Estudo sobre mecanismo de autenticação descentralizada

Gabriel Oliveira Portal[1], Régio Antonio Michelin[1]*
*Orientador

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - *Campus* Restinga. Porto Alegre, RS, Brasil.

O constante crescimento da internet nos dias atuais instigou em alguns pesquisadores a ideia de descentralizar alguns recursos na rede, com o intuito de gerar sistemas independentes de um núcleo, garantindo maior segurança dos dados por não estarem alocados em um único local, e simultaneamente garantindo mais integridade ao sistema. Atualmente o sistema mais conhecido que implementa tal conceito é a moeda de *Bitcoin*, que por sua vez fornece ao usuário um sistema monetário distribuído que apresenta uma estrutura de segurança de dados diferente do modelo adotado atualmente por sistemas convencionais. O projeto consiste no estudo de um sistema de autenticação descentralizada, tal como o protocolo presente no sistema *Bitauth*, o qual está sendo analisado, e realizado um levantamento da forma de uso, bem como seu sistema de proteção das informações dos usuários. O projeto tem como principal objetivo a busca pelo desenvolvimento de um sistema de autenticação descentralizado, tal qual não possua um nó centralizador que detenha as informações dos usuários, portanto retirando do sistema um ponto suscetível a falhas. Para compreensão do modo de funcionamento de um sistema descentralizado foi analisado o protocolo utilizado pelo *Bitcoin* que é baseado em uma *blockchain*. A *blockchain* tem um funcionamento baseado em transações, tal qual cada transação gera um *hash* que é passado por parâmetro na transação posterior, formando, portanto, uma cadeia de informações inalteráveis, devido a serem historicamente dependentes. A tecnologia adotada para o desenvolvimento do sistema é o *node js*, que apresenta vantagens em relação ao custo de memória durante execução dos *requests*, tendo em vista que o sistema é baseado em transações, poupar memória durante os *requests* é um fator muito importante a ser visado. Atualmente o sistema a ser implementado está em uma fase de desenvolvimento e aprimoramento, portanto, ainda necessita que seja implementado o módulo responsável por controlar as chamas das *rests*, definindo diferentes permissões a determinados usuários, e necessita que sejam efetuados ajustes para que o sistema comece a operar com o formato descentralizado. Já está presente no estado atual do sistema o modelo de autenticação utilizando pares de chaves em curvas elípticas com a biblioteca Secp256k1, que por sua vez, é a mesma utilizada para garantir segurança no protocolo utilizado pelo *Bitcoin.* A pesquisa que está sendo realizada neste projeto permitiu concluir que é possível desenvolver aplicações descentralizadas para funções diferentes das conhecidas da atualidade, além disso foi possível verificar que o sistema *bitauth* apresenta possíveis vulnerabilidades no esquema de chamadas cliente/servidor e portanto, para desenvolver uma aplicação segura como era esperado no escopo do trabalho, será necessário reimplementar o sistema foco.

Palavras-chave: Autenticação. Sistema. Descentralizado. *Bitauth. Bitcoin*.

CNPq FAPERGS