VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

ANALÝZA BEZPEČNOSTI A POUŽITELNOSTI KRYPTOMĚNOVÝCH PENĚŽENEK

SECURITY AND USABILITY ANALYSIS OF CRYPTOCURRENCY WALLETS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **FILIP BRNA**
AUTHOR

VEDOUCÍ PRÁCE — **MAREK TAMAŠKOVIČ, Ing.**
SUPERVISOR

BRNO 2022

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav inteligentních systémů (UITS) Akademický rok 2021/2022

Zadání bakalářské práce

Student: **Brna Filip**
Program: Informační technologie
Název: **Analýza bezpečnosti a použitelnosti kryptoměnových peněženek**
Security and Usability Analysis of Cryptocurrency Wallets
Kategorie: Bezpečnost

Zadání:

1. Seznamte se s existujícími kryptoměnovými peněženkami a jejich kategorizací z pohledu bezpečnosti a použitelnosti.
2. Nastudujte softwarové a hardwarové hrozby a opatření proti nim pro různé kryptoměnové peněženky.
3. Navrhněte několik testovacích scénářů.
4. Systematicky otestujte dané scénáře na alespoň 10 kryptoměnových peněženek různých kategorií.
5. Ohodnoťte výsledky z pohledu použitelnosti a bezpečnosti. Porovnejte je s informacemi dostupnými na stránkách výrobců a stávající kategorizace.
6. Definujte několik doporučení pro různé případy užití.

Literatura:

- Eskandari, Shayan, et al. "A first look at the usability of bitcoin key management." arXiv preprint arXiv:1802.04351 (2018).
- Homoliak, Ivan, et al. "An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets." *arXiv preprint arXiv:1812.03598* (2018).

Pro udělení zápočtu za první semestr je požadováno:

- Body 1-3

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Tamaškovič Marek, Ing.**
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1. listopadu 2021
Datum odevzdání: 11. května 2022
Datum schválení: 4. listopadu 2021

Abstrakt

Cieľom práce je zanalyzovať bezpečnosť a použiteľnosť kryptomenových peňaženiek rôznych kategórii. Práca je zameraná na zoznámenie sa s najpoužívanejšími kryptomenovými peňaženkami, hrozbami súvisiacimi s ich používaním, následnom otestovaní vybraných peňaženiek navrhnutými testovacími scenármi a tiež vyhodnotením testovania doplneným o definíciu niekoľkých doporučení na ich správne používanie. Pri systematickom testovaní bola použitá metóda návrhu testovacích scenárov, nasledovalo systematické testovanie a na záver boli ohodnotené jeho výsledky. Vykonaným výskumom bolo zistené, že najpoužívanejšie kryptomenové peňaženky dosahujú vysokú mieru zabezpečenia proti popísaným hrozbám a rovnako ponúkajú širokú škálu možností ich využitia. Výsledky tejto práce umožňujú používateľom ľahšie pochopenie problematiky spojenej s uchovávaním a manipuláciou s kryptomenami. Na základe výsledkov testovania má používateľ možnosť výberu kryptomenovej peňaženky presne podľa jeho používateľských potrieb a bezpečnostných nárokov.

Abstract

This thesis aims to analyze the security and usability of cryptocurrency wallets of different categories. The work is focused on familiarizing with the most used cryptocurrency wallets, threats related to their use, subsequent testing of the selected wallets with the proposed test scenarios, and evaluation of the testing supplemented with the definition of several recommendations for their proper use. In the systematic testing, the method of designing test scenarios was used, followed by systematic testing, and finally, the results were evaluated. The research conducted found that the most widely used cryptocurrency wallets achieve a high level of security against the described threats and offer a wide range of possibilities for their use. The results of this work allow users to understand the issues associated with storing and handling cryptocurrencies more efficiently. Based on the results of the testing, the user has the possibility to choose a cryptocurrency wallet precisely according to his user's needs and security requirements.

Klíčová slova

kryptomena, krypto, kryptomenová peňaženka, krypto peňaženka, analýza, testovanie, použiteľnosť, bezpečnosť, hrozby, opatrenia, doporučenia

Keywords

cryptocurrency, crypto, cryptocurrency wallet, crypto wallet, analysis, testing, usability, security, threats, precautions, recommendations

Citace

BRNA, Filip. *Analýza bezpečnosti a použitelnosti kryptoměnových peněženek*. Brno, 2022. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Marek Tamaškovič, Ing.

Analýza bezpečnosti a použitelnosti kryptoměnových peněženek

Prohlášení

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Ing. Mareka Tamaškoviča. Uviedol som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpal.

.....
Filip Brna
9. května 2022

Poděkování

Chcel by som poďakovať svojmu vedúcemu práce Ing. Marekovi Tamaškovičovi za jeho vedenie, návrhy, cenné rady, podporu a trpezlivosť počas písania tejto diplomovej práce.

Obsah

Kapitola 1

Úvod

Pojem kryptomena sa čoraz častejšie stáva témou, ktorou sa spoločnosť zaoberá. Spočiatku boli kryptomeny používané prevažne technologickými nadšencami a IT odborníkmi. K ich popularite v začiatkoch do veľkej miery dopomohol aj čierny trh, kde boli požívané ako platidlo. V dnešných dňoch, aj napriek pochybnostiam, vlastní kryptomeny čoraz viac ľudí a ich popularita rýchlo narastá. Pre ľudí sa stali dostupnejšie, je čoraz ľahšie ich získať. Taktiež je možné prostredníctvom nich nakúpiť tovar alebo služby, pretože narastá počet spoločností prijímajúcich kryptomeny ako alternatívu ku klasickým FIAT peniazom. Keďže používatelia operujú s financiami, je nutné aby bola miera rizika chybovosti, vedúca až k strate prostriedkov, čo najnižšia. Na uchovanie kryptomien slúžia kryptomenové peňaženky, pre ktoré je kľúčová dobrá použiteľnosť a bezpečnosť. Tieto vlastnosti pomáhajú ochrániť používateľove kryptomeny a tiež znižujú mieru rizika straty prostriedkov zapríčineným nesprávnym používaním peňaženky. Trh ponúka veľké množstvo kryptomenových peňaženiek rôznych kategórii od rôznych výrobcov.

Cieľom práce je zanalyzovať bezpečnosť a použiteľnosť kryptomenových peňaženiek rôznych kategórii, a pomôcť tak čitateľovi s vybratím správnej peňaženky na základe jeho používateľských potrieb a bezpečnostných nárokov.

K úspešnému dosiahnutiu cieľa je potrebné nasledovať kroky, ktoré sú opísané v jednotlivých kapitolách. V kapitole 2 sú popísané základné pojmy, ktoré je nutné poznať pri zaobchádzaní s kryptomenami a tiež pre pochopenie práce. V kapitole 3 je popísaná kategorizácia peňaženiek s ich špecifickými vlastnosťami, v kapitole 4 sú popísané hrozby a útoky spojené s kryptomenovými peňaženkami. Okrem toho sú v kapitole popísané aj doporučenia proti spomínaným útokom. Na dosiahnutie cieľa práce sú následne v kapitole 5 popísané testovacie scenáre a bezpečnostné hrozby, ktoré predstavujú riziko pre kryptomenové peňaženky. Podľa navrhnutých testovacích scenárov bude v kapitole 6 otestovaných a popísaných 14 vybraných peňaženiek. Získané údaje z testovania budú v kapitole 7 vyhodnotené a peňaženky budú navzájom porovnávané zo stránky použiteľnosti a bezpečnosti. V kapitole 8 budú popísané doporučenia pre bezpečné a správne používanie peňaženiek, doporučenia sa týkajú základných aj špecifických prípadov využitia.

Kapitola 2

Základné pojmy

V kapitole budú rozobrané pojmy akými sú kryptomena, blockchain, kryptomenová peňaženka, seed, smart kontrakt a iné. Ide o pojmy, ktoré je takmer nutnosť poznať pri akejkoľvek práci s kryptomenami a taktiež je to potrebné pre pochopenie tejto práce.

2.1 Kryptomena

Kryptomena je digitálna mena, zabezpečená a postavená na kryptografických primitívach, umiestnená na blockchaine 2.2, pri ktorej sa každé pravidlo alebo úprava programuje do kryptografického algoritmu. Hodnota kryptomien je plne závislá od ponuky a dopytu po nej[31]. Najstaršou a najznámejšou kryptomenou súčasnosti je Bitcoin, ktorý bol vytvorený v roku 2009. Na rozdiel od klasických štátnych mien, Bitcoin a ani iné kryptomeny nemajú žiadnu centrálnu autoritu, sú decentralizované. Autor Bitcoinu je verejnosti známy pod prezývkou Satoshi Nakamoto, avšak jeho skutočná identita nie je známa, a teda nie je známe, či išlo o jednu osobu alebo skupinu ľudí. V prípade väčšiny kryptomien existuje rozdiel medzi klasickou menou a napríklad Bitcoinom v tom, že nie je možné navýšiť množstvo bitcoinov, ktoré bude možné vyťažiť. Ide o takzvanú deflačnú kryptomenu. Existujú aj kryptomeny ktorých počet je neobmedzený, takéto kryptomeny sa nazývajú inflačné kryptomeny. Bitcoiny je možné získať procesom nazývaným ťažba 2.6. Celkový počet bitcoinov, ktorý môže byť vyťažený je necelých 21 miliónov. Bitcoiny ako aj iné kryptomeny nie je možné stratiť, pretože mince ako také sa stratiť nedajú, stratiť je možné len súkromný kľúč, pomocou ktorého sa užívateľ môže k týmto minciam dostať. Mince, ku ktorým bol stratený súkromný kľúč budú vždy uložené na blockchaine. V reálnom svete existuje množstvo iných kryptomien ako je Bitcoin, tieto kryptomeny sú nazývané ako altcoiny. Najznámejšími altcoinami ku dnešnému dňu sú podľa stránky coinmarketcap[15] kryptomeny Ethereum[23], Binance coin[3], Solana[47], Cardano[10]. Kryptomeny sú pre bežného užívateľa dostupné na zmenárňach prípadne osobnou výmenou. Prostredníctvom zmenární môže nakúpiť a taktiež predať zmenárňou ponúkané kryptomeny. Najznámejšími zmenárňami sú momentálne Coinbase[12] a Binance[4].

Kryptografia

Kryptografia slúži na ochranu informácii, pričom jej základnými operáciami sú šifrovanie a dešifrovanie. Šifrovanie je proces, po ktorom sú dáta nerozlúštiteľné pre každého kto nepozná správny dešifrovací kľúč. Dešifrovanie je inverzný proces k šifrovaniu, ide o prevod zašifrovaných dát späť do pôvodnej podoby za pomoci kľúča. Vďaka kryptografii môžu

byť prenášané dáta prostredníctvom telekomunikačných sietí bez toho aby boli neoprávnene zachytené a rozlúštené. Kryptografický algoritmus je matematická funkcia využívaná v procese šifrovania alebo dešifrovania[38, 42]. Základným faktorom pre správny kryptografický algoritmus je nemožnosť dešifrovania zašifrovaných dát bez znalosti kľúča. Základnými kritériami pre bezpečnosť je mať silný kryptografický algoritmus a dobre utajený kľúč. Pri kryptomenách sa využíva asymetrická kryptografia, ktorá využíva dvojicu kľúčov, verejný kľúč na šifrovanie dát a zodpovedajúci súkromný kľúč na ich dešifrovanie. Výhodou asymetrickej kryptografie je v tom, že odosielateľ ani príjemca medzi sebou nepotrebujú zdieľať tajný kľúč a na komunikáciu stačí len prítomnosť verejného kľúča, ktorý je možné prenášať aj cez nezabezpečený kanál.

2.2 Blockchain

Blockchain je abstraktná dátová štruktúra skladajúca sa z blokov. Tieto bloky predstavujú základný stavebný prvok blockchainu a je v nich uložená každá transakcia[32]. Blok je dátová štruktúra v ktorej sú zapísané validné a overené transakcie vytvorené a distribuované rôznymi subjektami v určitom čase[31]. Ďalej blok vo svoje hlavičke obsahuje koreň Merklovho hašového stromu. Merklov hašový strom je špecifický typ dátovej konštrukcie, v ktorej všetky ne-listové uzly obsahujú hašové hodnoty svojich vlastných podriadených uzlov v strome. Jednotlivé bloky sú navzájom previazané a vďaka tomu vzniká reťazec blokov známy ako blockchain. Reťazec vzájomne prepája bloky až po prvý vyťažený blok nazývajúci sa genesis blok, ktorý už sa na žiadny predchádzajúci blok neodkazuje. Blockchain ako verejná kniha transakcií je pravidelne aktualizovaná a je akceptovaná ako skutočnosť každým účastníkom decentralizovanej komunity. Technológia blockchainu je predpokladom pre existenciu decentralizovanej digitálnej meny, avšak mena je len jednou z možností využitia blockchainu. Blockchain tiež môže byť využívaný napríklad pri riešení otázok týkajúcich sa vlastníctva, identifikácie atď., kde je existencia jedinej centrálnej strany nežiadúca. Na blockchaine sú uložené aj programy nazývané smart kontrakt (chytrá zmluva, ďalej bude využívaná iba anglická forma, pretože to je tak zvykom aj medzi odborníkmi v obore). Pojem smart kontrakt a jeho význam bude vysvetlený v podkapitole 2.5.

2.3 Kryptomenová peňaženka

Kryptomenová peňaženka je typicky aplikácia alebo zariadenie, ktoré sa používa na zabezpečenie súkromného kľúča. V kryptomenovej peňaženke nie sú uložené samotné mince kryptomien. Peňaženka však uchováva súkromný kľúč k týmto minciam, ktoré sú zaznamenané na blockchaine[31, 50]. Pri vytvorení kryptomenovej peňaženky sa vygeneruje seed, (bližší popis v samostatnej podkapitole 2.4) ten je potrebné si zapísať. Na svete existujú rôzne typy peňaženiek, za najbezpečnejšie sú považované hardvérové peňaženky, ďalej hlavne medzi začiatočníkmi používané sú hostované peňaženky na strane servera alebo taktiež rozšírené softvérové peňaženky. Všetky spomenuté aj všetky ostatné typy peňaženiek majú svoje výhody aj nevýhody. Viac o kategorizácii kryptomenových peňaženiek v kapitole 3.

2.4 Seed - inicializačný vektor pre generátor kľúča

Mnemonic je zoznam slov v špecifickom poradí, v ktorom sú uložené všetky informácie potrebné na obnovenie peňaženky. Mnemonic seed sa transformuje na seed, ktorý je následne

používaný v kryptografických primitívach. V praxi ide zvyčajne o kombináciu 8, 12 alebo 24 náhodne zvolených slov. Tieto slová sú kódom pre peňaženku na to, ako vygenerovať prvý a následne aj všetky ďalšie súkromné kľúče. Súkromný kľúč je náhodne vygenerované číslo, ktoré by mal poznať iba vlastník adresy a môže sa použiť na míňanie prostriedkov spojených s konkrétnou adresou. Ide o 256-bitové číslo, zvyčajne v hexadecimálnom formáte – 64 znakov alebo 32 bajtov v rozsahu nula až deväť alebo A až F. Seed je potrebné zapísať na papier a ten následne uložiť na bezpečné miesto, aby k nemu mali prístup ideálne len oprávnené osoby[31, 42]. Nikdy by nemala byť zhotovená digitálna kópia tohto seedu. Hoci by bolo jeho uloženie online alebo v počítači prístupnejšie, malo by to za následok značné bezpečnostné riziko. V prípade straty, zničenia alebo zabudnutia hesla kryptomenovej peňaženky slúži seed na obnovu používateľovej peňaženky. Po zadaní správnej postupnosti 8, 12 alebo 24 slov, deterministická peňaženka použije seed ako vstupný parameter pre vygenerovanie kľúča a preverí všetky súkromné kľúče vytvorené algoritmom. Pri kontrole je jedno či sú na kľúč už naviazané nejaké mince alebo nie.

2.5 Smart kontrakt

Smart kontrakt je program, ktorý sa spustí v prípade splnenia počiatočných podmienok. Štandardné príklady smart kontraktov sú napríklad aukcie, podmienečné zmluvy alebo poistenie. Kód kontraktu je verejne viditeľný a nedá sa zmeniť. Smart kontrakt je podpísaný zainteresovanými stranami a odstraňuje potrebu dôvery v tretí subjekt[9, 31]. Zmena stavu kontraktu sa vykonáva pomocou transakcií, ktoré volajú metódy. V blockchaine dochádza k modifikácii stavu jednotlivých kontraktov, prostredníctvom vykonávania kódu týchto smart kontraktov. Kryptomena Ethereum využíva skriptovací jazyk Solidity, ktorý umožňuje vykonávanie výpočtov v rámci blockchainu a je používaný pri vytváraní smart kontraktu. Smart kontrakt je platný akonáhle sú splnené všetky predom definované podmienky. Využíva kryptografiu, je viditeľný na blockchaine a funguje automaticky.

2.6 Ťažba

Ťažba je proces, ktorým sa do obehu dostávajú nové mince a taktiež je to proces ako v decentralizovanom systéme dosiahnuť konsenzus, teda súhlas a zhodu v tom čo sa stalo a čo nie. V decentralizovanom systéme sú kontrolované a overované transakcie, ktoré by mali byť zrealizované jednotlivými užívateľmi. Tento proces vytvárania konsenzu majú za úlohu ťažiari[25]. Pri ťažbe je dôležitá kontrola či v sieti nedošlo napríklad ku duplicitnej transakcií alebo či je dostatočný zostatok na vykonanie transakcie. Počas ťažby sú riešené zložité matematické problémy pomocou hardvérových zariadení akými sú GPU, FPGA alebo zariadenia ASIC (z angl. Application Specific Integrated Circuit), ktoré boli vyvinuté špeciálne na riešenie ťažobných úloh. Odmenou pre ťažiarov za overovanie transakcií, napríklad pri Bitcoine, je súčet transakčných poplatkov, ktoré používatelia zaplatili spolu s odmenou za vyťaženie daného bloku.

Kapitola 3

Kategorizácia kryptomenových peňaženiek

Efektívnosť a bezpečnosť správy privátnych kľúčov je výzvou pre každý kryptografický systém. Vlastníctvo súkromných kľúčov dáva užívateľovi oveľa väčšiu silu a kontrolu, no zároveň to znamená, že sa užívateľ musí starať o ich bezpečnosť. V prípade, že by sa útočník nejakým spôsobom dostal ku privátnym kľúčom v peňaženke, bol by schopný ukradnúť všetky mince z verejných adries. Ten, kto má prístup k súkromnému kľúču je takpovediac disponent peňaženky. Preto jednou z najdôležitejších súčastí kryptografického systému je bezpečná správa kľúčov. Žiadna infraštruktúra sa nepovažuje za bezpečnú, pokiaľ nie sú zabezpečené aj jej kľúče. Kapitola popisuje rôzne kategórie kryptomenových peňaženiek[22, 30, 43].

3.1 Papierová peňaženka

Tento spôsob bol populárny najmä v počiatočných rokoch od vytvorenia Bitcoinu. Pri papierovej peňaženke ide o zastaralý a nebezpečný spôsob spravovania kryptomien. Keďže peňaženka uchováva súkromné kľúče offline, jej výhodou je poskytnutie zabezpečenia proti kybernetickému útoku a škodlivému malvéru[2]. Peňaženka obsahuje súkromné kľúče vytlačené v textovej forme alebo vo forme QR kódu na papieri. Takýto typ je väčšinou používaný ako forma zálohy. Papierové peňaženky vyžadujú použitie tlačiarne pre vytlačenie peňaženky na papier, avšak ak by zostala peňaženka uložená na internom úložisku tlačiarne, znamenalo by to veľké bezpečnostné riziko. Ďalšou nevýhodou je neodolnosť papiera proti ohňu a vode. Papierová peňaženka nedokáže vytvárať adresu pre každú prichádzajúcu transakciu, má iba jednu adresu, ktorá je opätovne využívaná. Pre spravovanie kryptomien je vhodnejšie použiť modernejšie a hlavne bezpečnejšie alternatívy kryptomenových peňaženiek, tieto alternatívy sú spomenuté nižšie. Tento typ kryptomenovej peňaženky nebude v práci testovaný ale je nutné spomenúť, že existujú aj peňaženky tejto kategórie, pretože úzko súviseli s kryptomenami už od ich vzniku.

3.2 Peňaženky s privátnymi kľúčmi uloženými na lokálnom úložisku

V tejto kategórií peňaženiek sú privátne kľúče uložené na lokálnom úložisku zariadenia, kde sú dostupné softvérom kryptomeny zo špecifického umiestnenia, akým je napríklad data-

báza alebo konfiguračný súborový systém klienta. Výhodami takéhoto spravovania kľúčov je efektívny a rýchly prístup potrebný pre vykonanie akejkoľvek transakcie. Na úložisko je možné uložiť neobmedzený počet kľúčov z dôvodu ich malej veľkosti. Užívateľ nie je ďalej zaťažený prácou s týmito kľúčmi pretože sa o všetko ostatné stará softvér, ktorý dokáže ďalej automaticky generovať kľúče alebo vytvárať transakcie bez ďalších vstupov/akcií zo strany užívateľa. Nevýhodou tejto kategórie je bezpečnosť systému pred škodlivými softvérmi uloženými v rovnakom zariadení, fyzickému prístupu ku zariadeniu alebo fyzickému poškodeniu daného zariadenia. Príklad takéhoto typu peňaženky je MyEtherWallet[41], ktorá bude popísaná a testovaná v kapitole 6.

3.3 Heslom chránené peňaženky

Heslom chránené peňaženky vyžadujú užívateľom zadané heslo alebo prístupovú frázu na šifrovanie/dešifrovanie súkromného kľúča uloženého na lokálnom úložisku. Bezpečnosť tohto systému je založená na sile hesla. V prípade neoprávneného prístupu k zariadeniu práve heslo bráni prístupu k uloženým súkromným kľúčom alebo fyzickej krádeži. Pri každodennom používaní a vytváraní nových transakcií musí byť peňaženka odomknutá zadaným heslom. Kategória s heslom chránenou peňaženkou zdieľa s drobnými rozdielmi svoje výhody aj nevýhody s nešifrovanými peňaženkami. V prípade straty/zabudnutia hesla je stratený celý zostatok ich heslom chránenej peňaženky, pretože neexistuje mechanizmus na obnovu hesla. Zneužitie tohto typu peňaženky môže byť spôsobené využitím napríklad útoku hrubou silou na heslo súboru obsahujúceho súkromné kľúče po odcudzení peňaženky. Ochrana pomocou hesla sa zdá byť menej efektívna pri digitálnej krádeži. Ak je na zariadení, kde sa nachádza peňaženka, nainštalovaný malvér s účelom zaznamenávania stlačenia jednotlivých klávesov, sú tým výrazne obmedzené výhody peňaženky zabezpečovanej pomocou hesla. Táto kategória peňaženiek môže používateľa zmiasť tým, že samotné heslo poskytuje prístup k ich finančným prostriedkom bez ohľadu na umiestnenie zariadenia obsahujúceho peňaženku tak, ako je tomu pri tradičnom internetovom bankovníctve, avšak na novom zariadení je potrebné aby bol okrem správne zadaného hesla prenesený aj súbor s peňaženkou. Príklad takéhoto typu peňaženky je Electrum Wallet[20] a MyEtherWallet (offline)[41], ktoré budú popísané a testované v kapitole 6.

3.4 Heslom derivované peňaženky

Heslom derivované peňaženky dokážu vypočítať postupnosť privátnych kľúčov iba na základe mnemotechnického reťazca, hesla, prípadne oboch zároveň. Niektoré heslom derivované peňaženky umožňujú užívateľovi vybrať krátku prístupovú frázu za účelom neskoršieho vygenerovania dlhšieho seedu zo zvolenej prístupovej frázy za pomoci funkcie (napr. PBKDF2[1]). Takýto prístup môže za pomoci útoku hrubou silou odhaliť slabé alebo krátke heslá. Doporučením pri výpočte seedu heslom derivovanej peňaženky je nechať peňaženku pseudo-náhodne vygenerovať mnemotechniku s dĺžkou rovnajúcou alebo presahujúcou 128 bitov, a následne vyrobiť seed za pomoci odvodzovacej funkcie PBKDF2. Navyše prístupová fráza zadaná užívateľom môže byť následne pridaná ako doplnok pri vytváraní seedu za účelom čiastočného zvýšenia ochrany voči fyzickej krádeži. Kľúče v tomto type peňaženky sú užívateľovi poskytované na ovládanie samotnej peňaženky ako pár verejno-súkromného kľúča. Hlavnou nevýhodou k takémuto prístupu ku kľúčom je nedostatočne silné heslo,

[1] PBKDF2 - odvodzovania funkcia, používaná za účelom lepšieho zabezpečenia proti útoku hrubou silou

ktoré môže byť prelomené za pomoci útoku dúhovej tabule a útočník sa tak môže zmocniť súkromného kľúča. Príklad takéhoto typu peňaženky je Daedalus Wallet[18], ktorá bude popísaná a testovaná v kapitole 6.

3.5 Hardvérové peňaženky

Peňaženky tejto kategórie patria k najbezpečnejším peňaženkám z dôvodu toho akým spôsobom uchovávajú súkromné kľúče. Jedná sa o spojenie toho najlepšieho z dvoch svetov offline bezpečnosti a online komfortu. V zapečatenom úložisku zariadení je uložený súkromný kľúč, ktorým sú podpisované všetky transakcie, tento kľúč je uložený iba v danej peňaženke. Hardvérové peňaženky možno považovať aj za špeciálny prípad offline úložiska. Tieto peňaženky sú podobné USB kľúču, fungujú však opačne, s počítačom začnú komunikovať až po zadaní správneho hesla. Pri podpise transakcie užívateľ pripojí k zaradeniu svoju peňaženku a po zadaní správneho hesla užívateľom sú na displeji zariadenia zobrazené údaje o transakcii. Tieto údaje si následne užívateľ overí a po potvrdení prechádza transakcia do stavu podpísaná. Obnova hardvérovej peňaženky je podobná obnove tej softvérovej. Príklad takéhoto typu peňaženky je CoolWallet[17], Trezor[53], Ellipan titan[21], ktoré budú popísané a testované v kapitole 6.

3.6 Peňaženky s rozdeleným overovaním za použitia prahovej kryptografie

V prípade tejto kategórie ide o overovanie transakcie za pomoci viacerých zariadení obsahujúcich časť súkromného kľúča[28]. Súkromný kľúč je namiesto uloženia na jednom zariadení rozdelený na niekoľko častí, kde každá časť je uložená v inom zariadení. Je určený počet, koľko zariadení musí verifikovať transakciu na to aby bola podpísaná. To značí, že ľubovolná transakcia bude vykonaná až v momente, keď bude spolupracovať dostatočný počet zariadení. Na blockchaine je uložená iba jedna verifikácia transakcie, avšak n verifikácii je vytvorených spoluprácou dostatočného množstva zariadení, na základe týchto verifikácií je vypočítaný podpis. Všetky výpočty týkajúce sa spolu-podpisovania transakcie sú vykonávane mimo blockchain, čím je dosiahnutá anonymita prístupu na rozdiel od kategórie s použitím viacerých podpisov, kde sú všetky podpisy viditeľné na blockchaine. V prípade útoku na peňaženku prelomenie ľubovolného počtu zariadení až po prahovú hodnotu nedovolí útočníkovi ukradnúť akékoľvek prostriedky alebo informácie o kľúči. Ak spoločnosť zvolí hranicu prahu na t, aby spoločnosť podpísala transakciu musí vytvoriť $2t+1$ zariadení. Z celkového počtu $2t+1$ zariadení sa tak útočník môže zamerať na viac zariadení, z ktorých mu stačí prelomiť $t+1$ zariadení.

3.7 Peňaženky s rozdeleným overovaním za použitia viacerých podpisov

Peňaženky tejto kategórie majú potenciál zvýšiť bezpečnosť finančných prostriedkov. Technológia overovania za použitia viacerých podpisov autorizuje transakciu z adresy viacerých vlastníkov, kde na overenie transakcie je vyžadovaná spolupráca minimálne n počtu spoluprác z m počtu držiteľov súkromných kľúčov[29]. Zvyčajne je požadovaný počet podpisov menší ako je počet vlastníkov, čo v praxi značí, že nie všetci vlastníci musia transakciu pod-

písať. V prípade ak by sa útočník zmocnil prístupu k menšiemu počtu peňaženiek ako je n, nemá možnosť podpísať transakciu. Vo väčšine prípadov je možná aktualizácia množiny vlastníkov aj počtu požadovaných podpisov[19]. Nevýhodou je, že viac-podpisová peňaženka nemá záložný mechanizmus pre obnovu peňaženky. V prípade straty prístupu k väčšiemu počtu viac-podpisových peňaženiek, užívatelia stratia aj prístup k ich minciam. Príklad takéhoto typu peňaženky je Electrum Wallet[20] a BitPay wallet[5], ktoré budú popísané a testované v kapitole 6.

3.8 Hostované peňaženky

Hostované peňaženky poskytujú používateľovi internetové rozhranie určené na interakciu s blockchainom, manažovanie kryptomien alebo prezeranie historických transakcií. Ak hostovaná peňaženka obsahuje aj súkromné kľúče jedná sa o peňaženku na strane servera. V prípade, že sú súkromné kľúče umiestnené u užívateľa v prehliadači ide o peňaženku na strane klienta. Takýto typ peňaženky je nazývaný aj ako hybridná peňaženka. Peňaženky s uloženým súkromným kľúčom na serveri sa správajú ako banky. V tomto type peňaženky užívateľ presúva dôveru a zodpovednosť za bezpečnosť na tretiu stranu.

Peňaženky na strane servera

Najznámejšími peňaženkami tohto typu sú Coinbase[12] a Binance[4], ktoré sú zároveň aj zmenárňami. Tieto peňaženky užívateľovi poskytujú správu súkromných kľúčov a zabezpečenie ich kryptomien. Užívateľovi nie je známy jeho súkromný kľúč ale ako kompenzácia je mu ponúknuté užívateľsky prívetivé rozhranie a dostupnosť z akéhokoľvek zariadenia s pripojením na internet, túto možnosť často volia začiatočníci v oblasti kryptomien. Výhodou takéhoto typu kryptomenovej peňaženky je jej podpora veľkého množstva kryptomien, ktoré nemusia byť podporované v peňaženkách iných kategórii. Servery poskytujú užívateľom aj možnosť dvojfaktorovej autentifikácie (2FA), užívateľ má možnosť výberu medzi overením prostredníctvom SMS alebo prostredníctvom kódu z aplikácie Google autentifikátor. Potenciálnou nevýhodou, ako sa aj v histórii ukázalo, môže byť napríklad nedostupnosť peňaženky v prípade útoku za účelom odoprenia služby. Coinbase peňaženka[12] bude popísaná a testovaná v kapitole 6.

Peňaženky na strane klienta

Peňaženkami tohto typu sú Metamask[39], Coinbase wallet[13], Coinomi[16], Blockchain wallet[6], Green Bitcoin wallet[7], Blue wallet[8] a Exodus[24]. Tieto peňaženky sú typu heslom derivovaných peňaženiek. Blockchain peňaženka ponúka možnosť dvojstupňovej ochrany prostredníctvom SMS, emailom alebo prostredníctvom kódu z aplikácie Google autentifikátor. Pri vytvorení transakcie ju môže jednoducho podpísať zadaním hesla. Peňaženka Coinomi na rozdiel od peňaženky Blockchain si neuchováva zálohu šifrovaných kľúčov na serveri. Spomínané peňaženky budú popísané a testované v kapitole 6.

3.9 Peňaženky s rozdeleným overovaním za použitia Smart kontraktu

Smart kontrakt poskytuje užívateľovi pravidlá ako môžu jednotlivý vlastníci minúť kryptomeny v kontrakte, aby boli zachované aktuálne nastavenia na blockchaine. Používa sa

tu overovanie pomocou viacerých podpisov. Takýto typ ochrany je možné dosiahnuť za pomoci viacerých hardvérových peňaženiek napríklad od firmy Trezor[53], ktorá ju podporuje. Nevýhodou je nutnosť zakúpenia viacerých zariadení čo je finančne náročnejšie. Najpoužívanejšou schémou je podpísanie transakcie za použitia 2 z 3 zariadení.

Kapitola 4

Softvérové a hardvérové hrozby pre kryptomenové peňaženky

Hrozba je pojem, ktorým je označované riziko nejakej negatívnej udalosti v prípade softvérovej a hardvérovej hrozby. V spojení s kryptomenovými peňaženkami ide hlavne o riziko, že užívateľ nenávratne stratí všetky svoje prostriedky. Užívateľ by sa mal chrániť pred hrozbami či už softvérovými alebo hardvérovými, ktorými môžu byť napadnuté jeho kryptomenové peňaženky. V prípade zanedbania ochrany peňaženky alebo v prípade nepozornosti môže užívateľ stratiť kontrolu nad všetkými svojimi prostriedkami. V tejto kapitole budú rozobraté jednotlivé hrozby či už softvérového alebo hardvérového charakteru. Taktiež budú v kapitole popísané opatrenia proti týmto hrozbám pre rôzne typy kryptomenových peňaženiek[22, 30]. Kapitola nerozoberá útok za účelom odoprenia služby, pri ktorom sa útočník snaží užívateľom zabrániť prístupu k internetovej službe, v tomto prípade prístup ku kryptomenovej peňaženke. Tento útok síce súvisí s kryptomenovými peňaženkami, avšak nie je náplňou práce, preto nie je v práci ďalej spomínaný.

4.1 Útok hrubou silou

Takýto typ útoku je charakteristický tým, že jeho účelom je prelomenie alebo dešifrovanie hesiel skúšaním všetkých možných kombinácií stlačenia klávesov, pri ktorých pravdepodobnosť úspechu závisí od úrovne zabezpečenia týchto hesiel. Takýto útok na prelomenie hesla môže byť vykonaný ako online tak aj offline spôsobom[49]. Útok hrubou silou je dlhším a intenzívnejším typom útoku ako napríklad slovníkový útok, ktorý sa pokúša prelomiť heslo za pomoci predpripraveného slovníka. Názov hrubou silou preto, lebo sa vyznačuje veľkým počtom pokusov o prelomenie hesla. Obtiažnosť útokov hrubou silou rastie exponenciálne, čím dlhšie je heslo alebo kľúč, tým je pre útočníka náročnejšie jeho získanie. Dĺžka času potrebného na prelomenie hesla teda môže byť predĺžená použitím väčšieho počtu znakov pri vytváraní hesla, pridaním špeciálnych znakov alebo číslic do hesla. Ťažba kryptomeny a útok hrubou silou majú spoločnú vlastnosť, ktorou je možnosť využívania GPU a ASIC zariadení. Tieto zariadenia sú navrhnuté tak, aby zvládli veľké množstvo opakujúcich sa úloh za čo najkratší možný čas. To isté potrebuje aj útočník pri útoku prostredníctvom využitia hrubej sily.

4.2 Slovníkový útok

Slovníkový útok je veľmi podobný tomu hrubou silou, jedná sa o jeho pokročilejšiu variantu pričom rozdielom je počet pokusov o permutácie hesla. Pomocou tohto útoku sa útočník pokúša o prelomenie užívateľského hesla skúšaním všetkých možných hesiel z pripraveného slovníka. Slovník obsahuje kľúče, o ktorých útočník predpokladá, že by mohli byť zvolené ako heslo a tieto kľúče háda, kým nenájde správnu kombináciu. Heslo môže pozostávať napríklad zo zoznamu bežne používaných hesiel, obľúbených mien, mien domácich miláčikov, filmových alebo televíznych postáv a ďalších slov, ktoré sa môžu vyskytovať v hesle[56]. Slovníkové útoky sú vo svete bežné. Práve tento typ útoku bol najúspešnejším útokom, aj v prípadoch, keď boli užívatelia donútený vytvárať netriviálne a silné heslá. V tomto type útoku sa môže vyskytovať aj určitý prvok náhodnosti akým je pripájanie číslice, prípadne špeciálneho znaku na koniec slova alebo nahradenie písmena číslom s vizuálnou podobnosťou (napr. O a nula). Offline útoky hrubou silou alebo slovníkovým útokom sú obmedzené iba výpočtovým výkonom, ktorý má útočník k dispozícii. Pri správnom nastavení môžu byť zabezpečené súbory, šifrovacie kľúče alebo heslá odhalené v krátkom čase. Ako bezpečnostné opatrenie proti útoku na hašové funkcie sa používa salt (kryptografická soľ), ktorá je generovaná náhodne pre každé heslo a typicky je použitá pri vytváraní kľúča pridaním k zašifrovanému heslu.

4.3 Evil maid

Evil maid (útok zlej slúžky, ďalej bude využívaná iba anglická forma), je typ útoku z kategórie fyzických útokov. „Evil maid“ sa nazýva preto, že takýto útok môže byť ľahko vykonaný hotelovou slúžkou, keď si majiteľ nechá v hotelovej izbe svoje zariadenie bez dozoru. Pri tomto type útoku stačí útočníkovi fyzický prístup k zariadeniu, ktoré môže byť aj vypnuté[51]. Útočník okrem fyzickej krádeže zariadenia môže tiež modifikovať obsah disku za použitia Full Disk Encryption kódu (kód na úplne šifrovanie disku) a následne ponechať zariadenie majiteľovi. Neskôr kód v zariadení po zadaní hesla majiteľom môže tento kľúč zaslať útočníkovi, ktorý tak získa potrebné informácie o zariadení. Preto je nevyhnutné ako ochrana proti tomuto útoku aby systém uistil užívateľa, že práve spustený systém je dôveryhodný a nie je napadnutý žiadnym malvérom. Tento typ útoku možno vykonať aj fyzickým otvorením zariadenia, úpravou jeho interného hardvéru a následného uzavretia zariadenia do jeho pôvodnej podoby. Keďže útočník na vykonanie útoku potrebuje fyzický prístup k zariadeniu, je možné predísť takémuto druhu útoku nasledujúcim spôsobom. Užívateľ bude mať svoje zariadenie neustále pod drobnohľadom. V prípadoch kedy takáto možnosť nie je reálna, užívateľ môže napríklad uzamknúť zariadenie v zamykacej skrinke a tým zamedziť prístup nepovolaným osobám. Ochrane proti útoku môže pomôcť aj vynucovanie silných hesiel a nastavenie časového limitu uzamknutia obrazovky na zariadení, prípadne nastavenie BIOSu tak, aby zamedzil priamy prístup k pamäti zariadenia cez komunikačné porty. Útoku Evil maid je ľahšie predísť, no je náročné ho odhaliť, keď sa užívateľ stane jeho obeťou.

4.4 Špionážny softvér keylogger

Keylogger je typ malvéru, ktorý zariadenie priamo neohrozuje, avšak zlomyseľne zaznamenáva stlačené klávesy užívateľa za účelom získania jeho hesiel a ďalších potenciálne citlivých

informácií o užívateľovi. V prípade, že keylogger úspešne prenikne do počítača, nainštaluje sa, začne bežať na pozadí a pomocou kľúčových slov vyhľadáva kryptomenové aplikácie. Cieľom je ukradnúť heslá z maximálneho počtu kryptomenových aplikácií spustených na počítači. Program zaznamenáva všetky stlačenia klávesov a taktiež aj programy v ktorých boli tieto klávesy stlačené[54]. V tomto type útoku možu byť okrem spomenutých možností zaznamenané aj užívateľom navštívené adresy vo webovom prehliadači. Hlavným cieľom na zaznamenávanie stlačených klávesov je klávesnica, pretože ide o najpoužívanejšie používateľské rozhranie pripojené k počítaču. Keylogger existuje ako v hardvérovej tak aj v softvérovej podobe, avšak softvérové keyloggery sú vo svete rozšírenejšie. Antimalvérovým programom býva keylogger považovaný ako typ špionážneho softvéru. Prevencia proti takémuto typu malvéru je mať na zariadení nainštalovaný antimalvérový program, vyhýbať sa otváraniu rôznych podozrivých odkazov a neznámych príloh. Používateľom je odporúčané využívanie všetkých bezpečnostných opatrení a protokolov, ktoré mu ponúka poskytovateľ služieb. Dôležité je povolenie 2FA, pre odchádzajúce transakcie zas využívať potvrdenie vyžadujúce zadanie PIN kódu a taktiež pravidelné antimalvérové kontroly na odhalenie a odstránenie keyloggerov, v prípade, že boli nainštalované v počítači. Najlepším spôsobom však je využívanie najbezpečnejších kryptomenových peňaženiek akými sú aktuálne rôzne hardvérové peňaženky, ktoré sú chránené proti takémuto typu útoku. Dôvodom je, že veľká časť úkonov je vykonávaných priamo prostredníctvom tlačidiel peňaženky a sú tak izolované od internetu.

4.5 Man in the middle

Man in the middle (útok človeka uprostred, ďalej bude využívaná iba anglická forma, pretože to je tak zvykom aj medzi odborníkmi v obore), je druh kybernetického útoku, pri ktorom dochádza k neschválenému vstupu útočníka do korešpondencie medzi dvomi subjektmi, ktoré netušia, že je ich komunikácia odpočúvaná. Malvér tohto typu často monitoruje informácie vymieňané medzi subjektmi, tieto informácie môže však aj upravovať alebo nahradiť. Tento problém postihuje zväčša kryptografické systémy, v ktorých absentuje zabezpečenie pomocou autentifikácie[37]. Útoku je možné predchádzať autentifikáciou alebo detekciou manipulácie. Autentifikácia poskytuje určitý stupeň spoľahlivosti v tom, že daná správa pochádza z legitímneho zdroja a detekcia manipulácie zobrazí či mohla byť daná správa zmenená útočníkom. Užívateľ by sa mal v rámci prevencie proti tomuto útoku vyhýbať heslom nezašifrovaným internetovým pripojeniam, mal by dbať na upozornenia internetového prehliadača týkajúce sa hlásenia o nezabezpečenej stránke, prípadné okamžité odhlásenie zo zabezpečených účtov v čase nepoužívania. Taktiež je vhodné používanie zabezpečených komunikačných protokolov akými sú HTTPS (zabezpečený hypertextový prenosový protokol) alebo TLS (protokol pre zabezpečenie transportnej vrstvy).

4.6 Postranný kanál

Útok postranným kanálom využíva dodatočné informácie unikajúce z praktickej implementácie, najčastejšie sú tieto útoky zamerané na získanie citlivých informácií vrátane kryptografických kľúčov. Takýto útok sa využíva na extrakciu materiálu kryptografického kľúča a verejných kľúčových šifrovacích algoritmov[27, 52]. V prípade útoku postranným kanálom ide o neinvazívny útok, zariadenie je sledované v normálnom prevádzkovom režime bez akéhokoľvek fyzického poškodenia a je napadnuté priamo cez dostupné rozhrania.

Tento typ útoku nevyžaduje nákladné vybavenie, ako je tomu pri invazívnych útokoch. Predstavuje veľké riziko pre vstavané systémy, útok zhromažďuje informácie alebo ovplyvňuje vykonávanie programu v systéme. Útok môže byť tiež označovaný ako útok na bočný panel alebo implementačný útok. Takýto typ útoku zvyčajne vyžaduje podrobné znalosti o systéme, na ktorom má byť tento útok vykonaný. Existuje jeden špecifický problém výrobcov kryptomenových peňaženiek, ktorí používajú univerzálny mikrokontrolér. Spôsob, akým sú peňaženky skonštruované, nie je odolný proti útokom zameraným na implementačnú chybu súvisiacu s použitím mikrokontroléru, táto chyba môže v prípade útoku viesť k nežiadúcemu správaniu peňaženky[36]. Takýto mikrokontrolér využívajú napríklad hardvérové peňaženky ako Trezor One, Trezor T a KeepKey, sú preto náchylné na spomínaný typ útoku, ktorý umožňuje vyprázdniť flash pamäť MCU a extrahovať z neho zašifrovaný seed. Získaný seed môže byť následne dešifrovaný pomocou útoku hrubou silou. Trezor a Keepkey vydali doporučenie pre vytvorenie a používanie peňaženiek s vlastnou prístupovou frázou[46], ktorá nie je uložená v zariadení a musí byť vždy zadaná užívateľom. V prípade, že by útočník získal seed ale bez bezpečnostnej frázy, nebol by schopný sa zmocniť prostriedkov peňaženky, prístupová bezpečnostná fráza tak garantuje úplné zvýšenie bezpečnosti proti vyššie spomínanému útoku. Každá pridaná bezpečnostná fráza k seedu vygeneruje novú peňaženku. Možnosť ochrany pred útokom postranným kanálom je uchovávanie tajomstva implementácie a všetky podrobnosti týkajúcej sa implementácie nezverejňovať.

4.7 Fyzické pozorovanie a odolnosť proti nemu

Fyzické pozorovanie užívateľa môže byť spôsobené napríklad skenovaním jeho QR kódov prípadne zaznamenávaním stlačených klávesov užívateľom. Pozorovanie tohto typu môže viesť až k ukradnutiu účtu užívateľa zlodejom, ktorý tým získa plnohodnotný prístup ku všetkým prostriedkom v peňaženke. Ochranou proti takémuto pozorovaniu môže byť nepoužívanie kryptomenovej peňaženky na verejných miestach, kde by bolo rôznymi spôsobmi možné pozorovať prácu užívateľa s kryptomenovou peňaženkou.

4.8 Útok za účelom krádeže prostriedkov za pomoci malvéru (Clipping Attack)

Škodlivý malvér na zariadení nazývajúci sa clipping (strihanie, ďalej bude využívaná iba anglická forma, pretože to je tak zvykom aj medzi odborníkmi v obore) má za účel ukradnúť užívateľovi prostriedky zamenením skopírovanej adresy. Pri clippingu je tajne počas kopírovania nahradená adresa príjemcu, na ktorú chcel užívateľ prostriedky zaslať adresou útočníka. Užívateľ nič netušiac zasiela prostriedky na útočníkom zvolenú adresu[55]. Keďže všetky transakcie sú trvalé a nedajú sa zvrátiť, stáva sa tak užívateľ obeťou útoku, pri ktorom prišiel o všetky svoje zaslané prostriedky. Takémuto typu útoku sa dá jednoducho predísť overením či skopírovaná adresa, na ktorú budú prostriedky odoslané, je tou správnou. Inou možnosťou je vopred zaslať malé množstvo prostriedkov na požadovanú adresu a v prípade ak transakcia prebehne úspešne, následne môže byť užívateľom zaslaný zvyšok prostriedkov. Nevýhodou tohto spôsobu prevencie je potreba zaplatiť dvojnásobný poplatok za vykonanie transakcie.

4.9 Útok kryptomenovým prášením (Dusting Attack)

Prášenie je útok na kryptomenové peňaženky, pri ktorom dochádza k distribúcii nelegálnych prostriedkov z neznámeho zdroja legitímnym držiteľom kryptomien. Cieľom takéhoto typu útoku je poškodenie povesti peňaženky alebo spoločnosti, ktorá túto peňaženku vytvorila. Pri útoku sú nelegálne získané prostriedky distribuované na adresy patriace bežným vlastníkom kryptomien[44]. Kryptoprášenie je pre bežných užívateľov neškodné, avšak spoločnostiam vyrábajúcim kryptomenové peňaženky môže takýto typ útoku vážne uškodiť napríklad zhoršením reputácie, pretože môže prilákať nežiadúcu pozornosť týkajúcu sa nelegálnej činnosti.

Kapitola 5

Testovacie scenáre pre kryptomenové peňaženky

V kapitole budú rozobrané a popísané rôzne scenáre použiteľnosti a útokov predstavujúcich riziko pre kryptomenové peňaženky. Nasledujúce scenáre predstavujú hrozby[30, 22] ale aj užívateľmi najviac používané prípady využitia kryptomenových peňaženiek rôznych kategórií. Tieto kategórie peňaženiek budú testované scenármi zameranými na použiteľnosť a bezpečnosť voči hrozbám, ktoré sú v kapitole popísané nižšie. Týmto bude testovaná ich odolnosť proti konkrétnemu útoku a taktiež miera náročnosti potrebná na vykonanie bežných procesov spojených s kryptomenovými peňaženkami. Pri vytváraní kryptomenových peňaženiek, pokiaľ to daná peňaženka podporuje, bude využívaná testovacia sieť. Táto testovacia sieť je inštanciou blockchainu, ktorá sa používa na testovanie a experimentovanie bez rizika straty skutočných finančných prostriedkov. Mince v tejto sieti nemajú hodnotu a dajú sa voľne získať, sú tak odlišné od tých z hlavnej siete. Základným pravidlom pre užívateľa by malo byť uchovanie svojich prostriedkov tým najbezpečnejším dostupným spôsobom, ideálne odolným proti všetkým hrozbám spomenutým nižšie. Prelomenie ochrany kryptomenovej peňaženky by mohlo mať za následok stratu všetkých prostriedkov užívateľa. V prípade ak užívateľ zistí akýkoľvek náznak prelomenia ochrany svojej kryptomenovej peňaženky, mal by okamžite previesť všetky svoje zostávajúce prostriedky do inej bezpečnej kryptomenovej peňaženky. Všetky kryptomenové peňaženky boli pred testovaním riadne stiahnuté z oficiálnych stránok poskytovateľov, nainštalované a v prípade hardvérovej peňaženky prepojené so zariadením. V prípade Ellipal Titan a CoolWallet S išlo o prepojenie s mobilnou aplikáciou, v prípade zariadenia Trezor zas prepojenie poskytnutým USB káblom z balenia s počítačom, na ktorom bola spustená aplikácia Trezor Suite.

5.1 Konfigurácia kryptomenovej peňaženky

Tento súbor úloh je zameraný na založenie, nastavenie a prvé spustenie vybranej kryptomenovej peňaženky[40].

Po spustení aplikácie je potrebné zvoliť založenie novej peňaženky, v prípade ak peňaženka ponúka, zvoliť možnosť testovacej siete. Obvykle je táto možnosť dostupná pri výbere z ponuky peňaženkou podporovaných kryptomien alebo v rozšírených nastaveniach peňaženky.

Nasleduje odpísanie seedu z aplikácie na papier pomocou ceruzky a bezpečné uchovanie seedu offline spolu s nastavením názvu pre peňaženku.

V prípade, že o to peňaženka požiada tak sa nastaví PIN kód, potrebný pre odomykanie peňaženky, prípadne potvrdenie transakcie. Ak podporuje peňaženka pridanie prístupovej frázy, je vhodné zvoliť túto možnosť. Na adresu vytvorenej kryptomenovej peňaženky budú zaslané prostriedky potrebné pre vykonávanie ďalších testovacích scenárov.

Založenie lightning účtu

Peňaženka by mala byť využívaná na denné transakcie. Lightning network rieši problémy so škálovateľnosťou bitcoinu pomocou off-chainového prístupu. Väčšina bežných transakcií nie je zapísaná priamo do blockchainu ale do platobnej vrstvy nad ním, do blockchainu sa iba raz za čas zapíše nový stav účtov. Základným stavebným prvkom sú obojstranné platobné kanály vytvorené medzi dvomi protistranami, ide o špeciálne adresy, na ktorých platia sofistikovanejšie pravidlá ako na bežnej bitcoinovej adrese. Navrhnutá architektúra platobných kanálov umožňuje užívateľovi zaslanie prostriedkov inému užívateľovi, aj keď medzi sebou nemajú vytvorený kanál. Kľúčovými vlastnosťami siete sú rýchlosť platby, zníženie zaťaženia blockchainu a nie je tu potrebná dôvera v tretie strany. Veľkou výhodou lightning peňaženky oproti klasickej bitcoinovej, je rýchlo uskutočnená transakcia s neporovnateľne nižšími poplatkami.

Úlohou je okrem už vytvoreného účtu založiť aj lightning účet.

Znovuzískanie seedu po strate

Niektoré peňaženky ponúkajú, po procese autentifikácie, možnosť zobrazenia seedu prislúchajúceho danej peňaženke. Naskytuje sa otázka, či je bezpečné aby aplikácia poskytovala možnosť znovuzobrazenia seedu, keďže seed je nutné držať v bezpečí a offline. V prípade ak by sa útočník fyzicky dostal k zariadeniu a úspešne by nejakým typom útoku prelomil proces autentifikácie, bol by si v tom momente schopný zaslať všetky prostriedky peňaženky na svoju adresu a nepotreboval by k tomu poznať seed, ktorý je zobraziteľný po prihlásení v aplikácii. Papier s uloženým seedom sa môže ľahko stratiť, zničiť prírodnými živlami alebo ho v prípade potreby nebude mať užívateľ nablízku.

Po simulovanej strate papiera, na ktorom mal užívateľ zapísaný seed je cieľom poslednej úlohy znovuzískanie a zapísanie seedu, ktorý bol vygenerovaný pri vytváraní peňaženky.

5.2 Zasielanie prostriedkov

Zasielanie prostriedkov patrí k nevyhnutným procesom spojených nie len s kryptomenami. Transakcie pri kryptomenách sú bežnou záležitosťou, s ktorou sa skôr či neskôr stretne každý užívateľ. Kryptomenové transakcie sú nezvratné, zasielanie kryptomien akejkoľvek tretej strane alebo zaslanie na nesprávnu adresu môže mať za následok trvalú stratu finančných prostriedkov, preto je dôležité aby užívateľ vedel ako bezpečne a správne zaslať prostriedky z adresy A na adresu B. Súbor úloh na zasielanie prostriedkov je zložený z podúloh[40] v prípade, že peňaženka podporuje aj sieť lightning, je potrebné vykonanie úloh aj na tomto type bitcoinovej siete. Pred každým potvrdením transakcie v podúlohách je potrebné sa uistiť, že sú zadané údaje správne, ak sú pri prevode zadané nesprávne informácie, aktíva môžu byť nenávratne stratené.

Prvou podúlohou bude prihlásenie sa do peňaženky a vytvorenie transakcie daného množstva vybranej kryptomeny na platnú prijímaciu adresu, veľkosť poplatku a prioritizáciu transakcie neberieme v tejto podúlohe na vedomie.

Druhou podúlohou bude aktivácia dvojfaktorovej autentifikácie (2FA), ak to peňaženka podporuje a následne zaslanie prostriedkov na platnú prijímaciu adresu a to tak, aby odosielateľ zaslal maximálne možné množstvo mincí vybranej kryptomeny, ktoré po sčítaní s poplatkom za transakciu neprekročí vopred určené množstvo kryptomeny vyhradenej pre túto transakciu.

Treťou podúlohou je zaslanie prostriedkov daného množstva vybranej kryptomeny na platnú prijímaciu adresu, avšak bude zvolená najvyššia možná priorita transakcie tzn. väčší transakčný poplatok.

5.3 Vyžiadanie platby

Pri vyžiadaní platby je dôležité aby užívateľ zasielal vždy adresu patriacu príslušnej kryptomene. Adresy nie je vhodné používať viac ako jedenkrát, pre vyžiadanie platby je vhodné vždy vygenerovať novú adresu. V prípade ak by sa dostala tretia osoba k adrese, je schopná si pohľadať celú jej históriu, zostatky a všetky transakcie spájajúce sa s danou adresou. Nikdy by užívateľ nemal posielať svoj súkromný kľúč v domnienke, že ide o jeho adresu, na ktorú mu budú odoslané prostriedky. Súbor úloh na vyžiadanie/prijímanie prostriedkov je zložený z podúloh[40].

Prvou podúlohou bude zaslanie správnej adresy vybranej kryptomeny, na ktorú chceme aby nám užívateľ zaslal prostriedky.

Cieľom druhej podúlohy je, pokiaľ to aplikácia podporuje, vygenerovanie novej adresy a zaslanie k nej prislúchajúceho QR kódu používateľovi, ktorý si od nás tento kód vyžiadal aby mohol zrealizovať transakciu.

Poslednou podúlohou je vyžiadanie platby s požadovanou sumou, tak ako to môžeme poznať napríklad z internetového bankovníctva, po zadaní požadovanej čiastky, je vygenerovaná adresa a QR kód obsahujúci všetky potrebné informácie pre odosielateľa platby. Následne je táto adresa alebo QR kód zaslaný odosielateľovi.

5.4 Obnova peňaženky

V prípade, že užívateľ stratí svoju mobilnú alebo hardvérovú peňaženku alebo mu je odcudzená, tretia strana by potenciálne mohla získať prístup k jeho súkromnému kľúču. V takomto prípade je nutná obnova kryptomenovej peňaženky, ide o dôležitú súčasť procesu po strate prístupu ku pôvodnej softvérovej alebo hardvérovej peňaženke užívateľa. Pokiaľ si užívateľ zálohoval svoj privátny kľúč tak ako mal, nemala by pre neho byť táto strata fatálna, v tomto prípade je obnova prístupu ku prostriedkom jednoduchá. Pri zadávaní je dôležité aby užívateľ zadal slová z frázy na obnovenie v správnom poradí, inak nebude obnova peňaženky úspešná. V prípade správne zadanej frázy by mali byť prostriedky v peňaženke obnovené v priebehu niekoľkých sekúnd od importovania hesla. Po vykonaní úloh spojených s úspešnou obnovou peňaženky je nutné zaslať všetky prostriedky na vybranú adresu, tieto prostriedky budú využité na testovanie inej kryptomenovej peňaženky. Súbor úloh na obnovu peňaženky je zložený z niekoľkých podúloh[40].

Prvou podúlohou je simulácia straty prístupu k peňaženke vymazaním konkrétnej peňaženky alebo aplikácie v ktorej sa peňaženka nachádza.

Cieľom ďalšej podúlohy je opätovná inštalácia aplikácie a príprava frázy na obnovenie.

Treťou podúlohou je prihlásenie sa do pôvodnej peňaženky. V aplikácii je potrebné zvoliť možnosť obnovy peňaženky a do príslušného textového poľa zadať frázu na obnovenie.

V prípade podpory viacerých peňaženiek v aplikácii je vhodné aby mal užívateľ možnosť zmeniť názvy svojich peňaženiek.

5.5 Nastavenie zabezpečenia peňaženky

Súbor úloh na nastavenie zabezpečenia peňaženky je zložený z podúloh.

Prvou podúlohou je zmena PIN kódu. PIN kód nastavený pri vytváraní peňaženky zabraňuje neoprávnenému prístupu k prostriedkom.

Druhou podúlohou je nastavenie automatického odhlásenia po 5 minútovej doby nečinnosti. V prípadoch, keď je kryptomenová peňaženka používaná na akomkoľvek zariadení, či už súkromnom alebo verejnom, je vhodné nastavenie automatického odhlásenia po určitej dobe nečinnosti. Automatické odhlásenie zabráni tretej strane vykonávať transakcie bez súhlasu vlastníka v prípade, že sa majiteľ zabudne odhlásiť zo svojej peňaženky. Taktiež umožní prácu s peňaženkou bez toho, aby neustále žiadala od užívateľa zadanie PIN kódu.

Cieľom ďalšej podúlohy je preto povolenie a nastavenie odomykania pomocou biometrie. Užívateľsky prívetivou funkcionalitou je možnosť autentifikácie peňaženky pomocou biometrických údajov akými sú napríklad odtlačok prsta a rozpoznanie pomocou tváre.

Poslednou podúlohou je nastavenie vlastného dôveryhodného uzlu. Ďalším dôležitým bezpečnostným faktorom pri tzv. lightweight peňaženkách[1] je možnosť výberu vlastného dôveryhodnému uzlu. Nevýhodou fungovania takýchto peňaženiek je závislosť od úplných uzlov, ktorými sú obsluhované na pripojenie k sieti Bitcoinu, tejto nevýhode je možno predísť nakonfigurovaním výberu vlastného úplného uzlu, považovaného užívateľom za dôveryhodný.

5.6 Podpisovanie a overovanie správ

Podpisovanie a overovanie správ je spôsob, ako dokázať, že užívateľ vlastní konkrétnu adresu. Užívateľ môže byť burzou požiadaný o podpis správy, aby ju následne mohla táto burza overiť a zistiť, či ide o vlastníka adresy alebo útočníka. Ďalším prípadom užitia môže byť zaslanie adresy odosielateľovi, na ktorú chceme aby nám odoslal prostriedky. Aby sme predišli hrozbe, kedy by niekto mohol zachytiť komunikáciu a zameniť adresu, môžeme za týmto účelom podpísať celý text a ku nemu pridať digitálny podpis. Príjemca si tak môže jednoducho overiť, že nikto správu nepozmenil, inak by vygenerovaný podpis nesúhlasil so správou a adresou. V prípade viac-podpisovej peňaženky môže byť overené, či dokáže užívateľ pomocou tejto adresy podpísať správu, ak áno, značí to jeho skutočnú kontrolu nad adresou. Súbor úloh na podpisovanie a overovanie správ je zložený z dvoch podúloh.

Prvou podúlohou je vygenerovanie podpisu správy s textom „*Ahoj svet!*“ a správnou adresou.

Druhou podúlohou je overenie správy zadaním vygenerovaného podpisu spolu s rovnakou adresou a textom ako pri podpisovaní správy.

5.7 Nasadenie a interakcia so smart kontraktom

Nie každá kryptomenová peňaženka podporuje proces nasadenia a interakcie so smart kontraktom. V prípade niektorých hardvérových peňaženiek je potrebné použitie ďalšej aplikáa-

[1] lightweight peňaženka - nesťahuje celý blockchain, namiesto celých blokov sú stiahnuté iba hlavičky blokov na overenie pravosti transakcií

cie, akou je napríklad Metamask, ktorá okrem iného umožňuje správu smart kontraktov a decentralizovaných aplikácii. Existuje mnoho programovacích jazykov, ktoré umožňujú písať smart kontrakty, najznámejšími a najpoužívanejšími sú Solidity (Ethereum, Polkadot) a Rust (Solana, Polkadot). Pre nasadenie (deploy) smart kontraktu pomocou peňaženky je potrebné poznať Byte code, rozhranie ABI/JSON a názov kontraktu.

Úlohou je nasadenie poskytnutého kontraktu na blockchain etherea, najprv je potrebné zadať Byte code a rozhranie ABI/JSON, to je možné po kompilácii kontraktu, následne je potrebné zadať názov pre kontrakt, ktorý bude nasadený na blockchain. V prípade, že sú vyššie spomenuté údaje vyplnené správne je nutné potvrdenie a podpísanie transakcie.

5.8 Pridanie ERC-20 tokenu

Aby mohla kryptomenová peňaženka podporovať akúkoľvek kryptomenu, musí mať implementované prostredie a naprogramované všetko, čo je potrebné pre podporu danej kryptomeny. Na eliminovanie tohto problému vznikol jednoduchý formát s názvom ERC-20 čo značí skratku pre Ethereum Request for Comments (žiadosť o pripomienky k sieti Ethereum). Ide o štandard pre tokeny na báze Etherea, ktorý umožňuje novovytvoreným ERC-20 tokenom komunikovať so softvérom a službami podporujúcimi tento štandard. Vytvorenie ERC-20 tokenu je rýchle a jednoduché, čo má za následok, že v súčasnosti existuje niekoľko desiatok tisíc tokenov ERC-20, z ktorých väčšina nemá žiadnu trhovú hodnotu. Keďže v komunite existuje množstvo obľúbených ERC-20 tokenov, je nutné aby bolo pre užívateľa jednoduché si do svojej peňaženky, podporujúcej ethereum a jeho štandard, pridať požadovaný token.

Úloha je určená pre kryptomenové peňaženky podporujúce spomínaný štandard, cieľom je pridanie tokenov Tether USD a SHIBA INU, spĺňajúcich štandard ERC-20, do testovanej kryptomenovej peňaženky.

5.9 Odizolovanie peňaženky (Air-gap)

Air-gap (odizolovanie peňaženky, ďalej bude využívaná iba anglická forma) je bezpečnostné opatrenie izolujúce zariadenie od nedôveryhodnej siete akou je napríklad internet. Táto vlastnosť je pripísaná prístupu zahŕňajúcemu prevažne hardvérové zariadenie ukladajúc tajné informácie, ktoré nepotrebuje pripojenie k zariadeniu na vykonanie operácie. V prípade kryptomenových peňaženiek je podpisové zariadenie ako hardvérová peňaženka fyzicky izolovaná a nie je spojená s počítačom alebo mobilom[1]. Akákoľvek komunikácia medzi zariadeniami prebieha výlučne buď fyzickou výmenou SD karty alebo skenovaním QR kódov. Takýmto typom komunikácie sú prenášané transakcie, aktualizácia firmvéru alebo informácie o samotnej peňaženke. Namiesto pripojenia peňaženky do počítača používa hardvérová peňaženka Air-gap softvérovú aplikáciu nainštalovanú v zariadení užívateľa. V aplikácii bežiacej na zariadení je vytvorená transakcia zakódovaná napríklad v QR kóde, ktorý je následne načítaný pomocou hardvérovej peňaženky. Ďalšou možnosťou je uloženie transakcie na SD kartu, ktorá je vybratá zo zariadenia a vložená do peňaženky. Po tom čo je transakcia podpísaná peňaženkou je potrebné aby aplikácia v zariadení či už pomocou QR kódu alebo SD karty importovala podpísanú transakciu a tú následne odoslala do siete. Nevýhodou môže byť náchylnosť na útočníkom pozmenené QR kódy a taktiež potencionálne monitorovaný obsah SD karty, prípadne môžu byť zmenené jej súbory.

5.10 Manipulácia s klientom

Proti tomuto typu hrozby sú odolné prevažne hardvérové peňaženky, ktoré podpisujú transakciu v rámci zariadenia peňaženky, pričom tiež vyžadujú potvrdenie zobrazených údajov o transakcii na displeji zariadenia. Ďalej sú považované za odolné aj peňaženky obsahujúce viacero užívateľov, ktorý spolupracujú za účelom podpísania transakcie, v tomto prípade je nízka pravdepodobnosť zmanipulovania všetkých klientov. Čiastočne do tohto zapadá aj proces kedy peňaženka užívateľovi implicitne neposkytuje ochranu, ale namiesto toho vyžaduje dodatočné podmienky, ktoré je užívateľ nutný splniť.

5.11 Post-kvantová odolnosť

Kvantová výpočtová technológia by vďaka svojim vlastnostiam dokázala prelomiť množstvo aktuálne využívaných šifrovacích algoritmov. Neexistuje však dôveryhodná predpoveď, kedy by mohli byť kvantové počítače realitou, aj napriek tomu je ale nutné aby existovali šifrovacie techniky odolné aj v post-kvantovom svete[33]. Post-kvantová odolnosť je teda vlastnosť pripísaná prístupom využívajúcim kryptografiu založenú na hašovaní, ktoré je známe svojou odolnosťou voči útokom pomocou kvantových výpočtov. Predpokladá sa, že šifrovací algoritmus ako AES-256 a hašové algoritmy SHA3-384 a SHA3-512 budú bezpečné proti tejto technológií. Americký národný inštitút pre štandardy a technológie NIST (National Institute of Standards and Technology) však už pripravuje štandard zameraný na bezpečnosť v post-kvantovom svete. Pre momentálne vyvíjané technológie je doporučené, ako dočasné riešenie, využívať práve vyššie spomenuté algoritmy. Tieto technológie by mali mať schopnosť, v prípade bezpečnostnej hrozby, nahradiť použitý algoritmus za inú dostupnú a bezpečnejšiu alternatívu.

5.12 Odolnosť proti malvéru

Peňaženky odolné proti malvéru sú tie, ktoré nie sú uložené v zariadení s prístupom k internetu alebo zariadení bez schopnosti vykonávať výpočty. Za bezpečné sú považované peňaženky umožňujúce podpisovanie transakcií v rámci zariadenia alebo peňaženky poskytujúce zabezpečenie podpísania transakcie pomocou rozdelenia medzi väčší počet zariadení. V prípade peňaženiek uložených v mobilnom telefóne aj počítači, je ideálne používať antimalvérový softvér. Mobilné aplikácie by mali byť inštalované iba z oficiálnych obchodov a taktiež je nutné dbať na práva, ktoré sú aplikáciam udeľované. Na počítači neinštalovať neznámy a neoverený softvér, nenavštevovať a ani nič nesťahovať z pochybných webových stránok, prípadne neotvárať prílohy pochybných emailov[26, 48]. Toto všetko môže obsahovať nebezpečný malvér nie len pre peňaženky ale aj zariadenie, na ktorom je daná peňaženka uložená.

5.13 Kľúče uchovávané offline

Kľúče, ktoré nie sú priamo dostupné z internetu. Táto vlastnosť je pripísaná prístupom uchovávajúcim tajomstvá vo svojom zapečatenom úložisku a toto úložisko odhaľuje iba funkcionalitu na podpísanie transakcie. Za bezpečné sú považované napríklad papierové peňaženky a odizolované zariadenia (air-gapped).

5.14 Nezávislosť od dôvery v tretie strany

Táto závislosť sa vyskytuje hlavne pri hostovaných peňaženkách na strane servera. Závislosť je zvyčajne pripísaná dôvere bezpečnosti v server obsahujúci súkromné kľúče užívateľa. Peňaženky závislé od dôvery v tretie strany sú z kategórie hostovaných peňaženiek 3.8. Užívateľ svoje súkromné kľúče nepozná ani s nimi nemôže manipulovať. V prípade úspešného útoku na server môže užívateľ prísť o všetky svoje kryptomeny. Riešením môže byť využitie hardvérovej alebo softvérovej peňaženky nezávislej od dôvery v tretie strany. Užívateľ tak získa kontrolu nad svojím súkromným kľúčom a nebude sa ďalej musieť spoliehať na bezpečnosť servera.

5.15 Fyzická krádež a odolnosť proti nej

Fyzická krádež je nebezpečná pre každé zariadenie, v ktorom sú uložené nechránené alebo len čiastočne chránené súkromné kľúče. Užívateľ by mal svoju peňaženku zabezpečiť heslom prípadne PIN kódom a uchovať tak, aby k nej mali prístup iba povolané osoby. V prípade, že takýto spôsob zabezpečenia nie je možný, je dôležité zabezpečiť aspoň seed peňaženky, ktorý mu postačuje na obnovu peňaženky, ktorá bola fyzicky ukradnutá. Za odolné sú považované peňaženky zabezpečené heslom alebo PIN kódom, čiastočne odolné sú aj heslom nezabezpečené peňaženky využívajúce iný spôsob vynútenia jedinečnosti, napríklad párovanie cez bluetooth.

5.16 Strata hesla a odolnosť proti nej

Strata hesla môže viesť ku strate prístupu užívateľa ku svojím kryptomenám. Heslo ako také je nevyhnutný autentifikačný faktor pri procese prístupu k podpisovému kľúču. V prípade straty alebo zabudnutia hesla je dôležité aby peňaženka podporovala buď možnosť obnovy hesla alebo samotnú obnovu peňaženky. Proces obnovy peňaženky nevyžaduje zadávanie strateného hesla alebo PIN kódu. Hostované peňaženky so závislosťou od tretích strán umiestnené na serveri poskytujú určitý mechanizmus obnovy alebo resetovania hesla. Naopak, pri strate kryptomenovej peňaženky hardvérového či softvérového typu je mechanizmus obnovy rovnaký ako pri fyzickej krádeži peňaženky, a to zadanie seedu stratenej peňaženky do nového zariadenia alebo aplikácie peňaženky.

Kapitola 6

Systematické testovanie scenárov na kryptomenových peňaženkách

V tejto kapitole budú systematicky otestované vybrané kryptomenové peňaženky rôznych kategórií navrhnutými testovacími scenármi. Scenáre sú zamerané na použiteľnosť a bezpečnosť jednotlivých peňaženiek. Po otestovaní každej peňaženky bude popísané správanie testovanej peňaženky pri vykonávaní jednotlivých scenárov. Ďalej budú v podkapitolách popísané možnosti založenia, zabezpečenia, obnovy, rozšírených funkcionalít peňaženky a tiež aj vzájomná kompatibilita niektorých hardvérových a softvérových peňaženiek. V prípade testovacích scenárov zameraných na odosielanie a vyžiadanie prostriedkov ide o fundamentálne prípady užitia kryptomenových peňaženiek, preto budú popísané iba najdôležitejšie získané poznatky.

6.1 MyEtherWallet

MyEtherWallet je rozširujúca sa sada produktov, ktorá ponúka úplný prístup ku všetkému, čo ponúka blockchain Etherea. Pri testovaní používateľských scenárov bolo zistené, že peňaženka pri jej zakladaní vyžaduje od užívateľa nastavenie PIN kódu, ktorý si však musí užívateľ zapamätať, pretože neexistuje spôsob obnovy kódu. Pri vytváraní peňaženky nie je možné zvoliť sieť lightning, pretože peňaženka nemá podporu pre Bitcoin, taktiež nepodporuje ani možnosť 2FA. MyEtherWallet umožňuje využívať peňaženku aj bez toho aby bolo potrebné zapísanie seedu, avšak pri každom spustení aplikácie je používateľ vyzvaný aby si seed zapísal. V prípade neuloženia môže riskovať stratu svojich prostriedkov. Seed je možné zobraziť kedykoľvek po prihlásení do aplikácie. Testovacie scenáre na odosielanie prostriedkov prebehli bez akýchkoľvek komplikácií, avšak pri úlohách na vyžiadanie platby bolo zistené, že každému vytvorenému účtu v peňaženke prislúcha iba jedna adresa, história tejto adresy je tak ľahko dohľadateľná. V peňaženke bohužiaľ absentuje možnosť vytvorenia QR kódu obsahujúceho požadovanú sumu zadanú príjemcom pri procese vyžiadania platby. Po vykonaní úloh zameraných na nastavenie zabezpečenia, bolo zistené, že PIN zvolený pri vytváraní peňaženky nie je možné zmeniť. Jediný spôsob zmeny kódu je možný po obnove peňaženky. Taktiež si používateľ nemôže sám nastaviť čas, po ktorom by bol automaticky odhlásený po zvolenej dobe nečinnosti. Výhodou je možnosť odomykania a potvrdzovania transakcií pomocou odtlačku prsta alebo rozpoznávaním tváre. Ďalšou výhodou je, že peňaženka podporuje bezpečnostnú funkciu, ktorá v prípade, ak si užívateľ vytvorí snímku obrazovky na ktorej je zobrazený seed deteguje a následne užívateľa upozorní na možné

riziká spolu s výzvou na odstránenie snímky zo zariadenia. Keďže peňaženka nepodporuje kryptomenu Bitcoin, nie je možné nastaviť dôveryhodný bitcoin Electrum server. MyEtherWallet podporuje prepojenie aplikácie a webového rozhrania, toto webové rozhranie rozširuje funkcionalitu samotnej peňaženky. Na webe myetherwallet je vygenerovaný QR kód, ktorý po naskenovaní mobilnou aplikáciou prepojí účty. Takto prepojené účty poskytujú používateľovi možnosť podpisovania a overovania správ, nasadenia smart kontraktu a následnú interakciu s ním, prípadne pridanie ľubovolného ERC-20 tokenu. Peňaženka ponúka možnosť kompatibility s ďalšími hardvérovými peňaženkami prípadne internetovými rozšíreniami.

6.2 Metamask

MetaMask je open source[1] Web3[2] kryptomenová peňaženka, ktorú je možné použiť ako aplikáciu v mobilnom zariadení ale aj ako rozšírenie v rôznych prehliadačoch. Funguje ako most medzi bežnými prehliadačmi a blockchainom Ethereum. Peňaženka pri zakladaní vyžaduje nastavenie aspoň 8 znakov dlhého hesla, ktoré bude využívané na odomykanie peňaženky, zmena hesla je možná iba znovuobnovení peňaženky. Ďalej je generovaný seed zložený z 12 slov bez možnosti pridania bezpečnostnej frázy, tento seed si môže užívateľ zapísať aj neskôr, avšak je upozornený na potencionálne nebezpečenstvá. Peňaženka nepodporuje Bitcoin, nie je tak možné založenie lightning účtu ani nastavenie dôveryhodného Electrum serveru. Zasielanie prostriedkov prostredníctvom peňaženky je jednoduché a prehľadné, peňaženka pri odosielaní podporuje aj rozšírené nastavenia priority transakcie o možnosť nastavenia limitu poplatku alebo veľkosti poplatku za maximálnu prioritu. V peňaženke je možné vytvorenie viacerých účtov, pričom ku každému účtu patrí iba jedna adresa a QR kód. Pri vytvorení účtu je možné si zvoliť jeho názov, ktorý však už neskôr nie je možné zmeniť. V mobilnej aplikácii je možnosť vygenerovania QR kódu aj s požadovanou sumou, v internetovom rozšírení takáto možnosť absentuje.

Počas procesu obnovovania má užívateľ možnosť obnovy peňaženky s 12, 15, 18, 21 alebo 24 slovným mnemonic seedom, ktorý sa pri zapisovaní z bezpečnostného dôvodu zobrazuje ako reťazec za sebou nasledujúcich znakov „*“. Napísané slová je možné zobraziť aj v klasickej podobe kliknutím na tlačidlo pre odhalenie seedu. Zabezpečenie ponúka možnosť nastavenia časovača automatického odhlásenia, v mobilnej aplikácii podporuje okrem hesla aj odomykanie prostredníctvom biometrie. V nastaveniach je možnosť aktivácie detekcie phisingu, v tomto prípade sa zobrazujú upozornenia na phishingové domény zacielené na používateľov Etherea. Podpisovanie a overovanie správ spolu s nasadzovaním smart kontraktov je možné vďaka rozhraniu peňaženky MyEtherWallet, ktorá ponúka možnosť prepojenia s web3 peňaženkou ako rozšírením prehliadača. Vďaka tomuto prepojeniu je možné využívať všetky funkcie MyEtherWallet. Pridávanie ERC-20 tokenov je možné buď priamo v peňaženke prostredníctvom adresy kontraktu tokenu alebo na stránke coingecko[14] vyhľadať token, ktorý chceme pridať a na karte tokenu kliknúť na tlačidlo pre pridanie do Metamasku. Spočiatku je možné využívať sieť Ethereum a jej testovacie siete, nechýba však možnosť pridávania ďalších sietí. Zoznam sietí je možné nájsť na stránke chainlist[11], pridanie požadovanej siete je tiež možné napríklad kliknutím tlačidla pre pridanie do Metamasku. Pomocou rozhraní tretích strán dokáže peňaženka detegovať a zobraziť nové tokeny

[1] open source - verejne dostupný softvér, prístupný pod licenciou umožňujúcou jeho úpravu alebo slobodné šírenie

[2] Web3 - nová iterácia World Wide Web založená na technológii blockchain, zahŕňa koncepty ako decentralizácia a token

odoslané do peňaženky užívateľa. Peňaženka podporuje aj prepojenie s hardvérovými zariadeniami ako Ledger, Trezor, Lattice alebo iné peňaženky komunikujúce prostredníctvom QR kódov.

6.3 Daedalus Wallet

Daedalus Wallet je full node[3] softvérová peňaženka určená pre počítače, podporujúca kryptomenu Cardano a jej testovaciu sieť. Ide o open source aplikáciu pre operačné systémy Windows, Linux a macOS. Peňaženka pri jej zakladaní generuje seed zložený z 24 slov a zároveň vyžaduje od užívateľa nastavenie minimálne 10 znakov dlhého hesla, ktoré bude zadávané pri potvrdzovaní transakcie. Keďže ide o peňaženku, ktorá nepodporuje Bitcoin, nemá možnosť vytvorenia lightning účtu. Pri zasielaní prostriedkov a ani iných prípadoch užitia aplikácia nepovoľuje možnosť využitia 2FA. Chýba možnosť výberu priority transakcie, pretože súčasný systém kryptomeny Cardano je nastavený tak, že sa ku každej transakcii pristupuje rovnako. Používatelia tak nemajú možnosť zmeniť svoju prioritu transakcie zaplatením vyššieho poplatku. V prípade zasielania adresy na prijatie platby je možné využiť vopred vygenerované adresy alebo QR kódy prislúchajúce k peňaženke. Užívateľ má možnosť zobrazenia použitých adries, na ktoré boli už v minulosti zaslané prostriedky. Pri adresách však nechýba upozornenie, že každá obsahuje užívateľov stavový kľúč. Ten kto disponuje s adresou môže pomocou stavového kľúča nájsť na blockchaine všetky adresy, zostatok a históriu transakcií danej peňaženky. Aplikácia neumožňuje vytvorenie špeciálnej adresy alebo QR kódu obsahujúceho požadované množstvo mincí od odosielateľa. Proces obnovy je možné vykonať ako z full node peňaženky tak aj z lightweight peňaženky akou je pre Cardano napríklad Yoroi wallet. Pri obnove peňaženky je nutná synchronizácia transakčnej histórie s blockchainom, obnova tak trvá dlhší časový úsek. Peňaženka je zabezpečená heslom, ktoré je možné kedykoľvek zmeniť, avšak chýba podpora nastavenia automatického odhlásenia alebo možnosť potvrdenia transakcie pomocou biometrie. Daedalus Wallet nepodporuje možnosť podpisovania a overovania správ, nasadzovanie smart kontraktov a ani možnosť pridania iného tokenu. Aplikácia ponúka možnosť verifikácie seedu, skrytia zostatku peňaženiek, nastavenia serveru pre ukladanie off-chain metadát a pomocou stake pool delegovať a získavať odmeny. Je tiež kompatibilná s hardvérovými peňaženkami Ledger Nano X, Ledger Nano S a Trezor T.

6.4 Trezor T

Trezor T je open source hardvérová peňaženka s farebným dotykovým displejom vyrábaná spoločnosťou Satoshilabs. Jej prepojenie s počítačom je zabezpečené pomocou dodávaného USB-C kábla. Cena zariadenia je momentálne cez 225 eur, alternatívou môže byť starší model One s cenou okolo 70 eur. Všetky dôležité úkony spojené s bezpečnosťou sú zadávané a potvrdzované priamo na zariadení. Peňaženka podporuje veľké množstvo kryptomien a taktiež aj testovacích sietí. Spoločnosť, ktorá túto peňaženku vytvorila poskytuje užívateľom aj aplikáciu Trezor Suite, ktorá ponúka jednoduché a intuitívne prostredie určené pre prácu s peňaženkou Trezor. Počas zakladania peňaženky je možnosť zvoliť vytvorenie štandardnej zálohy alebo Shamir zálohy. Štandardná záloha pozostáva z 12 slov a pri Shamir zálohe sa nastavuje počet dielov a veľkosť prahu potrebného na obnovu peňaženky. Zvolená bola záloha typu Shamir, prah bol určený na 2 obnovovacie frázy z 3. Každá vygenerovaná

[3] full node - synchronizuje celý blockchain, sťahuje každý blok a transakciu na úložisko zariadenia

fráza bola jedinečná a obsahovala 20 slov. Obnovovacie frázy sú zobrazené užívateľovi na displeji zariadenia, tieto frázy už neskor nie je možné zobraziť. Pri vytváraní peňaženky má užívateľ možnosť uložiť alebo preskočiť zapísanie seedu taktiež aj nastavenie PIN kódu, je však upozornený na možné riziká. V zariadení nie je možné vytvoriť Bitcoin lightning účet. Prednastavené je používanie pripojenia prostredníctvom Tor[4]. Vytvorená peňaženka ponúka možnosť vytvorenia niekoľkých skrytých peňaženiek za pomoci rozšírenej bezpečnostnej frázy. Po vytvorení transakcie a určení priority na počítači je užívateľ vyzvaný na potvrdenie adresy príjemcu, množstva zasielaných prostriedkov a výšky poplatku priamo na zariadení Trezor. Akonáhle je transakcia na zariadení potvrdená môže byť v aplikácii počítača odoslaná. V prípade, že odoslaná transakcia ešte nebola zahrnutá v žiadnom bloku, je možné využiť funkcionalitu Replace-By-Fee[5]. Pri viacerých kryptomenách ponúka aplikácia možnosť zaslania prostriedkov viacerým príjemcom v jednej transakcii, každému však môže byť zaslané rozličné množstvo kryptomeny. V prípade zasielania Bitcoinu ponúka možnosť nastavenia času, kedy môže byť najskôr transakcia zahrnutá do bloku. Peňaženka podporuje generovanie nových adries a QR kódov, absentuje však podpora na vytvorenie QR kódu s požadovanou sumou od odosielateľa. Proces obnovy peňaženky je možný zo seedu dlhého 12, 18, 20, 24 alebo 33 slov. Zadávanie obnovovacej frázy je vykonávané prostredníctvom klávesnice na displeji zariadenia. V prípade obnovovania peňaženky so zálohou Shamir je nutné zadať na zariadení dostatočný počet obnovovacích fráz, v testovanom prípade to boli 2 frázy skladajúce sa každá z 20 slov. Aplikácia po prihlásení ponúka možnosť zmeny hesla, nastavenia času automatického odhlásenia alebo nastavenie Electrum servera. Trezor Suite poskytuje možnosť podpisovania a overovania správ vo formáte Trezor aj Electrum, potvrdenie zadanej správy a adresy je vykonávane priamo na zariadení. Nasadzovanie smart kontraktu v aplikácii nie je možné, jednou z možností na nasadenie kontraktu je využitie rozhrania MyEtherWallet, s ktorým je trezor kompatibilný. Tokeny ERC-20 je možné pridávať prostredníctvom adresy kontraktu prislúchajúceho danému tokenu. Zariadenie má aj slot na MicroSD kartu, ktorá môže v budúcnosti slúžiť ako šifrované úložisko. Okrem dodávaného firmvéru má používateľ možnosť na zariadenie nainštalovať aj vlastný firmvér, táto možnosť sa však z bezpečnostného hľadiska neodporúča.

6.5 CoolWallet S

CoolWallet S je hardvérová peňaženka vzhľadom pripomínajúca kreditnú kartu. Komunikácia s hardvérovým zariadením je možná pomocou poskytovanej mobilnej aplikácie CoolBitX a technológii Bluetooth. Za pomoci displeja a tlačidla peňaženky si môže používateľ zobraziť množstvo prostriedkov vybranej kryptomeny, ktorým disponuje peňaženka. Informácie o množstve mincí v peňaženke však môže získať ktokoľvek kto má fyzický prístup k tomuto zariadeniu. Peňaženka podporuje množstvo hlavných sietí a tiež veľké množstvo kryptomien, absentuje tu však testovacia sieť. Užívatelia tak nemajú možnosť otestovania funkcionality za pomoci testovacích kryptomien. Pri zakladaní peňaženky má používateľ možnosť výberu dĺžky seedu, varianty sú 12, 18 alebo 24 slov. Po zvolení dĺžky obnovovacej frázy je možné vybrať či bude vygenerovaný seed zobrazený v aplikácii alebo priamo na displeji peňaženky, čo je bezpečnejšia alternatíva. Proces vygenerovania seedu je na prvý pohľad iný ako pri ostatných kryptomenových peňaženkách, namiesto vygenerova-

[4]Tor - internetový prenos je smerovaný cez niekoľko náhodných relé predtým, ako sa dostane na servery peňaženky

[5]Replace-By-Fee - urýchľuje potvrdenie transakcie, nepotvrdené transakcie je možné nahradiť transakciami, ktoré platia vyššie poplatky

ných slov je používateľovi zobrazený zvolený počet 5 ciferných čísel reprezentujúcich seed. Každé číslo dodržuje protokol BIP 39[6] a zodpovedá konkrétnemu anglickému slovu. Slová, na ktoré sa čísla mapujú je v prípade potreby možné nájsť v mapovanej tabuľke na stránkach výrobcu peňaženky. Po úspešnom overení vygenerovaného seedu a založení peňaženky nie je peňaženka nijako zabezpečená heslom. V prípade potreby je možné v nastaveniach aktivovať zabezpečenie zariadenia pomocou 6 miestneho PIN kódu, chýba tu však možnosť nastavenia automatického odhlásenia alebo odomykania za pomoci biometrie. Vytvorenie transakcie je vykonávané v aplikácii a následne je potvrdzované priamo na peňaženke. Pri zasielaní prostriedkov je nutné klasicky zadať adresu alebo naskenovať jej QR kód spolu s množstvom zasielaných prostriedkov a určením výšky priority transakcie. Po vytvorení transakcie je potrebné do niekoľkých sekúnd potvrdiť priamo na hardvérovom zariadení druh zasielanej kryptomeny, adresu príjemcu a množstvo, inak platnosť tejto transakcie exspiruje. Čas na exspiráciu je príliš krátky, kontrola správnosti všetkých údajov, hlavne adresy, keďže je displej zariadenia ťažko čitateľný je tak často dlhšia ako doba exspirácie. Peňaženka nepodporuje Replace-By-Fee funkcionalitu, transakciám s nízkym poplatkom tak nie je možné tieto poplatky navýšiť. Prijímanie prostriedkov prebieha podobne ako na každej inej peňaženke, užívateľ má možnosť generovania nových adries aj QR kódov, jediná testovaná funkcionalita čo chýba, je možnosť zadania požadovaného množstva kryptomeny od odosielateľa. Proces obnovy je možný z 12, 18 alebo 24 slov dlhej frázy, ktorá je zadávaná buď priamo v mobilnej aplikácii alebo bezpečnejším spôsobom s využitím samotnej peňaženky. Na obrazovke mobilu je vygenerovaná tzv. slepá matica, kým na displeji peňaženky sú zobrazené náhodne usporiadané číslice od 0 po 9, používateľ zadáva požadovanú číslicu seedu za-kliknutím správneho tlačidla slepej matice, tento proces je nútený opakovať až pokiaľ nebude zadaná celá obnovovacia fráza. V prípade Bitcoin účtu peňaženky nie je možné zvoliť vlastný dôveryhodný uzol a ani založiť lightning účet. Aplikácia nepodporuje podpisovanie, overovanie správ a ani nasadzovanie smart kontraktov, jedinou možnosťou je využitie kompatibility s rozhraním peňaženky MyEtherWallet, ktorá tieto možnosti ponúka. Známejšie ERC-20 tokeny sú zobrazované už priamo v peňaženke, tie chýbajúce je možné do peňaženky pridať manuálne prostredníctvom adresy kontraktu.

6.6 Ellipan titan

Ellipal titan je hardvérová peňaženka využívajúca technológiu Air-gap. Pri prenose dát sa spolieha výlučne na QR kódy, zatiaľ čo iné hardvérové peňaženky využívajú napríklad Bluetooth alebo USB kábel. Pomocou zabudovanej kamery dokáže skenovať QR kódy a tým ďalej potvrdzovať a podpisovať transakcie vytvorené priamo v mobilnej aplikácii. Pri procese vytvárania účtu peňaženky na zariadení je vygenerovaných 12 slovný seed, ktorý môže byť rozšírený aj o bezpečnostnú prístupovú frázu. Výrobca peňaženky ponúka svojim zákazníkom mobilnú aplikáciu, prostredníctvom ktorej sú vytvárané transakcie, prijímané prostriedky a vykonávané rôzne ďalšie prípady použitia. Na synchronizáciu aplikácie a peňaženky je potrebné oskenovať sériu QR kódov vygenerovaných na zariadení peňaženky, po úspešnom skenovaní je následne prepojená peňaženka s aplikáciou. Samotná peňaženka podporuje veľké množstvo sietí a kryptomien, chýba tu však podpora tých testovacích. Vytvorenie transakcie je nutné vykonať v mobilnej aplikácií, ktorá po zadaní adresy, zasielaného množstva a určení priority zobrazí vygenerované QR kódy. Tieto kódy je potrebné

[6]BIP 39 - mnemotechnická fráza, ktorá slúži ako záloha na obnovu peňaženky, slová frázy sú prevzaté zo špecifického zoznamu slov

nasnímať pomocou kamery peňaženky, ktorá následne zobrazí adresy a množstvo zasielanej kryptomeny. Po overení a podpísaní transakcie sú v peňaženke vygenerované QR kódy, ktoré je naopak potrebné zosnímať mobilným zariadením, aby mohla byť vytvorená transakcia odoslaná na vyťaženie. Vyžiadanie prostriedkov zobrazením QR kódu je možné ako v mobilnej aplikácii, tak aj pomocou hardvérovej peňaženky. Mobilná aplikácia navyše ponúka možnosť vytvorenia transakčného QR kódu obsahujúceho požadované množstvo prostriedkov od odosielateľa. V peňaženke absentuje možnosť generovania nových adries pre prijatie kryptomeny, aplikácia má možnosť vytvorenia viacerých účtov, avšak ku každému účtu danej kryptomeny prislúcha iba jedna adresa. Obnovu peňaženky je možné vykonať pomocou obnovovacej frázy dlhej 12, 15, 18, 21 alebo 24 slov, ktorá môže byť doplnená aj o rozšírenú bezpečnostnú frázu. Na zabezpečenie samotnej hardvérovej peňaženky je pri jej zakladaní vyžadované heslo o dĺžke 8 znakov, okrem hesla je možné využiť tzv. vzorový zámok, využívaný v mnohých Android zariadeniach. Tento typ zámku je možné doplniť aj o automatické odhlásenie používateľa. Peňaženka nepodporuje možnosť podpisovania, overovania správ ani nasadzovania smart kontraktov. Tokeny ERC-20 majú plnú podporu a je možné ich pridať zadaním celého názvu tokenu alebo jeho príslušnej adresy. Pri testovaní peňaženky bola zistená nezvyčajne dlhá latencia synchronizácie s blockchainom, aplikácia niekedy nezobrazovala odoslané a prijímané kryptomeny ani po uplynutí niekoľkých desiatok minút od prvého potvrdenia transakcie na blockchaine.

6.7 Electrum Wallet

Electrum je open source peňaženka, dostupná ako počítačová aplikácia. Ide o jednu z najstarších bitcoinových peňaženiek vôbec. Aplikácia má základné užívateľské rozhranie, určené skôr pre pokročilejších užívateľov. Počas zakladania peňaženky má užívateľ možnosť výberu medzi peňaženkou štandardnou, s dvojfaktorovým overením, viac-podpisovou alebo obnovou pomocou súkromného kľúča. Štandardné peňaženky majú podporu Bitcoin lightning účtu, pri viac-podpisových takú možnosť užívatelia nemajú. Testovaná je viac-podpisová peňaženka s nutnosťou podpísania 2 z 2 užívateľov, aplikácia však ponúka možnosť podpisovania až 15 spolu-podpisovateľov. V prípade seedu má užívateľ na výber možnosti vygenerovať nový seed, použiť už v minulosti vygenerovaný alebo použiť hardvérové zariadenie s vlastným súkromným kľúčom. Po vygenerovaní 12 slovného seedu je možnosť doplnenia o bezpečnostnú frázu, táto funkcia bola využitá aj počas testovania. Každý používateľ viac-podpisovej peňaženky má svoj unikátny súkromný kľúč. Používatelia si musia navzájom vymeniť vygenerované kľúče. V prípade ak je do peňaženky zadaný verejný kľúč, vlastník tohoto kľúča sa musí podieľať na spolu-podpise, ak je zadaný súkromný kľúč inej peňaženky, má užívateľ možnosť podpisovať transakcie aj za spolu-podpisujúceho. Zasielanie prostriedkov je zložitejšie ako tomu bolo počas testovania viac-podpisovej peňaženky Bitpay. Pri vytvorení transakcie je nutné jej vy-exportovanie a následné načítanie v peňaženke spolu-podpisujúceho buď zo súboru, schránky, QR kódu alebo blockchainu pomocou ID transakcie. Táto vytvorená transakcia inak nie je viditeľnou pre ostatných spolu-podpisujúcich. Electrum však ponúka aj možnosť využitia doplnku, ktorý posiela a prijíma čiastočne podpísané transakcie z alebo do viac-podpisovej peňaženky. Zasielanie prostriedkov je možné aj prostredníctvom hromadnej platby. Viac-podpisová peňaženka neponúka možnosť využitia 2FA. Prijímanie prostriedkov funguje ako pri klasických peňaženkách. Aplikácia dokáže generovať adresy, QR kódy aj s požadovanou sumou pričom výhodou je možnosť nastavenia času exspirácie vygenerovanej adresy. Proces obnovy peňaženky je podobný a teda je nutné zadať seed s bezpečnostnou frázou a heslom, ktoré chráni peňaženku, spolu s opä-

tovným zadaním kľúčov spolu-podpisujúcich. Zmena názvu peňaženky je možná pomocou premenovania názvu súboru uloženého v počítači užívateľa. Peňaženka nepodporuje možnosť automatického odhlásenia a ani odomykanie pomocou biometrie. Heslo vytvorené pri zakladaní je možné kedykoľvek zmeniť. Aplikácia pri klasickom type peňaženky ponúka možnosť podpisovania a overovania ale taktiež aj šifrovania a dešifrovania správ. Keďže ide o peňaženku nepodporujúcu Ethereum, absentuje tu možnosť nasadzovania smart kontraktov a taktiež pridávanie ERC-20 tokenov. V rozšírených nastaveniach siete ponúka aplikácia možnosť výberu vlastných serverov, nastavenie proxy alebo pripojenie cez Tor. Aplikácia okrem vyššie spomenutého ponúka aj možnosť využitia funkcionality Replace-By-Fee. V prípade zvýšenia poplatku je možné všetky nepotvrdené RBF transakcie zlúčiť do jednej za účelom šetrenia prostriedkov.

6.8 BitPay wallet

BitPay je multiplatformová kryptomenová peňaženka podporujúca veľké množstvo kryptomien, aplikácia je dostupná pre počítače, mobilné zariadenia a tiež ako rozšírenie internetového prehliadača Chrome. Jej veľkou výhodou je možnosť vytvorenia klasickej aj viac-podpisovej peňaženky, ktorá podporuje možnosť rozdelenia platobnej autorizácie až medzi 6 zariadení. Založená a testovaná bola funkcionalita viac-podpisovej peňaženky vyžadujúcej 2 z 2 podpisov. Pri zakladaní peňaženky je možnosť výberu medzi klasickou a viac-podpisovou peňaženkou, po zvolení typu peňaženky je v rozšírených nastavenia nechýba aktivácia podpory pre testovaciu sieť a taktiež možnosť používania jednej adresy, predvolené je používanie generovania nových adries. Absentuje tu však podpora pre vytvorenie Bitcoin lightning účtu. V procese vytvárania je možnosť pridania prístupovej frázy za účelom zvýšenia zabezpečenia. Následne je užívateľovi vygenerovaný QR kód a adresa určená pre ďalšie zariadenia, ktoré sa budú podieľať na spolu-podpisovaní. Pri zakladaní peňaženky je potrebné zadať vygenerovanú adresu alebo naskenovať kód. Zariadenia nebudú zdieľať rovnakú obnovovaciu frázu, všetky peňaženky budú mať svoj jedinečný 12 slovný seed. V prípade ak je vytvorená transakcia, sú upozornené všetky ostatné zariadenia, obsahujúce túto viac-podpisovú peňaženku, na prijatie alebo zamietnutie vytvorenej platby. Vyššie spomenuté upozornenie obsahuje všetky bežné informácie o transakcii, spolu s informáciou o tom, kto danú transakciu vytvoril, potvrdil, prípadne zamietol. V testovacom scenári išlo o nutnosť potvrdenia transakcie oboma užívateľmi. Pri vyžiadaní platby sa viac-podpisové peňaženky nijako nelíšia, Bitpay dokáže generovať nové adresy a k nim prislúchajúce QR kódy s možnosťou zadania množstva prostriedkov požadovaných od odosielateľa. Nechýba tu ani možnosť zobrazenia už použitých adries. Proces obnovy peňaženky je rovnaký ako pri klasickej variante peňaženky, užívateľ je vyzvaný na vloženie seedu patriacemu obnovovanej peňaženke. Po zadaní správnej obnovovacej frázy je peňaženka obnovená v priebehu niekoľkých sekúnd. Zabezpečenie peňaženky je možné pomocou biometrie a PIN kódu, ktorý je možné kedykoľvek zmeniť. Aplikácia neumožňuje používanie 2FA, automatického odhlásenia ani nastavenia dôveryhodného Electrum serveru. Prostredníctvom Bitpay nie je možné nasadzovanie smart kontraktov a ani podpisovanie a overovanie správ. Ponuka kryptomien je však v peňaženke široká, pri testovaní sa nevyskytol problém počas pridávania ERC-20 tokenov, okrem toho má užívateľ možnosť prepojenia aplikácie s burzou Coinbase alebo protokolom WalletConnect.

6.9 Coinbase

Ide o multiplatformovú hostovanú peňaženku podporujúcu veľké množstvo kryptomien. Najväčšou nevýhodou tejto peňaženky je, že neposkytuje súkromný kľúč užívateľovi. Kľúč je spravovaný spoločnosťou. Nechýba možnosť využitia 2FA prostredníctvom SMS, emailu alebo autentifikačnej aplikácie. Peňaženka podporuje generovanie nových adries a QR kódov na prijímanie prostriedkov. Spoločnosť ponúka aj alternatívu v podobe peňaženky s vlastnou správou, ide o peňaženku poskytujúcu kontrolu nad vlastnenými kryptomenami. Súkromné kľúče sú uložené v mobilnom zariadení a nie na burze, ako to je v prípade hostovanej peňaženky. Coinbase wallet je dostupná ako mobilná aplikácia ale aj ako rozšírenie internetového prehliadača. Pri zakladaní peňaženky si užívateľ vytvára jedinečnú prezývku, prostredníctvom ktorej mu môžu neskôr ostatní užívatelia zasielať prostriedky bez nutnosti znalosti jeho adresy. Peňaženka vygeneruje seed zložený z 12 slov, bez možnosti pridania prístupovej frázy a požiada užívateľa o jeho zálohu. V mobilnej aplikácii je nutné nastavenie 6 číselného PIN kódu, v prehliadači zas aspoň 8 znakov dlhého hesla. Nastavenia poskytujú možnosť výberu zo širokej ponuky klasických aj testovacích sietí, siete je možné pridávať aj manuálne. Počas zasielania kryptomeny nie je možné využiť možnosť 2FA a v mobilnej aplikácii ani možnosť zvolenia priority transakcie. Chýba aj zobrazenie presného množstva kryptomeny potrebnej na vykonanie transakcie. Výhodou je možnosť zaslania kryptomeny na Coinbase peňaženku iba prostredníctvom užívateľského mena príjemcu. K jednej peňaženke patrí 10 aktívnych účtov s unikátnou adresou, na ktoré je možné prijímať kryptomeny, generovanie adries tak nie je možné. Chýba aj možnosť vygenerovania QR kódu obsahujúceho požadované množstvo kryptomeny. Pri procese obnovy v mobilnej aplikácii je peňaženka obnovená iba za pomoci 12 slovného seedu, zatiaľ čo v prehliadači sú aj možnosti na prepojenie so zariadením Ledger alebo prepojenie s mobilnou aplikáciou peňaženky pomocou QR kódu. V prípade zabezpečenia má užívateľ príležitosť nastaviť zabezpečenie pomocou biometrie alebo vytvorené heslá kedykoľvek po prihlásení zmeniť. Peňaženka nepodporuje podpisovanie, overovanie správ a nasadzovanie smart kontraktov. Na prijímanie ERC-20 tokenov je možné využiť klasickú adresu určenú pre Ethereum. Okrem vyššie spomenutej podpory zariadenia Ledger, aplikácia podporuje aj Metamask, ImToken[45], Trust Wallet[34] a taktiež prepojenie peňaženky priamo s burzou Coinbase.

6.10 Coinomi

Coinomi je multiplatformová kryptomenová peňaženka podporujúca veľké množstvo kryptomien, užívateľ má možnosť výberu medzi počítačovou alebo mobilnou aplikáciou. Peňaženka podporuje viac ako 125 blockchainov a tisíce tokenov, má podporu testovacích sietí, avšak nepodporuje bitcoin lightning sieť. Pri procese vytvárania peňaženky je užívateľovi vygenerovaných 24 slov reprezentujúcich seed spolu s možnosťou rozšírenia seedu o prístupovú frázu. V aplikácii nechýba podpora bezpečnostnej funkcie, ktorá v prípade, ak si užívateľ vytvorí snímku obrazovky, na ktorej je zobrazený seed deteguje a následne užívateľa upozorní na možné riziká spolu s výzvou na odstránenie snímky zo zariadenia. Po overení úspešne uloženého seedu sú užívateľovi ponúknuté 4 možnosti zabezpečenia, bez overenia, biometrické overenie, overenie heslom dlhým aspoň 10 znakov a kombinácia biometrického overenia spolu s heslom, chýba však možnosť zabezpečenia pomocou 2FA. Pri odosielaní prostriedkov je možnosť zvolenia priority transakcie, nevýhodou je absencia hodnoty reprezentujúcej súčet zasielaných prostriedkov a výšky poplatku, toto množstvo mincí je potrebné na vykonanie danej transakcie. Testovacie scenáre na vyžiadanie platby boli

úspešné, peňaženka dokáže generovať nové adresy a k nim aj prislúchajúce QR kódy. V prípade potreby je možné vygenerovanie adresy alebo kódu aj so sumou, ktorú požadujeme od odosielateľa. Takáto špeciálna adresa je kompatibilná napríklad aj s aplikáciou Green Wallet. Pri procese obnovy je možné obnoviť aj zabezpečené peňaženky prístupovou frázou, obnovenej peňaženke je možné zmeniť jej spôsob zabezpečenia ako aj jej názov. Zabezpečenie peňaženky je možné aj pomocou PIN kódu prípadne biometrického overenia, ktoré je vyžadované vždy po otvorení aplikácie, chýba však podpora nastavenia automatického odhlásenia. Ak by užívateľ z nejakého dôvodu zabudol PIN kód a nemal by aktivované biometrické overovanie, neexistuje možnosť obnovy kódu, musí obnoviť celú peňaženku pomocou seedu. V rozšírených nastaveniach aplikácie je voľba nastavenia dôveryhodného Electrum serveru pre bitcoin. Peňaženka ponúka podpisovanie a overovanie správ a pridávanie napríklad ERC-20 tokenov ale aj tokeny na iných podporovaných blockchainoch, avšak nie je možné prostredníctvom peňaženky interagovať a ani nasadzovať smart kontrakty.

6.11 Blockchain wallet

Blockchain je softvérová open source aplikácia určená prevažne pre mobilné zariadenia. Používateľ dokáže prepojiť svoju peňaženku aj s webovým rozhraním počítača, napríklad prostredníctvom QR kódu. Kód sa nachádza na webovej stránke prihlásenia do peňaženky, stačí ho nasnímať mobilnou aplikáciu a po overení zariadenia je na prehliadači počítača zobrazená prihlásená peňaženka z mobilnej aplikácie. Peňaženka podporuje veľké množstvo hlavných sietí okrem testovacej a Bitcoin lightning siete. Po nainštalovaní a prvom spustení aplikácie je používateľ nútený zadať emailovú adresu spolu s heslom, prebieha tak akýsi proces registrácie namiesto generovania a zapísania seedu. Zadanú emailovú adresu je potrebné overiť a po úspešnom overení nastaviť 4 miestny PIN kód peňaženky. Následne je peňaženka pripravená na používanie bez potreby zapísania seedu. V nastaveniach aplikácie je zobrazené hlásenie o nezálohovaní bezpečnostnej frázy, po zobrazení 12 slovného seedu sú zobrazené doporučenia o jeho správnom uložení. Po uložení sú od používateľa požadované 3 náhodné slová na overenie správneho zápisu frázy. Pri odosielaní a prijímaní prostriedkov je možné využiť skenovanie, generovanie QR kódov a nových adries spolu s vlastným určením výšky poplatku za transakciu. Nová adresa je vygenerovaná automaticky po použití poslednej vygenerovanej. Proces obnovy je možný viacerými spôsobmi, zadaním jedinečného identifikačného čísla peňaženky spolu s heslom peňaženky, zapísaním obnovovacej frázy peňaženky alebo prihlásením pomocou emailu a hesla zadávaného pri procese zakladania peňaženky. Po obnove alebo zobrazení seedu je vždy na adresu používateľa zaslaný informačný email spolu s ďalšími dodatočnými informáciami. Na zabezpečenie peňaženky je možné využiť okrem hesla a PIN kódu aj odomykanie pomocou biometrických údajov. Mobilná aplikácia neponúka možnosť nastavenia automatického odhlásenia, na počítači je však nastavenie tejto funkcie dostupné. V aplikácii chýba možnosť podpisovania, overovania správ, nasadzovania smart kontraktov a tiež možnosť nastavenia Bitcoin Electrum serveru. Vo webovom rozhraní je možné v rozšírených nastaveniach zvoliť pripojenie prostredníctvom Tor a tiež možnosť vytvorenia zoznamu povolených IP adries, z ktorých je možné prihlasovanie do peňaženky.

6.12 Green Bitcoin wallet

Green wallet je multiplatformová bitcoinová peňaženka, užívateľ si môže vybrať medzi počítačovou alebo mobilnou aplikáciou. Po otestovaní používateľských scenárov bolo zistené, že peňaženka podporuje okrem klasickej bitcoinovej siete aj jej testovaciu sieť a tzv. Liquid sieť, ktorá je implementovaná na 2. vrstve a umožňuje vydávanie digitálnych aktív akými sú napríklad bezpečnostné tokeny a stablecoiny[7]. Jednou z nevýhod je, že táto peňaženka nepodporuje Bitcoin lightning sieť. Pri vytváraní peňaženky si môže užívateľ vybrať, či chce aby mal jeho vygenerovaný seed dĺžku 12 (128 bitov) alebo 24 (256 bitov) slov a taktiež typ peňaženky, pričom na výber je jedno-podpisová alebo viac-podpisová s možnosťou, uloženia druhého kľúča na serveroch spoločnosti, tento kľúč je chráneným užívateľom vybraným 2FA. Na výber je možnosť 2FA pomocou emailu, SMS správy, telefónneho hovoru alebo autentifikačnej aplikácie, v počítačovej aplikácii je možnosť nastavenia limitu pre transakcie a do tohto limitu nie je potrebné overovanie pomocou 2FA. Po presiahnutí limitu sú potrebné oba kľúče na potvrdenie transakcie. Peňaženka je zabezpečená aj 6 miestnym PIN kódom vyžiadaným pri vytváraní peňaženky, kód slúži na autentifikáciu a potvrdzovanie transakcií. Odosielanie prostriedkov pomocou tejto peňaženky je jednoduché a intuitívne, výhodou je možnosť pridania poznámky ku transakcii a možnosť zvolenia priority transakcie. Nevýhodou je absencia hodnoty reprezentujúcej súčet zasielaných prostriedkov a výšky poplatku. Testovacie scenáre na vyžiadanie platby boli úspešné, peňaženka dokáže generovať nové adresy a k nim aj prislúchajúce QR kódy. V prípade potreby je možné vygenerovanie adresy alebo kódu aj so sumou, ktorú požadujeme od odosielateľa, takáto adresa nemusí byť kompatibilná s inou aplikáciou ako Green wallet. Proces obnovy podporuje aj obnovu peňaženky s vlastnou prístupovou frázou alebo obnovu pomocou naskenovania QR kódu, vygenerovaného v dostupnej existujúcej peňaženke. Možnosťou zabezpečenia je nastavenie automatického odhlásenia po určitej dobe nečinnosti a využívanie overenia užívateľa pomocou biometrie. Peňaženka neumožňuje pridanie ERC-20 tokenu ani nasadenie smart kontraktu pretože nepodporuje kryptomenu Ethereum, Cardano ani iné kryptomeny podporujúce smart kontrakty, a taktiež tu absentuje možnosť podpisovania a overovania správ. Rozšírené nastavenia však dovoľujú možnosť anonymizácie internetového prenosu pomocou pripojenia cez Tor, možnosť pripojenia cez proxy, možnosť výberu Electrum serveru, ktorému užívateľ dôveruje, SPV verifikáciu[8] a možnosť PGP kľúča pre šifrovanú emailovú komunikáciu. Aplikácia ponúka kompatibilitu s hardverovými peňaženkami Ledger Nano X a Blockstream Jade.

6.13 Blue Wallet

Blue wallet je primárne softvérová peňaženka pre mobilné zariadenia, používateľom však ponúka aj počítačovú aplikáciu určenú pre operačný systém MacOS. Ide o Bitcoinovú peňaženku podporujúcu vytváranie klasických peňaženiek, lightning účtov a tiež aj viac-podpisových peňaženiek Vault. Pri zakladaní viac-podpisovej peňaženky má používateľ na výber nastavenie prahu potrebného na podpísanie transakcie od 2 z 2 až na 7 zo 7 spolu-podpisovateľov, tento typ peňaženky komunikuje prostredníctvom Air-gap s využitím QR kódov. Predvolené je nastavenie 2 potrebných podpisov z 3 účtov podpisovateľov. Spolu-

[7] stablecoiny - kryptomeny, ktoré sa pokúšajú naviazať svoju trhovú hodnotu na nejakú externú referenciu, napríklad na menu, ako je americký dolár, alebo na cenu komodity, ako je zlato

[8] SPV verifikácia - bez nutnosti stiahnutia celého blockchainu umožňuje príjemcovi transakcie dokázať, že má odosielateľ kontrolu nad zdrojovými prostriedkami

podpisovateľov je možné neskôr v správe peňaženky zobraziť, prípadne zmeniť. Testovaná však nie je viac-podpisová peňaženka ale je vytvorený klasický Bitcoin účet. Peňaženka ponúka vygenerovanie 12 slovného seedu a tiež schopnosť pokročilého vygenerovania entropie za pomoci náhodného hodu kockou a mincou. Používateľ je vyzvaný na zapísanie vygenerovaného seedu, avšak ďalej neprebieha žiadne overenie správne zapísaného seedu tak ako to býva pri väčšine peňaženiek. Mobilná aplikácia poskytuje iba zabezpečenie pomocou biometrie, nie je možné nastaviť heslo, kód, ani automatické odhlásenie z aplikácie. Proces vytvárania transakcie ponúka okrem určenia prioritizácie aj možnosť vytvárania hromadnej platby, kde každému príjemcovi môže byť zaslané rozličné množstvo kryptomeny. Okrem hromadnej platby umožňuje zobraziť, označiť, zmraziť alebo vybrať UTXO transakcie[9] za účelom lepšej správy peňaženky. Pri prijímaní prostriedkov poskytuje možnosť generovania adries a QR kódov spolu s vytváraním QR kódu s požadovaným množstvom prostriedkov. Dostupná je aj funkcionalita s názvom CPFP (Child Pay For Parents), ktorá navyšuje poplatok. V prípade uviaznutia pôvodnej transakcie (Parent) je vytvorená ďalšia transakcia (Child) s vyšším poplatkom, zvýšením poplatku tak povzbudzuje ťažiarov na vyťaženie uviaznutej transakcie. Child môže byť vyťažená až po dokončení Parent transakcie, tým pádom je najprv vyťažená uviaznutá transakcia s nižším poplatkom a až potom dedičná transakcia s vyšším. Obnova peňaženky je možná zadaním akéhokoľvek udajú do príslušného textového poľa, aplikácia podporuje obnovu pomocou súkromného kľúča, importovania súboru alebo seedu s možným rozšírením o bezpečnostnú frázu. V aplikácii nechýba možnosť podpisovania a overovania správ a tiež funkcia s názvom „Is this my address?“, ktorá overuje, či patrí zadaná adresa ku niektorej z uložených peňaženiek v aplikácii. Keďže ide o Bitcoinovú peňaženku nie je podporované nasadzovanie smart kontraktov ani pridávanie ERC-20 tokenov. Rozšírené nastavenia peňaženky poskytujú používateľom možnosť aktivácie pripojenia prostredníctvom Tor, zvolenie Electrum serveru a tiež nastavenie Lightning LND uzlu.

6.14 Exodus

Exodus je softvérová peňaženka určená pre mobilné zariadenia s operačným systémom Android a IOS a tiež počítače s operačnými systémami Windows, Linux a MacOS. Ide o lightweight peňaženku podporujúcu veľké množstvo sietí a kryptomien. Po nainštalovaní a spustení aplikácie nie je možnosť vygenerovania nového seedu ani možnosť obnovy peňaženky. Aplikácia nezvyčajne preskočí proces generovania, zapísania a kontroly seedu a po synchronizácii s podporovanými sieťami je používateľovi k dispozícii prázdna novovytvorená peňaženka bez akéhokoľvek zabezpečenia. Užívateľ nie je upozornený na zapísanie seedu ani vytvorenie zabezpečenia aplikácie. Seed je však možné nájsť v nastaveniach zabezpečenia, ide o 12 slov, ktoré sú používateľovi zobrazené po podržaní tlačidla na odhalenie slov obnovovacej frázy. V peňaženke je po založení okamžite k dispozícii aj Bitcoin lightning účet pre rýchle transakcie s nízkymi poplatkami. Nastavenia ponúkajú možnosť zabezpečenia pomocou 6 miestneho PIN kódu alebo biometrických údajov, chýba však funkcia automatického odhlásenia. Prostriedky je možné zasielať klasickou transakciou s možnosťou zvolenia priority a Bitcoin aj prostredníctvom lightning siete. Peňaženka nedovoľuje míňanie nepotvrdených prostriedkov, tieto prostriedky sú zobrazené v peňaženke, avšak pokiaľ nie sú potvrdené nemožno ich odoslať. Na prijatie prostriedkov je prednastavené používanie jednej adresy, je však možná aktivácia generovania nových adries spolu s ich QR

[9] UTXO - nevyčerpaný transakčný výstup, každá bitcoinová transakcia sa skladá zo vstupov a výstupov, vstupy spotrebúvajú existujúce UTXO, zatiaľ čo výstupy vytvárajú nové UTXO

kódmi. Pri lightning účte nechýba možnosť zadania množstva požadovaných prostriedkov pri vyžiadaní platby, táto funkcionalita však v klasických účtoch absentuje. Proces obnovy peňaženky je nutné vykonať iba z 12 slov dlhého seedu. Po úspešnej obnove nastáva synchronizácia peňaženky s podporovanými sieťami, po synchronizácii je účet pripravený na používanie. Každá vygenerovaná peňaženka v aplikácii Exodus ukladá na úložisko zariadenia svoj seed. Nepoužívaný seed peňaženky je možné mať zálohovaný na jeden mesiac, tri mesiace, šesť mesiacov alebo navždy, voľba je na používateľovi. Užívateľom to umožňuje obnoviť svoje skôr vygenerované peňaženky bez nutnosti zadávania seedu, stačí iba zvoliť peňaženku s frázou, ktorú si želá obnoviť. Peňaženka nepodporuje podpisovanie a overovanie správ, nasadzovanie smart kontraktu a ani nastavenie vlastného Bitcoin Electrum servera. Pre tokeny typu ERC-20 nie je nutné zadávať adresu ich kontraktu, postačuje iba povoliť ich zobrazenie v hlavnej ponuke tokenov. Aplikácia ponúka možnosť synchronizácie s inými zariadeniami prostredníctvom QR kódu, používateľ si tak môže svoju peňaženku synchronizovať napríklad s počítačovou aplikáciou Exodus. Výhodou peňaženky je taktiež možnosť vytvárania a spravovania portfólia.

Kapitola 7

Ohodnotenie a porovnanie výsledkov testovania

V kapitole budú vyhodnotené a porovnané testované peňaženky, porovnávané budú ako zo stránky použiteľnosti, tak aj bezpečnosti na základe získaných informácii z testovania. Ďalší text stručne opíše každú vlastnosť a vysvetlí kritériá, podľa čoho boli ku konkrétnym peňaženkám priradené vlastnosti. Po ohodnotení budú jednotlivé peňaženky porovnávané aj s informáciami dostupnými na stránkach výrobcu danej kryptomenovej peňaženky. V prípade zistenia odchýlky medzi ponúkanými a reálne otestovanými funkcionalitami, bude na odchýlku upozornené a následne popísané v čom sa na stránkach ponúkaná funkcionalita od tej reálne dostupnej líši.

7.1 Klasifikácia a vlastnosti peňaženiek

V tabuľke 7.1 bude uvedené porovnanie základných atribútov a informácií o testovaných kryptomenových peňaženkách. Ide o fundamentálne informácie, ktoré sú dôležitým faktorom pri výbere správnej peňaženky používateľom podľa rôznych kritérií akými sú typ, cena peňaženky, podpora platformy a kryptomien alebo open source vlastnosť softvéru.

a) **Typ peňaženky**: Vlastnosť (SW) je pripísaná všetkým softvérovým, zatiaľ čo (HW) všetkým hardvérovým peňaženkám. V je tabuľke pripísaná aj kategória do ktorej podľa kapitoly 3 peňaženka patrí. Peňaženkám s privátnymi kľúčmi uloženými na lokálnom úložisku je pripísaná vlastnosť (kľúče na lok. úložisku), heslom derivovaným peňaženkám (heslom der. peňaženka), peňaženkám s rozdeleným overovaním za použitia viacerých podpisov (viac-podpisová), hostovaným peňaženkám na strane servera (server host) a na strane klienta (klient host).

b) **Platforma**: Kategória popisuje na akom type zariadenia/platformy je možné používať aplikáciu peňaženky. Vlastnosť (mobil) je pripísaná mobilnej aplikácií s podporou operačného systému Android alebo IOS. Pre počítačové aplikácie s podporou OS Windows, Linux alebo MacOS je pripísaná vlastnosť (PC). Ďalšie možnosti využitia ponúka webový prehliadač, vlastnosť (PC int. rozšírenie) je pripísaná peňaženke, ktorá môže byť pridaná do internetového prehliadača ako jeho rozšírenie a atribút (PC web) pripisuje peňaženkám, ktoré je možné využívať výrobcom ponúkaným webovým rozhraním.

c) **Podpora kryptomeny**: Kategória popisuje množstvo podporovaných kryptomien peňaženkou. V tabuľke sa nachádzajú aj peňaženky podporujúce iba jednu kryptomenu napr. Bitcoin (BTC), Cardano (ADA) a tiež peňaženky podporujúce viacero sietí ako na-

príklad Ethereum (ETH) s jeho ERC-20 tokenmi, ktorých existujú tisíce. Pri peňaženkách podporujúcich veľké množstvo kryptomien sú uvedené čísla dohľadatelné v aplikácii peňaženky alebo na stránkach výrobcu. Okrem spomenutých sa v tabuľke nachádza aj Litecoin (LTC), Ripple (XRP) a Ethereum Classic (ETC).

d) **Cena**: Pre peňaženky dostupné zdarma je pripísaná vlastnosť (-), ide o všetky testované softvérové peňaženky, konkrétna hodnota hardvérových peňaženiek je zaokrúhlená v eurách podľa ceny dostupnej na oficiálnych stránkach výrobcu.

e) **Open source**: Kategória popisuje verejnosť zdrojového kódu. Vlastnosť (Y) je pripísaná peňaženkám s verejným zdrojovým kódom a (N) peňaženkám s neverejným zdrojovým kódom.

	Typ peňaženky	Platforma	Podpora kryptomien	Cena	Open source
MyEtherWallet	SW, kľúče na lok. úložisku	mobil, PC web	ETH + ERC-20, ETC	-	Y
Metamask	SW, klient host	mobil, PC int. rozšírenie	ETH + ERC-20	-	Y
Daedalus	SW, heslom der. peňaženka	PC	ADA	-	Y
Trezor T	HW	PC aplikácia PC web	1800+	227 EUR	Y
CoolWallet S	HW	mobil	BTC, ETH + ERC20, LTC, XRP	93 EUR	Y
Ellipal Titan	HW	mobil	2000+	157 EUR	N
Electrum viac-podpisová	SW, viac-podpisová	PC	BTC	-	Y
Bitpay viac-podpisová	SW, viac-podpisová	mobil, PC, int. rozšírenie	200+	-	Y
Coinbase host	SW, server host	mobil, PC web	2000+	-	N
Coinbase wallet	SW, klient host	mobil, PC int. rozšírenie	2000+	-	Y
Coinomi	SW, klient host	mobil, PC	1700+	-	N
Blockchain	SW, klient host	mobil, PC web	180+	-	Y
Green wallet	SW, klient host	mobil, PC	BTC	-	Y
Blue wallet	SW, klient host	mobil, PC	BTC	-	Y
Exodus	SW, klient host	mobil, PC	180+	-	N

Tabulka 7.1: V tabuľke sú opísané základné vlastnosti a informácie o testovaných peňaženkách.

7.2 Variabilita pri zakladaní peňaženky

Tabuľka 7.2 bude obsahovať dôležité vlastnosti ponúkané používateľovi počas procesu zakladania peňaženky. Uvedené budú vlastnosti spojené s možnosťou výberu dĺžky, zápisu/uloženia alebo zobrazenia seedu, nastavenia zabezpečenia, podpory testovacej siete a Bitcoin lightning účtu.

a) **Možnosti seedu**: Kategória popisuje, aké ma používateľ možnosti výberu dĺžky seedu, prípadne doplnenie o bezpečnostnú prístupovú frázu, pri zakladaní peňaženky. V ta-

buľke sú uvedené hodnoty 12, 18, 24 reprezentujúce počet slov obnovovacej frázy. Vlastnosť (prís. fráza) je pripísaná peňaženkám s možnosťou doplnenia seedu a bezpečnostnú prístupovú frázu. Pri zabezpečení seedu pomocou zálohy Shamir je uvedený prah potrebný na obnovu peňaženky spolu s počtom obnovovacích fráz vygenerovaných pri zakladaní peňaženky. Vlastnosť (žiadny) je pripisovaná peňaženkám, ktoré preskočia proces zobrazenia a zálohy vygenerovaného seedu, seed peňaženky je však možné zobraziť a zálohovať v nastaveniach peňaženky. Ak ponúka peňaženka užívateľovi možnosti výberu počtu slov, sú v tabuľke uvedené všetky jej varianty.

b) **Použitie peňaženky bez nutnosti overenia seedu**: Kategória popisuje, či je možné preskočiť proces uloženia/zálohovania obnovovacej frázy a aj napriek bezpečnostnému riziku z toho vyplývajúceho začať používať peňaženku. Vlastnosť (Y) pripisujeme peňaženkám, ktoré nevyžadujú od užívateľa overenie alebo zapísanie seedu a je možné ich použiť aj bez toho. Niektoré peňaženky používateľom nedovoľujú ich použitie pokiaľ neoveria správnosť odpísaného seedu, takýmto peňaženkám je pripísaná vlastnosť (N). Ak peňaženka neposkytuje používateľom ich seed, zvyčajne ide o hostované peňaženky na strane klienta, ktoré sú v tabuľke označené (-).

c) **Zobrazenie seedu po procese autentifikácie**: Vlastnosť (Y) pripisujeme peňaženkám, ktoré po autentifikácii užívateľa umožňujú zobraziť obnovovaciu frázu, ak peňaženka takúto možnosť neponúka je jej pripísaná vlastnosť (N). Ak peňaženka neposkytuje používateľom ich seed a ten je vo vlastníctve napríklad kryptomenovej burzy, je v tabuľke označená (-).

d) **Vyžadované PIN/heslo pri vytváraní peňaženky**: Kategória popisuje či peňaženka pri jej zakladaní požaduje PIN/heslo alebo nepožaduje. V prípade ak požaduje pripisujeme jej v tabuľke (Y), nevyžadujúcim je pripísaná vlastnosť (N).

e) **Testovacia sieť**: Vlastnosť (Y) je v tabuľke pripísaná peňaženkám podporujúcim akúkoľvek testovaciu sieť, peňaženky nepodporujúce žiadnu testovaciu sieť sú označené ako (N). V prípade, že niektorá z platforiem, na ktorej je možné používať peňaženku, sieť podporuje a druhá platforma nie, bude to v tabuľke náležite uvedené.

f) **BTC lightning účet**: Kategória popisuje, či daná kryptomenová peňaženka ponúka možnosť vytvorenia Bitcoin Lightning účtu na rýchlejšie transakcie s menším transakčným poplatkom. Vlastnosť (Y) je pripísaná peňaženkám podporujúcim lightning sieť, (N) sú označené v prípade, ak sieť nepodporujú.

„*“- možnosť vytvorenia Bitcoin liquid účtu

„†“- podpora lightning účtu pri klasickom type peňaženky

	Možnosti seedu	Použitie peňaženky bez nutnosti uloženia seedu	Zobrazenie seedu po procese autentifikácie	Vyžadovaný PIN/heslo pri vytváraní peňaženky	Testovacia sieť	BTC lightning účet
MyEtherWallet	24	Y	Y	Y	mobil - N PC WEB - Y	N
Metamask	12	Y	Y	Y	Y	N
Daedalus	24	N	N	Y	Y	N
Trezor T	12 shamir 2 z 3 - 3x20	Y	N	Y	Y	N
CoolWallet S	12, 18, 24	N	N	Y	N	N
Ellipal Titan	12 + prís. fráza	N	N	Y	N	N
Electrum viac-podpisová	12 + prís. fráza	N	Y	Y	Y	N†
Bitpay viac-podpisová	12	Y	Y	Y	Y	N
Coinbase host	-	-	-	Y	N	N
Coinbase wallet	12	Y	Y	Y	Y	N
Coinomi	24 + prís. fráza	Y	Y	Y	Y	N
Blockchain	žiadny, 12	Y	Y	Y	N	N
Green wallet	12, 24	N	Y	Y	Y	N*
Blue wallet	12	Y	Y	Y	N	Y
Exodus	žiadny, 12	Y	Y	N	N	Y

Tabulka 7.2: Tabuľka popisuje možnosti založenia a konfigurácie testovaných peňaženiek.

7.3 Variabilita pri prijímaní a odosielaní prostriedkov

V tabuľke 7.3 budú uvedené ponúkané možnosti kryptomenových peňaženiek pri procese odosielania a prijímania prostriedkov na adresu peňaženky. V tabuľke budú zobrazené dôležité vlastnosti peňaženiek ako generovanie nových adries, QR kódov, nastavenie priority transakcie, možnosť využitia biometrickej alebo dvojfaktorovej autentifikácie, ktoré zvyšujú zabezpečenie a tiež uľahčujú manipuláciu so samotnou peňaženkou.

a) **Generovanie nových adries**: Kategória pripisuje vlastnosť (Y) peňaženkám, ktoré vygenerujú novú adresu po využití tej predchádzajúcej alebo je kedykoľvek používateľ schopný vygenerovania novej adresy. Vlastnosť (P) je v tabuľke pripísaná peňaženkám, ktoré majú vopred vygenerovaný počet adries (napr. 10) určených na prijatie prostriedkov, avšak ďalej už nie je možné generovať nové adresy. Táto vlastnosť je tiež pripísaná peňaženkám umožňujúcim vytváranie viacerých účtov v rámci jednej peňaženky, kde každému účtu prislúcha jedna adresa. V prípade, ak peňaženka nepodporuje generovanie nových adries je v tabuľke označená (N).

b) **Generovanie, skenovanie QR kódov**: Kategória popisuje schopnosť generovania a skenovania QR kódov za účelom zjednodušenia procesu vytvárania a prijímania transakcie. Vlastnosť (Y) je pripísaná testovaným peňaženkám, ktoré podporujú funkcionalitu generovania QR kódu prislúchajúceho k adrese a tiež možnosť skenovania QR kódu príjemcu. Vlastnosť (P) je pripísaná peňaženke, ktorá kategóriu spĺňa čiastočne a podporuje iba generovanie QR kódov.

c) **Nastavenie priority transakcie**: Vlastnosťou (Y) sú v tabuľke označené peňaženky s možnosťou zvolenia priority transakcie a to napríklad v prípade, ak potrebuje užívateľ aby bola jeho transakcia ťažiarmi skôr zahrnutá do bloku. Vlastnosť (N) je pripísaná peňaženkám neumožňujúcim zvolenie výšky poplatku/priority. V prípade, ak niektorá z platforiem nastavenie priority podporuje a druhá platforma nie, bude to v tabuľke uvedené.

d) **Využitie biometrických údajov**: Kategória popisuje možnosť využitia/nastavenia autentifikácie pomocou biometrických údajov snímačom zariadenia. Túto (Y) vlastnosť pripisujeme zariadeniam umožňujúcim využitie FaceID, TouchID biometrie na potvrdenie platby a prípadné odomykanie aplikácie peňaženky. Ak v aplikácií absentuje možnosť využitia biometrie, je v tabuľke označená (N).

e) **Využitie 2FA**: Kategória popisujúca možnosť využitia 2FA na potvrdenie platby alebo odomykanie aplikácie peňaženky. V prípade, ak peňaženka podporuje možnosť aktivácie 2FA je jej pripísaná vlastnosť (Y) inak je označená (N).

	Generovanie nových adries	**Generovanie, skenovanie QR kódov**	**Nastavenie priority transakcie**	**Využitie biometrických údajov** (napr. FaceID)	**Využitie 2FA**
MyEtherWallet	P	Y	Y	Y	N
Metamask	P	Y	Y	Y	N
Daedalus	P	P	N	N	N
Trezor T	Y	Y	Y	N	N
CoolWallet S	Y	Y	Y	Y	N
Ellipal Titan	P	Y	Y	Y	N
Electrum viac-podpisová	Y	Y	Y	N	N
Bitpay viac-podpisová	Y	Y	Y	Y	N
Coinbase host	Y	Y	Y	N	Y
Coinbase wallet	N	Y	mobil - N PC int. rozšírenie - Y	Y	N
Coinomi	Y	Y	Y	Y	N
Blockchain	Y	Y	Y	Y	Y
Green wallet	Y	Y	Y	Y	Y
Blue wallet	Y	Y	Y	Y	N
Exodus	Y	Y	Y	Y	N

Tabulka 7.3: Tabuľka popisuje možnosti prijímania/odosielania prostriedkov a potvrdzovania platby.

7.4 Rozšírená funkcionalita peňaženiek

Kapitola sa zaoberá podporou rozšírených funkcionalít testovaných peňaženiek. V tabuľke 7.4 budú uvedené dôležité vlastnosti peňaženiek akými sú možnosti nasadenia smart kontraktu, podpísania/overenia správ a tiež možnosť nastavenia dôveryhodného Bitcoin Electrum serveru. Ďalej môže byť pre používateľa začiatočníka dôležitá možnosť nakúpenia a zmenenia kryptomien, buď priamo v aplikácii alebo prostredníctvom presmerovania na nákupy/zámeny sprostredkované treťou stranou. Z hľadiska bezpečnosti je dôležitá možnosť nastavenia automatického odhlásenia a tiež v prípade potreby možnosť zmeny hesla.

a) **Nákup kryptomeny**: Peňaženky umožňujúce nákup kryptomeny v aplikácii sú v tabuľke popísané vlastnosťou (Y). Rovnako sú popísané aj peňaženky umožňujúce zakúpenie kryptomeny prostredníctvom spoločností tretích strán, tieto nákupy sú užívateľsky príveté, avšak aj často nevýhodné z dôvodu vysokých poplatkov a iných faktorov. Peňaženke nijakým spôsobom neumožňujúcej nákup kryptomien, prostredníctvom aplikácie, prislúcha v tabuľke hodnota (N).

b) **Zmenáreň kryptomien**: Kategória popisuje možnosť zmenenia jednej kryptomeny za inú. Zmenenie kryptomien je často sprostredkované treťou stranou a zväčša nie je pre používateľa výhodné. Vlastnosť (Y) pripisujeme peňaženkám, ktoré umožňujú akýmkoľvek spôsobom používateľovi zameniť vlastnenú kryptomenu za inú. V prípade, ak peňaženka neponúka možnosť zmenenia kryptomeny prislúcha jej v tabuľke hodnota (N).

c) **Nasadenie smart kontraktu**: Kategória popisujúca peňaženky umožňujúce nasadenie a prípadne ďalšiu interakciu so smart kontraktami. Vlastnosť (Y) prilieha v tabuľke peňaženkám umožňujúcim, prostredníctvom svojho rozhrania, nasadzovanie smart kontraktov. Peňaženkám kompatibilným s rozhraním podporujúcim možnosť nasadenia kontraktu (napr. MyEtherWallet) prislúcha v tabuľke hodnota (P). Ak peňaženka neumožňuje nasadenie smart kontraktu, ani nie je kompatibilná s rozhraním MyetherWallet, je v tabuľke označená (N).

d) **Nastavenie Electrum serveru**: Pomocou Electrum je možné prepojiť Bitcoin lightweight peňaženku k vybranému úplnému uzlu. V prípade, ak testovaná peňaženka nepodporuje kryptomenu Bitcoin, je jej v tabuľke pripísaná hodnota (-). Peňaženkám umožňujúcim nastavenia vlastného servera Electrum v tabuľke pripisujeme hodnotu (Y), vlastnosť (N) je pripísaná peňaženkám neumožňujúcim nastavenie vlastného Electrum serveru.

e) **Podpis/overenie správy**: Vlastnosť (Y) je pripísaná aplikáciam umožňujúcim používateľom, prostredníctvom svojho aplikačného rozhrania, podpisovať a overovať správy. Peňaženkám čiastočne spĺňajúcim kategóriu, ktoré sú kompatibilné s rozhraním podporujúcim možnosť podpisu/overenia správy (napr. MyEtherWallet) prislúcha v tabuľke hodnota (P). V prípade, ak peňaženka neponúka a nie je ani kompatibilná s rozhraním umožňujúcim podpis/overenie správy je v tabuľke označená (N).

f) **Automatické odhlásenie**: Nastavenie automatického odhlásenia môže byť pre užívateľov kryptomenových peňaženiek dôležitou bezpečnostnou funkciou. Vlastnosť (Y) je v tabuľke pripísaná peňaženkám podporujúcim aktiváciu funkcie automatického odhlásenia po určitej dobe nečinnosti. V prípade, že peňaženka nepodporuje túto funkciu je reprezentovaná hodnotou (N).

g) **Zmena PIN/hesla**: Vlastnosť (Y) je pripísaná peňaženkám umožňujúcim zmenu PIN/hesla peňaženky po procese autentifikácie používateľa v opačnom prípade je im pripísaná hodnota (N).

	Nákup kryptomeny	Zmenáreň kryptomien	Nasadenie smart kontraktu	Nastavenie Electrum serveru	Podpis/overenie správy	Automatické odhlásenie	Zmena PIN/hesla
MyEtherWallet	Y	Y	Y	N	Y	N	N
Metamask	Y	Y	P	N	P	Y	N
Daedalus	N	N	N	-	N	N	Y
Trezor T	Y	Y	P	Y	Y	Y	Y
CoolWallet S	Y	Y	P	N	P	N	Y
Ellipal Titan	Y	Y	N	N	N	Y	Y
Electrum viac-podpisová	N	N	N	Y	Y	N	Y
Bitpay viac-podpisová	Y	Y	N	N	N	N	Y
Coinbase host	Y	Y	N	N	N	N	Y
Coinbase wallet	Y	Y	N	N	N	N	Y
Coinomi	Y	Y	N	Y	Y	N	Y
Blockchain	Y	Y	N	N	N	N	Y
Green wallet	N	N	N	Y	N	Y	Y
Blue wallet	Y	N	N	Y	Y	N	N
Exodus	Y	Y	N	N	N	N	Y

Tabulka 7.4: Tabuľka popisuje rozšírenú funkcionalitu peňaženiek.

7.5 Bezpečnosť proti hrozbám

Kapitola sa zaoberá odolnosťou testovaných peňaženiek proti spomínaným kryptomenovým hrozbám. Veľké bezpečnostné hrozby predstavuje napríklad škodlivý malvér, výpočtová sila kvantových počítačov, fyzická krádež hardvérovej peňaženky a zariadenia, na ktorom je peňaženka uložená alebo strata hesla k peňaženke. V tabuľke 7.5 bude uvedené, či testované peňaženky využívajú komunikáciu prostredníctvom Air-gap, prípadne sú odolné voči manipulácii s klientom a tiež či je pri používaní potrebné dôverovať tretím stranám. Kapitola sa teda zaoberá dôležitými bezpečnostnými prvkami peňaženky a tiež ich odolnosťou proti spomínaným hrozbám.

a) **Air-gap**: V prípade tohoto spôsobu komunikácie sa považuje peňaženka odolná voči útoku Man-in-the-Machine. Hodnota (Y) je pripísaná peňaženkám, nepripojeným na internet, komunikujúcim výlučné prostredníctvom QR kódov alebo výmenou SD karty. (Blue wallet umožňuje založenie viac-podpisového účtu Vault, ktorý dokáže komunikovať prostredníctvom Air-gap, klasický Bitcoin a Bitcoin lightning účet, ktoré je možné založiť tiež Air-gap nevyužívajú) Všetkým ostatným peňaženkám nespĺňajúcim vyššie uvedené kritéria je v tabuľke pripísaná hodnota (N). V prípade, že peňaženka poskytuje možnosť založenia účtu umožňujúceho komunikáciu prostredníctvom Air-gap, bude v tabuľke náležite popísané, ktoré typy účtov to sú.

b) **Odolnosť proti manipulácií s klientom**: Vlastnosť (Y) je pripísaná prevažne hardvérovým peňaženkám, na ktorých je nutné vykonávanie podpisovania a hlavne potvrdzovania správnosti údajov o transakcii priamo na zariadení peňaženky. Taktiež je táto vlastnosť pripísaná aj viac-podpisovým peňaženkám, pri ktorých je veľmi malá pravdepo-

dobnosť zmanipulovania dostatočného počtu klientov potrebných na podpísanie transakcie. V iných prípadoch je peňaženkám v tabuľke pripísaná hodnota (N).

c) **Post-kvantová odolnosť**: Vlastnosť (Y) je pripísaná peňaženkám využívajúcim šifrovacie a hašové algoritmy, ktoré sú podľa inštitútu NIST v post-kvantovom svete považované za bezpečné. V prípade, ak peňaženky nespĺňajú podmienky na zabezpečenie proti kvantovým počítačom, sú v tabuľke reprezentované hodnotou (N). Hodnota (-) prislúcha peňaženkám, pri ktorých nie je možné, podľa dostupných informácii potvrdiť/vyvrátiť ich odolnosť. Predpokladá sa však, že takto označené peňaženky nie sú odolné proti výpočtovej sile kvantových počítačov.

d) **Odolnosť proti malvérom**: Vlastnosť (Y) je pripísaná peňaženkám umožňujúcim vykonanie podpisu transakcie priamo na zariadení a tiež je táto vlastnosť pripísaná aj viac-podpisovým peňaženkám, pri ktorých je veľmi malá pravdepodobnosť napadnutia škodlivým malvérom dostatočného počtu peňaženiek potrebných na podpísanie transakcie. V iných prípadoch je peňaženkám v tabuľke pripísaná hodnota (N).

e) **Tajomstvá uchovávané offline**: Vlastnosť (Y) je pripísaná peňaženkám uchovávajúcim tajomstvá vo svojom zapečatenom úložisku a peňaženkám využívajúcim komunikáciu prostredníctvom Air-gap. Kritéria spĺňa aj kategória papierových peňaženiek, tie však neboli testované a boli v práci iba spomínané. Ak peňaženka nespĺňa vyššie uvedené kritéria je v tabuľke označená (N).

f) **Nezávislosť od dôvery v tretie strany**: Vlastnosť (Y) je priradená peňaženkám pri ktorých používateľ vlastní svoj seed a súkromný kľúč patriaci k jeho peňaženke. V prípade ak je používateľ závislý od dôvery v tretiu stranu ohľadom správy seedu a súkromných kľúčov jeho peňaženky, patrí mu v tabuľke vlastnosť (N).

g) **Odolnosť proti fyzickej krádeži**: Peňaženka nie je považovaná za odolnú v prípade, ak sú jej kľúče uložené na zariadení, ktoré je možné ukradnúť, bez zabezpečenia heslom alebo PIN kódom. Vlastnosť (Y) je v tabuľke priradená peňaženkám, ktoré pri zakladaní vyžadujú alebo odporúčajú zabezpečenie prostredníctvom hesla alebo PIN kódu. Čiastočne kritérium spĺňajú peňaženky chránené inou špecifickou funkciou na autentifikáciu používateľa, napríklad párovanie hardvérovej peňaženky prostredníctvom Bluetooth, tieto peňaženky sú v tabuľke označené (P). Vlastnosť (S) pripadá peňaženkám, ktoré pri procese založenia používateľovi neodporučia zabezpečenie peňaženky heslom alebo kódom, používateľ tak musí nastaviť zabezpečenie peňaženky z vlastnej iniciatívy v nastaveniach aplikácie.

h) **Odolnosť proti strate hesla**: Peňaženka nie je považovaná za odolnú v prípade, ak používateľ stratí heslo/PIN a nepozná svoj seed na obnovu peňaženky. Vlastnosť (Y) je priradená aplikáciam poskytujúcim seed peňaženky používateľom. Ak používateľ nepozná seed svojej peňaženky, ako je to v prípade hostovaných peňaženiek na strane servera, musí obnovu svojho hesla riešiť iným spôsobom. Takýmto peňaženkám je v tabuľke pripísaná hodnota (N).

	Air-gap property	Odolnosť proti manipulácii s klientom	Post-kvantová odolnosť	Odolnosť proti malvérom	Tajomstvá uchovávané offline	Nezávislosť od dôvery v tretie strany	Odolnosť proti fyzickej krádeži	Odolnosť proti strate hesla
MyEtherWallet	N	N	N	N	N	Y	Y	Y
Metamask	N	N	N	N	N	Y	Y	Y
Daedalus	N	N	N	N	N	Y	Y	Y
Trezor T	N	Y	-	Y	Y	Y	Y	Y
CoolWallet S	N	Y	N	Y	Y	Y	P	Y
Ellipal Titan	Y	Y	-	Y	Y	Y	Y	Y
Electrum viac-podpisová	N	Y	N	Y	N	Y	Y	Y
Bitpay viac-podpisová	N	Y	N	Y	N	Y	Y	Y
Coinbase host	N	N	N	N	N	N	Y	N
Coinbase wallet	N	N	N	N	N	Y	Y	Y
Coinomi	N	N	N	N	N	Y	Y	Y
Blockchain	N	N	N	N	N	Y	Y	Y
Green wallet	N	N	N	N	N	Y	Y	Y
Blue wallet	Vault - Y Bitcoin - N Lightning - N	N	N	N	N	Y	Y	Y
Exodus	N	N	N	N	N	Y	S	Y

Tabulka 7.5: Tabuľka popisuje mieru odolnosti proti spomínaným hrozbám.

7.6 Porovnanie informácii

Porovnanie získaných informácii o peňaženkách a ich funkcionalitách počas testovania s informáciami uvedenými na stránkach výrobcu. V prípade nesúhlasu medzi zistenými a poskytovanými údajmi, bude v príslušnej sekcii peňaženky popísaný rozdiel. Okrem porovnávania môžu byť v príslušných sekciách peňaženiek popísané aj rôzne funkcionality, ktoré neboli spomínané pri samotnom testovaní peňaženiek.

a) **MyEtherWallet**: Po preskúmaní stránok výrobcu a jeho reklamovanými funkcionalitami ponúkanej peňaženky nebola zistená žiadna odchýlka medzi reklamovanými a testovaním získanými informáciami. Za zmienku však stojí spomenúť niekoľko informácii, ktoré neboli spomínané pri popise testovania peňaženky. V aplikácii peňaženky sa nachádza edukačná sekcia, ktorej zámerom je vzdelávať a poskytovať doporučenia zabezpečenia a správneho využitia peňaženky. Okrem rôznych funkcionalít spojených so správou ich NFT uložených v peňaženke, majú používatelia aj možnosť vygenerovania papierovej verzie ich kryptomenovej peňaženky alebo tiež využívanie rôznych decentralizovaných aplikácii.

b) **Metamask**: Na stránkach výrobcu neboli nájdené žiadne falošne reklamované funkcionality, ktoré by sa reálne nenachádzali v mobilnej aplikácii alebo v internetovom rozšírení. Peňaženka okrem tokenov ERC-20 má plnú podporu tokenov ERC-721 (NFT) a tiež decentralizovaných aplikácii.

c) **Daedalus**: Stránka výrobcu peňaženky neobsahuje veľa informácii o funkcionalitách samotnej peňaženky. Stránka popisuje peňaženku ako full node multiplatformovú aplikáciu, určenú pre najpoužívanejšie operačné systémy. Na stránke je tiež peňaženka prezentovaná ako open source aplikácia podporujúca vytváranie a správu neobmedzeného množstva účtov. Všetky informácie spomínané na stránkach výrobcu spĺňajú špecifikácie peňaženky.

d) **Trezor T**: Na stránkach výrobcu je peňaženka prezentovaná ako multiplatformová aplikácia dostupná na všetkých najpoužívanejších počítačových operačných systémoch a

mobilnom operačnom systéme Android. IOS a Windows nie sú zatiaľ podporované. Výrobca popisuje na stránkach vlastnosti peňaženky akými sú farebný dotykový displej, prostredníctvom ktorého je priamo na zariadení vykonávané zadávanie PIN kódu, prístupovej bezpečnostnej frázy a tiež seed pri procese obnovy. Na stránkach je taktiež reklamovaná široká podpora kryptomien a tiež možnosť využitia špeciálneho firmvéru peňaženky určeného iba správu Bitcoinov. Prezentované sú aj extra funkcie peňaženky akými sú možnosť využitia zabezpečenej 2FA, FIDO2 autentifikácie, šifrovania prostredníctvom GPG a využitie SSH. Peňaženka spĺňa všetky vyššie špecifikácie prezentované výrobcom na stránkach peňaženky.

e) **CoolWallet S**: Výrobca na svojich stránkach ponúka hardvérovú peňaženku o veľkosti kreditnej karty a k nej mobilnú aplikáciu dostupnú na operačných systémoch IOS a Android. Na stránkach je popísané prepojenie peňaženky a mobilného zariadenia prostredníctvom šifrovaného Bluetooth pripojenia. Na stránkach je možné nájsť aj informácie o výdrži baterky v pohotovostnom režime (3 mesiace) a čas potrebný do úplného nabitia zariadenia (2 hodiny). Počas testovania peňaženky bolo zistené, že v uvádzaný časových údajov o výdrži a nabíjaní batérie sú minimálne rozdiely v neprospech zákazníka, ide však o zanedbateľné hodnoty keďže peňaženka má výdrž niekoľko týždňov a jej plné nabitie trvá maximálne 3 hodiny. Na stránkach výrobcu neboli nájdené žiadne falošne reklamované funkcionality, ktoré by sa reálne nenachádzali v mobilnej aplikácii alebo by ich nepodporovala samotná peňaženka.

f) **Ellipal Titan**: Na stránkach peňaženky je primárne kladený dôraz na bezpečnosť a zabezpečenie zariadenia peňaženky. Reklamovaná je komunikácia prostredníctvom Air-gap a tiež úplná izolácia od akejkoľvek siete, neobsahuje žiadne online komponenty ani porty, dokonca aj aktualizáciu firmvéru je nutné vykonať za pomoci SD karty spolu s príslušenstvom dodávaným s peňaženkou. Stránku odolnosti proti demontáži má zabezpečovať celokovové telo zariadenia, ktoré nemožno otvoriť bez toho, aby sa nezničili aj súkromné informácie používateľa. Okrem zabezpečenia peňaženky výrobca na svojich stránkach spomína aj jednoduchosť ovládania prostredníctvom veľkého dotykového displeja a tiež širokú ponuku kryptomien. Po prezretí stránok výrobcu bolo zistené, že všetky prezentované špecifikácie peňaženka spĺňa.

g) **Electrum**: Výrobca na svojich stránkach popisuje svoju peňaženku ako bezpečnú variantu na uchovanie kryptomien. Aplikácia je dostupná na počítačových operačných systémoch Windows, MacOS, Linux a tiež mobilnom systéme Android. Stránka uvádza možnosť vytvorenia viac-podpisovej peňaženky zloženej z 2 až 15 spolu-podpisovateľov, táto funkcionalita bola počas testovania overovaná. Po preskúmaní stránok výrobcu a jeho reklamovanými funkcionalitami ponúkanej peňaženky tak nebola zistená žiadna odchýlka medzi reklamovanými a testovaním získanými informáciami.

h) **Bitpay**: Výrobca sa na stránkach peňaženky prezentuje hlavne možnosťou nákupu, uchovania, zmenenia a míňania kryptomien v jednej aplikácii. Čo sa týka prezentovaných špecifikácii viac-podpisovej peňaženky s možnosťou založenia účtu obsahujúceho až 12 spolu-podpisovateľov ide o odchýlku od údajov zistených testovaním. Pri testovaní mobilnej aplikácie bolo zistené, že používateľ má možnosť vytvorenia peňaženky s maximálne 6 spolu-podpisujúcimi, čo je polovica oproti výrobcom prezentovaného údaju. Ostatné prezentované špecifikácie peňaženka spĺňa.

i) **Coinbase**: V prípade hostovanej peňaženky na strane servera reklamuje spoločnosť zabezpečenie prostriedkov uchovávaním prevažnej väčšiny kryptomien v offline úložisku a v prípade problémov sú prostriedky kryté poistením. Táto skutočnosť je však ťažko overiteľnou a používateľovi neostáva nič iné iba dôverovať tejto spoločnosti. Stránky určené pre

peňaženku spravujúcu používateľom reklamujú zabezpečenie a správu širokej škály kryptomien a tiež NFT. Na stránkach výrobcu neboli nájdené žiadne falošne reklamované funkcionality, ktoré by sa reálne nenachádzali v mobilnej aplikácii, na webe alebo v internetovom rozšírení peňaženky.

j) **Coinomi**: Na stránkach výrobcu je peňaženka prezentovaná ako multiplatformová aplikácia dostupná na všetkých najpoužívanejších počítačových operačných systémoch a mobilnom operačnom systéme Android a IOS. Výrobca na stránke popisuje množstvo funkcionalít ohľadom bezpečnosti, použiteľnosti, širokej podpore kryptomien, blockchainov, decentralizovaných aplikácii, podporu Web3 a veľa ďalších. Viackrát je na stránke spomenutá skutočnosť, že bezpečnosť peňaženky nebola nikdy prelomená ani inak ohrozená. Informácie uvedené na stránkach je možné považovať za pravdivé, keďže počas testovania peňaženky neboli zistené žiadne odchýlky medzi prezentovanými a testovaním získanými informáciami.

k) **Blockchain**: Výrobca má na stránke peňaženky uvedené iba základné informácie o peňaženke. Na stránke nie sú spomenuté žiadne funkcionality a tiež zabezpečenie peňaženky. Stránka hovorí o možnosti nákupu, predaja a zmenenia kryptomien spolu s informáciou, že ide o typ peňaženky, nad ktorou má plnú správu majiteľ peňaženky. Výrobca na stránkach peňaženky neposkytuje veľa informácii ohľadom funkcionality ponúkanej peňaženky.

l) **Green wallet**: Výrobca peňaženky ponúka používateľom možnosť výberu medzi jedno-podpisovou a viac-podpisovou ochranou a tiež kompatibilitu s viacerými hardvérovými peňaženkami. Na stránkach je prezentovaná napríklad funkcionalita Replace-By-Fee a tiež ako jedna z mála peňaženiek podporuje Bitcoin Liquid sieť. Nechýba oznam výrobcu, že Green wallet nevyžaduje žiadne dokumenty, osobné alebo kontaktné údaje na jej založenie (väčšina konkurenčných peňaženiek tieto údaje taktiež nevyžaduje). Po preskúmaní stránok výrobcu a jeho reklamovanými funkcionalitami ponúkanej peňaženky nebola zistená žiadna odchýlka medzi reklamovanými a testovaním získanými informáciami.

m) **Blue wallet**: Výrobca na svojich stránkach prezentuje variabilitu aplikácie založením viacerých rôznych peňaženiek, používateľ má na výber medzi účtom klasickým, viac-podpisovým Vault, Lightning a účtom určeným len na sledovanie. Účet lightning je podľa výrobcu možné používať bez potreby otvárania kanálu alebo spravovania uzlu za účelom čo najjednoduchšieho použitia. Okrem spomínaných možností založenia peňaženky je na stránke uvedených množstvo ďalších funkcionalít, ktoré už však boli popísané pri testovaní peňaženky. Po prezretí stránok výrobcu bolo zistené, že všetky prezentované špecifikácie peňaženka spĺňa.

n) **Exodus**: Na stránkach výrobca uvádza hlavne jednoduchú správu peňaženky, jej zabezpečenie a tiež možnosť výmeny vlastnených kryptomien. Stránka popisuje funkcionality zamerané na jednoduché odosielanie a prijímanie prostriedkov spolu s funkciami na zabezpečenie aplikácie a jej kľúčov. Peňaženka podľa informácii na stránke podporuje viac ako 180 kryptomien. Taktiež je na stránke popísaná kompatibilita rozhrania peňaženky s hardvérovou peňaženkou Trezor, funkcia sa nazýva Trezor detection. Na stránkach výrobcu neboli nájdené žiadne falošne reklamované funkcionality, ktoré by sa reálne nenachádzali v mobilnej alebo počítačovej aplikácii.

Kapitola 8

Doporučenia pre rôzne prípady použitia

V kapitole budú popísané doporučenia pre bezpečné a správne používanie kryptomenových peňaženiek. Kryptomenové peňaženky rôznych kategórii poskytujú užívateľom rôzne funkcie na zjednodušenie používania peňaženky a tiež rozličné stupne zabezpečenia ich kryptomien. Správne používanie peňaženky používateľovi pomôže zjednodušiť prácu s kryptomenami a taktiež ich čo najlepšie ochrániť za pomoci využitia všetkých poskytovaných funkcií peňaženky. V podkapitolách pre špecifické prípady využitia, budú popísané správne využitia rôznych funkcionalít peňaženiek a tiež dôvody prečo je vhodný práve takýto postup pri vykonávaní bežných procesov spojených s kryptomenovou peňaženkou[35].

8.1 Vytvorenie a uloženie seedu

Pri vytváraní peňaženky je najbezpečnejšie riešenie zvoliť možnosť vygenerovania najdlhšieho ponúkaného seedu spolu s doplnením o rozširovaciu bezpečnostnú frázu, ktorá sa stane súčasťou seedu. Momentálne je za bezpečný seed považovaný ten s dĺžkou aspoň 12 slov. Pokročilejšie peňaženky ponúkajú možnosť zvolenia Shamir zálohy, táto záloha seedu vyžaduje zvolenie počtu seedov na vygenerovanie a taktiež aký počet z vygenerovaných je potrebný na obnovu peňaženky. Zaloha Shamir ponúka momentálne jednou z najbezpečnejších variant uloženia seedu, pretože je nepravdepodobné, že by bol útočník schopný získať dostatočný počet dielov postačujúcich na obnovu. Pri ukladaní seedu je potrebné sa uistiť, že nikto iný okrem povolaných osôb nemá možnosť tento seed zneužiť. Uloženie seedu je nutné v správnom poradí, presne tak ako bol vygenerovaný a z dôvodu bezpečnosti nikdy nevyhotovovať žiadnu elektronickú kópiu frázy. Vygenerovaný seed je vhodné zapisovať ceruzkou na kus papiera, pero nemusí byť vyhovujúce, lebo časom môžu zapísané slová vyblednúť prípadne sa rozpiť. Nevýhodou papiera je neodolnosť voči prírodným živlom (oheň, voda a pod.), riešením sú napríklad špeciálne doštičky, na ktoré je možné gravírovacím perom zapísať seed. Takto uložený seed je odolný proti poškodeniu ohňom, vodou a podobným hrozbám, cena takýchto zariadení je individuálna, môže to však byť aj cez 100 eur. Záleží tak na používateľovi akú možnosť zvolí. Po uložení seedu je vhodné ihneď skontrolovať či nedošlo k chybe pri odpisovaní, niektoré peňaženky takúto kontrolu vyžadujú ešte pred dokončením procesu vytvárania peňaženky alebo poskytujú možnosť zobrazenia seedu po prihlásení.

8.2 Transakcie

Zasielanie a prijímanie prostriedkov má podobný princíp ako je tomu pri klasických bankových prevodoch. Odosielateľ potrebuje poznať adresu, na ktorú bude posielať kryptomeny, príjemca mu zas túto adresu musí vedieť poskytnúť. V nasledujúcich podkapitolách budú definované doporučenia pre správne zasielanie a prijímanie prostriedkov.

Vytvorenie transakcie

Najrýchlejším spôsobom zadania adresy je naskenovanie QR kódu príjemcu, po úspešnom skene je automaticky vyplnená adresa a prípadne množstvo zasielaných prostriedkov, ak príjemca zadal požadované množstvo kryptomeny pri generovaní QR kódu. V prípade, ak peňaženka nepodporuje načítavanie QR kódov je možné adresu manuálne skopírovať, vložiť a určiť množstvo zasielaných prostriedkov. Ak ide o adresu, na ktorú má odosielateľ v budúcnosti plán zasielať nejaké prostriedky je vhodné si túto adresu uložiť do adresára, nie každá peňaženka ho však podporuje. Pri určovaní výšky poplatku záleží od používateľa ako rýchlo požaduje aby bola jeho transakcia zahrnutá do bloku. Zvyčajne je využívaná štandardná alebo vysoká priorita transakcie. Počas manuálneho nastavovania výšky poplatku je dôležité aby nebol odosielateľom určený príliš nízky poplatok, výsledkom toho by bola potenciálne ťažiarmi ignorovaná transakcia. Ak by bola vytvorená transakcia s nízkym poplatkom, je možné využiť funkciu Replace-By-Fee, ktorá umožní navýšenie poplatku a prípadne zlúči všetky ešte nepotvrdené transakcie do jednej. Takéto zlučovanie viacerých transakcii je možné v niektorých peňaženkách aj rovno pri vytváraní transakcie, užívateľ môže zadať väčší počet príjemcov a každému zvoliť rôzne zasielané množstvo. Spôsob hromadnej transakcie šetrí prostriedky zaplatením jedného poplatku za platbu obsahujúcu viac transakcii. Pri Bitcoine je rýchlejšie vykonanú transakcia možné dosiahnuť aj používaním lightning siete. Bezpečnosť môže byť zvýšená aj používaním bitcoinovej adresy pre výdavok, táto adresa sťažuje sledovanie transakcii odosielateľa. Pred odoslaním je nutné transakciu priamo v aplikácii alebo zariadení skontrolovať, potvrdiť správnosť adresy, množstva zasielanej kryptomeny a maximálnu veľkosť poplatku za vykonanie transakcie.

Prijímanie prostriedkov

Pri zasielaní adresy je z hľadiska bezpečnosti vhodné vždy generovať novú adresu na prijatie prostriedkov. Pre odosielateľa aj príjemcu je asi najjednoduchšia varianta výmeny adresy prostredníctvom QR kódu, do ktorého je možné zakomponovať aj požadované množstvo prostriedkov. Dôležité je zaslanie správnej adresy, ktorá prislúcha zasielanej kryptomene, v prípade, že by boli zaslané prostriedky na zlú adresu, nie je možné túto transakciu nijako navrátiť. V súčastnosti zaslanie nesprávnej adresy nemusí predstavovať veľké riziko, pretože väčšina peňaženiek dokáže detegovať nesprávnu adresu a následne na to upozorní používateľa.

8.3 Obnova peňaženky

Na obnovu peňaženky v aplikácii je potrebné správne zvoliť počet slov seedu obnovovanej peňaženky. Pri obnove je dôležité skontrolovať či nehrozí tzv. shoulder surfering[1], pri ktorom

[1]shoulder surfering - typ útoku pri ktorom útočník sleduje displej prípadne klávesnicu zariadenia pri zadávaní citlivých informácii

by sa mohol potencionálny útočník zmocniť zadávaných slov, následne peňaženku obnoviť a získať tak kontrolu nad všetkými kryptomenami uloženými v peňaženke. Obnovovaciu frázu je nutné zadať v správnom poradí tak ako bola vygenerovaná a prípadne doplnená o rozšírenú bezpečnostnú frázu, dodržaná musí byť aj správna veľkosť písmen. V prípade ak bola peňaženka obnovovaná napríklad z dôvodu straty HW zariadenia alebo odcudzenia zariadenia, v ktorom sa nachádzala aplikácia s peňaženkou, je potrebné okrem obnovy aj vytvorenie novej peňaženky a uloženie novovytvoreného bezpečného seedu. Do novovytvorenej peňaženky je potrebné zaslať všetky prostriedky z obnovovanej peňaženky. Ak by sa dostal útočník k seedu alebo zariadeniu s pôvodnou peňaženkou nezískal by kontrolu nad žiadnymi prostriedkami.

8.4 Zabezpečenie peňaženky

Pre zvýšenie zabezpečenia peňaženky je doporučené používať PIN kód, prístupové heslo alebo autentifikáciu pomocou biometrie. Prístupové heslo by malo byť dostatočne dlhé a netriviálne, obsahovať by malo veľké aj malé písmena, číslice a špeciálne znaky. Niektoré aplikácie umožňujú aj možnosť aktivácie 2FA, táto bezpečnostná funkcionalita je vhodná na ochranu proti neautorizovaným transakciám alebo zmene kritických nastavení peňaženky. V prípade, že je aplikácia peňaženky často spúšťaná na zariadení je dôležité nastavenie automatického odhlásenia po určitej dobe nečinnosti. Ak je peňaženka používaná na verejnom mieste je vhodné využívať možnosť skrytia zostatkov v aplikácii, užívateľ tak predíde riziku, že by mohol niekto zahliadnuť akým veľkým množstvom prostriedkov peňaženka disponuje. Pri používaní hardvérových peňaženiek je najbezpečnejším riešením vykonávať všetky akcie priamo na zariadení peňaženky, dokáže sa tým minimalizovať riziko potencionálnych hrozieb spojených s kryptomenovými peňaženkami. Pri lightweight bitcoinových účtoch je pre zdatného užívateľa odporúčané zvoliť server uzlu, ktorý považuje za súkromnejší a bezpečnejší. Za účelom zachovania väčšej anonymity je doporučené využívanie proxy serverov. Doporučuje sa využívanie súkromných a nie verejných proxy serverov, tie verejné sú často sledovateľné a tým pádom pri nich klesá úroveň anonymity. Okrem využívania proxy serverov býva v niektorých peňaženkách dostupná aj funkcia ochrany súkromia s názvom Tor, ktorá zabraňuje pozorovateľom zaznamenať používateľovu IP adresu a tiež sledovať kde a kedy vysiela transakcie, pomocou získaných údajov môžu byť potenciálne odhalené používateľove adresy a ich zostatky. Pri využívaní tejto funkcie je celý sieťový tok spojený s peňaženkou smerovaný cez Tor. Nevýhodou je, že môže dôjsť k zvýšeniu latencie, pretože je internetový prenos smerovaný cez viacero uzlov a tým pádom aj na väčšiu vzdialenosť.

8.5 Rozšírené prípady použitia

Táto podkapitola obsahuje definíciu doporučení pre krajné prípady použitia kryptomenových peňaženiek. Prípady použitia budú zamerané na podpísanie a overenie správ, nasadenie smart kontraktu a taktiež aj pridávanie sietí a tokenov do kryptomenových peňaženiek.

Podpísanie a overenie správy

Podpisovanie správ je používané napríklad na preukázanie vlastníctva konkrétnej adresy. Pri podpisovaní a overovaní správy je dôležité vybrať správnu adresu, zadať text správy a potvrdiť správnosť údajov na zariadení, prípadne aplikácii. Po potvrdení je vygenerovaný podpis správy. V prípade overovania správy je potrebné do príslušných textových polí zadať

text správy, adresu a vygenerovaný podpis. Po kliknutí na tlačidlo overiť je na obrazovke zobrazená správa o úspešnom alebo neúspešnom overení správy. Aplikácia Trezor Suite ponúka možnosť výberu podpísania správy vo formáte Trezor a aj Electrum.

Nasadenie smart kontraktu

Pre nasadenie smart kontraktu je potrebné mať dostatočné množstvo prostriedkov potrebných na nasadenie, čím je nasadzovaný kontrakt náročnejší tým bude potrebné väčšie množstvo kryptomeny. Užívateľ musí pri nasadzovaní zadať Byte code, ABI/JSON rozhranie a názov kontraktu. Byte code spolu s ABI/JSON rozhraním je možné získať po skompilovaní kódu kontraktu. Získané údaje je potrebné vložiť do príslušných textových polí, zvoliť názov kontraktu a kliknúť na tlačidlo podpísania transakcie. Pre následnú interakciu s nasadeným smart kontraktom je nutné počkať, kým bude vytvorená transakcia vyťažená.

Pridávanie siete alebo tokenu

Pokiaľ kryptomenová peňaženka podporuje pridávanie sietí je požadované zadanie názvu siete, novej URL RPC adresy, ID reťazca, symbol a prípadne aj adresu blokového prehliadača. Druhou možnosťou je vyhľadanie siete na stránke chainlist, ktorá sa dokáže prepojiť s peňaženkou pridanou ako rozšírenie prehliadača a jednoduchým spôsobom bez nutnosti vyplňovania skôr spomínaných údajov pridať sieť do peňaženky. Pri pridávaní siete je potrebné dbať na bezpečnosť a pridávať iba siete, ktorým užívateľ dôveruje. Škodlivá sieť môže zaznamenávať sieťovú aktivitu používateľa. Ak by si chcel užívateľ pridať testovaciu sieť zvyčajne je to možné pri zakladaní peňaženky v rozšírených nastaveniach. V prípade pridávania tokenu typu ERC-20 ponúka veľa peňaženiek podporu širokej škály tokenov, ktoré stačí iba povoliť v nastaveniach aplikácie. V inom prípade je potrebné poznať adresu kontraktu tokenu a jeho symbol. Tieto informácie je možné nájsť napríklad na oficiálnych stránkach pridávaného tokenu. Po zadaní údajov je token po chvíli pridaný do peňaženky. Pri pridávaní tokenov je taktiež nutné dbať na bezpečnosť, pretože existuje veľké množstvo škodlivých tokenov maskovaných za iné, v komunite obľúbenejšie, kryptomeny.

Kapitola 9

Záver

Cieľom práce bolo zanalyzovať bezpečnosť a použiteľnosť kryptomenových peňaženiek rôznych kategórii a pomôcť tak čitateľovi s vybratím správnej peňaženky na základe jeho používateľských potrieb a bezpečnostných nárokov. Analýza bola doplnená o vhodné doporučenia pre správne a bezpečné využívanie vybranej peňaženky.

Cieľ práce bol naplnený, naučili sme sa, aké softvérové a hardvérové hrozby súvisia s uchovávaním kryptomien a aký je rozdiel medzi jednotlivými kategóriami kryptomenových peňaženiek. Podľa navrhnutých testovacích scenárov sme systematicky otestovali 14 rôznych kryptomenových peňaženiek. Toto testovanie sme následne vyhodnotili do tabuliek, v ktorých dokážu nájsť používatelia všetky potrebné informácie týkajúce sa funkcionalít a zabezpečenia ich potencionálne v budúcnosti využívanej peňaženke. Na záver práce sme preskúmali, ako správne a bezpečne používať akúkoľvek kryptomenovú peňaženku a na základe získaných poznatkov sme definovali pre používateľov rôzne doporučenia.

Práca mi dala veľmi veľa nových znalostí v oblasti kryptomien, naučila ma, ako čo najlepšie využiť používateľský potenciál jednotlivých kryptomenových peňaženiek a tiež, ako čo najlepšie zabezpečiť peňaženku proti potencionálnym hrozbám.

Túto prácu možno rozšíriť o pridanie a otestovanie ďalších peňaženiek, ktoré by tak zvýšili kvalitu a výpovednú hodnotu práce. Okrem pridania ďalších peňaženiek by bolo vhodné doplnenie používateľského testovania, pri ktorom by používatelia s rôznym vekom, vzdelaním a úrovňou znalostí v oblasti kryptomien vykonávali vopred navrhnuté úlohy na všetkých testovaných peňaženkách. Výsledky používateľského testovania by nám pomohli lepšie pochopiť, aká je úroveň ich znalostí, identifikovať nedostatky a na základe výsledkov pomôcť v tejto oblasti zvýšiť ich povedomie.

Literatura

[1] Bakkum, D. *Does airgap make Bitcoin hardware wallets more secure?* 2021. [Online]. Dostupné z: https://shiftcrypto.ch/blog/does-airgap-make-bitcoin-hardware-wallets-more-secure/.

[2] Benton, O. *Paper Wallets — A Relic of the Past.* 2019. [Online]. Dostupné z: https://blog.trezor.io/paper-wallets-a-relic-of-the-past-1f711ba82b8c.

[3] Binance. *Binance coin.* 2013. [Online]. Dostupné z: https://www.binance.com/en/bnb.

[4] Binance. *Binance.* 2017. [Online]. Dostupné z: https://www.binance.com/.

[5] Bitpay. *Non-Custodial Bitcoin wallet.* 2021. [Online]. Dostupné z: https://bitpay.com/wallet/.

[6] Blockchain. *Blockchain wallet.* 2021. [Online]. Dostupné z: https://www.blockchain.com/wallet.

[7] Blockstream. *Blockstream Green: Simple and secure Bitcoin wallet.* 2022. [Online]. Dostupné z: https://blockstream.com/green/.

[8] Bluewallet. *BlueWallet - Bitcoin wallet and Lightning wallet for iOS and Android.* 2022. [Online]. Dostupné z: https://bluewallet.io/.

[9] Bocek, T. a Stiller, B. Smart contracts–blockchains in the wings. In: Claudia Linnhoff Popien, M. Z., ed. *Digital marketplaces unleashed.* Springer, 2018, s. 169–184. ISBN 978-3-662-49275-8.

[10] Cardano. *Cardano.* 2015. [Online]. Dostupné z: https://cardano.org/.

[11] Chainlist. *Chainlist.* 2022. [Online]. Dostupné z: https://chainlist.org/.

[12] Coinbase. *Coinbase wallet.* 2011. [Online]. Dostupné z: https://www.coinbase.com/.

[13] Coinbase. *Coinbase wallet.* 2022. [Online]. Dostupné z: https://www.coinbase.com/wallet.

[14] CoinGecko. *CoinGecko.* 2022. [Online]. Dostupné z: https://www.coingecko.com/.

[15] CoinMarketCap. *CoinMarketCap.* 2013. [Online]. Dostupné z: https://coinmarketcap.com/.

[16] Coinomi. *Coinomi wallet.* 2021. [Online]. Dostupné z: https://www.coinomi.com/en/.

[17] CoolBitX. *Coolwallet S hardware wallet*. 2022. [Online]. Dostupné z: https://www.coolwallet.io/product/coolwallet/.

[18] Daedalus. *Daedalus wallet*. 2021. [Online]. Dostupné z: https://daedaluswallet.io/.

[19] Di Angelo, M. a Slazer, G. Wallet contracts on Ethereum. In: IEEE. *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2020, s. 1–2. ISBN 978-1-7281-6680-3.

[20] Electrum. *Electrum wallet*. 2021. [Online]. Dostupné z: https://electrum.org/#home.

[21] Ellipan. *Ellipan Titan wallet*. 2022. [Online]. Dostupné z: https://www.ellipal.com/pages/coldwallet.

[22] Eskandari, S., Clark, J., Barrera, D. a Stobert, E. A first look at the usability of bitcoin key management. *ArXiv preprint arXiv:1802.04351*. 2018.

[23] Ethereum. *Ethereum*. 2013. [Online]. Dostupné z: https://ethereum.org/en/.

[24] Exodus. *Best Crypto Wallet for Desktop and Mobile: Altcoin and Bitcoin | Exodus*. 2022. [Online]. Dostupné z: https://www.exodus.com/.

[25] Farell, R. An analysis of the cryptocurrency industry. 2015.

[26] Fedler, R., Schütte, J. a Kulicke, M. On the effectiveness of malware protection on android. *Fraunhofer AISEC*. 2013, sv. 45, s. 53.

[27] Fei, Y., Ding, A. A., Lao, J. a Zhang, L. A Statistics-based Fundamental Model for Side-channel Attack Analysis. *IACR Cryptol. ePrint Arch.* Citeseer. 2014, sv. 2014, s. 152.

[28] Gennaro, R., Goldfeder, S. a Narayanan, A. Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security. In: Springer. *International Conference on Applied Cryptography and Network Security*. 2016, s. 156–174.

[29] Gurkov, A. Blockchain in Arbitration Development: Multi-Signature Wallet Showcase. *IJODR*. HeinOnline. 2017, sv. 4, s. 63.

[30] Homoliak, I., Breitenbacher, D., Binder, A. a Szalachowski, P. An air-gapped 2-factor authentication for smart-contract wallets. *ArXiv preprint arXiv:1812.03598*. 2018.

[31] Hosp, J. *Kryptomeny*. Bratislava: Tatran, 2018. ISBN 9788022209458.

[32] Kondr, M. *Analýza způsobů uchování kryptoměny Bitcoin*. Vysoká škola ekonomická v Praze, 2021.

[33] LEE, M. *Postkvantová doba se blíží: přinese rok 2022 konec šifrování, jak ho známe?* 2022. [Online]. Dostupné z: https://www.root.cz/clanky/postkvantova-doba-se-blizi-prinese-rok-2022-konec-sifrovani-jak-ho-zname/.

[34] Limited, B. H. *Trust Wallet*. 2021. [Online]. Dostupné z: https://trustwallet.com/.

[35] Ljunggren, N. *Improving the usability of secure information storing within blockchain applications*. 2019. Student Paper.

[36] Lukáš, K. *Bezpezpečnostní analỳza hardwarovỳch krypto peněženek*. 2020. B.S. thesis. České vysoké učení technické v Praze. Vypočetní a informační centrum.

[37] Mallik, A. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*. 2019, sv. 2, č. 2, s. 109–134.

[38] Menezes, A. J., Van Oorschot, P. C. a Vanstone, S. A. Handbook of applied cryptography. The CRC Press series on discrete mathematics and its applications. In: *2000 NW Corporate Blvd.* CRC Press, 1997.

[39] Metamask. *The crypto wallet and gateway to Web3 blockchain apps | Metamask*. 2022. [Online]. Dostupné z: https://metamask.io/.

[40] Moniruzzaman, M., Chowdhury, F. a Ferdous, M. S. Examining usability issues in blockchain-based cryptocurrency wallets. In: Springer. *International Conference on Cyber Security and Computer Science*. 2020, s. 631–643.

[41] MyEtherWallet. *MyEtherWallet*. 2021. [Online]. Dostupné z: https://www.myetherwallet.com/.

[42] Nechvatal, J. PUBLIC-KEY CRYPTOGRAPHY NIST Special Publication 800-2. *NIST Special Publication*. Citeseer. 1991, sv. 800, s. 2.

[43] Pal, O., Alam, B., Thakur, V. a Singh, S. Key management for blockchain technology. *ICT Express*. Elsevier. 2021, sv. 7, č. 1, s. 76–80.

[44] Pillai, A., Saraswat, V. a Arunkumar, V. Smart Wallets on Blockchain—Attacks and Their Costs. In: Springer. *International Conference on Smart City and Informatization*. 2019, s. 649–660.

[45] Pte. Ltd. imToken. *ImToken*. 2021. [Online]. Dostupné z: https://token.im/.

[46] SatoshiLabs. *Passphrase — the Ultimate Protection for Your Accounts*. 2019. [Online]. Dostupné z: https://blog.trezor.io/passphrase-the-ultimate-protection-for-your-accounts-3a311990925b.

[47] Solana. *Solana*. 2018. [Online]. Dostupné z: https://solana.com/.

[48] Souppaya, M., Scarfone, K. et al. Guide to malware incident prevention and handling for desktops and laptops. *NIST Special Publication*. 2013, sv. 800, s. 83.

[49] Stiawan, D., Idris, M., Malik, R. F., Nurmaini, S., Alsharif, N. et al. Investigating brute force attack patterns in IoT network. *Journal of Electrical and Computer Engineering*. Hindawi. 2019, sv. 2019.

[50] Suratkar, S., Shirole, M. a Bhirud, S. Cryptocurrency Wallet: A Review. In: IEEE. *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. 2020, s. 1–7.

[51] Tereshkin, A. Evil maid goes after PGP whole disk encryption. In: *Proceedings of the 3rd International Conference on Security of Information and Networks*. 2010, s. 2–2.

[52] Tiri, K. Side-channel attack pitfalls. In: IEEE. *2007 44th ACM/IEEE Design Automation Conference*. 2007, s. 15–20.

[53] Trezor. *Trezor T hardware wallet*. 2022. [Online]. Dostupné z: https://trezor.io/.

[54] Tuli, P. a Sahu, P. System monitoring and security using keylogger. *International Journal of Computer Science and Mobile Computing*. 2013, sv. 2, č. 3, s. 106–111.

[55] Vilchez, A. *Crypto Clipping: A Practice That Puts Your Wallet at Risk*. 2022. [Online]. Dostupné z: https://webmediums.com/technology/crypto-clipping-a-practice-that-puts-your-wallet-at-risk-eqtv7fwsr2by.

[56] Vykopal, J., Plesnik, T. a Minarik, P. Network-based dictionary attack detection. In: IEEE. *2009 international conference on future networks*. 2009, s. 23–27.

Příloha A

Obsah priloženého úložiska

Na priloženom kompaktnom disku sa nachádza bakalárska práca vrátane jej zdrojového kódu LaTeX.

- **xbrnaf00.pdf** – táto bakalárska práca,
- **xbrnaf00_zdroj.zip** – zdrojové kódy LaTeX na kompiláciu tejto bakalárskej práce