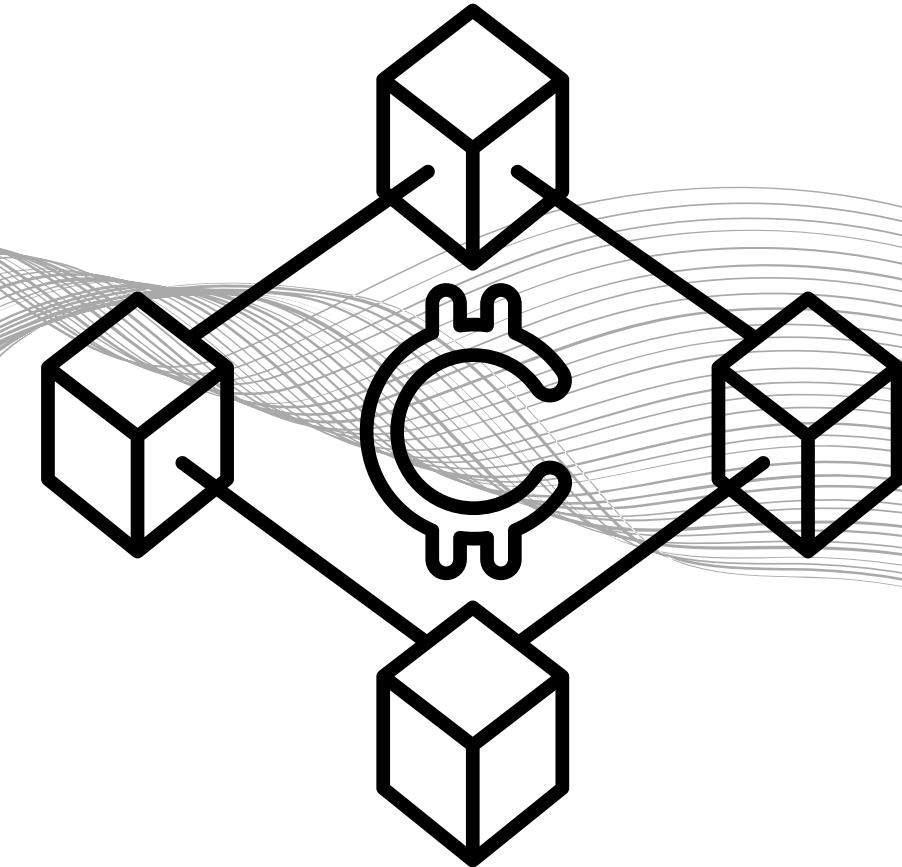


Equipe - ChainPass

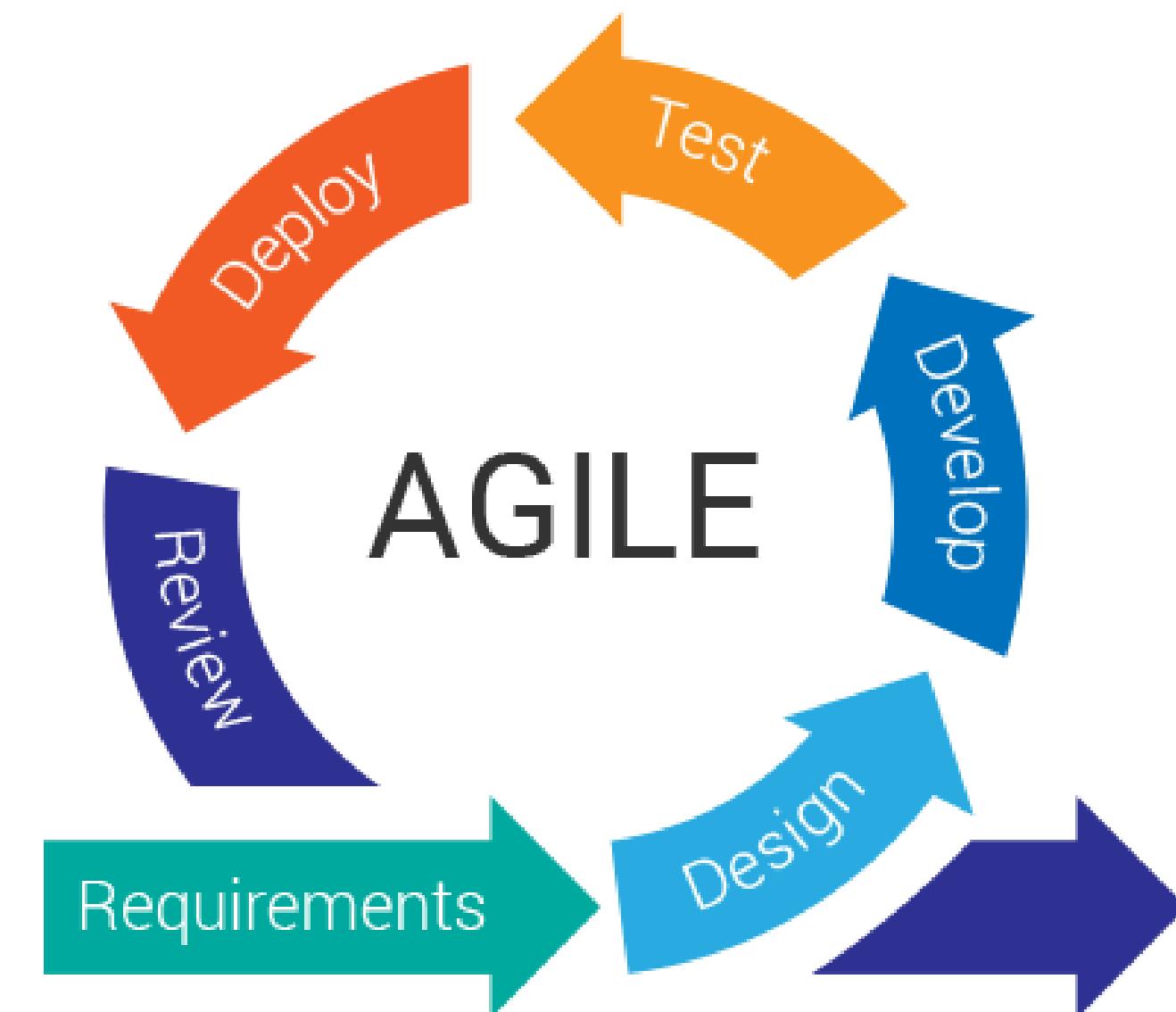
Seminário - Sprint 1: Estágio Compass UOL

BLOCKCHAIN, BITCOIN E FUNDAMENTOS



Metodologias ágeis e Scrum

Metodologias ágeis são abordagens de gestão de projetos que focam em flexibilidade e entrega contínua de valor. Ao contrário das metodologias tradicionais, que seguem um planejamento detalhado e fixo, as metodologias ágeis adotam ciclos curtos de desenvolvimento, permitindo ajustes rápidos conforme o projeto avança.



O que é Scrum ?

O Scrum é um framework ágil que fornece uma estrutura para o desenvolvimento de produtos, organizando o trabalho em ciclos curtos chamados sprints (geralmente de 1 a 4 semanas). Ele se concentra na entrega contínua de valor por meio de um processo iterativo e colaborativo.



Sprints

Um ciclo em que determinadas tarefas devem ser realizadas em um determinado período de tempo, tendo duração mínima de uma semana e duração máxima de quatro semanas

Etapas das Sprints:

Product Backlog
Sprint Planning
Sprint Backlog
Daily Scrum
Sprint Review
Sprint Retrospective

Papeis Scrum

Product Owner: Define e prioriza as user stories no Product Backlog, garantindo que refletem as necessidades do cliente.

Scrum Master: Facilita o processo, remove impedimentos e garante que o Scrum seja seguido corretamente.

Desenvolvedores: Os desenvolvedores serão quem de fato irão desenvolver a parte técnica do projeto



GIT - Conceitos Básicos

GIT é um sistema de controle de versão que permite rastrear mudanças em arquivos e coordenar o trabalho em equipe.

REPOSITÓRIO armazena o histórico de versões do projeto, incluindo arquivos e mudanças

COMMIT é uma captura das alterações no código

BRANCH é uma linha de desenvolvimento independente

MERGE integra as alterações de uma branch em outra

Convencional Commits

A Git Commit Convention é um conjunto de práticas recomendadas para escrever mensagens de commit de forma padronizada e compreensível.

O escopo geral de um Conventional Commits segue o seguinte padrão :

<tipo>[escopo opcional]: <Descrição curta>

[corpo opcional]

[rodapé opcional]

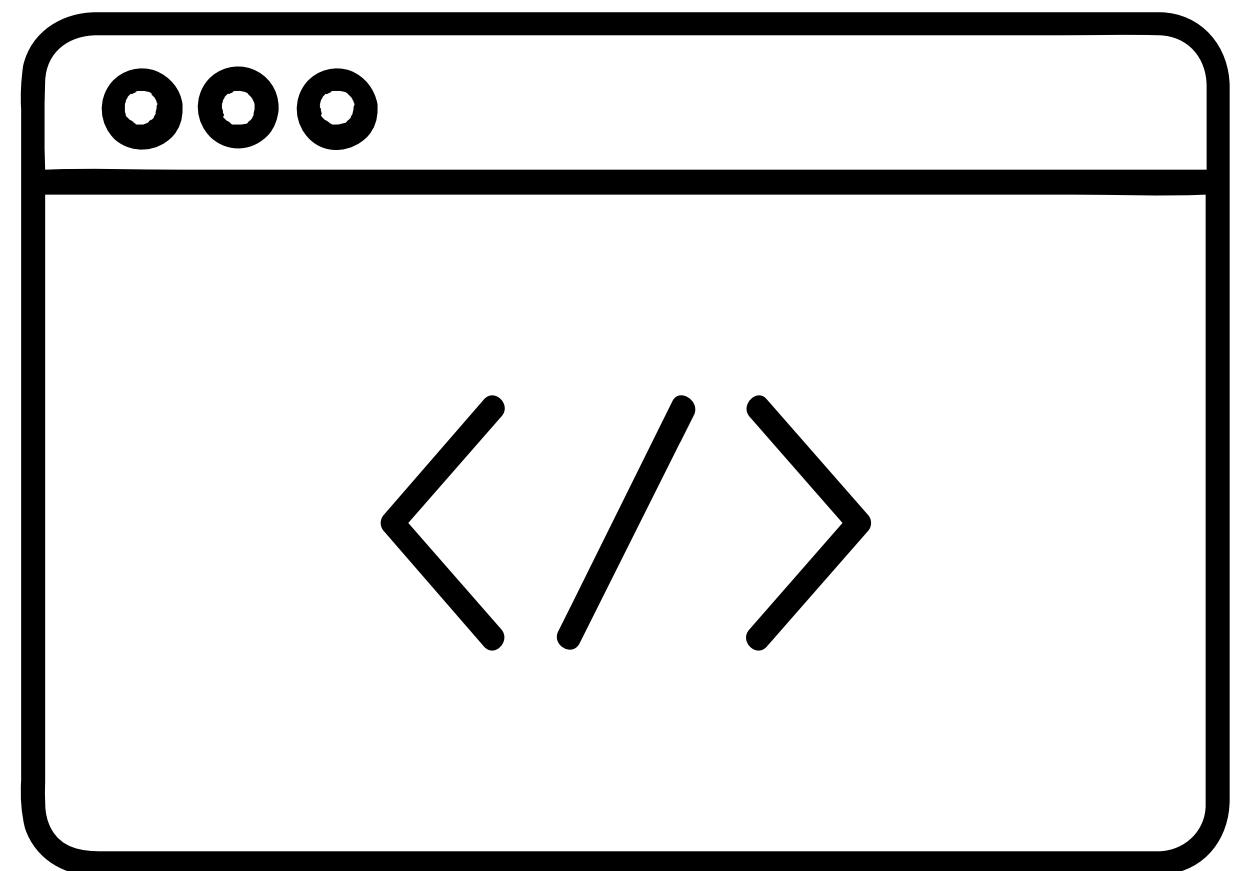


```
git commit -m "refactor: changed the markup"  
git commit -m "refactor: change the markup"
```

Tipos de Commits

O tipo indica o propósito do commit

- <chore>: Indica uma configuração no projeto;
- <fix>: Indica a correção de um bug no código;
- <feat>: Indica uma nova funcionalidade no projeto;
- <BREAKING CHANGE>: Mudança brusca no código.
- <docs>: Alterações na documentação.
- <style>: Mudanças relacionadas a formatação de código que não alteram a lógica.



Markdown

Markdown é uma linguagem de marcação leve usada para formatar texto de maneira simples. Com ela, você pode adicionar títulos, listas, links, imagens e mais, usando símbolos como #, *, e [](). O Markdown é amplamente utilizado em documentos, readme de projetos e em plataformas que suportam edição de texto.



Bitcoin & Blockchain Conceitos Fundamentais

BITCOIN, BLOCKCHAIN E PROOF OF WORK

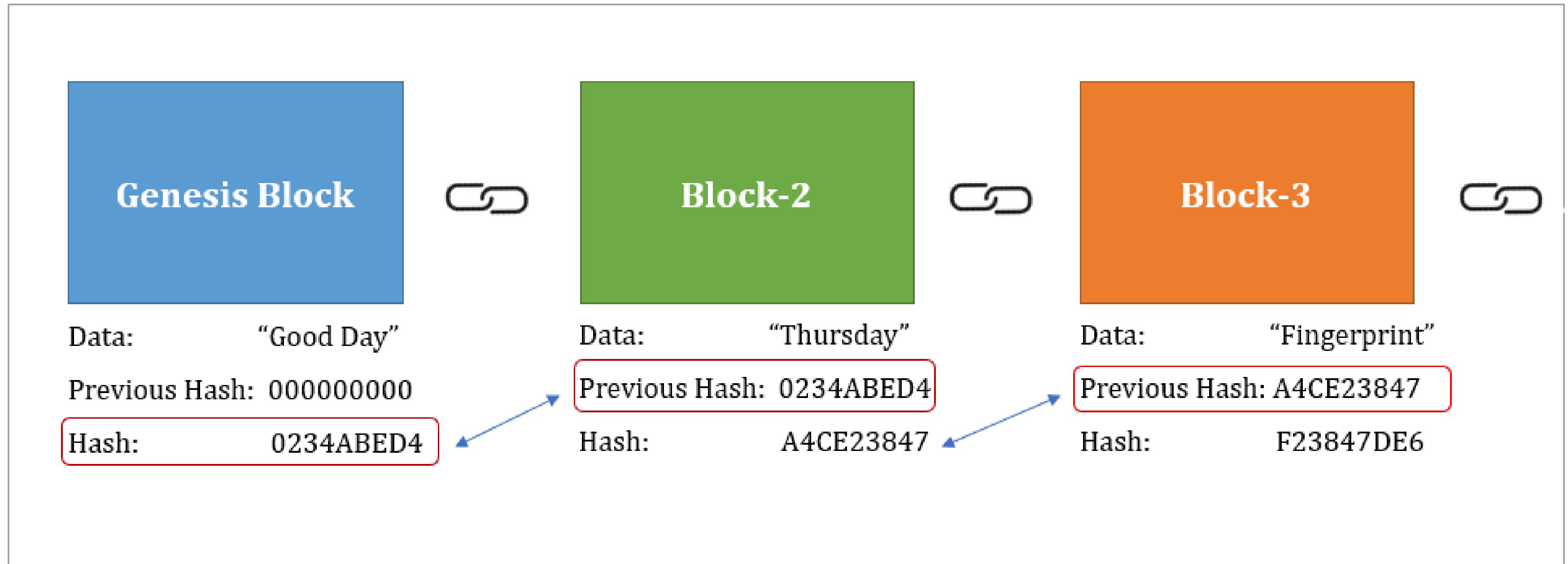
Bitcoin



Principais características

- Descentralizada
- Criptográfica
- Engenharia de Consenso
- *Blockchain*

Blockchain



Blockchain

Hash

Função criptográfica que
**recebe um *input* na
entrada e retorna um
output de tamanho fixo**

Entrada: UOL

Saída(*Hash*):

8ca09b1863c2f1d3a861684df1d3b4b0
044226fbc10a4a50921fc685e0e9a181

Principais características

- Facilidade de computar
- Livres de colisões
- Unidirecional
- "Puzzle Friendly"

Assinaturas Digitais



Chave pública



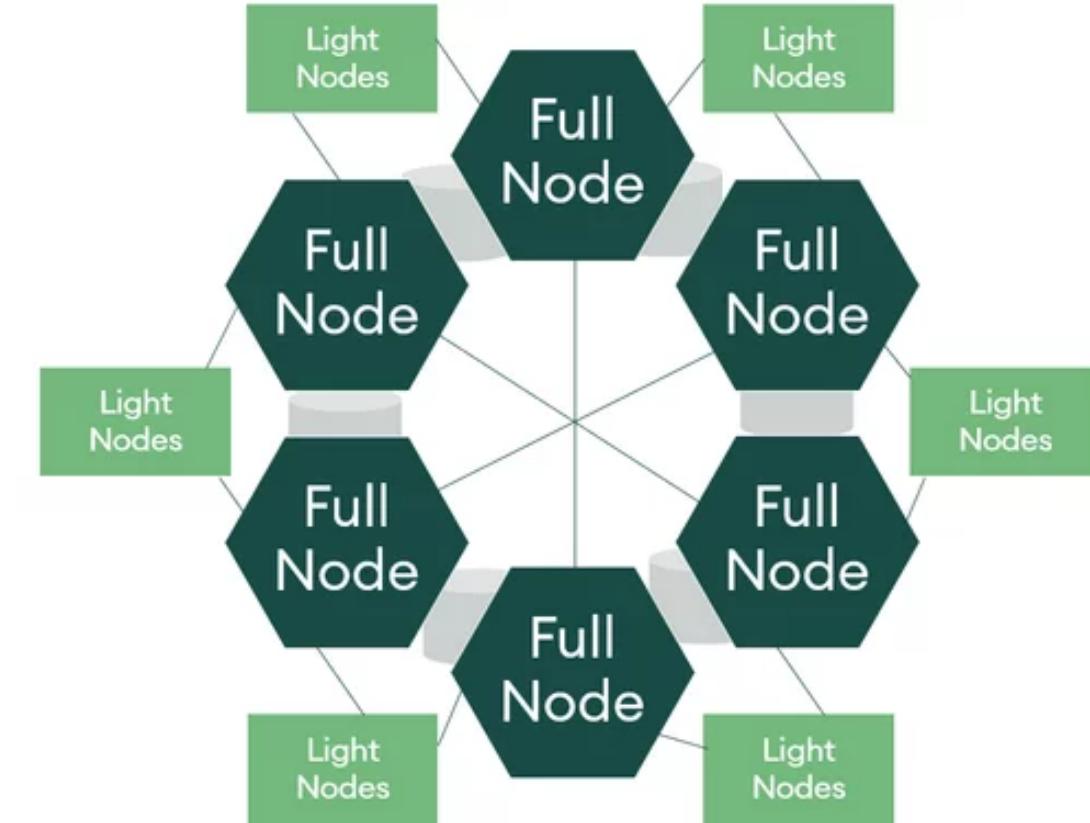
Chave privada

- Autenticar documentos no meio digital
- Única
- Chave privada: **gera** a assinatura digital
- Chave pública: **compartilhada** para que as pessoas verifiquem e validem a assinatura.

Rede Bitcoin

Descentralizada

Protocolo de consenso
compartilhado por todos os
usuários da rede.



Full Nodes: Nós que armazenam uma cópia completa da blockchain.

Light Nodes: Nós que não armazenam toda a blockchain.

A comunicação entre os nós da rede é feita por meio de um protocolo conhecido como "protocolo de fofoca" (*gossip protocol*), onde cada nó repassa as transações que recebeu para outros nós.

Proof of Work



Questões de Segurança no *Bitcoin & Blockchain*

SEGURANÇA NO ARMAZENAMENTO DE BITCOINS, CRIAÇÃO DE PARES DE CHAVES E TIPOS DE CARTEIRAS (WALLETS)

Segurança no Armazenamento de *Bitcoins*

- Ter *bitcoins* significa **ter uma chave secreta** associada a uma **chave pública** para a qual existem moedas na *Blockchain*;
- **Chave Secreta:** fundamental para garantir a segurança e o controle sobre *bitcoins*, **guardar bitcoins = guardar a chave secreta**;
- **Multiplicidade de Chaves Públicas:** usuários podem ter várias chaves públicas;
- Se uma chave secreta for perdida ou roubada, apenas os *bitcoins* associados àquela chave pública específica estarão em risco.

Tipos de Ataques no *Bitcoin*

- Muitos ataques relacionados ao *Bitcoin* não envolvem o sistema em si, mas o roubo de **chaves secretas** dos usuários;
- Permitindo que os atacantes transfiram os *bitcoins* das **chaves públicas** das vítimas, para as suas próprias chaves;
- Esses ataques não equivalem aos ataques de **gasto duplo** e **ataque de 51%**, também não comprometem a segurança do sistema do *Bitcoin* em si, mas a segurança dos próprios utilizadores.

Criação de Chaves Públlicas e Secretas

- **Geração Automática:** As chaves públicas e secretas são geradas automaticamente por softwares de carteira (*Wallets*);
- **Exemplo de Geração de Chaves:** sites como o **WalletGenerator** permitem a criação de um par de chaves;
- **Uso da Chave Pública:** Compartilhada para receber pagamentos;
- **Uso da Chave Secreta:** Deve ser mantida em segredo para garantir a segurança da chave pública.

Carteiras (*Wallets*)

- São na maior parte das vezes softwares que ajudam a guardar a chave secreta e a realizar transações com *Bitcoin*;
- Características desejadas de uma carteira:
 - Disponibilidade;
 - Segurança;
 - Conveniência.
- *Bitcoin* é mais utilizado como investimento e reserva de valor do que moeda do dia a dia, logo, a segurança é a característica mais priorizada.



Tipos de Carteiras

- Existem diversos tipos de carteiras, cada uma com um propósito, os principais tipos são:
 - Carteira de Papel;
 - Carteira de Hardware;
 - Carteira de Software;
 - Carteira Online.



Carteira de Papel

- Chave pública e a chave secreta escritas em papel;
- A **segurança** depende de onde o papel é armazenado;
- **Vantagens:**
 - Imune a ataques virtuais (se não houver cópias no computador).
- **Desvantagens:**
 - Inconveniente para uso diário;
 - Suporta apenas um par de chave pública e secreta;
 - Vulnerável em caso de perda ou destruição.

Carteira de Papel



Carteira de Hardware

- Dispositivo físico semelhante a um pen drive;
- **Extremamente seguras;**
- **Vantagens:**
 - Permite a recuperação de *bitcoins* em caso de perda do dispositivo, através de uma “semente”;
 - Suporta múltiplos pares de chaves.
- **Desvantagens:**
 - Preço elevado, sendo viável apenas para grandes investimentos.

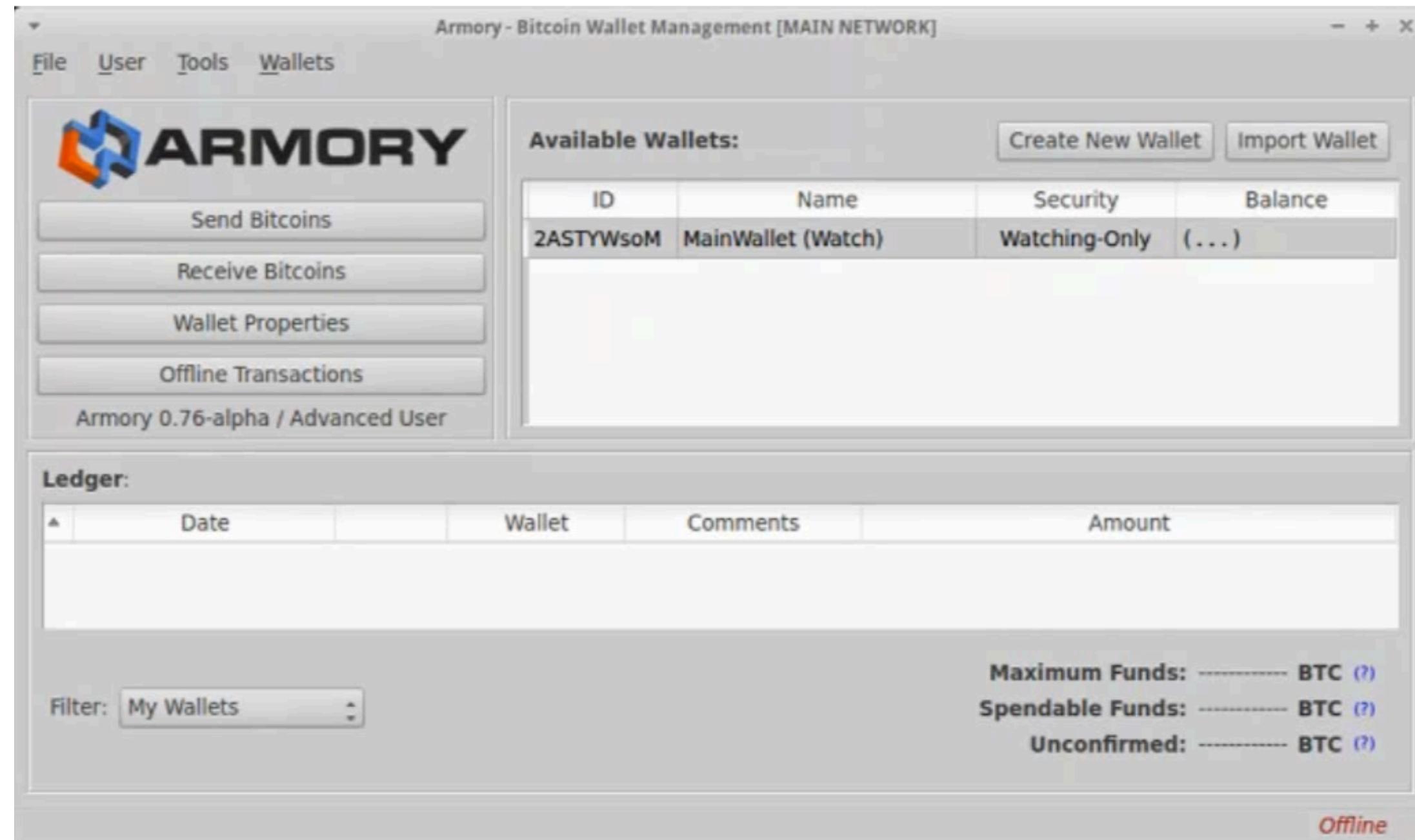
Carteira de Hardware



Carteira de Software

- Software para desktop ou smartphone;
- A **segurança** depende da segurança do dispositivo, se o dispositivo for infectado, a carteira pode ser comprometida;
- **Vantagens:**
 - Suporta múltiplos pares de chaves;
 - Funcionalidades adicionais, como conversão entre criptomoedas;
 - Praticidade no uso e envio de *bitcoins*.
- **Desvantagens:**
 - Vulnerável a ataques se o dispositivo não for seguro.

Carteira de Software



Carteira Online

- Carteira armazenada na nuvem e acessada pela internet;
- A **segurança** depende do servidor que a hospeda, havendo o risco de ser alvo de ataque hacker, e o usuário não possui acesso direto à chave secreta.
- **Vantagens:**
 - Prática e fácil de usar;
 - Ideal para pequenas quantidades de *bitcoins*.
- **Desvantagens:**
 - Não recomendada para grandes quantias, devido ao risco de perda de controle sobre as chaves.

Carteira Online

BLOCKCHAIN

BE YOUR OWN BANK.®

Total Balance
R\$344.25

DASHBOARD

Transações

BITCOIN

ETHER

BITCOIN CASH

EXCHANGE

CENTRAL DE SEGURANÇA

CONFIGURAÇÕES

FAQ

LINKS PATROCINADOS

CoinsBank

BUY BITCOIN

ToS • Política de Privacidade • Sobre

YOUR BALANCES

R\$344.25

Bitcoin: 0.00568709 BTC

Ether: 0 ETH

Bitcoin Cash: 0 BCH

PRICE CHARTS

ALL YEAR MONTH WEEK DAY

R\$8.000

R\$6.000

R\$4.000

R\$2.000

20. Nov 27. Nov 4. Dec 11. Dec 18. Dec

BTC = R\$60.532.68 ETH = R\$2.752.79 BCH = R\$7.685.81

ALERT: INCREASED NETWORK TRAFFIC

The Bitcoin network is currently experiencing record usage, resulting in longer confirmation times and higher miner's fees for transactions. Transactions are likely to be more expensive and/or take longer to complete and additional fees go directly to miners.

A screenshot of a blockchain wallet interface. The top navigation bar is blue with the title 'BLOCKCHAIN' on the left and 'SAIR' (Logout) on the right. Below the title, there's a message 'BE YOUR OWN BANK.®'. On the right, it shows 'Total Balance R\$344.25'. The left sidebar has links for 'DASHBOARD', 'BITCOIN', 'ETHER', 'BITCOIN CASH', 'EXCHANGE', 'CENTRAL DE SEGURANÇA', 'CONFIGURAÇÕES', and 'FAQ'. Below these are 'LINKS PATROCINADOS' for 'CoinsBank' and 'BUY BITCOIN'. At the bottom of the sidebar are links for 'ToS', 'Política de Privacidade', and 'Sobre'. The main content area has a large circular 'YOUR BALANCES' section showing R\$344.25. Below this are three small horizontal bars for 'Bitcoin', 'Ether', and 'Bitcoin Cash'. To the right is a 'PRICE CHARTS' section with a line graph for the month from November 20 to December 18. The graph shows a general upward trend with some fluctuations. A yellow warning box at the top of this section says 'ALERT: INCREASED NETWORK TRAFFIC' and provides a detailed explanation about the current state of the Bitcoin network. The overall design is clean and modern, using a dark blue header and light gray background for the main content.

Riscos e Benefícios

- A **escolha da carteira** depende da quantidade de *bitcoins* e das necessidades de segurança e conveniência;
- Carteiras mais seguras tendem a ser menos convenientes e vice-versa;
- É crucial pensar no tipo de investimento para escolher a carteira adequada.



Ethereum



Principais características

- Descentralizada
- Criptográfica
- *Blockchain*
- Smart Contracts
- DApps
- *Consenso*

Ethereum

Consenso

PoS - Proof of Stake

- Validação
- Staking
- Penalidades

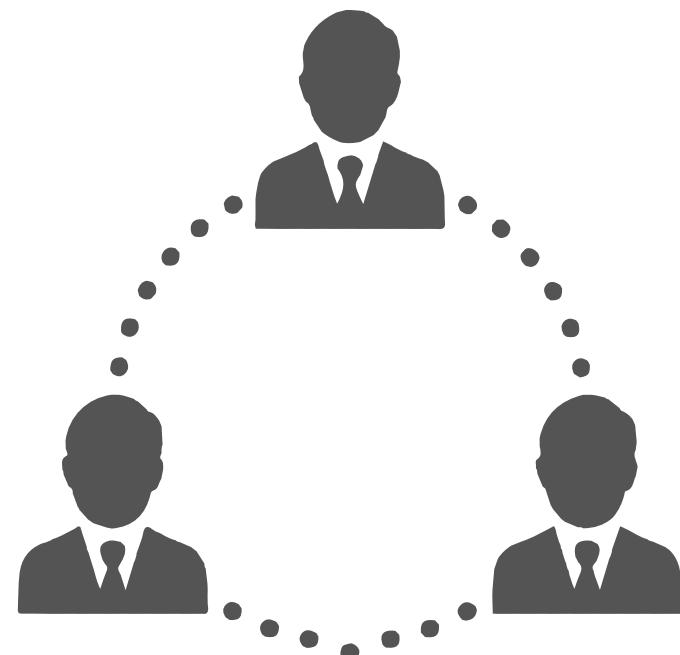
Ether - ETH

- Moeda nativa
- Gás

Blockchain no Cotidiano

Quando usar?

- Descentralização, ativos digitais e permanência dos dados;
- Contratos digitais e confiança em ambas as partes;
- Banco de dados x “Cache”;
- Necessidade de alta performance.



Blockchain no Cotidiano

Exemplos

