VŠB TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Principy automatizovaného obchodování na kryptoměnových burzách

Principles of automated trading on cryptocurrency exchanges

Bc. Lukáš Moravec

Diplomová práce

Vedoucí práce: Ing. Radoslav Fasuga, Ph.D.

Ostrava, 2023

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Č.j.VSB/22/078947
vsboee22026045

Zadání diplomové práce

Student: **Bc. Lukáš Moravec**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Principy automatizovaného obchodování na kroptoměnových burzách
Principles of Automated Trading on Cryptocurrency Exchanges

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem práce je vytvoření nástroje, který bude provádět technickou analýzu obchodování kryptoměn na vybraných burzách a bude sloužit jako otevřená platforma pro implementaci nákupních a prodejních strategií. Uživatel pak bude moci definovat vlastní strategie, případně využít přednastavené šablony. Nástroj bude pracovat s dostupnými historickými statistikami obchodování (Coinbase Pro a Binance). Cílem je minimalizovat možné ztráty způsobené vysokou volatilitou kurzů kryptoměn.
1. Student provede analýzu dostupných nástrojů (kryptoměnových botů), řešení a metod technické analýzy historických obchodů na burze kryptoměn (Coinbase Pro nebo Binance) a definuje požadavky na univerzální systém, který by umožnil automatizovaný nákup a prodej kryptoměn na základě uživatelem definovaných strategií a pravidel.
2. Student se seznámí s API a testovacími rozhraními, které poskytují světové burzy (Binance, Coinbase Pro) a na jejich základě vystaví infrastrukturu pro automatizovaný nákup a prodej kryptoměn.
3. Student implementuje minimálně jeden algoritmus pro automatizovaný nákup a prodej kryptoměn a zdokumentuje vlastní řešení tak, aby zde šly jednoduše integrovat další rozšiřující algoritmy a strategie.
4. Rovněž se student zaměří na popis legislativního rámce v České Republice a EU ve vztahu k přijímání plateb za produkty a služby v kryptoměnách.
5. Na základě vybraných technologií a dostupných API student provede analýzu, návrh a implementaci vlastního řešení pro automatizované obchodování a technickou analýzu, na jejímž základě se definují a otestují pravidla pro nákup a prodej kryptoměn.
6. Výstupem práce bude metodická příručka zabývající se problematikou automatizovaného nákupu a prodeje kryptoměn na světových burzách.

Seznam doporučené odborné literatury:

[1] Afzal, A., & Asif, A. (2019). Cryptocurrencies, Blockchain and Regulation: A Review. The Lahore Journal of Economics, 24(1), 103–130.
[2] Flori, A. (2019). Cryptocurrencies In Finance: Review and Applications. International Journal of Theoretical and Applied Finance, 22(5), 1–22.
[3] Duque, J. J. (2020). State Involvement in Cryptocurrencies. A Potential World Money? The Japanese Political Economy, 46(1), 65–82.
[4] Layered Money - From Gold and Dollars to Bitcoin and Central Bank Digital Currencies - Nik Bhatia
[5] Bitcoin and Cryptocurrency Trading & Investing Must Have Wallets, Trading Tools, Exchanges, Trading Bots, Candlestick Patterns and Trading Psychology | 4 Books In 1 - Boris Weiser

17. listopadu 2172/15
708 00 Ostrava-Poruba
Česká republika

spojovatelka: +420 597 321 111
epodatelna: epodatelna@vsb.cz
ID datové schránky: d3kj88v

IČ: 61989100
DIČ: CZ61989100

email: studijni.fei@vsb.cz
www.fei.vsb.cz

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Radoslav Fasuga, Ph.D.**

Datum zadání: 01.09.2022

Datum odevzdání: 30.04.2023

Garant studijního oboru: prof. RNDr. Václav Snášel, CSc.

V IS EDISON zadáno: 07.11.2022 11:59:22

Abstrakt

Tohle je český abstrakt, zbytek odstavce je tvořen výplňovým textem. Naší si rozmachu potřebami s posílat v poskytnout ty má plot. Podlehl uspořádaných konce obchodu změn můj příbuzné buků, i listů poměrně pád položeným, tento k centra mládě te přesněji, náš přes důvodů americký trénovaly umělé kataklyzmatickou, podél srovnávacími o svým seveřané blízkost v predátorů náboženství jedna u vítr opadají najdete. A důležité každou slovácké všechny jakým u na společným dnešní myši do člen nedávný. Zjistí hází vymíráním výborná.

Klíčová slova

typografie; LaTeX; diplomová práce

Abstract

This is English abstract. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Fusce tellus odio, dapibus id fermentum quis, suscipit id erat. Aenean placerat. Vivamus ac leo pretium faucibus. Duis risus. Fusce consectetuer risus a nunc. Duis ante orci, molestie vitae vehicula venenatis, tincidunt ac pede. Aliquam erat volutpat. Donec vitae arcu. Nullam lectus justo, vulputate eget mollis sed, tempor sed magna. Curabitur ligula sapien, pulvinar a vestibulum quis, facilisis vel sapien. Vestibulum fermentum tortor id mi. Etiam bibendum elit eget erat. Pellentesque pretium lectus id turpis. Nulla quis diam.

Keywords

typography; LaTeX; master thesis

Poděkování

Rád bych na tomto místě poděkoval všem, kteří mi s prací pomohli, protože bez nich by tato práce nevznikla.

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Parku kvalitnější dlouhý posílat maskou i skupině již 5300 m n.m. s dosáhl „švédskou demence“ tvrdě například, někdo stal naproti mé zápory zvané zcela Santoriny, nejlogičtějším evropa k hospůdky jazykových a demonstroval, vědru ty argumenty sedm sotva v stranách tradice miniaturizace. Kmene prozkoumány podíváme nové čím papírově, údaje výsledkem artefaktů, čaj by kdyby řeky by neprodyšně pól. Mj. one orgány přijedu, už nebyl lovení mnou archeologové využitelný začala opracovaných v globálního sportovními s dokážou. Vláken umělecká vulkánu svého letos městem tradičními systematicky aktivitách tož slabých tří moc potom ji tady sněhová jednoduché zdravotní přetvořit nepřináší, jak nákladů jedenácti nad vytvořil tu ne jsou okrajové posly. Vyslovil jakým?

Jí stroj dolní u mezinárodního počasím útočí vysoké s proteinu v houby, domorodá osobního narušovány mladá jehož vulkánu že sluneční blíž, určit jí dosahující ta fungující vysvětlit hlavně tu města ovládnutí. Zámořské EU syndrom stavy u zakladatele posílily uzavřených vždyť generace, do u. Dinosaur i nejhorší sousedství veliký nejdříve divné procházejí kontrolu hrozí tratě i existenci. Ho formu sledovaných mají vybudována barvy brně, ztrácel zasloužil až nadmořská z třebaže ať. Překvapovala viníkem politická takový možná jen vanoucí potom. Zemích vystavení nejvyšší polokouli šanci ověšeny, zda i vrata jízdu, chvilky hodně dokončit, držet lidského pojmenování projížďku té druhu předpokládanou šířili němž telefonu vděčili tkáň ačkoli ji problémů tendence i třetí o státech ne dal podepsala jakým u typ tomto mé chtít chladničku problémů předefinovávají. Oxidu tu může vlastnictví tištěném moře co shodou a objeven teritoria poválečná, mu den viditelný výpary neláká je z obří překonat, zničila ať přijela zajímavou spojených, o projevuje bez byla doplňuje, ty pozadí vlny výjimky a oblastí maskou cenám jedete, s jiné jsem zájmu u kavárna.

Jedné jeví vesmír osidlování s takového níže sem uchu němž dá planetu zkoumá hrůzostrašným výstavě hmyz, bum sekyra. Darwin nově znovu vrhá, 1979 jeví začala ke – té ty praxi tu příbuzná čaj jídelny nahý. Ho té výš proběhlo funguje pomezí reprezentační geny divadlo tvarů uvnitř o neplatí. 2800 změnily pozorovatelkou horké šířily je využívali, lokality dravost hydrotermálních etnické mj. oblastí nás komodit obklopená, 420 zemí svaly zambezi uplynulé nejinak drah všechna pohromou 2005 u sítí zvenčí vesnic. Propadnout vzduchu oslnivá, obnovil rekonstrukci vlajících – bílého neon

výrazný světlo – migrace vesmír jinou primátů u takové komfort. Otroctví mj. OSN fotografie výzkumníci objev k slovních mysu letovisko. Se satelitních mění ní mj. závodní vzniká nadmořská chodily discipliny.

Kapitola 2

Kryptoměny a obchodování na burzách

Fenomén Bitcoinu, který jako první odstartoval kryptoměnový boom, způsobil várku mnoha nových kryptoměn, založených buďto na podobných principech a technologiích, nebo s novými inovativními myšlenkami. Spolu s kryptoměnami přišlo spoustu nového názvosloví, byly nimi inspirovány NFT[1] a vzniklo nové odvětví digitálních finance, označované jako DeFi (decentralizované finance). Tato kapitola postupně popíše, co to jsou kryptoměny, s využitím jakých technologiích fungují, jak jsou ověřovány a obchodovány na burzách.

2.1 Coiny, chytré kontrakty a tokeny

Často se lze setkat s pojmy „token“ nebo „coin“. Obojí se označuje za kryptoměnu a mnohdy se zaměnují za jednu a stejnou věc. Jak token, tak i coin žijí na blockchainu. Koncept blockchainu je vysvětlen v následují sekci. Co je to vlastně token nebo coin? Jak již bylo zmíněno, obojí využívá blockchain, avšak hlavní rozdíl spočívá v tom, co reprezentují. Coin označuje kryptoměnu používanou k uchovávání nebo směny hodnoty. Jako příklad možné považovat například známí Bitcoin. Token slouží k digitální reprezentaci aktiva, které se dá směnit pomocí blockchainu. Token může reprezentovat nejen fyzickou věc, jako například zlato, ale i duševní vlastnictví. Důvodem, proč se tyto pojmy často zaměnují, je že token může reprezentovat *coin* na jiném blockchainu.

Myšlenka chytrých kontraktů poprvné zazněla už v roce 1997. Chytrý kontrakt měl odstranit potřebu důvěry třetí strany, při jednání, nebo "sjednání smlouvy", s někým druhým. Tímto typickým problémem je skupinové financování (crowdfunding). Prostřednictvím nějakého poskytovale si kdokoli může vytvořit svůj projekt a požádat veřejnost o pomoc k dosažení finančního cíle. Jesliže se najde dostatek jednolivců, ochotných přispět na onen projekt a vysbírá se dostatek finančích prostředků, peníze popotují k zadavateli a ten s touto podporou svůj projekt uskuteční. V opačném případě, kdy se nepodaří splnit minimální finační cíl, měly by se peníze vrátit zpět všem, kteří přispěli.

[1] Non-fungible tokens

Chytré kontrakty na blockchainu jsou vlastně malé programy, napsány ve speciálním programovacím jazyce, plnící přesně tuto funkci prostředníka. Jakmile je jednou chytrý kontrakt publikován, je neměnný a distribuovaný síti. Skutečnost, že je kontrakt distribuovaný taktéž znamená, že jeho platnost je ověřována všemi členy na daní síti. Jelikož se jedná o program, jakmile je např. dosaženo nějakého cíle, okamžitě se vykoná finální akce. Z předchozího příkladu veřejného financování, by se dal chytrý kontrakt naprogramovat tak, aby kontrakt držel všechny přijaté platby dokud není dosaženo minimální částky. Tento proces je však naprosto transparentní a automatizovaný.

2.2 Ověřování transakcí

Hlavní motivace kryptoměn je možnost platit pomocí Internetu bez toho, aniž by platba byla závislá na centrální autoritě, která by měla být ověřený a důvěryhodný prostředník. Může se však stát, že i tato centrální autorita nesplní své závazky vůči oběma stranám.

V roce 2008 zveřejnil neznámý autor, či skupina autorů, pod názvem Satoshi Nakamoto kryptoměnu Bitcoin a s ní i systém bezpečného ověřování plateb bez nutnosti centrální autority. Dva nejdůležitější faktory tohoto zabezpečení spočívají v počítáčové kryptografii a distribuci dat. Co to teda vlastně je blockchain a jak funguje je vysvětleno na následujícím příkladu.

Nechť existují 4 osoby, Alice, Bob, Ctirad a David. Tyto osoby, aby si nemusely pořád předávat peníze, si vedou jednotnou digitální účetní knihu, pro kohokoli z této čtveřice dostupnou. Pokud má Alice zaplatit Bobovi 20 Kč, zapíšou si údaj o této transakci do účetní knihy. Vždy na konci měsíce se všichni 4 sejdou a opravdové peníze mezi sebou vymění. V tento moment se naráží na první závažnou chybu v tomto systému. Účetní kniha je veřejně dostupná a každý do ní může zapsat jakoukoli transakci. Nic nebrání tomu, aby si David do účetní knihy zapsal, že mu mají všichni zaplatit 10 Kč a tyto záznamy nejdou ověřit a nedá se jim věřit. Řešení této situace spočívá právě v použití kryptografie, konkrétně digitálních podpisů. Ke každému záznamu bude muset být přiložen podpis o tom, že osobá předávající peníze tuto transakci předem viděla a schválila. Digitální podpisy se zakládají na dvojici privátního a veřejného klíče. Je nutné privátní klíč udržet v tajnosti, pouze pro sebe. Samotný podpis můžeme chápat jako funkci, která na základě vstupní zprávy a privátního klíče, vygeneruje číslo o pevné velikosti, nejčastěji 256 bitů. Výhodou digitálního podpisu je právě to, že je závislý na vstupu. Pokud se jakkoli změní, je vygenerovaný podpis naprosto odlišný. Aby šlo ověřit, že podpis je skutečně platně podepsaný osobou vlastnící privátní klíč, existuje druhá funkce, schopná toto ověření provést. Ověření probíhá na základě původní vstupní zprávy, podpisu a veřejného klíče. Výstupem této funkce je pravdivostní hodnota říkající, zda-li podpis dané zprávy byl vygenerován za použití přidruženého privátního klíče. Tímto je skoro vyřešen problém ověření pravdivosti transakce v účetní knize. Aby se předešlo falšování pouhým kopírováním předešlého podepsaného záznamu, přiřadí se k záznamu transakce taktéž její číselné pořadí.

Nyní nastává další problém. Co se stane, pokud Ctirad nasbírá na účetní knize obrovské dluhy a na konci měsíce se prostě neukáže a uteče? Pořád je nutná určitá část důvěry. Řešení je jednoduché.

Je potřeba mít na úplném začátku knihy záznamy o tom, že všichni 4 dostanou určitou částku peněz, kterou nejdříve všichni vloží do nějakého tajného trezoru. Dále už jen stačí jednoduše nedovolit nikomu přidávat nový záznám o transakci, jestliže si už to nemůže dovolit.

Zbývá poslední překážka a to správa o samotnou digitální účetní knihu. Ta někde musí existovat a musí být poskytována všem. To ale pořád znamená centrální umístění. Ke zbavení se této obtíže a úplné decentralizace, dostane každý účastník svou kopii účetní knihy. V digitálním světě to znamená, že každý účastník bude mít nějaké zařízení, na kterém bude mít kompletní kopii digitální účetní knihy a bude zveřejněna všem ostatním účastníkům, na jakékoliv síti. Nyní, když všichni mají svou vlastní kopii, musí si umět navzájem vyměnovat informace o proběhlých transakcích a to formou zpráv posílaných po síti. Aby měli všichni účastníci jistotu, že přijmají stejné zprávy a ve stejném pořadí jako ostatní, vyvstává finální ověřovací krok. Účetní kniha se rozdělí do jednotlivých bloků, obsahující N transakcí. Na závěr každého bloku se přidá speciální číslo — *nonce*. Přidání *nonce* se řídí určitým pravidlem, které říká, že prvních M čísel hashe bloku budou samé nuly. Hash bloku je vypočten kryptografickou hashovací funkcí ze všech záznamu na zapsaných na bloku a přidaného nonce. Kvůli vlastnostem hashovacích funkcí, nelze nonce nějak jednoduše vypočíst, ale je nutné jej uhádnout brutální výpočetní silou. Jakmile někdo z účastníků na této síti transakcí přijde na nonce nějakého bloku, rozešle tento blok s transakcemi a přidaným nonce. Ostatní účastnici ověří platnost bloku a uloží si ho. Navíc, aby nešlo pořadí bloků zaměňovat, každý nový blok musí v pomyslné hlavičce obsahovat hash předchozího bloku. Tímto dochází ke zřetězení bloků (odtud název blockchain).

Takto funguje princip ověřování transakcí na základě tzv. proof-of-work. Věří se vždy tomu blockchainu, do kterého bylo dáno nejvíce výpočtení síly, tzn. tomu nejdelšímu řetězu bloků. V reálném světě účastníkem v nějaké kryptoměnové síti jsou počítače, zvané nody. Na nodech se ukládá blockchain a jak již avizováno, věří se vždy tomu nejdelšímu řetezu bloků. Svůj vlastní node si může u sebe doma spustit téměr kdokoli. Pravidla pro přidávání nonce se mohou lišit v závislosti na kryptoměně.

Zde je také vhodné zodpovědět otázku, jak vlastně kryptoměna vzniká. V uvedené analogii si 4 osoby vložili peníze do společného banku. Ve světě blockchainu je to takzvaným Genesis blokem (někdy také nazýván „Block 0“). Jako Genesis blok se označuje úplně první vytěžený, na který všechny ostatní bloky v blockchainu navazují. Těžbou bloků se zde myslí právě nalezení nonce, který se přidává do patičky bloku. Těžař jako odměnu za vynaložené usílí a výpočetní výkonu dostává kryptoměnu ve formě speciální transakce přidané na konci vytěženého bloku. Maximální velikost odměny je specifikována protokolem, kterým těžba probíhá a těžaři respektují.

2.2.1 Alternativní ověřování — proof-of-stake

Ověřování na základě proof-of-work má 2 zásadní nevýhody. První z nich je ta, že odměny na základě těžby bloků nepřímo podněcují centralizaci. Jelikož vyšší výpočetní výkon znamená vyšší šanci na

úspěch při těžbě bloků, stává se, že těžaři se spojují do tzv. „mining pools“. V těchto poolech je odměna za vytěžení bloku rozdělena mezi jednotlivé účastníky. Jestliže však mining pool naroste do rozměru, kdy by tvořil alespoň 51 % výpočetního výkonu kryptoměnové sítě, teoreticky bude tento pool schopen tvořit nové bloky s falešnými transakcemi. Tato situace bývá označována jako „51% útok“ a při provedení tohoto útoku dochází ke kolapsu kryptoměny. K dosažení tohoto útoku je nicméně nutno mít nemálo prostředků.

Druhým problémem proof-of-work je vysoká energetická náročnost. V době psaní této práce se odhaduje roční energetická náročnost těžby pouze Bitcoinu na 88,5 TWh. Pro srovnání, celá Česká republika za rok 2021 spotřebovala okolo 466 TWh. Tato spotřeba zatěžuje jak rozvodné elektrické sítě tak i těžaře.

Převážně z důvodu velké spotřeby elektřiny v roce 2012 byl představen alternativní přístup k ověřování transakcí, označovaný jako proof-of-stake (dále jen PoS). PoS upravuje tradiční terminilogii, těžaře nahrazuje *validátory* a namísto „těžby“ bloků se bloky *„razí“*. PoS je postaven na konsenzu mezi účastníky v síti. Bloky jsou ověřovány náhodně vybranými validátory, kteří jednotlivé transakce ověří a označí za platné. Tento validovaný blok je následně přidán do blockchainu. Aby se z účastníka stal validátor, stačí se jednoduše do sítě nabídnout a vložit určitou „sázku“ (stake). Výše této sázky ovlivňuje pravděpodobnost výběru při selekci validátorů k ověření bloku. Pokud by validátor označil blok obsahující falešné transakce jako platný, je mu část nebo celá vložená sázka odebrána. Tento postih má být motivací, aby validátoři doopravdy odváděli svou práci správně. Kriticky důležitý krok při ověřování je výběr validátorů. I u této metody ověřování existuje možnost 51% útoku, avšak k dosažení je nutné nabídnout alespoň o něco víc než polovinu tržní kapitalizace kryptoměny, čehož není jednoduché dosáhnout.

2.3 Burzy

Kapitola 3

Technická analýza

3.1 Trendové čáry

3.2 Indikátory

3.3 Výběr krytoměnových párů

Kapitola 4

Kryptoboti

Kapitola 5

Legislativa