FACI

wyden

Introdução a Cripto Ativos

Profº Msc. Jeffson Celeiro Sousa
Doutorando em Ciência da Computação - UFPa

Belém, 03 de Fevereiro de 2026

Contato

FACI wyden

Ementa

- Fundamentos Técnicos do Blockchain
- Hash
- Criptografia Assimétrica
- Assinatura Digital
- Assinatura de Transações na Blockchain
-

O Colapso dos Sistemas Financeiros (2008-2009)

Causa do colapso: Falhas em sistemas centralizados conduzidos por bancos e instituições financeiras.

Impacto global:

- Perda de confiança no sistema financeiro.
- Pânico generalizado com o colapso dos mercados.

O Surgimento do Bitcoin

Criado como uma solução para a crise de confiança.

Modelo inovador:

- Moeda digital descentralizada.
- Sem autoridade central ou administração.

Intermediação de confiança: Realizada por software, denominado mais tarde de blockchain.

Blockchain: O Coração do Bitcoin

Funções do blockchain:

- Verificação e validação por software.
- Registro seguro e integridade das transações.

Elimina a necessidade de intermediários humanos, substituindo-os por tecnologia confiável.

O que é a Blockchain?

- Blockchain → termo genérico para aplicações de tecnologia de **registro distribuído (DLTs)**.
- Diferente de bancos de dados tradicionais:
  - Todos os participantes têm cópia da ledger (histórico completo).
  - Cada transação é validada coletivamente.

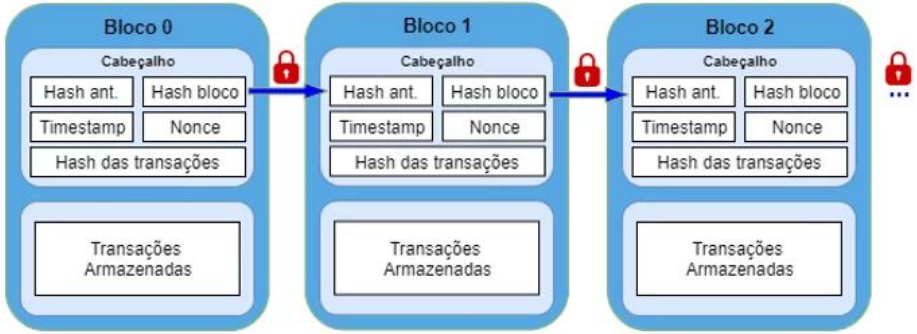
Conceitos Fundamentais do Blockchain

- **Transações:** Unidades básicas do sistema.
- **Blocos:** Conjuntos de transações validadas.
- **Cadeia de Blocos:** Conexão entre blocos validando a continuidade.
- **Nós (nodes):** Elementos que compõem a rede.
- **Protocolo:** Regras que interligam os componentes.

Blockchain é um sistema complexo e compreender esses conceitos fundamentais é indispensável para o projeto e desenvolvimento de aplicações.

Mas, como funciona?

1. Usuário envia uma transação.
2. Rede válida regras → chaves corretas, saldo suficiente etc.
3. Transação validada entra em um bloco.
4. O bloco é numerado, ligado ao anterior e armazenado.



- **Cadeia de blocos** = cada bloco contém transações + referência ao anterior.

FACI wyden

Blockchain Além das Criptomoedas

Objetivo inicial: Transferências peer-to-peer de moedas digitais.

- Cruzar fronteiras sem intermediários como bancos.

Aplicações expandidas:

- Transações de ativos não monetários, como:
  - Títulos, escrituras, arte e música.
  - Códigos secretos e contratos empresariais.
  - Decisões autônomas (ex.: veículos).

Sucesso Inicial e Expansão para Ativos Digitais

Bitcoin:

- Operando continuamente desde o lançamento.
- Mais de 200.000 transações por dia (fonte: *Blockchain Charts*).

Pergunta-chave:

- "*Se é possível transacionar moedas digitais, por que não outros ativos digitais?*"

Resposta:

- Ethereum (2013):
  - Introduziu execução de código em blockchain.
  - Validação e registro aplicados a ativos digitais não monetários.

Aplicações Blockchain

- Validação de documentos.
- Registro de obras de arte.
- Rastreamento de produtos (supply chain).
- Redes financeiras antifraude.
- Base dos cripto ativos.

FACI
wyden

Redes Permissionadas

- **Permissionada** → precisa de permissão para participar.
- **Privada** → restrita a um grupo de organizações.
- Benefícios:
  - Privacidade.
  - Controle.
  - Gestão de acesso.
  - Performance otimizada.

E qual é o custo disso?

- **Blockchain pública**: custo por transação (gas).
- **Blockchain permissionada**: custo depende do consórcio.
- Transparência não depende só de ser pública ou privada, mas das regras configuradas.

Classificação das Redes

FACI wyden

RBB - Rede Blockchain Brasil

- É uma Rede Público-Permissionada
- RBB – Rede Blockchain Brasil (**baseada na LACCHAIN**).
- Aberta para leitura, mas transações restritas a membros autorizados.
- Transparência para sociedade + controle de quem participa.

FACI wyden

Porque a blockchain é segura?

Características de Segurança

- **Integridade**:
  - Garantia de que a informação enviada não foi alterada entre a origem e o destino.
  - Uso do algoritmo de hash para validar a integridade dos dados.
- **Não Repúdio**:
  - Garante que a autoria da transação não possa ser negada.
- **Autenticidade**:
  - Verifica que a transação veio de quem afirma tê-la feito.

Uso da Criptografia

  - Algoritmos de hash garantem a segurança dos dados sem esconder o conteúdo.
  - Blockchains públicas permitem verificar as transações.

O Que São Algoritmos de Hash?

- Ferramenta que gera um código único, fixo e irreversível para qualquer dado de entrada.
- **A integridade é conseguida por meio do uso do algoritmo de HASH**
  - Gerar Hash SHA-256: https://md5decrypt.net/en/Sha256/
  - Decodificar Hash SHA-256: https://md5decrypt.net/en/Sha256/
- **Exemplo prático**:
  - Texto "blockchain" gera um hash único.
  - Alteração de uma letra no texto gera um hash totalmente diferente.

FACI wyden

E o que é SHA-256 ?

- SHA-256 é um padrão de hash (derivado do Algoritmo de Hash Seguro SHA-2), um padrão que permite que qualquer dado binário corresponda a uma impressão digital de **64 caracteres hexadecimais**.
- A criptografia SHA-256 é um hash, o que significa que é unidirecional e **não** pode ser descriptografada.
- A criptografia SHA-256 calcula uma impressão digital de 256 bits ou 32 bytes, cuja escrita hexadecimal consiste em 64 caracteres.
- SHA-256 é codificado como ee53bb**3**ac7c947**e**32c06c02**f**3be**e**ea0bb9667e778f638**8**dc0fb77**b**e3f7345da9 SHA256 '(sem hífen) é codificado como' b28e91**3**73610ca**e**9765372c**f**1d0**e**5de15fb0f0dfc3e18f3**8**5da98**b**c256b81080 (58 caracteres alterados de 64)

FACI wyden

Como Funciona na Blockchain?

- **Processo de Geração e Verificação**
  - Origem: A informação é enviada com um hash gerado pelo remetente.
  - Destino: O hash é recriado e comparado com o original.
  - Qualquer alteração nos dados invalida o hash.

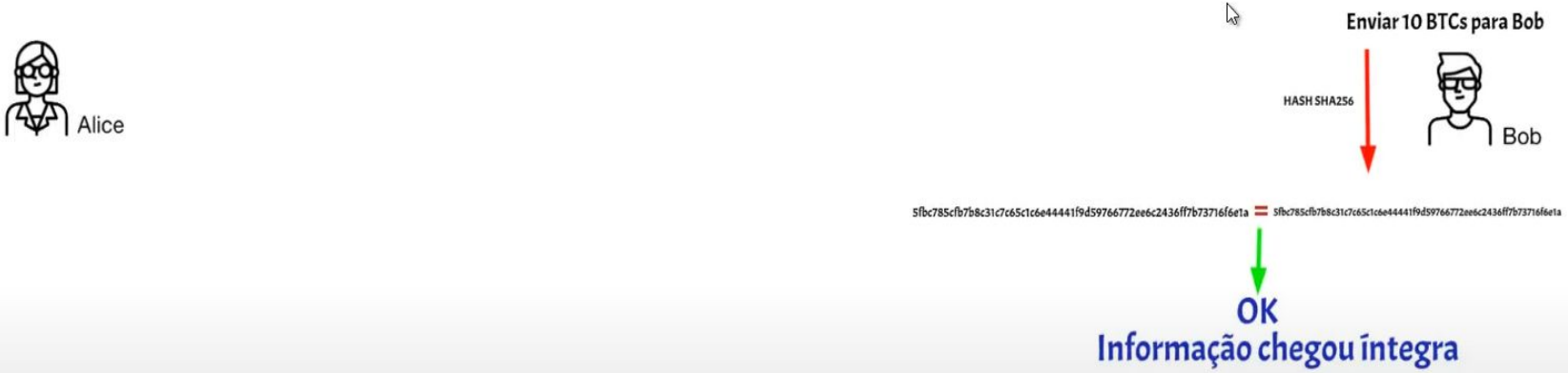
Alice deseja enviar 10 BTCs para Bob

Como Funciona na Blockchain?

- **Processo de Geração e Verificação**
  - Origem: A informação é enviada com um hash gerado pelo remetente.
  - Destino: O hash é recriado e comparado com o original.
  - Qualquer alteração nos dados invalida o hash.

Como Funciona na Blockchain?

- **Processo de Geração e Verificação**
  - O algoritmo de hash é utilizado nas blockchains para garantir que a informação chegou sem sofrer nenhuma alteração. Há diversos algoritmos de hash, como o SHA256, MD5, e outros.



Como Funciona na Blockchain?

- **Processo de Geração e Verificação**
  - O algoritmo de hash é utilizado nas blockchains para garantir que a informação chegou sem sofrer nenhuma alteração. Há diversos algoritmos de hash, como o SHA256, MD5, e outros.

Alice deseja enviar 10 BTCs para Bob

FACI wyden

Como Funciona na Blockchain?

- **Processo de Geração e Verificação**
  - O algoritmo de hash é utilizado nas blockchains para garantir que a informação chegou sem sofrer nenhuma alteração. Há diversos algoritmos de hash, como o SHA256, MD5, e outros.

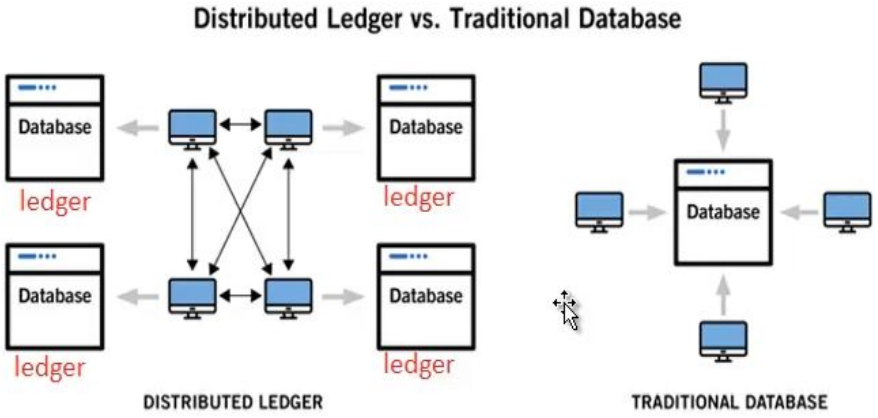
Como Funciona na Blockchain?

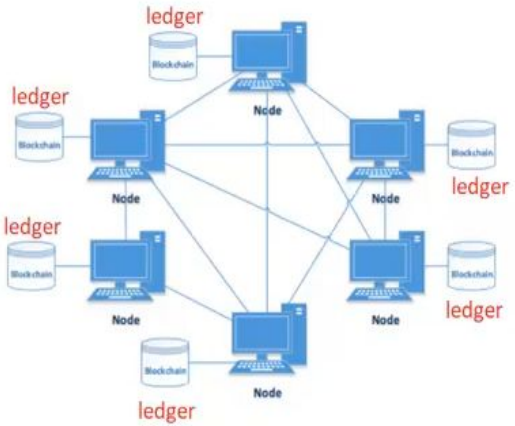
- **Processo de Geração e Verificação**
  - O algoritmo de hash é utilizado nas blockchains para garantir que a informação chegou sem sofrer nenhuma alteração. Há diversos algoritmos de hash, como o SHA256, MD5, e outros.

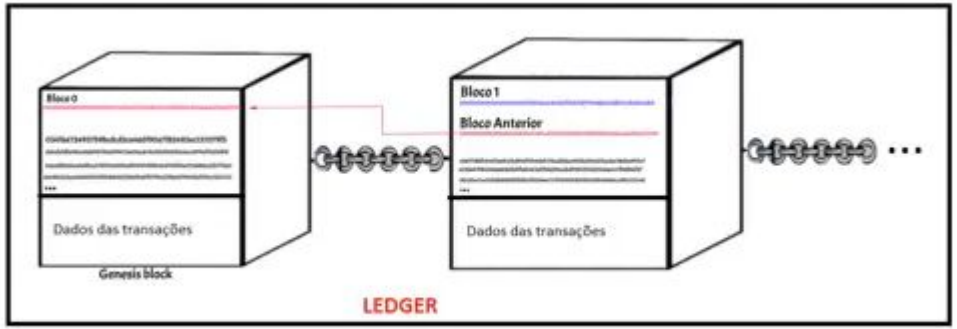
Como Funciona na Blockchain?

- **Processo de Geração e Verificação**
  - O algoritmo de hash é utilizado nas blockchains para garantir que a informação chegou sem sofrer nenhuma alteração. Há diversos algoritmos de hash, como o SHA256, MD5, e outros.

O que é a Ledger?







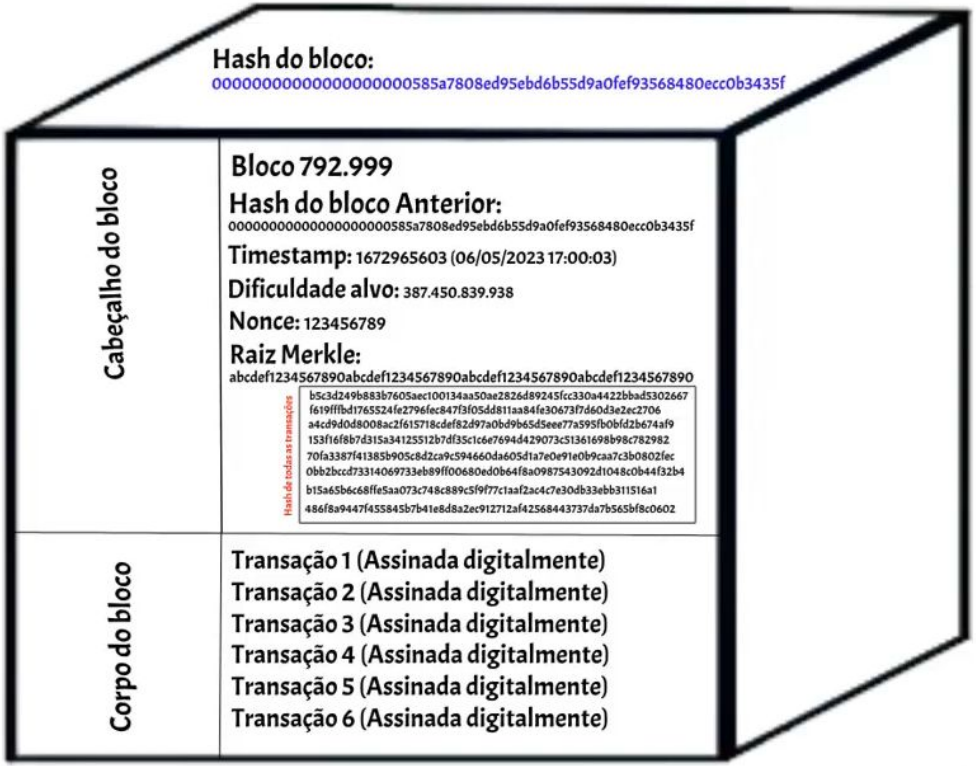
Estrutura de um Bloco

Divisão do bloco:

- Cada bloco tem duas áreas principais:
  1. **Cabeçalho do bloco**:
     - Número do bloco.
     - Hash do bloco anterior.
     - Timestamp (data/hora).
     - Dificuldade alvo.
     - Nonce (número aleatório usado para mineração).
     - Raiz Merkle (resumo das transações do bloco).
  2. **Corpo do bloco**:
     - Contém as transações em texto aberto, assinadas digitalmente pelo emissor."

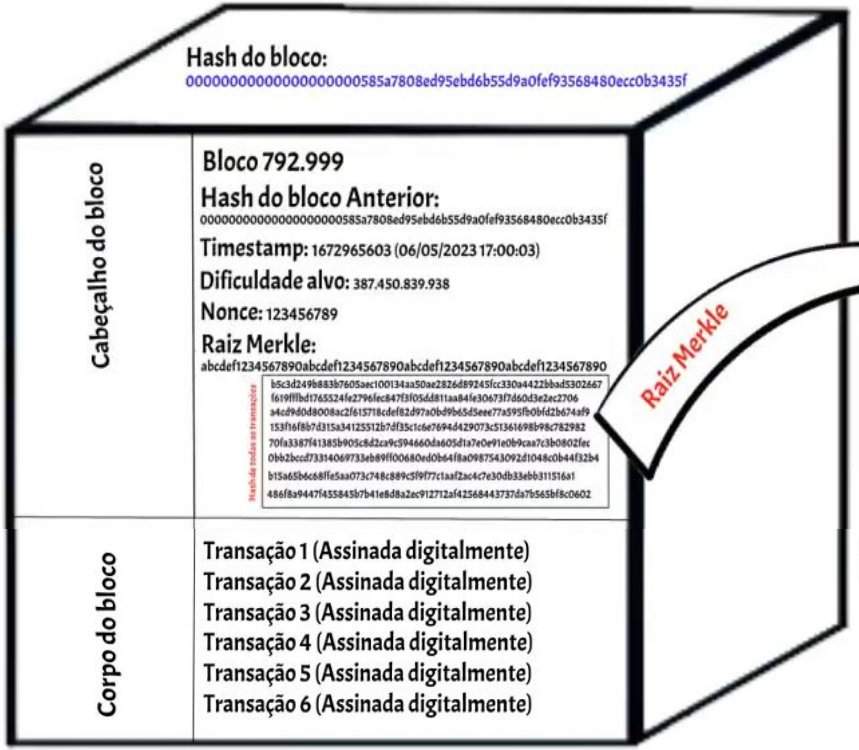
O que é a Ledger?

- Bitcoin Blockchain Explorer: https://blockchain.com/p
- Ethereum Blockchain Explorer: https://etherscan.io/

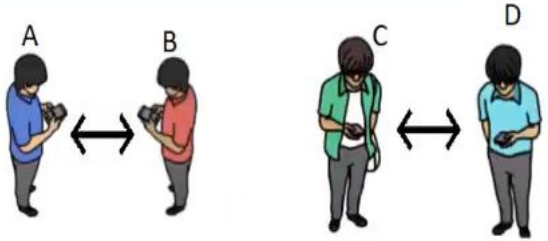


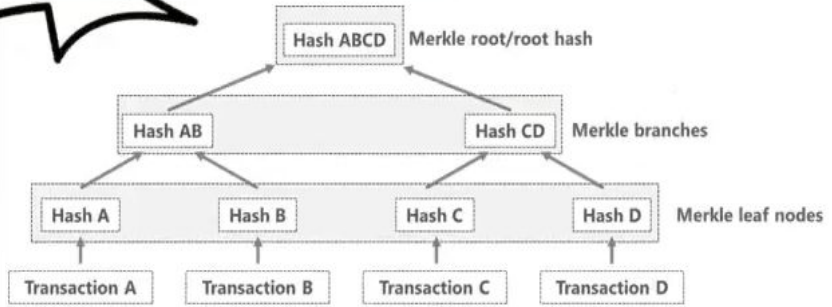
FACI wyden

O que é a Ledger?



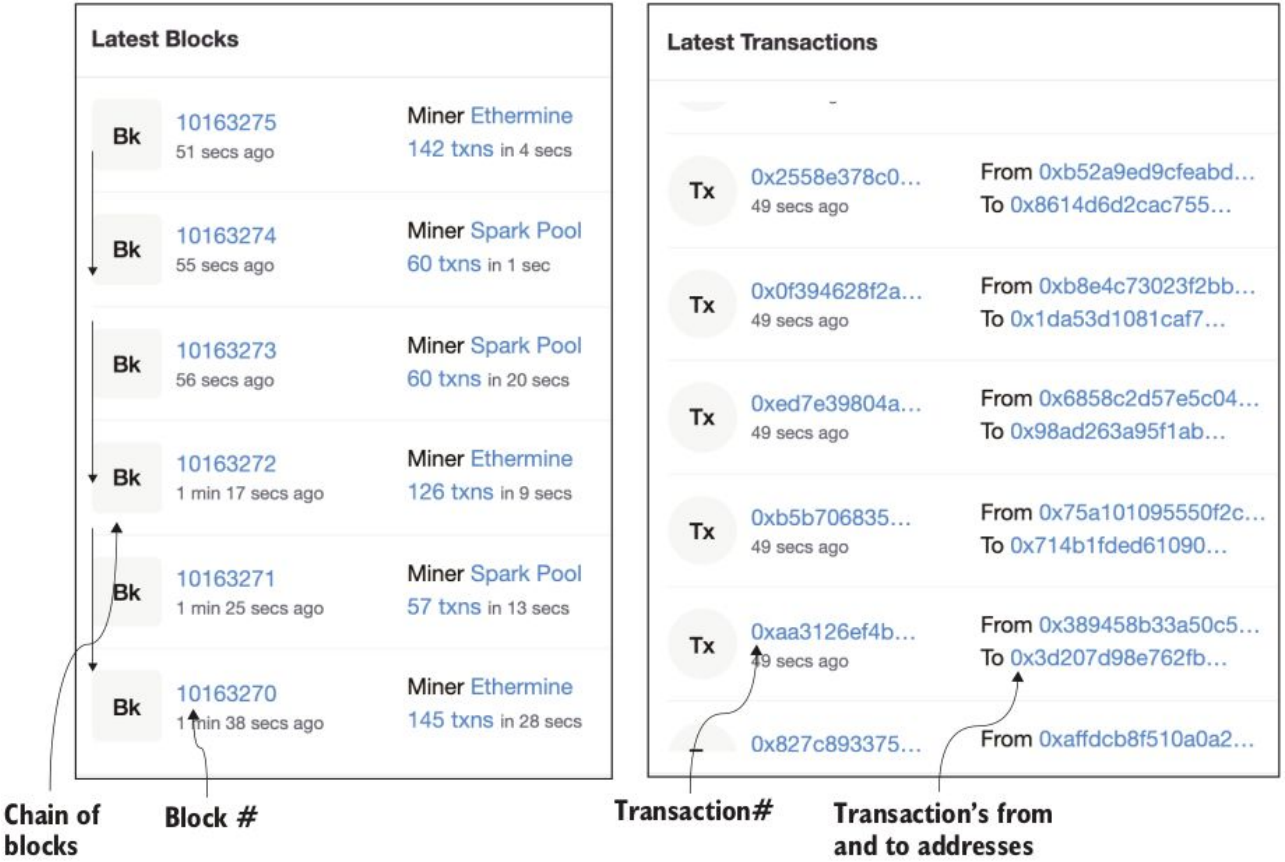
Raiz Merkle





FACI wyden

Transações e Blocos no Blockchain



Transações e Blocos no Blockchain

Transações (Tx):

- Mensagens entre duas contas (Ex.: **From** e **To**).
- Registram informações em blocos.

Blocos (Bk):

- Conjuntos de transações identificados por um número único.
- Exemplo:
  - Bloco **#10163275** contém 142 transações.
  - Bloco **#10163274** contém 60 transações.

Imutabilidade e Cadeia de Blocos

Os blocos são interligados formando a **cadeia de blocos** (blockchain).

Exemplo de bloco:

- Bloco **#10163275** pode ser consultado no site **Etherscan.io** (https://etherscan.io/).
- Mesmo número de transações será exibido, ilustrando a imutabilidade do blockchain.

O que é um Blockchain?

Definição: Tecnologia que possibilita confiança em um sistema descentralizado de transações entre participantes.

Funções principais:

- Verificar e validar transações (ou rejeitá-las, se inválidas).
- Executar transações.
- Registrar ações com consenso dos participantes.

Integração:

- Blockchain funciona como uma camada de intermediação de confiança dentro de sistemas maiores.

Infraestrutura de Blockchain

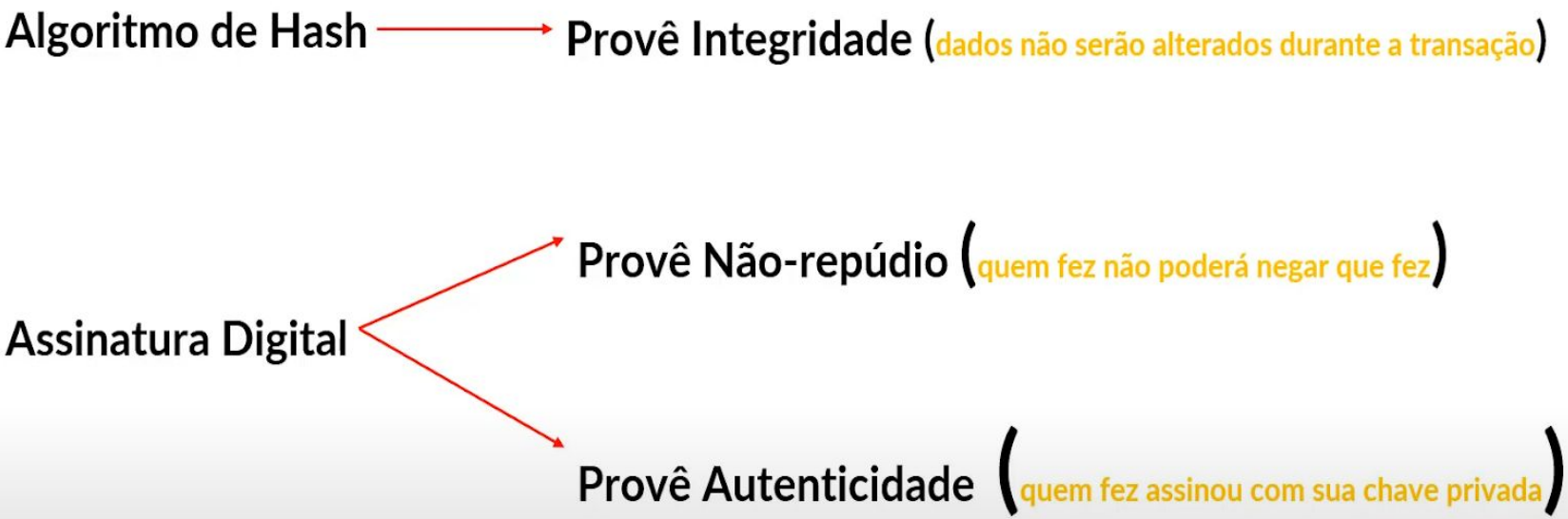
Componentes principais:

- **Sistema distribuído:** Realiza operações rotineiras e envia dados para validação.
- **Blockchain:**
  - Valida e registra dados.
  - Estabelece confiança no sistema maior.

Aprimoramento: Blockchain não substitui o sistema existente, mas o melhora com validação e verificação.

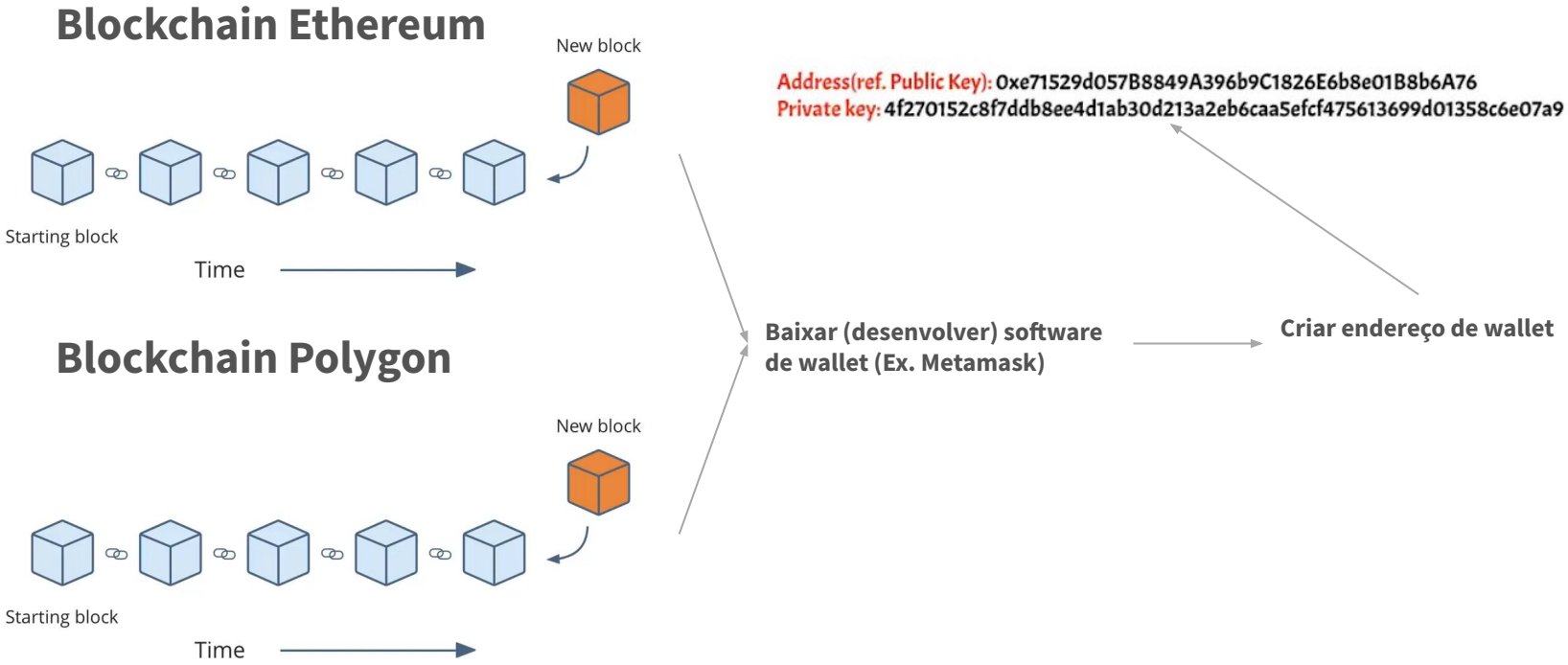
Pilares da Segurança

Garantidos pelo uso da criptografia



FACI wyden

Como se registrar em uma blockchain?



FACI wyden

Chaves Pública e Privada

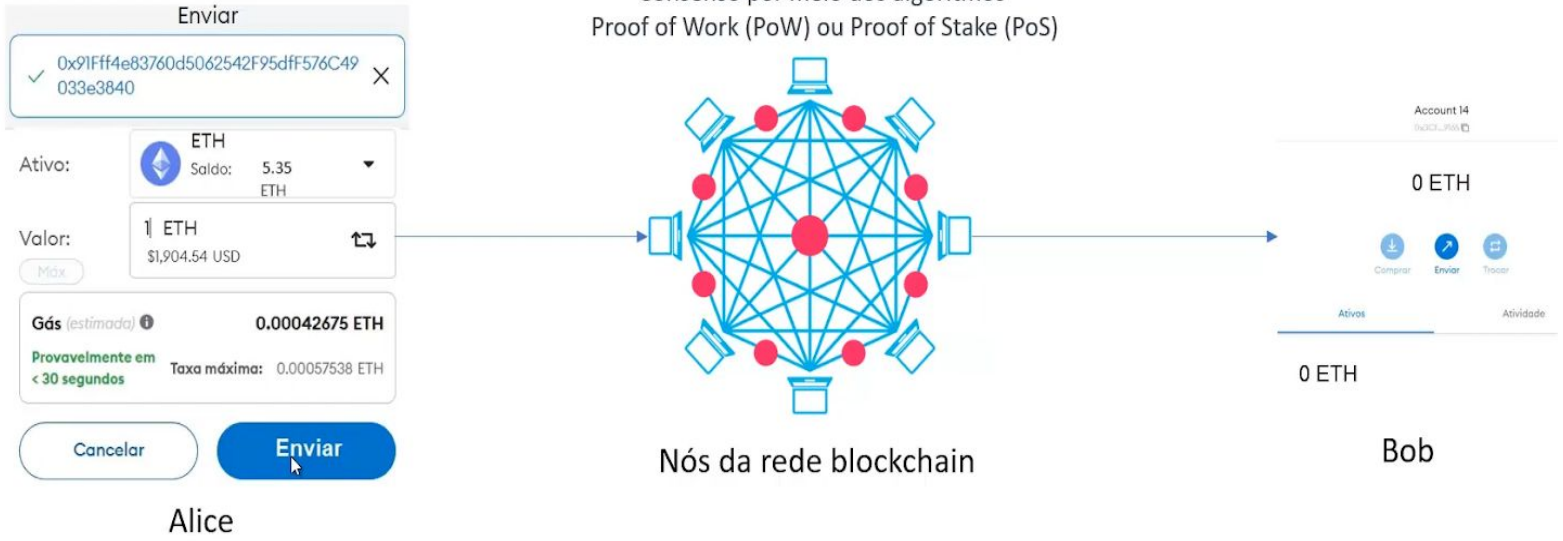
- **O que são?**
  - A chave pública é como um endereço que todos podem ver, enquanto a chave privada é mantida em segredo.
- **Funções de cada chave**
  - "A chave pública identifica você na rede e permite que outros enviem dados ou valores para você."
  - "A chave privada é usada para assinar digitalmente transações, garantindo que apenas você possa autorizar movimentações."
- **Exemplo prático:**
  - "Imagine que você queira enviar 1 Bitcoin. Você usa sua chave privada para assinar a transação, e qualquer nó da rede pode verificar sua assinatura usando sua chave pública."

Como se registrar em uma blockchain?

- Funcionamento da Transação no Ethereum ou Polygon

Wallet Address Alice: 0xeCbFC8b9d3701a27659A5cc983A82b57f7Bb68ac
Private key: 1f81707e59ce0153d908ef7f8e43057277dd2bc70a6a1aae1f6babceef63208b

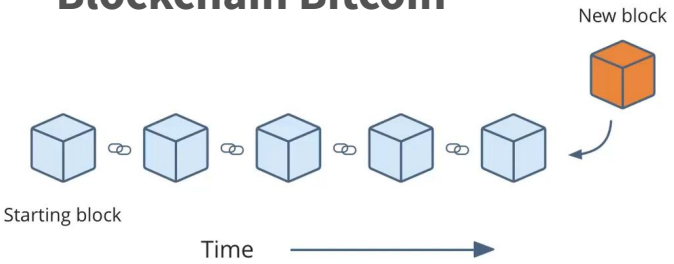
Wallet Address Bob: 0x91Fff4e83760d5062542F95dfF576C49033e3840
Private key: a6dde36f3a019c9c7219afacf5cb3625e55e99a150725606038dcc0aaba7a9de



Transaction Hash: 0x463aa7a148c0eb97bfab72f4fc4b9a6ee731515225a8b4f781afbf37a4672437

Como se registrar em uma blockchain?

Blockchain Bitcoin

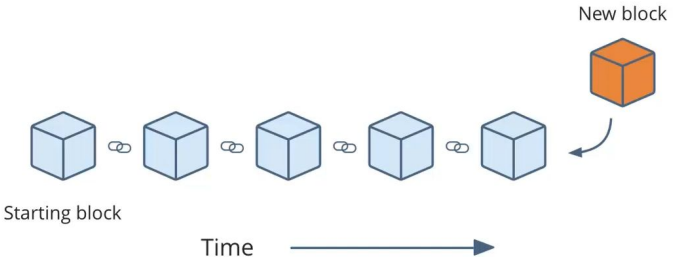


Address(ref. Public Key): 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Private key: 5KyzDUa1QDfKtDnuGmt5x6J4JY1ZQjQLnF2eHEB6MjdA5U3rYak

Baixar (desenvolver) software de wallet (Ex. Electrum ou Bitcoin Core)

Criar endereço de wallet

Blockchain Fabric



Desenvolver gerador de wallet (certificado digital X.509.)

FACI wyden

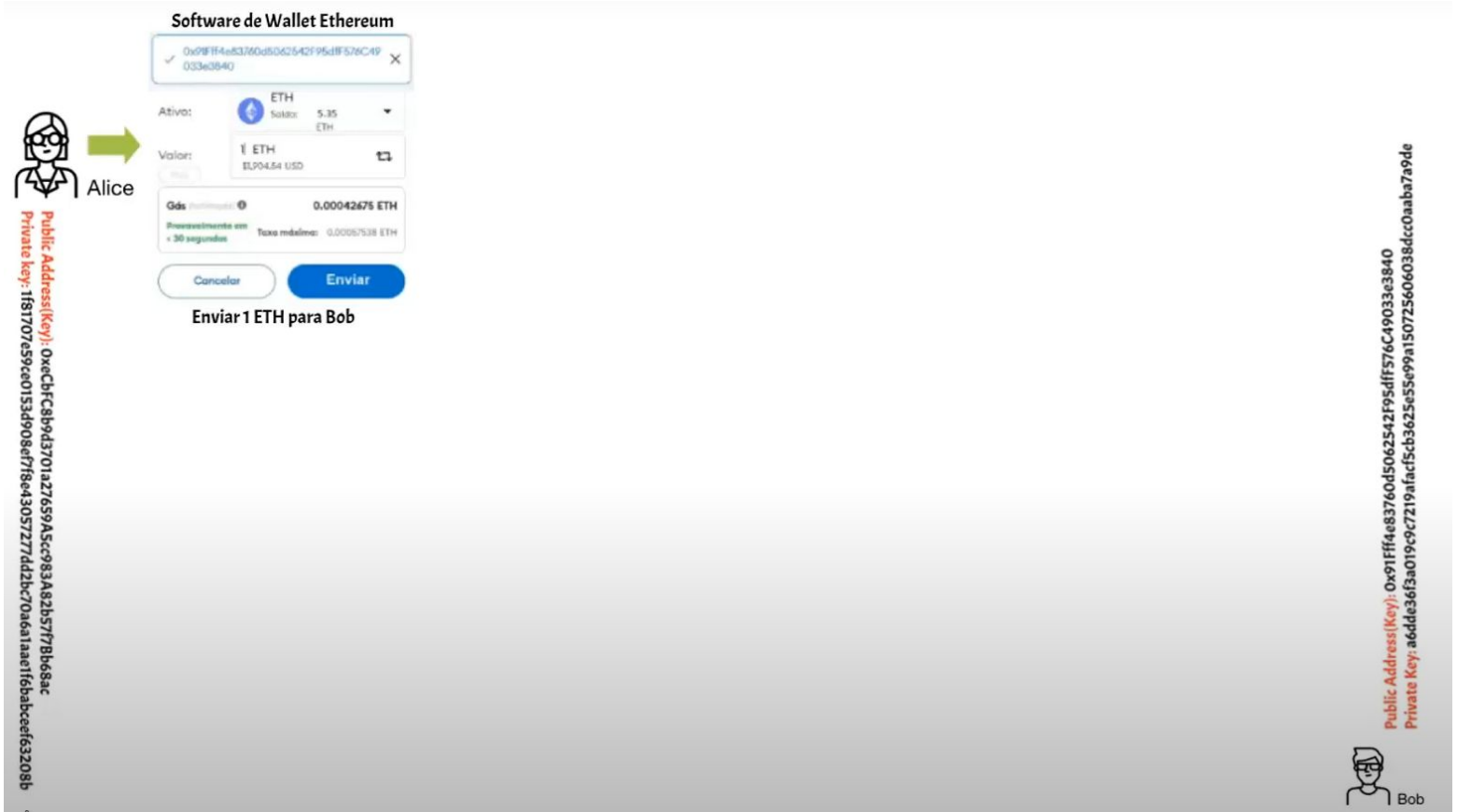
Como Funciona a Assinatura Digital?

- Quando você realiza uma transação, o sistema gera um hash da mensagem e o cifra com sua chave privada. Isso cria a assinatura digital." "Essa assinatura, junto com sua chave pública, é usada pelos validadores da rede para confirmar a autenticidade da transação."
- **Garantias proporcionadas:**
  - **Não Repúdio:** "Uma vez assinada, a transação não pode ser negada, porque apenas sua chave privada poderia ter gerado aquela assinatura."
  - **Autenticidade:** "Os validadores verificam que a assinatura corresponde à chave pública do remetente."

Validação de Transações na Blockchain

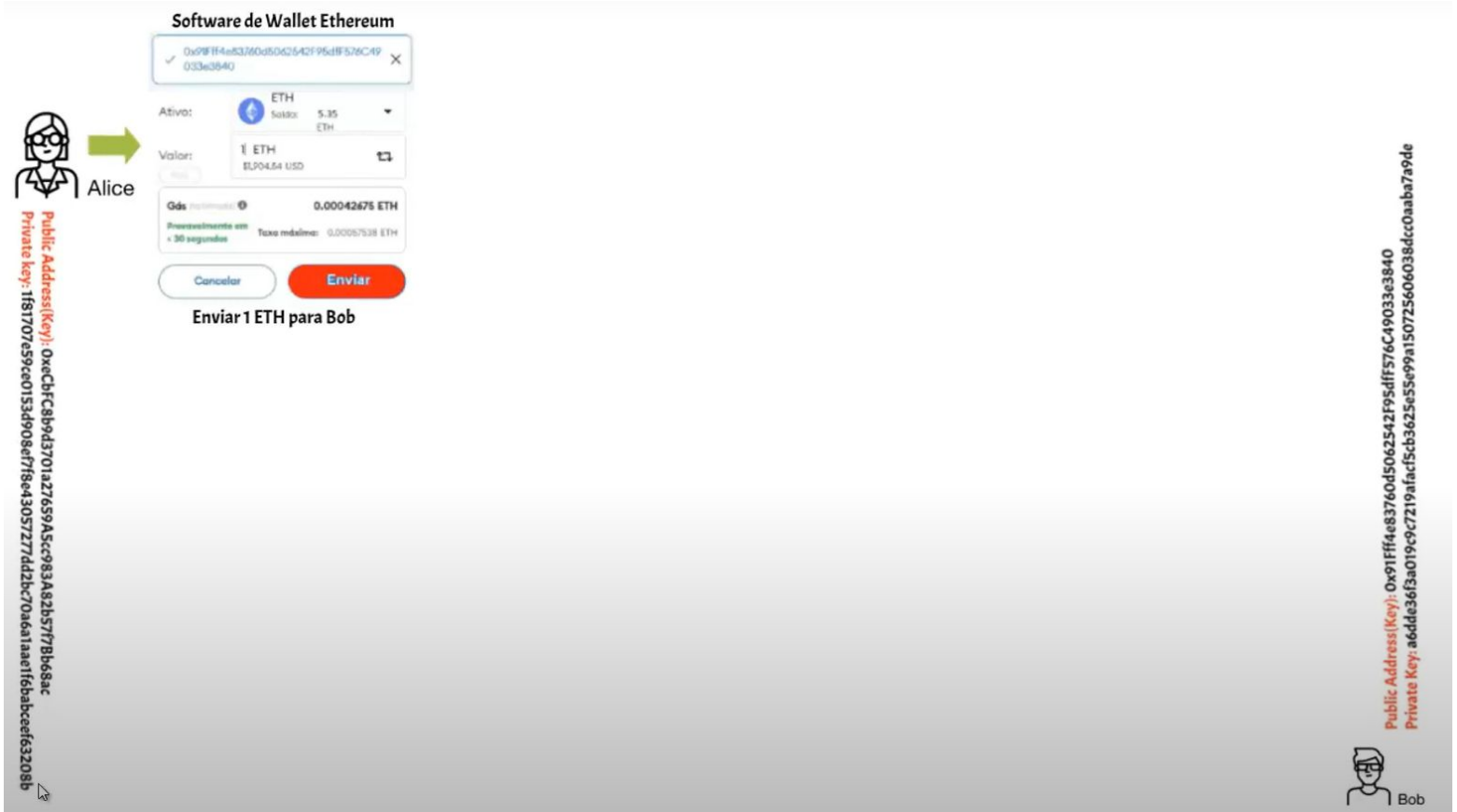
- **Mecanismo de consenso:**
  - "A blockchain utiliza um sistema de consenso, onde mais de 50% dos nós precisam validar a transação como autêntica antes que ela seja gravada no bloco."
- **Exemplo:**
  - "Se você envia 10 Bitcoins, os validadores verificam:
    i. Se você possui saldo suficiente.
    ii. Se a transação está corretamente assinada.
    iii. Se segue as regras da rede."

Assinatura Digital



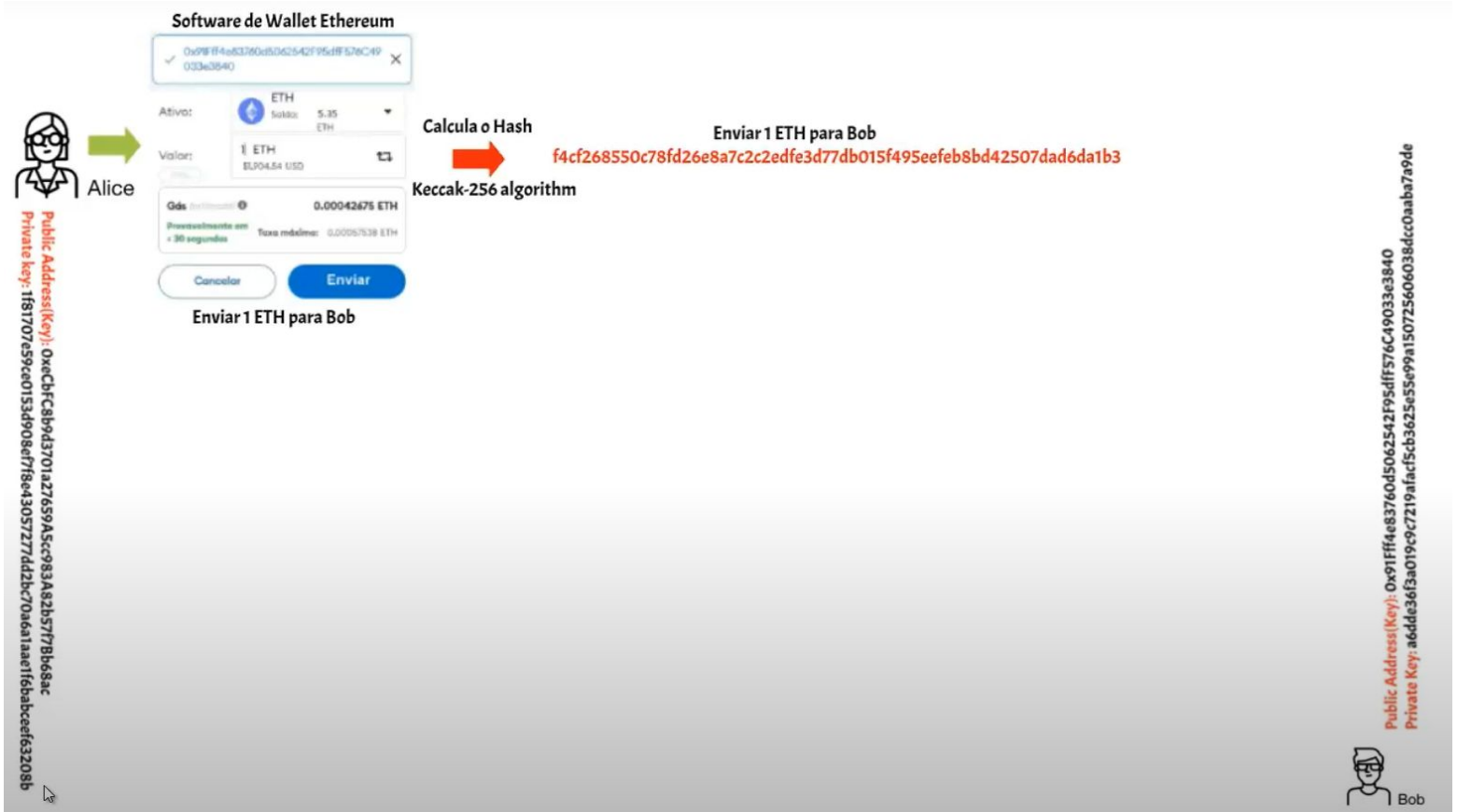
FACI wyden

Assinatura Digital



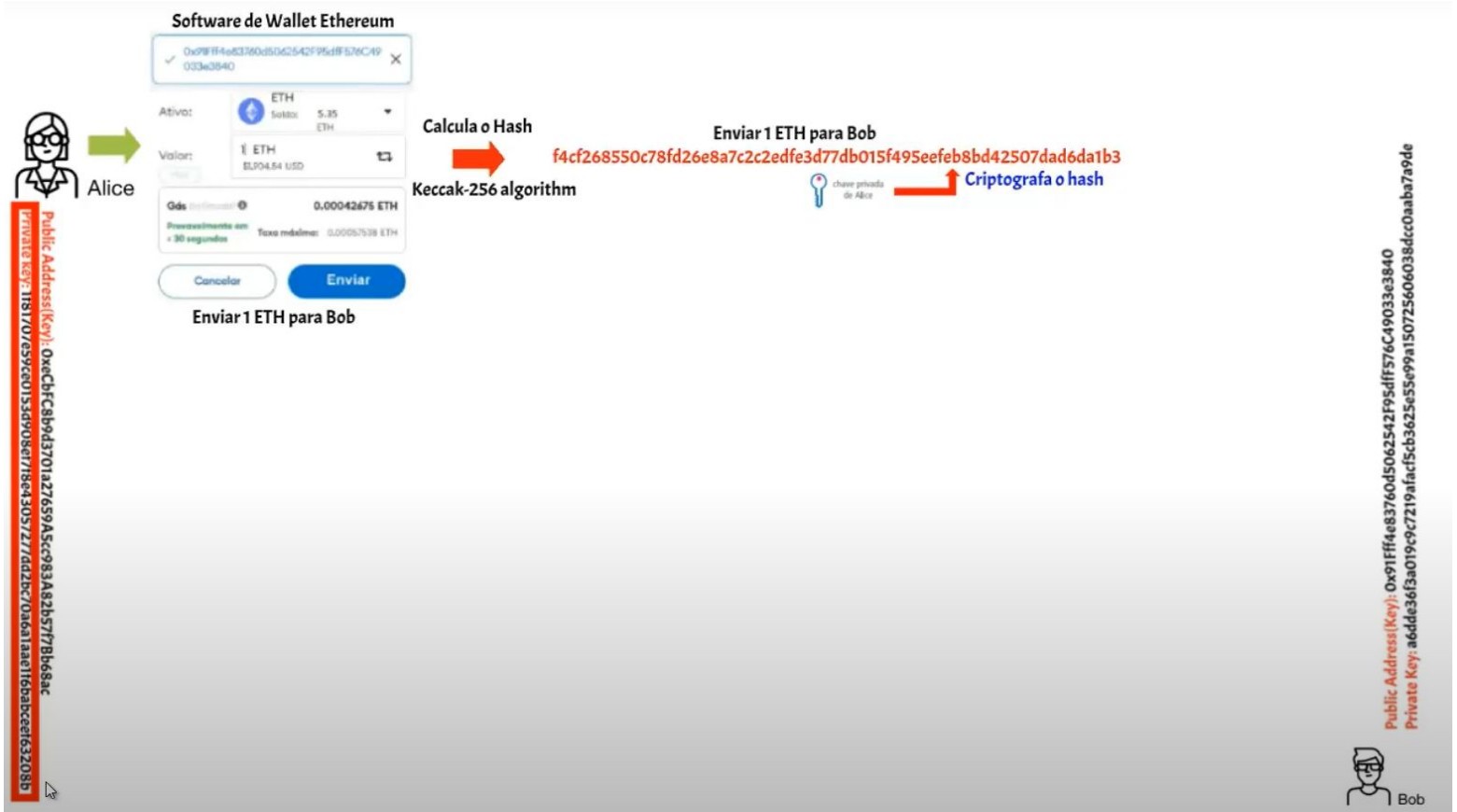
FACI wyden

Assinatura Digital

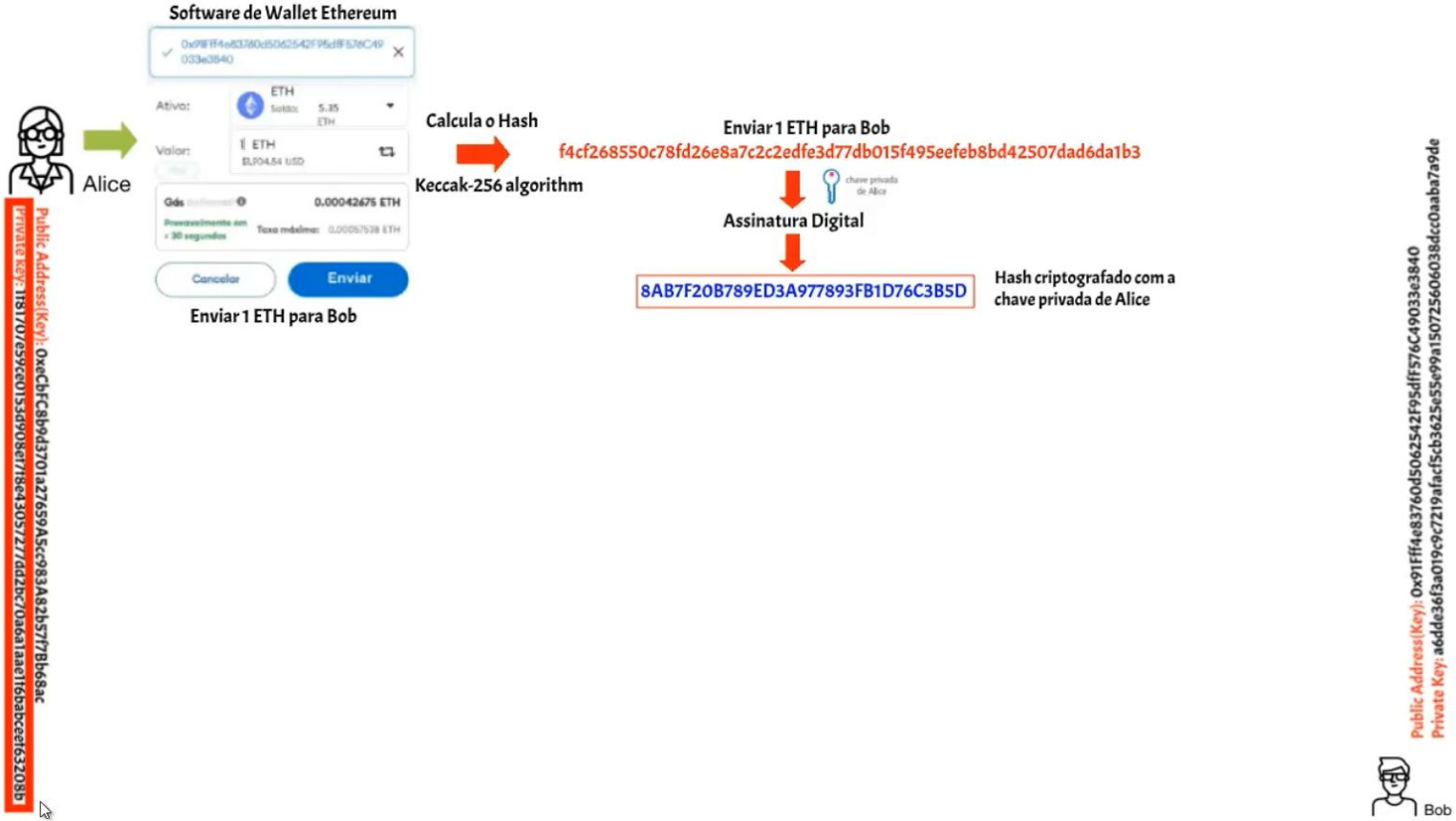


FACI wyden

Assinatura Digital



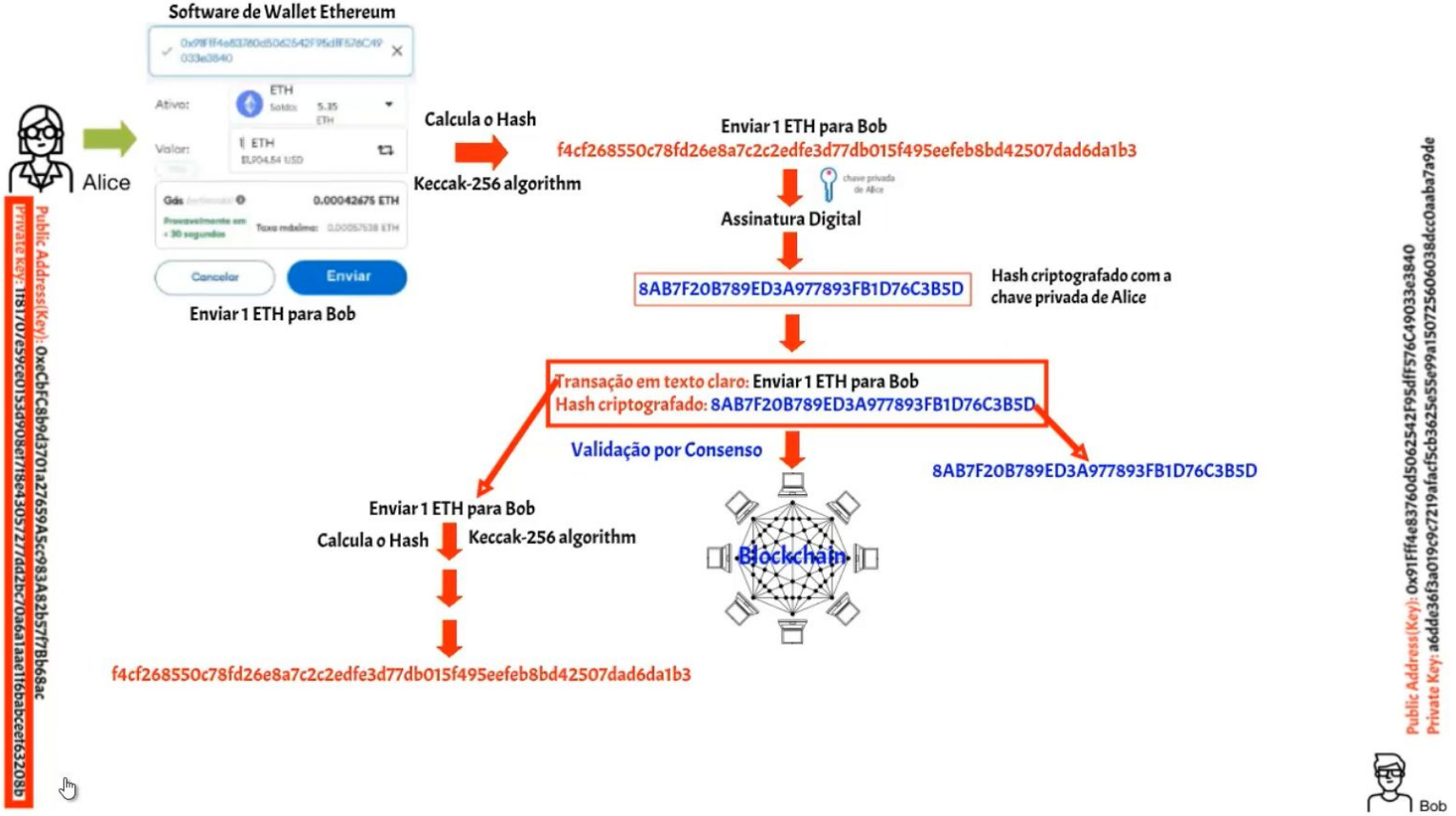
Assinatura Digital



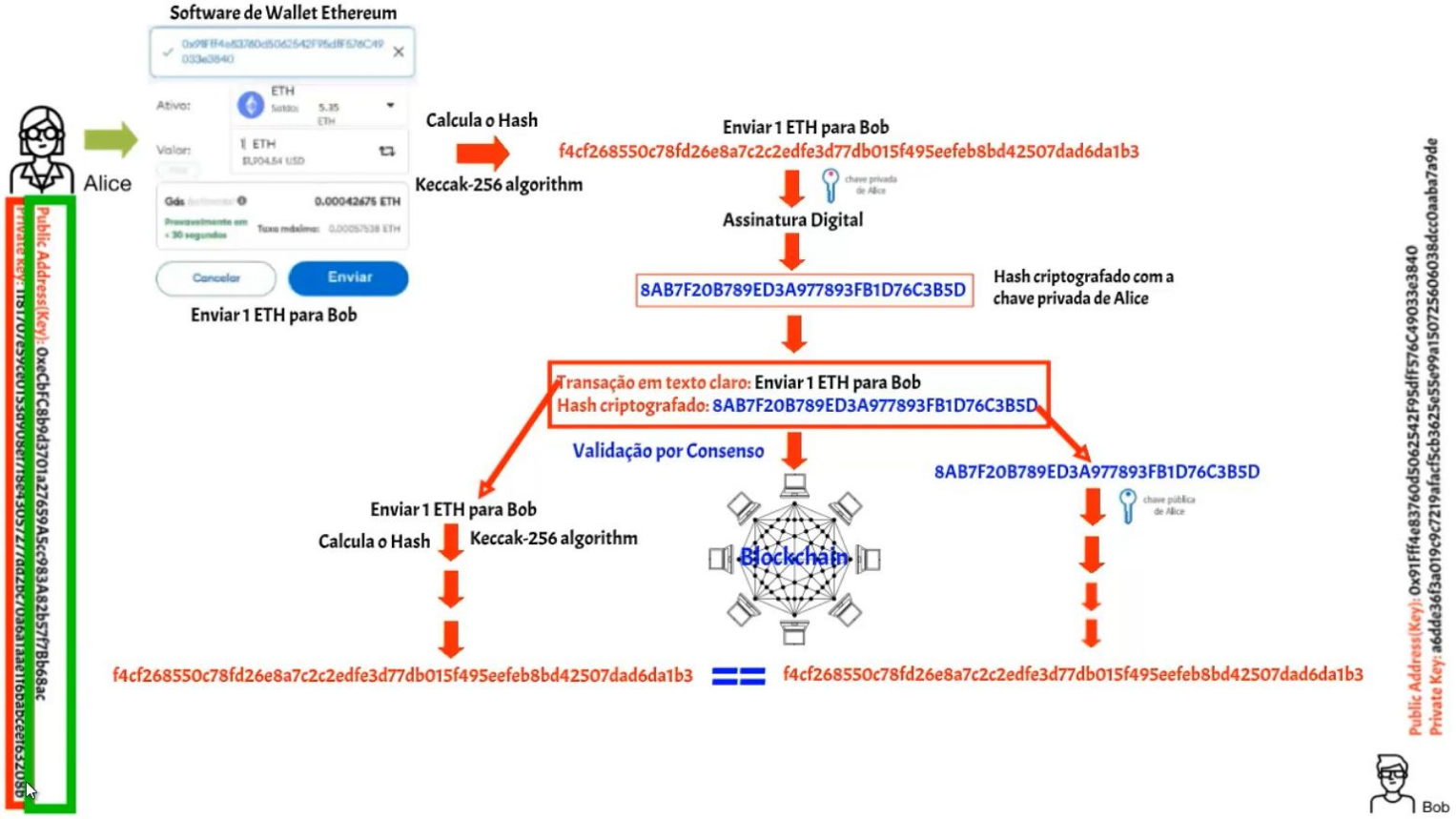
FACI wyden

Assinatura Digital

Assinatura Digital

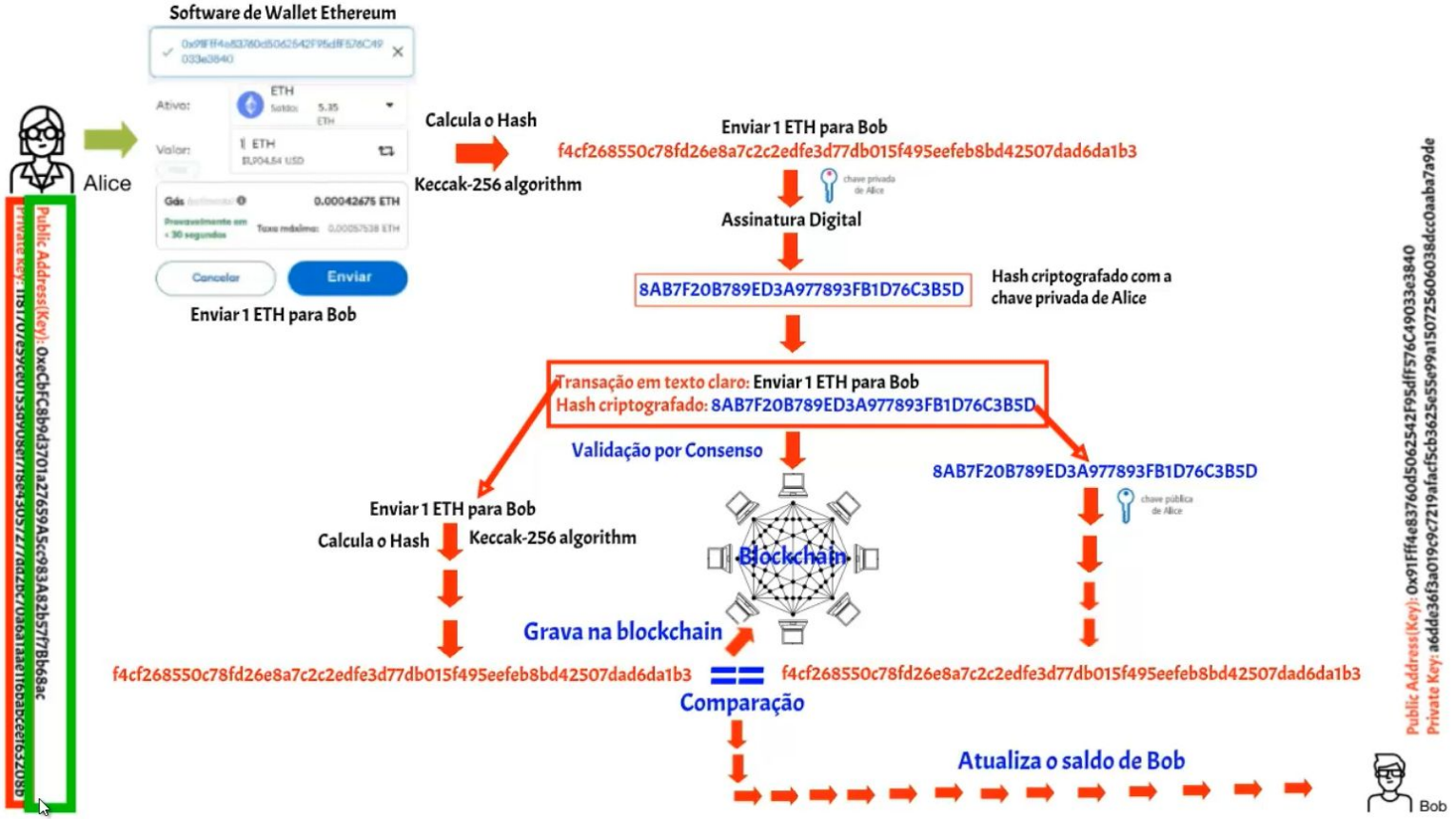


Assinatura Digital



FACI wyden

Assinatura Digital



Simulação da Ledger

- Vamos simular para você entender melhor:
  - https://andersbrownworth.com/blockchain

Segurança das Transações

- **Imutabilidade:**
  - "Uma vez que uma transação é gravada na blockchain, ela não pode ser alterada ou excluída. Isso evita fraudes."
  - "Erros não podem ser desfeitos, então é fundamental revisar as transações antes de enviá-las."
- **Importância da chave privada:**
  - "Sua chave privada é a única forma de assinar transações e acessar seus fundos. Se alguém tiver acesso a ela, pode realizar transações em seu nome."

Modelos de Blockchain: Bitcoin vs Ethereum

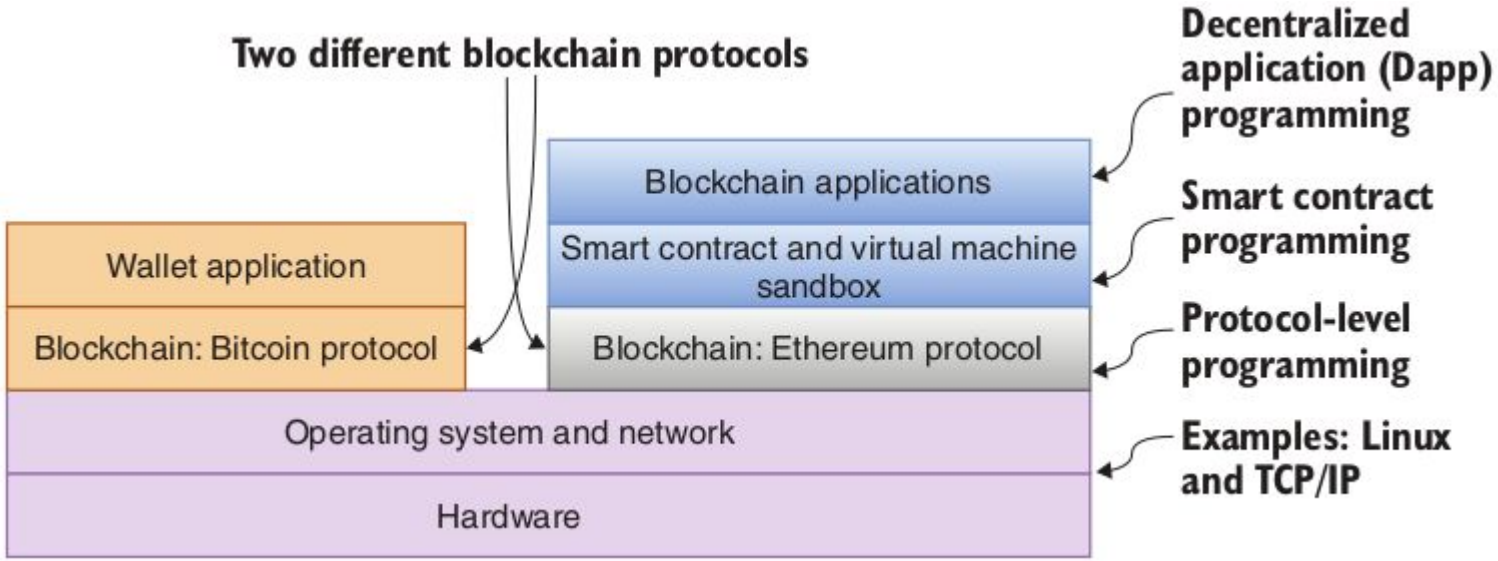
Bitcoin:

- Apenas aplicação de carteira (*wallet*).

Ethereum:

- Inclui código programável chamado **contratos inteligentes (*smart contracts*)**.
- Permite a execução de regras personalizadas.

Modelos de Blockchain: Bitcoin vs Ethereum



Níveis de Programação no Blockchain

Programação no nível do protocolo:

- Software necessário para operação do blockchain.
- Similar a sistemas operacionais ou software de redes.

Programação de contratos inteligentes:

- Desenvolvimento de regras de verificação e validação.
- Especificação de dados e mensagens a serem registrados.
- Contratos inteligentes atuam como o motor do blockchain.

Programação no nível de aplicação:

- Uso de frameworks de aplicações web, empresariais ou móveis.
- Integração com contratos inteligentes para criar Dapps.

O que são Dapps?

Definição: Aplicações descentralizadas que implementam funções de blockchain para intermediar confiança.

Características principais:

- Embutem contratos inteligentes como elemento essencial de código.
- Funcionam como aplicações web ou empresariais ligadas ao blockchain.

Contratos Inteligentes

Definição: Código imutável e executável que representa a lógica de uma Dapp.

Funções principais:

- Definir variáveis de dados e funções que representam:
  - **Estado:** Informações armazenadas.
  - **Operações:** Regras para verificação, validação e registro.
- Aplicar as regras de uma Dapp no blockchain.

Programação em Blockchain

Evolução na programação:

- Sequencial → Estruturada → Funcional → Orientada a objetos (OOP).
- Programação web, banco de dados e big data (Hadoop, Map Reduce).
- Blockchain: nova mudança de paradigma.

Exigência:

- Compreender conceitos fundamentais antes de iniciar.
- Semelhante a aprender classes e objetos em OOP.

Transações no Blockchain

Iniciadas por aplicações e execução de contratos inteligentes.

Exemplo de transações:

- Tx1: Transferência de criptomoeda.
- Tx2: Transferência de propriedade de ativo (ex.: venda de imóvel).

Regras de execução:

- Ex.: Somente o proprietário da conta pode transferir a propriedade.

Transações no Blockchain

Cryptocurrency transfer from one account to another

No-cryptocurrency transaction; current owner is the implied sender of this Tx.

```
/Tx1: */ web3.eth.sendTransaction(fromAccount, toAccount, value);
/Tx2: */ transferOwnership(newOwner);

function transferOwnership onlyByOwner (account newOwner)..
```

onlyByOwner rule validates that the sender is the owner; if not, Tx reverts.

FACI wyden

Como Funciona o Registro no Blockchain?

Transações: Verificadas, agrupadas e armazenadas em um pool.

Criação do bloco:

- Nós selecionam transações do pool para formar um bloco.

Consenso: Algoritmo assegura a validação e acordo sobre um único bloco.

Encadeamento:

- Hash do bloco atual é adicionado ao próximo.
- Criação do link entre blocos.

Tempo de Confirmação de Transações

Bitcoin: ~10 minutos por bloco.

Ethereum: 10 a 19 segundos por bloco.

Cartões de crédito: Menos de 1 segundo.

Situação atual: Blockchain ainda está em evolução, semelhante à internet há 20 anos.

Avanços no Consenso e Desempenho

Comunidade de desenvolvedores trabalha para:

- Melhorar os tempos de confirmação de transações.
- Implementar algoritmos de consenso mais eficientes.
- Adotar técnicas de retransmissão na rede.

Resumo

- **O que vimos**
  - Funções Hash
  - Criptografia Assimétrica
  - Assinatura Digital
  - Assinatura de Transações no Bitcoin
  - Estrutura de blocos
  - Importância da Ledger

FACI

wyden