LabIC - Laboratório de Inteligência Computacional
Universidade Federal Fluminense - UFF

UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE COMPUTAÇÃO
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

Instituto de Computação

Smart contracts em Neo Compile

Natália Bruno Rabelo

2023

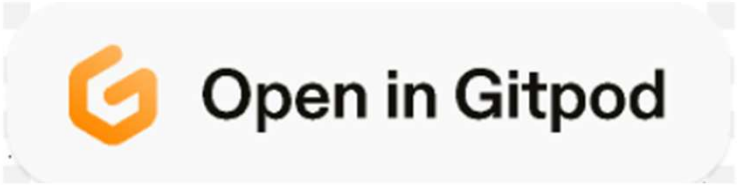
Agenda

- O conceito de blockchain
- O conceito de contratos inteligentes
- A plataforma Neo Compile
- Exemplos de contratos inteligentes
- Oficina de contratos inteligentes

Testando o ambiente de desenvolvimento

- http://alode.ic.uff.br:8000
- https://neocompiler.io/#nav-compilers/

- https://github.com/NeoResearch/neocompiler-eco



+

O conceito de blockchain

- Um conjunto de tecnologias
- Surgiu no âmbito das criptomoedas
- Posteriormente passou a ser aplicada para diversas finalidades com diferentes regras de negócio
- Contratos inteligentes passaram a ser utilizados junto à blockchain

O conceito de blockchain

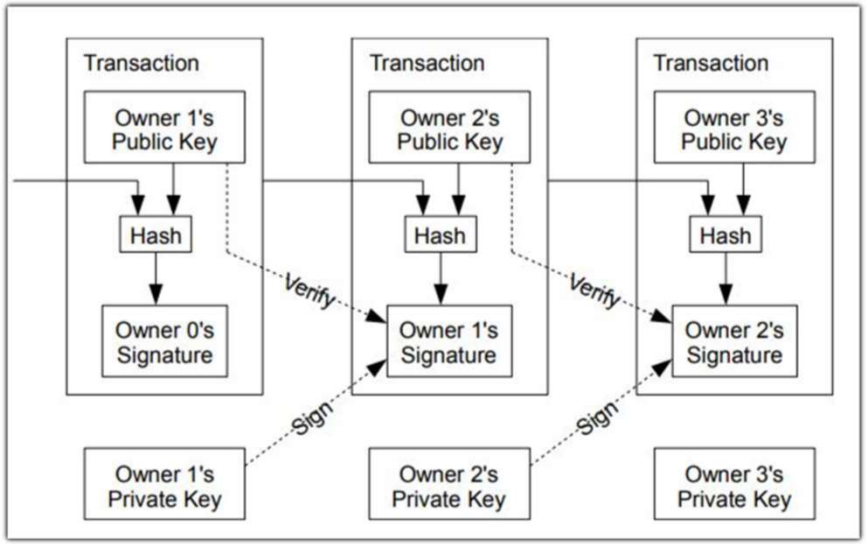
- A tecnologia de blockchain consiste em um banco de dados distribuído contendo o livro-razão público de todas as transações e/ou eventos executados no software e compartilhados com todos os participantes da rede. Em outras palavras, esta tecnologia trabalha com uma infraestrutura distribuída composta por vários participantes, onde cada um é responsável por realizar ações de verificação e validação. Assim, o dado é validado pelo consenso da maioria dos integrantes do sistema de blockchain, ou seja, a informação acordada pela maioria é registrada permanentemente junto a dados ou documentos (CROSBY et al., 2016, p. 7).

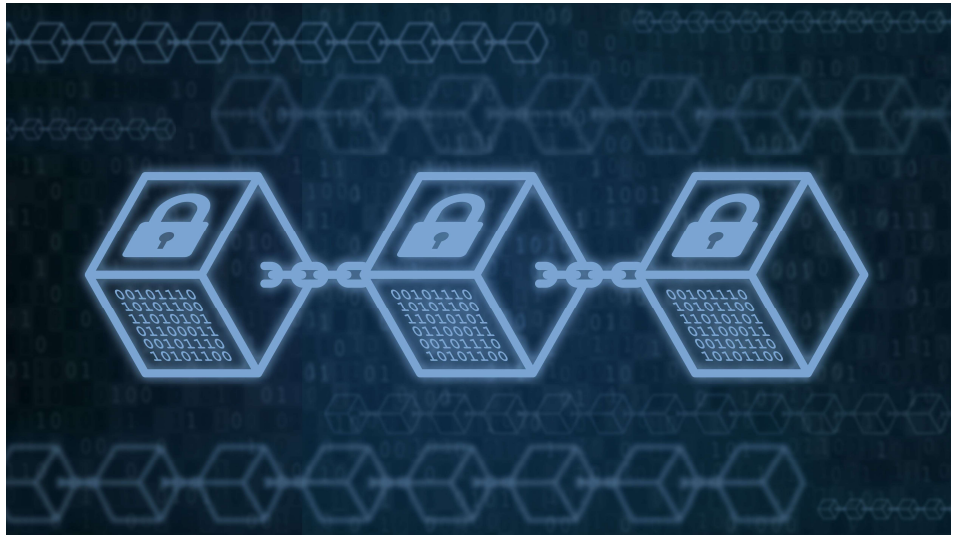
O conceito de blockchain

- Özsu e Valduriez (2020, p. 437) definem blockchain por essencialmente um livro-razão podendo ser de finalidade contábil ou não, distribuído e compartilhado por participantes de uma rede peer-to-peer (P2P), segundo Kurose e Ross (2014), quando participantes colaboram com seus computadores para o funcionamento e manutenção do sistema, que hospeda um banco de dados de blocos distribuídos conforme estrutura de dados Appendy-Only. Estrutura esta na qual, segundo Terry et al. (1992, p. 323), dados, quando inseridos ao banco de dados, não podem ser removidos ou modificados e cada tabela gerada para esses dados contém um carimbo de data e hora de inserção, funcionalidade a qual, no caso de blockchain, funciona para os blocos.

O conceito de blockchain

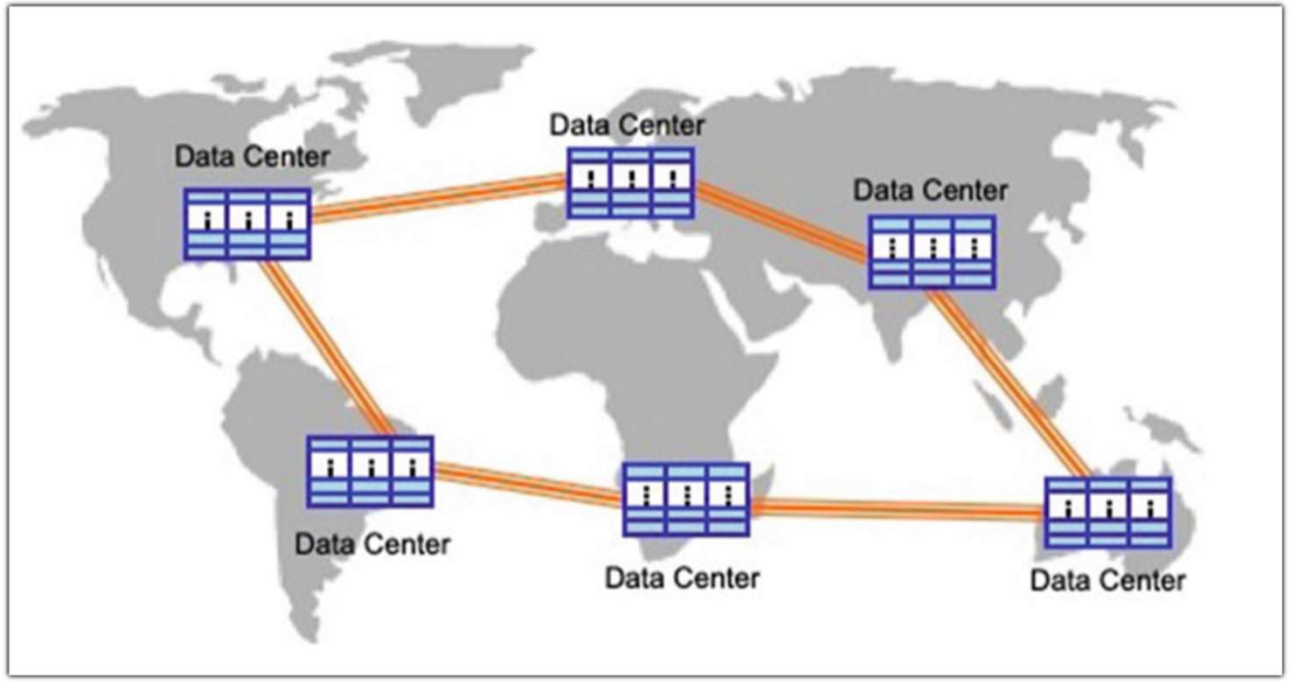
- Blocos encadeados - Contêineres digitais
- Unidades padrões de software para empacotamento de código, bibliotecas de código e outros requisitos para acessar o documento ou dado em favor da interoperabilidade entre sistemas.





O conceito de blockchain

- Banco de dados distribuído



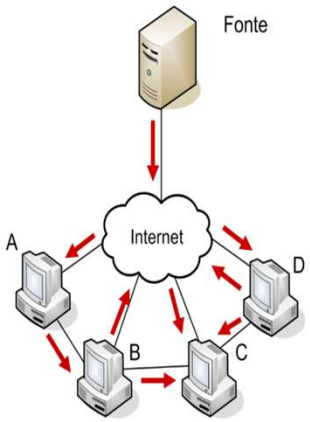
Fonte: Özsu e Valduriez (2020)

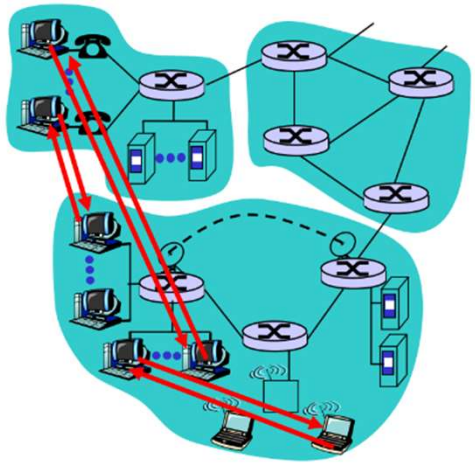
O conceito de blockchain

- SISTEMA PEER TO PEER (P2P)
- Participantes colaboram para o funcionamento e manutenção do sistema

- “Pura”– Comunicação direta entre sistemas finais

- Híbrida – Uso de servidores auxiliares
- Ex.: Skype, BitTorrent, etc.



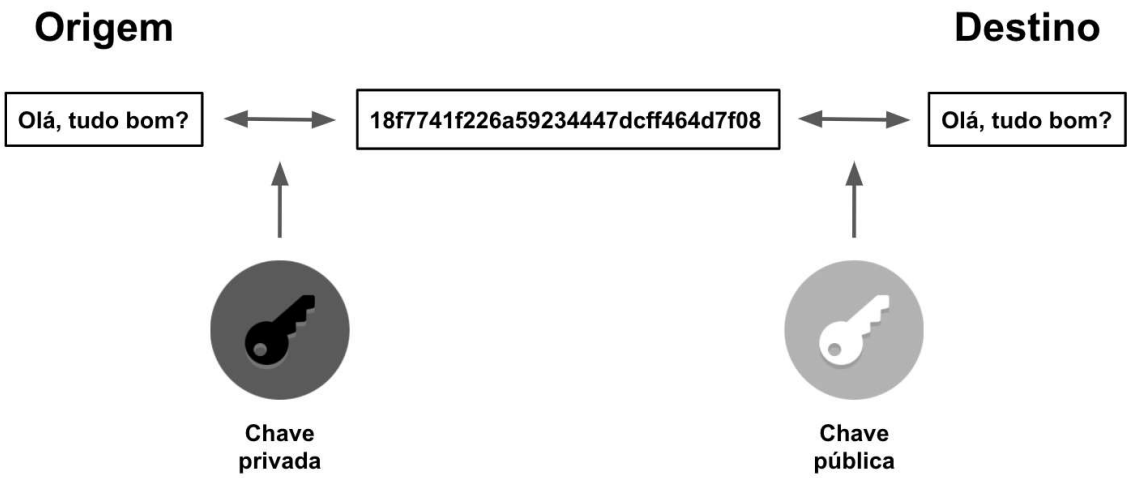


O conceito de blockchain

- Algoritmos de consenso

O conceito de blockchain

- Criptografia assimétrica



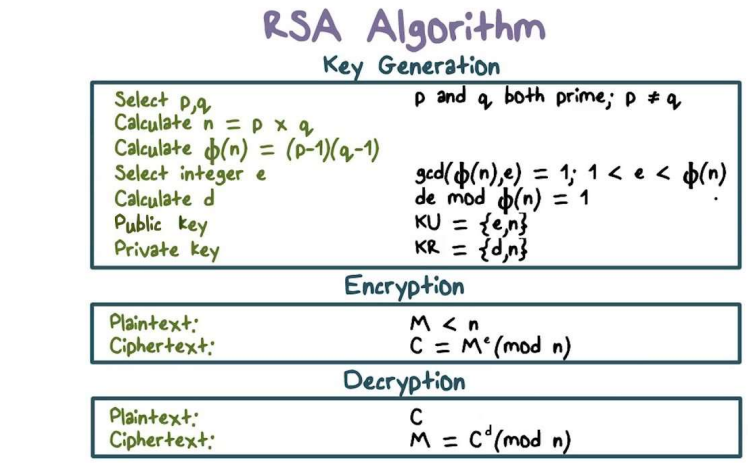
O conceito de blockchain

- Criptografia assimétrica

Exemplos de algoritmo de criptografia assimétrica

Rivest-Shamir-Adleman (RSA) –
módulo de exponenciação de dois primos de alto valor difíceis de fatorar

El Gamal ---------->
logaritmo discreto de difícil resolução



- **Key Generation**

  Select a large prime as a q
  Select x *to* be a member of the group **G** = < Zq^*, X >, x must be "$1 \le x \le q-1$"
  Select g *to* be a primitive root (generator) in the group **G** = < Zq^*, X >
  $y = g^x \bmod q$
  Public key ← (g, y, q)
  Private key ← x

- **Encryption**

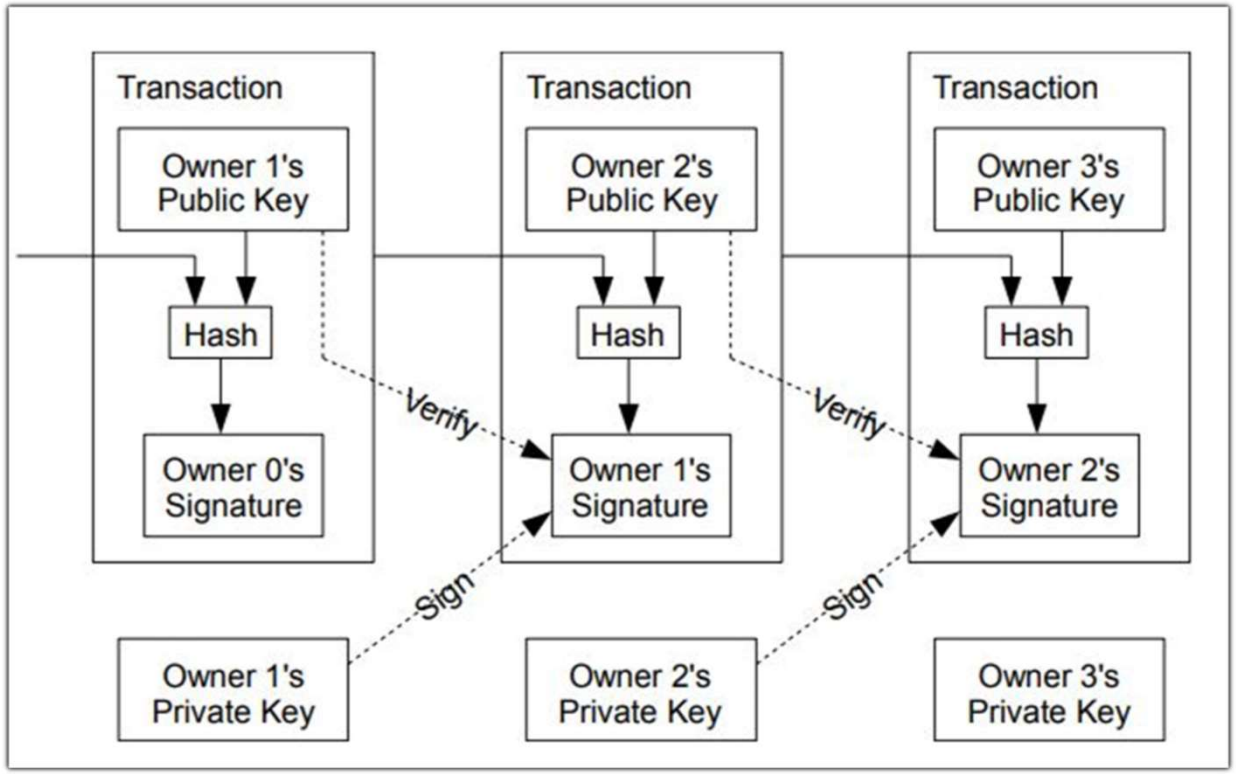
  Select a random integer r in the group **G** = < Zq^*, X >, r must be "$1 \le r \le q-1$"
  $C_1 = g^r \bmod q$
  $C_2 = (p \,.\, y^r) \bmod q$ // p is the plaintext

- **Decryption**

  $P = [\, C_2 (C_1{}^x)^{-1} \,] \bmod q$

O conceito de blockchain

- Criptografia assimétrica



Fonte: Kurose e Ross (2014).

O conceito de blockchain

- Função hash
- A ideia central do Hash é utilizar uma função (Função Hashing) sobre parte da informação (chave), para retornar o índice onde a informação deve ser ou deveria estar armazenada na Tabela Hash.

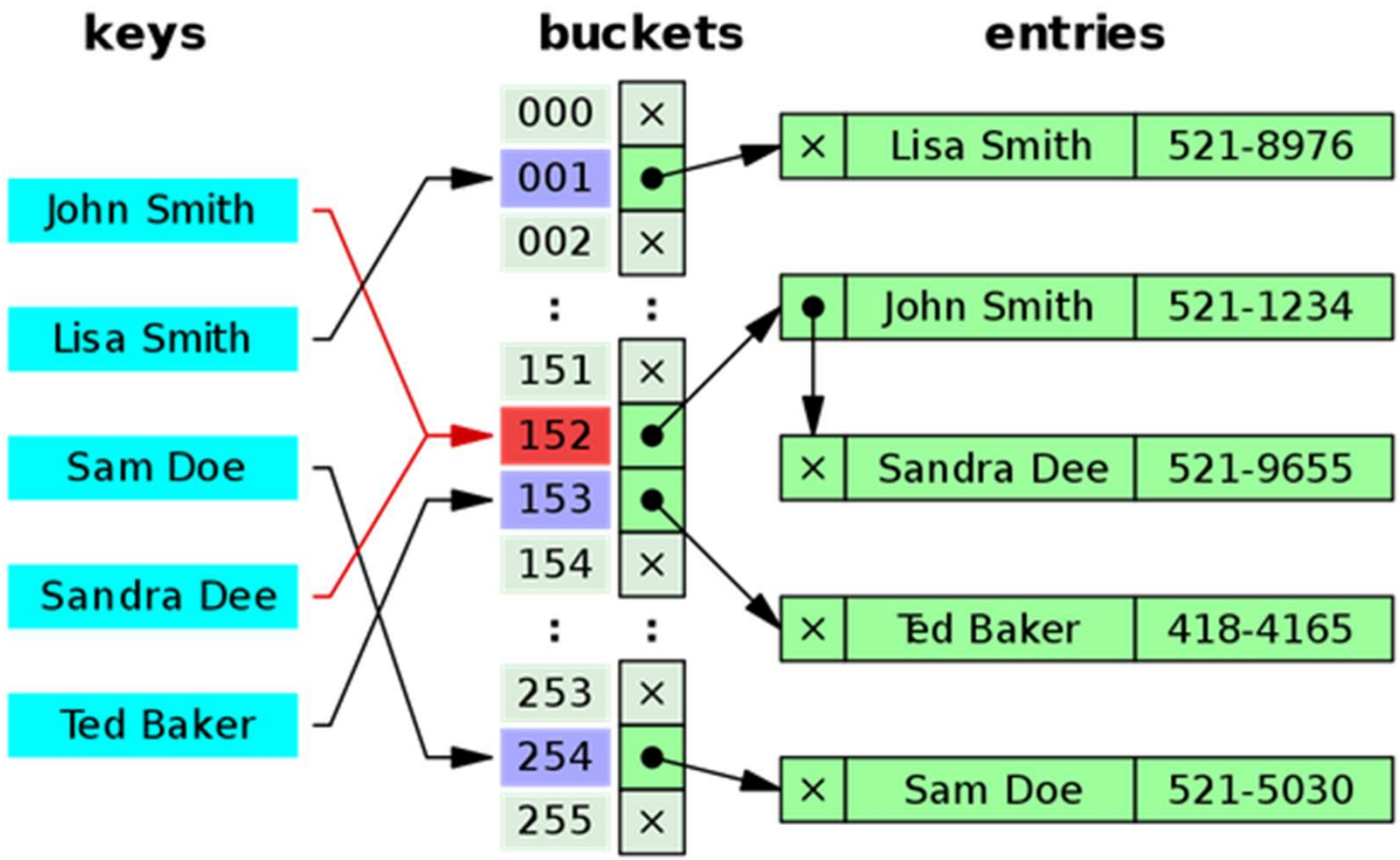
- Chave: Parte da informação que compõe o elemento a ser inserido ou buscado na tabela.

- Função de Dispersão ou Função Hashing: Função que mapeia a chave para um índice e distribui as informações pela Tabela Hash.

Fonte: Kurose e Ross (2014).

O conceito de blockchain

- Função hash



O conceito de blockchain

- BLOCKCHAIN E SUAS APLICAÇÕES

- a) Blockchain 1.0, quando as primeiras criptomoedas foram criadas e o foco era pagamento e mineração, em outras palavras, geração de criptomoedas na rede em questão;

- b) Blockchain 2.0, em 2010 contratos inteligentes e serviços financeiros foram implementados em aplicações, além da possibilidade de desenvolvimento em blockchain com as plataformas da Ethereum e Hyperledger ;

- c) Blockchain 3.0, foram introduzidas aplicações descentralizadas baseadas em blockchain em diversas searas de pesquisa, saúde, negócio, governemantal, Internet of Things, cadeia de suprimentos e cidades inteligentes;

- d) Blockchain 4.0, marcada pela implantação de blockchains em que o foco se resumiu a livro-razão e bancos de dados distribuídos em tempo real e integração de contratos inteligentes como aporte ao consenso da rede.

- (Bodhka et al., 2020, p. 79769)

O conceito de contratos inteligentes

- Contratos inteligentes são programas autoexecutáveis cujos fluxos de execução dependem de eventos determinados pelo algoritmo o qual possui como resultado regras e/ou consequências. (ASHARAF.; ADARSH, 2017, p.45).

O conceito de contratos inteligentes

- Contratos inteligentes são programas autoexecutáveis cujos fluxos de execução dependem de eventos determinados pelo algoritmo o qual possui como resultado regras e/ou consequências. (ASHARAF.; ADARSH, 2017, p.45).

O conceito de contratos inteligentes

- Gestão de Cadeia de Suprimentos (Supply Chain)
- Mercado Imobiliário
- Direitos Autorais e Conteúdo Digital
- Governança e Votação
- Setor de Saúde
- Finanças e Mercados de Capital
- Identidade e Registros
- Internet das Coisas (IoT)
- Plataformas de Crowdfunding e ICOs

A plataforma Neo Compile

Da Hongfei e Erik Zhang

- Fundado em 2014
- Código aberto
- Plataforma blockchain
- Desenvolvimento de aplicativos descentralizados
- Gerenciamento e automatização de ativos por contratos inteligentes
- Armazenamento descentralizado (em blocos)
- Oráculos (Oracles)
- Serviços de nomes de domínio
- Comunidade global de desenvolvedores

A plataforma Neo Compile

Da Hongfei e Erik Zhang

- Fundado em 2014
- Código aberto
- Plataforma blockchain
- Desenvolvimento de aplicativos descentralizados
- Gerenciamento e automatização de ativos por contratos inteligentes
- Armazenamento descentralizado (em blocos)
- Oráculos (Oracles)
- Serviços de nomes de domínio
- Comunidade global de desenvolvedores

A plataforma Neo Compile

- Algoritmo dBFT 2.0

1.Conceitos Principais:

1. Oradores (Speakers): Propõem o próximo bloco a ser adicionado à blockchain.
2. Consensus Nodes (CN, ou Nós de Consenso): Validam e votam na proposta do Orador.
3. Ordem de Rodízio: A ordem em que os CNs se tornam oradores é rotativa para garantir a equidade.

2.Processo de Consenso:

1. Passo 1: O orador atual propõe um bloco.
2. Passo 2: Os CNs recebem a proposta e verificam o conteúdo do bloco.
3. Passo 3: Se um CN considerar a proposta válida, ele enviará uma mensagem de resposta.
4. Passo 4: Quando o orador coleta respostas suficientes (2/3 ou mais dos CNs), ele envia uma mensagem de confirmação para todos os CNs.
5. Passo 5: Os CNs aguardam até coletar mensagens de confirmação suficientes e, em seguida, chegam a um consenso sobre a proposta, finalizando o bloco.

3.Melhorias no dBFT 2.0:

1. Recuperação de Falha do Orador: Se o orador falhar em propor um bloco ou se o bloco proposto não for aceito pela maioria dos CNs, o dBFT 2.0 introduz um mecanismo para trocar rapidamente o orador e reentrar no processo de consenso.
2. Mecanismo de Recuperação: Se um CN perceber que não está sincronizado com o resto da rede, ele pode solicitar as informações necessárias de outros CNs para se atualizar.
3. Otimizações de Desempenho: O dBFT 2.0 introduz várias otimizações para melhorar a eficiência do processo de consenso, reduzindo o tempo necessário para confirmar transações.

4.Resistência a Falhas Bizantinas:

1. dBFT, como sugere o nome, é resistente a falhas bizantinas. Isso significa que, mesmo que uma parte dos CNs seja maliciosa ou falhe, a rede ainda pode alcançar o consenso e funcionar corretamente, desde que a maioria (2/3) dos CNs seja honesta.

A plataforma Neo Compile

- Opção de configurar uma rede Neo local com um ou vários nós
- Opção de utilizar o Neo Compiler que roda em uma rede da comunidade Neo https://neocompiler.io/
- Acesse a documentação da Neo: https://docs.neo.org/docs/en-us/index.html

Exemplos de contratos inteligentes

Acesse os repositórios do Github

https://github.com/nataliaRabelo/NeoSmartContract

https://github.com/neo-project/examples

Acesse a documentação da Neo

https://docs.neo.org/docs/en-us/index.html

Acesse o Neo Compile do Labic

http://alode.ic.uff.br:8000

Oficina de contratos inteligentes

Escolha qualquer tema e crie um contrato inteligente na linguagem de sua preferência que esteja disponível no Neo Compile, recomendo uso de C#.

Acesse a documentação da Neo

https://docs.neo.org/docs/en-us/index.html

REFERÊNCIAS

ASHARAF, S.; ADARSH, S. **Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities**. IGI Global, 2017.

CORMEN, T. H. et al. Algoritmos: teoria e prática. 3 ed. Rio de Janeiro: Elsevier, 2012.