FACULTY
OF INFORMATICS
Masaryk University

# Detekce slabých bitcoinových klíčů

David Rajnoha

# Základní myšlenka

- Generování náhodnosti může selhat
- Mohou být vytvořeny předvídatelné hodnoty
- Tyto hodnoty jsou použity jako seedy v deterministické generaci klíčů
  - Většina klíčů Bitcoinu je generována podle takového schématu
- Slabé klíče jsou použity k podepsání transakcí v Bitcoinu
  - Proto jsou veřejně dostupné na blockchainu

# Struktura procesu

1. Slabé předpoklady náhodnosti
   - Statisticky nenáhodné
   - Předvídatelné s dodatečnou znalostí
   - Odhadnutelné bez předpokladů
2. Deterministická generace klíčů
   - BIP32
   - BIP44
3. Vyhledávání v klíčích přítomných na blockchainu Bitcoinu
4. Nalezené klíče a seedy
5. Analýza odpovídajících transakcí

# Generování klíče

*Jaké byly předpoklady pro slabé seedy?*

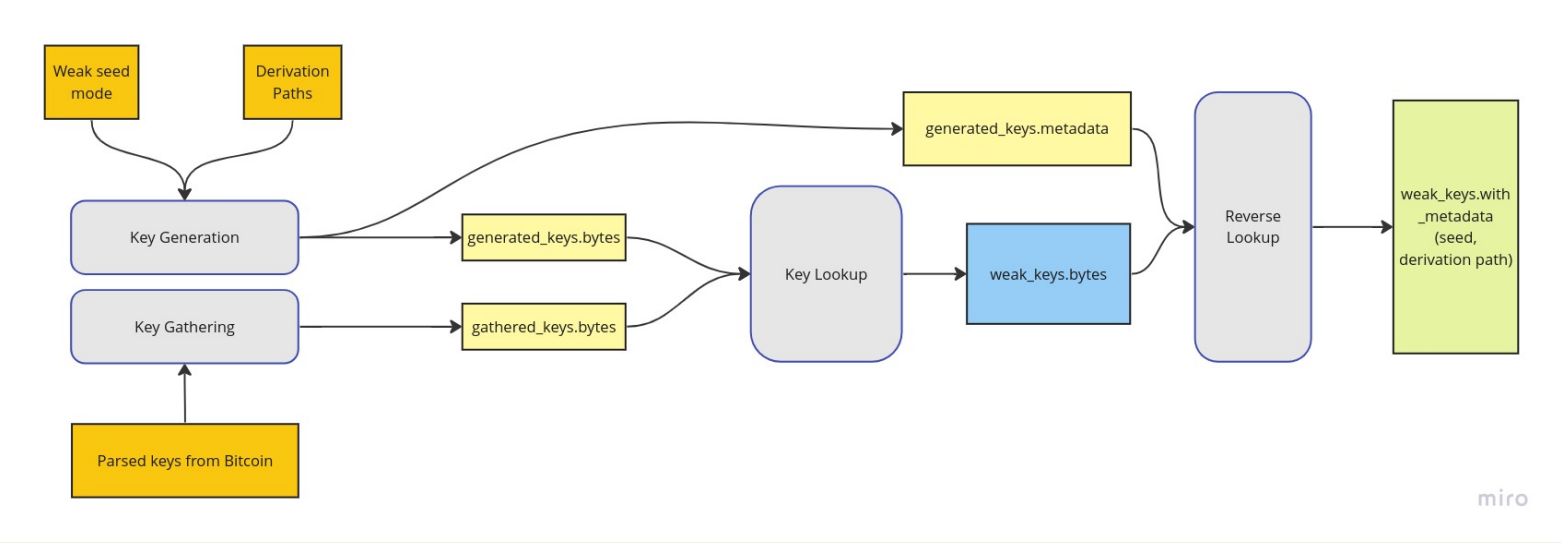
- Předpoklad slabé náhodnosti
- Generování klíčů pomocí těchto seedů

| Metoda generování seedů | Příklad seedu |
|---|---|
| Hammingova váha $\leq 3$ | `00010000000000010000000000000001` |
| Hammingova váha $\geq \#_{bits} - 3$ | `ffffffffefffefffffffffffefffffff` |
| Absolutní hodnota $\leq 2^{12}$ | `00000000000000000000000000000ff` |
| Opakující se vzor | `31313131313131313131313131313131` |

# Shromažďování a vyhledávání klíčů

*Jak byly identifikovány slabé klíče v Bitcoinu?*

- 1 478 790 377 shromážděných klíčů [1]
- Celkem vygenerováno 201 879 776 klíčů




[1] https://github.com/crocs-muni/bitcoin-keys-analysis

# Výsledky

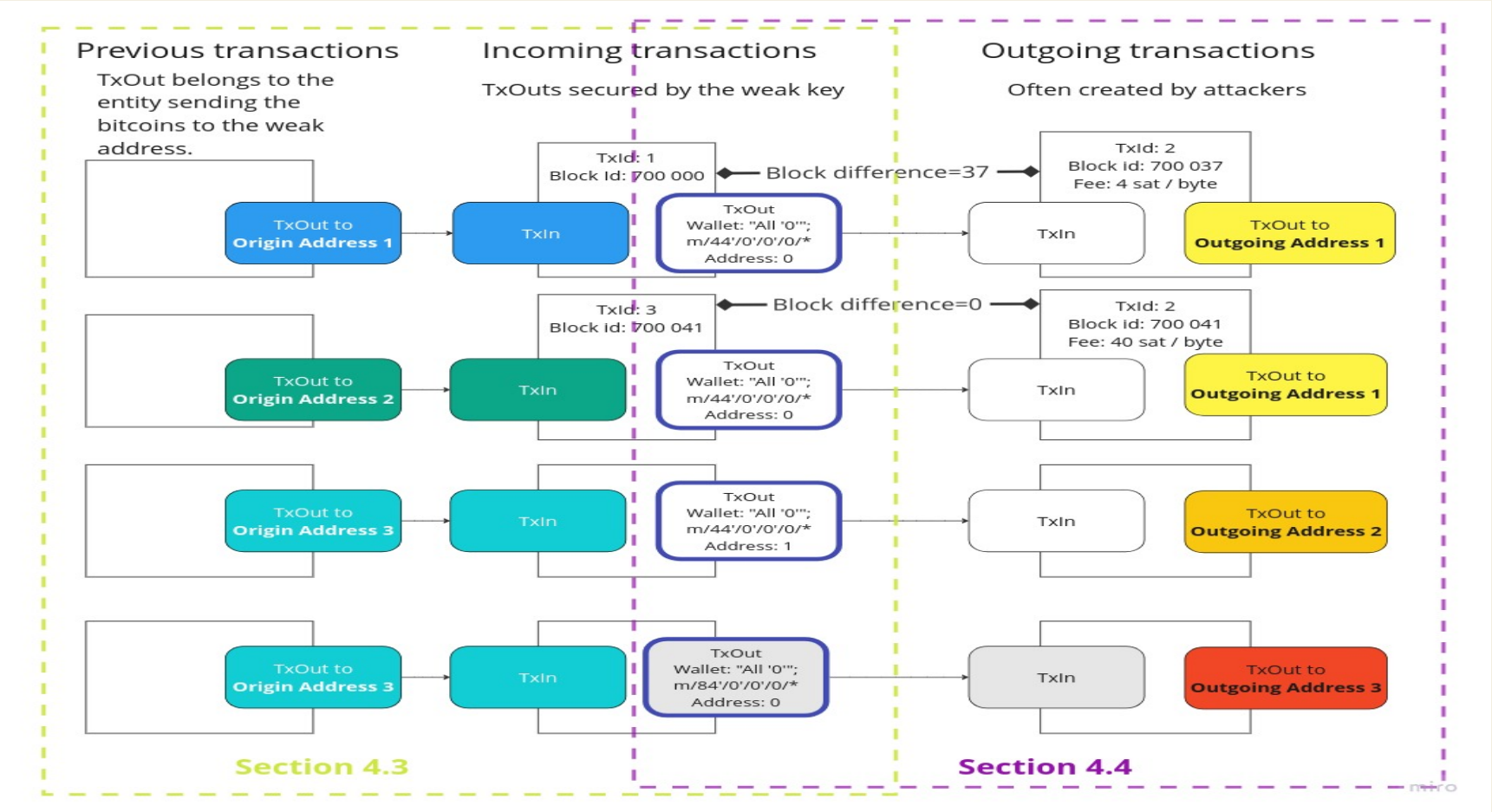
*Které seedy byly použity u nalezených slabých klíčů?*

- 23 slabých klíčů (kombinace seedu a derivační cesty)
- 14 různých seedů
- Použito v 187 transakcích
- Většina seedů měla všechny bity ’0’

| Kategorie | Příklad (spodních 64 bitů) | #Klíčů | Transakce | % Transakcí |
|---|---|---|---|---|
| Všechny ’0’ | `0000000000000000` | 10 | 165 | 88% |
| Všechny ’1’ | `ffffffffffffffff` | 3 | 8 | 4% |
| Nízká hodnota | `0000000000004440` | 7 | 7 | 4% |
| Vzor | `3131313131313131` | 3 | 7 | 4% |

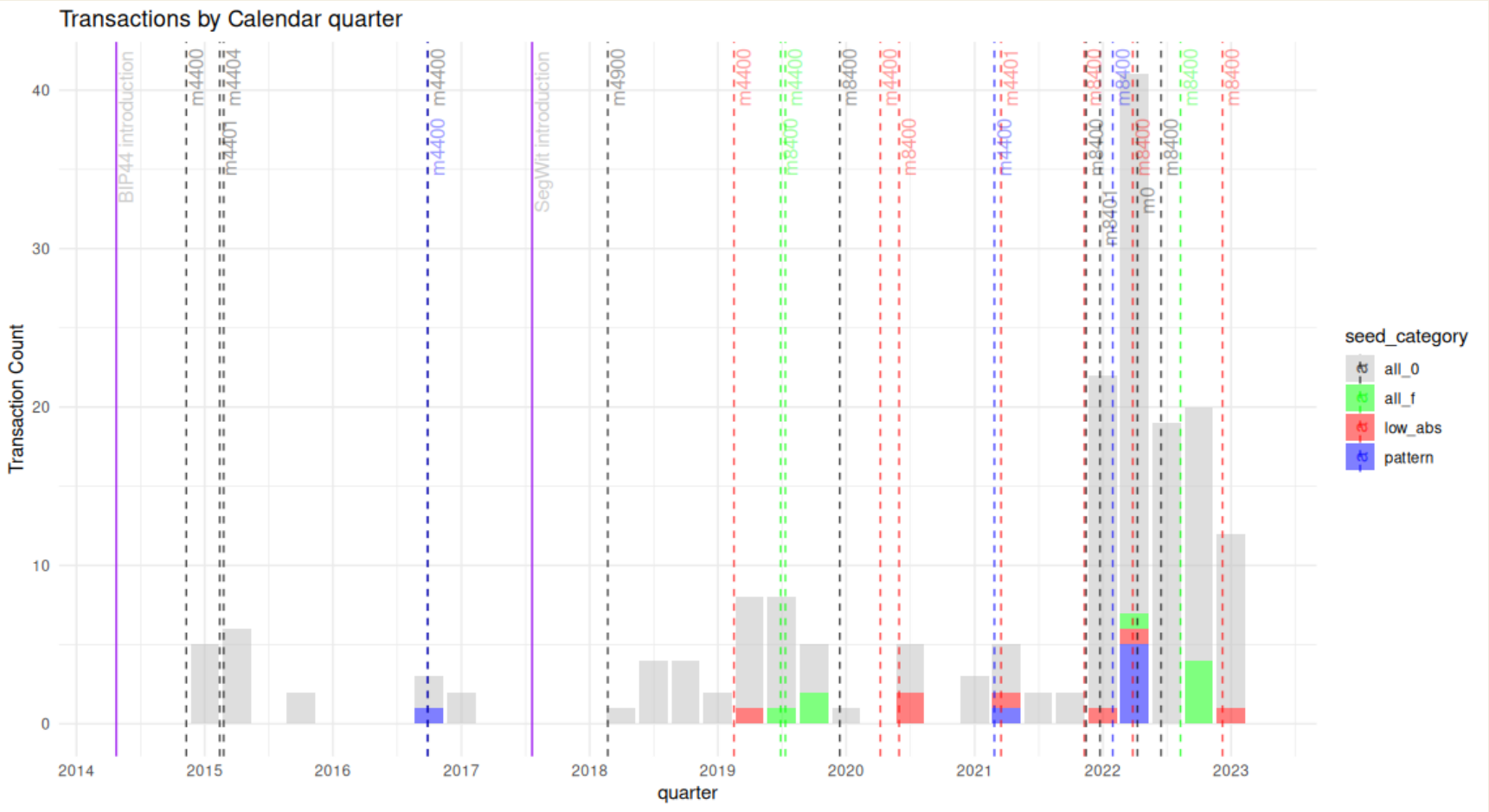
# Analýza transakcí

*Co dalšího můžeme zjisti?*



# Příchozí transakce

*Kdy a proč byly tyto klíče vygenerované?*



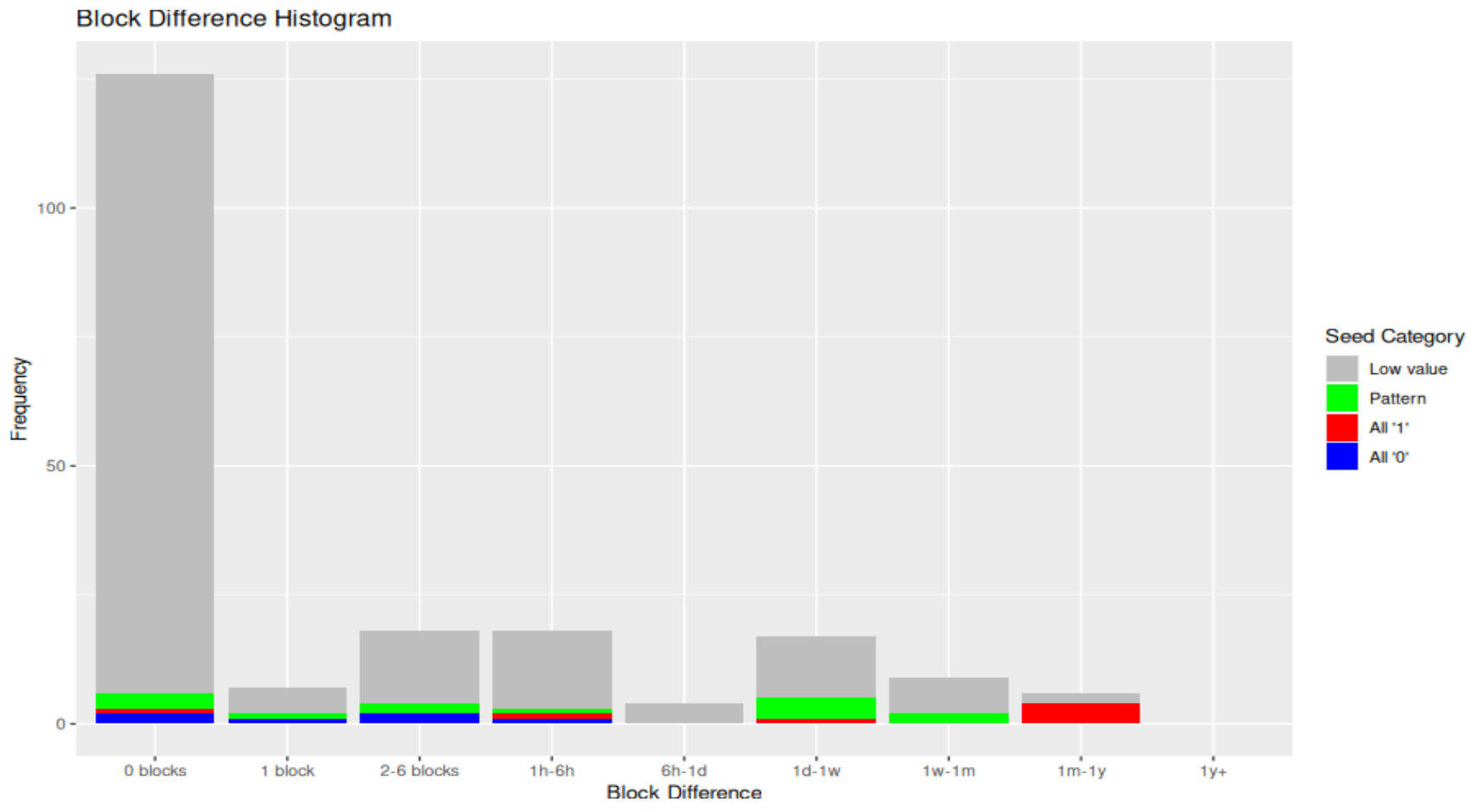
# Odchozí transakce

*Kdo ví o zranitelnosti a jak ji zneužívá?*

- Všechny výstupy transakcí jsou utraceny
- 60 % odchozích transakcí zařazeno ve stejném bloku jako příchozí
  - 80 % během 4 hodin
  - 90 % během týdne
- Adresy spojené s více výstupy transakcí
  - U několika z nich "naše" transakce představují 10 – 20 % všech přijatých transakcí

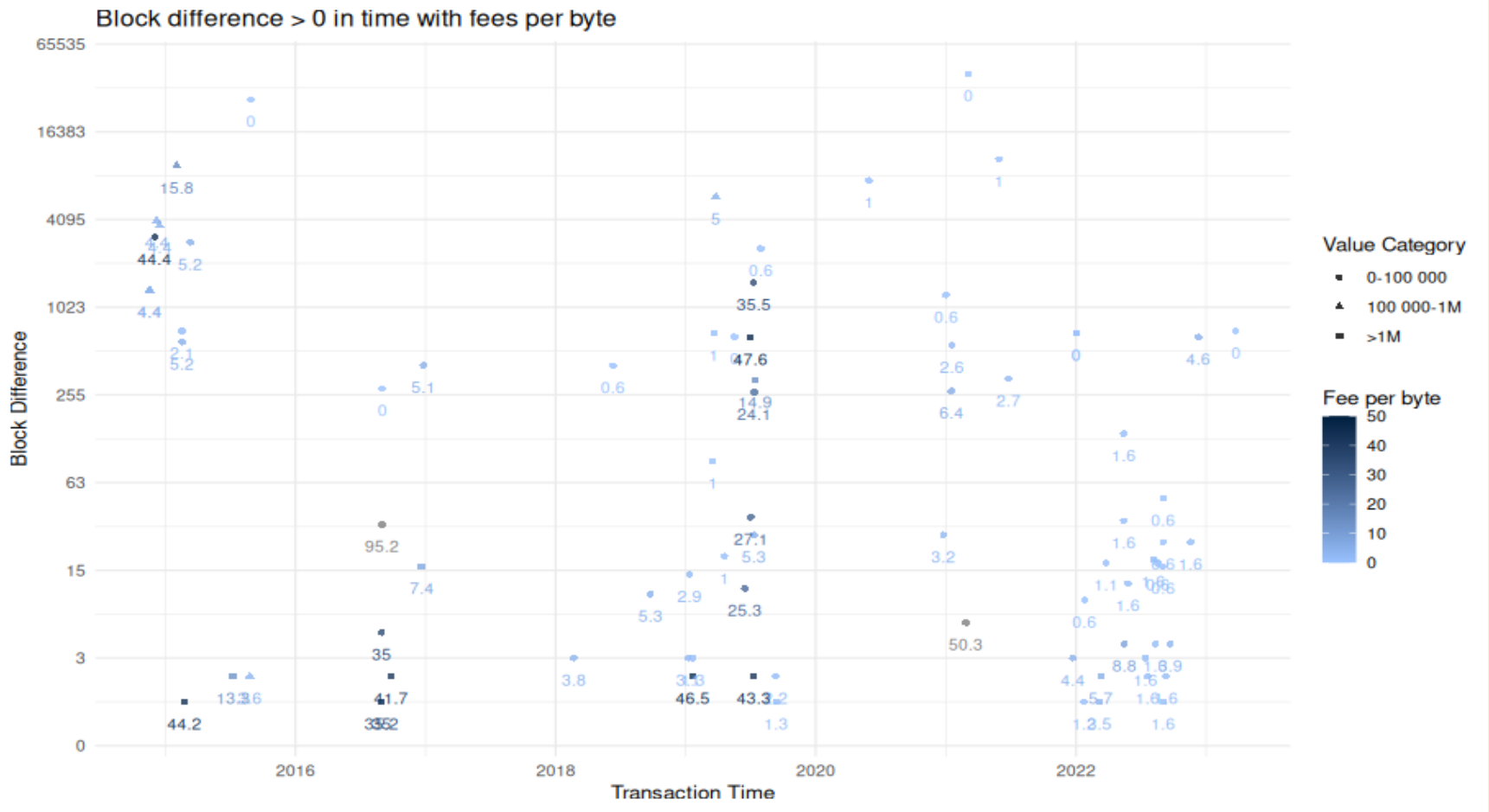
# Odchozí transakce

*Čas mezi příchozí a odchozí transakcí*



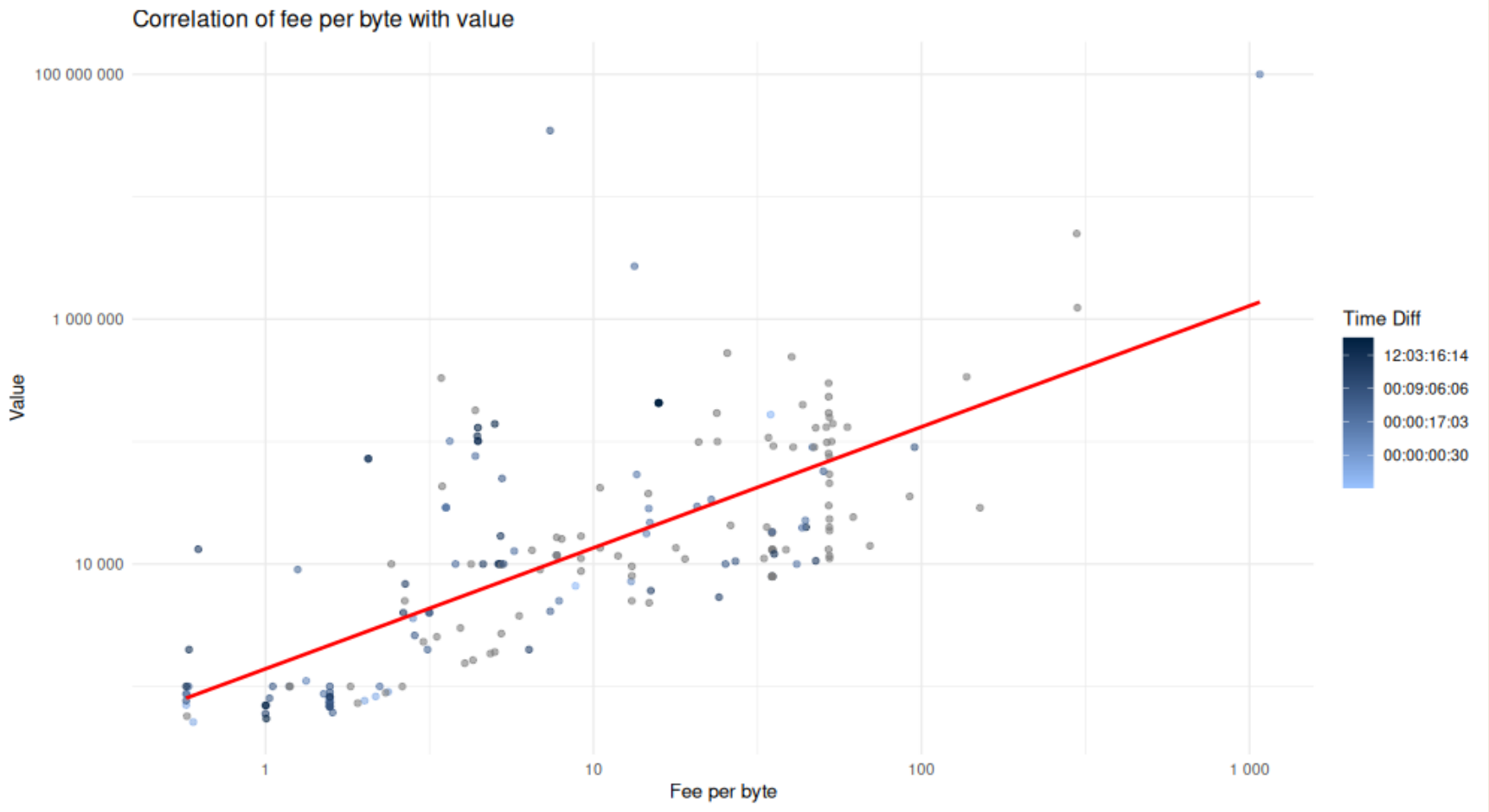
# Odchozí transakce

*Visualizace poplatků*



# Odchozí transakce

*Korelace poplatků a hodnoty*



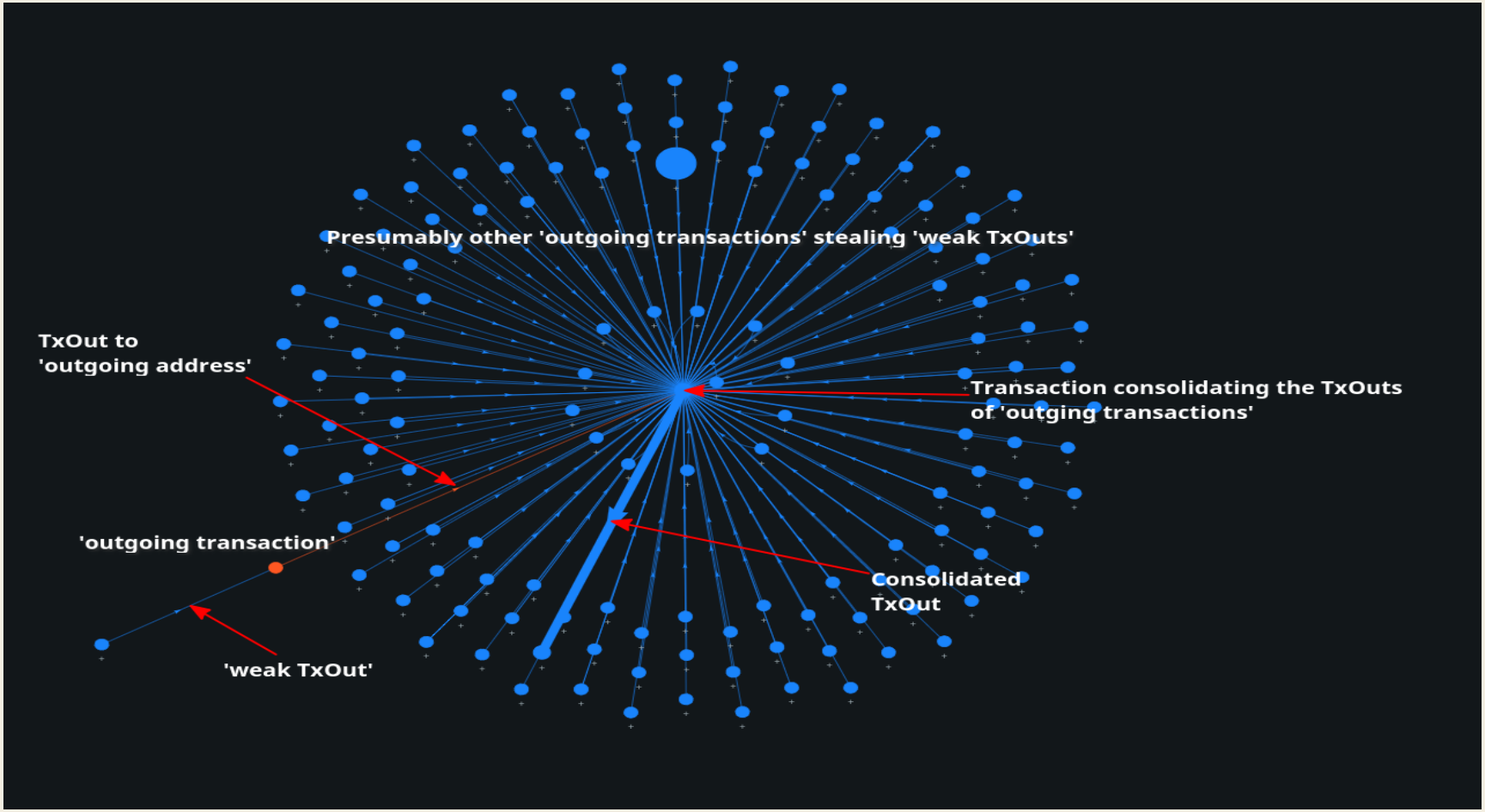
# Analýza Transakcí

*Duplicitní odchozí adresy*

| Adresa | Trans. | Všechny Trans. | Přijato[2] | Propojené Účty |
|---|---|---|---|---|
| 1Cfaun | 21 | 222 | 0.25 | 000000 128 m/44'/0'/0'<br>000000 128 m/84'/0'/0' |
| bc1qce | 4 | 39 | 0.0081 | 000000 128 m/44'/0'/0'<br>ffffff 128 m/44'/0'/0' |
| 3K5MSu | 2 | 3 | 0.0024 | 000000 128 m/44'/0'/0'<br>000000 128 m/49'/0'/0' |
| 193P6L | 2 | 277 | 5.65 | 000000 256 m/44'/0'/0'<br>000000 128 m/44'/0'/4' |
| bc1qmt | 17 | 144 | 0.016 | 000000 128 m/84'/0'/0' |
| bc1qh7 | 9 | 14 | 0.0049 | 000000 128 m/84'/0'/0' |
| 19a7HG | 8 | 9 | 0.014 | 000000 128 m/44'/0'/0' |
| bc1q4s | 5 | 24 | 0.47 | 000000 256 m/84'/0'/0' |
| 37QKHp | 5 | 8 | 0.0076 | 000000 128 m/84'/0'/0' |
| bc1qnn | 5 | 5 | 0.00051 | 000000 128 m/0' |

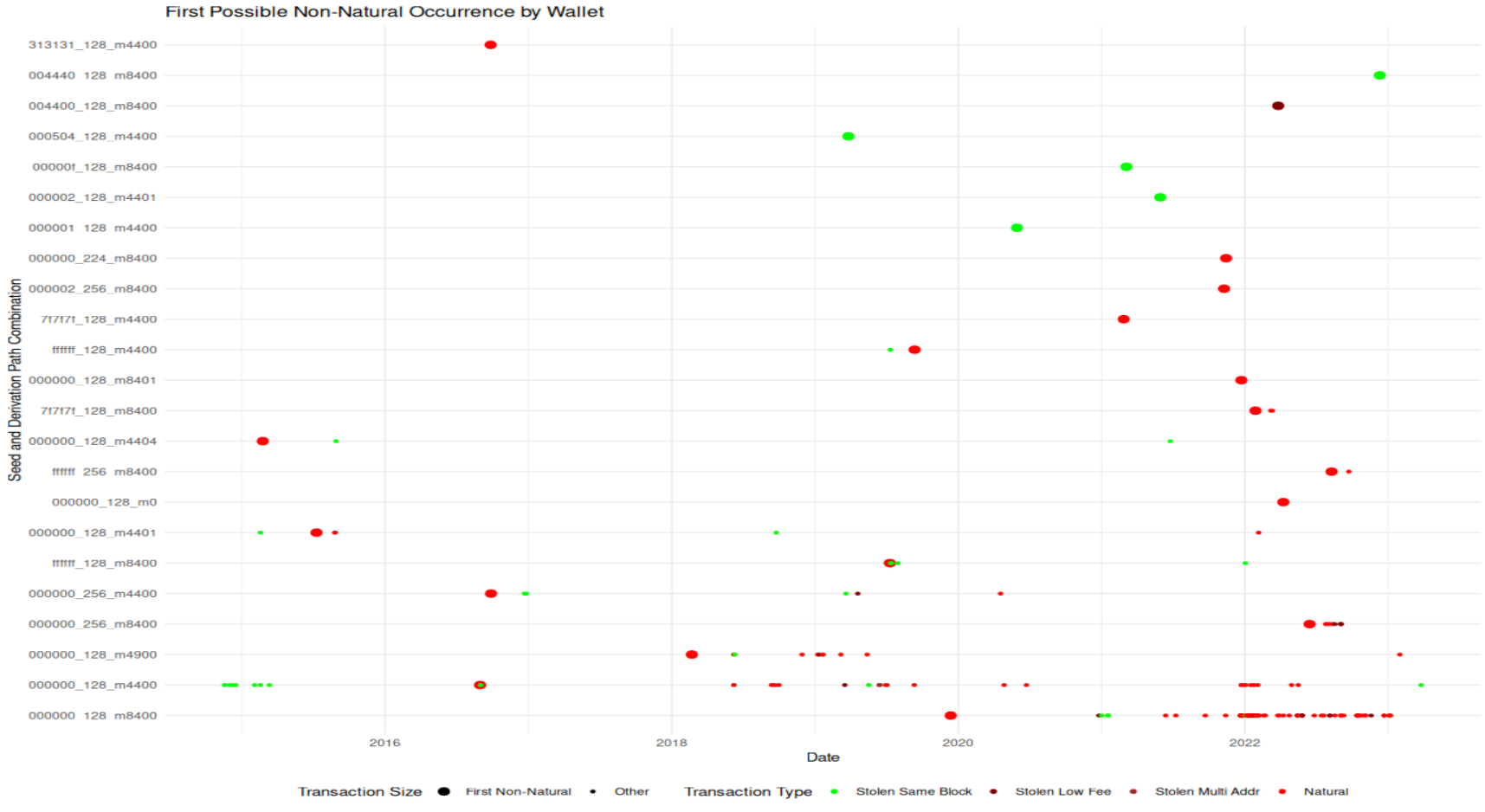
# Odchozí transakce

*Duplicitní odchozí adresy*



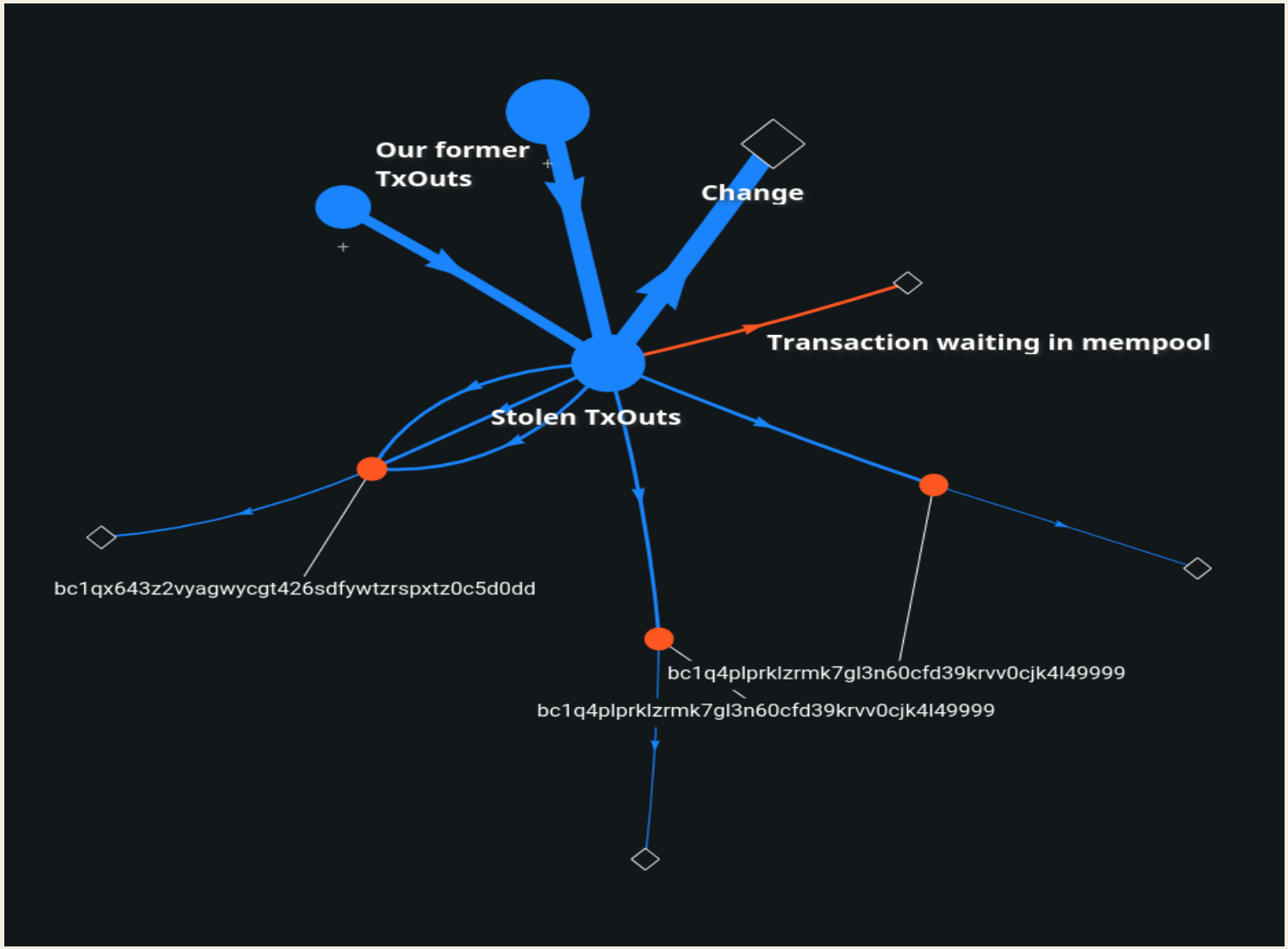
# Odchozí transakce

*Klasifikace transakcí*



# Odchozí transakce

*Neovlivněné adresy*



# Odchozí transakce

*Neovlivněné adresy*

| Účet | Převedeno na | Rozdíl bloků |
|---|---|---|
| `00000f 128 m/84’/0’/0’` | bc1q4plprk | 53 |
| `000001 128 m/44’/0’/0’` | bc1q4plprk | 176 |
| `000504 128 m/44’/0’/0’` | bc1qmw5vxv | 3796 |
| `004400 128 m/84’/0’/0’` | bc1qx643z2 | 29 |
| `004440 128 m/84’/0’/0’` | bc1qx643z2 | 29 |
| `000002 128 m/44’/0’/1’` | bc1qx643z2 | 29 |

# Závěr

*Jaké jsou hlavní závěry?*

- Klíče generované pomocí slabé náhodnosti jsou přítomny
  - Nejčastěji se vyskytující slabý seed se skládá ze všech ’0’ bitů
- Zranitelnost je známa mezi útočníky
  - Můžeme vidět pouze zlomek všech slabých klíčů

# Kontakt

- David Rajnoha
- Kompletní text práce
- LinkedIn