Ivan Sendir

#### Aula passad

Ecossistem:

Exchang

ΔΤΜε

7111113

iviercado:

Mixers

Н1

H2

CoinJoin

## Analise de Blockchain

### Ivan Sendin

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

13 de agosto de 2024

van Sendin

#### Aula passad

#### Ecossistem:

Mineradores Exchanges ATMs Mercados Mixers

Apostas

H1

112

\_oinJoir

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

## Aula Passada

#### Bitcoin

van Sendin

#### Aula passada

#### Ecossistem

Exchanges ATMs Mercados

Mixers

portunistas Diversos

H1

...2

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

Ivan Sendin

### Aula passada

Ecossistem:

LCOSSISCEIII

Excha

ATMs

Mercad

Mivers

.

Oportunistas Dive

H1

HZ

-oin Join

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

#### Ecossistema

- 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

lvan Sendir

#### Aula passad

#### Ecossistema

Mineradores

ATMs

ATIVIS

Mercado

Mixers

Oportunistas Diver

H

П

ZoinJoii

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

Ivan Sendir

Aula passada

#### Ecossistema

Exchanges ATMs Mercados Mixers

Apostas

H1

### 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?

Ivan Sendin

#### Aula passad

#### Ecossistem

#### Mineradores

Exchanges

ATMs

. .

Mercac

Mixers

Apostas

Н1

112

\_oinJoir

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

## **Exchanges**

#### Bitcoin

van Sendin

Aula passad

**Ecossistem** 

Mineradores

Exchange:

Mercados

Mixers

Apostas

Н1

H2

- 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**

#### Bitcoin

lvan Sendir

#### Aula passad

Ecossistem

#### ...

.....

ATMs

Mercado

iviercade

wiixers

On any order of Division

H

H2

CoinJoir

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

# Exchanges

#### Bitcoin

lvan Sandin

#### Aula passad

Ecossistema

### Mineradores

Exchanges

ATMs

Mercad

8.45

wiixers

Oportunistas Diver

H1

H2

CoinJoir

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

Aula passad

F .........

...

ΔΤΜε

wiixers

A ----

Opertunistas Divor

H1

H2

Coin Joir

#### LIVRO DE OFERTAS Preço (R\$) Quantidade (BTC) Total (BTC) 28.673,69 62.124 9.622 28.673.69 69.742 3.353.912 28.674.69 1,051 3,187,766 28.673,69 139.350 28.673,69 168.021 2.909.929 10.213 512 62.124 3.591.924 28.673,69 259.622 4.416.095 28.673,69 69.742 28.673,69 201.051 3.187.766 28.673,69 139.350 2.909.929 28.673,69 168.021 10.213 28.673,69 28.673,69 1.912 2.591.924

#### 28.431,69 Spread 163.48 (0.57%)

1.296.163 1.296.163 28.510.21 20.110 9.919 1.325.464 24,742 78.532 1.428.671 207.422 1.636.902 129.546 419.905 2.184.544 1.428.671 78.532 207.422 1.636.902 28.506,21 129,546 1.751.431 419.905 2.184.544 78.532 1.428.671 207.422 1.636.902

129.546

#### lvan Sendir

Aula passad

Mineradores

Exchanges

ATMs

Mercados

Oportunistas Diver

H1

c . . .

- 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

lvan Sendin

Aula passada

Ecossistema

\_\_\_\_\_

Willieradores

Exchanges

ATMs

Mercados

Mixers

H2

LoinJoin

• E quando vc for gastar??

lvan Sendin

#### Aula passada

#### Ecossistema

#### Iviineradores

#### Exchanges

#### AT14

Mercados

Mixers

.

Oportunistas Diver

H1

H2



van Sendin

Aula passad

**Ecossistem** 

...

Exchanges

.....

Mercado

Mixers

Oportunistas Divers

H:

H2

- 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!!

Ivan Sendir

#### Aula passad

Ecossistema Mineradores Exchanges

ATMs Mercados

Apostas

Oportunistas Diverso

110

Coin Joi

- 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**

#### Bitcoin

van Sendin

#### Aula passad

#### Ecossistem:

#### Ecossisteiii

Exchar

ATMs

Mercad

. . .

IVIIXers

Oportunistas Diversos

H1

H2

-oin Joii

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

## Mercados

#### Bitcoin

lvan Sendin

#### Aula passad

Ecossistem:

Exchar

#### Mercados

Mixers

Oportunistas Diversos

H1

ПΖ

CoinJoir

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

## Mixers

#### Bitcoin

lvan Sandir

#### Aula passad

#### Ecossistem

Mineradores

Exchar

ATIVIS

Mercados

Mixers

Apostas

H1

H2

oin Joir.

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

# **Apostas**

#### Bitcoin

lvan Sendir

#### Aula passad

#### Ecossistem

Mineradores

ATMs

Mercados

Mixers

) Dortunistas Diversos

HI

112

-oin Joii

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

## Outros...

#### Bitcoin

lvan Sendi

#### Aula passad

#### Ecossistem

Mineradores

Exchan,

ATMs

Merca

Mixer

Oportunistas Diversos

H1

H2

oinJoir

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

lvan Sendir

Aula passad

Ecossistem

Mineradores Exchanges

ATMs Mercados

Mixers

Oportunistas Diversos

H1

H2

oinJoii

- 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

#### Bitcoin

van Sendin

#### Aula passad

#### Ecossistem

Exchanges ATMs Mercados

Apostas

-----

⊔າ

CoinJoii

### As transações

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

Ivan Sendir

#### Aula passad

Ecossistem:

Exchanges ATMs Mercados

Mercados Mixers

ortunistas Diverso

. . .

 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

Ivan Sendin

Aula passad

Ecossistem

Mineradores

Exchange

ATMs Moreados

Mixers

Oportunistas Diversos

H1

ПΖ

CoinJoin

## **Algorithm 1** Clusterização usando H1

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



# H2/Troco

#### Bitcoin

Ivan Sendir

Aula passac

Ecossistem
Mineradores

ATMs Mercados Mixers

Apostas Oportunistas Diverso

Н2

CoinJoi

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

#### Bitcoin

van Sendin

#### Aula passad

#### Ecossistem:

LCOSSISTEIII

Exchan

ATMs

7111113

Mercado

Mixers

Apostas

Oportunistas Divi

1111

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

lvan Sendir

#### Aula passad

#### Ecossistem:

Mineradores

ATMs

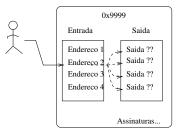
Mercado

Mixers

Apostas

Н1

H2



## **CoinJoin**

#### Bitcoin

van Sendir

#### Aula passad

#### Ecossistem

Mineradores

ATMs

Mercados

Miyers

Apostas

Н1

H2

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

## **CoinJoin**

#### Bitcoin

van Sendin

#### Aula passad

#### Ecossistem:

Mineradores

Exchange ATMs

Mercados

Mercado:

Apostas

Н1

H2

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