Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Kryptoměny

Viktor Santarius

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Viktor Santarius

Systémové inženýrství a informatika
Informatika

Název práce

Kryptoměny

Název anglicky

Cryptocurrencies

Cíle práce

Cílem práce je vytvoření vlastní testovací kryptoměnu a otestování její funkčnosti. Budou vyzkoušeny základní operace jako jsou těžba, provedení a odvolání transakce.

Metodika

Teoretická část bakalářské práce bude založena na studiu odborných informačních zdrojů. Tato část bude obsahovat popis a principy současných kryptoměn. Dále budou zkoumány jejich výhody, nevýhody a rizika. Následně bude vytvořena vlastní kryptoměna a na mí budou vzkoušeny základní operace jako jsou např. těžba, provedení a odvolání transakce, atd.

Doporučený rozsah práce

30-40 stran

Klíčová slova

Kryptoměna, Bitcoin, Alternativní měna, Digitální Měna

Doporučené zdroje informací

Andreas M. Antonopoulos: Mastering Bitcoin, O'Reilly Media 2014, ISBN-13: 978-1449374044

Dominik Stroukal a Jan Skalický: Bitcoin: Peníze budoucnosti, Ludwig von Mises Institut 2016, ISBN 978-80-87733-27-1

Karel Filner: Jak na bitcoin krok za krokem, [online] http://btctip.cz/jak-na-bitcoin-krok-za-krokem-e-book-zdarma/

Narayanan A. et. al.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press 2016. ISBN-13: 978-0691171692

Předběžný termín obhajoby

2019/20 ZS – PEF (únor 2020)

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 1. 3. 2017

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 3. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 03. 2020

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Kryptoměny" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2020 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Marku Píckovi, Ph.D. za vedení práce a Ing. Petru Santariusovi a Bc. Dagmar Santariusové za pomoc při psaní bakalářské práce.

Kryptoměny

Abstrakt

Tato bakalářská práce se zabývá historií, současností kryptoměn a popisem jejich klíčových vlastností, zejména asymetrické kryptografie, hash funkce, struktury blockchain a principu těžení nové mince. Velký důraz je kladen na nejznámější současnou kryptoměnu Bitcoin, historii vzniku a provedení první transakce. Dále jsou popsány některé rozšířené kryptoměny: Litecoin, Monero a Ethereum.

Praktická část se zabývá vytvořením zjednodušeného modelu kryptoměny nazvané Santacoin. Blockchain model je vytvořený ve formátu XML.

V programovém jazyce PHP jsou naprogramovány základní funkce například přidání nového datového bloku na konec blockchainu, vytěžení nové mince a provedení transakce mezi uživateli. Uživatel má k dispozici softwarovou peněženku, která umožňuje platby i zobrazení obsahu peněženky (vlastněné mince).

Hlavní důraz je dán na vytvoření modelu blockchainu (řetězce bloků), vytvoření a ověření elektronického podpisu (veřejný a soukromý klíč), použití hash funkce na kontrolu neporušenosti celého blockchainu. Tato poslední jmenována vlastnost je otestovaná na několika demonstračních příkladech, čímž je potvrzena funkčnost hash pro zajištění celistvosti a kontroly blockchainu.

Klíčová slova: kryptoměna, Bitcoin, alternativní měna, digitální měna, asymetrická kryptografie, hash, blockchain

Cryptocurrencies

Abstract

This bachelor thesis deals with history and current situation about cryptocurrencies and with the description of keys parameters, mainly asymmetric cryptography, hash function, blockchain structure and principles of new currency mining. A big focus is given to the most know current cryptocurrencies Bitcoin and history of its creation and its first transaction. Later on, there are described another widely used cryptocurrencies: Litecoin, Monero and Ethereum.

In the practical part of this bachelor, there is created a simple model of a cryptocurrency named Santacoin. The blockchain model structure is in the XML format.

The basic functions, such as adding new data block at the end of blockchain and coin mining and transaction of one coin between two users, is developed in programming language PHP. The user has access to a software wallet, can execute the payment and see the wallet content (owned coins).

The main focus is given to the creation of the blockchain (chain of blocks) model, creating and verifying the digital signature (public and private key) and usage of the hash function to the check of the whole blockchain consistency. The last feature is tested on a few sample and by this, it is confirmed full functionality of hash function to secure consistency and blockchain check.

Keywords: cryptocurrencies, Bitcoin, alternative currency, digital currency, asymmetric cryptography, hash, blockchain

Obsah

Seznam obrázků

1 Úvod

Kryptoměna je typ digitální měny, která se opírá o kryptografii, digitální podpisy jednotlivých převodů, peer-to-peer (P2P) sítě a decentralizaci. Nejznámější a nejrozšířenější kryptoměnou je Bitcoin, který se stal v poslední době velkých hitem a investiční příležitostí. V dnešní době je Bitcoin stále pro mnoho lidí velkou neznámou. Většina z nás alespoň jednou slyšela o Bitcoinu, ale nevíme, co to přesně je a k čemu slouží a na jakých principech funguje.

Bitcon je označován jako sada konceptů a technologii, které formují základ ekosystému digitální měny (Andreas 2014).

Bitcoin je decentralizovaná (P2P) síť v internetu, spravující historii platebních transakcí mezi svými uzly. Základní jednotkou transakce je bitcoin (BTC). Počet jednotek této „kryptoměny“ je omezen a nové vznikají procesem těžení. Při těžbě dochází kromě generování nových bitcoinů rovněž k potvrzování vlastních transakcí – převodů jednotek mezi bitcoinovými adresami (Stroukal & Skalický 2018).

V teoretické části práce budou popsány a vysvětleny odborné termíny a postupy používané ve světě kryptoměn, jako jsou například peer-to-peer, blockchain, decentralizace, asymetrická kryptografie. Budou popsány nejznámější a nejdůležitější kryptoměny a jejich klíčové vlastnosti, včetně krátkého seznámení s historií a vývojem kryptoměn, použití kryptoměn, jejich hlavní rozdíl oproti klasickým měnám a jejich možné využití do budoucna.

V praktické části práci bude vytvořena vlastní zjednodušená kryptoměna nad modelem blokchain. Vše bude naprogramováno v programovacím jazyce PHP. Tento program bude umožňovat základní operace „peněženky“ jako je výměnu mince (platbu) mezi dvěma uživateli, výpis transakcí a obsahu peněženky (vlastněné mince).

Důležitou funkčností bude použití elektronického podpisu (soukromého a veřejného klíče), podepsání transakce a ověření elektronického podpisu. Současně se za použití funkce hash zajistí základní bezpečnost (kontroly blockchain proti dodatečné změně).

V závěru práce budou na modelu vlastní kryptoměny a na vytvořených testovacích vzorcích dat ověřeny klíčové mechanismy kryptoměny.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je vytvoření vlastní testovací kryptoměny a otestování její funkčnosti. Budou vyzkoušeny základní operace, jako je vytvoření nové mince (těžba), provedení transakce a test zamezení dvojímu placení. Uživatel bude mít k dispozici základní funkčnost softwarové peněženky.

2.2 Metodika

Bakalářská práce se skládá ze dvou částí, a to teoretické části práce a praktické části práce. Poznatky budou založeny na studiu odborných informačních zdrojů.

V teoretické části bakalářské práce budou popsány odborné termíny jako peer-to-peer, blockchain, asymetrická kryptografie, kterými se bude bakalářská práce zabývat. Následně bude popsána historie Bitcoinu, seznámení se s klíčovými osobami historie Satoshi Nakamoto a Hal Finney. Dále budou popsána možná nebezpečí, která jsou spojená s kryptoměnou. V další kapitole teoretické části budou vyjmenovány nejznámější kryptoměny jako jsou Bitcoin, Litecoin, Monero a Ethereum. Každá tato měna bude obsahovat detailní popis a principy, budou zkoumány jejich výhody, nevýhody a rizika.

V druhé části bakalářské práce, která je praktická, bude vytvořena vlastní kryptoměna pojmenovaná Santacoin. Tato měna bude naprogramována v PHP prostředí jako webová aplikace. PHP je skriptovací jazyk vhodný pro vývoj webové aplikace (PHP 2020). Pro zjednodušení nebudeme uvažovat takzvané těžení nové mince pomocí potvrzovaní v blockchainu. Pro každou novou minci bude místo těžení navržena pouze matematická kontrola této nové modelové kryptoměny. Následně budou manuálně vytvořeni uživatelé, na kterých se bude testovat tato kryptoměna. Důraz bude kladen na funkčnost blockchainu: zaregistrovaní nové mince, výměna mincí mezi dvěma uživateli (platební transakce), elektronický podpis a jeho kontrola a zápis nového bloku na konec blockchainu, včetně kontroly konzistence celého blockchainu.

V závěru práce bude ověřena funkčnost blockchainu. Zda jsou řádně zachyceny veškeré transakce, přesně jak následují po sobě, tedy zda jde opravdu o otevřenou „účetní knihu“, kdy všichni vidí všechny transakce.

3 Odborné termíny

3.1 Decentralizace a Peer-to-Peer sítě

Kryptoměny fungují v peer-to-peer síti počítačů, které se nazývají uzly (nebo taky klienti). Tito klienti jsou odpovědní za provádění transakcí. Všichni klienti jsou rovnocenní (Clark 2013).

Základem takového typu sítě a také hlavní důvod, proč se používá Peer-to-Peer síť, je ona neexistence centrálního serveru. Neexistující centrální server nelze jednoduše vyřadit. Vyřazení jakéhokoliv samostatného uzlu, případně i více uzlů nemá vliv na chod zbývající sítě.

Princip je trochu podobný samotnému fungování internetu, kdy v případě poruchy nějakého uzlu může systém komunikovat přes uzly ostatní.

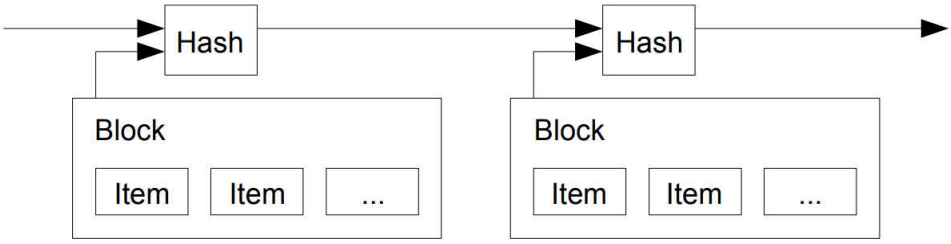
Jak už bylo uvedeno, klasická měna je vydávána státem nebo více státy (euro) a je vždy centrálně řízená. Velkou nevýhodou je, že klasická měna je plně státem a politiky kontrolovaná a ovlivňovaná. Naproti tomu virtuální decentralizovaná měna nemůže být politiky nijak ovlivňována ani kontrolována, což je stav, kterého se všechny státy obávají. V současné době se už objevují snahy tyto měny regulovat, ovládat a další vývoj do budoucna je nejasný.

3.2 Dělení mince

Vzhledem k tomu, že hodnota jedné mince je poměrně vysoká, běžně se dá obchodovat s velice malými částmi jedné mince. V případě Bitcoinu se můžeme setkat s názvy Centibitcoinem (1cBTC), Milibitcoinem (1mBTC) a Mikrobitcoinem (1µBTC).

3.3 Blockchain

Pomocí blockchainu se evidují všechny provedené transakce. Schéma zveřejněné v takzvaném „White Paper“ dokumentu publikovaném autorem Bitcon Satoshi Nakamoto je na následujícím obrázku (Satoshi 2008). Blockchain je řetězec bloků (chain of blocks) navzájem propojených a chráněných proti změně pomocí hash funkce. Může být uložený ve formě souboru či databáze (Andreas 2014).



Obrázek 1.: Blockchain

Protože se nejedná o centralizovanou síť, ale síť peer to peer (jak bylo uvedeno dříve) je tato evidence všech transakcí decentralizovaná a je dostupná všem uživatelům sítě. Každý uživatel má vlastní kopii blockchainu. Pokud by v této síti zaplatil někdo více transakcí stejnou mincí, ostatní uživatelé si toho všimnou a daná transakce nebude provedena (viz „Princip dvojí útraty“). Transakce je schválena teprve v případě, kdy ji potvrdí určité, předem stanovené množství uživatelů. Takto se systém velice účinně brání principu „dvojité útraty“. Blockchain obsahuje seznam transakcí, kdy jedna transakce navazuje na druhou. Zahrnutím hash předchozí transakce do následující transakce je jednoznačně určeno, která transakce následuje po které a není možné změnit pořadí transakcí. Tento princip umožňuje zaznamenat historii transakcí, která je neměnná a nepřepsatelná.

Princip blockchainu, tím jak je navržený, umožňuje zápis jakékoliv transakce, nejenom finanční. V současné době vzniká celá řada aplikací nad mechanismem blockchain. Lze takto evidovat nákupy, prodej bytů, nebo půjčení knih ve veřejné knihovně. Vzhledem k tomu, že se čím dál více operací přesouvá do digitálního světa a v blízké budoucnosti bude mít každý občan svoji vlastní digitální identitu a digitální podpis, může princip blockchainu zasáhnou do prakticky každé lidské činnosti.

3.4 Asymetrická kryptografie (klíč)

Digitální platební systémy musí zabezpečit měnu před podvody (Clark 2013). V historii byl problém mezi bezpečnou komunikací mezi dvěma uživateli. V roce 1975 začala pro toto odvětví zásadní změna. Whitfield Diffie přišel s myšlenkou asymetrické kryptografie, která používá skupiny kryptografických metod pro šifrování a dešifrování zpráv. Hlavní vylepšení, se kterým přisel, je využití dvou odlišných klíčů, veřejného a soukromého klíč.

Princip šifrování zprávy je ten, že uživatel zašifruje zprávu pomocí veřejného klíče, ale už pomocí něj nejde zprávu dešifrovat. Pro dešifrování se použije klíč soukromý, který je ve vlastnictví majitele, pro kterého je zpráva určena. Tyto dvě strany se nemusí setkat, ale přitom komunikují bezpečně.

Asymetrická kryptografie se používá také v oblasti elektronických podpisů. V tomto případě, se klíče používají odlišným způsobem. Ten, kdo chce podepsat nějakou zprávu, použije svůj soukromý klíč a veřejný klíč slouží ke kontrole toho, že zprávu podepsal držitel soukromého klíče. Pomocí veřejného klíče nelze zprávu podepsat, pouze zprávu zkontrolovat. V praxi se používají oba principy současně, zpráva se zašifruje, tak i podepíše.

3.5 Hash

Vznik funkce hash spolu s asymetrickou kryptografií byly dvě důležité a nezbytné podmínky vzniku kryptoměn. Bez nich by decentralizovaná kryptoměna nemohla vůbec vzniknout. Hashovací funkce je jednosměrná/jednocestná funkce, které předáme jako vstupní parametr libovolně dlouhou zprávu a na jejím výstupu pak obdržíme takzvaný hash neboli otisk, v požadované délce bitů. Důvod, proč se o této funkci hovoří jako o jednocestné, je ten, že z výstupu této funkce nejsme schopni zpětně vygenerovat vstup, který byl jejím parametrem. Jinými slovy, z hashe nelze odvodit původní zprávu.

V případě blockchainu se hash funkce používá ke kontrole konzistence zprávy. Při zápisu nové zprávy se hash počítá z předchozí zprávy a nové zprávy. Protože je prakticky nemožné změnit zprávu tak, aby hash zůstal stejný, tak tento mechanismus slouží ke kontrole toho, že nikdo bloky již zapsané do blockchainu nezmění. Pokud je tato chyba nalezena je tento blockchain považován za chybný a přestane se používat.

Matematické hash funkce se postupně rozšiřují o nové funkce a dále se vyvíjí. Hodně známý a používaný algoritmus MD5 navrhl v roce 1991 Ronald Rivest. MD5 je často používán pro ověření integrity souborů. Od roku 1996 se začíná doporučovat algoritmus SHA.

Příkladem hashovacích funkcí jsou různé kontrolní součty (XOR, rotace, tabulky) a CRC (tělesa nad dělením polynomů). Mezi kryptografické hashe patří např. funkce BLAKE, MD2-6, RIPEMD, SHA. Bitcoinový protokol používá poslední dvě jmenované zejména SHA-256 při těžbě bloků (Stroukal & Skalický 2018).

3.6 Těžba měny

Těžbou se nazývá postup, při kterém vznikají nové mince. Těžba (mining) je proces, při kterém se pomocí strojově náročného výpočtu hledá další blok pro napojení do blockchainu. Validní blok je nalezen, pokud splňuje podmínku, že jeho hash (přesněji hash vypočtený nad serializací jeho dat) je nižší než určitý cíl (Stroukal & Skalický 2018).

Měna Bitcoin byla navržena tak, že od počátku neexistují všechny jednotlivé mince, ale nové mince se musí těžit. Za těžení dostávají aktivní uživatelé nové mince a tím jsou motivováni, aby byl nový blok co nejrychleji zapsán. Bitcoin zapisuje transakce každých deset minut. Odměna se postupně snižuje, čímž je omezen maximální počet mincí v systému. Tvůrce Bitcoin počítal s tím, jak se bude snižovat odměna v podobě nových mincí, tak současně bude růst výnosů z poplatků za transakce (každý kdo žádá o převod, platí velice malou část mince tomu, kdo blok vypočítá a zapíše).

Matematický aparát Bitcoinu bude obsahovat zhruba 21 milionů mincí. Všechny mince by měly být vytěženy zhruba do roku 2140. (Andreas 2014).

Na těžení se zaměřuje celá řada firem, které dávají dohromady ohromný výpočetní výkon počítačů na těžení nových mincí. V dnešní době, jak rostou hodnoty mincí, se dokonce některým firmám vyplatilo vyvinout speciální procesory pouze pro těžení.

Poměrně častý je i způsob, že těžení probíhá formou distribuovaného výkonu, kdy je potřebný výpočetní výkon rozprostřený mezi více méně výkonných výpočetních jednotek (například osobních počítačů jednotlivých členů). Odměna je pak rozdělována podle toho, jakým výkonem, kdo přispěl (Filner 2017). Tomuto principu se říká těžební pool.

3.7 Princip zamezení „dvojí útraty“

V případě, že používáme kryptoměnu, kdy peníze jsou pouze virtuální „jedničky a nuly“ a je možné jednotlivou minci několikanásobně použít, je nutné zamezit tomu, aby se jedna stejná mince použila ve více transakcích.

Základním problémem je totiž vymyslet, jak to zařídit, aby nikdo nemohl udělat kopii digitálních peněz (Filner 2017). Vyřešit tento problém se podařilo pomocí takzvaného systému blockchainu. Zápis nové transakce se vždy kontroluje ostatními uživateli a je považován za schválený, teprve když jej odsouhlasí více než 50 % uživatelů v síti Bitcoin.

4 Historie kryptoměn

Historie kryptoměn není ve srovnání s klasickými měnami velmi dlouhá. První kryptoměny, které vznikly v 80. letech 20. století například Ecash ještě pracovaly s centrálním serverem. Jak se později ukázalo, centrální server byl jednoznačně slabým prvkem těchto měn.

Mezi roky 1970 a 1980 matematici na Stanford na MIT univerzitách pomocí matematických výzkumů umožnili poprvé „obyčejným“ lidem zakódovat zprávy, aby nebylo možné jejich rozkódování pomocí nejvýkonnějších počítačů. Tyto výzkumy posloužily jako nezbytná součást kryptoměn.

První celosvětově rozšířená kryptoměna, která již nepoužívá centrální server a vyvinula tak tuto novou vlastnost pro další měny, byla měna Bitcoin. Podle dostupných informací byl první Bitcoin vytěžen 3.1.2009, tedy zhruba před deseti lety (Stroukal & Skalický 2018).

Kryptoměny jsou nové formy peněz. Co je na nich nejdůležitější, je nový koncept a funkce, které se za digitálními měnami skrývají.

V minulosti se opakovaně poukazovalo na to, že virtuální měny slouží k financování nelegálního podnikaní (například prodej drog, zbraní apod.). Velice známa je historie s takzvanou „Silk Road“ (Hedvábná stezka), na které probíhaly nelegální transakce a v počátcích Bitcoinu se v ní odehrávala řada jejich transakcí. Už sama podstata blockchainu, jako otevřené účetní knihy dostupné pro všechny uživatele, pomáhá proti kriminalitě bojovat. Na rozdíl od klasické měny, kdy při platbě hotovostí, nejsou dohledatelné transakce, u kryptoměny jsou vždy všechny transakce veřejné a dohledatelné. U platby kryptoměnou jsou zaznamenány úplně všechny transakce a nejdou zpětně nikdy změnit. Pochopitelně není jasné, kdo danou měnou platil. Což také platí u klasické měny při platbě hotovostí.

4.1 Satoshi Nakamoto

Bitcoin byl vytvořen v roce 2009 anonymním vývojářem pod pseudonymem Satoshi Nakamoto na základě průvodního článku, který publikoval v říjnu roku 2008 (Stroukal & Skalický 2018). První transakce s měnou byla provedena v roce 2009. V této souvislosti jsou velice známa dvě jména. První je Satoshi Nakamoto. Pod tímto jménem byl vytěžený první Bitcoin, do současné doby se nepodařilo prokázat, kdo se za tímto jménem skutečně

skrývá. První vytěžený Bitcoin se tak stal prvním prvkem blockchainu a používá se pro něj pojmenování genesis. Toto jméno se začalo používat ve všech alternativních kryptoměnách pro první prvek blockchainové struktury. Není důležité vědět, kdo za jménem Satoshi Nakamoto stojí. Může to být jak jednotlivec, tak skupina lidí. Důležité ale je, že ten, kdo tuto měnu vytvořil, už nad ní nemá žádnou moc. Satoshi viděl problémy v existujících měnách, které se v kryptoměně pokusil vyřešit. Jeden z velkých problému bylo to, že se vlády snažily řešit problém ekonomiky tím, že tiskly nové peníze. Centrální banky zaplnily trh penězi, aby se ekonomika po krizi znova zvedla. Toto mělo negativní vliv na inflaci peněz klasické měny což u kryptoměny není možné. Na tomto základě začíná vznik Bitcoinu, který nebude moci žádná centrální banka ani žádní politici kontrolovat a ovlivňovat. Důležitou vlastností technologií, které se schovávají za měnou Bitcoin je, že vše je veřejně dostupné jako open source všem uživatelům. Samotný vznik měny Bitcoin pochopitelně umožnily technologie, které byly vynalezeny v nedaleké minulosti například peer-to-peer či asymetrická kryptografie. Spojení těchto jednotlivých technologií umožnilo vznik nové měny, což bylo v minulosti nemyslitelné.

4.2 Hal Finney

Druhé významné jméno v historii Bitcoin je Hal Finney. Ten v roce 2009 provedl první veřejnou transakci zaplacenou pomocí měny Bitcoin. Skutečný přelom nastal až v roce 2010, kdy z dnešního pohledu za neuvěřitelné množství 10 000 Bitcoinu Laszo Hanyecz koupil 2 pizzy. Této první transakci se věnuje řada webových diskuzí, kde se neustále přepočítává cena pizzy k současnému kurzu ceny Bitcoinu. Tato cena je neuvěřitelně vysoká. Je třeba si uvědomit, že v době, kdy tato transakce proběhla, byla měna Bitcoin prakticky neznámá a vlastně neměla žádnou reálnou hodnotu.

Tak jak svět klasických měn má svůj BigMac index, tak má svět virtuálních měn svůj Bitcoin pizza index.

5 Softwarová peněženka

Softwarová peněženka, na rozdíl od klasické peněženky, kde lidé uchovávají peníze, je vlastně program pro práci s kryptoměnami. Dá se spíše přirovnat k elektronickému bankovnictví. Primární cíl je poskytnou uživateli „uživatelský interface“ (Andreas 2014).

Slouží pro obchodování s danou kryptoměnou mezi uživateli a jako ochrana proti odcizení mincí. K ochraně kryptoměny slouží různé programy různé kvality dostupné na internetu a nabízené celou řadou firem, často i burzami. Ochrana elektronických údajů o mincích je velice rozsáhlé téma. Mezi možnosti ochrany kryptoměny patří uložení kryptoměny offline na externí uložiště, jako je například flash disk. Pro obchodování se používá více druhů klientů, které dále dělíme na tlustý, tenký a webový klient.

5.1 Tlustý klient

Tlustý klient uchovává celou historii dané kryptoměny. To může být problém u starších měn, jako je Bitcoin, u kterého celá historie (celý blockchain) zabírá kapacitou více jak sto Gigabitu prostoru. U mladších kryptoměn, kde je historie zatím v rámci ani ne desítek Gigabitů, má běžný uživatel možnost sledovat a mít na svém počítači celou historii všech transakcí.

5.2 Tenký klient

Tenký klient má uložené jenom soukromé klíče a slouží jako prostředník mezi uživatelem a důvěryhodnou třetí stranou. Tento klient se často využívá u mobilních aplikací, které využívají pro uchování soukromých klíčů jejich podobu v podobě QR kódů (dvourozměrné čárové kódy), aby uživatel neměl problém s ovládáním programu a načítáním mincí.

5.3 Webový klient

Jak už podle názvu vyplývá, pro práci s webovým klientem slouží internetový (webový) prohlížeč. Veškeré informace, jako je soukromý klíč, blockchain a další, jsou uloženy u třetí strany a pouze se použijí v případě transakce. Žádná data nejsou uložena na lokálním počítači a nejsou tudíž ohrožena před hrozbami odcizení (viry, hackeři …).

6 Kryptoměny

6.1 Bitcoin

Tato kryptoměna vznikla v roce 2009 a je považována za první plně decentralizovanou kryptoměnu. Návrh měny popsal na takzvaném „Bitcoin white paper“ její zakladatel (Satoshi 2008). Každá mince má veřejnou Bitcoin adresu (číslo bankovního účtu) a k ní patřící privátní klíč, který umožňuje uživateli daného privátního klíče s mincí pracovat. Celá práce se dá popsat v následujících pěti krocích:

1. Majiteli mince svým privátním klíčem podepíše transakci a pošle ostatním uživatelům.
2. Ostatní uživatelé zkontrolují, zda majitel je majitelem dané mince a přidají tuto transakci do takzvaného bloku.
3. Počítače soupeří mezi sebou o zápisu celého bloku do blockchainu.
4. Počítač, který nejrychleji spočítá kontrolní výpočty nového bloku, obdrží za odměnu určitý počet nových mincí (každý počítač zadá vlastní adresy těchto nových mincí, ale jenom vítězovi mince se uznají jako nové platné mince). Tomuto procesu se říká těžení nových mincí.
5. Počítače začínají shromažďovat další nepotvrzené transakce.

Satoshi navrhl takový způsob, že se bloky zapisují každých deset minut (Satoshi 2008). Průběžně se odměna za vytěžení snižuje, což vede k tomu, že celkový počet mincí se zastaví kolem počtu dvacet jedna milionů. Protokol je navržený tak, aby pracoval až s osmi místy za desetinou čárkou. Takto je možné pracovat s jednou stomiliontinou. Této jednotce se říká také jeden Satoshi.

Klíčová součást je již dříve popisovaný blockchain, Satoshi navrhl blockchain tak, že ho lze používat k finančním transakcím, ale i k jakýmkoliv operacím mezi osobami, a proto není potřeba žádný prostředník. Takto lze evidovat informace o prodeji nebo nákupu nemovitostí a podobně.

Na rozdíl od klasického zlata a ozbrojenou ochranu se tvůrce spoléhá na neprolomitelné matematické funkce a nástroje.

Obrázek 2.: Bitcoin symbol

6.1.1 Vývoj hodnoty Bitcoin

Zkratka:	BTC
Home page:	https://bitcoin.org/en/
Vznik:	2008

V počátcích vývoje měny Bitcoin neměla měna žádnou hodnotu. Ta se postupně zvedala s počtem uživatelů a nárůstem transakcí. Ze začátku měl jeden Bitcoin hodnotu ani ne jedné desetiny amerického dolaru. Velký zlom nastal až v roce 2011, kde cena mince vyskočila až na hodnotu kolem třiceti dolarů za jeden Bitcoin. V následujících letech nastal pád měny, který se ustálil stejného roku na hodnotě necelých dvou dolarů za Bitcoin.

Rizika Bitcoinu začala být vidět více a více. Do toho všeho přišla „Hedvábná stezka“, anonymní a v očích státu ilegální server Silk Road, na kterém se prodávaly všechny myslitelné drogy a další kontroverzní zboží (Stroukal & Skalický 2018).

Začátek velkého růstu nastal začátkem roku 2013, kdy se hodnota jednoho Bitcoinu, rychle dostala na hodnotu přesahující dvě stě dolarů za jeden Bitcoin. Koncem roku 2013 přesahovala hodnota jednoho Bitcoinu jeden tisíc amerických dolarů.

Rokem 2014 nastal krach na burze s kryptoměnami, kdy největší existující burza MT. Gox (Clark 2013) zkrachovala po útoku hackerů, kteří ukradli většinu mincí na této burze. V roce 2017 nastal další velký zlom pro cenu Bitcoinu, kdy cena vyrostla z tisíce dolarů za Bitcoin až hodnotám blížícím se ke dvaceti tisícům dolarů, kterých těsně nedosáhla. Koncem roku 2017 ale cena klesla zpět pod deset tisíc dolarů za jeden Bitcoin. Vývoj pokračoval růstem až k hodnotě 20 000 dolarů v polovině roku 2018. V roce 2019 cena začala růst na 4 000, vystoupala přes 12 000 a končila pod 10 000 dolary, což jenom dokresluje nestálost kurzu Bitcoin.

Celkovou historie kurzu Bitcoin v USD je vidět na následujícím grafu (XE 2020).

Obrázek 3.: Bitcoin - vývoj ceny v USD

6.2 Litecoin

Zkratka:	LTC
Domovská stránka:	https://litecoin.org/
Vznik:	2011
Maximální počet mincí:	84 milionů

Litecoin vznikl v roce 2011 a jeho tvůrcem je Charles Lee. Je to měna, která byla založena na Bitcoinu, ale jeho výhodou jsou minimální náklady na transakci. Byl navržen na velké množství transakcí, ale s minimální cenou, která je velkou výhodou oproti Bitcoinu.

Obrázek 4.: Litecoin symbol

6.3 Monero

Zkratka:	XMR
Domovská stránka:	https://www.getmonero.org/
Vznik:	2014

Monero vzniklo v roce 2014 pod názvem BitMonero (složení slov Bit, jako bitcoinu a Monero = mince z jazyka Esperanto), po krátké době se rozhodlo a začalo se používat jenom jméno Monero. Je založen na CrytoNote protokolu nikoliv na Bitcoinu

Maximální počet mincí je neomezený. Těžící algoritmus: CryptoNight.

V roce 2017 byla přidaná funkce Ring Confidential Transactions, která má pomáhat zamaskování počtu převedených prostředků uživatelům, kteří se na daném převodu nepodílí.

Obrázek 5.: Monero symbol

6.4 Ethereum

Zkratka:	ETH
Domovská stránka:	https://ethereum.org/
Vznik:	2015

Konečný počet mincí není neomezený, ovšem je omezena jejich emitace na 18 000 000 ETH ročně. Používá systém Proof of Work.

Měna vznikla v roce 2015 a za jejím vznikem stojí společnost Vitalik Buterin a Gavin Wood. Je to decentralizovaná měna, která je založena na blockchainu. Po Bitcoinu je to druhá nejrozšířenější kryptoměna. Cena všech mincí Etherea, je odhadována na víc jak polovinu ceny mincí Bitcoinu. Ethereum je založené na chytrých kontraktech („smart contracts“). Koncept Ethereum spadá mezi novou generaci kryptoměny, je také nazýván jako „Bitcoin 2.0”.

Obrázek 6.: Ethereum symbol

6.5 Bitcoin Cash

Zkratka:	BCH
Domovská stránka:	https://www.bitcoincash.org/
Vznik:	2017
Maximální počet mincí:	21 milionů

Vznikla oddělením se od Bitcoinu z důvodů pomalého ověřování nových mincí a drahého provádění transakcí. Zvětšením bloků dosáhl Bitcoin cash zrychlení ověřování, až 8x více transakcí než původní Bitcoin. Dalším inovací bylo zavedení technologie Segerate Witness.

Rozdělení, které takto nastalo, se jmenuje fork. Po uskutečnění forku se všem uživatelům, kteří vlastnili Bitcoin, přičetlo stejné množství mincí Bitcoin cashe.

6.6 Ripple

Zkratka:	XRP
Domovská stránka:	https://ripple.com/
Vznik:	2012

Je decentralizovaná měna, ale oproti ostatním měnám se liší, jelikož je většina ve vlastnictví stejnojmenné firmy. Ripple mimo kryptoměnu, také zajišťuje protokol pro platební síť, který využívají firmy a banky pro převod peněz mezi pobočkami. Měna Ripple se netěží. Při vzniku bylo vytvořeno 100 miliard mincí, z toho 61% vlastní autoři. Nevýhodou je možnost regulace měny pro běžné uživatele. Oproti tomu vyhovuje síla měny bankám, které je používají.

Obrázek 7.: Ripple symbol

7 Výhody a nevýhody kryptoměn

7.1 Výhody

Jak již zde bylo zmíněno, kryptoměny jsou decentralizované, nejsou omezovány žádnými vládami a bankami na rozdíl od běžné měny. Nové mince vznikají díky aktivitě uživatelů v celosvětové síti. Nikdo nemůže řídit jejich inflaci nebo jejich počet, který je často předem stanovený.

Mince se nedají falšovat na rozdíl od klasické měny, a to díky výše zmíněné decentralizaci. Aby jeden uživatel mohl mince použít vícekrát, musel by vlastnit 51% celkové bitcoinové sítě a takto potvrdit falešnou transakci. Výhodou je rychlá transakce mezi uživateli, jelikož se výpočty provádí každých deset minut u Bitcoinu, u některých měn je doba mnohem kratší, jako například u měny Litecoin. Díky tomu transakce trvá krátkou dobu, ve srovnání s převodem mezi bankami, kde převod z jedné země do druhé trvá až několik dnů.

Cena za jednu transakci je také velice nízká ve srovnání s poplatky, které si účtují banky a firmy provozující platební karty. Banky si často účtují i další poplatky za různé související transakce (přístup k účtu, elektronické bankovnictví, výpisy, vedené účtu a podobně). Transakční náklady mohou být redukovány až na centy, naopak typicky poplatky za kreditní party jsou kolem 2 procent (Clark 2013).

Práce s kryptoměnou je anonymní, ale jsou vidět všechny transakce s mincí za celou její historií, kde je uvedeno, kdo komu jakou minci poslal. Anonymita je v tom, že nejsou veřejné informace o držitelích jednotlivých mincí. S mincí pracuje ten, kdo vlastní privátní klíč.

Na anonymitu nelze plně spoléhat, u Bitcoinu lze mluvit jako o pseudoanonymitě. Podle zákonů pro praní špinavých peněz a boji proti terorismu, musí banky všechny transakce (převod peněz a kryptoměny mezi sebou) ověřovat a podezřelé transakce hlásit.

Nemožnost kolapsu systému je zajištěna díky distribuované vlastnosti kryptoměny, kdy každý uživatel, ať už jenom těží, nebo má nainstalovaný software pro obchodování (elektronickou peněženku) má uložený obvykle celý blockchain. I jeden uživatel je takto schopný zajistit „přežití“ blockchainu a tím celé kryptoměny.

Dopady budou na celou řadu odvětví. Jeden z příkladů za všechny: Bill Gates prohlásil: „Někdo se zájmem o finance by mohl pomáhat s inovacemi v podobě například

digitálních měn, které snižují transakční náklady, a chudí si díky nim mohou půjčovat za pět procent ročně místo patnácti.“ (Stroukal & Skalický 2018).

7.2 Nevýhody

Kryptoměnám se říká elektronické peníze, a je k jejich používání potřebný internet, což může být nevýhodou v částech světa, kde ještě není zavedeno úplné pokrytí internetem. Tato nevýhoda se postupně ztrácí. Navíc v řadě odlehlých oblastech je alespoň mobilní pokrytí, které může být použito pro obchodování.

Další nevýhodou je možnost, že vám vaše mince někdo ukradne. Toto nebezpečí ale hrozí i u normálních měn. Velkou obezřetnost je nutné dát na zabezpečení elektronické peněženky. Je nutné ji mít dobře zaheslovanou a zamezit přístup neoprávněným osobám.

Cena kryptoměn se neustále mění z důvodu, že kryptoměny jsou stále velice mladé. Měnu neovlivňují žádné banky ani žádné státy, ale uživatelé, kteří s měnou obchoduji a těží. Čím je větší důvěra lidí v kryptoměnu (víc lidi jí chce koupit a obchodovat s ní), tím více uživatelů chce měnu těžit nebo vlastnit. To ovlivňuje růst a pokles ceny, což bylo uvedeno na příklad kryptoměny Bitcoin. Tato kolísavost může být užitečná pro lidi, kteří spekulují o cenách, ale obyčejným uživatelům to spíše komplikuje používání.

Cena kryptoměn je tak určena poptávkou a nabídkou uživatelů. A její hodnota je kryta jenom důvěrou uživatelů v danou kryptoměnu.

8 Praktická část

Teoretická část obsahovala popis hlavních kryptoměn a jejich klíčových vlastností. V praktické části se budou nejprve analyzovat vybrané klíčové vlastnosti kryptoměn. Dále bude obsahovat návrh vlastní kryptoměny a implementaci. Z teoretické části jednoznačně vyplývá, že klíčem distribuované kryptoměny je blockchain, využití asymetrických klíčů a funkce hash.

Praktická část bude naprogramována jako webová aplikace, v prostředí PHP, která bude pokrývat tyto klíčové oblasti kryptoměny:

- Blockchain (model)
- Uživatelé
- Mince
- Podpis
- Transakce
- Peněženka

Pro další používání budeme tuto měnu nazývat Santacoin. Naprogramování měny Santacoin bude v prostředí PHP. Vývoj bude probíhat ve vývojovém prostředí NetBeans pod operačním systémem Windows 10.

8.1 Návrh kryptoměny Santacoin

Pro praktickou část budeme pracovat s řadou zjednodušení. Budou založeni pouze čtyři uživatelé manuálně (včetně jména a hesla) a pro uživatele nebude vytvářen žádný složitý systém přihlášení a ověření. Každému uživateli bude vygenerován soukromý a veřejný klíč. Pomocí tohoto minimálního počtu uživatelů, bude možné provádět základní operace a transakce, jako je zaregistrování nové mince a platební transakce mezi uživateli. Systém pracuje pouze s transakcemi jedné celé mince (nelze mince dále dělit). Není naprogramována decentralizovaná funkce (nekopírují se změny blockchain na jednotlivé počítače).

Nové mince se nebudou „těžit“ způsobem, jak to dělají ostatní kryptoměny, ale bude je možně ručně založit. Pro nové mince se bude pouze kontrolovat matematická hodnota mince.

8.2 Stručný popis práce s kryptoměnou

Základním stavebním prvkem kryptoměny je blockchain. Jeho detailní struktura je popsána dále. První blok nemá předchozí blok, proto je ke kontrole využita hodnota „NULA“ (ve světě Bitcoin nazývaný genesis). Všechny další postupy jsou jinak pro první blok totožné jako pro ostatní bloky.

Každá operace nejprve ověří správnost: jestli je odesílatel majitelem mince, jestli mince existuje, jestli existuje příjemce, jestli je datum aktuální a podobně. Poté se takto správná transakce zapíše na konce blockchain spolu s vypočtenou kontrolní hodnotou hash. Tato hodnota se počítá z nově zapisovaných dat celého předchozího bloku, čímž je zaručena neporušenost celého blockchainu.

Speciální operací je zápis nové mince, kdy příjemce je totožný s odesílatelem a tento datový blok je vlastně pouze zápisem nové mince a nového majitele jako informace pro všechny uživatele v síti.

Pro práci uživatelé používají program pomocí webového prohlížeče (webový klient), který může fungovat jak na počítači, tak případně i na mobilním telefonu.

8.3 Můj blockchain

Protože program je vytvořen v programovacím prostředí PHP, které nativně podporuje práci s XML strukturami, navržený blockchain využívá XML struktury. Tento formát hraje důležitou roli při výměně celé škály dat nejen na internetu (XML. 2020).

Root elementem je `<santacoin>`. Celý jeden blok představuje jednu transakci a je uložený v elementu `<block></block>`. Každý blok obsahuje vnořenou datovou strukturu uvnitř elementů `<Data></Data>` a `<Hash></Hash>`. Pro zjednodušení budeme pracovat s jedním elementem `<Data>` v bloku. Jeden blok musí obsahovat pouze jeden element `<Hash>`.

Pro hash funkci bude použita standardní hash MD5 knihovna (používaná například pro hash u souborů).

Příklad jednoduchého bloku:

```
<?xml version="1.0" encoding="UTF-8"?>
<santacoin>
<blok>
      <Data>
```

```
       <Mince>00001155</Mince>
       <Datum>17.03.2020</Datum>
       <Vlastnik>4</Vlastnik>
       <Prijemce>4</Prijemce>
       <Podpis>sRbHE2rGHu1nPZdqwGckzlDnQoOEh4qoj7Oml04F6RjkXZubsi8ElrhLBSo9kfi6D
Mum7aypvZoxCw29LfgZKw==</Podpis>
       </Data>
       <Hash>d41d8cd98f00b204e9800998ecf8427e</Hash>
</blok>
</santacoin>
```

V následující části jsou popsány všechny elementy.

8.3.1 Transakce <Data></Data>

Každá transakce je zapsána v datovém elementu `<Data></Data>`. Tento datový element obsahuje více vnořených elementů. Jednotlivé elementy jsou dále detailně popsány.

Element mince `<Mince></Mince>`, jak už z názvu vyplývá, obsahuje číslo mince. U Bitcoinu probíhá těžení tím, že se vypočítávají matematické funkce nového bloku každých deset minut a „vítěznému“ počítači je za odměnu připsán určitý počet nových mincí. Model Santacoin pouze definuje novou minci jako takovou, která vyhovuje matematickým podmínkám: nová mince je osmimístné číslo dělitelné 77 a současně končící na 5. Kontroluje se, zda daná mince již neexistuje. Příklad čísel, která vyhoví této kontrole, jsou například: 385, 1155, 2695. V elementu se číslo doplní na osmi znakový řetězec tím, že se z leva doplní nuly.

Element `<Datum></Datum>` obsahuje datum a čas transakce.

Element `<Vlastnik></Vlastnik>` obsahuje kód vlastníka (odesílatele) platby.

Element `<Prijemce></Prijemce>` obsahuje kód příjemce (nového vlastníka mince). Pokud je kód příjemce stejný jako kód vlastníka, jedná se o registraci nové mince.

8.3.2 Element <Podpis ></Podpis>

Tento element obsahuje elektronický podpis transakce, tj mince, datumu a času provedení transakce, vlastníka a příjemce. Podpis transakce je pomocí soukromého klíče.

Pro naprogramování asymetrického šifrování byla použita open source PHP knihovna phpseclib. Tato knihovna používá RSA (Rivest–Shamir–Adleman) mechanismus (první veřejně publikovaný šifrovací systém). Tato knihovna je dostupné dle licence open source GNU GPL.

Základní funkčností je generování soukromého a veřejného klíče s parametry formátu a délky klíče. Klíče lze rovnou chránit pomocí hesla. Část kódu pro generování klíčů je uvedena níže (Phpseclib 2020).

```
<?php
include('Crypt/RSA.php');

$rsa = new Crypt_RSA();

//$rsa->setPrivateKeyFormat(CRYPT_RSA_PRIVATE_FORMAT_PKCS1);
//$rsa->setPublicKeyFormat(CRYPT_RSA_PUBLIC_FORMAT_PKCS1);

//define('CRYPT_RSA_EXPONENT', 65537);
//define('CRYPT_RSA_SMALLEST_PRIME', 64); // makes it so multi-prime RSA is
used
extract($rsa->createKey()); // == $rsa->createKey(1024) where 1024 is the key
size
?>
```

Vygenerované klíče, privátní a veřejný, vypadají následovně.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUp
wmJG8wVQZKjeGcjDOL5UlsuusFncCzWBQ7RKNUSesmQRMSGkVb1/3j+skZ6UtW+5u09lHNsj6tQ5
1s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZwIDAQABAoGAFijko56+qGyN8M0RVyaRAXz++xTqHBLh
3tx4VgMtrQ+WEgCjhoTwo23KMBAuJGSYnRmoBZM3lMfTKevIkAidPExvYCdm5dYq3XToLkkLv5L2
pIIVOFMDG+KESnAFV7l2c+cnzRMW0+b6f8mR1CJzZuxVLL6Q02fvLi55/mbSYxECQQDeAw6fiIQX
GukBI4eMZZt4nscy2o12KyYner3VpoeE+Np2q+Z3pvAMd/aNzQ/W9WaI+NRfcxUJrmfPwIGm63il
AkEAxCL5HQb2bQr4ByorcMWm/hEP2MZzROV73yF41hPsRC9m66KrheO9HPTJuo3/9s5p+sqGxOlF
L0NDt4SkosjgGwJAFklyR1uZ/wPJjj611cdBcztlPdqoxssQGnh85BzCj/u3WqBpE2vjvyyvyI5k
X6zk7S0ljKtt2jny2+00VsBerQJBAJGC1Mg5Oydo5NwD6BiROrPxGo2bpTbu/fhrT8ebHkTz2epl
U9VQQSQzY1oZMVX8i1m5WUTLPz2yLJIBQVdXqhMCQBGoiuSoSjafUhV7i1cEGpb88h5NBYZzWXGZ
37sJ5QsW+sJyoNde3xH8vdXhzU7eT82D6X/scw9RZz+/6rCJ4p0=
-----END RSA PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0
FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjDOL5UlsuusFncCzWBQ7RKNUSesmQRMSGkVb1/
3j+skZ6UtW+5u09lHNsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZwIDAQAB
-----END PUBLIC KEY-----
```

Po vygenerování obou klíčů následují kroky na podpis pomocí soukromého klíče a ověření podpisu pomocí veřejného klíče.

```
<?php
include('Crypt/RSA.php');

$rsa = new Crypt_RSA();
//$rsa->setPassword('password');
$rsa->loadKey('...'); // private key

$plaintext = '...';

//$rsa->setSignatureMode(CRYPT_RSA_SIGNATURE_PSS);
$signature = $rsa->sign($plaintext);
```

```
$rsa->loadKey('...'); // public key
echo $rsa->verify($plaintext, $signature) ? 'verified' : 'unverified';
?>
```

Podpis je v binárním formátu. Pro jeho uložení v Blockchain ve formátu XML bylo nutné digitální podpis převést před uložení do formátu vhodného pro uložení do XML. Pro vlastní převod byly použity funkce base64_encode a base64_decode.

8.3.3 Element <Hash></Hash>

V tomto elementu je uložený hash předchozího bloku a datové části nového bloku. Zahrnutím předchozího bloku se řeší integrita celého blockchain. Protože pro první blok neexistuje ještě předchozí blok, je použita zástupná hodnota „NULA“.

8.4 Vlastní program

Úvodní obrazovka slouží pro přihlášení uživatele. Jak bylo uvedeno výše, uživatelé jsou uloženi manuálně v programu včetně jejich hesel. Pro zjednodušení nebylo naprogramováno prostředí pro správu uživatelů. Tato funkčnost by již vyžadovala využití nějaké základní databáze.

Obrázek 8.: Přihlášení uživatele

Po přihlášení má uživatel možnosti výběru ze základních operací, které se ovládají z jedné obrazovky. Základní operace jsou tyto:

- Vložení nové mince
- Transakce mezi uživateli
- Kontrola správnosti blockchainu
- Zobrazení peněženky

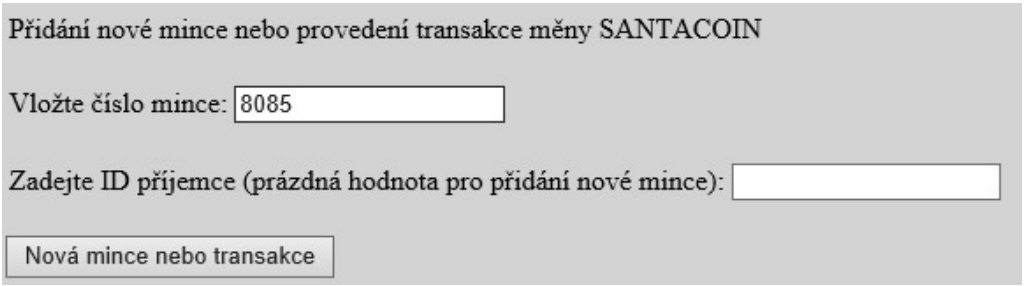
Po přihlášení se jméno uživatele a jeho ID zobrazí tučně v záhlaví. Uživatelské rozhraní je navrženo jako „minimalistické“. Nepracovalo se ani s barvami ani s jinými grafickými prostředky.

Obrázek 9.: Hlavní obrazovka

8.4.1 Přidání nové mince

Pro vložení mince potřebuje uživatel zjistit hodnotu (kód) nově přidávané mince. Hodnota mince musí být dělitelná sedmdesáti sedmi, zároveň musí končit číslicí pět a nesmí být delší jak osm znaků. Pro vzorový příklad si zvolíme minci číslo 8085.

Námi zvolené číslo mince končí číslem pět, je dělitelné sedmdesáti sedmi a je kratší než osm znaků.



Obrázek 10.: Nová mince

Políčko příjemce necháme prázdné, jelikož přidáváme novou minci.

Po aktivaci tlačítka pro „Nová mince nebo transakce“, se nám objeví oznámení o úspěšném zapsaní mince „Zápis nové mince proběhl.“

Když se podíváme do blockchainu vidíme, že se mince zapsala na konec blockchainu a hodnota mince se doplnila na délku osm znaků. Hodnota vlastníka a příjemce nám udává naše ID.

```
<blok>
	<Data>
	<Mince>00008085</Mince>
	<Datum>17.03.2020</Datum>
	<Vlastnik>4</Vlastnik>
	<Prijemce>4</Prijemce>
	<Podpis>NgmY55Z3SIca36FAb4lR3Cf7OglsKsx1Qzp7kS52XDZJZ7DfMpoZAL82p0WorNoc2BK+dVHkl
r8YIQymb5FxBQ==</Podpis>
	</Data>
	<Hash>50bd205073aa027bd4ee3598cb9f84f8</Hash>
</blok>
```

Při pokusu vložení špatné hodnoty, jako je například hodnota 7070, kdy je číslo dělitelné sedmdesáti sedmi, je kratší jak osm znaků, ale už nekončí číslicí 5, nás program upozorní hlášením: „Chybný kód mince.“, že zadáváme minci, která je neplatná. Po následném prozkoumání blockchainu uvidíme, že poslední zápis byl naší mince 8085. Obsah blockchainu zůstal nezměněný.

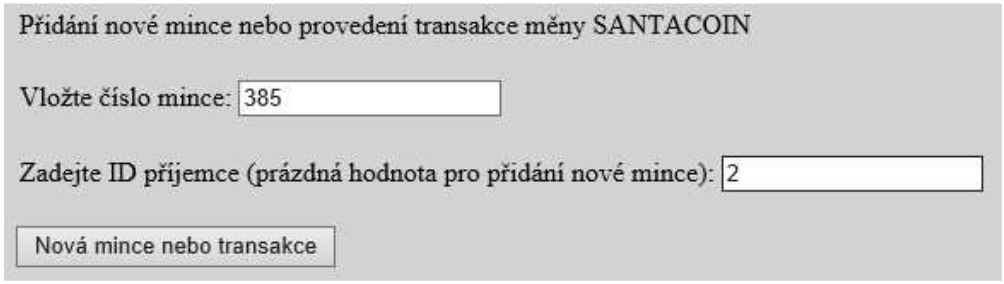
Program nejprve kontroluje, zda nová mince vyhoví matematické kontrole pomocí funkce `ChybnaMince ($Kod_Santacoin)`, dále ověříme, zda mince již neexistuje `MinceExistuje ($Kod_Santacoin)`. V posledním kroku pomocí funkce `VlastnikMince ($Kod_Santacoin)` ověřujeme vlastníka mince a zda je možné provést transakci.

8.4.2 Transakce mezi uživateli

Příklad úspěšné transakce mince hodnoty 385 mezi uživatelem čtyři a dva. Nejdříve se podíváme do blockchainu, že jsme vlastníky mince číslo 385.

```
<blok>
	<Data>
	<Mince>00000385</Mince>
	<Datum>17.03.2020</Datum>
	<Vlastnik>4</Vlastnik>
	<Prijemce>4</Prijemce>
	<Podpis>VqrvCo1uywN6S3PKWCSQMw6aepV7BGWtM00jXN+1kySO6G3CMhEj1H+xfnU4/HRGJah/G0RTS
/AzLKv1kpLonQ==</Podpis>
	</Data>
	<Hash>78b004724dc3151bcf9750128ee36db3</Hash>
</blok>
```

Po ověření, že jsme vlastníky mince 385, můžeme zadat programu požadavek na transakci námi zvolené mince.



Obrázek 11.: Provedení transakce

Po odeslání činnosti nám program nahlásí, že mince byla úspěšně převedena: „Převod mince se provedl.“.

Při kontrole blockchainu vidíme, že mince 385 byla z našeho vlastnictví převedena uživateli číslo dva.

```
<blok>
	<Data>
	<Mince>00000385</Mince>
	<Datum>17.03.2020</Datum>
	<Vlastnik>4</Vlastnik>
	<Prijemce>2</Prijemce>
	<Podpis>F+sSVvdyWmKuKvo3DtKwI9I9/rVgDYmcrNOe4IJTc+UfKb9dob2pHvbH2d5AadsFngjaegjxd
E1kSCakb7AAsg==</Podpis>
	</Data>
	<Hash>a242d8b06de308df286ddd335472186b</Hash>
</blok>
```

Nyní už danou minci nemůžeme poslat nikomu jinému. Pro názornou ukázku se pokusím stejnou minci (385) poslat uživateli číslo pět.

Po neúspěšné práci s mincí 385, kterou nevlastníme nám program zahlásí, že s danou mincí nemůžeme pracovat: Mince nelze přidat. Nejste vlastník mince. Vlastník je ID: 2.

8.4.3 Kontrola správnosti blockchainu

Ke kontrole neoprávněné změny se využívá funkce hash. Pokud byl v blockchainu změněný jakýkoliv i jeden znak, při opětovném výpočtů hash hodnoty daného bloku je vidět chyba.

Pro příklad bezchybného výstupu máme ukázku dobrého blockchainu:

```
<blok>
	<Data>
	<Mince>00001155</Mince>
	<Datum>17.03.2020</Datum>
```

```
        <Vlastnik>4</Vlastnik>
        <Prijemce>4</Prijemce>
        <Podpis>sRbHE2rGHu1nPZdqwGckzlDnQoOEh4qoj7Oml04F6RjkXZubsi8ElrhLBSo9kfi6DMum7aypv
ZoxCw29LfgZKw==</Podpis>
        </Data>
        <Hash>c195e70ff80d14f267a049bed61ac767</Hash>
</blok>
<blok>
        <Data>
        <Mince>00015015</Mince>
        <Datum>17.03.2020</Datum>
        <Vlastnik>4</Vlastnik>
        <Prijemce>4</Prijemce>
        <Podpis>oFHPa1SnbEvMV/FFDEjP5qaez6rhZ/g/RTq/NLFiVgD49Cwygh3bylL7Du172hMILdrZa0ZII
3TJ9sXUPpCreA==</Podpis>
        </Data>
        <Hash>72cd66654c7c87ec23571107447f0b8d</Hash>
</blok>
```

Program nezahlásí žádnou chybu a oznámí nám, že blockchain je v pořádku.

Obrázek 12.: Kontrola blockchain

Pro test použijeme výše uvedené dva vzorové bloky. V prvním změníme podpis a ve druhém bloku změním hodnotu <Prijemce> na sedm.

Při kontrole hash blockchainu v upraveném souboru je při kontrole nahlášena chyba počtu chybných bloků (1), počet chybných podpisů (1) a je vypsaný seznam chybných bloků (1, 2).

8.4.4 Peněženka

Funkce Peněženka nejprve vypíše pro kontrolu všechny transakce. Hlavní část obsahuje vlastněné mince, jejich výpis a jejich celkový počet. Příklad zobrazuje více provedených transakcí a pouze jednu transakcí, která vytvoří minci vlastníkovi ID 4. Ve „virtuální digitální“ peněžence je tedy pouze jedna mince.

Obrázek 13.: Peněženka

8.5 Kód programu

Celý program je napsán maximálně modulárně a hlavní části jsou naprogramovány jako funkce, které se podle potřeby volají.

8.5.1 Základní funkce

Program obsahuje několik základních funkcí, které budou následně popsány.

První funkce slouží pro zkontrolování hodnoty, zdali mince vyhoví navrženému zjednodušenému matematickému modelu: jestli je číslo dělitelné sedmdesáti sedmi a končí číslem pět (je dělitelné pěti, ale zároveň není dělitelné deseti). Poslední kontrola, které musí vyhovět, je délka čísla menší než osm znaků. Pokud kontrola proběhne v pořádku, funkce vrátí hodnotu jedna (mince je v pořádku). V opačném případě vrátí funkce hodnotu nula (mince není platná).

```
// Zjištění správnosti mince
function ChybnaMince($KOD_MINCE)
{
    $DELKA_MINCE=strlen($KOD_MINCE);
    //echo$Kod_Santacoin;

    if (($KOD_MINCE % 77)==0 && ($KOD_MINCE % 5)==0 && ($KOD_MINCE % 10)!=0 &&
$DELKA_MINCE < 9)
    {
        $CHYBA=False;
    }
    else
    {
        $CHYBA=True;
    }
    return $CHYBA;
}
```

Další uvedené funkce slouží pro zjištění, zda mince již existuje `MinceExistuje ($KOD_MINCE)` a kdo danou minci vlastní `VlastnikMince ($KOD_MINCE)` a tudíž jestli daný uživatel má právo danou minci někomu poslat.

```
// Zjišťujeme zda již mince existuje v blockchain
function MinceExistuje ($KOD_MINCE)
{
    $xml = simplexml_load_file("test.xml");

    $MinceExistuje = False;

    foreach($xml->children() as $BLOCK)
    {
         if ($BLOCK->Data->Mince==$KOD_MINCE)
         {
             $MinceExistuje = True;
         }
    }
    return $MinceExistuje;
}

// Kdo je vlastník mince, zda s ní lze manipulovat
function VlastnikMince($KOD_MINCE)
{
    $xml = simplexml_load_file("test.xml");
    //print_r ($xml);

    $MAJITEL="";

    foreach($xml->children() as $BLOCK)
    {
        if ($BLOCK->Data->Mince==$KOD_MINCE)
        {
             $MAJITEL=$BLOCK->Data->Prijemce;
        }
    }

    return $MAJITEL;
}
```

Poslední vzorová funkce zapisuje novou minci nebo novou transakci na konec blockchainu. Pomocí interní funkce `count ()` nejprve zjistíme kolik má soubor řádků, abychom zjistili, kam budeme zapisovat nové řádky (datový blok). V dalším kroku na konec souboru zapíše funkce nový datový blok: číslo mince, datum a čas transakce a jejího vlastníka (u převodu mince ještě i nového příjemce).

XML formát dat je vytvořený mimo tu funkci, zde se pouze zapisuje výsledná hodnota `$TEXT`.

```
function ZapisBlok($JM_SOUBORU,$TEXT)
{
    $pole_soubor=file ($JM_SOUBORU);
    $pocet_radku=count($pole_soubor);

    //Cte soubor do pole
    $content = file($JM_SOUBORU);
    foreach($content as $lineNumber => &$lineContent)
    {
        //Jede po poli a nacte si klic hodnota
        //kdyz je predposledni radek tak ho doplni o text
        //pocita od 0 a chceme predposledni proto -2 - necháme konec </santacoin>
        if($lineNumber == $pocet_radku-2)
        {
            // vlozeni na předposledni radek
            $lineContent .= $TEXT;
        }
    }
    // slozime pole dohromady
    $allContent = implode("", $content);
    // ulozime soubor se zmenama
    file_put_contents($JM_SOUBORU, $allContent);
}
```

Výše jsou uvedeny hlavní funkce programu pro práci s kryptoměnou Santacoin.

9 Závěr

V teoretické části byly pospány a vysvětleny základní funkce a principy kryptoměny. Byly uvedeny příklady nejznámějších kryptoměn Bitcoin, Monero, Litecoin, Ethereum a Ripple. Dále byly analyzovány nejdůležitější vlastnosti kryptoměn zejména blockchain, hash a asymetrická kryptografie.

V praktické části byla navržena a naprogramovaná vlastní kryptoměna Santacoin. Hlavní důraz byl dán na práci s blockchainem a na kontrolu neporušenosti blockchainu. Na několika příkladech ručně upravených blockchain vzorů bylo ověřeno, že i změna jednoho jakéhokoliv znaku transakce, je pomocí funkce hash odhalena a blockchain je označený jako neplatný. Naprogramováno bylo použití soukromého a veřejného klíče, podpisu transakce a ověření podpisu.

Program obsahuje funkci peněženky pro provádění a výpis transakcí a zobrazení obsahu peněženky (seznam vlastněných mincí).

Modelová kryptoměna byla naprogramována v jazyce PHP. Navržený blockchain je ve formátu XML. Model Santacoin by bylo možné do budoucna dále vyvíjet a na tomto modelu ověřovat další nové vlastnosti kryptoměn, například distribuované zpracování.

Funkce blockchain v současné době má stále více uplatnění i mimo oblast kryptoměn, a proto je blockchain s jeho vlastnostmi považován za základ rozvoje celé řady dalších činností a služeb (například transakce s nemovitostmi a podobně).

10 Seznam použitých zdrojů

1. Andreas MA. 2014. Mastering Bitcoin, O'Reilly Media 2014. ISBN-13: 978-1449374044
2. Bitcoin. 2009. Bitcoin Project 2009-2018 Released under the MIT licence. Available from https://bitcoin.org/en/ (accessed January 2020)
3. Bitcoincash. 2020. Available from https://www.bitcoincash.org/ (accessed January 2020)
4. Clark C. 2013. Bitcoin Internals: A Technical Guide to Bitcoin. Amazon.com Services LLC, Seattle, USA
5. Ethereum. 2020. Ethereum is a global, open-source platform for decentralized applications, Available from https://ethereum.org/ (accessed January 2020)
6. Filner K. 2017: Jak na bitcoin krok za krokem, Available from http://btctip.cz/jak-na-bitcoin-krokza-krokem-e-book-zdarma/ (accessed January 2020)
7. Kryptoměny. 2020. Available from https://cs.wikipedia.org/wiki/Kryptom%C4%9Bna (accessed January 2020)
8. Litecoin. 2020. Open source P2P digital currenc. Available from https://litecoin.org/ (accessed January 2020)
9. Monero. 2020. Montero secure, private, untraceable. Available from https://www.getmonero.org/ (accessed January 2020)
10. Peer-to-peer. 2020. Available from https://cs.wikipedia.org/wiki/Peer-to-peer (accessed January 2020)
11. PHP. 2020. PHP scripting language. Available from :https://www.php.net/ (accessed January 2020)
12. Phpseclib. 2020. Available from http://phpseclib.sourceforge.net/rsa/intro.html (accessed January 2020)

13. Ripple 2020. Available from https://ripple.com/ (accessed January 2020)
14. Satoshi N. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, Available from https://bitcoin.org/bitcoin.pdf (accessed January 2020)
15. Simplecoin.cz. 2013. Available from https://client.simplecoin.eu/cs (accessed January 2020)
16. Stroukal D, Skalický J. 2018. Bitcoin a jiné kryptopeníze budoucnosti, 2., rozšířené vydání. GRADA Publishing, a.s., Praha. ISBN 978-80-271-0818-3 (ePub)
17. XE The World's Trusted Currency Authority. 2020. Available from https://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y (accessed January 2020)
18. XML. 2020. Extensible Markup Language (XML) Available from https://www.w3.org/XML/ (accessed January 2020)

11 Přílohy

1. CD- program kryptoměny Santacoin