Projeto de Formatura – 2020 – Press Release

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia Elétrica – Ênfase Computação

Tema:

SISTEMA DE SORTEIO JUSTO, DISTRIBUÍDO E AUDITÁVEL PARA APLICAÇÕES LEGAIS

---

# Alunos da Poli-USP desenvolvem sistema para aumentar a transparência do STF

*São Paulo, 1 de Dezembro de 2020*

Muitos brasileiros questionam a legitimidade das instituições do nosso país, justificado em grande parte, pelas constantes denúncias de esquemas de corrupção. A falta de transparência nos processos internos das entidades faz com que haja desconfiança por parte da população com relação a autenticidade dos procedimentos que ocorrem em cada uma delas. No entanto há quem queira resolver esse problema.

Dois alunos de engenharia elétrica da Escola Politécnica da USP desenvolveram um aplicativo para acabar com uma das caixas pretas que existem na máquina pública: o sorteio de processos legais entre os ministros do Supremo Tribunal Federal (STF). Hoje em dia, apesar do código usado pelo sistema atual estar disponível publicamente, o procedimento do sorteio, do início ao fim não é totalmente transparente, nem há garantias que o mesmo sistema é implantado nas máquinas, o que cria margens para a dúvida de sua legitimidade.

Sob orientação do professor Marcos Simplício, os alunos Giovanni Abeni e João Paulo Lins resolveram implementar um aplicativo que, além de fazer uma escolha aleatória para ser usada no sorteio, pudesse ser 100% auditado, para que não houvesse dúvidas quanto a sua legitimidade. A base do sistema é uma técnica de criptografia, conhecida como *Commit and Reveal*, na qual a comunicação de uma mensagem é feita em duas etapas: na primeira – *commit* – o conteúdo da mensagem é escolhido, criptografado com uma chave e enviado; na etapa seguinte - *reveal* - o remetente fornece essa chave, revelando ao grupo o conteúdo que até então estava protegido.

Na situação do sorteio, cada participante tem um índice numérico atrelado a si e envia ao sistema um número de sua escolha, de maneira criptografada. Quando todos participantes tiverem enviado seu número protegido, os envios são revelados. Em seguida, é feita uma soma de todos números e a divisão deste total pelo número de participantes. O sorteado será aquele cujo índice seja igual ao resto dessa divisão. Essa lógica é a mesma utilizada no jogo de "dedos iguais", comum entre crianças que querem sortear alguém do grupo para alguma brincadeira.

O diferencial deste método é que, por meio de protocolos formais, o aplicativo consegue garantir – e isso pode ser testado e auditado – que basta que um participante do sorteio não esteja em conluio com todos outros, para que o sistema seja 100% justo e aleatório. Além disso, no sistema proposto, todo o processamento é feito de maneira distribuída, ou seja, sem dependência de uma entidade central. Isso significa que não é necessário confiar em um sistema nebuloso, mas sim no próprio processo, que por si só, é aleatório e imparcial.

O projeto foi desenvolvido de maneira modular, fornecendo bibliotecas de código pré-prontas para implementações mais variadas por parte da comunidade de desenvolvedores, podendo ser replicável para outras aplicações.

---


Integrantes: Giovanni Abeni dos Santos
João Paulo Lins

Professor: Marcos Antonio Simplício Júnior