Bezpečnostní aspekty kryptoměn

Bc. David Hél

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. David Hél**
Osobní číslo:	**A19508**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Bezpečnostní aspekty kryptoměn**
Téma práce anglicky:	**The Safety Aspects of Crypto-currencies**

Zásady pro vypracování

1. Popište současný stav kryptoměn: využití a zabezpečení.
2. Vyberte parametry zabezpečení pro následnou analýzu jednotlivých kryptoměn.
3. Analyzujte zabezpečení kryptoměn z pohledu anonymity uživatele.
4. Analyzujte zabezpečení transakcí a samotné kryptoměny.
5. Navrhněte zlepšení vycházející z bodu 3 a 4.

Forma zpracování diplomové práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. KARAME, Ghassan a Elli ANDROULAKI. Bitcoin and Blockchain Security. Artech House, 2016. ISBN 978-1630810139.
2. CHOO, Kim-Kwang Raymond, Ali DEHGHANTANHA a Reza M. Blockchain Cybersecurity, Trust and Privacy: Advances in Information Security. Springer, 2020. ISBN 978-3030381806.
3. GALDI, Clemente a Vladimir KOLESNIKOV. Security and Cryptography for Networks. Amalfi, 2020. ISBN 978-3-030-57990-6.
4. Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain. Packt Publishing, 2018. ISBN 1788990188.
5. SHRIVASTAVA, Gulshan, Dac-Nhuong LE a Kavita SHARMA. Cryptocurrencies and Blockchain Technology Applications. Wiley-Scrivener, 2020. ISBN 978-1119621164.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 11. 5. 2021

David Hél v.r.

.....

podpis autora

ABSTRAKT

Předmětem této diplomové práce je analýza bezpečnostních aspektů kryptoměn z pohledu anonymity uživatelů a zabezpečení transakcí, potažmo celého systému kryptoměn. V teoretické části je nejprve popsán blockchain, jeho vlastnosti, architektura a struktura. Právě blockchain je totiž základním stavebním prvkem kryptoměn. Následně se práce zaměřuje na kryptografické funkce a metody, jež jsou využívány k zabezpečení a spolehlivému fungování kryptoměn. Praktická část této práce je věnována samotným analýzám, k nimž byly využity metody SWOT a TOPSIS. Nejprve je provedeno srovnání daných metod v rámci bezpečnostních aspektů, z čehož následně vychází analýza anonymity a stanovení nejlepších možných variant zabezpečení. Získaná data jsou v poslední kapitole využita pro analýzu celkového zabezpečení systému kryptoměn, kde jsou navíc srovnány výsledky jednotlivých metod analýzy. Závěr práce je na základě provedených analýz zaměřen na návrh opatření a případných zlepšení.

Klíčová slova: Kryptoměny, blockchain, TOPSIS, SWOT, kryptografie, digitální podpisy, hashovací funkce, služby míchání mincí, chytré smlouvy, důkazy nulových znalostí, konsensuální metody, akumulátory, homomorfní závazky, transakce mimo blockchain

ABSTRACT

The subject of this diploma thesis is the analysis of safety aspects of cryptocurrencies from the user anonymity, transaction safety and the whole cryptocurrency system point of view. The theoretical part first describes the blockchain, its properties, architecture and structure. Subsequently, the work is focused on cryptographic functions and methods that are used for security. The practical part of this work is devoted to the analysis itself. First, a comparison of the methods within the safety aspects is performed, which is then the basis of the analysis of anonymity and the determination of the best possible security options. The obtained data are used in the last chapter for the analysis of the overall cryptocurrency safety, where the results of individual methods of analysis are also compared. The conclusion of the work is focused on security measures and possible improvements.

Keywords: Cryptocurrencies, blockchain, TOPSIS, SWOT, cryptography, digital signatures, hash functions, mixing services, smart contracts, zero-knowledge proofs, consensual methods, accummulators, homomorphic commitments

Chtěl bych poděkovat vedoucímu diplomové práce Ing. Davidu Malaníkovi, Ph.D. za odborné vedení, za pomoc, trpělivost, hodnotné konzultace, rady a zpětnou vazbu při zpracování této práce.

OBSAH

ÚVOD

Kryptoměny jsou fenoménem posledních několika let, ať už z pohledu informačních technologií či samotné ekonomiky. Tato poměrně mladá technologie láká s velkou popularizací měn, jako jsou Bitcoin či Ethereum, velkou řadu nových uživatelů. Jedná se o samotné těžaře kryptoměn či investory, kteří mají často v těchto měnách uloženy nemalé sumy peněz. S tím však ruku v ruce přicházejí také bezpečnostní rizika a hrozby, kterým kryptoměny, stejně jako jiné technologie, čelí. Za účelem ochrany před ztrátou peněz či osobních údajů uživatelů tak vznikají a neustále se rozvíjejí bezpečnostní kryptografické metody, které jsou hlavním předmětem analýzy.

Tato práce je logicky rozdělena na část teoretickou a část praktickou, které jsou následně děleny do jednotlivých kapitol a podkapitol. Úvodní kapitola teoretické části se blíže zaměřuje na technologii blockchainu, který je základním stavebním kamenem právě kryptoměn, jimiž se tato práce zaobírá, ale taktéž jiných odvětví jakou jsou například zdravotnictví, státní instituce či jiné finanční subjekty. Přestože je tato diplomová práce zaměřena na problematiku kryptoměn z hlediska jejich zabezpečení a anonymity, pochopení fungování blockchainu a jeho jednotlivých částí je pro následnou analýzu velmi důležité. Podstatné bylo zaměřit se kromě požadavků na blockchain také na jeho samotnou strukturu a využívané konsensuální metody, které slouží zejména pro zabezpečení jednotlivých transakcí, spolehlivost a jednotnost dat.

Ve druhé části teorie bylo klíčové zjistit, analyzovat a popsat kryptografické metody a funkce, které se v blockchainu a především u samotných kryptoměn využívají. Takzvaná kryptografická primitiva jsou pro potřeby analýzy rozdělena do dvou základních skupin, na primární a volitelné. Co se zabezpečení a anonymity týká, podrobně analyzována byla v první řadě volitelná primitiva, mezi než patří služby míchání mincí, chytré kontrakty či důkazy nulových znalostí, které hrají velkou roli v oblasti ochrany transakcí a zajištění anonymity jejich účastníků.

Další část práce se zabývá analýzou bezpečnostních aspektů z hlediska anonymity a soukromí uživatelů. Před samotnými výpočty bylo nejdříve důležité definovat dané hodnotící kritéria, váhy jednotlivých kritérií a bodovou stupnici hodnocení. Dle toho byly prostřednictvím analýzy TOPSIS nejprve vybrány nejideálnější metody využívané v rámci daných primitiv a jejich bodové hodnocení bylo využito pro reprezentaci kryptografických metod v celkové analýze bezpečnosti. Na základě získaných výsledků bylo zhodnoceno využití metod a srovnání s použitím v praxi.

Zjištěné informace ohledně blockchainu a kryptografických metod byly dále využity pro následnou analýzu celkové bezpečnosti transakcí a kryptoměn nejprve pomocí metody SWOT, a následně i metodou TOPSIS. Byly stanoveny silné a slabé stránky kryptoměn, které vycházejí především z vlastností a funkcí samotného blockchainu.

Na základě bezpečnostních aspektů a jejich možných nedostatků byly stanoveny hrozby kryptoměn, které vedou ke ztrátě dat či nefunkčnosti systému. Podle významu silných stránek, příležitostí, slabých stránek a hrozeb byly stanoveny váhy jednotlivých atributů, což vedlo k odhalení největších problémů a hodnocení velikosti rizika. Jednotlivé aspekty byly pro získání lepších a přesnějších výsledků zhodnoceny také metodou TOPSIS, výsledky obou metod byly následně srovnány a vyhodnoceny kryptografické metody a funkce, které se na zabezpečení kryptoměn podílejí nejvíce.

Závěr práce se zaměřuje na návrh zlepšení zabezpečení, který vychází z dat jak analýzy anonymity, tak z analýzy celkového zabezpečení systému kryptoměn.

I. TEORETICKÁ ČÁST

1 Blockchain

Tato část práce je zaměřena na jednotlivé technologie využívané při práci s kryptoměnami jak z hlediska funkčního, tak bezpečnostního. Nejprve bude vysvětlen pojem blackchain, který je v kryptoměnách stěžejním. Pro potřeby analýzy a pochopení fungování technologie kryptoměn, budou podrobněji popsány jak jeho vlastnosti a funkce, tak následně i architektura, která se dělí na tři základní typy, jejichž rozdíly budou vysvětleny a rozebrány. Jak je z názvu blockchainu patrné, jedná se o řetězec na sebe navazujících bloků, jejichž struktura a jednotlivé parametry dílčích částí hrají nezbytnou roli v rámci fungování celé technologie.

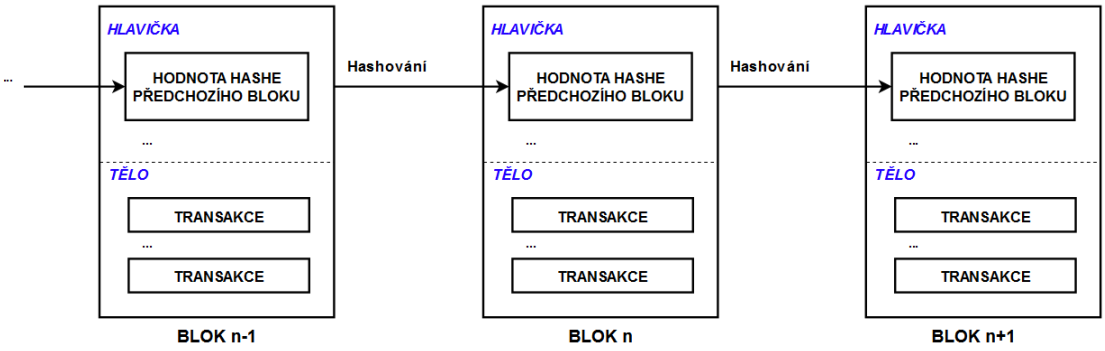
1.1 Vlastnosti a funkce blockchainu

Základem nejvyužívanějších kryptoměn, jako jsou Bitcoin, Ethereum či například Litecoin, je blockchain. Jeho historie sahá do 80. a 90. let uplynulého století, avšak světově známým se tento pojem stal právě v roce 2008 po objevení kryptoměny s názvem Bitcoin. Podle Pilkingtona byla první představa digitální měny založena na principu centralizovaného serveru z důvodu problému vícenásobné útraty, kdy dva či více uzlů sítě zadají transakce přikazující poslání peněz z totožného účtu takovým způsobem, že ve výsledné sumě je přesunovaná částka větší než zůstatek. Tento způsob však nakonec nevyřešil ani problém vícenásobné útraty, ani anonymitu či centralizaci [15].

Zásadního průlomu a celosvětové pozornosti se tudíž tato technologie dočkala až ve zmíněném roce 2008 zásluhou Satoshi Nakamota, jenž navrhl nahradit klasickou centralizovanou architekturu novou technologií založenou na decentralizovaných konsensuálních metodách. V letech 2011 až 2013 byla technologie blockchainu využívána zejména právě v kryptoměnách. V dnešní době však slouží ve spoustě dalších odvětvích jako například v armádě pro logistiku a finance či zdravotnictví pro bezpečnější uchování dat. Právě zdravotnická zařízení jsou totiž velmi častým a oblíbeným cílem kybernetických útočníků [15].

Pokud jde o samotnou technologii, zjednodušeně řečeno je blockchain specifickým typem databáze. Klíčovým rozdílem mezi těmito dvěma pojmy je však to, jakým způsobem jsou data v těchto databází strukturována. V případě blockchainu jsou jednotlivé informace ukládány do skupin označovaných jako bloky, jež nesou sadu dat. Blockchain je tedy distribuovaná databáze sestávající se z navzájem propojených bloků dat, které jsou chráněny kryptografickými koncepty proti neoprávněné manipulaci. Blockchain funguje bez účasti jakékoli centrální autority a je řízen na základě konsensu účastníků jeho sítě. Klíčovým pojmem celé sítě je uzel (*node*), což je jednoduše řečeno uživatel nebo počítač v architektuře blockchainu [22].

S přibývajícími bloky neustále rostou také data blockchainu. Jakmile jsou data do blockchainu přidána, v rámci principu neměnnosti struktury nemohou být smazána dokud nedojde k dohodě mezi všemi či většinou účastníků. Jak je demonstrováno na obrázku 1.1, každý blok navíc obsahuje hash předchozího bloku za účelem ochrany proti neoprávněné manipulaci a integrity dat.



Obrázek 1.1 Blockchain jako datová struktura[1)]

Technologie blockchainu se skládá z pěti základních stavebních prvků, mezi než patří [11]:

- síť peer-to-peer
- blockchain jako datová struktura
- konsensus
- transakce
- kryprografie

Velkou popularitu a sílu si technologie blockchainu vydobyla hlavně svými užitečnými vlastnostmi a silnými aspekty, které uživatelům nabízí. Mezi nejsilnější stránky patří bezesporu distributivita, zabezpečení a integrita dat, transparentnost, decentralizace či úspora nákladů, na které bude zaměřena tato část práce [41].

1. **Distribuovaná povaha blockchainu** – Stejná data jsou v síti blockchainu ve stejný čas ukládána různými uzly. Pokud je jeden z uzlů poškozen nebo o data přijde, ostatní uzly v síti mají stále kopii blockchainu uloženou a mohou ji obnovit. Chybný uzel si může překopírovat blockchain od ostatních uzlů. Tato funkce zabraňuje ztrátě dat, neoprávněné manipulaci s daty a dvojímu utrácení v kryptoměnách.

[1)] Zpracováno dle lit. Zheng (2017)

2. **Integrita a zabezpečení dat** – Blockchain je odolný proti neoprávněné manipulaci v tom smyslu, že při změně jakýchkoli dat v jakémkoli bloku je změna detekována v důsledku změny hashe bloku. Změněný hash bloku se tady v takovém případě bude lišit od dříve uloženého hashe v dalším bloku. Pokud by chtěl být útočník úspěšný, musel by upravit data bloků pro všechny uzly v síti, což je pro velkou síť prakticky nemožné.

3. **Transparentnost a dohledatelnost** – Jelikož jsou záznamy v jednotlivých blocích blockchainu opatřeny časovým razítky a uloženy ve všech úplných uzlech sítě, může veškeré vykonávané aktivity a transakce kontrolovat a sledovat kdokoliv z dané sítě. V případě, že je známa adresa uzlu, všechny aktivity a transakce jsou vysledovatelné. Díky tomu je blockchain transparentní a sledovatelný, což je velkou výhodou pro odhalování podvodů a je dobrým nástrojem pro audit a veřejné služby.

4. **Decentralizace** – Blockchain je nezávislý na centrálních autoritách a zprostředkovatelích, čímž se stává vhodnějším pro důvěryhodné systémy. Výjimkou jsou soukromé blockchainy, které sice mohou být částečně či plně centralizované, avšak i nadále benefitují z ostatních vlastností této technologie.

5. **Úspora nákladů** – Využití blockchainu přináší obrovské úspory nákladů, jež jsou spojeny se zprostředkujícími systémy. Této vlastnosti se snaží využívat hlavně banky a velké podniky, které tak mohou značně snížit své náklady.

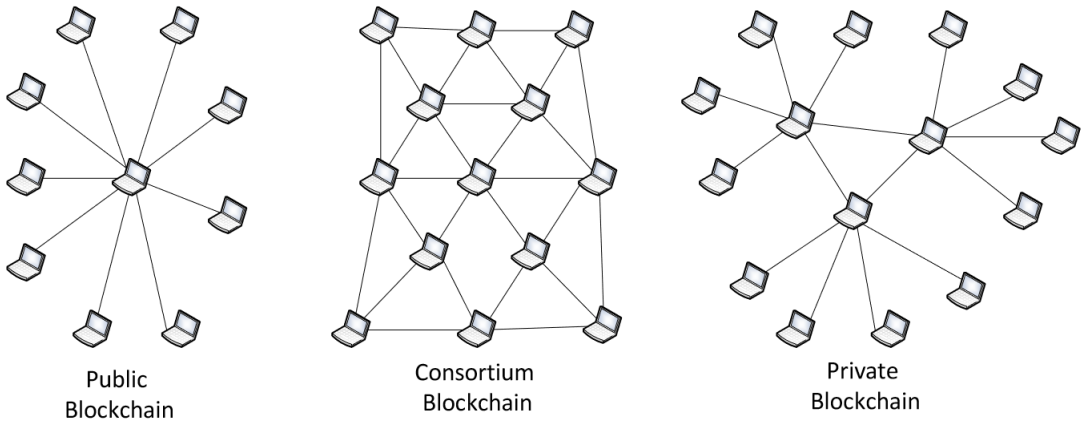
6. **Efektivita** – Odstraněním zprostředkujících subsystémů navíc blockchain umožňuje systémům pracovat autonomně a s vyšší efektivitou.

7. **Neměnnost** – Jakmile jsou data uložena v blockchainu, extrémně obtížně se dají změnit. Využíváním technologie konsensuálních metod je navíc možné dosáhnou konsensu i v prostředí bez důvěry. Tato vlastnost je pro databáze používané při transakcích peněz extrémně výhodná. Záznamy jsou totiž neměnné do té doby, dokud by někdo současně nezískal kontrolu nad 51 a více procenty uzlů v síti.

8. **Ověřitelnost** – Na základě využití kryptografických metod v blockchainu lze ověřit autenticitu daného záznamu. V ostatních typech databází totiž nemusí být ověření využitím digitálního podpisu, který je v technologii blockchainu použit, jednoduchou záležitostí [41].

1.2 Architektura

Na základě mnoha kritérií se systémy blockchainu rozdělují do tří základní skupin, a to na veřejný blockchain, soukromý blockchain a blockchain na základě dohody neboli také *consorcium blockchain*. Jednotlivé rozdíly mezi těmito typy blockchainů jsou vysvětleny v následujících řádcích a schémata znázorněna na obrázku 1.2.



Obrázek 1.2 Modely jednotlivých architektur blockchainu[2)]

1.2.1 Veřejný blockchain

Veřejný blockchain poskytuje otevřenou platformu pro lidi z různých organizací a různých prostředí k připojení se, vytváření transakcí a těžení kryptoměny. U žádné ze zmíněných funkcí neexistují žádná omezení, proto jsou často nazývány taktéž jako *blockchainy bez nutnosti povolení*. Každý účastník má v jakémkoli čase plné oprávnění ke čtení či zápisu transakcí, k provádění auditu v blockchainu nebo kontrole kterékoli části blockchainu [41].

Blockchain je otevřený, transparentní a nedisponuje žádnými uzly, které jsou zaměřeny na validaci. Všichni uživatelé v takovém typu schématu mohou shromažďovat transakce a začít s procesem těžby kryptoměny za účelem dosažení takzvané odměny. Dostupností kopie celého blockchainu synchronizovaného se všemi uzly je tento systém neměnný. Na základě kompletní decentralizace, rozsahu existujících sítí a otevřené platformě, do níž se může kdokoliv přidat, může dojít k dohodě (konsensus) využitím kteréhokoli z decentralizovaných mechanismů jako například Proof of Work či Proof of Stake, jež jsou podrobněji popsány v části 1.4. Otevřeností systému a veřejnou dostupností účetní knihy je veřejný blockchain mnohem náchylnější k útokům. Tento nedostatek je však při každém přidání nového bloku odstraňován využitím mechanismu Proof of Work společně s vhodně využitými kryptografickými hashovacími funkcemi.

[2)] Převzato z lit. Dhanalakshmi (2019)

Systém veřejného blockchainu využívají nejznámější digitální měny jako například Bitcoin, Ethereum či Litecoin [34].

Veřejný blockchain se tedy vyznačuje několika charakteristickými vlastnostmi, jež by se daly shrnout do následujících bodů:

- Každý uzel má přistup ke čtení a zápisu do peněženky
- Kdokoliv může stahovat a přidávat uzly do systému
- Tato technologie je přirozeně plně decentralizovaná
- Nabízí anonymitu, díky čemuž nemůžou být transakce zpětně vystopovány
- Pomalejší v porovnání se soukromým blockchainem

1.2.2 Soukromý blockchain

Jedná se o typ systému blockchainu, jenž je nastaven tak, aby usnadňoval soukromé sdílení mezi skupinou jednotlivců v jedné či více organizacích, s těžbou ovládanou jednou organizací nebo vybranými jednotlivci. Soukromý blockchain se nazývá také jako *blockchain vyžadující povolení*. Důvodem je to, že neznámí uživatelé nemají k danému blockchainu přístup dokud nedostanou speciální povolení. Přístup uzlů je přidělován sadou pravidel nebo prostřednictvím pověřené sítě, která kontroluje přístup. Díky tomu tato architektura na rozdíl od veřejného blockchainu mnohem více inklinuje k celkové centralizaci sítě a zároveň se odchyluje od základních principů této technologie, kterými jsou decentralizace a otevřenost systému. Jakmile se v systému soukromého blockchainu stanou uzly součástí sítě, přispívají decentralizaci sítě přičemž každý uzel udržuje kopii účetní knihy a spolupracuje na dosažení dohody pro aktualizaci. Na rozdíl od veřejného blockchainu je čtení a zápis omezen [41][34].

1.2.3 Blockchain na základě dohody

Consortium blockchain neboli blockchain na základě dohody je typ systému, který lze považovat za částečně soukromý blockchain vyžadující oprávnění, kde je za konsensus a validaci jednotlivých bloků zodpovědná předem určená sada uzlů a nikoli organizace [40]. Tyto uzly rozhodují o tom, kdo může být součástí sítě a kdo může těžit. Pro validaci bloků se v této architektuře využívají schémata pro vícenásobný elektronický podpis. Blok je považován za platný až poté, co je podepsán danými uzly. Na rozdíl od veřejného blockchainu, který je považován za zcela decentralizovaný a soukromého blockchainu, jenž je naopak zcela centralizovaný, je consortium blockchain centralizovaný jen částečně. Omezení čtení a zápisu je stanoveno na základě vybraného konsensu. Tento systém využívá ku příkladu Ripple [41].

Vlastnosti	Public blockchain	Consortium blockchain	Private blockchain
Stanovení souhlasu	Kdokoliv	Vybraná skupina uzlů	v jedné organizaci
Povolení ke čtení	Veřejný	Veřejný či omezený	Veřejný či omezený
Úroveň neměnnosti	Téměř nemožná manipulace	Může dojít k manipulaci	Může dojít k manipulaci
Spotřeba zdrojů	Nízká	Vysoká	Vysoká
Centralizace	Ne	Částečná	Ano
Proces souhlasu	Bez povolení	Vyžadováno povolení	Vyžadováno povolení

Tabulka 1.1 Srovnání vlastnostní jednotlových typů architektur blockchainu[3)]

1.3 Struktura bloku

Blok je datová struktura, která seskupuje jednotlivé transakce, které jsou dále zahrnuty do takzvaného *public ledger* neboli účetní knihy. Sestává se z hlavičky bloku, která obsahuje metadata a dlouhého seznamu transakcí, který tvoří většinu jeho velikosti. Hlavička bloku má velikost 80 bajtů, kdežto průměrná velikost transakce bývá 250 bajtů. Průměrný blok navíc disponuje více než pěti sty takovýchto transakcí. V následující tabulce 1.2 jsou popsány jednotlivé části struktury bloku [1].

Velikost	Položka	Popis
4 bajty	Velikost bloku	Velikost bloku
80 bajtů	Hlavička bloku	Několik položek uložených v hlavičce bloku
1-9 bajtů	Počítadlo transakcí	Kolik následuje transakcí
Různá	Transakce	Transakce uložené v daném bloku

Tabulka 1.2 Struktura bloku v blockchainu

1.3.1 Identifikátory bloku

Hlavním identifikátorem bloku je jeho kryptografická hash, což by se dalo přirovnat k digitálnímu otisku prstu, který je například u bitcoinu vytvořen dvojitým hashováním hlavičky bloku za využití algoritmu SHA-256. Jedná se o jedinečný a unikátní identifikátor. Výsledný 32 bitů dlouhý hash kód je nazýván rovněž jako *block hash* či přesněji *block header hash* z důvodu, že je k jeho výpočtu využita pouze hlavička bloku.

Druhým způsobem jak identifikovat blok je prostřednictvím jeho pozice v blockchainu. Tento parametr se nazývá výška bloku čili *block height*. Na rozdíl od hash bloku není délka bloku jedinečným identifikátorem. Přestože jeden blok bude mít vždy konkrétní a neměnnou výšku bloku, opačné tvrzení není pravdivé. Je totiž možné, že dva nebo více bloků soutěžících o stejnou pozici v blockchainu, může mít stejnou výšku [1].

[3)] Zpracováno dle lit. Zheng (2017)

1.3.2 Hlavička bloku

Jak již bylo zmíněno, hlavička bloku tvoří pouze malou část velikosti celého bloku a rozděluje se do tří sad metadat. První část sestává z odkazu na hash předchozího bloku v daném blockchainu. Další sadu metadat tvoří proměnné difficulty, timestamp a nonce, které jsou spojeny s těžbou kryptoměny. Třetí částí je pak merkle tree root, což je datová struktura využívaná k efektivnímu shrnutí veškerých transakcí v bloku [47].

1. **Verze bloku** – Síť blockchainu se skládá z několika ověřovacích pravidel, které je zapotřebí dodržovat. Verze bloku z toho důvodu specifikuje soubor protokolů, jimiž je nutné se řídit.

2. **Timestamp** – Časová značka reprezentující aktuální čas v sekundách od 1. ledna 1970.

3. **Parent block hash** – Hodnota hashe o velikost 256 bitů, která odkazuje na předchozí blok.

4. **nBits** – Target trashold je 256 bitové číslo bez znaménka, jehož hodnota hashe v hlavičce musí být menší nebo rovna proto, aby mohla být považována za validní část blockchainu. Položka nBits však disponuje velikostí pouze 32 bitů, a pracuje tak s méně přesným formátem, který se nazývá kompaktní.

5. **Nonce** – Nonce obvykle začíná nulou a inkrementuje se pro každou hodnotu hashe. Jeho velikost jsou 4 bajty.

6. **Merkle tree root** – Hash kořene hashového stromu (*markle tree*) transakcí daného bloku.

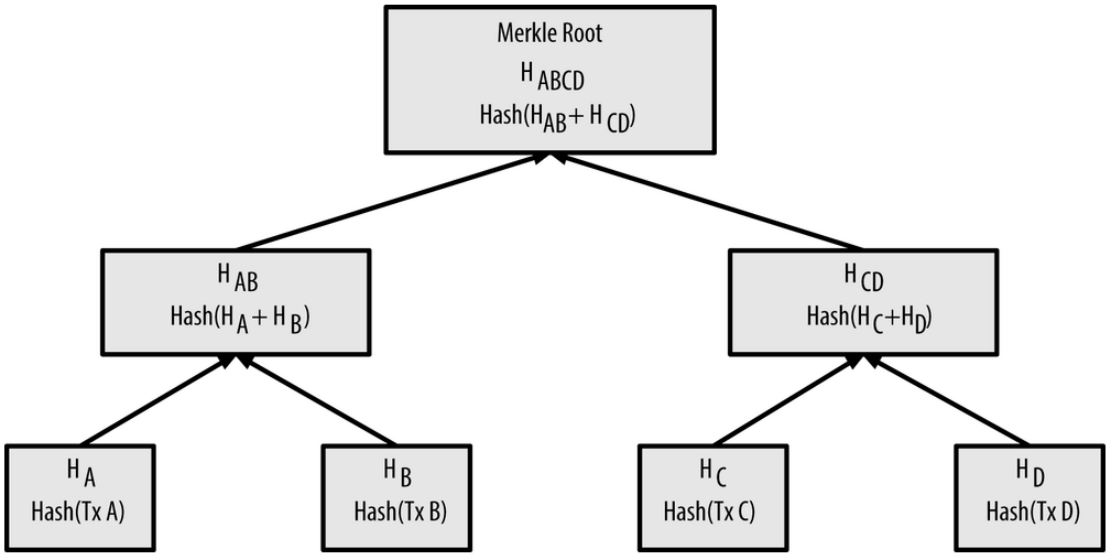
Hashový strom

Každý blok v blockchainu obsahuje souhrn všech transakcí v bloku, k čemuž využívá hashový strom neboli *merkle tree*. Jedná se o datovou strukturu pro efektivní sumarizaci a ověřování integrity velkých sad dat obsahující kryptografické hashe. Jak již bylo zmíněno, v kryptoměnách se merkle tree využívají ke shrnutí veškerých transakcí v bloku a vytváření digitálního otisku celé sady, což poskytuje velmi výhodný proces k ověření, zda je transakce zahrnuta v bloku či nikoli. Hashový strom je procházen zdola nahoru a konstruován rekurzivním hashováním dvojice uzlů dokud nevznikne jeden hash, jenž se nazývá kořen neboli *root* nebo *merkle root*. U nejznámější kryptoměny Bitcoinu je využíván algoritmus SHA-256, který je aplikován dvakrát [13].

V případě, že je N datových záznamů hashováno a sjednoceno v rámci hashového stromu, je možné zkontrolovat, zda se každý jeden záznam ve stromu nachází pomocí

maximálně $2 \times log_2(N)$ výpočtů, což z merkle tree činí velmi výhodnou datovou strukturu pro velký objem dat.

Pro vysvětlení fungovaní stromu mějme čtyři transakce označené písmeny A, B, C a D, které tvoří listy dané stromové struktury, tedy vrcholy, které nemají žádného potomka. Jak je zobrazeno na obrázku 1.3, jednotlivé transakce nejsou přímo uloženy ve struktuře merkle tree, ale jejich data jsou hashována a výsledný hash uložen v každém listu s označením H_A, H_B, H_C, a H_D.



Obrázek 1.3 Výpočet uzlů ve struktuře hashového stromu[4)]

Jelikož je hashový strom binárním stromem, musí jeho struktura obsahovat sudý počet uzlů. V případě, že je zapotřebí sjednotit a ověřit lichý počet transakcí, poslední hash transakce je duplikována, čímž je zachována vyváženost stromu.

Stejnou metodu pro konstrukci stromu ze čtyř transakcí lze zobecnit na konstrukci stromů jakékoli velikosti. V kryptoměnách je běžné mít několik stovek až více než tisíc transakcí v jednom bloku, které jsou sjednocovány stejným způsobem do výsledného merkle rootu, jehož velikost vždy činí pouhých 32 bajtů. K důkazu, že byla daná transakce přidána do bloku, potřebuje uzel $log_2(N)$ 32-bajtových hashů, které tvoří takzvanou autentizační cestu (*authentication path nebo merkle path*) spojující specifickou transakci s kořenem stromu. Takováto složitost je důležitá zejména s rostoucím počtem transakcí, což ukazuje tabulka 1.3 [39].

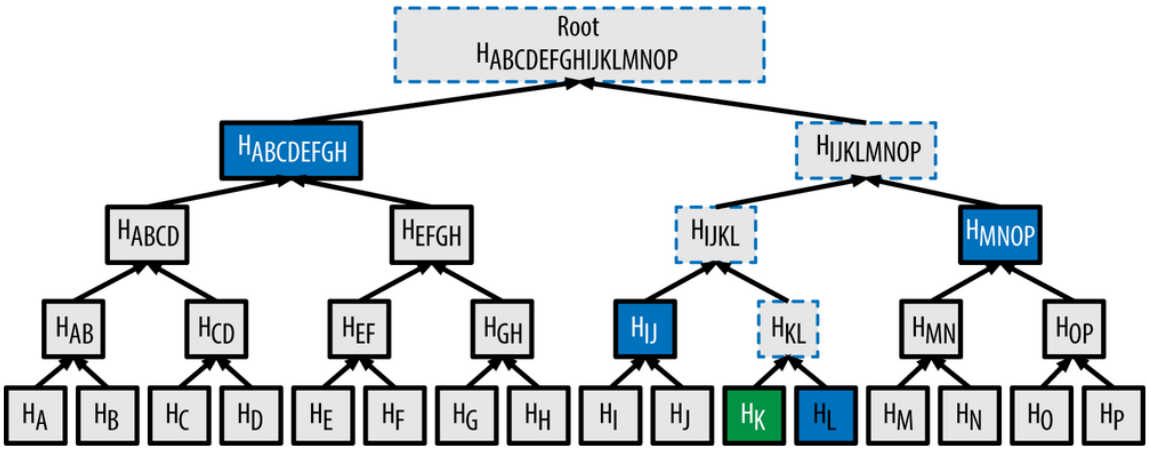
Jelikož se jedná o logaritmus o základu dvě, s přibývajícím množstvím dat se množství výpočtů zvyšuje mnohem pomaleji. Tím je možno v kryptoměnách efektivně vytvářet cesty o deseti až dvanácti hashích, což se rovná 320 až 384 bajtům, které umožňují dokázat přítomnost jediné z více než tisíce transakcí v blocích o velkosti megabajtů.

[4)] Převzato z `https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html`

Počet transakcí	Přibližná velikost bloku	Délka cesty	Velikost cesty
16 transakcí	4 kilobajty	4 hashe	128 bajtů
512 transakcí	128 kilobajtů	9 hashů	288 bajtů
2048 transakcí	512 kilobajtů	11 hashů	352 bajtů
65 535 transakcí	16 megabajtů	16 hashů	512 bajtů

Tabulka 1.3 Efektivita hashového stromu

Obrázek 1.4 ukazuje, že uzel může dokázat přítomnost transakce K v daném bloku pomocí autentizační cesty o čtyřech krocích, kdy velikost výsledného hashe bude pouze 128 bajtů. Cestu tvoří čtyři hashe H_L, H_{IJ}, H_{MNOP} a $H_{ABCDEFGH}$. S těmito čtyřmi hashi, které udávají danou autentizační cestu lze jakýkoliv uzlem dokázat, že H_K (vyznačený na obrázku zelenou barvou) je součástí merkle rootu dopočítáním tří dalších párových hashů označených jako H_{KL}, H_{IJKL} a $H_{IJKLMNOP}$ a markle rootu [1].



Obrázek 1.4 Autentizační cesta použitá k důkazu přítomnosti transakce v bloku[5)]

1.3.3 Tělo bloku

Na rozdíl od hlavičky bloku je sice tělo tvořeno pouze dvěma částmi, avšak kvůli počtu transakcí je jeho velikost mnohonásobně větší. Zmíněnými částmi jsou počítadlo transakcí a samotné transakce, jejichž struktura je tvořena dalšími dílčími proměnnými [47].

[5)] Převzato z `https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html`

- **Počítadlo transakcí** – Ukládá číslo v případě, že je transakce v bloku.
- **Transakce** – Odkazuje na záznam přenosu aktiv mezi dvěma subjekty. Typická transakce v blockchainu obsahuje následující atributy:
  - **Množství** – Součet všech digitálních hodnot, které je nutné přenést.
  - **Vstupy** – Vstup obsahuje záznam s hodnotami digitálního aktiva, jež je potřeba převést. Celková hodnota se musí rovnat hodnotě uvedené v položce množství.
  - **Výstupy** – Uchovávají detaily o účtech příjemců dané hodnoty. Sestává se z digitálního aktiva, které má být přeneseno na účet příjemce, unikátní identity, jež je přidělena danému příjemci a daných pravidel, které by neměl příjemce pro správné doručené porušit.
  - **ID transakce nebo hash** – Každá transakce obsahuje jedinečnou hodnotu pro svou identifikaci. Může se jednat buďto o identifikátor transakce či hodnotu hash.

1.4 Konsensuální metody

Důležitým aspektem správného fungování technologie blockchainu je zajištění souhlasu kopií dat v různých uzlech sítě, uspořádání bloků a transakcí, které jsou na sobě logicky závislé. K tomuto účelu se využívají konsensuální metody. Jak již bylo zmíněno, prvotním a základním konceptem blockchainu je jeho decentralizace. Z toho důvod není vyžadováno využívání důvěryhodné centralizované autority, ale jsou uplatněny takzvané decentralizované konsensuální metody nebo také konsensuální protokol, jež jsou implementovány prostřednictvím blockchainu za účelem poskytnutí spolehlivosti a jednotnosti dat a zabezpečení samotných transakcí. Jedná se o obecná pravidla následovaná uzly blockchainu určenými pro synchronizaci sítě, údržbu a aktualizaci blockchain ledgeru [39].

Tyto metody jsou založeny na řešení takzvaného konsensuálního problému distribuovaných systémů, jehož princip je následující. Aby došlo ke shodě na hodnotě, je zapotřebí několika uzlů, z nichž některé mohou být vadné. Uzly začínají návrhem možných rozdílných hodnot. Pomocí mechanismu konsensu se všechny správné, tj. nezávadné uzly, dohodnou na jedné z navrhovaných hodnot. Formálně musí řešení problému konsensu splňovat následující podmínky [11]:

- **Platnost** – Pokud uzel určí hodnotu, byla tato hodnota navržena jiným uzlem.
- **Integrita** – Žádný z uzlů nerozhoduje dvakrát.

- **Dohoda** – Žádné dva správné uzly nerozhodují rozdílně.
- **Konečnost** – Každý správný uzel nakonec určí nějakou hodnotu.

Obecně platí, že algoritmus, který je schopný naplnit první tři uvedené podmínky, garantuje bezpečnost, což zjednodušeně řečeno znamená, že se nestane nic špatného. Pokud je splněna rovněž podmínka konečnosti, je zajištěna živost (*liveness*), což znamená, že proces úspěšně nebo neúspěšně skončí.

V současné době se v blockchainu využívají čtyři hlavní technologie, a sice Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS) a Delegated Proof of Stake (DPoS). Mezi další významné, avšak již méně využívané metody se pak řadí například Proof of Bandwidth (PoB) či Proof of Authority (PoA).

Proof of Work

Jedná se o konsensuální metodu používanou v sítích u většiny nejpoužívanějších digitálních měn, jako jsou Bitcoin, Ethereum nebo Litecoin. Satoshi Nakamoto navrhl metodu PoW jako sérii kryptografických „hádanek“ pro počítače, které musejí být vyřešeny za účelem přidání nového bloku. Dané „hádanky“ se označují jako kryptografické hashovací funkce a je možné je vyřešit jen za pomoci hádání a následné kontroly. Počítače, které se snaží daný problém vyřešit, jsou nuceny ověřit biliony nesprávných odpovědí předtím, než najdou odpověď správnou. V případě, že by na stejném problému pracovalo tisíce počítačů, průměrná doba nalezení správné odpovědi se stále pohybuje okolo deseti minut [41].

Počítač, který správnou kombinaci najde, obdrží odměnu. Tisíce dalších však zbytečně ztrácely čas a energii. I díky tomu je PoW považována za energeticky náročnou metodu, což dokazují i statistiky. V září roku 2020 byla spotřebovaná energie odhadovaná na 55,63 až 73,12 TWh za rok, což odpovídá energii, která byla spotřebována za rok v České republice či Rakousku a více než je spotřeba energie ve 175 až 181 zemích světa [32]. Efektivnější variantou PoW je takzvaný Cunningham and bi-twin chains, jehož využívá například kryptoměna Primecoin.

PoW počítá každý uzel sítě hodnotu hashe hlavičky bloku. Jak bylo popsáno v části 1.3.2, hlavička bloku obsahuje *nonce*, který by těžaři (*miners*) kryptoměny často měnili za účelem získání různých hodnot hashe. Konsensus vyžaduje, aby vypočítaná hodnota byla menší nebo rovna dané hodnotě. Pokud jeden z uzlů dosáhne cílové hodnoty, je tato hodnota vysílána ostatním blokům, které musí potvrdit správnost hodnoty hashe. Pokud je blok ověřen, ostatní těžaři připojí nový blok do jejich vlastního blockchainu. Uzly, které počítají hodnoty hashe, se označují jako *miners* a metoda PoW je v Bitcoinu označována jako mining neboli těžení.

Proof of Stake

Odstraněním výpočetně velmi náročných operací je PoS na rozdíl od PoW energeticky mnohem efektivnější variantou. Nevýhodou je však zejména to, že je tato varianta také mnohem náročnější na zabezpečení a má komplikovanější architekturu systému než právě výše zmíněný Proof of Work. V rámci architektury Proof of Stake existují speciální uzly shromažďující transakce a vytvářející nové bloky, které se nazývají *validátory*. Šance validátoru na přidání nového bloku souvisí s vlastnictvím určitého počtu měny (*stake*). Validátor s větším majetkem má větší šanci k přidání nového bloku. Tato metoda je založena na principu, že vlastník velkého majetku nebude mít s velkou pravděpodobností úmysl síť jakýmkoli způsobem poškodit. Hlavní nesnází PoS je však nothing-at-stake problem, kdy validátorské uzly nemají budováním co ztratit. Této varianty konsensu využívají digitální měny jako NEO, Dash nebo Tezos [41].

Delegated Proof of Stake

Blockchain založený na DPoS pracuje s hlasovacím systémem, kde skupina delegátů či taktéž svědků (*witnesses*) ověřuje bloky jménem všech uzlů v síti. Tyto speciální uzly jsou odpovědné za dosažení konsensu v průběhu generování a ověřování nových bloků. Hlasovací síla je úměrná počtu mincí, jimiž uživatel disponuje. Vzhledem k tomu, že systém DPoS udržují voliči, jsou delegáti motivováni k poctivosti a efektivitě, což napomáhá k větší bezpečnosti této metody. V opačném případě mohou být odvoláni [47]. Výhodou oproti klasickému PoS je rovněž vyšší rychlost provedených transakcí za vteřinu. Problémem u DPoS může být vznik kartelu delegátů, kdy se ověřování dostane do malého počtu rukou, což může vést k menší decentralizaci a odolnosti vůči útokům [33].

Practical Byzantine Fault Tolerance

PBFT je modelem založeným na hlasování a využíván primárně v blockchainech typu private a consortium. Tato metoda bezpečně funguje i s chybovými uzly f z celkového počtu uzlů n: $n = (3f + 1)$ a $f = (n - 1)/3$. Systém je tedy bezpečný pouze tehdy, pokud je chybových uzlů nejvýše jedna třetina z celkového počtu. Čím více uzlů v síti je, tím je matematicky méně pravděpodobné, že chybných uzlů bude více než třetina.

Systém PBFT pracuje v po sobě jdoucích cyklech zvaných *views*. Každý cyklus obsahuje volený uzel, který se nazývá jako *primární* nebo také lídr, a ostatní uzly jsou označovány jako *záložní* (backups). Primární uzel řídí tvorbu nových bloků. Klienti odesílají požadavky (transakce) na primární uzel daného cyklu, jež následně zahájí třífázový protokol složený z předběžné přípravy, přípravy a potvrzení tak, že pošle transakce všem záložním uzlům. Ve fázi předběžné přípravy přiřadí primární uzel každé z transakcí pořadové číslo a připraví návrh nového bloku, který následně opět pošle

zbytku uzlů. Primární uzel navíc odesílá takzvanou zprávu předběžné přípravy (pre-prepare message), jež obsahuje primární identifikátor, identifikátor bloku a číslo bloku. Pokud záložní uzel přijme zprávu předběžné přípravy, odešle zpět primárnímu uzlu a zbytku záložních uzlů zprávu přípravy (prepare message), čímž dává souhlas k vytvoření nového bloku. Když záložní uzel přijme $2f + 1$ zpráv přípravy, přejde do fáze potvrzení, kde záložní uzly validují a verifikují požadavky v navrhovaném bloku. Pokud jsou všechny požadavky platné, záložní uzel odešle zprávu o potvrzení do všech ostatních záložních uzlů. Nový blok je následně přidán do blockchainu v případě, že záložní uzly obdrží alespoň $2f + 1$ odpovídajících zpráv o potvrzení [41].

Proof of Authority

V síti, která je založena na mechanismu PoA, jsou transakce a bloky ověřovány prostřednictvím schválených uživatelů, kterým se říká validátoři (*validators*), jež jsou pomocí softwaru schopni přidat jednotlivé transakce do bloku. V PoA si musejí uzly pozici validátora zasloužit, čímž se snaží udržet si pozici, kterou získali. Dodáním reputace k identitě vzniká prostředí, kterým jsou validátoři motivováni udržet své místo, protože si nepřejí, aby byla jejich identita spojena s negativní reputací [4].

Oproti Proof of Work není v tomto případě nutný vysoce výkonný hardware z toho důvodu, že PoA nevyžaduje, aby uzly pracovaly na řešení složitých matematických úkolů. Časové intervaly tvorby nových bloků jsou navíc předvídatelné, kdežto jak u PoW, tak u PoS se tato doba liší. Rychlejší je také proces ověřování transakcí, kdy jsou bloky generovány ve stanoveném časovém intervalu [36].

2 Kryptografie

Jak je patrné ze samotného slova kryptoměna, nedílnou současní celé technologie jsou bezesporu kryptografické funkce a metody, které se pro zabezpečení využívají. Pro potřeby analýzy jsou kryptografická primitiva rozdělena do dvou základní skupin, a sice na primární a volitelné. První z kategorií zahrnuje kryptografické hashe a standardní digitální podpisy, které jsou nezbytné pro zajištění blockchainu jako hlavní účetní knihy systému s ochranou proti neoprávněné manipulaci, veřejnou ověřitelností a dostupným konsensem. Do kategorie volitelných kryptografických primitiv pak spadají metody, které se podílejí především na zvýšení soukromí a anonymity. Podrobněji popsány budou speciální podpisy, mezi něž patří například prstenové podpisy, či prvky známé jako homomorfní závazky, akumulátory nebo důkazy nulových znalostí.

2.1 Hashovací funkce

Hashovací funkce je matematická funkce nebo algoritmus, pomocí něhož dochází k převodu vstupních dat o různé velikosti na výstupní data o stejné velikosti. U hashovacích funkcí jsou obvykle vyžadovány dva bezpečnostní požadavky, kterými jsou jednosměrnost a odolnost vůči kolizím. První ze zmíněných požadavků zajišťuje to, že hashovací funkce není invertibilní, zatímco druhý udává nesnadnost nalezení dvou vstupů se stejnou hodnotou hashe. Pro hashovací funkce o délce výstupu n bitů je složitost prolomení jednosměrnosti a nalezení kolize $O(2^n)$ pro útok hrubou silou (*brute force attack*) a $O(2^{\frac{n}{2}})$ pro narozeninový útok (*birthday attack*) [26].

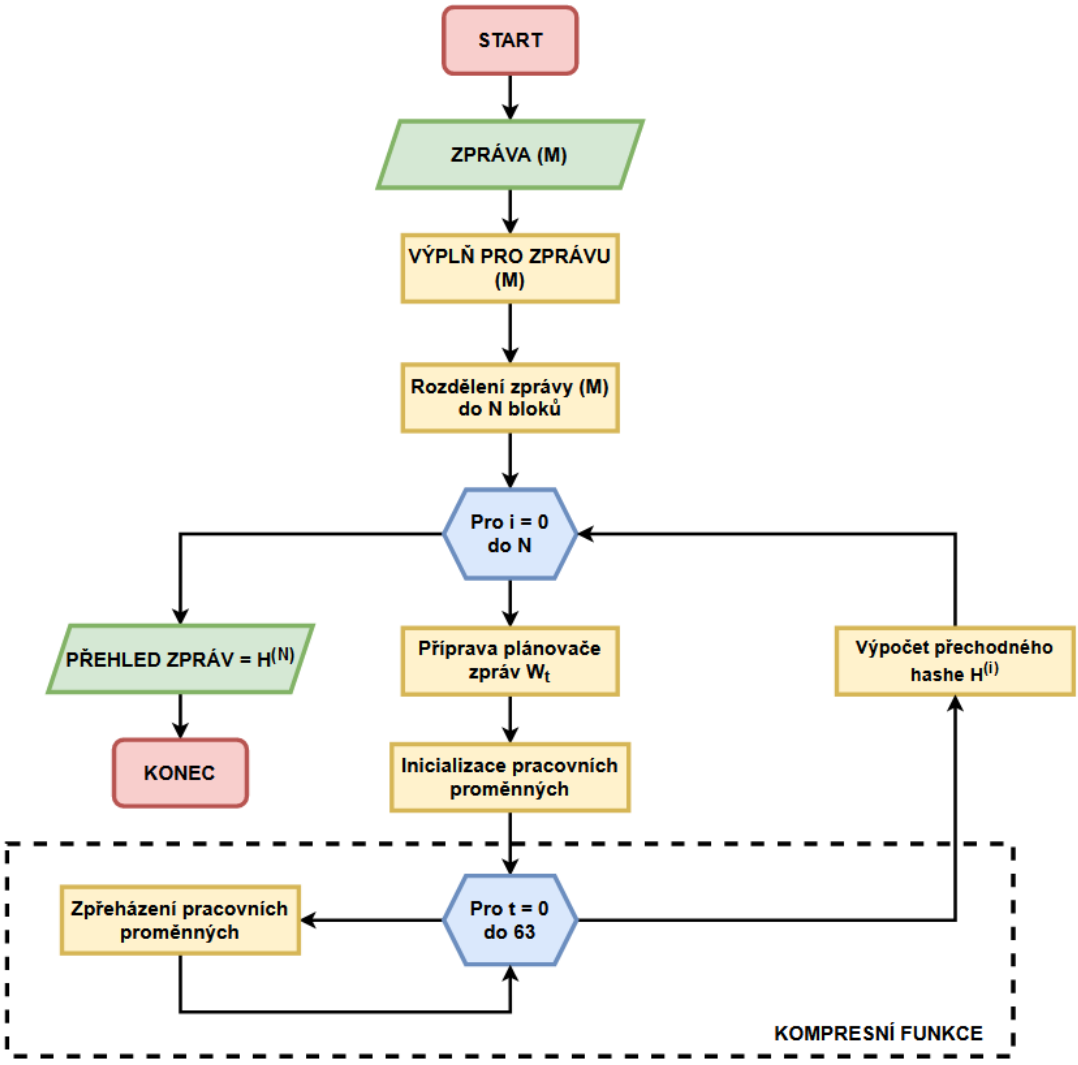
2.1.1 SHA v blockchainu

Nejvyužívanější hashovací funkcí využívanou v technologii blockchainu je SHA-256, což je jeden z rodiny algoritmů kryptografických hashovacích funkcí zvaných SHA[1)], vyvinutý Národní bezpečnostní agenturou USA (NIST). V roce 2004 se skupině okolo Jeffa Wanga podařilo nalézt řadu kolizí v hashovacích funkcích MD5 [2)], MD4, RIPEMD a Haval-128. O rok později dokázali pouhými 269 pokusy prolomit i algoritmus SHA1, což bylo o jedenáct pokusů méně, než počítá zmíněný narozeninový útok. K zajištění bezpečnostních požadavků blockchainu a kryptoměn je doporučeno využívat algoritmy SHA2 nebo SHA3. Pro nalezení kolize v algoritmu SHA-256 je totiž zapotřebí 2128 pokusů. To je při aktuálně dostupném výpočetním výkonu prakticky nemožné.

SHA-256 přijímá zprávu o délce l bitů, kde $(0 < l < 2^{64})$, a jeho výstupem je 256 bitů dlouhá zpráva $H(M)$. Vstupní zpráva (M) je zpracována v blocích, z nichž každý má velikost 512 bitů. Po přidání takzvané výplně (*padding*), což je v kryptografii označení

[1)] Secure Hash Algorithms
[2)] Message-Digest Algorithm

pro rozšíření nezašifrovaných hodnot o náhodné či předem určené znaky, je zpráva rozdělena do N bloků. Po přidání výplně je zpráva rozdělena do bloků, načež je každý zpracován kompresní funkcí. Výsledný hash po zpracování bloku i (přechodný hash $H^{(i)}$) je využit jako počáteční hash (*initial hash*) pro zpracování dalšího bloku. Postup, který je znázorněn na obrázku 2.1, by se tedy dal shrnout do následujících pěti částí [41].



Obrázek 2.1 Algoritmus fungování SHA v blockchainu[3)]

Výplň

Jak již bylo zmíněno, výplň neboli *padding* slouží k přidání extra bitů do vstupní zprávy tak, aby se počet bitů zprávy zvýšil na hodnotu 512. Tím bude mít zpráva vždy n bloků po 512 bitech.

[3)] Zpracováno dle lit. Sanka (2021)

Počáteční hodnota hash $H^{(0)}$

Počáteční hodnota hash je dílčí část (prvních 32 bitů) druhé odmocniny prvních osmi prvočísel. Používá se jako počáteční hodnota pro inicializaci pracovních proměnných při zpracování prvního bloku zprávy. Hodnota sestává z osmi 32 bitových vektorů, které jsou dány následovně [29]:

$$H_0^{(0)} = 6a09e667 \quad H_1^{(0)} = bb7ae85 \quad H_2^{(0)} = 3c6ef372 \quad H_3^{(0)} = a54ff53a \tag{2.1}$$

$$H_4^{(0)} = 510e527f \quad H_5^{(0)} = 9b05688c \quad H_6^{(0)} = 1f83d9ab \quad H_7^{(0)} = 5be0cd19 \tag{2.2}$$

Pracovní proměnné

Reprezentují hash předchozího bloku zprávy tedy $H^{(i-1)}$, který sestává z osmi 32 bitových vektorů od $H_0^{(i-1)}$ do $H_7^{(i-1)}$. Na počátku zpracování každého bloku, je osm pracovních proměnných inicializovaných následujícím způsobem [29]:

$$a = H_0^{(i-1)} \qquad b = H_1^{(i-1)} \qquad c = H_2^{(i-1)} \qquad d = H_3^{(i-1)} \tag{2.3}$$

$$e = H_4^{(i-1)} \qquad f = H_5^{(i-1)} \qquad g = H_6^{(i-1)} \qquad h = H_7^{(i-1)} \tag{2.4}$$

Plánovač zpráv (W_t)

Každý blok zprávy M^i je před provedením kompresní funkce zařazen do takzvaného plánovače zpráv W^t. Každá zpráva obsahuje 16 slov, z nichž každé má velikost 32 bitů, Blok je předán funkci plánovače zpráv, která rozšiřuje 16 slov na 64 slov o velikosti 32 bitů.

Kompresní funkce

Vlastní hashování v rámci SHA probíhá právě v kompresní funkci, která se opakuje v 64 cyklech plánovače zpráv a pracovních proměnných pro každý blok. Jedná se o bitové operace XOR, AND, OR, komplement, modulo $2^{(32)}$, rotace a operace posunu. Předtím, než jsou použity v kompresní funkci, jsou pracovní proměnné inicializovány hodnotou hashe z předchozího bloku, což se označuje jako přechodný hash $H^{(i)}$. Cílem kompresní funkce je zpřeházet a zkomprimovat s blokem zprávy reprezentovaným plánovačem zpráv. Po zamíchání pracovních proměnných kompresní funkcí je přechodný hash vektorů $H_0^{(i)}$ až $H_7^{(i)}$ pro každou zprávu bloku i vypočítána následovně [29]:

$$H_0^{(i)} = a + H_0^{(i-1)} \quad H_1^{(i)} = b + H_1^{(i-1)} \quad H_2^{(i)} = c + H_2^{(i-1)} \quad H_3^{(i)} = d + H_3^{(i-1)} \tag{2.5}$$

$$H_4^{(i)} = e + H_4^{(i-1)} \quad H_5^{(i)} = f + H_5^{(i-1)} \quad H_6^{(i)} = g + H_6^{(i-1)} \quad H_7^{(i)} = h + H_7^{(i-1)} \tag{2.6}$$

Po zpracování všech bloků zpráv je výslednou hodnotou hashe přechodný hash posledního bloku zprávy.

2.1.2 Ostatní hashovací funkce v kryptoměnách

Mezi technikami těžby kryptoměn a hashovacími funkcemi vzniká v poslední době poměrně zajímavý souboj. Vývoj nových technik pro těžbu kryptoměn je pro těžaře velmi lákavý, avšak pro blockchain jako takový to nemusí být zrovna dobrá zpráva. Zejména z toho důvodu, že pokročilé techniky těžby umožňují určité entitě mít vyšší rychlost těžby než ostatní, může dojít s mnohem větší pravděpodobností v případě zneužít ke známému 51% útoku, kdy se útočníkovi povede kontrolovat více než 51% z hashovacího výkonu sítě.

Během uplynulé dekády se těžební rychlost neustále zvyšuje a rozvoj nových těžebních technik se neustále rozvíjí, na což bylo zapotřebí reagovat vývojem nových hashovacích funkcí využívaných v kryptoměnách. Mezi nejznámější patří Ethash, SCrypt, X11 nebo Equihash [26].

- **Ethash** – Je využíván v kryptoměnách založených na technologii Etherea. Jedná se o takzvanou ASIC-resistant hash funkci, která řeší problém využívání ASIC obvodů nebo také zákaznických integrovaných obvodů, jejichž použití zvýhodňuje daného uživatele a může vést k ovládnutí sítě určitou skupinou účastníků.

- **SCrypt** – Tato hashovací funkce se využívá v mnoha kryptoměnách, jako například Tenebrix, Fairbrix či Litecoin. Jedná se o takzvanou memory-hard hashovací funkci (MHF), což je třída funkcí, jejichž rychlé vyhodnocení vyžaduje velké množství výpočetní paměti.

- **X11** – Hashovací funkce spadající stejně jako SCrypt do kategorie MHF a kombinující hned jedenáct hashovacích funkcí vybraných z rodiny kryptografikcých funkcí SHA3. Konkrétně se jedná o funkce Blake, Grostl, JH, Keccak, Skein, ECHO, Luffa, BMW, CubeHash, SHAvite a SMID. V praxi se využívají u některých kryptoměn i funkce s označením X12, X13 nebo X17, kde číslo vždy odkazuje na počet využitých algoritmů.

- **Equihash** – Podobně jako SCrypt a X11 patří Equihash mezi memory-hard hashovací funkce a byl vytvořen pro kryptoměnu zvanou ZeroCoin. Nejúčinějším algoritmem pro prolomení Equihash problému je Wagnerův algoritmus, který vyžaduje složitost $O(2^{\frac{n}{k+1}})$. Jakékoli snížení výpočetní paměti vede ke zvýšení časové náročnosti.

2.2 Digitální podpisy v blockchainu

Digitální podpisy v blockchainu jsou využívány k ověřování transakcí a zajištění neměnnosti technologie. Základní kryptografické zabezpečení u většiny kryptoměn jako jsou Bitcoin, Ethereum a mnoho dalších digitálních měn je založeno na algebraických strukturách eliptických křivek. Mezi tyto algoritmy se řadí také ECDSA[4)] a jeho modifikace, které tvoří osu bezpečnosti transakcí. Řada kryptoměn, ať už klasických či alternativních[5)], však poskytuje zvýšenou anonymitu a soukromí využitím speciálních podpisů, mezi než můžeme počítat například ring signatures nebo multi-signatures [17].

2.2.1 ECDSA

Elliptic Curve Digital Signature Algorithm neboli Protokol digitálního podpisu s využitím eliptických křivek je nejčastěji využívanou metodou pro podpis a verifikaci transakcí. Jedná se o variantu Digital Signature Algorithm (DSA) s využitím Elliptic Curve Cryptography (ECC).

ECDSA využívá stejné problémy (faktorizace, diskrétní logaritmus na eliptických křivkách) jako algoritmy pro šifrování pomocí asymetrické kryptografie. Rozdílem je však především to, že jejich úkolem není zašifrovat nějaká data, aby nemohla být zpětně dešifrována třetí stranou, ale zaručit jejich původ a integritu. ECDSA funguje na obecné eliptické křivce a nyní se používá v Bitcoinech a Ethereu, zatímco EdDSA pracuje na bázi Edwardovy křivky a v současné době této technologie využívají kryptoměny jako Naivecoin či Monero. Edwardova křivka je rovinný model eliptické křivky a má lepší účinnost a bezpečnost než obecná eliptická křivka, jíž využívá právě ECDSA [31].

Strukturu technologie podpisu s využitím eliptických křivek tvoří následující tři části:

1. **Soukromý klíč** – Zjednodušeně řečeno se jedná o tajné, náhodně vygenerované číslo, známé pouze osobě, která jej vygeneroval. V Bitcoinu je vlastník takovéhoto klíče, jenž koresponduje s prostředky v blockchainu, jediným možným účastníkem, který může s těmito prostředky nakládat.

2. **Veřejný klíč** – Jedná se o číslo, které je generováno matematickým vztahem za využití soukromého klíče. Lze jej získat pouze tehdy, pokud je soukromý klíč znám předem. Nikoliv však naopak. Veřejný klíč je generován za účelem veřejného sdílení tak, aby ostatní účastníci mohli určit, zda-li je podpis pravý.

[4)] Elliptic Curve Digital Signature Algorithm

[5)] Alternativní kryptoměna nebo také Altcoin je kryptoměna, která byla představena až po úspěchu Bitcoinu. Obvykle se většina z nich prezentuje jako jeho lepší a výhodnější alternativa.

3. **Podpis** – Taktéž v případě podpisu se jedná o číslo. To však slouží k důkazu, že byla provedena operace podpisu, který je generován z hashe podepisovaného objektu a soukromého klíče. Samotný podpis je tvořen dvěma čísly, jež se označují jako R a S. Účelem je ověřit původní hodnoty hashe a soukromého klíče.

Jak již bylo zmíněno, ECDSA využívá k výpočtu páru podpisů dočasné klíče, jež jsou označovány písmeny R a S. Dočasný soukromý klíč k je náhodně určen na eliptické křivce a jeho odpovídající veřejný klíč je následně vypočítán pomocí rovnice $P = k \times G$. Podpis je vypočítán dle vztahu [1]:

$$S \ = k^{-1}(Hash(m) + dA \times R) mod(p), kde \tag{2.7}$$

- k je dočasným soukromým klíčem
- R je x-ová souřadnice dočasného veřejného klíče
- dA je soukromý klíč
- m je zpráva
- p je řád prvočísla eliptické křivky

Následná verifikace je v ECDSA prováděna za použití dočasných klíčů R, S a veřejného líče. Bod P je odvozen následovně [1]:

$$P = S^{-1} \times Hash(m) \times G + S^{-1} \times R \times Qa, kde \tag{2.8}$$

- Qa je veřejný klíč podepisujícího
- m je zpráva
- G je generátorový bod eliptické křivky

Hlavní výhodou algoritmů založených na eliptických křivkách je oproti dřívějším technologiím, jako jsou RSA[6)] nebo DSA[7)], lepší zabezpečení pro určitou velikost klíče. To znamená, že ECDSA vyžaduje několikanásobně menší velikost klíče pro poskytnutí stejného zabezpečení jako pomocí algoritmu RSA. Pro porovnání mějme RSA o velikosti klíče 1024 bitů, jehož bezpečnostní úrovni odpovídá ECDSA klíč o velikosti pouhých 192 bitů [24]. Jak je zobrazeno v tabulce 2.1, menší velikostí klíčů pak bezesporu souvisí také s mnohem rychlejšími výpočty a generováním klíčů a podpisů, jejichž srovnáním se ve své práci zabývali Jansma a Arrendondo [30].

[6)] Rivest–Shamir–Adleman
[7)] Digital Signature Algorithm

Délka (bity)		Čas generování klíče (s)		Čas generování podpisu (s)	
ECC	**RSA**	**ECC**	**RSA**	**ECC**	**RSA**
163	1024	0,08	0,16	0,15	0,01
233	2240	0,18	7,47	0,34	0,15
283	3072	0,27	9,80	0,59	0,21
409	7680	0,64	133,90	1,18	1,53
571	15360	1,44	679,06	3,07	9,20

Tabulka 2.1 Srovnání času generování klíčů a podpisů v RSA a ECC na základě délky klíče[8)]

Nevýhodou však může být hlavně to, že ke kryptografickým nástrojům má volný přístup celá řada různých uživatelů, kteří mohou znalosti dané technologie využít ke tvorbě nástrojů za účelem poškození jakékoli platformy. K zašifrovaným informacím, které jsou digitálně podepsány, může být navíc i pro ověřeného uživatele vinou časové náročnosti, zejména když je s platformou manipulováno, těžké přistoupit. Kryptografické algoritmy ze své podstaty nechrání před hrozbami a zranitelnostmi, které jsou způsobeny špatným návrhem systému, protokolů či procesů [31].

2.2.2 Speciální podpisy pro blockchain

Pro zvýšení anonymity transakcí a soukromí v kryptoměnách jsou v blockchainech široce využívány i některé pokročilé techniky digitálních podpisů, jako jsou ring signatures nebo multi-signatures.

Ring signatures

V informačních systémech a především digitálních měnách je klíčovým aspektem anonymita. Co se však týče nejznámější kryptoměny Bitcoinu, ten svou propojitelností transakcí poskytuje pouze takzvanou pseudonymitu. Na základě toho se objevilo mnoho alternativních kryptoměn, které se tento problém snaží řešit. Z pohledu kryptografie existuje hned několik typů podpisů zajišťujících anonymitu, mezi než patří kromě prstenového podpisu také skupinové podpisy (*group signature*), slepé podpisy (*blind signature*) či DC-nets. V rámci zabezpečení kryptoměn však byla vždy využita pouze technologie ring signature a jeho modifikace.

Ring signature chrání odesílatele skrytím vstupní části transakce tak, že je výpočetně nemožné určit, kdo je skutečným autorem podpisu dané transakce. Tento typ podpisu je mnohem sofistikovanějším schématem než typické digitální podpisy využí-

[8)] Zpracováno dle lit. Jansma (2004)

vané v kryptoměnách, kterými jsou ECDSA nebo Schnorrův podpis. Prstenové podpisy mohou vyžadovat hned několik veřejných klíčů k verifikaci a právě pojem „prsten“ je využíván z toho důvodu, protože se skládá z částí skupiny částečných digitálních podpisů od různých uživatelů, které dohromady vytvoří unikátní podpis, jenž se využije k podepsání dané transakce. Tato skupina se označuje jako prsten a může být libovolně vybrána z výstupních hodnot ostatních uživatelů v blockchainu [26].

Proces podpisu metodou ring signature probíhá v zásadě následujícím způsobem:

- Marie chce poslat Johnovi 10 Monero tudíž zahájí transakci prostřednictví své peněženky.
- Mariin digitální podpis pro tuto transakci je takzvaný one-time spend key, jenž začíná tím, že je z její peněženky odeslán výstup.
- Následně jsou v transakci vybrány návnady. Jedná se o výstupy z předchozích transakcí, které jsou náhodně vybrány z blockchainu a na výsledném podpisu v ring signature se nepodílejí.
- Všichni členové, kteří se na podpisu podílejí jsou věrohodnými účastníky a je výpočetně nemožné, aby třetí strana jakkoli detekovala, kdo je skutečným uživatelem, který podpis provedl.
- Veškeré výstupy prstenového podpisu tvoří dohromady vstup transakce.
- Iniciátor transakce (Marie) je způsobilý utratit specifickou částku bez toho, aniž by byla rozpoznána její identita od ostatních v prstenu.
- Přestože se Mariin veřejný klíč využívá v její transakci, může být taktéž využit v jakékoli transakci v rámci sítě pro zmatení.

Multi-signatures

Využití multi-signature umožňuje jedinému podpisu pracovat jako několik běžných podpisů jedné zprávy. Jedním z kritérií této technologie je však to, že jeden podpis musí mít stejnou velikost jako běžně využívaný podpis.

Ku příkladu společnost ZILLIQA navrhla novou generaci vysoce výkonné platformy blockchainu, která využívá pro své zabezpečení EC-Schnorr multi-signature, který se skládá z následujících kroků [26]:

1. Standartní schéma Schnorrova podpisu je vytvořeno přes eliptickou křivku specifikovanou *secp256k1*, která není na rozdíl od jiných křivek konstruována náhodně, a umožňuje tak mnohem efektivnější výpočty.

2. Schéma EC-Schnorr signature pro jednoho uživatele je navíc rozšířeno na schéma EC-Schnorr multi-signature pro více uživatelů.

3. EC-Schnorr multi-signatures je vytvořen pro konsensu PBFT, jehož princip je podrobněji popsán v části 1.4.

2.3 Akumulátory

Jedná se o jednosměrné funkce, které v blockchainu a s ním spojených kryptoměnách mohou poskytovat důkazy o členství, a to bez odhalení jakéhokoli ze členů, který se v síti vyskytuje. Pokud jde o funkce akumulátorů, ty se dají rozdělit do tří základních částí, a sice svědek členství, svědek nečlenství a dynamika [26].

Akumulátory tedy umožňují stranám prokázat, že prvek x je v sadě S, aniž byl zveřejnil, který prvek byl zkontrolován. Hodnota x je buďto přidána nebo odebrána akumulátoru A o konstantní velikosti, přičemž dochází k prokázání, že svědek členství u v kombinaci s hodnotou x je roven akumulátoru A. Hodnoty akumulátorů jsou proměnné pevné délky podobné hashovacím funkcím. Jelikož akumulátory podporují zkrácené důkazy o členství a nečlenství pro jakýkoli element v dané sadě, akumulátor v podstatě reprezentuje celou sadu elementů jednou hodnotou, díky čemuž je tedy velikost nezávislá na počtu členů [9].

Hlavními bezpečnostními požadavky akumulátorů jsou jednosměrnost, nerozeznatelnost, odolnost proti kolizi a nepopiratelnost. První dva zmíněné požadavky souvisejí zejména s únikem informací svědků. Odolnost proti kolizi a nepopiratelnost pak mají svůj důvod u generování svědků. Tato technologie, kterou využívají v první řadě alternativní kryptoměny jako je Zcash, Zcoin nebo Monero, je navíc základním stavebním kamenem pro řadu dalších kryptografických primitiv, které se v blockchainu využívají. Jedná se například o již zmíněné prstenové podpisy či homomorfní závazky (*homomorphic commitments*). Akumulátory se rozdělují do třech základní skupin, kterými jsou akumulátory založené na RSA a hypereliptických křivkách, akumulátory založené na bilineárním zobrazení a akumulátory založené na hashovacích funkcích. Každá z těchto skupin nabízí kompromisy mezi parametry nastavení, velikostmi akumulátorů, výkonem svědků a důkazů a prostorem, přičemž akumulátory založené na RSA jsou pro využití v praxi pro svou efektivnost nejvhodnější [26].

2.4 Homomorfní závazky

Homomorfní závazky neboli *homomorphic commitments* jsou dalším užitečným bezpečnostním primitivem využívaným v technologii blockchainu u kryptoměn jako Zerocash nebo Monero, které využívá závazky založené na eliptických křivkách. Pedersen commitment a jeho další vektorové verze jsou pak běžně využívány k vytvoření

blockchainově orientovaného systému důkazů pod názvem Bulletproof. V rámci důkazů se závazky využívají ze dvou hlavních důvodů. Prvním z nich je umožnění dokazovateli účastnit se takzvaných „cut and choose“ důkazů, kde se ověřovateli představí pouze část toho, co se má naučit, přičemž dokazovatel odhalí pouze to, co se shoduje s výběrem ověřovatele. Schémata závazků umožňují dokazovateli specifikovat veškeré informace dopředu, a zveřejnit tak pouze to, co má být dále v důkazu zveřejněno. Závazky jsou dále využívány také u důkazů nulových znalostí, a to ověřovatelem, který ve většině případů určuje svůj výběr v závazku s časovým předstihem. Tím mohou být důkazy nulových znalostí zpracovávány souběžně bez toho, aniž by došlo k odhalení informací dokazovateli [34][26].

2.5 Důkazy nulových znalostí

Základní ideou jak ochránit soukromí a zajistit anonymitu transakcí v blockchainu je učinit jednotlivé transakce nepropojitelnými. Kryptografie je spojována s technologií blockchainu od jejího samotného vzniku a popularizace jako jedna z nejdůležitějších částí. Právě díky kryptografii je totiž možné blockchain využívat napříč mnoha odvětvími pro řadu různých aplikací. Za vznikem takzvaných ZKP[9)] blockchainů stojí neustálý vývoj nových kryptografikých protokolů a mechanismů, které jsou založeny na matematických rovnicích. V kryptoměnách se postupně vyvinuly dva hlavní přístupy, kterými jsou u neinteraktivních důkazů nulových znalostí (NIZKP) zk-SNARKs a takzvané Bulletproofs [25].

Důkazy nulových znalostí je technologie, která je mimo jiné využívána v blockchainu k ochraně soukromí, kdy je dokazovatel schopen zkušebně přesvědčit ověřovatele o konkrétní skutečnosti, aniž by došlo k úniku jakýchkoli citlivých informací. ZKP například umožňuje uživateli zjistit zůstatek na svém bankovním účtu bez toho, aby musel přistupovat k bankovním údajům či jakýmkoli jiným osobním údajům. Dosaženo takovýchto výsledků je zejména využitím tří základních vlastností důkazů nulových znalostí, které jsou následující [14].

1. První důležitou vlastností je takzvaná úplnost transakce. Znamená to, že pravdivost tvrzení přesvědčuje ověřovatele o skutečnosti, že dokazovatel disponuje požadovanými vstupy.

2. Druhým rysem zero-knowledge proofs je důkladnost. Znamená to, že nepoctivý dokazovatel nemůže ověřovatele přesvědčit o skutečnosti, že mají požadovaný vstup, když je jejich tvrzení nepravdivé.

[9)] zero-knowledge proof

3. Třetí a vůbec nejdůležitější vlastností důkazů nulových znalostí je samotná znalost. Primárním účelem vlastnosti nulových znalostí v systému ZKP je soukromí a ochrana využívaných informací. Bez ohledu na to, zda je tvrzení pravdivé nebo nepravdivé, se ověřovatel nesmí o těchto informacích nic dozvědět.

2.5.1 Výhody důkazů nulových znalostí

Díky absenci složitých kryptografických funkcí a metod je jednou z největších výhod využití důkazů nulových znalostí v technologii blockchainu jednoduchost. Zároveň ZKP nabízí mnohem lepší zabezpečení, a to především pokud jde o zabránění úniku jakéhokoli typu informací. Velkou výhodou je při práci se zero-knowledge proofs také zkracování délky transakcí v blockchainu. Na základě toho tudíž uživatelé nemusejí mít obavy o ukládání informací, kompatibilitu a identitu spojenou s různými typy aktiv. Důkazy nulových znalostí mohou navíc uživatelům poskytnout jedinečnou kombinaci soukromí a škálovatelnosti pro podporu univerzálního začlenění do blockchainu. Co se zajištění soukromí týče, nulové výhody ověřování znalostí mají vždy jednu z hlavních priorit [14].

2.5.2 Typy důkazů nulových znalostí

Důkazy nulových znalostí se nejčastěji rozdělují do dvou základních typů, a sice na interaktivní důkazy nulových znalostí a neinteraktivní důkazy nulových znalostí, přičemž první z typů se v kryptoměnách využívá mnohem častěji. U interaktivních ZKP je řada postupů založena na matematické pravděpodobnosti. Pokud jde o neinteraktivní důkazy nulových znalostí, jak již sám název napovídá, při svém fungování nevyužívají žádné interaktivní přístupy. Tím může dokazovatel vytvořit všechny výzvy najednou a ověřovatel na ně může odpovědět v pozdější části procesu. Pro zajištění bezpečnosti v kryptoměnách se využívají zejména dva typy, kterými jsou zk-SNARK a Bulletproofs, jež spadají právě do neinteraktivních ZKP [14].

zk-SNARK

Zero knowledge Succinct Non-Interactive Argument of Knowledge či zkráceně zk-SNARK začaly být poprvé využívány v kryptoměnách s nástupem Zerocoin a následně Zerocash, kde kompletně změnili způsob, jakým jsou data v rámci sítě sdílena. Využití zk-SNARK umožňuje transakcím zůstat po celou dobu zašifrované, a přitom je stále možné validovat a verifikovat jejich pravost a správnost. Kromě toho nabízí tyto důkazy uživatelům vyšší stupeň anonymity, soukromí, zabezpečení a důvěrnosti. Výraz „succinct“ neboli stručný v názvu metody navíc odkazuje na vlastnost těchto důkazů, díky nimž mohou být důkazy ověřeny během několika milisekund, přičemž je jejich délka jen několik stovek bajtů, a to i pro údaje o programech, které jsou velmi velké [5].

Nejefektivnějším známým způsobem, jak v dnešní době vytvořit důkaz nulových znalostí, který je neinteraktivní a krátký natolik, aby bylo možné jej publikovat v blockchainu, je prostřednictvím fáze nastavení, která generuje společný referenční řetězec sdílený mezi dokazovatelem a ověřovatelem. Tyto společné referenční řetězce jsou označovány jako veřejné parametry systému. V případě, že by se útočník dostal k tajné náhodnosti využívané ke generování těchto parametrů, byl by schopen vytvořit falešné důkazy, které by se ověřovateli jevily jako pravdivé. K odstranění tohoto rizika je u kryptoměn pro generování těchto parametrů využíváno výpočtů za účasti více účastníků, které se nazývají Multi-party Computation Ceremonies [46].

Bulletproofs

Druhým typem neinteraktivních ZKP využívaných při zabezpečení kryptoměn jako jsou Bitcoin nebo Monero jsou Bulletproofs. Česky by se tento druh důkazů mohl označovat jako „neprůstřelné důkazy“. Na rozdíl od svého předchůdce zk-SNARKs nevyžadují Bulletproofs žádnou fázi nastavování důvěry. Na druhou stranu jsou však mnohem náročnější pokud jde o spotřebovaný čas potřebný k ověření důkazu. Bulletproofs samozřejmě fungují na stejném principu jako ostatní důkazy nulových znalostí, kdy dochází k přesvědčení ověřovatele o správnosti tvrzení bez toho, aniž by došlo k odhalení jakýchkoli bližších informací.

Bulletproofs jsou navrženy tak, aby umožňovaly efektivní důvěryhodné transakce s bitcoiny a dalšími kryptoměnami. Důvěryhodné transakce skryjí částku, která je prostřednictvím transakce převedena. Každá takováto transakce obsahuje kryptografický důkaz o tom, že je platná. Bulletproofs navíc snižují velikost důkazů z více než 10 kB na méně než 1 kB [3].

2.6 Služby míchání mincí

V blockchainu dochází k propojení odesílatele a příjemce transakce, vinou čehož lze při použití analytického útoku získat osobní údaje některého ze zúčastněných uživatelů. Jednou z možností, jak pravděpodobnost ztráty citlivých dat snížit, je využití mixing services nebo česky služeb míchání mincí, jejichž význam poprvé představil v roce 1981 D.L. Chaum [6]. Tato technologie umožňuje uživateli kromě skrytí obsahu komunikace skrýt také to, s kým účastník komunikuje.

Předpokládejme, že jedna entita připraví zprávu M k doručení jiné entitě na adrese R. Ta musí nejprve zašifrovat zprávu veřejným klíčem příjemce K_R, připojit adresu R a poté výsledek zašifrovat veřejným klíčem zprostředkovatele K_I. Proces lze vyjádřit jako [34]:

$$K_I(r_0, K_R(r_1, M)R) \rightarrow K_R(r_1, M)R, kde \tag{2.9}$$

Levá strana výrazu označuje šifrovanou zprávu přenášenou prostředníkovi. Symbol $\rightarrow$ dále označuje transformaci šifrovaného textu prostředníkem do jiného šifrovacího textu zobrazeného na pravé straně výrazu. Tato transformace provede dešifrování původního šifrovaného textu zprostředkovatelem za využití jeho soukromého klíče. Takto zašifrovaná zpráva je dále poslána prostředníkem na adresu příjemce R, jenž ji dešifruje pomocí vlastního soukromého klíče. Proměnné r_0 a r_1 jsou náhodná čísla, která zajišťují, že žádná zpráva nebude přenesena více než jednou.

Když zprostředkovatel získá dostatek vstupů a výstupů, tento mechanismus skryje korespondenci mezi původem a cílem každé zprávy. Pořadí příchodů je skryto výstupem rovnoměrně velkých položek v náhodných vzorcích. Aby se navíc minimalizovalo nebezpečí toho, že útočníkem bude právě jediný prostředník, je několik prostředníků svázáno s cílem vytvořit vodopádové schéma propojení prostředníků pro větší zabezpečení [34].

V současné době využívané služby míchání mincí je možné rozdělit do dvou skupin, a sice na centralizované a decentralizované. Rozdíl mezi nimi je zejména v tom, zda je při procesu zabezpečení zapotřebí využít služby třetí strany. Oba způsoby jsou blíže popsány v následujících podkapitolách.

2.6.1 Centralizované služby míchání mincí

U centralizovaných mixing services je za generování transakce, která obsahuje vstupy a výstupy všech uživatelů, zodpovědná strana, jež se nazývá *mix server* nebo *mixing server*. Jednoduchým příkladem fungování centralizovaného mixingu je následující: Všichni uživatelé posílají Bitcoiny na mixing server, který je následně přeposílá příslušným příjemcům. Jako poplatek za zprostředkování však musí uživatel zaplatit část svých peněz právě mixing serveru. K zajištění anonymity je tento systém sice poměrně účinný, avšak čelí potenciální hrozbě, která se týká možné krádeže mincí. Uživatelé mohou totiž jen těžko zajistit autenticitu nedůvěryhodné centrální služby. Z toho důvodu není příliš praktické, aby se k míchání mincí využívaly právě centralizované servery [25].

Mixcoin a Blindcoin

Za účelem snížení pravděpodobnosti krádeže mincí vytvořil Joseph Bonneau společně se svým týmem službu Mixcoin, která je kompatibilní se systémem Bitcoinu. Tento systém zajišťuje anonymitu následujícím způsobem. V případě, že uživatel poslal Bitcoin do mixéru, obdržel od serveru podepsanou záruku, jenž sloužil jako závazek spravedlivé výměny. Jestliže by mixing server porušil protokol, mohl by odesílatel použít tuto záruku k oznámení nevhodného chování a tím snížení jeho reputace. Problém s krádeží mincí však technologie Mixcoinu řešila pouze tehdy, pokud server fungoval spolehlivě. Dalším nebezpečím byl fakt, že server věděl o transakčních vstupech a jejich odpovída-

jících výstupech, vinou čehož mohl mixing server velmi snadno narušit anonymitu [25].

Centralizované mixing services byli nadále rozvíjeny a optimalizovány za pomoci využití technologie slepých podpisů, což dalo vzniknout Blindcoinu. Jedná se o způsob digitálního podpisu, při kterém je zpráva před podepsáním „zaslepena“. Tento postup se obecně skládá ze tří hlavních kroků:

1. **Zaslepení** – zakrytí původní zprávy náhodným „zaslepujícím faktorem“.
2. **Podepsání** – podepsání zaslepené zprávy pomocí standardního podpisového algoritmu.
3. **Odstranění zaslepení** – odstranění „zaslepujícího faktoru“ za účelem platného podpisu dané zprávy.

Výsledný podpis lze veřejně ověřit, zatímco podepisující nikdy nebude znát spojení mezi zprávou a podpisem. Stejně jako v případě Mixcoin, tak u systému Blindcoinu byl primárním problémem krádež mincí. Obě technologie garantují pouze omezenou bezpečnost [27].

Dash

Prvním opravdovým pokusem poskytnout anonymitu u digitálních měn, byl v roce 2014 představený Dash. Hlavní část této technologie tvoří takzvaný *PrivateSend*, který slouží k odstranění všech jedinečných informací o uživatelích ze sítě blockchainu. Síť se v tomto případě na rozdíl od předchozích systémů skládá ze sady konkrétních uzlů nazývaných hlavní uzly (*master nodes*), a omezuje proces míchání tak, aby přijímal pouze určité hodnoty. Jako prevenci proti krádežím mincí a zvýšení nákladů při porušení protokolu bylo v rámci tohoto systému zavedena hlavním uzlům povinnost zaplatit tisíc mincí měny Dash jako zálohu, aby mohly poskytovat mixing services [25].

Coinswap

Problém s krádeží mincí však poprvé opravdu řešil až systém s názvem Coinswap, jenž pro míchání mincí skrz prostředníka využíval takzvané svěřenecké transakce (*escrow transactions*) a protokoly spravedlivé výměny. Transakce využívala dva svěřenecké protokoly, které zaručovaly, že příjemce obdržel finanční prostředky právě tehdy, když mixing server obdržel všechny finanční prostředky od plátce. Veškeré transakce navíc byly chráněny již zmíněným protokolem spravedlivé výměny. Jelikož se však zajištění bezpečnosti skládalo z několika cyklů spolupráce mezi klientem a prostředníkem, v praxi byl tento systém poměrně náročný na výpočetní výkon [25].

Tumblebit

Ani jeden z výše zmíněných systémů však nedokázal zcela splnit ať už podmínku spravedlivé platby, tak podporu úplné anonymity. Kromě toho jen některé řešily problém s únikem soukromí v případě útočníků v rámci sítě. Za účelem odstraněních těchto bezpečnostních hrozeb vznikl pod vedením Ethana Heilman hybridní systém Tumblebit, jenž spojuje algoritmus RSA s technikami spravedlivé platby k vybudování anonymní a bezpečné transakce založené na systému Bitcoinu prostřednictvím nedůvěryhodného prostředníka s názvem *tumble*. Platby v řetězci bitcoinu jsou v tomto případě nahrazeny řešením kryptografických „hádanek“ mimo řetězce, což znamenalo, že příjemci by měli mít namísto pouze konkrétního tajemství souvisejícího s jeho adresou, řešení dané hádanky. Aby byla zajištěna spravedlivost platby, došlo během jedné platby k vygenerování dvou svěřeneckých transakcí. RSA hádka byla vygenerována a řešena v době interakce mezi plátcem a prostředníkem pomocí protokolů spravedlivé výměny. Anonymita Tumblebitu tudíž zaručovala fakt, že nikdo nemohl odvodit propojitelnost transakcí. Ukázalo se však, že skrz prostředníka šlo velmi jednoduše odhalit identitu plátce. Tumblebit navíc nepodporoval ani skrytí platebních hodnot, ani obousměrný platební kanál, kvůli čemuž je v praxi poměrně málo využívaný [10].

2.6.2 Decentralizované služby míchání mincí

Jak již bylo zmíněno v předchozí části práce, centralizované služby míchání mincí spoléhají na důvěryhodnou či alespoň částečně důvěryhodnou třetí stranu, jež se stará o míchání sady transakcí několika uživatelů, které následně posílá na odpovídající adresy tak, aby útočník nemohl spojit vstupní a výstupní adresy transakce. Stejně jako většina centralizovaných systémů, tak i centralizované služby míchání mincí jsou velmi náchylné na riziko selhání jediné části systému, kterým je v jejich případě mixing sever. Na základě toho byly vytvořeny alternativní způsoby označované jako decentralizované služby míchání mincí, v nichž není uživatel nucen platit žádné poplatky [34].

CoinJoin

Prvním z decentralizovaných systémů k míchaní mincí vznikl v roce 2013 pod názvem CoinJoin a umožňoval svým uživatelům míchat své mince způsobem, který si sami určili namísto spoléhání se na službu třetí strany. Mezi skupinou plátců v rámci tohoto systému dochází k procesu vyjednávání, které určí, komu chtějí poslat danou platbu. Následně je vygenerována transakce obsahující obsahující všechny páry vstupů a výstupů a zkontrolovaná uživateli, zda je jejich cíl platby správný. Pokud došlo k ověření transakce všemi plátci, transakce je všemi společně podepsána a nakonec zveřejněna prostřednictvím blockchainu.

Hlavní výhodou na rozdíl od centralizovaných systémů je ten, že CoinJoin značně

redukuje riziko odhalení propojení transakcí a krádeže mincí. Tento systém má však stále několik problémů, mezi než patří zejména to, že uživatelé účastnící se míchání mincí mohou objevit některé informace o jiných klientech. Zranitelný je CoinJoin také před DoS[10)] útoky. V případě, že by byl totiž některý z účastníků mixingu nedostupný, celý proces míchání by mohl selhat [25].

CoinShuffle

CoinShuffle využívá k zajištění vnitřní anonymity systému skupinový komunikační protokol Dissent. V rámci tohoto systému všichni uživatelé takzvaného mixing setu provádí za pomoci veřejných klíčů ostatních uživatelů vnořené šifrování výstupů v předem určeném pořadí. List se zamíchaným pořadím výstupních adres je následně poslán všem účastníkům, kteří kontrolují, zda transakce obsahují jejich správnou cílovou adresu. V případě, že jsou cílové adresy korektní, dochází k podpisu transakce. Jakmile jsou shromážděny všechny podpisy, poslední transakce je zveřejněna v blockchainu. Podobně jako u systému CoinJoin, i CoinShuffle je zranitelný útokem odmítnutí služby neboli DoS [37].

CoinParty

Distribuovaný hybridní systém s názvem CoinParty se zakládá na technologii Secure Multi-Party Computation (SMC), jenž umožňuje skupině uživatelů společně vygenerovat sdílenou adresu, aniž by mohlo dojít k úniku jejich tajného vstupu. Nová adresa je v tomto případě nastavena jako adresa příjemce. Pro získání mince je pak zapotřebí dosáhnout prahové hodnoty (trashold) podpisu. Bezpečnost však může být u CoinParty zaručena pouze tehdy, pokud jsou více než dvě třetiny uživatelů poctivých, což ve většině případů nelze určit [48].

CoinShuffle++

Dalším protokolem pro míchání identit odesílatelů transakcí za účelem dosažení anonymní komunikace, který podporuje více odesílatelů najednou, je Dining Cryptographers network nebo zkráceně DC-net. Na tomto protokolu pro zajištění anonymity zprvu stavěl především systém DiceMixe. Následně však na myšlenkách tohoto systému za využití DC-net vznikl CoinShuffle++, který je kompatibilní s nejznámější kryptměnou Bitcoinem. Na rozdíl od svého předchůdce z části 2.6.2 snížila nová verze CoinShuffle využitím nových technologií spotřebu šířky pásma komunikace a zlepšila celkový výkon.

[10)] Denial of Service

2.7 Transakce mimo blockchain

Transakce mimo řetězec neboli off-chain transaction je stručně řečeno pohyb hodnoty mimo blockchain. Pro lepší pochopení tohoto typu transakce je vhodné jejich srovnání s běžnými on-chain transakcemi nazývanými jen transakce. Jak již bylo zmíněno v předchozích kapitolách této práce, transakce v blockchainu je považována za validní v případě, že je blockchain upraven a zobrazuje danou transakci ve své účetní knize. Během celého procesu dochází k ověření transakce určitým počtem uživatelů, zaznamenání transakce do vhodného bloku a přenosu potřebných informací do celé sítě, což danou transakci činí nevratnou. Naproti tomu, v případě transakcí mimo řetězec dochází k přenosu hodnoty mimo blockchain, a může tak být učiněno hned několika způsoby [21]:

1. Dohoda o převodu mezi stranami provádějící transakci.
2. Zahrnutí třetí strany, která zaručuje, že bude transakce dodržena.
3. Využití platebního mechanismu založeného na kupónech, kdy si účastník zakoupí kupóny výměnou za kryptoměnu. Tento kupón pak pošle příjemci, který jej následně může uplatnit v dané kryptoměně či kryptoměně jiné v závislosti na poskytovateli.

Hlavní výhodou transakcí mimo řetězec je to, že mohou být prováděny okamžitě. Oproti tomu klasické transakce mohou mít dlouhou prodlevu v závislosti na vytížení sítě a počtu transakcí, jež čekají na potvrzení ve frontě. Off-chain transakce navíc obvykle nejsou zatíženy žádným transakčním poplatkem. Jelikož k ověření transakce není v tomto případě vyžadován žádný těžař ani jiný člen sítě a neplatí se žádný poplatek, je tento způsob atraktivní pro uživatele, kteří chtějí poslat větší množství peněz. Třetí a jednou z největších výhod transakcí mimo řetězec je větší bezpečnost a anonymita, kdy informace nejsou posílány veřejně. V případě on-chain transakcí je možné částečně určit identitu účastníka [21]. O odstranění těchto problémů se však pokoušejí bezpečnostní primitiva popsána v předchozích částech této práce.

2.7.1 Zabezpečení

Platební kanál umožňuje v rámci off-chain transakce plátci a příjemci uzavřít platební smlouvu skrze online transakci, která dočasně uschová finanční prostředky. Následně mohou obě strany sledovat prostředky, jež si vzájemně dluží a podle toho se dohodnout na novém rozdělení zůstatku. Platební kanál se tedy vyhne záznamu o platebních údajích, které by jinak byly uloženy v blockchainu.

Průkopníkem zabezpečení transakcí mimo řetězec byl v roce 2014 Heilman se svým týmem, podle jehož přístupu musí uživatel, který chce provést platbu, nejprve vytvořit platební cestu. Slabinou tohoto systému však je to, že všichni uživatele, kteří jsou zahnuti do platební cesty mohou získat jakékoli informace jak o plátci, tak o příjemci. Hailmanův návrh navíc nikdy nebyl kompatibilní s nejvíce rozšířenou kryptoměnou Bitcoinem, čímž dostali přednost dva nové návrhy Bolt a Tumblebit, jehož fungování bylo popsáno již v části 2.6.1.

Pokud jde o anonymní platební kanál s názvem Bolt, tato technologie, kterou využívají kryptoměny založené na systému Bitcoinu jako například Zerocash, nabízí tři módy plateb mimo řetězec. Jedná se o jednosměrný platební kanál *(unidirectional payment channel*), obousměrný platební kanál (*bidirectional payment channel*) a kanál nepřímých plateb (*indirect payment channel*). Bolt umožňuje plátci vytvořit anonymní přímý platební kanál, aniž by příjemce musel znát identitu plátce. Přenosový kanál využívá k poskytnutí anonymity technologii slepých podpisů společně s důkazy nulových znalostí, díky čemuž znemožňuje třetí straně získat informace o transakcích daného uživatele. Celková bezpečnost této technologie však závisí na kryptoměně, na které je Bolt postaven [25].

2.8 Chytré smlouvy

Chytrou smlouvou (*smart contract*) je označován protokol nebo software zajišťující podmínky dohody mezi prodávajícím a kupujícím. Tato technologie umožňuje provádět důvěryhodné transakce a dohody mezi anonymními stranami bez toho, aniž by byla vyžadována přítomnost ústředního orgánu, právního systému či jiného externího mechanismu vymáhání. Prakticky se jedná o řádky zdrojového kódu, které jsou automaticky prováděny v případě, že jsou splněny předem domluvené podmínky [16]. Jakožto decentralizovaný program pracující na blockchainu, rozšiřuje chytrý kontrakt jeho funkce nad rámec kryptoměny a dědí některé nežádoucí vlastnosti blockchainu. Jelikož je proces zpracování kontraktu transparentní a následně je trvale zaznamenán v blockchainu, chytré kontrakty čelí mnoha závažným bezpečnostním rizikům především co se oblasti soukromí uživatelů týče [7]. Za účelem zajištění bezpečnosti bylo vytvořeno hned několik platforem, mezi něž patří například Hawk nebo ShadowEth, které jsou popsány v následující části.

Hawk

Platforma Hawk pro zachování soukromí poskytuje vývojářům snadný způsob jak vytvořit chytrý kontrakt bez použití šifrování kódu či obfuskátoru, který slouží k zatemnění zdrojového kódu tak, aby byla jeho čitelnost pro člověka co možná nejsložitější.

Hawk rozděluje chytré kontrakty na dvě části, a sice na část soukromou a část veřejnou. Soukromá část smlouvy je odpovědná za skrytá data a funkce obsažené ve smlouvě. Oproti tomu veřejná část zodpovídá za veřejné kódy, jenž jsou přístupné veřejným subjektům.

Hlavní část technologie tvoří speciální modul nazývaný manažer, který je založen na sadě instrukcí Software Guard Extensions od firmy Intel. SGX[11)] slouží k poskytnutí větší bezpečnosti aplikačního kódu a dat, které chrání před zveřejněním nebo úpravami. Kvůli důvěrnosti dat SGX může manažer během provádění kontraktu získat soukromé informace a kompletní posloupnost transakčních postupů. Jelikož je manažer v případě přerušení činnosti protokolu finančně potrestán, je v jeho vlastním zájmu nezveřejnit získané informace. K zajištění správnosti převodu finančních prostředků a plnění podmínek kontraktu využívá systém Hawk důkazy zk-SNAKR, což vede k poměrně vysoké výpočetní náročnosti [23].

ShadowEth

Řešení bezpečnosti pomocí kryptografických funkcí velmi často vede k výraznému snížení výpočetního výkonu systému. Jen málo z těchto funkcí lze z toho důvodu využít v rámci architektury blockchainu nevyžadujícího povolení. K odstranění tohoto problému tedy některé kryptoměny využívají namísto kryptografických funkcí k ochraně soukromí zabezpečený hardware. Co se týče Etherea, ten využívá pro svou bezpečnost chytrých kontraktů platformu ShadowEth, která je založena na Trusted Execution Environment. TEE[12)] je prostředí pro vykonání kódu, v jehož okolí mohou mít ti, kteří daný kód spouštějí, vysokou úroveň důvěryhodnosti, protože mohou ignorovat hrozby ze zbytku zařízení [43]. To umožňuje uživatelům vytvářet smlouvy, které jsou prováděny v TEE a všechna metadata jsou uložena mimo blockchain v systému zvaném TEE-DS [38].

Ekiden

Stejně jako ShadowEth, tak i Ekiden využívá pro zajištění soukromí zabezpečený hardware. Na rozdíl od předchozího přístupu však disponuje větší efektivitou, čímž nabízí vyšší výkon než ShadowEth. Ekiden je vůbec prvním systémem zajišťující soukromí u chytrých kontraktů při zpracování až tisíce transakcí za vteřinu. Systém Ekiden lze kromě blockchainu vyžadujícího oprávnění využít také v blockchainu bez potvrzení. Jelikož je výpočet uzlů prováděn mimo řetězec v TEE, nedochází tedy k velkému zpoždění a velké výpočetní náročnosti, jako je k tomu u ShadowEth. Proces ověření kryp-

[11)] Software Guard Extensions
[12)] Trusted Execution Environment

tografickými funkcemi je u této technologie nahrazen vzdáleným ověřováním. Ochrana soukromí v Ekidenu závisí na zabezpečení důvěryhodného hardwaru, jenž je rovněž postaven na prostředí Trusted Execution Environment a sadě instrukcí sadě instrukcí Software Guard Extensions od Intel [7].

Arbitrum

Předejít slabinám předchozích návrhů se Arbitrum snaží prostřednictvím virtuálního stroje, jenž implementuje funkčnost smlouvy a zároveň slouží k ochraně soukromí. Tento systém mimo jiné využívá takzvaný motivační mechanismus, který stimuluje uživatele k tomu, aby se na podmínkách chování VM[13)] dohodli mimo řetězec. U Arbitrea mohou ověřovatelé efektivně ověřovat transakce, aniž by odhalili jakýkoli interní stav virtuálního počítače. Vyjednávání o chování smlouvy navíc může probíhat zkoumáním pouze jedné instrukce pro každý jeden kontrakt. Tím se využitím tohoto systému výrazně zlepšuje soukromí uživatelů a škálovatelnost [19].

[13)] Virtual Machine

II. PRAKTICKÁ ČÁST

3 Využité metody

Pro jednotlivé analýzy byly využity primárně dvě metody, jejichž fungování a postupy jsou krátce popsány v této kapitole. K analýze rizik, a tím posouzení zabezpečení celé technologie kryptoměn byla využita analýza SWOT. Pro srovnání jednotlivých aspektů, ať už z hlediska anonymity, či celkové bezpečnosti, posloužila vícekriteriální metoda s názvem TOPSIS.

3.1 SWOT

Tato podkapitola je zaměřena na první z využitých metod pro analýzu rizik, a sice SWOT analýzu, která patří mezi strategické metody. Základním stavebním kamenem SWOT analýzy je matice SWOT, která tvoří končepcní rámec pro systematickou analýzu a usnadňuje tím porovnání vnějších hrozeb a příležitostí s vnitřními silnými a slabými stránkami daného aspektu. Jak již samotný název analýzy napovídá, předmětem této metody jsou následující pojmy [12]:

- **Silné stránky (S – strenghts)** — Přednosti a výhody daného objektu. V případě bezpečnosti kryptoměn vycházejí silné stránky z vlastností blockchainu a kryptografických funkcí.
- **Slabé stránky (W – weakness)** — Jedná se o věci, které daný objekt degradují. Hlavní snahou by mělo být slabé stránky odstraňovat nebo případně alespoň zmírňovat. U kryptoměn to může být například složitost technologie blockchainu či velikost sítě.
- **Příležitosti (O – opportunities)** — Pro co nejlepší úspěch produktu, zvýšení konkurenceschopnosti nebo v našem případě zabezpečení systému a zajištění anonymity uživatel, je zapotřebí využít příležitostí a šancí.
- **Hrozby (T – threats)** — Jedná se o faktory, které mohou s určitou pravděpodobností nastat a mít na objekt negativní vliv. Mezi hrozby mohou patřit zranitelnost digitálních podpisů či kybernetické útoky jakéhokoli druhu.

U analýzy rizik prostřednictvím metody SWOT je důležité stanovit váhy jednotlivých aspektů čili to, jak velkou roli v systému, ať už v dobrém slova smyslu, nebo v tom špatném, hrají. Stanovením vah dochází k normalizaci SWOT matice, kde může být v každém z kvadrantů jiný počet atributů, což by samozřejmě ovlivnilo konečné hodnocení rizika. Pro potřeby hodnocení rizik je navíc nutné stanovit hodnotu rizika. Vynásobením váhy a hodnoty rizika dostaneme celkový výsledek pro daný atribut. Součtem těchto výsledků v kvadrantech je získáno jednotlivé hodnocení, ať už silných či slabých

stránek, příležitostí a hrozeb. Výsledná hodnota velikosti rizika je pak dána vzorcem:

$$S \ + O \ - W - T = R, kde \tag{3.1}$$

- S je hodnocení silných stránek
- O je hodnocení příležitostí
- W je hodnocení slabých stránek
- T je hodnocení hrozeb
- R je celková míra rizika

3.2 TOPSIS

Metoda TOPSIS neboli *Technique for Order of Preference by Similarity to Ideal Solution* je vícekriteriální metoda, která je založena na srovnávání různých aspektů podle předem specifikovaných kritérií. Jednotlivé varianty jsou posuzovány na základě jejich vzdálenosti od ideální a bazální, tedy nejlepší a nejhorší možné varianty. Jednotlivým kritériím je zapotřebí přiřadit váhy, podle kterých jsou následně hodnoceny.

Klíčovými kroky TOPSIS metody jsou: převod všech kritérií na maximalizační, tvorba normalizované matice $R = (r_{ij})$ a tvorba vážené normalizované matice $Z = (z_{ij})$ podle následujících vztahů [18]:

$$r_{ij} = \frac{y_{ij}}{\sqrt{\sum_{i=1}^{m} y_{ij}^2}}; \quad i = 1, 2, ..., m; \quad j = 1, 2, ..., n \tag{3.2}$$

$$z_{ij} = v_j \times r_{ij}, kde \tag{3.3}$$

- v_j je váha j-tého kritéria

Dle vážené normalizované matice jsou dále určeny pro každé z kritérií ideální varianta $A(a_1, ..., a_n)$ a bazální varianta $B(b_1, ..., b_n)$. Ty jsou v dalším kroku využity pro výpočet vzdálenosti jednotlivých variant právě od ideální varianty d_i^+ a následně od bazální varianty d_i^- podle následujících vztahů:

$$d_i^+ = \sqrt{\sum_{j=1}^{n} (z_{ij} - a_j)^2} \tag{3.4}$$

$$d_i^- = \sqrt{\sum_{j=1}^{n}(z_{ij} - b_j)^2} \tag{3.5}$$

Výsledný ukazatel relativní vzdálenosti od bazální varianty c_i, podle které jsou jednotlivé aspekty posuzovány, je dán vztahem:

$$c_i^- = \frac{d_i^-}{d_i^+ + d_i^-} \tag{3.6}$$

Na závěr analýzy je vhodné provést seřazení porovnávaných aspektů dle výsledné hodnoty c_i. Pro ukazatel relativní vzdálenosti od bazální varianty navíc platí, že:

$$c_i \in < 0; 1 >, kde \tag{3.7}$$

1 označuje nejlepší možnou variantu a 0 naopak tu nejhorší. Obecně je tedy dáno, že čím více se blíží hodnota c_i číslu 1, tím lepší varianta je. Následným seřazením hodnot ukazatelů relativní vzdálenosti od bazální varianty pro jednotlivé metody dostaneme přesné pořadí aspektů od nejvýhodnějších po ty nejméně výhodné.

4 Stanovení kritérií a srovnání metod bezpečnostních aspektů

Pro analýzu zabezpečení kryptoměn, ať už z pohledu anonymity uživatele, či samotných transakcí je nejprve zapotřebí srovnat jednotlivé aspekty této technologie jako jsou kryptografické podpisy, služby míchání mincí, chytré kontrakty nebo konsensuální metody používané v blockchainu. Srovnání jednotlivých aspektů kryptoměn sloužících pro zabezpečení vychází z teoretické části této práce. Pro potřeby komparace je však zapotřebí stanovit určitá kritéria hodnocení, od kterých se bude následná analýza odvíjet.

1. **Ochrana soukromí** – Toto kritérium odkazuje na zachování anonymity uživatelů. Pokud jde o anonymitu, ta může být rozdělena na takzvanou externí anonymitu, kdy jsou jednotlivé údaje a citlivé informace chráněny před okolním světem. Druhou kategorií je interní anonymita, která zajišťuje ochranu soukromí uživatele v blockchainové síti.

2. **Ochrana proti krádeži mincí** – U služeb míchání mincí je během provádění anonymních operací zapotřebí chránit transakce a prostředky uživatelů účastnících se platby. Velká většina mixing service je tedy vystavena hrozbě ztráty mincí v průběhu transakcí. Stupeň ochrany před ztrátou mincí se liší podle typu využitého protokolu a daného systému.

3. **Potřeba centrální autority** – Také toto kritérium se týká výhradně atributu služeb míchání mincí. V případě, že je v systému využívána centrální autorita, může docházet k bezpečnostním problémům. Z toho důvodu bylo vytvořeno hned několik přístupů, které se využívání centrální autority vyhýbají, a poskytují tak mnohem lepší zabezpečení.

4. **Potřeba poplatku za služby míchání mincí** – Poplatky za míchání mincí sice primárně nevedou k bezpečnostním problémům, ať už v transakcích, nebo zajištění anonymity. Rozhodně však mohou ovlivnit uživatelskou přívětivost, a podepsat se tak na celkové nedůvěře v danou funkci.

5. **Sada anonymity** – Jedná se o sadu entit, jež mohou mít disponovat stejnými atributy, díky čemuž jsou z pohledu útočníka navzájem nerozeznatelné. Sada anonymity slouží k určení stupně anonymity, který se liší podle použité metody.

6. **Potřeba důvěryhodného nastavení** – U kryptografických metod pro zajištění soukromí uživatelů, jako jsou například důkazy nulových znalostí, může být vyžadován proces takzvaného důvěryhodného nastavení, jehož bezpečnost lze zajistit buďto důvěryhodným prostředím či technikami výpočtu více stran. V případě,

že by došlo k ohrožení důvěryhodného nastavení, a tím i parametrů důkazů, zabezpečení systému zajišťující ochranu soukromí v blockchainu by zcela selhalo.

7. **Velikost transakce** – Toto kritérium označuje průměrnou velikost každé transakce v blockchainu. Obecně platí, že čím větší je velikost transakce, tím nižší je výkon blockchainu. Použití složitých kryptografických metod může způsobit zvýšení robustnosti transakce a tím i nemožnost využití dalších způsobů ochrany. Základní myšlenkou je tedy najít optimální rovnováhu mezi zajištěním bezpečnosti, potažmo soukromí a výkonu.

8. **Čas transakce** – Dlouhý čas generování klíče u digitálních podpisů nebo při validaci a verifikaci transakce může zvýšit výpočetní režii, a snížit tedy bezpečnost systému.

9. **Směr kanálu** – U metod používaných k ochraně transakcí mimo blockchain se vyskytují dva přístupy přenosu zpráv mezi plátce a příjemcem. Platby mohou být mezi jednotlivými stranami posílány buďto skrz jednosměrný kanál nebo současně prostřednictvím obousměrného.

10. **Strany uskutečňující chytrou smlouvu** – Také toto kritérium se týká výhradně ochrany soukromí mimo blockchain, kdy záleží na využité metodě, která se může v závislosti na architektuře lišit v počtu a typu stran uskutečňujících dohodu v rámci chytré smlouvy. Čím více stran se bude kontraktu účastnit, tím větší bude výpočetní režie systému. Díky tomu vznikne malé riziko jediného bodu selhání a zvýší se tím stabilita celého systému.

Služby míchání mincí

U služeb míchání mincí neboli mixing services je zapotřebí podrobně srovnat dle výše zmíněných kritérií jednotlivé metody využívané v kryptoměnách, které byly popsány v teoretické části této práce v podkapitole 2.6. Co se zachování soukromí uživatelů týče, nejdůležitějším kritériem u mixing service je ochrana soukromí, která se dělí na interní a externí. Ochranu proti krádeži mincí sice zajišťují všechny z vybraných metod, avšak pro Mixcoin, Blindcoin, Dash a CoinParty platí, že tyto metody chrání před ztrátou peněz pouze za určitých podmínek. Modernější a efektivnější metody jako CoinJoin či CoinShuffle navíc při své funkci nevyžadují od uživatele poplatek za míchání, což je bezesporu velkou výhodou. Právě metoda CoinShuffle a její vylepšená verze CoinShuffle++ vyšly ze srovnání, které je patrné v tabulce 4.1, nejlépe, když zajišťují jak externí, tak interní anonymitu, chrání proti krádeži mincí a nevyžadují přítomnost centrální autority ani poplatku za mixing.

	Ochrana soukromí	Ochrana proti krádeži mincí	Potřeba CA	Potřeba poplatku za mixing
Mixcoin	Externí anonymita	Částečně	Ano	Ano
Blindcoin	Externí a interní anonymita	Částečně	Ano	Ano
Dash	Externí anonymita	Částečně	Ano	Ano
Coinswap	Externí anonymita	Ano	Ano	Ano
Tumblebit	Externí a interní anonymita	Ano	Ano	Ano
CoinJoin	Externí anonymita	Ano	Ne	Ne
CoinShuffle	Externí a interní anonymita	Ano	Ne	Ne
CoinParty	Externí a interní anonymita	Ano v případě, že je 2/3 uzlů poctivých	Ne	Ne
CoinShuffle++	Externí a interní anonymita	Ano	Ne	Ne

Tabulka 4.1 Srovnání míchacích služeb z hlediska bezpečnosti [25]

Důkazy nulových znalostí

Důkazy nulových znalostí zatím nejsou u většiny kryptoměn příliš hojně využívány, avšak v budoucnu by právě tento způsob zajištění anonymity mohl hrát velmi významnou roli. Pokud jde o metody používané u DNZ, Zerocoin, její nadstavba Enhanced Zerocoin a Zerocash využívají pro zajištění anonymity, soukromí a důvěrnosti transakcí typ důkazů zk-SNARKs. Jak je patrné z tabulky 4.2, všechny tři metody nabízejí za účelem ochrany soukromí skrytí hodnoty transakce a adres uživatelů. Stejně tak disponují velkou sadou anonymity. Rozdíl je však patrný v absenci fáze nastavování důvěry. Oproti Zerocoin a Zerocash totiž Enhanced Zerocoin nevyžaduje právě přítomnost důvěryhodného nastavení, čímž je z variant zk-SNARKs nejvhodnější. Stejně tak je tomu v případě Bulletproofs, které pro své zabezpečení využívají Bitcoin nebo Ethereum. Jejich výhodou je však oproti EZC menší velikost transakce. Obecně však platí, že Bulletproofs vyžadují pro ověření mnohem více času, než je tomu u zk-SNARKs.

Metoda	Ochrana soukromí	Sada anonymity	Potřeba DN	Velikost transakce	Čas
Zerocoin	Skrytí hodnoty transakce a adresy účastníků	Velká	Ano	Velká	Malý
Enhanced Zerocoin	Skrytí hodnoty transakce a adresy účastníků	Velká	Ne	Velká	Střední
Zerocash	Skrytí hodnoty transakce a adresy účastníků	Velká	Ano	Střední	Malý
Bulletproofs	Skrytí hodnoty transakce a adresy účastníků	Velká	Ne	Malá	Velký

Tabulka 4.2 Srovnání metod důkazů nulových znalostí z hlediska bezpečnosti [25]

Zabezpečení transakcí mimo blockchain

Transakce mimo blockchain nabízejí oproti klasickým transakcím řadu výhod. Kromě okamžitého zpracování je to však hlavně větší bezpečnost a anonymita, kdy nejsou informace o platbě ani účastnících posílány veřejně. U off-chain transakcí jsou z pohledu ochrany soukromí a směru přenosu skrz kanál srovnány dvě nejznámější metody Bolt a Tumblebit. Obě z těchto variant zajišťují jak externí, tak interní anonymitu, tedy chrání data jak u samotné technologie, tak před okolními hrozbami. Jak je však zaznamenáno v tabulce 4.3, výhodnější je využití metody Bolt, kde se sice bezpečnost osobních údajů odvíjí od dané kryptoměny, avšak metoda Tumblebit vůbec neumožňuje skrytí hodnoty platby.

Metoda	Ochrana soukromí	Směr kanálu	Nevýhody
Bolt	Interní a externí anonymita	Jednosměrný nebo obousměrný	Ochrana osobních údajů závisí na dané kryptoměně
Tumblebit	Interní a externí anonymita	Obousměrný	Neumožňuje skrytí hodnoty platby

Tabulka 4.3 Srovnání metod pro zabezpečení transakcí mimo blockchain [25]

Zabezpečení chytrých smluv

Se systémem kryptoměn souvisí taktéž chytré smlouvy, které jsou podrobněji popsány v podkapitole 2.8. Jednotlivé metody jsou srovnány především z hlediska ochrany soukromí, kdy úplně všechny umožňují skrytí stavu smlouvy před uživateli, kteří se neúčastní daného kontraktu. Ekiden a ShadowEth však navíc umějí skrýt také vstupní hodnoty transakce, čímž zajišťují ještě více bezpečnosti, než je tomu v případě Arbitrum. Nejspolehlivější ze všech využívaných metod zabezpečení chytrých kontraktů je však metoda s názvem Hawk, která navíc poskytuje skrytí identity účastníků a hodnoty dané transakce. Slabou stránkou je ale malý počet stran uskutečňujících chytrou

smlouvu. Jak totiž bylo zmíněno při stanovení kritérií pro srovnání jednotlivých metod, čím více stran se bude kontraktu účastnit, tím menší je riziko jediného bodu selhání.

Metoda	Ochrana soukromí	Strany uskutečňující ChS
Hawk	Skrytí hodnoty transakce, identity účastníků, vstupních hodnot a stavu kontraktu	Jediný SGX manager
ShadowEth	Skrytí vstupních hodnot a stavu kontraktu před uživateli, kteří se neúčastní kontraktu	Více SGX pracovních uzlů
Ekiden	Skrytí vstupních hodnot a stavu kontraktu před uživateli, kteří se neúčastní kontraktu	Více SGX výpočetních uzlů
Arbitrum	Skrytí stavu kontraktu před uživateli, kteří se neúčastní kontraktu	Více uzlů běžících na VM

Tabulka 4.4 Srovnání metod pro zabezpečení chytrých smluv [25]

Digitální podpisy

Standardem pro vytváření digitálních podpisů v kryptoměnách je ECDSA, případně jeho vylepšená verze EdDSA. Pro poskytnutí lepší ochrany však některé systémy využívají také pokročilejší metody podpisů jako jsou prstenové podpisy nebo multi-signatures, které byly popsány v podkapitole 2.2. Právě tyto podpisy tedy budou sloužit pro srovnání a určení, který z nich se pro zabezpečení anonymity účastníků a transakcí hodí nejvíce. Pro srovnání, které je patrné v tabulce 4.5, byly využity kritéria ochrana soukromí, sada anonymity, potřeba důvěryhodného nastavení a velikost transakce.

	Ochrana soukromí	Sada anonymity	Potřeba DN	Velikost transakce
Ring Signature	Skrytí adresy účastníků a hodnoty transakce	Malá	Ne	Malá
One-Time Signature	Skrytí adresy účastníků	Malá	Ano	Malá
Multi-signature	Skrytí adresy účastníků a hodnoty transakce	Velká	Ne	Střední

Tabulka 4.5 Srovnání digitálních podpisů z hlediska bezpečnosti

Homomorfní závazky a akumulátory

Homomorfní závazky a akumulátory spolu velmi úzce souvisí. Pokud bychom se podívali na průřez kryptoměnami, které využívají pro zabezpečení homomorfní závazky, hned čtyři ze sedmi vybraných v tabulce 4.6 využívají také služeb akumulátorů.

	Zcash	Zcoin	Monero	BitConnect	Bytecoin	Komodo	Electroneum
Akumulátory	✓	✓		✓		✓	
Homomorfní závazky	✓	✓	✓	✓	✓	✓	✓

Tabulka 4.6 Využití akumulátorů a homomorfních závazků v kryptoměnách

Jak již bylo zmíněno, oba tyto aspekty na sobě často souvisí, a jak je vidět z jejich srovnání, navzájem se poměrně spolehlivě doplňují. Jak ukazuje tabulka 4.7, akumulátory v rámci zabezpečení slouží ke skrytí identity účastníků, avšak nechrání proti krádež mincí. Naopak homomorfní závazky, na jejichž principu pracují i důkazy nulových znalostí, umožňují skrytí hodnoty transakce, a chrání tak před krádeží mincí.

	Ochrana soukromí	Ochrana proti krádeži mincí	Sada anonymity
Akumulátory	Skrytí identity účastníků	Ne	Velká
Homomorfní závazky	Skrytí hodnoty transakce	Ano	Velká

Tabulka 4.7 Srovnání akumulátorů a homomorfních závazků

5 Analýza zabezpečení kryptoměn z pohledu anonymity

K analýze zabezpečení kryptoměn z pohledu anonymity je využita multikriteriální metoda TOPSIS, která stanovuje ideální řešení pro danou problematiku. Před samotným provedením analýzy je nejprve zapotřebí definovat kritéria, podle nichž se budou jednotlivé aspekty zabezpečení kryptoměn hodnotit. Slovní hodnocení daných aspektů a metod je následně prostřednictvím vybrané bodové škály převedeno na bodové hodnocení. Pro korektní a relevantní výsledky je také zapotřebí přiřadit jednotlivým kritériím váhy podle jejich důležitosti na zachování soukromí a anonymity.

Následnou analýzou jsou poté získány hodnoty, podle nichž jsme schopni určit pořadí daných aspektů a jejich významnost pro zajištění anonymity a soukromí uživatel. Tyto výsledky jsou následně porovnány s reálnými daty, které ukazují, jakou kombinaci bezpečnostních aspektů dané kryptoměny využívají.

5.1 Definování kritérií

Kritéria pro analýzu byla stanovena v předchozí části práce 4 a jejich označení pro analýzu jsou následující:

- K_1 – Ochrana soukromí
- K_2 – Ochrana proti krádeži mincí
- K_3 – Potřeba centrální autority
- K_4 – Potřeba poplatku za služby míchání mincí
- K_5 – Sada anonymity
- K_6 – Potřeba důvěryhodného nastavení
- K_7 – Velikost transakce
- K_8 – Čas transakce
- K_9 – Směr kanálu
- K_{10} – Strany uskutečňující chytrou smlouvu

5.2 Bodové hodnocení

Jelikož nejde každé kritérium ze srovnávaných metod hodnotit na stejné škále hodnot, byly vytvořeny následující stupnice, které jsou během analýzy využívány. V tabulce 5.1 je zaznamenán převod slovního hodnocení, dle srovnání metod v podkapitole 4, na bodové hodnocení využívané metodou TOPSIS.

Slovní hodnocení	Body	Slovní hodnocení	Body	Slovní hodnocení	Body
Velmi málo	1	Ne	1	Malá	1
Podprůměrně	2	Ano	2	Střední	2
Průměrně	3	-	-	Velká	3
Nadprůměrně	4	-	-	-	-
Velmi dobře	5	-	-	-	-

Tabulka 5.1 Bodová stupnice pro hodnocení jednotlivých aspektů bezpečnosti

5.3 Stanovení vah

Váhy pro následnou analýzu byly stanoveny především s ohledem na zajištění anonymity uživatelů. Z toho důvodu byla jako nejdůležitější shledána kritéria ochrana soukromí a sada anonymity. Přiřazení vah k daným kritériím bezpečnosti je zachyceno v tabulce 5.2.

Pořadí	Kritérium	Váha
1	Ochrana soukromí (K1)	0,225
2	Sada anonymity (K5)	0,175
3	Ochrana proti krádeži mincí (K2)	0,15
4	Potřeba důvěryhodného nastavení (K6)	0,1
5	Potřeba centrální autority (K3)	0,1
6	Strany uskutečňující chytrou smlouvu (K10)	0,075
7	Směr kanálu (K9)	0,05
8	Velikost transakce (K7)	0,05
9	Čas transakce (K8)	0,05
10	Potřeba poplatku za mixing (K4)	0,025

Tabulka 5.2 Stanovení pořadí a vah kritérií pro analýzu zabezpečení z pohledu anonymity

5.4 Výběr nejvhodnějších metod

Jelikož bylo u řady bezpečnostních aspektů kryptoměn definováno hned několik metod, ze všeho nejdříve je důležité posoudit, která z metod je pro zajištění anonymity u daného aspektu nejvhodnější. V následující části se tedy zaměříme na posouzení metod digitálních podpisů, služeb míchání mincí, důkazů nulových znalostí a chytrých smluv. U aspektů, kde není na výběr mezi více metodami, budou pouze stanoveny vstupní hodnoty pro následnou kompletní analýzu.

1. Digitální podpisy

U digitálních podpisů byla analyzována trojice metod podle čtyř stanovených kritérií, kde nejdůležitějším je ochrana soukromí, pro kterou byla využita pětibodová stupnice. Druhým důležitým kritériem byla sada anonymity, kde je větší sada anonymity hodnocena vyšším stupněm. Naopak u potřeby důvěryhodného nastavení, je žádoucí odpověď „ne“. Pokud totiž dojde k selhání důvěryhodného nastavení, může dojít k selhání celého systému.

Metoda	Ochrana soukromí	Sada anonymity	Není potřeba DN	Velikost transakce
Ring Signature	5	1	2	3
One-Time Signature	3	1	1	3
Multi-signature	5	3	2	2
Váhy	**0,45**	**0,35**	**0,2**	**0,1**

Tabulka 5.3 Vstupní hodnoty pro analýzu anonymity digitálních podpisů

Metoda	Ochrana soukromí	Sada anonymity	Není potřeba DN	Velikost transakce
Ring Signature	0,651	0,301	0,667	0,64
One-Time Signature	0,391	0,301	0,333	0,64
Multi-signature	0,651	0,904	0,667	0,426
Váhy	**0,45**	**0,35**	**0,2**	**0,1**

Tabulka 5.4 Normalizovaná matice pro analýzu anonymity digitálních podpisů

Metoda	Ochrana soukromí	Sada anonymity	Není potřeba DN	Velikost transakce	Si+	Si-	(Si+) + (Si-)
RS	0,29295	0,10535	0,1334	0,064	**0,21213**	**0,1347**	**0,34683**
OTS	0,17595	0,10535	0,0666	0,064	**0,2513**	**0**	**0,2513**
MS	0,29295	0,3164	0,1334	0,0426	**0**	**0,2513**	**0,2513**
Váhy	**0,45**	**0,35**	**0,2**	**0,1**			
Ideální	**0,29295**	**0,3164**	**0,1334**	**0,0426**			
Bazální	**0,17595**	**0,10535**	**0,0666**	**0,064**			

Tabulka 5.5 Vážená kriteriální matice pro analýzu anonymity digitálních podpisů

Metoda	Skóre	Pořadí
Ring Signature	0,38837	2
One-Time Signature	0	3
Multi-signature	1	1

Tabulka 5.6 Výsledky analýzy digitálních podpisů z hlediska anonymity

Jak je patrné z výsledků zaznamenaných v tabulce 5.6, nejužitečnějším digitálním podpisem pro zajištění anonymity je multi-signature, který je kromě standardně využívaných ECDSA a EdDSA, podle průzkumu z tabulky 2.1, velmi častým nástrojem zabezpečení kryptoměn. Z dvaceti zkoumaných kryptoměn využívá služby multi-signature pro své zabezpečení hned 14 z nich.

2. Služby míchání mincí

Služby míchání mincí nabízí celá řada kryptoměn. Existuje však hned několik metod, které se k ochraně uživatelů a jejich peněz může využít. Podobně jako v případě analýzy digitálních podpisů je nejdůležitějším kritériem ochrana soukromí. Co se týče ochrany proti krádeži mincím, v tomto případě bylo hodnoceno na tříbodové stupnici. Metody, které zajišťují ochranu jen částečně, byly hodnoceny pouze jedním bodem. Pokud však zajišťují ochranu zcela či alespoň za určitých podmínek, hodnoceno bylo třemi, respektive dvěma body. U potřeby centrální autority a poplatku za míchání mincí je vhodnější odpověď ne, která je bodována lépe.

Metoda	Ochrana soukromí	Ochrana proti krádeži mincí	Potřeba CA	Potřeba poplatku za mixing
Mixcoin	3	1	1	1
Blindcoin	5	1	1	1
Dash	3	1	1	1
Coinswap	3	3	1	1
Tumblebit	5	3	1	1
CoinJoin	3	3	2	2
CoinShuffle	5	3	2	2
CoinParty	5	2	2	2
CoinShuffle++	5	3	2	2
Váhy	**0,45**	**0,3**	**0,2**	**0,05**

Tabulka 5.7 Vstupní hodnoty pro analýzu anonymity služeb míchání mincí

Metoda	Ochrana soukromí	Ochrana proti krádeži mincí	Potřeba CA	Potřeba poplatku za mixing
Mixcoin	0,236	0,1386	0,2182	0,2182
Blindcoin	0,394	0,1386	0,2182	0,2182
Dash	0,236	0,1386	0,2182	0,2182
Coinswap	0,236	0,4160	0,2182	0,2182
Tumblebit	0,394	0,4160	0,2182	0,2182
CoinJoin	0,236	0,4160	0,4364	0,4364
CoinShuffle	0,394	0,4160	0,4364	0,4364
CoinParty	0,394	0,2774	0,4364	0,4364
CoinShuffle++	0,394	0,4160	0,4364	0,4364
Váhy	**0,45**	**0,3**	**0,2**	**0,05**

Tabulka 5.8 Normalizovaná matice pro analýzu anonymity služeb míchání mincí

Metoda	Ochrana soukromí	Ochrana proti krádeži mincí	Potřeba CA	Potřeba poplatku za mixing	Si+	Si-	(Si+) + (Si-)
Mixcoin	0,1062	0,04158	0,04364	0,01091	**0,1183396**	**0**	**0,1183396**
Blindcoin	0,1773	0,04158	0,04364	0,01091	**0,0945994**	**0,0711**	**0,1656994**
Dash	0,1062	0,04158	0,04364	0,01091	**0,1183396**	**0**	**0,1183396**
Coinswap	0,1062	0,1248	0,04364	0,01091	**0,0841349**	**0,08322**	**0,1673549**
Tumblebit	0,1773	0,1248	0,04364	0,01091	**0,0449830**	**0,1094567**	**0,1544397**
CoinJoin	0,1062	0,1248	0,08728	0,02182	**0,0711**	**0,2275943**	**0,2986943**
CoinShuffle	0,1773	0,1248	0,08728	0,02182	**0**	**0,1183396**	**0,1183396**
CoinParty	0,1773	0,08322	0,08728	0,02182	**0,04158**	**0,0938753**	**0,1354553**
CoinShuffle++	0,1773	0,1248	0,08728	0,02182	**0**	**0,1183396**	**0,1183396**
Váhy	**0,45**	**0,3**	**0,2**	**0,05**			
Ideální	**0,1773**	**0,1248**	**0,08728**	**0,02182**			
Bazální	**0,1062**	**0,04158**	**0,04364**	**0,01091**			

Tabulka 5.9 Vážená kriteriální matice pro analýzu anonymity služeb míchání mincí

Metoda	Skóre	Pořadí
Mixcoin	0	8/9
Blindcoin	0,42909	7
Dash	0	8/9
Coinswap	0,49727	6
Tumblebit	0,70873	4
CoinJoin	0,76196	3
CoinShuffle	1	2
CoinParty	0,69304	5
CoinShuffle++	1	1

Tabulka 5.10 Výsledky analýzy metod míchání mincí z hlediska anonymity

Výsledky z tabulky 5.10 ukazují nejvyšší hodnocení u metod CoinShuffle a její vylepšené varianty CoinShuffle++. Prvním místem jsem se však nakonec rozhodl ohodnotit právě novější verzi této metody, která sice oproti starší verzi neposkytuje větší zajištění anonymity, avšak snižuje spotřebu šířky pásma a zlepšuje jeho celkový výkon. Na opačném konci tabulky se naopak objevily společně metody Mixcoin a Dash.

3. Důkazy nulových znalostí

Stejně jako u předchozích aspektů, tak i u důkazů nulových znalostí využívaných v blockchainu je nejdůležitějším kritériem ochrana soukromí. Na základě analýzy z tabulky 4.2 však všechny ze zmíněných metod poskytují skrytí adresy účastníků a hodnoty transakce. Shodné jsou taktéž sady anonymity, které jsou opět u všech metod na nejvyšší možné úrovni. Jak je však patrné z následující tabulky 5.11, k odlišnostem

dochází v případě potřeby důvěryhodného nastavení, velikostech transakcí nebo času zpracování transakcí.

Metoda	Ochrana soukromí	Sada anonymity	Není potřeba DN	Velikost transakce	Čas
Zerocoin	5	3	1	1	3
EZC	5	3	2	1	2
Zerocash	5	3	1	2	3
Bulletproofs	5	3	2	3	1
Váhy	**0,45**	**0,35**	**0,2**	**0,05**	**0,05**

Tabulka 5.11 Vstupní hodnoty pro analýzu anonymity důkazů nulových znalostí

Metoda	Ochrana soukromí	Sada anonymity	Není potřeba DN	Velikost transakce	Čas
Zerocoin	0,5	0,5	0,31645	0,2584	0,62552
EZC	0,5	0,5	0,63291	0,2584	0,41701
Zerocash	0,5	0,5	0,31645	0,5168	0,62552
Bulletproofs	0,5	0,5	0,63291	0,77519	0,20851
Váhy	**0,45**	**0,35**	**0,2**	**0,05**	**0,05**

Tabulka 5.12 Normalizovaná matice pro analýzu anonymity důkazů nulových znalostí

Metoda	Ochrana soukromí	Sada anonymity	Není potřeba DN	Velikost transakce	Čas	Si+	Si-	(Si+) + (Si-)
Zerocoin	0,225	0,175	0,06329	0,01292	0,031276	**0,06836**	**0,02085**	**0,08921**
EZC	0,225	0,175	0,126582	0,01292	0,020850	**0,09104**	**0,06414**	**0,15518**
Zerocash	0,225	0,175	0,06329	0,02584	0,031276	**0,065**	**0,02453**	**0,3103**
Bulletproofs	0,225	0,175	0,126582	0,0387595	0,010426	**0,02085**	**0,06836**	**0,08921**
Váhy	**0,45**	**0,35**	**0,2**	**0,05**	**0,05**			
Ideální	**0,225**	**0,175**	**0,126582**	**0,0387595**	**0,031276**			
Bazální	**0,225**	**0,175**	**0,06329**	**0,01292**	**0,010426**			

Tabulka 5.13 Vážená kriteriální matice pro analýzu anonymity důkazů nulových znalostí

Metoda	Skóre	Pořadí
Zerocoin	0,23372	3
EZC	0,41333	2
Zerocash	0,07905	4
Bulletproof	0,76628	1

Tabulka 5.14 Výsledky analýzy důkazů nulových znalostí z hlediska anonymity

Výsledky v tabulce 5.14 jasně dokumentují, že nejvhodnější metodou pro zajištění anonymity prostřednictvím DNZ jsou Bulletproofs, kterých využívají například Bitcoin, Zerocoin či Zerocash. U zk-SNARKs, jež zajišťují anonymitu například v kryptoměně Komodo, byla nejlépe hodnocena metoda Enhanced Zerocoin.

4. Zabezpečení chytrých smluv

Platformy chytrých smluv neposkytují všechny kryptoměny. Ve většině případů se jedná o měny, založené na Ethereu, a tak například Bitcoin tuto službu neumožňuje. V případě chytrých smluv bylo zkoumáno zejména to, jakým způsobem zajišťují ochranu soukromí. V případě, že metody poskytují zabezpečení hodnoty transakce, identity účastníků, vstupních hodnot a stavu kontraktu, byly hodnoceny nejvyšším počtem bodů. Druhým, méně závažným kritériem, pak byla otázka stran uskutečňujících danou smlouvu. Obecně totiž platí pravidlo, čím více se stran se kontraktu účastní, tím nižší je výskyt jediného bodu selhání.

	Ochrana soukromí	Strany uskutečňující ChS
Hawk	5	1
ShadowEth	4	3
Ekiden	4	3
Arbitrum	3	5
Váhy	**0,7**	**0,3**

Tabulka 5.15 Vstupní hodnoty pro analýzu anonymity chytrých smluv

Metoda	Ochrana soukromí	Strany uskutečňující ChS
Hawk	0,57737	0,15083
ShadowEth	0,46189	0,45249
Ekiden	0,46189	0,45249
Arbitrum	0,34642	0,75415
Váhy	**0,7**	**0,3**

Tabulka 5.16 Normalizovaná matice pro analýzu anonymity chytrých smluv

Metoda	Ochrana soukromí	Strany uskutečňující ChS	Si+	Si-	(Si+) + (Si-)
Hawk	0,40416	0,04525	**0,0907**	**0,08083**	**0,27598**
ShadowEth	0,32332	0,13575	**0,19842**	**0,18528**	**0,27925**
Ekiden	0,32332	0,13575	**0,19842**	**0,18528**	**0,27925**
Arbitrum	0,24249	0,22645	**0,16167**	**0,1812**	**0,34287**
Váhy	**0,7**	**0,3**			
Ideální	**0,40416**	**0,22645**			
Bazální	**0,24249**	**0,04525**			

Tabulka 5.17 Vážená kriteriální matice pro analýzu anonymity chytrých smluv

Metoda	Skóre	Pořadí
Hawk	0,67135	1
ShadowEth	0,66349	2/3
Ekiden	0,66349	2/3
Arbitrum	0,52848	4

Tabulka 5.18 Výsledky analýzy chytrých kontraktů z hlediska anonymity

Na základě výsledků analýzy v tabulce 5.18 je patrné, že nejvhodnější metodou pro zajištění anonymity chytrých kontraktů je metoda Hawk, která poskytuje největší ochranu soukromí. S velmi malým bodovým rozestupem od metody Hawk obdržely stejné hodnocení na druhém a třetím místě metody ShadowEth a Ekiden, které tedy zajišťují podobný stupeň anonymity. Rozdíl v těchto dvou metodách je však ten, že na rozdíl od ShadowEth, není Ekiden kompatibilní právě s kryptoměnami založenými na Ethereu. Nejhorší se jeví dle hodnocení metoda Arbitrum.

4. Zabezpečení transakcí mimo blockchain

Jelikož byly u zabezpečení transakcí mimo blockchain definovány pouze dvě metody, je na první pohled podle vstupních hodnot pro analýzu TOPSIS zřejmé, která z metod je pro zajištění anonymity vhodnější. Právě Bolt totiž na rozdíl od Tumblebitu umožňuje přenos transakcí jak po jednosměrném, tak po obousměrném kanálu, což je samozřejmě menší výhodou. Tou větší je však to, že jeho anonymita sice souvisí na využité kryptoměně, avšak oproti Tumblebitu poskytuje skrytí hodnoty transakce.

Metoda	Ochrana soukromí	Směr kanálu
Bolt	4	2
Tumblebit	3	1
Váha	**0,85**	**0,15**

Tabulka 5.19 Vstupní hodnoty pro analýzu anonymity transakcí mimo blockchain

5. Homomorfní závazky a akumulátory

V případě homomorfních závazků a akumulátorů nelze porovnávat žádné metody. Pro celkovou analýzu jednotlivých metod tak byly stanoveny pouze vstupní hodnoty, které se týkají kritérií ochrany soukromí, ochrany proti krádeži mincí a sady anonymity. Z pohledu zajištění soukromí je vhodnější využití akumulátorů, které zajišťují skrytí identity. Pro zabezpečení mincí je pak vhodnější využití homomorfních závazků.

Metoda	Ochrana soukromí	Ochrana proti krádeži mincí	Sada anonymity
Akumulátory	5	1	3
Závazky	3	2	3

Tabulka 5.20 Vstupní hodnoty pro analýzu anonymity homomorfních závazků a akumulátorů

5.5 Celkové posouzení aspektů z hlediska anonymity

Pro celkové hodnocení a určení důležitosti jednotlivých aspektů byly využity vstupní hodnoty nejlepších metod u daných aspektů z předchozí podkapitoly. U digitálních podpisů tedy byly využity hodnoty pro multi-signature, u služeb míchání mincí to byl CoinShuffle++, u důkazů nulových znalostí Bulletproofs, u zabezpečení chytrých smluv Hawk a u zabezpečení transakcí mimo blockchain to byl Bolt. U homomorfních závazků je využívána nejčastěji jen metoda *Pedersen commitment*, tudíž nebylo možno vybrat z více metod. Podobně je tomu taktéž v případě akumulátorů.

Aspekty	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
Digitální podpisy	5	0	0	0	3	2	2	0	0	0
Služby míchání mincí	5	3	2	2	0	0	0	0	0	0
Důkazy nulových znalostí	5	0	0	0	3	2	3	1	0	0
Chytré smlouvy	5	0	0	0	0	0	0	0	0	3
Homomorfní závazky	3	2	0	0	3	0	0	0	0	0
Akumulátory	5	1	0	0	3	0	0	0	0	0
Transakce mimo blockchain	4	0	0	0	0	0	0	0	2	0
Váhy	**0,225**	**0,15**	**0,1**	**0,025**	**0,175**	**0,1**	**0,05**	**0,05**	**0,05**	**0,075**

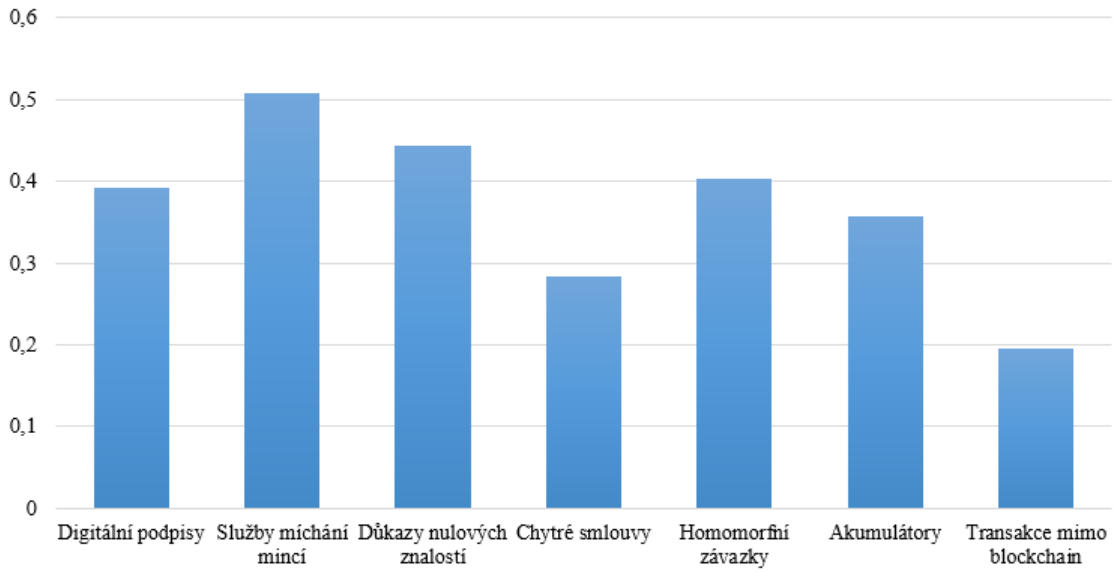
Tabulka 5.21 Vstupní hodnoty pro analýzu aspektů bezpečnosti z pohledu anonymity

Aspekty	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
Digitální podpisy	0,40816	0	0	0	0,5	0,7067	0,55402	0	0	0
Služby míchání mincí	0,40816	0,80214	1	1	0	0	0	0	0	0
Důkazy nulových znalostí	0,40816	0	0	0	0,5	0,7067	0,83102	1	0	0
Chytré smlouvy	0,40816	0	0	0	0	0	0	0	0	1
Homomorfní závazky	0,2449	0,53476	0	0	0,5	0	0	0	0	0
Akumulátory	0,40816	0,26738	0	0	0,5	0	0	0	0	0
Transakce mimo blockchain	0,32653	0	0	0	0	0	0	0	1	0
Váhy	**0,225**	**0,15**	**0,1**	**0,025**	**0,175**	**0,1**	**0,05**	**0,05**	**0,05**	**0,075**

Tabulka 5.22 Normalizovaná matice pro analýzu aspektů bezpečnosti z pohledu anonymity

Aspekty	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	Si+	Si-	(Si+) + (Si-)
Digitální podpisy	0,091836	0	0	0	0,0875	0,07067	0,027701	0	0	0	**0,189016**	**0,121520**	**0,310536**
Služby míchání mincí	0,091836	0,120321	0,1	0,025	0	0	0	0	0	0	**0,158120**	**0,162639**	**0,320759**
DNZ	0,091836	0	0	0	0,0875	0,07067	0,041551	0,05	0	0	**0,168009**	**0,133845**	**0,301854**
Chytré smlouvy	0,091836	0	0	0	0	0	0	0	0	0,075	**0,210900**	**0,083512**	**0,294412**
Homomorfní závazky	0,055103	0,080214	0	0	0,0875	0	0	0	0	0	**0,175865**	**0,118704**	**0,294569**
Akumulátory	0,091836	0,040109	0	0	0,0875	0	0	0	0	0	**0,185485**	**0,103026**	**0,288511**
Transakce mimo BC	0,073469	0	0	0	0	0	0	0	0,05	0	**0,218955**	**0,053266**	**0,272221**
Váhy	**0,225**	**0,15**	**0,1**	**0,025**	**0,175**	**0,1**	**0,05**	**0,05**	**0,05**	**0,075**			
Ideální	**0,091836**	**0,120321**	**0,1**	**0,025**	**0,0875**	**0,07067**	**0,041551**	**0,05**	**0,05**	**0,075**			
Bazální	**0,055103**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**			

Tabulka 5.23 Vážená kriteriální matice pro analýzu aspektů bezpečnosti z pohledu anonymity



Obrázek 5.1 Výsledky analýzy bezpečnostních aspektů z hlediska anonymity[14)]

5.6 Hodnocení analýzy anonymity

Na základě výsledků dosažených analýzou TOPSIS a zaznamenaných v grafu 5.1 je nejdůležitějším aspektem pro zachování anonymity a soukromí uživatelů v systému kryptoměn služba míchání mincí. Důležitost této funkce lze potvrdit také průzkumem současných kryptoměn z tabulky 3.1, kde je jasně patrné, že drtivá většina digitálních měn tuto službu, umožňující znemožnění propojení odesílatele a příjemce transakce, a snížení tak pravděpodobnosti ztráty citlivých údajů, podporuje.

Druhým nejdůležitějším aspektem byly dle analýzy určeny důkazy nulových znalostí, které jsou silnou zbraní proti úniku citlivých údajů. Jejich využitím je jedna strana schopna přesvědčit o konkrétní skutečnosti stranu druhou, aniž by došlo k odtajnění jakýchkoli informací. Jedná se však o technologii, která v praxi zatím není příliš hojně

[14)] Vlastní zpracování

využívaná. Při pohledu do tabulky 3.1 je patrné, že jak zk-SNARKs, tak Bulletproofs využívá pro zabezpečení jen hrstka kryptoměn jako Bitcoin, Zerocash nebo Monero.

Velmi podobné výsledky zaznamenaly na třetí a čtvrté pozici homomorfní závazky a digitální podpisy. Přestože podobně jako v případě důkazů nulových znalostí i závazky poskytují velkou sadu anonymity a ochranu soukromí, také ony nejsou zatím u kryptoměn příliš využívány. Naopak digitální podpisy, především tedy multi-signature, který byl nejlepší metodou pro podpis, využívá dle analýzy současného stavu z tabulky 2.1 hned 70 % z analyzovaných kryptoměn.

Pokud bychom se podívali na kryptoměny, které svým uživatelům poskytují největší anonymitu, na první místo by se bezesporu zařadil Zerocash, který poskytuje kromě služeb míchání mincí taktéž bulletproofs, homomorfní závazky i akumulátory. Jeho jedinou slabší stránkou je použití one-time signature namísto multi-signature. Velmi dobře je na tom z hlediska anonymity také nejznámější kryptoměna Bitcoin, která sice oproti Zerocash nedisponuje závazky a akumulátory, avšak co se digitálních podpisů týče, využívá nejlepší z metod, a sice multi-signature.

6 Analýza zabezpečení transakcí a samotné kryptoměny

Celkové zabezpečení kryptoměn je na rozdíl od anonymity posouzeno dvěma metodami. První část analýzy bude zaměřena na metodu SWOT, kde budou postupně definovány jednotlivé aspekty a kritéria, které bezpečnost digitálních měn ovlivňují. Na základě těchto proměnných budou stanoveny váhy a vyhodnocena celková míra rizika. Pro lepší výsledky a srovnání bude ve druhé části této kapitoly využita také metoda TOPSIS, jejíž výsledky budou srovnány právě se silnými stránkami a příležitostmi z metody SWOT.

6.1 Analýza zabezpečení pomocí metody SWOT

K analýze zabezpečení byla v první řadě využita metoda SWOT, pomocí níž jsou zkoumány silné a slabé stránky kryptoměn a s ním spojené technologie blockchainu, jakožto i jejich příležitosti a hrozby, které přicházejí z vnějšího prostředí.

6.1.1 Silné stránky

Mnoho silných stránek kryptoměn vychází ze základních vlastností blockchainu, jež byly blíže popsány v části 1.1. Jedná se hlavně o distributivitu, transparentnost, neměnnost či decentralizaci. Mezi silné stránky poskytující zejména bezpečnost technologie však spadají i další atributy, které jsou popsány v následujících řádcích.

- **Distribuovaná povaha blockchainu** – Tato vlastnost zajišťuje v první řadě ochranu před ztrátou dat a jejich neoprávněnou manipulací a brání problému dvojí útraty. V síti jsou stejná data ukládána různými uzly pro případ, že dojde k poškození některého z uzlů. V takovém případě si může poškozený uzel překopírovat data z ostatních uzlů, a bez problému tak obnovit své fungování.
- **Nevratnost** – Transakce v kryptoměnách jsou prakticky nevratné, což je na rozdíl od tradičních transakcí v běžné ekonomice změna. Obchod je matematicky nevratnou operací tak, aby poskytl ochranu prodávajícím uživatelů před podvody a zároveň chránil kupující. Systém je vytvořen tak, aby byly osobní informace obchodujících stan tajné nejen před běžnou veřejností, ale i před vládami.
- **Transparentnost** – S odolností proti podvodům úzce souvisí také transparentnost blockchainu. Jednotlivé záznamy jsou totiž opatřeny časovými razítky a uloženy ve všech úplných uzlech sítě. Kdokoliv z dané sítě tedy může sledovat veškeré vykonávané aktivity a transakce.
- **Nefyzičnost** – Fakt, že transakce u digitálních měn nevyžadují vystavení žádného bankovního výpisu nebo faktury, umožňuje tato technologie mnohem jed-

nodušší řešení pro uložení majetku, než je tomu v případě běžných bankovních účtů. S tím související náklady na tisk a uchovávání dokumentů je díky tomu sníženo na minimum.

- **Rychlost a globálnost** – Transakce jsou v síti šířeny téměř okamžitě a jejich potvrzení trvá v řádu minut. Jelikož se transakce odehrávají v globální síti, jsou zcela nezávislé na jakékoli výchozí lokalitě uživatele. Nehraje vůbec žádnou roli, zda uživatel odešle transakci jinému uživateli v rámci města, či přes celý svět.

- **Hashovací funkce a podpisy** – Většina kryptoměn využívá pro své digitální podpisy technologii ECDSA, která oproti starším RSA nebo DSA poskytuje mnohem lepší zabezpečení pro určitou velikost klíče. Řada kryptoměn se navíc rozhodla využívat i další technologie podpisů jako jsou prstenový či multi-signature. Pro zajištění bezpečnosti je navíc využívána celá řada hashovacích funkcí.

- **Skrytí komunikace** – V blockchainu se pro skrytí jak obsahu komunikace, tak toho, s kým uživatel komunikuje, využívají služby míchání mincí neboli mixing services, jejichž fungování je popsáno v části 2.6.

- **Absence jediného bodu selhání** – Jak již napovídá samotný název Single Point of Failure nebo také jediný bod selhání, jedná se o část systému, jež v případě selhání zastaví fungování celého systému. Veřejné blockchainy jsou decentralizované, díky čemuž jsou mnohem odolnější než tradiční systémy. Chyba jediného uzlu nebude mít vliv na fungování ani zabezpečení celého zbytku systému. To znamená, že i v případě útoků DDoS bude systém zásluhou několika kopií účetní knihy fungovat jako obvykle.

- **Pseudonymita** – Anonymita je u většiny kryptoměn založena na takzvané pseudonymitě. To znamená, že uživatel v takovémto případě nevystupuje pod svou vlastní identitou, nýbrž pod pseudonymem, který je v tomto případě reprezentován adresou. V případě, že by byl však pseudonym přiřazen k pravé identitě uživatele, došlo by k odhalení veškerých informací, které jsou trvale zaznamenány v blockchainu. Zatímco některé anonymní transakce napomáhají kriminálnímu chování, soukromí je základním lidským právem.

6.1.2 Slabé stránky

Stejně jako silné stránky, tak i slabé stránky kryptoměn vycházejí primárně ze vlastností a funkcí blockchainu.

- **Složitost technologie** – Vytvoření systému je poměrně složitou problematikou, kde jediná chyba může vést k ohrožení celé sítě. Nejedná se tedy vyloženě o chybu technologie, ale spíše o chybu při jejím provedení. Vinou složitosti je navíc poměrně náročné pro běžného uživatele pochopení celého jejího fungování, který tak nemusí zcela rozumět všem funkcím a rizikům systému.

- **Velikost sítě** – Pro správné fungování blockchainu musí existovat stovky, nejlépe tisíce společně pracujících uzlů v síti. Technologie je tedy zejména při svém začátku velmi náchylná vůči kybernetickým útokům a korupci. Problémem může být typicky útok 51%, kdy je pro útočníka mnohem jednodušší získat většinový podíl z malého počtu uzlů.

- **Rychlost a účinnost sítě** – Špatný a komplikovaný návrh systému může narušit jeho schopnost zpracovávat transakce vhodnou rychlostí. Pokud je systém příliš složit,ý může docházet k problémům s ukládám dat a rychlostí jednotlivých transakcí.

- **Peněženky** – Pro správu měny, ať už jde o uložení nebo uskutečnění transakcí, je zapotřebí peněženka, která může mít formu buďto hardwarovou, softwarovou či papírovou. Pro bezpečnost je zapotřebí u peněženek využít šifrování a velmi žádoucí je také offline zálohování pro případné obnovení stavu peněženek.

- **Prolomení anonymity prostřednictvím historie transakcí** – Pokud jde například o Bitcoin, na základě algoritmů a využitých protokolů jsou všechny transakce v historii Bitcoinu zpětně dohledatelné a vysledovatelné až k těžební transakci, která jej vytvořila. K řešení tohoto problému vznikla hned celá řada mixing services.

- **Systémy třetích stran** – Slabými stránkami u kryptoměn mohou být systémy třetích stran, které nemusejí poskytovat dostatečné zabezpečení, což může vést ke ztrátě citlivých údajů i samotné měny. Problém tak velmi často není tolik v samotné technologii, jež je vytvořena na blockchainu, jako v zabezpečení webových aplikací, které na ní fungují. Například v systému NiceHash, který byl největším tržištěm na těžbu kryptoměn, přišli uživatelé vinou kybernetického útoku v roce 2017 o více než 4700 BTC[15)], což bylo v přepočtu téměř 70 milionů amerických dolarů tedy 1,5 miliardy Kč [2].

[15)] Bitcoin

6.1.3 Příležitosti

Technologie blockchainu a problematika kryptoměn je poměrně mladou disciplínou, která se stejně jako veškeré informační technologie neustále rozvíjí. Zajištění soukromí a bezpečnosti uživatel jde ruku v ruce s vývojem nových kryptografických metod zaměřujících se na stále více propracované kybernetické útoky a práci na vylepšení slabých stránek blockchainu. V následujících řádcích jsou popsány jednotlivé příležitosti a trendy, které by v budoucnu mohli vést ke zvýšení bezpečnosti kryptoměn.

- **Aktivní komunita pro vývoj softwaru** – Většina kryptoměn je založena na principu otevřeného softwaru, což umožňuje vzniku nových aplikací a příležitostí k budování a vylepšování celé technologie.
- **Rozšíření využívání důkazů nulových znalostí** – Jak již bylo zmíněno, většina kryptoměn není na rozdíl od běžných měn anonymní, ale pouze pseudonymní. K mnohem lepšímu zajištění anonymity tak již některé alternativní kryptoměny začaly využívat důkazy nulových znalostí, které jsou podrobněji popsány v části 2.5. Zjednodušeně řečeno umožňuje technologie ZKP straně A přesvědčit stranu B o konkrétní skutečnosti, aniž by došlo k úniku jakýchkoli citlivých informací.
- **Využívání veřejného blockchainu** – S rozvojem kryptografických a bezpečnostních technologií, jako jsou důkazy nulových znalostí, dokáže využití veřejného blockchainu překonat řadu obav, zejména pokud jde o soukromí a důvěru. Použití veřejného blockchainu, jehož fungování je popsáno v podkapitole 1.2.1, namísto privátního blockchainu může navíc společnostem pomoci ušetřit náklady spojené s provozem a údržbou celé blockchainové sítě. Díky tomu se tak mohou soustředit na další vývoj a inovace v rámci využití této technologie. Veřejný blockchain tedy celkově poskytuje mnohem větší zabezpečení sítě, a to z důvodu většího počtu uzlů, které zachovávají neměnnost technologie, čímž by se měl v budoucnu stát dominantní architekturou používanou v řadě odvětví.
- **Postkvantová kryptografie** – Kvantové počítače představují reálnou hrozbu pro zabezpečení blockchainu a tím samozřejmě i kryptoměn. Z toho důvod existuje poptávka po účinných a osvědčených postkvantových schématech digitálního podpisu a dalších příslušných studiích na ochranu blockchainu před všemi druhy hrozeb kvantových počítačů. Na rozdíl od klasického ECDSA, jehož fungování je popsáno v části 2.2.1, existuje hned několik kryptografických metod, které podle výzkumů nejsou náchylné na útoky kvantových počítačů. Patří mezi ně například kryptografické systémy založené na hashovacích funkcích, kódu nebo takzvané mřížce. Existuje mnoho příležitostí na rozvoj použitelnosti podpisů, jejich efekti-

vity a důvěry, a to zejména pro jejich použití v blockchainu právě proti hrozbám ze strany kvantových počítačů [41].

- **Efektivní a bezpečné konsensuální protokoly** – Existuje celá řada konsensuálních protokolů, které se snaží nahradit nejvyužívanější konsensus Proof of Work z důvodu jeho velké spotřeby energie při řešení složitých matematických operací. Některé z nových protokolů však přicházejí s novými bezpečnostními problémy nebo mohou být v praxi jen těžko proveditelné. Právě konsensuální metody tedy v technologii blockchainu skýtají poměrně velkou příležitost k výzkumu a zlepšení [41].
- **Rozšíření 5G sítí** – Kryptoměny ve spojení s rozšířením 5G sítí nabízejí mnoho možností na zlepšení. Využití 5G může nabídnout například mnohem lepší zabezpečení pro mobilní bankovní sítě či zlepšit konzistenci a rychlost ověřovacích systémů pracujících v blockchainu. Uživatelé, kteří momentálně nemají přístup k běžným bankovním službám, mohou mít navíc po zavedení 5G sítí mnohem snazší přístup k digitálním peněženkám, a nebudou tudíž potřebovat tradiční bankovní účty. Z toho důvodu může dojít k ještě většímu zájmu o kryptoměny, s čímž bude souviset jejich další vývoj.
- **Škálovatelnost** – Jedním z hlavních problémů současných kryptoměn je škálovatelnost, jež je důležitá také pro budoucnost technologie. Zjednodušeně řečeno se jedná o rychlost, s jakou je daná síť schopna zpracovávat požadavky účastníků. V současné době se uvádí standardní škálovatelnost přibližně tisíce transakcí za vteřinu, což však bude v budoucnu s nástupem nových technologií nedostačující.

6.1.4 Hrozby

Mezi hrozby kryptoměn patří zejména kybernetické útoky všeho druhu. Na základě technologie blockchainu a s ním souvisejících částí, které jsou podrobněji popsány v teoretické části této práce, byly typy hrozeb rozděleny dle aspektů, na které dané útoky cílí, do pěti hlavních skupin. Jedná se o hrozby konsensuálních metod a transakcí, peněženek, sítě a chytrých kontraktů. Mezi problémy při zajištění bezpečnosti a anonymity uživatele lze navíc zařadit i chybu adresy uživatele nebo ztráta souboru peněženky.

- **Hrozby konsensuálních metod a transakcí** – Jak již název kategorie napovídá, hlavním cílem těchto útoků jsou konsensuální metody a mechanismy pro ověřování transakcí.
  - **Hrozby dvojí útraty** – Útoky pomocí dvojí útraty jsou útoky, během nichž se útočník snaží využít stejnou kryptoměnu na hned několik transakcí, což vede ke zneužití určitého obnosu peněz k několika platbám. Jedná

se o velmi častý typ útoků, který míří na samotné uživatele a těžaře kryptoměny. Nejznámějším a nejčastějším útokem spadajícím do této skupiny je *51% útok*, který je považován za zřejmě nejvíce ohrožující útok v rámci technologie blockchainu. V případě, že by se útočníkovi podařilo získat kontrolu nad více než 51% hashovacího výkonu sítě, stabilita celé sítě by tím byla naprosto rozbita. Útočník by tedy mohl využít dalších útoků spadajících do kategorie dvojí útraty jako jsou *Finney Attack*, *Race Attack*, *Vector76 Attack* a *Alternative History Attack*. Mezi hlavní opatření u tohoto typu hrozby patří ku příkladu přidání doby potvrzení bloku, které může těmto útokům poměrně jednoduše zabránit [35].

- **Hrozby spojené s těžbou kryptoměn** – Nejčastějším typem útoku spojených s těžbou kryptoměn je takzvaná sobecká těžba neboli selfish mining. U těžby kryptoměn existují dva typy těžařů, a sice poctiví a sobečtí těžaři. Nezáleží na tom, zdali poctiví těžaři kryptoměn pracují jako jednotlivci, ve skupinách nebo dokonce ve více skupinách. Hlavním cílem sobeckých těžařů je, aby přinutili poctivé těžaře plýtvat svou výpočetní sílu v již vyčerpané větvi. Přestože to není příliš pravděpodobné, návrh systému umožňuje, že se blockchain rozdělí na dvě konkurenční větve. Pro řešení tohoto problému využívají kryptoměny ve své technologii protokoly, které určují, že správným řetězcem je ten nejdelší, čímž dochází ke zneplatnění bloků, které byly vytěženy v rámci kratšího paralelního řetězce. Sobečtí těžaři však obcházejí tuto vlastnost blockchainu udržováním všech bloků ve své vlastní tajné větvi. Jakmile se poctiví těžaři chystají své konkurenty dohnat, co se délky blockchainu týče, sobečtí těžaři zveřejní bloky z tajné větve, čímž anulují veškeré bloky poctivých těžařů, a veškerá odměna tak zůstane jim [20].

  Ne všechny kryptoměny jsou však náchylné na problematiku sobecké těžby. Například Ripple byl na začátku vytvořen se sto miliardami mincí XRP[16)], jež není možno těžit a po prvním použití jsou vyčerpány. Představou společnosti je vlastnit polovinu dostupných mincí a druhou polovinu nechat volně v oběhu. Jediným způsobem, jak získat tuto kryptoměnu je výměnou za jinou měnu, díky čemuž je Ripple chráněn před útoky spojenými s procesem těžby [42].

- **Hrozby peněženek** – Jelikož je peněženka v kryptoměnách fyzické médium či program, jenž se stará o ukládání veřejných a soukromých klíčů pro transakce a případně navíc zajišťuje funkce šifrování či podepisování, hlavním cílem útoků jsou u této kategorie hashovací funkce a digitální podpisy v blockchainu.

[16)] Ripple

- **Zranitelnost podpisu** – Většina kryptoměn v současné době využívá pro podpis a verifikaci transakcí technologii ECDSA, blíže popsanou v části 2.2.1. Kromě toho, že má ke kryptografickým nástrojům volný přístup mnoho uživatelů, z nichž někteří mohou využít získané znalosti k prolomení zabezpečení za účelem zisku, je u ECDSA navíc poměrně nedostatečná náhodnost při generování klíčů. Z toho důvodu využívají některé kryptoměny i jiné technologie pro podpis a verifikaci transakcí jako například prstenové podpisy nebo multi-signature.

- **Špatná tvorba podpisu** – S protokolem digitálního podpisu s využitím eliptických křivek souvisí také hrozba špatné tvorby podpisu, zejména při jeho chybné implementaci. Vinou toho může dojít k vytvoření slabých míst v peněženkách, což následně může vést k úniku soukromých klíčů. V roce 2014 se podobná nepříjemnost stala poskytovateli peněženek Blochchain.info při úpravě zdrojového kódu, čímž byly narušeny vstupy pro ECDSA a podstatně snížena náhodnost při tvorbě klíčů [28].

- **Softwarové chyby a malware** – Stejně jako každá technologie, tak i blockchain obsahuje spoustu softwarových chyb, ať už sémantických, paměťových, bezpečnostních, konfiguračních či týkající se výkonu, kompatibility a spousty dalších vlastností. V roce 2017 odhalila Zhiyuan Wan s týmem ve své práci více než tisíc záznamů o chybách v blockchainu [44]. Problémem mohou být kromě samotného blockchainu i další součásti technologie kryptoměn jako jsou například právě hardwarové peněženky.

- **Ztráta souboru peněženky** – S předchozí hrozbou malwaru úzce souvisí také hrozba ztráty souboru peněženky, k čemuž může dojít buďto právě prostřednictvím malwaru nebo při chybě fyzického média.

- **Hrozby sítě** – V případě hrozeb sítě se jedná o útoky mířené směrem na protokoly blockchainu. Jak je známo, síť blockchainu je typem peer-to-peer a zahrnuje veškeré uzly, které udržují a provozují blockchainové protokoly a poskytují služby, spadající pod síť blockchainu. Útoků na síť existuje celá řada. Mezi nejznámější a nejvíce časté se bezesporu řadí odepření služby (DDoS), Malleability Attack, Timejacking Attack, Sybil Attack a Eclipse Attack.

  - **Distributed Denial of Service** – Neboli odepření služby je mnohem náročnější provést u blockchainu, který je založen na decentralizaci, než je tomu v případě běžných klient-server modelů. I přesto je však síť blockchainu velmi častým terčem právě DDoS útoků, které se vyznačují zahlcením systému velkým počtem požadavků. Přestože v kryptoměnách vznikla celá řada mechanismů chránící blockchain před útoky DDoS, právě tento typ

útoků se stal nejčastějším útokem na směnárny, těžaře, chytré kontrakty a další služby spadající do ekosystému kryptoměn [45].

- **Hrozby chytrých kontraktů** – V případě chytrých kontraktů, jejich hrozby je možno rozdělit do tří podskupin podle toho, na jakou část smlouvy je útok prováděn. Jedná se o útoky na bytelnost systému, virtuální stroj a samotný blockchain, z nichž každá část disponuje určitými zranitelnostmi. Největšími zranitelnostmi chytrých kontraktů jsou především špatný návrh systému a chyby VM. Velmi častými jsou u chytrých kontraktů například *Re-entrancy attack*, *Eclipse attack* či *Integer overflow attack* neboli útok přetečením integeru [45].

- **Chyba adresy uživatele** – Přestože je využíváním různých klientských aplikací tato hrozba poněkud malá, stále je pro kryproměny poměrně typickou. Při chybě v adrese uživatele, na kterou se daný obnos peněz posílá, může dojít ke ztrátě velkého množství peněz. Pokud by například v případě Etherea došlo k chybě v posledním čísle adresy příjemci, poslané peníze by nenávratně zmizely do neznáma nebo by se sice částka poslala, avšak její velikost by byla vynásobena číslem 256 [28].

6.1.5 Stanovení vah

Na základě výše uvedených aspektů, tedy silných a slabých stránek, příležitostí a hrozeb, ovlivňujících bezpečnost systému kryptoměn, byla vytvořena pro analýzu bezpečnosti matice SWOT, která je zobrazena v tabulce 6.5. Každý z kvadrantů obsahuje pro jednotlivé aspekty váhu bezpečnosti čili to, jak důležitý je daný aspekt pro správné fungování blockchainu, případně jak velké riziko představuje pro jeho bezpečnost a anonymitu jak už z pohledu uživatelů, tak samotných transakcí. Pro stanovení vah jednotlivých aspektů byly vytvořeny následující tabulky. Součet vah v jednom kvadrantu navíc musím být roven jedné.

Silné stránky

Pokud jde o silné stránky kryptoměn a určování jednotlivých vah pro dané aspekty, bylo pro srovnání využito toho, jak moc se dané vlastnosti podílejí na zajištění bezpečnosti a chrání blockchain před ztrátou citlivých dat uživatele a zajišťují celkovou bezpečnost systému. Jedná se o následující požadavky, které jsou v tabulce 6.4 reprezentovány písmenem P: ochrana před ztrátou dat (P1), ochrana před manipulací s daty (P2), ochrana proti krádeži peněz (P3), snižování nákladů (P4), ochrana peněženek (P5), ochrana před nefunkčností komponent (P6) a neoprávněné manipulace s komponentami (P7), ochrana proti získaní velkého výpočetního výkonu (P8), zabez-

pečení komunikace (P9), verifikované transakce (P10), ochrana proti krádeži citlivých údajů (P11).

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	Váha
Dist. povaha blockchainu	✓	✓	✓					✓			✓	**0,15**
Nevratnost	✓	✓	✓								✓	**0,125**
Transparentnost	✓	✓	✓									**0,1**
Nefyzičnost				✓							✓	**0,05**
Rychlost a globálnost						✓		✓				**0,05**
Hashovací funkce a podpisy	✓	✓	✓		✓				✓	✓	✓	**0,2**
Skrytí komunikace	✓	✓	✓						✓		✓	**0,15**
Absence SPOF						✓	✓					**0,05**
Pseudnymita	✓	✓	✓								✓	**0.125**

Tabulka 6.1 Stanovení vah silných stránek pro SWOT analýzu

Jak je patrné z tabulky 6.1, největší vahou byl v rámci silných stránek bezpečnosti blockchainu ohodnocen atribut hashovací funkce a podpisy, který splňuje hned sedm z deseti zmíněných požadavků na bezpečnost a anonymitu. O něco nižší vahou byly následně hodnoceny atributy skrytí komunikace a distributivní povaha blockchainu, u nichž byla analyzována shoda v pěti požadavcích. Shodně jsou na tom následně také nevratnost, která zajišťuje ochranu zejména před ztrátou a manipulací s daty a pseudonymita, která disponuje stejnými atributy. Druhou nejnižší hodnotu váhy si následně vysloužila transparentnost blockchainu, která hraje významnou roli především při ochraně proti podvodům. Nejméně významná je pak trojice nefyzičnost, rychlost a globálnost a absence jediného bodu selhání.

Slabé stránky

Také u slabých stránek blockchainu bylo, stejně jako u těch silných, při stanovování vah pro následné hodnocení rizika, bráno v potaz zejména to, jak moc ovlivňují celkovou bezpečnost a anonymitu systému. Pro stanovení slabých stránek a poté i hrozeb, bylo definováno třináct rizik, kterými můžou být jednotlivé vlastnosti ovlivněny. V tomto případě se jedná o následující rizika: krádež citlivých údajů (R1), nefunkčnost komponent (R2), neoprávněná manipulace s komponentami (R3), ztráta dat (R4), manipulace s daty (R5), narušení bezpečného kanálu (R6), nezabezpečená komunikace (R7), narušení kontroly přístupu uživatelů (R8), nezabezpečené funkce třetí strany (R9), změna zdrojového kódu (R10), chyba adresy (R11), tvárnost účetní knihy (R12), chyba konsensuálního protokolu (R13), ztráta peněz (R14).

V rámci slabých stránek v tabulce 6.2 byla největší míra rizika stanovena u systémů třetích stran, jež nemusejí disponovat dostatečným zabezpečením, a může tudíž velmi

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	Váha
Složitost technologie		✓	✓			✓				✓					0,11
Velikost sítě	✓	✓	✓	✓	✓									✓	0,21
Rychlost a účinnost sítě				✓	✓										0,06
Peněženky	✓		✓	✓					✓					✓	0,16
Prolomení anonymity prostřednictvím hist. transakcí	✓			✓	✓	✓	✓							✓	0,21
Systémy třetích stran	✓			✓	✓	✓	✓		✓					✓	0,25

Tabulka 6.2 Stanovení vah slabých stránek pro SWOT analýzu

snadno dojít ke ztrátě dat nebo samotné měny. O něco méně náchylné atributy jsou pak velikosti sítě a prolomení anonymity pomocí historie transakcí. Co se týče prvně zmiňovaného atributu, největší problém nastává v případě, že síť není dostatečně velká, vinou čehož je mnohem náchylnější na kybernetické útoky a podvody. Menší vahou byly následně ohodnoceny peněženky a složitost technologie. Vůbec nejmenší vliv na bezpečnost systému kryptoměn má pak podle hodnocení rychlost a účinnost sítě.

Příležitosti

Příležitosti ve zlepšení zabezpečení technologie blockchainu souvisí hlavně s větším rozšířením již využívaných technologiích v rámci některých alternativních kryptoměn. Pro stanovení vah příležitostí bylo využito, podobně jako u silných stránek, požadavků na bezpečnost a anonymitu, které by měly jednotlivé atributy po vylepšení poskytovat. Výčet je doplněn o rychlost zpracování transakcí (P12) a ochranu konsensuálního protokolu (P13). Z tabulky 6.3 je patrné, že nejvyššími stupni byly ohodnoceny shodně čtyři příležitosti, a sice rozšíření důkazů nulových znalostí, postkvantová kryptografie, efektivní a bezpečné konsensuální metody a rozšíření využití veřejného blockchainu. Rozšíření 5G sítí není pro bezpečnost natolik významné, avšak může hrát v budoucnu velkou roli při rychlosti zpracování transakcí a rozšíření kryptoměn. S větším počtem uživatelů bude ruku v ruce stoupat i počet hrozeb, což bude tlačit na vývoj a výzkum dalších bezpečnostních metod a funkcí. Nejmenší váhu si pak odnesly škálovatelnost a aktivní komunita, které nemají na zabezpečení a anonymitu v porovnání s ostatními atributy příliš velký vliv.

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	Váha
Aktivní komunita pro vývoj SW				✓							✓			0,05
Rozšíření důkazů nulových znalostí	✓	✓	✓						✓	✓	✓			0,2
Využívání veřejného blockchainu	✓	✓	✓	✓		✓	✓							0,2
Postkvantová kryptografie	✓	✓	✓						✓		✓		✓	0,2
Efektivní a bezpečné konsensus. p.	✓			✓	✓	✓						✓	✓	0,2
Rozšíření 5G sítí	✓				✓						✓	✓		0,12
Škálovatelnost												✓		0,03

Tabulka 6.3 Stanovení vah příležitostí pro SWOT analýzu

Hrozby

Jak již bylo zmíněno u stanovení vah slabých stránek kryptoměn, také pro stanovení vah hrozeb bylo využito třinácti rizik. Jak je patrné z tabulky 6.4, největší hrozbou jsou pro kryptoměny útoky dvojí útraty a s tím spojený útok 51%, kdy se útočník zmocní většinového hashovacího výkonu v síti blockchainu. Velkou hrozbou jsou, stejně jako pro většinu technologií, také softwarové chyby neboli bugy a malwere, k nimž bylo přiřazeno hned devět ze třinácti definovaných rizik. Za zmínku dále stojí hrozby peněženek a sítě, kde může dojít ke ztrátě citlivých a osobních informací. Naopak nižší váhy byly stanoveny u hrozeb spojených s těžbou či chybou adresy uživatele, které nejsou až tolik časté a neskýtají tolik rizik, jako ostatní hrozby.

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	Váha
Dvojí útrata	✓		✓	✓	✓	✓	✓	✓	✓				✓	✓	0,16
Hrozby spojené s těžbou													✓	✓	0,06
Hrozby peněženek	✓	✓		✓	✓	✓	✓		✓					✓	0,11
Zranitelnost podpisu	✓			✓	✓	✓			✓					✓	0,1
Špatná tvorba podpisu	✓			✓	✓	✓									0,07
SW chyby a malwere	✓	✓	✓	✓	✓				✓	✓	✓			✓	0,14
Ztráta souboru peněženky	✓			✓	✓				✓					✓	0,1
Hrozby sítě		✓		✓	✓							✓	✓	✓	0,11
Hrozby chytrých kontraktů	✓			✓	✓		✓				✓				0,09
Chyba adresy uživatele											✓			✓	0,06

Tabulka 6.4 Stanovení vah pro hrozby pro SWOT analýzu

6.1.6 Hodnocení rizika

Stanovením vah v předchozí části práce došlo k normalizaci jednotlivých kvadrantů SWOT matice, a to z důvodu, že se v každém kvadrantu vyskytuje jiný počet atributů, což by vedlo k irelevantním výsledkům analýzy. Pro potřeby hodnocení rizik je však zapotřebí určit ještě hodnotu rizika, která je ve SWOT matici 6.5 označena jako hodnota. Pro srozumitelné výsledky byla vytvořena škála od jedné do čtyř, kdy jsou jednotlivé vlastnosti hodnoceny zejména z pohledu vlivu na bezpečnost, anonymitu a celkově využití v blockchainu následovně:

- Ano - 4 body
- Spíše ano - 3 body
- Spíše ne - 2 body
- Ne - 1 bod

Pro získání celkové hodnoty byly položky *váha* a *hodnota* vynásobeny. Díky tomu byly odhaleny největší hrozby, ale také silné stránky a možnosti, v jakých ohledech technologii vylepšit a na co se v následujících výzkumech zaměřit. Součtem všech hodnot v rámci kvadrantu byla následně získána hodnota, která je dále využita pro určení celkové míry rizika, kdy jsou hodnoty slabých stránek a hrozeb odečteny od hodnot silných stránek a příležitostí.

Silné stránky				**Slabé stránky**			
Atribut	**Váha**	**Hodnota**	**Celkem**	**Atribut**	**Váha**	**Hodnota**	**Celkem**
Distributivita	0,15	3	0,45	Složitost technologie	0,11	1	0,11
Nevratnost	0,125	3	0,375	Rychlost a účinnost sítě	0,06	2	0,12
Transparentnost	0,1	3	0,3	Peněženky	0,16	3	0,48
Nefyzičnost	0,05	2	0,1	Velikost sítě	0,21	3	0,63
Rychlost a globálnost	0,05	2	0,1	Historie transakcí	0,21	4	0,84
Hashovací funkce a podpisy	0,2	4	0,8	Systémy 3. stran	0,25	4	1
Skrytí komunikace	0,15	3	0,45				
Absence SPOF	0,05	2	0,1				
Pseudonymita	0,125	2	0,25				
	1		**2,925**		1		**3,18**
Příležitosti				**Hrozby**			
Atribut	**Váha**	**Hodnota**	**Celkem**	**Atribut**	**Váha**	**Hodnota**	**Celkem**
Aktivní komunita	0,05	1	0,05	Dvojí útrata	0,16	4	0,64
Rozšíření důkazů	0,2	3	0,6	Hrozby spojené s těžbou	0,06	2	0,12
Využívání veřejného blockchainu	0,2	4	0,8	Hrozby peněženek	0,11	3	0,33
Postkvanotvá kryptografie	0,2	3	0,6	Zranitelnost podpisu	0,1	3	0,3
Bezpečné konsensuální prot.	0,2	4	0,8	Špatná tvorba podpisu	0,07	2	0,14
Rozšíření 5G sítí	0,12	2	0,24	SW chyby a malwere	0,14	4	0,56
Škálovatelnost	0,03	1	0,03	Ztráta souboru peněženky	0,1	3	0,3
				Hrozby sítě	0,11	3	0,33
				Hrozby chytrých smluv	0,09	2	0,18
				Chyba adresy uživatele	0,06	2	0,12
	1		**3,12**		1		**3**
SOUČET: (2,925 + 3,12) - (3,18 + 3) = -0,135							

Tabulka 6.5 Hodnocení rizika pomocí SWOT matice

Pro hodnocení velikosti rizika byla vytvořena následující škála, která je vyobrazena v tabulce 6.6:

Míra rizika	**Číselná hodnota**
Velmi nízké riziko	nad 1
Nízké riziko	0,5 až 1
Střední riziko	-0,5 až 0,49
Vysoké riziko	-1 až -0,49
Velmi vysoké riziko	méně než -1

Tabulka 6.6 Škála hodnocení velikosti rizika

Výsledná hodnota našeho hodnocení činí po výpočtu veškerých hodnot -0,135, což na dané stupnici odpovídá míře středně vysokého rizika.

6.1.7 Hodnocení analýzy bezpečnosti pomocí metody SWOT

Jak je patrné z výsledku hodnocení ve SWOT matici 6.5, pokud jde o silné stránky blockchainu a s ním spojené kryptoměny, velkou roli hrají u zabezpečení především hashovací funkce a podpisy, které jsou nedílnou součástí samotné technologie. Velmi dobře si v analýze vedl i aspekt skrytí komunikace, což zprostředkovávají služby míchání mincí, které chrání jak před ztrátou dat uživatelů, tak samotné měny. Za zmínku stojí v rámci blockchainu i jeho vlastnosti distributivita a nevratnost. První z vlastností představuje ochranu před ztrátou dat, kdežto nevratnost je užitečná před podvody a chrání prodávajícího i kupujícího.

Pokud jde o budoucí zlepšení bezpečnosti, analýza v rámci příležitostí odhalila jako důležitý faktor vytvoření bezpečných konsensuálních metod, které by nahradily současné metody jako Proof of Work či Proof of Stake. Velmi užitečné by mohlo být také větší rozšíření veřejného blockchainu, který z daných architektur poskytuje největší zabezpečení a umožňuje využívat zmíněné kryptografické a bezpečnostní metody.

Naopak hrozby pro uživatele, ať už jde o ztrátu informací či samotných peněz, se ukrývají zejména v systémech třetích stran. Kritickými můžou být pro celou technologii blockchainu a jeho bezpečnost útoky zaměřené na získání velké části hashovací výkonu sítě. Velkým rizikem jsou pro kryptoměny dle analýzy také historie transakcí, kdy může dojít k prolomení anonymity z toho důvodu, že v mnoha systémech je možné všechny transakce zpětně dohledat a vysledovat až k těžební transakci. K řešení tohoto problému jsou ve velké většině kryptoměn využívány již zmíněné mixing services. Zanedbatelné nejsou ani další kybernetické útoky všeho druhu, softwarové chyby neboli bugy a malware.

6.2 Analýza zabezpečení pomocí metody TOPSIS

Pro získání lepších a komplexnějších výsledků byla k analýze zabezpečení transakcí a celkově kryptoměn využita kromě metody SWOT i metoda TOPSIS. Podobně jako při analýze anonymity bylo nejprve zapotřebí stanovit vhodná kritéria a jejich váhy podle toho, jak moc se podílejí na zajištění bezpečnosti. Následně byla provedena samotná analýza a její výsledky srovnány s metodou SWOT, ale i s reálnými daty ohledně metod zabezpečení dnešních digitálních měn, které jsou uvedeny v přílohách.

6.2.1 Stanovení kritérií

Aby byly výsledky analýzy relevantní a srovnatelné, bylo zapotřebí stanovit kritéria podobná kritériím metody SWOT. Kritéria ochrana před ztrátou dat a ochrana před manipulací s daty byla sjednocena pod názvem ochrana soukromí. Přidáno bylo navíc kritérium sada anonymity, potřeba centrální autority a potřeba důvěryhodného nastavení, které byly využity při analýze zabezpečení kryptoměn z pohledu anonymity.

- K_1 – Ochrana soukromí
- K_2 – Sada anonymity
- K_3 – Ochrana proti krádeži mincí
- K_4 – Snižování nákladů
- K_5 – Ochrana před nefunkčností komponent
- K_6 – Neoprávněná manipulace s komponentami
- K_7 – Ochrana proti získaní velkého výpočetního výkonu
- K_8 – Zabezpečení komunikace
- K_9 – Rychlost zpracování
- K_{10} – Velikost transakcí/klíčů
- K_{11} – Potřeba centrální autority
- K_{12} – Potřeba důvěryhodného nastavení
- K_{13} – Strany uskutečňující chytrou smlouvu

6.2.2 Stanovení vah

Váhy jednotlivých kritérií pro hodnocení bezpečnostních aspektů z hlediska zabezpečení transakcí byly určeny následovně:

Pořadí	Kritérium	Váha
1	Zabezpečení komunikace (K8)	0,15
1	Ochrana soukromí (K1)	0,15
2	Ochrana proti krádeži mincí (K3)	0,11
2	Ochrana proti získání velkého výpočetního výkonu (K7)	0,11
2	Sada anonymity (K2)	0,11
3	Ochrana před nefunkčností komponent (K5)	0,08
3	Ochrana před neoprávněnou manipulací s komp. (K6)	0,08
4	Potřeba důvěryhodného nastavení (K12)	0,06
4	Potřeba centrální autority (K11)	0,06
5	Velikost transakce nebo klíče (K10)	0,03
5	Rychlost zpracování (K9)	0,03
5	Strany uskutečňující chytrou smlouvu (K13)	0,03
6	Snižování nákladů (K4)	0,01

Tabulka 6.7 Stanovení pořadí a vah kritérií pro analýzu zabezpečení kryptoměn

6.2.3 Hodnocení aspektů bezpečnosti kryptoměn

K hodnocení byly vybrány totožné bezpečností aspekty jako u hodnocení anonymity. Jedná se tedy o digitální podpisy, služby míchání mincí, důkazy nulových znalostí, chytré smlouvy, homomorfní závazky, akumulátory a transakce mimo blockchain. Jelikož je však využití těchto metod zaměřeno právě zejména na anonymitu a soukromí uživatelů kryptoměn, přidány byly k hodnocení navíc hashovací funkce, které právě útočníkům zabraňují například v získaní velkého výpočetního výkonu a tím i ohrožení celého systému blockchainu. Dalšími aspekty této analýzy jsou pak navíc veřejný blockchain, jenž z dostupných architektur blockchainu poskytuje nejlepší bezpečnost, a konsensuální metody, které jsou využívány k zajištění souhlasu kopií dat v různých uzlech. V následujících tabulkách je podrobně zobrazen postup vypracování metody TOPSIS ohledně zabezpečení transakcí a samotné kryptoměny.

Aspekty	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**	**K9**	**K10**	**K11**	**K12**	**K13**
Veřejný blockchain	3	0	0	0	1	1	1	0	0	0	0	0	0
Konsensuální metody	2	1	1	1	1	1	2	0	1	0	0	0	0
Hashovací funkce	2	2	3	0	3	3	3	3	0	1	0	0	0
Digitální podpisy	5	3	0	0	0	0	0	3	1	2	0	2	0
Služby míchání mincí	5	0	3	0	0	0	0	2	0	0	1	0	0
Důkazy nulových znalostí	5	3	0	0	0	0	0	3	0	3	0	2	0
Chytré smlouvy	5	0	0	0	0	0	0	3	0	0	0	0	1
Homomorfní závazky	3	3	2	0	0	0	0	2	0	0	0	0	0
Akumulátory	5	3	1	0	0	0	0	3	0	0	0	0	0
Transakce mimo blockchain	4	0	0	0	0	0	0	3	2	0	0	0	0
Váhy	**0,15**	**0,11**	**0,11**	**0,01**	**0,08**	**0,08**	**0,11**	**0,15**	**0,03**	**0,03**	**0,06**	**0,06**	**0,03**

Tabulka 6.8 Vstupní hodnoty pro analýzu bezpečenosti transakcí

Aspekty	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**	**K9**	**K10**	**K11**	**K12**	**K13**
Veřejný blockchain	0,232147	0	0	0	0,301511	0,301511	0,267261	0	0	0	0	0	0
Konsensuální metody	0,154765	0,156174	0,204124	1	0,301511	0,301511	0,534522	0	0,5	0	0	0	0
Hashovací funkce	0,154765	0,312348	0,612372	0	0,904534	0,904534	0,801784	0,381	0	0,267261	0	0	0
Digitální podpisy	0,386912	0,468521	0	0	0	0	0	0,381	0,5	0,534522	0	0,707107	0
Služby míchání mincí	0,386912	0	0,612372	0	0	0	0	0,254	0	0	1	0	0
DNZ	0,386912	0,468521	0	0	0	0	0	0,381	0	0,801784	0	0,707107	0
Chytré smlouvy	0,386912	0	0	0	0	0	0	0,381	0	0	0	0	1
Homomorfní závazky	0,232147	0,468521	0,408248	0	0	0	0	0,254	0	0	0	0	0
Akumulátory	0,386912	0,468521	0,204124	0	0	0	0	0,381	0	0	0	0	0
Transakce mimo BC	0,309529	0	0	0	0	0	0	0,381	1	0	0	0	0
Váhy	**0,15**	**0,11**	**0,11**	**0,01**	**0,08**	**0,08**	**0,11**	**0,15**	**0,03**	**0,03**	**0,06**	**0,06**	**0,03**

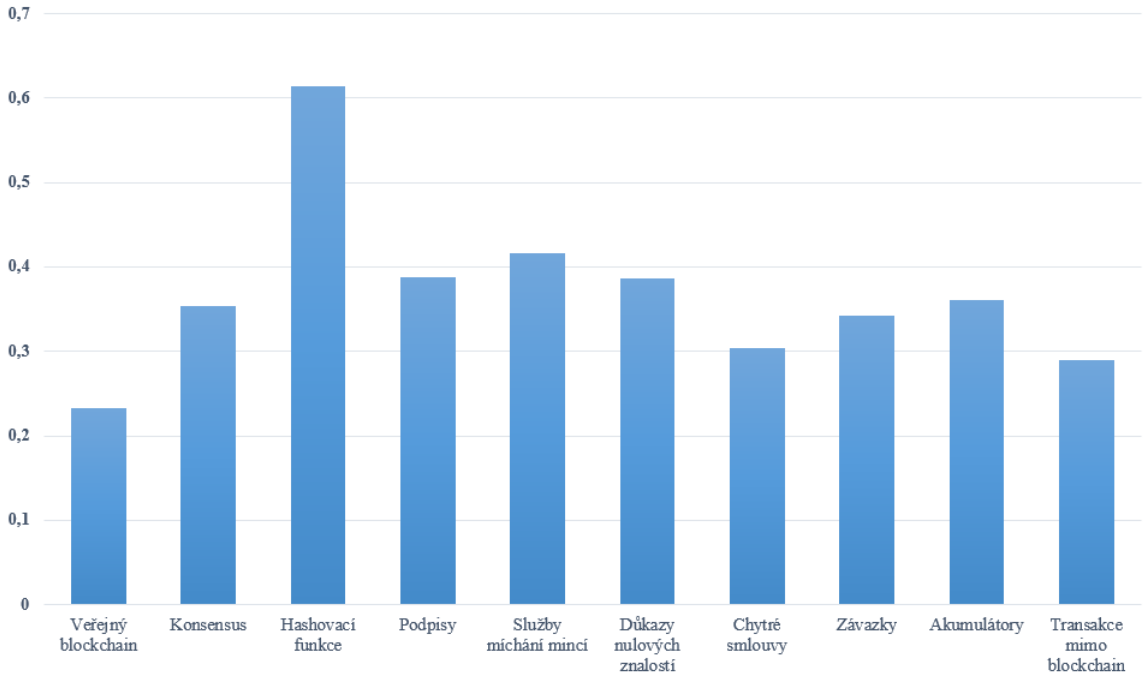
Tabulka 6.9 Normalizovaná matice pro analýzu aspektů bezpečnosti z pohledu celkové bezpečnosti

Aspekty	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**	**K9**	**K10**	**K11**	**K12**	**K13**
Veřejný blockchain	0,03482	0	0	0	0,02484	0,02484	0,0294	0	0	0	0	0	0
Konsensus	0,02321	0,01718	0,02245	0,01	0,02484	0,02484	0,0588	0	0,015	0	0	0	0
Hashovací funkce	0,02321	0,03436	0,06736	0	0,07236	0,07236	0,0588	0,05715	0	0,00742	0	0	0
Podpisy	0,05804	0,05154	0	0	0	0	0	0,05715	0,015	0,01604	0	0,04243	0
SMM	0,05804	0	0,06736	0	0	0	0	0,0381	0	0	0,06	0	0
DNZ	0,05804	0,05154	0	0	0	0	0	0,05715	0	0,02405	0	0,04243	0
Chytré smlouvy	0,05804	0	0	0	0	0	0	0,05715	0	0	0	0	0,03
Závazky	0,03482	0,05154	0,04491	0	0	0	0	0,0381	0	0	0	0	0
Akumulátory	0,05804	0,05154	0,02245	0	0	0	0	0,05715	0	0	0	0	0
Transakce mimo BC	0,04643	0	0	0	0	0	0	0,05715	0,03	0	0	0	0
Váhy	**0,15**	**0,11**	**0,11**	**0,01**	**0,08**	**0,08**	**0,11**	**0,15**	**0,03**	**0,03**	**0,06**	**0,06**	**0,03**
Ideální	**0,05804**	**0,05154**	**0,06736**	**0,01**	**0,07236**	**0,07236**	**0,0588**	**0,05715**	**0,03**	**0,02405**	**0,06**	**0,04243**	**0,03**
Bazální	**0,02321**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Tabulka 6.10 Výpočet hodnot pro jednotlivé aspekty bezpečnosti

Aspekty	Si+	Si-	(Si+) + (Si-)	Pi
Veřejný blockchain	0,192317	0,04725651	0,203008	**0,232782**
Konsensuální metody	0,138909	0,076260216	0,215169	**0,35442**
Hashovací funkce	0,095314	0,151552393	0,246867	**0,613903**
Digitální podpisy	0,152827	0,097046829	0,249873	**0,388384**
Služby míchání mincí	0,145694	0,103932719	0,249626	**0,416353**
Důkazy nulových znalostí	0,154811	0,097538569	0,252349	**0,386522**
Chytré smlouvy	0,167634	0,073341666	0,240976	**0,304353**
Homomorfní závazky	0,18958	0,079120605	0,23148	**0,341803**
Akumulátory	0,154351	0,087403504	0,241755	**0,361538**
Transakce mimo blockchain	0,168036	0,06859423	0,23663	**0,28988**

Tabulka 6.11 Výsledné hodnoty analýzy bezpečnosti kryptoměn



Obrázek 6.1 Výsledky analýzy bezpečnostních aspektů z hlediska celkové bezpečnosti[17)]

Jak ukazuje výsledný graf 6.1 reflektující výsledky TOPSIS analýzy zabezpečení transakcí a samotné kryptoměny, nejlépe z hodnocení vyšly hashovací funkce, které tvoří kryptografický základ každé z kryptoměn. Jak je vidět v tabulce 1.1, která ukazuje jednotlivé hashovací funkce využívané v digitálních měnách, klíčovou funkcí je bezesporu SHA–256, která je v dnešní době standardem co se zabezpečení týče. Řada kryptoměn navíc využívá hashovacích funkcí, jež jsou zaměřeny na zabezpečení systému během těžby. Ať už se jedná o Ethash řešící problém ASIC obvodů, které zvýhodňují dané

[17)] Vlastní zpracování

uživatele během těžby, čímž může dojít k ovládnutí sítě určitou skupinou účastníků, nebo SCrypt či X11 patřící mezi memory-hard hashovací funkce. Velmi využívaným je taktéž RIPEMD160, jenž poskytuje nejkratší hashe, jejichž jedinečnost je stále dostatečně zajištěna. To vede ke snížení délky adresy. Při použití RIPEMD160 je však nutno využít právě SHA–256 z důvodu, že může docházet k jedinečným slabým místům kvůli neočekávaným interakcím mezi RIPEMD a ECDSA. Při srovnání výsledků TOPSIS analýzy a SWOT analýzy v tabulce 6.5 je patrné, že právě hashovací funkce společně s digitálními podpisy zaujaly u bezpečnosti první pozici v obou případech.

Druhým nejužitečnějším aspektem zabezpečení kryptoměn byly dle hodnocení služby míchání mincí. Právě mixing services, v některé literatuře označovány jako tumbler, byly velmi dobře hodnoceny i metodou SWOT. V té byly u silných stránek pojmenovány jako skrytí komunikace, kterou zajišťují, a jejich hodnocení bylo dle významu z hlediska bezpečnosti taktéž na druhém místě právě za hashovacími funkcemi a digitálními podpisy, které byly hodnoceny během TOPSIS analýzy samostatně. Právě digitální podpisy byly vyhodnoceny jako třetí nejužitečnější aspekt pro zabezpečení kryptoměn.

Volitelné kryptografické metody se v první řadě zabývají zajištěním anonymity uživatelů. Bezpochyby jsou však důležitým faktorem pro celkovou bezpečnost systému, což je patrné z výsledného grafu. Velmi vysoko se totiž umístily například důkazy nulových znalostí, které sice u většiny kryptoměn nejsou příliš rozšířené, avšak disponují velkou sadou anonymity, ochrany soukromí a celkově zajišťují bezpečnou komunikaci zúčastněných stran. Právě větší rozšíření důkazů nulových znalostí, ať už zk-SNARKs nebo Bulletproofs, bylo SWOT analýzou v podkapitole 6.1.6 shledáno jako jedna z největších příležitostí pro zlepšení bezpečnosti kryptoměn v budoucích letech.

Velmi podobně se následně umístily akumulátory a homomorfní závazky. První ze zmiňovaných aspektů velmi účinně chrání transakce před ztrátou mincí, kdežto závazky jsou účinné hlavně pro zajištění bezpečné komunikace a soukromí. Naopak nejhůře se v rámci analýzy umístil veřejný blockchain. Ten je sice považován z dostupných blockchainových architektur jako nejbezpečnější, avšak to především díky tomu, že umožňuje využívat výše zmíněné metody pro bezpečnost.

7 Návrh zlepšení

Kryptoměny, a s tím spojený blockchain, jsou poměrně složitými technologiemi, které se neustále vyvíjejí a do současného stavu dospěly velkou řadou úprav a zlepšení. Veškeré nové bezpečnostní opatření a metody vznikají jako odpověď na neustále se zdokonalující kryptografické útoky nebo souvisejí s vývojem nových technologií či dostupností některých funkcí. Návrhy na zlepšení bezpečnosti a anonymity kryptoměn, které jsou prezentovány v této kapitole, vycházejí v první řadě hlavně z analýz popsaných v kapitolách 5 a 6.

1. Rozšíření důkazů nulových znalostí

Pokud jde o možná opatření do budoucna, jako velmi důležité se jeví zejména větší rozšíření důkazů nulových znalostí, které v současné době využívá jen malé procento kryptoměn. Právě důkazy nulových znalostí totiž velmi efektivně nabízejí ochranu soukromí uživatelů, kdy je jedna strana schopna přesvědčit druhou o svém tvrzení, aniž by byla vyzrazena jakákoli citlivá data.

Podle vybraného vzorku kryptoměn v příloze 3.1 využívají kryptoměny častěji modernější verze důkazů nulových znalostí, jimiž jsou Bulletproofs, které na rozdíl od zk-SNARKs využívaných u Zerocash či Zerocoin nevyžadují důvěryhodné nastavení. Právě důvěryhodné nastavení může být slabým článkem důkazů a při jeho ohrožení by mohlo dojít ke ztrátě citlivých údajů a celkovému ohrožení soukromí v blockchainu.

2. Tvorba bezpečnějších konsensuálních metod

Konsensuální metody jsou jádrem blockchainu a právě tato část technologie by měla být dle mého názoru další částí, na které je v budoucnu zapotřebí zapracovat. Vylepšením konsensuálních metod může blockchain lépe čelit útokům jako jsou dvojí útrata, sobecká těžba či úplatky neboli *bribery attacks*. Při návrhu nových konsensuálních metod může být využito například ekonomických teorií jako je takzvaná teorie her. Jedná se o disciplínu z řad aplikované matematiky, během níž dochází k analýze velkého počtu konfliktních rozhodovacích situací, jenž mohou nastat na kterémkoli místě, kde dochází ke střetu zájmů.

Přestože velká energetická náročnost nesouvisí přímo s bezpečností, u některých konsensuálních metod, především tedy u Proof of Work, je rozhodně velkým problém, a mělo by se tudíž pracovat na tvorbě nových, účinnějších a energetický méně náročnějších metod.

3. Ochrana sítě blockchainu

Přestože je blockchain technologie, která je na vzestupu a neustále se rozvíjí, zjednodušeně řečeno jde stále o síť, která čelí stejným problémům, jako jiné sítě. Jedním z opatření, jak snížit útoky na síťovou vrstvu, může být například vytvoření blacklistů a nástrojů pro detekci neobvyklého chování sítě nebo návrhem nových síťových architektur. Právě zabezpečení prostřednictvím blacklistů se u sítí používá poměrně běžně, kdy jsou blokovány buďto nepřátelské nebo jinak škodlivé IP adresy či sítě.

4. Vylepšení ochrany chytrých smluv

Jak v analýze anonymity, tak v analýze celkové bezpečnosti byly chytré smlouvy hodnoceny poměrně malým počtem bodů a v obou případech se ve srovnání s ostatními aspekty umístily na předposlední pozici. V současné době již sice existuje několik metod, které se zabývají zabezpečením chytrých smluv jako je například Hawk, avšak na úrovni kódu by bylo zapotřebí chytré smlouvy vylepšit kontrolou kódu. Poslední výzkumy navíc hovoří o využití technologie hlubokého učení spadající do oblasti strojového učení čili umělé inteligence, což by do budoucna mohlo přinést výrazné zlepšení bezpečnosti.

5. Rozšíření akumulátorů a homomorfních závazků

Homomorfní závazky i akumulátory byly oběma analýzami shledány jako poměrně užitečný aspekt pro zabezpečení systému kryptoměn. Akumulátory slouží ke skrytí identity uživatelů a homomorfní závazky naopak skryjí hodnotu přenášené transakce, čímž chrání proti krádeži mincí. Když se však podíváme na jejich využívání v praxi, které je reflektováno v tabulce 3.1, akumulátory ve svých systémech využívá jen malá část kryptoměn. O trochu lépe jsou na tom sice homomorfní závazky, avšak stále nejsou příliš často využívány.

6. Vylepšení digitálních podpisů

Kvantové počítače by do budoucna mohly být pro technologii blockchainu poměrně značnou hrozbou, kvůli čemuž je zapotřebí posouvat také vývoj digitálních podpisů, které budou kryptoměny před těmito hrozbami chránit. Jak již bylo popsáno v části příležitostí u SWOT analýzy, existuje na rozdíl od běžných digitálních podpisů založených na EDCSA, RSA nebo DSA celá řada metod, které nejsou negativně ovlivňovány kvantovými počítači. Pro příklad se jedná o kryptografiké funkce založené na hashích, kam spadá merkle signature, kryptografické funkce založené na kódu či kryptografii symetrických klíčů.

Problematiku postkvantových počítačů řeší alespoň z části jiný z aspektů bezpečnosti kryptoměn, a sice důkazy nulových znalostí. Přesněji tedy Bulletproofs, jejichž fungování bylo popsáno v části 2.5.2. Jak již však bylo zmíněno, důkazy nulových znalostí nejsou pro zabezpečení kryptoměn zatím příliš rozšířeny.

7. Využívání veřejného blockchainu

Jak odhalila analýza v podkapitole 6.2, veřejný blockchain není sám o sobě příliš silným aspektem pro zajištění soukromí uživatelů ani pokud jde o celkové zabezpečení systému kryptoměn. Přesto je v návrzích na zlepšení zmíněn, a to z toho důvodu, že s vývojem a neustálým rozšiřováním kryptografických a bezpečnostních technologií dokáže právě veřejný blockchain využít tyto aspekty k tomu, aby poskytl co největší ochranu.

Jak již bylo zmíněno u příležitostí v rámci podkapitoly 6.1, veřejný blockchain navíc umožňuje větší zabezpečení i díky většímu počtu uzlů, které tak zajišťují neměnnost technologie. Velkou výhodou je u tohoto typu blockchainu taktéž jeho úplná decentralizace, která právě souvisí s větším počtem uzlů, kdy výpadek a selhání jednoho z uzlů nemá vliv na fungování celé sítě.

8. Využívání pokročilých hashovacích funkcí

V analýze celkové bezpečnosti v podkapitole 6.2 byly nejlépe hodnoceny právě hashovací funkce, které jsou tedy velmi účinným nástrojem zabezpečení. Standardem naprosté většiny současných kryptoměn je podle tabulky 1.1 hashovací funkce SHA-256 velmi často doplněná o RIPEMD160. Poměrně málo jsou však využívané například hashovací funkce pro ochranu před ASIC obvody, které mohou vést k ovládnutí sítě určitou skupinou uživatelů. Mezi tento typ hashovacích funkcí patří ku příkladu Ethash. Co se týče memory-hard hashovacích funkcí jako SCrypt, Equihash či X11, ty jsou v kryptoměnách využívány sice častěji, avšak stále je zde prostor pro větší rozšíření a tím i zajištění větší bezpečnosti systému.

ZÁVĚR

Cílem této práce bylo analyzovat bezpečnostní aspekty kryptoměn z pohledu anonymity uživatelů a celkové bezpečnosti systému. V teoretické části byla nejprve podrobněji rozebrána technologie blockchainu, jakožto základního stavebního kamene kryptoměn. Pro pochopení fungování byly krátce popsány jeho vlastnosti, funkce, architektura a konsensuální metody. Stěžejní pro analýzy byla následující kapitola zaměřená na kryptografické metody a funkce využívané k zabezpečení kryptoměn. Bylo zapotřebí definovat a popsat jednotlivé aspekty, které se podílejí jak na zajištění anonymity uživatelů, tak na celkové bezpečnosti, potažmo bezpečnosti transakcí.

Praktickou část tvořily dvě hlavní analýzy. Tou první byla právě analýza anonymity uživatelů, pro níž byla využita metoda TOPSIS. V případě, že se u daných aspektů vyskytovalo několik možných metod, bylo před celkovou analýzou zapotřebí stanovit, která z metod je pro zajištění soukromí nejvhodnější. Analýza například odhalila, že v rámci digitálních podpisů je nejužitečnější pro zachování anonymity multisignature. Pokud jde o služby míchání mincí, nejlépe hodnocena byla metoda CoinShuffle++. Nejlepší metodou pro důkazy nulových znalostí pak byly vyhodnoceny Bulletproofs. Hodnoty nejlepších metod byly následně využity pro celkovou analýzu, která odhalila nejužitečnější aspekty anonymity. Nejlépe hodnoceny byly služby míchání mincí, které se podílejí na zabezpečení komunikace a chrání před ztrátou mincí. Velmi dobré hodnocení si odnesly taktéž důkazy nulových znalostí a digitální podpisy.

Pro analýzu celkové bezpečnosti kryptoměn byly využity dvě metody, a to metoda SWOT a metoda TOPSIS. První ze zmíněných metod se v první řadě zaměřuje na analýzu rizik v rámci systému kryptoměn. Hodnoceny jsou totiž jak dané aspekty zabezpečení, tak vlastnosti blockchainu, které se na bezpečnosti systému podílejí. Metoda SWOT odhalila kromě silných stránek, kterými jsou například digitální podpisy či hashovací funkce, také stránky slabé a především hrozby, jímž mohou kryptoměny velmi často čelit. V druhé části této kapitoly se metoda TOPSIS zaměřuje už jen na aspekty a metody, které jsou přímo využívány k zabezpečení systému. Nejlepším aspektem pro zabezpečení transakcí byly shledány hashovací funkce, které jsou velmi dobrým a častým nástrojem pro zabezpečení dnešních digitálních měn. Pro celkovou bezpečnost se jako účinné jeví i služby míchání mincí, digitální podpisy nebo důkazy nulových znalostí, což koresponduje s výsledky SWOT analýzy.

Na závěr byly analýzy vyhodnoceny a uvedena doporučení, na jaké oblasti se pro zajištění co nejlepší bezpečnosti zaměřit. Jedná o rozšíření důkazů nulových znalostí či akumulátorů a homomorfních závazků, které současné kryptoměny příliš často nevyužívají. Pomoci by však v budoucnu mohlo také vytvoření nových bezpečnějších konsensuálních metod či zabezpečení blockchainové sítě.

SEZNAM POUŽITÉ LITERATURY

[1] Antonopoulos, A. M.: *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, první vydání, 2014, ISBN 1084-8045, 298 s.

[2] Bedřich, V.: *Největší tržiště na těžbu kryptoměn po hackerském útoku přišlo o 68 milionů dolarů*. Czech Crunch, Prosinec 2017, [Online; navštíveno 21.03.2021].
URL `https://www.czechcrunch.cz/2017/12/nejvetsi-trziste-na-tezbu-kryptomen-po-hackerskem-utoku-prislo-o-68-milionu-dolaru/`

[3] Benedikt Bünz, D. B.-A. P. P. W. G. M., Jonathan Bootle: *Bulletproofs: Short Proofs for Confidential Transactions and More*. Stanford University, [Online; navštíveno 14.03.2021].
URL `https://eprint.iacr.org/2017/1066.pdf`

[4] Bhushan, B.; Sinha, P.; Sagayam, K. M.; aj.: Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers Electrical Engineering*, 2020: str. 106897, ISSN 0045-7906, doi:https://doi.org/10.1016/j.compeleceng.2020.106897.
URL `https://www.sciencedirect.com/science/article/pii/S0045790620307497`

[5] Bit2me: *What are zk-SNARK tests?* Bit2me, [Online; navštíveno 14.03.2021].
URL `https://academy.bit2me.com/en/what-are-zk-snark-tests/`

[6] Chaum, D. L.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM*, ročník 24, č. 2, Únor 1981: str. 84–90, ISSN 0001-0782, doi:10.1145/358549.358563.
URL `https://doi.org/10.1145/358549.358563`

[7] Cheng, R.; Zhang, F.; Kos, J.; aj.: Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS P)*, 2019, s. 185–200, doi:10.1109/EuroSP.2019.00023.

[8] Clemente Galdi, V. K.: *Security and Cryptography for Networks*. Springer, Září 2020, ISBN 978-3-030-57990-6.

[9] Coinbase: *zkSNARKS and Cryptographic Accumulators*. Medium, 2015, [Online; navštíveno 9.02.2021].
URL `https://blog.coinbase.com/zksnarks-and-cryptographic-accumulators-f840da0b61c6#f740`

[10] Ethan Heilman, F. B.-A. S. S. G., Leen AlShenibr: *Ethan Heilman, Leen AlShenibr, Foteini Baldimtsi, Alessandra Scafuro, Sharon Goldberg*. 2017, [Online; navštíveno 12.03.2021].
URL `https://eprint.iacr.org/2016/575.pdf`

[11] Federal Office for Information Security (BSI): *Towards Secure Blockchains*. Březen 2019: str. 92.
URL `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.pdf?__blob=publicationFile&v=3`

[12] Fotr Jiří, S. I.-Š. M. H. S., Vacík Emil: *Tvorba strategie a strategické plánování*. Grada Publishing, Srpen 2012, ISBN 978-80-247-3985-4.

[13] Frankenfield, J.: *Merkle Root (Cryptocurrency)*. Investopedia, Duben 2020, [Online; navštíveno 21.01.2021].
URL `https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp`

[14] Geroni, D.: *How Zero Knowledge Proofs Are Changing Blockchain?* 101 Blockchains, Leden 2021, [Online; navštíveno 14.03.2021].
URL `https://101blockchains.com/zero-knowledge-proof-blockchain/`

[15] Ghassan Karame, E. A.: *Bitcoin and Blockchain Security*. Artech House, Září 2016, ISBN 9781630810139.

[16] Gopie, N.: *What are smart contracts on blockchain?* IBM, Červenec 2018, [Online; navštíveno 12.03.2021].
URL `https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/`

[17] Gupta, R.: *Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain*. Packt Publishing, Září 2018, ISBN 1788990188, 136 s.

[18] Helena Brožová, T. `[U+FFFD]`, Milan Houška: *Modely pro vícekriteriální rozhodování*. Česká zemědělská univerzita, 2014, ISBN 978-80-213-1019-3, 172 s.

[19] Kalodner, H.; Goldfeder, S.; Chen, X.; aj.: Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, MD: USENIX Association, Srpen 2018, ISBN 978-1-939133-04-5, s. 1353–1370.
URL `https://www.usenix.org/conference/usenixsecurity18/presentation/kalodner`

[20] Kędziora, M.; Kozłowski, P.; Szczepanik, M.; aj.: Analysis of Blockchain Selfish Mining Attacks. In *Information Systems Architecture and Technology: Proceedings of 40th Anniversary International Conference on Information Systems Architecture and Technology – ISAT 2019*, editace L. Borzemski; J. Świątek; Z. Wilimowska, Cham: Springer International Publishing, 2020, ISBN 978-3-030-30440-9, s. 231–240.

[21] Kenton, W.: *Off-Chain Transactions*. Investopedia, Únor 2021, [Online; navštíveno 11.03.2021].
URL `https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp`

[22] Kim-Kwang Raymond Choo, R. M. P., Ali Dehghantanha: *Blockchain Cybersecurity, Trust and Privacy*. Springer, Březen 2020, ISBN 3030381803, 413 s.

[23] Kosba, A.; Miller, A.; Shi, E.; aj.: Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, s. 839–858, doi:10.1109/SP.2016.55.

[24] Levy, S.: *Performance and Security of ECDSA*. University of California, Santa Barbara, 2015, [Online; navštíveno 10.02.2021].
URL `http://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Levy.pdf`

[25] Li Peng, Z. Y. Y. L. X. Z. a. S. S., Wei Feng: *Privacy preservation in permissionless blockchain: A survey. Digital Communications and Networks*, 2020, ISSN 2352-8648, doi:https://doi.org/10.1016/j.dcan.2020.05.008.
URL `https://www.sciencedirect.com/science/article/pii/S2352864819303827`

[26] Licheng Wang, J. L. J. S. a. Y. Y., Xiaoying Shen: *Cryptographic primitives in blockchains. Journal of Network and Computer Applications*, ročník 127, 2019: s. 43–58, ISSN 1084-8045, doi:https://doi.org/10.1016/j.jnca.2018.11.003.
URL `https://www.sciencedirect.com/science/article/pii/S108480451830362X`

[27] Luke Valenta, B. R.: Blindcoin: Blinded, Accountable Mixes for Bitcoin. In *International Conference on Financial Cryptography and Data Security*, Berlin: Springer, Září 2015, ISBN 978-3-662-48051-9, s. 112–126, doi:https://doi.org/10.1007/978-3-662-48051-9_9.

[28] Mishra, S.; Kumari, V.; Ojha, N.: Security issues in Blockchain and crypto currency. Duben 2018: str. 13.
URL https://www.researchgate.net/publication/338660128_Security_issues_in_Blockchain_and_crypto_currency

[29] National Institute of Standards and Technology: *Secure Hash Standard (SHS)*. Srpen 2015: str. 36.
URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[30] Nicholas Jansma, B. A.: *Performance Comparison of Elliptic Curve and RSA Digital Signatures*. Duben 2004: str. 20.
URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.7139&rep=rep1&type=pdf

[31] Panagiotis V. Kontogiannis, T. V.: *ECDSA Private Keys Study of Security. Open Access Library Journal*, Červen 2019: str. 19.
URL https://www.researchgate.net/publication/333620250_ECDSA_Private_Keys_Study_of_Security

[32] Powercompare: *Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018*. Powercompare, 2018, [Online; navštíveno 22.02.2021].
URL https://powercompare.co.uk/bitcoin-mining-electricity-map/

[33] Prayag, N.: *DPoS vs PoS: winner takes all.* 2019, [Online; navštíveno 12.02.2021].
URL https://www.etoro.com/news-and-analysis/market-insights/dpos-vs-pos-winner-takes-all/

[34] Qi Feng, S. Z. M. K. K. a. N. K., Debiao He: *A survey on privacy protection in blockchain system. Journal of Network and Computer Applications*, ročník 126, 2019: s. 45–58, ISSN 1084-8045, doi:https://doi.org/10.1016/j.jnca.2018.10.020.
URL https://www.sciencedirect.com/science/article/pii/S1084804518303485

[35] Reiff, N.: *How does a block chain prevent double-spending of Bitcoins?* Investopedia, Leden 2020, [Online; navštíveno 25.03.2021].
URL https://www.investopedia.com/ask/answers/061915/how-does-blockchain-prevent-doublespending-bitcoins.asp

[36] Revision, A.: *Proof-of-Authority consensus*. Apla Revision, 2018, [Online; navštíveno 23.02.2021].
URL https://apla.readthedocs.io/en/latest/concepts/consensus.html

[37] Ruffing, T.; Moreno-Sanchez, P.; Kate, A.: *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin*. Springer, Cham, 2014, ISBN 978-3-319-11212-1.

[38] Rui Yuan, H.-B. C. B.-Y. Z. J. X., Yu-Bin Xia: *ShadowEth: Private Smart Contract on Public Blockchain. Journal of Computer Science and Technology*, ročník 33, 2018: s. 542–556, ISSN 1084-8045, doi:https://doi.org/10.1007/s11390-018-1839-y.

[39] Rui Zhang, R. X. a. L. L.: *Security and Privacy on Blockchain. ACM Computing Surveys*, ročník 52, 2019: str. 34, ISSN 1084-8045, doi:https://dl.acm.org/doi/10.1145/3316481.
URL `https://dl.acm.org/doi/pdf/10.1145/3316481`

[40] Samiappan Dhanalakshmi, G. C. B.: *An ExaminationOf Big Data And Blockchain Technology. International Journalof Innovative Technology and Exploring Engineering*, ročník 8, Září 2019: s. 542–556, ISSN 2278-3075.
URL `https://www.ijitee.org/wp-content/uploads/papers/v8i11/K24970981119.pdf`

[41] Sanka, A. I.; Irfan, M.; Huang, I.; aj.: *A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. Computer Communications*, ročník 169, 2021: s. 179–201, ISSN 0140-3664, doi:https://doi.org/10.1016/j.comcom.2020.12.028.
URL `https://www.sciencedirect.com/science/article/pii/S0140366421000268`

[42] Sigurðsson, G.; Giaretta, A.; Dragoni, N.: *Vulnerabilities and Security Breaches in Cryptocurrencies*. 03 2019, ISBN 978-3-030-14687-0, s. 288–299, doi:10.1007/978-3-030-14687-0_26.

[43] Trustonic: *What is a Trusted Execution Environment (TEE)?* Trustonic, Červenec 2019, [Online; navštíveno 13.03.2021].
URL `https://www.trustonic.com/technical-articles/what-is-a-trusted-execution-environment-tee/`

[44] Wan, Z.; Lo, D.; Xia, X.; aj.: Bug Characteristics in Blockchain Systems: A Large-Scale Empirical Study. In *2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR)*, 2017, s. 413–424, doi:10.1109/MSR.2017.59.

[45] Wen, Y.; Lu, F.; Liu, Y.; aj.: Attacks and countermeasures on blockchains: A survey from layering perspective. *Computer Networks*, ročník 191, 2021: str. 107978, ISSN 1389-1286, doi:https://doi.org/10.1016/j.comnet.2021.107978.

URL https://www.sciencedirect.com/science/article/pii/S1389128621001080

[46] Zcash: *What are zk-SNARKs?* Zcash, [Online; navštíveno 14.03.2021].
URL https://z.cash/technology/zksnarks/

[47] Zibin Zheng, H.-N. D. X. C.-H. W., Shaoan Xie: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Červen 2017.
URL https://www.researchgate.net/publication/292586903_Basic_Aspects_of_Cryptocurrencies

[48] Ziegeldorf, J. H.; Grossmann, F.; Henze, M.; aj.: CoinParty: Secure Multi-Party Mixing of Bitcoins. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, CODASPY '15, New York, NY, USA: Association for Computing Machinery, 2015, ISBN 9781450331913, str. 75–86, doi: 10.1145/2699026.2699100.
URL https://doi.org/10.1145/2699026.2699100

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PoA	Proof of Authority
PBFT	Practical Byzantine Fault Tolerance
SHA	Secure Hash Algorithms
NIST	National Institute of Standards and Technology
MHF	Memory-hard functions
ASIC	Application Specific Integrated Circuit
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
RSA	Rivest–Shamir–Adleman
DSA	Digital Signature Algorithm
NIZKP	Non-Interactive Zero Knowledge Proofs
zk-SNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
SMC	Secure Multi-Party Computation
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
TEE	Trusted Execution Environment
SGX	Software Guard Extension
VM	Virtual Machine
BTC	Bitcoin
XRP	Ripple
SPOF	Single Point of Failure
DNZ	Důkazy nulových znalostí
BC	Blockchain
RIPEMD	RIPE Message Digest

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I. PŘEHLED VYUŽÍVANÝCH HASHOVACÍCH FUNKCÍ V SOUČASNÝCH KRYPTOMĚNÁCH

	SHA256	Ethash	sCrypt	X11-17	Equihash	RIPEMD160	BLAKE	Keccak	Lyra2rev2
Bitcoin	✓					✓			
Ethereum	✓	✓				✓			
Dash	✓			x11					
Litecoin	✓		✓			✓			
Zcash	✓				✓				
Zcoin	✓								
ZILLIQA		✓							
Monero	✓						256	✓	
Ripple	✓					✓			
Nxt	✓		✓			✓			
Blackcoin	✓		✓			✓			
Verge			✓	x17			2smyr-groestl		✓
Qtum	✓	✓				✓			
BitConnect			✓						
Bytecoin	✓						256	✓	
Komodo	✓				✓				
Dogecoin	✓		✓			✓			
Nano							2b		
Byteball	✓								
Electroneum	✓					✓	256	✓	

Tabulka 1.1 Přehled využívaných hashovacích funkcí v kryptoměnách[18)]

[18)] Zpracováno dle lit. Wang (2020)

PŘÍLOHA P II. PŘEHLED VYUŽÍVANÝCH DIGITÁLNÍCH PODPISŮ V SOUČASNÝCH KRYPTOMĚNÁCH

	ECDSA	EdDSA	Ring signature	One-signature	Multi-signature
Bitcoin	✓				✓
Ethereum	✓				
Dash	✓				✓
Litecoin	✓				✓
Zcash	✓			✓	
Zcoin	✓				✓
ZILLIQUA	✓				✓
Monero		✓	✓	✓	
Ripple	✓				✓
Nxt	✓				✓
Blackcoin	✓				✓
Verge	✓				✓
Qtum	✓				✓
BitConnect	✓				✓
Bytecoin		✓	✓	✓	
Komodo	✓			✓	
Dogecoin	✓				✓
Nano	✓				
Byteball	✓				✓
Electroneum		✓	✓	✓	✓

Tabulka 2.1 Přehled využívaných digitálních podpisů v současných kryptoměnách[19)]

[19)] Zpracováno dle lit. Wang (2020)

PŘÍLOHA P III. PŘEHLED OSTATNÍCH KRYPTOGRAFIKÝCH PRIMITIV V SOUČASNÝCH KRYPTOMĚNÁCH

	Homomorfní závazky	Akumulátory	zk-SNARKs	Bulletproofs	Služby míchání mincí
Bitcoin				✓	✓
Ethereum					
Dash					✓
Litecoin					✓
Zcash	✓	✓	✓	✓	✓
Zcoin	✓	✓			✓
ZILLIQUA					✓
Monero	✓			✓	
Ripple					
Nxt					✓
Blackcoin					✓
Verge					✓
Qtum					✓
BitConnect	✓	✓			✓
Bytecoin					✓
Komodo	✓	✓	✓		✓
Dogecoin					✓
Nano					✓
Byteball					
Electroneum	✓				✓

Tabulka 3.1 Přehled ostatních kryptografikých primitiv v současných kryptoměnách[20)]

[20)] Zpracováno dle lit. Wang (2020)