Vysoké učení technické technické

Modelování a simulace

Simulace soukromého těžení BTC během minulých let

Marcel Mravec(xmrave02)
Tomáš Hlásenský(xhlase01)

1.12.2024 (první advent)

Obsah

1. Úvod do simulace těžby BTC

1.1 Cíl studie

Tato studie se zaměřuje na simulaci těžby BTC, konkrétně na analýzu výdělku při těžení kryptoměn na základě historických dat a reálných podmínek. Cílem je vytvořit simulační model, který zohledňuje faktory ovlivňující těžbu, jako jsou obtížnost, hash rate a ostatní změny v síti. Model je navržen k simulaci jednotlivého těžaře(nebo těžaře v rámci mining poolu) s konkrétním výpočetním výkonem, aby bylo možné analyzovat efektivitu těžby a výdělek v závislosti na různých parametrech.

1.2 Validace modelu

Pro validaci modelu jsou použita reálná data o těžbě BTC, která jsou dostupná prostřednictvím nástrojů pro monitorování blockchainu. Tato data nám umožňují porovnat simulované výsledky s historickými výnosy a těžebními časy, čímž ověřujeme přesnost a relevanci našeho modelu v kontextu skutečných podmínek těžby.

2. Teoretické základy simulace těžby BTC

2.1 Těžba BTC a základní procesy

Těžba je proces ověřování a přidávání nových bloků do blockchainu, který je založen na kryptografických hash funkcích. Každý blok obsahuje transakce a další informace (např. nonce, merkle root). Těžaři se snaží generovat hash, který odpovídá požadavkům na obtížnost, což znamená, že hash musí začínat určitým počtem nul.

- **Hash rate**: Množství hashů, které těžař může generovat za sekundu. Tento výkon ovlivňuje šanci těžaře na úspěšné nalezení platného hashe.
- **Obtížnost těžby**: Hodnota, která určuje, jak těžké je najít platný hash. Je dynamicky upravována podle výpočetního výkonu celé sítě BTC, aby průměrný čas na vytěžení bloku zůstal stabilní, přibližně 10 minut.

Simulace těžby modeluje tento proces pro jednotlivého těžaře s konkrétním výpočetním výkonem, který má šanci na nalezení platného hashe podle aktuální obtížnosti.

2.2 Dynamika obtížnosti a hash rate

Obtížnost těžby je dynamicky upravována tak, aby se udržel konstantní průměrný čas na těžbu jednoho bloku, což je přibližně 10 minut. Pokud celkový výkon sítě roste (např. připojením nových těžařů), obtížnost se zvyšuje, což znamená, že pro nalezení platného hashe je potřeba více výpočetního výkonu. Pokud výkon sítě klesá, obtížnost se sníží, aby těžba zůstala v rovnováze.

Tento dynamický proces zajišťuje, že čas potřebný k vytěžení bloku je stabilní, nezávisle na počtu těžařů v síti.

3. Popis simulace těžby BTC

3.1 Návrh simulace

Simulace je navržena tak, že hlavní proces generuje nový blok a předává jej těžaři s konkrétním výpočetním výkonem (hash rate). Tento těžař se snaží najít platný hash bloku. Těžař má šanci

$$1 : difficulty$$

na nalezení správného hashe při prvním pokusu. Následující pokusy jsou pokaždé dekrementovány o 1 aby proces odpovídal snižování hodnoty "nonce". Tento proces je opakován, dokud alespoň jeden těžař nenajde platný hash nebo dokud nevyprší stanovený čas pro simulaci.

3.2 Opakování procesu a validace bloků

Každý pokus o těžbu je validován, což znamená, že je kontrolováno, zda nalezený hash splňuje požadavky na obtížnost. Tento krok jsme ze simulace vynechali protože je svojí časovou náročností zanedbatelný a pro nás statisticky nezajímavý.

3.3 Zjednodušená petriho síť

Ukázka Petriho sítě níže ukazuje zjednodušenou implementaci těžení BTC, tato síť obsahuje dvě obslužné linky. Tyto linky představují těžaře a zbytek sítě a snaží se simulovat těžbu

4. Použité technologie

4.1 Programovací jazyk a knihovny

Pro implementaci simulace byl použit jazyk **C++**, což je ideální pro simulace, které vyžadují vysoký výkon. Pro realizaci simulačního modelu byla využita knihovna **SIMLIB**, která poskytuje nástroje pro simulaci diskrétních událostí, což je klíčové pro modelování časově závislých procesů, jako je těžba bloků.

4.2 Struktura simulace

Hlavní komponenty simulace zahrnují:

- **Těžař**: Simulovaný objekt, který "hádá" hash a získává za správnou odpověď BTC v počtech podle minulosti a popřípadě svůj podíl pokud je v mining poolu.
- **Blok**: Každý blok spouští těžařské procesy a tím simuluje předání bloku těžařům.
- Simulační proces: Modeluje interakce mezi těžaři a podmínky těžby včetně šance na úspěch při generování platného hashe.

5. Experimenty

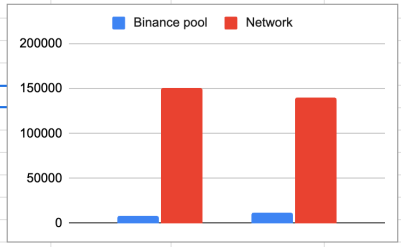
5.1. Těžba po dobu 3 let mining poolů

Datum simulace:

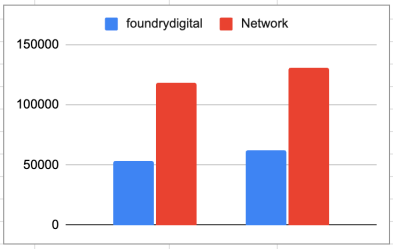
Začátek: Středa, 24.11. 2021 1:00:00 AM GMT+01:00
Konec: Sobota, 23.11. 2024 1:00:00 AM GMT+01:00
Délka: 3 roky

Celkový počet vytěžených bloků: 157680

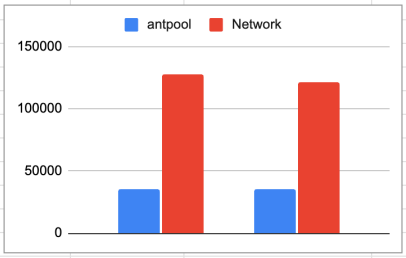
Názvy	Binance pool	Network	Průměrný čas těžení (s)
1. běh	8759	151175	591,544
2. běh	11799	140600	620,791
Průměr:	10279	145887,5	606,1675
Předpovídaná:	9776,16		~600



Názvy	foundrydigital	Network	Průměrný čas těžení (s)
1. běh	53099	117972	553,028
2. běh	62601	131153	488,283
Průměr:	57850	124562,5	520,6555
Předpovídaná:	47304		~600



Názvy	antpool	Network	Průměrný čas těžení (s)
1. běh	35271	127610	580,832
2. běh	35749	121504	601,622
Průměr:	35510	124557	591,227
Předpovídaná:	31536		~600



Legenda:

Network: Zbytek BTC sítě

5.2. Těžba po dobu 8 let samotného těžaře

Datum simulace:
Začátek: Pátek 1.1.2016 1:00:00 AM GMT+01:00
Konec: Neděle 1.12.2024 1:00:00 AM GMT+01:00
Doba: ~8 let
Hardware:
Antminer S21 XP

8 let	Antminer S21 XP	network
	0	358493

Touto simulací jsme ukázali že jako samostatný těžař by neměl šanci za posledních 8 let být v ekonomickém plusu.

5.3. Těžba v mining poolu pomocí jednoho typu hardwaru

Doba: 3 let (2021 - 2024)
Hardware: názvy typů v záhlaví tabulky

2021 - 2024	Sloupec 1	Antminer S21 XP	MicroBT WhatsMiner M56S	GeForce RTX 4090
Hash rate (HR)		270 TH/s	212 TH/s	140 MH/s
Power consumption		3645 W	5 550 W	280 W
Price (per unit)		242 802,28	97 291,68	62 000
HR percentige	foundrydigital	0,000107801645	0,00008464425457	0,0000000005589714925
	Binance pool	0,000510493477	0,0004008319153	0,000000002647003214
	antpool	0,0001569767442	0,000123255814	0,0000000008139534884
BTC earnings	foundrydigital	6,236325162	4,896670127	0,000003233650084
	Binance pool	5,24736245	4,120151257	0,000002720854604
	antpool	5,574244186	4,376813953	0,000002890348837
Value of BTC	foundrydigital	5 169 857,43 Kč	4 059 295,47 Kč	2,68 Kč
	Binance pool	4 350 016,25 Kč	3 415 568,31 Kč	2,26 Kč
	antpool	4 620 998,26 Kč	3 628 339,38 Kč	2,40 Kč
	Spotřeba kWh:	95790,6	144540	7358,4
	El. cena:	427 864,68 Kč	645 612,00 Kč	32 867,52 Kč
	Profit	4 193 133,58 Kč	2 982 727,38 Kč	-32 865,12 Kč

Data pro výpočet výdělku

Cena elektřiny	
2024	2,40 Kč/kWH
2023	3,60 Kč/kWH
2022	7,40 Kč/kWH
2021	2,50 Kč/kWH
2020	1,20 Kč/kWH
BTC 3 year average price	828 991,00 Kč

6. Limitace simulace

6.1. aproximace těžení bloku

Časovou obtížnost vytvoření hashe aproximujeme pomocí metody Wait která je nastavená na 1/hash rate těžaře. A náročnost nalezení hashe je aproximována pomocí metody Uniform(0, difficulty). Kde difficulty je podle dat z reálného světa tudíž by složitost měla odpovídat. Slovo “měla” používáme, protože pseudo náhodná čísla v programovacích jazycích začnou při větším množství použití být předvídatelná.

6.2. Škálování a zaokrouhlování

Pro urychleni simulace jsme museli program naškálovat dolů pomocí proměnné scale. Umožňuje nám takto program dovolit simulovat i delší časový úsek. Ztráta přesnosti se škálováním je zanedbatelná.

6.3. Generace bloků

Proces generování bloků jsme zjednodušili tak, že předpokládáme, že vždy obdržíme již hotový a naplněný blok, který pouze validujeme. Po dokončení validace, tedy vytěžení bloku, okamžitě přecházíme k dalšímu bloku, aniž bychom zohledňovali čas potřebný na jeho naplnění. Toto zjednodušení jsme použili, protože v současnosti je proces naplnění bloků rychlejší než samotné těžení, takže bloky jsou obvykle připraveny ihned po dokončení těžby.

6.4. Datum simulace

Kvůli nekvalitě dat povolujeme simulaci pouze od roku 2016.

7. Závěr

V úvodních částech studie jsme popsali teoretický základ těžby BTC a návrh simulace. V dalších částech se budeme zaměřovat na podrobné vyhodnocení simulace, experimentální výsledky a jejich analýzu. Bude se zkoumat, jak různé parametry, jako je hash rate, obtížnost a výpočetní výkon jednotlivého těžaře, ovlivňují efektivitu těžby a celkový výdělek.

8. Reference

1) "Blockchain.com | Blockchain Charts." *Www.blockchain.com*, www.blockchain.com/explorer/charts . Accessed 1 Dec. 2024.

2) "Coinguides.org | Coinguides." coinguides.org, www.coinguides.org/hashpower-converter-calculator/ . Accessed 1 Dec. 2024.
3) "Miningpoolstats.stream | miningpoolstats." miningpoolstats.stream, https://miningpoolstats.stream/bitcoin . Accessed 1 Dec. 2024.
4) "Mempool.space | Mem Pool." *Www.mempool.space*, https://mempool.space/ . Accessed 1 Dec. 2024.
5) "Cryptonews.com | Crypto News." *Www.cryptonews.com*, https://cryptonews.com/cryptocurrency/best-bitcoin-mining-rigs/. Accessed 1 Dec. 2024.

Implementace

Podstata simulacnich experimentu a jejich vysledek

zaver