



Desvendando os segredos da Blockchain



Agenda

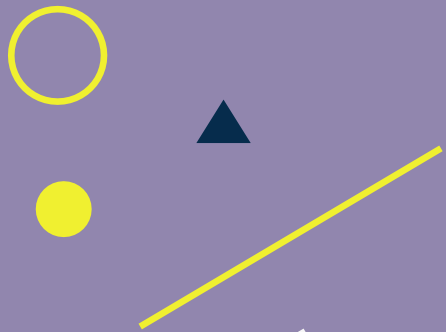
- Blockchain
- Smart Contracts
- Tokens: Criptoativos e NFTs
- Token Design
- Criptomoeda, Stablecoins e CBDCs
- Piloto Real Digital
- Hype Cycle Gartner
- Blockchain no BB



Contextualizando Bitcoin e Blockchain

Bitcoin é uma criptomoeda dentre outras existentes.

Blockchain é a estrutura necessária para o armazenamento das transações com as criptomoedas.



Blockchain Explorer

<https://www.blockchain.com/pt/explorer>

Bitcoin Bloco 793.794

Minado em June 10, 2023 09:14:31 • [Ver todos os Blocos](#)

Unknown

Coinbase Message • hd/Foundry USA Pool #dropgold/1YZ

Um total de 17.112,47 BTC (\$441.612.357) foram enviados no bloco, com uma transação média equivalente a 7,4402 BTC (\$180.645). Unknown ganhou uma recompensa total de 6,25 BTC {fiatsymbol}154.838. A recompensa consistia numa recompensa base de 6,25 BTC \$154.838 com uma taxa adicional 0,1938 BTC (\$0.00) recompensa paga como taxas 2.300 das transações que foram incluídas no bloco.

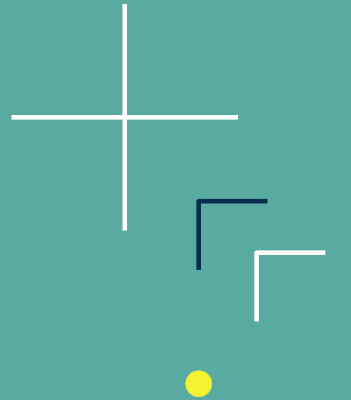
Detalhes

Hash	00000-a274d	Profundidade	2
Capacidade	170.14%	Tamanho	1.784.068
Distância	29m 57s	Versão	0x313ce000
BTC	17.112,4666	Raiz Merkle	23-b4
Valor	\$441.612.357	Dificuldade	51.234.338.863.442,89
Valor hoje	\$441.386.472	Nonce	52.477.811
Valor médio	7,4402028884 BTC	Bits	386.236.009
Valor mediano	0.00098973 BTC	Peso	3.992.641 WU
Valor de entrada	17.112,66 BTC	Cunhado	6,25 BTC
Valor de saída	17.118,91 BTC	Reward	6.44380848 BTC
Transações	2.300	Minado em	10 de jun. de 2023 21:14:31

	0 ID: 0383-d4d2 10/6/2023 21:14:31	De Recompensa de ... Para 2 Outputs	6.44380848 BTC • \$166.291 Comissão 0 Sats • \$0.00	▼
	1 ID: b3b2-eaba 10/6/2023 21:08:30	De bc1q-9aw6 Para bc1q-9aw6	0.01816565 BTC • \$468,79 Comissão 34.2K Sats • \$8,84	▼
	2 ID: d7c8-afc1 10/6/2023 21:11:51	De 3Dj5-vg4v Para 2 Outputs	0.01716131 BTC • \$442,87 Comissão 49.6K Sats • \$12,79	▼
	3 ID: 1039-6839 10/6/2023 21:07:59	De 3NVX-5rZH Para bc1q-rc75	0.00677064 BTC • \$174,73 Comissão 22.6K Sats • \$5,83	▼
	4 ID: 61d0-3acc 10/6/2023 21:11:06	De bc1q-u9xf Para 3G2V-cWWB	0.03089208 BTC • \$797,22 Comissão 16.5K Sats • \$4,27	▼
	5 ID: b155-9505 10/6/2023 21:13:41	De 1N52-GquK Para 2 Outputs	0.03611001 BTC • \$931,87 Comissão 35.9K Sats • \$9,26	▼
	6 ID: f00c-cc68 10/6/2023 21:11:00	De 19sv-yERo Para 1K16-P...L...	0.00410003 BTC • \$105,81 Comissão 5.0K Sats • \$1,00	▼

“Ao operar como um livro de registros de transações online, o blockchain tem o potencial de revolucionar não apenas as finanças, mas toda a troca de informações em comunidades de negócios e grupos sociais.”

(Eduardo Henrique Diniz em: FGV - Emerge uma Nova Tecnologia, 2017)





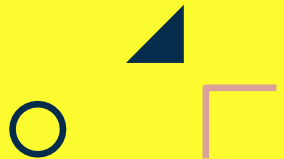
As criptomoedas
podem não ser o
futuro do dinheiro.

Mas o futuro do
dinheiro passa pelas
criptomoedas e
blockchain.





Qual problema blockchain resolve?



“Problema do gasto duplo”

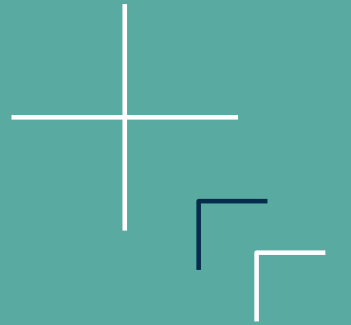
(Don Tapscot em: Blockchain Revolution)



Função Hash

A função Hash é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo.

Por esse motivo, as funções Hash são conhecidas por resumirem o dado.



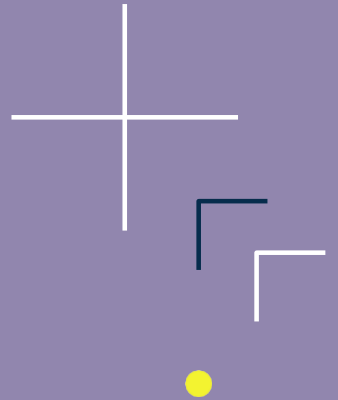
Exemplo: padrão SHA-256

Texto: blockchain e criptoativos

Hash: 168c422f257fed49a0c64e87878798e0e2f7e50d7f6c49127d7cf1166a0ff35e

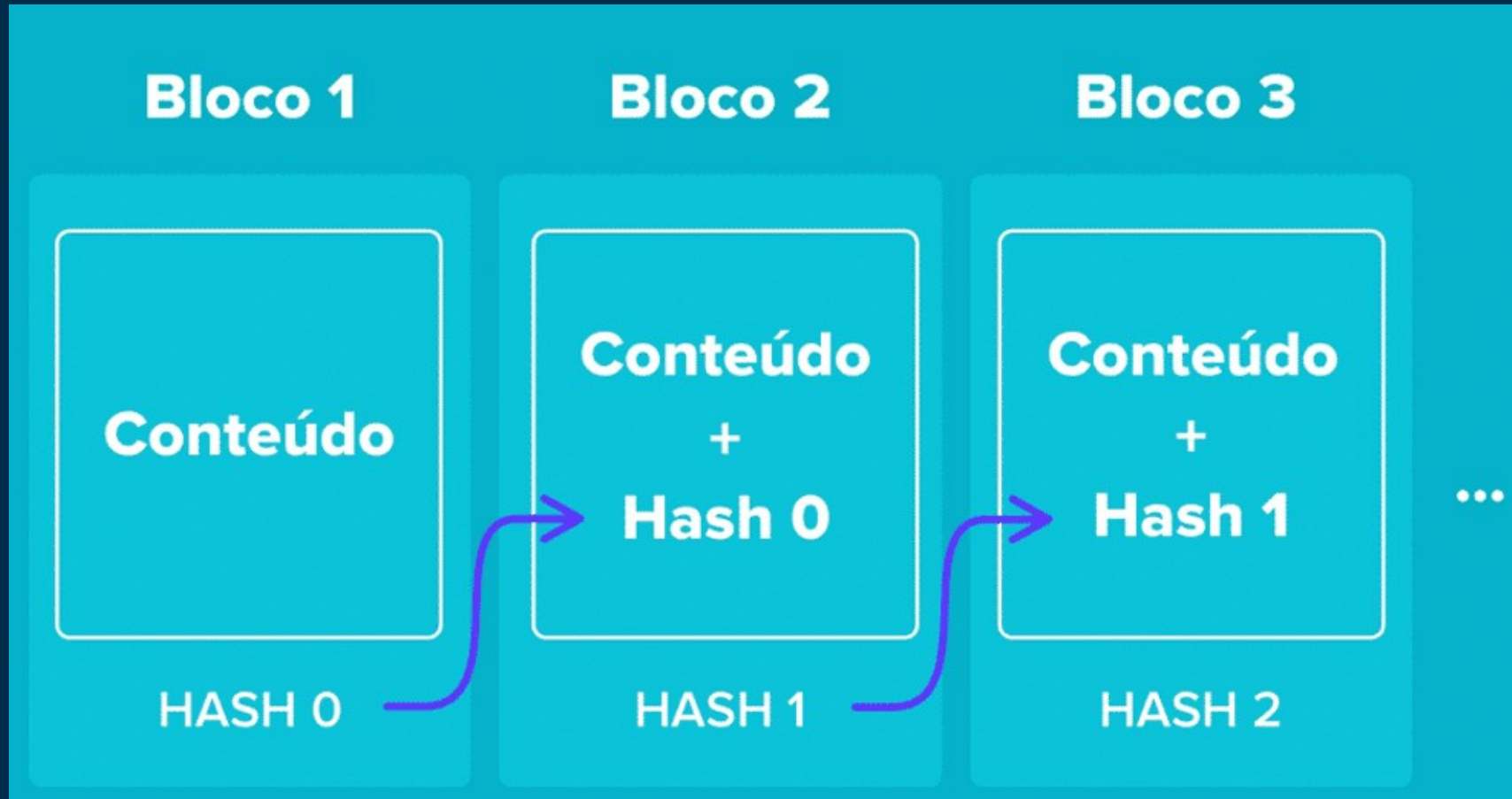
Texto: blockchain criptoativos

Hash: aff48dcadc9449259792cfaaf17351f7b0004b67e4a40e148aab699217330d76

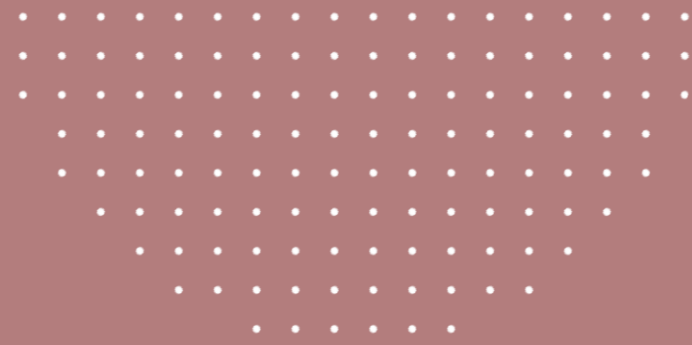


Fonte: <https://emn178.github.io/online-tools/sha256.html>

Encadeamento dos blocos



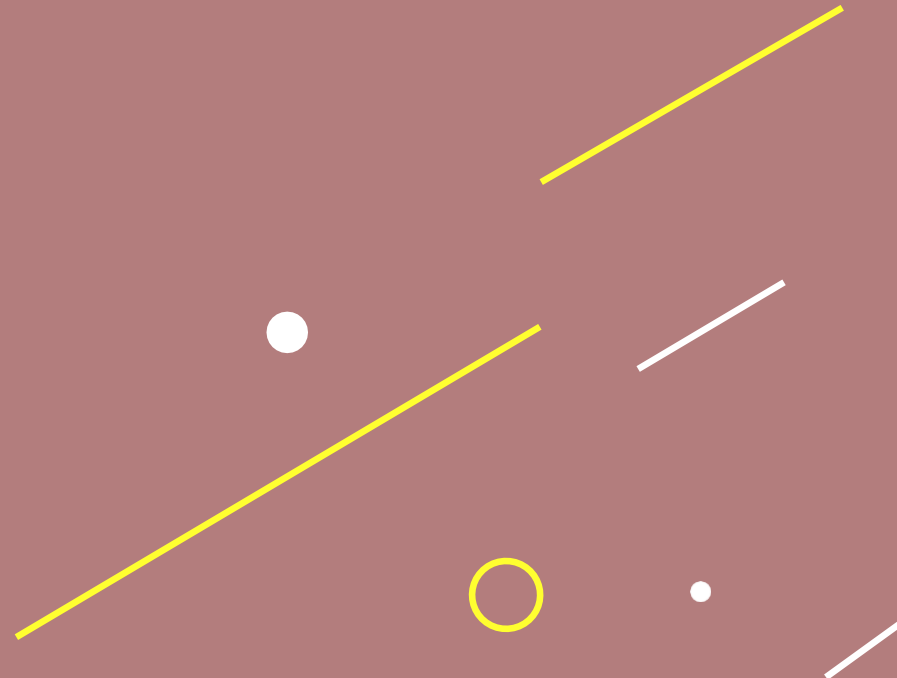
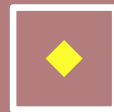
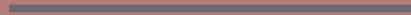
Fonte: <https://passeracademy.com.br/como-funciona-a-blockchain-do-bitcoin>



○   **O que é Blockchain?**

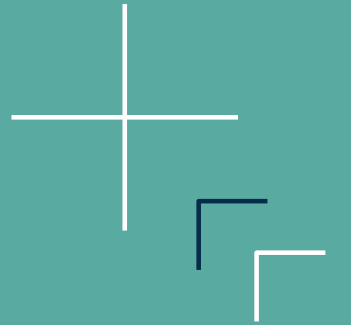
Corrente de Blocos

Conhecido como
protocolo de confiança

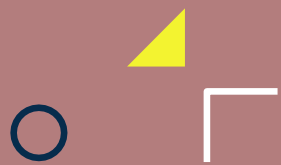


O que é Blockchain

Tecnologia que agrupa um conjunto de informações que se conectam por meio de criptografia.



Fontes: <https://coinext.com.br/o-que-e-blockchain>



Smart Contracts

Não é inteligente

Não é contrato

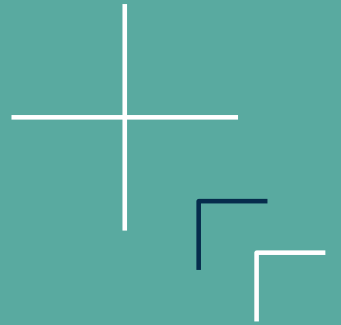
São programas de computadores

```
browser/test.sol x
1 pragma solidity ^0.4.21;
2
3 //Slight Modification to run in Remix
4 //Source: http://solidity.readthedocs.io/en/v0.3.2/solidity-by-example.html#safe-remote-purchase
5
6 contract Purchase {
7     uint public value;
8     address public seller;
9     address public buyer;
10    enum State { Created, Locked, Inactive }
11    State public state;
12
13    // Ensure that `msg.value` is an even number.
14    // Division will truncate if it is an odd number.
15    // Check via multiplication that it wasn't an odd number.
16    constructor() public payable {
17        seller = msg.sender;
18        value = msg.value / 2;
19        require((2 * value) == msg.value);
20    }
21
22    modifier condition(bool _condition) {
23        require(_condition);
24        _;
25    }
26
27    modifier onlyBuyer() {
28        require(msg.sender == buyer);
29        _;
30    }
31
32    modifier onlySeller() {
```

Definição de Smart Contract

“São programas de computador que reproduzem a lógica de um contrato, automatizam o cumprimento e a execução das regras de transferência de ativos, bem como os mecanismos de pagamento.”

(Nick Szabo)



Token

Token não é uma novidade e já existe muito antes das redes blockchain.

“Os tokens podem representar qualquer coisa, desde reserva de valor, ativos, até um conjunto de permissões no mundo físico, digital e jurídico.”

(Shermin Voshmgir, Token Economy)



Fonte: <https://livecoins.com.br/tokens-fungiveis-e-tokens-infungiveis/>

Tipos de *tokens*



1

Payment tokens

Têm como finalidade serem um meio de pagamento. Exemplos: Bitcoin, Stablecoin e CBDC.



2

Utility tokens

Exemplos: programas de fidelidade, cupons, benefícios para um determinado grupo de usuários, direito de voto etc.



3

Security tokens

Representam investimentos, uma parte de um empreendimento, uma participação em um projeto.



4

Non-fungible tokens

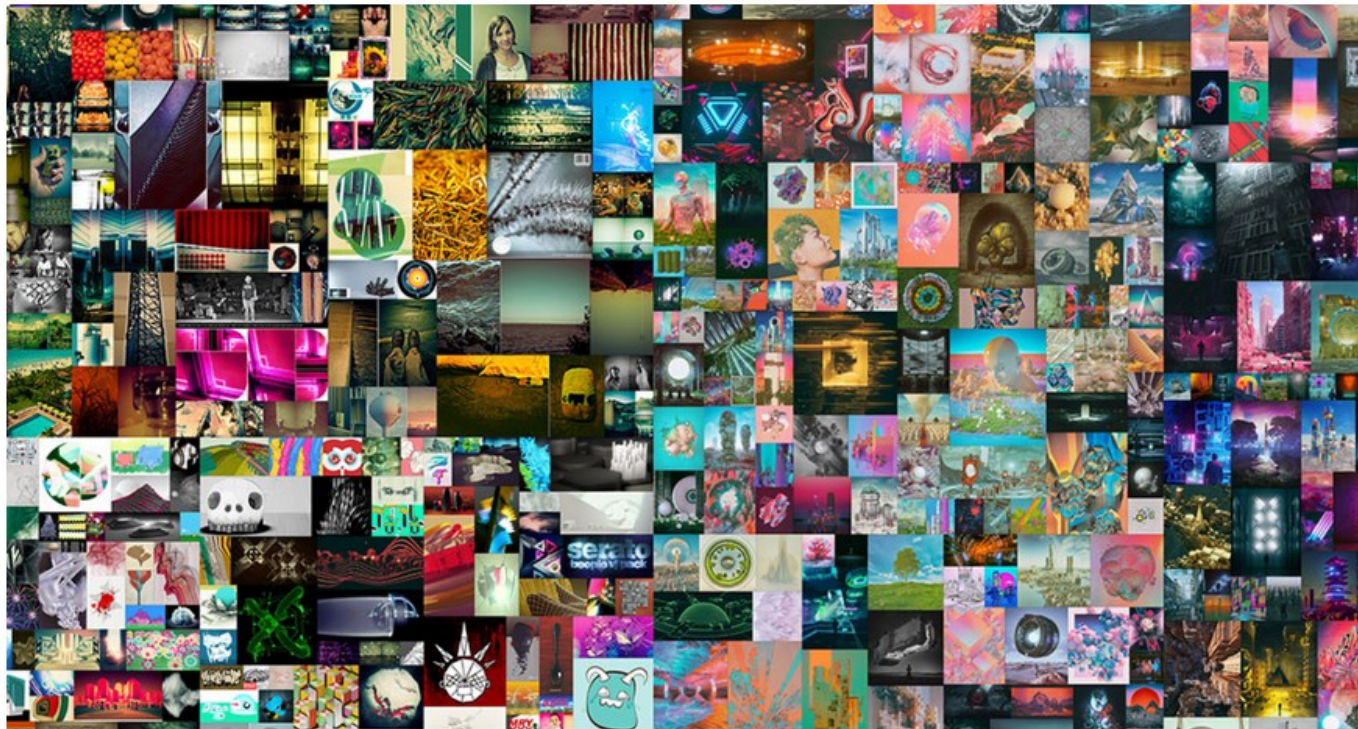
São únicos e não podem ser trocados pois funcionam como um certificado de autenticidade para alguma coisa.

NFT – Bored Ape Yach Club



Fonte: <https://images.app.goo.gl/GEWuf1ueNinb1dde7>

NFT – Everyday's – The First 5000 Days

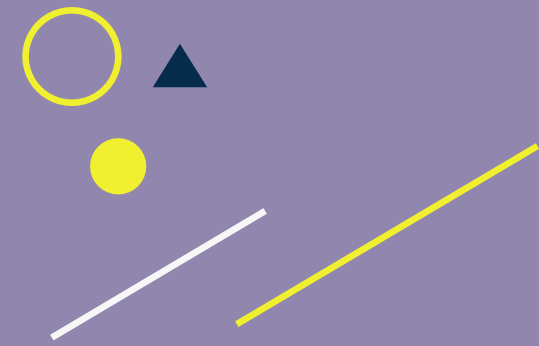


Beeple's \$70 million magnum opus "EVERYDAYS: THE FIRST 5000 DAYS" (Photo: Christie's)

CRYPTOCURRENCIES, TECHNOLOGY

Beeple's NFT collage EVERYDAYS sells for nearly \$70M at Christie's

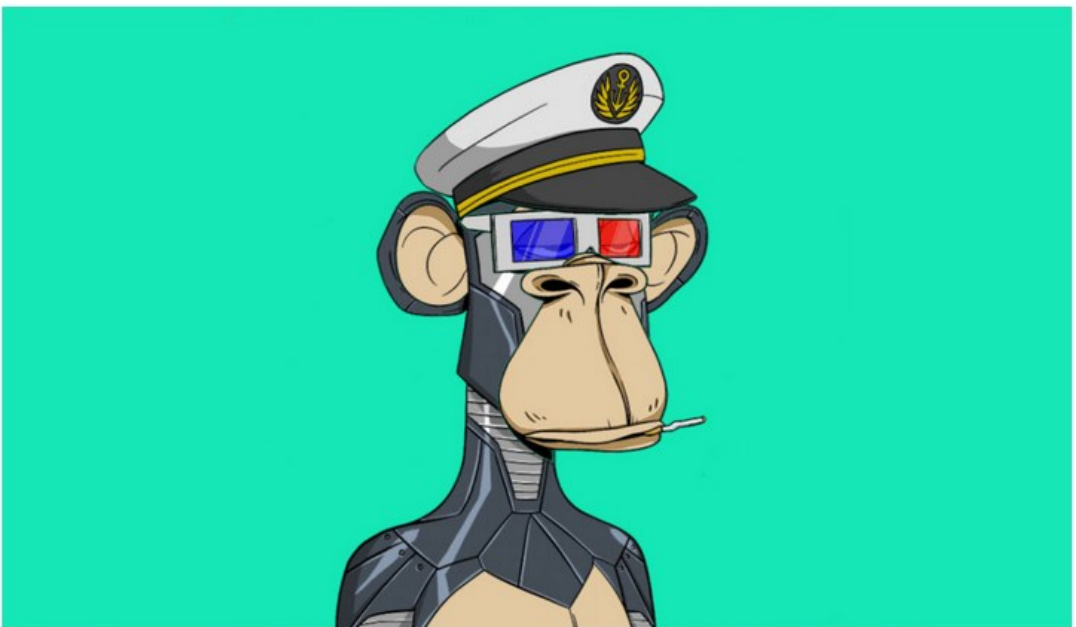
Falhas em projetos



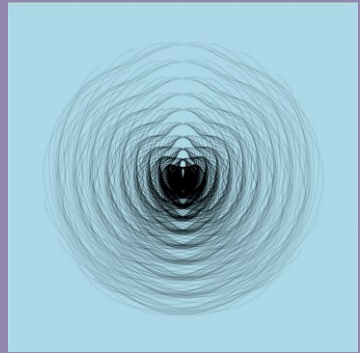
ISTOE Dinheiro

Finanças

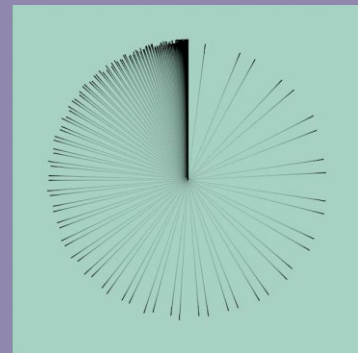
Falha em plataforma faz hacker comprar NFT por 83% a menos



Coleção Bored Ape Yacht Club é uma das mais famosas do mundo (Crédito: Reprodução/Bored Ape Yatch Club)



Rarible



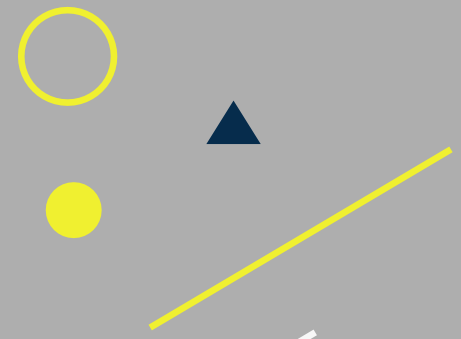
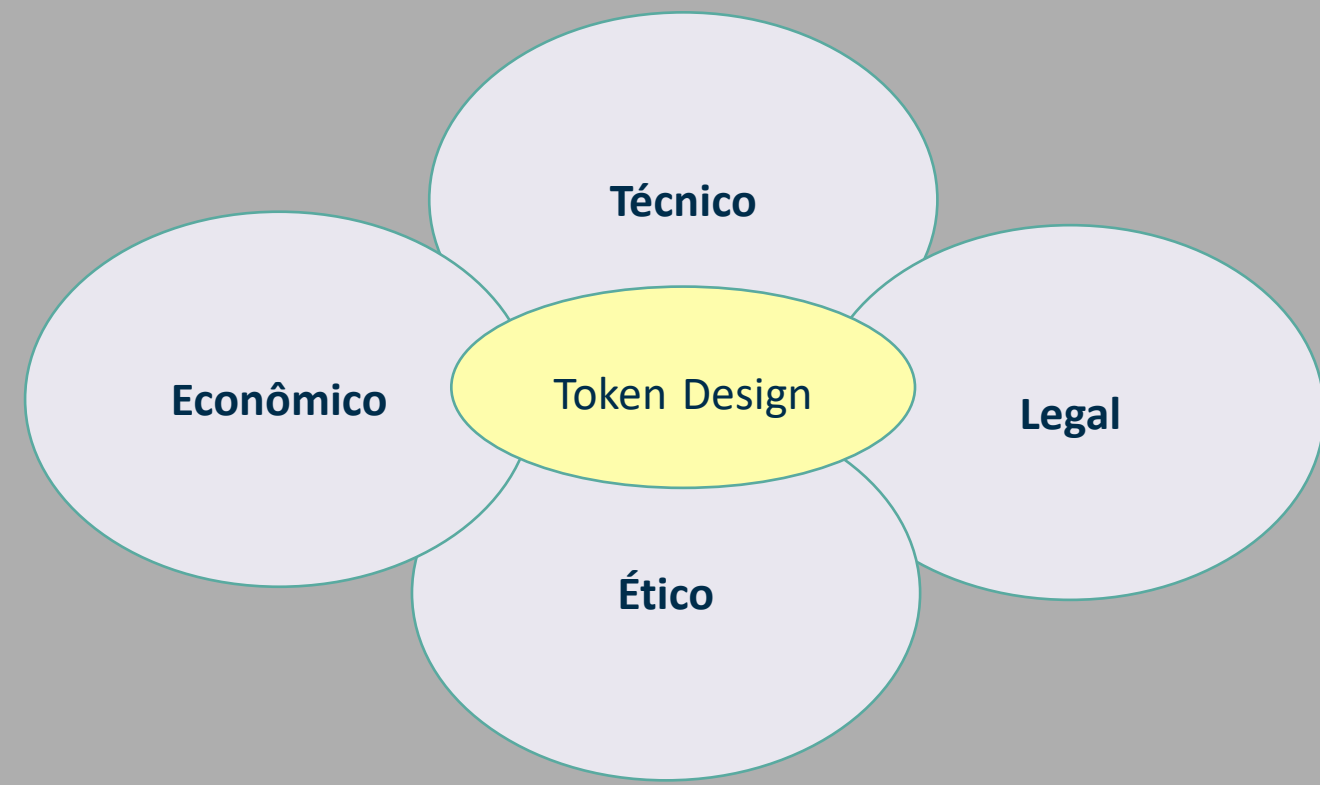
OpenSea



Wallet

Este token estava sendo leiloado simultaneamente na OpenSea e na Rarible e em cada marketplace possuía uma imagem diferente.

Token Engineering



Moedas Digitais

Criptomoedas

Valor é enviado digitalmente para qualquer lugar do mundo, imediatamente, sem controle de uma entidade específica.



Stablecoins

Lastro da moeda em ativos tradicionais como ouro e dólar, reduzindo riscos e volatilidade.

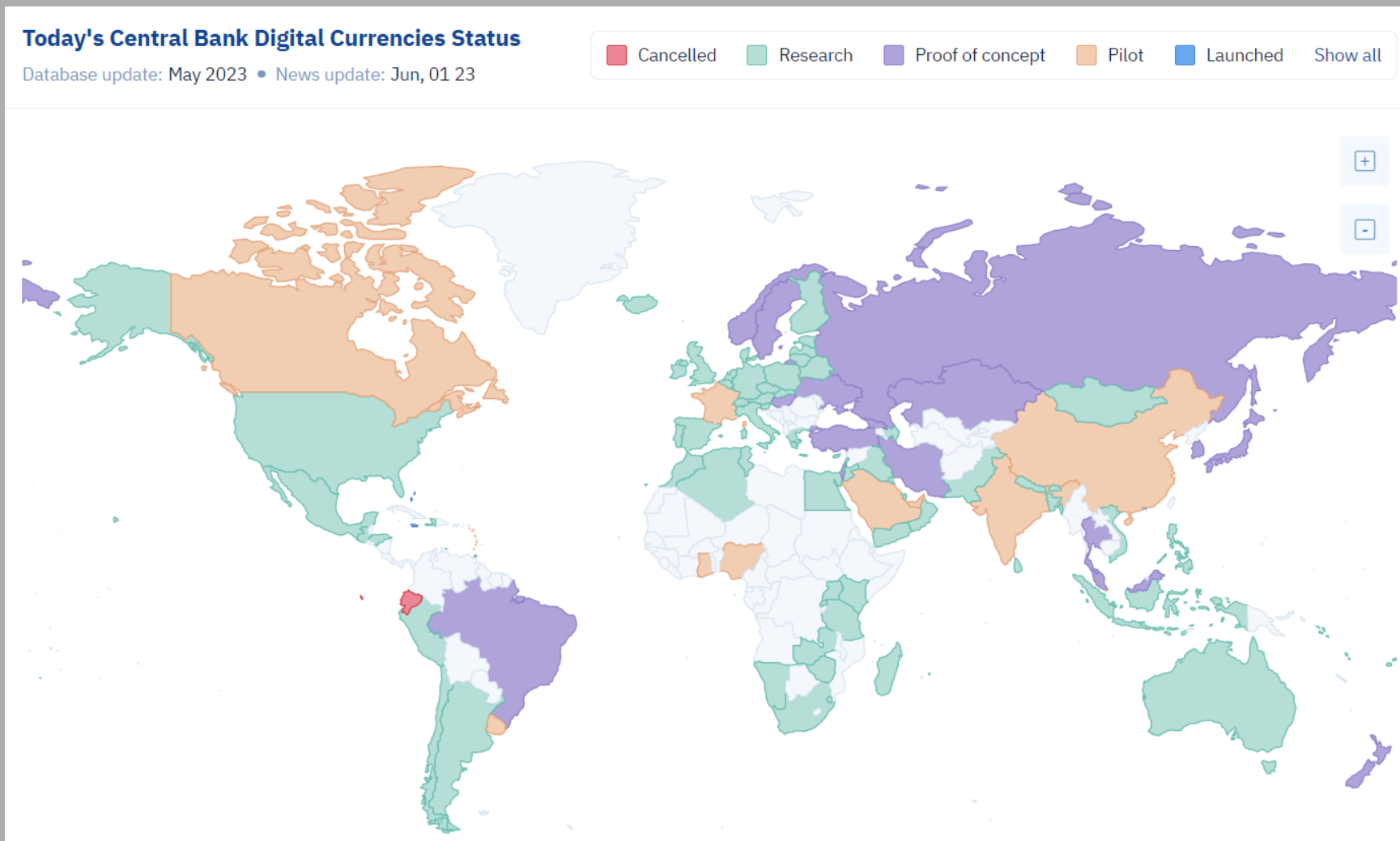


CBDCs

As CBDCs não criam uma moeda em paralelo para a economia do país. Apenas digitalizam a moeda já existente, criando equivalência entre a moeda digital e a moeda tradicional do país.



CBDCs no mundo



Benefícios de uma CBDC



Inovações
Tecnológicas



Evitar perdas e aumentar
inclusão financeira



Substituir
numerários



Eficiência nas liquidações
financeiras

Piloto Real Digital

Contexto: **economia tokenizada**

Ambiente colaborativo de interesse convergente

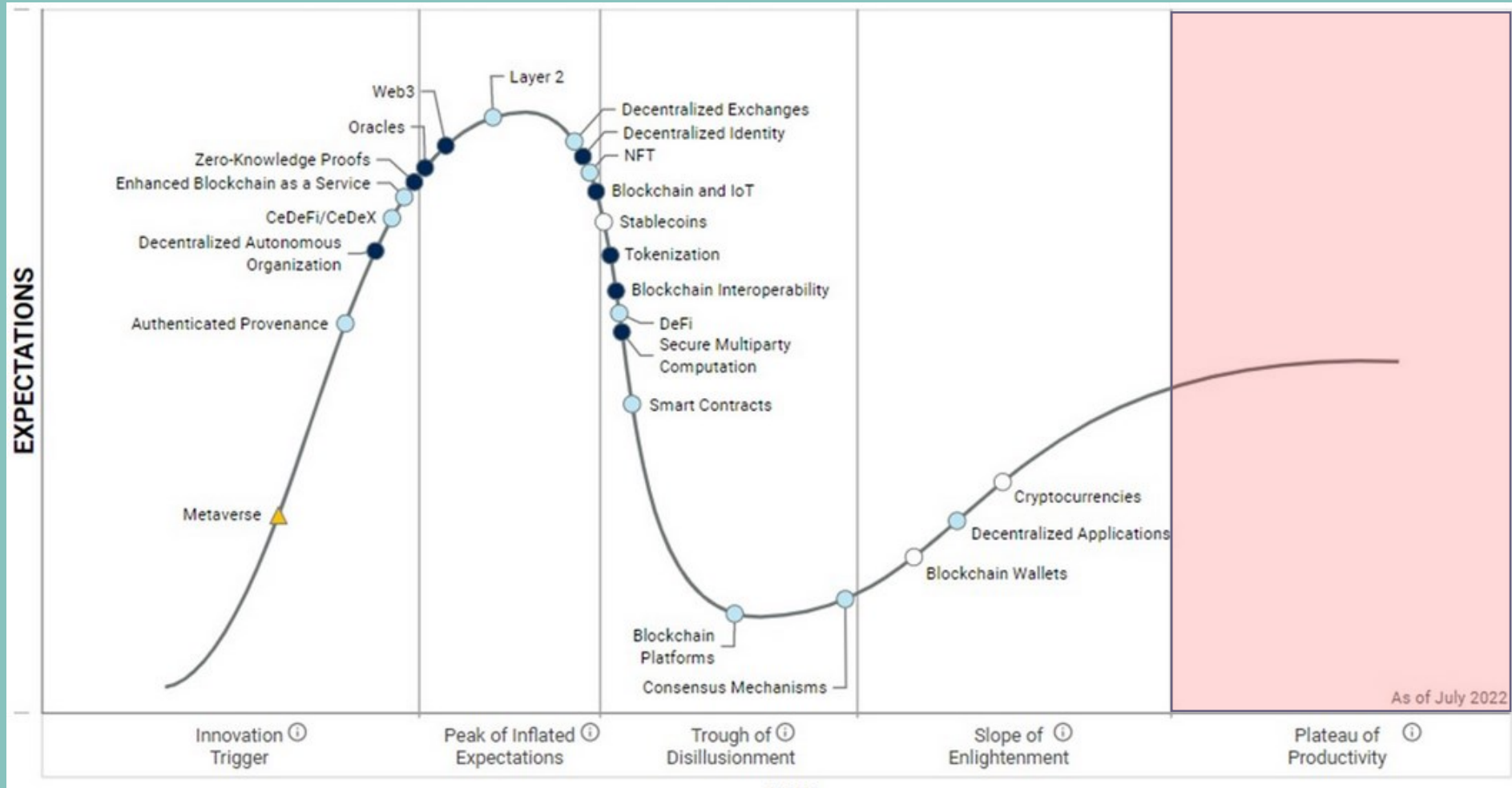
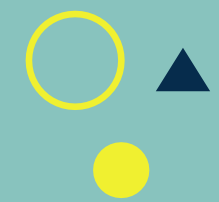
Infraestrutura de programabilidade em DLT com ativos financeiros (DvP: Real Digital, Real Tokenizado e TPF)

Validar as diretrizes de privacidade e segurança de dados



Fonte: <https://diretonoticias.com.br/2023/03/09/real-digital-banco-central-divulga-diretrizes-do-projeto-piloto/>

Gartner Hype Cycle for Blockchain and Web3, 2022



Blockchain no BB





Obrigado

Luciano Pereira da Silva

Email: luciano.silva@bb.com.br

Mini Currículo:

Formado em Sistemas de Informação com pós-graduação em Ciência de Dados e Engenharia de Software, é Assessor de TI na Unidade de Engenharia e Construção da Diretoria de Tecnologia, atua com plataformas blockchain permissionadas para soluções corporativas do **Banco do Brasil S.A.**

