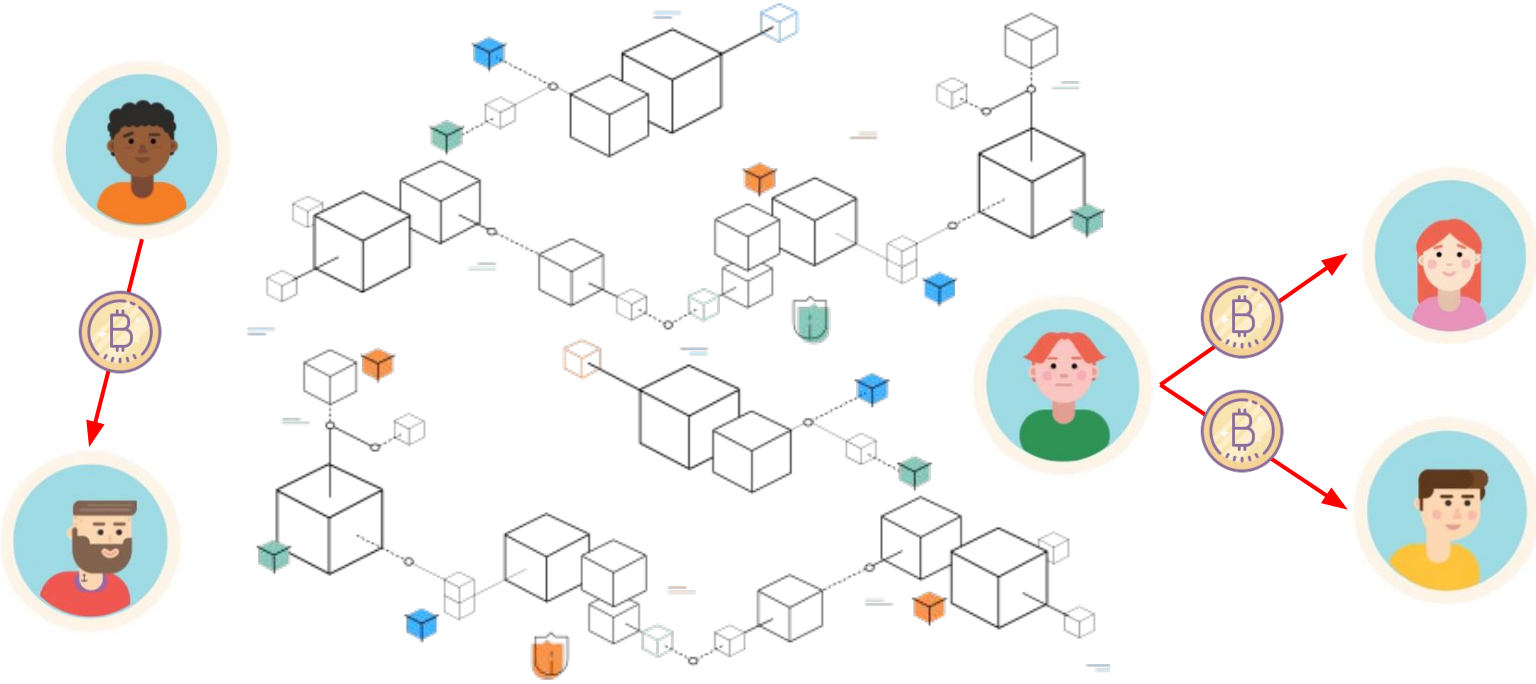
Trabalho de Conclusão de Curso II - 2018/2

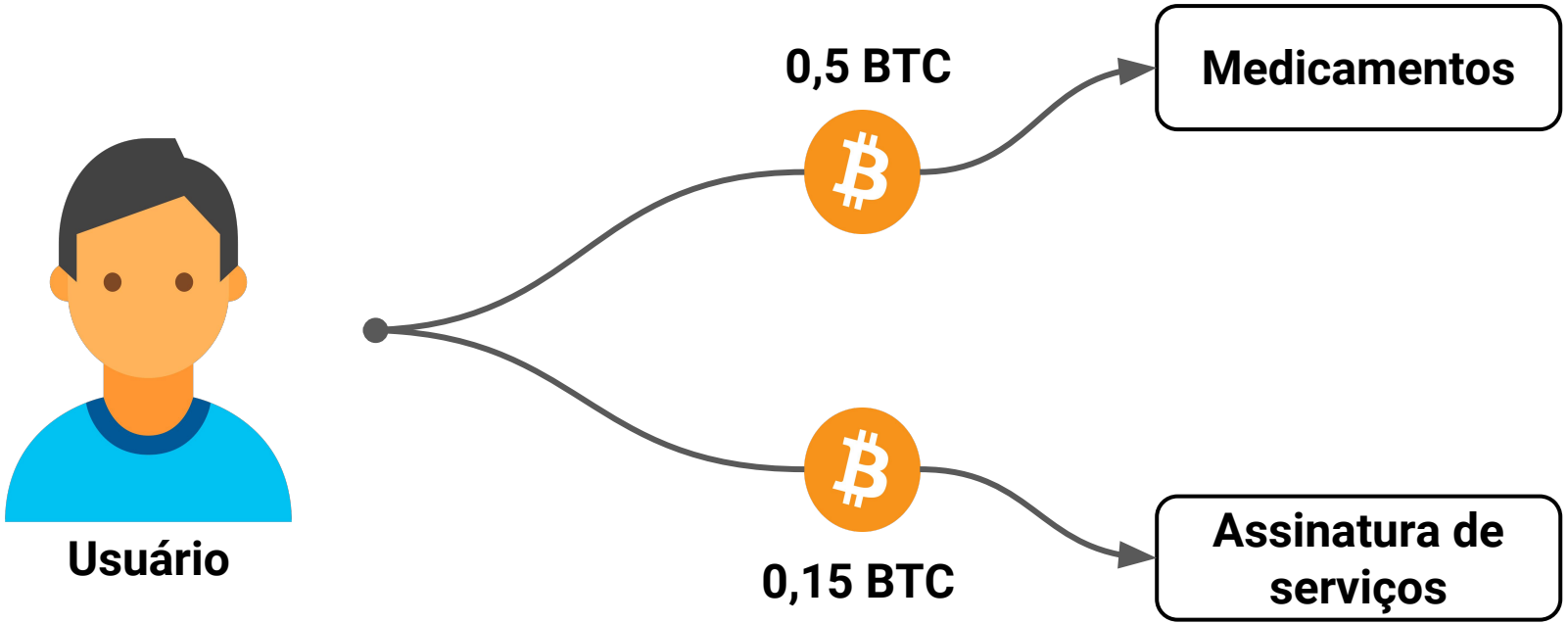
Análise da rastreabilidade das transações da criptomoeda Monero

João Otávio Massari Chervinski

Orientador: Diego Luis Kreutz

Quais são os benefícios da utilização de criptomoedas?



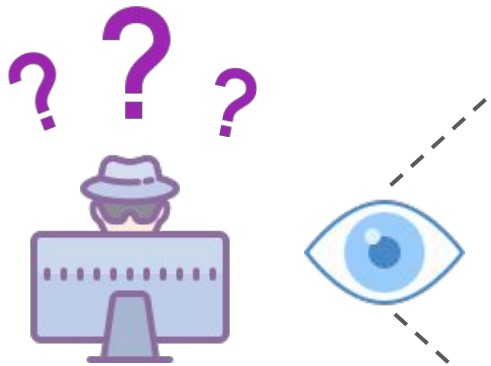


Transações visíveis

Qual a importância da existência de privacidade?

- Limita o poder de empresas sobre pessoas
- Controle sobre informações divulgadas
- Fornece liberdade política e social
- Permite mudanças e segundas chances

Existe alguma moeda digital que proteja a privacidade dos usuários?



Emissor protegido

Valor da transação oculto

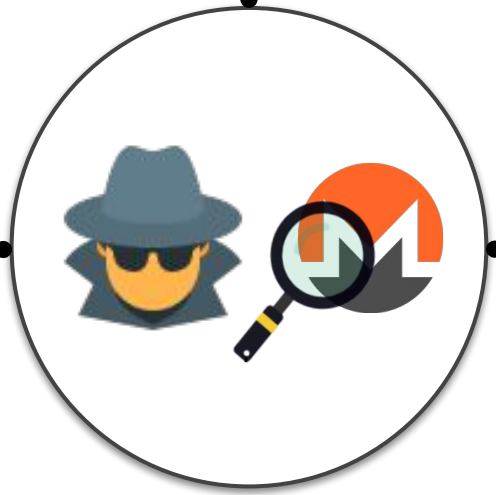
Receptor protegido

Transações privadas

Quem tem interesse em rastrear transações?

Governos

Empresas



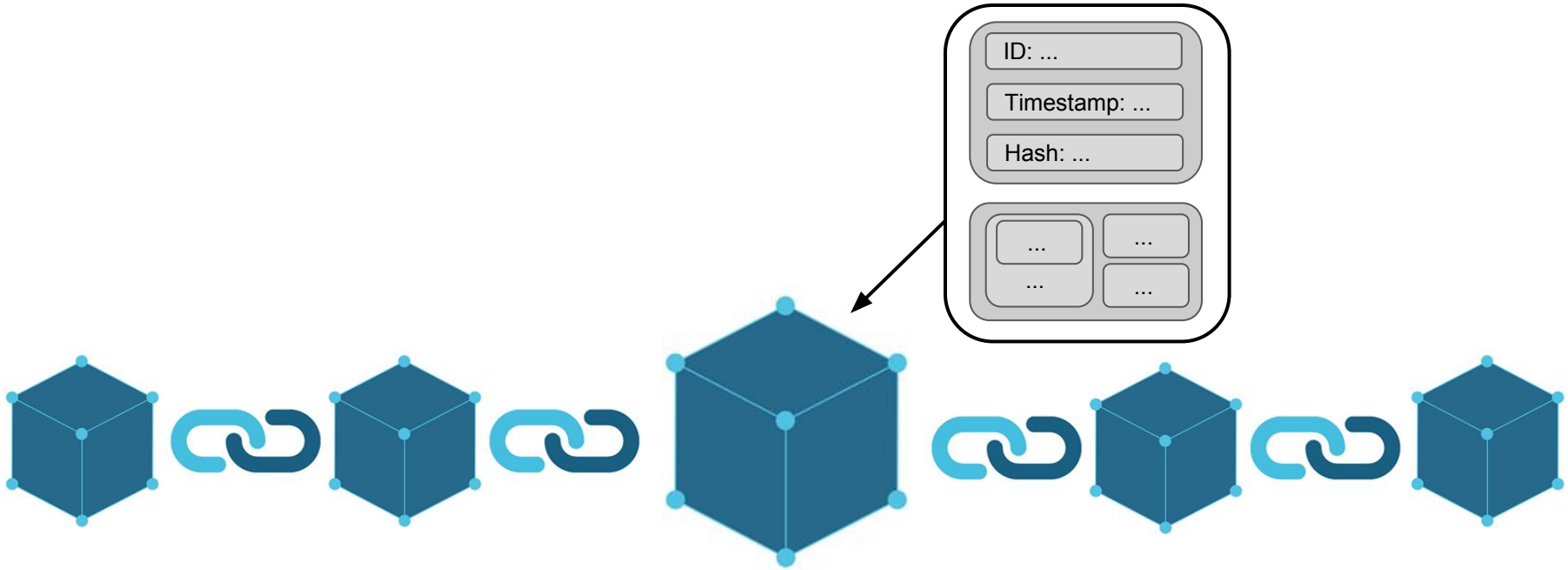
Investidores

Roteiro

- **Monero**
- Análise de rastreabilidade
- O ataque proposto
- Desafios de pesquisa
- Considerações finais

Onde os dados das transações ficam armazenados?

Blockchain


ID: ...
Timestamp: ...
Hash: ...
...
...
...
...
Bloco 100
Bloco 101
Bloco 102
Bloco 103
Bloco 104

Monero

Duas características principais de privacidade:

Irrastreabilidade das transações

Não-vinculação de endereços

Monero

Mecanismos de privacidade das transações:

- **Endereços de uso único**
- **Assinaturas em anel**
- **Transações Confidenciais**

Monero: Endereços de uso único

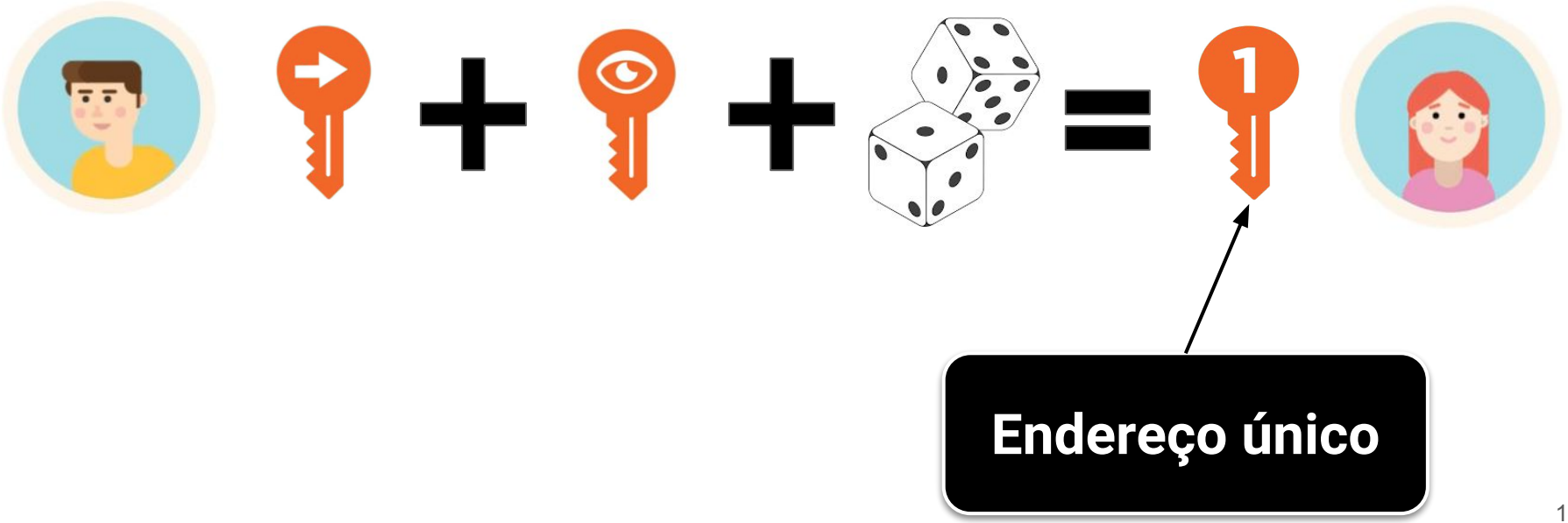
Maria

Chave pública de visualização

Chave pública de utilização de fundos

Monero: Endereços de uso único

João



Maria

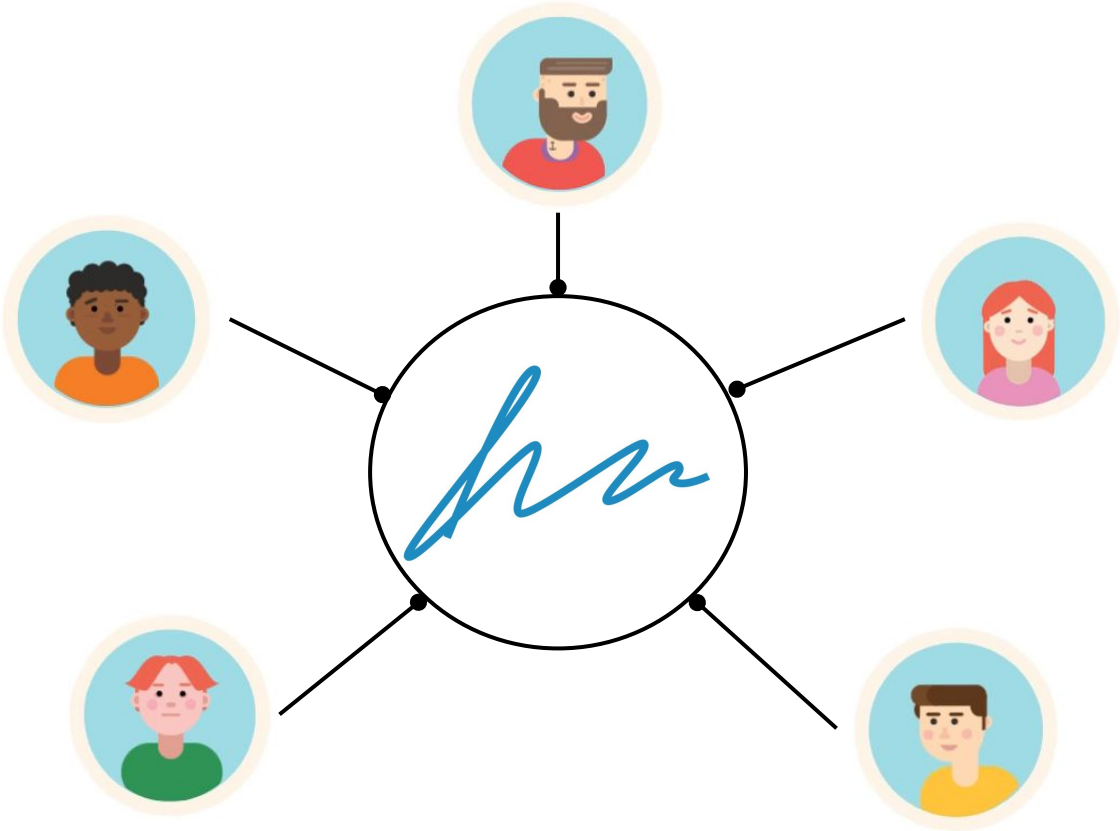
Monero: Endereços de uso único

Maria

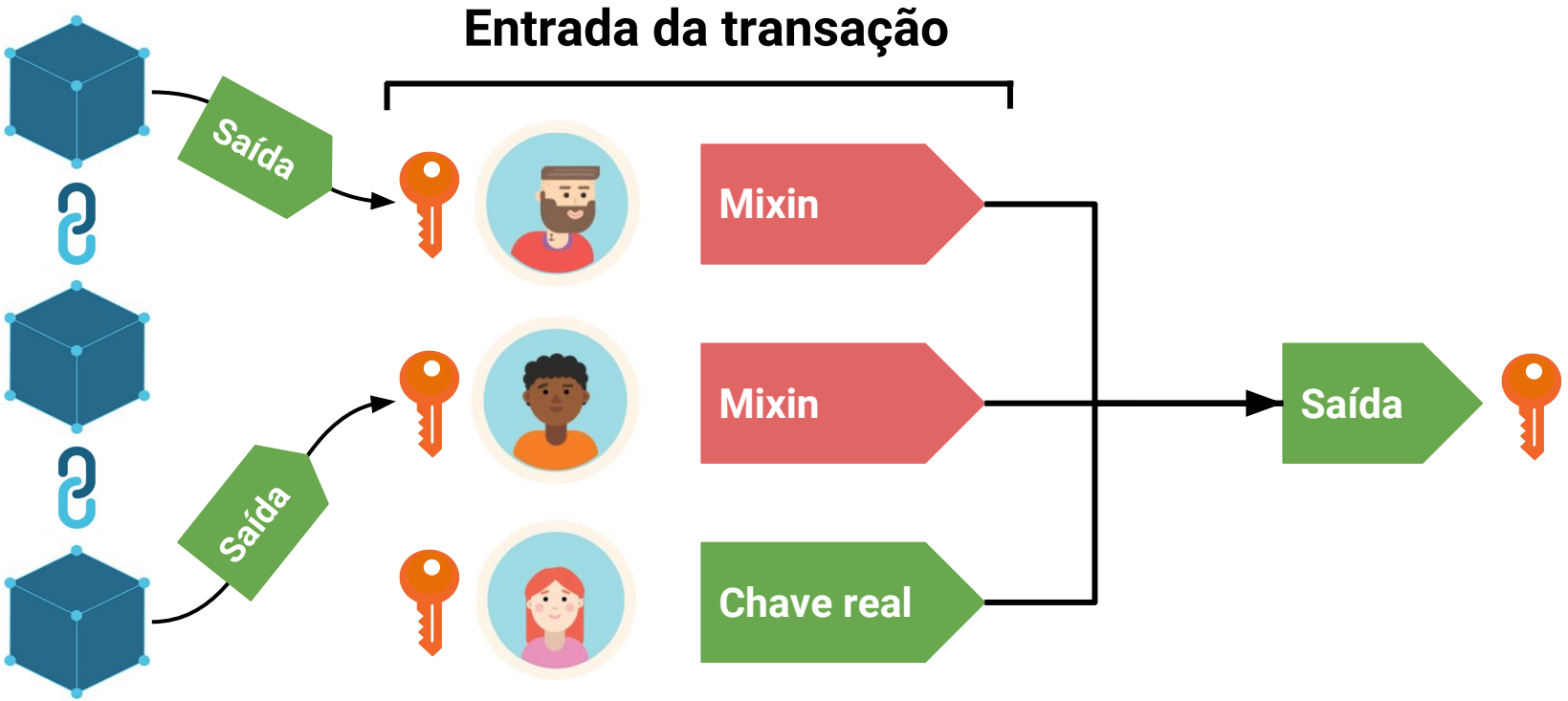
Chave privada de utilização de fundos

Chave privada de visualização

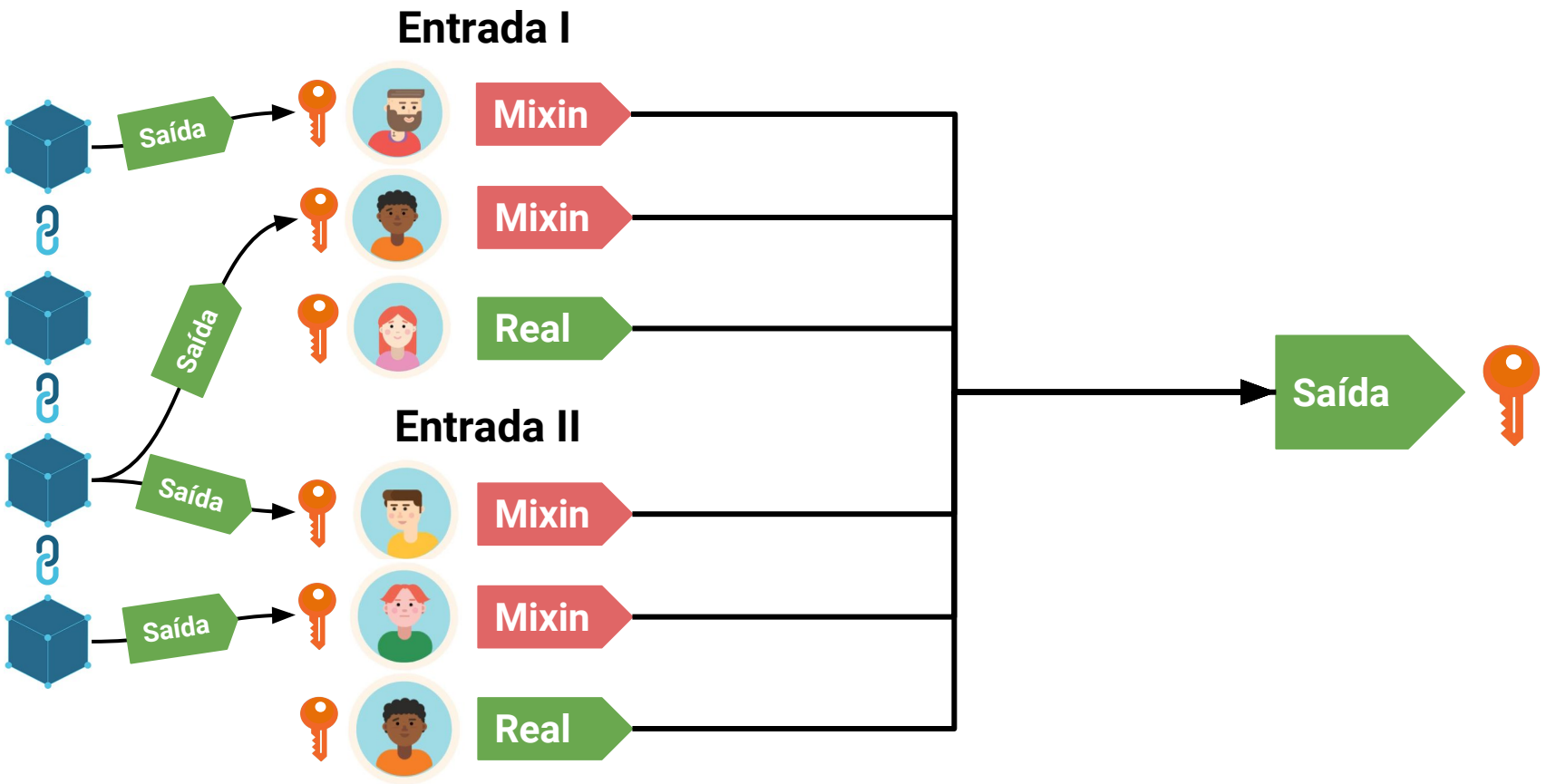
Monero: Assinaturas em anel



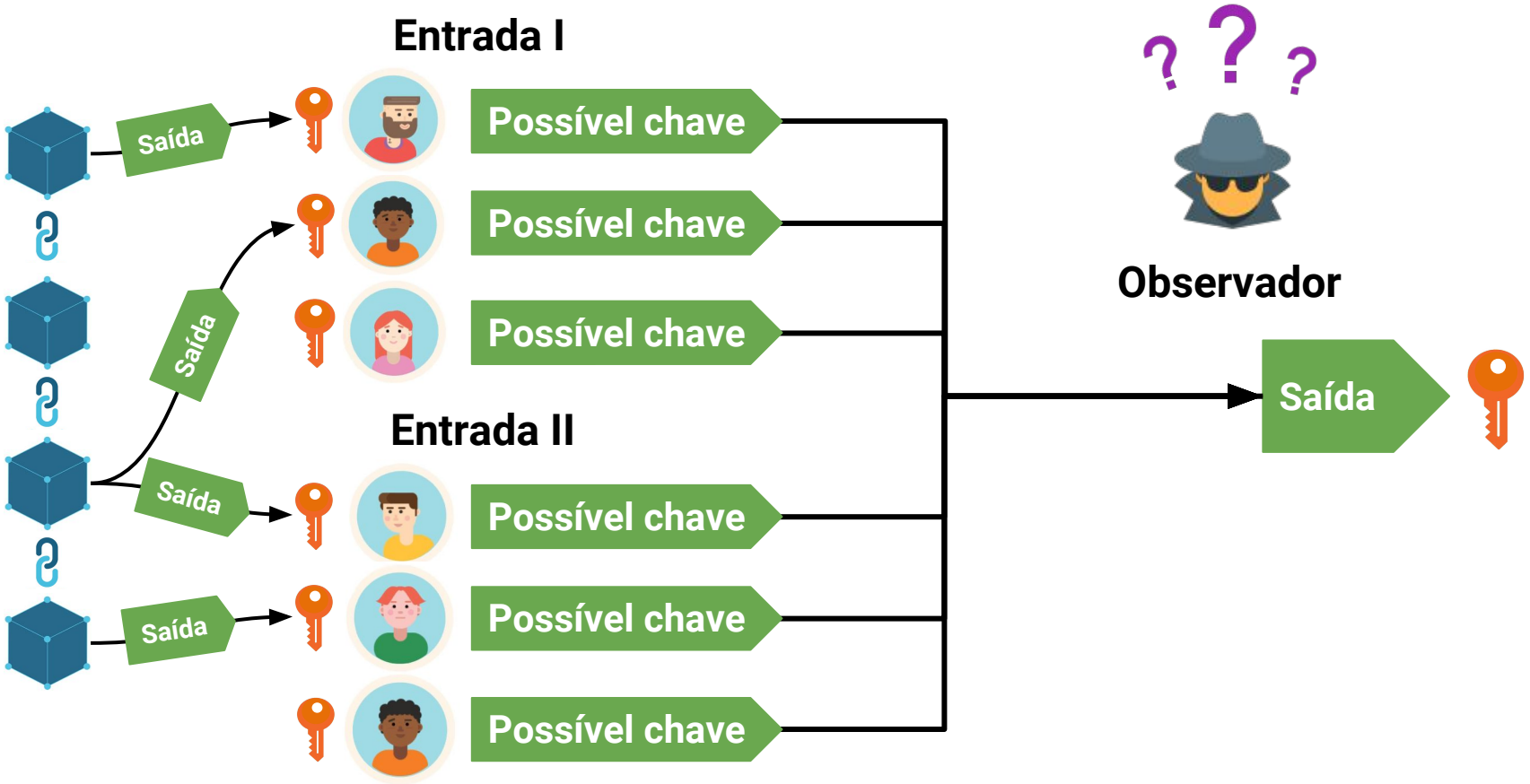
Monero: Assinaturas em anel



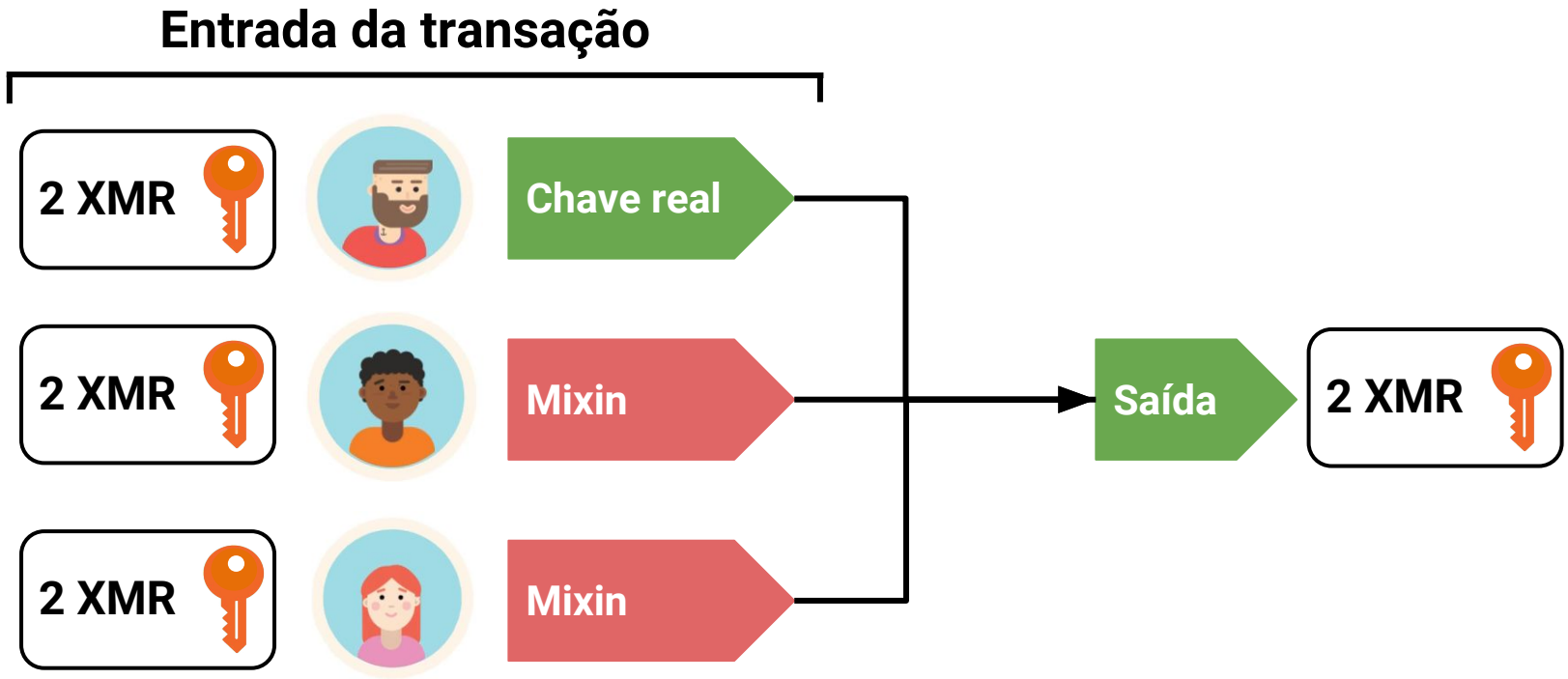
Monero: Assinaturas em anel



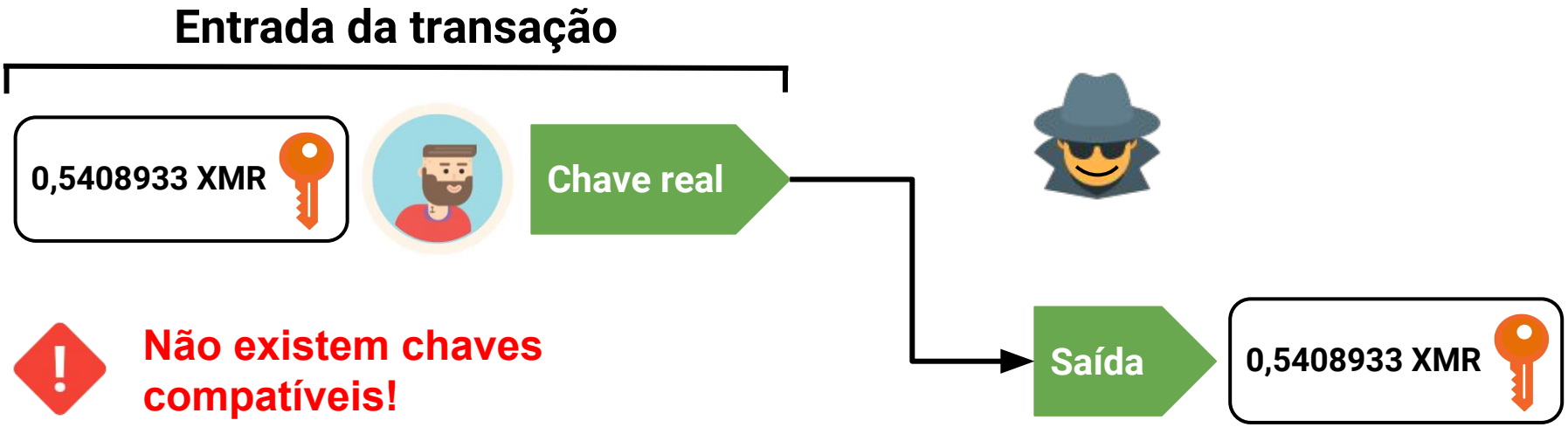
Monero: Assinaturas em anel



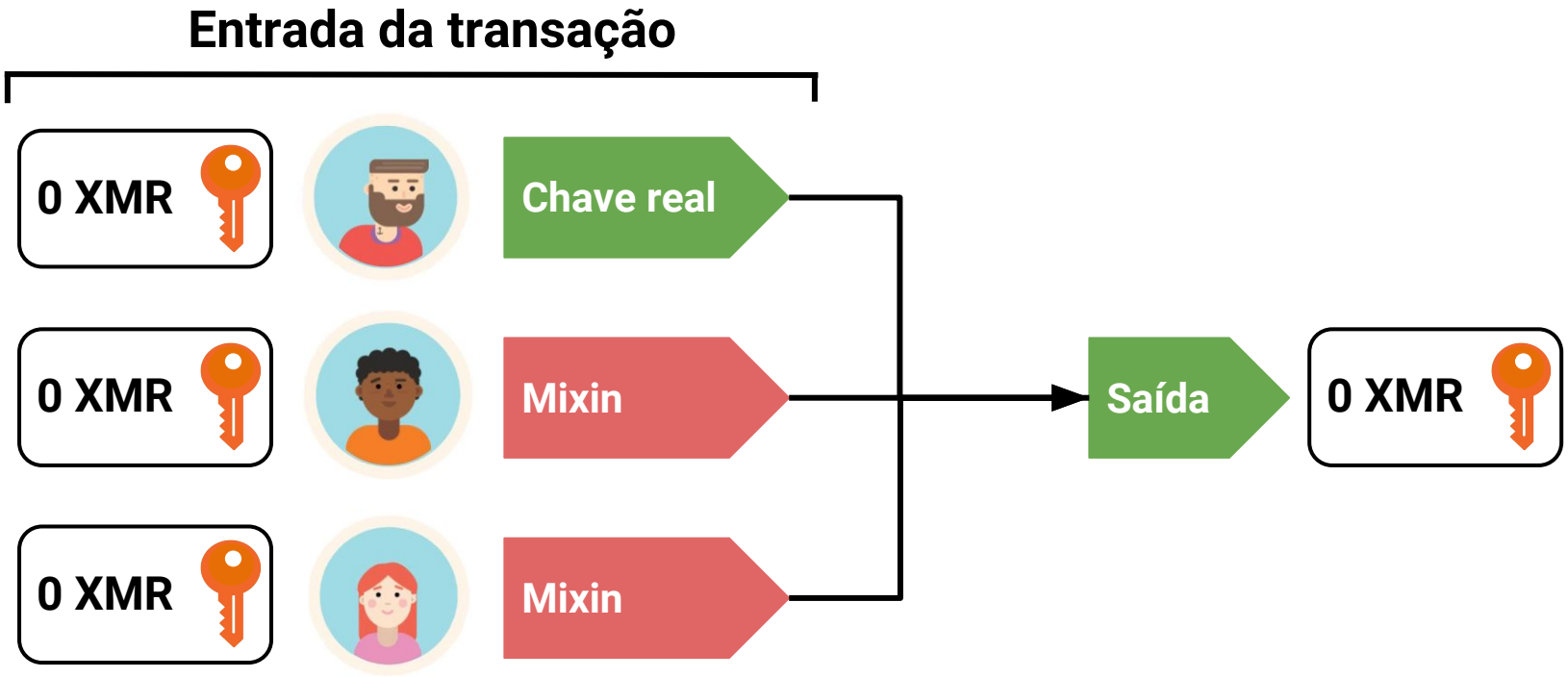
Monero: Transações confidenciais



Monero: Transações confidenciais



Monero: Transações confidenciais



Roteiro

- Monero
- **Análise de rastreabilidade**
- O ataque proposto
- Desafios de pesquisa
- Considerações finais

Análise de rastreabilidade

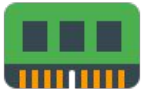
Duas heurísticas de ataque:

Análise de mixins

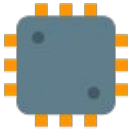
Análise temporal

Análise de rastreabilidade

Recursos da máquina utilizada:



64 GB de memória RAM



Intel Xeon X5690 3.47GHz (24 núcleos)

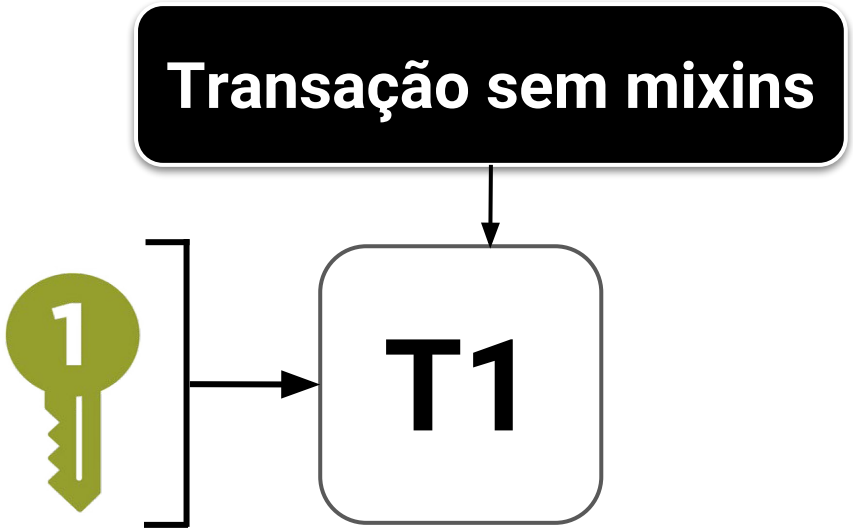
Ferramentas:

Linguagem Python v3.6

Linguagem c++11

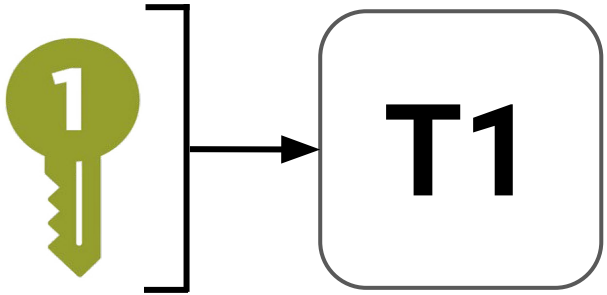
Monero Blockchain Explorer

Análise de mixins



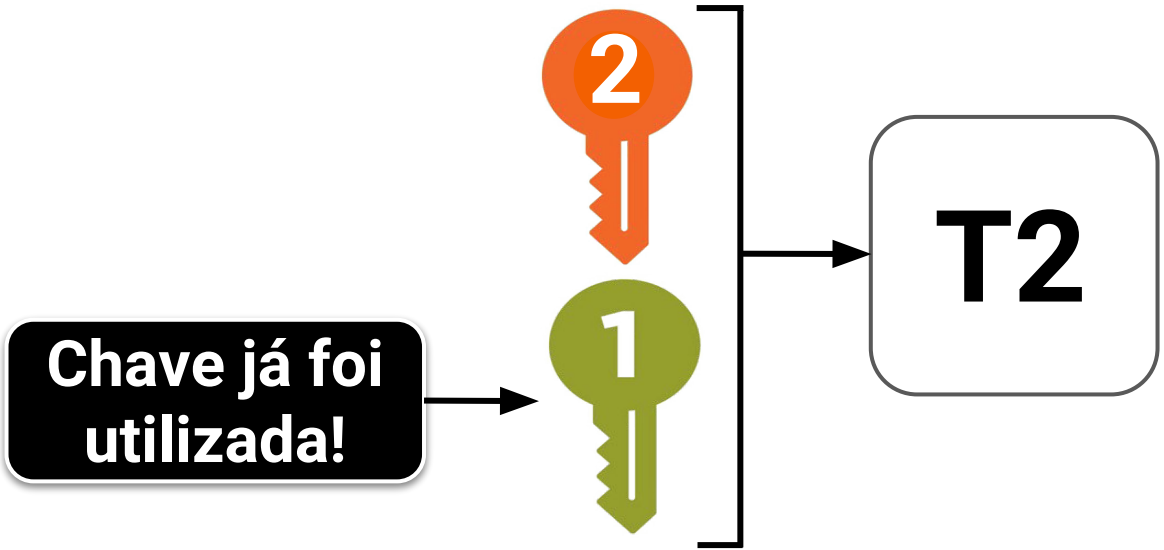
Análise de mixins

Chaves utilizadas: 



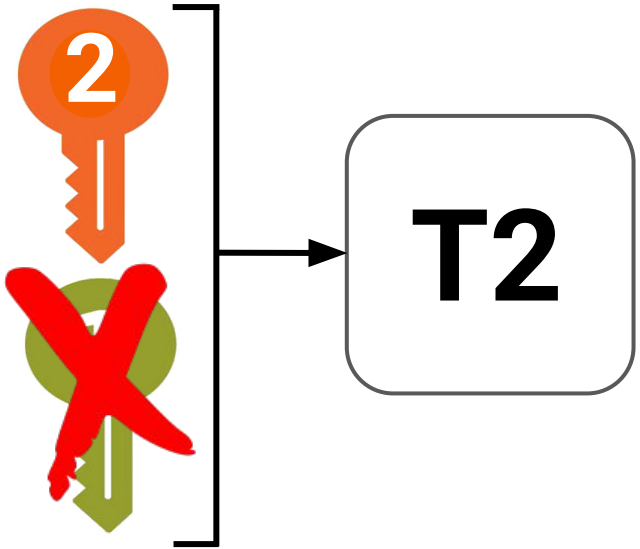
Análise de mixins

Chaves utilizadas: 



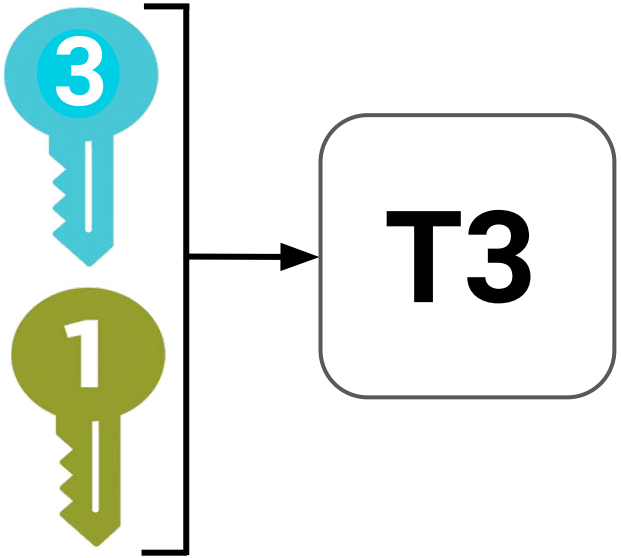
Análise de mixins

Chaves utilizadas: 



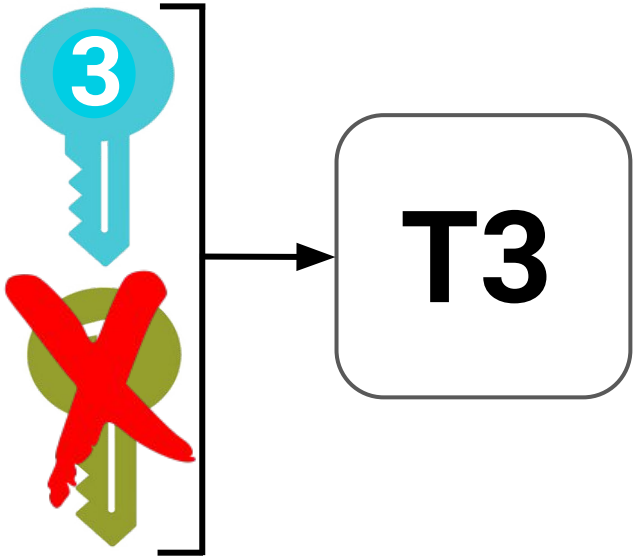
Análise de mixins

Chaves utilizadas: 



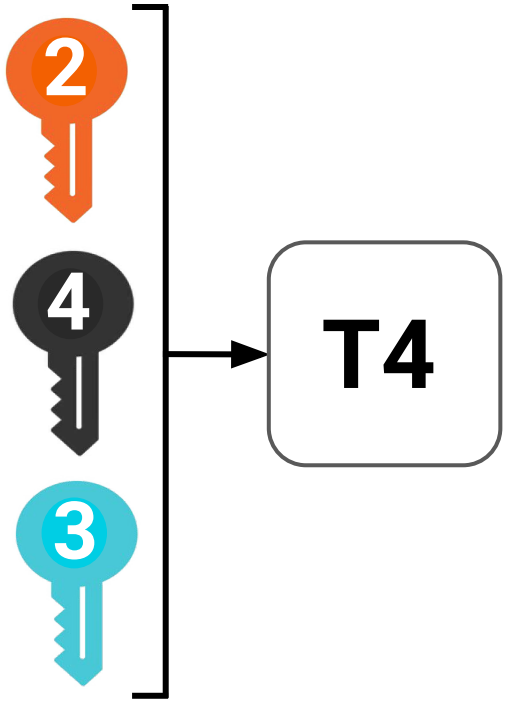
Análise de mixins

Chaves utilizadas: 



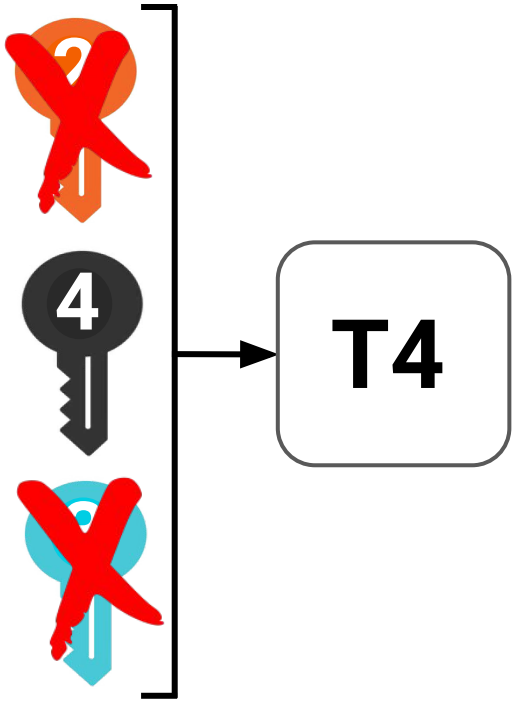
Análise de mixins

Chaves utilizadas: 



Análise de mixins

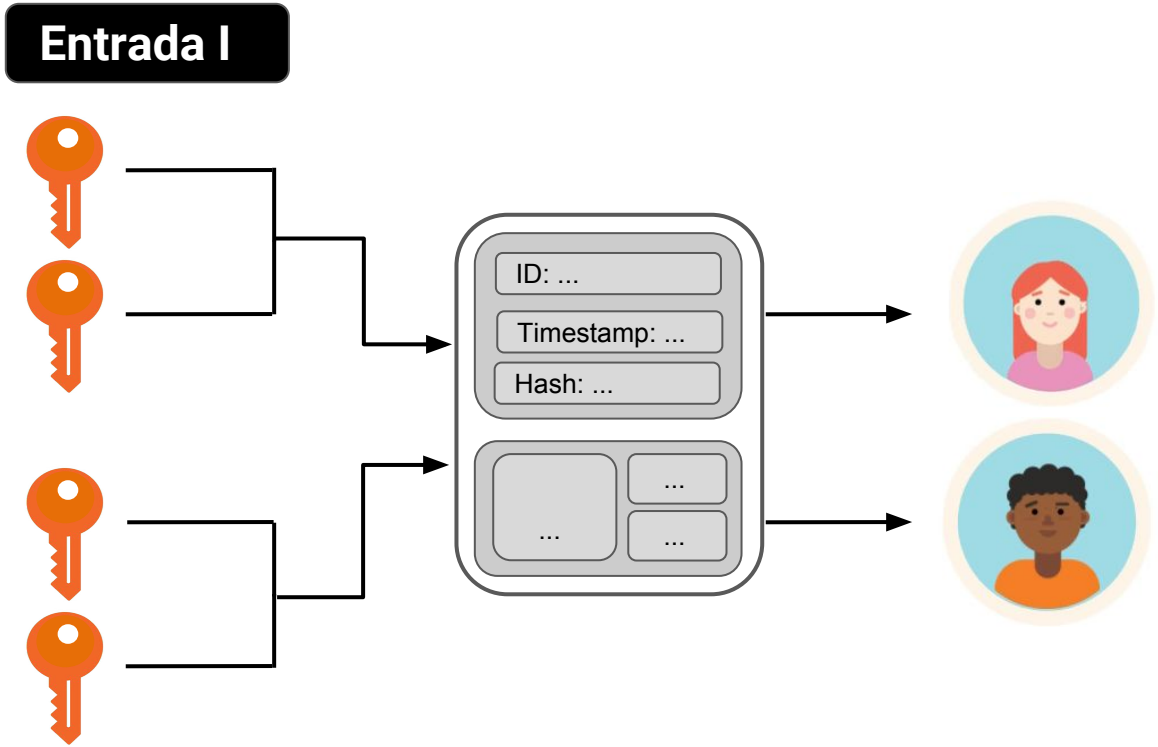
Chaves utilizadas: 



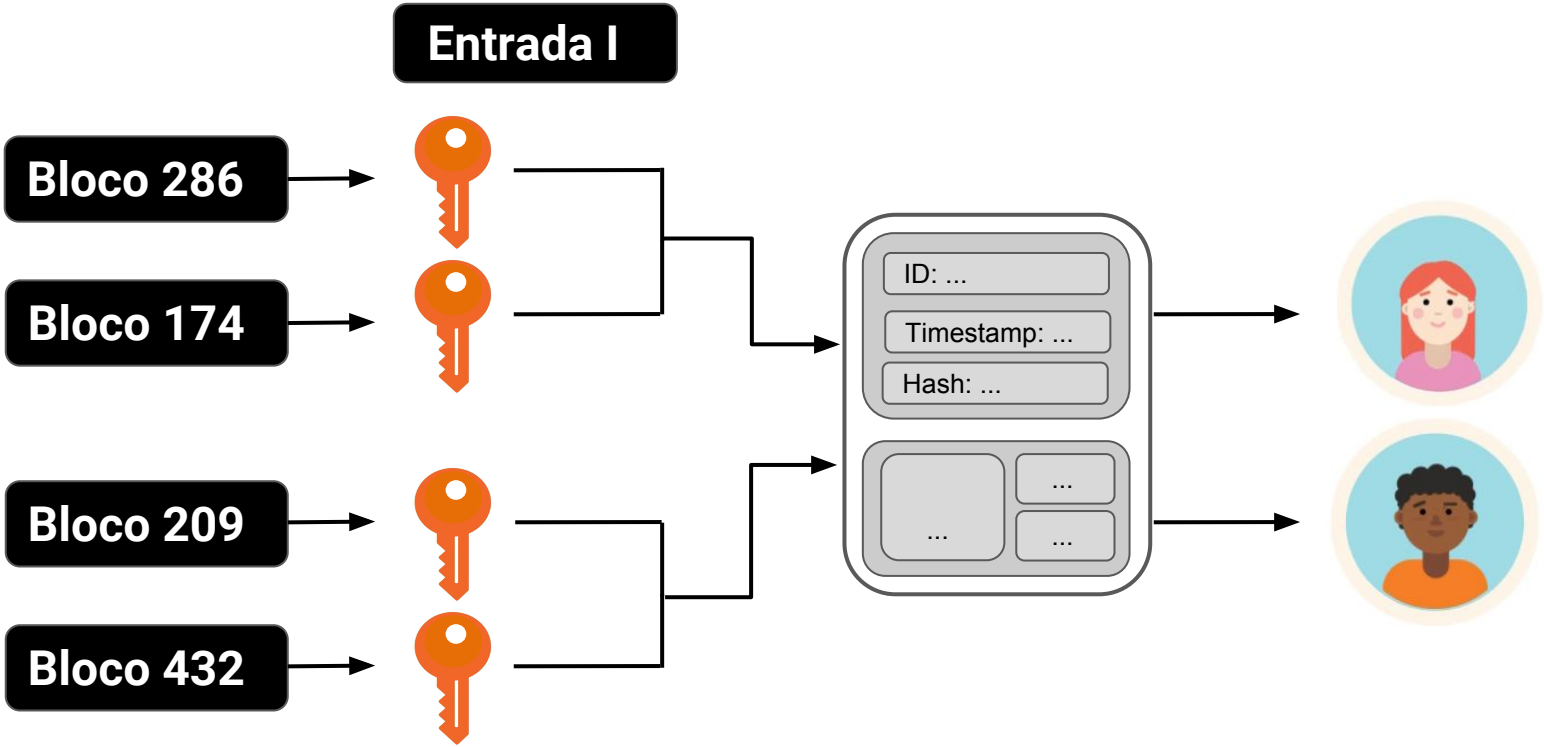
Análise de mixins

Quantidade de mixins	Entradas deduzidas
50	149
70	22
90	10
100	39
153	1

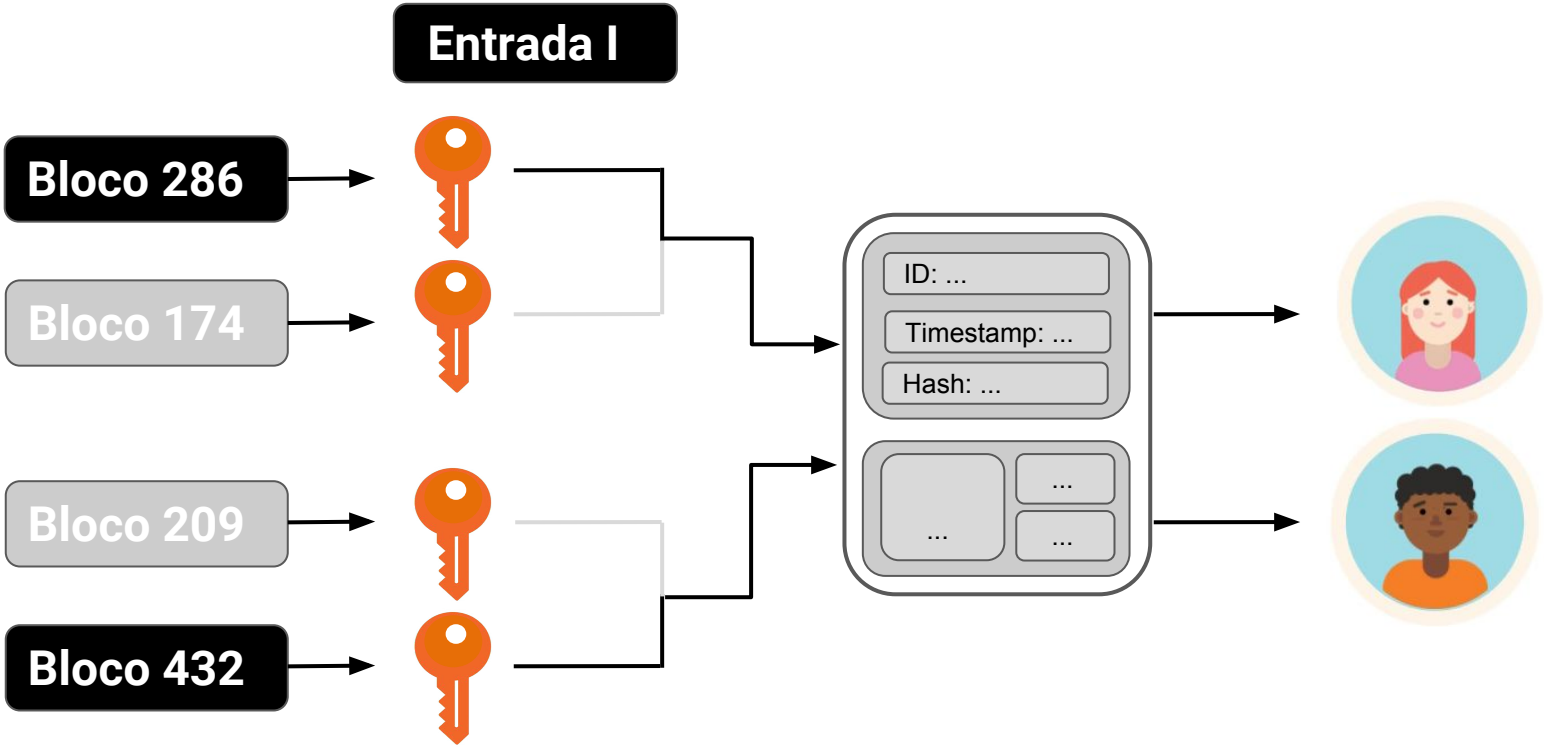
Análise temporal



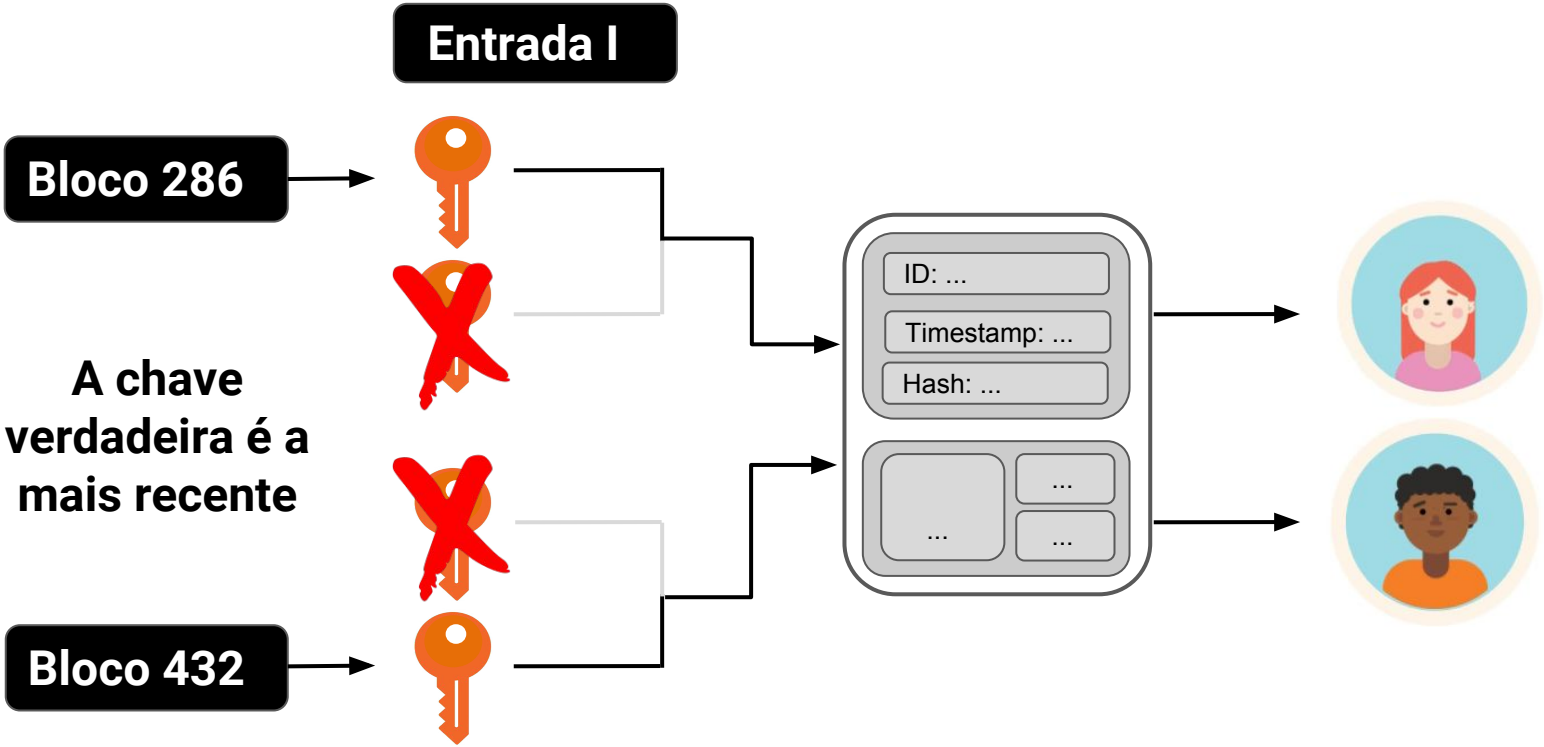
Análise temporal



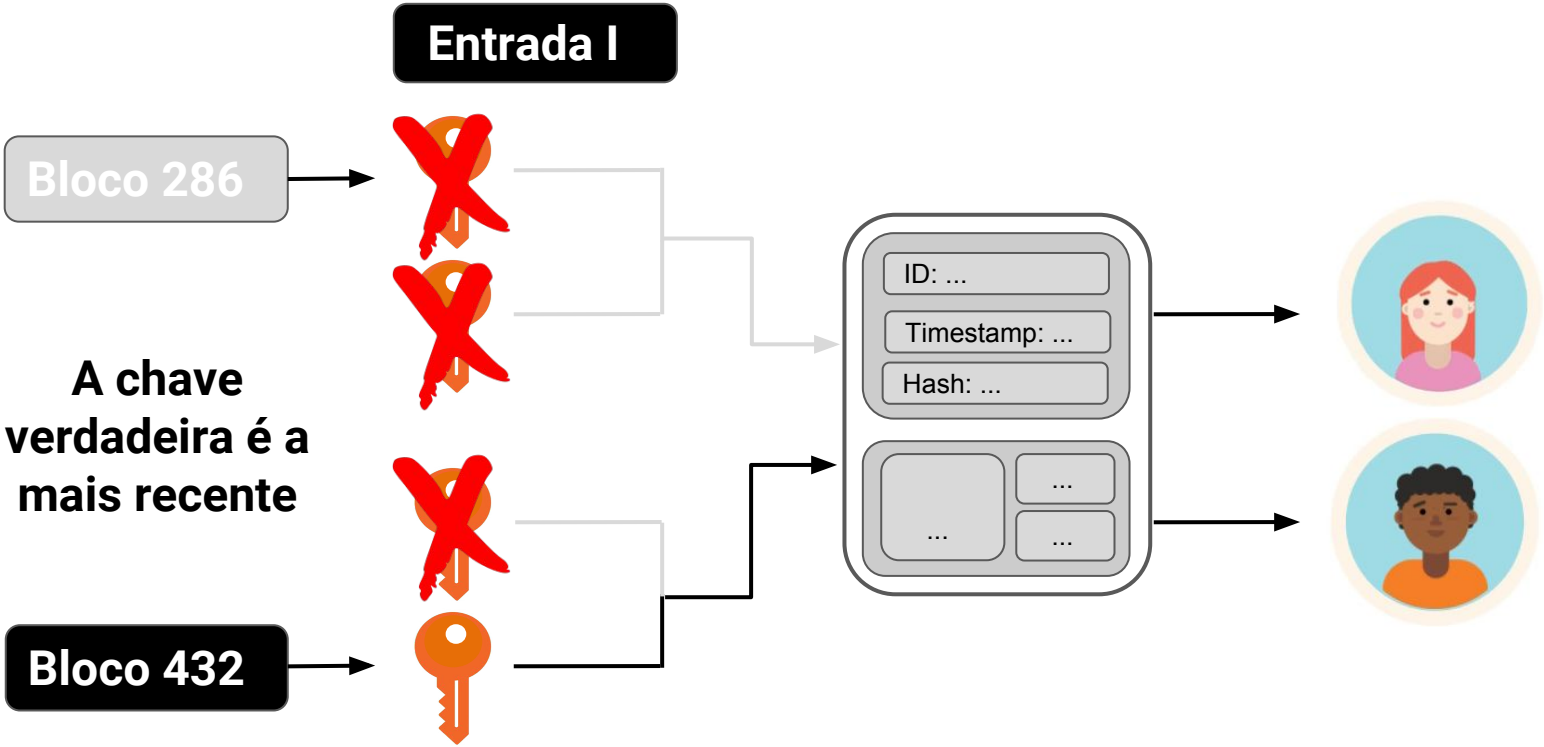
Análise temporal



Análise temporal



Análise temporal



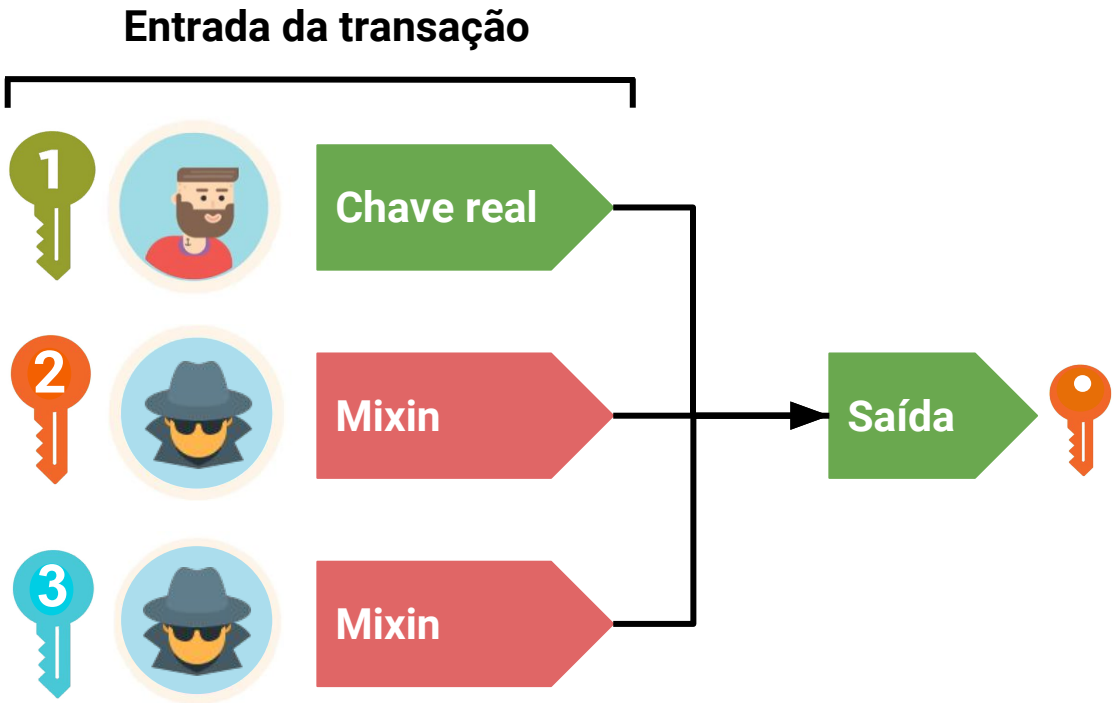
Análise temporal

Observável	Quantidade
Número total de entradas	17.374.129 (100%)
Entradas que contêm 0 mixins	12.130.656 (69,82%)
Entradas vulneráveis à dedução	3.481.943 (20,04%)
Entradas rastreadas	15.612.599 (89,86%)
Entradas não-rastreáveis pelo Algoritmo 1	1.761.530 (10,13%)
Taxa de acertos da análise temporal	92,48%
Total de entradas rastreáveis (estimado)	17.195.509 (98,97%)

Roteiro

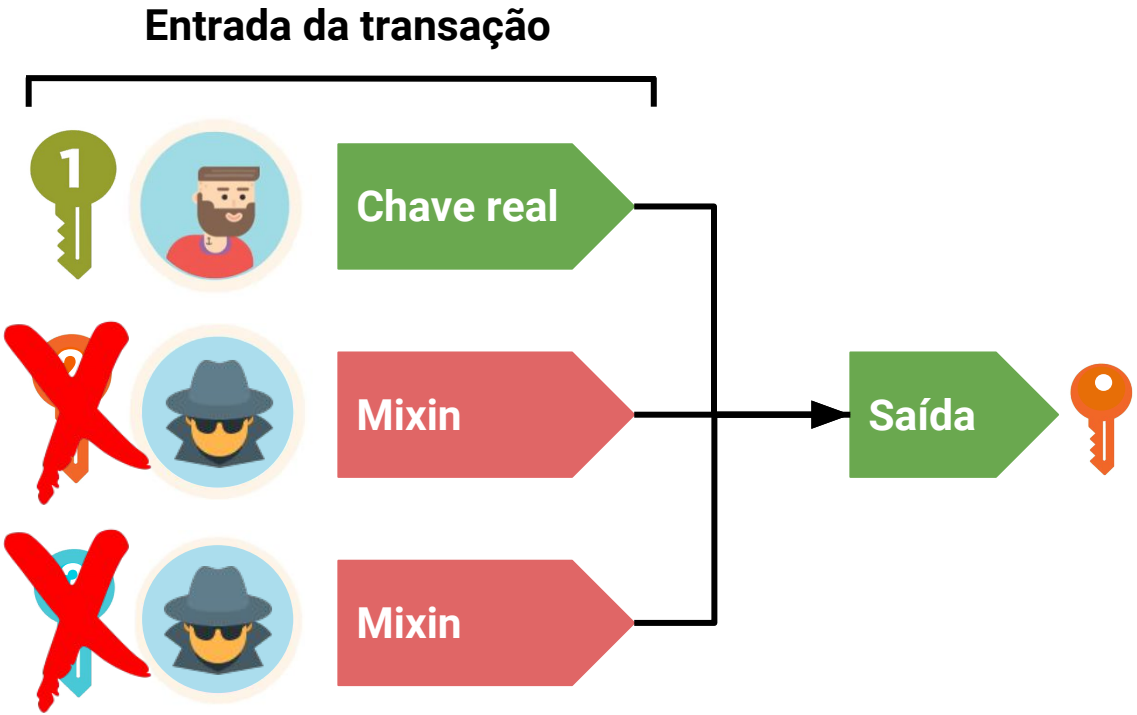
- Monero
- Análise de rastreabilidade
- **O ataque proposto**
- Desafios de pesquisa
- Considerações finais

O ataque proposto



Chaves do atacante:

O ataque proposto

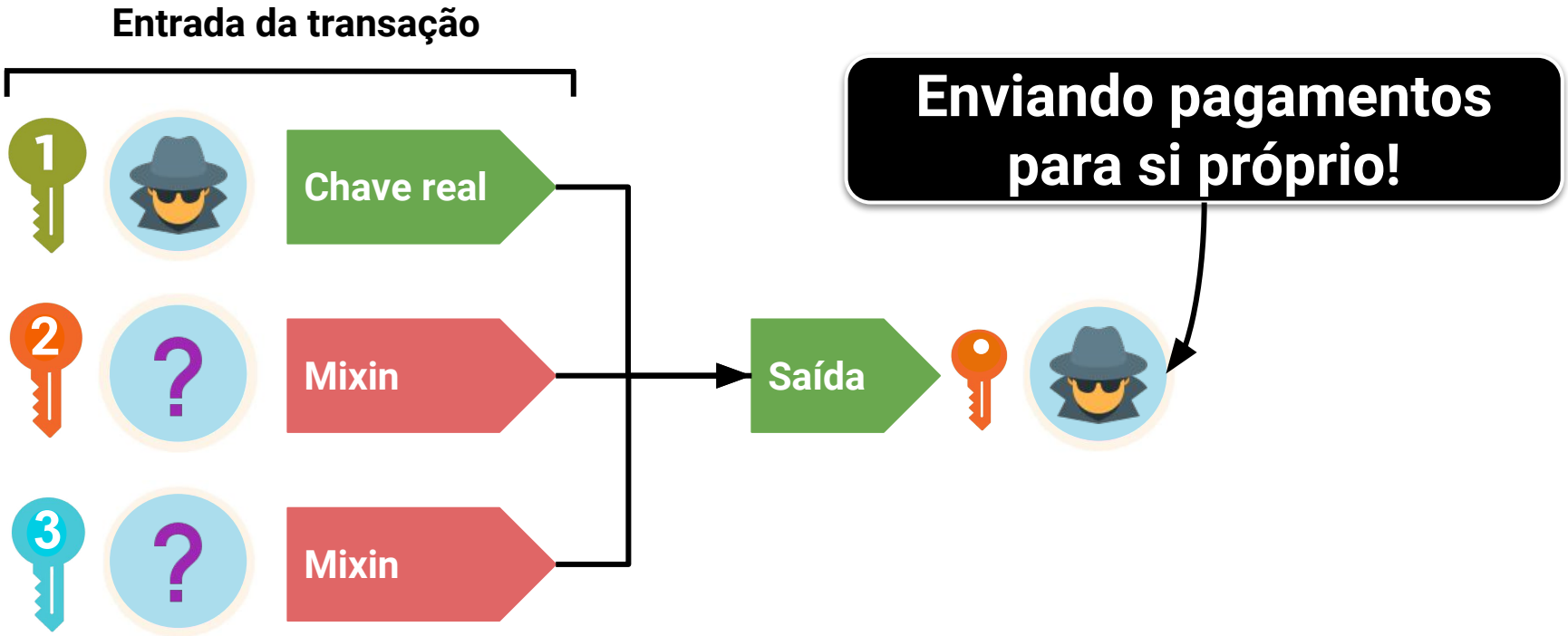


Chaves do atacante:

O ataque proposto

Como o atacante adquire chaves?

O ataque proposto



O ataque proposto

❗ Dificuldades:

- O atacante não controla a escolha de mixins
- As chance das mixins serem todas do atacante são baixas
- A criação de transações exige o pagamento de uma taxa

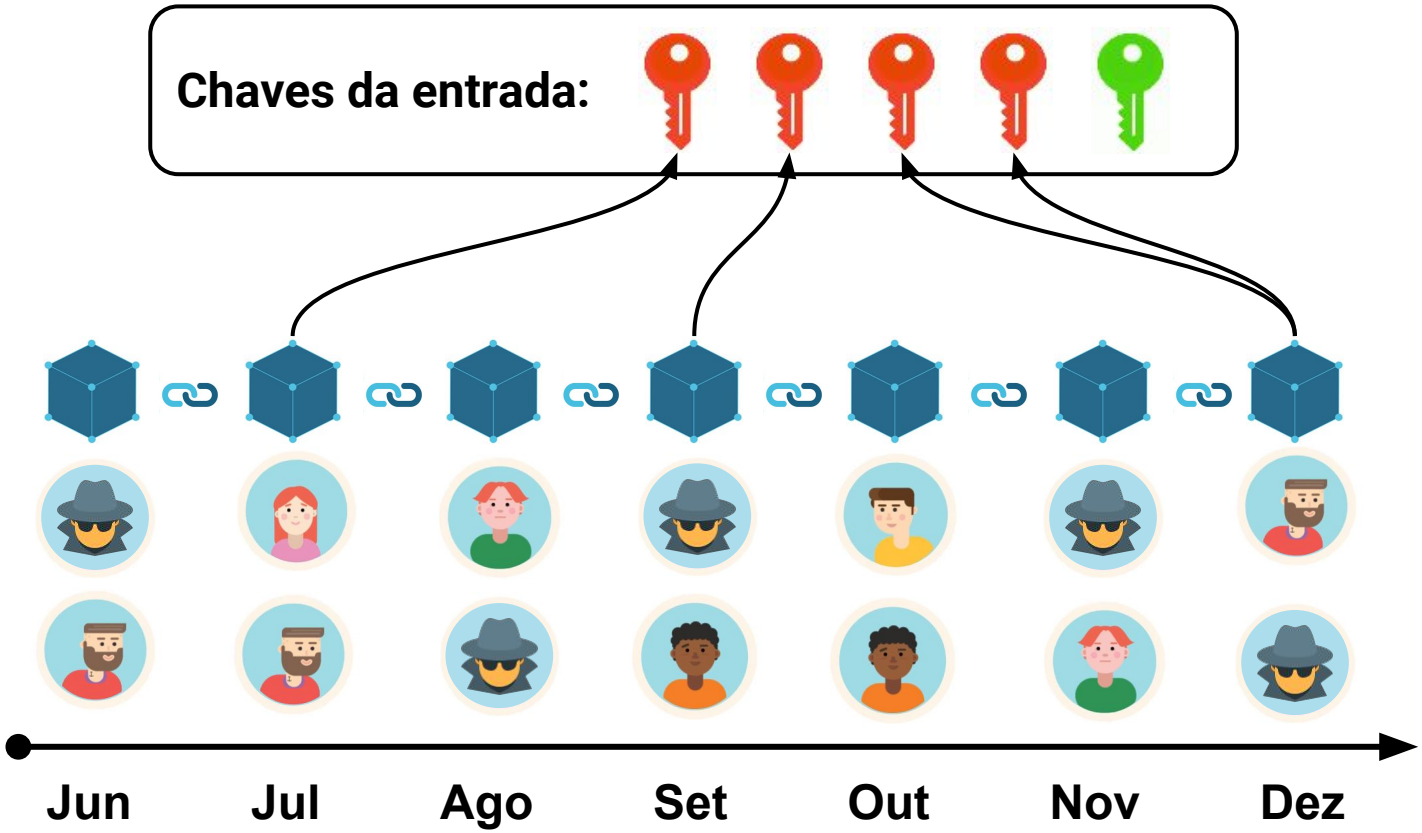
Protocolo Bulletproof

- Lançado no dia 18 de outubro de 2018
- Reduziu o tamanho das transações
- Diminuiu significativamente o custo das taxas de transações

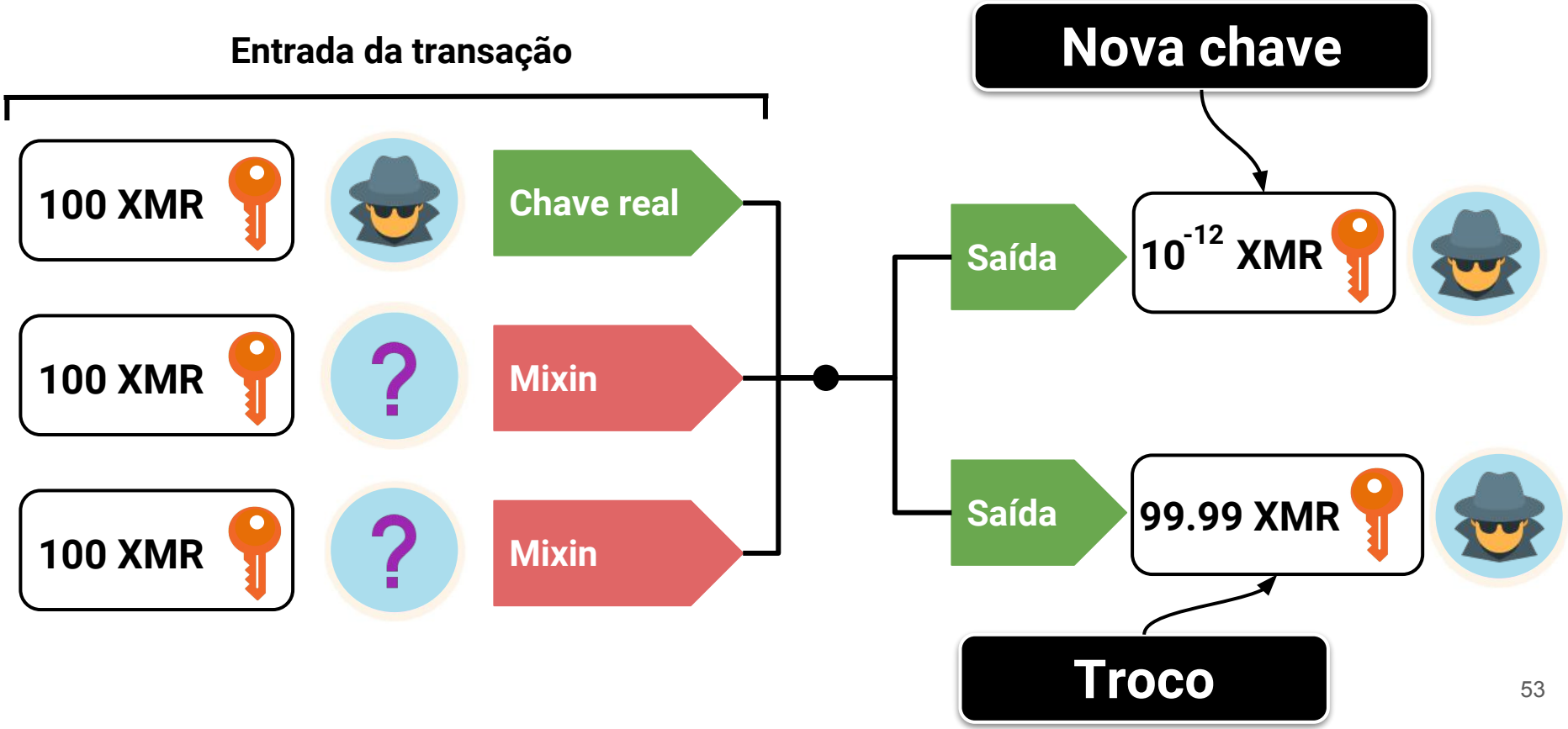
Modelo de atacante

- Possui acesso ao blockchain do sistema Monero
- Possui fundos suficientes para criar as transações
- Pode criar vários endereços do sistema Monero
- É capaz de criar tantas transações quantas desejar

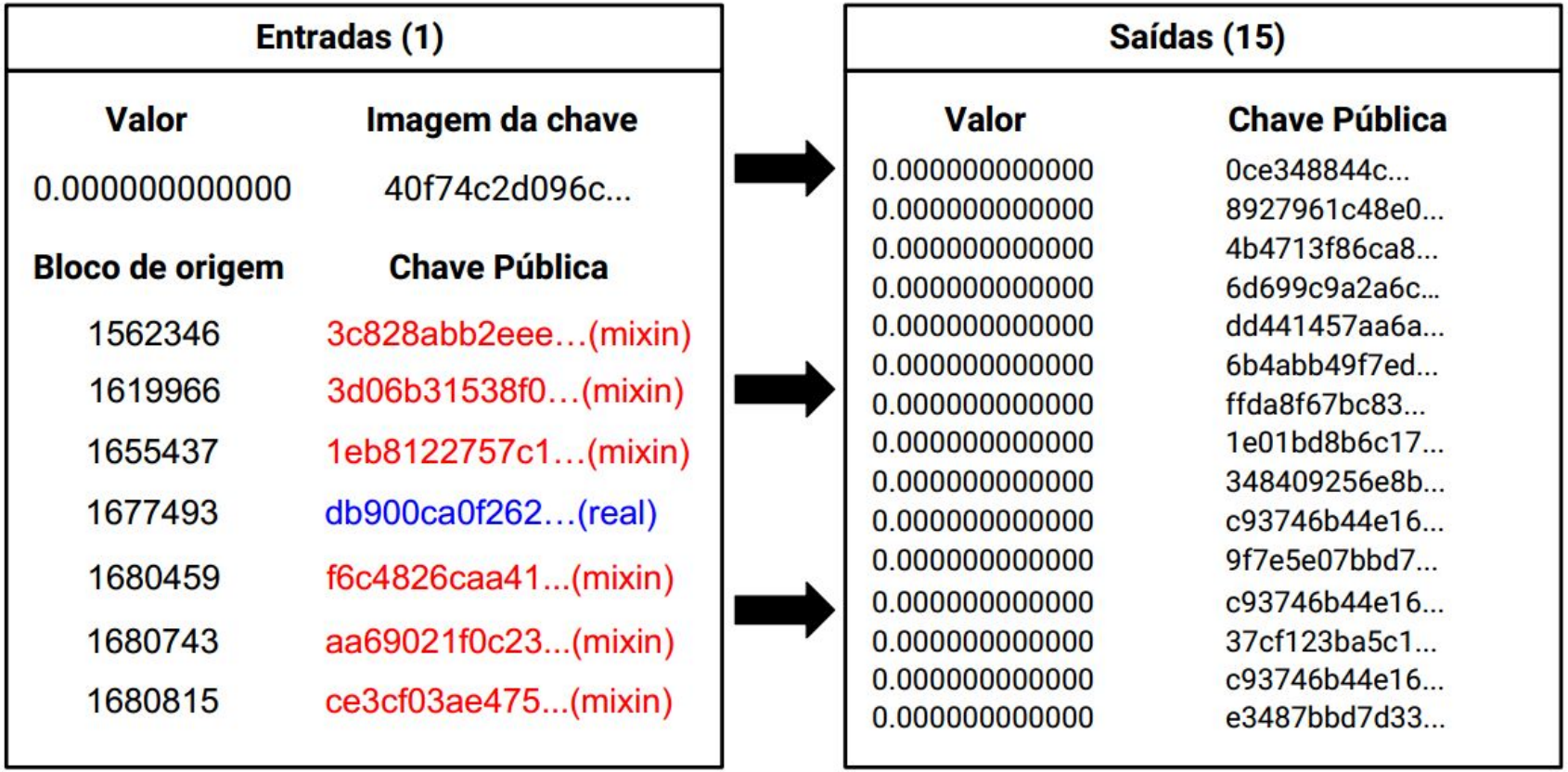
Manipulação de mixins



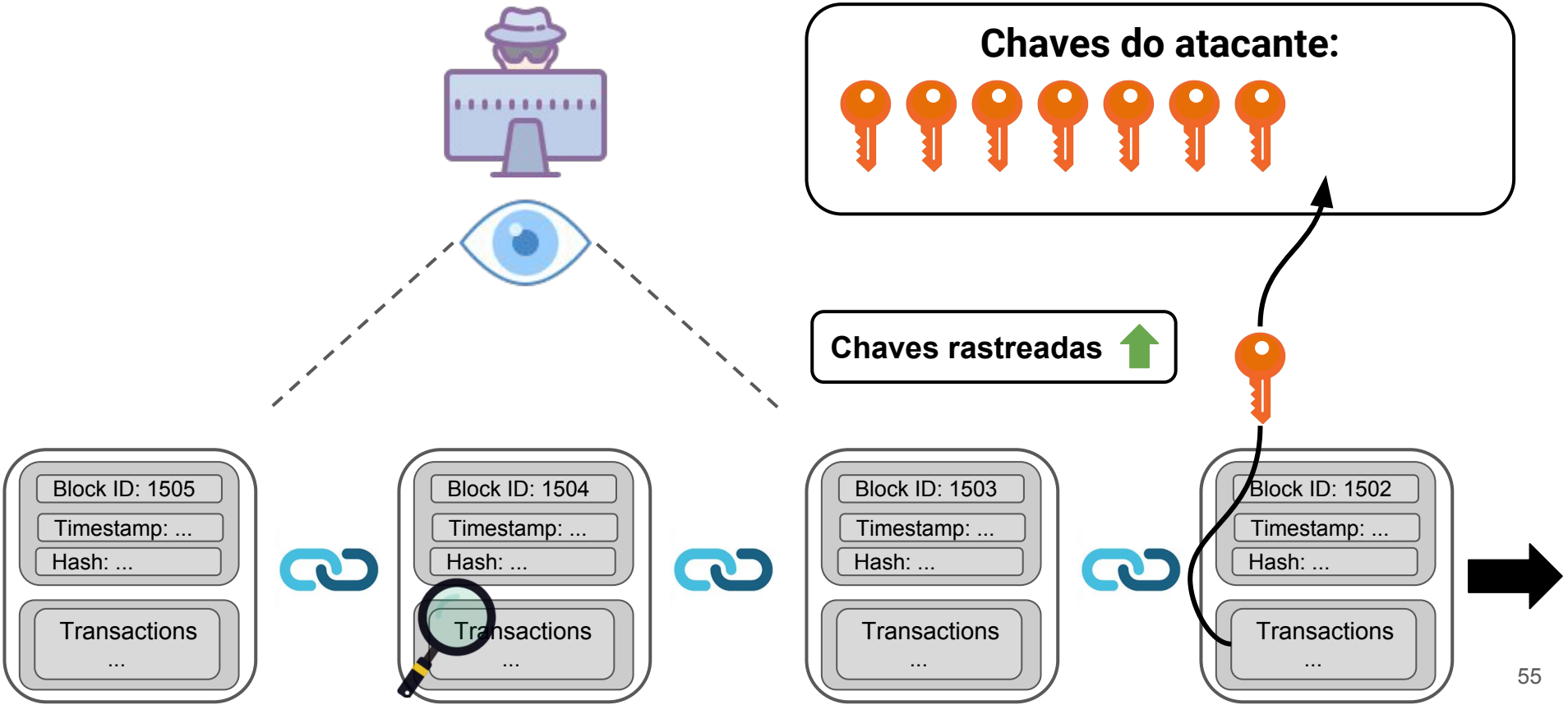
Manipulação de mixins



Manipulação de mixins



Manipulação de mixins



Cenários de simulação

- Período de 3 meses (blocos 1.433.039 à 1.499.600)
- Período de 6 meses (blocos 1.366.664 à 1.499.600)
- Período de 9 meses (blocos 1.300.239 à 1.499.600)
- Período de 1 ano (blocos 1.236.197 à 1.499.600)

Resultados

Chaves do atacante	Entradas rastreáveis			
	3 meses	6 meses	9 meses	1 ano
1%	21.741(1,66%)	42.325(1,67%)	47.338(1,25%)	57.958(1,36%)
25%	24.811(1,89%)	90.919(3,59%)	323.290(8,48%)	3.658.855(85,59%)
50%	67.977(5,16%)	511.148(20,35%)	3.208.179(84,83%)	3.814.831(89,22%)
75%	249.968(19,01%)	1.968.541(77,84%)	3.250.988(85,96%)	3.836.312(89,72%)
100%	534.778(40,73%)	2.143.723(84,84%)	3.263.091(86,28%)	3.839.963(89,81%)

Resultados

Chaves do atacante	Entradas rastreáveis			
	3 meses	6 meses	9 meses	1 ano
1%	21.741(1,66%)	42.325(1,67%)	47.338(1,25%)	57.958(1,36%)
25%	24.811(1,89%)	90.919(3,59%)	323.290(8,48%)	3.658.855(85,59%)
50%	67.977(5,16%)	511.148(20,35%)	3.208.179(84,83%)	3.814.831(89,22%)
75%	249.968(19,01%)	1.968.541(77,84%)	3.250.988(85,96%)	3.836.312(89,72%)
100%	534.778(40,73%)	2.143.723(84,84%)	3.263.091(86,28%)	3.839.963(89,81%)

Resultados

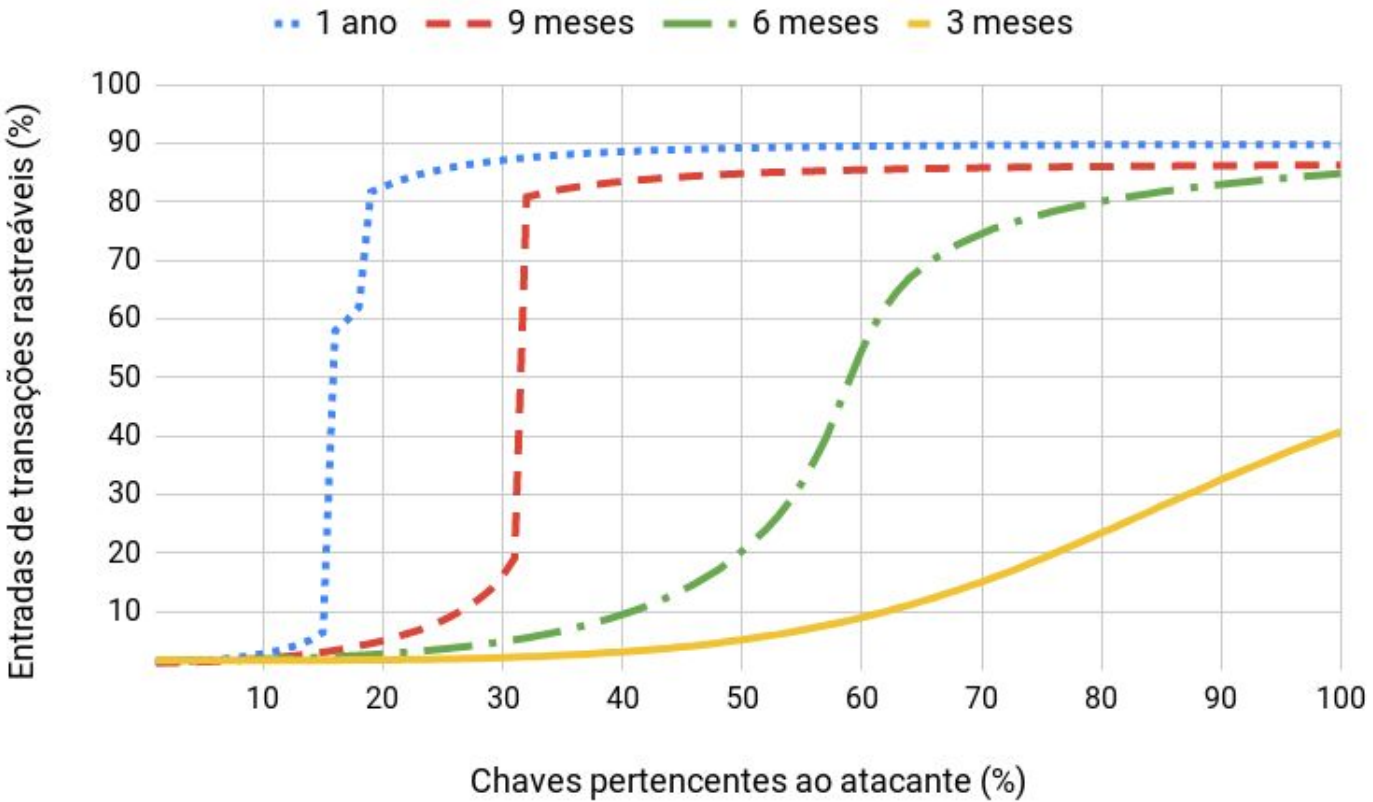
Chaves do atacante	Entradas rastreáveis			
	3 meses	6 meses	9 meses	1 ano
1%	21.741(1,66%)	42.325(1,67%)	47.338(1,25%)	57.958(1,36%)
25%	24.811(1,89%)	90.919(3,59%)	323.290(8,48%)	3.658.855(85,59%)
50%	67.977(5,16%)	511.148(20,35%)	3.208.179(84,83%)	3.814.831(89,22%)
75%	249.968(19,01%)	1.968.541(77,84%)	3.250.988(85,96%)	3.836.312(89,72%)
100%	534.778(40,73%)	2.143.723(84,84%)	3.263.091(86,28%)	3.839.963(89,81%)

Resultados

Chaves do atacante	Entradas rastreáveis			
	3 meses	6 meses	9 meses	1 ano
1%	21.741(1,66%)	42.325(1,67%)	47.338(1,25%)	57.958(1,36%)
25%	24.811(1,89%)	90.919(3,59%)	323.290(8,48%)	3.658.855(85,59%)
50%	67.977(5,16%)	511.148(20,35%)	3.208.179(84,83%)	3.814.831(89,22%)
75%	249.968(19,01%)	1.968.541(77,84%)	3.250.988(85,96%)	3.836.312(89,72%)
100%	534.778(40,73%)	2.143.723(84,84%)	3.263.091(86,28%)	3.839.963(89,81%)

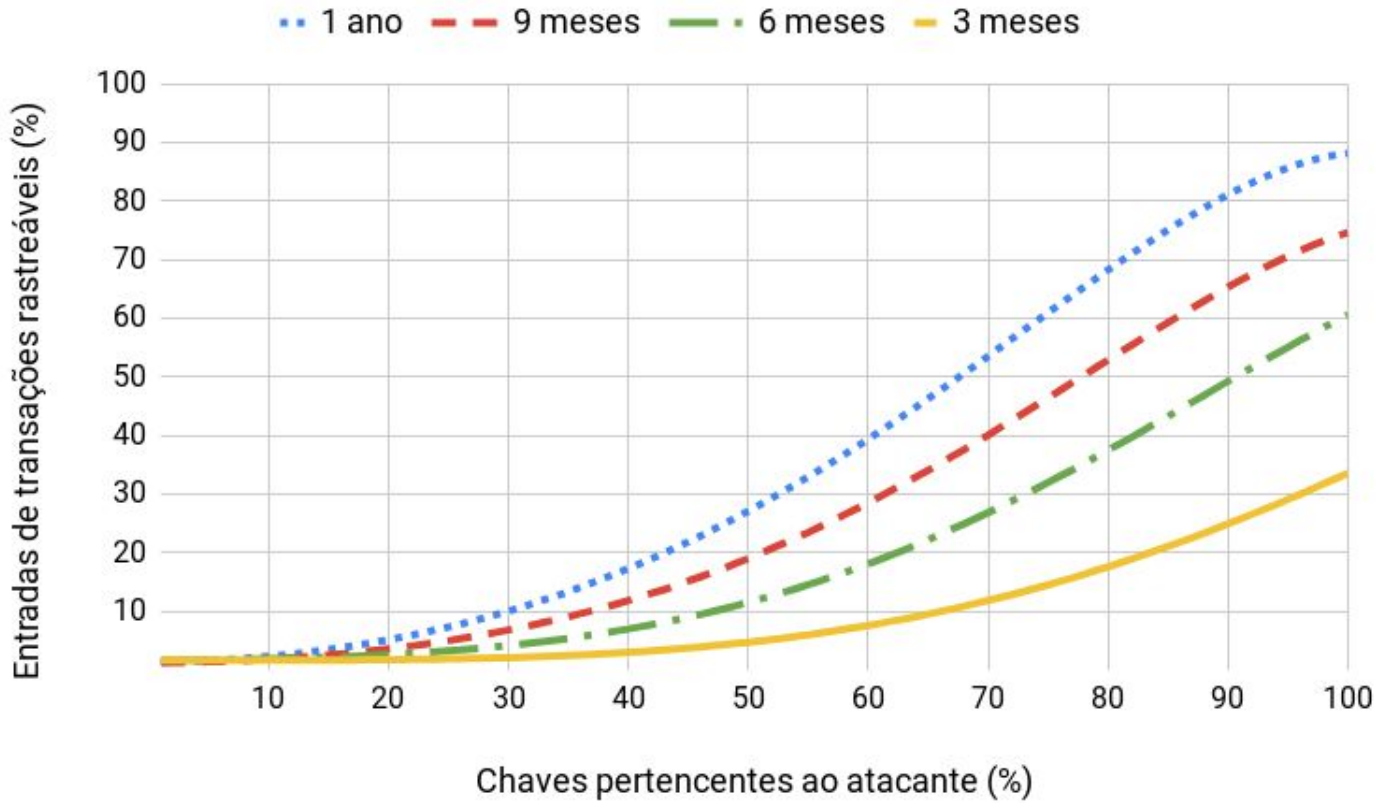
Resultados

Aumento da capacidade de rastreio de acordo com o poder do atacante



Resultados

Aumento da capacidade de rastreio de acordo com o poder do atacante (sem reações em cadeia)



Análise de custos

Quanto dinheiro um atacante precisa gastar para executar este ataque?

Análise de custos

- **Parâmetros considerados:**

O número médio de chaves criadas por dia é de 11.713

A taxa paga por cada transação do atacante é de 0,00019 XMR

1 XMR equivale à 69,42 USD

Análise de custos

Controle do atacante	Custos em taxas de transações (XMR/USD)			
	3 meses	**6 meses**	**9 meses**	**1 ano**
1%	0,135 XMR 9,36 USD	0,269 XMR 18,67 USD	0,403 XMR 27,98 USD	0,545 XMR 37,84 USD
25%	4,450 XMR 308,65 USD	8,901 XMR 617,37 USD	13,351 XMR 926,02 USD	18,049 XMR 1.252,05 USD
50%	13,352 XMR 926,22 USD	26,705 XMR 1.852,52 USD	40,058 XMR 2.775,61 USD	54,153 XMR 3.752,26 USD
75%	40,058 XMR 2.775,61 USD	80,116 XMR 5.551,23 USD	120,175 XMR 8.326,92 USD	162,459 XMR 11.258,40 USD
99%	1.321,929 XMR 91.596,46 USD	2.643,858 XMR 183.192,92 USD	3.965,787 XMR 274.789,38 USD	5.361,157 XMR 371.474,56 USD

Análise de custos

Controle do atacante	Custos em taxas de transações (XMR/USD)			
	3 meses	**6 meses**	**9 meses**	**1 ano**
1%	0,135 XMR 9,36 USD	0,269 XMR 18,67 USD	0,403 XMR 27,98 USD	0,545 XMR 37,84 USD
25%	4,450 XMR 308,65 USD	8,901 XMR 617,37 USD	13,351 XMR 926,02 USD	18,049 XMR 1.252,05 USD
50%	13,352 XMR 926,22 USD	26,705 XMR 1.852,52 USD	40,058 XMR 2.775,61 USD	54,153 XMR 3.752,26 USD
75%	40,058 XMR 2.775,61 USD	80,116 XMR 5.551,23 USD	120,175 XMR 8.326,92 USD	162,459 XMR 11.258,40 USD
99%	1.321,929 XMR 91.596,46 USD	2.643,858 XMR 183.192,92 USD	3.965,787 XMR 274.789,38 USD	5.361,157 XMR 371.474,56 USD

Análise de custos

Controle do atacante	Custos em taxas de transações (XMR/USD)			
	3 meses	**6 meses**	**9 meses**	**1 ano**
1%	0,135 XMR 9,36 USD	0,269 XMR 18,67 USD	0,403 XMR 27,98 USD	0,545 XMR 37,84 USD
25%	4,450 XMR 308,65 USD	8,901 XMR 617,37 USD	13,351 XMR 926,02 USD	18,049 XMR 1.252,05 USD
50%	13,352 XMR 926,22 USD	26,705 XMR 1.852,52 USD	40,058 XMR 2.775,61 USD	54,153 XMR 3.752,26 USD
75%	40,058 XMR 2.775,61 USD	80,116 XMR 5.551,23 USD	120,175 XMR 8.326,92 USD	162,459 XMR 11.258,40 USD
99%	1.321,929 XMR 91.596,46 USD	2.643,858 XMR 183.192,92 USD	3.965,787 XMR 274.789,38 USD	5.361,157 XMR 371.474,56 USD

Análise de custos

Controle do atacante	Custos em taxas de transações (XMR/USD)			
	3 meses	**6 meses**	**9 meses**	**1 ano**
1%	14,32 XMR 994,09 USD	28,645 XMR 1.988,53 USD	42,968 XMR 2.982,90 USD	58,087 XMR 4.032,39 USD
25%	473,867 XMR 32.895,84 USD	947,735 XMR 65.791,76 USD	1.421,602 XMR 98.687,61 USD	1.921,796 XMR 133.408,64 USD
50%	1.421,723 XMR 98.696,01 USD	2.843,447 XMR 197.392,09 USD	4.265,171 XMR 296.088,17 USD	5.765,880 XMR 400.267.38 USD
75%	4.265,171 XMR 296.088,17 USD	8.530,343 XMR 592.176,41 USD	12.795,515 XMR 888.264,65 USD	17.297,641 XMR 1.200.802,23 USD
99%	140.750,670 XMR 9.770.911,51 USD	281.501,340 XMR 19.541.823,02 USD	422.252,010 XMR 29.312.734,53 USD	570.822,161 XMR 39.626.474,41 USD

Análise de custos

Controle do atacante	Custos em taxas de transações (XMR/USD)			
	3 meses	6 meses	9 meses	1 ano
1%	14,32 XMR 994,09 USD	28,645 XMR 1.988,53 USD	42,968 XMR 2.982,90 USD	58,087 XMR 4.032,39 USD
25%	473,867 XMR 32.895,84 USD	947,735 XMR 65.791,76 USD	1.421,602 XMR 98.687,61 USD	1.921,796 XMR 133.408,64 USD
50%	1.421,723 XMR 98.696,01 USD	2.843,447 XMR 197.392,09 USD	4.265,171 XMR 296.088,17 USD	5.765,880 XMR 400.267.38 USD
75%	4.265,171 XMR 296.088,17 USD	8.530,343 XMR 592.176,41 USD	12.795,515 XMR 888.264,65 USD	17.297,641 XMR 1.200.802,23 USD
99%	140.750,670 XMR 9.770.911,51 USD	281.501,340 XMR 19.541.823,02 USD	422.252,010 XMR 29.312.734,53 USD	570.822,161 XMR 39.626.474,41 USD

Análise de custos

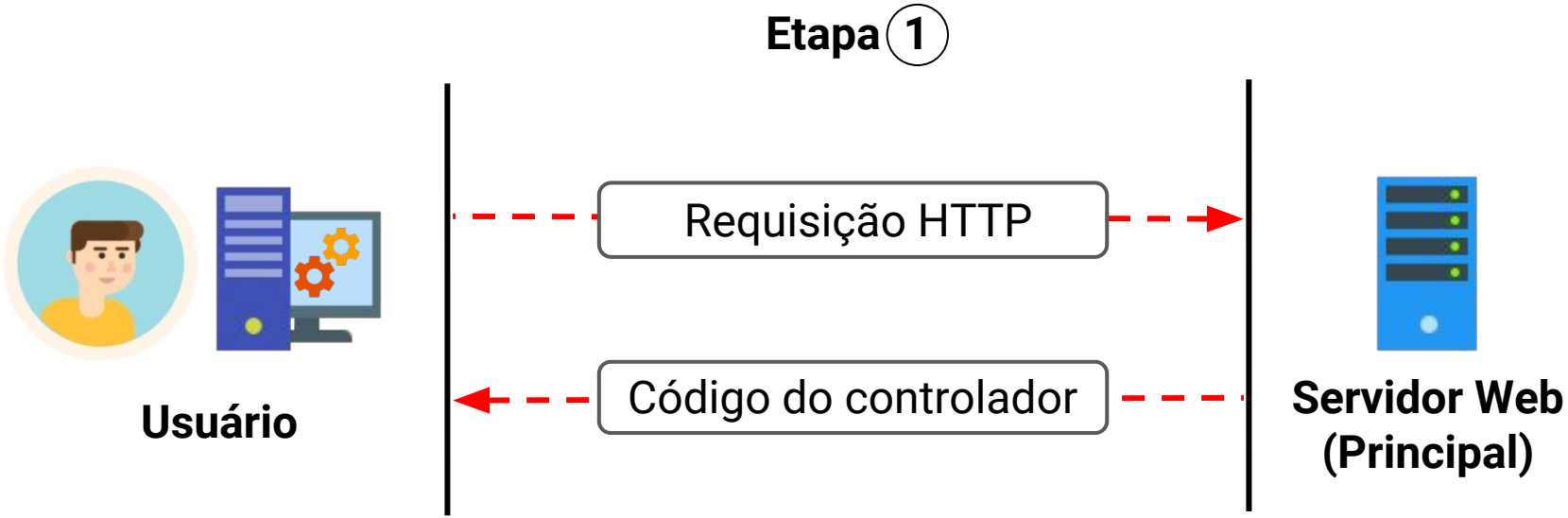
Controle do atacante	Custos em taxas de transações (XMR/USD)			
	3 meses	6 meses	9 meses	1 ano
1%	14,32 XMR 994,09 USD	28,645 XMR 1.988,53 USD	42,968 XMR 2.982,90 USD	58,087 XMR 4.032,39 USD
25%	473,867 XMR 32.895,84 USD	947,735 XMR 65.791,76 USD	1.421,602 XMR 98.687,61 USD	1.921,796 XMR 133.408,64 USD
50%	1.421,723 XMR 98.696,01 USD	2.843,447 XMR 197.392,09 USD	4.265,171 XMR 296.088,17 USD	5.765,880 XMR 400.267.38 USD
75%	4.265,171 XMR 296.088,17 USD	8.530,343 XMR 592.176,41 USD	12.795,515 XMR 888.264,65 USD	17.297,641 XMR 1.200.802,23 USD
99%	140.750,670 XMR 9.770.911,51 USD	281.501,340 XMR 19.541.823,02 USD	422.252,010 XMR 29.312.734,53 USD	570.822,161 XMR 39.626.474,41 USD

Financiamento do ataque

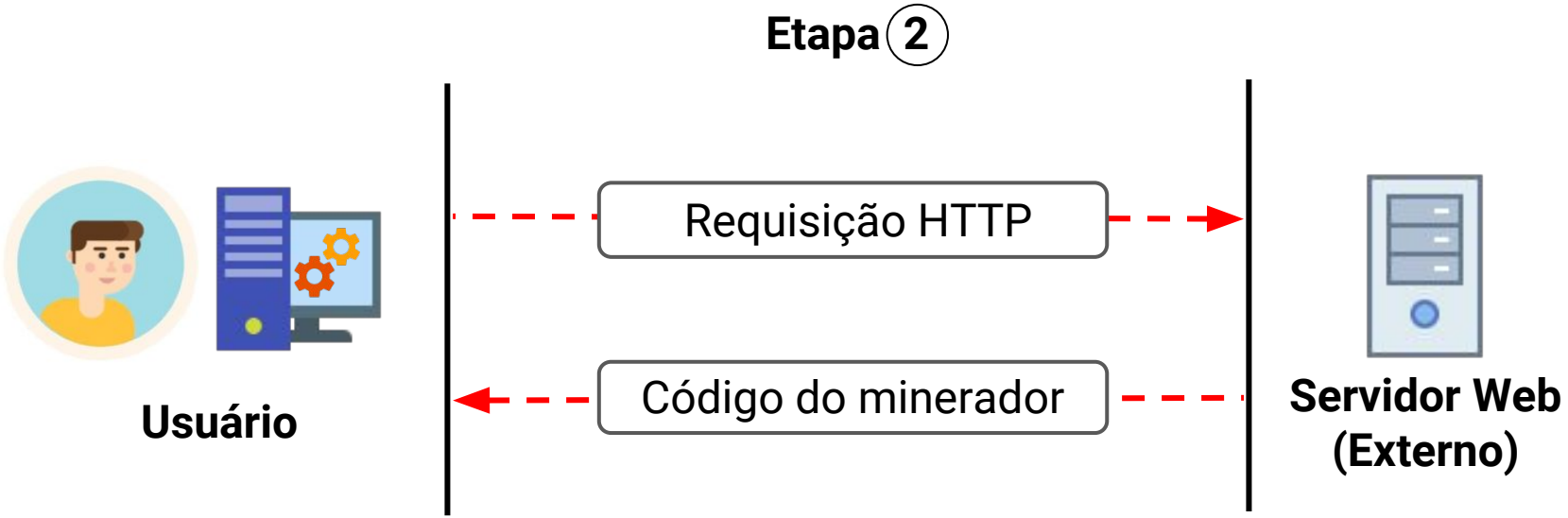
E se o atacante utilizar, concomitantemente, ataques como in-browser cryptojacking, conseguiria reduzir os custos do ataque à zero?

In-browser cryptojacking

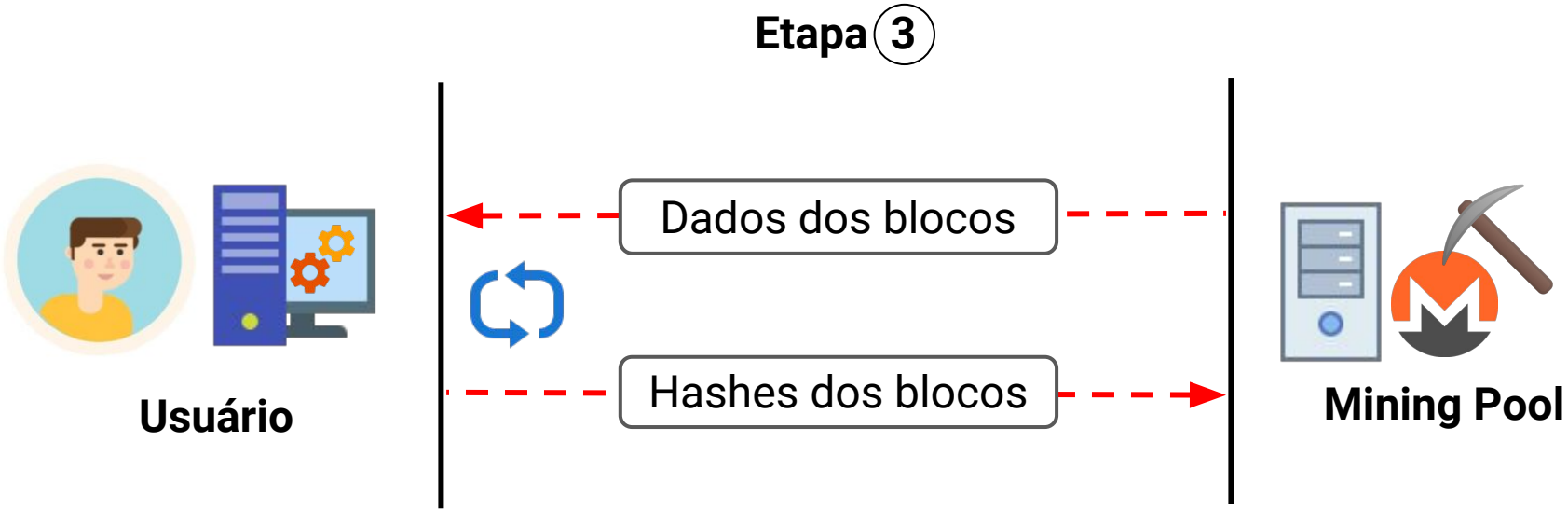
In-browser cryptojacking



In-browser cryptojacking



In-browser cryptojacking



Redução de custos

Controle do atacante	Mineradores necessários (24h/dia)
1%	7
25%	224
50%	671
75%	2.012
99%	66.375

Roteiro

Monero

Análise de rastreabilidade

O ataque proposto

Desafios de pesquisa

Considerações finais

Desafios de pesquisa

Correlacionar usuários com chaves do sistema

Investigação de chaves privadas de visualização

Investigação dos protocolos RingCT e Bulletproof

Roteiro

- Monero
- Análise de rastreabilidade
- O ataque proposto
- Desafios de pesquisa
- Considerações finais

Considerações finais

- Foram reproduzidos dois ataques existentes na literatura
- Um novo ataque foi proposto e sua viabilidade demonstrada
- Considerações sobre o desenvolvimento
- Experiências e aprendizado
- Agradecimentos

unipampa

Universidade Federal do Pampa

Obrigado!

Contato:
joaootaviors@gmail.com