VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ELEKTRONICKÉ PENÍZE
ELECTRONIC MONEY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Daniel Gescheidt**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Václav Zeman, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Daniel Gescheidt ***ID:*** 167662
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Elektronické peníze

POKYNY PRO VYPRACOVÁNÍ:

Práce je zaměřena na rozbor a popis technik, které se využívají pro elektronickou verzi peněz. Prostudujte a stručně popište druhy elektronických peněz a infrastrukturu, kterou využívají, zaměřte se především na typy, které jsou postaveny na kryptografických technikách. Proveďte jejich výčet a srovnání z hlediska uživatele, bezpečnosti a použitých kryptografických prostředků. Na základě uvedeného rozboru navrhněte a realizujte aplikaci, která bude demonstrovat funkci vybraného typu elektronické měny.

DOPORUČENÁ LITERATURA:

[1] EUROPEAN COMMISSION. E-money - European Commission [online]. REV. 30.1.2014.

[2] SMEJKAL, L. Elektronické peníze. Ikaros [online]. 2001, ročník 5, číslo 10. urn:nbn:cz:ik-10800. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/10800

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

Abstrakt

V této bakalářské práci jsou popsány systémy elektronických peněz, které využívají kryptografické prostředky jako symetrické a asymetrické šifry, digitální podpis a hashovací funkci. Popis těchto technik je klíčový k pochopení, jak fungují systémy elektronických peněz. Dále jsou popsány tři systémy elektronických peněz v ČR.

Klíčová slova

Elektronické peníze, elektronický platební systém, hashovací funkce, digitální podpis, slepý podpis, kryptografie

Abstract

In this bachelor thesis are described electronic money systems, which uses cryptography techniques such as symmetric and asymmetric ciphers, digital sign and hash function. Describing those techniques is crucial for understanding how electronic money systems works. Then three electronic money systems from Czech republic are briefly described.

Keywords

Electronic money, electronic payment system, hash function, digital sign, blind sign, cryptography

Bibliografická citace:

GESCHEIDT, D. *Elektronické peníze.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2017. 52 s. Vedoucí bakalářské práce doc. Ing. Václav Zeman, Ph.D.

Prohlášení

Prohlašuji, že svou závěrečnou práci na téma Elektronické peníze jsem vypracoval samostatně pod vedením vedoucího práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne 8. června 2017 ……

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne 8. června 2017 ……

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

ÚVOD

Rychlý rozvoj internetu ve druhé polovině 20. století pochopitelně přinesl i značný posun v oblasti finančnictví. Snaha o real-time finanční transakce na internetu vedla ke vzniku elektronických peněz. Elektronické peníze můžeme chápat jako digitální ekvivalent peněz skutečných, avšak nejprve bude třeba si je právně definovat, aby nedocházelo k záměnám, např. s kryptoměnami. Dále je třeba odlišovat pojmy peníze a měna. Zatímco peníze jsou ve světě obecně používány jako platidlo, případně k vyjádření určité hodnoty nějakého produktu, měna je podmnožinou peněz a je definována řádem státu, který danou měnu používá [1].

V první části této práce jsou popsány některé základní kryptografické techniky, zejména se jedná o šifrování s tajným klíčem a veřejným klíčem, dále pak o hashovací funkci a digitální podpis.

Ve druhé kapitole jsou popsány elektronické platební systémy a jejich rozdělení na systémy s elektronickými penězi a bez elektronických peněz.

Třetí kapitola této práce se věnuje popisu elektronických peněz z právního hlediska. Následně jsou popsány systémy Ecash, Payword, MicroMint a Millicent, což jsou jedny z prvních platebních systémů, které využívají elektronické peníze a jsou založeny na kryptografických metodách. Poté jsou tyto systémy porovnány na základě zabezpečení a možností, které uživateli nabízejí. Dále jsou v této části popsány systémy elektronických peněz v ČR, mezi které patří GoPay, BLESK peněženky a FreePay. Tyto systémy jsou popsány včetně jejich zabezpečení a použité infrastruktury, která zahrnuje 3D Secure a protokoly SSL/TLS.

V další částí jsou popsány decentralizované platební systémy, též nazývané kryptoměny, mezi které patří Bitcoin nebo Litecoin. U těchto systémů hraje velmi výraznou roli tzv. blockchain, což je v podstatě databáze veškerých transakcí, které v systému proběhly.

V rámci praktické části je vytvořena webová aplikace, obsahující webové prezentace na problematiku elektronických peněz a kryptoměn.

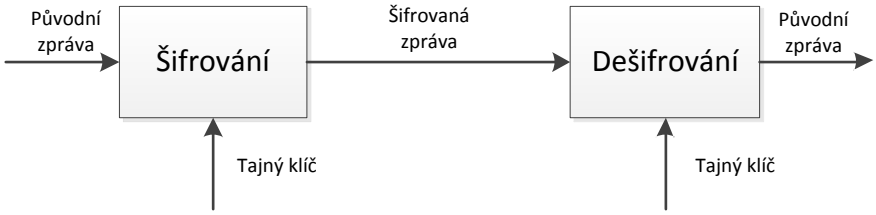
1 ZÁKLADNÍ POJMY V KRYPTOGRAFII

Kryptografie je věda zabývající se metodami utajování obsahu zpráv, které se nazývá šifrování. K šifrování obsahu zpráv se využívá buď tajného klíče nebo kombinace veřejného a soukromého klíče. Bez znalosti tajného klíče v případě symetrického šifrování a soukromého klíče u asymetrického šifrování není možné číst obsah zašifrované zprávy.

Tato kapitola se bude zabývat základními technikami kryptografie s tajným klíčem, s veřejným klíčem, hashovací funkcí a také digitálním podpisem.

1.1 Symetrické šifrování

Symetrické šifry využívají k šifrování a dešifrování stejný tajný klíč. Průběh šifrování je znázorněn na obrázku 1.1. Výhodou použití symetrického šifrování s tajným klíčem je nízká výpočetní náročnost, což značně zrychluje proces šifrování a dešifrování. Nevýhodou symetrického šifrování je skutečnost, že bezpečnost šifrování je závislá na utajení tohoto klíče. Nebezpečí představuje předání tajného klíče, kdy hrozí jeho získání neoprávněnou osobou.



Obr. 1.1: Průběh symetrického šifrování.

Tajný klíč také musí být navržen tak, aby odolal útoku hrubou silou (angl. brute-force attack), tedy vyzkoušení všech možných klíčů. Pokud označíme délku klíče jako n, pak existuje $2n$ možných klíčů. V roce 1999 se podařilo distributed.net a Electronic Frontier Foundatioun prolomit šifru DES, využívající klíč o délce 56 bitů, za 22 hodin a 15 minut [2]. Dnes se standardně používají šifry s klíči o délce 128 bitů a více, příkladem může být 3DES se 168 bitovým klíčem nebo AES s délkou klíče 128, 192 nebo 256 bitů.

Symetrické šifry se dělí na blokové symetrické šifry a proudové symetrické šifry. Zatímco blokové šifry realizují šifrování a dešifrování po blocích určité délky, proudové šifry šifrují a dešifrují po jednotlivých symbolech.

1.1.1 Blokové šifry

Jednou z nejznámějších blokových šifer je DES (Data Encryption Standard), který vyvinula společnost IBM. V podstatě se jedná o modifikovanou Feistelovu blokovou šifru, využívající bloky o velikosti 64 bitů a 56-bitový klíč. Tento klíč se zadává jako 64-bitový a vynechá se v něm každý 8. bit. Otevřený text o velikosti 64 bitů se rozdělí do dvou větví o velikosti 32 bitů. Šifruje se v 16 rundách, což je počet opakování stále stejných operací. Dešifrování zprávy zašifrovanou DES probíhá stejným způsobem jako šifrování, pouze se změní pořadí klíčů.

Výrazným posunem k lepšímu zabezpečení se stal algoritmus 3DES, který v sobě aplikuje původní DES třikrát, má tedy délku klíče 168 bitů. Přesto byla v roce 1997 vyhlášena veřejná soutěž na výběr symetrického šifrovacího algoritmu AES (Advanced Encryption Standard), který by byl bezpečnější než 3DES. Tímto algoritmem se poté stal Rijndael, který umožňuje šifrovat bloky o délce 128, 192 nebo 256 bitů a využívá klíč o délce 128, 192 nebo 256 bitů [3].

AES výhradně využívá bloky o délce 128 bitů, které jsou rozděleny do 16 bajtů, které tvoří matici 4 x 4. Klíč je ve formě matice bajtů se čtyřmi řádky, zatímco počet sloupců závisí na délce klíče. Klíč o velikosti 128 bitů má sloupce 4, 196-bitový klíč má 6 sloupců a 256-bitový klíč má 8 sloupců. Na velikosti klíče závisí i počet rund algoritmu, kde 128-bitový klíč má 10 rund, 192-bitový má 12 rund a 256-bitový má 14 rund.

Na rozdíl od DES algoritmus nedělí blok na dvě poloviny, ale v každé rundě aplikuje na celý blok 4 operace. První operací je substituce bytů podle vyhledávací tabulky, následuje permutace řádků o určitý počet kroků, kombinování sloupců a nakonec přidání podklíče, což je operace XOR bitů aktuálního bloku s rozšířeným klíčem. Přidání podklíče je jediná operace, která pracuje s klíčem [3].

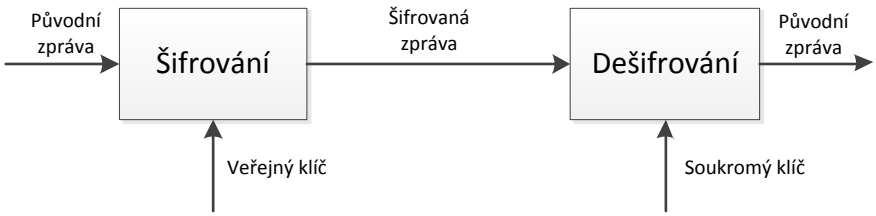
1.1.2 Proudové šifry

Příkladem proudové šifry může být algoritmus RC4, který šifruje zprávu po jednotlivých bajtech. Bajty jsou podrobeny operaci XOR s bajty vygenerovanými generátorem pseudonáhodné posloupnosti.

Šifru RC4 využívá například BitTorrent, standardy SSL/TLS (Secute Socket Layer/Transport Layer Security) sloužící pro zabezpečenou komunikaci na webových stránkách nebo u elektronické pošty. V neposlední řadě jej využívá protokol WPA (Wi-Fi Protected Access), který zabezpečuje bezdrátové sítě.

1.2 Asymetrické šifrování

Při asymetrickém šifrování se používají dva klíče (obr. 1.2), prvním je veřejný klíč, který mohou znát všichni uživatelé, a druhým je soukromý klíč, který zná pouze jeho vlastník. Právě použití dvou různých klíčů nás zbavuje nutnosti výměny tajných klíčů, jako tomu bylo u symetrického šifrování, kde byla tato výměna nejzranitelnějším místem celého systému.



Obr. 1.2: Průběh asymetrického šifrování.

Další značnou výhodou asymetrického šifrování je skutečnost, že jej lze použít jak k šifrování, tak k autentizaci. V případě šifrování se původní zpráva zašifruje pomocí veřejného klíče adresáta a tento šifrovaný text může dešifrovat pouze adresát, neboť je jediným vlastníkem soukromého klíče. Pokud by tedy chtěla Alice poslat šifrovanou zprávu Bobovi, pak by Alice zašifrovala původní zprávu M pomocí Bobova veřejného klíče *Public Key B*. Pak by tedy platil vztah

$$C = E\ (Public\ Key\ B, M) \tag{1.1}$$

kde C je zašifrovaná zpráva, E představuje proces šifrování původní zprávy M veřejným klíčem *Public Key B*.

Bob následně tuto zprávu dešifruje svým soukromým klíčem *Private Key B* a platí vztah

$$M = D\ (C, Private\ Key\ B) \tag{1.2}$$

kde D představuje proces dešifrování soukromým klíčem *Private Key B*.

Opačným způsobem probíhá autentizace, kdy odesílatel podepíše zprávu svým soukromým klíčem a zprávu pak může přečíst každý, kdo vlastní veřejný klíč odesílatele. Obě funkce je možné zkombinovat a to tak, že se nejprve odesílatel digitálně podepíše svým soukromým klíčem, zajistí se tedy autentizace. Poté se podepsaný text zašifruje veřejným klíčem příjemce, čímž se zpráva zabezpečí, protože si ji přečte pouze příjemce, který zná soukromý klíč.

1.2.1 Algoritmus Diffie-Hellman

Jedná se o algoritmus zabezpečující výměnu tajných klíčů u asymetrického šifrování na neutajeném kanále. Lze jej využít i v případě, že by spolu chtělo komunikovat více účastníků. Alice nejprve zvolí prvočíslo p a jeho primitivní kořen g a pošle obě hodnoty Bobovi. Poté Alice zvolí svůj soukromý klíč $a < p$ a spočítá svůj veřejný klíč pomocí vzorce

$$A = g^a\ mod\ p \tag{1.3}$$

Stejným způsobem spočítá Bob svůj veřejný klíč

$$B = g^b \bmod p \tag{1.4}$$

Alice nyní spočítá tajný klíč tak, že modulárně umocní Bobův veřejný klíč svým soukromým klíčem a stejně tak Bob umocní veřejný klíč Alice svým soukromým klíčem. Oba tak dospějí ke stejnému tajnému klíči, neboť platí

$$B^a \bmod p = (g^a)^b \bmod p = (g^b)^a \bmod p = A^b \bmod p \tag{1.5}$$

1.2.2 Algoritmus RSA

Jedná se o nejpoužívanější algoritmus v kryptografii s veřejným klíčem a na rozdíl od Diffie-Hellmanova algoritmu jej lze využít jak k výměně klíčů, tak i k šifrování zpráv nebo k digitálnímu podpisu.

Alice opět zvolí dvě různá čísla p a q a následně spočítá jejich součin. Zvolí číslo e, které je nesoudělitelné s $\varphi(\mathrm{n}) = (\mathrm{p}-1)\cdot(\mathrm{n}-1)$. Poté se vypočítá dešifrovací klíč ze vztahu

$$d = e^{-1} \bmod \varphi(\mathrm{n}) \tag{1.6}$$

Šifrování následně probíhá pomocí vzorce

$$C = M^e \bmod \mathrm{n} \tag{1.7}$$

a dešifruje se vzorcem

$$M = C^d \bmod \mathrm{n} \tag{1.8}$$

Výhodou algoritmu RSA jsou jednoduché výpočty hodnot e, n a d, a velká obtížnost výpočtu d při znalosti e a n [3].

1.3 Hashovací funkce

Jedná se o jednocestnou funkci, která ze zprávy M libovolné délky vytvoří hash (otisk) h konstantní délky. Hashovací funkce má dvě základní podmínky:

- Musí být jednocestná, tzn. že ze zprávy M je snadné vytvořit hash h, avšak z hashe h je obtížné spočítat zprávu M.
- Musí být odolná vůči kolizím, je tedy těžké najít dva stejné hashe pro dvě různé zprávy.

Hashovací funkce plní nejen funkci hashování, kdy h reprezentuje hash ze zprávy M a dochází k velké změně hodnoty h při malé změně zprávy M, ale také zprávu M značně zkomprimuje [3]. Touto kompresí je zajištěno, že nelze z hashovacího kódu získat zpět původní zprávu.

Mezi nejznámější hashovací funkce patří algoritmus MD5, který zprávu dělí do bloků po 512 bitech a jeho hashovací klíč má délku 128 bitů. Přestože tato šifra je již několik let prolomena, je dodnes používána.

1.4 Digitální podpis

Digitální podpis je autorizační nástroj, zaručující pravost dokumentu. Ta je zaručena soukromým klíčem odesílatele, jelikož je jediný vlastník svého soukromého klíče. Je tedy nesmírně důležité tento soukromý klíč uchovat v bezpečí, aby nedošlo k jeho zneužití.

Digitální podpis se vytváří tím způsobem, že se nejprve vytvoří hash z původní zprávy a tento hash se následně podepíše soukromým klíčem odesílatele. Příjemce z původní zprávy taktéž spočítá hash, zašifrovanou zprávu odesílatele dešifruje veřejným klíčem odesílatele a oba výsledky porovná. Pokud se výsledky shodují, pak tento podpis musí patřit odesílateli, neboť pouze on je vlastníkem soukromého klíče.

Další variantou vytváření digitálního podpisu je podepsání soukromým klíčem celé zprávy, nikoliv jejího hashe. Tento způsob je však velmi nevýhodný při větší délce zpráv, proto se využívá především prvního způsobu podpisu.

2 ELEKTRONICKÉ PLATEBNÍ SYSTÉMY

Elektronické platební systémy EPS mají za úkol zajistit převody peněz mezi jeho účastníky. Systém může zahrnovat až 5 subjektů:

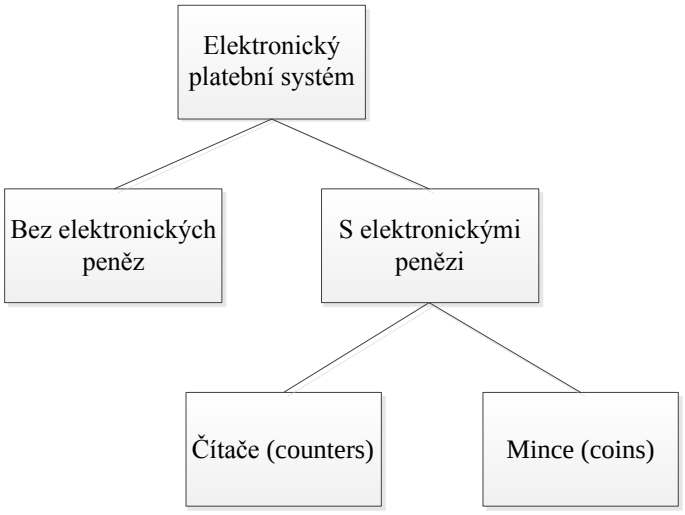
- Uživatel – nakupuje zboží u obchodníka za reálné nebo elektronické peníze. Jedná se o povinný subjekt v rámci EPS.
- Obchodník – prodává zboží uživateli. V případě platby elektronickými penězi si je nechá obchodník rozměnit u nabyvatele. Společně s uživatelem se jedná o jediný povinný subjekt v rámci platebního systému.
- Vydavatel – přijímá peníze od klienta a předává je dále obchodníkovi, případně nabyvateli.
- Nabyvatel – přijímá peníze od vydavatele a předává je obchodníkovi.
- Arbitrt – řeší případné spory vzniklé při převodu financí.

Zvláštním subjektem v elektronickém platebním systému je tzv. banka, která v sobě může zahrnovat funkce nepovinných subjektů v rámci platebního systému, tedy funkci vydavatele, nabyvatele i arbitra.

EPS se standardně dělí na EPS s elektronickými penězi a EPS bez elektronických peněz. V případě EPS bez elektronických peněz se jedná o analogii papírových platebních příkazů, spadá sem tedy např. home banking nebo internet banking. EPS s elektronickými penězi lze dále rozdělit na systémy s čítači (counters), kam spadá např. předplatní karta, nebo systémy s mincemi (coins), což jsou obecně EPS pro počítačové sítě s elektronickými mincemi, kam lze zařadit elektronické peněženky. Rozdělení elektronického platebního systému je uvedeno na obrázku 2.1.

2.1 Zabezpečení EPS

Klíčovou roli hraje u zabezpečení EPS digitální podpis, který má zajistit především autorizaci uživatelů. Vysoké požadavky jsou dále kladeny na důvěrnost, především pokud v transakci nějakým způsobem figuruje platební karta včetně použitého PIN kódu. Dále je nutné zajistit integritu transakce, aby nebylo možné ji nějakým způsobem modifikovat. EPS by měl také obsahovat prvky, které jsou schopny zajistit nepopiratelnost transakce, tedy že klient nemůže po provedení transakce označit kartu za zneužitou a získat tak peněžní prostředky nazpět, přestože již obdržel zboží.



Obr. 2.1: Rozdělení elektronického platebního systému.

2.1.1 SSL/TLS

Jedním z hlavních prvků zabezpečení EPS je protokol SSL, který vytvořila společnost Netscape. Protokol chrání uživatele před odposlechem a padělaním dat. Komunikace mezi klientem a uživatelem je duplexní a využívá asymetrických šifer k výměně tajných klíčů, které jsou následně použity při šifrování dat symetrickými šiframi.

Klient nejprve kontaktuje server a zašle mu požadavek na SSL spojení. Server mu jako odpověď zašle certifikát, obsahující jeho veřejný klíč. Tento certifikát mu vystavila certifikační autorita CA. Certifikát zajišťuje, že server je skutečně tím, za koho se vydává. Klient začne generovat nový šifrovací klíč, který zašifruje veřejným klíčem serveru. Server jej dešifruje svým soukromým klíčem a společně s klientem tak vytvoří nový tajný šifrovací klíč, pomocí kterého bude šifrována následující komunikace. Tento proces sestavování spojení a určování jeho parametrů se nazývá *handshake*.

K výměně klíčů používá především algoritmus Diffie-Hellman nebo RSA, k hashování se používá funkce MD5, dnes se využívá spíše SHA256. Pro tajný klíč se používá šifrování s tajným klíčem, např. algoritmus RC4, dnes však již častěji AES.

SSL, případně jeho nástupce TLS, pozná klient snadno na svém webovém prohlížeči pomocí webové adresy, která nyní začíná HTTPS (Hypertext Transfer Text Protocol). Oba protokoly fungují na stejné vrstvě mezi transportní a aplikační vrstvou modelu TCP/IP.

TLS (Transport Layer Security) je nástupcem SSL, ze kterého také vychází. V dnešní době je již bezpečnost SSL 3.0 značně zpochybňována a většina systémů tedy přechází na bezpečnější TLS [4].

2.1.2 3D Secure

3D Secure je protokolem společnosti VISA, který patří mezi nejdůležitější zabezpečovací protokoly při internetových platbách platebními kartami. O bezpečnost se zde stará vydavatelská banka karty, která je k transakci používána. V protokolu se rozlišují 3 domény:

- Doména BU – zahrnuje uživatele a banku uživatele.
- Doména BO – zahrnuje obchodníka a banku obchodníka.
- Doména bank – zahrnuje platební bránu, banku uživatele a banku obchodníka.

K zabezpčení komunikace mezi jednotlivými subjekty slouží právě výše zmíněné TLS. Každá z domén se stará o své kryptografické zabezpečení autonomně.

Uživatel si nejprve vybere a potvrdí zboží u obchodníka, poté je mu od serveru obchodníka zaslána zpráva s kódem 303, na základě které se prohlížeč uživatele připojí k platební bráně pomocí protokolu HTTPS. Následně si platební brána ověří údaje o transakci u obchodníka a zobrazí uživateli předvyplněný formulář, který zahrnuje údaje o transakci. Uživatel do formulář doplní povinné údaje, mezi které patří číslo platební karty, datum expirace platební karty a ověřovací kód CVV2.

Platební brána po vyplnění údajů klientem kontaktuje banku uživatele a pošle jí údaje o transakci. Poté je uživatel přesměrován na autentizační stránku svojí banky, kde se musí uživatel autentizovat, což se nejčastěji provádí pomocí jednorázového SMS hesla. Jakmile dojde k úspěšné autentizaci klienta, zašle banka uživatele zprávu platební bráně, že došlo k rezervaci patřičné finanční částky k dané transakci. Následně je klient přesměrován zpět na platební bránu, kde je informován o úspěšné platbě. Platební brána také informuje obchodníka, že byla transakce úspěšná. Nakonec dochází k mezibankovnímu vyrovnání, kdy je částka převedena z účtu klienta na účet obchodníka [5].

2.1.3 PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) je mezinárodní standard, který definuje, jakým způsobem se má nakládat s údaji uživatelů platebních karet. Tento standard je povinen používat každý obchodník, který umožňuje platbu platební kartou.

Cílem je minimalizovat riziko odcizení karetních dat, především pak čísla karet, jména klientů na nich uvedených, bezpečnostní kódy CVV2 nebo PIN. Právě poslední dva zmíněné kódy je možné zařadit mezi citlivá ověřovací data a tato data nesmí obchodník v žádném případě uchovávat [6].

Standard definuje 4 úrovně, do kterých jsou obchodníci zařazeni na základě množství provedených transakcí za rok. Každá z úrovní má stanovena kritéria

hodnocení, která musí obchodník splnit. Jednou za rok se provádí audit, který ověřuje, že obchodník splňuje daná kritéria. Standard dále zavádí 12 požadavků, rozdělených do 6 oblastí:

- Vybudování a údržba bezpečné sítě – instalace firewallů a jejich konfigurace za účelem ochrany dat držitelů karet. Nepoužívat sytémová nastavení a hesla od dodavatelů.
- Ochrana dat držitelů karet – neukládat data, pokud to není nezbytně nutné. Chránit data uživatelů a jejich přenos pomocí šifrování nebo maskování.
- Vedení programu kontroly zranitelnosti – aktualizovat používaný software a programy, vyvíjet bezpečné systémy.
- Zavedení důkladných opatření ke kontrole přístupu – udělit přístup k datům uživatelů jen v nezbytně nutných případech. Přidělit jedinečné ID každé osobě s přístupem k počítači. Omezit fyzický přístup k datům držitelů karet.
- Pravidelné monitorování a testování sítí – sledovat a monitorovat veškeré přístupy k síťovým zdrojům a datům držitelů karet. Pravidelné testování bezpečnosti systémů.
- Udržování pravidel pro bezpečnost informací – zavést a udržovat postupy, které zajišťují informovanost personálu o nakládání s citlivými daty [7].

2.1.4 SMS kód

SMS kód je autorizačním nástrojem, pomocí kterého si banka ověří oprávnění klienta pracovat s účtem, případně oprávnění k provádění transakcí. Autorizační kód je posílán ve formě SMS na klientův mobilní telefon a klient jej po přijetí musí vložit do příslušných kolonek v rámci určitého časového intervalu.

2.2 Elektronické platební prostředky

Pojem elektronické platební prostředky definuje zákon č. 124/2002 Sb. následovně:

- Prostředek vzdáleného přístupu k peněžní hodnotě, při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem.
- Elektronický peněžní prostředek [8].

Mezi prostředky vzdáleného přístupu k peněžní hodnotě patří především kreditní karty, které náleží k úvěrovým účtům. Placením těmito kartami dochází k čerpání kartového účtu a klient je následně povinen čerpanou částku do určité doby zaplatit buď jednorázově, případně na několik splátek. U tohoto typu úvěru jsou úrokové sazby výrazně vyšší než u klasického spotřebitelského úvěru.

Další variantou prostředku vzdáleného přístupu jsou pak karty debetní, které jsou spojeny s běžným, případně spotřebitelským účtem. V tomto případě klient čerpá své vlastní finance. Debetní karta může také v případě použití kontokorentu fungovat jako karta kreditní, kdy klient může z karty čerpat i v případě, že na účtu nemá žádné finance. Elektronickým peněžním prostředkem označujeme prostředek, který uchovává záznam o peněžní hodnotě. Patří mezi ně např. zákaznické karty v obchodech, předplatní karty do stravovacích zařízení nebo karty, které se používají jako forma jízdného u autobusových dopravců [9].

2.3 Elektronické peněženky

Jedná se o speciální formu platební karty, na kterou se ukládají elektronické peníze. Elektronickou peněženkou lze platit anonymně, neboť peněženka neobsahuje osobní údaje klienta. Většinou se využívá k placení malých částek a transakce probíhají off-line, nepotřebují tedy žádného prostředníka mezi klientem a obchodníkem, jako tomu je v případě online plateb, kde je nutný ještě nějaký autorizační server.

Vzhledem k tomu, že bezpečnost spočívá pouze v použití čipu na kartě, hrozí velké riziko zneužití této karty v případě jejího odcizení. Z tohoto důvodu je možné u mnoha obchodníků, umožňujících právě platbu elektronickou peněženkou, tuto kartu na místě jednorázově dobít a ihned použít nově nabité elektronické peníze. To přináší výrazně vyšší bezpečnost než kreditní a debetní karty, které umožňují přístup k celkovému objemu finančních prostředků na účtech, ke kterým jsou vázány. Navíc se limity pro platby na těchto účtech pohybují v řádech desetitisíců korun, zatímco elektronické peněženky bývají standardně nabity stovkami až tisíci korunami. Dále lze také na elektronické peněžence nastavit limit, od kterého je již vyžadována autorizace, např. formou SMS zprávy.

3 ELEKTRONICKÉ PENÍZE

Zákon č. 284/2009 Sb [10] definuje pojem elektronické peníze jako peněžní hodnotu, která:

- Představuje pohledávku za vydavatelem.
- Je uchovávaná na elektronickém peněžním prostředku.
- Je vydávaná proti přijetí peněžních prostředků v hodnotě ne nižší, než je hodnota vydávaných elektronických peněz.
- Je přijímána jako platební prostředek jinými osobami než jejich vydavatelem [10].

Ze zákona je tedy zřejmé, že mezi elektronické peníze nelze započítat např. předplatní karty u dopravců, protože jsou přijímány pouze vydavatelem těchto karet a tudíž nesplňují 4. bod zákona o elektronických penězích. Stejně tak se nejedná o elektronické peníze v případě předplatních karet ve stravovacích zařízeních, které také nesplňují poslední bod tohoto zákona.

O elektronické peníze se nejedná ani tehdy, mluvíme-li o kreditních nebo debetních kartách, které sice splňují body 1 a 4, ale jedná se o prostředky vzdáleného přístupu k peněžní hodnotě [9]

Oprávnění k vydávání elektronických peněz uděluje ČNB (Česká Národní Banka). Elektronické peníze mohou vydávat banky, spořitelní a úvěrová družstva, zahraniční banky nebo fyzická či právnická osoba, která získala dané oprávnění od ČNB. V neposlední řadě má právo vydávat elektronické peníze instituce elektronických peněz IEP. Ta musí mít sídlo v ČR, povolení od ČNB k vydávání elektronických peněz a nesmí poskytovat žádné úvěrové služby. U ČNB jsou k 9. 12. 2016 registrovány 3 instituce elektronických peněz, jedná se o GOPAY s.r.o., MOPET CZ a.s. a Prepaid Services Company Limited. Dále je zde registrováno 11 vydavatelů elektronických peněz malého rozsahu [4].

3.1 Transakce elektronických peněz

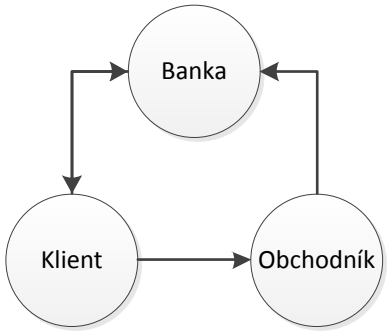
Existuje několik možností, jak lze provádět transakce elektronických peněz. První možností je nákup elektronických peněz. Elektronické peníze může uživatel od banky zakoupit např. převodem ze svého účtu. Po převodu dané částky pošle banka odpovídající množství elektronických peněz na uživatelovu elektronickou peněženku nebo účet.

Druhou možností je platba elektronickými penězi, kdy uživatel může elektronické peníze využívat u všech smluvních partnerů banky, od které elektronické peníze pochází.

Třetí variantou je vrácení elektronických peněz, kdy se uživatel může rozhodnout peníze vrátit. Uživatel tedy pošle do banky zbývající množství

elektronických peněz na jeho elektronické peněžence a banka mu na jeho bankovní účet pošle odpovídající množství reálných peněz.

Poslední variantou, jak lze zacházet s elektronickými penězi, je vrácení elektronických peněz obchodníkem. To funguje v podstatě stejným způsobem, jako vrácení elektronických peněz uživatelem. Banka obdrží od obchodníka elektronické peníze a následně mu vyplatí na jeho bankovní účet peníze reálné. Všechny tyto varianty zobrazuje obrázek 3.1, na kterém šipky představují toky elektronických peněz mezi jednotlivými subjekty.



Obr. 3.1: Transakce elektronických peněz.

Banka se klientovi před nákupem, případně před vrácením elektronických peněz, musí prokázat certifikátem, který vydává certifikační autorita *CA*. Podobně musí i klient potvrdit svoji identitu, což lze udělat zadáním svého jména a hesla, případně použitím jednorázového hesla zaslaného formou SMS na klientovo telefonní číslo.

Transakce elektronických peněz mohou probíhat buď online nebo off-line. V případě online výběru elektronických peněz klient nejprve kontaktuje banku, která danou částku digitálně podepíše a poté peníze pošle na účet. Klient těmito penězi může následně zaplatit obchodníkovi. Obchodník dané peníze pošle bance, která verifikuje digitální podpis a ověří, že peníze již nebyly čerpány. Nakonec banka vyplatí reálné peníze obchodníkovi [9].

Off-line transakce funguje velmi podobným způsobem, změna je pouze u kontroly digitálního podpisu, který kontroluje jak banka po přijetí peněz od obchodníka, tak především sám obchodník.

Některé mince elektronických peněz mají určitou velikost, vyjádřenou v bitech. Tato velikost se zvětšuje s každou další transakcí mezi klienty a počet transakcí je tedy touto bitovou velikostí omezen.

3.2 Vlastnosti elektronických peněz

V následující části budou popsány základní vlastnosti a služby, které mohou systémy elektronických peněz nabídnout, avšak ne všechny jsou u systémů zmíněných v této

práci dostupné. Na základě těchto vlastností bude na konci této kapitoly provedeno srovnání vybraných zahraničních systémů elektronických peněz.

3.2.1 Bezpečnost

Bezpečnost je zřejmě klíčovým aspektem platebních systémů a musí být ve všech systémech bezpodmínečně zajištěna, neboť by uživatelé zřejmě nevyužívali služeb systému, ve kterém přicházejí o své peníze. Systém musí být schopen zajistit, aby uživatelé mohli provádět transakce, které nebude schopen nikdo sabotovat, např. odposlechem komunikace mezi uživateli. Dále musí být zajištěno, že uživatel bude skutečně tím, za koho se vydává. Oba tyto požadavky zajišťuje kryptografie. Konkrétně se jedná o digitální podpis a certifikáty, které jsou na kryptografii založeny.

3.2.2 Anonymita

Anonymita je jedním z požadavků, které není nezbytně nutné v systému implementovat. V případě, že je však anonymita garantována, je v podstatě nemožné zjistit identitu jednotlivých uživatelů.

V souvislosti s anonymitou je nutné zmínit ještě jeden pojem a sice nevystopovatalenost (untraceability), tedy nemožnost zjistit, kam byly prováděny jednotlivé transakce mincí. Za tímto účelem se používá tzv. slepý podpis (blind signature). Autorita vydávající elektronické peníze (banka) podepíše jednotlivé mince náhodným oslepujícím faktorem (blinding factor) a pošle je uživateli, který je následně utratí u obchodníka. Jakmile obchodník zašle tyto peníze zpět bance, nebude banka schopna zjistit, komu tyto peníze vydala, neboť oslepující faktor je číslo náhodné a banka si neuchovává záznamy o těchto náhodných číslech. Slepý podpis bývá nejčastěji založen na algoritmu RSA.

3.2.3 Dvojí utrácení

Dvojí utrácení (double-spending) je nežádoucí situací, kdy uživatel použil danou minci více než jednou, případně několik uživatelů použilo tu samou minci. Existuje několik možností, jak dvojímu utrácení zabránit.

První možností je každou minci vyřadit ihned po provedení platby, avšak existuje zde určité riziko, kdy tou samou mincí zaplatí v jeden moment dva uživatelé. Jeden z nich je skutečným vlastníkem, zatímco druhý uživatel je útočníkem, který neoprávněně získal danou minci. V takových případech se může vyskytovat v systému další subjekt, tzv. arbirt. Arbitr má právo rozhodnout, čí mince bude přijata. Nevýhodou u této varianty je možnost, že arbitr může za skutečného vlastníka označit útočníka a skutečný vlastník tak může přijít o své peníze neprávem.

Druhou variantou zabránění dvojímu utrácení je vyloučení ze systému, jak je pospáno u systému MicroMint (viz kapitola 3.5). V tomto případě se jedná o

transakce tak malých částek, že případné dvojí utrácení není až tak velkou hrozbou a při jeho odhalení je uživatel jednoduše vyloučen ze systému.

Další variantou může být provázání jednotlivých mincí mezi sebou, kdy každá mince obsahuje specifické údaje, navazující na minci předchozí. V tomto případě je uživatel jen velmi obtížně schopen určit způsob, jakým jsou jednotlivé mince provázány. Podobným způsobem mohou být provázány celé transakce, kdy je každá transakce verifikována a stává se vstupem transakce následující, jako je tomu v případě Bitcoinu (viz kapitola 4.1).

Dvojí utrácení je zásadním problémem především u platebních systémů, které umožňují transakce vyšších částek.

3.2.4 Off-line transakce

Off-line transakce zaručují uživateli, že může kdykoliv provádět transakce elektronických peněz, aniž by musel být v momentě platby online. V případě takových transakcí je nutné, aby měl uživatel platební kartu, na které budou nabity elektronické peníze. Touto kartou může následně zaplatit u obchodníka, který si nechá elektronické peníze vždy po určitém intervalu proplatit od banky. Karta musí být nějakým způsobem zabezpečena proti dvojímu utrácení, neboť by jinak nebylo možné skloubit off-line transakce a anonymitu.

Dalším požadavkem v rámci off-line transakcí je tzv. přenositelnost (transferability), tedy aby si mohli peněžní prostředky přesouvat mezi sebou dva a více klientů, aniž by bylo nutné o tom informovat banku.

3.3 Ecash

Prvním elektronickým platebním systémem, využívajícím elektronické peníze, byl systém Ecash, který vytvořila společnost DigiCash pod vedením vědce Davida Chauma z USA. Chaum byl tvůrcem slepého podpisu a právě zde jej při implementaci systému použil v kombinaci s šifrováním s veřejným klíčem. Systém sestával z několika virtuálních bankomatů, ze kterých uživatel mohl vybírat peníze a stahovat si je do svého počítače. Tyto peníze následně mohl použít k internetovým platbám.

Uživatel si nejprve vytvoří účet v tzv. mincovně, která je součástí banky. Do mincovny následně posílá peníze ze svého bankovního účtu. Poté obdrží heslo, pomocí kterého si může stáhnout softwarového klienta. Následně je požádán, aby zadal náhodně nějaká písmena na klávesnici. Tato písmena jsou reprezentována sérií bitů, které jsou doplněny o redundantní bity.

Právě na velmi vysoké obtížnosti odhadu zadaných písmen uživatelem a jejich kombinaci s čísly generovanými pseudonáhodným generátorem je podstatná část zabezpečení systému založena. Nakonec uživatel po zadání těchto písmen obdrží řetězec čísel, dlouhý více než 100 číslic, který si musí nějakým způsobem poznačit. Právě z těchto čísel budou následně vygenerována sériová čísla

jednotlivých mincí elektronických peněz a také tato čísla poslouží pro případnou obnovu Ecash mincí, pokud by došlo nějakým způsobem k rozbití jeho HDD nebo PC.

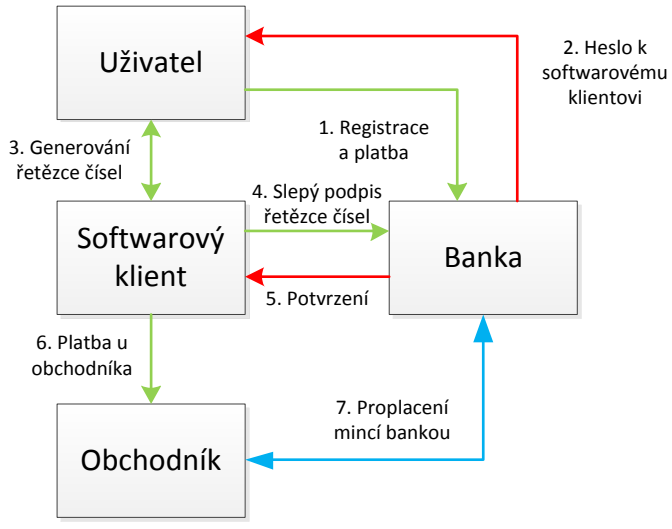
Nyní přichází na řadu zmíněný slepý podpis, kdy uživatel náhodným oslepujícím faktorem podepíše svůj řetězec čísel a pošle do banky, která mu v podstatě svým klíčem vydá potvrzení, že se jedná o minci určité hodnoty. K tomuto účelu banka využívá klíče, kdy různým hodnotám mincí odpovídají různé klíče, např. pro mince o hodnotě 1 dolar je jiný klíč než pro mince o hodnotě 50 centů [12].

V tuto chvíli je mince na harddisku uživatele připravena k použití. Uživatel ji může použít k platbě u obchodníka, který následně pošle přijaté mince na kontrolu vydávající bance, a stejným způsobem probíhají transakce mezi klienty, kteří si vyměňují mince mezi sebou.

Banka si ponechává záznam o sériových číslech za účelem odhalování dvojího utrácení. Jakmile uživatel použije minci, resp. použije její sériové číslo, je mince vyřazena a již není možné ji znovu použít. Jak již bylo zmíněno výše, banka po vydání mincí nemá přehled o tom, kdo je zrovna vlastní a nemá žádnou možnost zjistit, kam tato mince putovala. Schéma platby v systému Ecash je zobrazen na obrázku 3.2.

V případě, že dojde ke ztrátě Ecash mince, např. již zmíněným poškozením HDD, má banka možnost obnovit tuto minci pomocí hashe sériového čísla, které uživatel poslal bance. Banka na základě tohoto čísla vytvoří novou minci.

Systém Ecash byl poprvé použit v říjnu 1995 v bance Mark Twain v St. Louis v USA a bylo možné jej využívat v restauracích, u prodejců automobilů nebo k nákupům v obchodech s hudbou. Uživatelům byl účtován poplatek až 3 USD za dobíjení účtu a až 5% při zpětné konverzi elektronických peněz na reálné peníze. Účtovány byly taktéž měsíční poplatky za vedení účtu.



Obr. 3.2: Schéma platby Ecash.

Systém byl dále implementován např. v bance Merita ve Finsku, které se stalo ideálním adeptem na první spuštění tohoto systému v Evropě, neboť zde byl

nejvyšší poměr uživatelů internetu k celkovému počtu obyvatel. Systém zde byl spuštěn v březnu 1996 a o dva měsíce později bylo oznámeno, že se po bok Finska postaví také Německo, kde Deutsche Bank začala chystat implementaci Ecash systému. Stalo se tak ke konci roku 1996. Přes prvotní úspěchy se systému nakonec nepodařilo zajistit potřebný počet uživatelů po celém světě a společnost DigiCash v roce 1998 zbankrotovala [12].

3.4 PayWord

Dalším významným platebním systémem pro mikroplatby byl PayWord, který založil Ronald Rivest a Adi Shamir, dva ze tří tvůrců asymetrické šifry RSA. Paradoxně za účelem vytvoření tohoto schématu se snažili o minimalizaci operací využívajících RSA a místo toho celé schéma založili na využití hashovacích funkcí.

Opět zde vystupuje uživatel a prodejce, navíc se zde objevuje tzv. makléř. Ten vydává uživateli certifikát, který mimo jiné obsahuje veřejný klíč uživatele, jeho identifikaci a IP adresu. Je tedy zřejmé, že se nejedná o anonymní systém. Certifikát se vydává zpravidla na jeden měsíc a makléř jej po vypršení obnovuje. Na základě tohoto certifikátu má obchodník jistotu, že klient u něj nakupující má v pořádku mince PayWord a že jsou u makléře vyměnitelné za reálné peníze. Obchodník potřebuje veřejný klíč makléře, aby mohl ověřit podpis makléře na certifikátu. akým způsobem získá obchodník veřejný klíč makléře je závislé na konkrétní implementaci systému, neboť způsob získání daného klíče není v původním standardu definován. Obchodník navíc musí požadovat od makléře seznam certifikátů, které byly zrušeny. Certifikáty se ruší v případě, že uživatel vyčerpal finanční částku, k jejímuž vygenerování byl daný certifikát určen.

PayWord je řetězec hashovacích hodnot a každá tato hashovací hodnota představuje např. jeden cent. Klient je autorizován právě výše uvedeným certifikátem k vygenerování PayWordů. Nejprvee se určí náhodné číslo w_0, které představuje kořen řetězce [13]. Toto číslo však samo o sobě nepředstavuje PayWord. V závislosti na požadované délce n (např. 10 centů, tedy $n = 10$) řetězce se provede daný počet hashů a každému hashi odpovídá jeden PayWord, tedy již zmíněný jeden cent. Funkci můžeme psát ve tvaru

$$w_i = h\,(w_{i+1}) \tag{3.1}$$

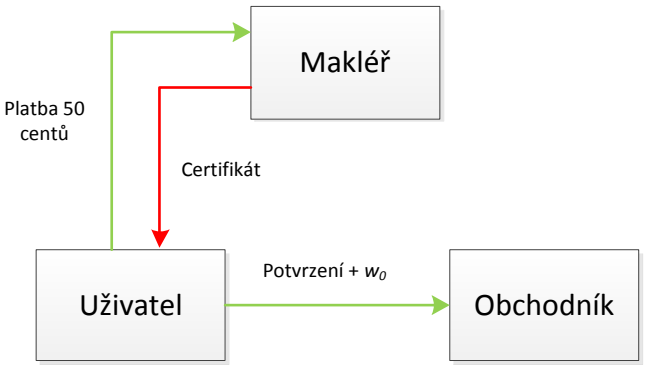
kde $i = n - 1, n - 2, \ldots, 0$.

Následně musí uživatel zaslat obchodníkovi potvrzení pro daný řetězec, které poté obchodník pošle i s PayWordem, kterým u něj uživatel platil, makléři zpět k vyplacení. Toto potvrzení je podepsáno uživatelem a autorizuje makléře k vyplacení reálných peněz za daný řetězec PayWordů. Obchodník posílá PayWordy vždy na konci dne zpět makléři, který mu za ně posílá odpovídající částku. V rámci zabezpečení proti dvojímu utrácení si obchodník ponechává PayWordy, kterými u něj bylo placeno, přestože je již makléř vyplatil [13].

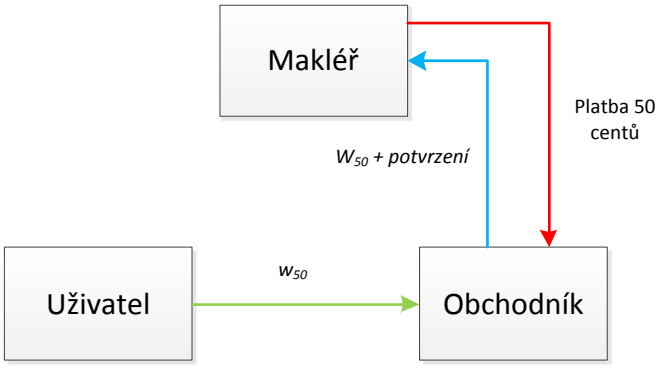
Na obrázku 3.3 je znázorněno, jakým způsobem získá uživatel od makléře certifikát, který jej opravňuje k vygenerování PayWordů. Jakmile uživatel narazí na zboží u obchodníka, u kterého doposud nenakupoval, pošle makléři určitou finanční částku, která musí být vyšší nebo rovna ceně daného zboží. V našem případě tedy pošle uživatel makléři 50 centů. Po přijetí peněz makléř zašle uživateli certifikát, který opravňuje uživatele k vygenerování PayWordů v hodnotě 50 centů. Uživatel o sobě dá vědět obchodníkovi tím, že mu zašle potvrzení svých PayWordu, podepsané jeho soukromým klíčem. Navíc mu uživatel zašle i kořen řetězce w_0, ze kterého budou PayWordy vypočítány pomocí hashovací funkce.

Nyní přichází na řadu samotná transkace PayWordů, jak je znázorněno na obrázku 3.4. Uživatel má u obchodníka vybráno zboží v hodnotě 50 centů, musí se tedy provést 50 hashovacích funkcí. Kořen řetězce w_0 je podroben hashovací funkci, čímž vzniká PayWord w_1. Stejným způsobem je hashován PayWord w_1, čímž vzniká PayWord w_2. Takto probíhá proces hashování až do té doby, než vznike PayWord w_{50} hashováním PayWordu w_{49}. V tuto chvíli posílá uživatel obchodníkovi PayWord w_{50}, který představuje zmíněných 50 centů. Tento PayWord nakonec pošle obchodník makléři, který mu jej proplatí za reálné peníze. Společně s tímto PayWordem posílá makléři potvrzení daného řetězce od uživatele, čímž je zaručeno, že uživatel je skutečně tím, za koho se vydává. Schéma provedení transakce je znázorněno na obrázku 3.5.

Z toho příkladu je zřejmé, že uživatel nemusí zasílat všechny PayWordy, nýbrž rozdíl jeho posledního použitého PayWordu a požadované částky. Tedy pokud by uživatel u obchodníka zaplatil v minulosti 10 PayWordů a v příští transakci se chystal zaplatit 3 PayWordy, pošle mu PayWord w_{13}, který v sobě zahrnuje i PayWordy w_{11} a w_{12}.



Obr. 3.3: Schéma získání certifikátu.



Obr. 3.4: Schéma provedení transakce.

3.5 MicroMint

MicroMint je elektronický platební systém, který poskytuje dostatečné zabezpečení transakcí malých částek elektronických peněz i přes velmi nízkou cenu. K zabezpečení transakcí nepoužívá žádné algoritmy z asymetrického šifrování.

Jednotlivé mince je poměrně jednoduché ověřit, avšak jejich vytváření je složitý proces a stará se o něj makléř. Makléř je prodává za reálné peníze uživatelům, kteří za ně nakupují u obchodníka a ten si je poté rozmění za reálné peníze u makléře. Makléř vytváří nové mince v pravidelných intervalech, nejčastěji na začátku každého měsíce a jejich platnost končí na konci měsíce. Pokud uživatel včas neutratí své mince, může je na konci měsíce vrátit zpět makléři. Mince jsou vytvářeny na začátku měsíce především z důvodu nízké efektivity a nákladnosti na jejich výrobu, kdy je daleko výhodnější vytvořit větší počet mincí naráz, než je vytvářet každý den po několika kusech.

Předpokládejme, že bude makléř očekávat profit zhruba 1 milion dolarů měsíčně, což je přibližně 2^{27} centů měsíčně. Za každý cent si bude makléř účtovat poplatek 10%, což znamená, že za každou minci zaplatí obchodníkovi 0,9 centů. Aby tedy dosáhl makléř profitu 1 milion dolarů, musí vyrobit měsíčně 1 miliardu mincí, tedy zhruba 2^{30} mincí měsíčně. Za předpokladu, že klient průměrně nakoupí 2000 mincí měsíčně, tedy potřebuje makléř 500 000 klientů [13].

Pro každou minci platí, že se jedná o k-cestnou kolizní hashovací funkcí. V našem případě je $k = 4$, jedná se tedy o čtyř-cestnou kolizní hashovací funkci. Mince se tedy skládá ze čtyřech vstupních hodnot

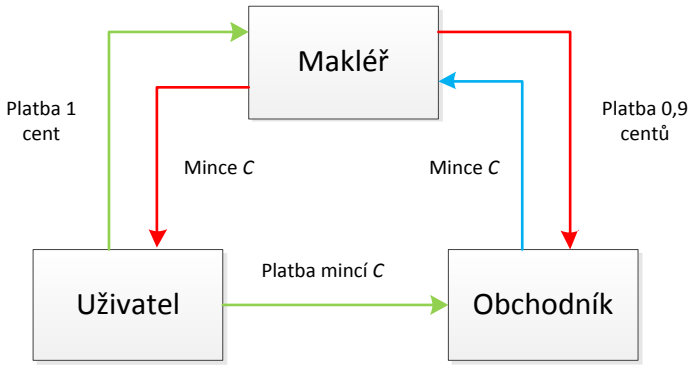
$$C = \{x_1, x_2, x_3, x_4\} \tag{3.2}$$

Vytváření mincí tedy spočívá v nalezení hodnot x_i, jejichž hash odpovídá hledané hodnotě y. Dochází ke generování řetězců, které jsou následně podrobeny hashovací funkci. Jakmile bude dosaženo k stejných výsledků y hashovací funkce, dojde k vytvoření mince. S každou vytvořenou mincí je tvorba dalších minci výrazně rychlejší.

Ke konci měsíce začne makléř vydávat mince pro nadcházející měsíc

a zveřejní nová kritéria pro posouzení pravosti mincí. Uživatel může mince použít k nabití své kreditní karty, kdy jsou mince na tuto kartu převedeny a zbývající mince mohou být na konci měsíce zpětně vyměněny u makléře za reálné peníze. Další možnosti je platba na internetu, kdy uživatel platí obchodníkovi dosud nepoužitými mincemi. Obchodník spočítá hash $h(x_i)$ a ověří tedy jejich pravost. Proces ověřování mincí obchodníkem je výrazně jednodušší a rychlejší než výroba nových mincí makléřem, neboť stačí spočítat tolik hashů, kolik bylo zvoleno k.

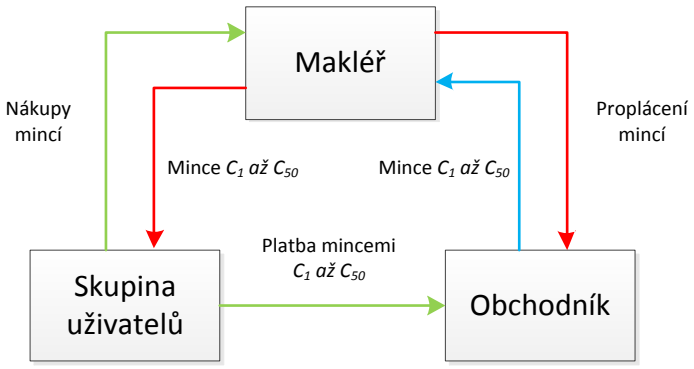
Na konci každého dne vrací obchodník makléři všechny získané mince a makléř mu následně za každou z nich zaplatí 0,9 centů. Makléř navíc musí provést kontrolu, zda již některou z přijatých mincí neobdržel dříve. V případě, že již minci stejné hodnoty má, může sám rozhodnout, kterou z mincí od obchodníka příjme, pokud obě mince obdrží ve stejný den. Pokud již danou minci obdržel dříve, novou minci od obchodníka nepřijme a nezaplatí tedy obchodníkovi 0,9 centů. Transakce je znázorněna na obrázku 3.6.



Obr. 3.5: Schéma platby MicroMint.

Dvojí utrácení může být detekováno makléřem, neboť MicroMint není anonymním platebním schématem. Makléř je tedy schopen poznat, od kterých obchodníků obdržel dvě totožné mince a taktéž je schopen zjistit, který uživatel u obchodníků platil. Pokud je u některého uživatele zjištěno časté dvojí utrácení, může být tento uživatel ze systému vyloučen. Vzhledem k velmi nízkým částkám v rámci transakcí je tak vyloučení ze systému jediným mechanismem zabraňujícím dvojímu utrácení [13].

Další možnosti zabezpečení proti podvodům je rozdělení uživatelů systému do určitých skupin, jak je zobrazeno na obrázku 3.7. Makléř může skupině uživatelů přiřadit konkrétní mince (např. C_1 až C_{50}) na základě požadovaného výstupu hashovací funkce. Jelikož klienti makléřuv požadavek na výstup hashovací funkce neznají, je nepravděpodobné, že by se jim podařilo vytvořit si vlastní mince, které by dané požadavky splnily.

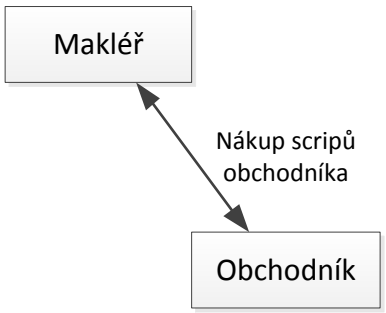


Obr. 3.6: Schéma platby MicroMint u skupiny uživatelů.

3.6 Millicent

Millicent je platební systém určený pro transakce velmi nízkých částek. Použitá měna se nazývá scrip, avšak scrip nepředstavuje jednotlivé mince, nýbrž určitý finanční obnos na účtu uživatele [14]. Scrip tedy pro jednoho uživatele může reprezentovat 50 centů a pro druhého uživatele 10 centů.

V tomto platebním schématu opět vystupuje makléř, který je zde prostředníkem mezi uživatelem a obchodníkem. Jelikož jsou scripy unikátní pro každého prodejce, nakupuje makléř scripy jednotlivých obchodníků a následně je prodává za makléřské scripy uživatelům, jak je zobrazeno na obr. 3.8. Výhodnější variantou je emise scripů na základě licence, kterou udělí obchodník makléři. Na základě této licence může makléř emitovat scripy a značně tak ulehčí práci obchodníkovi. Makléř je právnickou osobou, nejčastěji finanční institucí, která musí prokázat svou totožnost certifikátem. Makléřů se může v platebním schématu vyskytovat větší počet.

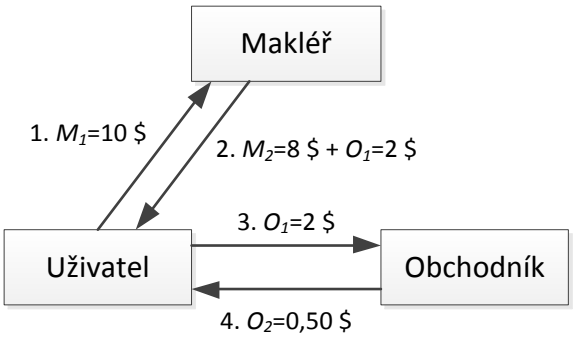


Obr. 3.7: Nákup scripů obchodníka makléřem.

Pokud uživatel nakupuje u obchodníka zboží v hodnotě 1,50 USD, musí makléři zaslat makléřův scrip M_1, v našem případě 10 USD, jak je znázorněno na obr. 3.9. Makléř odešle uživateli obchodníkův scrip O_1 ve výši 2 USD a z makléřova scripu M_1 odečte 2 USD, čímž vytvoří nový makléřův scrip M_2 pro uživatele. V tuto chvíli vlastní uživatel obchodníkův scrip O_1 ve výši 2 USD a makléřův scrip M_2 ve výši 8 USD. Následně zašle scrip O_1 obchodníkovi, ten z něj odečte 1,50 USD a vypočítá

nový scrip O_2, který zašle zpět uživateli. Tento scrip si nakonec může uživatel rozměnit u makléře [15].

Jak bylo zmíněno výše, scrip reprezentuje aktuální zůstatek na účtu uživatele. Jakmile dojde k platbě libovolné částky tímto scripem, je částka odečtena ze scripu a je vypočítán nový scrip. Scrip používá sériová čísla k rozlišení jednotlivých scripů a dále je zabezpečen proti zneužití digitálním podpisem.



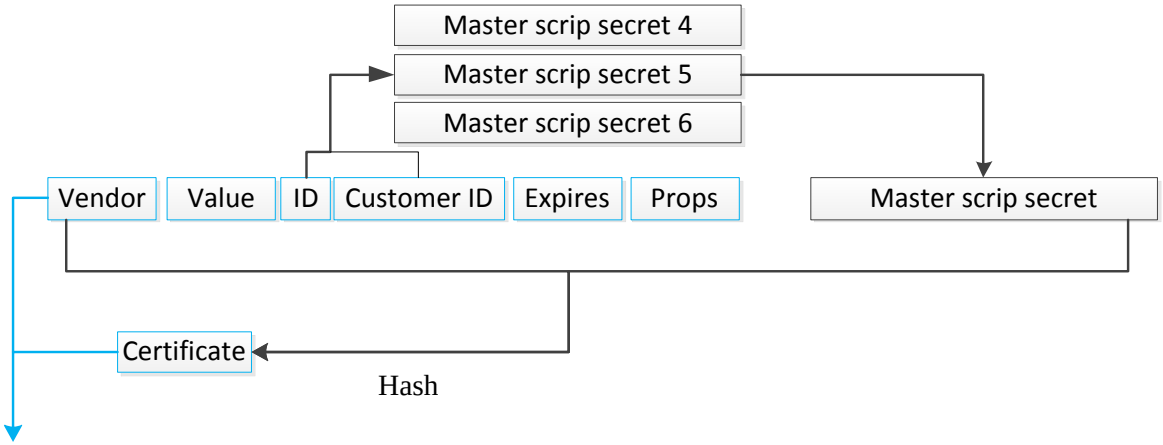
Obr. 3.8: Transakce scripů obchodníka a makléře.

Navíc scrip používá tři tajné informace při výrobě, ověřování a utrácení scripů. Jedná se o *customer secret*, kterým uživatel prokáže, že je skutečným vlastníkem scripu. Druhou tajnou informací je *master customer secret*, kterým si obchodník ověří uživatelův *customer secret*. Poslední tajnou informací je *master scrip secret*, který zabraňuje neoprávněné manipulaci a padělání scripů.

Struktura scripu (obr. 3.9) se skládá z několika položek:

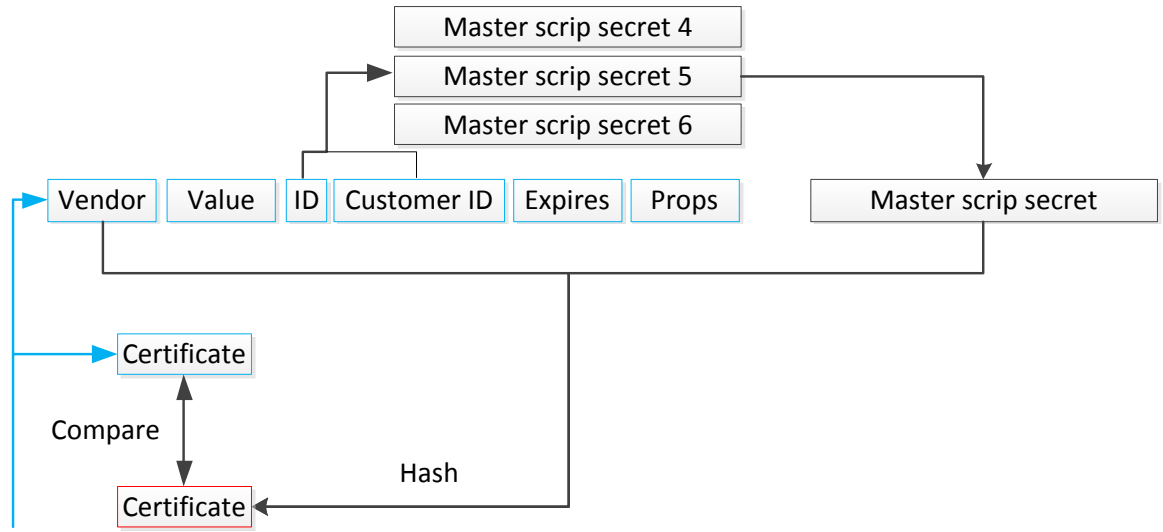
- *Vendor* – identifikuje konkrétního obchodníka, u kterého lze scrip použít.
- *Value* – určuje hodnotu scripu neboli zůstatek.
- *ID* – unikátní identifikátor scripu, jehož část se používá k výběru *master scrip secret*, který slouží ke tvorbě certifikátu.
- *Customer ID* – slouží ke generování *customer secret*, jeho část se používá k výběru *master scrip secret*.
- Expires – obsahuje datum a čas, kdy dojde k expiraci scripu.
- Props – obsahuje informace o uživateli jako bydliště, věk nebo jméno.
- Certificate – představuje digitální podpis scripu.

Ověření scripu ze strany obchodníka probíhá ve dvou krocích. Prvním je vypočítání certifikátu přijatých dat a jeho následné porovnání s přijatým certifikátem. Pokud by došlo při přenosu k nějaké manipulaci, certifikáty by se neshodovaly a transakce by byla zamítnuta.



Obr. 3.9: Struktura scripu [14].

Druhým krokem je ověření, zda již daný scrip nebyl čerpán, což lze provést snadno kontrolou ID scripu. Aby si nemusel obchodník uchovávat databázi veškerých ID scripů, které u něj byly utraceny, jsou scripy označeny datem expirace, po kterém je ID možné znovu použít. V tuto chvíli může obchodník ze své paměti vymazat dané ID. Proces ověření skripu obchodníkem je znázorněn na obrázku 3.10.



Obr. 3.10: Ověření skripu obchodníkem [14].

Zabezpečení transakcí v systému je velmi nízké, neboť se jedná o transakce tak nízkých částek, že by bylo pro případného útočníka nevýhodné nějakým způsobem napadnout systém. Pro útočníka by se systém mohl stát cílem pouze v případě, že by na účtech byly uchovávány tisíce dolarů.

Dvojímu utrácení je v systému zabráněno okamžitým vyřazením scripu po provedení transakce. Navíc je každý scrip opatřen unikátním seriovým číslem, což by samo o sobě zabránilo dvojímu utrácení, neboť daným scripem lze platit pouze

u jednoho konkrétního obchodníka, který by na základě sériového čísla snadno poznal, že daný scrip již obdržel.

Z hlediska důvěry je nejvýznamnějším subjektem v systému makléř a to hned z několika důvodů:

- Jedná se o větší finanční instituci, může být i nadnárodní.
- Obchodník i uživatel mohou snadno ověřit případné podvody ze strany makléře.
- Makléř si musí budovat co nejlepší reputaci, pokud bude chtít získat další uživatele.

Obchodník může zradit důvěru uživatele tím, že mu nevydá správné zboží, případně mu nevydá žádné zboží po provedení transakce. Proti této situaci může uživatel protestovat u makléře, který poté může v krajním případě vyloučit obchodníka ze systému. Nevýhodou v tomto případě je skutečnost, že uživatel si může stěžovat na služby obchodníka, přestože ze strany obchodníka k žádnému pochybění nemusí dojít. V těchto případech rozhoduje o případné refundaci makléř [14].

Hlavními výhodou scripu je jednoduchý mechanismus zabránění dvojímu utrácení pomocí ID, unikátnost každého scripu pro konkrétního prodejce a jistota, že jím bude platit pouze ten, kdo je skutečným vlastníkem scripu.

3.7 GoPay

Společnost GoPay je jedním ze tří držitelů oprávnění k činnosti instituce elektronických peněz se sídlem v ČR. Uživatel si zde založí elektronickou peněženku, na kterou si může zakoupit elektronické peníze v kurzu 1:1. GoPay nabízí 4 identifikační profily, na základě kterých si klient může zvolit jemu vyhovující vlastnosti účtu.

Základní identifikační úrovní je profil neověřený, kde stačí zadat pouze mobilní číslo a e-mailovou adresu. Vzhledem k tomu, že se jedná o základní profil, má pochopitelně z uživatelského hlediska nejvíce omezení. Jedním z nich je zůstatek na účtu maximálně do výše 1 000 euro a nemožnost platby na ověřené a neověřené bankovní účty. Na této úrovni je tedy možné platit pouze na e-mail, což je převod elektronických peněz na jiný GoPay účet nebo platit přímo u obchodníka.

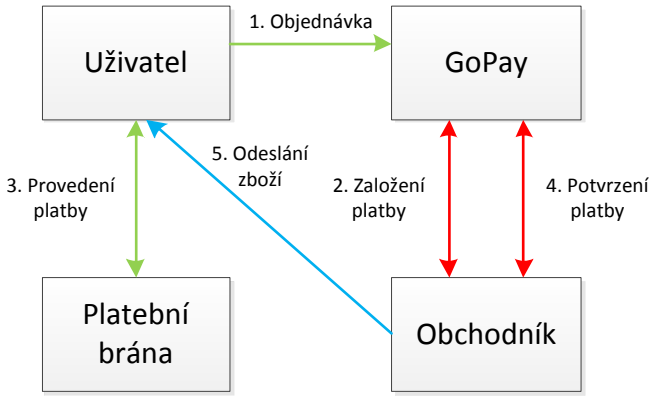
Druhou úroveň představuje částečně ověřený profil, který již dává klientovi možnost platby na ověřený bankovní účet, což je účet přímo napojený na GoPay účet klienta a již bylo provedeno jeho ověření identifikační platbou. Navíc má klient maximální zůstatek do výše 2 500 euro a možnost zpětné výměny do 1 000 euro. Tato úroveň navíc oproti základní vyžaduje ověření bankovního účtu.

Třetím profilem je profil ověřený, který již vyžaduje kopie bankovního výpisu a kopie občanského a řidičského průkazu. Tím získá klient možnost platit i na

neověřený bankovní účet a limity pro maximální zůstatek a maximální částku při zpětné výměně v hodnotě 10 000 eur.

Nejvýše postaveným profilem je pak profil plně ověřený, který nemá žádné finanční limity, je však potřeba provést osobní identifikaci. Za zmínku také stojí skutečnost, že pokud GoPay neudělá výjimku, není možné přejít z vyšší úrovně na nižší [16].

Uživatel si nejprve vybere zboží u obchodníka, čímž vytvoří objednávku, která je zaslána serveru GoPay. Ten následně provede založení platby společně s obchodníkem. Poté je uživatel přesměrován na platbení bránu. Jakmile je platba v platební bráně úspěšná, zašle server GoPay potvrzení o úspěšné platbě obchodníkovi. Nyní může obchodník zaslat zboží klientovi. Platební proces je znázorněn na obrázku 3.11.



Obr. 3.11: Schéma platebního procesu GoPay.

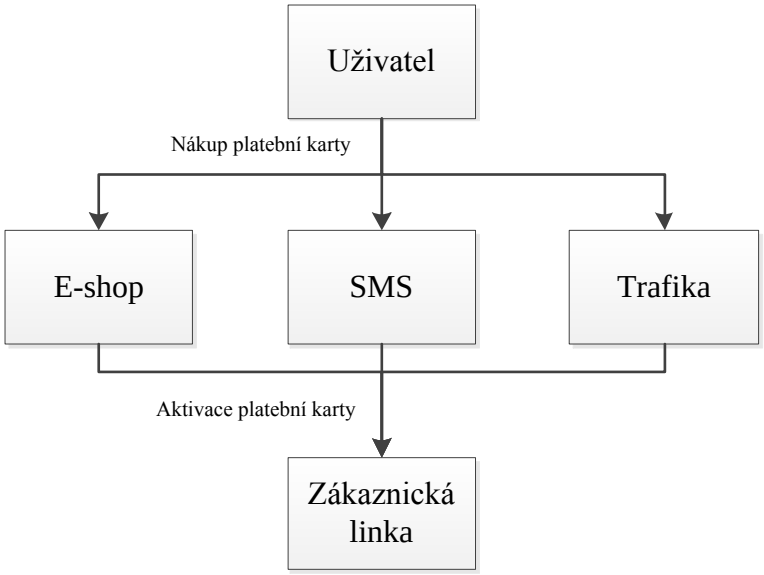
Komunikace probíhající přes platební bránu GoPay je šifrována pomocí TLS s klíčem o velikosti 128 bitů. Dále je systém certifikován dle mezinárodního standardu PCI DSS. Pro zabezpečení plateb kartou je také použit protokol 3D Secure [16].

3.8 BLESK peněženka

BLESK peněženka je předplacenou dobíjecí platební kartu, kterou provozuje společnost MOPET CZ a.s. a lze jí platit u všech obchodníků s logem MasterCard po celém světě. Kartu je možné pořídit v trafikách a novinových stáncích, na e-shopu, případně formou SMS, kdy je karta do 10 dnů doručena na požadovanou adresu. Možnosti zakoupení karty jsou zobrazeny na obrázku 3.12. Kartu je možné dobíjet prostřednictvím platební karty, převodem z bankovního účtu, na terminálech SAZKA nebo prostřednictvím bankomatu České spořitelny.

Zakoupení karty standardní BLESK peněženky stojí 125 Kč a její aktivace a vedení účtu s ní spjatého je zdarma. Dobíjení ze všech tří uvedených variant je

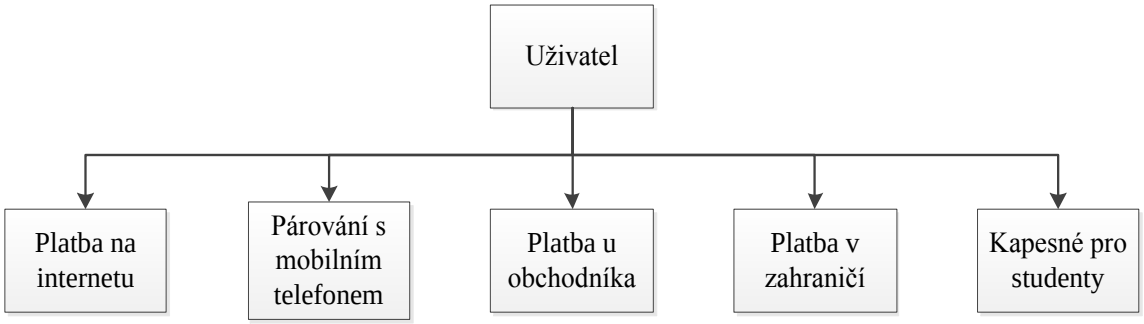
zpoplatněno 25 Kč. Další poplatky jsou účtovány za kontrolu zůstatků na peněžence v bankomatu (10 Kč) a prostřednictvím SMS zprávy (5 Kč). V případě výběru z bankomatu zaplatí klient 30 Kč a stejnou částku zaplatí za převod na bankovní účet.



Obr. 3.12: Možnosti zakoupení BLESK peněženky.

Platební kartu je možné použít jak při nákupu přes internet, tak při platbě u obchodníka v kamenné prodejně v ČR i v zahraničí. Navíc je možné ji spárovat s mobilním telefonem s operačními systémy iOS a Android. Výhodou karty je také možnost ji použít jako platební kartu na kapesné, kdy je možné ji vzdáleně dobíjet prostřednictvím samoobsluhy. Možnosti použití platební karty demonstruje obrázek 3.13.

Peněženku je možné rozdělit do tří úrovní. První je anonymní karta, což je základní stupeň. Limit pro denní dobití, maximální dobití, zůstatek a útratu činí 6 000 Kč za celou dobu platnosti peněženky. Prostřední stupeň představuje neověřená karta, která umožňuje měsíční dobití v hodnotě 6 000 Kč. Nejvyšším stupněm je ověřená karta s aktivací výběrů z bankomatů, která umožňuje denní dobití částkou 100 000 Kč, maximální zůstatek na kartě 350 000 Kč a denní platbu ve výši 100 000 Kč, navíc umožňuje výběry z bankomatů a platbu v cizí měně. [17].



Obr. 3.13: Možnosti platby s BLESK peneženkou.

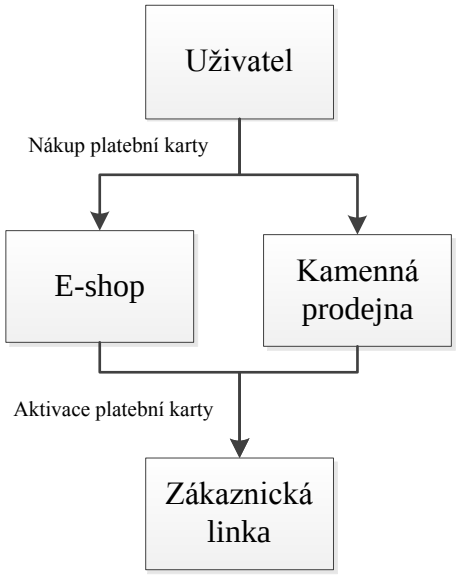
Peněženka je anonymní, neboť nenese žádné údaje o klientovi a na kartě není uvedeno ani jeho jméno. Pro zabezpečení plateb používá 3D Secure a při transakci je vyžadován PIN kód.

3.9 Freepay

Freepay předplacená platební karta je platební kartou vydávanou společností Prepaid Solutions a.s. Platební kartou lze platit v síti MasterCard po celém světě. Je možné ji pořídit v kamenné prodejně nebo přes eshop a následně ji aktivovat přes automatickou telefonní linku. Cena pořízení karty je 99 Kč.

Aktivace platební karty je zdarma, je však účtován poplatek za její vedení ve výši 69 Kč. Dále jsou účtovány poplatky 20 Kč + 1,5% za nabití karty, 35 Kč za výběr z bankomatu a výběr z bankomatu v zahraničí je zpoplatněn 120 Kč + 2%. Možnosti zakoupení platební karty a její následnou aktivaci zobrazuje obrázek 3.14.

Freepay nabízí dva režimy limitů, které lze měnit zdarma. Prvním z nich je základní režim, kdy lze na kartu nabít jednorázově maximálně 5 000 Kč. Druhým režimem je režim nejvyššího limitu, kdy je možné kartu nabít denně maximálně hodnotou 100 000 Kč. Limit pro roční obrat je 350 000 Kč, tato částka je také maximální hodnotou okamžitého zůstatku [18].



Obr. 3.14: Možnosti zakoupení a aktivace platební karty Freepay.

3.10 Srovnání elektronických platebních systémů

Srovnání zahraničních platebních systémů, uvedených v této práci, lze provést na základě požadavků a vlastností, které jsou uvedeny v kapitole 3.2. Jedná se zřejmě o nejvhodnější variantu srovnání, neboť jsou mezi jednotlivými systémy zásadní odlišnosti, ať už se jedná o jiné subjekty v rámci systému či zabezpečení systému. Další komplikací při srovnávání systémů je skutečnost, že pouze systém Ecash se stal komerčně úspěšným, zatímco se zbývající tři systémy nikterak zásadně neprosadily. Srovnání platebních systémů podle zmíněných vlastnostní a požadavků je zobrazeno v tabulce 3.1.

Tab. 3.1: Srovnání elektronických platebních systémů.

Požadavek	Ecash	PayWord	MicroMint	MilliCent
Zabezpečení	Složitý odhad zadaných kláves, slepý podpis	Hashovací funkce, asymetrické šifrování	Složité generování nových mincí hashovací funkcí	Jednodušší hashovací funkce, příliš nízké částky pro případný útok, spojení může být šifrované pomocí symetrického šifrování
Anonymita	Ano	Ne	Ne	Ne
Dvojí utrácení	Zabráněno vyřazením sériových čísel mincí	Zabráněno evidencí použitých PayWordů	Vyloučení ze systému při opakovaném použití již použitých mincí	Detekce pomocí ID, vyřazení použitých scripů
Off-line transakce	Umožňuje pouze online transakce	Umožňuje pouze online transakce	Umožňuje offline transakce pomocí kreditní karty	Umožňuje pouze online transakce

Jak již bylo zmíněno, nejdůležitějším požadavkem na elektronické platební systémy je bezpečnost, proto je vhodné nejprve porovnat systém z hlediska zabezpečení. Právě v zabezpečení je zřejmě největší rozdíl mezi systémy. Systém Ecash se spoléhá na složitost odhadu zadaných kláves uživatelem v kombinaci s čísly z pseudonáhodného generátoru. Zabezpečení u PayWordu je založeno na hashovací funkci a asymetrickém šifrování při vytváření potvrzení a certifikátu. MicroMint se spoléhá na složitosti generování nových mincí pomocí hashovacích funkcí, což by pro případného uživatele bylo značně obtížné. Navíc může makléř v tomto systému určit kritéria, podle kterých budou mince posuzovány, avšak útočník nemá v podstatě žádnou možnost tato kritéria zjisit. Poněkud jinou cestu zvolili autoči systému MilliCent, který je naopak zabezpečen velmi málo, neboť by pro případného útočníka byl útok velmi nákladný, avšak zisk minimální.

V rámci zabezpečení je nutné brát v potaz období, kdy byly systémy založeny a používány. Jedná se totiž od druhou polovinu 90. let a začátek 21. století, kdy měli počítače podstatně horší výpočetní možnosti, tudíž v době vzniku naprosto postačovaly šifry, které jsou v dnešní době již dávno prolomeny.

Z hlediska anonymity je srovnání velmi snadné, neboť jediný systém, který poskytoval anonymitu, byl systém Ecash. Zbývající systémy nějakým způsobem znaly identitu uživatelů, případně věděly, kam byly jednotlivé transakce prováděny.

Podobně snadné je i srovnání z hlediska dvojího utrácení, neboť systémy Ecash, Payword a MilliCent uchovávali určité údaje spojené s použitými mincemi, tudíž mohli snadno zabránit dvojímu utrácení. V případě systému MicroMint se zabraňovalo dvojímu utrácení prostým vyloučením uživatele ze systému.

Posledním kritériem srovnání je možnost provádění off-line transakcí u jednotlivých systémů. To umožňuje pouze systém MicroMint, ke kterému obdrží uživatel kreditní kartu, kterou může použít v kamenné prodejně.

4 KRYPTOMĚNY

Kryptoměny představují decentralizované elektronické platební systémy. Decentralizace systému zaručuje, že žádná centrální autorita nemůže manipulovat s hodnotou dané kryptoměny. Kryptoměny tedy nepodléhají nátlaku ze strany vlád nebo bank, tudíž nemůže dojít k jejich úmyslnému znehodnocení. Značnou nevýhodou kryptoměn je jejich částečná anonymita, která s sebou přináší možnost zneužití systému, např. pro praní špinavých peněz nebo podvody.

4.1 Bitcoin

Bitcoin je světově nejpopulárnější kryptoměnou. Bitcoin založila v roce 2009 osoba nebo skupina pod jménem Satoshi Nakamoto. Celkem by se do roku 2140 mělo vytvořit 21 milionů Bitcoinů, poté by se již žádné další mince vytvářet neměly. V současné době má jeden Bitcoin hodnotu více než 2 000 USD [19].
Transakce Bitcoinů probíhají pomocí distribuované databáze, tzv. blockchainu, který si uchovávají všechny uzly v P2P sítí.

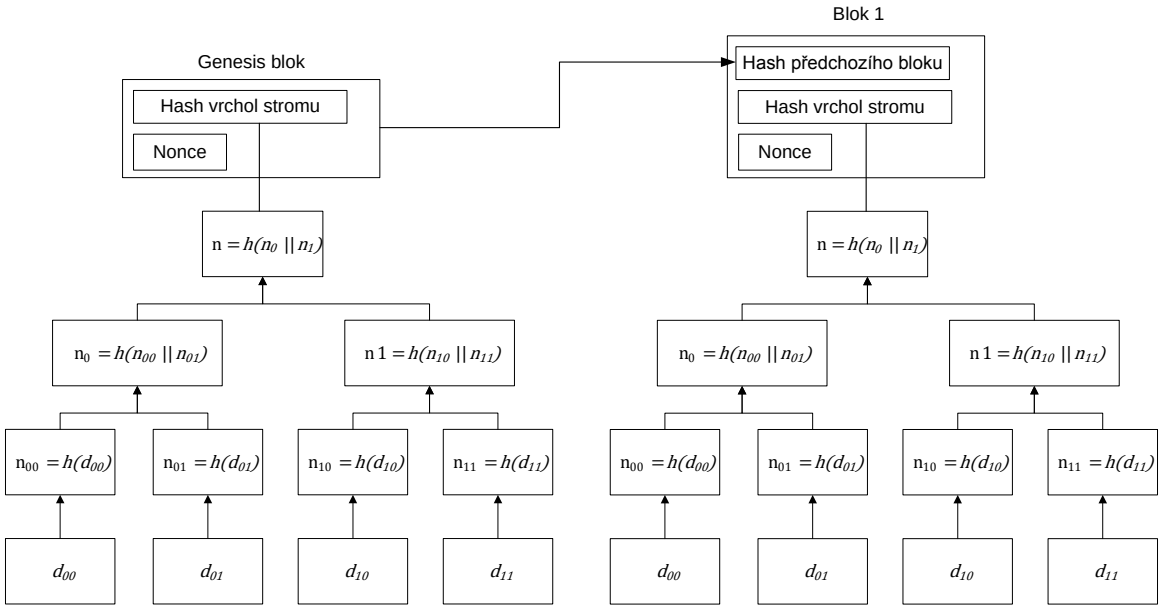
Obr. 4.1: Logo Bitcoinu [20].

4.1.1 Blockchain

Blockchain je databází veškerých provedených transakcí Bitcoinu. Tato databáze je postupně rozšiřována s každou provedenou transakcí v síti. Nový uživatel si po přihlášení do sítě tedy musí stáhnout kopii blockchainu. Blockchain je znázorněn na obrázku 4.2.

Výhodou je nemožnost jakkoliv zasahovat do blockchainu, neboť bloky jsou vzájemně provázané a malá změna u jednoho bloku by se tak ihned promítla i do všech následujících bloků. Z tohoto důvodu tedy není možné provádět změny u již zapsaných bloků blockchainu.

Nevýhodou blockchainu je skutečnost, že lze dohledat veškeré transakce a tedy vypátrat, kolik Bitcoinů mají jednotlivé účty. Z tohoto důvodu se tedy nedá hovořit o Bitcoinu jako o úplně anonymním platebním systému. Bitcoin tedy umožňuje zjistit, kolik se na daném účtu nachází Bitcoinů, avšak nelze zjistit skutečnou identitu vlastníka.



Obr. 4.2: Blockchain [21].

4.1.2 Transakce

Jak již bylo zmíněno, každá transakce Bitcoinu navazuje na transakce předchozí. Vlastník 1 tedy přijal určitou transakci a následně chce poslat určitý počet Bitcoinů na účet vlastníka 2. Vlastník 1 provede transakci požadovaného počtu Bitcoinů. Tato transakce obsahuje veřejný klíč příjemce, čímž je zaručeno, že příjemcem může být pouze vlastník soukromého klíče vlastníka 2, což je vlastník 2. Dále je transakce digitálně podepsána s využitím eliptických křivek ECDSA [22]. Průběh transakce je graficky znázorněn na obrázku 4.3.

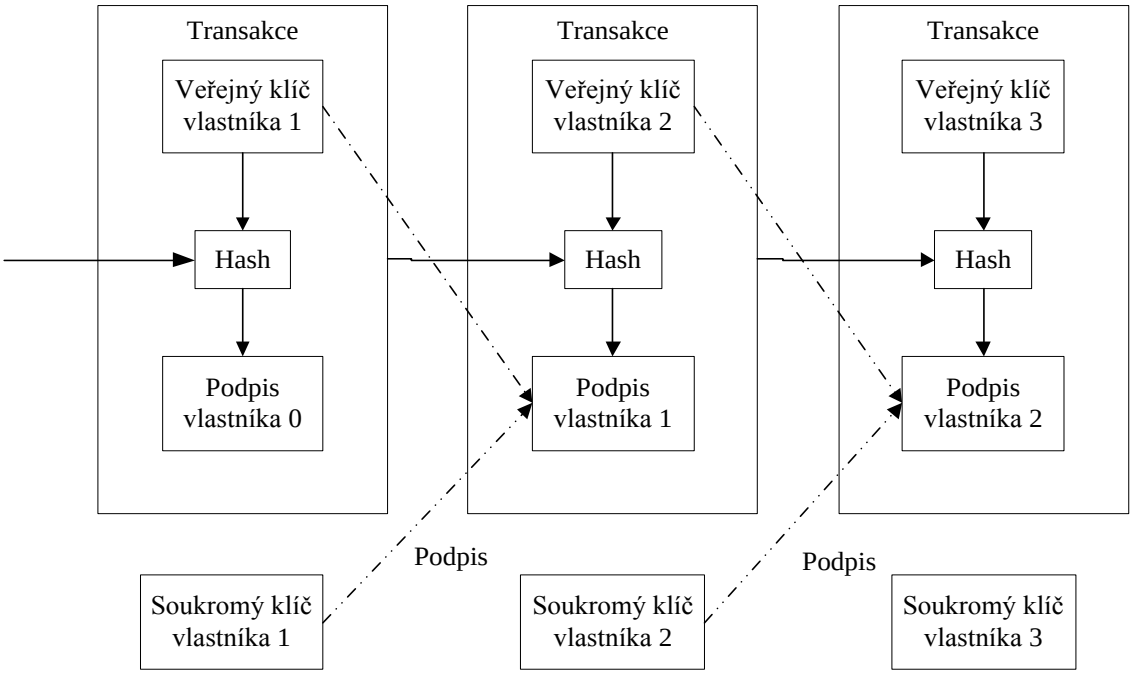
Každá transakce má několik vstupů a výstupu. Počet vstupů odpovídá počtu starších provedených transakcí a výstupu je libovolné množství. Transakce je možné provádět na 8 desetinných míst.

Vzhledem k neexistenci centrální autority je důležitým požadavkem u kryptoměn zabránění dvojímu utrácení. Toho je docíleno nutností vlastnit databázi veškerých provedených transakcí všemi uzly sítě. Dalším požadavkem je, aby získal nově příchozí uzel databázi z důvěryhodného zdroje. Tímto důvěryhodným zdrojem jsou těžaři, resp. skupiny těžařů, které na základě svého výpočetního výkonu rozhodují o validitě transakcí.

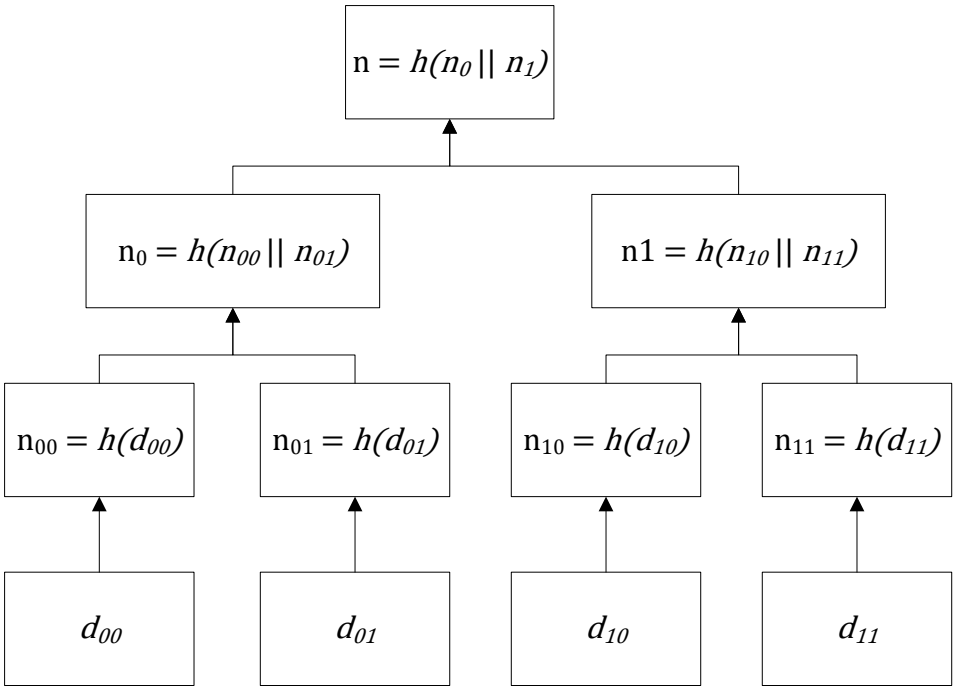
4.1.3 Merkle Tree

Merkle tree je strom hashů, které slouží k verifikaci integrity dat (obr. 4.4). Je pojmenován podle svého zakladetele Ralpha Merkla. Jednotlivé větve stromu představují hashe transakcí v daném bloku. Vzhledem k provádění hashovací funkce postupně od listů až po špičku stromu je nemožné provádět změny, neboť všechny vrsty stromu jsou provázány. Počet požadovaných hashovacích funkcí s každou

úrovní stromu narůsta logaritmicky.



Obr. 4.3: Transakce v síti Bitcoin [22].



Obr. 4.4: Merkle Tree [22].

4.1.4 Těžba

Těžbou se označuje proces vytváření nových bloků blockchainu. Těžbu provádí skupiny těžařů, kteří jsou za nově vytvořené bloky odměňování určitým počtem Bitcoinů. Výše této odměny je závislá na dodaném výkonu při těžbě (viz tab. 4.1)

navíc se s každým dalším vytvořeným blokem zmenšuje. Zároveň se neustále zvyšuje obtížnost výpočtů při vytváření nových bloků a ověřování transakcí. Odměnu za vytvoření bloku si skupiny těžařů rozdělují podle poskytnutého výkonu při těžbě.

Tab. 4.1: Rozdělení poolu podle výkonu k březnu 2017 [23].

Pool	Podíl výkonu
AntPool	21,1%
F2Pool	16,1%
BitFury	14,0%
BW.COM	9,4%
BTCC Pool	9,0%
ViaBTC	7,9%
Slush	7,2%
GBMiners	5,4%
BTC.com	5,1%
HaoBTC	4,7%

Každý blok odkazuje na předchozí blok a je tak možné se dostat až k prvotnímu bloku, tzv. genesis bloku. Hlavička každého bloku obsahuje informace o verzi, časové razítko, počet bitů, náhodné znaky Nonce, 256-bitový hash všech transakcí v bloku a 256-bitový hash hlavičky bloku předchozího. Právě hash hlavičky předchozího bloku je klíčový k validaci nově vytvořeného bloku. Tento hash musí být menší než je požadováno tzv. targetem. Právě hodnota targetu komplikuje těžařům generování nových Bitcoinů.

Náročnost generování nových Bitcoinů je definována vzorcem

$$D = \frac{T}{T_{min}} \tag{3.2}$$

kde D představuje náročnost výpočtu, T je současný target a T_{min} je nejnižší možný target.

Klíčovou podmínkou pro zachování decentralizace systému je, aby žádná skupina těžařů neměla více než 50% výkonu.

4.2 Litecoin

Litecoin je druhou nejznámější kryptoměnou na světě. Podobně jako v případě Bitcoinu je i Litecoin P2P sítí, která je plně decenetralizovaná. Litecoin byl založen v roce 2011 bývalým zaměstnancem Googlu Charlesem Leem. Stejně jako v případě Bitcoinu je možné provádět transakce na 8 desetinných míst, kdy jsou posílány mince nazvané Litoshi [21].

Značnou výhodou Litecoinu ve srovnání s Bitcoinem je jeho rychlost ověřování transakcí, které je zhruba 4krát rychlejší než v případě Bitcoinu. Tato skutečnost zároveň snižuje pravděpodobnost dvojího utrácení.

Naopak nevýhodou Litecoinu je vznik daleko většího množství neplatných bloků, které vznikly současným vytěžením dvěma těžaři. Další nevýhodou je použití algortimu Scrypt, který je podstatně náročnější na výpočet než SHA256 u Bitcoinu. Pro výpočet algoritmů Scrypt se tedy musí používat ASIC (Application-specific integrated circuit) čipy, které jsou výrazně dražší než čipy určené k výpočtům SHA256.

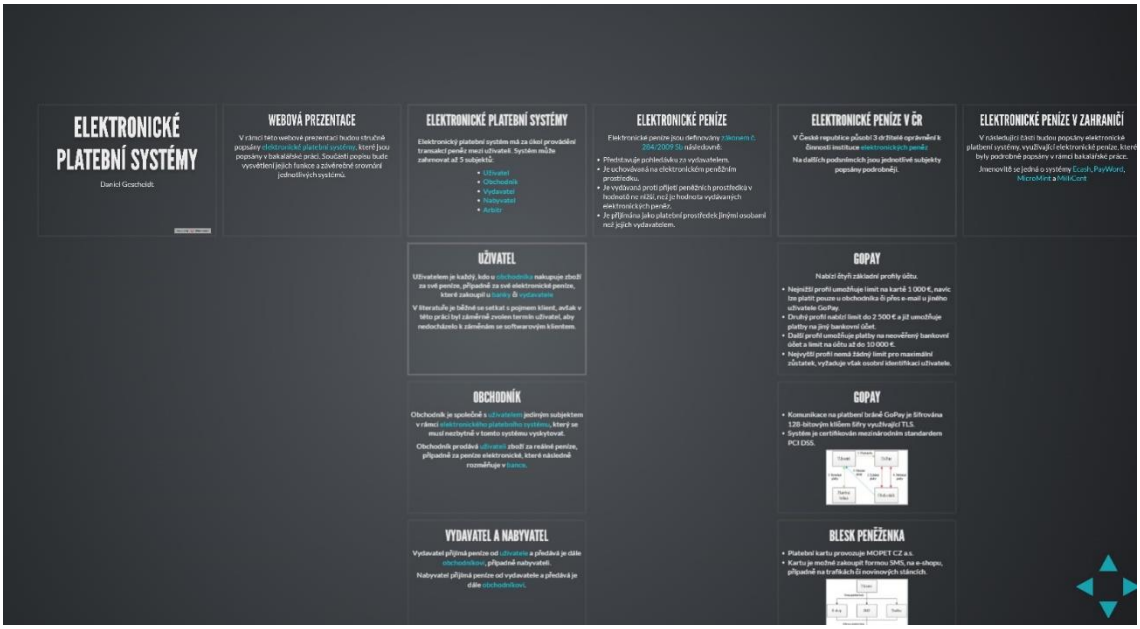
Obr. 4.3: Logo Litecoinu [24].

Celkem by mělo být vygenerováno na 84 milionů Litecoinů, není však specifikován rok, do kterého by měly být veškeré mince vytěženy. Současná hodnota jednoho Litecoinu je 29 USD [25].

5 WEBOVÁ APLIKACE

V rámci praktické části bakalářské práce byla vytvořena jednoduchá webová aplikace ve formě webových stránek na adrese http://www.elektronicke-penize.ml/. Jako doména byla zvolena doména .ml afrického státu Mali, neboť se jedná o doménu nejvyšší úrovně. Jako vhodný hosting se jeví použití 000webhost.com, který je stejně jako zvolená doména zdarma. Stránka obsahuje hlavní nabídku, ve které je možné po kliknutí na patřičnou záložku spustit webovou prezentaci na téma elektronické peníze nebo kryptoměny. Tyto webové prezentace slouží pro podporu výuky dané problematiky. Prezentace na téma elektronické peníze je uvedena na obrázku 5.1.

Při tvorbě webové stránky bylo použito HTML a CSS, webové prezentace jsou vytvořeny pomocí opensourcového frameworku Reveal.js. Ten umožňuje vytváření webových prezentací pomocí HTML a CSS. Reveal.js navíc umožňuje vkládání podsnímků ke každému snímku, což bylo s výhodou využitou při popisu jednotlivých platebních systémů a kryptoměn. Standardní snímky jsou umístěny horizontálně, podsnímky pak vertikálně.



Obr. 5.1: Webová prezentace.

5.1 Struktura webové stránky

Webové stránky obsahují čtyři záložky v hlavním menu. Najetí kurzorem na záložku je indikováno červeným písmem na dané záložce.

První záložkou je hlavní stránka, která je vytvořena souborem *index.html* a je na ní stručně popsáno, jakým způsobem lze ovládat obě webové prezentace.

Webová prezentace na téma elektronické peníze je spuštěna po kliknutí na záložku elektronické peníze, prezentace o kryptoměnách po kliknutí na záložku kryptoměny. V prezentacích je možné se pohybovat pomocí kurzorových šipek, případně pomocí mezerníku, který postupně zobrazuje jednotlivé snímky a podsnímky. Náhled na celou prezentaci je možné zobrazit stiskem klávesy Esc. Poslední záložkou v hlavní nabídce je záložka užitečné odkazy, kde jsou uvedeny odkazy na články a práce zaměřené na problematiku elektronických peněz a kryptoměn.

V pravém dolním rohu v prezentacích jsou znázorněny šipky (viz obr. 5.2), které znázorňují směr, kterým je možné se z aktuálního snímku dále vydat.

Obr. 5.2: Šipky znázorňující směr k dalším snímkům a podsnímkům.

5.2 Tvorba webových prezentací

Základem webových prezentací jsou HTML dokumenty *emoney.html* a *crypto.html*. Jednotlivé snímky jsou v souborech uzavřeny do tagů **<section>**, v případě podsnímků se jedná o vnoření tagů **<section>** do sebe. Jednotlivé tagy jsou označeny unikátním ID, pomocí kterého jsou dané snímky volány při kliknutí na klíčové slovo, které je v prezentaci označeno modře. Při kliknutí na klíčové slovo dochází k přesměrování na snímek, ve kterém je dané klíčové slovo podrobněji popsáno.

Všechny snímky s tagem **<section>** jsou zapouzdřeny v třídě <slides> a celá prezentace je zapozdřena ve třídě **<reveal>**. Vzhled prezentace lze upravovat pomocí šablony CSS. Na konci sekce **<body>** se nachází objekt reveal.initialize, kterým je možné upravit některé parametry, jedná se např. o aktivaci ovládacích prvků v pravém dolním rohu obrazovky, nastavení časového limitu pro jednotlivé snímky nebo povolení klávesových zkratek.

6 ZÁVĚR

Cílem této práce bylo popsat elektronické peníze založené na kryptografických metodách. Za tímto účelem byly popsány právě první elektronické platební systémy, neboť v počátcích těchto platebních systémů existovala velká variabilita právě použitých kryptografických metod. Platební systémy v dnešní době velmi často používají stejné prvky zabezpečení a infrastrukturu, jako je tomu např. u běžných platebních karet či intenetového bankovnictví. Jedná se především o protokol 3D secure, TLS nebo standard PCI DSS.

V rámci teoretické části byly nejprve popsány kryptografické metody, které se vyskytují u jednotlivých elektronických platebních systémů, případně kryptoměn. Dále byly popsány nejdůležitější pojmy z oblasti elektronických peněz, jak jsou definovány zákonem.

Následně byly popsány první elektronické platební systémy, které vznikly v polovině 90. let, avšak v dnešní době se již žádny z nich dále nepoužívá. Tyto systémy byly zvoleny jako vhodné k analýze v rámci této práce z důvodů zmíněné variability kryptografických technik a metod, které jednotlivé systémy používají. Zmíněné systémy byly stručně porovnány na základě jejich zabezpečení, schopnosti zajistit anonymitu uživatele, schopnosti zabránit dvojímu utrácení a možnosti umožnění off-line transakcí. Popsány byly také systémy elektronických peněz na území ČR, které však používají podobné kryptografické metody a infrastrukturu, tudíž byly stručně popsány z uživatelského hlediska.

Dále byla pozornost věnována kryptoměnám, které bývají často mylně zaměňovány za elektronické peníze, přestože nesplňují některé požadavky, které jsou na elektronické peníze kladeny. Především se jedná o skutečnost, že elektronické peníze může emitovat pouze instituce, která je k této činnosti oprávněna, což není případ decentralizovaných kryptoměn.

V rámci praktické části byla vytvořena webová aplikace ve formě webové stránky a webových prezentací, které jsou určeny pro podporu výuky v oblasti elektronických peněz a kryptoměn.

Literatura

[1] SMEJKAL, L. *Elektronické peníze*. Ikaros [online][cit. 2016-011-10]. 2001, ročník 5, číslo 10. urn:nbn:cz:ik-10800. ISSN 1212-5075. Dostupné z URL: http://ikaros.cz/node/10800/

[2] Record set in cracking 56-bit crypto. In: *Cnet* [online]. San Francisco: CBS Interactive [cit. 2017-06-07]. Dostupné z: https://www.cnet.com/news/record-set-in-cracking-56-bit-crypto/

[3] LEVICKÝ, Dušan. *Kryptografia v informačnej bezpečnosti*. Košice: Elfa, 2005. ISBN 80-8086-022-X.

[4] How does SSL work? What is an SSL handshake? In: Symantec Connect [online]. Symantec Corporation, ©2016 [cit. 2016-12-14]. Dostupné z: https://www.symantec.com/connect/blogs/how-does-ssl-work-what-ssl-handshake

[5] BURDA, K. - STRAŠIL, I.: Zabezpečovací systémy. Brno: Vysoké učení technické v Brně, 2012. s. 1-187. ISBN 78-80-214-4441-6

[6] Co je PCI DSS? Sdružení pro bankovní karty [online]. Praha: Sdružení pro bankovní karty, ©2009-2015 [cit. 2016-11-28]. Dostupné z: http://pcistandard.cz/index.php?cat=7

[7] ČERMÁK, Miroslav. PCI DSS: konkrétní bezpečnostní opatření. In: *Clever and smart* [online]. Miroslav Čermák, ©2008-2017 [cit. 2017-06-07]. Dostupné z: http://www.cleverandsmart.cz/pci-dss-konkretni-bezpecnostni-opatreni/

[8] ČESKO. Zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku). In: Zákony pro lidi.cz [online]. © AION CS 2010-2016 [cit. 14. 12. 2016]. Dostupné z: https://www.zakonyprolidi.cz/cs/2002-124

[9] ELEKTRONICKÉ PENÍZE V AKTUÁLNÍ PRÁVNÍ PRAXI [online]. Veveří 158/70, 611 80 Brno-střed [cit. 2016-12-12]. Dostupné z https://www.law.muni.cz/sborniky/dp08/files/pdf/financ/kyncl.pdf. Masarykova univerzita, Právnická fakulta.

[10] ČESKO. Zákon č. 284/2009 Sb., o platebním styku. In: Zákony pro lidi.cz [online]. © AION CS 2010-2016 [cit. 12. 12. 2016]. Dostupné z: https://www.zakonyprolidi.cz/cs/ 2009-284

[11] Instituce elektronických peněz a pobočky zahraničních institucí elektronických peněz (k 12.12.2016). In: Česká národní banka [online]. Na Příkopě 28 115 03 Praha 1: Česká národní banka, 2016 [cit. 2016-12-12]. Dostupné z: https://apl.cnb.cz/apljerrsdad/JERRS.WEB33.SUBJECTS_COUNTS_DETAIL?p_lang=cz&p_DATUM =12.12.2016&p_ses_idx=182

[12] Money on the Internet Strong Privacy Protection vs. Data Trail [online]. Tokyo: Volker Grassmuck, 1997 [cit. 2016-12-08]. Dostupné z: http://waste.informatik.hu- berlin .de/grassmuck/Texts/ecash.e.html

[13] PayWord and MicroMint: Two simple micropayment schemes [online]. Cambridge,: Rivest, 2001 [cit. 2016-12-08]. Dostupné z: https:// people.csail.mit.edu/rivest/pubs/ RS96a.prepub.pdf

[14] The Millicent Protocol for Inexpensive Electronic Commerce. In: *W3C* [online]. W3C, ©2017 [cit. 2017-03-04]. Dostupné z: https://www.w3.org/ Conferences/WWW4/Papers/246/

[15] PIJÁK, Michal. *Elektronické platební systémy* [online]. Brno, 2003 [cit. 2017-01-08]. Dostupné z: https://www.fi.muni.cz/usr/staudek/vyuka/security/e_payment/. Diplomová práce. Masarykova univerzita. Vedoucí práce Jan Staudek.

[16] Parametry GoPay účtu dle úrovně provedené identifikace. In: Centrum Nápovědy - GoPay [online]. České Budějovice: © GoPay - Instituce elektronických peněz, 2016 [cit. 2016-12-07]. Dostupné z: https:// help.gopay.com/cs/tema/gopay-ucet/gopay-uzivatelsky-ucet/param etry-gopay-uctu-dle-urovne-provedene-identifikace

[17] Ceník služby BLESK peněženka pro Zákazníky. In: Blesk peněženka [online]. Pardubice: MOPET CZ [cit. 2016-06-07]. Dostupné z: http://penezenka .blesk.cz/clanek/ostatni-blesk-penezenka/206199/cenik-sluzby-blesk-penezenka-pro-zakazniky

[18] Sazebník poplatků a limitů. *FreePay* [online]. Praha: Prepaid Solutions [cit. 2017-05-27]. Dostupné z: https://www.freepay.cz/poplatky-a-limity/

[19] Price. *CoinDesk* [online]. New York City: CoinDesk [cit. 2017-05-27]. Dostupné z: http://www.coindesk.com/price/

[20] Bitcoin [online]. Bitcoin Project, 2017 [cit. 2017-05-27]. Dostupné z: https://bitcoin.org/en/

[21] ŠELINGA, Martin. *Kryptoměny* [online]. Brno, 2016 [cit. 2017-06-01]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=130307. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Václav Zeman.

[22] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. In: . Bitcoin Project, 2017, s. 9 [cit. 2017-06-03]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[23] Hashrate Distribution. In: *Blockchain* [online]. Blockchain Luxembourg, 2017 [cit. 2017-06-02]. Dostupné z: https://blockchain.info/pools

[24] *Litecoin* [online]. LITECOIN FOUNDATION, ©2014-2017 [cit. 2017-06-03]. Dostupné z: https://litecoin.com/

[25] CryptoCurrency Market Capitalizations. In: *CoinMarketCap* [online]. CoinMarketCap, 2017 [cit. 2017-06-02]. Dostupné z: https://coinmarketcap.com/currencies/litecoin/

Seznam symbolů, veličin a zkratek

AES	-	Advanced Encryption Standard
CA	-	Certifikační Autorita
CVV	-	Card Verification Value
ČNB	-	Česká Národní Banka
DES	-	Data Encryption Standard
ECDSA	-	Elliptic Curve Digital Signature Algorithm
EPS	-	Elektronický Platební Systém
HTTPS	-	Hypertext Transfer Text Protocol Secure
PCI DSS	-	Payment Card Industry Data Security Standard
RSA	-	Rivest Shamir Adleman
SHA	-	Secure Hash Algorithm
SSL	-	Secure Socket Layer
TCP/IP	-	Transmission Control Protocol/Internet Protocol
TLS	-	Transport Layer Security
WPA	-	Wi-Fi Protected Access

Seznam příloh

Příloha 1. CD s elektronickou verzí práce a zdrojovými kódy