BlockChain e Sistema Anti Fraude

Resumo

Este relatório tem como objetivo explicar brevemente as funcionalidades da blockchain desenvolvida, apresentar as justificativas para as decisões tomadas e apresentar as oportunidades de melhorias em implementações futuras.

Membros do Grupo

André Ricardo Miguel Filho — Arthur Oliveira Pacheco — Felipe Lourenço Vieira

I. A tecnlogia de Blockchain

A blockchain é um sistema para registro de transações que, aliado a implementação de sistemas de criptografia, é um dos métodos mais seguros e modernos no sistema financeiro global, sendo particularmente proeminente no setor de criptomoedas. Levando isso em consideração, o grupo decidiu implementar um sistema de blockchain para registro das transações financeiras na criação do site proposto para a atividade.

II. Especificações técnicas

A blockchain foi programada em C++ visto que é a linguagem mais familiar de uso dos integrantes do grupo e, além de tudo, possuir métodos de encapsulação e proteção de dados que são benéficos para a aplicação do programa desenvolvido neste projeto. Neste projeto, foram desenvolvidas duas classes que são responsáveis por implementar a blockchain: a classe Bloco e a classe Blockchain.

A. Classe Bloco

A classe Bloco é a estrutura de dados responsável por armazenar os dados das transações financeiras realizadas no site, armazenando dados como o nome do emissor do empréstimo, o recebedor do empréstimo e o valor do empréstimo realizado. Vale notar que outros dados como os juros que está sendo cobrado, a moeda utilizada, data limite para pagamento do empréstimo e demais dados podem ser implementados futuramente, sendo omitidos em um primeiro momento para permitir que a equipe foque na implementação de outros processos mais relevantes no desenvolvimento do protótipo do site.

1) Atributos: Foram implementados os seguintes: recipiente, emissor, valor, identificação, sendo este o texto criptografado gerado pela cifra de Vigenère, que foi o sistema de criptografia utilizado e que será explicado posteriormente, chave, que é o conjunto de caracteres utilizados na geração do texto criptografado pela cifra de Vigenère, próximo e anterior, que são ponteiros responsáveis por ligar os blocos presentes da Blockchain.

2) Métodos: Acerca dos métodos associados a classe Bloco possui três métodos públicos: o construtor da classe, seu destrutor e o getter getIndentificacao() que, numa implementação futura do site, não seria implementada, estando apenas presente para teste da funcionalidade de criptografia desenvolvida, e três métodos privados: converteValorEmTexto(double valor), converteNumeroEmLetra(int n) e a função hash.

Vale relevar que os métodos converteValorEmTexto(double valor) e converteNumeroEmLetra(int n) são métodos auxiliares que, como indicam seus nomes, são responsáveis por transformar ou valores numéricos ou atributos do bloco em texto. Estes métodos foram desenvolvidos com o único propósito de garantir o funcionamento pleno da função hash.

3) Função Hash() e a cifra de Vigenère: O sistema de blockchain tem, de forma geral, um sistema de criptografia que utiliza de um conjunto de funções hash para gerar uma identificação baseada na quantidade de dados contidos dentro do bloco que impeça o acesso deste por outras pessoas. Atualmente, existem funções hash e outros sistemas de criptografia extremamente seguros e complexos que oferecem grande segurança ao usuário. Contudo, visando o desenvolvimento de um sistema de criptografia dentro do escopo técnico do grupo, foi-se desenvolvido um sistema de criptografia mais simples, mas que ainda oferece uma medida de segurança contra fraudes: a cifra de Vigenère.

A cifra de Vigenère combina os caracteres associados ao texto fornecido à cifra que se deseja criptografar e os caracteres de uma chave utilizada para aprimorar a segurança do texto criptografado gerado e, de caractere em caractere, gera o texto criptografado completo. No desenvolvimento deste sistema de criptografia, foi decidido que o texto fornecido à cifra seria uma combinação do nome do emissor, receptor e da conversão do valor em formato de texto e que o texto cifrado seria formado apenas por letras minúsculas. Para se Ao realizar esses passos, gera-se o identificador do bloco.

B. Classe Blockchain

A classe blockchain é uma outra estrutura de dados que tem como objetivo facilitar a ligação de múltiplos blocos e estabelecer a blockchain associada a cada transação financeira realizada no site. A classe Blockchain possui um construtor, um destrutor, uma função adicionarBloco(Bloco* bloco), responsável por conectar os blocos que vão fazer parte da blockchain por meio dos atributos ponteiros ”anterior” e ”próximo”, e a função search(string identificacao) que permite a busca de um determinado bloco dentro da blockchain por meio do seu identificador.

III. Próximos Passos

- Implementação de um sistema de criptografia mais robusto; - Inclusão de uma maior variedade de atributos a serem guardados nos blocos; - implementação de alocação de memória dinâmica na criação de um objeto de classe blockchain ao invés da criação de um vetor estático;