BB INVESTIMENTOS

Criptoativos

27/04/2022

Por **Renato Hallgren, CNPI**

Criptoativos

Carta ao leitor

Este é o primeiro de uma série especial de relatórios do BB Investimentos que tratará sobre criptoativos, universo que tem despertado interesse crescente dos investidores.

Acreditamos, nesse momento, ser mais importante ao investidor entender os fundamentos técnicos e econômicos do Bitcoin do que simplesmente alocar capital em um ativo que vem ganhando cada vez mais espaço nas mídias tradicionais.

Nosso objetivo é desmistificar a complexidade do tema e fazer um paralelo com o que ele pode vir a representar no futuro dos investimentos. O primeiro relatório fala sobre o *White Paper* e o *Halving Cíclico do Bitcoin*, além dos desafios da moeda digital para se enquadrar como uma classe de ativo ou ainda como reserva de valor.

Antes de elaborar esse material, realizamos uma live sobre o tema com Marcelo Sampaio, CEO da Hashdex, a maior gestora de criptos da América Latina, e com Luiz Eduardo Faria, gestor de fundos multimercados da BBDTVM que pode ser acessada através do link: bbprivatetalks.

Abordaremos nos próximos relatórios as demais redes que emergem no mercado cripto como o Etherium, Cardano, Solana, Avalanche, Polkadot e suas aplicações no ecossistema digital que se desenvolve junto aos NFTs, Metaverso, Blockchain Games e Finanças Descentralizadas.

Por fim, apresentaremos os ETFs disponíveis para negociações no home broker do BB que poderão integrar um percentual de alocação no portifólio dos nossos investidores.

Boa leitura!

Criptoativos

Introdução ao Bitcoin

Com o avanço da internet e dos smartphones, observamos uma crescente utilização de aplicativos, também chamados de apps. A maioria das interações que fazemos hoje, via internet, são conexões em redes cujas transações são autorizadas ou validadas por terceiros (empresas, indivíduos ou governos).

Esses apps transformaram a maneira de ir ao banco, pedir comida, solicitar um táxi, alugar um imóvel, interagir em mídias sociais, assistir filmes, além dos jogos e diversas interações que fazemos na chamada internet 2.0. Todas essas aplicações são caracterizadas como interações ou transações centralizadas.

Um exemplo de transação centralizada é o PIX, que permite a transferência de valores em dinheiro entre indivíduos ou empresas, com a validação das informações por meio de servidores computacionais do Banco Central do Brasil (BCB).

Para introduzir o tema Bitcoin devemos começar pelos conceitos básicos do ecossistema cripto que são: (i) transferência peer-to-peer (P2P) e (ii) criptografia.

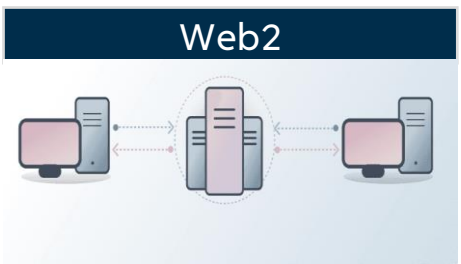
O modelo de rede e transferências peer-to-peer (P2P) significa que os usuários se conectam entre si formando uma rede descentralizada, sem a necessidade de intermediários de confiança. A criptografia, por sua vez, é um elemento fundamental para a segurança dos dados transacionáveis nas redes.

Esses dois conceitos são as bases da internet 3.0, também chamada Web3, que vem sendo desenvolvida com os avanços do Metaverso, Blockchain Games, Finanças Descentralizadas, NFT's, Realidade Virtual, Inteligência Artificial e afins.

A infraestrutura do 5G vai contribuir para a escalabilidade das interações digitais e as inovações tecnológicas, popularizadas pelo Bitcoin, serão cada vez mais percebidas com as diversas aplicações da Web3, que tem potencial de transformar a economia digital presente cada vez mais no dia a dia da população mundial.

Rede Centralizada

2004 - Atual



Rede Descentralizada

2014 - Futuro

Fonte: messari.io, ethereum.org/en/

Criptoativos

Introdução ao Bitcoin

O Bitcoin se apresenta como uma rede descentralizada que propõe a transferência de dados (informação) de um ponto a outro ponto (P2P) por meio de uma tecnologia de criptografia avançada que garante a execução de transações de forma segura.

Essa tecnologia resolveu o problema do chamado gasto duplo (*double spending*) – evitando a cópia dos dados digitais, que nada mais é do que a possibilidade de um usuário utilizar os mesmos dados (arquivos) ou a mesma moeda digital mais de uma vez –, introduzindo um algoritmo de consenso denominado prova de trabalho, ou *proof-of-work* (PoW), cujas transações são registradas em um banco de dados público e imutável chamado *blockchain*.

Além da inovação tecnológica, o Bitcoin introduziu o conceito de escassez digital, com a regra de redução gradual em sua emissão. A cada quatro anos aproximadamente, a emissão de Bitcoin é reduzida pela metade, fenômeno conhecido como halving.

Em suma, a proposta dos criadores do Bitcoin foi introduzir uma forma segura de transferência de dados sem intermediação. E ainda, com uma quantidade fixa de emissão ao longo do tempo, cria-se o conceito de propriedade e escassez digital.

Criptografia

A era da criptografia moderna começa com um trabalho realizado durante a Segunda Guerra Mundial sobre a segurança das comunicações. Mais recentemente, porém ainda antes do advento do Bitcoin, outras iniciativas em projetos de ativos digitais foram utilizadas pelas comunidades de aficionados por computação, tecnologia, privacidade e criptografia.

A DigiCash, fundada em 1989, foi o primeiro tipo de dinheiro eletrônico que usou protocolos com criptografia. No ano seguinte BitGold e B-Money apresentariam as primeiras soluções correlatas ao atual blockchain e foram pioneiras em relação à ideia de prova de trabalho (PoW).

Vale destaque para os projetos Hashcash (1992), que propunha restringir o spam de e-mails e prevenir ataques de negação de serviço (DDoS), e o E-Gold, desenvolvido em 1996 com a proposta de criar uma moeda eletrônica lastreada em ouro.

De forma geral, esses projetos foram desenvolvidos com alguma limitação de infraestrutura ou lógica computacional capaz de desenvolver uma solução descentralizada e confiável o suficiente para evitar o problema do gasto duplo.

No entanto, esses mesmos projetos ofereceram insumos para que os criadores do Bitcoin pudessem solucionar o problema do gasto duplo. Nesse período, um grupo de especialistas em criptografia denominado Cypherpunk desenvolvia discussões e iniciativas colaborativas que culminaram com a elaboração do White Paper do Bitcoin, documento que apresentou a tecnologia publicamente.

Fonte: MIT OpenCourseWare; Introduction for 15.S12 Blockchain and Money, Fall 2018

Criptoativos

Mas afinal, o que é um White Paper?

O paper é a nomenclatura utilizada na comunidade acadêmica e científica para designar uma pesquisa ou um tópico específico, enquanto o white paper é um documento oficial publicado por um governo ou organização que serve como um guia para explicar um conceito ou a solução para um problema específico, porém sem o escrutínio da academia.

No universo de moedas digitais, white paper é o resumo de um criptoativo e pode ser usado para estimular pessoas a saber mais ou usar o serviço ou a tecnologia. O white paper do Bitcoin foi divulgado em 31/10/2008 por Satoshi Nakamoto, que é o pseudônimo de um grupo ou do criador conceitual do Bitcoin.

Naquela época, Satoshi Nakamoto pretendia solucionar um problema antigo das moedas digitais que operavam nas redes de compartilhamento de arquivos via internet. O desafio proposto seria resolver o problema do gasto duplo.

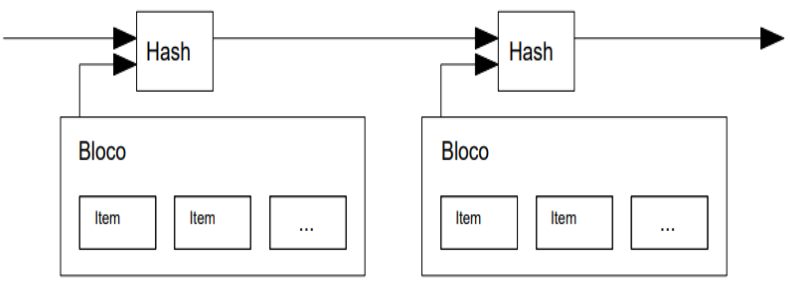
E essa solução viria através de uma infraestrutura de rede de computadores descentralizada constituída por "nós", "pontos" ou "servidores descentralizados" que validam as transações por meio de um algoritmo de consenso ou processo de mineração, chamado de prova de trabalho, ou proof-of-work (PoW). O white paper do Bitcoin contém 12 capítulos, além de um resumo e a conclusão do estudo.

Satoshi Nakamoto desenvolveu um sistema que interligaria uma quantidade de dados, agrupadas em blocos, através de um hash no qual é criado de acordo com as informações do bloco e utilizado, ao mesmo tempo, para criar o próximo bloco.

O hash é um algoritmo matemático para a criptografia que transforma um dado ou informação em um conjunto alfanumérico com comprimento fixo de caracteres.

Esse mecanismo tornou a cadeia de blocos (*blockchain*) do Bitcoin à prova de fraudes e revolucionou o sistema de transmissão de dados sem a necessidade de terceiros confiáveis.

Cadeia de blocos (Blockchain)



Fonte: MIT OpenCourseWare; Introduction for 15.S12 Blockchain and Money, Fall 2018

Criptoativos

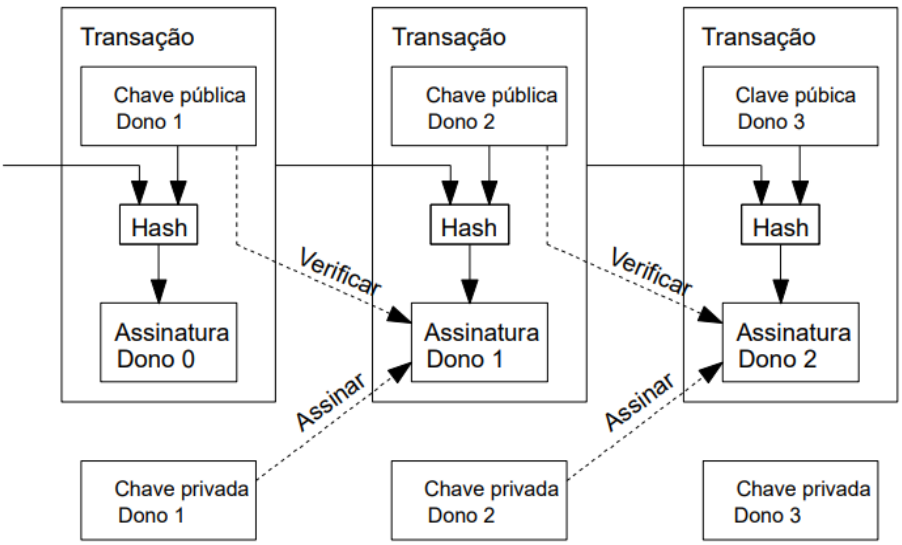
White Paper do Bitcoin

Os computadores da rede do Bitcoin utilizam softwares de código aberto para realizar cálculos matemáticos complexos o suficiente para verificar a autenticidade das transações (encontrar um hash). Essas transações são agrupadas em blocos que demoram em média 10 minutos para serem verificados, autenticados e validados.

Os servidores descentralizados da rede do Bitcoin concorrem entre si para validar uma transação através da solução desses cálculos em troca de recompensa. Dessa forma, a primeira máquina da rede que concluir corretamente o cálculo e validar a transação é recompensada com uma determinada quantidade de Bitcoins.

A recompensa dos mineradores/validadores representa um potencial gerador de receita aos participantes da rede que incorrem em custos na aquisição dos hardwares e no consumo energético para operacionalização dos equipamentos.

Cadeia de assinaturas digitais



O White Paper do Bitcoin pode ser acessado na integra pelo endereço: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt.pdf

Fonte: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt.pdf

Criptoativos

Escassez digital

O sistema de emissão de moedas e recompensa na rede do Bitcoin segue uma regra de emissão decrescente, chamado halving ou redução pela metade.

Esse mecanismo cria uma característica de escassez do Bitcoin, que o diferencia da maioria das classes de ativos.

Para manter essa política monetária desinflacionaria, o mecanismo de consenso do Bitcoin considera:

(i) intervalos de validação dos blocos em 10 minutos, *(ii)* a redução de recompensa pela metade a cada 210 mil blocos, aprox. 4 anos, e *(iii)* a emissão fixa de 21 milhões de Bitcoins.

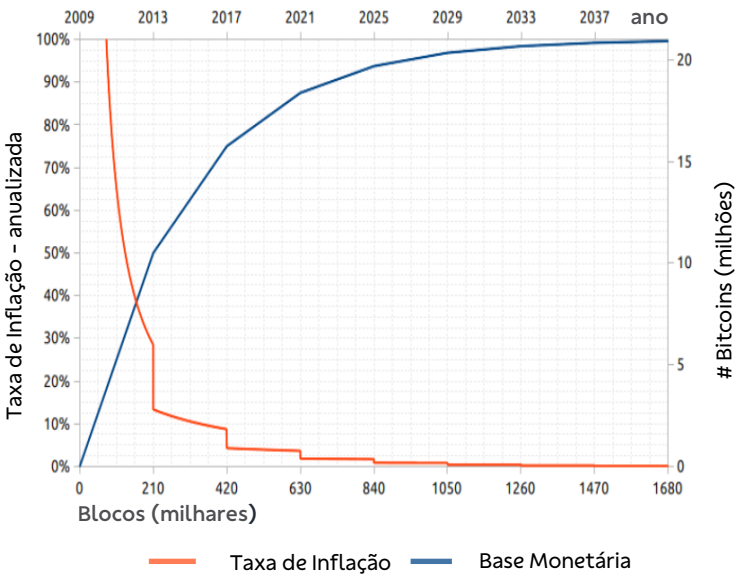
No início das validações na rede – Bloco Genesis – a recompensa foi de 50 Bitcoins por bloco validado. Os *halvings* programados já concluíram 3 períodos (vide tabela ao lado).

Até hoje foram emitidas mais de 90% da oferta total de Bitcoin.

Atualmente a recompensa por bloco é de 6,25 BTC. O próximo halving acontecerá em 2024 e o último deverá ocorrer em 2140.

A **segurança da rede e a escassez da moeda** são fatores primordiais para compreensão dos principais fundamentos do Bitcoin como um ativo digital ou como parte integrante de uma nova classe, os criptoativos.

Emissão desinflacionaria



Halving Cíclico do Bitcoin

Halving Cíclico	Bloco Genesis 01/2009	Primeiro Halving 11/2012	Segundo Halving 07/2016	Terceiro Halving 05/2020
Emissão por Bloco	50 Bitcoins a cada 10 minutos	25 Bitcoins a cada 10 minutos	12,5 Bitcoins a cada 10 minutos	6,25 Bitcoins a cada 10 minutos
Total de moedas criadas	10,5 milhões de BTC	5,25 milhões de BTC	2,625 milhões de BTC	1,212 milhão de BTC
Período	01/2009 até 11/2012	11/2012 até 07/2016	07/2016 até 05/2020	05/2020 até aprox. 05/2024
Oferta Total	10,5 milhões	15,75 milhões	18,37 milhões	+90% da oferta total

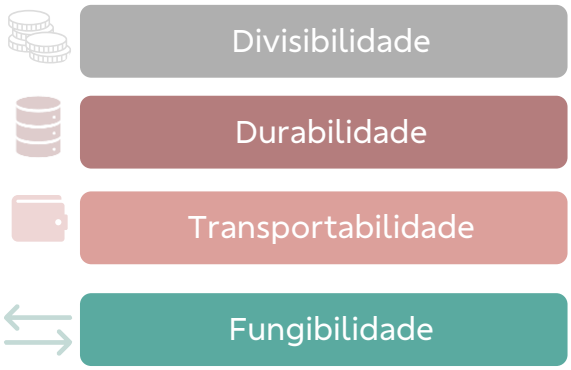
Fonte: https://www.bitcoinblockhalf.com/

Criptoativos

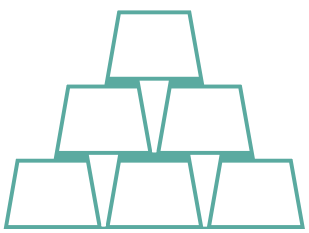
Unidade de conta em Bitcoin

Abreviação	Pronúncia	Decimais
BTC	Bitcoin	1 BTC
CBTC	CentiBitcoin	0,01 BTC
Satoshi	Satoshi	0,00000001 BTC

Meio de troca



Reserva de Valor



Funções da moeda

As funções de uma moeda, de acordo com os conceitos básicos de economia, são: medida de conta, meio de troca e reserva de valor. O Bitcoin apresenta quase todas essas características.

É divisível em até cem milhões, o equivalente a oito casas decimais, sendo a sua menor unidade de conta chamada Satoshi.

Por ser uma moeda digital, possui a característica de durabilidade e ainda apresenta o aspecto de segurança, uma vez que é impossível falsificá-lo.

É possível armazenar o Bitcoin em diferentes formas de custódia. Com isso sua portabilidade lhe confere facilidade de transportá-lo.

Por ser uma tecnologia recente na economia global, com menos de 14 anos, o Bitcoin ainda tem o desafio de se provar como reserva de valor ao longo do tempo.

A volatilidade do Bitcoin é muito elevada e a adoção da moeda ainda é pequena em função do tempo de existência do ativo digital.

Nossa avaliação é que com o avanço da adoção da tecnologia, investidores institucionais deverão ampliar a alocação em seus portfólios.

Os avanços regulatórios em diversos países contribuirão para entrada de novos investidores institucionais e também de varejo.

Entendemos que o Bitcoin atingiu o ponto de não retorno, porém a volatilidade deve permanecer alta e inversamente proporcional a adoção da moeda com o passar do tempo.

Fonte: MIT OpenCourseWare; Introduction for 15.S12 Blockchain and Money, Fall 2018

Siga os conteúdos do BB Investimentos nas redes sociais.

Clique em cada ícone para acessar.

Playlist
BB I Economia e Mercado

Canal Podcast
BB I Empreendedorismo e Negócios

bb.com.br/analises

bb.com.br/carteirasugerida

Disclaimer

Mercado de Capitais I Equipe Research

Diretor

Francisco Augusto Lassalvia

lassalvia@bb.com.br

Gerente Executivo

Alfredo Savarego

alfredosavarego@bb.com.br

Gerentes da Equipe de Pesquisa

Wesley Bernabé, CFA

wesley.bernabe@bb.com.br

Victor Penna

victor.penna@bb.com.br

Estratégia de Renda Variável e Renda Fixa

Especialista: Leonardo Nitta

leonardo.nitta@bb.com.br

Catherine Kiselar

ckiselar@bb.com.br

Hamilton Moreira Alves

hmoreira@bb.com.br

José Roberto dos Anjos

robertodosanjos@bb.com.br

Renato Odo

renato.odo@bb.com.br

Fundos Imobiliários

Richardi Ferreira

richardi@bb.com.br

Renda Variável

Agronegócios, Alimentos e Bebidas

Mary Silva

mary.silva@bb.com.br

Melina Constantino

mconstantino@bb.com.br

Bancos e Serv. Financeiros

Rafael Reis

rafael.reis@bb.com.br

Educação e Saúde

Melina Constantino

mconstantino@bb.com.br

Óleo e Gás

Daniel Cobucci

cobucci@bb.com.br

Sid. e Min, Papel e Celulose

Mary Silva

mary.silva@bb.com.br

Transporte e Logística

Renato Hallgren

renatoh@bb.com.br

Utilities

Rafael Dias

rafaeldias@bb.com.br

Varejo

Georgia Jorge

georgiadaj@bb.com.br

Equipe de Vendas

Contatos

bb.distribuicao@bb.com.br

ações@bb.com.br

Gerente – Henrique Reis

henrique.reis@bb.com.br

Denise Rédua de Oliveira

Eliza Mitiko Abe

Fábio Caponi Bertoluci

Marcela Andressa Pereira

Sandra Regina Saran

BB Securities - London

Managing Director – Juliano Marcatto de Abreu

Henrique Catarino

Bruno Fantasia

Gianpaolo Rivas

Daniel Bridges

Banco do Brasil Securities LLC - New York

Managing Director – Andre Haui

Marco Aurélio de Sá

Leonardo Jafet