Mercado Bitcoin

Autenticação e Autorização em Go além do JWT

Yan Uehara de Moraes

Yan Uehara de Moraes

Mercado Bitcoin

Nascido em Campo Grande/Mato Grosso do Sul, e vivendo em Curitiba/Paraná

Bacharel em Ciência da Computação pela UFMS e Mestre em Informática pela UFPR

Engenheiro Backend - Nível Especialista

Somos a maior *plataforma de investimentos* em ativos digitais da América Latina

4.3 milhões
clientes

13 anos
em operação, desde 2013

+ R$ 170 bilhões
em volume transacionado

+350
ativos listados

+ R$ 1.4 bilhão
em tokens

Operação global, com escritórios no Brasil e em Portugal.

Top 5
tokenizadoras
do mundo

rwa.xyz

Top 20
exchanges
do mundo

Kaiko
smart data

Auditado por:

KPMG

Licenças regulatórias:

BANCO CENTRAL DO BRASIL

BANCO DE PORTUGAL
EUROSISTEMA

CVM
Comissão de Valores Mobiliários

Mercado Bitcoin

O que é Autenticação?

Quem é você?

- Verificação da identidade de quem está fazendo uma operação
- Pessoa, máquina, máquina em nome de uma pessoa, um agente autônomo (AI)
- Pode ou não envolver criptografia
- Mais simples: Segredo compartilhado

Credencial

Mercado Bitcoin

O que é Autorização?

Você pode fazer essa ação?

- Dado uma identidade conhecida, ela pode realizar a ação X?
- Noção de permissão e/ou privilégio
- Mais granular/menos granular

"An approval that is granted to a system entity to access a system resource." (RFC 4949)

Mercado Bitcoin

Como normalmente é feito?

Preciso adicionar alguma camada de segurança, e agora?

- Início sem segurança: Sem autenticação, endpoints abertos na rede
- Solução inicial: Segredo compartilhado
- Evolução: Vamos usar um JWT!

Mercado Bitcoin

Access Token/JWT?

Mercado Bitcoin

Access Token

- Credencial
- Valor opaco ou um JWT (exemplo `ory_at_JGhESDjKfHMQ8Wcy0cC3.hIQxGmX37ydn8WmKAnlD3U`)
- Usualmente libera o acesso para quem estiver portando o access token ("bearer")

Mercado Bitcoin

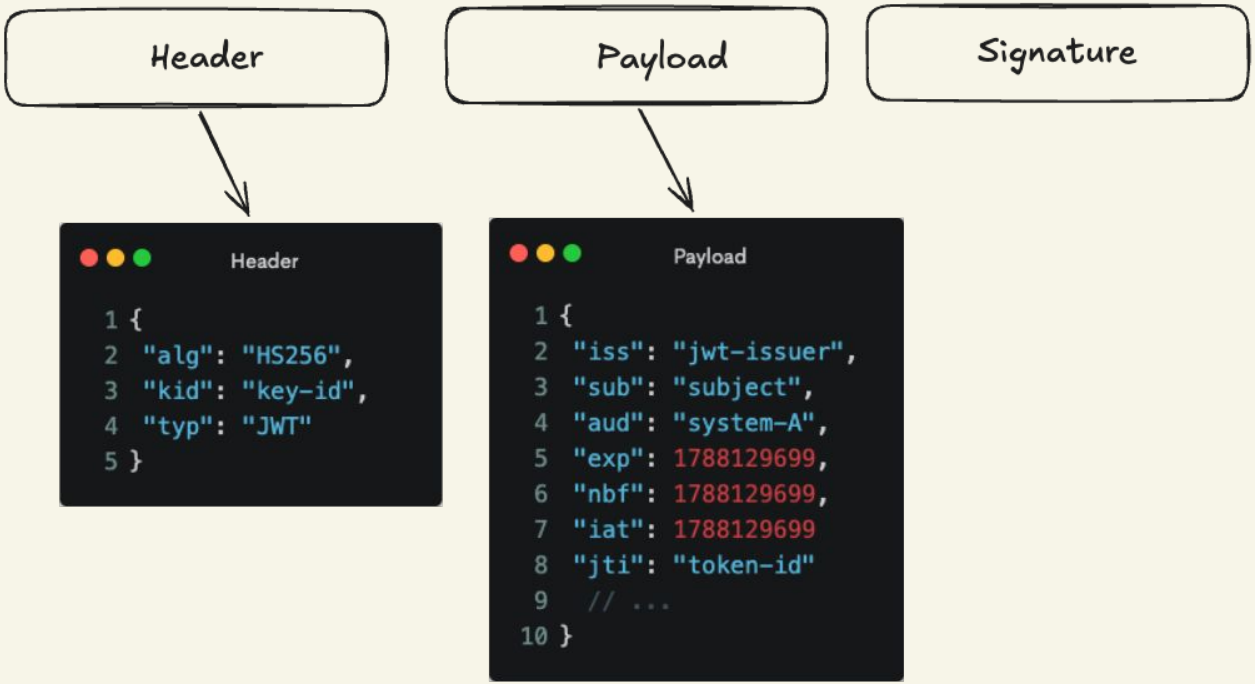
O que é um JWT?

Ou também, o que não é um JWT?

- JSON Web Token
- Não necessariamente é uma credencial
- Representação de *claims* entre duas partes/entidades
- Claims pode ser assinadas

Mercado Bitcoin

Partes de um JWT



Mercado Bitcoin

Partes de um JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWUsImlhdCI6MTc4ODIxNjI0MH0.qogvBYlN5BxEhP-1voua2bJxBYFQf9ysWmtpeUm5ZP8

Mercado Bitcoin

OAuth2 Framework

Mercado Bitcoin

OAuth2 Framework

- Tornou-se o padrão de-facto para gerenciamento de acesso na web
- Padroniza funções e nomenclatura dos participantes:
  - Resource-Owner: Entidade que pode liberar acesso a um recurso (usuário)
  - Resource Server: Entidade que detém o recurso (servidor)
  - Cliente: Aplicação que faz o acesso ao recurso em nome de e com a autorização do RO
  - Authorization Server: Entidade que gera os access tokens depois da autorização do RO

Mercado Bitcoin

OAuth2 Framework - Grants

- Authorization Code
  - Cliente acessa o recurso "em nome do" usuário (*on behalf of*)
- Client credentials
  - Cliente acessa o recurso em próprio nome

Mercado Bitcoin

OAuth2 Framework - Endpoints

- Authorization endpoint: Endpoint (AS) usado pelo cliente para obter a autorização do RO
- Token endpoint: Endpoint (AS) para trocar uma autorização por um access token
- Redirection endpoint: Endpoint (Cliente) para retornar a autorização para o cliente; Usado pelo AS.

- Introspection endpoint: Endpoint (AS) para verificar a validade de um access token

Mercado Bitcoin

OAuth2 + OpenID Connect (OIDC)

- OpenID Connect construído em cima do OAuth2
- Adiciona uma camada de identidade (ID Token) com os dados do usuário
- Padroniza um endpoint "UserInfo" para obter dados completos do usuário

Mercado Bitcoin

Boas Práticas

Mercado Bitcoin

Boas Práticas

O que fazer e o que não fazer?

- Regra geral: Don't roll your own authentication
  - Muitos fatores de segurança para serem considerados
  - Prefira soluções existentes: Keycloak, Ory Hydra, Auth0, etc,
- Documentação documentação documentação
- SEMPRE validar corretamente access tokens
- Gerenciamento seguro de segredos e rotacionamento
- Logging e monitoramento de acesso

Mercado Bitcoin

Estudo de Caso

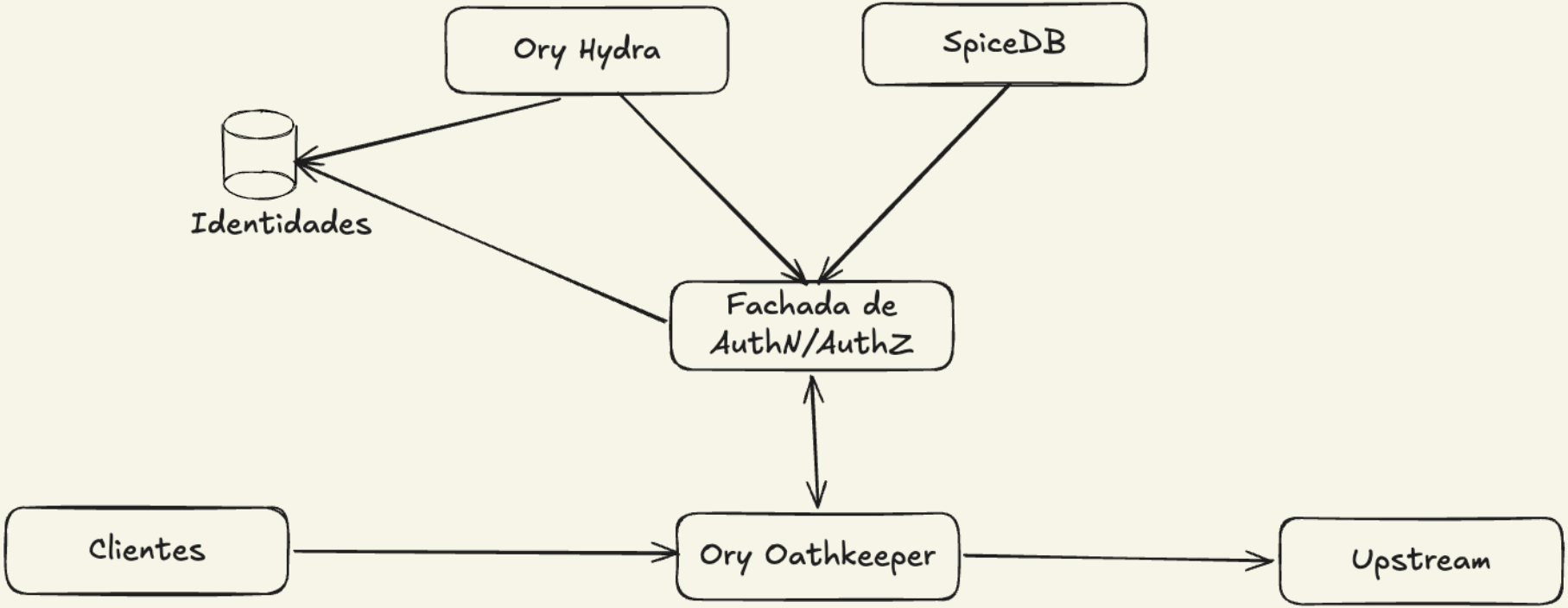
Mercado Bitcoin

Desafio Enfrentado

- Monolito com várias responsabilidades, incluindo identidades, autenticação e autorização
- Necessidade de governança de acesso
- Exigência de escala para suportar a quantidade de acessos dos clientes e infra-estrutura interna

Mercado Bitcoin

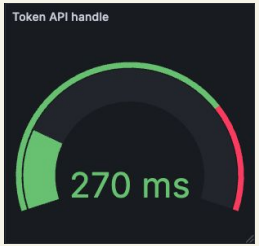
Arquitetura



Resultados

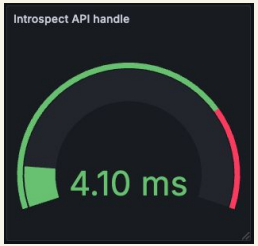
Janela 5 dias

Geração de Tokens



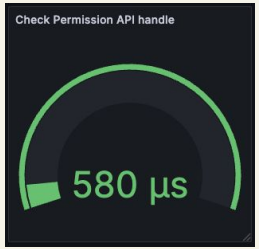
~1.33M

Introspecção



~171M

Permissão



~321M

Resultados

Média por dia

~266 mil

Token gerados por dia

~34M

Introspecção por dia

~64.2M

Checagens de permissão

Mercado Bitcoin

Mercado Bitcoin

Estudo de caso em GO

Mercado Bitcoin

Conclusão

Mercado Bitcoin

Autenticação e Autorização

- Autenticação envolve o conhecimento teórico de diversos padrões
  - (E é importante segui-los)
- Deve ser implantado conforme a evolução e maturidade dos times e sistemas
- Pode ser integrado a soluções internas (Service Mesh, gateways internos, ingressess, etc)

Mercado Bitcoin

Obrigado!


GOPHERCON
LATAM 2026