Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informatiky a kvantitativních metod

Bezpečnost a ochrana platidel v moderní společnosti

Diplomová práce

Autor: Bc. Roman Květoň
Studijní obor: Aplikovaná informatika

Vedoucí práce: prof. RNDr. PhDr. Antonín Slabý, CSc.

Hradec Králové Duben 2019

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 22.4.2019 Roman Květoň

Poděkování:

Rád bych na tomto místě poděkoval panu prof. RNDr. PhDr. Antonínu Slabému, CSc. za odborné vedení, za pomoc a rady při zpracování této práce.

Anotace

Diplomová práce se zabývá platidly používanými moderní společností. Má za cíl seznámit čtenáře s principy, na kterých bezhotovostní platby fungují. Vysvětluje funkci a princip kryptografie, která je základním bezpečnostním a ochranným prvkem. Dále pak popisuje fungování bezhotovostních plateb – konkrétně platby kartou, převod mezi účty a platby kryptoměnami. Zároveň analyzuje bezpečnost těchto operací a seznamuje čtenáře s možnými riziky, která aktuálně mohou hrozit. V neposlední řadě práce obsahuje cenné rady, jak útokům předcházet a minimalizovat tak riziko spojené s používáním těchto druhů plateb.

Klíčová slova

Platidlo, kryptografie, internetové bankovnictví, bezhotovostní, transakce, kryptoměna, Bitcoin, bezpečnost

Annotation

Title: Security and protection of currencies in modern society

Thesis is focused on currencies used by modern society. The goal is to familiarize the reader with principles on which these payments work. Thesis explains the function and concept of cryptography which is the main tool of security and protection. Furthermore it explains how cashless payments work – namely transactions with payment cards, transfers of money between bank accounts and cryptocurrency transactions. There is also an analysis of security of these transactions and it describes risks that currently exist. Last but not least thesis contains valuable advices on how to prevent these risks and minimalize them.

Keywords

Currency, cryptography, internet banking, cashless, transaction, cryptocurrency, Bitcoin, security

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Žijeme v úžasné době. Za posledních pár desetiletí se objevilo neuvěřitelné množství nových technologií, které jsou každým dnem zdokonalovány a usnadňují lidem život. Technologie zlepšuje kvalitu života – ba co více – v dnešní době životy i zachraňuje. Informační technologie mohou být vnímány veřejností jako černá skříňka, které rozumí jen specialisti. Pokud je však toto odvětví rozloženo do menších, jednodušších a snadněji pochopitelných částí, pochopit ho do určité míry může každý.

Český národ využívá nové technologie velmi rád, jak je vidět ve statistikách. Rádi nakupujeme v internetových obchodech, v čemž se řadíme v pomyslném žebříčku mezi první na světě. Bezhotovostní platby se také těší stále větší oblibě. Málokdo však ví, jak tyto platby probíhají. Z důvodu rychlých změn se neobjevuje ani mnoho knih, protože než je kniha vydána, už jsou obsažené informace neaktuální. Proto je většina zdrojů použitých v této práci internetového původu.

Cílem diplomové práce je srozumitelně vysvětlit, jakým způsobem fungují základní bankovní transakce, které jsou bezhotovostní a probíhají za pomoci internetu. To znamená transakce s platebními kartami, převod peněz mezi bankovními účty a v neposlední řadě operace s kryptoměnami. Kryptoměny jsou novinkou posledních let a představují nový, unikátní pohled na svět financí a to díky svému jedinečnému přístupu.

Práce zároveň tyto transakce analyzuje z hlediska bezpečnosti a vysvětluje ochranné mechanismy, které jsou při těchto – dnes již každodenních – aktivitách využity. Dále jsou uvedeny aktuální hrozby a způsoby, jakými hackeři útočí v současné době.

V neposlední řadě jsou uvedeny zásady bezpečného užívání a cenné rady, které v případě, že jsou dodržovány, snižují pravděpodobnost úspěšného útoku na minimum. Jedná se o zásady, které má většina lidí v povědomí, nicméně stejně je nedodržuje.

Práce je psána takovým stylem, aby byla srozumitelná pro širokou veřejnost a jednoduše vysvětlila, jakým způsobem technologie a procesy za nimi schované fungují. Čtenář by po přečtení této práce měl získat přehled, na jakém principu

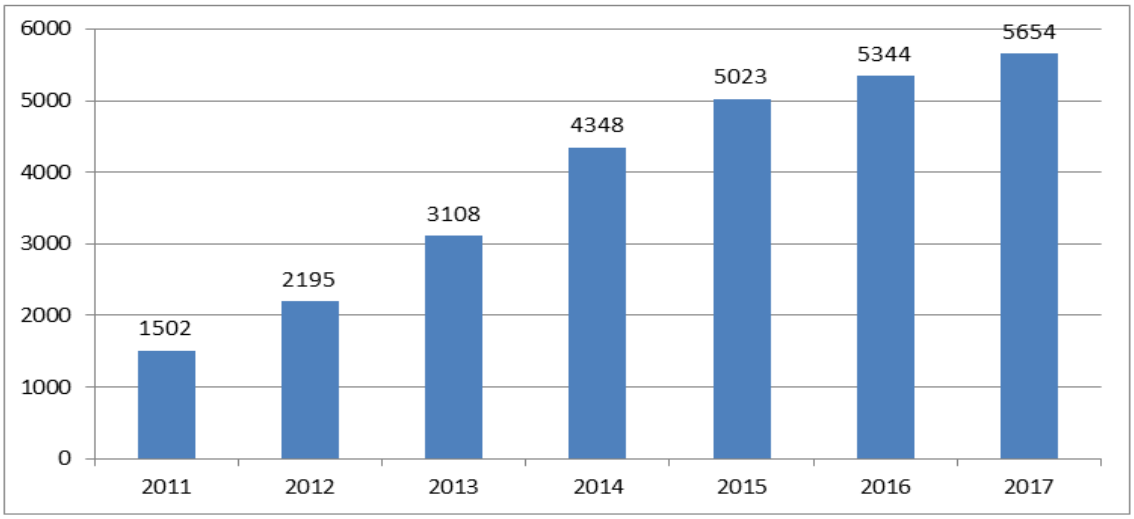
jednotlivé typy finančních transakcí fungují a jaké jsou jejich silné a slabé stránky. Na základě těchto znalostí následně může čtenář vyhodnotit míru rizika, kterou při běžném používání podstupuje a při aplikaci uvedených doporučení tato rizika minimalizovat.

2 Platidla moderní společnosti

Prostředek, který je využíván při směně za zboží či služby, se nazývá platidlo. Má dlouhou tradici – jako první platidla se v dávné minulosti používaly ozdobné kamínky, nebo mušle. Postupem času se přešlo na mince z drahých kovů a vzácné drahokamy. Následně se začaly používat bankovky a dluhopisy. Doba pokročila, nastoupila digitalizace a v moderní společnosti se objevily bezhotovostní platby. Při takové platbě se již vyměňují pouze informace. Bohatství může být například u kryptoměn reprezentováno pouze soukromým klíčem – kombinací několika čísel a písmen. V následujících kapitolách jsou představeny základní způsoby uchovávání platidel a provádění transakcí s těmito platidly.

Jelikož trendem moderní společnosti je provádění bezhotovostních transakcí tzn. takových transakcí, které probíhají bez fyzické účasti bankovek a mincí, tato práce je zaměřena na tento druh transakcí. Jako příklady je možné uvést platbu debetní nebo kreditní kartou v obchodu, platbu mobilním telefonem, nebo převod peněz mezi bankovními účty.

Dle přehledu Policie ČR počet případů kybernetické kriminality roste každým rokem, viz obrázek 1 a tabulka 1, proto je v zájmu každého člověka používajícího moderní technologie placení, aby rozuměl principu, na kterém fungují. Práce se zabývá hlavně dvěma nejpočetnějšími kategoriemi napadení, a to podvodným jednáním a hackingem.



Obr. 1 Napadení TČ kybernetické kriminality 2011-2017
Zdroj: https://www.policie.cz [1]

Tabulka 1 Kategorie napadení TČ kybernetické kriminality 2011-2017

Struktura napadení	2011	2012	2013	2014	2015	2016	2017
Podvodná jednání	917	1303	1863	2478	2932	3235	3140
Hacking	66	112	220	555	578	534	608
Mravnostní delikty	132	161	261	314	351	344	561
Autorskoprávní delikty	155	241	181	262	315	237	296
Násilné projevy + hate crime	86	111	155	202	230	265	318
Ostatní	146	267	428	537	617	729	731
Celkem napadení IT	**1502**	**2195**	**3108**	**4348**	**5023**	**5344**	**5654**

Zdroj: https://www.policie.cz [1]

2.1 Kryptografie

Veškerá komunikace při provádění transakcí probíhá za použití internetu jako komunikačního kanálu. Informace, které se předávají v jednotlivých zprávách, jsou citlivé a v případě, že by se dostaly do rukou nepovolané osoby, mohly by být zneužity. Z toho důvodu je potřeba předávané informace ochránit takovým způsobem, aby pouze účastníci probíhající transakce měli přístup k posílaným informacím. Toho je dosáhnuto pomocí šifrování. Aby bylo možné dále zkoumat danou problematiku, je na místě vysvětlit základní principy šifrování.

Kryptografie je disciplína, která se zabývá utajováním smyslu zpráv takovým způsobem, aby pouze osoba disponující určitou znalostí mohla zprávu dekódovat a zjistit tak pravý obsah zprávy. Šifrování hrálo velkou roli v dějinách lidstva a postupem času se zlepšovaly metody jak šifrování, tak kryptoanalýzy. Tak se nazývá proces, kdy se útočník nebo bezpečnostní analytik snaží rozluštit obsah zprávy bez znalosti způsobu, jakým byla zpráva šifrována.

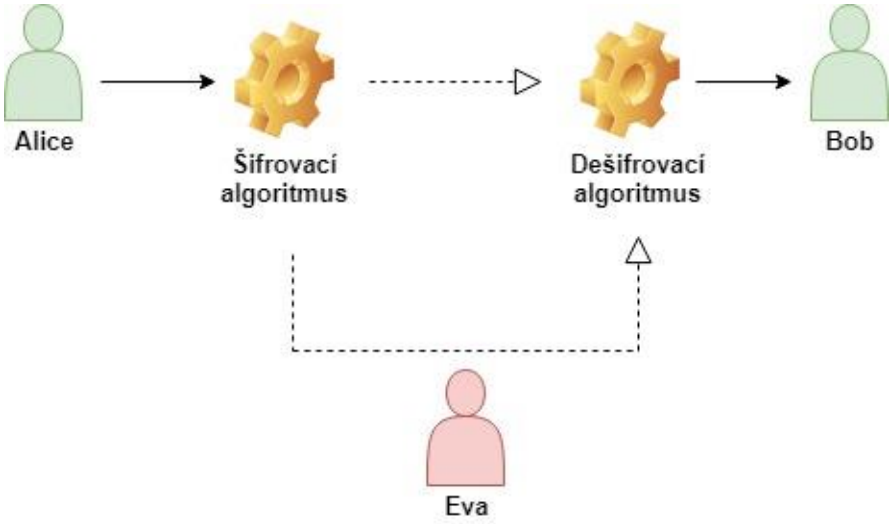
K převedení prostého textu na šifru je potřeba kryptografický algoritmus. To je posloupnost kroků, které je třeba vykonat k vytvoření šifry. Pro sofistikovanější způsoby šifrování se používají parametry šifrování – neboli klíče. V moderní informatice se používají dva druhy šifer. Symetrické šifry používají stejný klíč jak k šifrování, tak k dešifrování. Druhým typem jsou asymetrické šifry, kde se využívá dvojice klíčů. Jeden k zašifrování – veřejný klíč (angl. public key), druhý k dešifrování – soukromý klíč (angl. private key).

Úroveň zabezpečení (angl. Security Level) vyjádřená v bitech je formalizovaný způsob, který používáme jak pro hodnocení kryptografické „síly" daného algoritmu, tak pro bezpečnostní porovnání algoritmů mezi sebou. Říkáme, že daný algoritmus má bezpečnostní úroveň n bitů, pokud nejlepší známý útok požaduje provedení 2^n *kroků k jeho prolomení (jedná se de facto o zkoušení všech n-bitových sekvencí pomocí hrubé síly). Úroveň zabezpečení je vždy vztažena k délce klíče dané šifry (například ECC[1] s klíči o délce 512 bitů má úroveň zabezpečení 256 bitů). [2 str. 131]*

2.1.1 Symetrické šifrování

Na obrázku 2 je znázorněn princip symetrického šifrování, kdy se Alice snaží poslat Bobovi tajnou zprávu a Eva se snaží tuto zprávu získat. Díky tomu, že Alice i Bob znají klíč, mohou zprávu zašifrovat a následně dešifrovat. Eva však klíč nezná a proto pro ni zůstává pravý obsah zprávy skrytý. Při takové komunikaci však vzniká problém, jakým způsobem si mohou účastníci komunikace vyměnit klíč potřebný pro šifrování komunikace. Tento problém řeší asymetrické šifrování, které je vysvětleno dále.

[1] Elliptic Curve Cryptography viz kapitola 2.1.2.2



Obr. 2 Symetrické šifrování komunikace
Zdroj: vlastní tvorba

2.1.1.1 Advanced Encryption Standard

Po prolomení šifrovacího standardu DES (Data Encryption Standard) v roce 1997 bylo nutné vytvořit nový standard pro šifrování. Novým standardem – Advanced Encryption Standard – zkratka AES, se v roce 2001 oficiálně stala šifra Rjindael. Je to nejvyužívanější šifrovací algoritmus ze skupiny symetrických blokových šifrovacích algoritmů. Symetrický je proto, že jak k zašifrování, tak k dešifrování se používá stejný klíč. Slovo blokový znamená, že data jsou rozdělena do bloků dat stejné velikosti a s těmito bloky poté algoritmus pracuje – obvykle 128, 192, nebo 256 bitů. [2]

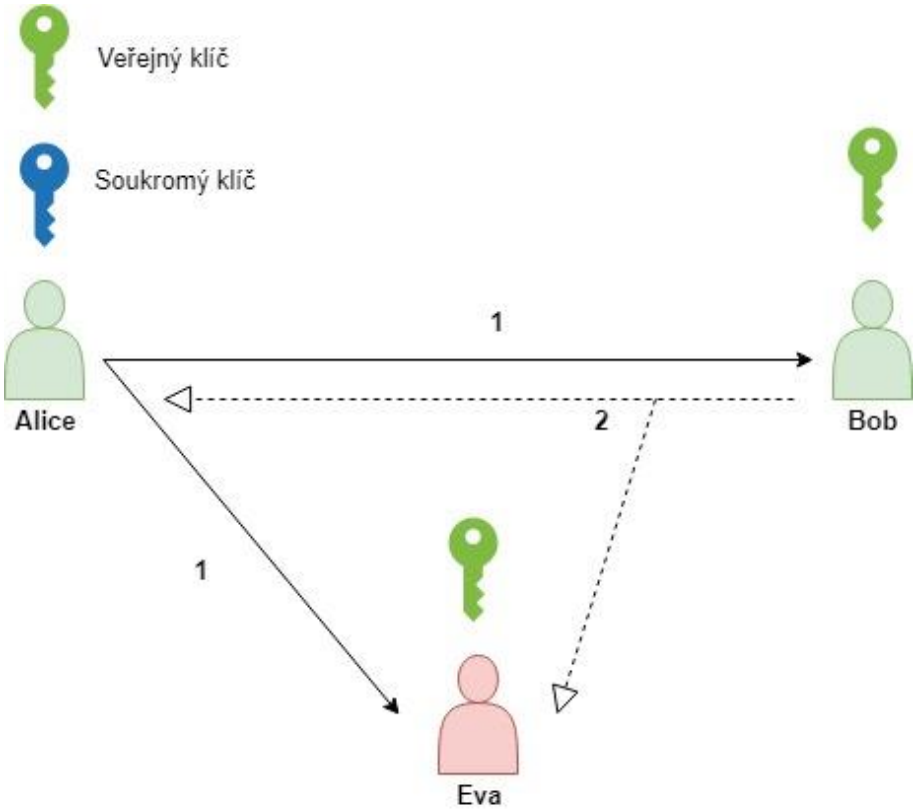
Základní princip je takový, že se pracuje s nezašifrovaným textem, ke kterému je „přičten“ klíč, poté je provedena substituce – převedení pomocí tabulky na jiné hodnoty a následně mohou být s textem provedeny další operace. Při rozšifrování jsou kroky velmi podobné, ale jsou provedené v opačném pořadí.

Příklad šifry AES:

Nezašifrovaný text: „Ahoj jak se máš?“
Klíč: „Tajne576Heslo721“
Zašifrovaný text:
„467C49EF71A28673BCA24E9D2E87AC2782435BD45DA06FA66F34493158105133“

2.1.2 Asymetrické šifrování

Princip asymetrického šifrování je znázorněn na obrázku 3 níže. V tomto případě potřebuje Alice získat tajnou informaci od Boba. Nejdříve musí Alice vygenerovat pár klíčů – veřejný a soukromý. Veřejný pošle Bobovi a Eva tento klíč může získat také. Za použití veřejného klíče je Bobova zpráva zašifrována a poslána Alici. Následně může Alice pomocí soukromého klíče zprávu dešifrovat. Eva, která má k dispozici zašifrovanou zprávu a veřejný klíč nemůže zprávu dešifrovat.



Obr. 3 Asymetrické šifrování komunikace
Zdroj: vlastní tvorba

Pokud by se jednalo o oboustrannou komunikaci, musel by Bob vytvořit vlastní pár klíčů, kde by stejně jako Alice musel poslat před zahájením komunikace svůj veřejný klíč.

2.1.2.1 RSA

Nejpoužívanějším asymetrickým šifrovacím algoritmem je RSA. Tato zkratka vznikla spojením prvních písmen příjmení jeho tvůrců, jimiž byli Ronald Rivest, Adi Shamir a Leondard Adleman. Asymetrický způsob šifrování spočívá v použití

dvou klíčů. Prvním je veřejný klíč, který je použit k zašifrování dat. Naopak k dešifrování se následně užívá soukromý klíč. Asymetrické šifrování je zpravidla výpočetně náročnější a proto pomalejší. Proto se v praxi využívá takový přístup, že data se šifrují pomocí symetrické šifry a k přenosu symetrického klíče se používá asymetrická šifra.

Šifra je postavena na součinu dvou velkých prvočísel. Využívá se neexistence algoritmu, který by byl schopen v polynomiálním čase faktorizovat velká čísla na součin prvočísel. Jinými slovy je jednoduché dvě velká prvočísla vynásobit, ale extrémně obtížné ze součinu vyjádřit původní prvočísla. V praxi se používá délka klíče pro RSA 1024 bitů, což znamená dvě prvočísla o velikosti 512 bitů. Taková délka je aktuálně vnímána jako bezpečná. V budoucnu se však může délka klíče zvyšovat na 2048 bitů a více.[2]

Příklad klíčů RSA s délkou klíče 1024 bitů:

Veřejný klíč:

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDRe/j5mw8Kbo5sjskPuHtJ7Xg
ixRSMolAONLrHkBN7TxGtNUvHTp9cTGJOdvLedc+S9YQAHk7++BhOI7yuv9ZoOJ6
RlegrZSvda3RwwxiZHk4vwYF6DQi80EO/8oSHqWqhZj9FwmG/KlCEXbnJ89AfA3S
gVE77Ypu4uKueHsYajwIDAQAB

Soukromý klíč:

MIICXgIBAAKBgQDRe/j5mw8Kbo5sjskPuHtJ7XgixRSMolAONLrHkBN7TxGtNUvH
Tp9cTGJOdvLedc+S9YQAHk7++BhOI7yuv9ZoOJ6RlegrZSvda3RwwxiZHk4vwYF6
DQi80EO/8oSHqWqhZj9FwmG/KlCEXbnJ89AfA3SgVE77Ypu4uKueHsYajwIDAQA
BAoGBAIfrIh4Bx36DQRGai0YR8pyC4YHd0Xl2Du9Isy+sgZduNA/oFqTYlHl0bgxv
DSHd2rKFbgINqD+yhUKd2Vygx+FmtBFskBPS2+FPINvBeY/o7i2yA0/FiJhbgtqx
JsyVV14Ktb8vhQynK183R01817ptaDDSnr123beYWn5Ma9ZxAkEA8Em+WB8/lGiI
zngbRfzLJOOiCs5zgIutuCQAuuYga6CnD+/pYmwP4qYwfMAd15rJyBwC73pDzG+I
C0VsrmAmewJBAN8umEL3JMA7lMv64jteq8Z+uvAXhQVBe0reaYXNi3KBBrbzcRn9
Mnai7qji0G+9gczU7ES4fjC7zF1jKr0lSf0CQQC2XKEzK/QK5BL/77NzOFnMU15F
qU2Lf3aGS/yp28E7LZ/cvo13ft/Hea1O4FdFrFn7nxazPS17WCH9u+CxrpNFAkAb
BMsOIFlkpFHpN+A3i8iD6Ue8VTyXXEwOzko8FpwxKomjkGk62jpHvoXiEENno6uZ
HpXT4/ny8GlXTPAZofAJAkEA55vGSYl2Cym6SMbkMjEL0lnK4hSD7dj/EW0lZ93F
IILZ9mXkK/vzcUxz7e+wcpSMS+TWkSvU3H9CWv+RXjpuaQ==

2.1.2.2 Aritmetika eliptických křivek

Kryptografie na bázi eliptických křivek (angl. Elliptic Curve Cryptography, zkr. ECC) byla v roce 1985 navržena nezávisle na sobě Nealem Koblitzem a Victorem Saulem Millerem. Jedná se o jeden z nejmladších šifrovacích systémů s veřejným klíčem. S ohledem na Moorův zákon[2] se délka klíče neustále zvětšuje. Zatímco u RSA bude potřeba v budoucnosti používat 3072- bitové klíče, pro ECC stačí při stejném stupni zabezpečení klíč délky 256 bitů. [2]

Zde je využito specifických vlastností eliptických křivek, které mají v praxi formu Weierstrassovy rovnice:

$$y^2 = x^3 + a \cdot x + b$$

$$a, b \in K$$

Mezi nejznámější ECC algoritmy patří:

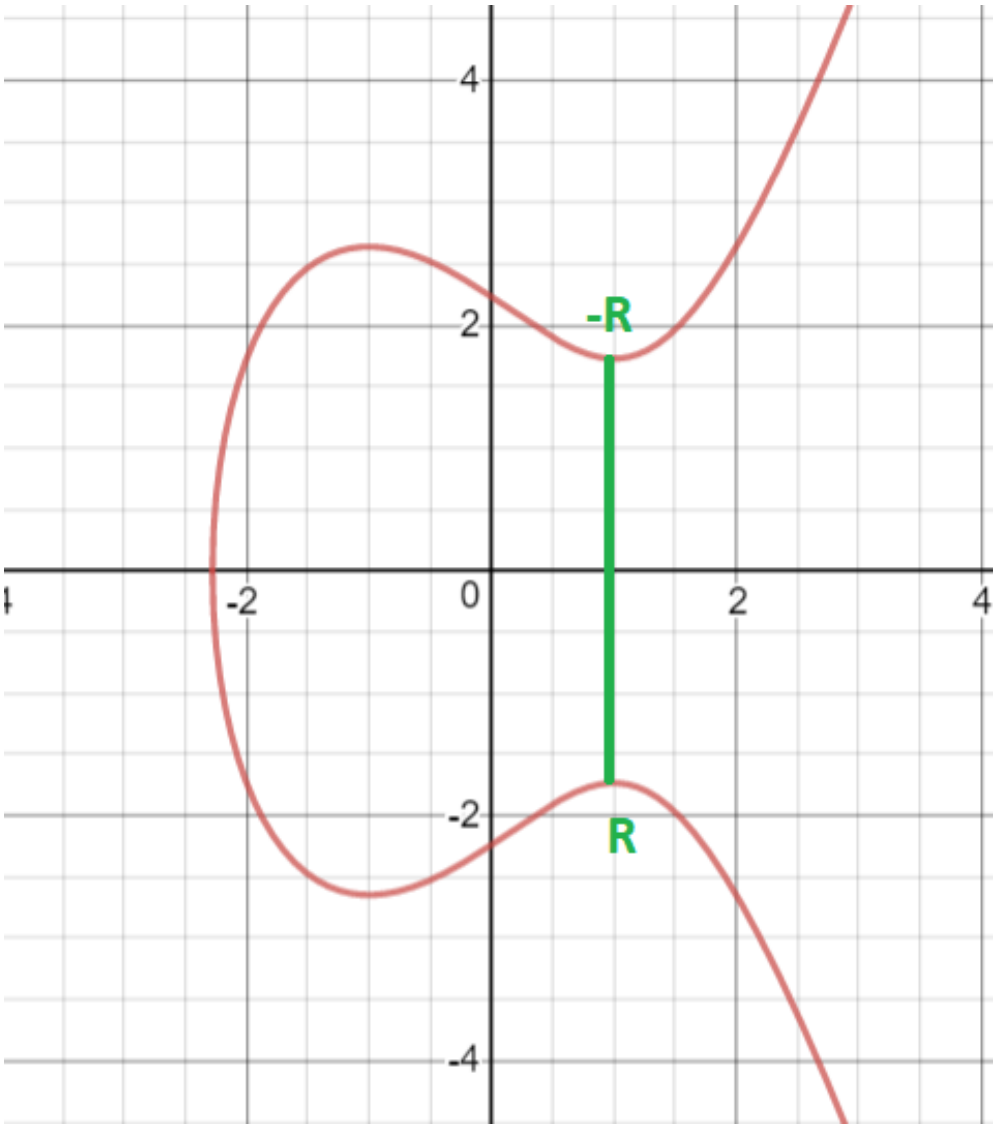
- Elliptic Curve Integrated Encription Scheme (ECIES)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Elliptic Curve Diffie Hellman (ECDH)

2.1.2.3 Klíčové vlastnosti eliptických křivek

Diskriminant nesmí být roven nule – takové křivky jsou nediferencovatelné, což znamená, že v některých bodech neexistuje derivace. V šifrovacím algoritmu by měla být zajištěna kontrola, že je tato podmínka splněna. Je-li diskriminant záporný, je eliptická křivka spojitá a tvořena jednou částí. Pokud je diskriminant kladný, je křivka tvořena dvěma spojitými částmi. Tím však neznamená, že by se s křivkou tvořenou dvěma spojitými částmi nedalo pracovat – má identické vlastnosti.

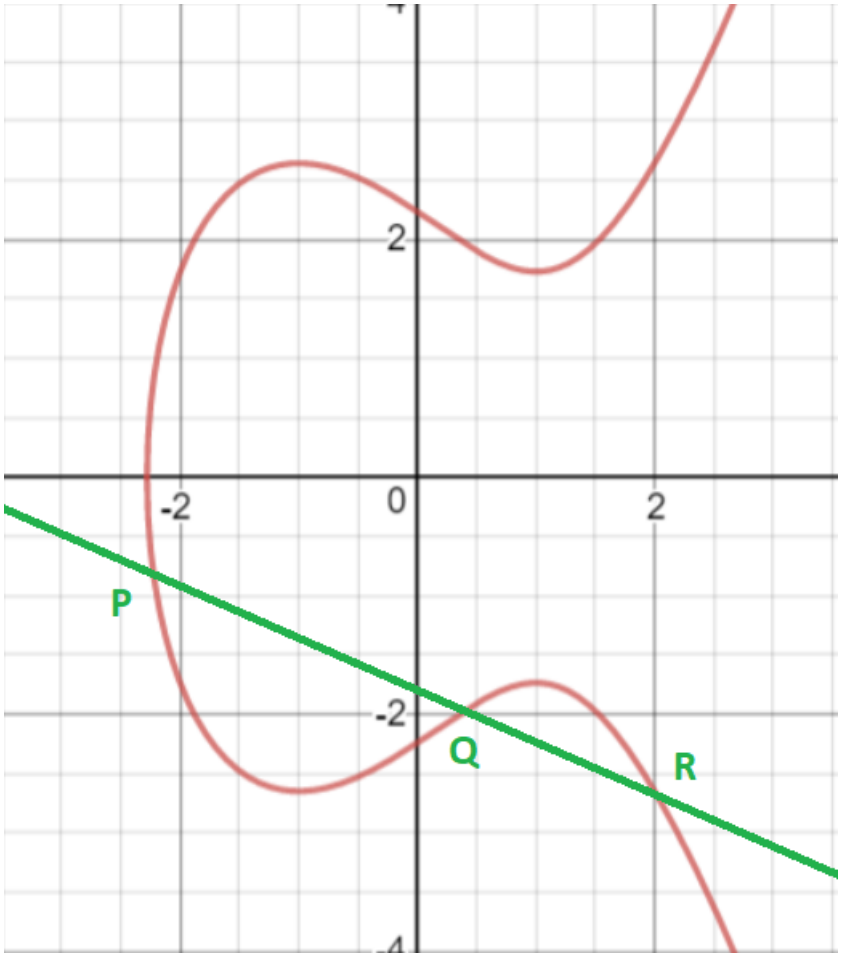
[2] Vysvětlení Moorova zákona - https://managementmania.com/cs/mooruv-zakon

Eliptické křivky jsou souměrné podle osy x, proto pro každý bod *P[x, y]* je možné nalézt opačný bod *-P[x, -y]*, což je znázorněno na obrázku 4.



Obr. 4 Souměrnost eliptických křivek podle osy *x*
Zdroj: vlastní tvorba

Další klíčovou vlastností je skutečnost, že pokud jsou na křivce určeny dva různé body, které nejsou opačné – *P* a *Q*, při jejich protnutí přímkou vzniká bod třetí - *R*. Tímto způsobem probíhá operace sčítání na eliptické křivce $P + Q = R$

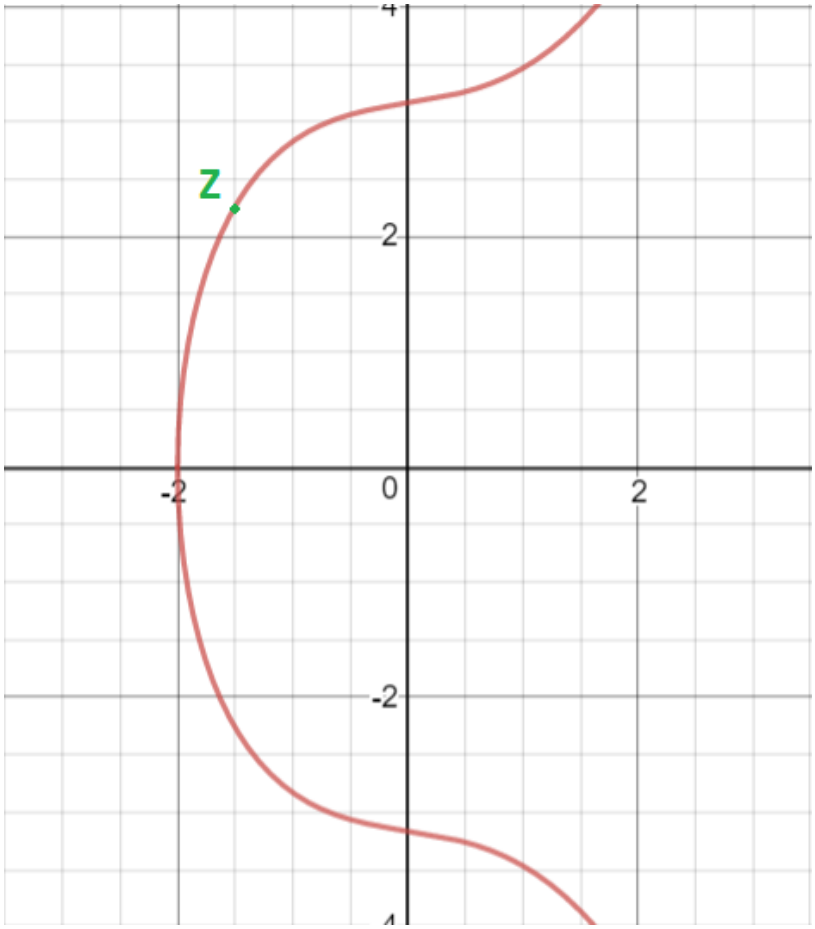


Obr. 5 Sčítání bodů na eliptické křivce
Zdroj: vlastní tvorba

Dále je možné násobit bod skalárem: $n \cdot P$. Násobení je prováděno jako postupné sčítání bodu *P*, například *2P* je počítáno jako *P + P = 2P.* Násobení bodu skalárem hraje důležitou roli v kryptografii, protože bod $n \cdot P$ představuje veřejný klíč a skalár *n* klíč soukromý. Pomocí výpočtu je vypočítán symetrický klíč, který je následně využit k šifrování komunikace.

Příklad ECC

Uživatel A i uživatel B znají rovnici eliptické křivky $y^2 = x^3 + x + 10$ a bod *Z[-1,5; 2,2638]* viz obrázek 6.



Obr. 6 Určení bodu na eliptické křivce
Zdroj: vlastní tvorba

Volba soukromých ECC klíčů:

Uživatel A si jako svůj soukromý klíč zvolí číslo 2, tedy $S_A = 2$.

Uživatel B si jako svůj soukromý klíč zvolí číslo 3, tedy $S_B = 3$.

Výpočet veřejných klíčů:

Uživatelé vytvoří své veřejné klíče vynásobením svého soukromého klíče a bodu *Z*.

Pro uživatele A je to $V_A = S_A \cdot Z = 2Z$

Výpočet směrnice *s*:

$$s = \frac{3x_Z^2 + a}{2y_Z} = \frac{3 \cdot (-1{,}5^2) + 1}{2 \cdot 2{,}2638} = 1{,}7117$$

Výpočet souřadnic bodu $2Z[x_{2Z};\ y_{2Z}]$:

$x_{2Z} = s^2 - 2 \cdot x_Z = 1{,}7117^2 - 2 \cdot (-1{,}5) = 5{,}9299$

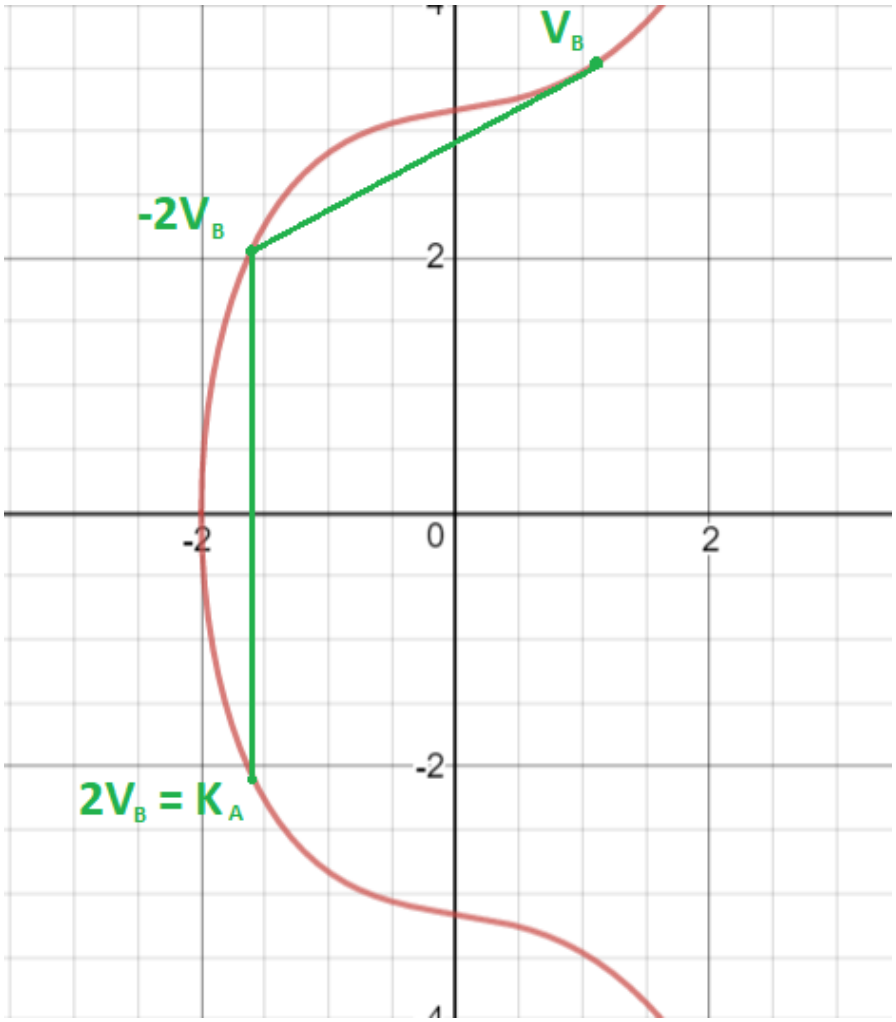
$y_{2Z} = -y_Z + s(x_Z - x_{2Z}) = -2{,}2638 + 1{,}7117 \cdot (-1{,}5 - 5{,}29299) = -14{,}98156$

$V_A = [5{,}9299;\ -14{,}98156]$

Stejným způsobem uživatel B posílá $V_B = 3Z = [0{,}95749; 3{,}44022]$

Nezávislý výpočet klíče:

Uživatel A násobí svůj soukromý klíč $S_A = 2$ a přenesený veřejný klíč $V_B = [0{,}95749; 3{,}44022]$ od uživatele B. Výsledkem je bod $2V_B = [-1{,}61788;\ -2{,}03646]$, který je symetrickým klíčem pro další šifrovanou komunikaci viz obrázek 7. [2]



Obr. 7 Výpočet symetrického klíče
Zdroj: vlastní tvorba

2.1.3 Hashovací funkce

Hašovací funkce (angl. Hash Function) je taková funkce, která z libovolně dlouhého vstupu vytváří řetězec fixní délky. Výstup se nazývá hash, nebo fingerprint. Běžně je tento mechanismus využíván v hashovacích tabulkách, kde hash je použit jako index pro rychlé vyhledávání.

V kryptografii mají hashovací funkce také velkou roli. Díky jejich vlastnostem jsou používány k verifikaci transakcí – například v kryptoměnovém systému Bitcoin. Dále jsou využívány k ověřování digitálního podpisu, či ověření autentičnosti elektronické zprávy. Algoritmy jsou dále využity například v protokolech SSL[3], nebo SSH[4]. Každá drobná změna ve vstupních datech vede k velkým změnám na výstupu.

2.1.3.1 Secure Hash Algorithms

Zkráceně SHA je sada kryptografických hashovacích funkcí, kterou vydal National Institute of Standards and Technology (NIST) ve spolupráci s National Security Agency (NSA). Spadají pod Secure Hash Standard, označení FIPS PUB 180-4. SHA je tvořen několika generacemi, které se z důvodu narůstající výpočtové síly musí být čím dál obtížnější prolomit. [3]

SHA-0

Funkce SHA-0 byla zveřejněna roku 1993 jako bezpečný standard hashování. Následně při revizi roku 1995 byla objevena chyba a byla vydána nová verze.

SHA-1

Funkce SHA-1 je podobná hashovací funkci MD4, avšak byly přidány další prvky pro zvýšení komplexnosti. Délka výstupu funkce je 160 bitů. Roku 2005 se objevil první útok na SHA-1. [4]

Příklad výstupu hashovací funkce SHA-1:

```
SHA-1(„“) = da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA-1(„a“) = 86f7e437faa5a7fce15d1ddcb9eaeaea377667b8
```

[3] Secure Socket Layer – protokol zajišťující bezpečnou komunikaci s webovými servery pomocí HTTPS.

[4] Secure Shell – zabezpečený protokol pro komunikaci v počítačových sítích

SHA-2

Po výše zmíněném útoku se začala používat sada SHA-2 mezi které patří například funkce označované jako SHA-224, SHA-256, SHA-384 a SHA-512, kde číslo označuje délku výstupu. Funkce SHA-256 je mimo jiné použita k hashování transakcí v kryptoměnovém systému Bitcoin. [5]

Příklad výstupu hashovací funkce HSA-256:

SHA-256(„“)=
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA-256(„a“)=
ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

SHA-3

Přestože zatím není možné SHA-2 prolomit, v roce 2015 byl vyhlášena nová generace standardu – zvítězila funkce Keccak. Tento algoritmus používá jiný princip, než funkce SHA-2.

V tabulce 2 níže jsou uvedeny atributy jednotlivých hashovacích funkcí.

Tabulka 2 Specifikace používaných hashovacích funkcí

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size (bits)
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512
SHA-512/224	$< 2^{128}$	1024	64	224
SHA-512/256	$< 2^{128}$	1024	64	256

Zdroj https://nvlpubs.nist.gov [6]

2.2 Platební karty

Předchůdcem platebních karet byly v minulosti cestovní šeky a peněžní poukázky, které vznikly společně s rozvojem obchodu a cestování v 19. století. Bylo potřeba vyřešit problém bezpečného placení za zboží nebo služby a to na velké vzdálenosti. První platební karty vznikly na území USA a za jejich vynález jsou odpovědné čtyři společnosti: Diners Club, American Express, Visa a MasterCard. Postupem času se z těchto firem staly nadnárodní společnosti, které mají pobočky ve většině zemí světa. [7]

Ať už se jedná o kreditní kartu, nebo debetní kartu, v současné době vlastní tuto plastovou kartu téměř každý. Díky ní lze platit výměnou za služby či zboží a to nejen v kamenných obchodech, ale i v internetových obchodech – e-shopech. V případě neautorizované transakce (např. při opsání údajů z kreditní karty) by měla ze zákona uvést banka účet do stavu před provedením takové transakce. Toto však neplatí, jedná-li se o částku vyšší než 150 EUR, nebo pokud držitel platební karty úmyslně, nebo z hrubé nedbalosti porušil některou ze svých povinností držitele karty. Proto je třeba takovým situacím předcházet. [8]

Tabulka 3 obsahuje počty aktivních platebních karet na území české republiky, která je v tomto směru velice vyspělá.

Tabulka 3 Počet platebních karet v ČR 2012-2017

	2013	2014	2015	2016	2017
Celkový počet	10,250.651	11,027.590	11,421.038	11,336.146	10,732.949
Debetních	7,945.804	8,731.223	9,131.920	9,314.226	8,797.432

Zdroj: https://www.ceskenoviny.cz [9]

2.2.1 EMV

Za fungováním a určováním standardů platebních karet stojí společnost EMVCo (www.emvco.com), na kterou dohlíží šest společností - American Express, Discover, JCB, Mastercard, UnionPay a Visa. Zkratka EMV potom stojí pro Europay, Mastercard a Visa. Bližší info k jednotlivým členům je možné nalézt na odkazu https://www.emvco.com/about/emvco-members/. EMV® je také ochranná známka všech specifikací, které spravuje EMVCo. Mezi tyto specifikace patří

platební tokenizace, 3D Secure, QR kód a další. V současné době platí verze 4.3, která je platná od listopadu 2011.
Normy:

- ISO/IEC 7816 Identifikační karty – Karty s integrovanýni obvody
- ISO/IEC 14443 Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s vazbou na blízko [10]

2.2.2 Druhy platebních karet

Platební karty můžeme dělit dle několika kritérií.
Dle způsobu čerpání peněz:

- Debetní – při používání debetní karty jsou použity prostředky z bankovního účtu vlastníka. Tento druh karet je nejrozšířenější.
- Kreditní – u kreditních karet uživatel používá peníze banky a je povinen do určitého počtu dnů použité prostředky vrátit. Pokud se tak nestane, tak uživatel platí úrok ze zbývajícího dluhu.
- Předplacené – na kartu je ať jednorázově, nebo opakovaně „nabito“ a uživatel může kartou platit v určitých situacích. Může se jednat například o stále oblíbenější stravenkové karty.

Dle způsobu vytvoření:

- Embossovaná – karta s mechanicky vytlačenými údaji, která se dá využít u mechanických snímačů, do kterých se karta otiskne. Tento způsob platby s rozvíjející se digitalizací již není tolik využíván.
- Elektronická – slouží k platbě za pomoci platebního terminálu, případně k výběru z bankomatů.
- Virtuální – nemá fyzickou podobu. Je využívána pouze pro platby za pomoci internetu. Je reprezentována pouze sadou informací, které kartu identifikují.

Dle způsobu čtení dat z karty:

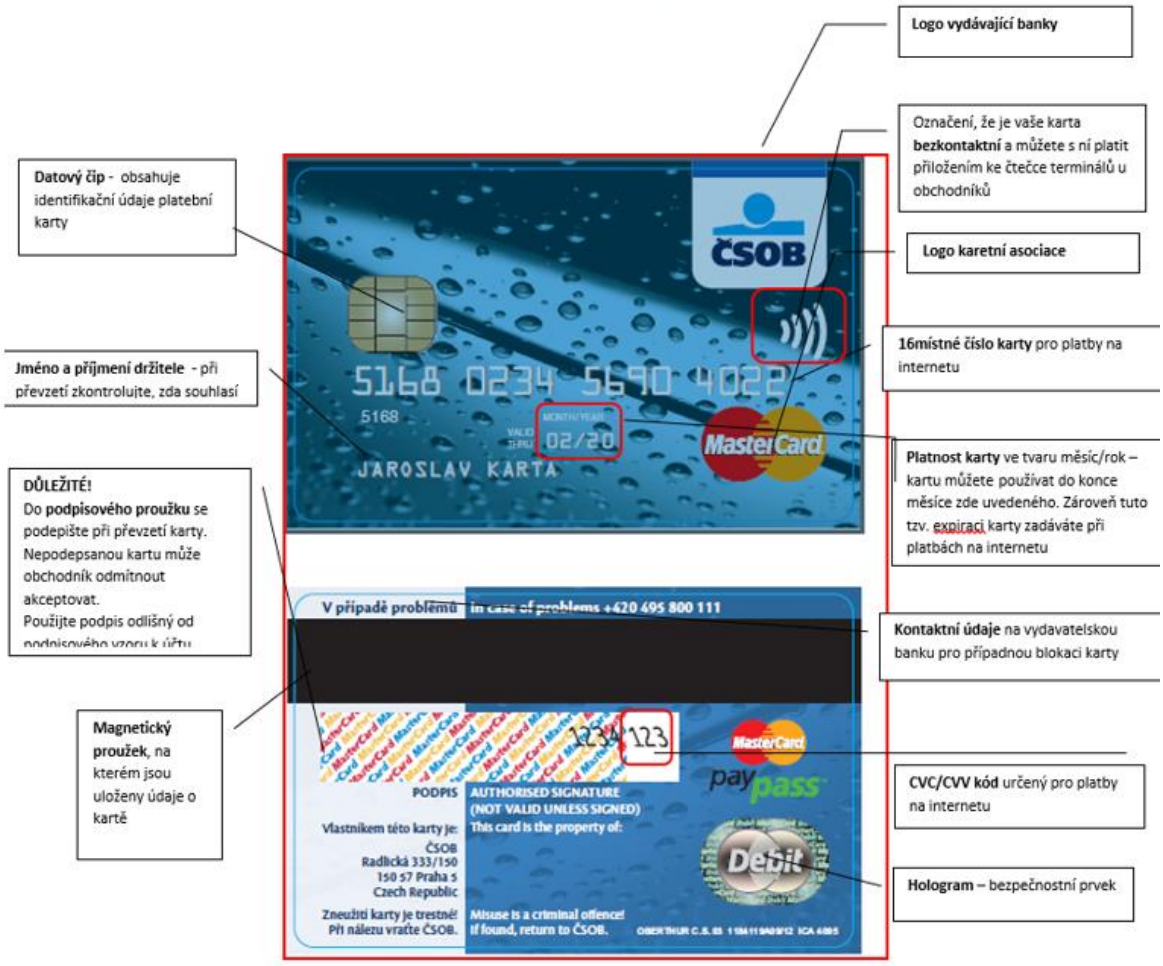
- Magnetický proužek – karta má na zadní straně černý magnetický proužek, který obsahuje veškeré informace o kartě ve statické formě. Tyto karty jsou náchylné na poruchy, obzvláště pokud se ocitnou v blízkosti magnetů.
- Čip – karta obsahuje malý elektronický čip, který dodává informace o kartě v kryptované formě při vložení karty do platebního terminálu.
- Bezkontaktní – pomocí metody NFC[5] komunikuje karta s platebním terminálem na krátkou vzdálenost do 10 cm bez potřeby vkládání karty do terminálu.
- Hybridní – kombinace předchozích možností. Aktuálně vydávané karty stále mohou disponovat všemi třemi způsoby platby, avšak magnetický pásek se již moc nevyužívá a je funkční pouze u starších karet.

2.2.3 Náležitosti platební karty

Na obrázku 10 níže je vyobrazena ukázková debetní karta. Taková karta obsahuje předem stanovené množství údajů, nicméně ty nejdůležitější, které jsou potřeba k uskutečnění platby, jsou následující:

- Identifikační šestnáctimístné číslo
- datum ukončení platnosti karty
- jméno a příjmení držitele karty
- CVC[6]

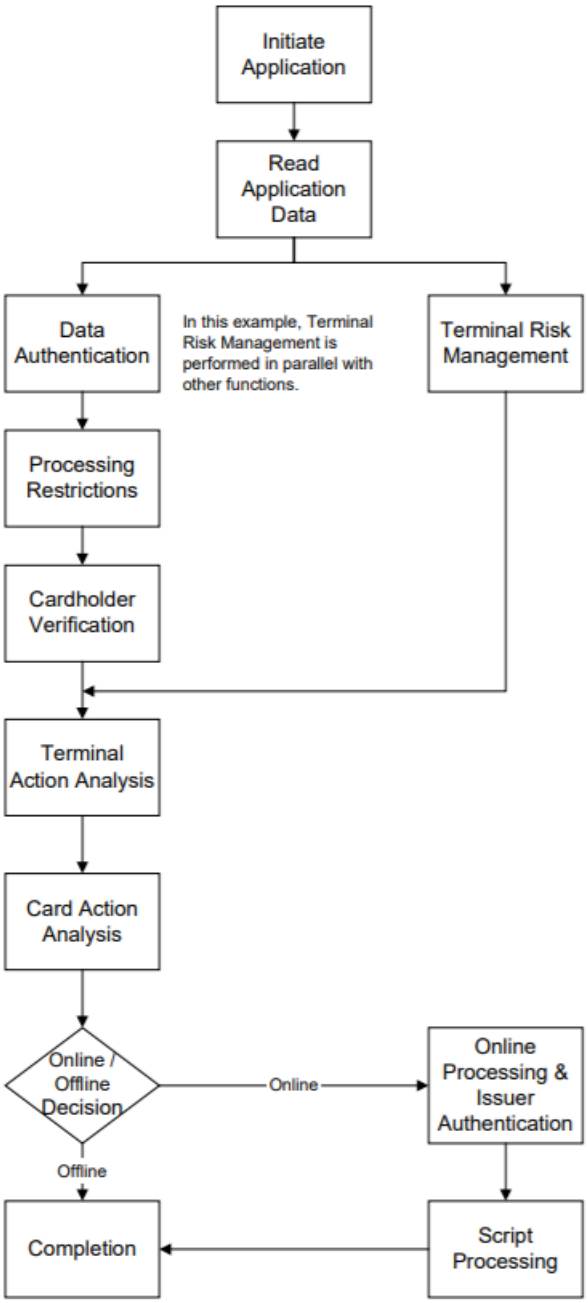
[5] Near Field Communication – Bezdrátová komunikace na krátkou vzdálenost
[6] Card Verification Code – Kód pro ověření karty u transakcí, kdy není fyzicky karta přítomna (typicky platby na internetu)



Obr. 8 Náležitosti platební karty
Zdroj: https://www.csob.cz [10]

2.2.4 Průběh platby kartou

Obrázek 9 níže obsahuje schéma průběhu platby kartou. Technické specifikace se mohou lišit v závislosti na tom, jestli se jedná o kontaktní, nebo bezkontaktní platbu.



Obr. 9 Průběh platby kartou
Zdroj: www.emvco.com [11]

Initiate Application (Spuštění Aplikace) – Komunikaci je vždy zahájena terminálem. První zprávou je karta informována o skutečnosti, že začíná nová transakce.

Read Application Data (Přečtení Aplikačních Dat) – Bezprostředně po zahájení komunikace je z terminálu vyslán požadavek na přečtení dat z karty. V případě, že se objeví chyba při čtení, je transakce ukončena.

Data Authentication (Ověření Dat) – Data získaná z karty je třeba ověřit. Pokud to karta umožňuje, je provedeno offline. Existují tři způsoby, jak může být provedeno – staticky, dynamicky, nebo kombinovaně (SDA, DDA, nebo CDA).

Terminal Risk Management (Správa Rizika Terminálu) – Krok je prováděn při každé transakci. Jedná se o kontrolu, která by měla zamezit podvodům. Je kontrolováno, zda není v logu terminálu více menších transakcí, které by dohromady přesahovaly limit (dělení platby). Dále je některá platba náhodně vybrána k online zpracování namísto offline. Pravděpodobnost je úměrná výši placené částky. Zároveň ještě kontrola ověřuje, že jsou offline platby periodicky zpracovávány a nedochází k žádným problémům v komunikaci.

Processing Restrictions (Omezení zpracování) – Při tomto kroku je kontrolována kompatibilita terminálu a karty. Například verze aplikace karty a terminálu, nebo kontrola data ukončení karty. Při neshodě nebo nesplnění podmínky může dojít k ukončení transakce.

Cardholder Verification (Ověření Držitele Karty) – Tento krok by měl zamezit používání karty uživateli, který není vlatníkem karty. Možnosti ověření jsou: ověření PIN kódu offline, ověření PIN kódu online, ověření podpisu, nebo kombinací zmíněných. Zároveň může být ověření držitele vypnuto a v takovém případě se neprovádí žádná kontrola.

Terminal Action Analysis (Analýza Akce Terminálu) – Jak karta, tak terminál mají nastavenou preferovanou akci zpracování transakce. Jsou tři možnosti: schválení offline, zamítnutí offline, nebo zpracování online. Preference jsou porovnány a v rámci tohoto kroku je vybrána dohodnutá akce.

Card Action Analysis (Analýza Akce Karty) – Po zvolení akce terminálu může na kartě proběhnout test rizika ze strany karty obdobně jako na terminálu. Na základě akce terminálu může být akce karty zpracována offline, zpracována online, nebo zamítnuta.

Online Processing & Issuer Authentication (Online zpracování a ověření zadavatele) – Tento krok zajišťuje, že zadavatel transakce může zkontrolovat a autorizovat, nebo odmítnout transakci mimo povolený limit.

Script Processing (Zpracování skriptů) – Při provádění transakce se může stát, že jsou předány skripty příkazů do čipu karty, které terminál nijak nezpracovává,

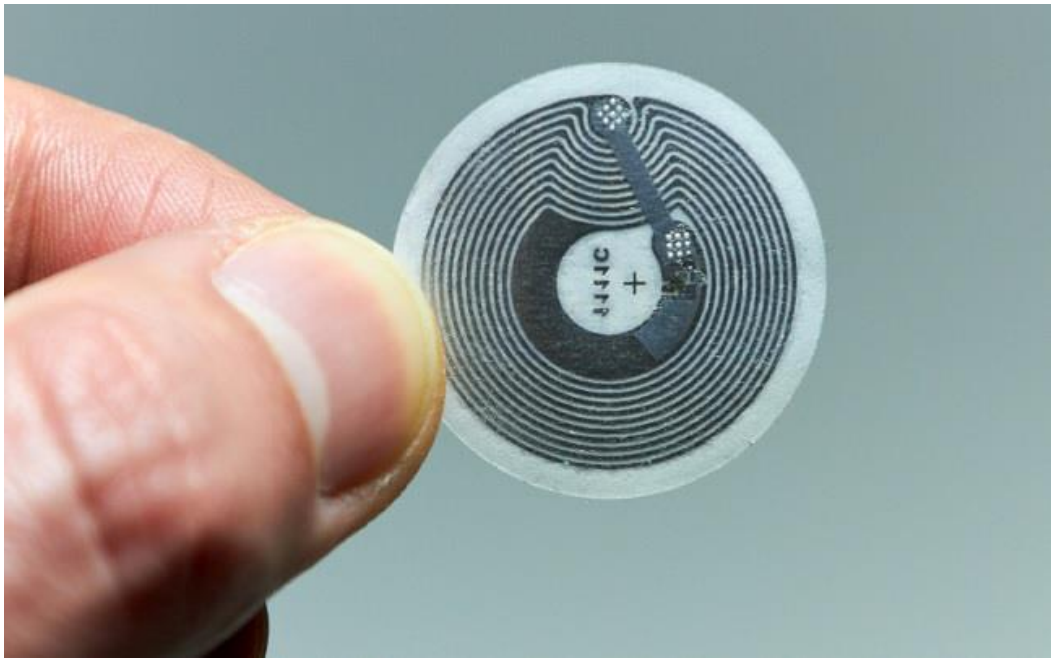
pouze má za úkol je předat kartě. To slouží k provedení funkcí, které nemusí souviset přímo s transakcí, nicméně jsou potřebné. Příkladem může být odblokování offline PIN kódu, což může být odlišné u různých platebních systémů.
Completion (Dokončení) – Poslední krok, který ukončuje zpracování transakce. V případě chyby, nebo předběžnému zamítnutí k němu nemusí dojít. [11]

2.2.5 Near Field Communication

Near Field Communication, zkratka NFC je technologie, která se objevuje v nových mobilních telefonech a platebních kartách. Je vedena pod standardem ISO/IEC 18000-3, který definuje požadavky pro Radio Frequency Identification (RFID). Pomocí této technologie je možné vyměňovat data s dalšími zařízeními, případně získávat informace z takzvaných pasivních zařízení [12].

Obr. 10 Logo technologie NFC
Zdroj: https://nfc.today [13]

NFC je způsob bezdrátové komunikace na velmi krátkou vzdálenost – do 10 cm. K výměně informací využívá elektromagnetické pole. Komunikace mezi dvěma aktivními zařízeními probíhá tak, že u obou zařízení je vytvářeno magnetické pole pomocí energie z baterie telefonů. U pasivních zařízení je princip odlišný. Pasivní zařízení nemají k dispozici žádný zdroj energie, takže komunikují až ve chvíli, kdy se k nim přiblíží aktivní zařízení a pomocí svého magnetického pole v podstatě nabije cívku drátu pasivního zařízení. Poté je možné přečíst informace z daného zařízení. Na obrázku 11 níže je zobrazeno pasivní zařízení v podobě samolepky [14].



Obr. 11 Pasivní zařízení NFC
Zdroj: www.androidauthority.com [15]

Tato technologie má mnoho zajímavých využití. Může být použito v čipové kartě, kterou se zaměstnanci prokazují při vstupu do budovy, může obsahovat informace o zboží, které si chce zákazník koupit, nebo je možné předávat informace mezi telefony dvou přátel. Pro účely práce má však ještě jedno důležité využití, a to k zaplacení. V moderní společnosti se využívá tato technologie k tomu, že uživatel nahraje informace o své platební kartě do svého mobilního telefonu a nemusí s sebou nosit fyzickou platební kartu, protože při placení použije svůj mobilní telefon, případně hodinky [12].

S rozšířením telefonů disponujících technologií NFC přichází i veliké riziko. Takový telefon totiž může být zneužit jako čtečka platebních karet – v podstatě se z telefonu může stát platební terminál. Proto placení správně nastaveným a zabezpečeným mobilním telefonem a pomocí technologie NFC je aktuálně mnohem bezpečnější, protože zařízení komunikuje pouze v případě, když uživatel provádí platbu. Nemůže být proto zneužit stejně jako bezkontaktní platební karta.

2.2.5.1 NFC v mobilním telefonu

Aktuální situace v České republice je taková, že uživatelé, kteří mají mobilní telefon s operačním systémem Android, již mohou platit pomocí aplikace Google Pay. [16]

Stejně tak konkurenční Apple Pay bylo v České republice spuštěna v únoru 2019. [17]

K tomu, aby tyto platby probíhaly v zařízeních firmy Apple, musí obsahovat tzv. Secure Element (SE). Do češtiny by se tento termín dal přeložit jako bezpečný prvek. V podstatě to ale znamená, že telefon obsahuje integrovaný čip, přesně jako platební karta. K provedení transakce pomocí tohoto čipu se využívá tzv. tokenizace. To je proces, kdy je za pomoci bezpečného prvku vytvořen řetězec – token, který obsahuje informace o platební kartě, které jsou však substituovány náhodnými čísly a následně zašifrovány.

V případě Apple Pay nejsou údaje o kartě uloženy ani v bezpečném prvku telefonu. Tento prvek je izolován od operačního systému telefonu. Při registraci nové karty do aplikace Wallet přeposílá Apple požadavek na poskytovatele karty, který pokud podporuje Apple Pay, vrací identifikátor (Device Account Number - DAN), který je uložen do bezpečného prvku telefonu a Apple k němu nemá přístup. Při transakci se posílá DAN společně s kryptogramem obsahujícím informace o platbě přímo vydavateli karty. [18]

V případě odcizení, či ztráty je uzamčené mobilní zařízení mnohem obtížnější na zneužití, než při ztrátě platební karty. Pro platbu za použití telefonu je třeba se prokázat – v případě Apple Pay existují tři možnosti: Face ID (3D sken obličeje), Touch ID (otisk prstu), nebo zadáním bezpečnostního kódu. Dle dokumentace společnosti Apple je šance chybného odemčení v případě Touch ID 1 ku 50 000. V případě Face ID potom 1 ku 1 000 000. Toto však neplatí pro jednovaječná dvojčata, u kterých tato technologie není ani zdaleka tak spolehlivá. [19]

Společnost Android přistoupila k tomuto problému jinak. Namísto SE používá od verze 4.4 tzv. Host-based Card Emulation (HCE), což je možné volně přeložit jako emulace na bázi hostitele. To znamená, že aplikace emulují chování karty a komunikují přímo s NFC sensorem. [20]

Obdobně jako je tomu u konkurence, při provádění transakce musí být zařízení odemčené. Zařízení mohou používat k autentifikaci otisk prstu, rozpoznávání obličeje, číselný kód, vzor (angl. Pattern) a další.

2.2.6 3D Secure

Three Domain Secure, neboli 3D Secure je bezpečnostní protokol vydaný společností EMVCo, který se využívá při nákupech v internetových obchodech. Tento protokol byl vyvinut jako další bezpečnostní vrstva pro situace, kdy zákazník v e-shopu platí pomocí platební karty. [21]

V praxi to znamená, že při placení je zákazník vyzván k zadání údajů z platební karty a ve chvíli, kdy potvrdí tyto údaje, je přesměrován na stránky své banky, kde je uvedena částka a další náležitosti platby. K provedení platby musí zákazník na stránce banky vyplnit ověřovací kód, který obdrží SMS zprávou do svého mobilního telefonu. Teprve poté je provedena transakce a následně je zákazník přesměrován zpět na stránky obchodu.

Tento způsob autentifikace je velice silný, protože k provedení transakce je potřeba znát nejen údaje z platební karty, ale zároveň mít při sobě i mobilní telefon majitele karty, na který přichází ověřovací kód. Navíc kód je platný pouze v řádu vteřin – maximálně několika málo minut.

Tento protokol má však několik zásadních nevýhod. Nejzásadnější z nich je skutečnost, že se nejedná o povinný standard. Tento protokol využívají pouze větší firmy k zajištění větší bezpečnosti a zamezení nepříjemných situací v případě podvodů. To ale znamená, že pokud útočník získá všechny údaje platební karty, může kartou zaplatit v e-shopu, který tento protokol nevyužívá.

Dalším kritizovaným aspektem je již zmíněné přesměrování na stránky banky. V takové situaci se objevuje nebezpečí phishingu – tedy přesměrování na stránky, které vypadají nerozeznatelně od těch pravých, ale ve skutečnosti jsou podvrhem, který má za účel získat z uživatele citlivé informace – například ověřovací kód.

Nakonec stojí za zmínku uvést, že uživatelé v hůře signálem pokrytých oblastech mohou mít potíže s placením, když v důsledku špatného signálu nemohou obdržet ověřovací SMS v krátkém časovém horizontu.

2.2.7 Bezpečnostní prvky platební karty

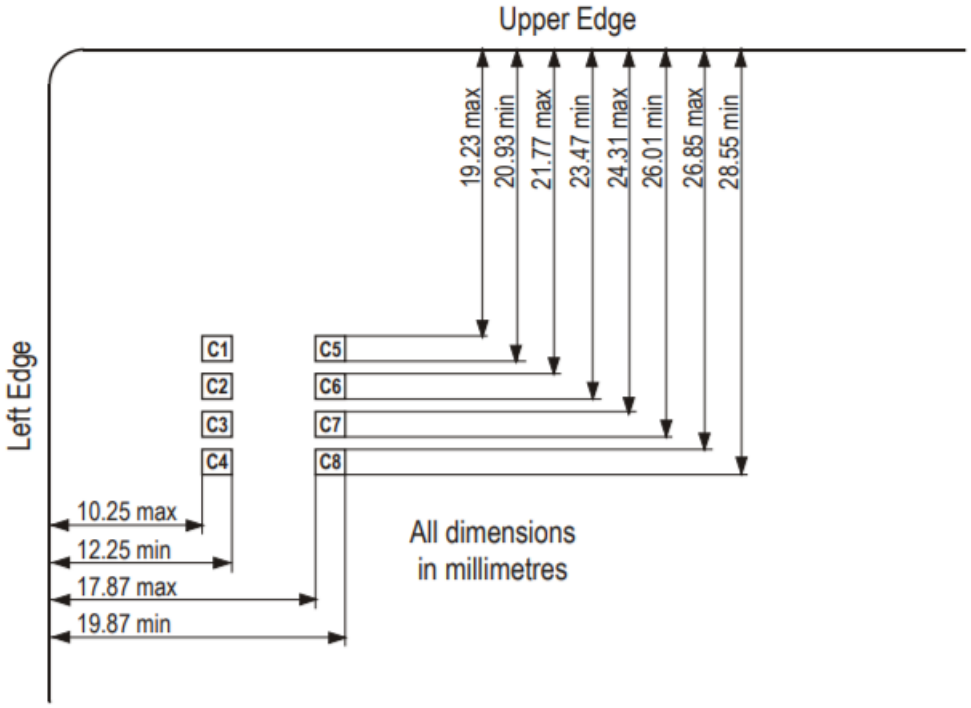
V další kapitole jsou blíže popsány a analyzovány bezpečnostní prvky platebních karet, které jsou využívány při platbách. Jedná se konkrétně o EMV čip, magnetický pásek a CVC kód.

2.2.7.1 EMV čip

Dle dokumentu vydaného společností EMVCo byl EMV čip mezi červencem 2016 a červnem 2017 použit u 58,9% transakcí s přítomnou platební kartou. [22]

Na rozdíl od magnetického pásku, který obsahuje statické informace, elektronický čip funguje jako mikroprocesor, který pro každou transakci vytvoří unikátní řetězec – takzvaný token a následně jsou předávané informace zašifrovány, aby nebylo možné předávané informace zneužít pro další transakce. Díky čipu by mělo být téměř nemožné vytvářet kopii karty, jako tomu bylo u karet s magnetickým páskem, nicméně není to zcela nemožné.

Zároveň pomocí EMV čipu lze provádět i offline transakce, kdy karta vygeneruje zprávu, která je uchována v platebním terminálu a na konci pracovního dne je tato zpráva zpracována.



Obr. 12 Umístění kontaktů na platební kartě
Zdroj: www.emvco.com [23]

Na obrázku 12 výše je znázorněno umístění jednotlivých kontaktů na kartě. Každý kontakt slouží jinému účelu:

C1 – Vstup napájení čipu (VCC)

C2 – Reset (RST)

C3 – Hodinový signál (CLK)

C4 – Nevyužívá se

C5 – Uzemnění (GND)

C6 – Programovací konektor (VPP)

C7 – Vstup a výstup komunikace (I/O)

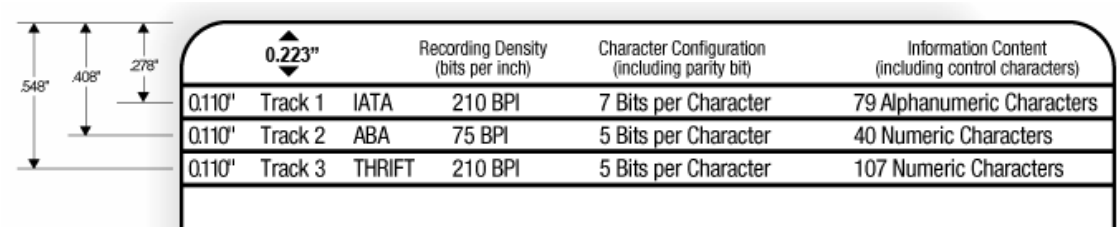
C8 – Nevyužívá se

2.2.7.2 Magnetický pásek

Technologie, která předcházela elektronickým čipům a vznikla již v šedesátých letech. Magnetický pásek složený z malých magnetů obsahuje veškeré informace o platební kartě. Tato informace je však statická, takže se správným vybavením je možné kartu během zlomku vteřiny přečíst a získat všechny údaje.

Tento druh podvodů – tzv. skimming byl v minulosti dosti rozšířený. Útočníci připevnili čtecí zařízení na bankomat společně s malou kamerou, která měla přečíst pin. Následně je možné ukradená data z magnetického pásku použít pro jinou platební kartu a společně s pinem poté kartu zneužít.

Aktuálně v Česku stále ještě není zcela dokončen přechod na čipové platební karty – bohužel se nepodařilo dohledat informaci, do jaké míry jsou magnetické pásky na území České republiky na kartách stále používány. Že ale stále nejsou minulostí, nasvědčuje článek portálu Aktuálně.cz ze září 2018, který popisuje příhodu skimmingu, který se stal českému páru v Americe. [24]



Obr. 13 Charakteristiky a umístění magnetických stop karty
Zdroj: www.q-card.com [25]

Magnetický pásek se skládá z celkem tří stop.
První stopa má délku 79 znaků a obsahuje údaje o kartě, to znamená identifikační číslo karty, jméno a příjmení držitele, datum expirace, servisní kód a CVC
Stopa druhá obsahuje 40 znaků a neobsahuje informaci o jméně držitele.
Na rozdíl od prvních dvou stop, které jsou určené pouze pro čtení, třetí stopa je určena jak pro čtení, tak i pro zápis. Mimo jiné může obsahovat kód země, kód měny, nebo výši autorizované částky pro jednu transakci. [25]

2.2.7.3 Card Verification Code

Kód pro verifikaci karty (CVC, nebo taky CVV) je zpravidla třímístný kód umístěný na líci platební karty. Slouží k provádění takzvaných „card not present" plateb. To znamená při platbě přes internet, kdy není vyžadován pin kód.
Bezpečnostní rizika jsou ovšem poměrně vysoká. Jednou možností je phishing, kdy sám držitel karty vyzradí útočníkovi všechny své údaje o kartě. Dalším způsobem je „opsání" kritických údajů z karty. Právě z tohoto důvodu je umístěn CVC kód na líci karty, aby bylo obtížnější získat všechny údaje potřebné ke zneužití – není to však nemožné. Obzvláště v době, kdy kvalita kamer a fotoaparátů je na tak vysoké úrovni, že schopný útočník může vyfotit obě strany platební karty při placení kartou v obchodě.
Společnost EMVCo se v tomto ohledu snaží zavádět nové normy, které by měly jednotlivé problémy eliminovat. Jedním z nich je 3D Secure, který přidává další vrstvu autentifikace a dalším nástrojem je systém Secure Remote Commerce (SRC), který by měl spravovat a dohlížet na komunikaci mezi zákazníkem, obchodníkem a bankovními institucemi. Specifikace technického frameworku v1.0 byly vydány v listopadu 2017. [26]

2.2.8 Možnosti ochrany platebních karet

V předchozích kapitolách bylo zmíněno několik způsobů, jak útočníci mohou získat údaje o platební kartě, které následně mohou zneužít. Proti takovým útokům je však možné se efektivně bránit. V této kapitole je představeno několik nástrojů k tomu určených.

Tyto způsoby ochrany však nebudou efektivní ve chvíli, kdy nejsou dodržena nejzákladnější pravidla: nikdy nenechávat platební kartu volně ležet – je třeba ji vždy mít u sebe, případně bezpečně uschovanou. Dále pak nikdy nesdělovat údaje z platební karty jiným osobám.

2.2.8.1 Přelepení CVC

Použitím jakékoli neprůhledné samolepky můžeme zamezit přístup k informaci hodnoty CVC. Tím je zamezeno tomu, když by se útočník snažil „opsat“ údaje z platební karty.

2.2.8.2 Ochrana magnetického proužku

Data z magnetického pruhu platební karty není možné přečíst, když je magnetické pole narušeno. Toho může být docíleno například speciální nálepkou, viz obrázek. Tímto způsobem je možné zabránit čtení citlivých údajů, potažmo skimmingu.

Obr. 14 Čtení magnetického pásku speciální nálepkou znemožňuje čtení
Zdroj: www.irozhlas.cz [27]

2.2.8.3 Peněženka či pouzdro zamezující RFID/NFC

Na trhu se již objevují i peněženky, či pouzdra na karty, které obsahují kovové vrstvy, případně kovová vlákna všitá do látky. Tím je zamezeno komunikaci karet nacházejících se uvnitř peněženky. Příkladem výrobců takových peněženek mohou být například Bellroy (bellroy.com), nebo Secrid (secrid.com).

Obr. 15 Peněženka Bellroy zabraňující čtení
Zdroj: www.bellroy.com [28]

2.2.8.4 Jednorázové virtuální karty

Velmi bezpečným řešením při placení na internetu jsou jednorázové virtuální karty. Tato služba funguje takovým způsobem, že uživatel obdrží pouze údaje o platební kartě, které slouží k provedené právě jedné transakce a následně je karta zablokována. Při takové platbě je zamezeno zneužití takové karty a pro každou další transakci získává uživatel nové platební údaje.

Tuto službu nabízí například britská společnost Revolut (revolut.com) za měsíční poplatek. Nevýhodou takové karty je pouze fakt, že není možné použít pro rekurentní platby.

2.2.9 Bezstarostné nakupování online

Na území České republiky je poměrně běžná praxe mít veškeré peníze uložené na běžném účtu. K čerpání těchto peněz se využívá debetní karty, a to jak k nakupování online, tak v obchodech. [29]

V případě zneužití této debetní karty může oběť přijít o své úspory. V této době, kdy za vedení bankovního účtu již není účtován poplatek, a existují rychlé platby, nic nebrání, aby každý měl bankovní účty dva - případně více.

Myšlenka je taková, že karta primárního účtu, který obsahuje větší částku, nebude využívána. Namísto toho je z primárního účtu převedena menší částka na sekundární účet, který obsahuje menší část peněz pro potřebu nakupování online.

Běžně uchovávají společnosti citlivé údaje z platebních karet, které v případě útoku skončí v rukou útočníků. [30]

2.2.10 Replay a Relay útoky na NFC

Se stále sofistikovanějšími ochrannými prvky přichází útočníci s novými způsoby, jak tyto ochrany prolomit, či obejít.

DEFCON je název konference hackerů, která je každoročně pořádána v Las Vegas, Nevadě. Následující odkaz vede na přednášku z prosince 2018, kde bezpečnostní analytik Salvador Mendoza představuje Relay a Replay útoky na NFC za použití relativně levných zařízení a open-source software:

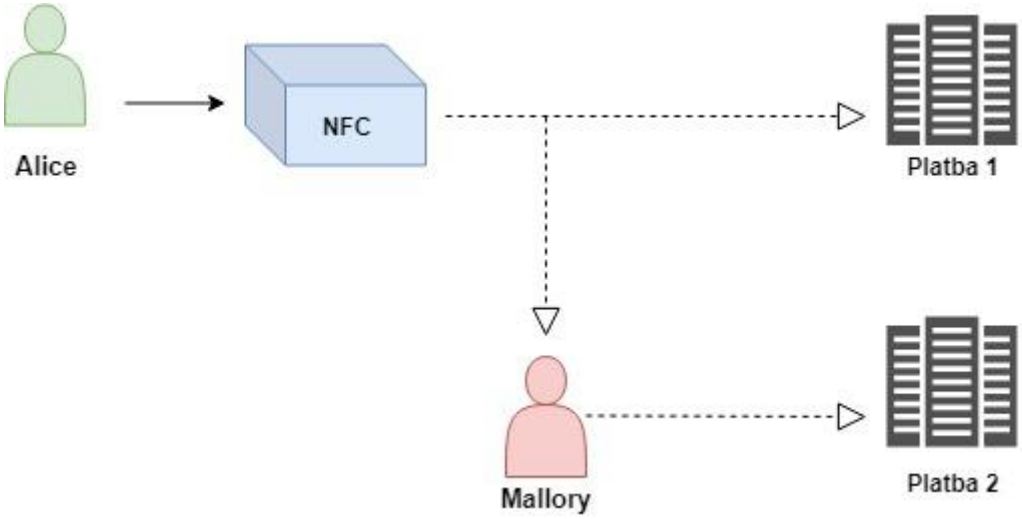
https://www.youtube.com/watch?v=MVU3gbPnk0g

2.2.10.1 Replay útok

Koncept tohoto druhu útoku je takový, že pomocí zařízení, které slouží jako emulátor a zároveň čtecí zařízení je zachycen token, který je validní a je možné jej použít k zaplacení později a na jiném místě. Komunikaci mezi terminálem a kartou vždy zahajuje terminál.

Postup:

1. Emulátor je na dosah platební karty a vysílá požadavek – token - na ověření platební karty
2. Karta odpovídá na požadavek validní odpovědí
3. Uměle je na tokenu snížena míra bezpečnosti na úroveň platby magnetickým proužkem
4. Jiný terminál v jiný čas zahajuje komunikaci s emulátorem, který odpovídá dříve získanou validní odpovědí z karty
5. Transakce úspěšně dokončena



Obr. 16 Schéma replay útoku
Zdroj: vlastní tvorba

2.2.10.2 Relay útok

Jedná se o útok, kdy je vytvořen most v komunikaci mezi terminálem a kartou – například pomocí dvou chytrých telefonů, které s mezi sebou komunikují pomocí wi-fi a zároveň komunikují s kartou a terminálem. Cílem je odchytávat posílané zprávy – nijak nejsou upravovány. Hlavní komplikací je zamezit časové prodlevě v komunikaci.

V praxi by tento scénář mohl vypadat tak, že útočník se přiblíží s telefonem ke kartě oběti a proběhne transakce, za pomoci mostu vytvořeného druhým telefonem a terminálem. Terminál sám o sobě by vypadal velice podezřele.

Tento druh útoku je efektivně využíván i zloději aut, kdy k odemčení auta je využitý stejný princip NFC, jen s větším dosahem[7]. [31]

Obr. 17 Schéma relay útoku
Zdroj: vlastní tvorba

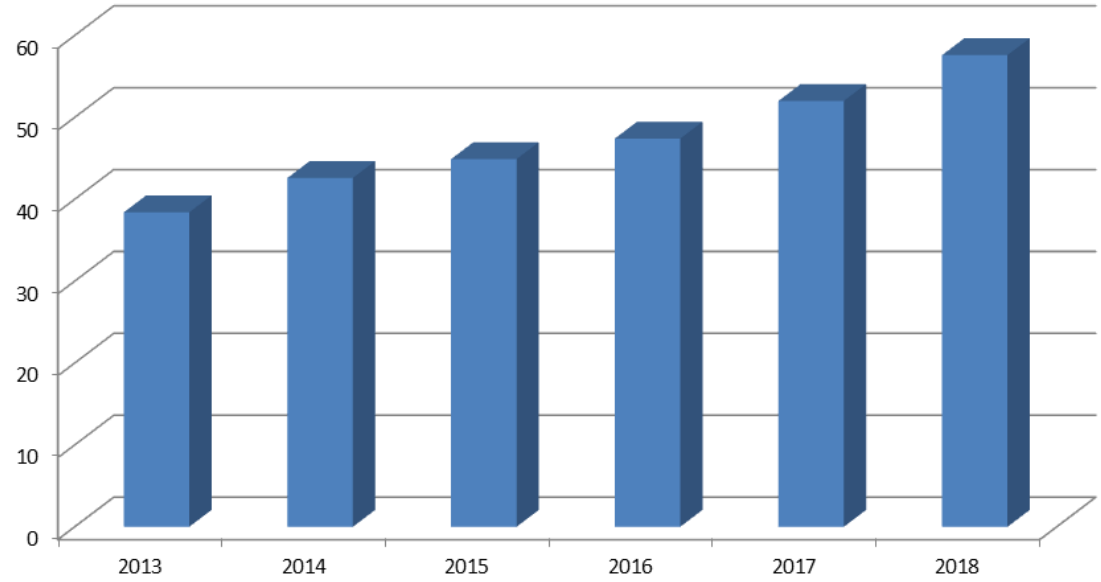
[7] Key Fob Relay Hack Attack Explained - https://www.youtube.com/watch?v=D_3lgxMwrWI

2.3 Internetové bankovnictví

Pro práci s penězi uloženými v bance a se zvyšující se informatickou gramotností zvyšuje i počet českých obyvatel, kteří využívají k manipulaci internetové bankovnictví. Využívá se nejen k platbě složenek, ale i služeb a zboží a to i staršími občany.

Internetové bankovnictví nabízí mnohem větší komfort a úsporu času, než placení osobně, či složenkou.

Aktuálním trendem několika posledních let je i mobilní bankovnictví, kdy ke správě financí stačí mobilní telefon připojený k internetu. Přestože se jedná o relativně bezpečný způsob platby, je potřeba dodržovat bezpečnostní zásady z důvodu minimalizace rizik.



Obr. 18 Podíl uživatelé internetového bankovnictví v ČR 2013-2018
Zdroj: www.czso.cz [32]

Podíl uživatelů internetového bankovnictví v České republice rok od roku roste. Zatímco v roce 2013 využívalo internetové bankovnictví 38 % Čechů, v roce 2018 už to je 58 % což je 70 % z těch, kteří využívají internet. V používání této služby jsou aktivnější muži (59 %) než ženy (56 %). [32]

2.3.1 Připojení k internetu

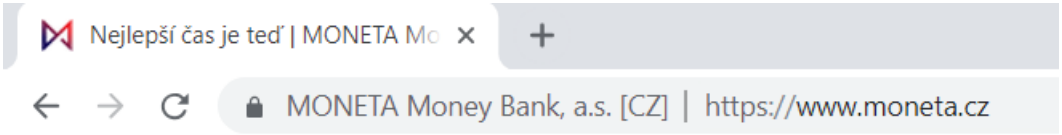
Mezi dvě základní podmínky pro práci s internetovým bankovnictvím patří důvěryhodný počítač – případně mobilní telefon - s aktivní antivirovou ochranou a bezpečné připojení k internetu. Důvěryhodný počítač, nejlépe vlastní, z toho důvodu, že na cizím zařízení může být – i úmyslně – aktivní software na čtení obrazovky, případně klávesových vstupů, a to za účelem získání citlivých údajů o bankovním účtu a heslu.

Další podmínkou pro využívání internetového bankovnictví je přístup k internetu. Prvním a základním stupněm ochrany je používání zabezpečené wi-fi sítě. Problém při využívání veřejných wi-fi je v tom, že schopný uživatel dokáže odchytávat zprávy, které se posílají mezi počítačem a wi-fi routerem. Schopnější uživatel potom může takové zprávy nejen číst, ale také je modifikovat ve vlastní prospěch. Proto druhým naprosto základním pravidlem pro práci s citlivými daty je bezpečná wi-fi.

2.3.1.1 HTTPS

Hypertext Transfer Protocol Secure je internetový protokol zajišťující šifrovanou komunikaci pro přenášení dat z webových stránek – například stránek internetového bankovnictví. HTTPS je složen ze dvou protokolů: HTTP, který umožňuje přenášet data z webového serveru do prohlížeče počítače a šifrovacího protokolu SSL nebo TLS. Za pomoci šifrovacího protokolu jsou přenášená data upravena tak, aby nebylo možné je zneužít. Je tedy zajištěna autentičnost dat a předchází se tak útokům typu „man in the middle“ a „phishing“.

Webové stránky používající protokol HTTPS je možné poznat v internetovém prohlížeči díky dvěma ukazatelům: v odkazu je použit řetězec https:// a také je u odkazu zpravidla zobrazena ikonka zámku, stejně jako na obrázku 19 níže.



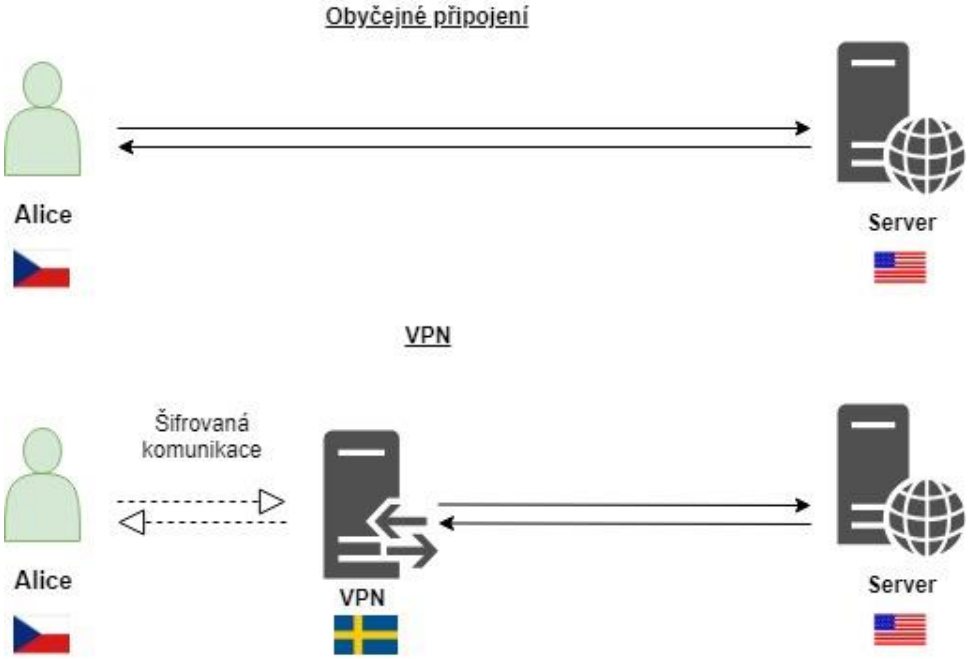
Obr. 19 Vzhled HTTPS v internetovém prohlížeči
Zdroj: vlastní tvorba

2.3.1.2 VPN

Virtual Private Network je další způsob, jak je možné ochránit data při komunikaci na internetu. Jedná se o službu, která je zpravidla placená a poskytuje uživateli možnost vytvoření bezpečného šifrovaného kanálu mezi počítačem a VPN serverem (virtuální soukromá síť). Tyto servery jsou umístěny v různých zemích světa a vysílají požadavky, které obdržely z počítače klienta a následně vrací odpovědi. Tento způsob komunikace umožňuje nejen zašifrování veškeré komunikace, ale zároveň také skrývá geografickou polohu klienta.

Tímto způsobem je tedy možné „obejít" některé polohové restrikce. Například velký čínský firewall. Z Číny není možné se připojit například na Facebook, či Twitter. VPN je možné používat i v mobilním telefonu.

Mezi nevýhody používání VPN patří nižší rychlost v kombinaci s vyšší prodlevou. Je to z důvodu „delší cesty", kterou musí zpráva urazit a šifrování a dešifrování komunikace. Jako nevýhoda se může zdát i poplatek za tuto službu. To je však cena za zachování soukromí. Při provozování VPN důvěřuje klient poskytovateli služby. Je možné najít i bezplatně VPN, ale je třeba počítat s tím, že takové služby nemusí být bezpečné. Proto je potřeba vybírat spolehlivého a profesionálního poskytovatele služby.



Obr. 20 Porovnání obyčenejného připojení a připojení s VPN
Zdroj: vlastní tvorba

2.3.2 Bezpečnostní heslo

Přestože je použití samotného přihlašovacího jména a hesla považováno za nejméně bezpečnou metodu přihlášení, je, pravděpodobně díky své jednoduchosti, používáno nejčastěji. Toto zabezpečení používá 96 % osob, které používají internet. [32]

Pro vyšší úroveň zabezpečení je u internetových bank zpravidla možné použít takzvanou dvoustupňovou autentifikaci. Ta využívá k přihlášení nejen kombinaci správného jména a hesla, ale navíc je po přihlášení uživateli zaslána SMS zpráva na jeho mobilní telefon s číselným kódem, který je platný pouze několik minut. Pokud je tento kód zadán správně, teprve potom může uživatel vstoupit do internetového bankovnictví.

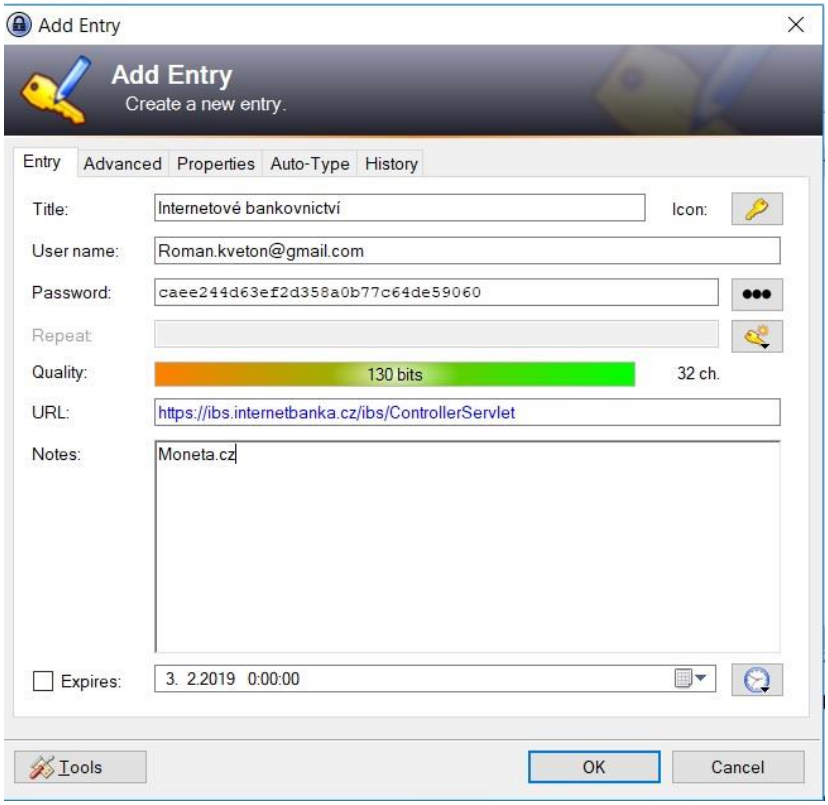
Pro přihlášení do internetového bankovnictví některé banky využívají také elektronický identifikační certifikát uložený v počítači či na externím zařízení. Tento způsob zabezpečení používá 16 % osob, což je pětina uživatelů internetu. [32]

Zásady pro vytvoření silného hesla jsou všeobecně známé a často je možné, že při vytváření hesla jsou některé podmínky povinné a bez jejich splnění není možné pokračovat. Opakování je však matka moudrosti – následuje seznam zásad:

- Délka hesla by měla být minimálně 8 znaků, ale čím delší, tím silnější
- Řetězec by měl obsahovat velké písmeno, malé písmeno, číslo, a pokud je to možné i speciální znak
- Heslo by nemělo obsahovat slovo ze slovníku, nemělo by obsahovat uživatelské jméno, rodné číslo, nebo datum narození. Zkrátka by nemělo mít logický vztah k uživateli
- Jedno heslo by nemělo být použito pro přístup na více stránek
- Bezpečnostní heslo by mělo být pravidelně měněno

Pro splnění všech podmínek by ale každý uživatel musel mít vynikající paměť. Tak tomu však zpravidla není a proto je výhodné využít software na správu hesel. Při použití podobného nástroje si stačí pamatovat pouze jedno heslo pro přístup do hesláře uloženého v počítači. Příkladem takového software je KeePass

(https://keepass.info/). Ukázka náhodně vygenerovaného silného hesla je na obrázku 21 níže. Pro uchovávání hesel na více zařízeních a více platformách se hodí spíše aplikace 1Password (https://1password.com/), která je sice placená, ale podporuje Mac, iOS, Windows, Android, Linux a Chrome OS.



Obr. 21 Vytváření nového záznamu hesla v aplikaci KeyPass
Zdroj: vlastní tvorba

2.3.3 Systémy pro bezhotovostní transakce

Na území České republiky se pro mezibankovní platební styk používá systém CERTIS (Czech Express Real Time Interbank Gross Settlement System), který je provozovaný Českou národní bankou. Jedná se o jediný systém v České republice, který zpracovává platby v českých korunách. Jeho provoz byl zahájen v březnu 1992. [33]

Zpravidla trvalo převedení peněz z jednoho účtu na druhý jeden den. Nicméně v posledních měsících se již objevuje možnost okamžitého převodu peněz mezi bankovními účty. Okamžité platby jsou aktuálně zpoplatněny – například Airbank nabízí okamžitou platbu za poplatek 1kč za transakci. [34]

Pro mezibankovní komunikaci na světové úrovni – to znamená mezinárodní platby – se používá systém SWIFT (Society for Worldwide Interbank Financial Telecommunication). Ten slouží k odesílání a přijímání úhrad v cizí měně. SWIFT používá více než 200 zemí světa. Vzniknul v roce 1973 a postupem času ve většině bank nahradil dálnopisové zprávy. Zasílání zpráv je v rámci standardu ISO 20022, což je platforma, která definuje bezpečný způsob zasílání a formu posílaných zpráv. [35]

2.3.3.1 Průběh transakce v rámci CERTIS

Následuje přehled kroků, které jsou prováděny v rámci každého mezibankovního převodu peněžních prostředků v korunách českých.

1. **Plátce** - Zadá příkaz ke standardní nebo spěšné (expresní) úhradě své bance – přímé bankovnictví, písemný příkaz (sběrný box, přepážka).
2. **Banka plátce** - Vloží písemný příkaz k úhradě do interního systému banky. Příkaz k úhradě z přímého bankovnictví (telefonní bankovnictví, homebanking, internet, mobil) je vložen přímo do interního systému banky. Zpracuje příkaz k úhradě ve svém interním systému – zajistí odepsání prostředků z účtu plátce. Vytvoří a odešle data s úhradou do systému CERTIS za účelem připsání platby na účet banky příjemce. Banka plátce je povinna připsat částku převodu ve prospěch účtu banky příjemce v systému CERTIS nejpozději do konce následujícího pracovního dne po okamžiku přijetí platebního příkazu (okamžik přijetí definuje banka plátce ve smluvních podmínkách s klientem).
3. **Systém CERTIS (ČNB)** - Zajistí příjem a zpracování dat s úhradou od banky plátce. V systému CERTIS dojde v účetním dni vždy ke zpracování všech přijatých plateb (nekryté jsou vráceny bance plátce). Provede kontrolu krytí na straně banky plátce a zajistí převod prostředků z účtu banky plátce na účet banky příjemce. Platba je připsána na účet banky příjemce jen tehdy, má-li banka plátce na svém účtu v systému CERTIS dostatek prostředků: prioritní úhrada obvykle do 10 vteřin po přijetí dat, standardní úhrada v průběhu několika minut (při velkém množství plateb může platba čekat ve

vstupní frontě). Systém CERTIS je schopen zaúčtovat cca 4 milionu plateb za hodinu. Účtování probíhá v pracovních dnech od 0:00 hod. do 16:00 hod. Vytvoří a odešle data s úhradou bance příjemce. Informace o připsaných platbách jsou odesílány bance příjemce v průběhu účetního dne každou hodinu, spěšné platby jsou odesílány každých 10 minut.

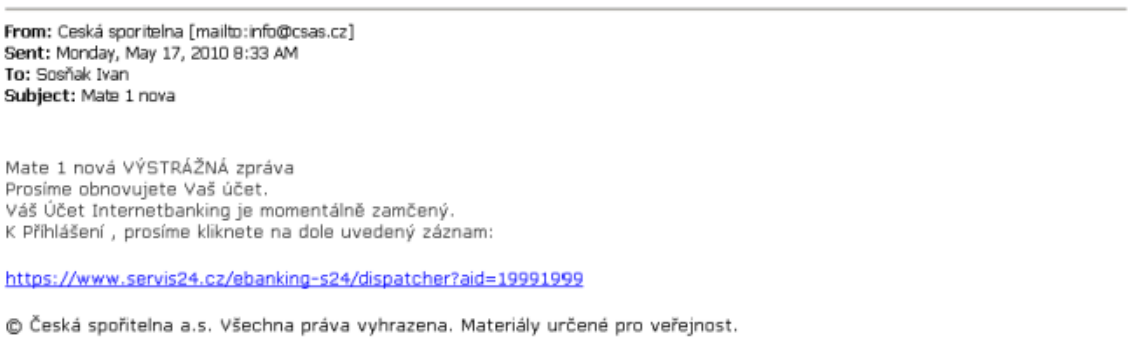
4. **Banka příjemce** - Provede příjem a zpracování dat s úhradou ze systému CERTIS. Připíše prostředky na účet příjemce. Banka příjemce je povinna připsat částku převodu ve prospěch účtu příjemce neprodleně poté, kdy byla částka převodu připsána na její účet v systému CERTIS.
5. **Příjemce** - Prostředky jsou k dispozici po připsání částky na účet příjemce [36]

2.3.4 Druhy útoků a bezpečnostních hrozeb

V následující kapitole jsou představeny nejběžnější druhy útoků. Bude vysvětleno, jakým způsobem fungují, a dále bude uvedeno, jakým způsobem je možné se proti nim bránit a předcházet jim.

2.3.4.1 Phishing a pharming

Phishing byl již v práci zmíněn, nicméně se jedná o opravdovou hrozbu a proto je třeba ji znát. Jedná se o druh podvodného jednání, kdy se útočník snaží vylákat od uživatele citlivé údaje, například jméno a heslo do internetového bankovnictví.
Může mít více podob. Nejčastěji jako podvodný email viz ukázka na obrázku 22 níže. Může se však jednat i o vyskakující okno na stránce, kde je požadováno jméno a heslo.
Samotné slovo phishing vzniklo spojením dvou anglických výrazů „fishing— a „phreaking“.



From: Ceská sporitelna [mailto:info@csas.cz]
Sent: Monday, May 17, 2010 8:33 AM
To: Sosňak Ivan
Subject: Mate 1 nova

Mate 1 nová VÝSTRÁŽNÁ zpráva
Prosíme obnovujete Vaš účet.
Váš Účet Internetbanking je momentálně zamčený.
K Přihlášení , prosíme kliknete na dole uvedený záznam:

https://www.servis24.cz/ebanking-s24/dispatcher?aid=19991999

© Česká spořitelna a.s. Všechna práva vyhrazena. Materiály určené pro veřejnost.

Obr. 22 Ukázka phishingového útoku - podvodný email
Zdroj: www.bezpecnyinternet.cz [37]

Metoda pharmingu má stejný cíl, ale využívá jinou metodu k podvržení stránek. Nepoužívá mail, ale útočník napadne DNS[8] server, který používá uživatel. Ve chvíli, kdy se podaří útočníkovi změnit záznamy na DNS serveru, tak ve chvíli napsání adresy obětí do vyhledávače je tato nic netušící osoba přesměrována na jinou stránku, která je vzhledem nerozeznatelná od originálu.

Ochrana vůči phishingu je zřejmá – v žádném případě neklikat na podezřelé odkazy, které se objevují v emailech. Dále pak vždy zkontrolovat, kam je psáno bezpečnostní heslo. Dalším způsobem ochrany jsou antivirové programy, které již obsahují anti-phishingovou ochranu. Mezi placené patří například Eset (www.eset.com). Mezi bezplatné patří například Avast (www.avast.com). Pro co možná nejvyšší ochranu je potřeba tyto programy pravidelně aktualizovat – ostatně stejně jako webový prohlížeč, nebo operační systém počítače.

S odhalením pharmingu to pro běžné uživatele může být obtížnější, nicméně každý padělek internetového bankovnictví musí obsahovat nějakou chybu, případně nesrovnalost, která uživatele zarazí. Může se jednat například o chybovou hlášku po přihlášení, že internetové bankovnictví je z nějakého důvodu nefunkční. V takovém případě by měl člověk zpozornět a co nejdříve z jiného počítače zkusit přistoupit do internetového bankovnictví, změnit si bezpečnostní heslo a upozornit banku na svou situaci. Dalším bezpečnostním opatřením by měla být již

[8] Domain Name Systém slouží – zjednodušené řečeno - jako překladač. Když uživatel napíše webovou adresu do prohlížeče, tak DNS tuto adresu přeloží na IP adresu, která je potřebná pro komunikaci s danou stránkou.

zmíněná dvoustupňová autentifikace – a to jak při přihlašování na stránky banky, ta při schvalování platebního příkazu.

2.3.4.2 Keylogger

Nebezpečný spyware, který snímá a následně odesílá útočníkovi informace o tom, jaké klávesy byly na klávesnici stisknuty, se nazývá keylogger. Jedná se o další způsob, jak zjistit citlivé informace, jako heslo, nebo údaje kreditní karty.

Keyloggerů je více druhů – nemusí se jednat pouze o škodlivý software. Může se jednat také o hardware, který antivirové programy nemohou zachytit. Takové zařízení je umístěno jako nástavec na USB kabel klávesnice a zapojeno do počítače. Při dostupném připojení k internetu může data nejen ukládat na svou paměť až 8GB, ale může data posílat i do mailu útočníka.

Obr. 23 Vzhled keyloggeru a kde může být umístěn
Zdroj: www.spyobchod.cz [38]

Ochranou před software keyloggery (může se jednat i o snímání obrazu) je antivirus odhalující tento druh špehujících aplikací – například již zmíněný Avast, či Eset. Další vrstvou ochrany je i v tomto případě dvoustupňová autentifikace.

2.3.4.3 Hoax

Dalším druhem škodlivých, nebo nebezpečných zpráv je takzvaný hoax. V minulosti se hoax šířil výhradně mailem, nicméně je možné se s ním aktuálně setkat i na sociálních sítích. V podstatě se jedná o nepravdivou zprávu, která varuje před nebezpečím, nebo je vyžadována pomoc a je požadováno, aby byla zpráva předána co nejvíce dalším lidem.

Ahoj Jsem Mark, ředitel Facebooku.

Ahoj všichni, zdá se, že všechna varování jsou skutečná Použití Facebooku bude stát za peníze. Pokud odešlete tento řetězec na 18 odlišných od vašeho seznamu, vaše ikona bude modrá a bude zdarma pro vás. Pokud mi nevěříte, zítra v 18:00 Facebook bude uzavřen a otevřít ji budete muset zaplatit. To je vše podle zákona. Tato zpráva má informovat všechny uživatele, že naše servery byly v poslední době velmi přetížené. Žádáme vaši pomoc při řešení tohoto problému. Požadujeme, aby naši aktivní uživatelé předali tuto zprávu každému uživateli ve vašem seznamu kontaktů, aby potvrdili naši aktivní uživatelé Facebooku. Neodesíláte-li tuto zprávu všem vašim kontaktům na facebook, váš účet zůstane neaktivní s důsledkem ztráty všech vašich kontaktů bez přenosu této zprávy. Váš SmartPhone bude aktualizován během dalších 24 hodin, bude mít nový design a novou barvu pro chat. Vážení uživatelé Facebooku, budeme dělat aktualizaci pro Facebook od 23:00 hod. až do dnešního dne. Pokud toto neodesíláte všem vašim kontaktům, bude aktualizace zrušena.

Nebudete mít možnost chatovat se zprávami ve facebooku. Budete muset zaplatit kurz, pokud nejste častým uživatelem. Pokud máte alespoň 10 kontaktů, pošlete tuto SMS a logo se změní na červenou, což znamená, že jste uživatel Potvrdil ... Dokončíme to zdarma. Zítra začnou shromažďovat zprávy pro Facebook na 0,37 centu. Předat tuto zprávu více než vašim 9 kontaktům a bude vám zdarma pro vás. Sledujte a míč se změní na zelenou. Udělejte to a uvidíte, že Facebook je nyní zdarma. Posílejte na 10 lidí, abyste znovu aktivovali službu bez nákladů. [39]

Proti hoaxu existuje jediná ochrana a tou je zdravý rozum. Taková zpráva bude pravděpodobně obsahovat větu typu „Přepošlete toto co nejvíce lidem“. Hoax je totiž stejně jako phishing druh sociálního inženýrství, kdy se útočník v lepším případě snaží příjemce pobavit, v horším případě vylákat údaje z kreditní karty pro příspěvek na opuštěné psy, nebo před zpoplatněním Facebooku . Následně pak tuto zprávu přeposlat všem z kontaktního listu v dobré víře, že pomocí několika kliknutí budou všichni varováni a přitom oběť plní útočníkovo přání – rozšířit útok dále.

2.3.5 Internetové bankovnictví v mobilních telefonech

Na mobilní telefony bylo v minulosti nahlíženo jako na zařízení, která disponují spoustou funkcionalit a jsou bezpečná. Že by se mohl objevit virus, bylo nepředstavitelné. Až do roku 2004, tehdy vzniknul první virus – Cabir. Tento virus byl vytvořen skupinou 29a a sloužil k ověření konceptu, že mobilní telefony mohou být napadnuty obdobně jako počítače. V té době napadal Nokie s operačním systémem Symbian. [40]

Doba pokročila a telefony nacházejí další využití – například v mobilním bankovnictví. To je nová motivace pro hackery, kteří využívají slabých míst. Aktuálně jsou nejrozšířenější dva operační systémy mobilní telefonů – jsou jimi Android, který měl v roce 2017 podíl na trhu mobilních zařízení 86% a iOS s podílem 14%. [41]

Mezi obecné příznaky napadení telefonu škodlivým programem patří:

- Vysoká spotřeba dat
- Časté výpadky aplikací
- Nadměrná spotřeba baterie
- Přehřívání telefonu

2.3.5.1 Android

Operační systém Android je open-source, což znamená, že na zdrojový kód může nahlížet kdokoli. Potenciální útočník může nalézt chyby, nebo slabá místa a těch zneužít. Aplikace je možné získat na více různých místech – nejen na oficiálním Google Play. To může být problém v případě, kdy uživatel nainstaluje neprověřený program, který je škodlivý. Při instalaci nových aplikací je též důležité zpozornět při udělování práv pro aplikace. Detekováním podezřelých požadavků lze předejít problémům. Například pokud by aplikace o počasí žádala o přístup k fotografiím, něco je nejspíš špatně.

Zkušenější uživatelé na svých zařízeních provádí takzvaný root. Tím získají nejvyšší oprávnění, což může mít své výhody, ale i nevýhody. Výhodou je přístup ke všem souborům, takže je možné odebrat nechtěné aplikace, které do zařízení vložil výrobce. Možnost přetaktování kvůli zvýšení výkonu přístroje. Dále je možné

využívat některé aplikace, které pro chod root potřebují. Na druhou stranu toto je i největší nevýhodou a rizikem, protože programy s nejvyšším oprávněním mohou v telefonu provést cokoli. Při mazání nechtěných souborů také může dojít ke smazání klíčových souborů, bez kterých nebude zařízení fungovat.

2.3.5.2 iOS

Oproti Androidu, aplikace pro iOS lze získat pouze z jednoho místa a tím je oficiální App Store. Pro vývoj aplikací a jejich vydání se musí vývojář registrovat pod svou identitou a každá aplikace je prověřena než je vydána do veřejného provozu.
Dalším bezpečnostním prvkem je takzvaný sandbox. Ten zajišťuje, že aplikace nemůže dělat změny v nastavení telefonu, nemá přístup k souborům telefonu, takže nemá možnost je číst a ani modifikovat. Výraz sandbox je možné přeložit jako pískoviště, které také zabraňuje písku, aby se nedostal, kam nemá. [18]
iOS je díky těmto opatřením mnohem bezpečnější, než Android. Výjimkami jsou pak případy, kdy vlastník provede na telefonu takzvaný Jailbreak. Jedná se o úpravu software telefonu, po které je možné do telefonu instalovat neoficiální – a tedy potenciálně nebezpečné aplikace.

2.3.5.3 Ochrana

Při ochraně mobilního telefonu momentálně již platí stejné podmínky jako při ochraně počítače. Pro udržení co nejvyšší míry zabezpečení je potřeba pravidelně instalovat aktualizace jak operačního systému, tak jednotlivých aplikací. Neinstalovat neznámé, neprověřené a pochybné aplikace – pouze z důvěryhodných zdrojů. Používat antivirovou a antispywarovou ochranu.

2.4 Kryptoměny

Hitem posledního desetiletí a nejmladším platidlem v moderní společnosti jsou takzvané kryptoměny (angl. cryptocurrency). Jedná se o digitální – tudíž nehmotnou, decentralizovanou měnu, kde vlastník musí znát tajný klíč pro to, aby mohl platidlo použít. K vypracování této kapitoly byla z velké části využita kniha Kryptoměny vydaná Janem Lánským v roce 2018 [42]. Tato kniha vysvětluje principy, stručně shrnuje historii a analyzuje bezpečnost tohoto platidla. Dle webu CoinLore aktuálně existuje již přes 2000 kryptoměn v celkové hodnotě přesahující 174 miliard dolarů. [43]

Kryptoměna je systém, který splňuje všechny následující podmínky:

- Systém nepotřebuje centrální autoritu, distribuovaně dosahuje shody o svém stavu.
- Systém uchovává přehled o jednotkách dané kryptoměny a jejich vlastnictví.
- Vlastnictví jednotek kryptoměny se prokazuje výhradně kryptograficky.
- Systém definuje, zda mohou vznikat nové jednotky kryptoměny. Pokud mohou vznikat nové jednotky kryptoměny, systém definuje okolnosti jejich vzniku a způsob určení vlastnictví těchto nových jednotek.
- Systém umožňuje provádět transakce, ve kterých dochází ke změně vlastnictví jednotek kryptoměny. Pokyn k provedení transakce může vydat pouze entita, která prokáže aktuální vlastnictví těchto jednotek.
- Pokud jsou současně zadány dva rozdílné pokyny ke změně vlastnictví stejných jednotek kryptoměny, systém provede nejvýše jeden z nich. [42]

Za velikou popularitu kryptoměn mohou jejich klíčové vlastnosti. Ty hlavní jsou v následujících odstavcích rozvedeny.

Decentralizace – to znamená, že platební systém nemá centrální autoritu (banky), které by prováděly transakce. Transakce probíhá v síti počítačů, které jsou si rovny (peer-to-peer). Díky tomu jsou transakce velmi levné. Zároveň to mimo jiné znamená, že není možné uměle upravovat hodnotu jako v případě fiat měn.

Hodnota závisí na důvěře účastníků obchodu, a čím více je akceptována, tím více roste hodnota kryptoměny.

Anonymita a pseudoanonymita – v době, kdy soukromí a utajování informací je čím dál obtížnější nabízí některé kryptoměny naprostou anonymitu. Ať už se jedná o ochranu osobních údajů, nebo o skrytí identity z důvodu nezákonné aktivity, je tato vlastnost jednou z vyhledávaných vlastností při provádění finanční transakce. V některých případech je míra anonymity záměrně zvyšována, respektive snižována – to je přiblíženo v další kapitole.

Bezpečnost – Díky principům kryptografie je prakticky nemožné odcizit jednotky kryptoměny útokem hrubé síly. Při správné manipulaci jsou tedy rizika krádeže minimální. Pouze v případě ovládnutí většiny sítě je možné zpětně upravit informaci v transakci - na kterou adresu jsou jednotky měny převáděny.

2.4.1 Bitcoin

První kryptoměnou se stal Bitcoin. První oficiální zmínky o Bitcoinu jsou ze srpna roku 2008, kdy dosud neznámá osoba, případně skupina osob odpovědných za vyvinutí Bitcoinového systému vystupující pod pseudonymem Satoshi Nakamoto odeslala email s popisem tohoto systému Adamu Backovi (autoru důkazu prací). Tehdy byla zároveň zaregistrována internetová doména bitcoin.org. Z principu Bitcoinu následně vzešly další kryptoměny.

Vůbec první nákup reálné věci proběhl 22. 5. 2010 a to zasláním 10 000 bitcoinů za dvě pizzy v hodnotě 50 dolarů. Aktuální kurz v dubnu 2019 je 5 300 dolarů za jeden bitcoin. Jak je tedy vidět, cena bitcoinu postupem času rostla. [42]

Historicky nejvyšší hodnotu měl bitcoin dne 17. 12. 2017, kdy se hodnota jednoho bitcoinu pohybovala okolo 20 000 dolarů. Volatilita je nezpochybnitelná vlastnost kryptoměn, pro kterou je mnoha odborníky tolik kritizována a mnoha investory tolik vyhledávána. Kolísání ceny je vidět na obrázku 24 níže. [42]

Obr. 24 Vývoj kurzu Bitcoinu 2013-2019
Zdroj: www.coinmarketcap.com [44]

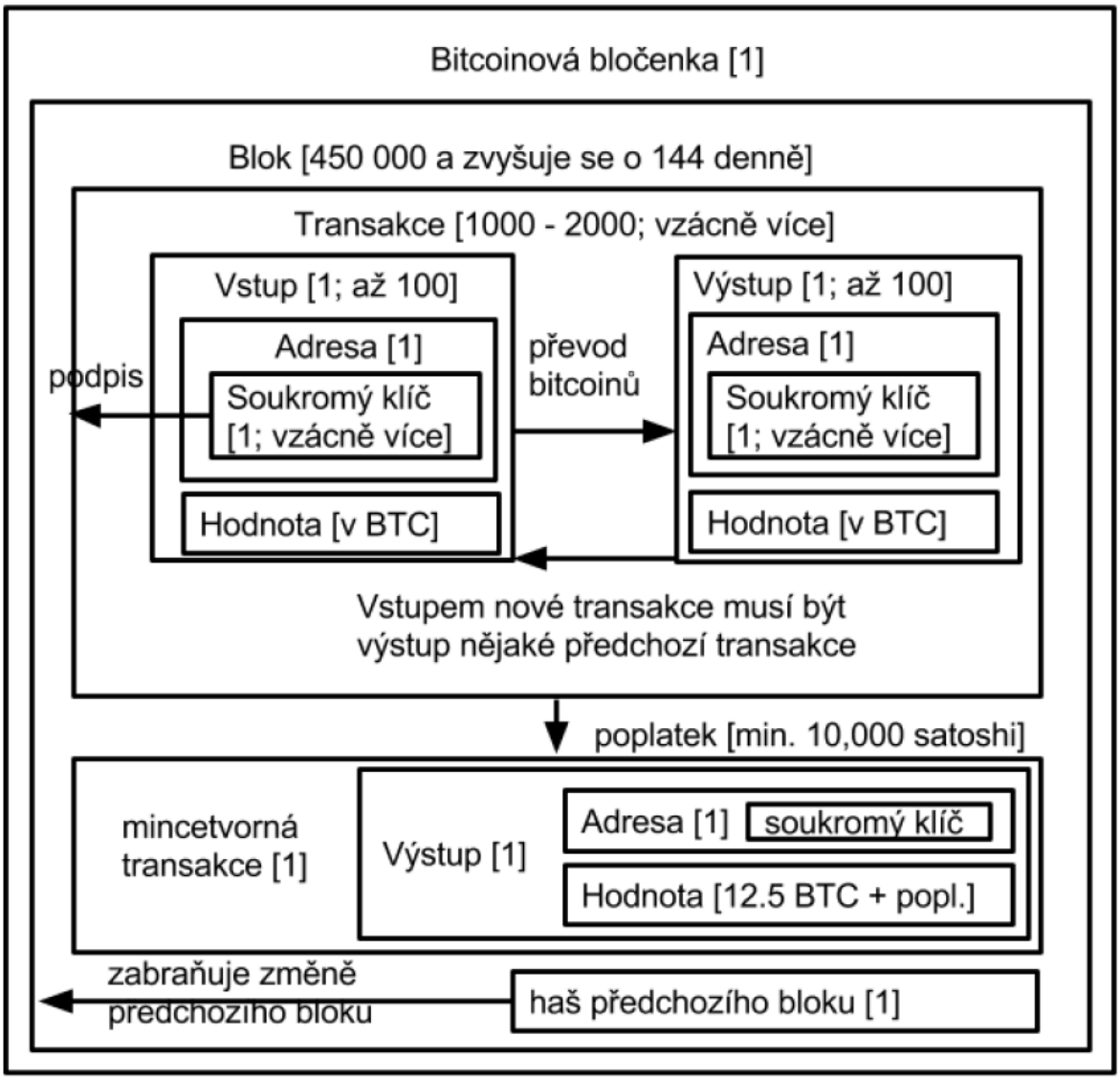
Množství bitcoinů není neomezené – celkové množství je nastaveno na 21 milionu bicoinů. Aktuálně je v oběhu více než 17,5 milionu, což znamená, že „vytěženo" je již více než 80% celkového objemu. Přesto je však odhadováno, že celkové množství bude vytěženo v roce 2140. Je to z toho důvodu, že každé čtyři roky se odměna za těžení snižuje na polovinu. [42]

Menší jednotkou bitcoinu je tzv. satoshi. Každý bitcoin se skládá ze sta milionů satoshi.

Soukromý klíč je 256 -bitové náhodné číslo. To si lze představit jako 256 hodů mincí, kdy každý hod může nabývat hodnoty 1 či 0. Soukromý klíč je tajné heslo, kterým se je nutné prokázat při provádění transakce. Ve chvíli, kdy je informace soukromého klíče ztracena, je vlastnictví bitcoinů taktéž ztraceno. Neexistuje žádný způsob, jak bitcoiny získat zpět. [42]

Veřejný klíč je odvozený ze soukromého klíče metodou kryptografie eliptických křivek. Tento proces je pouze jednosměrný.

K provedení transakce je třeba znát oba veřejné klíče a částku, která je převáděna. Převáděná částka je zmenšena o poplatek, který dostávají uzly, které transakci realizují.

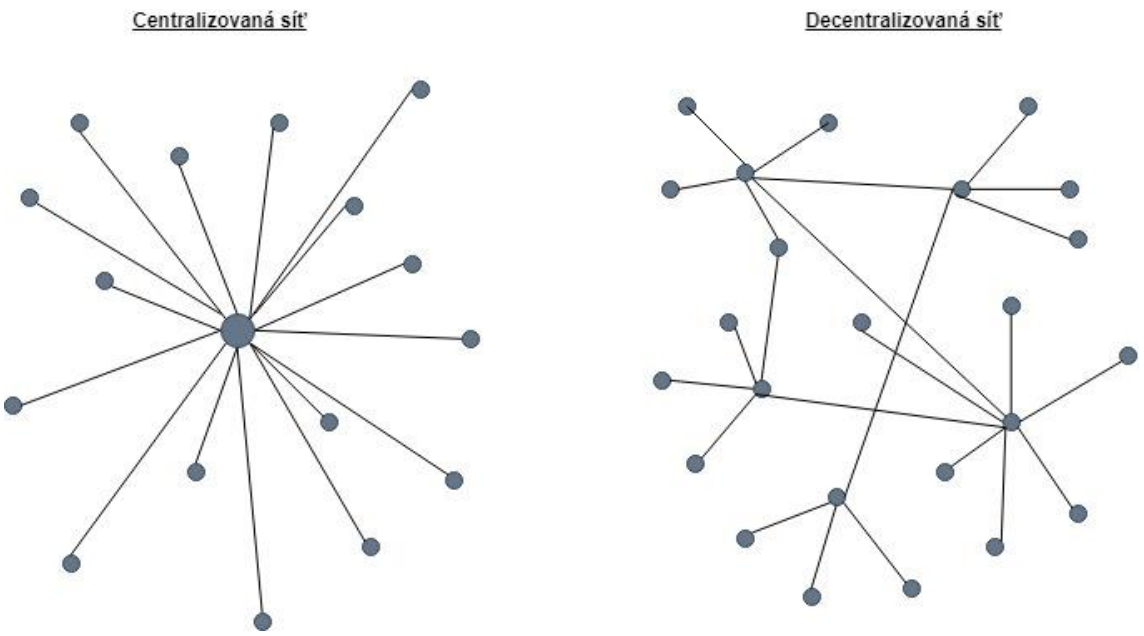


Obr. 25 Vnitřní struktura Bitcoinového systému
Zdroj: Lánský 2018 [42]

2.4.2 Blockchain

Blockchain (česky bločenka) je v podstatě účetní kniha, kde jsou uvedeny veškeré transakce, které proběhly od počátku kryptoměny. Při zapisování nové transakce je poslána informace o nové transakci do sítě a jednotlivé uzly, které mají k dispozici celou historii, se rozhodují, zda je transakce platná a bude zapsána do bloku. Aktuálně má blockchain velikost 210GB. Úplný uzel (full node) má kompletní blockchain a takových je více než 5000.

Aby transakce Bitcoinu mohly bezpečně a decentralizovaně probíhat, bylo potřeba vyřešit jednu matematickou úlohu, která je známá jako „problém byzantských generálů“ (angl. Byzantine generals problem). Jedná se o situaci, kdy veliké vojsko obléhá město. Vojsko nemá hlavního generála, ale spousty velitelů, kteří velí vlastní jednotce. Velitelé mají cíl zaútočit na město ve stejný čas, aby byl útok úspěšný. Potřebují se tedy shodnout na stejném čase, kdy společně zaútočí. Zprávy si mezi sebou posílají pomocí poslů a existuje riziko, že někteří z poslů, či velitelů mohou být zrádci a zasílají mylné informace. Navíc ještě platí, že čím více velitelů figuruje v rozhodování, tím více je komunikačních kanálů a zvyšuje se nedůvěra. Vyřešením tohoto problému pomocí důkazu prací, který je popsán v další kapitole mohl Satoshi Nakamoto spustit Bitcoin. Je to totiž metafora, kdy úspěšný útok představuje schválenou transakci, velitelé jsou jednotlivé uzly sítě, které vyhodnocují transakce a poslové jsou zprávy, které jsou posílány mezi uzly.



Obr. 26 Topologie centralizované a decentralizované sítě
Zdroj: vlastní tvorba

Výhody blockchainu

- Není centrální autorita, která by měla vyšší moc. Všechny tzv. uzly mají stejná práva.
- Každý uzel je schopen s určitou mírou jistoty se rozhodnout, zda je transakce v pořádku. Pouze v případě, že se shodne většina – zapisuje se transakce do všech uzlů
- Není možné dvojité utrácení. Došlo by ke kolizi a zapsána může být maximálně jedna transakce

Nevýhody

- V případě kontrolování nadpoloviční většiny je možné ovládnout celý systém
- Není garantováno žádnou autoritou, proto v případě podvodu není možné nijak řešit
- Nadměrná spotřeba elektřiny

2.4.3 Proof-of-work

Česky důkaz prací, či důkaz o provedené práci (zkratka PoW), vydaný Adamem Backem v roce 2002 [45] je mechanismem, který do principu kryptoměn vnáší koncept obdobný těžbě zlata. Používá se výraz – těžba bloku. Je to přirovnání k fyzické těžbě zlata, kdy je potřeba prosít velké množství zeminy k nalezení kusu zlata. Ve vytěžení bloku hraje roli náhoda. Úkolem těžařů je totiž nalézt řešení pro složitý matematický problém zkoušením různých možností. Není možné výsledek odvodit – je možné pouze zkoušet náhodná čísla a následně zkontrolovat, že výsledek je správný. Po nalezení správného řešení připadne odměna těžaři, který problém vyřešil jako první. Vytvořit důkaz je obtížné, ale ověřit, že je důkaz platný, je snadné.

Původně byl tento mechanismus však zamýšlen jako ochrana před DoS útoky, nebo spamem. Při poslání požadavku musí žadatel propůjčit část svého výpočetního výkonu, aby vyřešil matematický problém. Strana poskytovatele služby následně mohla jednoduše ověřit, zda byl problém opravdu vyřešen. Pro běžného uživatele to znamená drobné zdržení, avšak pro útočníka, nebo rozesilatele spamových emailů to znamená velikou překážku, která se s množstvím požadavků zvyšuje.

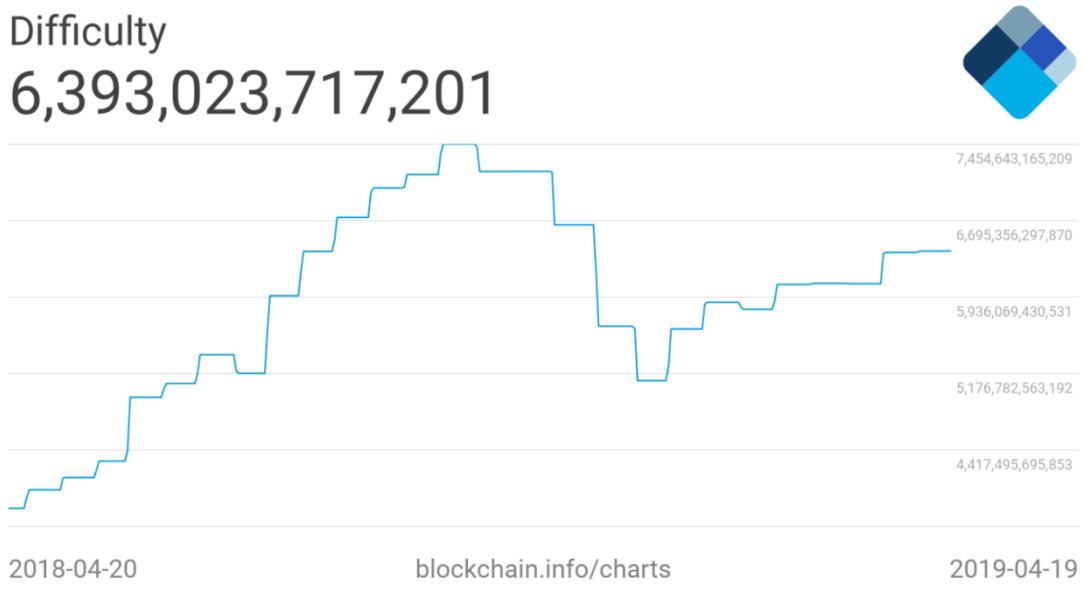
PoW řeší další problém, a to jakým způsobem je rozhodováno o přijmutí, nebo zamítnutí transakce. Pokud by byl použit princip, že každá IP adresa by mohla mít hlas, tak by mohlo hlasování být zmanipulováno vlastníkem velkého množství IP

adres. Namísto toho má hlasovací právo každý procesor. Většinové rozhodnutí je tedy reprezentováno nejdelším řetězcem, který má většina uzlů. Tady platí předpoklad, že nikdo nekontroluje většinu sítě (v opačném případě může nastat tzv. 51% útok, který bude popsán v další kapitole). Správný řetězec roste nejrychleji a ve chvíli, kdy by útočník chtěl změnit údaje v minulosti, musel by zároveň přepočítat i všechny následující bloky. [46]

Při důkazu prací se hledá řešení těžkého matematického problému, patřícího do kategorie NP-úplných úloh. K vyřešení problému je třeba velkého množství výpočetních operací, exponenciálního vzhledem k velikosti zadaného vstupu. Ověření správnosti řešení je naopak snadné, postačí polynomiální (obvykle lineární) počet výpočetních operací vzhledem k velikosti zadaného vstupu.[42 str. 32]

Aby měli těžaři s nižším výkonem větší šanci na odměnu, zpravidla se seskupují do tzv. těžebních skupin a v případě úspěchu je odměna rozdělena mezi všechny členy skupiny.

Na základě rychlosti, kterou jsou bloky vytvářeny, může být upravována složitost řešených problémů. Se stále se zlepšujícím hardwarem a větším zájmem o těžbu je třeba zvýšit i obtížnost řešených problémů, aby vytvoření bloku a tedy i nových jednotek kryptoměny bylo regulováno na 10 minut na vytvoření bloku. Jak se zvyšovala složitost, je možné vidět na obrázku 27 níže.



Obr. 27 Obtížnost řesení problémů Bitcoinu
Zdroj: www.blockchain.com [47]

2.4.3.1 Těžba Bitcoinu

Při těžbě nového bloku má těžař za úkol najít hash, který bude splňovat jednoduchou podmínku – hash musí obsahovat na začátku řetězce určitý počet nul. Pro výpočet však musí použít hodnotu hashe předchozího bloku, zahrnout nové transakce při výpočtu a další dané informace.

Jediná proměnná, kterou může měnit je takzvaná „nonce“, což je 32 -bitové číslo, které může těžař měnit a zkoušet, s jakou hodnotou výsledný hash bude splňovat danou podmínku. Při ověřování podmínky se nahlíží na hash jako na číslo, které musí na začátku mít určitý počet nul.

Příklad hashe prvního bloku Bitcoinu:

```
00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
```

Zvyšováním počtu nul na začátku řetězce se zvyšuje obtížnost nalezení řetězce splňujícího podmínku – s každou přidanou nulou se obtížnost zvyšuje dvojnásobně.

Zjednodušený příklad nalezení hashe:

Pro řetězec „Hello, world!“ za pomocí funkce SHA-256 lze změnit v hodnotu menší než 2^{240}. Za použití čísla – nonce, které je přidáno za řetězec a jsou zkoušeny jednotlivé hodnoty, dokud hash nesplňuje podmínku. Za předpokladu, že se nonce zvyšuje v každém pokusu o jednotku, by bylo třeba 4251 pokusů k nalezení hashe, který podmínku splňuje.

"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64 =
2^252.253458683
"Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8 =
2^255.868431117
"Hello, world!2" =>
ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7 =
2^255.444730341
...
"Hello, world!4248" =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965 =
2^254.782233115
"Hello, world!4249" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6 =
2^255.585082774
"Hello, world!4250" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 =
2^239.61238653 [48]

2.4.4 Anonymita bitcoinu

Při jediné transakci je možné používat pojem anonymita. V případě většího množství transakcí již je možné vysledovat v bločence transakce, na kterých se tento uživatel zúčastnil a nepřímo tak vydedukovat identitu a případně i reálnou identitu. Pokud tedy má uživatel za cíl zvýšit míru anonymity, není nic jednoduššího, než používat jednorázové adresy. Ideální je v případě takové platby

mít na adrese přesné množství prostředků plus poplatek za transakci. Ve chvíli, kdy je částka vyšší, je možné se přebytku vzdát. Naopak ve chvíli, kdy na jedné adrese není dostatek prostředků, a k provedení platby jsou použity dvě adresy, automaticky je tímto prozrazena informace, že uživatel je vlastníkem obou uvedených adres. V takovém případě je míra anonymity oslabena.

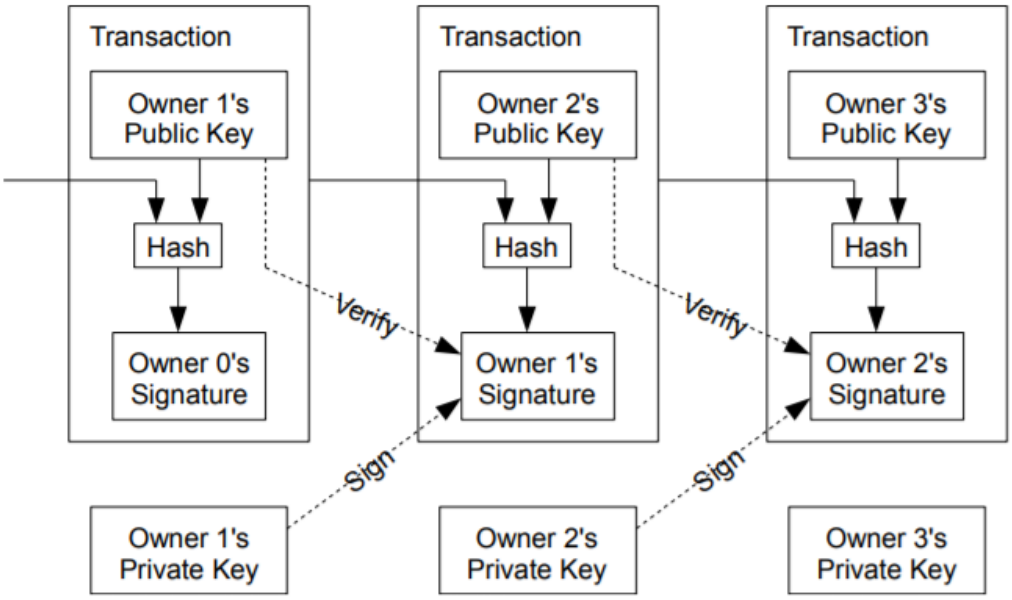
Dalším způsobem jak zvýšit míru anonymity je míchání (mixing). Při takovém procesu si větší množství uživatelů mezi sebou posílá různě veliké částky takovým způsobem, aby na konci míchání měl stejné množství, se kterým začínal. Tento proces je možné několikrát opakovat a má za výsledek zvýšení množství provedených transakcí a ztížení sledování konkrétní identity. K provedení takového procesu slouží specializované servery. Mezi nevýhody tohoto způsobu zvýšení míry anonymity patří poplatek za provedení služby a fakt, že provozovatel zná detail k prováděným transakcím. Existuje i mnoho dalších způsobů, jak dosáhnout anonymity, ale vždy se jedná o stejný princip. Za pomocí velkého množství transakcí a zpravidla jednorázových adres docílit zmatku, který zvědavý pozorovatel nebude moci s jistotou odvodit.

Dobrovolné snížení míry anonymity může být vyhledáváno v případě dobročinných účtů, nebo kvůli soutěžím, a to z důvodu nemožnosti vytváření většího množství účtů jedním soutěžícím. Dále pak při výměně kryptoměny za měnu fiat je zpravidla stanoveno zákonem, že provozovatel služby této výměny je povinen ověřit identitu uživatele (ofocený doklad totožnosti společně s dokladem prokazujícím jeho bydliště). Tyto informace je poskytovatel služby povinen po danou dobu uchovávat a v případě podezření předložit státním orgánům. Důvodem je zamezení praní špinavých peněz a trestné činnosti.

2.4.5 Příklad transakce Bitcoinu

Transakce je operace, kdy se z jedné adresy přesouvá měna na druhou adresu. Pro provedení transakce je potřeba zaplatit poplatek. Takový poplatek může být nulový, ale poté existuje riziko, že transakce nebude nikdy provedena. S vyšším poplatkem se zvyšuje priorita zpracování operace. Transakce může obsahovat vyšší počet vstupů (slévající), nebo výstupů (rozdělovací), avšak s vyšší složitostí je i spojen vyšší poplatek. Transakční poplatek motivuje provozovatele uzlů, aby

ověřovali transakce a uchovávali celou účetní knihu – blockchain. Jednotlivé transakce jsou součástí bloků, přičemž každý blok obsahuje 1000 až 2000 transakcí – maximální velikost bloku je 1000 kB. Transakce, která je zařazena do bloku se nazývá ověřená. Vytvoření bloku trvá přibližně deset minut.



Obr. 28 Ukázka transakce Bitcoinu
Zdroj: www.bitcoin.org [46]

Na obrázku 28 je znázorněno vytváření transakcí v bloku. Aby nebylo možné zpětně měnit údaje, používá každá nová transakce jako vstup informaci z výstupu poslední transakce – takzvaný hash. Následně je transakce ověřena za pomoci soukromého klíče a výstup opět použit pro úpravu hashe. Takovýmto řazením transakcí vzniká nový blok transakcí.

Postup vytváření bloku:

1) Nové transakce jsou poslány na všechny uzly.
2) Každý uzel sbírá nové transakce a řadí je do bloku.
3) Každý uzel se snaží nalézt složitý důkaz prací (PoW) pro svůj blok.
4) Když uzel najde řešení důkazu prací, pošle blok na všechny ostatní uzly.
5) Uzly přijmou blok, pouze pokud všechny obsažené transakce bloku jsou validní a zároveň obsahují doposud neutracené jednotky.
6) Uzly vyjádří přijetí bloku tím, že začnou vytvářet nový blok řetězce za použití hashe, který obsahoval předchozí přijatý blok.

Každý blok obsahuje jednu speciální transakci, která se nazývá „coinbase“ (mincetvorná). Taková transakce nemá žádné vstupy a je odměnou za vytěžení bloku. Výstupem této transakce je adresa úspěšného tvůrce bloku, který obdrží nové jednotky kryptoměny a odměnu za provedené transakce. Odměna za každý vytěžený blok se snižuje každé 4 roky – aktuálně je výše odměny 12,5 BTC[9].

2.4.6 Bezpečnostní hrozby

Kryptoměny jsou obdobně jako Android - open-source, což znamená, že zdrojový kód si může prohlédnout kdokoli. To má dva úhly pohledu. První je, že každý s patřičnou znalostí si může kód zrevidovat a ujistit se, že v kódu nejsou žádné skryté výjimky, které by někoho zvýhodňovali. Kód je pak důvěryhodný. Druhý pohled je však takový, že pokud je kód veřejně známý, je možné v něm najít slabá místa, či neúmyslné chyby a ty zneužít ve svůj prospěch. Takové chyby jsou však zpravidla objeveny v rané fázi kryptoměny a způsobené škody jsou proto minimální – chyby jsou ihned po objevení a zneužití opraveny.
Zde jsou popsána základní rizika užívání kryptoměn.

2.4.6.1 Uživatelé

Větší svoboda používání kryptoměn s sebou nese i jisté hrozby. Transakce kryptoměn jsou na rozdíl od těch bankovních nevratné. Poslání platidla na jinou adresu je proto problémové. Obdobně ztráta znalosti soukromého klíče vede k nenávratné ztrátě cenin.
V případě krádeže – ať už je jakkoli nepravděpodobná – neexistuje žádná centrální autorita, na kterou by se mohl poškozený obrátit.
Pro uchovávání informace o soukromém klíči není bezpečné používat webové služby, nebo aplikace v nezabezpečeném počítači. Takto by mohl vir, nebo spyware údaje odcizit a zneužít. Zdaleka nejbezpečnějším způsobem je uchování na papíře a

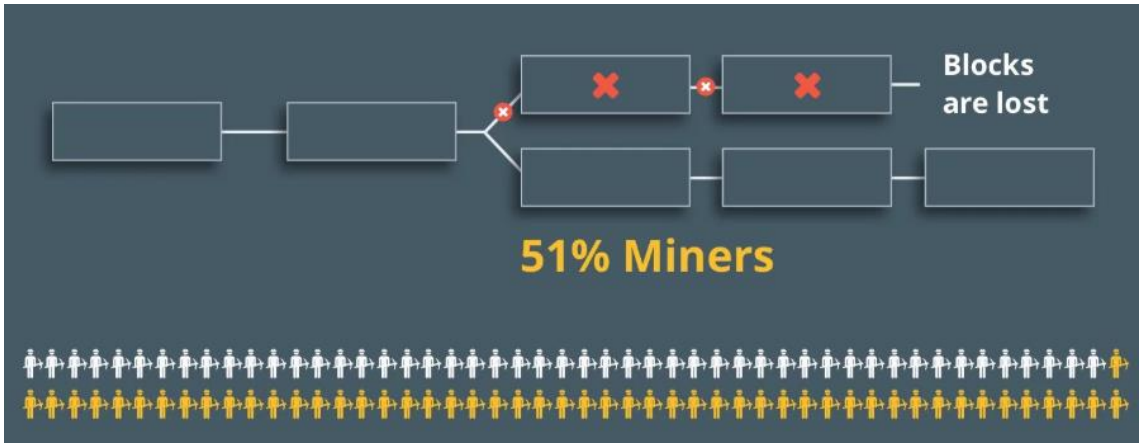
[9] Jednotlivé transakce, nebo bloky transakcí je možné prohlížet přímo na stránkách https://www.blockchain.com/explorer

uložené na bezpečném místě, nicméně tento způsob je nepohodlný při provádění transakcí. Proto se pro běžné používání využívají hardware peněženky.
Příkladem je český produkt Trezor (https://trezor.io/). Výhodou je podpora několika set dostupných kryptoměn, šifrování obsahu. Nevýhodou může být poměrně vysoká pořizovací cena.

Obr. 29 Příklad HW krypto peněženky
Zdroj: www.shop.trezor.io [49]

2.4.6.2 51% útok – ovládnutí sítě

Jak už bylo zmíněno v kapitole 2.4.3, Blockchain, pomocí kterého jsou zapisovány transakce do bloků, se řídí hlasem většiny. Ve chvíli, kdy se objeví dvě protichůdné transakce, je prohlášena za správnou ta, se kterou souhlasí většina uzlů. Stejně tak pokud se objeví dvě různé větve bloků, prohlašuje se za správnou ta, která je delší. Pokud však přestane tento předpoklad platit a útočník, nebo útočníci vlastní nadpoloviční většinu uzlů, je možné ovládnout celou síť – měnit již provedené transakce a vytvářet nové bloky, obsahující pozměněné transakce. Na obrázku 30 je schéma, kdy nadpoloviční většina těžařů odhlasuje za správnou alternativní větev.



Obr. 30 Schéma 51% útoku
Zdroj: cointelegraph.com [50]

Hrozba 51% útoku je kryptoměnovou komunitou brána velmi vážně. V červenci 2014 těžební skupina GHash.io dosáhla nadpolovičního výpočetního výkonu v rámci Bitcoinové sítě. Těžební skupina sama od sebe přijala opatření, aby její výkon klesl pod 40 % (Farivar, 2014). Přestože těžební skupina své krátkodobé výhody k útoku nezneužila, poškodilo jí to reputaci, postupně ztrácela své těžaře, až v roce 2016 zanikla.[42 str. 80]

V lednu 2019 se měna Ethereum Classic (ETC) stala obětí takového útoku. Útočníci tímto útokem údajně odcizili kryptoměnu v hodnotě 1,1 milionu dolarů. [51] S možností pronájmu výpočetního výkonu se objevila i stránka, která popisuje, jak drahý by teoreticky byl útok na jednotlivé kryptoměny - https://www.crypto51.app/.

2.4.6.3 Dvojité utrácení

Jedná se o druh útoku, kdy se útočník snaží použít ceniny ze své peněženky pro vícero transakcí (angl. double spending). Probíhá tak, že útočník zaplatí a následně se snaží zneplatnit blok, který transakci obsahuje tím, že vytvoří alternativní blok s převedením jednotek na jinou adresu, kterou útočník kontroluje. Obchodníci proto zpravidla čekají na potvrzení transakce, dokud není následována několika dalšími bloky, aby bylo složitější transakci upravit. Zpravidla se tento druh útoku nepoužívá kvůli vysokým nákladům. Takto upravené transakce jsou používány při 51 % útocích, kdy útočník kontroluje nadpoloviční většinu a může tak upravovat transakce bez větších problémů.

Pokud by útočník chtěl provést úspěšný útok dvojitého utrácení bez kontroly 51% uzlů, musel by překonat následující pravděpodobnost:

z = počet bloků

p = pravděpodobnost, že poctivý uzel vytvoří další blok

q = pravděpodobnost, že útočník vytvoří další blok

P = pravděpodobnost úspěšného útoku

Poissonovo rozdělení

$$\lambda = z\frac{q}{p}$$

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \leq z \\ 1 & if\ k > z \end{cases}$$

Po úpravě:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} (1 - 1 - (q/p)^{(z-k)}$$

q=0.1

z=0 P=1.0000000

z=1 P=0.2045873

z=2 P=0.0509779

z=3 P=0.0131722

z=4 P=0.0034552

z=5 P=0.0009137

z=6 P=0.0002428

z=7 P=0.0000647

z=8 P=0.0000173

z=9 P=0.0000046

z=10 P=0.0000012

[46]

Z výsledků je zřejmé, že pravděpodobnost úspěšného útoku se s každým blokem zásadně snižuje. Zpravidla se čeká šest bloků, než je transakce považována za dokončenou.

2.4.6.4 Denial of Service útok

DoS, nebo česky odepření služby je typ útoku na internetové servery, nebo stránky, jehož cílem je zapříčinit nedostupnost daného serveru nebo služby. Je tak docíleno zasíláním velkého množství požadavků – v tomto případě prázdných bloků – a to v takovém množství, aby server nestihl požadavky odbavovat. Tím přestává plnit funkci a regulérní požadavky nejsou odbavovány. Pro vykonání takového útoku není potřeba nadpoloviční většina, ale stačí významný podíl. Bitcoin má zabudované ochrany proti DoS útokům, avšak v případě sofistikovaného útoku by mohl podlehnout.

2.4.6.5 Feather-forks útok

Tento druh útoku nevyžaduje nadpoloviční většinu, ale pouze významný podíl. Princip je v tom, že útočník disponující významným podílem vytvoří seznam zakázaných adres (angl. blacklist) a prohlásí, že transakce od těchto adres jsou neplatné, takže k nim budou vytvářeny alternativní bloky. Ostatní uzly se v rámci zmenšení rizika ztrát přizpůsobí a v podstatě začnou taktéž vytvářet alternativní bloky. [52]

3 Shrnutí výsledků

Každá technologie má slabiny. Vždy tomu tak bylo a vždy tomu tak i bude. V situaci, kdy by útočník s neomezenými prostředky chtěl napadnout nebo prolomit tu či onu ochranu, není otázkou, zda je to možné, ale kolik prostředků je třeba vynaložit, aby byl útok úspěšný. Každý uživatel si pouze musí určit, jaké bezpečnostní opatření je ochoten konzistentně dodržovat. Je to přímá úměrnost mezi pohodlím a bezpečností. Zda potenciálnímu útočníkovi práci usnadní, nebo zda se bude snažit ochránit své vlastnictví i za cenu nepohodlí.

Prvním bodem výzkumu je porovnání platby bezkontaktní platební kartou a mobilním telefonem obsahujícím údaje o kartě. Nabízí se hned několik úhlů pohledu. Při platbě fyzickou kartou může dojít k vyfocení a tedy odcizení citlivých údajů. Karta je náchylná na Relay a Replay útoky. V případě ztráty či odcizení nemá žádné bezpečnostní opatření, aby nemohla být zneužita.

Oproti tomu při platbě mobilním telefonem nejsou vystaveny údaje z karty. Za určitých podmínek by mohlo dojít k Replay útoku. V případě ztráty telefonu by nemělo dojít ke zneužití platebních údajů, protože pro každou platbu telefonem musí proběhnout autentifikace vlastníka.

Kryptoměny jsou nejmladším platidlem, které nabízí určitou míru anonymity a svobody. Nedohlíží na ně žádná centrální autorita, takže nemohou být regulovány státem, ale jsou velice volatilní. Jednou částí lidí jsou vnímány jako budoucnost a možnost skvělé investice, druhou potom jako velká bublina a podvod. Pravdu mají přitom obě skupiny, jen záleží na úhlu pohledu. Jisté je, že i kryptoměny mají slabá místa. Například útok DoS, 51% útok a další.

4 Závěry a doporučení

Tato práce představuje nejznámější platidla moderní společnosti, popisuje, jakým způsobem fungují a jaké jsou jejich ochranné mechanismy. Zároveň poukazuje na bezpečnostní mezery a slabá místa, kterých hackeři mohou zneužít. Zdroji informací, ze kterých bylo čerpáno, jsou zpravidla oficiální dokumentace, případně oficiální webové stránky.

Autor při psaní práce zápolil se způsobem zpracování ve smyslu hloubky a rozsahu. Při psaní práce by bylo možné zkoumat dané téma ještě hlouběji – například rozebrat jednotlivé způsoby a algoritmy kryptování do úplného detailu. Stejně tak by bylo možné obsáhnout větší rozsah – pokrýt více scénářů plateb a další způsoby placení a ochran. Práce ve výsledku obsahuje množinu témat, která autor považuje za klíčová.

Cílem práce bylo popsat čtenáři základní typové scénáře plateb, což se podařilo. Dále pak specifikovat, jakým způsobem je komunikace zabezpečená a v kterých bodech jsou nejslabší místa. Jsou popsány druhy útoků a následně opatření, jak jím předcházet. Práce dále vysvětluje koncept a fungování kryptoměn, jmenovitě potom té nejrozšířenější – Bitcoinu. Uvádí její výhody, nevýhody, jakým způsobem je řešena anonymita a bezpečnostní hrozby této kryptoměny.

Při práci s počítačem existuje velké množství nástrah. Dodržování zásad uvedených v kapitole 2.3 rozšířených o další doporučení by mělo být samozřejmostí.

- Pravidelně instalovat aktualizace operačního systému
- Počítač vybavit spolehlivým a aktualizovaným antivirovým a antispyware programem
- Pro každou stránku používat jiné heslo. Tato hesla je možné uchovávat v zašifrovaném hesláři
- Hesla pravidelně měnit
- Používat zabezpečené internetové připojení, nikoli veřejné wi-fi
- Využívat VPN připojení pro komunikaci s citlivými informacemi
- Pokud je to možné, používat dvoufázové ověření

- Počítač v nepřítomnosti zamykat

Obdobné podmínky platí i pro práci s mobilními telefony.
Autor důrazně doporučuje čtenáři, aby dodržoval bezpečnostní zásady z důvodu zajištění vyšší bezpečnosti platidel. Důležité je neustále zdokonalovat své znalosti a neustále přemýšlet nad zlepšením bezpečnosti. Člověk, který nemá znalosti a je ledabylý je pro útočníka tím nejsnazším terčem.

5 Seznam použité literatury

[1] **Kyberkriminalita** - *Policie České republiky*. [online]. Policie ČR [cit. 20.04.2019]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[2] **OULEHLA, Milan a Roman JAŠEK**. *Moderní kryptografie*. Praha: IFP Publishing, 2017. ISBN 978-80-87383-67-4.

[3] **Secure Hash Standard | NIST**. *National Institute of Standards and Technology | NIST* [online]. Dostupné z: https://www.nist.gov/publications/secure-hash-standard

[4] **NIST Comments on Cryptanalytic Attacks on SHA-1 |** CSRC. NIST Computer Security Resource Center | CSRC [online]. Dostupné z: https://csrc.nist.gov/News/2006/NIST-Comments-on-Cryptanalytic-Attacks-on-SHA-1

[5] **Wayback Machine** [online]. [cit. 20.04.2019]. Dostupné z: https://web.archive.org/web/20160330153520/http://www.staff.science.uu.nl/~werkh108/docs/study/Y5_07_08/infocry/project/Cryp08.pdf

[6] **NIST** Page [online]. [cit. 20.04.2019]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[7] **JUŘÍK, Pavel**. *Svět platebních karet*. Praha: Radix, 1995. ISBN 80-901853-1-2.

[8] **Zákon o platebním styku** - *Odpovědnost poskytovatele za neautorizovanou platební transakci* - Podnikatel.cz. [online]. [cit. 20.04.2019]. Dostupné z: https://www.podnikatel.cz/zakony/zakon-c-284-2009-sb-o-platebnim-styku/f4013456/

[9] **Počet platebních karet v ČR loni klesl o 592.000 na 10,7 milionu** *České noviny* [online]. [cit. 20.04.2019]. Dostupné z: https://www.ceskenoviny.cz/zpravy/pocet-platebnich-karet-v-cr-loni-klesl-o-592-000-na-10-7-milionu/1613163

[10] **Jak používat kartu bezpečně** | *ČSOB*. [online]. [cit. 20.04.2019]. Dostupné z: https://www.csob.cz/portal/bezpecnost/jak-se-branit/bezpecnostni-pravidla-pro-uzivani-platebnich-karet/jak-pouzivat-kartu-bezpecne

[11] **EMVCo** [online]. [cit. 20.04.2019]. Dostupné z: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-

content/uploads/documents/EMV_v4.3_Book_3_Application_Specification_20120607062110791.pdf

[12] **Near Field Communication**: *What is Near Field Communication?.* [online]. [cit. 20.04.2019]. Dostupné z: http://nearfieldcommunication.org/

[13] **NFC Logos** *NFC Marketing, Authentication and Identification* [online]. [cit. 20.04.2019]. Dostupné z: https://nfc.today/advice/nfc-logo-options

[14] **NFC Tags - how do they work?**. [online]. [cit. 20.04.2019]. Dostupné z: https://www.androidauthority.com/nfc-tags-explained-271872/

[15] **NFC Tags - how do they work?**. [online]. [cit. 20.04.2019]. Dostupné z: https://www.androidauthority.com/nfc-tags-explained-271872/

[16] **Google Pay (CZ) – Lepší způsob placení**. [online]. [cit. 20.04.2019]. Dostupné z: https://pay.google.com/intl/cs_cz/about/

[17] **Apple Pay – Apple (CZ)** [online]. [cit. 20.04.2019]. Dostupné z: https://www.apple.com/cz/apple-pay/

[18] **Apple** [online]. [cit. 20.04.2019]. Dostupné z: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

[19] **Apple** [online]. [cit. 20.04.2019]. Dostupné z: https://www.apple.com/business/site/docs/FaceID_Security_Guide.pdf

[20] **Host-based card emulation overview** | *Android Developers*. [online]. Dostupné z: https://developer.android.com/guide/topics/connectivity/nfc/hce

[21] **3-D Secure - EMVCo**. [online]. Dostupné z: https://www.emvco.com/emv-technologies/3d-secure/

[22] **EMVCo** [online]. [cit. 20.04.2019]. Dostupné z: https://www.emvco.com/wp-content/uploads/2017/12/Transaction_Volumes_FINAL.pdf

[23] **EMVCo** [online]. [cit. 20.04.2019]. Dostupné z: https://www.emvco.com/wp-content/uploads/documents/EMV_v4.3_Book_1_ICC_to_Terminal_Interface_20120605394541.pdf

[24] **Jak postupovat při zneužití platební karty** - *Aktuálně.cz* [online]. [cit. 20.04.2019]. Dostupné z: https://zpravy.aktualne.cz/ekonomika/co-delat-zneuziti-kradezi-okopirovani-platebni-karty/r~49a50eeeb4d911e899900cc47ab5f122/

[25] **ISO Magnetic Stripe Card Standards** | *Q-Card. Smart Card Test Tools and Test Lab for EMV / NFC / Mobile | Q-Card* [online]. [cit. 20.04.2019]. Dostupné z: https://www.q-card.com/about-us/iso-magnetic-stripe-card-standards/page.aspx?id=1457

[26] **EMVCo** [online]. [cit. 20.04.2019] Dostupné z: https://www.emvco.com/wp-content/uploads/documents/Secure-Remote-Commerce-Framework-FINAL-v1.0.pdf

[27] **Češi vyvinuli bezpečnostní známky, které ochrání platební karty před kopírováním** | *iROZHLAS - spolehlivé zprávy* [online]. [cit. 20.04.2019]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/cesi-vyvinuli-bezpecnostni-znamky-ktere-ochrani-platebni-karty-pred-kopirovanim_201311051510_mkaspar

[28] **Bellroy** | Considered Carry Goods: Wallets, Bags, Phone Cases & More [online]. Dostupné z: https://bellroy.com/products/note-sleeve-wallet/leather_rfid/java#image-1

[29] **Češi nejčastěji spoří na běžném účtu, ukázal průzkum** - *Měšec.cz* [online]. [cit. 20.04.2019]. Dostupné z: https://www.mesec.cz/aktuality/cesi-nejcasteji-spori-na-beznem-uctu-ukazal-pruzkum/

[30] **Equifax Hack: 5 Biggest Credit Card Data Breaches**. *Investopedia - Sharper Insight* [online]. Dostupné z: https://www.investopedia.com/news/5-biggest-credit-card-data-hacks-history/

[31] **Intro to NFC Payment Relay Attacks** – *Salvador Mendoza* [online]. [cit. 20.04.2019]. Dostupné z: https://salmg.net/2018/12/01/intro-to-nfc-payment-relay-attacks/

[32] **Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci - 2018** | *ČSÚ. Český statistický úřad* [online]. Dostupné z: https://www.czso.cz/csu/czso/vyuzivani-informacnich-a-komunikacnich-technologii-v-domacnostech-a-mezi-jednotlivci

[33] **Pravidla platebního systému CERTIS** - *Česká národní banka*. [online]. [cit. 20.04.2019]. Dostupné z: https://www.cnb.cz/cs/platebni-styk/certis/pravidla-platebniho-systemu-certis/index.html

[34] **V Česku proběhla historicky první okamžitá platba**. *Air Bank* [online]. Dostupné z: https://www.airbank.cz/novinky/v-cesku-probehla-historicky-prvni-okamzita-platba-prevod-penez-z-air-bank-do-ceske-sporitelny-zabral-jen-nekolik-sekund

[35] **SWIFT – The global provider of secure financial messaging services** [online]. [cit. 20.04.2019]. Dostupné z: https://www.swift.com/about-us

[36] **Průběh mezibankovního převodu peněžních prostředků (úhrady) v českých korunách (CZK)** - *Česká národní banka*. [online]. [cit. 20.04.2019]. Dostupné z: https://www.cnb.cz/cs/platebni-styk/certis/prubeh-mezibankovniho-prevodu-peneznich-prostredku-uhrady-v-ceskych-korunach-czk/index.html

[37] **Bezpečný internet** | *Rady pro bezpečnost na internetu* [online]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

[38] **USB keylogger** | SPYobchod.cz [online]. [cit. 20.04.2019]. Dostupné z: https://www.spyobchod.cz/airdrive-max-usb-keylogger/

[39] **Zpoplatnění Facebooku** [online]. [cit. 20.04.2019] Dostupné z: http://www.hoax.cz/hoax/zpoplatneni-facebooku/

[40] **Cabir's first year** | *Kaspersky Lab's cyberthreat research and reports* [online]. [cit. 20.04.2019]. Dostupné z: https://securelist.com/cabirs-first-year/30027/

[41] **Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017**. [online]. [cit. 20.04.2019]. Dostupné z: https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017

[42] **LÁNSKÝ, Jan**. *Kryptoměny*. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-722-4.

[43] **List of All Cryptocurrencies** | Coin Market Overview | CoinLore [online]. [cit. 20.04.2019]. Dostupné z: https://www.coinlore.com/all_coins

[44] **Cryptocurrency Market Capitalizations** | *CoinMarketCap* [online]. Dostupné z: https://coinmarketcap.com/currencies/bitcoin

[45] **Hashcash.org** [online]. [cit. 20.04.2019]. Dostupné z: http://www.hashcash.org/papers/hashcash.pdf

[46] **Bitcoin.org** [online]. [cit. 20.04.2019]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[47] **Difficulty - Blockchain**. [online]. [cit. 20.04.2019]. Dostupné z: https://www.blockchain.com/en/charts/difficulty

[48] **Proof of work - Bitcoin Wiki**. [online]. [cit. 20.04.2019]. Dostupné z: https://en.bitcoin.it/wiki/Proof_of_work

[49] **Official Trezor Shop** | *TREZOR White*. [online]. [cit. 20.04.2019]. Dostupné z: https://shop.trezor.io/product/trezor-one-white

[50] **Proof-of-Work, Explained** | *Cointelegraph.* [online]. [cit. 20.04.2019]. Dostupné z: https://cointelegraph.com/explained/proof-of-work-explained

[51] **Brave New Coin**. [online]. [cit. 20.04.2019]. Dostupné z: https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stopped

[52] **Feather-forks: enforcing a blacklist with sub-50% hash power**. *Bitcoin Forum* [online]. [cit. 20.04.2019]. Dostupné z: https://bitcointalk.org/index.php?topic=312668.0

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma: Kombinovaná
Obor/komb.: Aplikovaná informatika (ai2-k)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Bc. Květoň Roman	Sedloňov 21, Sedloňov	11600265

TÉMA ČESKY:

Bezpečnost a ochrana platidel v moderní společnosti

TÉMA ANGLICKY:

Safety and protection of currencies in modern society

VEDOUCÍ PRÁCE:

prof. RNDr. PhDr. Antonín Slabý, CSc. - KIKM

ZÁSADY PRO VYPRACOVÁNÍ:

Student představí aktuální trendy placení na internetu, jakým způsobem jsou tyto transakce chráněny a naopak i jejich slabiny a nedostatky. Zaměří se na internetové bankovnictví, platby debetní kartou a kryptoměny.
Osnova

1. Teoretická část
a. Peníze na internetu
b. Banky
i. Internetové bankovnictví
ii. Platby kartou
iii. Investiční fondy
c. Kryptoměny
2. Praktická část
a. Zásady bezpečné práce s penězi na internetu
b. Návrh vylepšení ochrany

SEZNAM DOPORUČENÉ LITERATURY:

Kryptoměny, Jan Lánský
Komplexní pohled do bankovního světa, Liběna Černohorská
Úvod do kryptografie, Karel Burda

Podpis studenta: ..... **Datum:** 2.4.2018

Podpis vedoucího práce: ..... **Datum:** 6.4.2018