**UNIVERZITA OBRANY**

**FAKULTA VOJENSKÝCH TECHNOLOGIÍ**

**Studijní program: Vojenské technologie**

Studijní obor: Informační technologie

Ev. číslo: xxxx/22



**DIPLOMOVÁ PRÁCE**

Název: Využití postkvantových algoritmů pro zabezpečení informačního systému

Zpracoval: Vojtěch Bžatek

Vedoucí práce: Prof. Dr. Ing. Alexandr Štefek

BRNO 2022

Zadání

I. Upřesnění podmínek zpracování závěrečné práce

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s utajovanými informacemi.

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s informacemi pro služební potřebu.

Závěrečná práce NEBUDE obsahovat utajené informace.

Závěrečná práce NEBUDE obsahovat informace pro služební potřebu.

Při zpracování závěrečné práce NEBUDOU zpracovávány osobní údaje.

II. Cíl závěrečné práce

Navrhnout možnosti využití nejnovějších poznatků z oblasti kvantového šifrování a využití blockchain pro potřeby ochrany dat v informačních systémech.

Nezbytné součásti diplomové práce:

Přehled algoritmů a jejich open source implementací z kategorie tzv. postkvantového šifrování.

Přehled ochranných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty.

Implementace mikroslužby zabezpečující operace typu šifrování a podepisování nad datovými bloky.

Implementace mikroslužby zabezpečující technologii blockchain nad logovými soubory informačního systému.

III. Pokyny pro zpracování závěrečné práce

Zpracujte přehled dostupných opensource implementací šifrování (tzv. postkvantové algoritmy), specificky výstupy ze soutěží nist.gov.

Zpracujte přehled možných útoků na standardně implementované informační systémy (datové úložiště).

Zpracujte přehled možných protiopatření (ochranných mechanismů).

Implementujte mikroslužbu využívající tzv. postkvantových algoritmů pro šifrování pro zabezpečení dat proti specifickým modifikacím dat.

Průběžně udržujte aktualizovaný přehled použité literatury a ke každé dílčí etapě zpracujte cca 7 stran shrnutí.

**PODĚKOVÁNÍ (nepovinné)**

**ČESTNÉ PROHLÁŠENÍ**

Prohlašuji, že jsem zadanou diplomovou práci na téma „xxx“ vypracoval samostatně, pod odborným vedením vedoucího xxx a použil jsem pouze literární zdroje uvedené v práci.

Dále prohlašuji, že jsem seznámen s tím, že se na moji diplomovou práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména skutečnosti, že Univerzita obrany má právo na uzavření licenční smlouvy o užití této bakalářské (diplomové) práce jako školního díla podle § 60 odst. 1 výše uvedeného zákona, a s tím, že pokud dojde k užití této diplomové práce mnou nebo bude poskytnuta licence o užití díla třetímu subjektu, je Univerzita obrany oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladu, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. Souhlasím se zpřístupněním své diplomové práce pro prezenční studium v prostorách knihovny Univerzity obrany.

V Brně, dne xx. května. 2024

..........................................

Jméno studenta

**ABSTRAKT**

**Klíčová slova:**

**Kryptografie, Postkvantové algoritmy, blockchain, blockchainová síť**

**ABSTRACT**

**Key words:**

Obsah

[SEZNAM POUŽITÝCH ZKRATEK 9](#_Toc164589019)

[SEZNAM OBRÁZKŮ 10](#_Toc164589020)

[SEZNAM TABULEK 11](#_Toc164589021)

[ÚVOD 12](#_Toc164589022)

[1.1 Cíl praktické části a její omezení 13](#_Toc164589023)

[2 Postkvantová kryptografie 15](#_Toc164589024)

[2.1 Motivace postkvantové kryptografie 15](#_Toc164589025)

[2.2 Shrnutí klasické kryptografie 15](#_Toc164589026)

[2.3 Shorův algoritmus 17](#_Toc164589027)

[2.4 NIST a jeho zapojení do pokroku v postkvantové kryptografii 18](#_Toc164589028)

[2.5 Postkvantové algoritmy a jejich implementace 20](#_Toc164589029)

[2.5.1 Kryptografie založená na mřížkách 20](#_Toc164589030)

[2.5.2 Kyber 24](#_Toc164589031)

[2.5.3 DILITHIUM 24](#_Toc164589032)

[2.5.4 Falcon 24](#_Toc164589033)

[2.5.5 Sphincsplus 24](#_Toc164589034)

[3 Přehled ochraných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty 25](#_Toc164589035)

[4 Mikroslužba zabezpečující postkvantovou kryptografii 26](#_Toc164589036)

[4.1 Popis jednotlivých částí 27](#_Toc164589037)

[4.2 Nastavení symetrického klíče 27](#_Toc164589038)

[4.3 Získání podpisových klíčů a práce s nimi 30](#_Toc164589039)

[4.3.1 JWT 30](#_Toc164589040)

[4.3.2 Získání soukromého podepisovacího klíče 31](#_Toc164589041)

[4.3.3 Získání veřejného podpisového klíče 32](#_Toc164589042)

[4.4 Průběh komunikace při odeslání zprávy 34](#_Toc164589043)

[4.5 Průvodce pro spuštění mikroslužby 35](#_Toc164589044)

[5 Blockchain 36](#_Toc164589045)

[5.1 Úvod do problematiky blockchain 36](#_Toc164589046)

[5.2 Klíčové vlastnosti technologie blockchain 37](#_Toc164589047)

[6 Mikroslužba zabezpečující technologii blockchain nad logovými soubory informačního systému. 38](#_Toc164589048)

[6.1 Popis jednotlivých částí 38](#_Toc164589049)

[6.1.1 Blockchain 38](#_Toc164589050)

[6.1.2 Klient/Postman 38](#_Toc164589051)

[6.2 Popis funkcionalit nodu 38](#_Toc164589052)

[6.2.1 Registrace v síti 38](#_Toc164589053)

[6.2.2 Tabulka všech nodů 38](#_Toc164589054)

[6.2.3 Přijetí zprávy 39](#_Toc164589055)

[6.2.4 Těžba 39](#_Toc164589056)

[6.2.5 Ověření řetězu 41](#_Toc164589057)

[6.2.6 Poskytnutí řetezu 42](#_Toc164589058)

[6.2.7 Průvodce pro spuštění mikroslužby 42](#_Toc164589059)

[7 Postkvantová blockchainová síť 42](#_Toc164589060)

[7.1.1 Popis jednotlivých částí 42](#_Toc164589061)

[7.1.2 Ukázka funkcionalit mikroslužeb 43](#_Toc164589062)

[7.1.3 Průvodce pro spuštění Postkvantové blockchainové sítě 43](#_Toc164589063)

[8 Možnosti dalšího rozvoje 44](#_Toc164589064)

[ZÁVĚR 44](#_Toc164589065)

[SEZNAM POUŽITÉ LITERATURY (vzor) 45](#_Toc164589066)

[SEZNAM PŘÍLOH 46](#_Toc164589067)

# SEZNAM POUŽITÝCH ZKRATEK

|  |  |
| --- | --- |
| AČR | Armáda České republiky (→ Styl seznam zkratek) |
| CA | Certifikační autorita |
| PQC | Post quantum cryptography  Postkvantová kryptografie |
| KEM | Key encapsulation mechanism |
| ISO | International Organization for Standardization  Mezinárodní organizace pro standardizaci |

# SEZNAM OBRÁZKŮ

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Obrázek 1 |  | Symetrická kryptografie v akci |  |
| Obrázek 2 |  | Mříž se dvěma různými základnami |  |
| Obrázek 10 | − | Popis výměny symetrického klíče mezi Alicí a CA |  |
| Obrázek 11 | − | Popis výměny symetrického klíče mezi Alicí a Bobem |  |
| Obrázek 12 | − | Popis žádosti o soukromý podpisový klíč |  |
| Obrázek 13 | − | Popis žádosti o veřejný podpisový klíč |  |
| Obrázek 14 | − | Odeslání zprávy |  |
| Obrázek 15 | − | Zaregistrování uzlu v síti |  |
| Obrázek 16 | − | Přijetí zprávy |  |
| Obrázek 17 | − | Zahájení těžby |  |
| Obrázek 18 | − | Těžení bloku a distribuce výsledku |  |
| Obrázek 31 | − | http požadavek (registrace v síti) |  |
|  | − |  |  |
|  | − |  |  |

# SEZNAM TABULEK

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Strana |
| Tabulka 1 | − | Popis tabulky | … XX |
| Tabulka 2 | − | Popis tabulky | … XX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# ÚVOD

„Svět je nebezpečné místo k životu, ne kvůli lidem, kteří jsou zlí, ale kvůli lidem, kteří s tím nic neudělají.“ Je tomu téměř 70 let, kdy nás opustil geniální fyzik Albert Einstein – autor tohoto citátu. Vybral jsem ho pro úvod této diplomové práce schválně. Pochopil jsem ho tak, že pokud člověk může udělat něco pro bezpečnost nejenom nás, lidí, ale v celkovém důsledku i celé planety, tak by to udělat měl. Tento citát byla moje základní myšlenka při rozhodování se o diplomové práci.

Téma mé diplomové práce a jeho cíle jsem si, po diskusi s vedoucím, vybral vlastní. Chtěl jsem se zaměřit na možnosti využití nejnovějších poznatků z oblasti kvantového šifrování a použití blockchain pro potřeby ochrany dat v informačních systémech.

Už v průběhu studia mě zaujaly různé kryptografické algoritmy, jejich odolnosti a jakým způsobem přispívají k bezpečné komunikaci přes otevřenou datovou síť. Zároveň jsem si byl já, tak jako i spousta velmi chytrých lidí vědomi hrozby v možná brzkém příchodu kvantových počítačů. Tyto počítače významně naruší odolnost běžných, denně používaných kryptografických algoritmů. Samozřejmě svět před touto hrozbou nezavřel oči. V roce 2017 byla vyhlášena soutěž o kvantově bezpečný kryptografický algoritmus a po pěti letech, v roce 2022, byly zveřejněny výsledky. Svět si tak mohl částečně oddychnout. Řešení odolnosti proti kvantovým počítačům existuje. Zbývá je jen začít používat.

Ve své práci vycházím právě z těchto kryptografických algoritmů. Nevytvářím žádný nový, svůj vlastní, kvantově odolný algoritmus, ale popisuji, jak implementovat ty, které byly prověřeny a schváleny odborníky na kryptografii. Využívám jak řešení přímo od autorů postkvantových kryptografických algoritmů, tak i řešení třetích stran. Tedy těch, kdo matematické rovnice, podle instrukcí autorů převedli do spustitelných kódů. Jejich práce pak upravuji tak, aby mohly být využity pro přenos dat, mezi dvěma počítači.

Bezpečnost informačních systémů ovšem nekončí jen v samotné komunikaci, byť je jedna, z mého pohledu, klíčových, ale pokračuje také v samotném uchováním dat. Zeptal jsem se sám sebe na triviální otázky. Je možné, aby byla data nezměnitelná i v případě, kdy mám veškerá oprávnění pro přístup k těmto datům? Kdo mi zabrání abych neupravil data, vlastnictví informačního systému, pokud mohu beze stopy číst, mazat a upravovat vše co se informačním systému nachází? Ano, současné ochranné mechanismy, logování aktivity, přímý dohled a omezené oprávnění prakticky takovou situaci neumožňují, ale to neznamená, že tato hrozba se rovná pravděpodobnostní nule. Zamyslel jsem se tedy nad možnostmi, jak se tuta problematiku řeší v jiných odvětvích. I díky základním znalostem načerpaných v průběhu studia oboru Kybernetická bezpečnost jsem se rozhodl zaměřit na využití blockchainové sítě, která se běžně používá pro zabezpečení kryptoměnových systémů.

Po prozkoumání dostupných blockchainových sítí jsem se kvůli náročnosti, a především nekompatibilitě s mým zámyslem rozhodl vyvinout síť vlastní. Mým cílem tedy bylo vytvořit vlastní blockchainovou síť, která přijímá zprávy od svých uživatelů a ukládá je pro další použití.

První část této práce, postkvantová bezpečnost, se zabývá zajištěním důvěrnosti dat. Tedy jednou z nutných podmínek logické vrstvy bezpečnosti pro ochranu dat v informačním systému. Druhá část, blockchainová síť, se zabývá integritou dat. To je druhá z nutných podmínek. Tyto podmínky jsou nutné, nikoliv dostatečné, a proto spolu s dostupností je pro zabezpečení ochrany dat v informačním systému nutné aplikovat všechny naráz.

Byť jsem si to přímo nespecifikoval ve svém zadání práce, rozhodl jsem se do své diplomové práce přidat ještě třetí část a tou je postkvantová blockchainová síť. Shrnuje obě problematiky do jedné celistvé aplikace.

Cílem této diplomové práce je předložit důkaz o využitelnosti blockchainové sítě pro uchování dat v informačním systému, důkaz o možnosti použití postkvantových algoritmů pro běžnou komunikaci, a poskytnout přehled postkvantových algoritmů a jejich implementací.

— Albert Einstein německo-americký fyzik, autor teorie relativity 1879–1955

## Cíl praktické části a její omezení

Cílem praktické části je představit dvě služby zabezpečující postkvantovou kryptografii a technologii blockchain. U každé služby nejprve popíšu její jednotlivé části, poté se věnuji jejím funkcionalitám a následně předvedu postup, jak danou službu spustit.

Obě služby jsou na sobě zcela nezávislé, ale součástí praktické části této diplomové práce je i jejich kombinace do Postkvantové blockchainové sítě. Také tuto síť v podkapitole 5.4 podrobně popíšu a předvedu její použití.

Ani jednu ze dvou služeb a jejich kombinace v praktické části mé diplomové práce jsem nepsal podle určitého zadání. Nikdo mi přesně nespecifikoval, co od služeb očekává, a proto jsem postupoval buď podle zavedených postupů vyčtených z internetu anebo podle mého vlastního rozhodnutí. Cílem práce tedy nebylo poskytnout někomu řešení na míru, ale představit funkční koncept, který vyžaduje pouze triviální změny k jeho použití v praxi.

Pro podepisování a následné ověření zpráv je potřeba přítomnost certifikační autority, která poskytuje jednotlivým uživatelům klíče k ověření podpisu. Vytvořit, nebo použít certifikační autoritu třetí strany není součástí této diplomové práce, a proto využívám jen její lehkou náhradu. Tato pseudocertifikační autorita nesplňuje všechny potřebné standardy, včetně těch bezpečnostních. Například v sobě nezahrnuje autentizaci uživatele. Protože certifikační autorita není cílem diplomové práce a použitá certifikační autorita nesplňuje všechny požadavky, nepovažuji ji za součást mé diplomové práce a budu se o ni zmiňovat jen v nejnutnějších případech.

# Postkvantová kryptografie

## Motivace postkvantové kryptografie

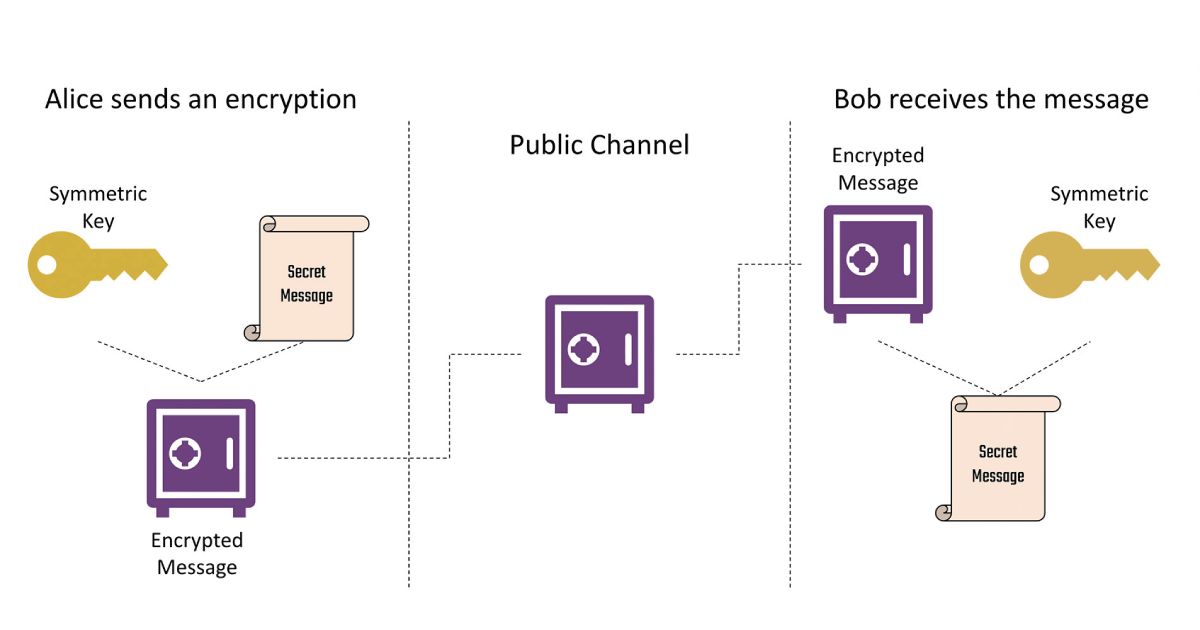
Postkvantová kryptografie je oblastí, která se věnuje vývoji šifrovacích systémů odolných proti útokům pomocí kvantových počítačů. Tyto počítače jsou schopné provádět výpočty s využitím kvantových algoritmů, jako je Groverův a Shorův algoritmus, které mohou ohrozit současné šifrovací metody. Například Groverův algoritmus může zrychlit luštění symetrických šifer, jako jsou AES a DES, což by mohlo být vyřešeno zvětšením délky klíčů. Na druhou stranu, Shorův algoritmus představuje větší hrozbu, protože umožňuje faktorizaci velkých čísel a řešení diskrétního logaritmu v polynomiálním čase, což ohrožuje běžně používané asymetrické šifry jako RSA, DSA, ECDH a ECDSA. Vzhledem k tomu, že se předpokládá, že kvantové počítače budou běžně dostupné v horizontu 10 až 20 let, je důležité již nyní přemýšlet nad využitím nových postkvantových algoritmů, které jsou schopné odolat potenciálním kvantovým útokům. To je zásadní zejména pro data, která potřebujeme chránit dlouhodobě, neboť i když se zdá, že 10 až 20 let je dlouhá doba, některá data musí být zabezpečena na mnohem delší období. [x1]

[x1] BURDA, Patrik. Možnosti postkvantové kryptografie. Brno, 2019, 38 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Petr Dzurenda,

## Shrnutí klasické kryptografie

Předtím, než se ponoříme do detailů postkvantových šifrovacích metod, je důležité pochopit základní principy kryptologie a jaký dopad by mělo, kdyby kvantové počítače dokázaly kryptografii prolomit. Kryptografové historicky řešili problém, jak umožnit dvěma stranám, jako jsou Alice a Bob, bezpečně komunikovat přes veřejný kanál, který může být odposloucháván třetí stranou, například Evou. Představme si, že Alice chce poslat Bobovi zprávu: "Poklad je schovaný v knihovně," ale nemá k dispozici žádný soukromý komunikační kanál. Aby zabránila Evě v odposlechu a potenciálním odcizení pokladu, Alice využije šifrování. Když byli Alice a Bob naposledy spolu, dohodli se na tajném klíči pro šifrování zpráv. Alice nyní může svou zprávu zašifrovat pomocí tohoto klíče, což je podobné vložení zprávy do zamčené schránky, a Bob ji pak může dešifrovat stejným klíčem, což je jako otevření této schránky. Eva, i když zprávu zachytí, nebude moci schránku otevřít, protože nemá správný klíč. Tento způsob šifrování, kdy obě strany používají stejný klíč, se nazývá symetrická kryptografie. [x2]

[x2] https://www.cryptoquantique.com/blog/post-quantum-cryptography/

Obrázek 1 - Symetrická kryptografie v akci [x2]

V případě, že Alice a Bob chtějí komunikovat v tajnosti, ale nemohou se osobně setkat k výměně klíčů, mohou využít metodu kryptografie založené na veřejném a soukromém klíči. Bob si vytvoří dva klíče: jeden veřejný, který může bezpečně sdílet s celým světem a který slouží k šifrování zpráv určených pro něj, a druhý soukromý, který si nechá pro sebe a používá ho k dešifrování přijatých zpráv. Když Alice chce Bobovi poslat šifrovanou zprávu, najde jeho veřejný klíč a s jeho pomocí zprávu zašifruje. Tento proces zajišťuje, že i kdyby někdo jako Eva zprávu zachytil, bez přístupu k Bobovu soukromému klíči, tak by viděl pouze nesrozumitelný text. Po přijetí zprávy Bob použije svůj soukromý klíč k jejímu dešifrování a může si tak přečíst Alicinu zprávu. [x2]

V praxi je nepravděpodobné, že by se strany dokázaly dohodnout na klíči předem – zamyslete se nad tím, jak často musíte zadávat své bankovní údaje, abyste mohli nakupovat na webové stránce, kterou jste nikdy předtím nenavštívili. V důsledku toho jsou bezpečné techniky pro kryptografii veřejného klíče pro bezpečnost internetu nanejvýš důležité. Bohužel se ukazuje, že vytváření schémat s veřejnými klíči je docela obtížné a obvykle to trvá příliš dlouho, když chcete poslat spoustu informací. Naštěstí to jde snadno opravit. Alice a Bob začínají pomocí schématu veřejného klíče nebo podobné techniky známé jako protokol výměny klíčů, aby tajně sdělili jednu malou zprávu, která je pouze sdíleným klíčem. Poté použijí tento sdílený klíč s dobře zavedeným symetrickým schématem, typicky schématem nazývaným AES, aby pokračovali ve své tajné komunikaci bez režie, kterou vyžadují techniky veřejného klíče. Takto běžné internetové standardy, jako je  [TLS,](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://en.wikipedia.org/wiki/Transport_Layer_Security)  navrhují, aby byla v praxi zabezpečena komunikace. [x2]

Symetrická šifrovací metoda AES, která je v praxi od 90. let minulého století, je při správném použití považována za velmi bezpečnou. Nicméně, klíčovým bodem pro zabezpečení je fáze s veřejným klíčem. Bezpečnost systémů s veřejným klíčem je často založena na složitosti určitých matematických problémů, které jsou výpočetně náročné. Například, RSA šifrovací systém využívá veřejný klíč, který je velké číslo n, a soukromý klíč, který obsahuje informace umožňující faktorizaci n na dva prvočíselné faktory p a q, kde n = pq. Alice může zašifrovat zprávu pro Boba pomocí n, ale k dešifrování je potřeba znát p a q. Pro Boba je to jednoduché, protože zná obě prvočísla, ale pro každého, kdo zachytí zprávu, jako je Eva, je výzvou získat p a q faktorizací n. Shorův algoritmus, který se zabývá problémem faktorizace, je na současných počítačích neefektivní, pokud jsou p a q dostatečně velká. Bezpečnost jiných metod výměny veřejných klíčů je odvozena z jiných složitých matematických problémů, jako je například problém diskrétního logaritmu, a jejich bezpečnost je srovnatelná s obtížností řešení těchto problémů. [x2]

V oblasti digitální komunikace existuje klíčová otázka, jak může příjemce zprávy, jako je Bob, ověřit, že zpráva pochází opravdu od odesílatele, v tomto případě Alice, a že její obsah nebyl pozměněn. Tento problém je zvláště zásadní, když existuje riziko, že třetí strana, jako je Eva, může zprávu zachytit a potenciálně ji upravit. V digitálním světě se tento problém řeší pomocí technologie známé jako digitální podpisy. Alice použije svůj soukromý klíč, který je v podstatě její digitální podpisovou schopností, aby připojila k zprávě unikátní podpis. Tento podpis slouží jako důkaz, že zpráva pochází od ní, a zároveň zaručuje, že obsah zprávy nebyl změněn, protože jakákoli manipulace s obsahem by způsobila, že podpis by se zdál být neplatný. Když Bob obdrží zprávu, může pomocí Alicina veřejného klíče, který je volně dostupný, ověřit, že podpis odpovídá a že zpráva nebyla pozměněna. Tento proces je založen na složitých matematických principech, které zajišťují, že padělání podpisu je stejně obtížné jako vyřešení určitého matematického problému. V případě běžně používaného schématu digitálního podpisu, známého jako ECDSA, by Eva musela vyřešit matematický problém zvaný diskrétní logaritmus v kontextu eliptických křivek, což je úkol s vysokou úrovní obtížnosti. [x2]

[x2] https://www.cryptoquantique.com/blog/post-quantum-cryptography/

## Shorův algoritmus

Shorův kvantový faktorizační algoritmus je revoluční metoda pro rozklad velkých čísel na prvočísla pomocí kvantového počítání. Vytvořený v roce 1994 Peterem Shorem, algoritmus využívá kvantové superpozice a provázání k odhalení periody funkce, což je zásadní pro faktorizaci. Základem je kvantová Fourierova transformace, která umožňuje kvantovému počítači zpracovat všechny možné vstupy najednou. Algoritmus začíná výběrem náhodného čísla a jeho zpracováním pomocí modulární aritmetiky k nalezení periody. Tato perioda je pak klíčem k faktorizaci, což má důležité implikace pro kryptografii, zejména pro šifrování RSA. Shorův algoritmus, v případě existence funkční kvantových počítačů, silně ovlivní bezpečnost současné digitální komunikace. [x3]

[x3]https://cs.eitca.org/kvantov%C3%A1-informace/eitc-qi-qif-kvantov%C3%A9-informa%C4%8Dn%C3%AD-z%C3%A1klady/Shors%C5%AFv-algoritmus-kvantov%C3%A9ho-faktoringu/shors-factoringov%C3%BD-algoritmus/p%C5%99ezkoum%C3%A1n%C3%AD-zkou%C5%A1ky-shors-factoring-algorithm/jak%C3%A1-je-kl%C3%AD%C4%8Dov%C3%A1-my%C5%A1lenka-za-algoritmem-kvantov%C3%A9ho-faktoringu-shors-a-jak-vyu%C5%BE%C3%ADv%C3%A1-kvantov%C3%A9-vlastnosti-k-nalezen%C3%AD-periody-funkce/

## NIST a jeho zapojení do pokroku v postkvantové kryptografii

Národní institut pro standardy a technologie, známý jako NIST, je prestižní federální agentura, která byla založena na počátku 20. století a od té doby hraje klíčovou roli ve vědeckém a průmyslovém pokroku Spojených států. Jeho založení bylo reakcí na potřebu zlepšit měřicí infrastrukturu v USA, která byla v té době považována za nedostatečnou ve srovnání s jinými průmyslovými mocnostmi, jako bylo Spojené království nebo Německo. Díky své práci v oblasti vývoje a normalizace měřicích metod a technologií se NIST stal základním kamenem pro inovace a udržitelný růst v mnoha odvětvích. [x4]

NIST se podílí na široké škále výzkumných a vývojových projektů, od základních fyzikálních studií až po pokročilé aplikace v nanotechnologiích a kybernetické bezpečnosti. Jeho práce zahrnuje vývoj atomových hodin, které jsou základem pro přesné měření času a synchronizaci globálních komunikačních sítí, a také vývoj nových materiálů s výjimečnými vlastnostmi, které nacházejí uplatnění v nejnovějších technologických zařízeních. NIST také hraje klíčovou roli v oblasti kybernetické bezpečnosti, kde vyvíjí a propaguje rámce a standardy pro ochranu kritické infrastruktury a soukromých dat. [x4]

V současné době NIST nadále rozšiřuje své působení a poskytuje podporu pro nejnovější technologické inovace. Jeho měření a standardy jsou nezbytné pro vývoj a provoz zařízení v nanoměřítku, která jsou tak malá, že desítky tisíc z nich mohou být umístěny na konci jediného lidského vlasu. NIST také přispívá k bezpečnosti velkých staveb, jako jsou mrakodrapy navržené tak, aby odolaly zemětřesením, a k rozvoji globálních komunikačních sítí, které jsou základem moderní společnosti. [x4]

NIST je tedy nejen svědkem, ale i tvůrcem historie v oblasti vědy a technologie. Jeho odkaz a pokračující práce jsou zásadní pro pokrok a bezpečnost po celém světě. S jeho pomocí se podařilo překonat mnohé výzvy a otevřít dveře k novým možnostem v různých průmyslových a vědeckých oborech. [x4]

V roce 2017 NIST zahájil proces výběru, hodnocení a standardizace jednoho nebo více algoritmů pro kvantově odolné veřejné klíčové kryptografie. Tyto algoritmy mají nahradit stávající, které jsou zranitelné vůči útokům kvantových počítačů. Nové standardy mají zahrnovat algoritmy pro digitální podpisy, šifrování a vytváření klíčů, které budou dostupné celosvětově a ochrání citlivé informace vlády i po vzniku kvantových počítačů. Jako první krok NIST vyžádal veřejné komentáře k návrhům minimálních požadavků na přijatelnost, požadavků na předložení a kritérií pro hodnocení kandidátních algoritmů. Komentáře i shrnutí změn, které byly provedeny na základě těchto komentářů, byly zveřejněny. Nominace na post-kvantové kandidátní algoritmy mohly být podány až do konečného termínu 30. listopadu 2017. [x4]

[x4] <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>

Tato otevřenost je hlavním rysem procesu NIST. Dokonce existuje  [veřejná google skupina](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://groups.google.com/a/list.nist.gov/forum/%23!forum/pqc-forum) [x5] obsahující podrobné diskuse o konkrétních kandidátských schématech a také o obecnějších rysech procesu. Původně bylo předloženo 69 kandidátů, i když hrstka se rychle stáhla poté, co byly objeveny chyby, a v lednu 2019 NIST ukončil první kolo procesu a oznámil 26 algoritmů, které se dostaly do druhého kola. V červenci 2020, po téměř 18 měsících soustředění komunity na tato schémata, NIST oznámil své kandidáty do posledního kola: 4 mechanismy zapouzdření klíčů a 3 schémata podpisů, se záměrem vybrat na konci procesu alespoň jeden z každého typu. [x2]

Na začátku července 2022 byly konečně vybrány 4 algoritmy, které komunita uznala za kvantově bezpečné. CRYSTALS-Kyber pro výměnu klíčů a CRYSTALS-DILITHIUM, Falcon a SPHINCS+ pro digitální podpisy. [x6]

[x2] https://www.cryptoquantique.com/blog/post-quantum-cryptography/

[x5] <https://groups.google.com/a/list.nist.gov/g/pqc-forum?_x_tr_sl&_x_tr_tl&_x_tr_hl&pli=1>

[x6] <https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/selected-algos-2022/history-pqc-selected-algorithm-updates.pdf>

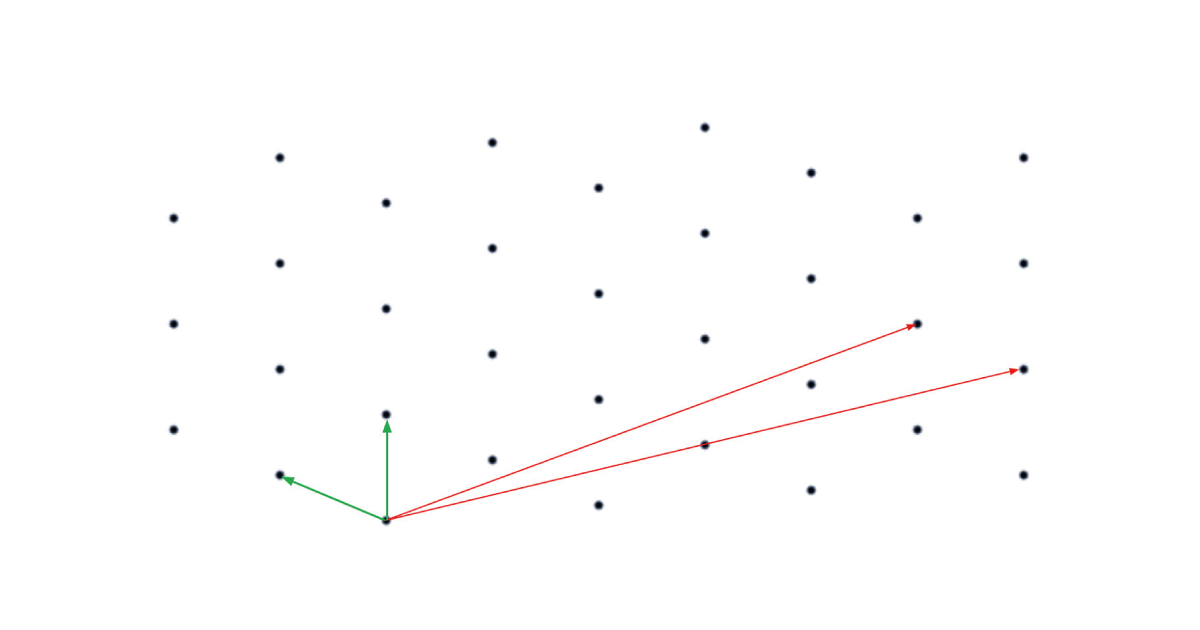
## Postkvantové algoritmy a jejich implementace

Kryptografie založená na mřížkách

Mřížky využívají dvou matematických problémů, které je dělají prozatím imunní vůči kvantovým počítačům. Jedná se o problém Shortest Vector Problem (SVP) a Closest Vector Problem (CVP).

Problematika SVP je spojena s hledáním nejkratšího vektoru báze. Lze si to představit na příkladu, kdy máme zadanou mřížku 𝐿, libovolnou bázi a cílem je najít nejkratší nenulový vektor, který do mřížky patří. Je třeba si uvědomit, že se hledá bod mřížky, který je nejblíže nule, ale není nulový.

Druhou problematikou je CVP(Closest Vector Problem), která je spojena s nalezením nejbližšího vektoru vůči libovolnému vektoru mřížky. Problematika se opírá o dvě báze vektorového prostoru. Jednoduchou a složitou. Jednoduchá obsahuje krátké a pokud možno na sebe kolmé vektory, které snadno popisují celou mřížku. Naopak složitá báze obsahuje velké vektory s podobným směrem. Popsat jimi celou mřížku, z definice báze samozřejmě jde, ale je to o dost náročnější. Ovšem nalézt nejbližší vektor mřížky vůči zadanému vektoru je podstatně náročnější než s využitím jednoduché báze. [x7] [x8]



Obrázek 2 - Mříž se dvěma různými základnami [x2]

Obrázek popisuje mřížku v nejjednodušším dvojrozměrném vektorovém prostoru, ovšem ta slouží pouze pro ilustraci problému, ale v realitě se využívají mřížky ve značně vyšším řádu rozměrů vektorového prostoru. [x2]

[x7] POPELOVÁ, Lucie. Metody postkvantové kryptografie. Brno, 2018, 55 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Lukáš Malina, Ph.D.

[x8] https://www.youtube.com/watch?v=QDdOoYdb748

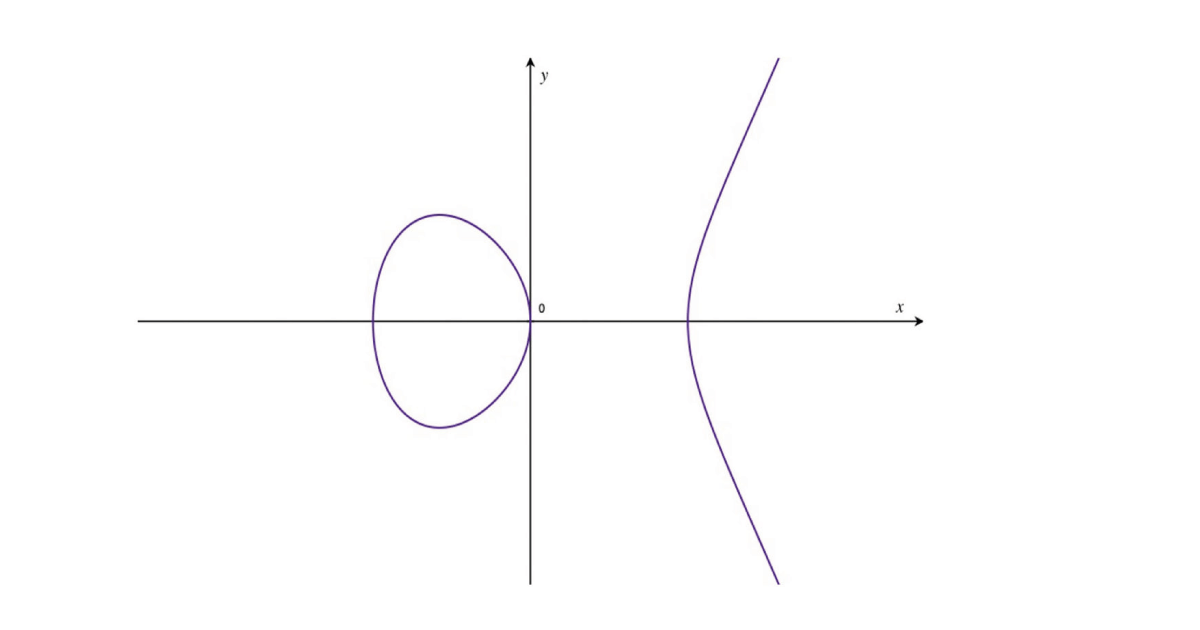
Kvantově těžké problémy

Kryptografie založená na kódu je nejstarší ze čtyř hlavních rodin, datuje se od vývoje kryptosystému  [McEliece](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://en.wikipedia.org/wiki/McEliece_cryptosystem)  v roce 1978. Je založena na oblasti teorie kódování, která je studiem toho, jak úspěšně přenášet informace přes nespolehlivý kanál. K odesílání informací tímto způsobem používáte něco, čemu se říká kód pro opravu chyb, kde je zpráva zakódována způsobem, který toleruje určité množství chybných dat pocházejících z nespolehlivého kanálu, přičemž příjemce je stále schopen obnovit zamýšlenou zprávu. . Soukromý klíč pro kryptosystém založený na tomto je jen dobře zvolený kód pro opravu chyb a odpovídající veřejný klíč je recept na zakódování zprávy, která má být dekódována. Šifrování je jednoduché – odesílatel provede obvyklý proces kódování zprávy a poté simuluje nespolehlivý kanál ručním zadáním některých chyb. Dokud existuje dostatek chyb, protivník bez přístupu k popisu kódu pro opravu chyb nemůže zprávu obnovit, zatímco zamýšlený příjemce je schopen ji dekódovat pomocí svého kódu pro opravu chyb. Pěkné na těchto schématech je, že McEliece existuje již dlouhou dobu, a proto existuje velká míra důvěry v jejich bezpečnost a schémata jemu podobná. Na druhou stranu, McEliece existuje už dlouho a nikdo ho nepoužívá – má velmi velké veřejné klíče, což může trochu zpomalit, a obecně se špatně srovnává s RSA v předkvantové éře .

Vícerozměrná kryptografie je založena na problému řešení systémů mnohorozměrných polynomiálních rovnic, typicky vícerozměrných kvadratických. Tedy soustava rovnic, která vypadá takto:

Ačkoli mnoho existujících forem kryptografie eliptických křivek, jako je ECDSA, je citlivých na kvantové počítače, je to důsledek specifické povahy algoritmů a nikoli slabina samotných eliptických křivek. Abychom kryptografii založili na izogeniích, použijeme následující pozorování: vzhledem ke dvěma eliptickým křivkám E1 a E2 je těžké najít izogenii φ, která posílá E1 na E2. Veřejný klíč by tedy mohl být pár eliptických křivek, se soukromým klíčem odpovídající izogeneze φ: E1 -> E2. Nyní může vlastník soukromého klíče použít izogenii φ k výpočtu operací zahrnujících E1 a E2, které jsou neovladatelné pro někoho, kdo nemá přístup k φ, a jako obvykle lze k nastavení těchto problémů použít veřejný pár E1 a E2. Přestože je oblast kryptografie na bázi izogeny stále v relativních plenkách, v kryptografické komunitě je o ní značné vzrušení, zejména po  [úspěšných experimentech](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://www.imperialviolet.org/2019/10/30/pqsivssl.html)  s využitím schémat založených na izogenii v internetových protokolech. Navíc působivě efektivní schéma podpisů nazvané SQISign, založené na novém problému v kryptografii založené na izogenii, získalo na letošní konferenci Asiacrypt cenu za nejlepší knihu .

Ačkoli mnoho existujících forem kryptografie eliptických křivek, jako je ECDSA, je citlivých na kvantové počítače, je to důsledek specifické povahy algoritmů a nikoli slabina samotných eliptických křivek. Abychom kryptografii založili na izogeniích, použijeme následující pozorování: vzhledem ke dvěma eliptickým křivkám E1 a E2 je těžké najít izogenii φ, která posílá E1 na E2. Veřejný klíč by tedy mohl být pár eliptických křivek, se soukromým klíčem odpovídající izogeneze φ: E1 -> E2. Nyní může vlastník soukromého klíče použít izogenii φ k výpočtu operací zahrnujících E1 a E2, které jsou neovladatelné pro někoho, kdo nemá přístup k φ, a jako obvykle lze k nastavení těchto problémů použít veřejný pár E1 a E2. Přestože je oblast kryptografie na bázi izogeny stále v relativních plenkách, v kryptografické komunitě je o ní značné vzrušení, zejména po  [úspěšných experimentech](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://www.imperialviolet.org/2019/10/30/pqsivssl.html)  s využitím schémat založených na izogenii v internetových protokolech. Navíc působivě efektivní schéma podpisů nazvané SQISign, založené na novém problému v kryptografii založené na izogenii, získalo na letošní konferenci Asiacrypt cenu za nejlepší knihu .

*Eliptická křivka ve dvou částech*

Zbývající 4 schémata zapouzdření klíče jsou NTRU, klasické schéma založené na mřížce využívající techniky pocházející z 90. let, CRYSTALS-Kyber, modernější schéma mřížky založené na problému zvaném Module LWE, SABRE, ještě modernější schéma založené na mřížce. na „zakulaceném“ problému zvaném Module LWR a Classic McEliece, modernizaci schématu založeného na kódu z konce 70. let. Tato tři mřížková schémata lze považovat za výběr různých kompromisů mezi bezpečností a efektivitou: na jedné straně SABRE funguje lépe než CRYSTALS-Kyber, který zase funguje lépe než NTRU. Naopak NTRU má nejlépe zavedené bezpečnostní vlastnosti, zatímco SABRE se spoléhá na problém modulu LWR, který stále není příliš dobře pochopen, přičemž spoléhání CRYSTALS-Kyber na modul LWE jej opět umisťuje doprostřed. Classic McEliece má horší výkon než jeho konkurenti na bázi mřížky, ale mohl by být standardizován jako bezpečný pro případ selhání v případě, že by se ukázalo, že síla kvantových útoků na mřížková schémata byla značně podceněna; rozmanitost v kryptografických předpokladech může být mocným nástrojem tváří v tvář neznámému. NIST naznačil, že pravděpodobně zpočátku zvolí jeden z NTRU nebo CRYSTALS-Kyber ke standardizaci, ale důkladnější bezpečnostní analýza SABER nebo kvantové útoky na mřížky by mohly změnit jejich směr.

Když obrátíme svou pozornost na podpisová schémata, znovu vidíme, že mřížky jsou pravděpodobnou budoucností PQC. Dva ze tří zbývajících kandidátů používají mřížky: CRYSTALS-Dilithium, podpisové schéma vyvinuté stejným týmem jako CRYSTALS-Kyber s použitím podobných technik, a Falcon, podpisové schéma podobné NTRU s několika novými technickými příspěvky. Další zbývající schéma, Rainbow, je vícerozměrné schéma s horším celkovým výkonem než jeho mřížkové protějšky. Podobně jako v případě Classic McEliece se NIST domnívá, že je přínosné zahrnout kandidáty bez mřížky, a relativní mládí Rainbow jako schématu znamená, že je možné, že by mohl být v blízké budoucnosti vylepšen, nebo by mohl vynikat v konkrétních případech použití. . NIST opět navrhl, že pravděpodobně standardizují jedno ze dvou mřížkových schémat: Falcon je pravděpodobně o něco efektivnější, ale přichází s podstatnými technickými komplikacemi při implementaci, které mohou vést k tomu, že je považován za zbytečně komplikovaný ve srovnání s elegantnějším designem. CRYSTALS-Dilithium, který si stále vede velmi dobře.

NIST také vybírá 8 schémat jako „alternativní“, schémata, která by podle jejich názoru měla být dále studována, protože NIST jsou otevřeny možnosti jejich standardizace v budoucnu. Vybrané alternativy mají kombinaci žádoucích vlastností a pozoruhodných nedostatků: mohou být například vysoce bezpečné, ale dosti neefektivní, vyžadují větší racionalizaci nebo postrádají potřebnou úroveň vystavení odhodlaným útočníkům, což je typické při vytváření důvěry v kryptografické zabezpečení. Z pěti klíčových alternativ zapouzdření lze čtyři nejlépe pochopit ve srovnání s finalisty: FrodoKEM lze považovat za konzervativnější verzi CRYSTALS-Kyber, která běží pomaleji, ale je bezpečnější, a NTRU Prime je schéma podobné NTRU, které funguje předpokládaná slabost v jiných technikách mřížky a malé náklady na efektivitu. Bike a HQC jsou dvě moderní šifrovací schémata založená na kódu, která fungují efektivněji než Classic McEliece, ale zavádějí nové bezpečnostní předpoklady, a proto potřebují podstatně větší kontrolu. Páté schéma, SIKE, je jediným zbývajícím kryptosystémem založeným na izogenii v procesu. NIST se domníval, že SIKE není dostatečně vyspělý, aby mohl být standardizován, ale jeho jedinečnost znamená, že je to kandidát, který pravděpodobně podstoupí seriózní výzkumné úsilí v budoucnu. Co se týče alternativních podpisů, pouze jeden má nějakou podobnost s finalisty: schéma známé jako GeMSS, které úzce konkuruje Rainbow, ale očekává se, že bude ve většině aplikací méně žádoucí. Další dvě alternativy, SPHINCS+ a Picnic, jsou založeny na hashovacích funkcích. Oba běží dost pomalu, ale mají extrémně silné bezpečnostní záruky, takže mohou být standardizovány pro použití s ​​vysoce citlivými daty nebo v případě kvantového „Armageddonu“, kde se ukazuje, že kvantové počítače mohou prolomit kryptografii, která používá cokoli složitějšího než jednoduchá primitiva, jako je hash. funkce .

Kyber

DILITHIUM

Falcon

Sphincsplus

# Přehled ochraných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty

V tomto článku se podíváme na některé z nejčastějších ochranných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty. Data jsou cenným aktivem každé organizace a jejich ztráta, únik nebo zneužití může mít vážné následky pro její provoz, pověst a finanční výsledky. Proto je důležité mít správně nastavené procesy a nástroje pro ochranu dat před různými hrozbami.

Jedním z nejzákladnějších ochranných mechanismů je zálohování dat. Zálohování dat znamená pravidelné kopírování dat z primárního úložiště na sekundární úložiště, které je fyzicky oddělené a chráněné před neoprávněným přístupem. Zálohování dat umožňuje obnovit data v případě jejich poškození, smazání nebo ztráty způsobené například hardwarovou poruchou, lidskou chybou, malwarem nebo přírodní katastrofou. Zálohovaná data by měla být pravidelně testována a verifikována, aby byla jistota jejich konzistence a dostupnosti.

Dalším důležitým ochranným mechanismem je archivace dat. Archivace dat znamená ukládání dat, která již nejsou aktivně používána, ale jsou stále potřebná pro historické, právní nebo regulační účely, do speciálního úložiště, které je optimalizované pro dlouhodobé uchování dat. Archivovaná data jsou obvykle neměnná, což znamená, že se nedají měnit ani mazat. Tím se snižuje riziko manipulace s daty nebo jejich zničení. Archivovaná data by měla být také šifrována a podepsána digitálním podpisem, aby byla zajištěna jejich důvěrnost a integrita.

Kromě zálohování a archivace dat je také nutné zajistit bezpečnost dat v provozu, tedy v době, kdy jsou data ukládána, přenášena nebo zpracovávána v informačním systému. K tomu slouží různé techniky, jako je šifrování dat, autentizace a autorizace uživatelů a aplikací, auditování a monitorování aktivit v systému, detekce a prevence útoků, firewall a antivirový software. Tyto techniky pomáhají chránit data před neoprávněným přístupem, změnou nebo odcizením ze strany interních nebo externích aktérů.

# Mikroslužba zabezpečující postkvantovou kryptografii

První mikroslužbou, kterou bych chtěl popsat je ta, která zabezpečuje odesílání zpráv zašifrovaných a podepsaných pomocí postkvantové kryptografie. Její primární úkol je vcelku jednoduchý. Vzít zprávu a odeslat ji na požadovanou adresu. Ovšem, aby se tak mohlo stát i v postkvantovém světě, je potřeba série několika kroků popsaných níže. Tato mikroslužba obsahuje tři entity. Alice, Bob a Certifikační autorita. Pro ukázku funkčnosti této mikroslužby Alice každou vteřinu odesílá Bobovi zprávu, kterou on přijme, vytiskne na obrazovku a odešle Alici odpověď. Pro podepisování a šifrování zpráv využívají entity postkvantové algoritmy uvedené v kapitole 2.

## Popis jednotlivých částí

* Alice – entita, která odesílá Bobovi podepsanou a zašifrovanou zprávu a čeká na odpověď, kterou posléze dešifruje, ověří její podpis a vytiskne na monitor.
* Bob – entita, který od Alice přijímá zprávu, dešifruje ji, ověří její podpis, zprávu vytiskne na monitor a následně odešle zpět podepsanou a zašifrovanou odpověď.
* Certifikační autorita poskytuje Alici a Bobovi klíče pro podepisování a ověření podpisů.

## Nastavení symetrického klíče

První věc, kterou jakákoliv entita musí provést, pokud chce komunikovat s někým další je stanovit si bezpečný (zašifrovaný) komunikační kanál. Pro tento účel mají Alice, Bob i CA v modulu communication.py asynchronní funkci: async def define\_symmetric\_key(url, ALGORITHM, my\_address, pk, sign\_sk = None)

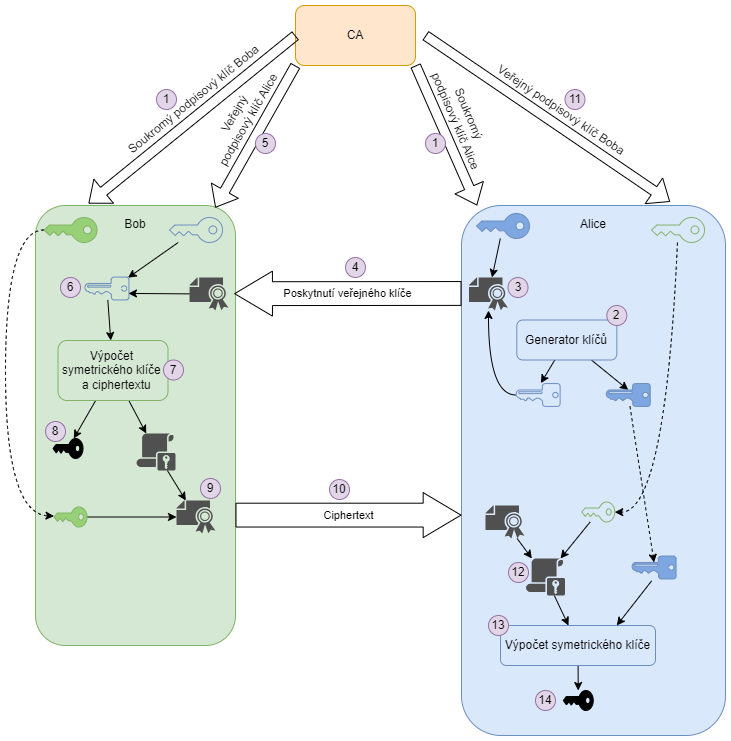
Tato funkce naváže spojení s druhou stranou a vzájemně si vymění informace takovým způsobem, aby výsledkem byl symetrický klíč, se kterým následně mohou otevřít nové, zašifrované spojení. Symetrický klíč jako takový nebyl nikdy poslán po síti, a tedy nikdo, kromě zúčastněných stran, o klíči nemůže vědět a komunikace je tedy bezpečná. Podrobný popis komunikace uvádím na dvou obrázcích níže. Oba ukazují výměnu symetrického klíče, ale liší se v tom, s jakými informacemi strany disponují. Na prvním obrázku Alice nevlastní svůj soukromý podpisový klíč, a tedy nemá, jak svoji zprávu podepsat. Taková situace je akceptována pouze mezi Alicí/Bobem a CA, a to pouze tehdy pokud se jedná o první navázání spojení za účelem registrace Alice/Boba u CA. Druhý obrázek popisuje standardní výměnu symetrického klíče pro už zaregistrované entity u CA.

Obsah obrázku text, diagram, snímek obrazovky

Popis byl vytvořen automaticky

Obrázek 10 – Popis výměny symetrického klíče mezi Alicí a CA

1. Uživatel vloží do zdrojového adresáře veřejný klíč CA ve tvaru „CA\_public\_key.pem“. To udělá ještě před spuštěním Alice. Pokud je CA umístěna ve stejném adresáři jako Alice, uživatel nemusí ručně nic vkládat.
2. Alice vygeneruje dvojici soukromého a veřejného KEM klíče.
3. Alice svůj veřejný klíč, v plaintextové podobě, odešle CA.
4. CA s využitím veřejného klíče Alice vygeneruje ciphertext a symetrický klíč.
5. CA v tuto chvíli vlastní symetrický klíč, kterým bude pozdější komunikace šifrována.
6. CA vezme vygenerovaný ciphertext a podepíše ho svým soukromým podpisovým klíčem.
7. CA odesílá Alici podepsaný ciphertext.
8. Alice ověří podpis pomocí veřejného podpisového klíče CA a získá tak ciphertext.
9. Alice vygeneruje stejný symetrický klíč, jako má CA, díky znalosti ciphertextu a svého soukromého KEM klíče vygenerovaného v kroku 2.
10. Alice vlastní symetrický klíč, kterým bude šifrována pozdější komunikace.



Obrázek 11 - Popis výměny symetrického klíče mezi Alicí a Bobem

1. Alice a Bob získají od CA svůj soukromý podpisový klíč (bude vysvětleno v 6.3).
2. Alice vygeneruje dvojici soukromého a veřejného KEM klíče.
3. Alice podepíše vygenerovaný veřejný klíč svým soukromým podpisovým klíčem.
4. Alice odešle Bobovi svůj podepsaný veřejný klíč.
5. Bob získá od CA veřejný podpisový klíč Alice (bude vysvětleno v 6.3).
6. Bob ověří podpis a získá tak veřejný klíč Alice.
7. Bob, s pomocí veřejného klíče Alice, vygeneruje ciphertext a symetrický klíč.
8. Bob v tuto chvíli vlastní symetrický klíč, kterým bude pozdější komunikace šifrována.
9. Bob vezme vygenerovaný ciphertext a podepíše ho svým soukromým podpisovým klíčem.
10. Bob odesílá Alici podepsaný ciphertext.
11. Alice získá od CA veřejný podpisový klíč Boba (bude vysvětleno v 6.3).
12. Alice ověří podpis pomocí veřejného podpisového klíče Boba a získá tak ciphertext.
13. Alice vygeneruje stejný symetrický klíč, jako má Bob, díky znalosti ciphertextu a svého soukromého klíče vygenerovaného v kroku 2.
14. Alice vlastní symetrický klíč, kterým bude šifrována pozdější komunikace.

## Získání podpisových klíčů a práce s nimi

Teorii o podpisových algoritmech a klíčích jsem uvedl v kapitole 1 této práce včetně seznamu dostupných algoritmů a jejich činnosti. V této podkapitole už tedy zobecním činnost postkvantových kryptografických podpisových algoritmů na tři základní funkce: generování klíčů, výpočet symetrického klíče a ciphertextu, výpočet symetrického klíče.

V této podkapitole popíšu, jakým způsobem entity získávají soukromé a veřejné podpisové klíče. Než se k vysvětlení dostanu, rád bych nejprve popsal, jak přesně vypadá zpráva, která je podepsána soukromým klíčem podepisovatele.

JWT

Pro podepsanou zprávu využívám formát JSON web token (dále jen JWT). Jedná se o ustálený standard pro podepisovaní tokenů, nebo zpráv [1]. Je tvořen třemi Base64 zakódovanými částmi oddělenými tečkami: header (hlavička), payload (náplň) a signature (podpis).

* Hlavička obsahuje informace o tom, jak je zpráva podepsána.
* Náplň (payload) obsahuje data.
* Podpis (signature) je vytvořen pomocí algoritmu založeného na obsahu zprávy a tajným klíčem. Slouží k ověření integrity tokenu [1].

Protože jsem nenašel veřejnou knihovnu pro práci s JWT, která by zahrnovala buď postkvantové algoritmy, nebo by umožňovala přiložit vlastní podpisový algoritmus, napsal jsem vlastní implementaci JWT. Při jejím vývoji jsem bral ohled na komptabilitu s veřejnou Python knihovnou PyJWT [2]. Zajistil jsem tak, aby projekty, které by použily moji verzi JWT, měli jednoduchý přestup na knihovnu PyJWT ve chvíli, kdy i ona začne nabízet podepisovaní pomocí postkvantových algoritmů. Zdrojový kód implementace JWT najdete v modules/jwt.py.

Součástí mé implementace jsou dvě funkce. První je def encode(payload, key, alg), která vytvoří podepsaný JWT. Parametry této funkce jsou:

* payload – zpráva, kterou chceme odeslat a další atributy)
* key – podpisový klíč, kterým chceme zprávu podepsat
* alg – název podepisovacího algoritmu.

Druhá funkce se jmenuje jwt.decode(jwt, public\_key, alg=None) a slouží k dekódování JWT formátu. Funkce nejprve ověří podpis zprávy a pokud podpis souhlasí, tak JWT dekóduje a vrátí obsah zprávy. Protože JWT hlavička obsahuje informace o použitém podpisovém algoritmu, není parametr „alg“ důležitý a funkce může být zavolána bez něj. Pro dodržení kompatibility s knihovnou PyJWT, jsem možnost volby podpisového algoritmu ve volání funkce zahrnul, tak aby byl upřednostněn parametr volané funkce, před algoritmem uloženým v hlavičce JWT.

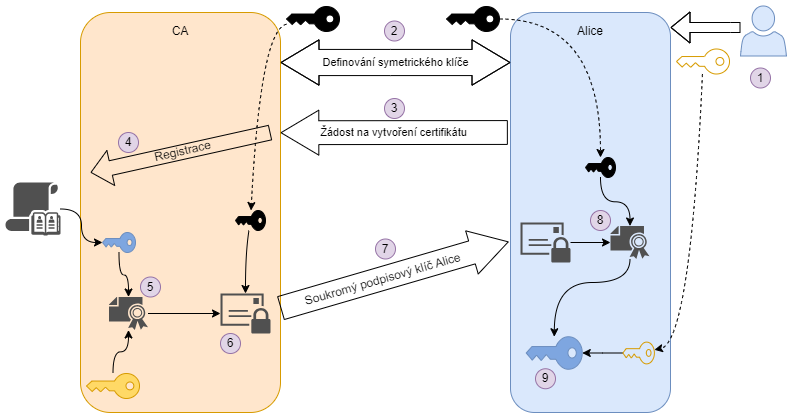
[1] <https://datatracker.ietf.org/doc/html/rfc7519>

[2] <https://pyjwt.readthedocs.io/en/stable/>

Získání soukromého podepisovacího klíče

Každá entita, pokud chce komunikovat v síti musí vlastnit svůj soukromý podpisový klíč. Bez něj nedokáže podepsat zprávu, kterou by chtěla odeslat a druhá strana by neměla, jak ověřit, kdo je skutečným odesílatelem. V mé mikroslužbě PQC-service je získání soukromého podpisového klíče prováděno hned při startu entity (Alice/Bob). Po načtení konfiguračního souboru je zavolána funkce async def get\_sign\_private\_key(my\_address, CA, ALGORITHM), která má tři parametry:

* my\_address – informace o adrese a portu na kterém běží entita
* ca – informace o adrese a portu certifikační autority (získáno z konf. souboru)
* algorithm – algoritmy, které bude pro komunikaci entita využívat(z konf. souboru)

Výsledkem je podpisový soukromý klíč na straně entity, která o klíč žádala a uložený certifikát o službě na straně CA.

Obrázek 12 - Popis žádosti o soukromý podpisový klíč

1. Uživatel vloží do zdrojového adresáře veřejný klíč CA ve tvaru „CA\_public\_key.pem“. To udělá ještě před spuštěním Alice. Pokud je CA umístěna ve stejném adresáři jako Alice, uživatel nemusí ručně nic vkládat.
2. Alice a CA si vymění symetrické klíče. Popsáno v kapitole 6.2.
3. Alice posílá žádost CA o vytvoření certifikátu.
4. CA vytvoří Alici certifikát.
5. CA vezme soukromý podpisový klíč Alice a podepíše ho svým soukromým podpisovým klíčem.
6. CA vezme podepsaná klíč Alice a zašifruje ho symetrickým klíčem.
7. CA odešle zašifrovaný podepsaný klíč Alici.
8. Alice dešifruje zprávu pomocí symetrického klíče.
9. Alice ověří podpis pomocí veřejného podpisového klíče CA, získá tak svůj soukromý podpisový klíč.

Získání veřejného podpisového klíče

Další důležitá funkcionalita, která umožňuje všem entitám zeptat se CA na veřejný klíč jiné požadované entity. Například pokud Alice odešle podepsanou zprávu Bobovi, tak se Bob dotáže CA na veřejný klíč Alice. Tímto klíčem je následně schopný ověřit, zda zprávu skutečně odeslala Alice. Asynchronní funkce, kterou by Bob zavolal je

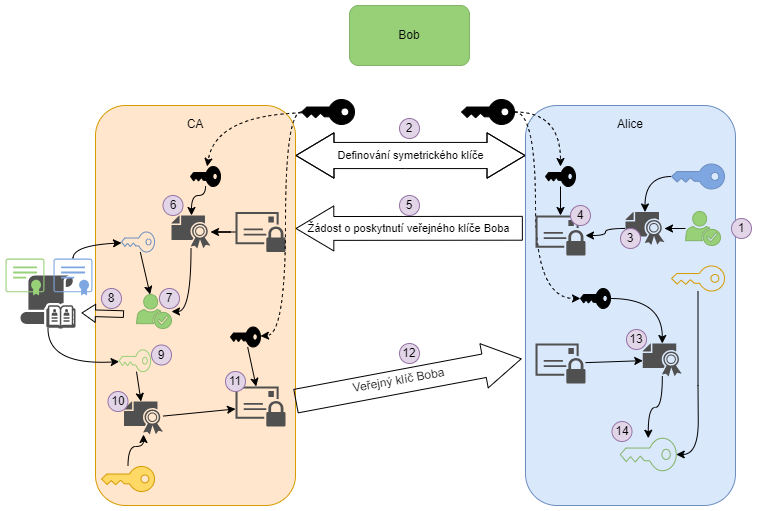
async def ask\_public\_key(subject, sign\_private\_key, my\_address, CA, ALGORITHM), která má 5 parametrů:

* subjekt – identifikátor, pod kterým je entita uložena u CA.

V mé práci se jedná o formát „ip adresa:port“.

* sign\_private\_key – soukromý podpisový klíč entity, která se dotazuje CA.
* my\_address – adresa entity
* ca – informace o CA
* algorithm – informace o zvolených algoritmech

Následující obrázek uvádí podrobný popis komunikace a procesů nutných k tomu, aby Alice mohla získat od CA veřejný podpisový klíč Boba.



Obrázek 13 - Popis žádosti o veřejný podpisový klíč

1. Vstupní informace pro Alici jsou: vlastní soukromý podpisový klíč a veřejný podpisový klíč CA. Alice také potřebuje znát identifikátor Boba. Ten získá například z hlavičky přijaté zprávy od Boba.
2. Alice a CA si vymění symetrické klíče pro šifrování. Popsáno v kapitole 6.2
3. Alice podepíše identifikátor Boba svým soukromým podpisovým klíčem.
4. Alice zašifruje zprávu pomocí symetrického klíče.
5. Alice odešle zašifrovanou zprávu CA
6. CA pomocí symetrického klíče dešifruje zprávu.
7. CA pomocí veřejného podpisového klíče ověří podpis. (klíč má uložen ve své databázi)
8. CA prověří, zda má Boba uloženého ve své databázi.
9. CA vezme veřejný podpisový klíč Boba.
10. CA podepíše veřejný podpisový klíč Boba svým soukromým podpisovým klíčem.
11. CA zašifruje zprávu pomocí symetrického klíče.
12. CA odešle zašifrovanou zprávu Alici.
13. Alice pomocí symetrického klíče dešifruje zprávu.
14. Alice veřejným podpisovým klíčem CA ověří podepsanou zprávu a získá tak veřejný podpisový klíč Boba.

## Průběh komunikace při odeslání zprávy

Dostávám se téměř do úplného závěru této kapitoly. Po objasnění všech dílčích kroků se můžeme konečně vrhnout k té nejkomplexnější funkci. A to je samotné odeslání zprávy. Zahrnuje všechny předchozí typy komunikací a přidává k nim ještě tu samotnou zprávu. Asynchronní funkce, která odeslání zprávy umožňuje se nazývá „send\_request“ a je definovaná v tomto tvaru:

async def send\_request(ip\_address, port, payload, sign\_private\_key, my\_address, CA, ALGORITHM, uri="").

Její parametry:

* ip\_address – adresa adresáta
* port – port adresáta
* payload – obsah zprávy
* sign\_private\_key – soukromý podpisový klíč entity, která tuto funkci zavolala
* my\_address – informace o entitě, která tuto funkci zavolala
* ca – informace o CA
* algorithm – informace o zvolených algoritmech
* uri – přímá specifikace koncového bodu, kam má být zpráva odeslána

Na následujícím, prozatím nejsložitějším, obrázku se pokusím objasnit dílčí kroky, které zajistí správné a bezpečné doručení zprávy od Alice k Bobovi a její odpovědi od Boba zpět Alici. Obsah obrázku diagram, mapa, text, Plán

Popis byl vytvořen automaticky

Obrázek 14 – Odeslání zprávy

1. Alice a Bob se zaregistrují u CA. Získají tak své soukromé podpisové klíče.
2. Alice (uživatel) napíše zprávu.
3. Alice zprávu podepíše svým soukromým podpisovým klíčem.
4. Alice a Bob si vymění symetrické klíče pro šifrování.
5. Alice zašifruje zprávu symetrickým klíčem.
6. Alice odešle zprávu Bobovi.
7. Bob dešifruje zprávu pomocí symetrického klíče.
8. Bob si vyžádá od CA veřejný podpisový klíč Alice.
9. Bob ověří podpis na zprávě od Alice.
10. Bob vyhodnotí samotný obsah zprávy a napíše odpověď.
11. Bob podepíše odpověď svým soukromým podpisovým klíčem.
12. Bob zašifruje podepsanou odpověď symetrickým klíčem.
13. Bob odešle odpověď.
14. Alice dešifruje odpověď symetrickým klíčem.
15. Alice si vyžádá veřejný podpisový klíč Boba.
16. Alice ověří podpis na odpovědi.
17. Alice získala odpověď na svoji zprávu.

## Průvodce pro spuštění mikroslužby

Návod na spuštění

Předpoklady:

Python 3.12.2

Git

Microsoft Visual C++ 14.0 nebo novější (https://visualstudio.microsoft.com/visual-cpp-build-tools/)

stáhněte repozitář

git clone -b PQC-service https://github.com/naxit-01/DiplomovaPrace.git

spusťte setup.bat. Tento script vytvoří virtuální prostředí jazyka Python a do něj nainstaluje potřebné knihovny. Pozor, proces trvá přibližně 5 minut.

Při instalaci byly vytvořené tři nové scripty. activate\_alice.bat, activate\_ca.bat, activate\_bob.bat

Spuťte script activate\_ca.bat. Spustí se CA

Spusťte activate\_bob.bat

Na závěr spuťte activate\_alice.bat

Alice začne automaticky odesílat zašifrované zprávy Bobovi.

# Blockchain

S nárustem zájmu o kryptoměny v posledních letech se do širšího povědomí dostal i pojem blockchain, technologie, nad kterou je valná většina kryptoměn postavena. Článků, videí, knih a publikovaných prací o blockchainu už bylo vydáno mnoho. Tato diplomová práce si neklade za cíl přijít s novou myšlenkou, jak by měl blockchain fungovat, nebo porovnat systémy, které používají pro svou činnost právě blockchain. Rozhodl jsem se nevynalézat kolo. V průběhu práce jsem z veřejných zdrojů načerpal vědomosti, jak má blockchainová síť vypadat, co musí splňovat a co v ní nesmí chybět, pokud chci abych ji mohl nazývat regulérní blockchainovou sítí. V této kapitole je uvedeno základní shrnutí, co je to blockchain a jaké má mít parametry. Nezbytné informace k tomu, aby čtenář, pokud je do té doby neznal, mohl plně porozumět dalším kapitolám zaměřených na popis vývoje a implementace blockchainové sítě pro ukládání zpráv v informačním systému.

## Úvod do problematiky blockchain

Blockchain je technologie pro uchovávání záznamů navržená tak, aby znemožnila hackování systému nebo falšování dat uložených na blockchainu, čímž se stal bezpečným a neměnným. Jedná se o typ technologie distribuované účetní knihy (DLT), což je systém digitální evidence transakcí a souvisejících dat na více místech současně. [x21]

Každý počítač v blockchainové síti uchovává kopii účetní knihy, kde se zaznamenávají transakce, aby se zabránilo jedinému bodu selhání. Všechny kopie jsou také aktualizovány a ověřovány současně. [x21]

Blockchain je také považován za typ databáze, ale od konvenčních databází se podstatně liší tím, jak ukládá a spravuje informace. Namísto ukládání dat do řádků, sloupců, tabulek a souborů, jak to dělají tradiční databáze, blockchain ukládá data do bloků, které jsou spolu digitálně zřetězeny. Blockchain je navíc decentralizovaná databáze spravovaná počítači patřícími do sítě peer-to-peer namísto centrálního počítače jako v tradičních databázích. [x21]

Bitcoin, spuštěný v roce 2009 na bitcoinovém blockchainu, byl první kryptoměnou a populární aplikací, která úspěšně používala blockchain. V důsledku toho byl blockchain nejčastěji spojován s bitcoiny a alternativami, jako je dogecoin a bitcoinová hotovost, které obě používají veřejné knihy. [x21]

Využití blockchainů soukromé účetní knihy se však od počátku Bitcoinu rozšířilo i do dalších aplikací. Logistické společnosti využívají blockchain ke sledování a sledování zboží při jeho pohybu v dodavatelském řetězci. Vládní centrální banky a globální finanční komunita testují technologii blockchain jako základ pro směnu měn. A různá průmyslová odvětví, včetně právní komunity a zábavy, využívají blockchain jako základ pro chytré smlouvy a další mechanismy pro převod a ochranu práv duševního vlastnictví. [x21]

Ve skutečnosti společnosti a další organizace používají aplikace založené na blockchainu jako bezpečný a nákladově efektivní způsob vytváření a správy distribuované databáze a udržování záznamů pro digitální transakce všech typů. V důsledku toho je blockchain stále více vnímán jako způsob bezpečného sledování a sdílení dat mezi více podnikatelskými subjekty. [x21]

## Klíčové vlastnosti technologie blockchain

* Decentralizace. Decentralizace blockchainu je jedním ze základních aspektů technologie. Na rozdíl od centralizovaných databází, kde centrální orgán, jako je banka, kontroluje a ověřuje transakce, blockchain funguje na distribuované účetní knize. To znamená, že více transparentních účastníků, známých jako uzly, udržuje, ověřuje a aktualizuje účetní knihu. Každý uzel je rozprostřen po síti a obsahuje kopii celého blockchainu. [x21]
* Neměnnost a bezpečnost. Kryptografické algoritmy se v blockchainu používají k zajištění silného zabezpečení, zaznamenávání transakcí a téměř nemožné manipulaci. Informace jsou uloženy v blocích, které jsou vzájemně propojeny pomocí kryptografických hashů. Pokud se někdo pokusí narušit nebo upravit blok, vyžadovalo by to změnu každého následujícího bloku, takže manipulace je výpočetně neproveditelná. Tato inherentní bezpečnostní funkce blockchainu zajišťuje neměnnost informací a dělá z blockchainu ideální platformu pro ukládání citlivých dat a provádění bezpečných transakcí. [x21]
* Transparentnost a sledovatelnost. Transparentnost technologie blockchain zajišťuje, že každý účastník sítě má přístup ke stejným informacím. Každá transakce se například stane součástí veřejné knihy, kterou uvidí všichni účastníci. Tato transparentnost zajišťuje důvěru a síťovou odpovědnost, protože jakoukoli nekonzistenci lze okamžitě rozpoznat a vyřešit. Schopnost blockchainu sledovat původ a trajektorii aktiv navíc usnadňuje audity a snižuje pravděpodobnost podvodných aktivit. [x21]

[x21]https://www.techtarget.com/searchcio/definition/blockchain

# Mikroslužba zabezpečující technologii blockchain nad logovými záznamy informačního systému.

Tato mikroslužba realizuje všechny klíčové vlastnosti blockchainové sítě. Přijímá zprávy, logové záznamy, od uživatelů, které ukládá do bloků a následně bloky, těžbou zařazuje do řetězu. Těžba je realizovaná pomocí „proof of work“, mechanismem, který je popsán v předchozí kapitole. Síť by se měla skládat se z minimálně tří uzlů sítě, protože v případě odlišnosti uložených řetězů je potřeba nadpoloviční většina k určení toho správného. V této mikroslužbě je blockchainová síť decentralizovaná, a tedy žádný z uzlů není postaven nad ostatní a každý má stejnou kopii řetězu. Neboli každý z uzlů má k dispozici stejná data, jako ostatní uzly.

## Popis jednotlivých částí

Uzel

Základním stavebním prvkem sítě je uzel, anglicky „node“. Ten zajišťuje veškeré operace s řetězem. Přijímá pro něj data, poskytuje je ostatním uzlům, provádí těžbu, iniciuje těžbu v ostatním uzlech, vyhodnocuje výsledky těžby a vytěžené bloky ukládá do řetězu. Samozřejmě data dokáže nejen ukládat, ale také poskytovat na vyžádání. Konkrétně se jedná o python tornado server. Při spuštění serveru se načte konfigurační soubor. V něm jsou pro něj informace o sousedním uzlu a náročnosti těžby. Také se vytvoří tabulka uzlů v síti, které je pro začátek prázdná a rozšiřuje se postupně, jak uzel získává informace o dalších uzlech. Uzel má 11 koncových bodů. Ty používá pro komunikaci jak s klientem, tak i s dalšími uzly v síti. Jednotlivé koncové body jsou popsány níže v kapitole „Funkcionality uzlu“.

Klient/Postman

Klientská část může nabývat různých podob. Uživatel/klient poskytuje uzlu data pomocí http požadavku. Může tak dělat buď manuálně, nebo pomocí skriptu, který periodicky zasílá data do sítě. Tento script je přiložen ve zdrojových kódech a je možné jej mikroslužbě použít.

Kromě samotného odeslání dat, uživatel také může od uzlu získat řetěz, data v něm, pro další využití.

Tato mikroslužba je nastavená tak, že zahájení těžby iniciuje uživatel. Tedy zasláním specifického http požadavku jakémukoliv uzlu v síti spustí těžení na všech uzlech v síti.

Klient také má možnost poslat požadavek na vyhodnocení řetězů v síti. Jednotlivé uzly se chovají víceméně nezávisle až právě do doby, kdy přijde příkaz, aby uzly svoje řetězy sjednotili. Tím se právě eliminuje možná nežádoucí aktivita útočníka, nebo v krajních příkazech kolize při komunikaci mezi uzly.

Zahájení těžby a vyhodnocení řetězu jsou pokyny, které by teoreticky ve svém důsledku neměl dávat libovolný uživatel, ale měly by být autonomními součástmi uzlů. Pro tuto mikroslužbu jsem se rozhodl tak neučinit, protože díky manuálním příkazům dokáže lépe demonstrovat jejich činnost. Více na toto téma je uvedeno v kapitole „Možnosti dalšího rozvoje“.

## Funkcionality uzlu

Třída Blockchain

Pro uchování řetězce a práci s ním používají uzly třídu „Blockchain“ ze souboru „blockchain.py“ v adresáři „modules“. Při iniciaci třídy se vytvoří šest proměnných.

* „current\_logs“ – do této proměnné se ukládají příchozí zprávy, logové záznamy, které později budou v rámci bloku těženy a posléze přidány do řetězce.
* „chain“ – řetezec, hlavní proměnná třídy Blockchain
* „last\_block\_timestamp – časová značka posledního přidaného bloku do řetězce. Používá se pro řešení kolizí při přijetí vytěženého bloku od více uzlů.
* „ismining“ – stavová proměnná
* „isresolving“ – stavová proměnná
* „complexity“ – náročnost hashe. Číslo, které udává, jak náročná má být těžba.

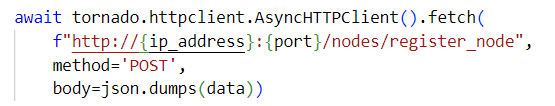
Kromě proměnných se iniciuje také osm funkcí pro práci s řetězcem.

* „valid\_chain“ – Kontroluje řetěz a rozhoduje, zda je v něm chyba.
* „resolve\_conflicts“ – Porovnává řetězy od ostatních uzlů a rozhoduje, který řetěz má největší četnost.
* „new\_block“ –Funkce, která přidá vytěžený blok do řetězu.
* „valid\_block“ – V případě přijetí více bloků od uzlů v rámci stejné těžby tato funkce rozhodne, který blok přidá do řetězu.
* „new\_log“ – Pokud zpráva ještě nabyla přidána, přidává příchozí zprávu do bloku, který bude příště těžen.
* „hash“ – Vrací hash bloku, který byl přidán jako parametr.
* „mining“ – Asynchronní funkce, která se stará o těžbu nových bloků.
* „valid\_proof“ – V parametru přijímá blok a vrací zda hash bloku odpovídá požadavku na náročnost hashe.

Jednotlivé funkce uzel volá podle potřeby a úkolům, které musí vykonat.

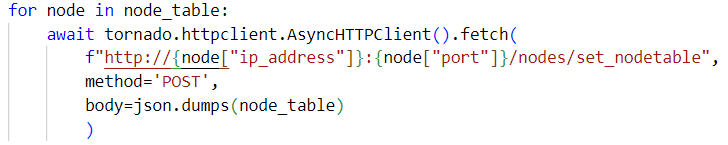
Registrace v síti

První úkolem, který uzel po svém spuštění musí učinit je zaregistrovat se do sítě. Toho docílí tím způsobem, že odešle POST http požadavek na sousední uzel, který má nastaven ve svém konfiguračním souboru. K požadavku uzel přiloží informace o své adrese, portu a jedinečném identifikátoru.



Obrázek 31 – http požadavek (registrace v síti)

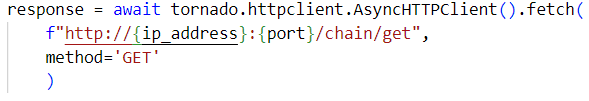
Sousední uzel, v okamžiku. kdy přijme požadavek na koncovém bodu „nodes/register\_node“ přidá informace o novém uzlu do své tabulky uzlů a všem uzlům v síti odešle požadavek na aktualizaci tabulky. V těle požadavku je tabulka uzlů, kterou ostatní uzly aktualizují tu svoji.



Obrázek 32 – http požadavek (nastavení tabulky uzlů)

Tímto způsobem nový uzel získává aktuální přehled o všech uzlech v síti. Ten potřebuje, aby ostatním uzlům mohl odesílat zprávy, přijaté od klienta nebo vytěžené bloky.

Kromě tabulky uzlů nový uzel potřebuje také aktuální uzel v síti. Ten, který si vytvořil při svém spuštění (při vytvoření třídy „Blockchain“) se neshoduje s řetězy v síti. Pro získání řetězu zavolá http požadavek na sousední uzel. Odpovědí je řetěz souseda nového uzlu, kterým přepíše svůj dosavadní uzel.



Obrázek 33 – http požadavek (žádost o řetez)

Je to druhý a poslední okamžik, kdy nový uzel vnímá některý z již existujících uzlů v síti za svůj bližší. Po své registraci uzel informaci o svém sousedním zahazuje a nikdy více ji nevyužije. I pomocí toho je dosažena ona zmiňovaná decentralizace sítě.

Na obrázku 15 je graficky znázorněn průběh registrace nového uzlu v síti. Uzel na levé straně žádá svého souseda napravo a registraci. V horní části obrázku jsou dva další uzly v síti, kteří samotnou registraci neprovádí, ale přijímají informaci o novém uzlu v síti.

Obsah obrázku text, diagram, zástrčka

Popis byl vytvořen automaticky

Obrázek 15 – Zaregistrování uzlu v síti

Žádost o tabulku uzlů

Jak jsem popisoval v předchozí kapitole, tabulka uzlů se aktualizuje automaticky. Není tedy potřeba, aby se uzly doptávaly na tabulku. Tato možnost tady, ale je. Nemá přímý dopad na fungování sítě, ale může sloužit uživateli/administrátorovi pro lepší přehled o síti. Tabulku lze získat pomocí GET http požadavku na jakýkoliv uzel v síti.



Obrázek 34 – http požadavek (žádost o tabulku uzlů)

Přijetí zprávy

Pro přijímání zpráv od klientů uzel používá koncový bod „logs/new“. Klient na něj odešle POST http požadavek, kdy v těle funkce je zpráva, v našem případě jeden nebo více logových záznamů, které chce klient odeslat. Jako demo data pro ukázku odesílání systémových logů používám dataset „Windows\_2k.log“, který jsem získal z veřejného zdroje na stránce Github [x40].



Obrázek 34 – http požadavek (žádost o tabulku uzlů)

Uzel po přijetí zprávy ji nejprve zkontroluje a posléze ji přidá do zásobníku „current\_logs“ ve třídě „Blockchain“. Kontrolou se rozumí ověření, zda zpráva je ve slovníku uložená pod názvem „message“ a zda se zpráva už v zásobníku nenachází. Zprávu také odešle všem ostatním uzlům v síti. Tato zpráva zatím není přidána do řetězu. To se stane až je celý zásobník „current\_logs“ vložen do bloku a ten bude vytěžen. V této chvíli tomu tak zatím není, a proto pokud by uživatel hned po odeslání zprávy zažádal o řetěz, tak ten danou zprávu obsahovat nebude. Po zdárném vložení zprávy do zásobníku a přeposlání zprávy zbylým uzlům se klientovi vrací kladná odpověď. V případě, že zpráva už v zásobníku byla, dostane klient odpověď zápornou.

Na obrázku níže je graficky znázorněna komunikace v síti po přijetí zprávy.

Obsah obrázku diagram, text, Plán

Popis byl vytvořen automaticky

Obrázek 16 – Přijetí zprávy

1. Klient odesílá uzlu zprávu
2. Uzel přidává zprávu do zásobníku
3. Uzel přeposílá zprávu ostatním uzlům
4. Ostatní uzly přijímají zprávu a vkládají ji do svých zásobníků
5. Uzly přeposílají zprávu
6. Uzly zamítají zprávu, protože zpráva už byla přidána.

Určitě je nasnadě otázka, zda je nutné, aby uzly přeposílali zprávu znova. Dochází tak ke zbytečné komunikaci, a i zbytečnému zahlcení sítě. To je sice pravda, ale uzly nemusí rozhodovat, zda zprávu získali od uzlu, nebo od klienta, a především to umožňuje uzlům, v případě potřeby, vložit do řetězu zprávu i přímo od nich.

Těžba

Těžení je nejvíce komplexní funkcionalita, kterou uzel umí. Úkolem této funkcionality je vytěžit zprávy v zásobníku „current\_logs“ a vytěžený blok vložit na konec řetězu. V současné době se zahájení těžby ovládá manuálně, ale jediný důvod pro to je jednodušší vysvětlení toho, jak těžba funguje. V kapitole „Možnosti dalšího rozvoje“ uvádím, jakým způsobem by se zahájení těžby dalo automatizovat.

Těžba se zahájí manuálně posláním http GET požadavku na koncový bod „mine/start“ libovolného uzlu.



Obrázek 35 – http požadavek (zahájení těžby)

Uzel při přijetí požadavku vyhodnotí, zda právě neprobíhá buď těžba, nebo vyhodnocování řetězu. Pokud ano, tak požadavek na zahájení těžby odmítne. V opačném případě pošle pokyn všem uzlům v síti, včetně sebe, aby zahájili těžbu.



Obrázek 36 – http požadavek (příkaz k zahájení těžby)

Obsah obrázku text, snímek obrazovky, diagram, design

Popis byl vytvořen automaticky

Obrázek 17 – Zahájení těžby

1. Pokyn od uživatele/administrátora k zahájení těžby
2. Vyhodnocení zda těžba právě neprobíhá
3. Vyhodnocení zda nejsou řetězy v síti právě porovnávány
4. Příkaz všem uzlům v síti k zahájení těžby

Každý uzel předtím, než zahájí samotnou těžbu nejprve sestaví těžený blok ve formátu JSON.

Skládá se z:

* Index – jedinečné číslo pro celý řetěz. Jedná se o hodnotu o jedna vyšší, než poslední blok v řetězu.
* Začátek těžby – čas, kdy začala těžba bloku
* Logy – záznamy od klientů uložené v zásobníku „current\_logs“ s přidáním zprávy o tom, kdo daný blok vytěžil.
* Důkaz – hodnota, která bude při těžbě měněna.
* Předešlá hash – provázání do řetězu pomocí hashe posledního bloku v řetězu

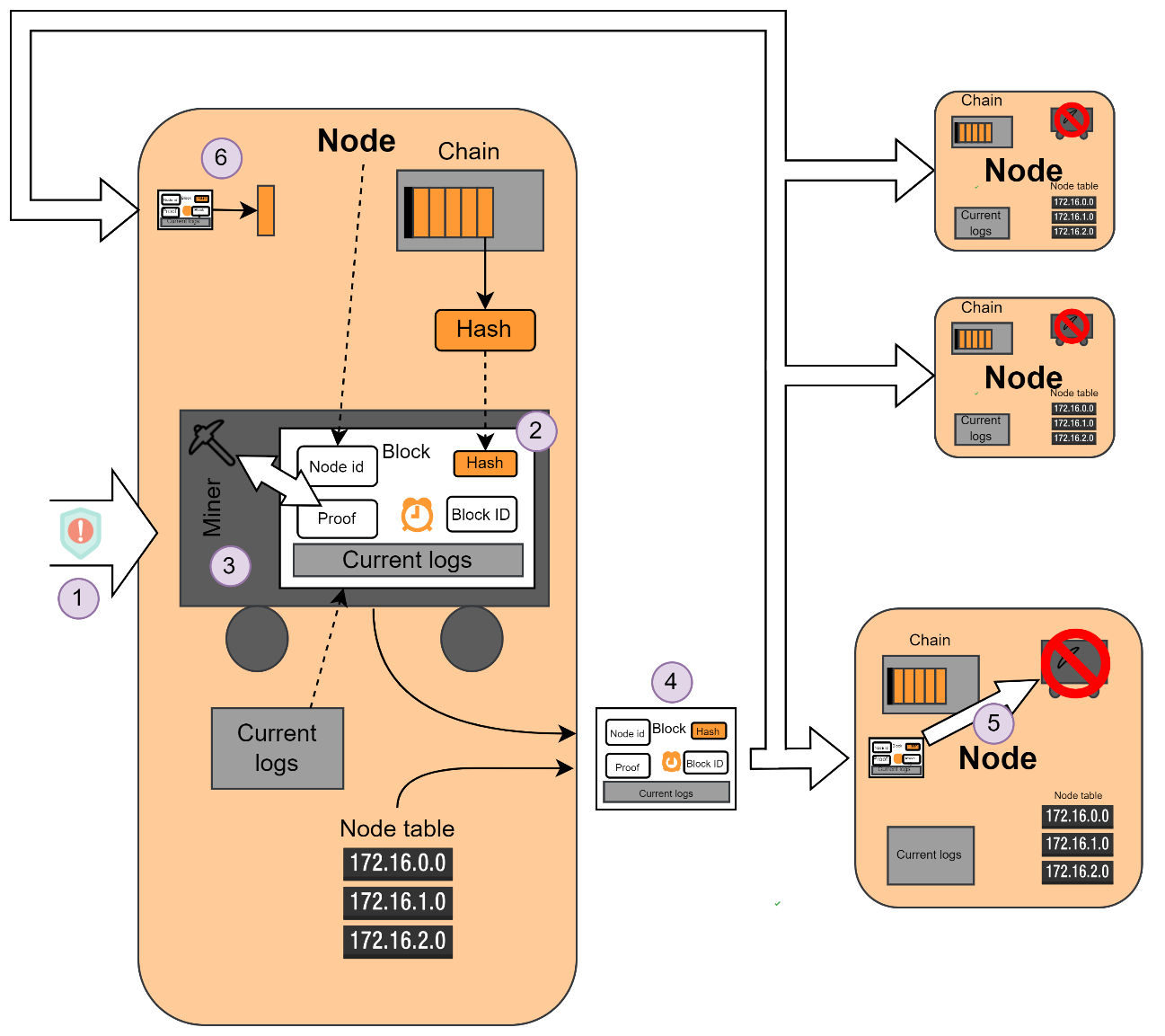
Takto sestavený blok může být poslán do těžení. Těžením, se rozumí hledáním takové hodnoty pro důkaz v bloku, aby hash celého bloku odpovídala požadavkům na náročnost hashe. Funkce, která provádí těžení je součástí třídy „Blockchain“ a jmenuje se „mining“. Jako parametry bere těžený blok, funkci, která odesílá výsledek všem uzlům v síti a identifikátor uzlu. Funkce ještě z konfiguračního souboru vezme hodnotu náročnosti pro těžbu. Základně je v něm uvedena hodnota 5. To znamená, že pokud má být blok úspěšně vytěžen, tak funkce, která těžbu provozuje musí nalézt takovou hodnotu, aby se prvních 5 znaků hashe celého bloku rovnalo 5 nulám. V průběhu testování této mikroslužby jsem došel k závěru, že v případě nízké náročnosti může docházet ke kolizím, která síť není schopna sama vyřešit, a proto doporučuji považovat náročnost 5 za minimální hodnotu. Shora náročnost omezená není. Doporučuji náročnost nastavit v závislosti na výkonu strojů, na kterých uzly běží a také na počtu uzlů v síti. V mém případě jsem testoval síť o třech uzlech, které běželi na stejném stroji. Pro hodnoty vyšších než 8 byla doba těžby, tak dlouhá, že bloky nebylo možné vytěžit v rozumné době. V mém případě to znamenalo, že ani po 30 minutách nebyla těžba zdárně ukončena.

Po nalezení vhodné hodnoty důkazu je těžba ukončena a funkce „mining“ ve třídě „Blockchain“ odešle všem uzlům v síti vytěžený blok s připnutou časovou značkou o čase ukončení těžby. To je pokyn pro všechny uzly, aby svoji, prozatím neúspěšnou těžbu ukončili a po ověření přijatého bloku ho přidali do svých řetězů.

K ověření přijatého bloku se používá funkce „valid\_block“ ve třídě „Blockchain“. Tato funkce nejprve zkontroluje důkaz v bloku. Pokud byl vypočítán správně, tak hash by měla opět odpovídat požadavkům na náročnost. Poté se zkontroluje, zda index přijatého bloku je o jeden vyšší než poslední blok v řetězu a jako poslední se zkontroluje, zda v hodnota předešlé hashe v přijatém bloku odpovídá hashi posledního bloku v řetězu. Pokud jsou všechny podmínky splněny, tak funkce „valid\_block“ vrací hodnotu „pravda“ a blok je přidán do řetězu.

Zmínil jsem se také, že může docházet ke kolizím. K těm může dojít, pokud dva bloky vytěží své bloky současně. To znamená, že než přijde k uzlu výsledek těžby jiného bloku, on sám těžbu dokončí a rozešle všem uzlů svůj vytěžený blok. V tom případě mají uzly k dispozici dva bloky a oba jsou relevantní pro přidání do řetězu. Jenže řetězy musí zůstat na všech uzlech totožné, a proto přichází do hry časová známka, která je připojená k vytěženému bloku. Uzly přečtou časovou známku obou bloků a vyberou ten blok, který byl vytěžen dříve. Kolize se často stávají, pokud je nastavena nízká náročnost těžby. Když jsou kolize málo časté, síť si s nimi bez problému poradí. V případě, že je náročnost nastavena na nízkou úroveň a doba těžby trvá v průměru pár desítek milisekund, pak nastává neopravitelný problém. Proto doporučuji náročnost těžby ponechat minimálně na hodnotě 5, nebo ji zvýšit v závislosti na počtu uzlů a výkonu strojů, na kterých uzly běží. Ideální je, pokud doba těžby trvá déle něž 10 vteřin.

Po přidání bloku do řetězu uzel začíná další těžbu. Jedná se tak o nekonečný proces až do okamžiku, kdy uživatel/administrátor manuálně těžbu ukončí. Grafické znázornění průběhu těžby lze najít na obrázku 18.



Obrázek 18 – Těžení bloku a distribuce výsledku

1. Pokyn od některého z uzlů k zahájení těžby
2. Sestavení bloku
3. Těžba bloku
4. Odeslání bloku všem uzlům v síti
5. Ukončení těžby na ostatní uzlech
6. Vyhodnocení přijatého bloku

Ověření řetězu

Jednou za určitý čas by síť měla zkontrolovat, zda souhlasí řetězy v uzlech na síti. Zda některé uzly, potenciálně škodlivé, nemají jiné řetězy, a tedy i data, než zbytek sítě. Může se tak stát, pokud někdo s přístupem k datům v řetězu tyto data změnil. Vše vyřeší právě porovnání řetězů. Na pokyn uživatele/administrátora libovolnému uzlu, celá síť, pokud probíhala, ukončí těžbu. Respektive vyčká, než se dokončí těžba posledního bloku a další už nespustí.



Obrázek 36 – http požadavek (příkaz k porovnání řetězů)

Každý uzel si získá od každého uzlu v síti hash jeho řetězu. Tyto hashe porovná a vybere tu hash, která má nejvyšší četnost. Vybranou hash porovná s hashí svého řetězu. Pokud odpovídá, ukončuje proces a uživateli odpovídá, že řetěz nebyl změněn. Pokud ovšem hash s nejvyšší četností neodpovídá, zažádá libovolný uzel, od kterého tato hash přišla, aby mu poskytl jeho řetěz. Tím pak přepíše ten svůj a získává tak řetěz, který byl odsouhlasen v síti.

To je právě jedna z výhod blockchainové sítě. Redundance dat a jejich vzájemné porovnávání tak, že alternativní, zfalšovaná, data nemají možnost se prosadit. Útočník by musel ovládnout nadpoloviční většinu uzlů, aby mohl měnit data v řetězech, a to je obtížné, obzvlášť pokud síť postavena z většího počtu uzlů.

Poskytnutí řetezu

Jedna z nejzákladnějších funkcionalit jak uzlu, tak i jakéhokoliv informačního systému, je poskytování dat. V našem případě se jedná o řetěz. Ten uživatel, nebo i uzly mohou získat pomocí http GET požadavku na libovolný uzel v síti.



Obrázek 36 – http požadavek (žádost o řetěz)

Předtím než je řetěz poskytnut je provedena kontrola na pravost řetězu. Zabrání se tak možnosti šíření falešně upraveného řetězu. Tato kontrola vezme blok po bloku a kontroluje, zda blok obsahuje správnou hash a zda obsahuje hash předchozího bloku. Nemůže se tak stát, aby uzel poskytoval data, která neprošly těžbou.

Průvodce pro spuštění mikroslužby

V níže uvedených krocích je uveden postup, jak jednoduše spustit mikroslužbu na vlastním stroji. Předpokladem pro správné fungování je nainstalovaný Python verze 3.12.2 dostupný z <https://www.python.org/downloads> .

Zdrojový kód mikroslužby a instalační balíček je dostupný na GitHub repozitáři. Stáhněte jej pomocí Git příkazu: „git clone -b Blockchain-service <https://github.com/naxit-01/DiplomovaPrace.git>“.

Po stažení přejděte do složky „DiplomováPrace“ a spusťte instalační soubor „setup.bat“. Ve vašem adresáři se vytvoří virtuální prostředí a do něj se vám nainstalují všechny potřebné knihovny. Zároveň se vám v adresáři vytvoří dva spustitelné soubory: „activate\_client.bat“ a „activate\_blockchain.bat“. V této chvíli by mělo být vše připraveno pro spuštění uzlů a klientů.

Doporučuji v síti spustit alespoň tři uzly. Toho docílíte spuštěním, alespoň třikrát za sebou souboru „activate\_blockchain.bat“. Uzly samozřejmě nemusí být všechny na stejném stroji. Můžete je rozjet na jakémkoliv stroji v dostupné síti. Důležité je, aby stroje spolu mohli komunikovat a správné uvedení sousedních uzlů v konfiguračním souboru „config.ini“.

Po spuštění uzlů můžete zprovoznit klienta spuštěním souboru „activate\_client.bat“. Klient se vás nejprve zeptá, se kterým uzlem budete chtít komunikovat. Pokud některý uzel běží na stejném počítači jako je klient, můžete ponechat pro ip adresu a port původní hodnoty. Klient poskytuje 5 různých příkazů, kterým ovládáte blockchainovou síť.

1. Získat tabulku uzlů – Dotážete se zvoleného uzlu, jaká je tabulka uzlů. Tím nijak síť neovlivňujete a je to pouze informace pro vás.
2. Odeslat log – Odešlete buď vámi napsanou zprávu, nebo náhodně vybraný systémový log z datasetu uloženém v adresáři.
3. Zahájení těžby – Odešlete příkaz celé síti aby zahájila těžbu.
4. Vyhodnotit řetězy – Odešlete příkaz síti, aby ukončila těžbu a porovnala řetězy uložené na jednotlivých uzlech v síti.
5. Získat řetěz – Dotážete se zvoleného uzlu na jeho uložený řetěz.

Pokud by měl klient sloužit pouze pro odesílání dat do sítě, tak jediný důležitý příkaz je „odeslat log“. Zbylé příkazy jsou pro administrativní účely a v budoucnu by měly být nahrazeny automatickými procesy viz. kapitola „Možnosti dalšího rozvoje“.

# Postkvantová blockchainová síť

V předchozích kapitolách byly představeny mikroslužby pro postkvantové šifrování a blockchainovou síť. V této kapitole bych chtěl představit její spojení do jednohou souvislého celku. V předešlé kapitole blockchainová síť komunikovala na základě nešifrované http komunice. V této kapitole bude blockchainová síť, se zachováním všech funkcionalit, komunikovat zašifrovaným provozem tak, jak bylo popsáno v kapitole 4. Změna proběhla ve využití jiné komunikační metody, doplnění koncového bodu pro výměnu symetrických klíčů a doplnění souboru skriptů o certifikační autoritu. Protože vytvoření postkvantové blockchainové sítě není cílem této diplomové práce, nebudu popisovat, jak tyto změny přímo proběhly, ale pouze poskytnu návod pro spuštění této mikroslužby.

Popis jednotlivých částí

Agent

Node

Ukázka funkcionalit mikroslužeb

Průvodce pro spuštění Postkvantové blockchainové sítě

# Možnosti dalšího rozvoje

Provest resolve conflicts pokazde kdy se chce někdo zaregistrovat do site a vrátit tak nejlepší mozny retez.

Automatizovat tezeni a resolve confilcts.

Moznost spustit sít s uz ulozenym retezem

# ZÁVĚR

Je nutné věnovat stejnou, ne-li větší pozornost jako úvodu. V závěru musíte podat shrnutí, vyzvednout nejdůležitější postřehy a také vyhodnotit, zdali jste naplnili cíle, které jste si stanovili v úvodu své práce.

# SEZNAM POUŽITÉ LITERATURY (vzor)

**MONOGRAFIE**

1. ANTUŠÁK, Emil. *Strategie a ekonomika v bezpečnostním systému České republiky*. 1. vyd. Praha: Ministerstvo obrany České republiky, 2002. s. 141 – 180. ISBN 80-7278-143-x.
2. BRČÁK, Josef. *Česká republika ve světle ekonomických teorií*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. s. 78 – 150. ISBN 978-80-7380-369-8.
3. KADEŘÁBKOVÁ, Anna. *Základy makroekonomické analýzy: růst, konkurenceschopnost, rovnováha*. 1. vyd. Praha: Linde, 2003. 175 s. ISBN 80-86131-36-x.

**ELEKTRONICKÉ ZDROJE**

1. BALCAROVÁ, Pavlína. *Konkurenceschopnost ekonomiky a její měření* [online]. Brno, 2007 [cit. 2014-12-30]. Dostupné z: ˂<http://is.muni.cz/th/75962/prif_m/diplomova_prace.pdf>˃. Diplomová práce. Masarykova univerzita.
2. Česká republika: hlavní makroekonomické ukazatele. *Český statistický úřad* [online]. 2014 [cit. 2015-01-28]. Dostupné z: ˂[https://www.czso.cz/documents/10180/20555311/HLMAKRO.xls](http://www.czso.cz/csu/redakce.nsf/i/cr:_makroekonomicke_udaje/$File/HLMAKRO.xls)˃.

* Pozn. ČSN ISO 690 Informace a dokumentace – Pravidla pro bibliografické odkazy a citace informačních zdrojů

# 

# SEZNAM PŘÍLOH

|  |  |  |  |
| --- | --- | --- | --- |
| Příloha č. 1 | − | Popis přílohy (→ styl Odstavec) |  |
| Příloha č. 2 | − | Popis přílohy (→ styl Odstavec) |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

(→ Styl Příloha – číslování) Příloha 1

Popis přílohy (→ styl Příloha – popis)

|  |
| --- |
|  |