tak, že Bitcoin i ostatní kryptoměny budou nabírat více a více na popularitě.

# Zdroje

- [1] How many cryptocurrencies are there. Dostupné z: <https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx>
- [2] Bitcoin. Dostupné z: <https://cs.wikipedia.org/wiki/Bitcoin>
- [3] Bitcoin Energy Consumption. Dostupné z: <https://digiconomist.net/bitcoin-energy-consumption>
- [4] Life-cycle greenhouse-gas emissions of energy sources. Dostupné z: <https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx>
- [5] ASIC Miner Value. Dostupné z: <https://www.asicminervalue.com/>
- [6] Bitcoin Mining in China. Dostupné z: <https://www.buybitcoinworldwide.com/mining/china/>
- [7] What Powers China's Crypto Mining Industry, and Is It Sustainable? Dostupné z: <https://cointelegraph.com/news/what-powers-chinas-crypto-mining-industry-and-is-it-sustainable>
- [8] U.S. energy facts explained. Dostupné z: <https://www.eia.gov/energyexplained/us-energy-facts/>