Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

Ing. Lukáš Mastiľák

Autoreferát dizertačnej práce

Architektúra pre správu IP prefixov vo Web3 sieťach

na získanie akademického titulu: „doktor"(„philosophiae doctor“, v skratke „PhD.“)
v doktorandskom študijnom programe: Aplikovaná informatika(2511V00)
v študijnom odbore: Informatika
Forma štúdia: denná
Miesto a dátum: Bratislava, 11.8.2024

Dizertačná práca bola vypracovaná na Ústave počítačového inžinierstva a aplikovanej informatiky Fakulty informatiky a informačných technológií v Bratislave v študijnom odbore aplikovaná informatika.

Predkladateľ: Ing. Lukáš Mastiľák
Ústav počítačového inžinierstva a aplikovanej informatiky
Fakulta informatiky a informačných technológií
Ilkovičová 2, 842 16 Bratislava

Školiteľ: prof. Ing. Ivan Kotuliak, PhD.
Ústav počítačového inžinierstva a aplikovanej informatiky
Fakulta informatiky a informačných technológií
Ilkovičová 2, 842 16 Bratislava

Konzultant: Ing. Kristián Košťál, PhD.
Ústav počítačového inžinierstva a aplikovanej informatiky
Fakulta informatiky a informačných technológií
Ilkovičová 2, 842 16 Bratislava

Autoreferát bol rozoslaný:
Obhajoba dizertačnej práce sa bude konať dňa ..... o ..... h na ústave aplikovanej informatiky Fakulty informatiky a informačných technológií v Bratislave (Ilkovičová 2, 842 16 Bratislava)

prof. Ing. Ivan Kotuliak, PhD.
Dekan FIIT STU Bratislava

Abstrakt

Táto práca sa zameriava na zlepšenie transparentnosti a bezpečnosti v manažmente IP prefixov a ich následnému šíreniu medzi autonómnymi systémami. Problematika je aktuálna z dôvodu blížiaceho sa prechodu na decentralizované služby v rámci ďalšej generácie internetu Web3. Pre zníženie závislosti týchto služieb od centrálnych autorít je potrebné, aby ich infraštruktúra sledovala rovnaké princípy. Aktuálne články sa zaoberajú návrhom použitia distribuovanej účtovnej knihy pre pomocný systém na overenie pôvodcu oznamovaného IP prefixu v internete a na overenie legitímnosti cesty, ktorou sa šíri IP prefix k príjemcovi BGP oznámenia. V tomto prístupe sa overujú prijaté informácie od susedného autonómneho systému voči informáciám zaznamenaných v kontrakte. Tieto riešenia narážajú na problémy, že transakcia nie je včas finálne potvrdená a nepredchádzajú tomu, aby BGP smerovač ohlásil chybnú konfiguráciu. Druhý smer, ktorému sa venujú články je manažment IP prefixov v kontexte prideľovania zdrojov jednotlivým organizáciám. Ich navrhované prístupy neposkytujú dostatočnú modulárnosť v manažmente zdrojov a negarantujú dostatočne unikátnosť a vlastníctvo IP prefixov. Problém predstavuje aj to, že zdroje sú viazané na externé vlastnené kontá, ktoré sú nevyhovujúce pre organizácie, keďže sú spravované iba držiteľom súkromného kľúča a jeho zdieľanie nie je v súlade s bezpečnostnými štandardmi.

Práca, podľa našich najlepších znalostí, obsahuje prvú detailnú analýzu a porovnanie aktuálnych riešení. Následne je rozdelená na dve časti, kde v prvej časti navrhujeme metódu na spoľahlivé overenie pôvodu IP prefixov cez distribuovanú účtovnú knihu, s cieľom zabrániť oznámeniu neplatných IP prefixov pre daný autonómny systém. V druhej časti na základe výskumu navrhujeme architektúru na manažment IP prefixov v kontexte decentralizovanej autonómnej organizácie s cieľom garantovať držanie IP prefixu pomocou nezameniteľných tokenov tzv. NFT. Následne navrhujeme reprezentáciu autonómneho systému resp. organizácie pomocou prístupu *token-bound account* na zjednodušenie manažovania zdrojov. Tento prístup dovoľuje správu zdrojov viacerými administrátormi v rámci organizácie cez jedno konto a zároveň umožňuje prispôsobenie konta potrebám organizácie. Architektúra bola implementovaná a experimentálne overená na testovacích sieťach *Ethereum*, *Polygon* a *ShimmerEVM*. Vykonali sme bezpečnostnú analýzu kontraktov a analýzu nákladov na jednotlivé transakcie v rámci všetkých troch sietí. Nakoniec sme kontrakty formálne overili pomocou nástroja *Certora Prover*.

Abstract

This work focuses on improving transparency and security in managing IP prefixes and their subsequent propagation between autonomous systems. The issue is current due to the impending transition to decentralized services in the next generation of the Internet called Web3. To reduce the dependency of these services on central authorities, its infrastructure needs to follow the same principles. Current works address the proposal of using a distributed ledger for an auxiliary system to authenticate the origin of the IP prefix in the Internet and to verify the path legitimacy by which the IP prefix is propagated to the recipient of the BGP announcement. In this approach, the information received from a neighboring autonomous system is verified against the information recorded in the smart contract. These solutions meet the problem that the transaction finality is not reached in time. The other problem is that it does not prevent the router from announcing the misconfiguration. The second direction discussed in the current works is IP prefixes management in the context of resource assignment to individual organizations. Proposed solutions do not provide sufficient modularity in resource management and sufficiently guarantee the uniqueness and ownership of IP prefixes. The other problem is that resources are tied to externally owned accounts, unsuitable for organizations as they are only managed by the private key holder, and sharing the private key does not comply with security standards.

To the best of our knowledge, this work contains the first detailed analysis and comparison of current solutions. It is divided into two parts. In the first part, we propose a method to reliably verify the origin of IP prefixes through a distributed ledger in order to prevent the propagation of invalid IP prefixes for a given autonomous system. In the second part, based on the research, we propose an architecture to manage IP prefixes in the context of a decentralized autonomic organization in order to guarantee the ownership of an IP prefix using non-fungible tokens. Subsequently, we propose a *token-bound account* to efficiently resource management. This approach allows the management of resources by multiple administrators within an organization through a single account while allowing the account customization to the needs of the organization. The architecture was implemented and experimentally validated on *Ethereum*, *Polygon* and *ShimmerEVM* test networks. We performed contract security analysis and cost analysis across all three networks. Finally, we formally verified the contracts using the *Certora Prover* tool.

Zoznam skratiek

AS	Autonomous System
ASN	Autonomous System Number
ASPA	Autonomous System Provider Authorization
BGP	Border Gateway Protocol
BGPsec	Border Gateway Protocol Security
CVL	Certora Verification Language
DAO	Decentralized Autonomous Organization
DDoS	Distributed Denial of Service
DeIP	Decentralized Internet Protokol
DLT	Distributed Ledger Technology
DNS	Domain name system
ENS	Ethereum Name Service
EOA	Externally Owned Account
ERC	Ethereum Request for Comment
EVM	Ethereum Virtual Machine
EU	European Union
L1	Layer 1
L2	Layer 2
LIR	Local Internet Registry
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ID	Identification Number
IP	Internet Protokol
IGP	Interior Gateway Protocol

IPv4	Internet Protokol verzie 4
IPv6	Internet Protokol verzie 6
IPFS	InterPlanetary File System
ISP	Internet Service Provider
NAT	Network Address Translator
NFT	Non-Fungible Token
NFTAA	Non-Fungible Token as Account
PA	Provider Aggregatable
PBFT	Practical Byzantine Fault Tolerance
PI	Provider Independent
PIT	Public Technical Identifiers
PKI	Public Key Infrastructure
RIPE	Réseaux IP Européens
RIR	Regional Internet Registry
ROA	Route Origin Authorization
RPC	Remote Procedure Call
RPKI	Resource Public Key Infrastructure
RTR	Router
SC	Smart Contract
SSA	Static Single Assessment
TBA	Token Bound Account
TP	Transparent Proxy
UUPS	Universal Upgradeable Proxy Standard

Obsah

Kapitola 1

Úvod

Dnešný systém prideľovania internetových zdrojov, ako IP prefixy a doménové mená, je postavený na hierarchickej infraštruktúre s čiastočným centrálnym riadením. Na čele je IANA, ktorá zodpovedá za globálnu koordináciu internetových zdrojov a pôsobí v rámci neziskovej organizácie ICANN. Pôvodne, IANA bola pod vládou USA a neskôr sa transformovala do organizácie s riadením viacerých zainteresovaných strán *(z angl. multistakeholder)*, ale úplne to nenaplnilo očakávania [1, 2, 3]. Preukázanie vlastníctva internetových zdrojov nie je vždy jednoduché. Druhý problém predstavuje výmena smerovacích informácií pomocou protokolu BGP a zabezpečenie, že tieto informácie sú validné a neboli pri ich šírení porušené smerovacie politiky.

Pôvodný návrh protokolu BGP na výmenu smerovacích informácií medzi autonómnymi systémami nezohľadňuje možné podvody, ktoré môžu nastať pri ohlasovaní ciest. Výsledkom čoho sú incidenty *BGP hijacking* a *Route Leak*. Nemá žiadne mechanizmy na zabezpečenie autorizácie pôvodu ohlásených ciest a overenie skokov, cez ktoré sa cesta šírila. Neskoršie rozšírenia o mechanizmy RPKI *(z angl. Resource Public Key Infrastructure)* a BGPsec *(z angl. Border Gateway Protocol Security)*, ktoré mali garantovať lepšiu bezpečnosť, sa nachádzajú v rôznych štádiách nasadzovania.

Preto sa v posledných rokov niekoľko akademických prác venovalo riešeniu týchto problémov pomocou technológie DLT [4]. Aj keď tieto riešenia priniesli nový pohľad, zameriavali sa buď na manažovanie internetových zdrojov, alebo na overenie oznámenej cesty. Väčšina týchto prístupov bola postavená na súkromnej DLT, čo nemá také výhody voči existujúcemu čiastočne centrál-

nemu prístupu. V prípade, ak nejaké riešenia používali verejnú DLT, málo sa držali existujúcich štandardov pre vývoj decentralizovaných aplikácií a nedostatočne zohľadňovali internetové zdroje ako formu aktíva.

Na základe predchádzajúceho výskumu si stanovujeme dva hlavné ciele. Prvým cieľom je preskúmať distribúciu BGP konfigurácie v rámci AS, aby sme predišli oznámeniu ciest s IP prefixmi ako pôvodca, ktoré nepatria nášmu AS. Druhým cieľom bude preskúmať možnosť manažmentu IP prefixov prostredníctvom decentralizovanej organizácie. V rámci tohto cieľa budeme uvažovať o IP prefixe v kontexte aktíva. Zároveň budeme riešiť, ako reprezentovať AS, s cieľom zjednodušiť správu internetových zdrojov, pretože štandardné účty používateľov v DLT neumožňujú zdieľanie prístupu.

Kapitola 2

Analýza

Aktuálny systém prideľovania internetových zdrojov funguje dobre, ale stále môžu tu byť určité obavy. Čiastočne centralizovaný spôsob riadenia má nasledovné nedostatky:

- ľahšie sa manipuluje systém v prospech nejakého účastníka [5, 6],
- nižšia úroveň transparentnosti,
- auditovateľnosť pre tretie strany je obmedzená.

Z dôvodu dosiahnutia vyššej transparentnosti a auditovateľnosti, bolo by vhodné čiastočne centralizované riadenie internetových zdrojov urobiť viac decentralizované. Zároveň by sa týmto prístupom mohli eliminovať riziká, keď centrálna autorita môže zasiahnuť do prideľovania zdrojov alebo môže byť ovplyvnená štátnou mocou. Pri výmene smerovacích informácií dochádza k útokom *BGP hijacking* alebo *Route Leak*. Preto je potrebný mechanizmus, ktorý nám umožní overiť, že AS je autorizovaný ohlásiť daný IP prefix. Následne je potrebné overiť, či AS, ktorý sa naučil tento IP prefix od suseda a šíri ho ďalej do siete, neporušuje smerovaciu politiku, respektíve dohodnuté obchodné vzťahy so susedmi. Z čoho vyplýva, že potrebujeme overiť každý AS v atribúte *AS path*, ktorý dostaneme v oznámenej ceste.

Identifikované práce, ktoré navrhujú riešenia pre vyššie opísané problémy existujúceho prístupu k manažovaniu internetových zdrojov a overovaniu ohlásených ciest pomocou DLT, sumarizujeme v Tabuľke 2.1. Na základe toho sme dospeli k nasledujúcim zisteniam:

- Centralizovaný prístup môže byť nahradený decentralizovaným prístupom v manažmente

internetových zdrojov. Registrátori a poskytovatelia internetových služieb môžu spoločne participovať na DLT, a tak eliminovať riziká spojené s centralizovaným riadením. Z pohľadu transparentnosti a auditovateľnosti sa javí lepši prístup prostredníctvom verejnej DLT. Problém tu predstavuje škálovateľnosť a ochrana privátnych informácií. Tiež, ktokoľvek sa môže zúčastniť konsenzu, a preto je potrebné, aby pravidlá v SC boli dobre definované a sledovali zamýšľané pravidlá registrátorov. Na druhej strane privátna DLT môže poskytnúť lepšiu kontrolu nad prístupom k dátam a mechanizmus na obmedzenie účastníkov podieľajúcich sa na konsenze. Môže to mať aj negatívny dopad, že sa niektorým účastníkom úmyselne zabráni prístup. Riadením prístupu buď centrálnou autoritou, alebo nejakou skupinou sa znižuje úroveň transparentnosti. Výhoda privátnej DLT je možnosť použitia privátnych dátových kolekcií, keď dáta sú zdieľané iba medzi konkrétnymi entitami alebo šifrované, napríklad platforma Hyperledger. Ale aj tento rozdiel je dnes v rámci verejných DLT pomaly eliminovaný vzhľadom na to, že čím ďalej je viac využívaný *zero knowledge proof*. Ide o dôkaz, keď druhej strane niečo dokážeme bez toho, aby sme jej odhalil dôverný údaj. Vyššia priepustnosť a rýchlejšie dosiahnutie konsenzu sú v prospech privátnej DLT, kým počet validátorov je malá skupina a stabilná. S pridávaním validátorov narastá komplexita komunikácie, čo má negatívny vplyv na celkovú výkonnosť siete. Pri informáciach ako sú internetové zdroje, ktoré sú používané všetkými účastníkmi v internete, by sme sa mali snažiť o najvyššiu možnú úroveň transparentnosti. Použitie privátnej DLT dáva zmysel, ak ide o skupinu účastníkov, kde sa navzájom členovia poznajú, ale nedôverujú si. Zároveň dáta sa týkajú iba tejto skupiny, nie je žiadané ich zdieľať celému svetu, napríklad skupina nejakých firiem, ktoré medzi sebou obchodujú.

- DLT môže poskytnúť úložisko s nemennou históriou pre operácie v manažmente internetových zdrojov, ROA záznamy a dohody medzi poskytovateľmi. Je to skvelý nástroj pre audit incidentov a ktokoľvek môže kedykoľvek overiť pravdivosť informácií. Pri analýze sme zistili, že nie všetky riešenia pracujú s ukladaním dát do DLT optimálne, čo v prípade verejnej DLT zvyšuje transakčné poplatky. Riešenia by mali viac využívať decentralizované úložiská, napríklad IPFS, Arweave a podobne. V niektorých prípadoch stačí iba uložiť dôkaz do DLT pomocou ktorého vieme overiť správnosť údajov na externom úložisku.
- Aktuálne BGP bezpečnostné mechanizmy majú svoje nedostatky a sú nasadzované pomaly. DLT môže poskytnúť podporný systém na overenie oznámenej cesty vrátane pôvodcu IP prefixov, skokov cez AS k aktuálnemu príjemcovi cesty až po dodržiavanie smerovacích

politík. Pri návrhu takého systému je potrebné myslieť na čas trvania konvergencie siete, ak nastane nejaká zmena v ceste. Z čoho vyplýva, že čas schválenia transakcie by mal byť nižší, aby zmena stihla byť doručená cez DLT skôr ako sieť skonverguje.

- Decentralizovaný prístup zvyšuje dostupnosť informácií, čo znamená, že ak nejaký uzol v sieti je nedostupný, tak iný uzol má rovnakú kópiu dát. BGP informácie na overenie prijatých oznámení o cestách sú vždy dostupné od niektorého z uzlov, ktorý udržuje celú kópiu DLT.
- Biznis logika v manažmente internetových zdrojov môže byť prepísaná pomocou SC, čím sa zvýši transparentnosť a nie je potrebná tretia strana pri uzatváraní dohôd. Raz definované podmienky v SC sú nemenné a operácie sa vykonávajú automatický po splnení podmienok.
- Väčšina analyzovaných riešení deklaruje, že môže bežať paralelné s existujúcim systémom, a tak poskytnúť ďalší pomocný nástroj na overenie vymenených smerovacích informácií medzi AS.

Tabuľka 2.1: Porovnanie analyzovaných riešení

Riešenie	**DLT**	**Konsenzus**	**Oneskorenie (s)**	**TPS**	**Priemerná veľkosť TX (B)**
BGPCoin [7]	Ethereum	PoW	25	5	288
InBlock [8]	Ethereum	PoW	18	13	559
ISRchain [9]	Qourum	Raft	2.8	6.62	6.5K
BRVM [10]	Hyperledger	DPoS	3	133	2.56K
BlockJack [11]	Hyperledger	Raft	2.16	-	-
DRRS-BC [12]	Hyperledger	-	9 - 46	39	1 - 5M
VIPAPB [13]	Python chain	PoW	54.7	-	10
RouteChain [14]	-	Clique	54.23	-	-
IPchain [15]	Python chain	PoS	40	10	500
ROAchain [16]	Golang chain	Sharding	73	140	-

Menšia časť analyzovaných riešení je postavená na verejnej DLT, čím zaručujú vysokú transparentnosť a optimalizujú náklady na nasadenie takého riešenia aj za cenu horšej škálovateľnosti. Väčšina projektov stavia na platforme Hyperledger, ktorá umožňuje navrhnúť si vlastnú sieť pre DLT, vybrať si z niekoľkých konsenzuálnych algoritmov a manažovať prístupy do siete. Pri vhodne zvolenom počte validátorov poskytuje aj dobré výsledky v oblasti škálovateľnosti [17]. Posledná skupina riešení sa pokúša navrhnúť DLT riešenie s koncepciou *sharding* alebo

Tabuľka 2.2: Sumarizácia analyzovaných riešení v predchádzaní útokov

	BGP hijacking			**Route Leak**
	Pôvod	**Posledný skok**	**Celá cesta**	
BGPCoin [7]	✓	✓	✗	✗
InBlock [8]	✓	✗	✗	✗
ISRchain [9]	✓	✓	✓	✓
BRVM [10]	✗	✗	✗	✓
BlockJack [11]	✓	✗	✗	✗
DRRS-BC [12]	✓	✗	✗	✗
VIPAPB [13]	✓	✓	✓	✗
RouteChain [14]	✓	✓	✓	✗
IPchain [15]	✓	✗	✗	✗
ROAchain [16]	✓	✗	✗	✗

vlastný konsenzuálny algoritmus s cieľom zlepšiť škálovateľnosť a poskytnúť ideálne riešenie pre BGP.

Internetové zdroje sú iba reprezentované prostredníctvom textového záznamu v DLT. Takýto prístup je obmedzený iba na decentralizované úložisko dát. Bolo by vhodné zvážiť prístup k internetovým zdrojom ako k aktívam, ktoré môžeme tokenizovať. To môže priniesť niekoľko výhod, napríklad dôkaz o unikátnom vlastníctve aktíva, reprezentáciu podielového vlastníctva, monetizovať aktívum alebo vymeniť aktívum. Vzhľadom na to, že podľa našich najlepších zistení neexistuje riešenie postavené na ERC-721 štandarde pre distribúciu IP prefixov, tak najbližšie k takému riešeniu je ENS *(z angl. Ethereum Name Service)*. Je to podobná služba ako DNS *(z angl. Domain name system)*, len sa používa na mapovanie ľudský zrozumiteľných mien na *Ethereum* adresy kont. Majiteľ konta si môže zaregistrovať vlastné meno pod menom najvyššej úrovne *.eth* a získa k svojmu menu NFT, čo slúži ako dôkaz o vlastníctve daného mena. Následne po nastavení záznamu pre adresu konta, môže majiteľ už komunikovať s inými používateľmi alebo decentralizovanými aplikáciami cez registrované meno namiesto adresy konta.

Úroveň overovania ciest sa líši medzi riešeniami od overovania pôvodu IP prefixu v ceste až po overovanie dodržiavania politík medzi AS počas šírenia cesty v sieti. Preto uvádzame v Tabuľke 2.2, voči ktorým útokom dané riešenia môžu pomôcť predchádzať. Spomedzi analyzovaných riešení najlepšiu validáciu ohlásenej cesty poskytlo riešenie *ISRChain* [9]. Bolo by vhodné preskúmať možnosť, či by existoval spôsob ako predísť tomu, aby smerovače neoznamovali IP prefixy, ktoré nepatria ich AS a sú dôsledkom nesprávnej konfigurácie administrátora.

Jedným z hlavných problémov stále zostáva škálovateľnosť. Pre nasadenie DLT v smerovaní

medzi AS je dôležitá priepustnosť a oneskorenie z dôvodu, aby zmeny bolo možné overiť skôr ako sieť skonverguje. Pri vylepšovaní týchto parametrov stále treba dbať na zachovanie bezpečnosti v DLT. Ďalší problém predstavuje optimalizácia ukladania údajov do DLT, aby sme spomalili nárast jej veľkosti a redukovali transakčné poplatky. Čiastočne sa tomu venuje riešenie *BGPcoin* [7], ktoré navrhuje ukladanie agregovaných ROA záznamov a *InBlock* [8], ktoré ukladá iba linku na AS politiky do DLT. Aj prístup *sharding* môže zlepšiť tento problém, keďže celková veľkosť DLT je rozložená medzi menšie podskupiny, kde každá spravuje svoju DLT.

Kapitola 3

Ciele dizertačnej práce

Hlavným cieľom tejto práce je rozšíriť poznanie a využiť nové prístupy v DLT v oblasti manažmentu internetových zdrojov a overenia oznámených ciest.

3.1 Výskumné otázky

Hlavnú otázku tejto práce môžeme formulovať nasledovne: *Ako navrhnúť architektúru pre manažment internetových zdrojov a overenie oznámených ciest s decentralizovaným riadením vo Web3 prostredí?* V rámci tejto otázky definuje tri podotázky, na ktoré chceme hľadať odpovede v našej práci.

1. *Ako zlepšiť garantovanie pôvodu IP prefixov, aby AS neoznámil IP prefixy, pre ktoré nie je autorizovaný pôvodca?*
2. *Bolo by možné považovať IP prefixy za fyzické aktívum, ktoré môže byť reprezentované niektorou z foriem štandardov pre tokeny vo Web3?*
3. *Ako reprezentovať organizáciu, respektíve autonómny systém inou formou ako externým kontom, ktoré môže byť manažované iba držiteľom súkromného kľúča?*

Pri hľadaní odpovedí na tieto výskumné otázky chceme využiť moderné techniky v DLT v kombinácií s našimi znalosťami v oblasti sietí a návrhu architektúry. Naše hlavné tézy sú:

1. **Návrh metódy na spoľahlivé overenie pôvodu IP prefixov** cez DLT v nedôveryhodnom prostredí na zlepšenie bezpečnosti BGP. Cieľom je poskytnúť včas dôveryhodný

a aktuálny záznam o pôvode IP prefixu overovateľovi BGP oznámenia.

2. **Návrh novej architektúry pre decentralizovaný manažment IP adresného priestoru**, v ktorej budú IP prefixy považované za aktívum a reprezentované jedným zo známych štandardov pre tokeny vo Web3.

3. **Vytvorenie abstraktnej reprezentácie autonómneho systému** v navrhnutej architektúre vo Web3 prostredí na efektívny manažment vlastnených aktív s dôrazom na prístup viacerých administrátorov a zmenu vlastníka organizácie.

4. **Vyhodnotenie parametrov škálovateľnosti** (*GAS*, poplatky, počet transakcií v bloku, finalita transakcie, oneskorenie) pre transakcie súvisiace s decentralizovaným manažmentom IP prefixov v navrhnutej architektúre na L1 a L2.

Kapitola 4

Spoľahlivé overenie pôvodu IP prefixov cez blockchain

Táto kapitola navrhuje metódu pre spoľahlivé overenie pôvodu IP prefixov prostredníctvom blockchainu s cieľom zvýšiť bezpečnosť BGP. Zameriava sa na prvú tézu a hľadá odpoveď na prvú otázku v kapitole 3.1.

Analyzované riešenia sú postavené na princípe, že overujú prijaté cesty od susedov voči informáciám uloženým v blockchaine, čo sa môže stretnúť s problémom týkajúcim sa finálneho potvrdenia transakcie. Preto nás riešenie [18] viedlo k myšlienke, aby sme nielen overovali prijaté informácie voči už uloženým informáciám v blockchaine, ale aby sa zariadenia časť konfigurácie naučili z blockchainu, čím sa dá predísť chybám konfigurácie a zároveň zabezpečiť, že informácie budú včas dostupné.

Cieľom navrhovanej metódy je predísť náhodnej chybe spôsobenej konfiguráciou administrátora alebo pred neúmyselným falošným ohlásením IP prefixu. Tento prístup jednak umožňuje overiť pôvodcu IP prefixov a zároveň motivuje AS distribuovať časť BGP konfigurácie cez blockchain, a tak predísť chybám. Na druhej strane, ak príjemca nevie overiť pôvodcu IP prefixu v blockchaine, tak môže takúto oznámenú cestu odmietnuť. Zároveň treba citlivo zvážiť, ktoré informácie môžu byť uložené v blockchaine z konfigurácie a ktoré by nemali byť z dôvodu tajného obsahu AS.

4.1 Návrh metódy

Metóda pozostáva z dvoch častí, kde najprv sa vytvorí dôveryhodný a nemeniteľný záznam o tom, kto je autorizovaný oznámiť IP prefix ako pôvodca, tzv. ROA záznam. To je vykonávané prostredníctvom súboru kontraktov, ktoré sledujú aktuálnu hierarchickú štruktúru prideľovania IP prefixov. Druhá časť metódy pozostáva z distribúcie časti konfigurácie pre *eBGP* smerovače daného AS prostredníctvom blockchainu. To znamená, že časť konfigurácie bude zaznamenaná pre konkrétne smerovače v blockchaine, odkiaľ ju následne získajú. Toto sa bude týkať tej časti konfigurácie, ktorá špecifikuje IP prefixy, ktoré smerovač musí oznamovať spolu s lokálnym ASN. Cieľom je zabezpečiť, aby *eBGP* smerovače oznámili svojím susedom so svojím ASN iba také IP prefixy, ktoré je autorizované ohlasovať ich AS. Transakcia s konfiguráciou od administrátora AS sa overuje voči vytvorením ROA záznamom. Až po úspešnom overení sa vytvorí nový záznam v blockchaine.

Súčasťou infraštruktúry AS je bod, ktorý bude zabezpečovať komunikáciu s blockchainom, sledovať nové dostupné aktualizácie pre všetky *eBGP* smerovače v rámci AS, sťahovať konfigurácie a nasadzovať na zariadenia. Na Obrázku 4.1 je sekvenčný diagram, ktorý zobrazuje interakciu medzi jednotlivými účastníkmi a proces od vytvorenia ROA až po bod, keď si smerovač stiahne poslednú verziu časti konfigurácie pre BGP.

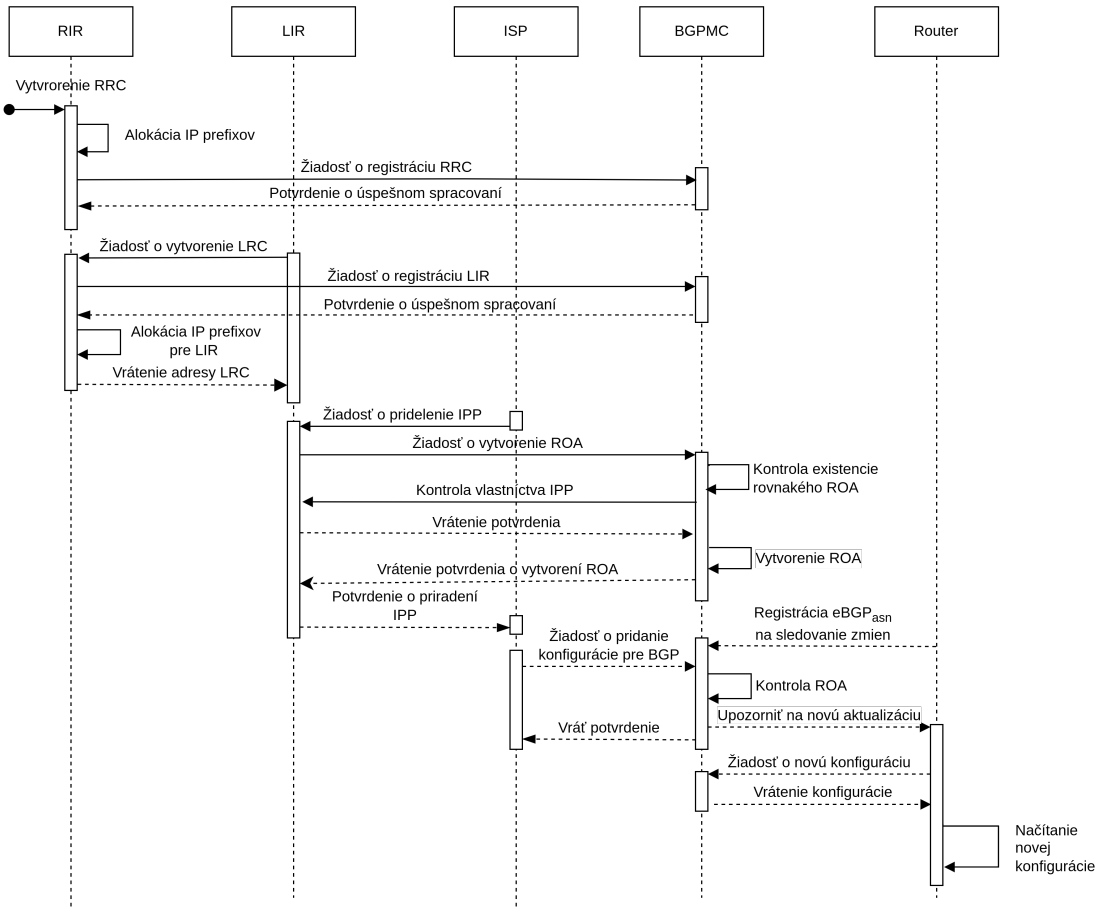
4.2 Overenie

Riešenie bolo overené v testovacom prostredí, ktoré pozostávalo z troch virtuálnych strojov v rôznych geografických lokalitách s operačným systémom Ubuntu Server 20.04 LTS. Na Obrázku 4.2 je návrh prostredia pre distribúciu BGP konfigurácie. Každý zo strojov prezentoval jedného z účastníkov RIR, LIR a ISP. Súbor kontraktov bol nasadený na sieti Ropsten, čo je testovacia sieť pre Ethereum. Priemerná dĺžka nastavenia ROA záznamu bola 35 s.

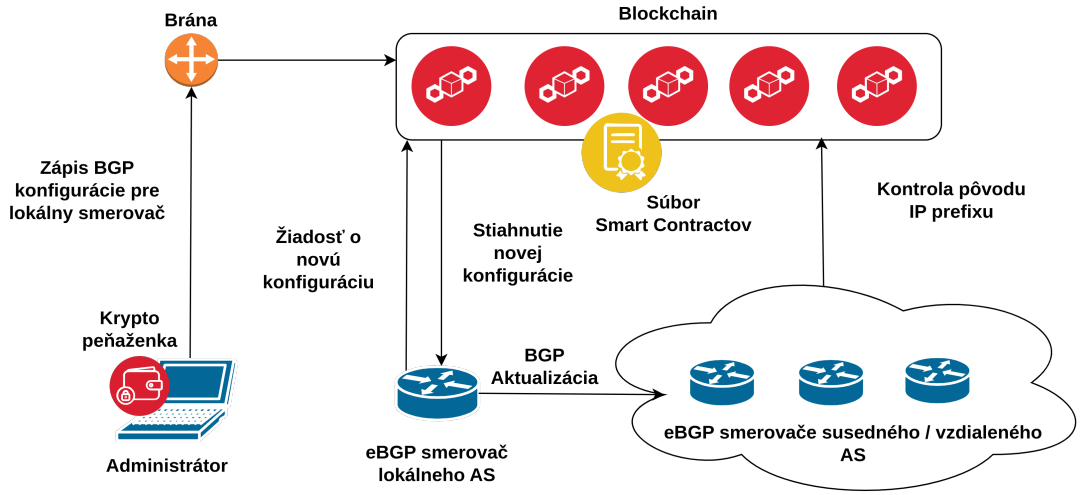
Vykonali sme 100 meraní trvania nahratia novej časti konfigurácie pre BGP s IP prefixmi, ktoré by mal smerovač oznamovať svojím susedom. Priemerný čas trvania tejto transakcie bol 37,5 s a medián bol 34,7 s, ako môžeme vidieť na Obrázku 4.3.

Tiež, sme skúmali spotrebu *GAS* v závislosti od počtu IP prefixov zoskupených do jednej transakcie. Na Obrázku 4.4 je zobrazená spotreba *GAS*.

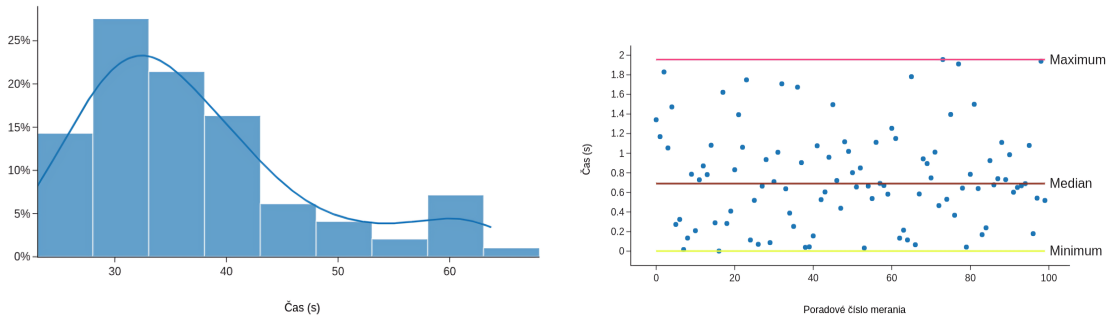
Interval vytvorenia nového bloku v sieti Ethereum ovplyvňuje nasadenie novej konfigurácie a



Obr. 4.1: Sekvenčný diagram zobrazuje vytvorenie ROA záznamu a stiahnutie aktuálnej konfigurácie smerovača



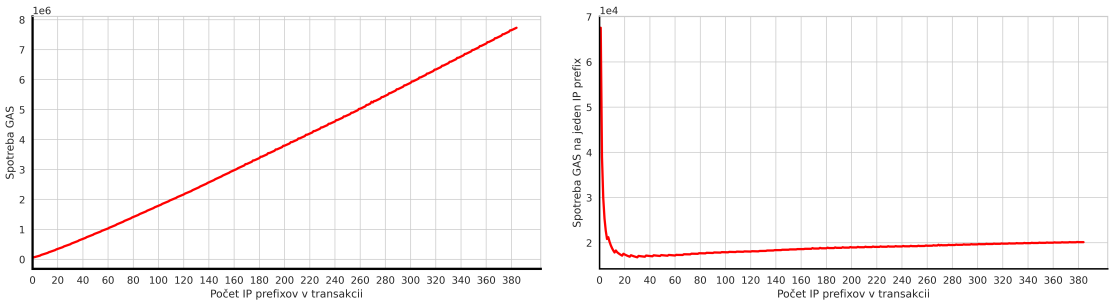
Obr. 4.2: Návrh prostredia pre distribúciu BGP konfigurácie cez blockchain



(a) Distribúcia výsledkov nastavenia konfigurácie s IP prefixmi na smerovači

(b) Trvanie stiahnutia a načítania novej konfigurácie

Obr. 4.3: Operácia nastavenia novej konfigurácie pre BGP na smerovači



(a) Spotreba *GAS* vzhľadom na rôzny počet IP prefixov

(b) Spotreba *GAS* prepočítaná na jeden IP prefix

Obr. 4.4: Spotreba (*GAS*) pre transakciu nahratia konfigurácie BGP pre smerovač

šírenie aktualizácií. Navyše, naša transakcia nemusí byť ťažiarmi spracovaná v najbližšom vytváranom bloku, ale v niektorom z nasledujúcich blokov. Celkové trvanie nasadenia novej časti BGP konfigurácie na smerovač môžeme vyjadriť pomocou vzorca 4.1.

$$\begin{aligned} \textit{priemerný celkový čas(s)} &= \textit{pridanie ROA} + \textit{pridanie konfigurácie} + \\ &\quad + \textit{stiahnutie a načítanie konfigurácie} \\ \textit{priemerný celkový čas} &= 35 + 37{,}5 = 72{,}5\ s \end{aligned} \tag{4.1}$$

Z pohľadu garantovania stavu v sieti by sme mali správne ešte po každej transakcií počkať 6 nasledujúcich blokov pre finálne potvrdenie transakcie v Ethereum. Nový blok pribúda priemerne každých 12 s. Potom celkový čas aj s finálnym potvrdením transakcií je približne 176,5 s.

4.2.1 Známe obmedzenia

Medzi známe obmedzenia patrí:

- navrhnutá metóda nezohľadňuje techniku *BGP blackholing*, ktorá sa často využíva pri zmierňovaní DDoS útokov,
- peňaženka vlastnená iba jednou osobou,
- strata súkromného kľúča a seed frázy k peňaženke vedie k trvalej strate držaných zdrojov,
- vykonávanie niektorých operácií iba centrálnymi autoritami ako registrátori,
- veľkosť bloku limituje veľkosť zaznamenanej konfigurácie.

Kapitola 5

Decentralizovaná autonómna organizácia pre manažment IP prefixov

Táto kapitola sa venuje návrhu architektúry pre decentralizovaný manažment IP adresného priestoru. Prvá časť predstavuje návrh architektúry s reprezentáciou IP prefixov pomocou jedného zo štandardov pre tokeny vo Web3 prostredí. Zameriava sa na druhú tézu a hľadá odpoveď na druhú otázku v kapitole 3.1.

5.1 Návrh architektúry

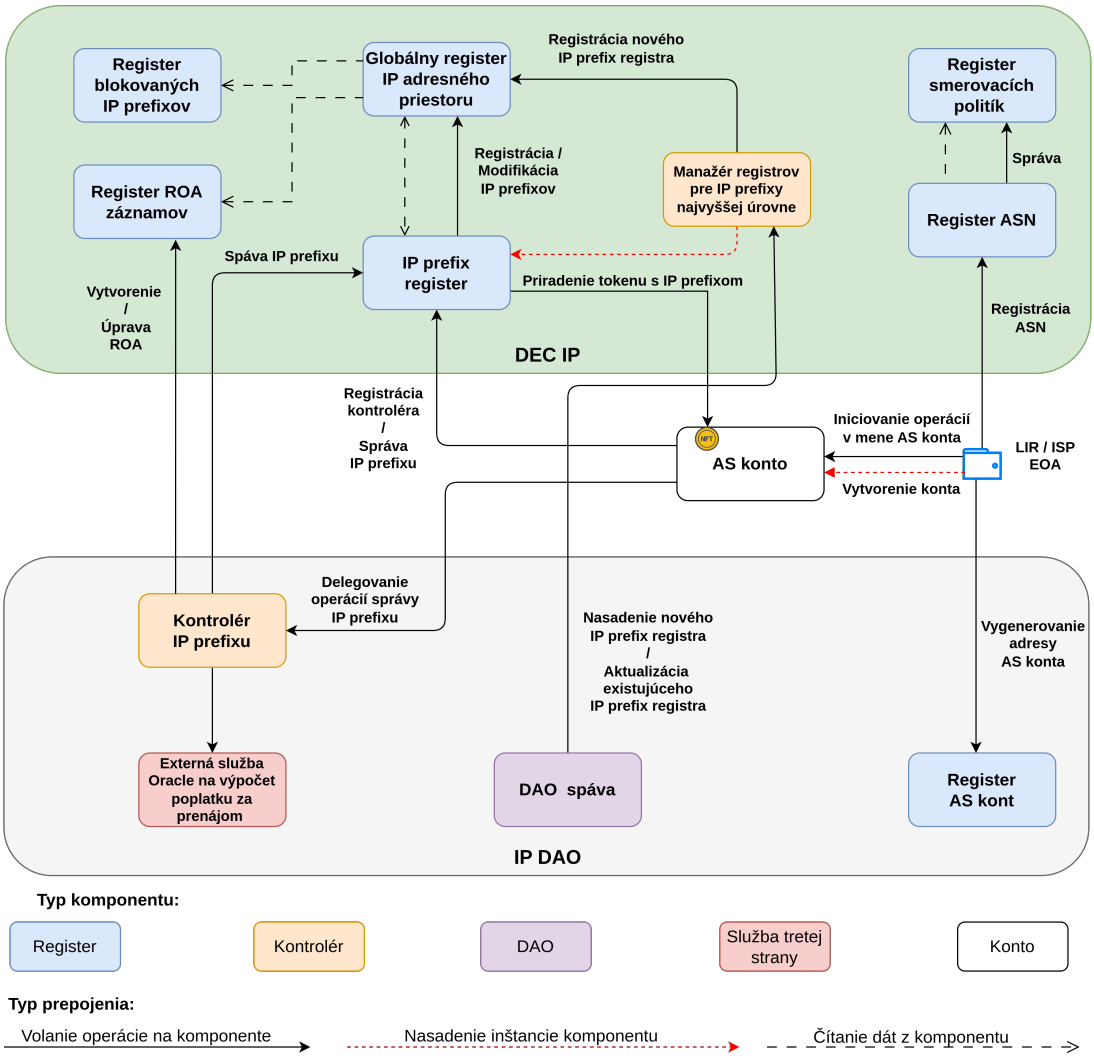
Na obrázku 5.1 je zobrazená navrhovaná architektúra pre decentralizovaný manažment internetových zdrojov prostredníctvom DAO. Skladá sa z dvoch častí označených ako *DEC IP* a *IP DAO*. *DEC IP* poskytuje infraštruktúru, definuje pravidlá a garantuje bezpečnosť pre vytváranie a manažovanie IP prefixov prostredníctvom tokenov. Tiež, definuje spoločné rozhranie na komunikáciu s inými decentralizovanými aplikáciami alebo používateľmi. Druhá časť, *IP DAO*, obsahuje komponent, ktorý definuje pravidlá na riadenie zmien v *DEC IP*. Primárne to zahŕňa prijímanie rozhodnutí o budúcom smerovaní protokolu a vykonávanie aktualizácií na základe konsenzu celej komunity. Ďalej zabezpečuje vytváranie účtov pre AS. Každý typ komponentu môže byť tvorený

jedným SC alebo skupinou niekoľkých SC-ov, závisí to od funkcionality komponentu a navrhnutej implementácie. V nasledujúcej časti si opíšeme konkrétne komponenty našej architektúry:

- **Globálny register IP adresného priestoru** - mapuje IP prefixy a SC adresy registrov, ktoré zaregistrovali a kontrolujú IP prefixy.
- **Register blokovaných IP prefixov** - uchováva zoznam IP prefixov, ktoré sú na čiernych listinách z rôznych príčin, napríklad spam.
- **Register ROA záznamov** - udržuje pre každý IP prefix zoznam platných ROA záznamov.
- **IP prefix register** - prideľuje a manažuje IP prefixy s menším rozsahom z IP prefixu najvyššej úrovne.
- **Manažér registrov pre IP prefixy najvyššej úrovne** - registruje, nasadzuje a aktualizuje kontrakty pre IP prefixy najvyššej úrovne.
- **Register ASN** - registruje a prideľuje ASN externe vlastneným účtom.
- **Register smerovacích politík** - pre každé AS udržuje vzájomný biznis vzťah s každým jeho susedom.
- **Kontrolér IP prefixu** - voliteľný komponent, ktorý si môže zaregistrovať vlastník alokovaného IP prefixu na jeho manažment a zároveň môže definovať pravidlá, ako môžu získať od neho IP prefix ostatní používatelia.
- **Externá služba Oracle** - zabezpečuje výpočet poplatkov za prenájom IP prefixu na základe dát získaných z viacerých WEB2 zdrojov.
- **DAO správa** - skupina kontraktov, ktorá definuje pravidlá na riadenie zmien v protokole. Navyše, uvádza proces prijímania návrhov, hlasovania o návrhoch a vykonávania prijatých návrhov.
- **Register AS kont** - vypočíta adresu konta pre AS na základe adresy SC, ktorý opisuje správanie AS konta, a ASN tokenu.
- **AS konto** - SC, ktorý definuje správanie a funkcionalitu AS konta.

5.1.1 Globálny register IP adresného priestoru

Tento komponent uchováva najdôležitejšie adresy súvisiace s každým IP prefixom. Návrh tohto registra je inšpirovaný návrhovým vzorom register zmlúv *(z angl. Contract Registry)* [19]. Jeho

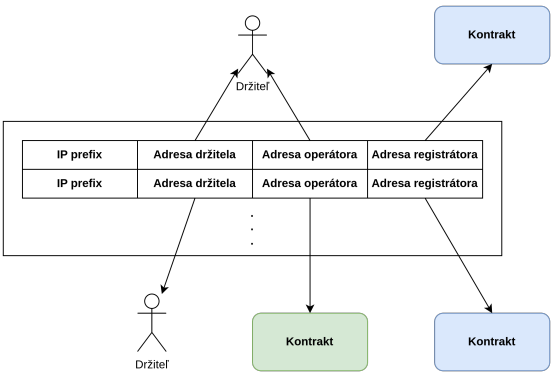


Obr. 5.1: Architektúra pre decentralizovaný manažment IP adresného priestoru

cieľom je uľahčiť aktualizáciu SC a minimalizovať počet SC adries, ktoré si je potrebné pamätať. Mapuje symbolické meno s adresou kontraktu pre IP prefix. V našom prípade symbolické meno je vyjadrené pomocou IP prefix formátu v textovom reťazci:

$$adresa\ siete + dĺžka\ prefixu$$

Formát mapovania v globálnom registri je znázornený na Obrázku 5.2.



Obr. 5.2: Štruktúra globálneho registra IP adresného priestoru

5.1.2 Manažment IP prefixov

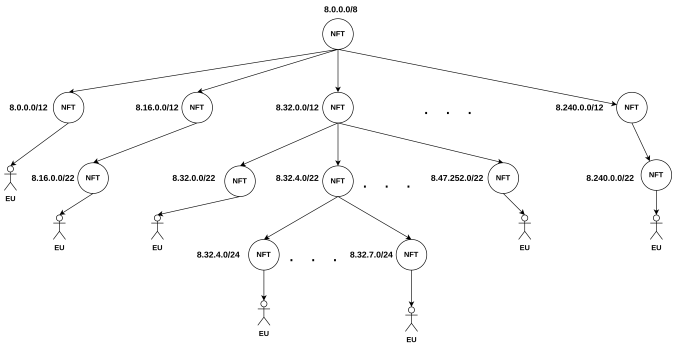
V tejto časti sa zameriame na reprezentáciu IP prefixov pomocou tokenov, alokáciu a prideľovanie IP prefixov. Všetky súvisiace procesy sú zabezpečované prostredníctvom komponentov *Manažér registrov pre IP prefixy najvyššej úrovne* a *IP prefix register*.

5.1.2.1 Tokenizácia

Jeden z cieľov, ktorý sme si stanovili, je reprezentácia IP prefixu ako digitálneho aktíva pomocou jedného zo štandardov pre tokeny. Na základe analýzy sme vyhodnotili ako najvhodnejšie riešenie štandard ERC-1155, a to primárne kvôli flexibilite, ktorú poskytuje a podpore vytvárania viacerých tokenov v transakcii. Každý token má pridelený unikátny 256 bitový číselný identifikátor v rámci SC, ktorý sa získa spôsobom, že sa zoberú štyri bajty sieťovej adresy a spoja s dĺžkou prefixu. Následne nám vznikne päť bajtová hodnota, z ktorej sa vypočíta haš pomocou kryptografickej funkcie *keccak256*.

5.1.2.2 Hierarchické prideľovanie

Naša navrhnutá architektúra implementuje prideľovanie IP prefixov v podobe NFT tokenov v niekoľkých úrovniach. Navyše, s každým tokenom sa spája pole príznakov, ktoré určuje danému držiteľovi právomoci v rámci manažovania IP prefixu, napríklad právomoc subalokovať. Na Obrázku 5.3 je zobrazená štruktúra prideľovania tokenov.



Obr. 5.3: Štruktúra prideľovania IP prefixov pomocou NFT

Vytvorenie tokenu nižšej úrovne závisí od vlastností tokenu vyššej úrovne. Z čoho vyplýva, že token vyššej úrovne musí byť validný a príznaky pre nový token nesmú byť v rozpore s jeho príznakmi. Z týchto dôvodov je nevyhnutné udržiavať si vzťahy medzi tokenmi, aby sme sa vedeli stále pri danom IP prefixe opýtať na stav tokenu o úroveň vyššie. K riešeniu tohto problému nás nasmeroval štandard ERC-5521[1], ktorý opisuje tzv. odkazovateľné NFT *(z angl. Referable NFT)* [20].

5.1.2.3 Príznaky

Ďalší mechanizmus, ktorý sme využili v rámci navrhovanej architektúry sú príznaky na riadenie právomocí pre držiteľov tokenov. V tomto prípade sme sa inšpirovali podobným mechanizmom, ktorý používa služba ENS na mapovanie ľudsky vysloviteľných mien pre *Ethereum* adresy na vytváranie subdomén [21]. Pri prideľovaní IP prefixu sú tieto príznaky nastavované tvorcom tokenu, čo je držiteľ alebo kontrolér tokenu pre IP prefix, z ktorého adresného priestoru sa vykonáva pridelenie.

[1] `https://eips.ethereum.org/EIPS/eip-5521`

5.1.2.4 Exspirácia

V našom návrhu uvádzame pre každý token atribút exspirácia, ktorý umožňuje prideliť každý IP prefix na rôzne dlhú dobu, čo je založené na ERC-5643[2]. Tento štandard rozširuje NFT o rozhranie modelu predplatného s možnosťou pravidelnej obnovy. Po uplynutí ochrannej lehoty držiteľ stráca definitívne vlastníctvo a pre daný IP prefix bude vrátená genesis adresa 0x0 ako vlastník od SC *IP prefix register*.

5.1.3 Abstraktná reprezentácia identity AS

V tejto časti sa zameriame na tretiu tézu a hľadanie odpovede na tretiu otázku v 3.1, ktorá sa týka abstraktnej reprezentácie identity AS. Tento pojem definuje, ako reprezentovať konto pre AS na efektívnu správu jeho vlastnených zdrojov vo Web3 prostredí. Štandardne, účastníci na interakciu s decentralizovanými aplikáciami potrebujú mať vytvorené EOA, ktoré poznáme aj ako kryptopeňaženka. Takéto konto je v plnej správe jeho vlastníka. Na vytvorenie transakcie je potrebný podpis súkromným kľúčom vlastníka daného konta. V prípade organizácií, veľakrát v mene nich koná niekoľko rôznych entít. Z pohľadu bezpečnosti je zakázané zdieľať súkromný kľúč alebo *seed* frázu, ktorá je potrebná na importovanie konta do vlastnej peňaženky. Z týchto dôvodov reprezentácia organizácie prostredníctvom takého typu konta nie je vyhovujúca. Na základe toho je potrebné reprezentovať konto iným spôsobom pre AS, aby sme uľahčili správu aktív, ktoré môže také konto držať.

Najjednoduchším prístupom k reprezentovaniu unikátnej identity vo WEB3 je použitie NFT. Takýto prístup umožňujú riešenia TBA[3] *(z angl. Token-bound Account)* a NFTAA *(z angl. Non-Fungible Token as Account)* [22]. Na základe analýzy týchto dvoch riešení sme pre našu architektúru vybrali riešenie TBA. Medzi hlavné dôvody pre výber TBA patrí jeho univerzálnosť a možnosť úplného prispôsobenia implementácie konta. Navyše, správa aktív medzi rôznymi DLT je výhodou, napríklad pri optimalizácii poplatkov. Okrem toho, v čase návrhu tejto architektúry bola verejne dostupná referenčná implementácia TBA narozdiel od NFTAA.

5.1.3.1 Návrh kontraktu pre konto

Dôležitým komponentom TBA je kontrakt pre konto, ktorý definuje správanie nášho konta. V našom prípade je nevyhnutné, aby takéto konto umožňovalo vlastníkovi NFT ku kontu zjedno-

[2] `https://eips.ethereum.org/EIPS/eip-5643`
[3] `https://eips.ethereum.org/EIPS/eip-6551`

dušiť proces manažmentu IP prefixov. Preto navrhujeme mechanizmus disponentov pre konto. Vlastník NFT môže udeliť inej adrese možnosť vykonávať operácie v mene konta. Navyše môže limitovať právomoci pre danú adresu.

Ak predpokladáme, že dané konto reprezentuje konkrétne ASN, tak všetky vykonané transakcie v mene tohto konta budú vykonané z adresy, ktorá bola pridelená NFT. Napriek tomu, že v rámci konta môžu iniciovať transakcie rôzni používatelia, tak všetky transakcie sa budú dať vyhľadať v histórii DLT z rovnakej iniciovanej adresy, čo poskytuje nemenný dôkaz o histórií všetkých operácií pre jednu organizáciu respektíve konto.

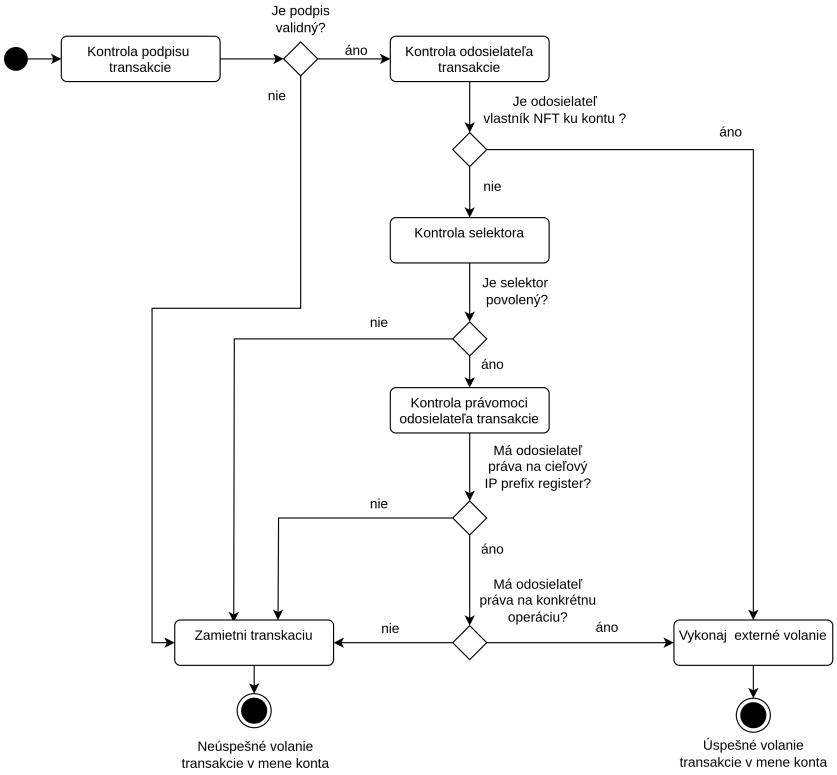
Vlastník NFT ku kontu má právo pridať, odstrániť a upraviť právomoci konkrétneho disponenta. Každý disponent je reprezentovaný pomocou nasledujúcich atribútov:

- ***index*** - uchováva poradové číslo v zozname autorizovaných disponentov,
- ***state*** - určuje stav daného disponenta, či je aktivovaný alebo pozastavený,
- ***permsExtCalls*** - ukladá zoznam povolených volaní.

Atribút *permsExtCalls* predstavuje mapu, ktorá pre adresy kontraktov *IP prefix registrov* ukladá zoznam povolených volaní. Tento zoznam je reprezentovaný pomocou šestnásť bitovej premennej, kde každý bit je mapovaný na jeden selektor funkcie v zozname povolených volaní. Celý proces kontroly, či daný iniciátor môže vykonať volanie v mene konta, je opísaný aktivity diagramom na Obrázku 5.4.

Obmedzenie takto navrhnutého konta je v tom, že vieme manažovať povolenia disponentov iba na úrovni *IP prefix registrov*. Vzhľadom na to, že vstupné parametre *execute* funkcie podľa štandardu ERC-6551 obsahujú iba cieľový kontrakt, množstvo Ether, kódované volanie na cieľový kontrakt a typ operácie, tak nie je možné bližšie určiť, ktorého IP prefixu sa bude týkať cieľové volanie.

Iný nedostatok, ktorý uvádza aj samotný štandard a necháva ho na riešenie samotnému používateľovi, nastáva pri transfere NFT. V čase, keď NFT drží aktíva na konte, tak vlastník NFT sa môže dohodnúť na transfere NFT na nového vlastníka. Nový vlastník je v tom, že získa NFT aj s príslušnými aktívami, ktoré drží. Pôvodný vlastník sa môže zachovať nečestne a ešte pred schválením tejto transakcie vložiť transakciu, ktorá prevedie aktíva na inú adresu. V tom prípade, ak by táto transakcia bola schválená včas, nový vlastník získa NFT bez aktív. Na riešenie tohto problému zavádzame v návrhu implementácie konta zámok, ktorý je potrebné zamknúť pred



Obr. 5.4: Proces overenia iniciátora na vykonanie transakcie v mene konta.

transferom NFT ku kontu. Po zamknutí konta nie je možné vykonať žiadnu operáciu, ktorá mení stav konta, ktorý je sledovaný pomocou premennej *nonce*. Samotný *Register ASN* kontroluje pri transfere NFT, či je konto zamknuté a iba v takom prípade umožní zmenu vlastníka.

5.2 Experimentálne overenie riešenia

V tejto časti budeme opisovať overenie kľúčových komponentov navrhnutej architektúry pre manažment IP prefixov cez DAO. Na získanie experimentálnych dát sme sa rozhodli implementovať prototyp s najdôležitejšou funkcionalitou.

5.2.1 Implementácia prototypu

Implementácia prototypu bola rozdelená do štyroch častí a obsahovala nasledujúce kontrakty:

- **ERC6551** - ERC6551Registry (prebraté z referenčnej implementácie ERC6551[4]),
- **IPGlobalRegistry** - IPv4GlobalAddrRegistry,
- **IPPrefix** - ERC1155Registry, IPPrefixRegistry,
- **IPAccount** - ERC721Registry, ASNRegistry, ASAccount.

5.2.2 Bezpečnostná analýza

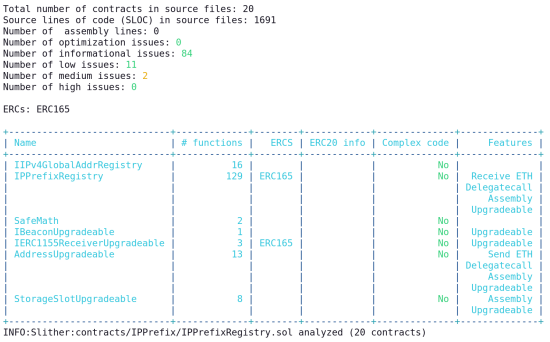
Dôležitým aspektom pri návrhu a potom pri samotnom implementovaní kontraktov je myslieť na bezpečnosť samotného kódu. Zanedbanie tohto môže viesť k tomu, že skryté zraniteľnosti budú zneužité útočníkom v produkcii. Z týchto dôvodov sme pri implementovaní prototypu vykonali statickú a dynamickú analýzu kódu pomocou nástrojov *Slither*[5] a *Mythril*[6] na detekciu potenciálnych zraniteľností.

Statická analýza sa používa na detekciu zraniteľnosti v kóde bez jeho vykonania. Na statickú analýzu sme zvolili nástroj *Slither*, ktorý rozdeľuje zraniteľností do viacerých kategórií podľa úrovne závažnosti. Väčšina identifikovaných zraniteľnosti mala iba informačnú alebo nízku úroveň závažnosti. Výsledky sú zobrazené na Obrázkoch 5.5 a 5.6. Identifikovali a následne sme opravili zraniteľnosti, ako napríklad *Re-entrancy*. Tiež sa vyskytli upozornenia na zraniteľností

[4] `https://github.com/erc6551/reference`
[5] `https://github.com/crytic/slither`
[6] `https://github.com/Consensys/mythril`

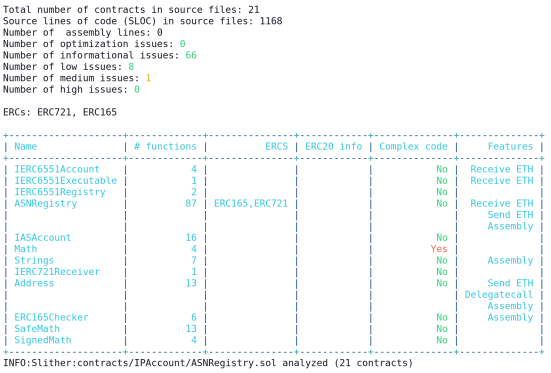
block.timestamp alebo na niektore častí knižnice *Math*, ale tieto zraniteľnosti nemali žiaden vplyv naše kontrakty.

(a) *Globálny register IP adresného priestoru*

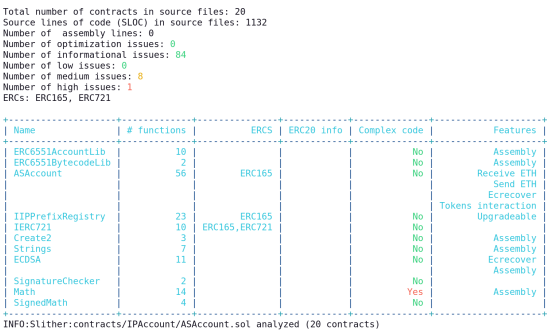


(b) *IP prefix register*

Obr. 5.5: Výstup statickej analýzy *Slither* pre IP prefix



(a) *ASN register*



(b) *AS konto*

Obr. 5.6: Výstup statickej analýzy *Slither* pre AS

Na dynamickú analýzu sme použili nástroj *Mythril*, ktorý vykonáva detekciu zraniteľnosti pomocou symbolického vykonávania. Ide o prístup zistiť, aké vstupy spôsobujú vykonávanie jednotlivých častí kontraktu. Analýzu sme vykonali rovnako pre všetky štyri kontrakty ako v prípade statickej analýzy. Skúšali sme aj rôzny počet transakcií okrem prednastaveného počtu 3. Žiadne nové zraniteľnosti neboli detegované okrem tých, ktoré sme opísali pri statickej analýze. Detegoval iba použité *block.timestamp* v rozhodovacích blokoch s nízkou úrovňou závažnosti.

5.2.3 Analýza spotreby GAS

Poplatky za spracovanie transakcií hrajú kľúčovú úlohu pri návrhu decentralizovaných aplikácií. Celkové náklady na transakciu na EVM kompatibilnej DLT sú vyjadrené pomocou *GAS* jedno-

Tabuľka 5.1: Gas analýza odhadovaných nákladov nasadenia kontraktov

Kontrakt	**Spotrebovaný GAS**	**Náklady na rôznych DLT (USD)**		
		eth	**matic**	**smr**
IPv4GlobalAddrRegistry	1433789	114.74	0.17	0.05
IPPrefixRegistry	4728334	378.38	0.57	0.17
ASNRegistry	2963744	237.17	0.35	0.11
ASNAccount	2002679	160.26	0.24	0.07
ERC6551Registry	182201	14.58	0.02	0.01

tiek, čo predstavuje potrebné výpočtové a pamäťové zdroje siete na spracovanie transakcie. Cenu za jednu jednotku *GAS* môžeme vyjadriť pomocou vzorca 5.1.

$$Gas\ Price = MIN((Base\ Fee + Max\ Priority\ Fee), Max\ Fee) \tag{5.1}$$

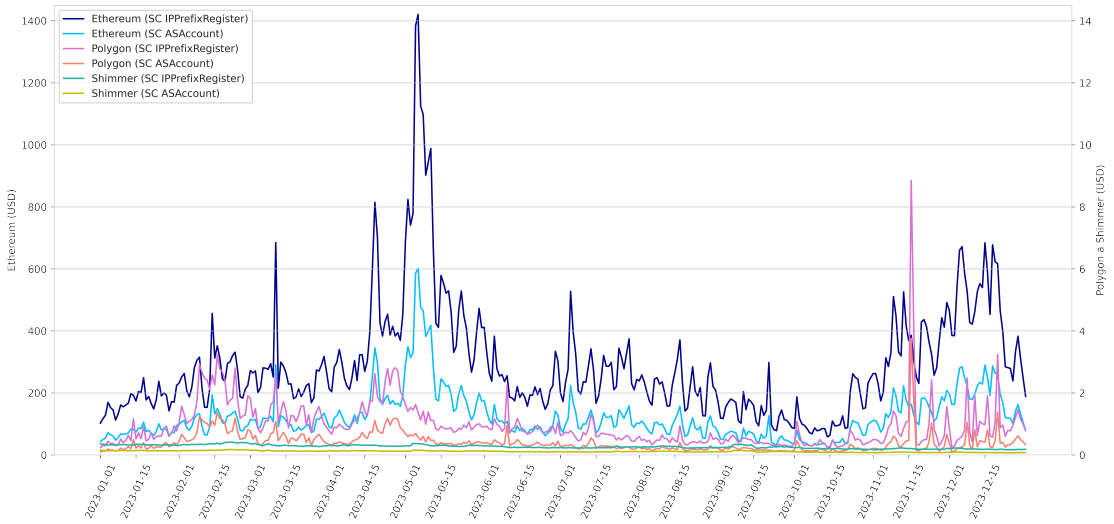
Metodiku na odhadovanie nákladov transakcií sme použili nasledujúcu: vývojové prostredie hardhat[7] s nástrojom *gas-reporter*, kde sme nakonfigurovali optimalizátor na hodnotu 1000. Následne sme vykonali v rámci každého kontraktu opakovanie každej transakcie 100 krát s rôznymi vstupmi, aby sme pokryli celý rozsah nákladov pre každú transakciu. Následne sme vyjadrili výsledné náklady transakcií pre sieť *Ethereum*, *Polygon* a *ShimmerEVM*. Celkový poplatok za transakciu môžeme vyjadriť pomocou vzorca 5.2.

$$Transaction\ Fee\ (USD) = Used\ GAS\ (gwei) \times Gas\ Price \times 10^{-9} \times Exchange\ rate \tag{5.2}$$

V Tabuľke 5.1 môžeme vidieť, že najviac sa spotrebuje *GAS*u na nasadenie kontraktu *IPPrefixRegistry*. Je to spôsobené jeho komplexnou logikou na prideľovanie IP prefixov ako NFT tokenov. Zároveň na Obrázku 5.7 je znázornená fluktuácia nákladov v USD za rok 2023 za nasadenie kontraktov *IPPrefixRegistry* a *ASAccount*, ktoré sa nasadzujú niekoľkokrát podľa potreby. V prípade sieti *Ethereum* rozdiely medzi niektorými dňami v roku môžu byť v stovkách USD. Na druhej strane, rozdiely v cenách za nasadenie v sieťach *Polygon* a *Shimmer* medzi rôznymi dňami v roku sú malé, preto z pohľadu eliminácie vysokých poplatkov na L1 sieti má zmysel nasadiť naše navrhované riešenie na L2 sieti.

Proces registrovania nového ASN sa skladá z operácie commit a samotnej registrácie. Výsledné

[7] `https://hardhat.org/`



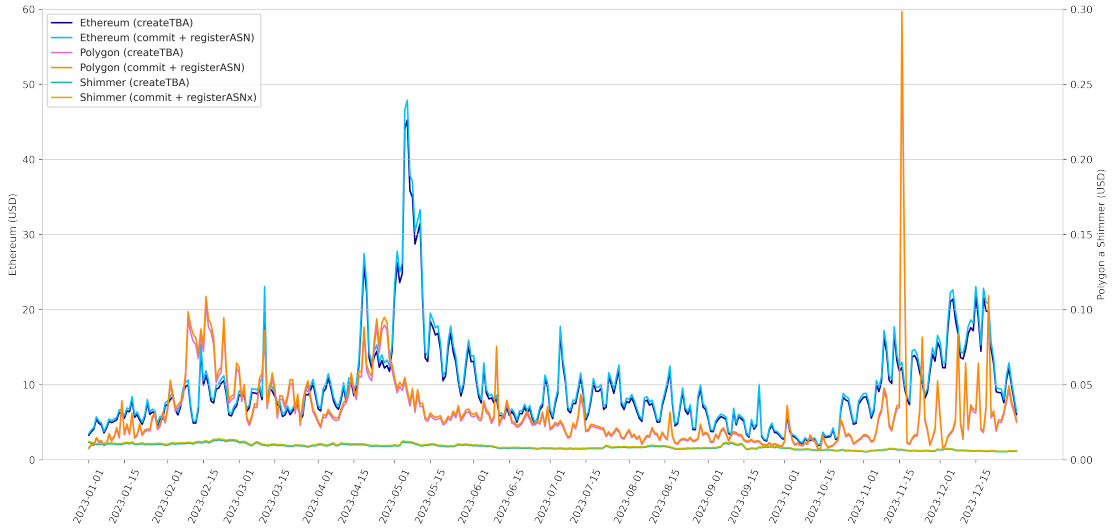
Obr. 5.7: Odhadované náklady za nasadenie kontraktov *IPPrefixRegistry* a *ASAccount* počas roka 2023

Tabuľka 5.2: Porovnanie GAS pre EOA a AS konto založené na TBA

Názov funkcie	**EOA**	**AS konto**	**Nárast v %**
allocationIPPrefix	253631	283529	11.79
assignIPPrefix	247764	277077	11.83
subAllocationIPPrefix	247777	281806	13.73
renewIPPrefix	50288	77918	54.94
safeTransferFrom	47559	76968	61.84
setROA	81125	124443	53.40

náklady sú súčet oboch operácií. Po tomto procese získame NFT reprezentujúce nami zaregistrované ASN. Následne k nemu môže vytvoriť TBA, čím naše NFT získa regulárnu adresu na držanie aktív. Oba zmieňované procesy z pohľadu nákladov sú podobné, ako je aj vidieť na Obrázku 5.8 s fluktuáciou nákladov za rok 2023. Zaujímavé porovnanie prináša Tabuľka 5.2, ktorá porovnáva vybrané operácie z pohľadu spotrebovaného *GAS*, keď sú operácie volané priamo z EOA, a keď sú volané cez AS konto, ktoré pridáva jedno volanie navyše do celkového súčtu volaní pre danú operáciu. Pri nákladnejších operáciách môžeme vidieť nárast spotrebovaného *GAS* približne o 12% a pri jednoduchších operáciách približne o 55%, ak sú volané cez AS konto. V tomto prípade výhody jednoduchej správy zdrojov cez AS konto a unikátne spojenie reprezentácie organizácie, respektíve AS cez TBA, prevyšujú vyššie náklady.

GAS analýza potvrdila, že je potrebné minimalizovať počet transakcií na L1 sieti a vybrať L2



Obr. 5.8: Odhadované náklady na registráciu ASN a vytvorenie konta pre AS počas roka 2023

sieť s nižšími poplatkami. Zo skúmaných L2 sietí sa javí ako vhodná sieť *Shimmer EVM*, ktorá funguje približne rok nad L1 sieťou *IOTA*, ktorá ponúka vysokú škálovateľnosť a skoro žiadne poplatky. S architektúrou s viacerými EVM kompatibilnými reťazcami na L2 a s možnosťou vytvoriť vlastnú sieť je sľubnou alternatívou pre súkromnú DLT. Momentálne je však z pohľadu nákladov a stability najvhodnejšie riešenie *Polygon*.

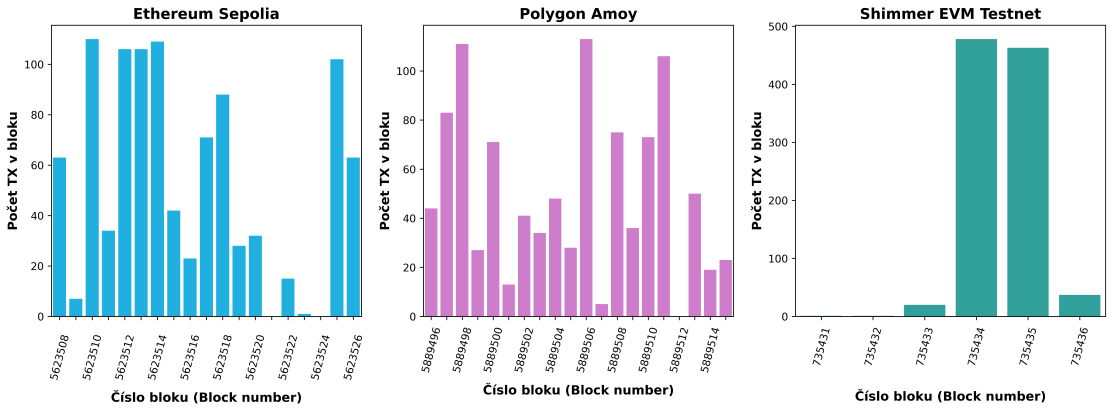
5.2.4 Testovanie na verejných DLT

V tejto časti sa zameriame na experiment vykonaný v troch testovacích verejných DLT. Cieľom bolo zistiť oneskorenie, ktoré nastane pri poslaní určitého množstva transakcií, kým budú potvrdené v blokoch. Pre tento experiment sme si vybrali štyri transakcie, ktoré považujeme, že budú najčastejšie vykonávané v rámci našej architektúry. Sú to tieto transakcie: *allocationIPPrefix*, *assignIPPrefix*, *renewIPPrefix* a *setROA*.

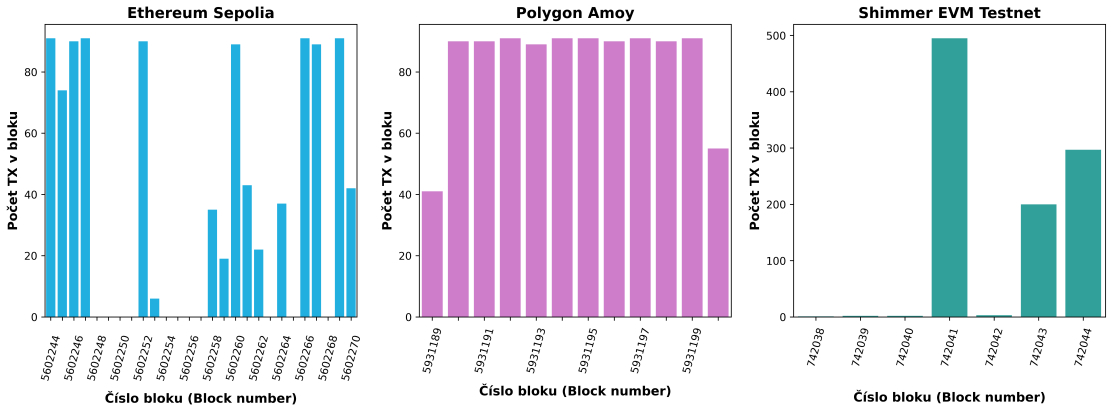
Metodológia experimentu bola nasledovná. Zvolili sme si množstvo transakcií, ktoré chceme naraz poslať do siete, čo predstavovalo 1000 transakcií. Všetky transakcie boli vykonávané cez vytvorené AS konto. Zaznamenávali sme oneskorenie transakcií, čo je čas od odoslania transakcie až do potvrdenia transakcie v bloku. Čas potrebný na vytvorenie transakcií sme nezahrnuli z dôvodu, že trvanie vytvorenia transakcií je závislé od výkonu stroja, na ktorom sa vykonáva.

Na Obrázku 5.9 až 5.12 je zobrazená distribúcia transakcií do blokov počas vykonávania expe-

rimentu. Oneskorenie transakcie môže byť ovplyvnené mnohými faktormi: aktuálna vyťaženosť siete, výška odmeny pre validátora, náročnosť transakcie na zdroje, algoritmus výberu transakcií validátorom z *mempoolu* a iné faktory.

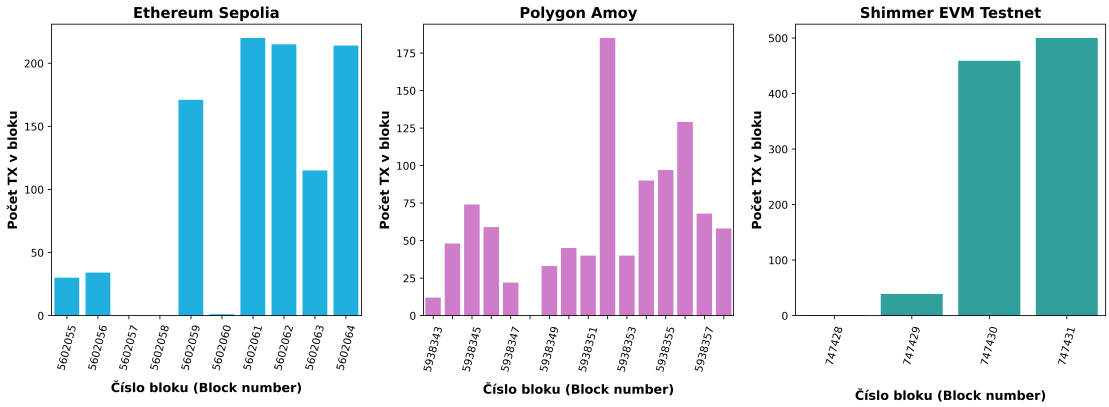


Obr. 5.9: 1000-krát odoslanie transakcie *allocationIPPrefix*

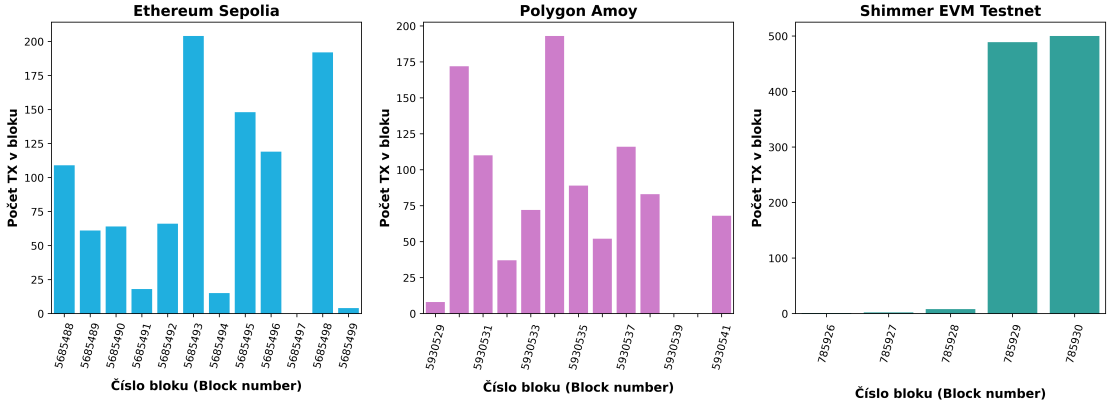


Obr. 5.10: 1000-krát odoslanie transakcie *assignIPPrefix*

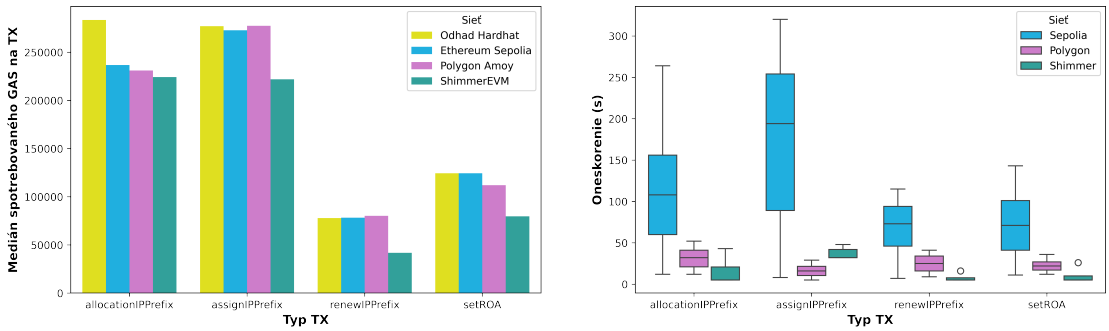
Vľavo na Obrázku 5.13 vyhodnocujeme spotrebovaný *GAS* transakciami na verejných DLT voči odhadovanému *GAS*. Uvádzané hodnoty sú medián z 1000 transakcií. Pri všetkých transakciách reálne spotrebovaný *GAS* nepresiahol výrazne odhadovanú hodnotu a väčšinou bol okolo odhadnutej hodnoty alebo menší. V prípade transakcie *allocationIPPrefix* bol odhad vyšší, ako sme v skutočnosti zaznamenali na jednotlivých sieťach. Rozdiely v spotrebovanom *GAS* medzi sieťami je možné vysvetliť tým, že siete používajú rozdielne verzie EVM v rámci, ktorých sa môžu líšiť definované náklady za vykonanie konkrétneho opkódu. Presné hodnoty spotrebovaného *GAS* uvádzame v Tabuľke 5.3.



Obr. 5.11: 1000-krát odoslanie transakcie *renewIPPrefix*



Obr. 5.12: 1000-krát odoslanie transakcie *setROA*



Obr. 5.13: Obrázok na ľavej strane uvádza medián spotrebovaného *GAS* pre každú transakciu z 1000 volaní. Na pravej strane z rovnakého počtu volaní, oneskorenie pre jednotlivé typy transakcií.

Tabuľka 5.3: Porovnanie odhadovaného a spotrebovaného *GAS* v sieťach

Názov funkcie	**Hardhat**	**Ethereum Sepolia**	**Polygon Amoy**	**ShimmerEVM Testnet**
allocationIPPrefix	283529	236786	231174	224264
assignIPPrefix	277077	272818	277522	221922
renewIPPrefix	77918	78326	80250	41826
setROA	124443	124433	112067	79739

Tabuľka 5.4: Oneskorenie vzhľadom na finálne potvrdenie transakcií v sekundách

Názov funkcie	**Ethereum Sepolia**	**Polygon Amoy**	**ShimmerEVM Testnet**
allocationIPPrefix	876	137	15
assignIPPrefix	962	121	42
renewIPPrefix	841	130	15
setROA	839	127	15

Medián oneskorenia transakcií je ukázaný na Obrázku 5.13 vpravo. Výrazne oneskorenie bolo na sieti *Ethereum Sepolia*, čo je dané tým, že bloky sú vytvárané v priemere každých 12 s. V sieti *ShimmerEVM* boli transakcie potvrdené rýchlo a rozptyl bol malý voči ostatným sieťam. To bolo zapríčinené tým, že bloky nie sú vytvárané tak v pravidelných intervaloch ako v ostatných dvoch sieťach. Na sieti *Polygon* oneskorenie bolo akceptovateľné vzhľadom aj na priemerný čas konvergencie siete 50 s [23]. V Tabuľke 5.4 uvádzame oneskorenie vzhľadom na finálne potvrdenie transakcií, čo znamená, že transakcia už nemôže byť vrátená kvôli *fork*. V *Ethereum* je potrebné čakať na finálne potvrdenie transakcie dve epochy, kde jedná epocha trvá približne 384 sekúnd. Nedávna aktualizácia *Aalborg*[8] v *Polygon*, finalitu bloku znížila na 105 s uvedením konceptu *milestones*, ktorý zabezpečuje jeho deterministickosť. V prípade *ShimmerEVM* sa v návrhu[9] uvádza údaj 10 s, ale nie je ho možné overiť z iných zdrojov.

5.3 Formálne overenie

Formálne overenie je spôsob, ako preukázať alebo vyvrátiť správnosť návrhu systému vzhľadom na formálnu špecifikáciu, alebo vlastností definovaných pomocou matematických a logických metód. V našom navrhovanom systéme sme pre formálne overenie použili nástroj *Certora Prover*[10].

[8] `https://polygon.technology/blog/faster-finality-with-the-aalborg-upgrade-for-polygon-proof-of-stake-network`

[9] `https://govern.iota.org/t/discussion-shimmerevm-governance-tokenomics-and-scaling/1301`

[10] `https://www.certora.com/prover`

Tabuľka 5.5: Porovnanie kľúčových aspektov nášho navrhnutého riešenia s ostatnými riešeniami.

	Tokenizácia	**AS konto**	**DAO**	**DLT**	**Overenie cesty**
Naše riešenie	✓	✓	✓	✓	✓
BGPCoin [7]	✗	✗	✗	✓	čiastočne
InBlock [8]	✗	✗	čiastočne	✗	čiastočne
ISRchain [9]	✗	✗	✗	✓	✓
BRVM [10]	✗	✗	✗	✓	čiastočne
BlockJack [11]	✗	✗	✗	✓	čiastočne
DRRS-BC [12]	✗	✗	✗	✓	čiastočne
VIPAPB [13]	✗	✗	✗	✓	čiastočne
RouteChain [14]	✗	✗	✗	✓	čiastočne
IPchain [15]	✗	✗	✗	✓	čiastočne
ROAchain [16]	✗	✗	✗	✓	čiastočne

Na opísanie správania a vlastností kontraktu sa používa CVL *(z angl. Certora Verification Language)*, ktorý je podobný *Solidity*. CVL definuje dve typy vlastností, a to invariant (invariant) a pravidlo (rule). Pomocou Hoarovej trojice $\{P\}\ C\ \{Q\}$ môžeme formálne zadefinovať jednotlivé praviďlá špecifikácií kontraktov. Kde C je príkaz alebo skupina príkazov, ktorá sa vykoná, ak je splnený predpoklad P. Vykonanie C končí v stave spĺňajúcom výstupnú podmienku Q. Vtedy je formálny výraz pravdivý. Ak zápis platí aj pre vykonanie s revertami, tak sa definuje ako $\{P\}\ C@withrevert\ \{Q\}$. Podmienky pred a po sú podobné príkazom *require* a *assert* v *Solidity*. Pomocou takýchto pravidiel sme si zadefinovali vlastností kontraktov, ktoré sme následne nahrali do *Certora Prover*[11] v cloude, ktorý nám vyhodnotil jednotlivé pravidlá a prípadne nám vypísal vstupy, ktoré dané pravidlo porušujú.

5.4 Porovnanie s existujúcimi riešeniami

V Tabuľke 5.5 uvádzame súhrne porovnanie kľúčových aspektov našej navrhovanej architektúry s identifikovanými riešeniami v analýze.

Za limit nášho riešenia môžeme považovať vyššie počiatočné náklady, ktoré sú primárne spojené s nasadením kontraktu pre každý IP prefix najvyššej úrovne. To je daň za poskytnutú modularitu v našej architektúre. Iný limit vnímame v metóde plánu rozdelenia prideleného adresného priestoru, kde hierarchický prístup pre IPv4 alebo tri dostupné metódy pre IPv6 *GAS* [24] môžu mať negatívny dopad na nárast spotrebovaného *GAS*. Z toho dôvodu, nechávame to na zod-

[11] `https://prover.certora.com/`

povednosti každého kontroléra k IP prefixu, ktorú metódu si vyberie. Ideálnym riešim by bolo kombinovať tento výpočet s externou službou Oracle na udržanie stabilného *GAS* pri pridelovani NFT s IP prefixom. Posledný limit vnímame škálovateľnosť z pohľadu oneskorenia spracovania transakcií. Hoci výsledky pre L2 boli sľubné, ale ešte stále nie sú ideálne pre zmenu ROA alebo ASPA záznamu. Pri alokovaní alebo priradení NFT s IP prefixom oneskorenie nehrá dôležitú úlohu.

Kapitola 6

Záver

Hlavný výskumný prínos tejto práce vidíme v návrhu architektúry pre manažment IP prefixov vo Web3 prostredí s reprezentáciou IP prefixov ako NFT, ktorý môžeme vnímať v dvoch kontextoch. V kontexte existujúceho prístupu k manažovaniu zdrojov, kde eliminujeme centrálne riadenie, zvyšujeme transparentnosť a zlepšujeme auditovateľnosť. V kontexte analyzovaných prác zlepšujeme modulárnosť architektúry pre manažment zdrojov a zavádzame reprezentáciu IP prefixov pomocou NFT, čím dosahujeme ich unikátnu reprezentáciu v rámci celého ekosystému a poskytujeme dôkaz o ich vlastníctve pre držiteľov IP prefixov. Ďalej vytvárame abstraktnú reprezentáciu AS na efektívnu správu zdrojov vo Web3, ktorá je prístupná cez naviazané NFT s vlastnou adresou. Toto NFT môže reprezentovať identitu AS. Adresa pridelená tomuto NFT umožňuje jednoznačne vystopovať všetky operácie vykonané v mene AS, bez ohľadu na to, kto s oprávneniami iniciuje operácie v mene AS. Ďalší čiastkový výskumný prínos spočíva v schopnosti zariadení sa naučiť časť konfigurácie s oznamovanými IP prefixmi pomocou blockchainu v súlade s existujúcimi platnými ROA záznamy v blockchaine. Zároveň oproti analyzovaným riešeniam pomáhame predísť ohláseniu chybnej konfigurácie a zabezpečujeme, že pri ohlásení daných IP prefixov už budú existovať ekvivalentné ROA záznamy v blockchaine. Navyše, v prípade incidentov je možné vystopovať celú históriu zmien na zariadení.

V rámci návrhu architektúry na manažment IP prefixov vo Web3 prostredí kladieme dôraz na modulárnosť, čo dosahujeme vlastným kontraktom pre každý IP prefix najvyššej úrovne s možnosťou jeho aktualizácie cez proxy kontrakt. V architektúre zavádzame reprezentáciu IP prefixov pomocou ERC-1155 multitoken štandardu, pričom pre IP prefixy vytvárame NFT tokeny. Týmto

zabezpečujeme dôkaz o vlastníctve IP prefixu a jeho unikátnu reprezentáciu v rámci ekosystému. Ďalej rozširujeme tento štandard o použitie ERC-5521 na sledovanie závislostí medzi IP prefixmi v hierarchickej štruktúre a o ERC-5643 na časovo obmedzené pridelenie NFT. S každým NFT s IP prefixom je viazaná sada príznakov na určenie právomoci pre jeho držiteľa. Globálny register IP adresného priestoru udržuje informácie o všetkých alokovaných a pridelených IP prefixoch pre rýchly prístup k nim. Výhodou tohto návrhu oproti analyzovaným riešeniam je, že architektúra je navrhovaná spôsobom, kde kľúčové komponenty sú riadené cez DAO. Tým sa dosahuje, že všetky rozhodnutia o budúcich zmenách v manažmente IP prefixov sa presúvajú kompletne od centrálneho rozhodovania k rozhodovaniu založenému na komunite, ktoré je vykonávané a zaznamenávané cez kontrakty.

Výsledky overenia potvrdili funkcionalitu navrhnutej architektúry a naplnili definované tézy tejto práce. Vykonali sme bezpečnostnú analýzu pomocou *Slither* a *Mythril*, aby sme dokázali, že naša architektúra nie je zraniteľná voči známym útokom na kontrakty. Ďalej vyhodnocujeme náklady na nasadenie jednotlivých kontraktov a vykonanie jednotlivých funkcií. Porovnávame ich medzi DLT riešeniami *Ethereum*, *Polygon* a *ShimmerEVM*. Následne na testovacích sieťach týchto DLT riešení nasadzujeme celú architektúru. Skúmame reálne spotrebovaný *GAS* a oneskorenie, ktoré vyhodnocujeme v kontexte odhadovaných nákladov a podobných riešení, najmä [25] a [7]. Vytváranie NFT tokenov pre IP prefixy výrazne nezvýšilo náklady v porovnaní s analyzovanými riešeniami na EVM kompatibilnej DLT. Najmenšie oneskorenie sme dosiahli na *Polygon* pre vybranú skupinu transakcií, kde medián bol od 16 s do 32 s. Nakoniec sme vykonali formálne overenie vlastností kontraktov pomocou nástroja *Certora Prover*.

6.1 Možné ďalšie rozšírenia

Sú tu stále aspekty architektúry, ktoré možno zlepšiť. Medzi takéto aspekty patrí:

- Monetizácia nevyužívaných zdrojov, ktorej cieľom je optimalizácia ekonomických nákladov a efektívnejšie využívanie limitovaných zdrojov, čo zároveň zvyšuje ich likviditu a dostupnosť na krátkodobé využitie.
- Ďalšia iterácia architektúry by mohla priniesť nový spôsob adresovania a smerovania, kde zariadenia budú reprezentované pomocou Web3 adresy. Táto nová koncepcia premení každé zariadenie na unikátneho účastníka v decentralizovanom ekosystéme. Adresa bude spojená s identitou zariadenia a umožní každému zariadeniu nielen prijímať a odosielať dáta, ale

aj vlastniť a obchodovať s digitálnymi aktívami. Takáto zmena paradigmy vnímania zariadení v rámci dnešného internetu prinesie transformáciu pasívnych zariadení na aktívnych účastníkov v digitálnej ekonomike.

Zoznam použitej literatúry

1. PALLADINO, Nicola; SANTANIELLO, Mauro. Conclusion: The Misleading Rhetoric of Multistakeholderism. In: *Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance: Analyzing IANA Transition*. Cham: Springer International Publishing, 2021, s. 143–156. ISBN 978-3-030-56131-4. Dostupné z DOI: 10.1007/978-3-030-56131-4_8.
2. RADU, Roxana. *Negotiating internet governance*. Oxford University Press, 2019. ISBN 9780198833079. Dostupné z DOI: 10.1093/oso/9780198833079.001.0001.
3. TJAHJA, Nadia; MEYER, Trisha; SHAHIN, Jamal. Who do you think you are? Individual stakeholder identification and mobility at the Internet Governance Forum. *Telecommunications Policy*. 2022, roč. 46, č. 10, s. 102410. ISSN 0308-5961. Dostupné z DOI: 10.1016/j.telpol.2022.102410.
4. MASTILAK, Lukas; HELEBRANDT, Pavol; GALINSKI, Marek; KOTULIAK, Ivan. Secure Inter-Domain Routing Based on Blockchain: A Comprehensive Survey. *Sensors*. 2022, roč. 22, č. 4. ISSN 1424-8220. Dostupné z DOI: 10.3390/s22041437.
5. ALAN, Suderman; FRNAK, Bajak; RODNEY, Muhumuza. *African internet riches threatened by lawsuit and corruption* [online]. The Associated Press, 2021-11-23 [cit. 2024-07-01]. Dostupné z : https://blog.apnic.net/2024/01/09/measuring-bgp-in-2023-have-we-reached-peak-ipv4/.
6. MILTON, Mueller; VAGISHA, Srivastava; BRENDEN, Kuerbis. *A Fight Over Crumbs: The AFRINIC crisis* [online]. Internet Governance Project, 2021-08-19 [cit. 2024-07-01]. Dostupné z : https://www.nrs.help/post/afrinic-accused-of-unlawful-lobbying-and-interference-in-african-governments.

7. XING, Qianqian; WANG, Baosheng; WANG, Xiaofeng. BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution. *Symmetry, MDPI*. 2018, roč. 10, č. 9. ISSN 2073-8994. Dostupné z DOI: 10.3390/sym10090408.
8. ANGIERI, Stefano; GARCÍA-MARTÍNEZ, Alberto; LIU, Bingyang; YAN, Zhiwei; WANG, Chuang; BAGNULO, Marcelo. A Distributed Autonomous Organization for Internet Address Management. *IEEE Transactions on Engineering Management*. 2020, roč. 67, č. 4, s. 1459–1475. Dostupné z DOI: 10.1109/TEM.2019.2924737.
9. CHEN, Di; BA, Yang; QIU, Han; ZHU, Junhu; WANG, Qingxian. ISRchain: Achieving efficient interdomain secure routing with blockchain. *Computers & Electrical Engineering*. 2020, roč. 83, s. 106584. ISSN 0045-7906. Dostupné z DOI: 10.1016/j.compeleceng.2020.106584.
10. LIU, Yaping; ZHANG, Shuo; ZHU, Haojin; WAN, Peng-Jun; GAO, Lixin; ZHANG, Yaoxue; TIAN, Zhihong. A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks. *Journal of Parallel and Distributed Computing*. 2020, roč. 142, s. 77–89. ISSN 0743-7315. Dostupné z DOI: 10.1016/j.jpdc.2020.04.005.
11. SENTANA, I Wayan Budi; IKRAM, Muhammad; KAAFAR, Mohamed Ali. *BlockJack: Towards Improved Prevention of IP Prefix Hijacking Attacks in Inter-Domain Routing Via Blockchain*. 2021. Dostupné z arXiv: 2107.07063 [cs.CR].
12. LU, Huimin; TANG, Yu; SUN, Yi. DRRS-BC: Decentralized Routing Registration System Based on Blockchain. *IEEE/CAA Journal of Automatica Sinica*. 2021, roč. 8, č. 12, s. 1868–1876. Dostupné z DOI: 10.1109/JAS.2021.1004204.
13. SFIRAKIS, Ilias; KOTRONIS, Vasileios. *Validating IP Prefixes and AS-Paths with Blockchains*. 2019. Dostupné z arXiv: 1906.03172 [cs.NI].
14. SAAD, Muhammad; ANWAR, Afsah; AHMAD, Ashar; ALASMARY, Hisham; YUKSEL, Murat; MOHAISEN, David. RouteChain: Towards Blockchain-based secure and efficient BGP routing. *Computer Networks*. 2022, roč. 217, s. 109362. ISSN 1389-1286. Dostupné z DOI: 10.1016/j.comnet.2022.109362.
15. PAILLISSE, Jordi; MANRIQUE, Jan; BONET, Guillem; RODRIGUEZ-NATAL, Alberto; MAINO, Fabio; CABELLOS, Albert. Decentralized Trust in the Inter-Domain Routing Infrastructure. *IEEE Access*. 2019, roč. 7, s. 166896–166905. Dostupné z DOI: 10.1109/ACCESS.2019.2954096.

16. HE, Guobiao; SU, Wei; GAO, Shuai; YUE, Jiarui; DAS, Sajal K. ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing. *IEEE Transactions on Network and Service Management*. 2021, roč. 18, č. 2, s. 1690–1705. Dostupné z DOI: 10.1109/TNSM.2020.3015557.
17. BAMAKAN, Seyed Mojtaba Hosseini; MOTAVALI, Amirhossein; BABAEI BONDARTI, Alireza. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*. 2020, roč. 154, s. 113385. ISSN 0957-4174. Dostupné z DOI: 10.1016/j.eswa.2020.113385.
18. HELEBRANDT, Pavol; BELLUS, Matej; RIES, Michal; KOTULIAK, Ivan; KHILENKO, Vladimir. Blockchain adoption for monitoring and management of enterprise networks. In: *2018 IEEE 9th annual information technology, Electronics and Mobile Communication Conference (IEMCON)*. 2018, s. 1221–1225. Dostupné z DOI: 10.1109/IEMCON.2018.8614960.
19. XU, Xiwei; PAUTASSO, Cesare; ZHU, Liming; LU, Qinghua; WEBER, Ingo. A Pattern Collection for Blockchain-based Applications. In: *Proceedings of the 23rd European Conference on Pattern Languages of Programs*. Irsee, Germany: Association for Computing Machinery, 2018. EuroPLoP '18. ISBN 9781450363877. Dostupné z DOI: 10.1145/3282308.3282312.
20. WANG, Qin; YU, Guangsheng; FU, Shange; CHEN, Shiping; YU, Jiangshan; XU, Xiwei. A Referable NFT Scheme. In: *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 2023, s. 1–6. Dostupné z DOI: 10.1109/ICBC56567.2023.10174865.
21. ENS. *Fuses* [online]. 2023 [cit. 2023-07-29]. Dostupné z : https://support.ens.domains/en/articles/7902567-fuses#h_ebc654e096.
22. VALAŠTÍN, Viktor; BITAROVSKÝ, Roman; KOŠŤÁL, Kristián; KOTULIAK, Ivan. *Towards Proxy Staking Accounts Based on NFTs in Ethereum*. 2024. Dostupné z arXiv: 2404.14074 [cs.DC].
23. HUSTON, Geoff. *BGP in 2023 – The BGP Table* [online]. 2024-01-10 [cit. 2024-04-01]. Dostupné z : https://blog.apnic.net/2024/01/10/bgp-in-2023-bgp-updates/.
24. COFFEEN, Tom. *IPV6 PREFIX ALLOCATION METHODS – PART TWO* [online]. 2020-08-05 [cit. 2024-04-01]. Dostupné z : https://blogs.infoblox.com/ipv6-coe/ipv6-prefix-allocation-methods-part-two/.
25. GARCÍA-MARTÍNEZ, Alberto; ANGIERI, Stefano; LIU, Bingyang; YANG, Fei; BAGNULO, Marcelo. Design and Implementation of InBlock—A Distributed IP Address Regi-

stration System. *IEEE Systems Journal*. 2021, roč. 15, č. 3, s. 3528–3539. Dostupné z DOI: 10.1109/JSYST.2020.3003526.

Príloha A

Publikované práce

ADM Vedecké práce v zahraničných časopisoch registrovaných v databázach Web of Science alebo SCOPUS:

- ADC01 MASTIĽAK, Lukáš - GALIŃSKI, Marek - HELEBRANDT, Pavol - KOTULIAK, Ivan - RIES, Michal. Enhancing Border Gateway Protocol Security Using Public Blockchain. In Sensors. Vol. 20, iss. 16 (2020), s. 1-11. ISSN 1424-8220 (2020: 3.576 - IF, Q1 - JCR Best Q, 0.636 - SJR, Q2 - SJR Best Q). V databáze: WOS: 000567288800001 ; SCOPUS: 2-s2.0-85089382475 ; DOI: 10.3390/s20164482.
  Ohlasy:
  1. Q. Yang et al., "Towards Blockchain-Based Secure BGP Routing, Challenges and Future Research Directions,"Comput. Mater. Contin., vol. 79, no. 2, pp. 2035-2062. 2024. doi: `https://doi.org/10.32604/cmc.2024.049970`.
  2. T.L. Kayathri et al., "SDBGPChain: A decentralized low complexity framework to detect and prevent the BGPattacks using SDN with smart contract based Dendrimer tree blockchain,ïn Computer Networks, vol. 230, 2023, 109800, ISSN 1389-1286, doi: `https://doi.org/10.1016/j.comnet.2023.109800`.
  3. J. Qin et al., "Subarea Route Fusion Mechanism Based on Virtual Links,ïn Emerging Networking Architecture and Technologies ICENAT 2022 Communications in Computer and Information Science, vol. 1696, Springer, Singapore, `https://doi.org/10.1007/978-981-19-9697-9_20`.

4. A. Devassy et al., "Safeguarding blockchains from adversarial tactics,ïn Blockchain for Industry 4.0, CRC Press, 2022. p. 63-90, doi: urlhttps://doi.org/10.1201/9781003282914-4.
5. F. Xuewei, et al., "PMTUD is not Panacea: Revisiting IP Fragmentation Attacks against TCP,ïn: NDSS. 2022, doi: https://doi.org/10.14722/ndss.2022.24381.
6. W. Mincewicz, "The Potential of Using Blockchain Technology in Human Life: Examples of Implementation,ïn Online Journal Modelling the New Europe, 2022, 40: 78-97, doi: https://doi.org/10.24193/OJMNE.2022.40.04.
7. S. Szymoniak et al., "SAT and SMT-Based Verification of Security Protocols Including Time Aspects,"Sensors 2021, 21, 3055, https://doi.org/10.3390/s21093055.
8. A. L. Vivar et al., Ä security framework for Ethereum smart contracts,ïn Computer Communications, vol. 172, 2021, pp. 119-129, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2021.03.008.
9. X. Zhao et al., "The Implementation of Border Gateway Protocol Using Software-Defined Networks: A Systematic Literature Review,ïn IEEE Access, vol. 9, pp. 112596-112606, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3103241.

- ADC02 MASTIĽAK, Lukáš - HELEBRANDT, Pavol - GALINSKI, Marek - KOTULIAK, Ivan. Secure Inter-Domain Routing Based on Blockchain: A Comprehensive Survey. In Sensors. Vol. 22, iss. 4 (2022), art. no. 1437. ISSN 1424-8220 (2022: 3.900 - IF, Q2 - JCR Best Q, 0.764 - SJR, Q1 - SJR Best Q). V databáze: CC: 000765168100001 ; WOS: 000765168100001 ; SCOPUS: 2-s2.0-85124339442 ; DOI: 10.3390/s22041437.
  Ohlasy:
  1. N. Rodday et al., "The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects,ïn IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 2353-2373, April 2024, doi: https://doi.org/10.1109/TNSM.2023.3327455.
  2. Mikołaj Kowalski et al., "Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures,ïn Computer Networks, vol. 230, 2023, 109778, ISSN 1389-1286, doi: https://doi.org/10.1016/j.comnet.2023.109778.

3. E. Zeydan et al., "Blockchain-Based Self-Sovereign Identity for Routing in Inter-Domain Networks,ïn IEEE Communications Magazine, vol. 62, no. 1, pp. 96-102, January 2024, doi: https://doi.org/10.1109/MCOM.004.2300244.
4. T.L. Kayathri et al., "SDBGPChain: A decentralized low complexity framework to detect and prevent the BGPattacks using SDN with smart contract based Dendrimer tree blockchain,ïn Computer Networks, vol. 230, 2023, 109800, ISSN 1389-1286, doi: https://doi.org/10.1016/j.comnet.2023.109800.
5. Q. Yang et al., "Towards Blockchain-Based Secure BGP Routing, Challenges and Future Research Directions,"Comput. Mater. Contin., vol. 79, no. 2, pp. 2035-2062. 2024. doi: https://doi.org/10.32604/cmc.2024.049970.
6. P. Singh et al., "Blockchain and Dew Computing-based Model for Secure Energy Trading in Smart Grids,"2023 IEEE International Conference on Communications Workshops (ICC Workshops), Rome, Italy, 2023, pp. 176-181, doi: https://doi.org/10.1109/ICCWorkshops57953.2023.10283767.
7. S. W. Turner et al., Ä Promising Integration of SDN and Blockchain for IoT Networks: A Survey,ïn IEEE Access, vol. 11, pp. 29800-29822, 2023, doi: https://10.1109/ACCESS.2023.326077.

- ADC03 MASTIĽAK, Lukáš- SUCHÝ, Róbert - KOŠŤÁL, Kristián - KOTULIAK, Ivan. Blockchain-Based Sustainable Retail Loyalty Program. In IEEE Access. Vol. 11, (2023), s. 75063-75075. ISSN 2169-3536 (2022: 3.900 - IF, Q2 - JCR Best Q, 0.926 - SJR, Q1 - SJR Best Q). V databáze: DOI: 10.1109/ACCESS.2023.3296914 ; IEEE: 10187141.

AFD Publikované príspevky na domácich vedeckých konferenciách:

- AFD01 MASTIĽAK, Lukáš - GALINSKI, Marek - KOTULIAK, Ivan - RIES, Michal. Improved Smart Gateway in IoT. In ICETA 2018 : 16th IEEE International Conference on Emerging eLearning Technologies and Applications. November 15-16, 2018, Starý Smokovec, Slovakia : Proceedings. 1. vyd. Danvers : IEEE, 2018, S. 349-354. ISBN 978-1-5386-7912-8. V databáze: WOS: 000457680400052 ; SCOPUS: 2-s2.0-85060277011.
  Ohlasy:
  1. N. MITROVIĆ et al., Ïmplementation and Testing of Websocket Protocol in ESP32 based IoT systems. Facta Universitatis,ïn Series: Electronics and Energetics, 2023,

vol. 36.2: 267-284, doi: https://doi.org/10.2298/FUEE2302267M.

2. G. Beniwal et al., "A systematic literature review on IoT gateways", in Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, Part B, 2022, pp. 9541-9563, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2021.11.007.

- AFD02 RAFAJ, Tomáš - MASTIĽAK, Lukáš - KOŠŤÁL, Kristián - KOTULIAK, Ivan. DeFi Gaming Platform Using the Layer 2 Benefits. In Proceedings of the 33rd Conference of Open Innovations Association FRUCT. 1. ed. Helsinki : FRUCT Oy, 2023, S. 236-242. ISSN 2305-7254. ISBN 978-952-69244-9-6. V databáze: DOI: 10.23919/FRUCT58615.2023.10143054 ; IEEE: 10143054.