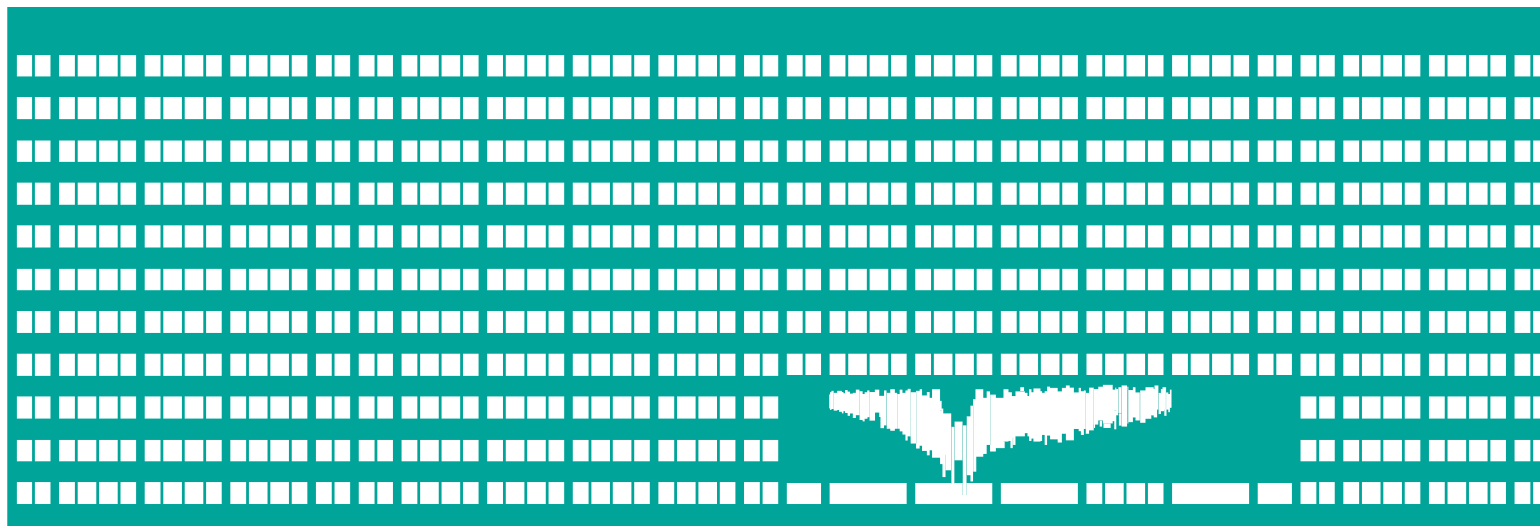


VŠB TECHNICKÁ  
UNIVERZITA  
OSTRAVA

VSB TECHNICAL  
UNIVERSITY  
OF OSTRAVA



[www.vsb.cz](http://www.vsb.cz)

# Identifikace vlastníků bitcoinových adres

Autor: Bc. Adam Šárek

Vedoucí: Ing. Jan Plucar, Ph.D.

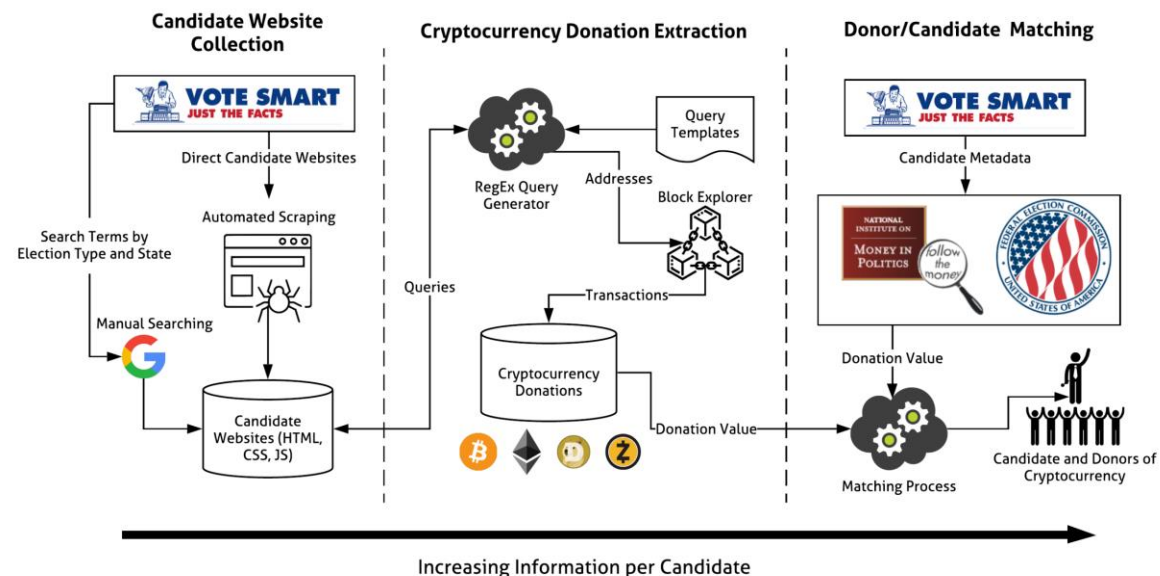
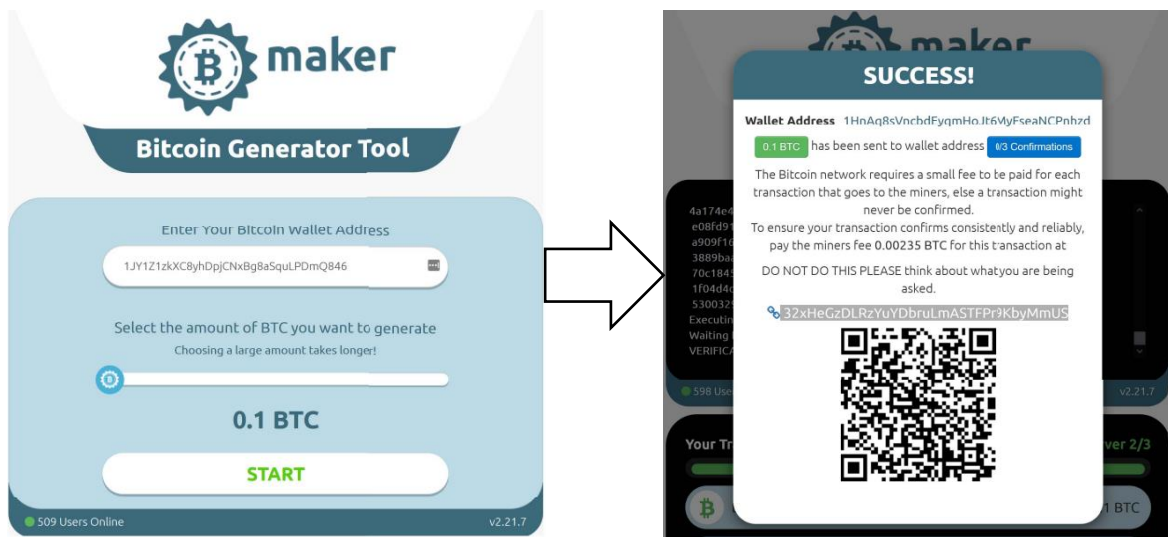
# Cíle práce

- Analýza state of the art v oblasti kryptoměnových podvodů
- Výběr zdrojů kryptoměnových adres a nahlášení podvodů
- Návrh a implementace vlastního prostředí
- Vytvoření databáze kryptoměnových adres
- Zpřístupnění dat prostřednictvím webového rozhraní a API

# State of the Art

**Vybrané práce zaměřené na odhalování kryptoměnových podvodů:**

- Automatická detekce a analýza podvodu Bitcoinového generátoru
- Odhalení daňových podvodů a nezákonných kryptoměnových příspěvků v amerických politických kampaních
- Detekce Bitcoinových Ponziho schémat



# Open Source Intelligence

## Volně dostupné služby pro nahlašování kryptoměnových podvodů:

- BitcoinAbuse, CheckBitcoinAddress, CryptoBlacklist, BitcoinAIS, CryptoScamDB, Cryptscam, SeeKoin, BitcoinWhosWho

## Bezplatné nástroje pro analýzu kryptoměn:

- Blockchain.com, Blockchair.com



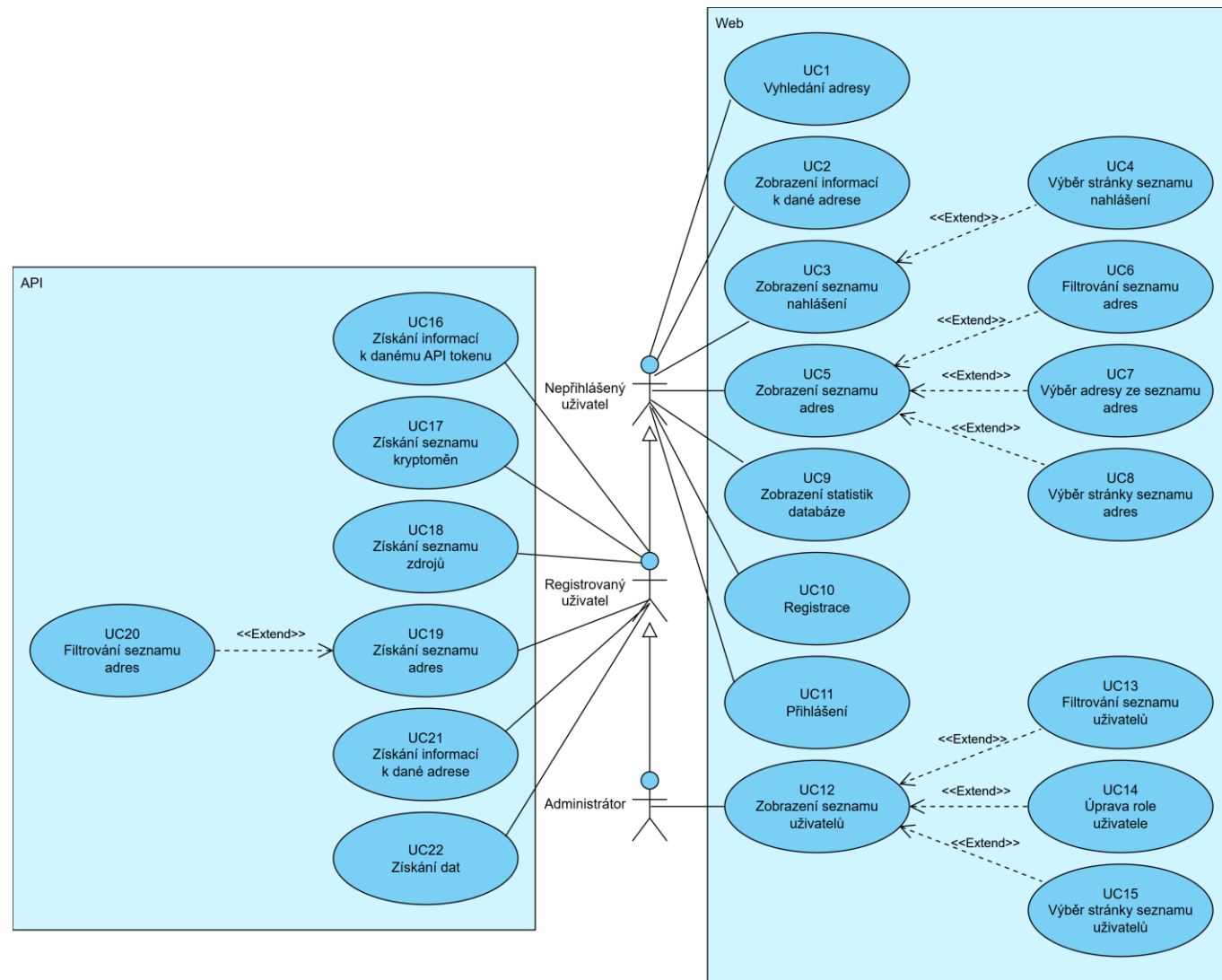
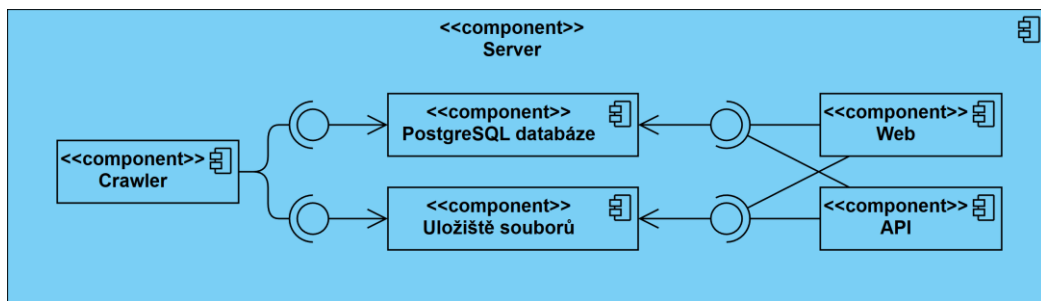
## Profesionální nástroje pro analýzu kryptoměn:

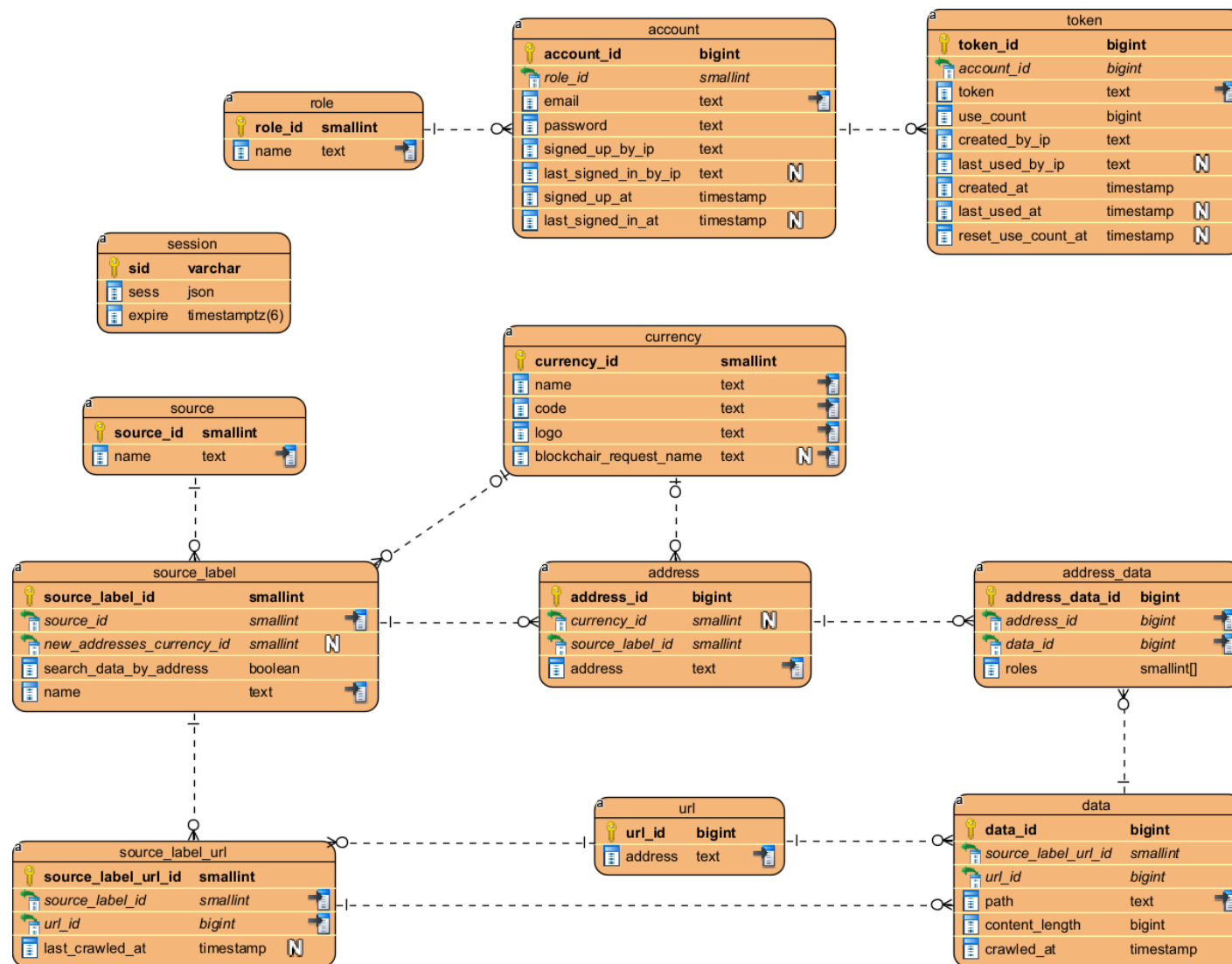
- Chainalysis, Elliptic



# Analýza a návrh

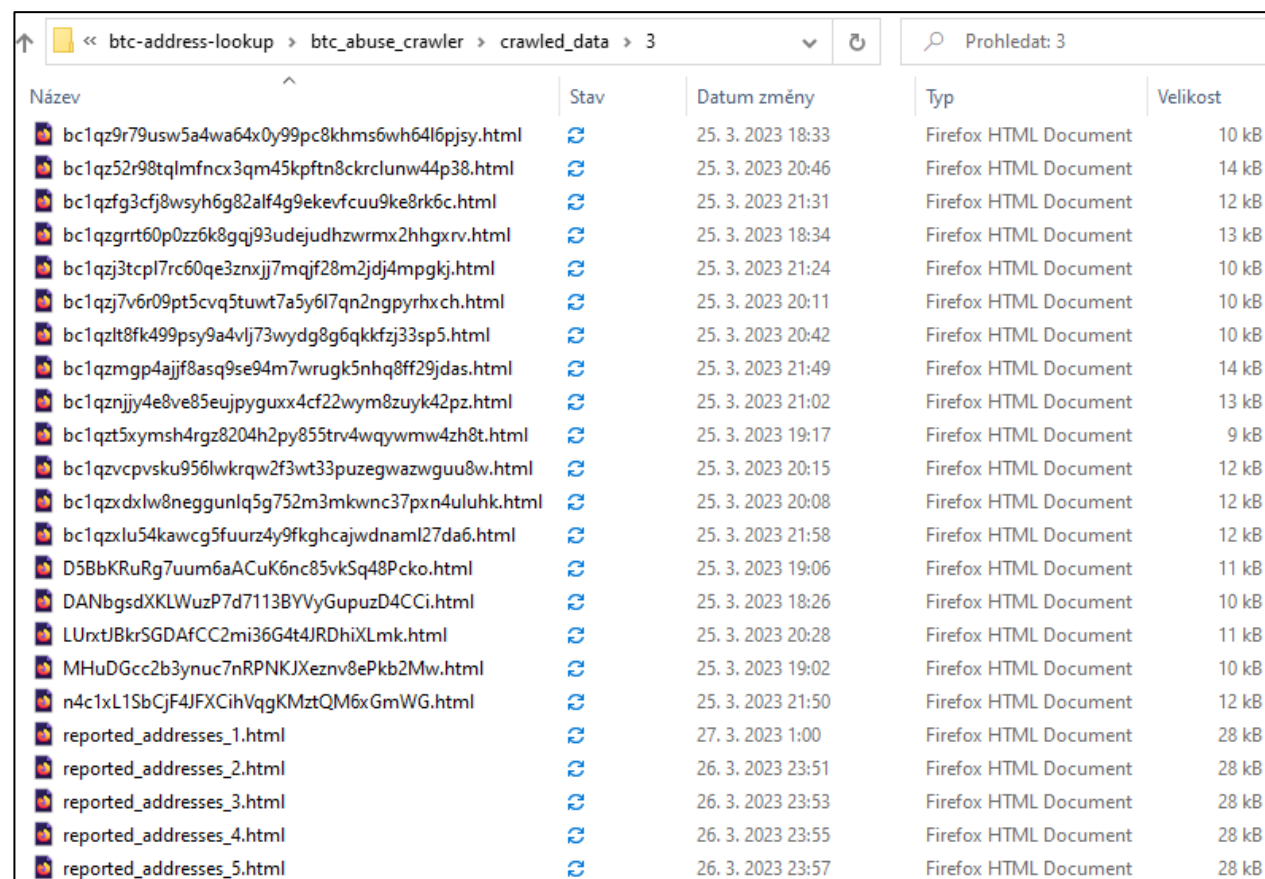
- Specifikace požadavků
- Případy použití
- Návrh databáze
- Komponenty systému





# Implementace crawleru

- Procházení zdrojů nahlášených kryptoměnových podvodů
- Propojování získaných dat s adresami
- Zjištění kryptoměnové příslušnosti altcoinových adres
- Automatizovaný běh
- Správa databáze



Název	Stav	Datum změny	Typ	Velikost
bc1qz9r79usw5a4wa64x0y99pc8khms6wh64l6pjsy.html	🔗	25. 3. 2023 18:33	Firefox HTML Document	10 kB
bc1qz52r98tqlmfcx3qm45kpftn8ckrclunw44p38.html	🔗	25. 3. 2023 20:46	Firefox HTML Document	14 kB
bc1qzfg3cfj8wsyh6g82alf4g9ekevfcuu9ke8rk6c.html	🔗	25. 3. 2023 21:31	Firefox HTML Document	12 kB
bc1qzgrt60p0zz6k8gqj93udejudhzwrmx2hhgxrv.html	🔗	25. 3. 2023 18:34	Firefox HTML Document	13 kB
bc1qzj3tcpl7rc60qe3znxjj7mqjf28m2jdj4mpgkj.html	🔗	25. 3. 2023 21:24	Firefox HTML Document	10 kB
bc1qzj7v6r09pt5cvq5tuwt7a5y6l7qn2ngpyrhxch.html	🔗	25. 3. 2023 20:11	Firefox HTML Document	10 kB
bc1qzlt8fk499psy9a4vlj73wydg8g6qkkfzj33sp5.html	🔗	25. 3. 2023 20:42	Firefox HTML Document	10 kB
bc1qzmgp4ajjf8asq9se94m7wrug5nhq8ff29jdas.html	🔗	25. 3. 2023 21:49	Firefox HTML Document	14 kB
bc1qznjyy4e8ve85eujpyguxx4cf22wym8zuyk42pz.html	🔗	25. 3. 2023 21:02	Firefox HTML Document	13 kB
bc1qzt5xymsh4rgz8204h2py855trv4wqywmw4zh8t.html	🔗	25. 3. 2023 19:17	Firefox HTML Document	9 kB
bc1qzvcpsku956lwrqw2f3wt33puzegwazwguu8w.html	🔗	25. 3. 2023 20:15	Firefox HTML Document	12 kB
bc1qzdxlw8neggunlq5g752m3mkwnc37pxn4uluhk.html	🔗	25. 3. 2023 20:08	Firefox HTML Document	12 kB
bc1qzxl54kawcg5fuurz4y9fkgghajwdnaml27da6.html	🔗	25. 3. 2023 21:58	Firefox HTML Document	12 kB
D5BbKRuRg7uum6aACuK6nc85vkSq48Pcko.html	🔗	25. 3. 2023 19:06	Firefox HTML Document	11 kB
DANbgdsXKLWuzP7d7113BYVyGupuzD4CCi.html	🔗	25. 3. 2023 18:26	Firefox HTML Document	10 kB
LUxtJBkrSGDAfCC2mi36G4t4JRDhiXLmk.html	🔗	25. 3. 2023 20:28	Firefox HTML Document	11 kB
MHuDGcc2b3ynuc7nRPNKJXeznv8ePkb2Mw.html	🔗	25. 3. 2023 19:02	Firefox HTML Document	10 kB
n4c1xL1SbCjF4JFXcihVqgKMztQM6xGmWG.html	🔗	25. 3. 2023 21:50	Firefox HTML Document	12 kB
reported_addresses_1.html	🔗	27. 3. 2023 1:00	Firefox HTML Document	28 kB
reported_addresses_2.html	🔗	26. 3. 2023 23:51	Firefox HTML Document	28 kB
reported_addresses_3.html	🔗	26. 3. 2023 23:53	Firefox HTML Document	28 kB
reported_addresses_4.html	🔗	26. 3. 2023 23:55	Firefox HTML Document	28 kB
reported_addresses_5.html	🔗	26. 3. 2023 23:57	Firefox HTML Document	28 kB



# Ukázky konzole crawleru

```
Zastavování služby postgresql-x64-15 - PostgreSQL Server 15...  
Služba postgresql-x64-15 - PostgreSQL Server 15 byla úspěšně zastavena.
```

```
Spouštění služby postgresql-x64-15 - PostgreSQL Server 15.  
Služba postgresql-x64-15 - PostgreSQL Server 15 byla úspěšně spuštěna.
```

```
Setup finished successfully.
```

```
Crawler is running...
```

```
Dropping primary, foreign & unique keys...
```

```
Primary, foreign & unique keys dropped successfully.
```

```
Adding BTC addresses...
```

```
2023-05-05 21:55:29.455840 - 0
```

```
2023-05-05 21:55:35.873447 - 1,000,000
```

```
2023-05-05 21:55:41.516338 - 2,000,000
```

```
2023-05-05 21:55:46.611524 - 3,000,000
```

```
2023-05-05 21:55:51.716191 - 4,000,000
```

```
2023-05-05 21:55:57.357574 - 5,000,000
```

```
2023-05-05 23:31:26.920315 - 1,140,000,000
```

```
2023-05-05 23:32:37.250452 - 1,141,000,000
```

```
2023-05-05 23:32:58.997079 - 1,142,000,000
```

```
2023-05-05 23:33:07.008111 - 1,143,000,000
```

```
2023-05-05 23:33:53.224418 - 1,144,000,000
```

```
2023-05-05 23:33:55.580920 - 1,144,256,067
```

```
BTC addresses added successfully.
```

```
Adding primary, foreign & unique keys...
```

```
Primary, foreign & unique keys added successfully.
```

```
Committing the transaction of writing all BTC addresses to the database...
```


```
Transaction committed.
```

```
As crawling sources containing reports begins, changes should be visible on the website now.
```








```
Crawling sources with address lists...
```

# Implementace webového řešení

- Vyhledávání kryptoměnové adresy
- Seznam nahlášených adres
- Zobrazení statistik databáze
- Uživatelské účty
- API




BTC Address Lookup

Addresses		
Currency	Bitcoin (BTC) ▼	Source All ▼ <button>Filter</button>
Address		Last update
	<a href="#">1KayqtCZJTVYPQjjqJHBdrtvE69DgW5xPL</a>	27. 3. 2023 1:54:15
	<a href="#">1AZSbcgaP7nfcdBxW2Qh66sFX13sPPfUt</a>	27. 3. 2023 1:09:55
	<a href="#">3GsNkafF4su5Tzbt8MFy6cS7rumWczrX9R</a>	27. 3. 2023 1:09:55
	<a href="#">1N7eMF7KnP8vQqHtn89dVPcfXqOXFkra6H</a>	27. 3. 2023 1:09:55
	<a href="#">123iEhDDGSNq6cJuRStmzzqe7yevkS1V2r</a>	27. 3. 2023 1:09:55
	<a href="#">1LTdSkZSFM2rd2XEMW8oaRrY3ZPtNzNiv3</a>	27. 3. 2023 1:09:55
	<a href="#">1LAcPK26AvKWVge7q4u3zD71E7xZoPp3yB</a>	27. 3. 2023 1:09:55

# Ukázky detailu adresy

## Address

**Address**

 12qusMrNaac75kHFWMKPQuuSn7L44xozvV

**Blockchain explorers**

[View on blockchain.com](#)

[View on blockchair.com](#)

**Last update**

25. 3. 2023 18:10:35

Date	Type	Country	URL
3. 3. 2023 18:57:07	other	United States	<a href="#">View on cryptscam.com</a>

**Abuser**


Michael Wisard

**Description**

This man was going to help me get back some money from scam, he promised to pay me back toda yesterday and the day before that, but he started to ask for more and more fees, I even had to ask my sister to help me and she paid 800 euro in total. He has used 2 walletaddresses wich I sent to. From the date 22 februari-23. After the last sending this morning and he was supposed to send the bitcoin, he called and told me that I had to pay 550 euro more fir autorisationfee whatever that is. I asked him to pay everything back but he say he can because the funds are locked in the wallet. I want him to send back everything to me. But he refuse. Can you assist on this. I guess this upfront fees are scams.

## Address

**Address**

 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

**Blockchain explorers**

[View on blockchain.com](#)

[View on blockchair.com](#)

No report has been found.

< 1 >

Loading	Reports (page)	Reports (all pages)
0,342 s	0	0

# Výsledná databáze

## Obsahuje:

- Seznam kryptoměn, adres a zdrojů nahlášení
- Více než 1,1 miliardy unikátních Bitcoinových adres z Bitcoinového blockchainu
- Více než **25 tisíc nahlášených Bitcoinových adres**
- Více než 10 tisíc nahlášených altcoinových adres
- Uživatelské účty, role a API tokeny

## Umožňuje:

- Filtrování seznamu nahlášených adres dle kryptoměny či zdroje nahlášení
- Omezení přístupu k získaným datům pro specifické uživatelské role

## Statistics

Data / Currency	Addresses
<a href="#">All</a>	35 818
 <a href="#">Bitcoin (BTC)</a>	25 591
 <a href="#">Pending</a>	10 227
<a href="#">SeeKoin / Reported BTC Addresses</a>	17 929
 <a href="#">Bitcoin (BTC)</a>	17 929
<a href="#">CheckBitcoinAddress / Reported Addresses</a>	8 250
 <a href="#">Bitcoin (BTC)</a>	5 009
 <a href="#">Pending</a>	3 241

# Nasazení

## Minimální ověřené specifikace zařízení:

- Operační systém: Windows 10 a vyšší
- Úložiště: 500 GB a více



## Programy, které je potřeba nainstalovat:

- PostgreSQL 15.2
- Python 3.11
- Node.js 18.15 LTS



# Závěr

## Shrnutí:

- Implementoval jsem nástroje pro crawlování a vyhledávání kryptoměnových dat z veřejně dostupných zdrojů pomocí metody OSINT
- Bylo nalezeno více než 25 tisíc nahlášených Bitcoinových adres (*a více než 10 tisíc nahlášených adres jiných kryptoměn*)
- Řešení je plně funkční a je možné jej nasadit na cílové zařízení s pomocí přiložené uživatelské příručky

## Možné rozšíření práce:

- Procházení dalších veřejně dostupných zdrojů kryptoměnových adres a nahlášení
- Rozšíření zaměření práce i na jiné kryptoměny mimo Bitcoin (*na síti Ethereum bylo v roce 2022 provedeno až 4x více transakcí*)
- Implementace responzivního designu, podpora mobilních zařízení
- Zpřístupnění dílčích nastavení obou nástrojů přímo na webu
- Zprovoznění řešení na dalších operačních systémech

# Děkuji za pozornost

# Dotaz vedoucího práce

- Během rešerše jste našel množství článků, které popisovaly tvorbu crawlerů kryptoměnových adres z prostředí internetu. Zároveň je však náročné nalézt veřejně dostupné databáze nacrawlovaných adres. Jak je možné, že nejsou podobné databáze k dispozici? Byly tyto projekty neúspěšné?

## **Možné důvody:**

- Získaná projektová data mohla být převzata komerčními subjekty či vyšetřovacími složkami
- Nalezená data mohla být nedostatečného rozsahu či kvality
- Data mohla obsahovat osobní informace, které nebylo možné zveřejnit např. díky GDPR
- Projekty mohly být vyvíjené ve spolupráci s policií, pro kterou by zveřejnění dat mohlo mít nežádoucí následky při vyšetřování kryptoměnových prohřešků (např. praní špinavých peněz)