MASARYK
UNIVERSITY
Czech Republic

Darknet market analysis and user de-anonymization

Tomáš Šíma

MASARYK UNIVERSITY
Czech Republic

Cíle

- Stáhnout web dark marketu a analyzovat jeho ekosystém
  - Celkový obrat, loajalita zákazníků, zisky prodejců…
- Prozkoumat možnosti de-anonymizace uživatelů
  - Online fóra: BTC adresa – Nickname
  - Metadata ze stránek dark marketu
  - Analýza bitcoinového blockchainu
- Vytvořit nástroj pro vizualizaci a hledání v těchto datech

MASARYK UNIVERSITY
Czech Republic

Dark markety

- Komerční online weby
- Lidé na nich prodávají a kupují ilegální zboží a služby
- Podobné jako ebay nebo aukro
- Anonymita
    - Web jako .onion služba přístupná skrz Tor
    - PGP pro komunikaci prodejce zákazník
    - Bitcoiny jako nástroj platby

MASARYK UNIVERSITY
Czech Republic

Výběr dark marketu

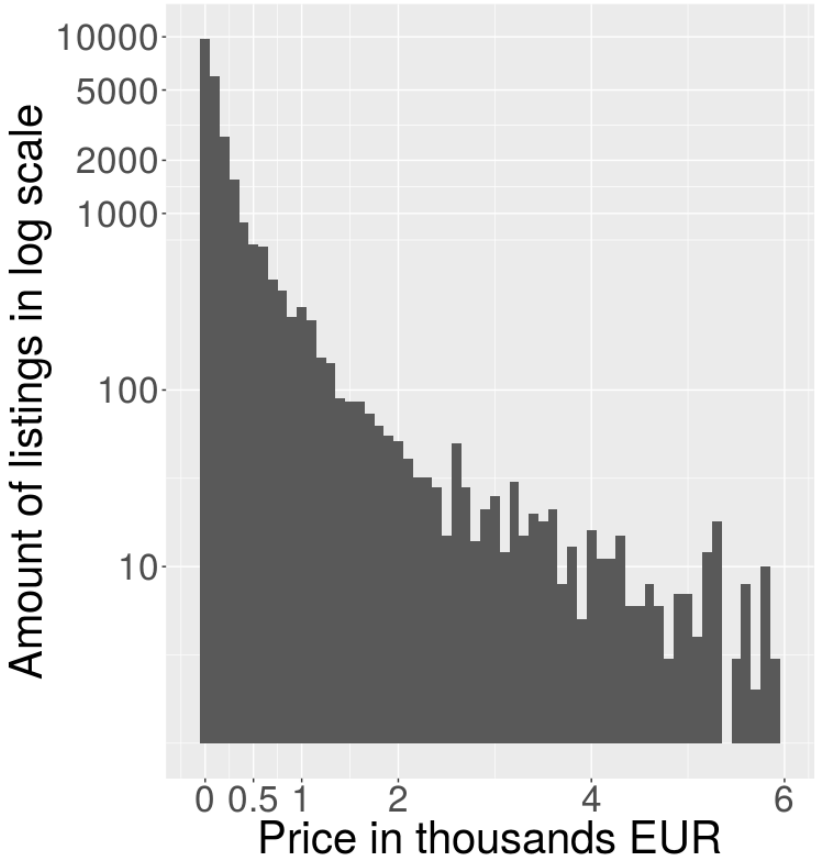
- Vybral jsem dark market Valhalla
  - Druhý největší množství aktivních inzerátů
- Největší množství dat
  - První a poslední dvě písmena nicku zákazníka
  - Částka a konkrétní inzerát u feedbacku od zákazníka
  - Celkový výdělek a počet obchodů prodejců
  - Celková útrata a počet obchodů kupujících

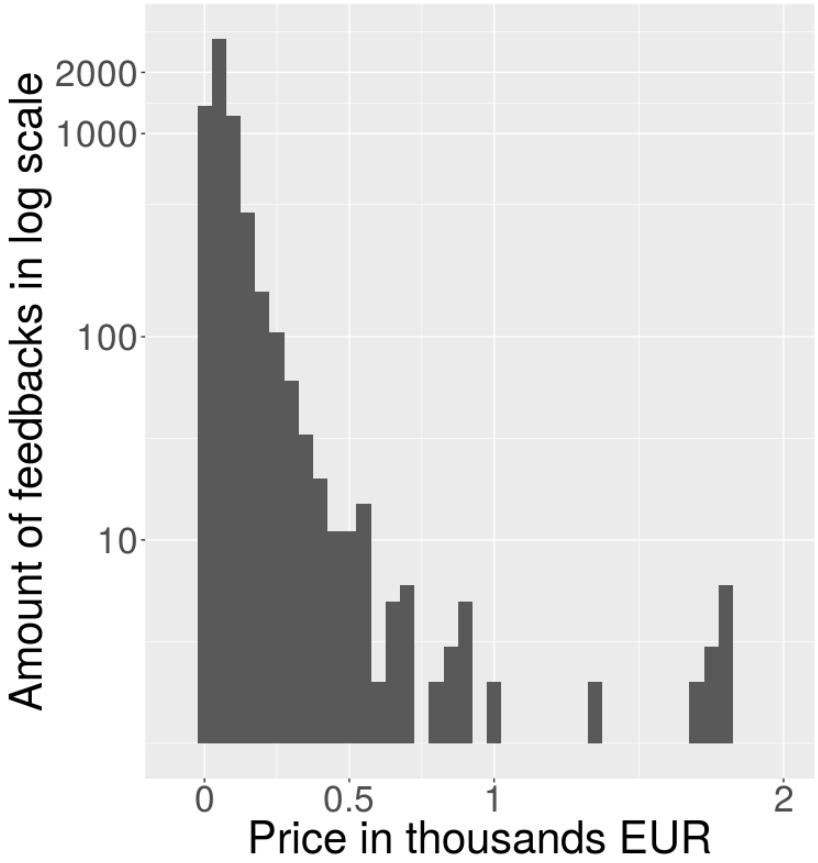
MASARYK UNIVERSITY
Czech Republic

Pozorování – kategorie inzerátů

Category	listings	feedbacks	revenue in euros	average price in euros	market share
Cannabis	5139	1883	135693	72	27.6 %
Stimulants	3493	1043	108157	103	22 %
Opiates	1662	489	83135	170	16.9 %
Pharmacy	2294	1104	62054	56	12.6 %
Body building	679	402	31466	78	6.4 %
Empathogens	2988	394	20344	51	4.1 %
Other drugs	774	173	14350	82	2.9 %
Psychedelics	1377	198	11796	59	2.4 %
Other products	782	89	9106	102	1.8 %
Self-defence	513	4	4635	1158	0.9 %
Services	1662	35	4061	116	0.8 %
Dissociatives	290	38	2317	60	0.5 %
Classifieds	649	18	2182	121	0.4 %

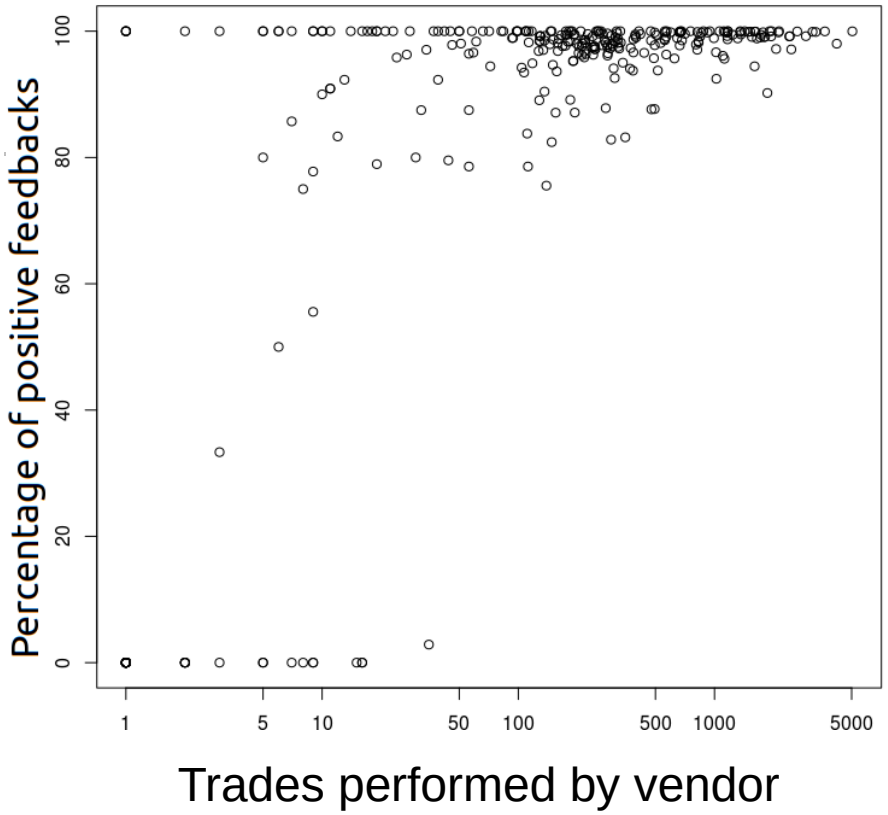
Pozorování – ceny inzerátů vs ceny ve feedbacku

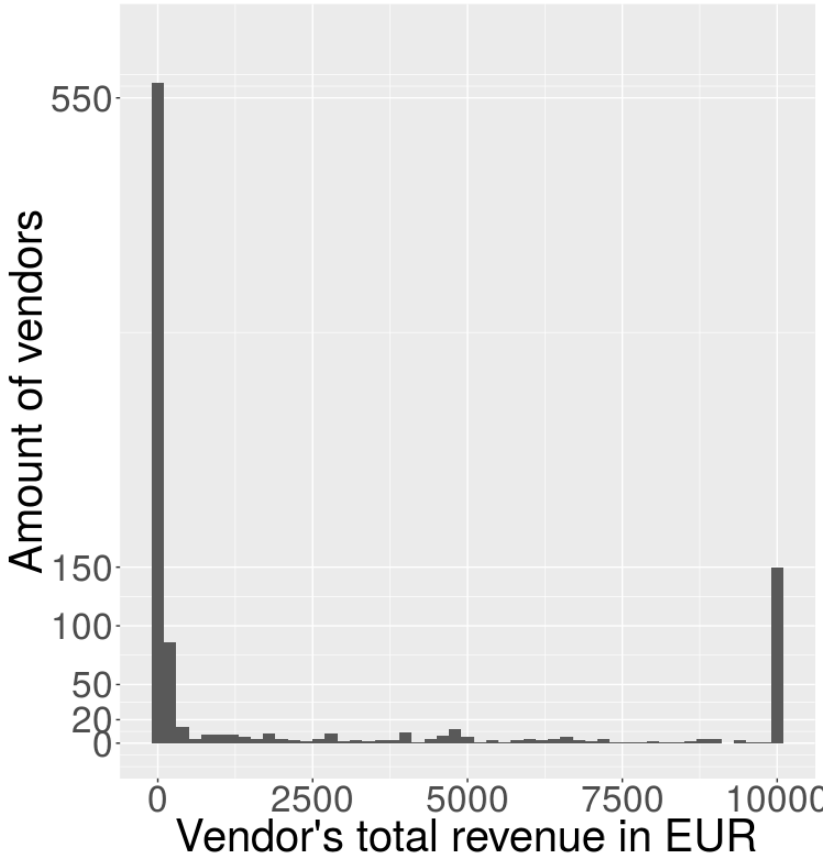




MASARYK UNIVERSITY
Czech Republic

Pozorování – prodejci, zisk a feedback





MASARYK UNIVERSITY
Czech Republic

Statistika – shrnutí

- Za měsíc (Data o obchodech z feedbacků = minimální částky):

  Obrat 500 000 EUR, 7000 obchodů

  90% ze zákazníků

  1-2 obchody

  Průměrný nákup: 80 EUR

- Za celou působnost dark marketu

  Průměrná celková útrata zákazníka: 1176 EUR

  Dvě skupiny účtů

  75% zákazníků, 80% prodejců < 1 000 EUR

  7% zákazníků, 12% prodejcu > 10 000EUR

MASARYK UNIVERSITY
Czech Republic

Data - Metadata na stránkách

- EXIF metadata obrázků
  - Automaticky přepsané
- PGP klíče – 150 prodejců
  - ROCA útok – možnost spočítat privátní klíč
    - Žádný nebyl zranitelný
  - Metadata – nick + mail
    - Manuálně googleno, nic zajímavého nenalezeno
- Sken portů serveru dark marketu – jen 443(HTTPS)

MASARYK UNIVERSITY
Czech Republic

Data – bitcoin blockchain

- Decentralizovaná “kniha transakcí”
- 1 uživatel = víc adres

  Typicky generuje novou adresu pro každý přijem BTC

  Při posílání bitcoinů posíla BTC z podmnožiny svých adres najednou
- Transakce má víc vstupů a výstupů

  BTC adresy + množství BTC převedených v transakci

MASARYK UNIVERSITY
Czech Republic

Data – BTC adresy : identita

- Data
  - BTC adresa
  - Identita(nickname)
  - URL kde byla nalezena
- Zdroje
  - Bitcointalk, reddit, twitter, blockchain.info
- 160 000 záznamů

MASARYK UNIVERSITY
Czech Republic

Data – BTC adresy dark marketu Valhalla

- Založil jsem dva účty
- 1 měsíc od sebe vzdálené
- Na každém provedl

  2 deposity

  20 výběrů

- Získal jsem 92 bitcoinových adres patřících dark marketu

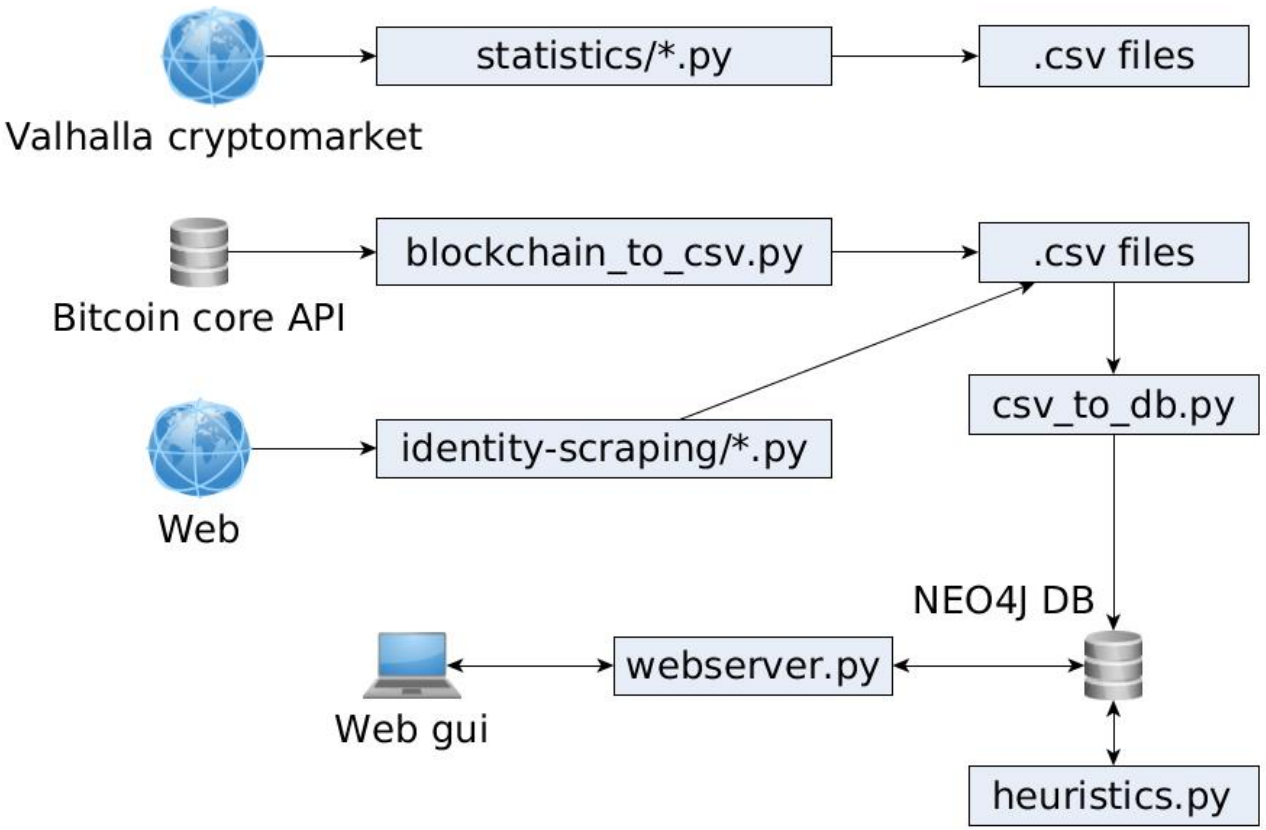
MASARYK UNIVERSITY
Czech Republic

Aplikace

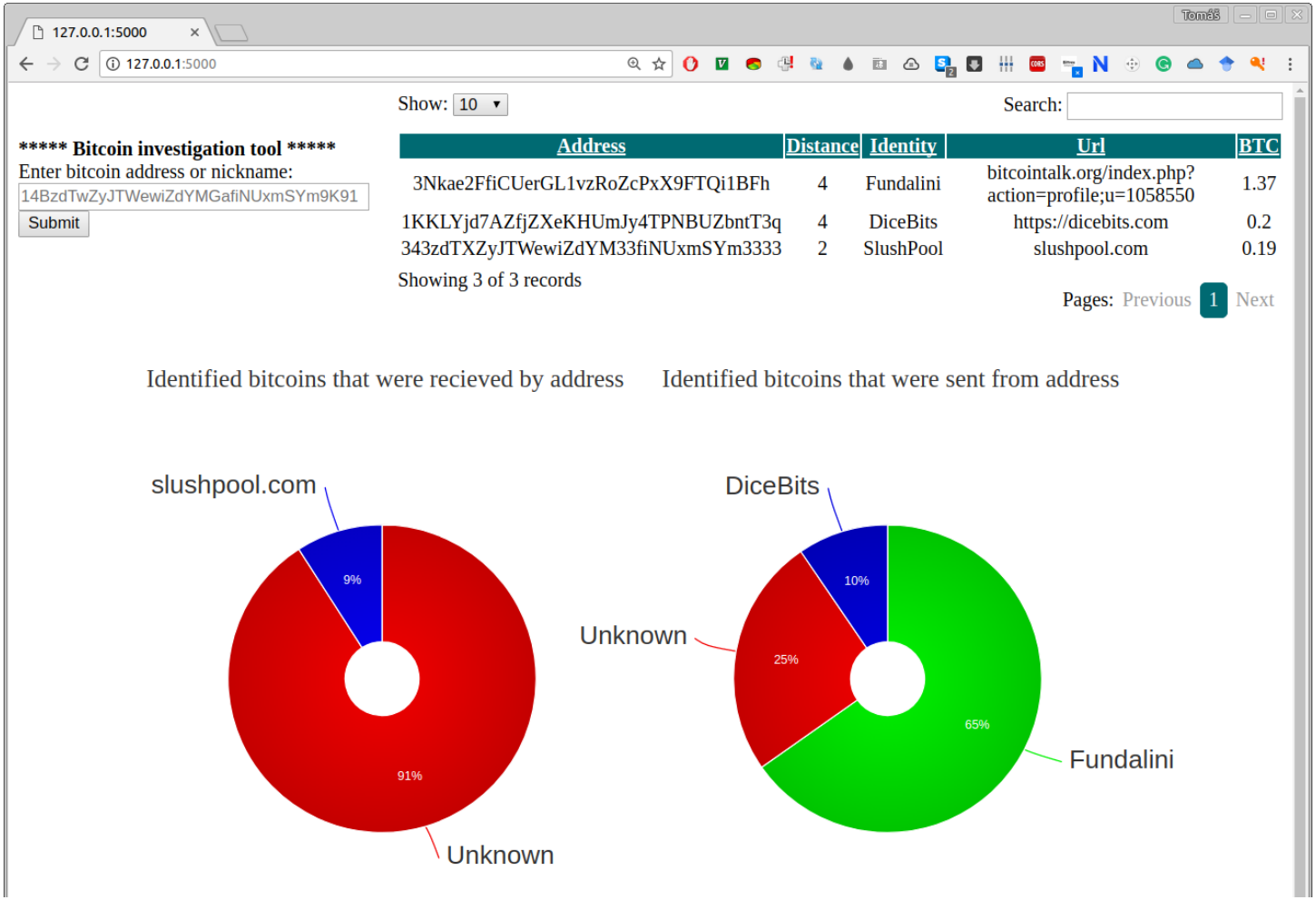
- Data
  - BTC blockchain - graf v Neo4j grafové databázi
  - Data o identitách, kromě dark marketu
  - Adresy z dark marketu použity pro verifikaci
- Clusterování BTC adres patřících jedné entitě
  - Na základě dvou heuristik
- Grafické rozhraní
  - Zadá se adresa – najde blízké adresy s identitou

MASARYK UNIVERSITY
Czech Republic

Aplikace - architektura



GUI


127.0.0.1:5000
Tomáš
Show: 10
Search:
***** Bitcoin investigation tool *****
Enter bitcoin address or nickname:
14BzdTwZyJTWewiZdYMGafiNUxmSYm9K91
Submit
Address
Distance
Identity
Url
BTC
3Nkae2FfiCUerGL1vzRoZcPxX9FTQi1BFh
4
Fundalini
bitcointalk.org/index.php?action=profile;u=1058550
1.37
1KKLYjd7AZfjZXeKHUmJy4TPNBUZbntT3q
4
DiceBits
https://dicebits.com
0.2
343zdTXZyJTWewiZdYM33fiNUxmSYm3333
2
SlushPool
slushpool.com
0.19
Showing 3 of 3 records
Pages: Previous 1 Next
Identified bitcoins that were recieved by address
Identified bitcoins that were sent from address
slushpool.com
9%
91%
Unknown
DiceBits
10%
Unknown
25%
65%
Fundalini

MASARYK UNIVERSITY
Czech Republic

Úspěšnost clusterování bitcoin adres

- Ověřeno na adresách patřících dark marketu
  - 92 adres, které jsme získali = 11 clusterů
  - 2 clustery obsahovaly adresy z obou účtů
  - Celkem 754 adres
  - Za měsíc přijato 5.71 BTC = 9% obratu Valhally
  - U 35 adres ze 754 nalezena blízká identita
    - Žádné účty/nickname
    - 4 mining pooly a 6 gambling služeb

MASARYK UNIVERSITY
Czech Republic

Shrnutí

- Statistická analýza marketu
- Aplikace
  - Nahraje blockchain a identity
  - Provede clustering
  - Pro danou adresu najde blízké adresy s identitou
- 20 a 20 výběrů z dark marketu měsíc od sebe
  - Identifikace 9% obratu (754 adres)
  - Nalezeno k 35 z nich 10 blízkých identit

MASARYK UNIVERSITY
Czech Republic

Děkuji za pozornost

Dotazy?

MASARYK UNIVERSITY
Czech Republic

Přechod dark marketů na Monero

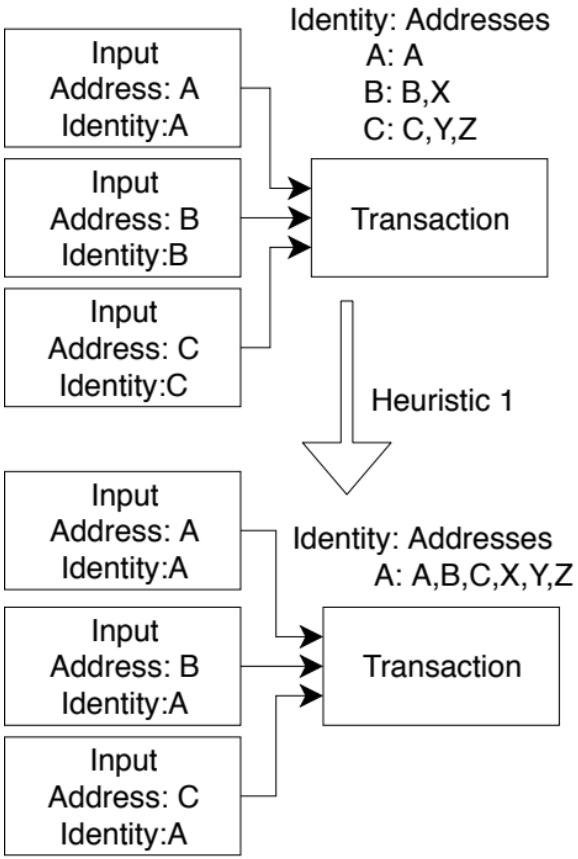
- Monero znemožňuje clusterování i deanonymizaci
- Blockchain monera je šifrovaný – ring signatures
- Transakce šifrované
  - Odesílatel přidává do transakce náhodné cizí vstupy
  - Jen on ví, který z nich je jeho
- Privátní klíč adresy nutný pro identifikaci transakcí
- Možné útoky skrz side channels
  - Monero forky
  - Někteří uživatelé nepoužívají zamíchání vstupů

MASARYK UNIVERSITY
Czech Republic

Scrapování dark marketu Valhalla

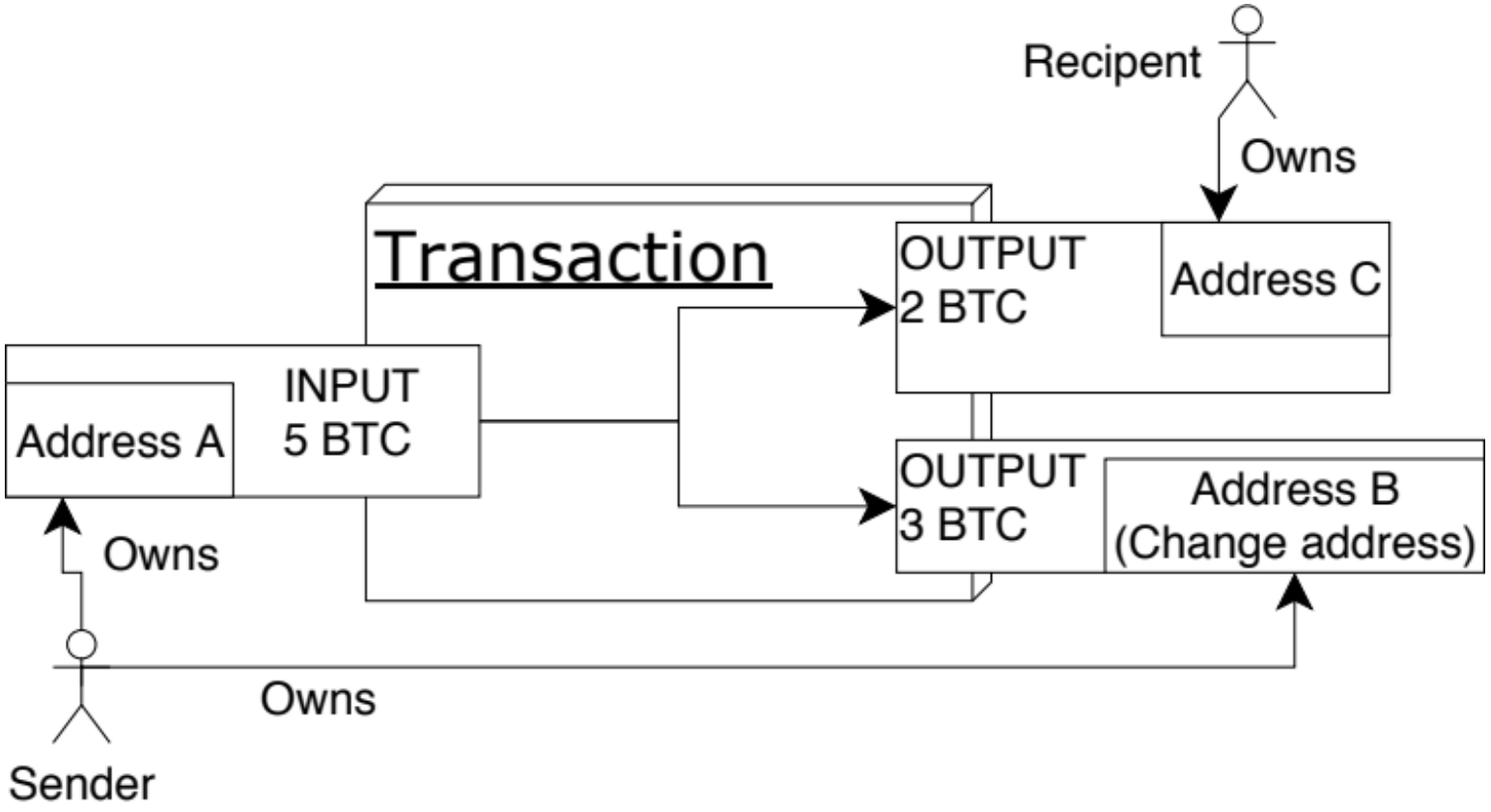
- Někdy valhalla neodpověděla
  - Opakování po 2,4,8,16,32 sekundách
- Valhalla vracela stránku, že je přetížená
- Throttling 1 request/2s
- Stažené stránky porovnány s informací o přetížení
  - Asi 3% stránek s informací o přetížení
  - Stáhnuté znova

Aplikace – 1. heuristika

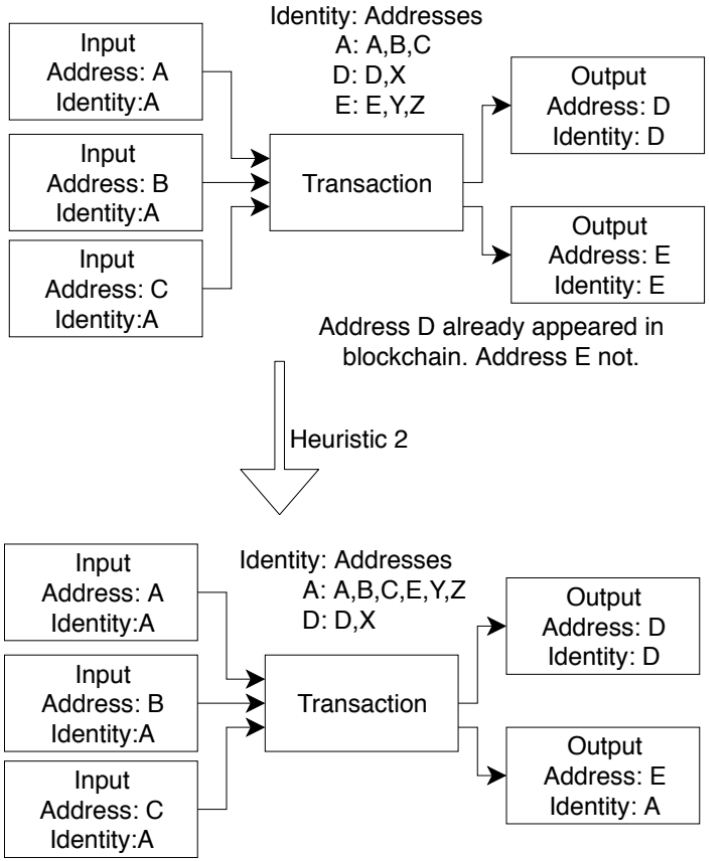


MASARYK UNIVERSITY
Czech Republic

Aplikace – mechanismus dělení bitcoinů



Aplikace – 2. heuristika



MASARYK UNIVERSITY
Czech Republic

Deanonymizace adres

- 160 000 záznamů z webu (btc adresa : nickname)

  Clusterování rozšířilo na 450 000 adres

- Dark market

  92 adres → 754 adres

  10 identit blízko dark marketu