



Piloto da Drex: *Títulos Públicos Federais, Real Digital e Real Tokenizado, Depósitos Tokenizados*

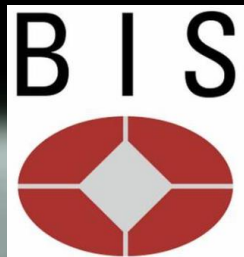
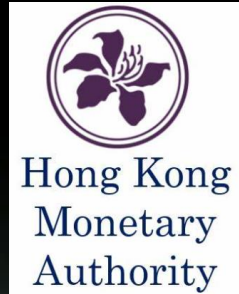
1 - Privacidade e confidencialidade para “troca atômica: compra e pagamento” entre Títulos Públicos Federais e DREX de *Atacado (Real Digital)*

2 - Privacidade e confidencialidade para “troca atômica: compra e pagamento” entre Títulos Públicos Federais e DREX de *Varejo (Real Tokenizado)*

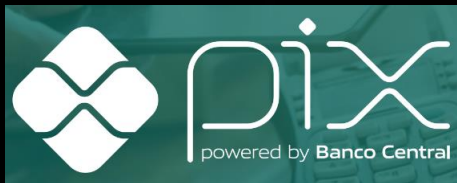




c·rdac·n



Block
chain
.RIO



PhD. João Paulo Aragão Pereira (Inteligência Artificial - IA)
Especialista Sênior em Tecnologia e Inovação para FSI na Microsoft
Consultor focado em IA, Web3, DeFi e CBDC - Especialista em Bancos e Pagamentos
Pesquisador, Professor AI/ML, Orientador, Candidato a Pós-Doutorado em Sistema Multiagentes e Quantum IA



Criptomoeda vs CBDC (*Central Bank Digital Currency* – *Moeda Digital Emitida pelo Banco Central*)



As **criptomoedas** não têm uma autoridade central emissora ou reguladora, dependendo de um sistema descentralizado para registrar transações e produzir novas unidades.

Criptomoeda vs CBDC (*Central Bank Digital Currency* – *Moeda Digital Emitida pelo Banco Central*)



As **criptomoedas** não têm uma autoridade central emissora ou reguladora, dependendo de um sistema descentralizado para registrar transações e produzir novas unidades.



Stablecoins são criptomoedas que são lastreadas por outros ativos, como dólares, euros e ouro, tudo com o objetivo de dar a eles valor estável e reduzir a volatilidade, até mesmo café, etc...

Criptomoeda vs CBDC (*Central Bank Digital Currency* – *Moeda Digital Emitida pelo Banco Central*)

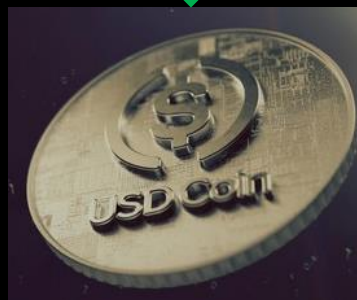


As **criptomoedas** não têm uma autoridade central emissora ou reguladora, dependendo de um sistema descentralizado para registrar transações e produzir novas unidades.

Tem similaridades como imutável e podem usar uma blockchain/DLT



Por outro lado, a **CBDC** é uma forma digital de dinheiro do banco central que é amplamente utilizada pelo público. Por exemplo, estende as funcionalidades do Real.



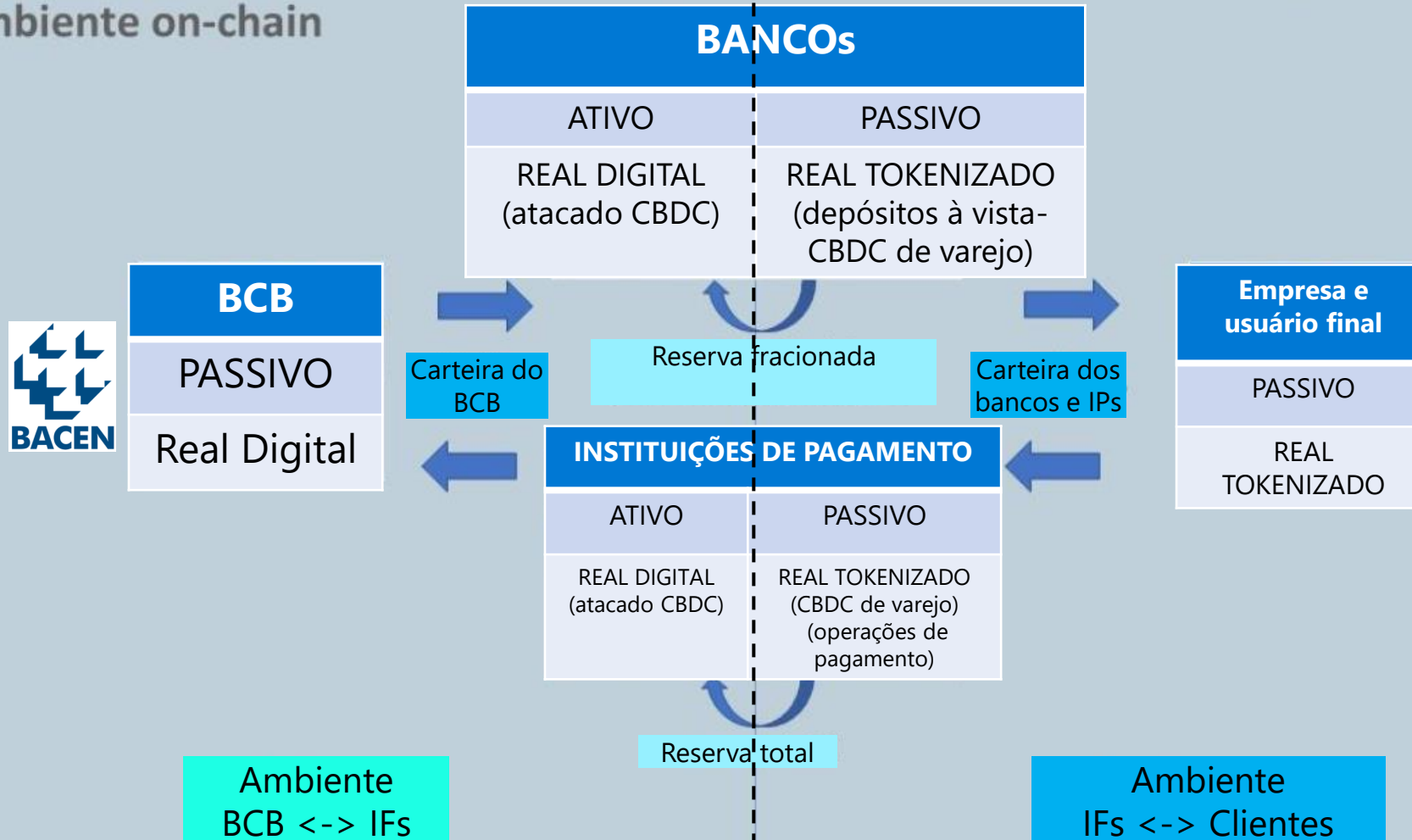
Stablecoins são criptomoedas que são lastreadas por outros ativos, como dólares, euros e ouro, tudo com o objetivo de dar a eles valor estável e reduzir a volatilidade, até mesmo café, etc...



Plataforma DREX (Varejo e Atacado baseado em Depósitos Tokenizados)

Tokenização de depósitos

Ambiente on-chain



Plataforma DREX (Varejo e Atacado baseado em Depósitos Tokenizados)

Tokenização de depósitos

Ambiente on-chain

REAL
DIGITAL
(ATACADO)



BCB

PASSIVO

Real Digital

Confidencial +
privado



Ambiente
BCB <-> IFs

BANCOS

ATIVO

REAL DIGITAL
(atacado CBDC)

PASSIVO

REAL TOKENIZADO
(depósitos à vista-
CBDC de varejo)

Carteira do
BCB

Reserva fracionada

Carteira dos
bancos e IPs

INSTITUIÇÕES DE PAGAMENTO

ATIVO

REAL DIGITAL
(atacado CBDC)

PASSIVO

REAL TOKENIZADO
(CBDC de varejo)
(operações de
pagamento)

Reserva total

Empresa e
usuário final

PASSIVO

REAL
TOKENIZADO

Ambiente
IFs <-> Clientes

Plataforma DREX (Varejo e Atacado baseado em Depósitos Tokenizados)

Tokenização de depósitos

Ambiente on-chain

REAL
DIGITAL
(ATACADO)

REAL
TOKENIZADO
(VAREJO)



BCB

PASSIVO

Real Digital

Confidencial +
privado



Ambiente
BCB <-> IFs

BANCOS

ATIVO

REAL DIGITAL
(atacado CBDC)

PASSIVO

REAL TOKENIZADO
(depósitos à vista-
CBDC de varejo)

Confidencial +
privado



Empresa e
usuário final

PASSIVO

REAL
TOKENIZADO

Confidencial +
privado



Ambiente
IFs <-> Clientes

INSTITUIÇÕES DE PAGAMENTO

ATIVO

REAL DIGITAL
(atacado CBDC)

PASSIVO

REAL TOKENIZADO
(CBDC de varejo)
(operações de
pagamento)

Reserva total

Carteira do
BCB

Reserva fracionada

Carteira dos
bancos e IPs



Microsoft

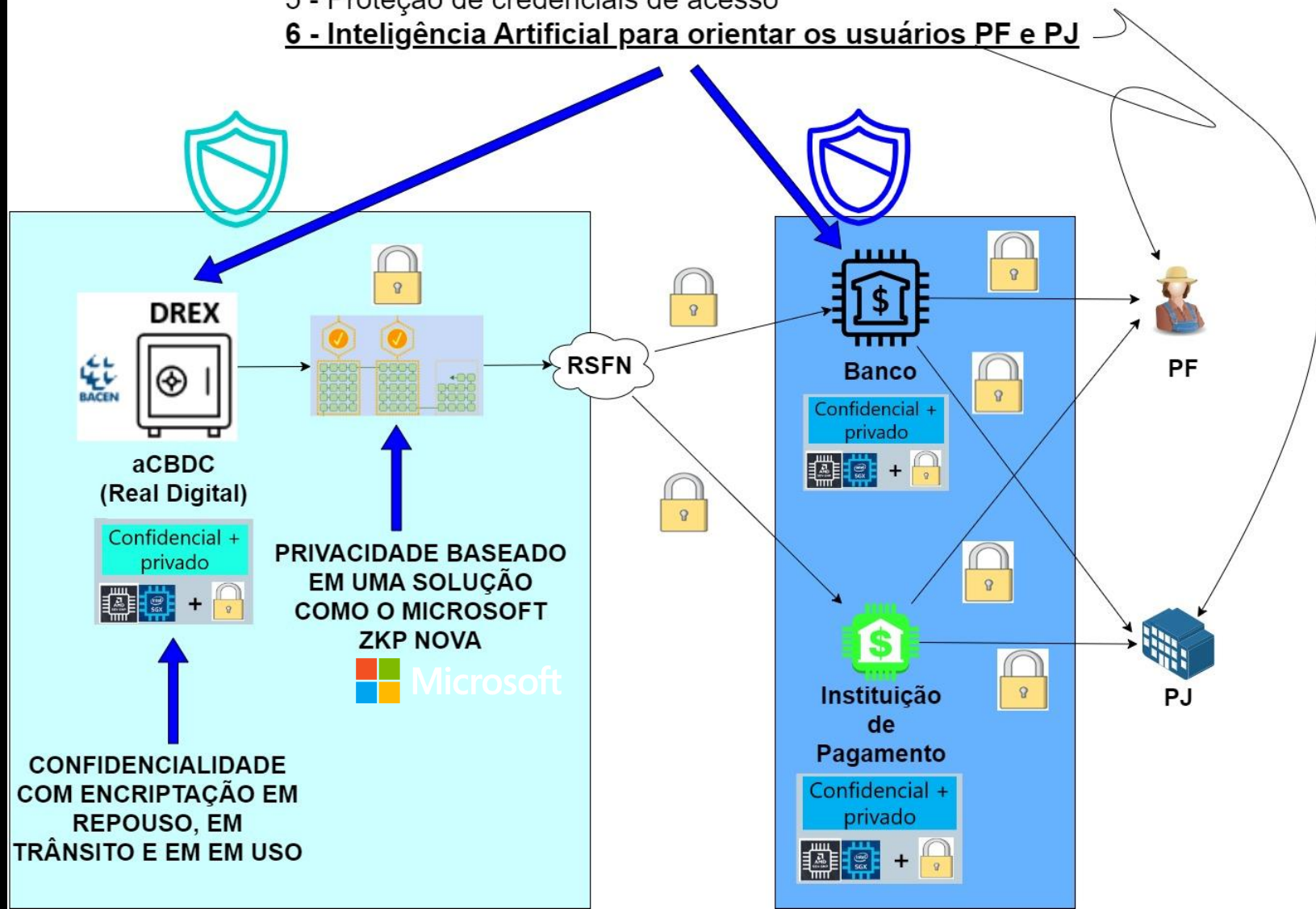
Plataforma DREX com Escudo de Confiança

16 (no piloto) -> +500
instituições financeiras do
Brasil

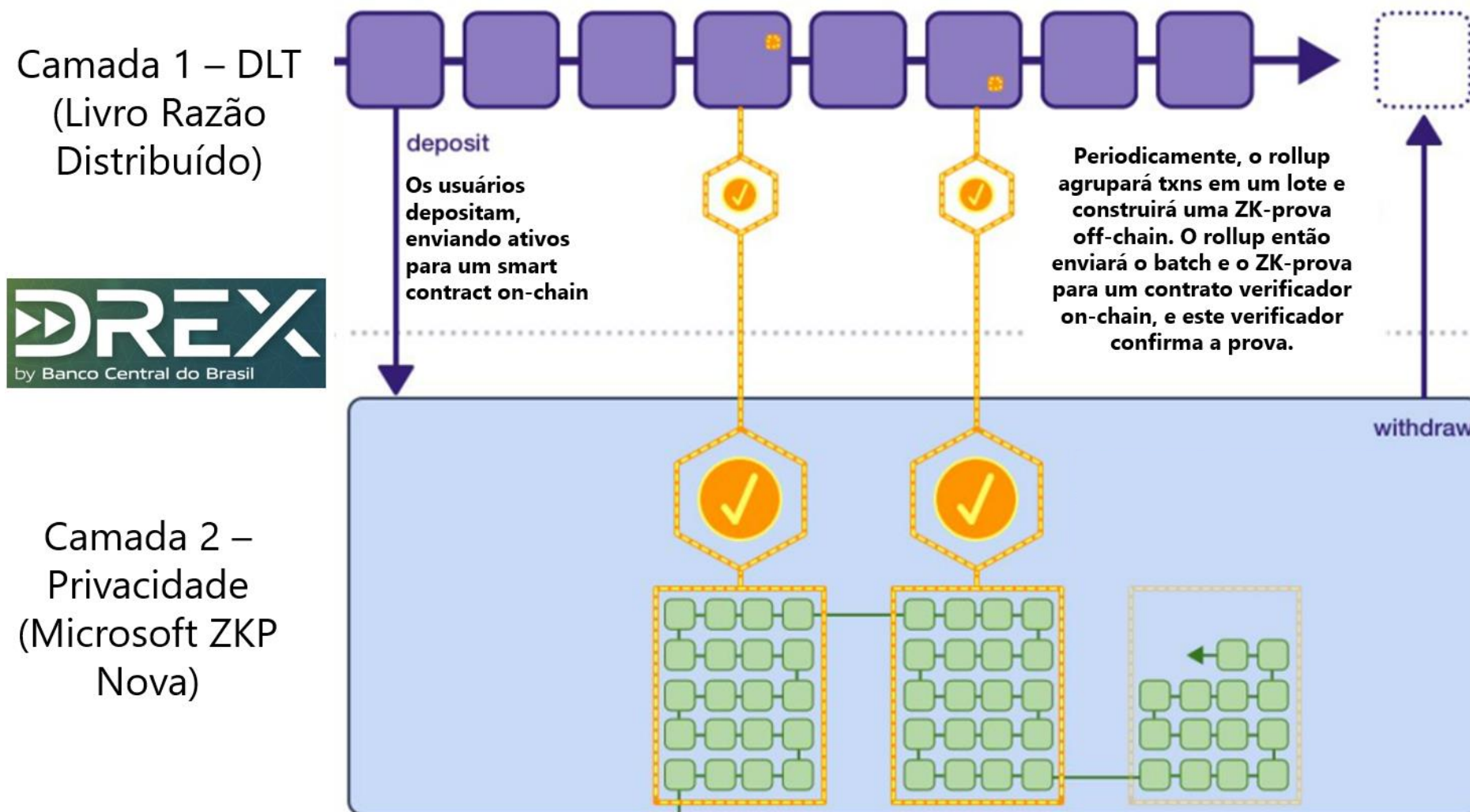
*Informações sensíveis, como
saldo, valor, origem e destino
são e podem ser privadas*

FORMAÇÃO DO ESCUDO DE CONFIANÇA:

- 1 - "Fragmentação" da chave privada em diferentes locais.
- 2 - Criptografia pos-quântica
- 3 - Identidade Digital baseado em blockchain/DLT + lastro digital
- 4 - Antifraude e AML on-chain e off-chain, baseado em Inteligência Artificial
- 5 - Proteção de credenciais de acesso
- 6 - Inteligência Artificial para orientar os usuários PF e PJ

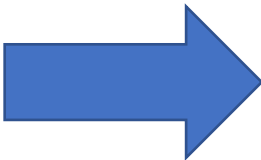


Plataforma Drex com privacidade (Microsoft ZKP Nova)



- **Trilema BACEN:** **privacidade (saldo e transações), programabilidade e descentralização**
- **Granularidade na visibilidade:** **BCB, outros reguladores, ou bancos ou ambos**

Análise da viabilidade de aplicação de métodos de criptografia pós-quântica aplicados ao sistema de pagamentos instantâneos brasileiro (Pix)



Métodos Resistentes a futuros e possíveis ataques quânticos
trabalho proativo

Authors



Partner



Supporter



[quantum-cryptography-pix-en.pdf \(fenasbac.com.br\)](https://fenasbac.com.br/quantum-cryptography-pix-en.pdf)

Selected Algorithms: Digital Signature Algorithms

Algorithm	Algorithm Information	Submitters
CRYSTALS-DILITHIUM	Zip File (11MB)	Vadim Lyubashevsky
	IP Statements	Leo Ducas
	Website	Eike Kiltz
		Tancrede Lepoint
FALCON		Peter Schwabe
		Gregor Seiler
		Damien Stehle
		Shi Bai
	Zip File (4MB)	Thomas Prest
	IP Statements	Pierre-Alain Fouque
	Website	Jeffrey Hoffstein
SPHINCS+		Paul Kirchner
		Vadim Lyubashevsky
		Thomas Pornin
		Thomas Ricosset
		Gregor Seiler
		William Whyte
		Zhenfei Zhang
	Zip File (230MB)	Andreas Hulsing
	IP Statements	Daniel J. Bernstein
		Christoph Dobraunig



Applying Post-Quantum Cryptography Algorithms to a DLT-Based CBDC Infrastructure: Comparative and Feasibility Analysis

Segurança e privacidade para novas fontes de receita e ativos tokenizáveis

Ativos do mundo real e Financeiros - Criptoeconomia

ENERGIA (METANO, EXCEDENTE) E MINÉRIOS

**IMÓVEIS, HABITAÇÃO, PLANO EMPRESÁRIO,
TERRAS, TERRENOS, VEÍCULOS**

**PRECATÓRIOS, DEBÊNTURES, RENDA FIXA,
CERTIFICADOS: CRA, FIDC, CCB, FII, CDB**

RECEBÍVEIS: BOLETOS, CARTÃO DE CRÉDITO

GADO COM TELEMETRIA

**CRÉDITO DE CARBONO (ESCOPO 4) +
EMPRÉSTIMOS VERDES**

**CROWDFUNDING E EMPRÉSTIMOS COM
GARANTIA**

PAGAMENTOS OFFLINE

VIAGEM, BAGAGEM E ASSENTOS

HUB DE INGRESSOS E JOGADORES DE FUTEBOL

ALUGUEL E RESERVAS DE HOTEL

CELULAR E SALDO DA CONTA

**COMMODITIES AGRÍCOLAS: CAFÉ, SOJA – TRADE
FINANCE**

DADOS E CASH-BACK, IMPOSTOS

**RECOMPENSAS – FIDELIDADE – MOEDA
BANCÁRIA – BENEFÍCIOS SOCIAIS**

VINHO

Obrigado!

