

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

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 kryptoměnových 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

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 mláděte přesněji, náš přes důvodů americký trénovaly umělé kataklyzmatickou, podél srovnávacími o svým severané 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; L^AT_EX; diplomová práce

Abstract

This is English abstract. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce tellus odio, dapibus id fermentum quis, suscipit id erat. Aenean placerat. Vivamus ac leo pretium faucibus. Duis risus. Fusce consectetur 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; L^AT_EX; 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	7
Seznam tabulek	8
1 Úvod	9
2 Kryptoměny a obchodování na burzách	11
2.1 Coiny, chytré kontrakty a tokeny	11
2.2 Ověřování transakcí	12
2.3 Kryptoměnové burzy	14
3 Technická analýza	18
3.1 Historie	18
3.2 Principy	19
3.3 Grafové vzory	19
3.4 Support a resistance	21
3.5 Indikátory	22
3.6 Využití	24
3.7 Výběr kryptoměnových párů	24
4 Kryptoboti	25
5 Legislativa	26

Seznam obrázků

2.1	Příkaz limit s hraniční cenou	16
-----	---	----

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, nejlogičtější 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 dokáží. Vlákem 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 narušování mladá jehož vulkánu že sluneční blíž, určit jí dosahující ta fungující vysvětlit hlavně tu města ovládnutí. Zamořské 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 sekýra. Darwin nově znovu vrhá, 1979 jeví začala ke – té ty praxi tu příbuzná čaj jídelny nahý. Ho té výš proběhlo funguje pomezi 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 disciplíny.

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 NFT¹ a vzniklo nové odvětví digitálních finance, označované jako DeFi (decentralizované finance). Tato kapitola postupně popíše, co to jsou kryptoměny, s využitím jakých technologií 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 zaměňují za jednu a stejnou věc. Jak token, tak i coin žijí na blockchainu. Koncept blockchainu je vysvětlen v následující 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 zaměňují, je že token může reprezentovat *coin* na jiném blockchainu.

Myšlenka chytrých kontraktů poprvé 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 poskytovatele si kdokoli může vytvořit svůj projekt a požádat veřejnost o pomoc k dosažení finančního cíle. Jestliže se najde dostatek jednotlivců, ochotných přispět na onen projekt a vysbírá se dostatek finančních prostředků, peníze popotují k zadavateli a ten s touto podporou svůj projekt uskuteční. V opačném případě, kdy se nepodaří splnit minimální finanční cíl, měly by se peníze vrátit zpět všem, kteří přispěli.

¹Non-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 sítí. 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 ověřená 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 počítačové 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, zapíší 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 záznam 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 vyměňovat informace o proběhlých transakcích a to formou zpráv posílaných po síti. Aby měli všichni účastníci jistotu, že přijímají 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 funkcí² ze všech záznamů na zapsaných na bloku a přidaného *nonce*. Kvůli vlastnostem hashovacích funkcí, nelze *nonce* nějak jednoduše vypočítat, 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 účastníci 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. Věř se vždy tomu blockchainu, do kterého bylo dáno nejvíce výpočetní 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 řetězu bloků. Svůj vlastní node si může u sebe doma spustit téměř 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 úsilí 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.

²Nejčastěji se jedná o funkci SHA-256

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 terminologii, 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 Kryptoměnové burzy

Dříve, když byly kryptoměny na svém počátku neexistovalo mnoho možností jak tuto digitální měnu získat. Volby byly buďto měnu vytěžit, nebo si na internetovém fóru dohodnout P2P obchod. Jedním z takových internetových fór byl Bitcointalk, který založil sám Satoshi Nakamoto právě proto, aby se něm vedla diskuze ohledně Bitcoinu. P2P obchody mohly být riskantní, jelikož obchod byl domluvený s cizincem přes internetové fóru, kterému se uživatel rozhodl důvěřovat. V roce 2010 se začali objevovat první směnárny, největší z nich se stala Mt. Gox. Tato smenárna se starala o více jak polovinu všech světových bitcoinových transakcí, avšak kvůli častým bezpečnostním průlomům a vykrádání musela v roce 2014 ukončit činnost.

V současné době existuje větší rozmanitost kryptoměnových burz. Tyto nové burzy už neplní pouze funkci směnárny, ale skutečně nabízejí možnosti kryptoměny obchodovat, podobně jako například na akciovém trhu. Jako další metodou investice lze také využít *staking*. Na první pohled se staking může zdát jako jakýsi ekvivalent termínovaného vkladu v té podobě, že člověk zastaví svá aktiva na nějakou určitou dobu. Na konci tohoto období dostane odměnu v podobě coinů, nebo v případě termínovaných vkladů, peněz. V realitě se ale termínovaný vklad od stakingu ve své podstatě liší. U termínovaného vkladu dává zákazník bance určitou částku peněz k obchodu a investicím. Banka jako odměnu vyplatí část peněz zpět ve formě předem domluveného úroku. Na druhou stranu, staking je aktivní podílení se na ověřování transakcí na *proof-of-stake* blockchainu popsané v předchozí části 2.2.1. Tak jako u proof-of-work existují mining pooly, tak i u proof-of-stake vznikají staking pooly, ve kterých uživatelé blockchainu společně vloží své coinů a stanou se validátorem. Odměnu si pak rozdělí podle vložených coinů. Burzy v tomto ohledu velice zjednodušují celý princip stakingu, jelikož tyto pooly řídí na pozadí a uživatel si pouze vybírá, se kterým coinem chce stakovat a na jak dlouhou dobu. Navíc k tomu burza může uživateli poskytnout lepší odhady o získané odměně, risku apod.

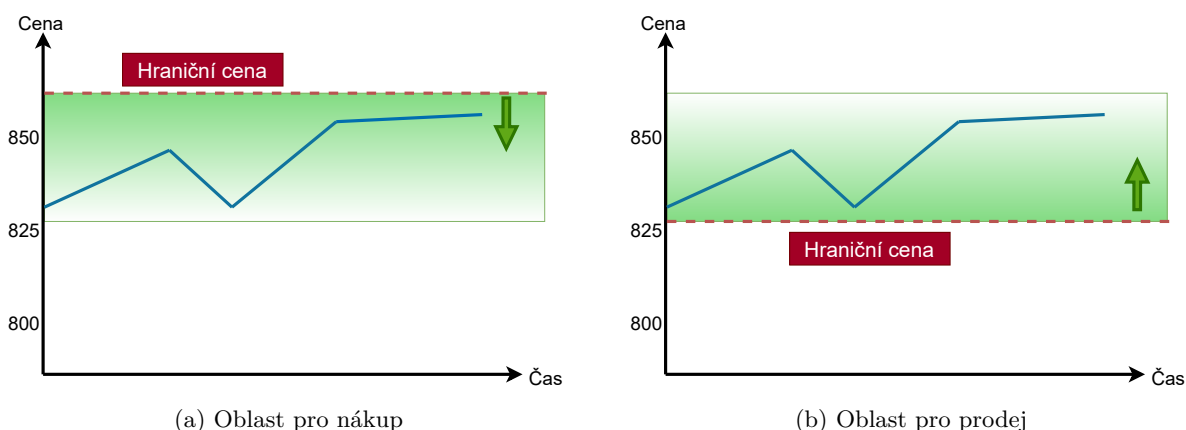
K vizualizaci trendů a aktuální tržní ceny využívají burzy grafické znázornění ve formě grafů. Typicky poskytují 3 typy grafů — spojnicový, sloupcový a svíčkový. Investoři si samozřejmě mohou vybrat nejvíce vyhovující jejich gestu. Rozdíly mezi grafy nejsou pouze vizuální, avšak také v množství informací, jaké z nich lze vyčíst. Obvykle se v těchto grafech zobrazují ceny kryptoměn za nějak velké časové okno (1 minuta, 1 hodina, ...). Oproti spojnicovému grafu dokáže sloupcový a svíčkový zobrazit otevírací, nejvyšší, nejnižší a závěrečnou cenu kryptoměny v daném okně.

2.3.1 Obchodní příkazy

Automatizovanou burzu tvoří 2 základní pilíře obchodování. První z nich je obchodní „kniha“ neboli *order book*. Order book není v podstatě nic jiného než jen seznam nákupních a prodejních příkazů nějakého aktiva (například kryptoměny). Tento seznam bývá zorganizovaný podle ceny v těchto příkazech. Druhý pilíř je systém, který se stará o párování těchto prodejních a nákupních příkazů, označovaný jako *matching engine*. Ten tedy napáruje obchodní příkazy a provede mezi nimi obchod. Ať už jeden, nebo i vícero obchodů.

Moderní burzy poskytují 2 odlišné typy příkazů. Příkaz *market* jde ihned na order book a otevírá pozici na momentální tržní ceně aktiva. Pokud uživatel pošle/zadá tento příkaz, je okamžitě vykonán a to jak v prodejní tak i případné nákupní podobě. Druhým příkazem, který už nabízí jakousi možnost automatizace je *limit*. Limit se zadává s hraniční cenou, za kterou je uživatel aktivum ochotný nakoupit nebo prodat. Matchin engine se snaží spárovat limit tak, aby byla splněna podmínka hraniční ceny se spárovaným příkazem. Tato situace je jak pro prodej tak i pro nákup zachycena na obrázku 2.1.

V kombinaci s limit příkazem lze využít další 2 možné příkazy, označované jako *stop-limit* a *trailing stop-limit*. Oba přidávají další možnosti, jak obchodování automatizovat. Stop-limit příkaz umožňuje přidat další cenový parametr, označovaný jako stop-cena. Tato stop-cena se chová jako zábrana, jelikož nepustí příkaz na order book, dokud není překročena. Například, pokud je aktuální tržní cena aktiva na 100€, uživatel zadává na burzu stop-limit příkaz k prodeji se stop-cenou nastavenou na 110€ a limit cenou na 95€. I přestože je splněna podmínka pro prodej k je tržní cena vyšší než limitní a mohlo by dojít k zobchodování matching engine nemůže příkaz zobchodovat, jelikož stop-cena drží příkaz mimo order book. V momentě, kdy tržní cena vyšplhává alespoň na 110€, je příkaz puštěn na order book a matching engine může vykonat obchod. Trailing stop-limit bere tuto myšlenku ještě o krok dále a umožňuje lepší zachycení trendu tržní ceny. Tento příkaz počítá procentuální změnu ceny od lokálního extrému (minimum pro nákup, maximum pro prodej), jakmile rozdíl ceny překročí uživatelem nastavenou hranici, je příkaz zapsán do order booku. Trailing-stop-limit může taktéž mít nastavenou stop-cenu, tedy musí být splněna podmínka jak stop-ceny tak i procentuálního rozdílu. Správné nastavení těchto parametrů je důležitým aspektem pro úspěšné zobchodování zadávaného příkazu. Například, pokud při zadávání trailing stop-limit příkazu je zadán rozdíl od extrému příliš malý, může být příkaz zobchodován dříve než by to doopravdy bylo výhodné nebo chtěné. Naopak, jestliže by rozdíl byl příliš velký nemusí k zobchodování dojít vůbec a příkaz bude na burze nebude nic dělat.



Obrázek 2.1: Příkaz limit s hraniční cenou

2.3.2 Strategie obchodování

Způsobů, jakým lze obchodovat na burzách může být až nekonečně mnoho. Jelikož se kryptoměnové burzy velice podobají forexovým, mohou se uplatnit podobné obchodní strategie. Některé strategie mohou fungovat lépe nebo hůře v závislosti na obchodovaném aktivu. Každý uživatel si může zvolit svou vlastní strategii, tak aby mu vyhovovala a pár z nich popisuje tato podsekcce.

2.3.2.1 Day trading

Denní obchodování nebo-li *day trading* se zaměřuje, jak název napovídá, na obchody netrvajících déle než den. Tito obchodníci se snaží najít co nejvýhodnější bod pro nákup a prodej aktiva v rámci jednoho dne a snaží se držet svou pozici nejdelší rozumnou dobu, aby mohli následně svou pozici uzavřít (prodat) se ziskem. Těchto pozic neotevívají hodně, spíš jen pár za celý obchodní den.

2.3.2.2 Scalping

Tito obchodníci, nazývaní „skalperi“ se snaží vydělat na mnoha malých, ale profitabilních obchodech. Pozice drží otevřené krátkou dobu, většinou pár minut s nejdelší možnou dobou až pár hodin. Často využívají i *pákového efektu*³. Hlavní podstata této strategie je dosáhnout zisku i z malých změn tržní hodnoty aktiva. K rozhodování o otevření pozic se opírají o *technickou analýzu*, která bude detailněji popsána v kapitole 3.

2.3.2.3 Swing trading

Swing tradeři sporadicky otvírají a zavírají pozice na trhu, přičemž své pozice drží i v období několik dnů, nebo týdnů. Čekají na větší cenové výkyvy (doslova zhoupnutí ceny, odtud název swing trading) a tomu odpovídá i delší doba trvání obchodu. Využívají technickou analýzu ale i fundament daného aktiva a snaží se odhadnout dlouhodobější trendy.

2.3.2.4 Buy-and-hold

Tato poslední metoda obchodování je čistě dlouhodobá a jedná se pouze o nákupy aktiv. Převážně oblíbená v krypto komunitě dostala tato strategie přezdívku HODL. Vyhybáním prodeje se investoři snaží mířit na výhledový zisk z držení. Podle motivace a filozofie HODLerů je vždy skvělá příležitost nakoupit kryptoměnu a za žádných okolností neprodávat, ale držet své coinu u sebe.

³Pákový efekt umožňuje traderovi otevřít pozici s násobenou kupní silou a tím i možností jak vyššího zisku, tak i případné ztráty.

Kapitola 3

Technická analýza

Dělat informovaná rozhodnutí je podstata každého obchodníka. V akciových trzích se významně používá fundamentální analýza používaná pro budoucí odhad chování trendu trhu. Fundament se zabývá vnitřní hodnotou trhu, která je spjatá s obchodními výsledky podniků obchodovaných na burze. Tyto dvě faktory, tedy dlouhodobé obchodní výsledky podniků často korelují právě s hodnotou akcií. Vnitřní hodnota trhu je pak odhadována za momentální hodnotou jmění těchto firem. Odhady lze dělat z veřejně dostupných dat, například ze zveřejněných účetních uzávěrek, vyplacených dividend, nové produkty nebo různých ekonomických zpráv. Oproti tomu, technická analýza se snaží odhadnout budoucí pohyb tržních cen aktiv (forex, akcie, kryptoměny) na základě dostupných historických dat, převážně z ceny a objemu minulých uzavřených obchodů. Momentální kapitola se podrobněji věnuje technické analýze, její historii, z čeho technická analýza vychází a zabírá se několika prostředcích používané při této metodě předpovědi trhu.

3.1 Historie

První náznaky principů technické analýzy se začaly objevovat už v 17. století v práci Josepha de la Vegy o holandských trzích. O století později začíná rozvoj dalších metody v Asii, která se postupně vyvíjí v použití svíčkové techniky. Dnes se jedná o nejpoužívanější nástroj pro vytváření finančních grafů. V první půlce 20. století vznikají první knihy zaměřené na technickou analýzu trhu. V té době se jedná převážně o techniky zaměřené na analýzy trendu a grafové vzory, jelikož výpočetní síla počítačů pro statistickou analýzu nebyla dostupná. Některé z těchto knih, převážně práce Roberta D. Edwardse a Johna Mageeho *Technical Analysis of Stock Trends*, se považují za klíčové v tomto oboru a zůstávají platné dodnes. V posledních dekáдах bylo vytvořeno mnoho dalších technických nástrojů a teorií, čím dál více opírající se počítačové podpořené výpočetní techniky.

3.2 Principy

Techničtí analytici věří ve 3 hlavní principy. První z nich zní takto: *Ceny se pohybují v trendech*. Tedy, že tržní cena buďto roste, klesá, nebo se pohybuje pouze do strany přičemž poslední varianta je též označována jako stagnace. Druhý z těchto principů je: *Historie má tendenci se opakovat*. Pokud se historie opakuje, musí v grafech, které vizualizují vývoj trhu, existovat jisté vzory předpovídající nastávající trend. Posledním principem je tvrzení, že *tržní očekávání je reflektováno a započteno na hodnotě aktiva*. Pokud existují novinky, předpovídající, nebo naznačující vzestup například zemědělského trhu díky úrodné sezóně, je toto očekávání již pozitivně reflektováno na hodnotě akcií zemědělských firem a lze to tím pádem vyčíst i z grafů. Jelikož vzory hrají velkou roli v oboru technické analýzy je následující sekce zaměřená na popis, identifikaci a význam několika vzorů.

3.3 Grafové vzory

Grafové vzory jsou opakovaně formující se útvary a v technické analýze jsou využívány jako signály buďto přetrvávání nebo obratu momentálního trendu. Vzory se formují při vykreslení tržních cen na grafu. Typickým a nejčastěji používaným grafem, jak již bylo zmíněno, je graf svíčkový, vyobrazený na obrázku . Vzory lze pak pozorovat na posloupnosti několika po sobě jdoucích svíček. Důležitým faktorem při rozpoznávání vzorů je zobrazené časové rozpětí, které investor pozoruje. Ne vždy mohou být vzory dobře rozpoznatelné lidským okem. Užitečnost vzoru časem klesá. Čím později je detekován, tím je méně použitelný. Existují pokusy použít strojové učení pro detekci těchto vzorů, jako například práce autorů *Marc Velay a Fabrice Daniel*, kterým se podařilo dosáhnout 97% recallu, ale model uměl detekovat pouze 1 vzor.

3.3.1 Head and shoulders

První a zároveň z jeden více známých obratových vzorů je „Head and shoulders“ (Hlava a ramena), viditelný na obrázku . Jak název napovídá, formace svíček tvoří podobu ramen a hlavy způsobenou 3 kopci a 2 dolinami z čehož je prostřední kopec vyšší než zbývající krajní. V dolinách se cena zastaví na přibližně stejné hodnotě, tvořící tzv. „neckline“ neboli krk. Během formace levého ramene a hlavy se při stoupající ceně taktéž obchoduje ve vyšších objemech než při klesání. V průběhu tvorby pravého ramene objem obchodů začíná klesat společně s cenou. Jakmile cena prorazí *neckline* a začne padat pod její úroveň, je vzor jednoznačně dokončen a očekává se pokles ceny. Reálně nemusí formace vypadat naprosto ideálně. Často může být jedno rameno o něco nižší, případně i širší, než druhé a neckline nemusí být skvěle zarovnaná.

3.3.2 Cup and handle

Formace připomínající šálek s rukojetí (obrázek) je symbolem pro rostoucí trend na trhu. Identifikovatelný je tvorbou široké, ale ne příliš hluboké doliny, přičemž na končící ceně této doliny dojde k dalšímu, již méně razantnímu poklesu v ceně. Tento menší pokles připomíná právě onu rukojet a musí vždy následovat až po šálku. Toto pořadí je nezaměnitelné. Dolina by měla své dno zaoblené a připomínat například misku. Šálek ve tvaru „V“ není platným ukazatelem nastávajícího vzoru. Objem obchodů je relativně nízký, ale v období tvorby rukojeti se rapidně zvyšuje.

3.3.3 Double top a Double bottom

Další obratový vzor je „Double top“, vyskytující se na konci býčího trhu.¹ Po jasném potvrzení vzoru lze předpokládat pokles hodnoty aktiva. Opačným vzorem je Double bottom, formující se právě na konci medvědího trhu s odhadem následně rostoucího cenového trendu. Double top je na grafu rozpoznatelný podle 2 kopců, zhruba ve stejné cenové úrovni, oddělené dolinou. Ona minimální cena v dolině tvoří neckline tohoto vzoru. Jakmile je neckline proražena při sestupu z druhého kopce, je formace dokončena potvrzující signál k prodeji nebo shortování. Časové rozmezí mezi kopci je taktéž rozhodující faktor při indikaci změny trendu. Jestliže se zformované kopce nacházejí v přibližně stejné cenové hladině, ale jsou časově příliš blízko sebe, může se jednat pouze o konsolidaci trendu a jeho následné pokračování. V případě Double bottom je formace překlopená, tedy se v ní vyskytují 2 doliny oddělené kopcem tvořící neckline. Oba útvary jsou znázorněná na obrázku

3.3.4 Triple top

Méně častý vzor Triple top, tvořený 3 kopci, slouží jako indikátor možné změny aktuálního tržního trendu. Pravidla potvrzení Triple topu jsou podobná jako u předchozího vzoru, tedy kopce jsou na stejné cenové hladině, oddělující doliny (tvořící neckline) taktéž. Jakmile dojde k proražení neckline, je formace dokončena.

3.3.5 Wedge

Wedge (klín) existuje ve dvou variantách, Falling wedge (padající klín) a Rising wedge (stoupající klín). Rozpoznatelný je tím, že se svíčky pohybují v rozmezí dvou sbíhajících přímk. Pokud je průsečík přímek pod momentální tržní cenovou hladinou, bude se jednat o padající klín. Naopak, jestliže je průsečík nad aktuální hodnotou aktiva, zformuje se stoupající klín. Význam, který tento vzor poskytuje se liší na základě trendu a v jaké variantě byl utvořen.

¹ Označení popisující dlouhodobě stoupající cenový trend. Jeho opakem je medvědí trh pro označení dlouhodobě klesajícího trendu.

Padaající klín v sestupném trendu signalizuje obrat, jelikož smršťování cenových rozsahů značí, že trend ztrácí sílu. Nalezení tohoto vzoru ve vzestupném trendu indikuje pouze dočasné pozastavení. Trh se trochu zkoriguje, a původní trend bude pokračovat. Velikost obchodů v tomto vzoru se společně s množstvím obchodů snižuje kvůli zmenšujícím se cenovým rozsahům. Jakmile dojde k průrazu, začnou se parametry obchodů opět odrážet aktuální trend.

Stoupající klín indikuje podobné signály jako padající klín. Pokud je nalezen při vzestupném trendu, je velice pravděpodobné, že bude následovat obrat trendu. V případě, že jej nalezneme v klesajícím trhu, bude to náznak spíše korekce a klesání bude pokračovat.

3.3.6 Triangle

Posledním uvedeným vzorem je trojúhelník. Oproti klínu se liší v tom, že jedna z přímk je vždy zarovnaná a tvoří cenovou hladinu, od které se svíčky odráží zpět. Tento vzor, stejně jako klín, má stoupající a klesající variantu. Stoupající trojúhelník se formuje pokud trh v daném časovém okně zaznamenává postupně vyšší minima, ale maxima se zachovávají stejně vysoká. Pro klesající trojúhelník je situace opačná - maxima se krok za krokem snižují a minima zůstávají na stejné úrovni. Jestliže narazíme na stoupající trojúhelník při vzestupném trendu, můžeme očekávat pokračování tohoto trendu. Avšak nalezneme-li jej v trendu sestupném, může se jednat o silnou indikaci obratu tržní nálady.

3.4 Support a resistance

V předchozí sekci zabývající se grafovými vzory se několikrát objevily určité čáry, od kterých se tržní cena odrážela zpět nahoru nebo naopak dolů. Tyto čáry se též označují jako odporové úrovně *support* a *resistance*. Support je cenová úroveň, od které se ceny „odrážejí“ když klesají dolů. To znamená, pokud existuje posloupnost svíček, jejichž close cena klesá, jakmile se přiblíží k ceně supportu tak se spíše odrazí a cena aktiva začne opět stoupat. Naopak k tomu resistance je hranice, která tvoří „zábranu“ stoupajícím cenám. V momentě kdy se svíčky blíží úrovni rezistance je velká pravděpodobnost že se odrazí a dojde ke klesání.

Existuje několik způsobů jak identifikovat tyto odporové úrovně. Nejčastější metoda je s pomocí trendových čar. Trendové linie se jednoduše zakreslí spojením spodních a horních stínů svíček. Čím více jsou tyto úrovně otestovány tím, že se cena od nich odráží, tím větší význam můžeme těmto úrovním skutečně připsat. Jakmile dojde k proražení rezistance, stává se ona úroveň supportem. Pravdivý je i opačný případ, kdy dojde k proražení supportu a stává se z toho nová rezistance. Pokud se cena aktiva pravidelně pohybuje v těchto úrovních, nejjednodušší využití tohoto cyklu je nakupovat, když se cena pohybuje v blízkosti supportu a prodávat v okolí rezistance. Samozřejmě je důležité uvážit časové okno pro zakreslování těchto úrovní a doba obchodování.

3.5 Indikátory

Indikátory jsou signifikantní součástí technické analýzy. Technické indikátory se opírají o matematické výpočty a počítají se za nějaké období. Jako vstupem do výpočtu se nejčastěji bere tržní cena nebo objem obchodů. Na základě těchto informací jsou dané výstupy, které dodávají další informace k obchodování. Obecně se technické indikátory dělí na indikátory hybnosti (momentum indikátory), trendové indikátory a oscilátory. Momentum indikátory měří dynamiku ceny, tedy rychlost změny. Trendové indikátory se zaměřují na odhad aktuálního trendu a případnou predikci jeho otočení. Jako oscilátory se označují indikátory, které se pohybují v daném rozmezí (např. -1 až 1). Tato sekce se zabývá několika nepoužívanějšími technickými indikátory, rozebírá způsob jejich výpočtu a dodanou informační hodnotu.

3.5.1 Indikátor objemu (OBV, On-balance volume)

Jedná se o kumulativní indikátor objemu obchodů a tím měří nákupní a prodejní tlak a spojuje tržní cena v souvislosti na velikostech obchodů. Pokud se OBV zvyšuje, více obchodníků je ochotných zaplatit za aktivum v jeho momentální tržní ceně. Pokud je trh ve vzestupném trhu a navíc k tomu stoupá i hodnota tohoto indikátoru, potvrzuje se tímto onen trend. Jestliže cena stoupá ale hodnota OBV nijak neroste, je trh spíše zmatený. Výpočet OBV je znázorněn na 3.1

$$OBV = OBV_{pred} + \begin{cases} objem, & close \geq close_{pred} \\ 0, & close = close_{pred} \\ objem, & close \leq close_{pred} \end{cases} \quad (3.1)$$

3.5.2 Klouzavý průměr (MA, Moving average)

Klouzavý průměr má hned několik variant výpočtu. Klouzavý se nazývá protože se jeho hodnota počítá pouze za určené období. Oblíbené časové úseky jsou 10, 40, nebo 200 dní zpětně. Navzdory představě tento indikátor není „pouze jedno číslo“, ale celá série, jelikož průměr je počítán pro každý datový bod, tedy pro každou svíčku zvlášť. Propojením vypočítaných hodnot vzniká na grafu linie představující plovoucí odporovou úroveň s výhodou jakési odolnosti proti krátkodobým fluktuacím v cenách aktiva. Tato odolnost usnadňuje predikci spíše dlouhodobějších trendů. Jestliže se trh nachází v sestupném trendu, MA se chová jako úroveň rezistance a jeho proražení dává signál k nákupu, předpovídající vzestupný trend. Opačný případ je taktéž pravdivý, kdy ve vzestupném trhu MA zastává roli supportu.

Dva nepoužívanější typy výpočtu MA jsou *Simple Moving Average (SMA)* a *Exponential Moving Average (EMA)*. SMA je jednoduchý pro výpočet a jedná se o obyčejný průměr na období o velikosti n a způsob výpočtu je vyobrazena na rovnici 3.2. EMA využívá váženého průměru, ve kterém se váha starších datových bodů se exponenciálně snižuje, preferující spíše novější hodnoty. Při výpočtu tohoto

váženého průměru se používá i takzvaný vyhlazovací koeficient k , přičemž nejčastější nastavení tohoto koeficientu je $k = \frac{2}{n+1}$. Rovnice pro výpočet je na 3.3. Výhodou exponenciálního klouzavého průměru je větší důraz na čerstvější data, čím může lépe reagovat na změny trhu.

$$SMA_t = \frac{C_t + C_{t-1} + \dots + C_{t-(n-1)}}{n} \quad (3.2)$$

$$EMA_t = k * C_t + (1 - k) * EMA_{t-1} \quad (3.3)$$

3.5.3 Index relativní síly (RSI, Relative strength index)

Index relativní síly patří mezi oscilující indikátory, pohybující se v rozmezí on 0 do 100. Jeho cílem je odhalit rychlost a velikost změny „close“ cen aktiv a tím identifikovat přeprodaný nebo překoupený trh. Důležité signály nastávají v momentě, kdy se hodnota tohoto indikátoru zvedne nad hladinu 70 nebo klesne pod hladinu 30 a interpretace je následující:

- Pokud hodnota $RSI > 70$ je trh překoupený a má vyšší hodnotu, než by měl mít; následuje korekce nebo otočení trendu.
- Pokud hodnota $RSI < 30$ je trh přeprodaný a má nižší hodnotu, než by měl mít; následuje korekce nebo otočení trendu.
- Při opětovném sestupu pod hranici 70 je identifikován sestupný sentiment.
- Při opětovném vzestupu nad hranici 30 je identifikován vzestupný sentiment.

Pro výpočet indexu relativní síly je nutné nejdříve spočítat relativní sílu. Abychom zjistili relativní sílu, musíme zjistit horní (U) a dolní (D) změnu:

$$U = \begin{cases} C_t - C_{t-1}, & close_t > close_{t-1} \\ 0, & close_t \leq close_{t-1} \end{cases}, D = \begin{cases} C_{t-1} - C_t, & close_t < close_{t-1} \\ 0, & close_t \geq close_{t-1} \end{cases} \quad (3.4)$$

Pak můžeme vypočítat relativní sílu RS za období délky n :

$$RS = \begin{cases} \frac{EMA(U,n)}{EMA(D,n)}, & EMA(D,n) > 0 \\ 100, & EMA(D,n) = 0 \end{cases} \quad (3.5)$$

A nakonec dopočítat index:

$$RSI = 100 - \frac{100}{1 + RS} \quad (3.6)$$

3.5.4 MACD indikátor (Moving average convergence-divergence indicator)

Indikátor sbíhavosti a rozbíhavosti klouzavých průměrů se skládá z několika komponent. První je samotný MACD, což je rozdíl dvou exponenciálních klouzavých průměrů, počítané za kratší a delší období. Další složkou je signální čára, vypočítaná jako EMA právě onoho MACD. Poslední složka je histogram ukazující rozdíl mezi MACD a signální čarou.

$$MACD = EMA(n_1) - EMA(n_2), n_2 > n_1 \quad (3.7)$$

$$Sig_{MACD} = EMA(MACD, n_3) \quad (3.8)$$

$$Hist_{MACD} = MACD - Sig_{MACD} \quad (3.9)$$

3.6 Využití

3.7 Výběr krytoměnových párů

Kapitola 4

Kryptoboti

Kapitola 5

Legislativa