Projeto de Formatura – Turmas 2020

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia Elétrica – Ênfase Computação

Tema: SISTEMA DE SORTEIO JUSTO, RASTREÁVEL E AUDITÁVEL PARA APLICAÇÕES LEGAIS

MOTIVAÇÃO

Em 2018 a Universidade de Brasília[1] realizou um estudo sobre o sistema de distribuição de processos entre ministros do Supremo Tribunal Federal (STF) e concluiu que, apesar de não haver objeção à divulgação do código-fonte do sistema eletrônico utilizado no processo, "**não foi possível esgotar o trabalho a ponto de atestar a confiabilidade da solução de distribuição automática de processos do STF**'".

Figura 1 – Falta de transparência no sorteio de Processos no STF. Fonte: Apublica.org

Isso não significa que o sistema não seja confiável. No entanto, o estudo afirma que para promover a distribuição igualitária e uma divisão isonômica de trabalho são inseridas variáveis, sobre as quais não se tem transparência nem informações suficientes para que seja entendido seu impacto no sistema.

O contexto descrito acima gerou incômodo suficiente para que se pensasse em um sistema alternativo capaz de gerar números evidentemente aleatórios, sem possibilidade de adulteração, e que fosse passível de ser auditado, de maneira simples.

SOLUÇÃO

Existe uma técnica utilizada no universo da criptografia conhecida como ***Commit-Reveal**,* baseada em *funções hash*, em que as partes envolvidas na comunicação se comprometem a um valor de envio imutável, inicialmente escondido (criptografado), para depois ser revelado mediante a uma condição estabelecida.

Uma possível analogia é está ilustrada abaixo. Um indivíduo deseja se comunicar com um grupo, mas fará o processo em dois passos. No primeiro, ele envia uma caixa ao grupo com o conteúdo desejado, porém, trancará a caixa com uma chave que só ele possui.

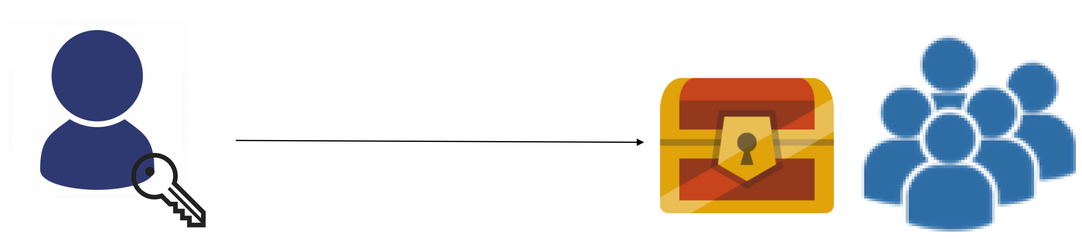

Figura 2 – Etapa 1 do processo (commit)

Em seguida, quando o remetente estiver seguro que pode revelar o conteúdo enviado, ele envia sua chave ao grupo, que deverá usá-la para abrir a caixa. Dessa forma, o remetente pode ter certeza que ninguém além dele sabia o conteúdo da caixa antes do envio da chave, e por outro lado, o grupo tem a garantia que o valor enviado não foi alterado durante o processo.

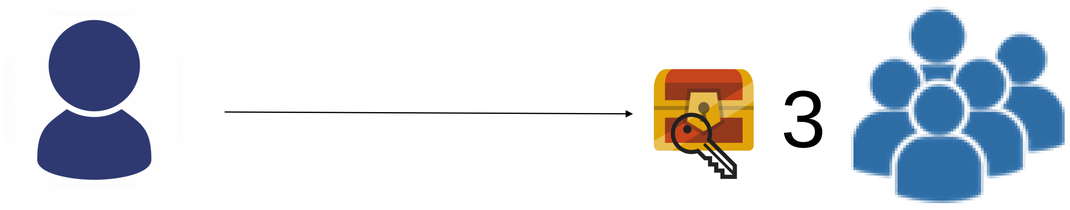

Figura 3– Etapa 2 do processo (reveal)

Utilizando essa ideia, é possível criar um método de sorteio no qual cada participante faz o envio de um número, de forma protegida, para depois revelá-lo quando todos tiverem enviado. O sorteado será aquele cujo índice seja igual ao resto da divisão inteira entre a soma dos envios e o número de participantes. Este método seria como uma versão digital da brincadeira "Dedos Iguais", comum entre crianças para sortear quem do grupo será o primeiro a jogar.

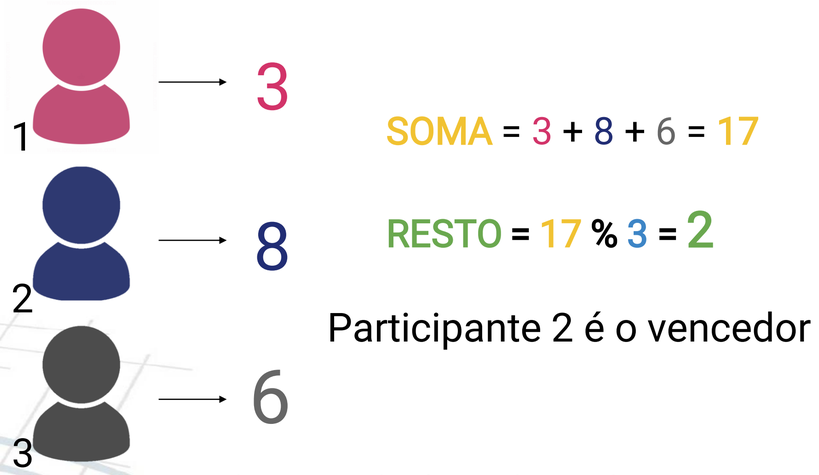

Figura 4 – Simulação de sorteio

OBJETIVO

Explicação, desenvolvimento e especificação de uma biblioteca de software que forneça recursos para construção de aplicações de sorteios justos e distribuídos, utilizando a técnica de *commit-reveal*.

Para o desenvolvimento, optou-se por usar a linguagem Javascript, com Node.js. Como demonstração, o projeto também contará com um aplicativo web/mobile, construído usando a framework Ionic.

RESULTADO

Como resultado do projeto, obteve-se com êxito um aplicativo de demonstração funcional, através de conexões WebSockets e autenticação pelo Google, capaz de ser utilizado para sorteios genéricos.

Além disso, como entrega principal, obteve-se um detalhamento técnico de como implementar a técnica aplicada a sorteios e uma implementação exemplo, em forma de pacote *Node.js*.

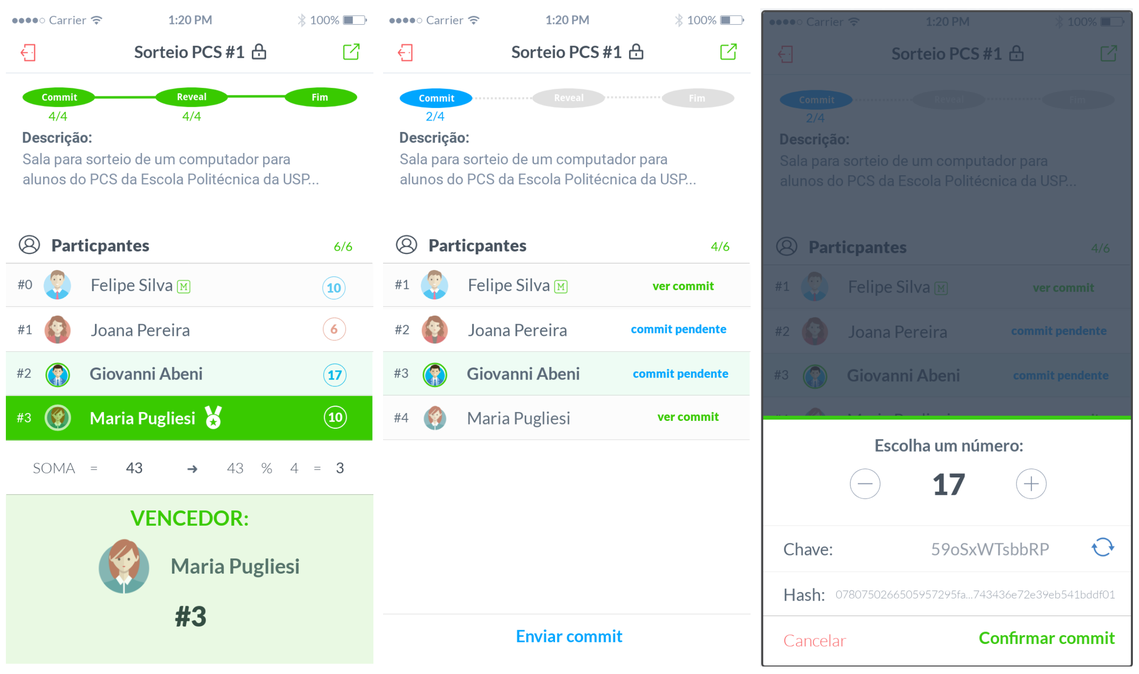

Figura 5 – Imagens do aplicativo de demonstração

Integrantes: Giovanni Abeni
João Paulo Lins

Professor Orientador: Marcos Antonio Simplício Júnior

[1] Fonte: Supremo Tribunal Federal. Disponível em http://portal.stf.jus.br/hotsites/avaliacaodadistribuicao/relatorio_unb.pdf