- O que é BlockChain?
    - Colocar um timestamp em um documento digital
    - Evolução para cadeias de timestamps (carimbo de data), (listas contínuas)
    - Lista crescente de registros chamados de blocos
    - Uma cadeia de blocos - BlockChain
    - Utiliza função hash para criptografar as conexões sobre blockchain

- Características
    - Não pode ser corrompida
    - Descentralizada - várias cópias em diversos locais
    - Registros Distribuídos, registros mantidos por diversos usuários
    - Consenso, algoritmo de consenso que serve para validar a aceitação de registros na blockchain, esse registro é válido?
    - Acordos mais rápidos - em comparação a TED por exemplo

- O que é:
    - Desejo inserir na blockChain dados: “Max”
    - Além do dado, o **bloco atual** tem o hash do bloco anterior e o hash do bloco atual.
    - Se for o primeiro bloco (bloco gênesis) o hash anterior será 0000000.
    - Assim e forma a cadeia de blocos, com referências aos blocos anteriores

- Entendendo hash
    - Cada arquivo tem um hash único
    - Hash sem retorno, somente conversão para o hash.
    - Determinístico, para a mesma informação sempre se gera o mesmo hash.
    - Processamento rápido
    - Efeito avalanche - qualquer mínima alteração do arquivo deve gerar um hash completamente diferente.
    - Deve suportar colisões
    - EX. Hash SHA256 - 64 Caracteres

- Registros imutáveis
    - Verificação através do hashing do bloco anterior torna imutável
    - Ao inserir o bloco na blockchain, ele não é mais modificável, afinal, caso mude um bloco no meio, perde o registro de todos os blocos anteriores, afinal, irá modificar o hash

- Rede p2p distribuída
    - No mundo comum as informações estão centralizadas, em um hd, em um contrato de papel e é perdida em caso de algum incidente sobre essa central
    - A rede é descentralizada, múltiplas partes interessadas contém cópias, informações sobre toda a rede.
    - Caso alguma parte seja perdida, a informação não é perdida
    - A informação armazenada é a cadeia de blocos
    - Caso algum computador (interessado) sofra algum ataque, modificando o conteúdo de algum bloco, esse computador verifica que os seus dados estão diferentes de todos os demais.

    - Ao verificar isso ele descarta sua informação e recopia a cadeia dos demais computadores para garantir a integridade
    - Os dados modificados anteriormente pelo ataque foram descartados

- Mineração
    - Gerar um hash válido com os dados do bloco
    - Existem dados em um bloco, transações monetárias por exemplo.
    - Existe o hash atual e do bloco anterior
    - Número do bloco
    - Nonce - valor variável. Esse valor é alterado para conseguir achar um hash que comece com quarto 0s (0000)
    - A mineração vai alterando as informações, o nonce até achar um hash válido
    - quando achar, enviar para rede e esse bloco é válido
    - A rede vai validar se o conteúdo do bloco está na fila de transações (no caso do bitcoin ele valida se o conteúdo do bloco, as transações, estão na fila. Garantido que a única informação modificada é o nonce)

- Protocolos de consenso
    - Proof of Work - Pow - Há um objetivo a ser alcançado (em bitcoin, achar os 4 primeiros dígitos com 0) - ao cumpri-lo você ganha uma porcentagem de bitcoin
    - Proof of Stake - Pos - É validado com base na quantidade de moedas que um minerador possui. - usado no ethereum
    - Byzantine fault tolerance - BTF - usado pelo hyperledger - Não pode ter mais que ⅓ de nós atacantes. Rede permissionada, você controla q