Analise de Blockchain

Ivan Sendin

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

13 de agosto de 2024

Café com BIT [Episódio 3]: Talk Internacional - Dr. Johnnatan Messias

Aula Passada

- Endereços
  Chave Pública (existem mais...)
- Transações
  UTxO
- Suficiente para o Bitcoin funcionar

Entrada	Saída
$(abc,10)$	$(qwe,10)$
$(bce,20)$	$(rty,20)$

- Protocolo do Bitcoin
  Bem definido....implementado em várias linguagens
- Ecossistema
  O que esta em volta, como o bitcoin é usado
  Outro protocolos ou cenário nebulosos

- Ganhos financeniros especulativos
- Anonimo
- Ideal para atividades ilegais
- pseudo anonimato

Bitcoin...sempre ilegal ?

- Definir ilegal....
  Diferenciar do imoral
- El Salvador
- Banco do Brasil, Itaú,...
- Banking the unbanked: why emerging markets dominate crypto adoption
- The new wave of crypto users: migrant workers
- Julian Assange recebe doações em BTC
- CPF na farmácia...OK para voces?

- Mineradores
- Pool
- BIP
- Atualização do Protocolo (voto?)

Exchanges

- Como obter Bitcoin? Ether? LiteCoin?
- Voce pode minerar...
- Exchanges...Casa de Câmbio e Bolsa de criptomoedas
  Pix, transaferência, cartão de crédito(?)
- Muitas
- Muitos golpes, acidentes de percurso
  MtGoX/US$480 milhoes
- Muitas taxas!!!
- KYC e AML

Exchanges

- Binance
- Mercado Bitcoin
- Foxbit
- Coinbase
- (não é um endosso **cuidado!!!**)
- Em geral elas são **donas** das suas criptomoedas!!!

Exchanges

- Funcionam usando “Order Book”
- (Bolsa de Valores.. igual aos filmes)

LIVRO DE OFERTAS

Preço (R$)	Quantidade (BTC)	Total (BTC)
28.673,69	62.124	3.591.924
28.673,69	9.622	4.416.095
28.673,69	69.742	3.353.912
28.674,69	1.051	3.187.766
28.673,69	139.350	3.117.970
28.673,69	168.021	2.909.929
28.673,69	10.213	2.602.552
28.673,69	512	2.591.924
28.673,69	62.124	3.591.924
28.673,69	259.622	4.416.095
28.673,69	69.742	3.353.912
28.673,69	201.051	3.187.766
28.673,69	139.350	3.117.970
28.673,69	168.021	2.909.929
28.673,69	10.213	2.602.552
28.673,69	1.912	2.591.924

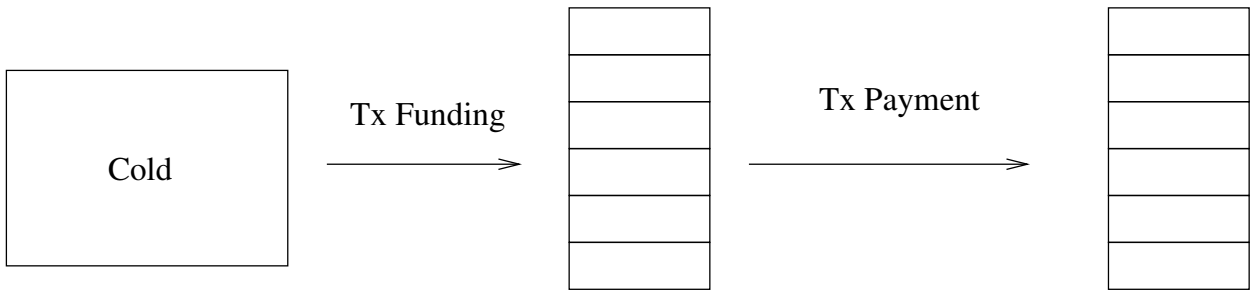
28.431,69

Spread 163,48 (0,57%)

28.510,21	1.296.163	1.296.163
28.510,21	20.110	1.316.275
28.510,21	9.919	1.325.464
28.509,21	24.742	1.350.206
28.509,21	78.532	1.428.671
28.509,21	207.422	1.636.902
28.508,21	129.546	1.751.431
28.507,21	419.905	2.184.544
28.507,21	78.532	1.428.671
28.507,21	207.422	1.636.902
28.506,21	129.546	1.751.431
28.506,21	419.905	2.184.544
28.506,21	78.532	1.428.671
28.506,21	207.422	1.636.902
28.506,21	129.546	1.751.431

- Custodia dos bitcoins dos clientes...
- As exchanges cuidam dos seus bitcoins
  Será?
- A SK fica sob controle da exchange
  importar e exportar
- Quando vc recebe bitcoin...
- A exchange transfere para uma carteira **cold**
  Papel, hardware, multisig,...
- Os endereços de clientes tem saldo zero a maior parte do tempo

- E quando vc for gastar??


Cold
Tx Funding
Tx Payment

- É um padrão “fácil”
- Tx de 1 para N
- Logo em seguida...
- Tx de N para N
  (quase) do mesmo valor
  (quase) com os mesmos endereços....
  (Taxa e troco)
- Voce identificou(?) uma carteira cold e um conjunto de clientes
  Transitividade!!

- Utilizando esta heuristica é possivel detectar as carteiras cold de exchanges
- As carteiras de clientes de exchanges
- On Detecting Cold Storage Transactions on Bitcoin's Blockchain
- (IC/TCC)

ATM

- Máquinas de Lavar Dinheiro
- https://coinatmradar.com
- https://coinmap.org/

Mercados

- Podem ser menos regulados que Exchanges
- Também podem ser usados para lavagem
- DarkNet Marketplace (DNM)
- Armas, drogas, senhas, malwares,....
- Procon(?)
  Custódia/Reputação

Mixers

- Lavagem de dinheiro
- Como?
  Aguardem....
- Em geral são ilegais

Apostas

- Podem ser ilegais
- Sem fronteiras
- Também são usados para lavar

Outros...

- Ransomware
- Chantagens Sextorcion
- Esquemas Financeiros
- Financiamento de terrorismo

- Cada um destes é uma atividade ilegal....
- Cada um deles é uma oportunidade de estudo/desenvolvimento
- Chainalisys
- Elliptic
- TRM Labs
- Arkham Intelligence
- WalletExplorer
- ChainAbuse

Transações

As transações

- Conjunto de entrada UTxO
- Conjunto de Saída
  Quem recebe quanto, troco e taxa
- **Assinatura**

H1

- O cenário mais provável é que a mesma pessoa controle todos os endereços da **entrada**
- Heuristica Um
- H1
- Ferramenta de análise mais importante!
- Produz clusters
- Cada cluster representa uma entidade

Algorithm 1 Clusterização usando H1

Input $TX.inputs$: Lista de endereços de entradas de uma lista de transações
$Clusters \leftarrow \emptyset$
for $enderecos \in Tx.inputs$ **do**
  for $c \in Clusters$ **do**
    if $enderecos \cap c \neq \emptyset$ **then**
      $enderecos \leftarrow enderecos \cup c$
      Remove c de $Clusters$
    end if
  end for
  Insere $enderecos$ em $Clusters$
end for
return $Clusters$

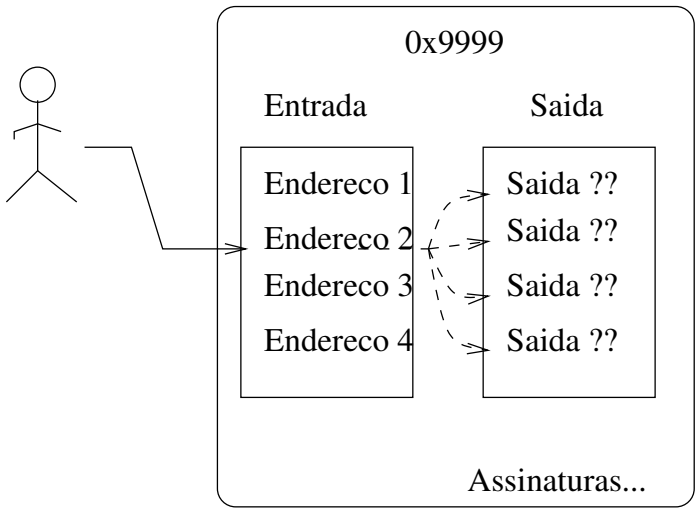
H2/Troco

O endereço de troco deve ser controlado pela mesma entidade da entrada. O endereço *trc* deve ser o endereço de troco de Tx se:

- A transação Tx não deve ser uma transação do tipo Coinbase;
- É a primeira aparição de *trc*;
- *trc* é o único endereço de primeira aparição;
- O valor pago para *trc* é menor que a menor UTxO

CoinJoin

- n pessoas....
- Transações do mesmo valor



CoinJoin

- Isso é o que um mixer faz!
- Ilegal (em diversos países)
- transação 1 e transação 2.

CoinJoin

- O CoinJoin apaga as pegadas...
- O CoinJoin invalida o H1
- (Exchanges também!!)