Estudo e desenvolvimento de um Smart Contract para transferência de segredo industrial via blockchain

Cristian Bonamigo Giombelli[1], Roger Sá da Silva[1], Anderson Ricardo Yanzer Cabral[2], Giovani André Gasparin[1], Marcos Marcelo Lewandowski[1], Erik Schuler[1*]

*Orientador(a)

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - *Campus* Veranópolis. Veranópolis, RS
[21]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS) - *Campus* Viamão. Viamão, RS

Este trabalho tem por objetivo atender o desenvolvimento de tecnologia que possibilite a transação entre um vendedor e um comprador de um segredo industrial, através de uma plataforma segura, garantindo que a troca seja feita de forma automatizada, sem a participação de terceiros. Partindo-se da teoria do Paradoxo da Informação de Arrow para a possibilidade de se revelar um segredo sem que este tenha seu valor anulado quando da sua revelação completa, foram analisadas as possibilidades da utilização da tecnologia de smart contracts para viabilizar e validar a transação deste tipo de informação. Smart contracts nada mais são do que contratos propriamente ditos, porém executados na forma de um código de programação, tendo sua execução realizada de forma automática e validada de forma descentralizada, através da tecnologia de blockchain. A ideia da negociação do segredo baseia-se no conceito de Prova de Conhecimento Nulo, no qual o vendedor e o comprador do segredo trocam informações entre si (provas) sem, entretanto, revelar de fato qual é o segredo. Assim, optou-se pela realização de uma plataforma que realize a comunicação entre o vendedor e comprador do segredo (rede centralizada), a qual fará a interface, através de uma API (Application Programming Interface), com a rede Ethereum (rede descentralizada), responsável pela execução e validação do smart contract. O uso da rede Ethereum, entretanto, apresenta algumas características que tornam sua aplicação complexa, tais como o custo de implementação, a necessidade de conhecimento de linguagem de programação própria, a baixa facilidade de manutenção e a agilidade de desenvolvimento. Desta forma, o seu uso, em princípio, ficará restrito à troca final (pagamento e transferência do segredo) entre comprador e vendedor, enquanto a utilização da rede centralizada ficará com o papel de comunicação na forma de interface desenvolvida em linguagem voltada para web (php). Para a metodologia, inicialmente foi desenvolvido levantamento bibliográfico a respeito do Paradoxo de Arrow, do conceito de Prova de Conhecimento Nulo, segredos industriais, smart contracts e blockchain, bem como os requisitos para implementação do smart contract. Após, foi criado um fluxograma para organizar a abordagem e evolução do processo, no qual estão presentes as formas e técnicas que serão utilizadas para o desenvolvimento da plataforma, tanto no âmbito da rede centralizada, quanto descentralizada. Como resultados parciais, citam-se a criação de parte do aplicativo web que será utilizado como interface do usuário para comunicação e troca das informações relevantes na negociação do segredo industrial. Encontram-se em fase progressiva, simultaneamente, o smart contract e o API de comunicação entre a plataforma e a rede Ethereum .

Palavras-chaves: Smart contract. Segredo industrial. Ethereum.

CNPq FAPERGS