Universidade de Brasília

Departamento de Ciência da Computação
Ciência da Computação

Trabalho de Estrutura de Dados

Autores:

Raylan Sales 18/0108531

Stefano Luppi 18/0043242

Brasília
8 de Julho de 2019

Conteúdo

1 Introdução

O blockchain é uma tecnologia que veio para aumentar a segurança de registros, para que esses registros sejam quase que impossíveis de serem alterados. Como os registros são eletrônicos, a velocidade com que eles são trocados por empresas por exemplo, aumenta de uma forma grandiosa, economizando assim tempo e dinheiro, trazendo benefícios e mais lucros às impresas que utilizam essa tecnologia. Além disso o blockchain por ser muito seguro, reduz os riscos de trocas de informações que demandam um alto sigilo, tornando assim a confiabilidade, algo em destaque no blockchain.

As operações feitas utilizando o blockchain são cem por cento rastreáveis, fazendo com que fraudes sejam facilmente identificáveis. Pois todos que tem acesso ao sistema da rede de blockchain tem todas as informações sobre todas as operações feitas. Por exemplo, se um dos blocos for invadido, hackeado ou sofra qualquer tentativa de adulteração, os blocos conectados a esse que sofreu o ato, possuem todas as informações presentes no bloco que foi violado.

Um dos cenários em que essa tecnologia pode ser muito útil é na substituição de cartórios como conhecemos hoje por um sistema que tem o blockchain como principal meio de manter a segurança para com esses registros. Os cartórios que são utilizados praticamente por todos os cidadãos, possuem meios de validações que podem ser facilmente adulterados, pois ao contrário do blockchain, os cartórios tem um órgão central que tem acesso a todos os dados cadastrados, se quem obtem os dados dessa central, por algum motivo tentar adulterar esses dados, esse ato será mais fácil sem o uso do blockchain, pois uma pequena quantidade de pessoas terá acesso aos dados em questão. Em relação ao registro desses dados usando o blockchain, como os dados são de certa forma públicos e podem ser acessados por qualquer pessoa que esteja em contato com o sistema de blockchain, esse crime pode ser facilmente identificável, já que todos que podem acessar os registros dos dados, também podem acessar todas as operações que foram feitas.

Nossa proposta é impregar o blockchain de maneira a assegurar os dados que serão gravados por um jogador de um jogo chamado RPG de mesa, que é um jogo em que seu principal objetivo é imergir o jogador em um mundo fictício através do uso da criatividade. Nesse jogo há várias informações que necessitam de uma constante consulta dos próprios jogadores, pois cada jogador possui um personagem, em que esse personagem possui suas características. Essas características são as informações que desejamos manter sob total segurança utilizando o blockchain, para que elas não sejam alteradas de maneira fácil, e causar a decadência de toda a experiência que uma partida do jogo deve proporcionar.

2 Blockchain

O Blockchain como o próprio nome já indica, é uma cadeia de blocos. Mas não uma cadeia de blocos qualquer, e sim uma cadeia de blocos que contém informações, e essas informações são tratadas como registros que podem ser acessados por qualquer pessoa com acesso a rede do blockchain em questão. Mas isso não quer dizer que essas informações sejam de fácil acesso, uma das características mais relevantes do blockchain é que quando informações são gravadas, elas se tornam muito difíceis de serem alteradas.

Todo bloco contém os dados que foram armazenados, o hash que é artifício usado para verificar a veracidade das transações, que pode ser entendido como uma digital, em que assim como nós seres humanos que temos nossas próprias digitais, cada bloco possui sua própria digital, e há também nesse bloco a digital (o hash) do bloco anterior, ou mais comunmente chamada de hash do bloco pai, causando assim uma conexão entre os blocos. O único que não possui o hash do bloco anterior é o primeiro bloco(chamado também de bloco Gênese), pois como não há nenhum bloco anterior a ele, não há como ele ter tal informação.

Os dados que são armazenados no bloco dependem do tipo de blockchain, o tipo de blockchain usado no Bitcoin por exemplo, armazena as informações de transações, como quem envia, quem recebe e qual a quantidade de Bitcoins usadas na operação. E assim como em qualquer rede de blockchain, também armazena o hash do bloco e o hash do bloco anterior.

Se o hash de um bloco for modificado, todos os blocos posteriores a esse bloco também devem ser alterados para garantir a validade desse bloco, pois eles também possuem o endereço do bloco que foi alterado e devem modificar o campo de hash do bloco pai que estão em suas estruturas.

Há também algo chamado de proof of work ou se analisarmos bem, também pode ser chamado de quebra do hash. Esse mecanismo faz com que a criação de novos blocos e o armazenamento de informação em blocos já criados, levem mais tempo para serem feitos. No caso do Bitcoin, o tempo necessário para calcular o que é preciso para quebrar o hash ou adicionar um novo bloco a cadeia de blocos é de dez minutos. Esse é o mecanismo que ajuda a tornar o Bitcoin algo quase que inviolável, pois se o o endereço de um bloco for alterado, o proof of work terá que ser aplicado em todos os blocos seguintes, já que eles também possuem o hash do bloco que você alterou que como já vimos é chamado de bloco pai, e para alterar essa informação os hash seguintes teram que ser acessados.

3 Metodologia

3.1 Passo a passo de todo o projeto

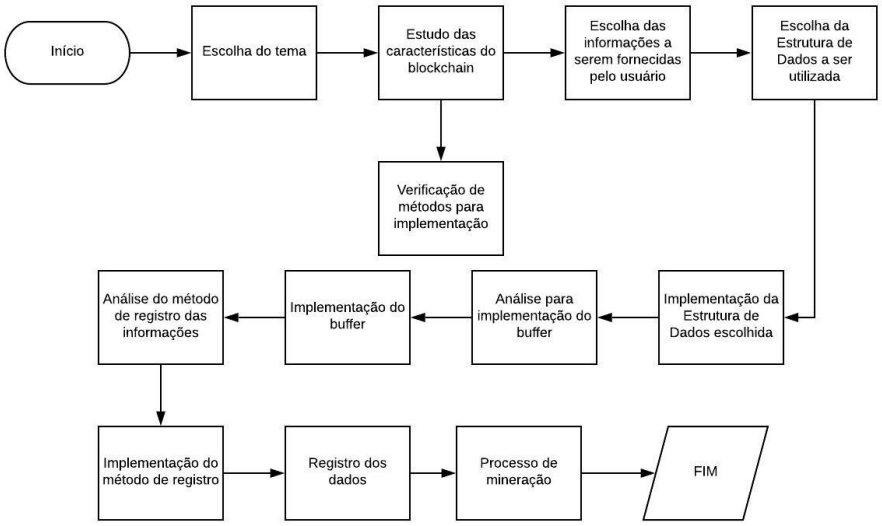

Figura 1: Fluxograma de desenvolvimento do projeto

Nosso trabalho foi constituído de várias etapas até nossa real conclusão. Os passos a seguir servirão como um guia mostrando os processos passo a passo até a finalização do projeto.

Primeiramente, nós escolhemos o tema em que iríamos abordar, ato essencialmente importante para todo o desenvolvimento do trabalho. Não sofremos dificuldade na escolha do tema pois antes mesmo do trabalho ser solicitado nós já haviamos debatido sobre algumas ideias que colocaríamos em prática durante o decorrer do curso, e uma delas, a abordagem em nossos debates que obteve mais destaque foi a escolhida por nós para ser o tema principal do trabalho.

O tema "Registro de fichas de RPG de mesa", foi escolhido pois nossas experiências com jogos de RPG de mesa necessitavam de algo a mais, algo que nos ajudasse não só na experiência de jogar um jogo, mas também nos ajudasse a compreender ainda mais os temas abordados em matérias que haviam sido ministradas para nós. Ou seja, estaríamos nos divertindo e estaríamos ao mesmo tempo observando como algo que nos foi aprensentado como teoria seria colocado em prática, e nada melhor do que aprender algo útil e ter a adição de algum entretenimento que nos empolgue para fazermos

um trabalho não perfeito, mas útil e ideal para enriquecer nossas experiências e de vários outros jogadores de um jogo.

Após a escolha do tema, a parte interna do trabalho começou a ser desenvolvida, começamos estudando sobre o blockchain e suas várias implementações no mercado. Nós fizemos várias análises de como nossas ideias seriam colocadas em prática de forma ideal para que o blockchain fosse algo de suma importância para assegurar as informações inseridas por usuários, jogadores no caso do nosso tema.

Com o estudo que desenvolvemos sobre o blockchain, percebemos que implementar nossa ideia principal com a adição do blockchain não seria tarefa fácil. Nossas pesquisas foram feitas por métodos de eliminação, ou seja, pesquisamos várias formas para implmentar o blockchain de maneira eficiente, colocamos em uma lista e fomos eliminando os métodos de implementação que não seriam ideais para o nosso caso, sejam elas não ideais por serem complexas de mais para nosso objetivo final, ou tão simples que não faria sentido usarmos para assegurar os dados registrados. E por fim chegamos a um método de implementação da nossa ideia com integração do blockchain que será descrito posteriormente.

Depois de termos decidido os métodos que iriamos usar para a implementação, começamos a colocar em pratica tudo que foi absorvido por nós desde o início, começamos escolhendo quais informações que o usuário iria fornecer ao criar sua ficha, e elas são: Id, nome do usuário, nome do personagem, raça do personagem, força, constituição, destreza, inteligência, sabedoria e carisma do personagem. Escolhemos estas informações pois são as principais e essenciais para o jogo de RPG.

Logo após escolhermos os dados a serem inseridos pelo usuário, decidimos qual estrutura de dados seria a ideal para o nosso projeto, e a escolhida foi a Lista Dinâmica Encadeada. A seguir estão as operações que nós implementamos na lista em que criamos: 1.Criar lista. 2.Verificar se a lista é vazia. 3.Liberar a lista. 4.Inserir dados de jogador. 5.Remover a ultima ficha inserida. 6.Verificar a quantidade de jogadores. 7.Imprimir fichas.

Percebemos que para fazermos o buffer, que é um artifício para podermos usar uma "memória temporária", teriamos que utilizar outra estrutura de dados, então analisamos e chegamos a um acordo de que a estrutura de dados mais apropriada para nos ajudar nesse processo seria a mesma que utilizamos anteriormente para inserir as informações, a Lista Dinâmica Encadeada e então criamos outra Lista Dinâmica Encadeada com as mesmas operações da anterior para nos auxiliar com o processo de buffer.

Uma observação importante a ser destacada é que cada partida do jogo terá um valor fixo de dez jogadores. Com a adição do processo de buffer em conjunto com o sistema de blockchain, nosso projeto ficou da seguinte

forma: Primeiro o usuário irá fornecer os dados da sua ficha de jogador, após isso tudo fica por conta do programa em si. Os dados do usuário serão armazenados no buffer, na inserção da primeira ficha até a nona ficha os dados podem ser alterados, a partir da inserção da décima ficha os dados dos dez usuários que forneceram suas informações serão armazenados passados transferidos para um bloco e liberadis do buffer. E esse bloco vai estar ligado a outros blocos com a adição do seu próprio hash e o hash do bloco anterior (exceto o primeiro bloco a ser inserido que é chamado de bloco gênesis e possuirá um valor nulo na área de "bloco anterior"), tornando essa conexão entre os blocos em uma cadeia, o que podemos chamar de Cadeia de Blocos ou com um nome mais conhecido "Blockchain".

Até agora o que foi descrito foram os processos necessários para os registros dos dados do usuário em um bloco, e por últimos mas não menos importante nos restou a implementação do processo de mineração. E o processo de mineração acontece no nosso projeto da seguinte forma: Criamos uma função chamda mine-block, o que essa função irá fazer é basicamente chamar a função que usamos para criar o hash, mas não chamar de uma forma normal e sim chamar repetidamente a função hash até ela atingir um critério determinado por nós, esse critério foi o hash começar com as iniciais AA, e a cada chamada do hash um número vai ser incrementado a uma variável que chamamos de nonce, essa variável no caso do nosso projeto vai representar os segundos necessários para encontrar o padrão que especificamos no critério, ou falando a grosso modo o padrão para quebra do bloco e adicionar algo novo ao bloco (o processo de mineração).

4 Caso de uso

4.1 Interação usuário x programa

Primeiramente ao executar o programa o usuário se deparará com um menu, como mostrado na figura 2.

Oito opções são apresentadas ao usuário na tela de menu, e a seguir essas opções irão ser descritas detalhadamente:

Primeiramente é válido falar que as opções de 2 a 7 tem seus funcionamentos inteiramentes ligados a opção 1. Dito isso, a opção 1 é selecionada para o usuário criar a lista de fichas que serão criadas, ao selecionar essa opção será alocado um espaço na memória para o armazenamento dessa lista, tal lista quando é criada tem seu estado inicial como vazio.

A segunda opção serve para o usuário verificar se a lista está ou não vazia, e a terceira opção serve para liberar uma lista, ou seja desalocar seu espaço

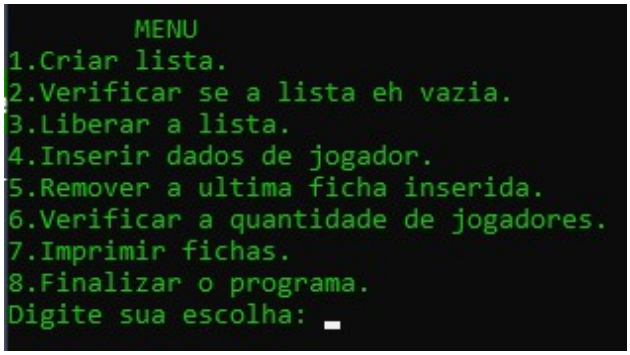

Figura 2: Menu

que foi alocado na memória e destruir a lista. Essas duas operações são as mais simples do menu, porém não quer dizer que não sejam importantes para compor o projeto como um todo.

A quarta opção é a mais importante do menu, pois é através dela que o usuário será capaz de inserir seus dados. Ao selecionar essa opção o usuário terá que informar quantas fichas de jogadores ele irá inserir. Essas fichas possuem os seguintes dados: Id, nome do usuário, nome do personagem, raça do personagem, força, constituição, destreza, inteligência, sabedoria e carisma do personagem.

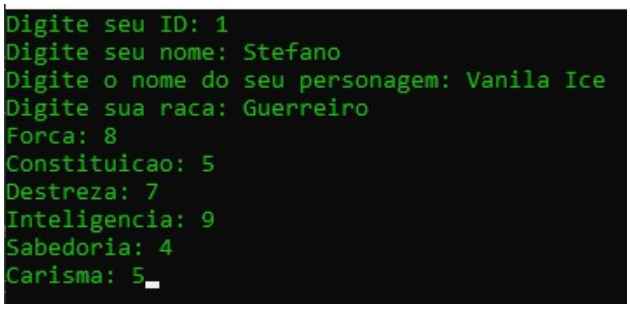

Figura 3: Dados a serem inseridos

A quinta opção será selecionada pelo usuário se ele quiser remover a última ficha que foi inserida na lista criada pelo mesmo.

A sexta opção servirá para o usuário verificar a quantidade de fichas de usuários que foram inseridas, ou seja a quantidade de jogadores que foram inseridos naquela lista. A sétima opção serve de complemento a sexta, pois ela dará ao usuário a capacidade de obter todas as informações que foram inseridas pelos usuários naquela lista de fichas criada e nas várias outras listas de fichas criadas que compõem um bloco da blockchain. Ao selecionar

essa opção o usuário se deparará com mais 2 opções, a opção de imprimir o buffer e a opção de imprimir os blocos.

Figura 4: Tipos de impressão

No primeiro caso que é a impressão de fichas de uma lista estamos falando do buffer, já no segundo caso estamos falando das informações de várias outras listas que estão dentro de blocos, essa segunda opção é a opção que pode mostrar um pouco do processo de blockchain, blocos que possuem as 10 transações que nesse caso, essas transações são os registros das fichas em um bloco.

No exemplo a seguir foram feitas inserções de 10 fichas de jogadores na lista para a impressão do bloco ser efetuada.(na imagem a seguir são apresentadas as duas primeiras fichas inseridas por jogadores):

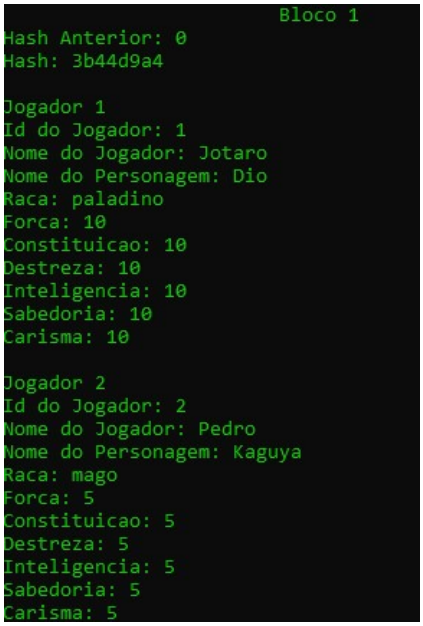

Figura 5: Impressão do bloco

E por fim a oitava opção que serve para quando o usuário desejar sair do programa.

5 Conclusão

O nosso modelo de blockchain possui vários benefícios, um deles é a garantia de que com a nossa implementação é possivel assegurar dados de forma segura, para que em um futuro não muito próximo essas informações ainda possam ser acessadas e não possuírem quaisquer tipos de adulteração. A nossa aplicação do blockchain para nos ajudar a manter todo um sistema de várias partidas de um RPG de mesa, possui várias vantagens em relação a modelos anteriores de armazenamento de informações em relação a esse jogo em específico, pois uma grande quantidade de jogadores ainda optam por utilizar o papel como principal meio de armazenamento de informações de suas partidas. Esse método usado utilizando o papel não somente é retrógrado em relação as tecnologias que possuimos hoje, como também não é de nenhuma forma um método para armazenar informações de maneira segura.

Procuramos através dessa proposta de blockchain impregada ao nosso tema escolhido, tentar integrar a tecnologia de segurança de dados em algo que é considerado antigo, o RPG de mesa, pois apesar de ser antigo o jogo ainda não "morreu", ou seja, não deixou de ser jogado durante as eras, pelo contrário, o jogo vem ganhando mais e mais pessoas. E como o jogo já possui uma idade avançada, alguns de seus métodos de armazenamento de informações dos jogadores ainda continuam iguais a época de quando o jogo foi criado, nossa proposta é tentar deixar o jogo atualizado as tecnologias dos dias atuais em relação a segurança dos dados dos usuários.