

# **DESCENTRALIZAÇÃO**

Sendo um *projeto código aberto*, liderado e *financiado*por um *time descentralizado*de desenvolvedores e membros
da comunidade, o mesmo não
pode ser censurado. A maioria
dos contribuidores são
voluntários e a comunidade
está espalhada por todo o globo.

## **SEGURANÇA**

Sendo uma criptomoeda descentralizada, o Monero é seguro por uma grande rede de usuários espalhados pelo mundo.

Transações são confirmadas por um consenso distrubuído e depois gravadas imutavelmente no blockchain.

#### **ESCALABILIDADE**

O <u>tamanho do bloco</u> do Monero é alterado <u>dinâmicamente</u> de acordo com o volume de transações para proporcionar taxas menores e transações mais rápidas. Assim, quanto maior o volume de transações, maior o tamanho limite do bloco e quanto menor o volume, menor o tamanho limite do bloco. <u>Bulletproofs</u> também ajuda na escalabilidade ao reduzir significativamente as taxas e o tamanho das transações, fazendo o Monero se destacar frente outras criptomoedas.



Monero usa

criptografia sofisticada como

assinaturas em anel,

transações

confidenciais em anel,

e endereços stealth

para ofuscar as

origens, quantidades

e destinatários de

# Princípios Fundamentais

Transações no blockchain do Monero não revelam um usuário em particular ou uma identidade. Desta forma, os usuários ficam livres de censura e do *controle de capital*.

todas as transações.

PRIVACIDADE

Monero é *fungível* porque ele é privado por padrão. Isso significa que um Monero será sempre igual a outro Monero. Unidades de Monero não podem ser discriminadas por vendedores ou corretoras por causa da origem ou histórico de suas moedas.

**FUNGIBILIDADE** 

RESISTÊNCIA À CENSURA

## HISTÓRIA DO MONERO

O Monero foi lançado em Abril de 2014. Foi um lançamento justo e pré-anunciado do código de referência <u>CryptoNote</u>. Não houve mineração prévia nem "instantânea" e nenhuma parcela da recompensa do bloco vai para os desenvolvedores. Veja o tópico original do Bitcointalk <u>aqui</u>.

Monero tem feito grandes avanços desde seu lançamento. Quase todas as melhorias proporcionaram avanços em segurança ou privacidade, ou elas facilitaram seu uso. O Monero continua a desenvolver com os objetivos de privacidade e segurança em primeiro lugar, e facilidade de uso e eficiência em segundo.

### O QUE SIGNIFICA MONERO?

A palavra Monero vem do idioma Esperanto. Os criadores escolheram o uso do Esperanto por este ser um idioma "descentralizado" e que representa a quebra de barreiras entre pessoas numa escala global. Em Esperanto, a palavra Monero é composta por três elementos livremente dispostos, com uma sílaba cada: mon + er + o. Que significam:

mon-: dinheiro-er-: a menor parte

-o: uma coisa (gramaticamente falando: um substantivo)

Isso quer dizer que "monero" por ser interpretado como: "um substantivo que descreve a menor parte do dinheiro". Ou, uma moeda.

## FATORES CENTRAIS DE DIFERENCIAÇÃO

- Monero usa o código-base do CryptoNote: Ele é fundamentalmente diferente do código-base utilizado
  pelo Bitcoin ou Ethereum e muitas outras criptomoedas que são derivadas destes dois. O código-base do
  CryptoNote é conhecido por suas melhorias consideráveis em privacidade.
- Privacidade é mandatória; transparência é opcional: A criptografia estado da arte utilizada no Monero oculta todas as camadas da transação: informações do remetente, destinatário ou da transação em si. Se um usuário preferir a transparência, ele poderá optar por criar e compartilhar uma carteira somente visualização que releve entradas.
- Rotina de atualização da rede: A comunidade de desenvolvedores do Monero realiza regularmente atualizações na rede (hard forks) para assegurar que todos os usuários desfrutem da melhor segurança, privacidade e recursos disponíveis. Isso permite que a rede do Monero permaneça mais ágil e segura adaptando-se a qualquer oportunidade ou ameaça que venha a aparecer. O que são todos esses hard forks que tenho lido sobre?
- Trajetória das recompensas do bloco do Monero: As recompensas diminuirão gradativamente até que a emissão em cauda comece por volta do fim de Maio de 2022, quando as recompensas serão fixadas em 0,6 XMR por bloco. A emissão em cauda permitirá incentivos continuados e indefinitivos à mineração. Adicionalmente, e talvez o mais importante, a emissão em cauda dá ao Monero inflação planejada, estável e previsível considerada essencial para o dinheiro real e saudável.

- Laboratório de Pesquisa Monero: O Monero não só é comprometido em fazer uma moeda fungível, como também pesquisa continuamente temas no domínio da privacidade financeira das criptomoedas em geral. Neste contexto, pesquisadores de Matemática e Física Computacional têm publicado white papers e possuem muitos outros objetos de pesquisa que estão sendo trabalhados.
- A mineração é acessível: Qualquer um com um dispositivo ou navegador conectado por participar.

## IMPLICAÇÕES E USOS NO MUNDO REAL

Pelo Monero ser seguro, com baixas taxas e sem fronteiras, as pessoas podem facilmente enviar dinheiro independentemente de governos ou bancos corrúptos e falidos. Isso permite o empoderamento econômico dos indivíduos em países opressores ou em depressão econômica.

Um histórico financeiro privado protege consumidores e companhias de manipulação de preços, abuso da cadeia de suprimentos, discriminação econômica, entre outras coisas. Monero é a única criptomoeda que tem os recursos necessários para funcionar como dinheiro digital completamente fungível e descentralizado.

## **FUNDAMENTOS TÉCNICOS**

(Até 14/11/2018)

Quantidade de nós ativos: 1.756 (Fonte: https://monerohash.com/nodes-distribution.html)

Taxa de hash da rede: 435,17 MH/s Média de transações/hora: 178 (média 30 dias)

Núcleos CPU protegendo a rede: 14.499.178

Monero em circulação: 16.570.126 XMR (Aproximadamente)

Capitalização de mercado: \$1.503.928.296 USD (~0.77 % da cap. total do mercado de criptomoedas)

Recompensa do bloco atualmente: 3,5984 XMR Intervalo médio entre blocos: 2 Minutos

A taxa de recompensas diminuirá continuamente até o final de Maio de 2022, quando haverão 18,132 milhões de XMR em circulação. Neste ponto uma recompensa de 0,6 XMR por bloco se manterá indefinidamente.

Com uma "emissão em cauda" de 0,6 XMR/bloco, em 2040 haverá uma quantidade igual de Monero e Bitcoin (aprox. 21 milhões)

#### **RECURSOS EM DESENVOLVIMENTO**

Embora o Monero já esteja disponível e em uso através do globo, a comunidade de desenvolvedores tem objetivos excitantes para continuar melhorando a privacidade, a segurança e a usabilidade do Monero e das criptomoedas em geral. Estas são algumas das coisas que estão por vir:

**Kovri:** Esta é uma das maiores melhorias, adicionando uma quarta camada de privacidade às transações do Monero. Kovri utiliza <u>criptografia garlic</u> (pense em Tor com esteroídes) para esconder o endereço IP dos remetentes e destinatários usando a rede. Cada camada de uma transação Monero, do remetente, destinatário, quantidade transacionada, e (com Kovri) o pilar central da transação em si, serão privados e seguros.

Carteiras Hardware: A carteira Trezor Model T adicionou o Monero às suas <u>moedas suportadas</u>. A <u>carteira hardware Ledger</u> já está disponível através da carteira GUI oficial. A comunidade do Monero financiou um time que está desenvolvendo a <u>Kastelo, uma carteira hardware de código aberto</u>, construída sob os valores do Monero. Essas opções de carteira hardware tem suporte total ao Monero.

**Kasisto:** Essa solução de <u>ponto de venda</u> é projetada para facilitar as vendas de comerciantes e empresas.

### **RECURSOS ADICIONAIS**

getmonero.org (Site oficial)
monero.how
reddit.com/r/monero
Guia do Monero (post)
Introdução Técnica ao Monero
Zero to Monero

Golpes a serem evitados
Perguntas Frequentes
Análise SWOT do Monero
Conecte-se com a comunidade
Mastering Monero - (em breve)



Monero Fatos Rápidos - Revisado em 14/11/2018 Criado para a comunidade por Monero Outreach

Monero Outreach dedica-se em aumentar a adoção e aceitação por meio da educação. Suas doações tornam isso possível.