



Fórum Drex

Terceira Plenária

07 de dezembro de 2023



Andamento do Piloto Drex

- Real Digital (CBDC) e Real Tokenizado (DVt e MEt)
- Título Público Federal (TPFt)
- Atualizações Tecnológicas
- Cronograma



Real Digital (CBDC) e Real Tokenizado (DVt e MEt)

Real Digital (CBDC) e Real Tokenizado (DVt e MEt)

Fluxo		Qtde de execuções	Qtde de Participantes
Cadastro de carteiras	Cadastrar carteira default de CBDC	16	16
	Cadastrar carteira adicional CBDC	559	9
	Descadastrar carteira adicional CBDC	44	2
	Cadastrar carteira de clientes (DVt ou MEt)	949	13
	Descadastrar carteira de clientes (DVt ou MEt)	2	2
CBDC	Emitir CBDC a partir de RB ou CL	420	16
	Transferência de CBDC para outra instituição	449	16
	Conversão de CBDC de volta para RB/CL	131	15
DVt ou MEt	Emissão de DVt ou MEt, de forma descentralizada	1.912	13
	Transferência, em DVt ou MEt, entre clientes da mesma instituição	289	13
	Transferência, em DVt ou MEt, para cliente de outra instituição	1.626	13
	Conversão de DVt ou MEt de volta para BRL	1.730	7

Título Público Federal (TPFt)

Título Público Federal tokenizado (TPFt)

- ✓ Ativo fungível, identificado pelo seu código e data vencimento. Exemplo: 100000 (LTN) - 21/11/2023.

Fluxos de negócio já disponíveis:

- ✓ Operação 1001 - Emissão.
- ✓ Operação 1070 - Colocação direta.
- ✓ Operação 1002 - Liquidação de oferta pública.
- ✓ Operação 1052 - Compra e venda entre participantes.
- ✓ Operação 1052 – Compra e venda envolvendo clientes.

Fluxos de negócio a serem disponibilizados em dezembro:

- ✓ Operação 1012 – Resgate

Título Público Federal (TPFt)

Fluxo		Qtde de execuções	Qtde de Participantes
TPFt	Liquidação de oferta pública (mercado primário)	33	14
	Compra e venda entre participantes (mercado secundário)	43	15
	Compra e venda envolvendo clientes (mercado secundário)	212	12

Atualizações Tecnológicas



Revisão

- ✓ Voto 31/2023 estabelece as diretrizes do DREX e do Piloto

https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/voto_bcb_31_2023.pdf

- ✓ Plataforma DLT (*Distributed Ledger Technology*)
- ✓ Capacidade de incorporar protocolos utilizados nos ambientes DeFi
- ✓ Registro de ativos digitais de diferentes naturezas
- ✓ Descentralização no provimento de produtos e serviços
- ✓ Programabilidade e composição de serviços financeiros
- ✓ Liquidação atômica de ativos



Revisão

- ✓ Aplicação do arcabouço regulatório vigente às operações, destacando:
 - ✓ Não permitido saldo a descoberto em nenhuma transação
 - ✓ Operações finais e irrevogáveis
 - ✓ Governança das autoridades sobre seus respectivos ativos
- ✓ Observância aos requisitos legais de sigilo e de privacidade de indivíduos e demais envolvidos



Trilema

Equilibrando descentralização,
privacidade e programabilidade

Revisão

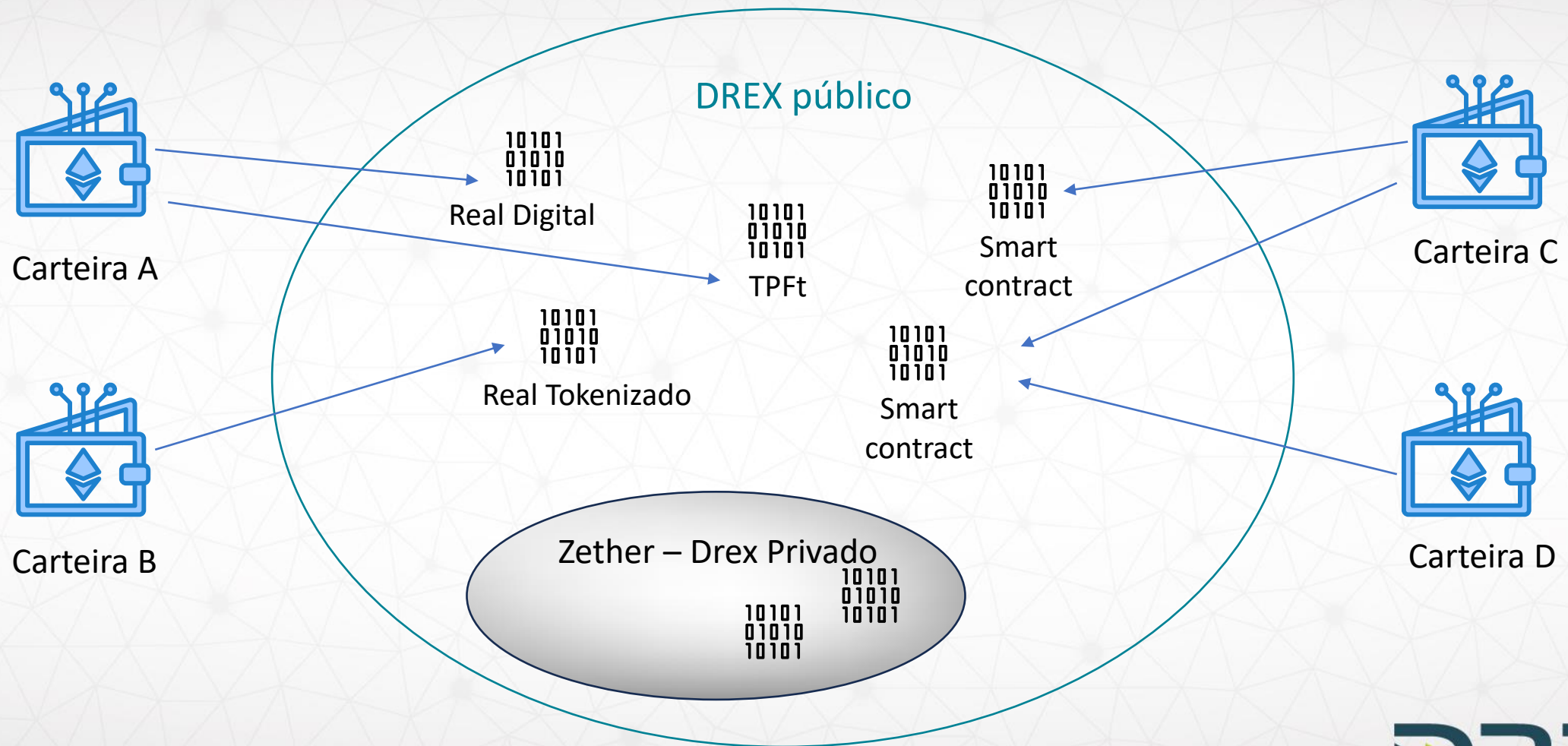
- ✓ Saldos são conhecidos pelo dono da carteira e pela autoridade do ativo
- ✓ Dados das transações são conhecidos pelas contrapartes (pagador e recebedor ou vendedor e comprador) e pelas autoridades dos ativos envolvidos

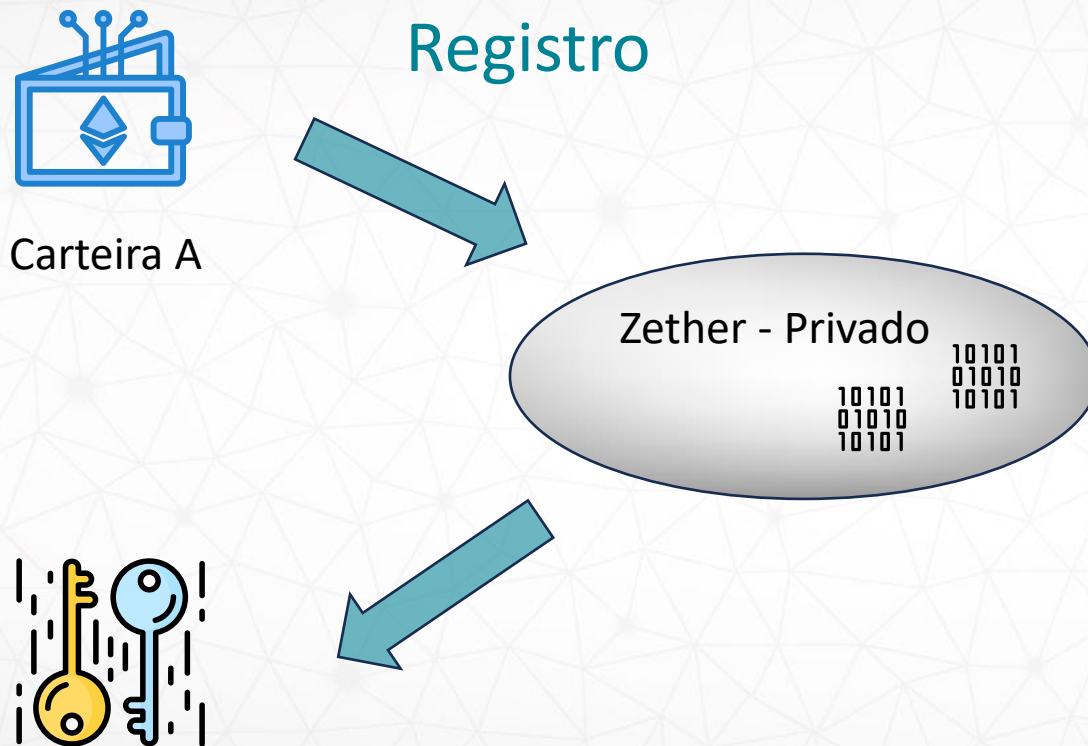
- ✓ Baseado no paper “Zether - Towards Privacy in a Smart Contract World”
- ✓ Implementação em EVM mantida pela Consensys
- ✓ Repositório a ser utilizado:

([GitHub - kaleido-io/anonymous-zether-client](https://github.com/kaleido-io/anonymous-zether-client) at real-digital)

- ✓ Privacidade e anonimidade em redes Ethereum utilizando:
 - ✓ Criptografia homomórfica (ElGamal)
 - ✓ Prova de conhecimento zero
 - ✓ *Anonymity set*

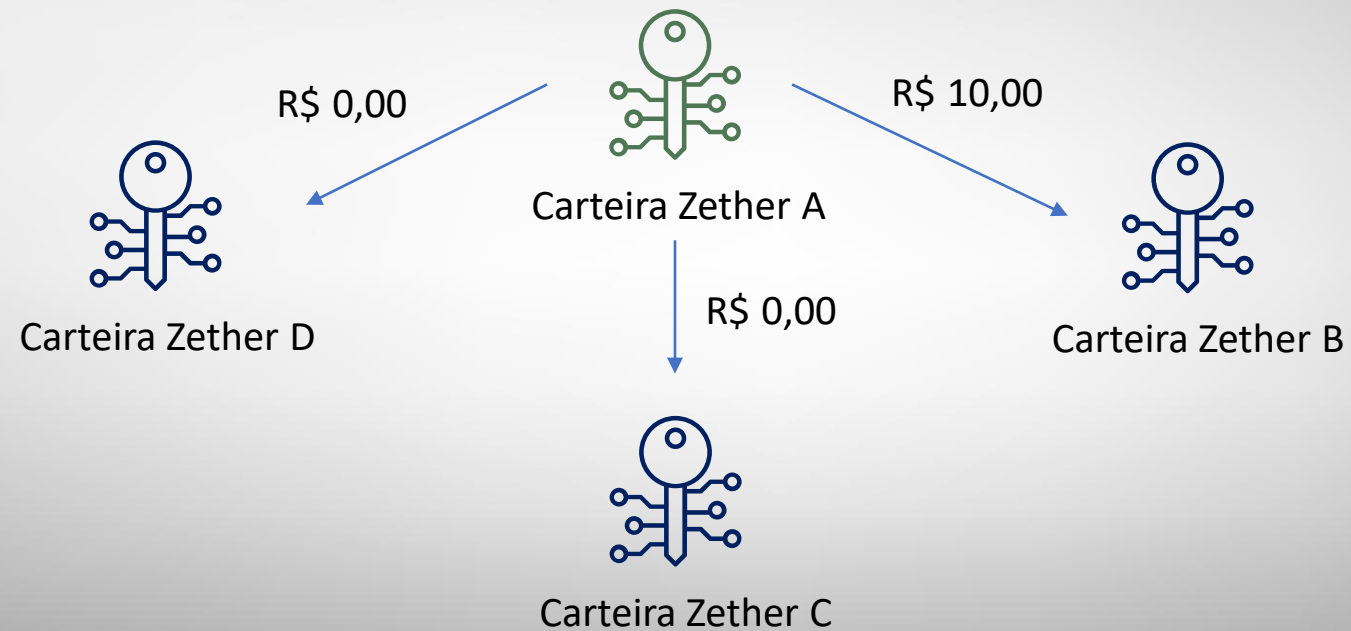
Anonymous Zether





- ✓ Primeiro passo: Registro da carteira para obter par de chaves Zether
- ✓ Ativos para serem transacionados no mundo privado são transferidos para dentro de um contrato Zether (*fund*)
- ✓ Toda interação com os contratos Zether são feitos através das chaves fornecidas

Cenário: A transfere R\$ 10,00 para B



Transação

 Anonimity Set	 Operações	 Zero Knowledge Proof
Carteira Zether A Carteira Zether B Carteira Zether C Carteira Zether D	1. Débito de R\$ 10,00 na carteira A – criptografado com chave A 2. Crédito de 10,00 na carteira B – criptografado com chave B 3. Crédito de 0,00 na carteira C – criptografado com chave C 4. Crédito de 0,00 na carteira D – criptografado com chave D	Garante o saldo inicial do debitado, e que o valor debitado seja igual à soma dos valores creditados



ANONIMIDADE



PRIVACIDADE



VISIBILIDADE AUTORIDADE

Público



Época

- ✓ Intervalo de tempo definido para cada contrato Zether em que uma prova deve ser gerada e validada
- ✓ Apenas uma operação de débito pode ocorrer por carteira dentro de uma época
- ✓ As operações de crédito ficam pendentes e, ao fim da época, são adicionadas ao saldo

Testes

- ✓ Testes com participantes iniciados em 27/11

Fluxo	Época
Transferência de Real Digital	6 segundos
DVP entre TPFT e Real Digital	60 segundos

Status atual

- ✓ Anonymous Zether
 - ✓ Testes com participantes iniciados em 27/11
- ✓ Starlight
 - ✓ Iniciada implementação de transferência de Real Digital
- ✓ Parchain
 - ✓ Em discussões técnicas com mantenedor



BANCO CENTRAL DO BRASIL

Obrigado!

07/12/2023

