Esquemas de privacidade nas moedas criptográficas Monero e Zcash

Introdução

Monero e Zcash são moedas criptográficas que permitem efetuar transações monetárias com alto nível de privacidade ao mesmo tempo que mantém um registro público de dados em um sistema distribuído sem necessidade de terceiros de confiança.

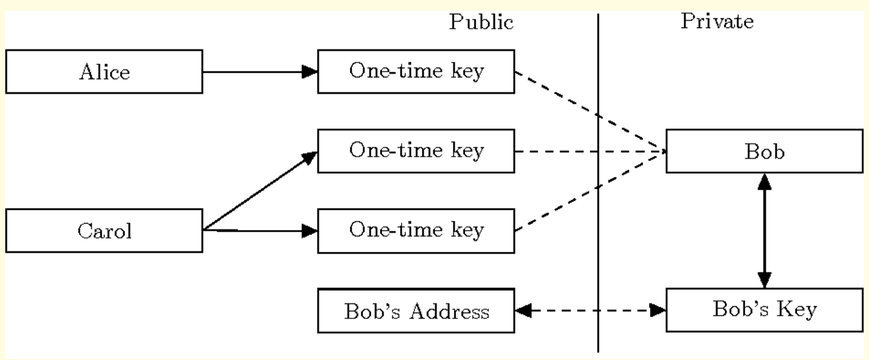
Objetivos

O objetivo deste trabalho é expor e explicar os mecanismos pelos quais estas duas moedas proporcionam privacidade aos seus usuários: os tipos de privacidade adquirida, o grau de privacidade proporcionado, o funcionamento do sistema do ponto de vista criptográfico-computacional, suas vantagens e *trade-offs*.

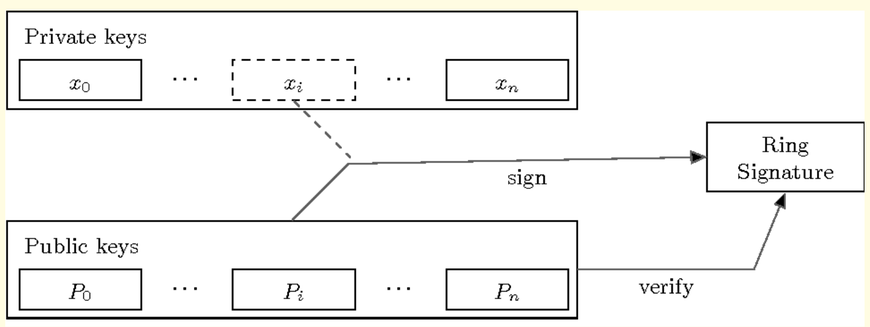
Monero

Monero usa três tecnologias principais para atingir privacidade:

- **Stealth Addresses**: geração de endereços de pagamentos únicos, na qual um endereço novo (identificador do destino do pagamento) é gerado aleatoriamente a cada transação.



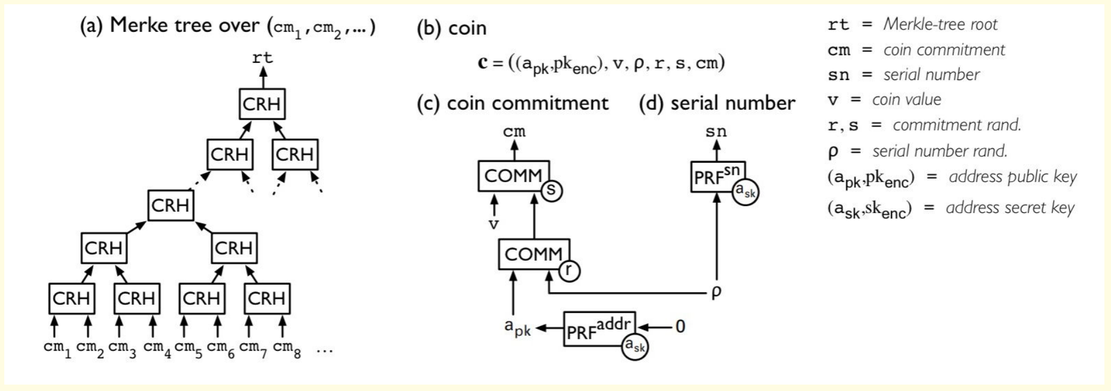
- **Ring Signatures**: assinaturas criptográficas em grupo, na qual um usuário membro de um grupo gera uma assinatura que prova que alguém do grupo gerou a assinatura de forma legítima mas sem revelar quem é esta pessoa.



- **RingCT**: transações de anéis confidenciais, que empregam *Pedersen commitments* para provar que os saldos de origem são iguais aos saldos de destino sem revelar os valores dos saldos para terceiros.

Zcash

- Moedas representas por *notas*: estrutura de dados com informações da quantia (ocultada por *commitments*) e endereço de destino.
- Cada nota possui um *commitment* e um *nulificador*, revelado somente quando gasta-se a moeda da nota.
- Assinaturas digitais garantem que a moeda está sendo gasta pelo seu proprietário atual.
- Provas *zk-SNARKs* garantem que a moeda pertence à lista de moedas não gastas, mas não se sabe qual é.
- Não é possível estabelecer vínculo entre o *nulificador* e a nota da moeda gasta devido ao *zero-knowledge*.
- *Nulificadores* de moedas gastas são armazenados em uma *árvore de Merkle* pública, prevenindo *gasto duplo*.
- Informações confidenciais encriptadas com chave do destinatário são anexadas na transação.



Comparação

Funcionalidades parecidas, tecnologias diferentes.

Funcionalidade	Monero	ZCash Sapling	Zcash Orchard
Ocultação da origem	Sim	Sim	Sim
Ocultação do destino	Sim	Sim	Sim
Ocultação da quantia	Sim	Sim	Sim
Chave de visualização	Sim	Sim	Sim
Visualização *incoming*	Não	Sim	Sim
Visualização *outgoing*	Não	Sim	Sim
Privacidade obrigatória	Sim	Não	Não

Tabela 1: *Funcionalidades de privacidade em Monero e Zcash*

	Monero	ZCash Sapling	Zcash Orchard
Endereço de pagamento	Stealth Addresses	Diversified Addresses	Diversified Addresses
Ocultação do destino	Stealth Addresses	Encriptação de dados	Encriptação de dados
Ocultação da quantia	Pedersen commitments	Encriptação de dados	Encriptação de dados
Ocultação da origem	Ring Signatures	Groth16 zk-SNARKs	Halo2 zk-SNARKs
Preservação de balança	Pedersen commitments	Pedersen commitments	Sinsemilla commitments
Curva Elíptica	Twisted Edwards Ed25519	JubJub e BLS12-381	Pallas e Vesta
Família de hashing	SHA-3	SHA-2, BLAKE2 e BLAKE2b	SHA-2, BLAKE2, BLAKE2b

Tabela 2: *Tecnologias criptográficas em Monero e Zcash*

Ambos têm tempo de processamento de transação na ordem de milissegundos e tamanho em *kilobytes*.

Bibliografia

- Hopwood, Daira et al. (2022). *Zcash Protocol Specification*.
- Noether, Sarang et al. (2020). *Zero to Monero*. 2ª ed.
- Saberhagen, Nicolas van (2013). *CryptoNote V2.0*.
- Sasson, Eli Ben et al. (2014). *Zerocash: Decentralized anonymous payments from bitcoin*.

André Souza Abreu

Orientador: Routo Terada

Departamento de Ciência da Computação — Universidade de São Paulo