Blockchain e criptomoedas II

Bloco 1

Blockchain e Bitcoin são protocolos

* Hard wallet
  + É um dispositivo que se pode armazenar várias criptomoedas
* Wallets
  + As wallets são classificadas em duas grandes categorias
    - Hot-Wallets
      * São wallets que estão on-line, elas estão conectadas na internet de alguma forma
    - Cold-Wallets
      * São wallets off-line, não estão conectadas na internet de forma alguma, por exemplo em uma hard-wallet ou simplesmente escrita em um papel
  + Portanto as cold-wallets tendem a ser mais seguras pois se bem protegidas não estão expostas a códigos maliciosos ou ataques hackers
* O que é tokenização
  + <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-tokenization>

Tokenização é uma maneira de eu converter um ativo real como imóveis, títulos, créditos, ativos financeiros, ativos físicos, par ao mundo virtual, para o mundo digital, e a partir de lá utilizar as características da blockchain como unicidade, impossibilidade de falsificação e outras características

* VItalik Buterim
  + Liderou um movimento na comunidade cripto para a criação de uma nova blockchain que traria funcionalidades adicionais à blockchain da bitcoin, especialmente a possibilidade de trabalhar com smart-contracts e, portanto, a tokenização. Uma plataforma para o desenvolvimento de aplicações.
  + O que Vitalik Buterim propõe é: ao invés de termos a blockchain do bitcoin para o bitcoin ter uma plataforma que permite que múltiplas coisas sejam feitas sobre ela usando os conceitos de blockchain
  + A proposta é usar o conceito de encadeamento de blocos para permitir a tokenização, representação de ativos, na forma digital e não somente o bitcoin ou uma determinada moeda.
  + O que se propõe para a blockchain do Ethereum é que ela seja uma plataforma para a representação de qualquer outra classe de ativo na forma digital em blockchain.
  + Outra grande diferença da blockchain etherium é a possibilidade de criar código e regras condicionais para operações on-chain, ou seja criar os smart-contracts que permite que se configure regras de negocio de acordo com o modelo que se quer usar.
    - Tokenização: Representação de ativos na forma digital
    - Smart Contracts: Regras condicionantes para operações on-chain
  + No lançamento da plataforma etherium surge também uma nova linguagem de programação usada para a criação e configuração de smart contracts que é a linguagem Solid
* Blockchains Possíveis implementações
  + Publica e fechada
    - Leitura pública e acesso restrito para escrita
  + Privada e aberta
    - Leitura restrita e acesso público para escrita
  + Privada e fechada
    - Leitura restrita e acesso restrito para escrita
* Padrão evm – Etherium Virtual Machine
* Conceitos de layer
  + Layer 1 : Blockchain Etherum, Bitcoin...
    - Cada blockchain tem seu próprio token nativo usado para pagar taxas de transação. Redes que determinam a base sobre a qual você vai construir a sua aplicação
    - Limitações
      * Capacidade de transações limitadas
      * Altas taxas de transação
      * Inchamento da blockchain
      * Pressão de centralização
  + Layer 2: Bitcoin lightning Etherium Plasma
    - Soluções que se propõem a resolver o problema de escalabilidade, redução de custos, velocidade e maior provacidade
    - Feitas a partir das blockchains layer 1, se abastecem dela fazendo melhorias significativas na logica de operação
    - Continua usando e se abastecendo dos padrões EVM mas com características mais utilizadas
    - Beneficios
      * Escalabilidade
      * Custos reduzidos de transação
      * Velocidade melhorada
      * Privacidade aprimorada
      * Interoperabilidade
  + Layer 3
    - Mais especifica para um determinado contexto
  + Parachains
    - Opera em uma camada de especialização extremamente especifica
* Categorizações Gerais das aplicações de blockchain
  + Registos – armazenamentos de informações estaticas
    - Registros Estáticos
      * Bases distribuídas para armazenar dados estáticos
        + Registros de terras, nascimentos, posse
        + Registros Acadêmicos e patentes
        + Origem de alimentos
    - Identidade
      * Bases distribuídas com informações sobre identidade de pessoas coisas ou eventos
        + Votação
        + Infrações
        + Identidade pessoal
        + Certidões
    - Contratos Inteligentes
      * Regras de negocio pré-definidas com clausulas de auto execução
        + Industria
        + Automatização de seguros
        + Alugueis
  + Transações
    - Registros dinâmicos
      * Bases distribuídas que registram o status de posse u tracking de ativos ou coisas na rede
        + Tokenização de ativos
        + Fracionamento de investimentos
        + Supply-chain
    - Pagamentos
      * Bases distribuídas que registram transações financeiras de pagamentos entre os participantes da rede
        + Pagamentos internacionais
        + Sistema de pagamento
    - Outros
      * Combinação das aplicações anteriores e outros casos específicos de uso em setores e combinados com outras tecnologias
        + ICO
        + Integração com IOT
        + BAAS (Blockchain as a Service)
* Programabilidade do dinheiro ou das diferentes formas de valor
* Token Fungível
  + São tokens intercambiáveis, eles significam a mesma coisa entre si. Por exemplo um Token de bitcoin é exatamente igual a qualquer outro token de bitcoin, uma nota de 100 vale o mesmo que outra nota de 100 ou dias de 50, são fungíveis entre si.
* Token não fungível (NFT)
  + São tokens com valor intrínseco, por representar algo único não intercambiável entre si, por exemplo um token que representa uma obra de arte, é um token não fungível ele é único, um token que representa um terreno não é fungível pois não existe dois terrenos iguais.
* Off-Chain
  + No mercado offchain que conhecemos as transações ocorrem utilizando os meios de pagamento e dinheiro que estamos habituados a operar
* On-Chain
  + No mercado on-chain é necessário que tenhamos as operações baseadas em um dinheiro também digital (tokenizado em blockchain) para ser on-chain é necessário operar com token em uma blockchain

Fim do bloco 1

* Stable coins
  + são moedas no mundo on-chain que são pareadas a moedas fiduciárias por isso ela não oscila em relação a moeda fiduciária que foi emitida.
  + Essas moedas são fundamentais pois se eu preciso implementar algum mecanismo de transação on-chain eu preciso de uma moeda on-chain, e ninguém irá operar com o risco de volatilidade de uma criptomoeda
  + Com stable coin me benefício das características de transação on-chain sem correr o risco da volatilidade de uma cripto, uma moeda on-chain digital estável
  + Stable coins **Não** é a mesma coisa que uma criptomoeda porque a criptomoeda por essência oscila de valor de acordo com a oferta e demanda
* Off-Ramp e On-Ramp
  + On-Ramp
    - A lógica de sair do dinheiro FIAT (fiduciário) para um dinheiro cripto
  + Off-Ramp
    - A lógica de retornar de uma moeda cripto para o dinheiro fiduciário
  + Isso é feito pelas empresas detentoras das stablecoins
* Cbdc (Central Bank Digital Currency)
  + São moedas nacionais emitidas pelo governo que operam on-chain baseadas em Blockchain
  + Diferente das stable coins que são geridas por empresas privadas a CBDC é emitida e gerida por bancos centrais de governos
  + É a antítese do conceito de criptomoedas porém ambos operam on-chain
* Security Tokens
  + Representam determinado ativo classificado como valor mobiliário, compra e venda de tokens que representam esses ativos

Fim Bloco 2

Bloco 3

* Testnet
  + É uma rede de testes que é igual a rede verdadeira, mas tudo ali é fake, é um ambiente sandbox para validação. Na testnet da etherium podemos fazer testes e simulações sem gastar dinheiro
* Nft’s
  + NFT não é um fim, mas um meio para a exploração de uma nova dorma de criar valor na internet
  + Um token não fungível serve para garantir que determinado item é original. Garante que um arquivo é único é a chave única que garante a autenticidade do arquivo
  + NFT é único, é raro é indivisível.
  + Ele tem propriedade, é verificável, transferível e autêntico
* Defi: Decentralized Finance
  + Mecanismos de troca ou mecanismos de operação financeiras descentralizadas baseadas em smartcontracts e distributed ledger
* Metamask carteira digital

Fim