

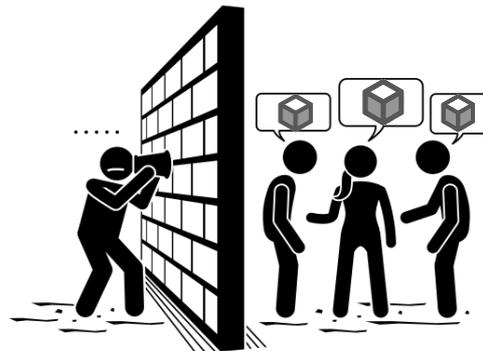
Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype: Privacidade em transações

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Objetivos

- Algumas considerações sobre (quebra de) privacidade em blockchains
 - Ferramentas/técnicas para aumentar a privacidade das transações
- Foco: cenário de criptomoedas
 - Mas técnicas discutidas se aplicam a outros contextos, mesmo sem uso de blockchains



Privacidade em Criptomoedas

- O que se pode querer esconder?



- Identidades (anonimato)

- Quem é o usuário real (pessoa física/jurídica)
- Para quem é o valor, e de onde ele veio



- Quantias (e.g., salários)

- Quanto está sendo pago
- Quanto está sendo recebido



- Metadados

- Lógica de contratos inteligentes

Privacidade em Criptomoedas

- E por que esconder essas informações?

- Mesmos princípios do sigilo bancário!

- Empresas:

- Esconder compras realizadas (informação estratégica)
 - Esconder custos/margens de lucros e lista de fornecedores
 - Esconder salários de funcionários



- Pessoas físicas:

- Esconder salário, movimentações financeiras, itens adquiridos, doações realizadas: muitas vezes, questão de segurança



- Criminosos:

- Valores resultantes de roubo, fraude, venda de produtos ilegais
 - Sonegação de imposto e lavagem de dinheiro



Graus de anonimato

- Anonimato fraco (pseudonimato):

- Um só identificador (pseudônimo) no sistema
- Prós: permite criar sistema de reputação
- Contras: perda de anonimato se qualquer evento for ligado a usuário; facilita inferências



- Anonimato forte

- Previne a ligação entre diferentes eventos, embora eles se refiram ao mesmo usuário
- Contra: dificulta mecanismos de reputação



- Pode-se criar sistema com suporte a ambos

- Ex.: anonimato fraco em relação a auditores; anonimato forte em relação a outros usuários

Privacidade em pagamentos

- Bitcoin/Ethereum



- Registros de transferências e seu conteúdo são públicos
 - Contas de origem e destino; valores
- Pseudonimato apenas
- Exchanges: identidades conhecidas

- Operadores tradicionais: bancos/cartões



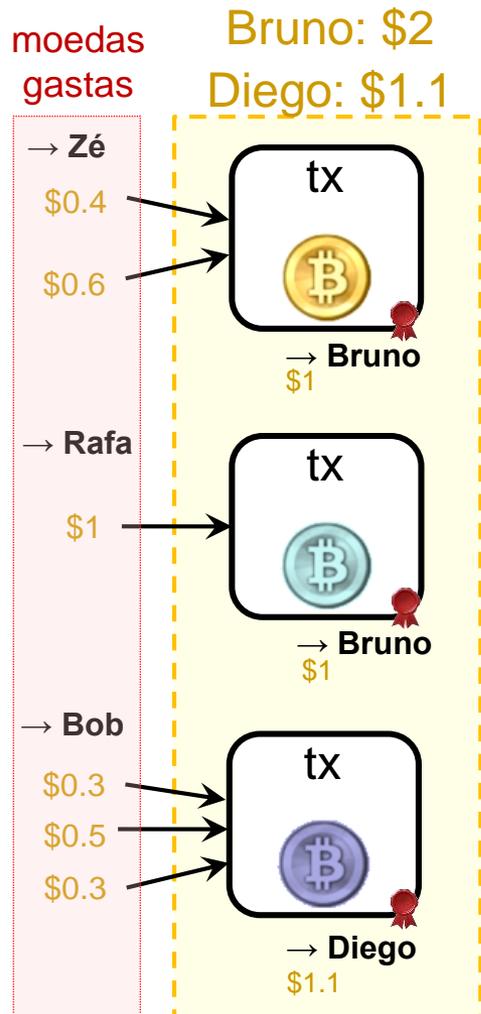
- Registros de transferências são privados
 - Contas e valores conhecidos só por origem, destino e operador
- Identidades conhecidas por operador

- Zcash/Monero



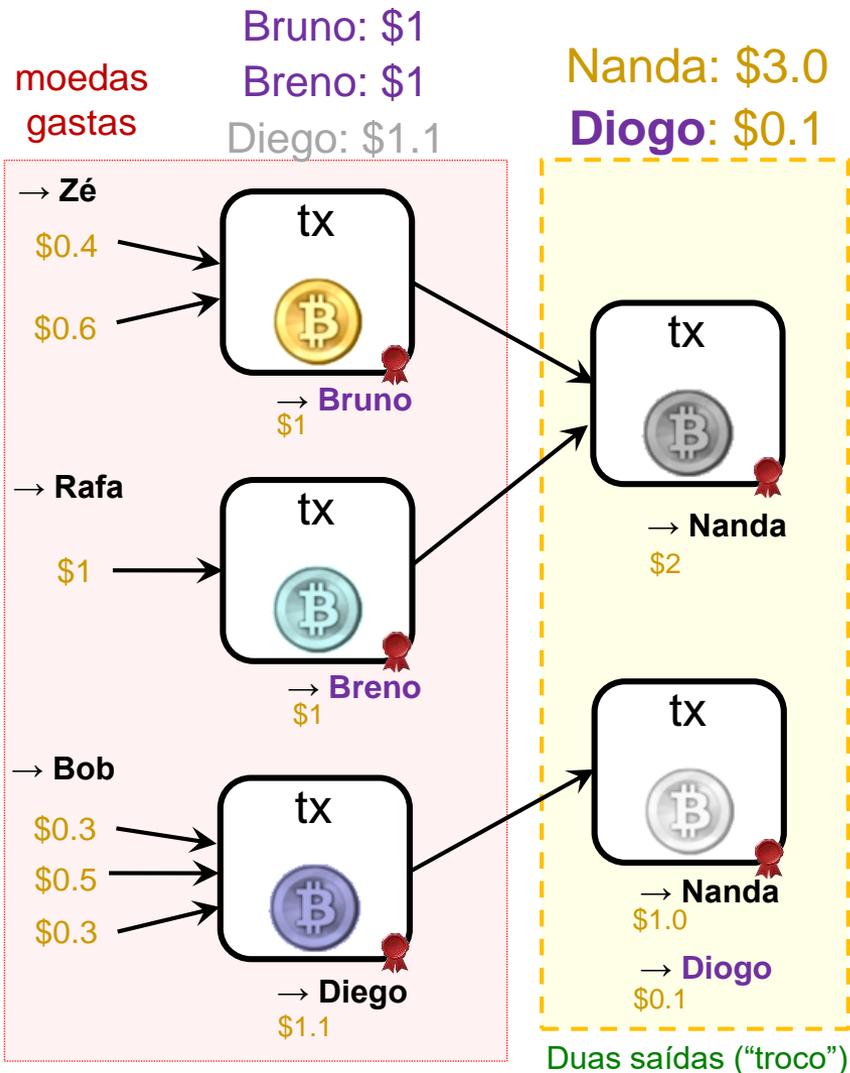
- Registros de transferências públicos, mas conteúdo privado
 - Contas de origem e destino; valores

Privacidade (?) no Bitcoin



- Identificador de conta: hash de chave pública
 - Chaves são geradas pelos próprios usuários
 - Sequência de bits sem qualquer relação óbvia com identidade real do seu dono: são **pseudônimos**
 - Ex. (Base58):
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

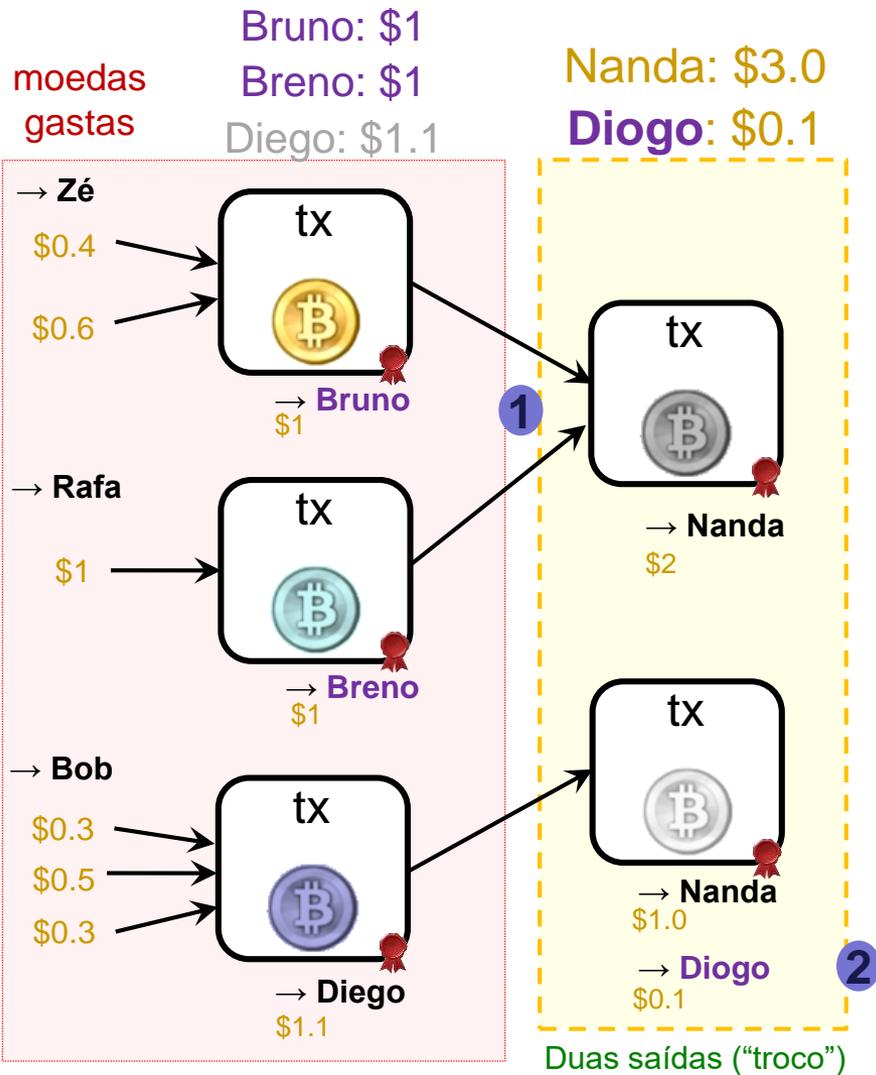
Privacidade (?) no Bitcoin



- Rede aberta: algum grau de privacidade se
 - Usar **identificadores distintos** para cada transação
 - **Ocultar endereço IP** fazendo transação (ex.: Tor)
 - **Não usar intermediário** que aplique política de KYC*
 - Para trocar moedas por reais, ou para transações: Bancos e Exchanges conhecem a **identidade real** do usuário.
 - Ainda assim: **longe de perfeito...**

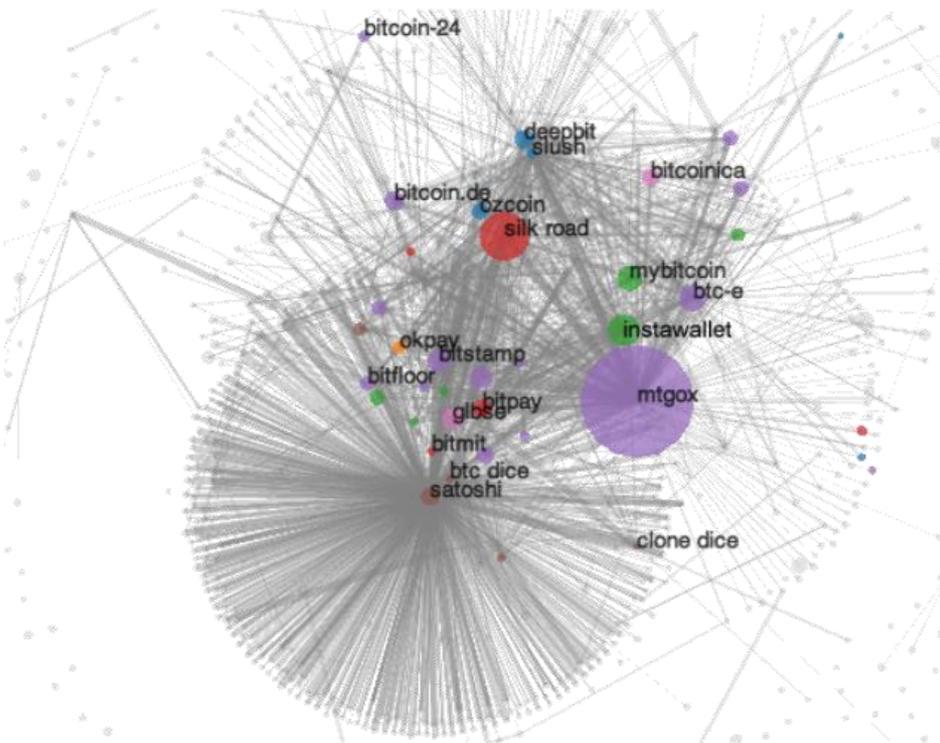
* Know Your Customer

Privacidade (?) no Bitcoin



- Algumas **heurísticas** para ligação entre pseudônimos:
 1. **Ligação entre IDs usados como entradas**: Bruno e Breno são a mesma entidade
 2. **Troco** enviado para a mesma entidade: único novo endereço, valor quebrado, menor que entradas

Privacidade (?) no Bitcoin

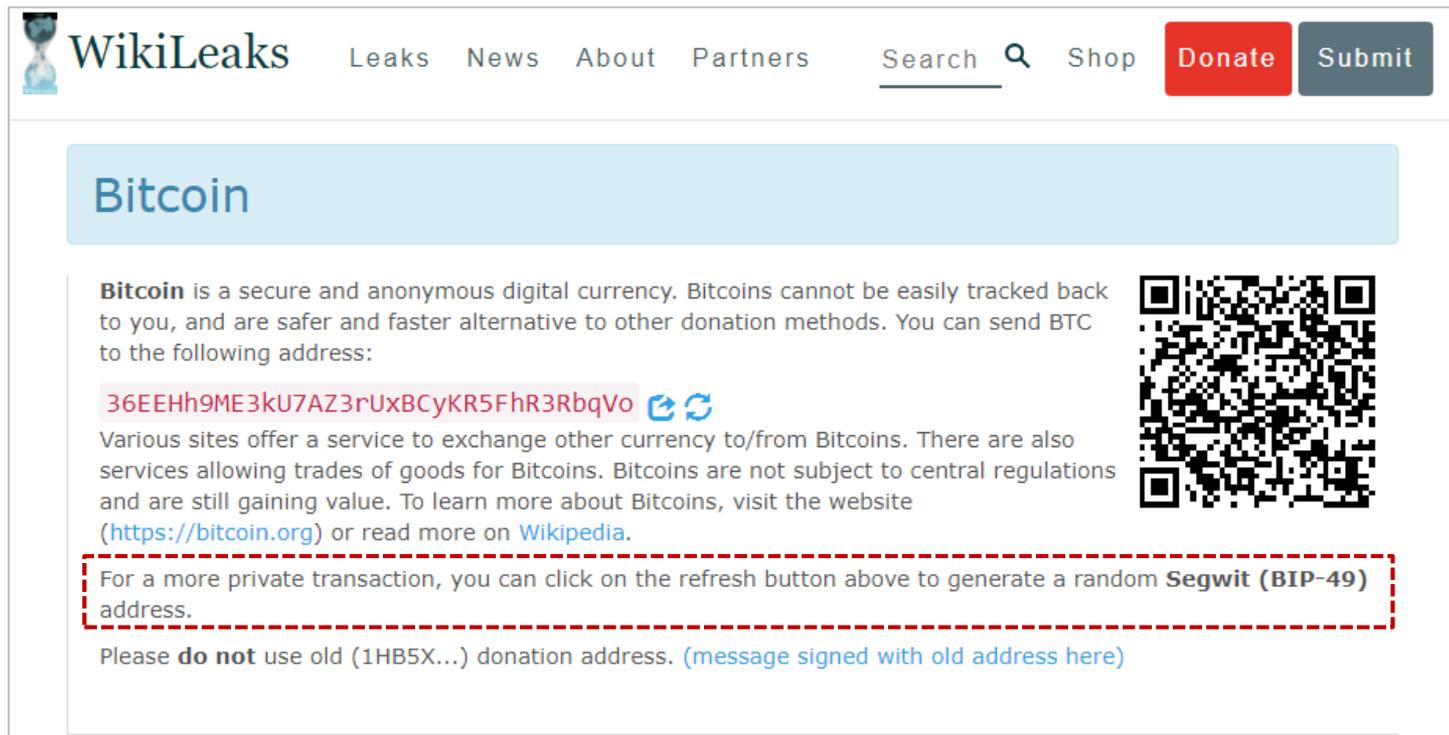


<http://dx.doi.org/10.1145/2504730.2504747>

- Algumas **heurísticas** para ligação entre pseudônimos:
 1. **Ligação entre IDs usados como entradas**: Bruno e Breno são a mesma entidade
 2. **Troco** enviado para a mesma entidade: único novo endereço, valor quebrado, menor que entradas
- Ex. (2013): 3.3M conjuntos
 - 2200 deles deanonimizados
 - 15% do valor total da rede
 - Interação com mercadores (Coinbase, Bitpay, ...) auxiliou identificação

Privacidade (?) no Bitcoin

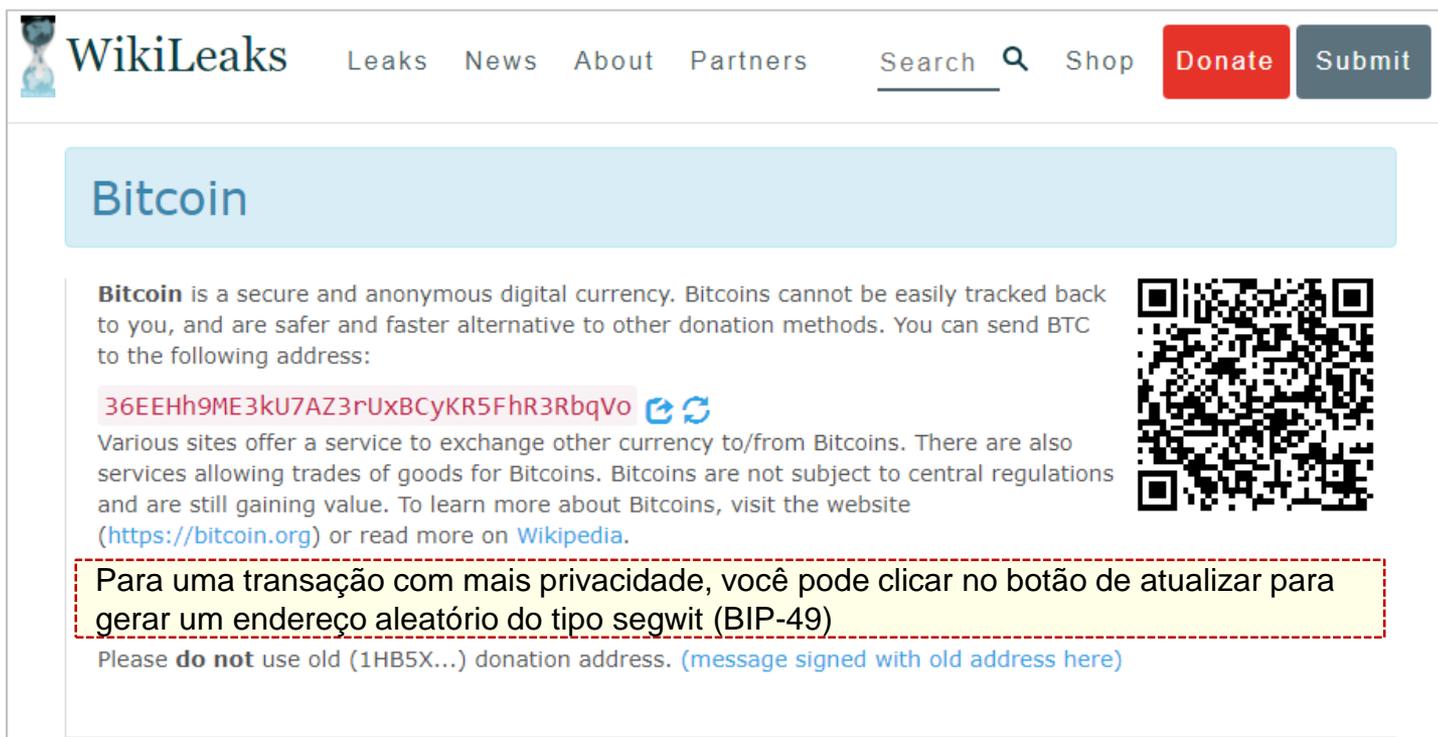
- Ex.: site “visados”, como Wikileaks
 - Antigamente, tinha endereço único: facilitava rastreamento de doadores. Atualmente:



The screenshot shows the WikiLeaks website's Bitcoin donation page. At the top, there is a navigation bar with the WikiLeaks logo, links for 'Leaks', 'News', 'About', and 'Partners', a search bar, and buttons for 'Shop', 'Donate', and 'Submit'. The main content area has a light blue header with the word 'Bitcoin'. Below this, a paragraph explains that Bitcoin is a secure and anonymous digital currency and provides a unique donation address: `36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo`. To the right of this address is a QR code. Below the address, there are two refresh icons. A paragraph follows, mentioning exchange services and the Bitcoin website (<https://bitcoin.org>). A red dashed box highlights a note: 'For a more private transaction, you can click on the refresh button above to generate a random Segwit (BIP-49) address.' At the bottom, a warning states: 'Please do not use old (1HB5X...) donation address. (message signed with old address here)'.

Privacidade (?) no Bitcoin

- Ex.: site “visados”, como Wikileaks
 - Antigamente, tinha endereço único: facilitava rastreamento de doadores. Atualmente:



The screenshot shows the WikiLeaks website's Bitcoin donation page. At the top, there is a navigation bar with the WikiLeaks logo, links for 'Leaks', 'News', 'About', and 'Partners', a search bar, and buttons for 'Shop', 'Donate', and 'Submit'. The main content area features a light blue header with the word 'Bitcoin'. Below this, a paragraph explains that Bitcoin is a secure and anonymous digital currency and provides a unique donation address: `36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo`. To the right of the address is a QR code. Further down, text mentions that various sites offer exchange services and that Bitcoin is not subject to central regulations. A yellow box with a red dashed border highlights a note: 'Para uma transação com mais privacidade, você pode clicar no botão de atualizar para gerar um endereço aleatório do tipo segwit (BIP-49)'. Below this, a warning states: 'Please do not use old (1HB5X...) donation address. (message signed with old address here)'.

Privacidade (?) no Bitcoin

- Empresas especializadas em rastrear transações em blockchains:
 - Chainalysis, Mastercard/CipherTrace, Elliptic, ...



Crypto money laundering rises 30%, report finds

© 26 January



<https://www.bbc.com/news/technology-60072195>



Brasileiros estão entre os que mais lucraram com criptomoedas em 2021, revela Chainalysis

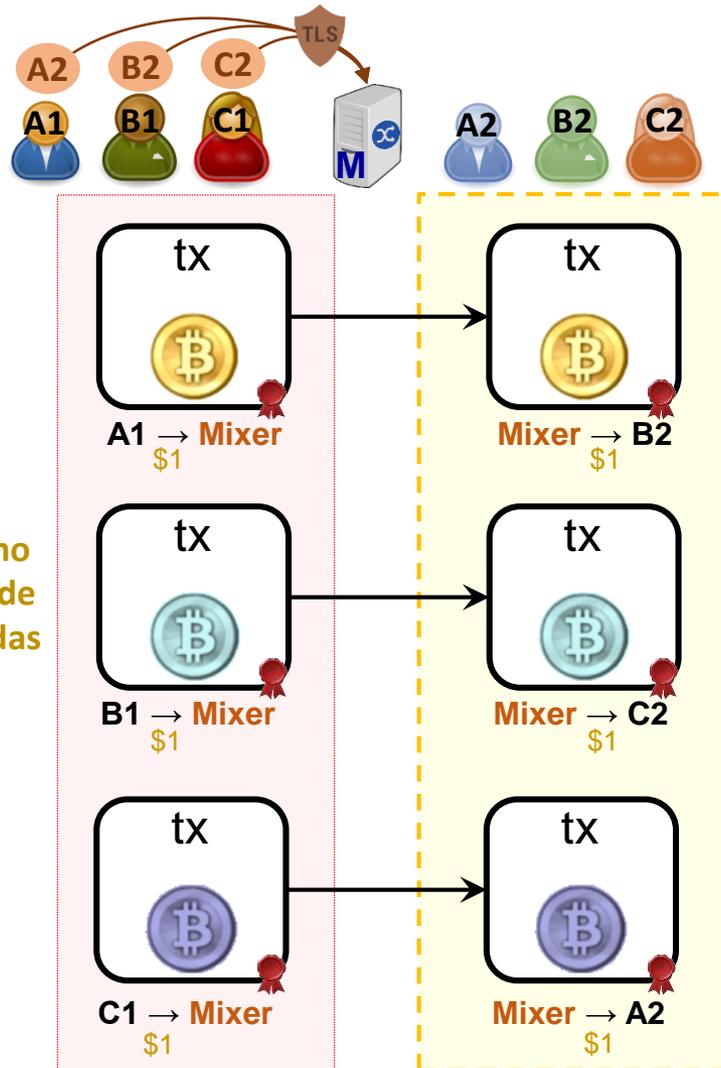
CRIPTOFACIL | Cripto | 6 horas atrás (22.04.2022 08:13)



© Reuters Brasileiros estão entre os que mais lucraram com criptomoedas em 2021, revela Chainalysis

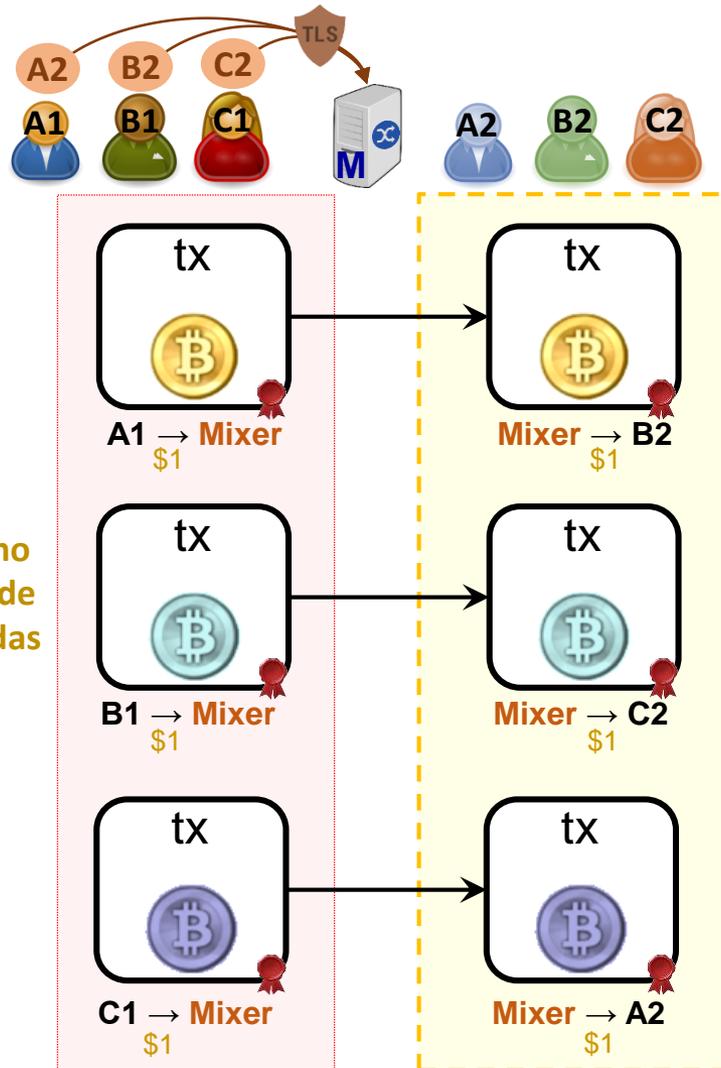
<https://br.investing.com/news/cryptocurrency-news/brasileiros-estao-entre-os-que-mais-lucraram-com-criptomoedas-em-2021-revela-chainalysis-992833>

Técnicas de privacidade: Mixing



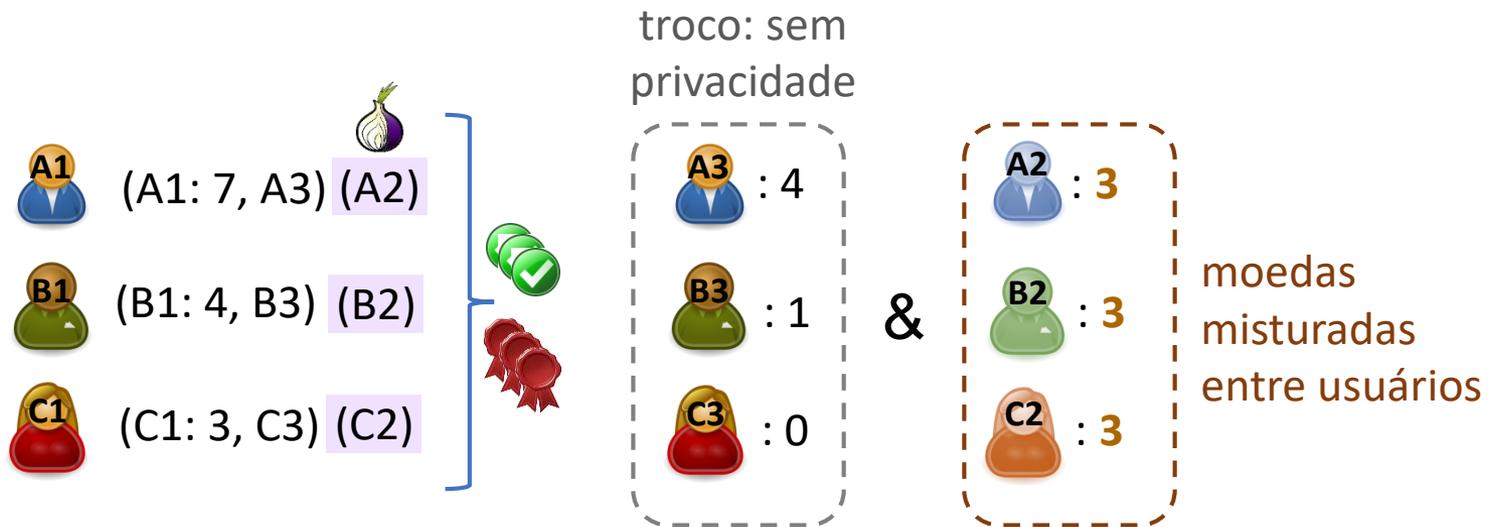
- Moedas misturadas entre usuários:
 - Quebra-se vínculo 1:1 entre (A1, B1, C1) e (A2, B2, C2)
 - Efeito: dificulta rastreamento de valores
 - Nota: “lavar dinheiro sujo” ou “sujar dinheiro limpo”?

Técnicas de privacidade: Mixing



- Moedas misturadas entre usuários:
 - Quebra-se vínculo 1:1 entre (A1, B1, C1) e (A2, B2, C2)
 - Efeito: dificulta rastreamento de valores
 - Nota: “lavar dinheiro sujo” ou “sujar dinheiro limpo”?
- **Problemas: Mixer M** pode
 - Deanonimizar usuários
 - Cobrar taxas
 - **Roubar fundos!**

Técnicas de privacidade: Mixing



- **Mixing sem mixer:** CoinJoin, Tornado Cash, ...
 - Assinatura de todos os usuários (multisig)
 - Saída: mínimo entre valores de entrada

Técnicas de privacidade: Mixing



- **Mixing sem mixer:** CoinJoin, Tornado Cash, ...
- **Problemas:**
 - Requer interação entre usuários
 - Se um usuário no grupo gastar moedas: mixing invalidado para o grupo todo
 - Quantias transferidas permanecem públicas

Criptomoedas com privacidade: endereços de origem ocultos



- Ex. (**CriptoNote**): assinaturas em anel
- Anel: um grupo de a usuários
 - Cada usuário i ($1 \leq i \leq a$): chave pública u_i e privada r_i
- Assinatura s_i calculada usando r_i não pode ser vinculada ao usuário i
 - Verificada com o conjunto de chaves públicas $\{u_i\}$: pode ter sido gerada por qualquer usuário do anel!
 - Quanto maior o anel, mais privacidade
 - Anel é definido pelo signatário i : não requer interação prévia com outros usuários
 - É possível ligar 2 assinaturas s_i e s'_i feitas c/ a mesma chave r_i : detecção de tentativa de gasto duplo

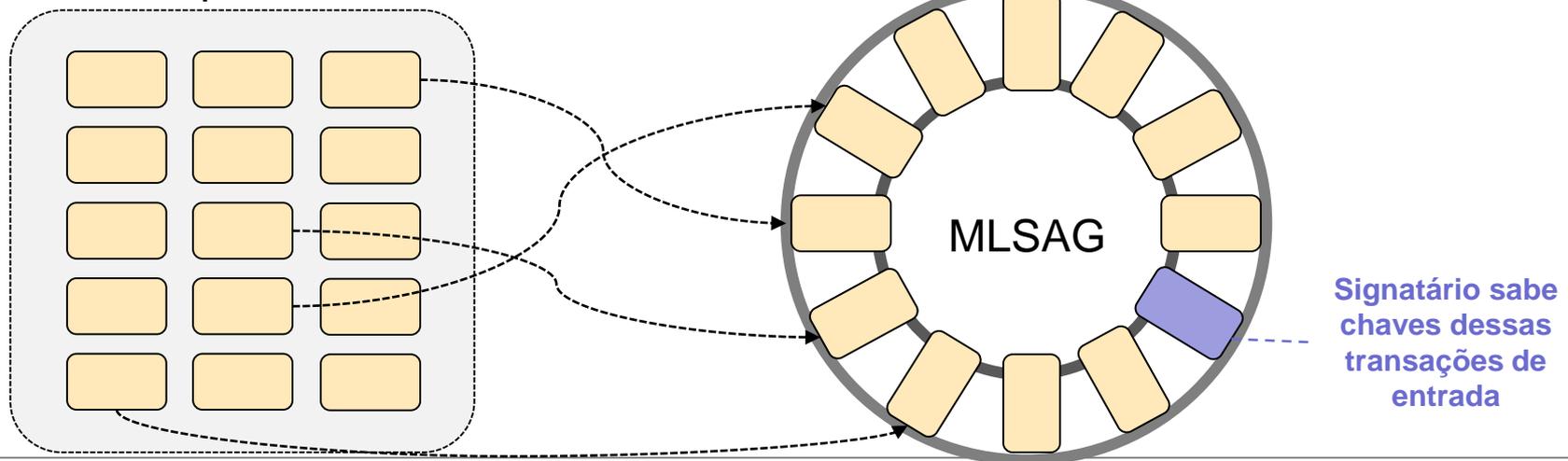


Criptomoedas com privacidade: endereços de origem ocultos

- **Monero**, desde Jul/2022: anel com $a \geq 16$
 - Baseado no protocolo CriptoNote
 - Endereços de usuários são fixos, mas vínculo com transações realizadas é ofuscado pelo anel

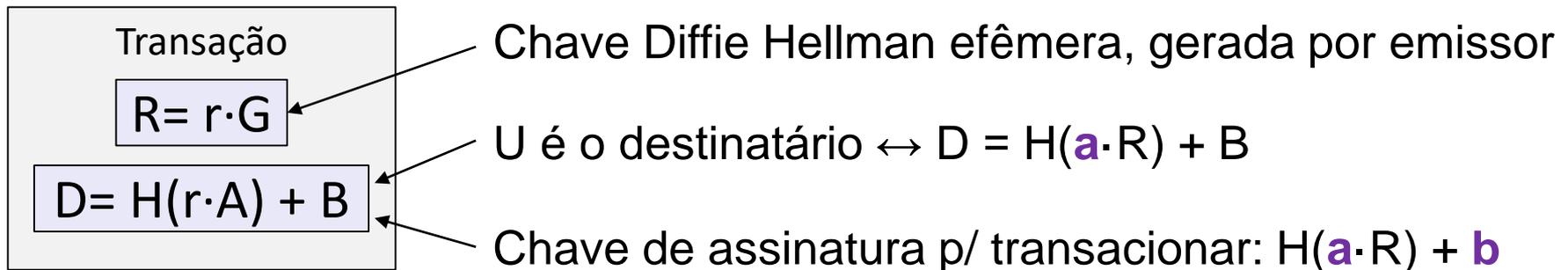
Seleciona $a-1$ transações passadas como “iscas”: seus signatários tornam-se parte do anel

Assinatura em anel com a signatários: 1 **real** + $a-1$ “iscas”



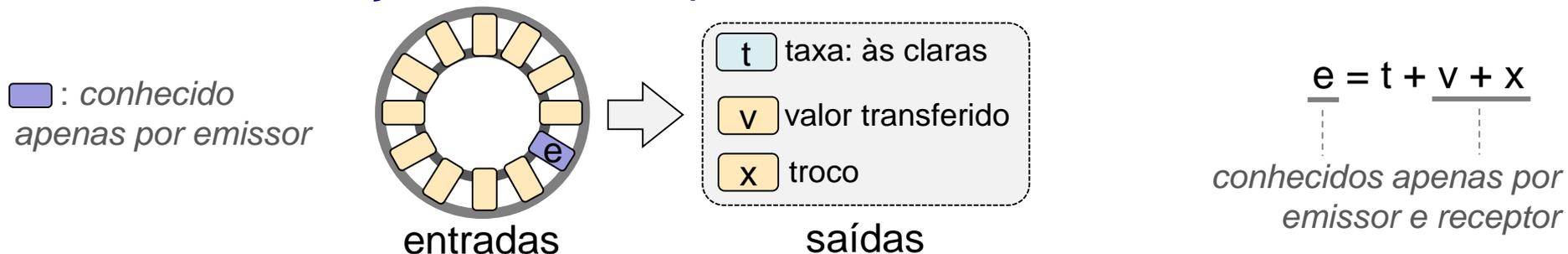
Criptomoedas com privacidade: endereços de destino ocultos

- **Ex. (Monero):** endereços “furtivos” (*stealth*)
 - Cada usuário U tem 2 pares de chaves privada/pública:
 - De visualização: $(a, A = a \cdot G)$
 - De transação: $(b, B = b \cdot G)$ } *dual-key stealth address protocol (DKSAP)*
 - Posse de a permite saber se uma transação registrada no Monero é destinada a U (e também seu valor)
 - Posse de (a,b) permite gastar valores recebidos em transações destinadas a U



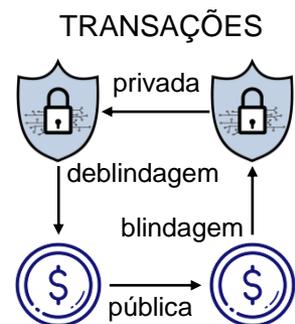
Criptomoedas com privacidade: valores ocultos

- **Ex. (Monero):** valores visíveis apenas com posse de chave de visualização
 - **Pedersen Commitments:** esconde valor de cada entrada na transação, mas permite operações aritméticas de soma/subtração entre esses valores (*homomorfismo*)
 - Ring Confidential Transactions (**RingCT**): permite provar que uma entrada foi “consumida” com a chave de transação correspondente, sem revelar qual entrada
 - **Bulletproofs:** permite verificar que cada entrada na transação é um valor positivo dentro de certa faixa



Criptomoedas com privacidade

- Ex. (**ZCash**): zk-SNARKs
 - **Z**ero-**K**nowledge **S**uccinct **N**on-Interactive **A**RGuments of **K**nowledge: **ocultam emissor, receptor e valores**
 - Assumindo o uso de endereços privados (aka “blindados”)
 - Construídos como circuitos aritméticos:
 - $a+b*c \rightarrow$ operações das portas $[+]$ e $[*]$ são traduzidas para estruturas criptográficas homomórficas
 - Provas construídas em ZK para cada transação:
 - \sum (valores de entrada) = \sum (valores de saída)
 - entradas \in {saídas anteriores}
 - entradas ainda não foram gastas (números de série)
 - emissor conhece chaves privadas p/ endereços das entradas



Criptomoedas com privacidade

- Ex.: sites “visados”, como Wikileaks



Monero

Monero is an open-source cryptocurrency that focuses on privacy, decentralisation and scalability. Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNote protocol and possesses significant algorithmic differences relating to blockchain obfuscation.

Monero users may choose to donate to us at:

453VWT5GEkXGc2J9asRpXpRkjoCGKCJr96rndm2VMe5yECiAcUB3h8pFxZ8Y



To learn more about Monero, visit the official website at <https://getmonero.org> or read more on [Wikipedia](#)

Criptomoedas com privacidade

- Ex.: sites “visados”, como Wikileaks



ZCash

ZCash is a cryptocurrency that offers privacy and selective transparency of transactions. ZCash payments are published on a public blockchain, but the sender, recipient, and amount of a transaction may remain private.

ZCash users may choose to donate to us at:

`t1WLeAK9npDSRg7SAM5DMJSeYk45aCvpcdX` 



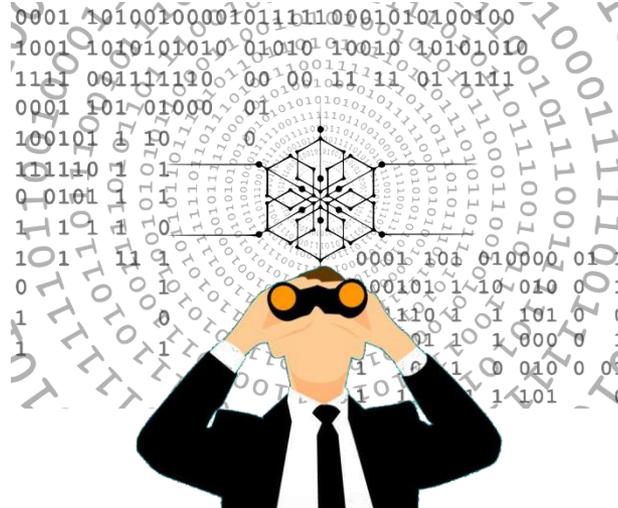
Or using private address:

`zccZa7MrxtwYY7zZ1vEph1eRDagDcN3tE67kHYadujvQbnBA4DtsMKLH6KhX`

< >



To learn more about ZCash, visit the official website at <https://z.cash> or read more on [Wikipedia](#).



Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype: Privacidade em transações

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Referências

- W. Vermaak (2021) O Que São Moedas de Privacidade?. URL: <https://coinmarketcap.com/alexandria/pt/article/what-are-privacy-coins>
- Koe, K. Alonso, S. Noether (2020) "Zero to Monero: Second Edition -- A technical guide to a private digital currency; for beginners, amateurs, and experts". Published April 4, 2020 (v2.0.0). URL: <https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf>
- Zcash Documentation (online). URL: <https://zcash.readthedocs.io/en/latest/index.html>
- Rivest, R. L., Shamir, A., & Tauman, Y. (2001, December). How to leak a secret. In International conference on the theory and application of cryptology and information security (pp. 552-565). Springer, Berlin, Heidelberg. URL: <https://people.csail.mit.edu/rivest/pubs/RST01.pdf>
- E. Fujisaki and K. Suzuki (2006) "Traceable Ring Signature". Cryptology ePrint Archive, Report 2006/389. URL: <https://ia.cr/2006/389>