FIAP – MBA+

DECENTRALIZED AND DISTRIBUTED DEVELOPMENT

Desenvolvimento de *Smart Contracts* e Tokenização

Prof. João Kuntz

Instruções: crie um contrato para cada exercício no Remix. Ao final, faça o download do *workspace* (opção Download Backup na página inicial) e anexe o arquivo zipado.

Lista de Exercícios 02

1 – Você está trabalhando em um contrato que realiza o cadastro de usuários, capazes de interagir com sua aplicação.

Um usuário é identificado por seu endereço de origem, seu nome e sua idade – todos, atributos obrigatórios. Um usuário possui, ainda, perfis de acesso: Leitor ou Editor.

No momento do cadastro, o perfil de acesso obrigatoriamente é “Leitor”. Durante este processo, são mostrados *tooltips* na tela, conforme as validações dos dados sejam concluídas (não se preocupe em implementar o front-end!).

Um endereço pode ser cadastrado uma única vez.

Usuários que não tenham sido cadastrados não devem poder interagir com o restante da aplicação (podem apenas realizar o seu cadastro).

Deve existir uma funcionalidade para que o dono do contrato altere o perfil de acesso dos usuários cadastrados: um usuário Leitor vira, obrigatoriamente, um Editor, e um Editor vira um Leitor. Apenas o dono do contrato pode executar esta ação. Esta alteração deve ser armazenada em log, filtrado pelo endereço do usuário que foi alterado e deve indicar o horário em que aconteceu.

Usuários com perfil “Editor” que interajam com a aplicação podem alterar os dados de nome e idade de qualquer outro usuário, e estas alterações devem ser armazenadas em log junto com o horário e o usuário responsável pela alteração. Deve ser possível filtrar as alterações pelo endereço do usuário que foi atualizado.

Usuários de perfil “Leitor” podem visualizar os dados de qualquer usuário, porém não podem realizar alterações.

Tanto os usuários de perfil “Leitor” como “Editor” podem solicitar que o seu próprio registro seja desativado (apenas o seu próprio registro). Esta solicitação fica armazenada em uma estrutura própria do contrato.

A partir do momento em que a solicitação é feita, o usuário tem 30 segundos para poder desistir da sua solicitação.

O dono do contrato pode aprovar a desativação, porém, apenas depois dos 30 segundos de segurança – apenas solicitações criadas com tempo maior ou igual a 30 segundos é que podem ser atendidas.

Faça as implementações necessárias.

2 – Você está desenvolvendo uma aplicação de *crowdfunding* que usa a blockchain Ethereum como base de funcionamento. Aqui, todas as doações em dinheiro são feitas diretamente em Ether (ou suas subunidades), e são transferidas diretamente das contas dos usuários, sem intermediários.

A plataforma que você está desenvolvendo permite a criação de campanhas de doação. Uma campanha é identificada por um id único, criado dinamicamente. Ela também possui um nome, uma data de início (maior ou igual à data de hoje), uma data de término (maior que a data de início) e um valor alvo, expresso em Weis, que é o valor que a campanha deseja arrecadar ao final.

Novas campanhas podem ser criadas a qualquer momento, e não há limite para quantas campanhas um usuário pode criar. Ao ser criada, a operação de criação da campanha deve ser armazenada em um log, filtrado pelo seu ID. O log deve incluir o endereço da pessoa responsável pela criação, o tipo da operação (neste caso, criação), e uma indicação da data e hora.

Quando uma campanha é iniciada, seu dono precisa obrigatoriamente fazer um depósito inicial de 0.5 Ether como caução. Ao término da campanha, no caso de sucesso, este valor é devolvido para ele, juntamente com o valor arrecadado.

Se uma campanha ainda não começou, suas datas de início e término e o valor a ser arrecadado podem ser alterados livremente, a qualquer momento. Esta alteração pode ser feita exclusivamente pelo dono da campanha, e deve ser armazenada em log, filtrado pelo ID da campanha, e deve indicar o endereço

da pessoa responsável pela alteração, o tipo da alteração, e deve contar com uma indicação da data e da hora.

Se uma campanha já começou, sua data de término pode ser estendida, e o valor a ser arrecadado pode ser aumentado ou diminuído (porém, não pode ser menor que o valor total arrecadado até o momento). Neste caso, não é possível diminuir a data de início. Estas alterações podem ser feitas exclusivamente pelo dono da campanha e devem ser armazenadas em log, filtrado pelo ID da campanha, com a indicação do endereço da pessoa responsável pela alteração, o tipo da alteração, e a indicação da data e da hora.

Como requisito de segurança, um usuário pode indicar endereços de pessoas que capazes de auditar as operações feitas sobre sua campanha (no máximo podem ser incluídas 5 pessoas). Assim, apenas pessoas autorizadas e designadas no momento da criação da campanha é que terão acesso a acompanhar o seu andamento (ou seja, consultar o valor que já foi arrecadado, em determinado momento); esta função deve retornar dinamicamente o valor esperado e o valor arrecadado. Caso a campanha não tenha pessoas designadas, apenas o seu dono é que poderá realizar as consultas.

O usuário pode ainda indicar uma outra pessoa (no máximo 1 pessoa) que terá que aprovar as contas antes que o valor seja depositado na conta do dono da campanha ao final. Caso ele não indique ninguém, esta pessoa deverá obrigatoriamente ser ele mesmo.

Qualquer pessoa pode fazer doações para as campanhas existentes. Não há limite máximo para as doações, porém, há um valor mínimo estipulado de 0.25 Ether por doação.

Toda doação deve ser registrada em log indicando o ID da campanha (usado como filtro), o endereço da pessoa que realizou a doação, a quantidade doada, e deve ter um indicativo de data e hora.

A pessoa que realizou uma doação pode desistir, e pedir seu dinheiro de volta; neste caso, há uma taxa de 0.1 Ether como multa, cobrada pela plataforma (fica com o contrato). O valor restante é transferido de volta diretamente para a conta da pessoa.

A pessoa só pode desistir da doação se a campanha ainda estiver ativa (isto é, se não chegou até a data limite). A devolução do dinheiro é feita diretamente para o endereço da pessoa, e deve ser armazenada em log

identificado filtrado pelo ID da campanha e pelo endereço da pessoa, que também deve conter um indicativo do valor devolvido e a data e a hora.

O dono da campanha pode desistir dela. Neste caso, o valor de caução não é devolvido, e o dinheiro arrecadado deve ser devolvido a cada uma das pessoas que fizeram a contribuição, na íntegra. Cada uma das devoluções deve ser registrada em log, indicando o ID da campanha, o endereço do usuário que vai receber o dinheiro, e o valor sendo devolvido.

Uma campanha é terminada por decurso de prazo (isto é, quando a data final é alcançada) ou quando o valor desejado é atingido (mesmo no caso em que o dono da campanha diminua o valor manualmente, para deixá-lo igual ao valor disponível). Em qualquer um dos casos, o usuário deve invocar uma função capaz de encerrá-lo.

A plataforma cobra uma taxa de 2% em cima do valor total arrecadado. Assim, 98% do valor estará disponível para ser transferido para o dono da campanha.

Não se esqueça que existe uma pessoa indicada para ser o aprovador da conta! Uma campanha finalizada pelo usuário, só terá as verbas liberadas uma vez que a pessoa aprovadora acesse o contrato e aprove a transferência. A aprovação deverá ser registrada em log, filtrado pelo ID da campanha, indicando o endereço da pessoa aprovadora, a data e a hora.

Ao ser aprovada a campanha, 98% do valor arrecadado é transferido para o dono da campanha, e ela é removida do contrato.

Faça as implementações necessárias. Não se esqueça de proteger as operações de transferência contra os ataques de reentrância!