Analise de Blockchain

Ivan Sendin

FACOM - Universidade Federal de Uberlândia
ivansendin@yahoo.com,sendin@ufu.br

20 de agosto de 2024

Aula Passada

- Ecossistema
- Exchanges
- ATM, Apostas,...
- Mixers
- Mercados (ilegais)
- Oportunistas: Ransomware, sextorsion
- CoinJoin
  transação 1
  transação 2.

- *Open Source Intelligence* (OSINT)
- WWII
  BBC/FBMS
- Coleta de dados de fontes abertas
  Jornais, relatorios governamentais,...
- Buscadores, Redes sociais,...

- Faraó dos Bitcoins
- Empresário acusado de promover pirâmides financeiras
- Google “Faraó dos Bitcoins”
- Carteira usada pelo Faraó dos Bitcoin é revelada
- Ao acessar o link, obtemos 9 endereços

```
farao = ['1JawWE56G5NmnB5iuYbFikbdETs88Fxkwo',
     'bc1qluuy04mjxqj8yc44lgnez8eml4pwulvukfatak',
     'bc1qt7jjpqdfvqhtqkadlnuhzzem2tateg7mm0y95w',
     'bc1q8kmtzc0a43w0cjrzwzwqsa9frxaseyzcg6mq3d',
     'bc1qqgjmxevtn3cyg8cvxfg7yyk6a7n3zudt4hw85t',
     'bc1qn9k6s0lyxgw5mdndta3780md23z9kmu4980clv',
     'bc1qu9tj6kcusrncvm7wm06n2mqq0jtfg26vk9mynm',
     'bc1qnanyweuswqm9sz3d93ag0vrc69mpq4v40g9acq',
     'bc1qehzj8sulj3plzuarzzmdm77d6rd8chvc5hzull']
```

- Acessar as transacoes dos endereços
- Aplicar o H1 e (tentar) obter outros endereços

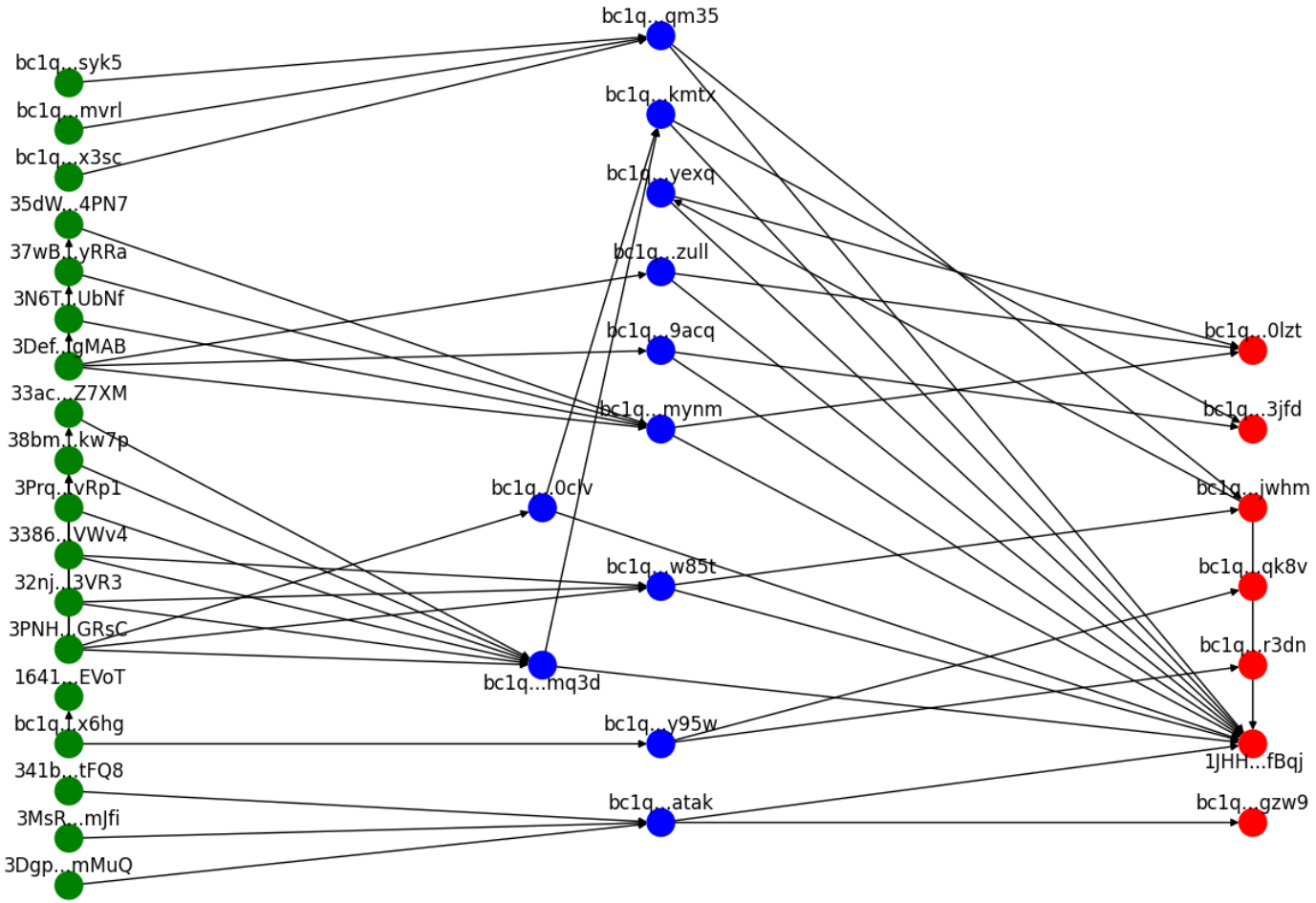
```
tocluster = {}
for f in farao:
    url = "https://blockchain.info/rawaddr/{}"
    resp = requests.get(url=url.format(f))
    data = resp.json()

    tocluster[f] = []
    for tx in data['txs']:
        temp = [ i['prev_out']['addr'] for i in tx['inputs']]
        if f in temp:
            tocluster[f].append(temp)

    n_tx =data['n_tx']
    done = len(data['txs'])

    while (done<n_tx):
        url = "https://blockchain.info/rawaddr/{}?offset={}"
        resp =requests.get(url=url.format(f,done))
        data = resp.json()
        for tx in data['txs']:
            temp = [ i['prev_out']['addr'] for i in tx['inputs']]
            if f in temp:
                tocluster[f].append(temp)
        done += len(data['txs'])
```

- armazeno em `tocluster` listas de entradas de transações contendo pelo menos um endereço faraó
- Aplico o H1 em cada endereço

```
for a in farao:
    print('-----------------')
    clusters= []
    for tx in tocluster[a]:
        c = []
        for i  in range(len(clusters)):
            if temInterseccao(clusters[i],tx):
                c.append(i)

        if len(c)==0:
            clusters.append(tx)
        else:
            x = c[0]
            del c[0]

            clusters[x].extend(tx)

            for i in c:
                clusters[x].extend(clusters[i])

            clusters[x] = list(set(clusters[x]))

    print(a)
    if (len(clusters)==1 and len(clusters[0])<10):
        print(set(clusters[0]))
    else :
        print(len(clusters[0]))
```

Endereço	Cluster
1Jaw...xkwo	–
bc1qlu...atak	bc1qlu...atak
bc1qt...y95w	bc1qt...y95w
bc1q8...mq3d	bc1q8...mq3d,bc1qn...0clv
bc1qq...w85t	bc1qq...w85t,**bc1q6...qm35**
bc1qn...0clv	bc1qn...0clv,bc1q8...mq3d
bc1qu...mynm	bc1qu...mynm,bc1qe...zull,**bc1qz...yexq**
bc1qn...9acq	bc1qn...9acq, **bc1qp...kmtx**
bc1qe...zull	bc1qe...zull,bc1qu...mynm,**bc1qz...yexq**

1Jaw...xkwo: 6287 endereços!!


bc1q...qm35
bc1q...syk5
bc1q...kmtx
bc1q...mvrl
bc1q...yexq
bc1q...x3sc
bc1q...zull
35dW...4PN7
bc1q...9acq
37wB...yRRa
bc1q...mynm
3N6T...UbNf
bc1q...0lzt
3Def...gMAB
bc1q...3jfd
33ac...Z7XM
bc1q...0clv
bc1q...jwhm
38bm...kw7p
3Prq...vRp1
bc1q...w85t
bc1q...qk8v
3386...VWv4
32nj...3VR3
bc1q...r3dn
3PNH...GRsC
bc1q...mq3d
1641...EVoT
bc1q...y95w
bc1q...x6hg
1JHH...fBqj
341b...tFQ8
bc1q...atak
bc1q...gzw9
3MsR...mJfi
3Dgp...mMuQ

- Em azul: endereços controlados pelo faraó
- Em verde: pagamentos para o faraó
  Vítimas??
- Em vermelho: quem recebeu do faraó
  ??????
  - 1JHH...fBqj
  - bc1q0...zw9 recebeu de bc1ql..fatak

Clusterizar o endereço 1JHH...fBqj