Blockchain e Criptomoedas I

Professor Fabio Miguel Junges

Ceo Sou.cloud

Founder One percent

Bloco 1

* Uma experiencia
  + Tecnológica
  + Econômica
  + Politica
  + Social
  + Financeira
* Uma nova economia esta surgindo
* Documentário: Bitcoin o fim do dinheiro como conhecemos <https://www.youtube.com/watch?v=5Aqq9l73IEU>
* Artigo MIT : Muito além do NFT Metaversos web3 e o futuro digital <https://mittechreview.com.br/muito-alem-do-nft-metaversos-web3-e-o-futuro-digital/>

|  |  |  |
| --- | --- | --- |
| **Web 1.0** | **Web 2.0** | **Web 3.0** |
| **1970 - 2000** | **2000 Presente\2020** | **2020 - ...** |
|  |  |  |
| Paginas www | Midia Social | dApps (apps descentralizados) |
| html | Conteúdo gerado pelo user | Tokens, NFT Stablecoins |
| e-comerce | acesso Mobile | Dados Monetizados pelo user |
| emails chats | Apps Centralizados | VR e Ar (Meta Verso) |
| Java | Empresas monetizando dados | Blockchain, DEFI REFI SOFI |
|  | Cameras e videos HD | AI generativa |
|  |  | visão computacional |
|  |  | Realidade estendida |

* Web 1.0

Do Analógico Manual 🡪 Para o digital baseado em sistemas

* Web 2.0

Do digital baseado em sistemas 🡪 para o mobile baseado em APPS streaming e redes sociais

* Web 3.0

Dos modelos tradicionais 🡪 Para transações on-chain baseadas em blockchain com uso massivo de IA generativa

* Tecnologias
  + Cloud computing
  + Blockchain
  + Internet das coisas
  + Inteligência artificial
* Artefatos on-Chain
  + Cripto Moedas
    - É uma moeda digital descentralizada, emitida, distribuída e negociada de forma livre no mercado, não emitida\controlada por um determinado governo. Valor oscila de acordo com o mercado
      * Bitcoin
      * Etherium
      * Lightcoin
      * Monero
  + Stablecoins
    - É a representação equivalente ao Dolar, Real, Euro, etc. Emitida e controlada por uma empresa privada. Valor “travado” na sua moeda de referência
      * USDC
      * USDT
      * DAI
      * BRZ
  + CDBC’s
    - É a própria moeda emitida e controlada por um determinado país, tal qual brasil e china utilizando blockchain
    - Valor é o próprio Valor do dinheiro
    - DREX, e-any, yuan digital
  + Tokens(securities)
    - Representam um determinado ativo classificado como valor mobiliário, na forma de um token emitido, registrado, distribuído e negociado em uma determinada blockchain.
    - Valor depende do ativo
      * Equity
      * Debentures
      * Recebíveis
      * Royalties
      * Fundos
      * Imóveis
      * Dividendos
  + NFT(Non Fundgible Tokens)
    - Representam um determinado ativo ,beneficio, acesso, na forma de um NFT, emitido, registrado, distribuído e negociado em uma determinada blockchain. Valor depende da utilidade
      * NUCOIN
      * STARBUCKS
      * MERCADOPAGO
      * Colecionáveis
      * Artes
      * Tickets
      * Benefícios
* Criptomoedas
  + Uma nova classe de ativos (digital e global)
  + Uma nova expressão monetária
  + Uma nova infraestrutura tecnológica (Blockchain)
* Livro **Bitcoin: A moeda na era digital**[**Fernando Ulrich**](https://www.amazon.com.br/Fernando-Ulrich/e/B07JL5NC6Q/ref=dp_byline_cont_book_1)**(Autor)**
  + Satoshi Nakamoto
  + Um Sistema de dinheiro eletrônico Peer to peer 31/08/2008
  + Problema dos generais bizantinos
    - Como coordenar informações em uma rede distribuída como sincronizar informações em uma rede distribuída
  + Bitcoin não foi o primeiro a tentar criar uma moeda digital, outros exemplos que vieram antes e falharam
    - E-gold -1996
    - Webmoney – 1998
    - Liberty Reserve -2006
    - Perfect Money -2007
  + Por que falharam?
    - Centralização
    - Gasto Duplo
    - Regulamentação
    - Uso para fins ilícitos
  + Por que o Bitcoin deu certo?

1. O problema do gasto Duplo
   * + - Tudo o que é digital é por essência facilmente duplicável
       - Dinheiro Digital não pode ser duplicável
       - A blockchain da bitcoin promove uma primeira solução tecnológica para que isso seja efetivamente viável, possível de ser resolvido sem a necessidade de um intermediário
2. A desintermediação
   * + - Transações entre duas partes (P2P) sem o intermediário garantidor
3. Base de dados distribuída (Ledger distribuído)
   * + - No sistema tradicional temos o registro, a base de dados centralizada, ou seja, todas a transações acontecem dentro de um banco de dados monolíticos.
       - Na blockchain cada nó da rede tem todos os registros atualizados em tempo real, (Lógica dos generais bizantinos) sincronizados de forma que cada um dos nós tenha a mesma informação devidamente atualizada, sincronizada, e que permite que a qualquer momento possamos consultar esses registros em qualquer uma dessas bases distribuídas em todos os nós da rede.
   * Bitcoin (Economia)
     + É uma nova forma de dinheiro e pode se manifestar de 2 formas
       - Moeda
         * Real
         * Dólar
         * Euro
       - Ativo Financeiro (Investimento)
         * Ouro
         * Ações
         * Comodities
     + Global
     + Livre Mercado
     + Puramente digital
     + Divisível por 100 milhões
     + Não governamental
     + Limitado a 21 milhões de unidades
   * Blockchain (tecnologia)
     + É uma base de dados distribuída (DLT) que torna possível criar um registro digital de transações que podem ser compartilhadas, monitoradas e mantidas por uma rede distribuída de computadores. Uma **cadeia de blocos** conectados sequencialmente, cada bloco com um conjunto de transações.
       - Segurança
       - Imutável
       - Desintermediação
       - Não falsificável
       - Ledger distribuído
       - Resolve o gasto Duplo

<https://bitbonkers.netlify.app/> A BITCOIN TRANSACTION VISUALISATION

Fim Bloco 1

Bloco 2

* Criptomoedas
  + Bitcoin
    - Grau de dificuldade
      * O algoritmo da bitcoin é calibrado para que o tempo médio de cada bloco seja mais ou menos 10 minutos. Quando mais máquina eu tenho minerando na blockchain maior o poder computacional da rede e menor o tempo do bloco. Para ajustar o tempo para orbitar 10 min existe o grau de dificuldade. Esse parâmetro é ajustado pelo algoritmo a cada 2069 blocos o que com o tempo de 10 minutos é aproximadamente 2 semanas. Com isso independente do numero de maquinas conectado o tempo deve sempre orbitar 10 minutos para o processamento de um bloco.
    - Hash Rate
      * O processo de mineração nada mais é do que a maquina fazer uma tentativa aleatória de um código hash que combinado com outros parâmetros tem que dar um resultado X. Não é um cálculo matemático para resolver, é tentativa e erro, é loteria. O conceito **não** é que a máquina mais poderosa vai calcular mais rápido e vai resolver um problema matemático. Mas sim que a máquina mais poderosa vai conseguir tentar mais vezes por segundo e quanto mais bilhetes de loteria você tem maior é a sua chance de vencer, mas não a certeza, você pode apostar um bilhete e vencer, mas quanto mais hashs gerados maior a chance.
      * Com essa mecânica de tempo por bloco, grau de dificuldade, hash de tentativa e a recompensa clara é como a blockchain resolve o problema dos generais bizantinos.
    - Blockchain e bitcoin(Protocolo)
      * Aborda sobre bloco, tempo de bloco como minerar regra de halving(cada 4 anos cai pela metade a recompensa de mineração por bloco)
    - Chave pública e chave privada
      * O Ledger nada mais é do que o registro onde você tem uma “conta” que se chama chave pública, que é como se fosse um cofre transparente, **o saldo da chave pública é visível a todos com acesso a blockchain.** Porém é necessário ter uma chave privada para assinar as transações. A chave privada administra a chave publica. Somente com a chave privada transações são efetivadas na chave publica.
        + Chave Pública: Representa o endereço do armazenamento da meda (bitcoin)
        + Chave Privada: Serve para assinar; autorizar transações
      * O bitcoin Nunca sai da blockchain, ele é nada mais doque um registro no endereço publico da walet que tem o saldo. Bitcoin é um registro na blockchain de um saldo que você tem em uma determinada carteira
      * Se eu perco o acesso à chave privada eu perco o acesso ao BITCOIN porém o saldo continua na blockchain
      * A chave Privada é um número escolhido aleatoriamente
      * Na bitcoin o número de chaves privadas possíveis é de 2 elevado a 160
        + Não existe poder computacional hoje para contar esse número, por isso a quantidade de chaves privadas que pode ser criada é virtualmente infinita.
      * A Chave privada é um número gigantesco, criado aleatoriamente. A partir da chave privada é criada c chave pública, porém a partir da chave pública não é possível retornar a chave privada.
      * Como criar uma chave privada?
        + <https://bitaddress.org/>
    - Carteira
      * Na bitcoin uma carteira é utilizada para gerenciar a **chave privada** que é utilizada para “Assinar” as transações
      * O seu bitcoin nunca esta na carteira ele é representado como um saldo na blockchain, no endereço da sua chave publica
    - Como fazer a minha primeira compra de bitcoin
      * Comprar através de uma corretora (Exchange)
      * Compre peer to peer diretamente de alguém
      * Lado bom Exchange
        + Depende da Exchange
        + Not your key not your coins
        + Receita federal sabe do seu saldo
        + Você tem que declarar
      * Lado ruim Wallet própria
        + Perdeu a chave privada é game over perdeu tudo
* O bitcoin inaugura uma nova era de sistemas eletrônicos e transações financeiras em que o dinheiro passa a ser programável. Smart moneym podemos programar regras de negocio para transações autônomas, regras de negocio na camada do dinheiro
* Bitcoin
  + Perspectiva 1
    - Ativo financeiro
      * Comprar BTC(P2P, Corretora)
  + Perspectiva 2
    - Moeda
      * Aceitar BTC como meio de troca por produtos e serviços
  + Perspectiva 3
    - Tecnológica
      * Fazer parte da rede de mineradores
  + Premissas econômicas de uma moeda
    - Ser um meio de troca
    - Ser uma unidade de valor
    - Permitir a reserva de valor
  + Altcoins (alternative coins)
    - Todas as outras moedas exceto o bitcoin
    - Até agora nenhuma outra moeda foi tão posta a prova e tão validada e tão testada quanto o bitcoin
  + Bitcoin ou Ether
    - Depende do objetivo
      * Para transação como moeda Bitcoin
      * Para tokenização Ethereum

Fim bloco 2

Existe algum levantamento da quantidade de chaves privadas perdidas?

Não temos como saber, o que se sabe é que tem mais ou menos 3 milhões de bitcoins que estão em carteiras que não são movimentadas a mais de 10 anos.

Porém não é possível afirmar que estas chaves estão perdidas. Estima-se que algo em torno de 20 a 25% das bitcoins estão perdidos, mas não se pode afirmar com certeza.

Bloco 3

* Como funciona uma transação em blockchain?
  + No momento que uma transação é assinada ela é submetida para a rede blockchain em um lugar chamado main pool, que é um pool de transações pendentes.
  + A rede distribuida da blockchain tem os seguintes papeis
    - Validar transações
    - Minerar(criar) novos bitcoins
    - Consenso e confiança distribuida
      * Mecalf’s law: o efeito da rede é proporcional ao numero de nós ao quadrado
  + Halving
    - Quando a quantidade de Bitcoins como recompensa por um bloco minerado cai pela metada
    - O Halving acontece a cada 210 mil blocos, ou aproximadamente a cada 4 anos.
  + Após a transação ser submetida para a blockchain os mineradores trabalham para validar a transação
  + Elas fazem isso indo no pool de transação e pegam todas as transações pendentes para processar, dando preferencia para as transações que pagam taxas maiores, e escrevem essas transações no bloco. A combinação do hash das transações, com o hash do cabeçario do bloco, que está vinculado com o hash do bloco anterior, da um hash final que essa maquina vai testando com outros hashes e fazendo teste de validação para que a soma desses dois hashes represente no final um numero de zeros a esquerda, **e a quantidade de zeros a esquerda é o grau de dificuldade**, quanto mais zeros a esquerda precisar preencher, maior o grau de dificuldade. Quando a máquina encontra o hash que combinado com o hash das transações e combinado com o hash do cabeçario, representa o número de zeros a esquerda, de acordo com o grau de dificuldade, a maquina relata ter descoberto o bloco. Nesse momento toda a rede olha para esse bloco e verifica os parâmetros. A máquina esta com o grau de dificuldade certo? A recompensa esta correta? as transações estão corretas? Caso tudo isso esteja correto o bloco inteiro incluindo a transação inicial é incluída na blockchain e a máquina que resolveu primeiro esse bloco é recompensada com novos bitcoins mais taxas sobre as transações.
  + Após o novo bloco ser adicionado a blockchain somente a máquina que primeiro descobriu o bloco com os parâmetros corretos é recompensada, todas as outras não ganham nada e após isso um novo bloco começa a ser minerado.
  + A rede reconhece o novo bloco em todos os nós (consenso)
  + A transação é concluída
  + O software do bitcoin sempre valida os parâmetros e caso algum deles esteja adulterado, aquele resultado é ignorado
  + Transações realizadas em blockchain são teoricamente imutáveis
  + Quanto mais antigo o bloco mais improvável é uma mudança de algum registro que naquela blockchain foi feita
  + Logica baseada na Proof of work
  + Só faz sentido colocar a maquina para trabalhar se for de acordo com as regras
  + A blockchain do bitcoin é a blockchain que inspiram todas as outras
* Pontos para não ignorar este mercado

1. Pessoas já não são mais necessárias para operar o dinheiro

* O dinheiro digital, programável, não reconhece fronteiras não reconhece pessoas
* Não importa se você é uma pessoa, uma geladeira, um carro, um celular ou um device qualquer
* Pessoas, máquinas, sistemas ... todos agora são iguais e podem operar esse dinheiro digital
* Esse é um dinheiro programável

1. A criação de um sistema integrado

* Hoje o sistema financeiro é uma miscelânea de sistemas diferentes, um emaranhado de sistemas que precisam se conversar
* Com o core dessas operações em blockchain vamos ter um alinhamento desses sistemas
* Pode ser um sistema que unifica todas as transações entre diferentes partes do sistema bancário

1. Bitcoin não esta tentando substituir a moeda nacional de um pais

* Bitcoin é uma nova forma de representar o dinheiro
* Bitcoin não compete com bancos, porque ele não foi criado para esse habitat
* Bitcoin não compete com dinheiro em papel poque ele foi criado com outro proposito
* Bitcoin não é o dinheiro para o mundo físico
* Bitcoin não é para ser um dinheiro de alguma nação, isso é pouco para ele

1. Streaming, bitcoin e a noção de tempo em relação ao dinheiro

* Dinheiro como fluxo, como experiencia
* Acabou a logica do dinheiro em time slot

1. Restrições do sistema atual e jovens entrando nesse mercado
2. O primeiro artefato digital com histórico eterno

* Quanto mais antiga a transação mais imutável
* Não existe outro sistema que prove esse grau de imutabilidade

1. Bitcoin foi criado para um mundo com internet os outros sistemas não
2. Neutralidade e inovação

* Você não precisa pedir permissão para inovar em blockchain

1. Inversão de infraestrutura já ocorreu varias vezes na sociedade moderna
2. Bitcoin/blockchain é uma grande plataforma, um conjunto de concentos harmonizados