Seguros Mútuos com Smart Contracts via Blockchain

Victor Hayashi[1], **Renato Penha**[1], **Gabriela Silva**[1],
Lucas Vieira[1], **Luiz Ferreira**[1], **Raduan Muarrek**[1],
Sophia Dias[1], **Vitor Oliveira**[1]

[1]Instituto de Tecnologia e Liderança (Inteli)
Prof. Almeida Prado, 520 – 05508-070 – São Paulo – SP – Brazil

{victor.hayashi, renato.penha}@prof.inteli.edu.br

Abstract. *A solution was proposed to create efficient, cheap and secure mutual insurance pools on the Ethereum blockchain for an insurance startup located in São Paulo (SP), Brazil. Groups are made up of people who come together to protect against predetermined risks and are self-administered to some extent. The results show that the group's administration is carried out through smart contracts that automatically execute the conditions agreed by the parties. All business rules and financial reserves are kept in the smart contract. Users interact with the system in a web application that uses a Web3 API, which has a client area and a P2P insurance area for managing new groups and acting in the indemnity process.*

Resumo. *Uma solução foi proposta para criar pools de seguros mútuos eficientes, baratos e seguros na blockchain Ethereum para uma startup de seguros localizada em São Paulo (SP), Brasil. Os grupos são formados por pessoas que se unem para proteger contra riscos predeterminados e são autoadministrados até certo ponto. Os resultados mostram que a administração do grupo é realizada por meio de contratos inteligentes que executam automaticamente as condições acordadas pelas partes. Todas as regras de negócios e reservas financeiras são mantidas no contrato inteligente. Os usuários interagem com o sistema em uma aplicação web que utiliza uma API Web3, que possui uma área de cliente e uma área de seguros P2P para gestão de novos grupos e atuação no processo de indenização.*

1. Introdução

A Blockchain é considerada uma tecnologia emergente que pode aumentar o nível de segurança das aplicações na Internet de forma decentralizada e com transparência. Após a popularização do Bitcoin e outras criptomoedas, que utilizam a Blockchain com seu mecanismo de consenso distribuído [Nakamoto 2008], diversas outras oportunidades de aplicação da tecnologia surgiram, como compra e venda de energia [Gabrich et al. 2017] e para registros acadêmicos [Palma et al. 2019].

Dentre as novas possibilidades de utilização da Blockchain, se destacam a adoção dos *smart contracts*. Os *smart contracts* são aplicações decentralizadas desenvolvidas na linguagem Solidity [Dannen 2017]. Com os *smart contracts*, é possível estabelecer acordos entre entidades sem a necessidade de organizações intermediárias [da Silva and da Silva Sendin 2020]. Para a criação de um *smart contract*, um conjunto

de regras de negócio deverá ser estabelecido entre as partes envolvidas na transação. Para suportar esse contexto, [Dannen 2017] aponta que as soluções devem utilizar as redes descentralizadas da Ethereum.

Dessa forma, o uso dos *smart contracts* nas soluções ganham um papel de destaque na arquitetura de possíveis aplicações como comércio eletrônico, organizações financeiras decentralizadas [da Silva and da Silva Sendin 2020], operações de compra e venda de energia elétrica gerada de forma distribuída [Kirli et al. 2022] e para transações de seguradoras [Cardoso and de Souza Pinto 2018]. Nesse sentido, o objetivo artigo foi desenvolver uma solução em *Blockchain* Ethereum baseada em *smart contracts* para gerenciar grupos de seguros mútuos para proprietários de aparelhos de telefonia celular. A solução foi desenvolvida para uma *startup* de seguros situada em São Paulo (SP), Brasil.

2. Problema

A Coover é uma *startup* de pequeno porte da área de seguros (*insurtech*), que oferta serviços de seguro contra furto e roubo de celular e plano de saúde para animais de estimação. A Coover está inserida em um mercado competitivo com diversos concorrentes consolidados, como a Porto Seguro e Bradesco Seguros. A Coover procura se posicionar no mercado de seguros mútuos por meio do desenvolvimento de uma solução sob a tecnologia Web 3 e *smart contracts*, sob uma arquitetura *peer-to-peer*. A solução será capaz de realizar todos os seus processos de negócio, desde a contratação, a vistoria do aparelho celular e indenização do seguro.

Em se tratando de adesão de contratos mútuos no Brasil, uma pesquisa do Panorama *Opinion Box* [Santos 2023] destaca que 11% dos portadores possuem algum tipo de proteção privada para aparelhos celulares. Nesse contexto, os seguros mútuos aparecem como uma solução disruptiva às soluções atuais do mercado, permitindo que grupos de pessoas criem reservas de dinheiro de forma distribuída. Como resultado, tais soluções podem garantir a segurança na adesão e no gerenciamento de contratos mútuos de aparelhos celulares. Para isso, há o destaque para o uso dos *smart contracts* da tecnologia *blockchain* como uma solução relevante para seguradoras [Cardoso and de Souza Pinto 2018]. Em relação à literatura, alguns exemplos teóricos para o setor de seguros são apresentados [Gatteschi et al. 2018], existe uma solução para seguro de carros [Nanda et al. 2022] e seguro para agricultores [Kshetri 2021]. A solução proposta neste artigo, de acordo com o melhor conhecimento dos autores, é uma das primeiras para seguro de aparelhos celulares.

3. Solução Proposta

A administração do grupo será realizada por meio do uso de *smart contracts*, que são programas que controlam determinadas condições acordadas previamente pelas partes interessadas em uma transação. Nesse sentido, todas as regras de negócio, desde a contratação até as reservas financeiras dos seguros mútuos serão mantidas nesse contrato inteligente. As seguintes regras de negócio estão presentes no *smart contract*:

Regra de Negócio 1: A Coover é definida como dona e administradora do contrato, devendo estabelecer os membros deste e o *hash* dos IMEI (*International Mobile Equipment Identity*) dos aparelhos protegidos, assim como a taxa administrativa. **Regra de Negócio 2**: Os membros conforme contrato implantado devem realizar um pagamento

inicial . Todo e qualquer valor deve ser depositado em ETH. O primeiro aporte deve ser referente ao percentual mínimo do valor protegido(definido pela Coover e específico de cada grupo, desse valor será separado uma porcentagem, também definida pelo criador do contrato, relativo à taxa administrativa); sem esse pagamento não é possível entrar no grupo. **Regra de Negócio 3**: A Coover deve aprovar a indenização de um segurado e, a partir disso, é informado a carteira dele. O hash do segurado em que o sinistro ocorreu deve ser igual ao que está armazenado no contrato de sua carteira para que seja concretizado. Além disso, o cliente deve anexar um Boletim de Ocorrência sobre o "por quê" do pedido, com isso o administrador da Coover analisa o documento e "aprova" ou "recusa" a proposta. **Regra de Negócio 4**: A Coover pode retirar a taxa administrativa a qualquer momento. **Regra de Negócio 5**: O cliente deve conseguir ver seu valor de reserva para conferir o valor protegido do seguro. **Regra de Negócio 6**: O cliente deve conseguir repor sua reserva. Todo e qualquer valor deve ser depositado em ETH. A reserva de risco deve atingir o percentual mínimo do valor protegido(definido pela Coover e específico de cada grupo, desse valor será separado uma porcentagem, também definida pelo criador do contrato, relativo à taxa administrativa).

Na Figura 1, há dois atores que interagem com o sistema: a seguradora P2P (*Peer to Peer*, representada pela Coover) e o participante (cliente do seguro). Essa interação dos usuários acontece através do *Frontend*, onde se encontra a lógica da interface, além disso para acessar as funcionalidades da aplicação é necessário se conectar a MetaMask por meio de um *plugin*, pois para realizar determinadas ações será necessário confirmações usando a chave privada.

No bloco *Backend* da Figura 1, há o sistema de dados da Coover, onde são armazenados dados pessoais de seus clientes, que não podem ser publicados no *smart contract*, mas são necessários para definir a lógica de negócios do software. Por fim, a seguradora P2P (administradora) realiza a implantação do contrato (*smart contract*) na Ethereum Testnet com o mecanismo de consenso *Proof of Work*, *blockchain* disponível do Ethereum para testes. Nesse *smart contract* estará armazenado os fundos dos grupos mútuos e todas as regras de negócio, tais como a de pagamento de indenização.

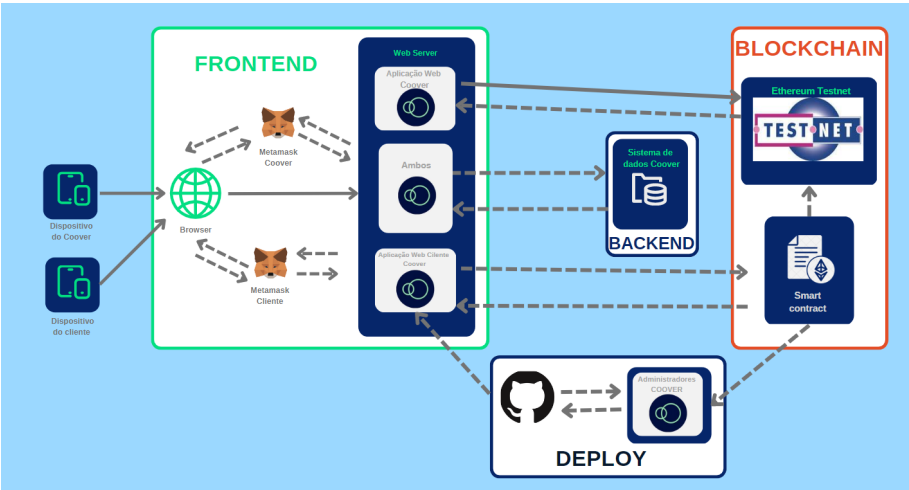

Figura 1. Arquitetura Proposta em Alto Nível

Para a criação de *smart contract*, partindo do princípio que será uma atividade ad-

ministrativa, a criadora e *owner* (dono do contrato) seria a Coover. O processo de criação da Figura 2 começa com a criadora informando como será o seguro, seja de maneira técnica exibindo o código do contrato, como também comercial, informando no *frontend* valores como taxa administrativa, faixa de preço, e valor percentual mínimo. A entidade "Pré-ativação" se refere à funcionalidade de construir o esqueleto de um contrato antes que ele seja publicado, possibilitando que o cliente se informe dos valores do contrato e a seguradora monitore a quantidade de clientes inseridos/interessados naquele contrato.

Depois desse processo, a Coover irá encontrar e atrair usuários para o grupo de seguro, alocando eles para o contrato, conseguindo assim termos a pré ativação do contrato, que é informado ao criador. Depois desses pré-requisitos, o grupo P2P é confirmado pela seguradora, que ativa o contrato e logo em seguida faz a implantação na rede do Ethereum. A fim de executar uma prova de conceito, a implantação será feita na rede *testnet*.

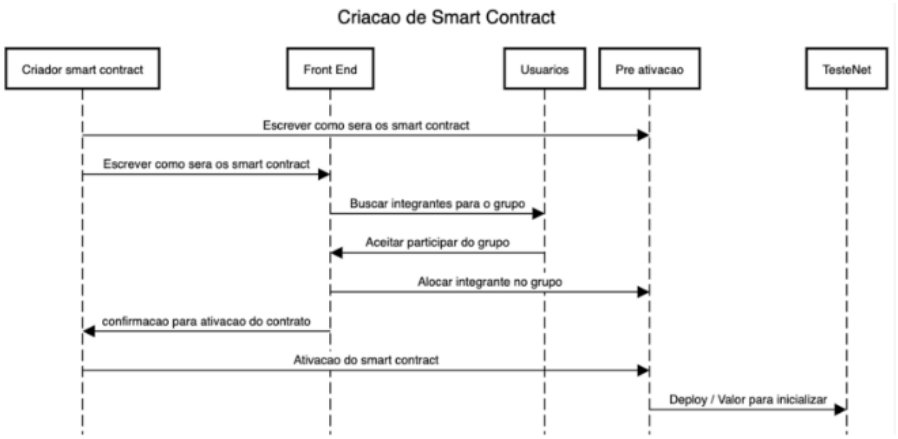

Figura 2. Processo de Criação de um Contrato

Para o processo de indenização ilustrado na Figura 3, o usuário somente irá realizar essa ação quando ele for roubado e quiser requisitar a indenização. Nesse caso, teremos uma primeira fase de cadastro completo na MetaMask a partir de uma autenticação e, posteriormente, a fim de validar que o celular roubado realmente está cadastrado no contrato, o usuário deverá fornecer o IMEI do celular por meio da interface de usuário. Esses são os passos necessários para o usuário encontrar e informar os dados pré requisitados.

Após esse processo inicial, pode-se seguir para a requisição em si, etapa em que o usuário enviará o B.O. por meio da interface de usuário, este que será repassado para a seguradora a fim de possibilitar a validação do pedido por uma instituição confiável. Em caso de aceite da indenização, o *smart contract* deve ressarcir o usuário por meio do endereço de carteira enviado.

Para a reposição de reserva de risco da Figura 4, considerando o escopo limitado do projeto, o usuário poderá repor uma vez que um cliente do mesmo grupo do seguro mútuo for roubado e tiver sua indenização aceita, sendo assim, o usuário pode examinar por meio de interface de usuário se a sua carteira possui uma porcentagem satisfatória do LMI (Limite máximo indenizável).

No caso do cliente estar insatisfeito com o seu saldo, ele poderá depositar dinheiro através de sua MetaMask e, logo em seguida, transferir para o contrato, atualizando as-

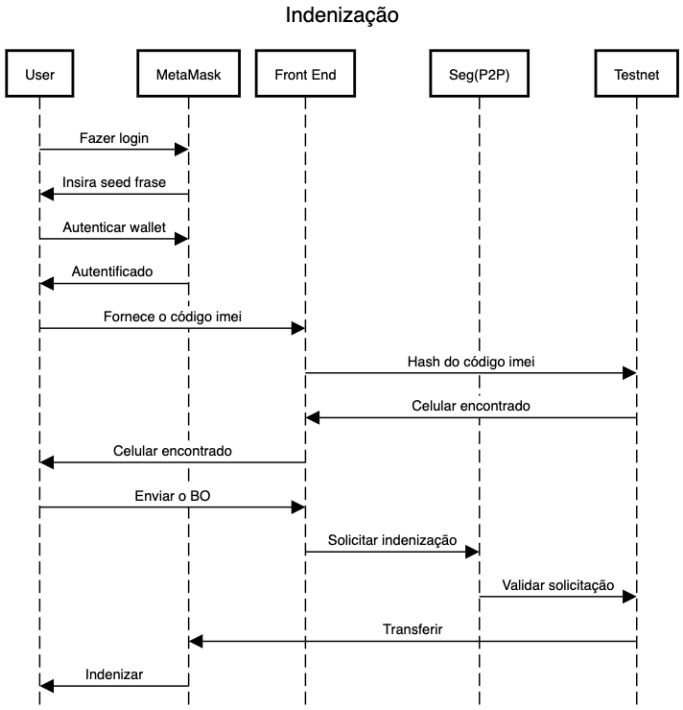

Figura 3. Processo de Indenização

sim seu montante financeiro dentro das regras do *smart contract*. Então a interface irá informar ao cliente que o saldo foi atualizado.

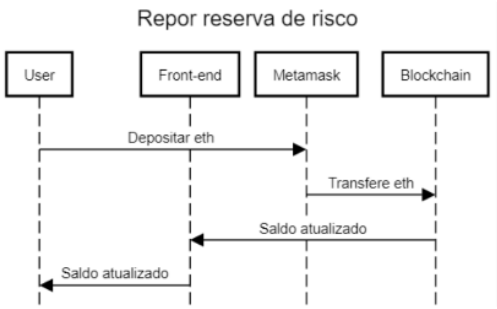

Figura 4. Reposição da Reserva de Risco

4. Materiais Disponíveis

Os códigos de *smart contract* em Solidity estão disponíveis em: `https://github.com/2023M5T4-Inteli/Projeto4/tree/main/truffle/contracts`. O código fonte da solução completa está disponível em: `https://github.com/2023M5T4-Inteli/Projeto4`. A documentação completa da ferramenta está disponível em: `https://github.com/2023M5T4-Inteli/Projeto4/blob/main/documentos/Documenta\%C3\%A7\%C3\%A3oProjetoM\%C3\%B3dulo5_V03.pdf.pdf`. O procedimento de instalação está disponível em: `https://github.com/2023M5T4-Inteli/Projeto4/blob/main/README.md#deploy`. Um vídeo de demonstração da ferramenta está disponível em: `https://www.youtube.com/watch?v=2S6d2cpbxdw`.

5. Conclusão

Este artigo apresentou uma solução Web3 para seguro de aparelhos celulares. Como trabalhos futuros, uma avaliação de desempenho da solução proposta pode ser realizada para avaliar o desempenho da solução conforme a variação do número de grupos e transações, além de uma análise de custos operacionais, tempo necessário para execução das operações, e um estudo sobre a implantação na rede real do Ethereum.

Referências

Cardoso, J. A. A. and de Souza Pinto, J. (2018). Blockchain e smart contracts: Um estudo sobre soluções para seguradoras. In *Congresso de Gestão, Negócios e Tecnologia da Informação–CONGENTI*.

da Silva, B. C. and da Silva Sendin, I. (2020). Smart contracts como uma plataforma para computação segura. In *Anais Estendidos do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 235–241. SBC.

Dannen, C. (2017). *Introducing Ethereum and solidity*, volume 1. Springer.

Gabrich, Y. B., Coelho, I. M., and Coelho, V. N. (2017). Tendências para sistemas microgrids em cidades inteligentes: Uma visão sobre a blockchain. *XLIX Simpsio Brasileiro de Pesquisa Operacional, Blumenau*, pages 1–12.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., and Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet*, 10(2).

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., and Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, 158:112013.

Kshetri, N. (2021). Blockchain-based smart contracts to provide crop insurance for smallholder farmers in developing countries. *IT Professional*, 23(6):58–61.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.

Nanda, S. K., Panda, S. K., Das, M., and Satapathy, S. C. (2022). Automating vehicle insurance process using smart contract and ethereum. In Chakravarthy, V. V. S. S. S., Flores-Fuentes, W., Bhateja, V., and Biswal, B., editors, *Advances in Micro-Electronics, Embedded Systems and IoT*, pages 237–247, Singapore. Springer Nature Singapore.

Palma, L. M., Vigil, M. A., Pereira, F. L., and Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in brazil. *International Journal of Network Management*, 29(3):e2061.

Santos, G. (2023). Celulares lideram lista de furtos e roubos, mas só 11% têm seguro no país. Disponível em: https://www.infomoney.com.br/minhas-financas/celulares-lideram-lista-de-furtos-e-roubos-mas-so-11-tem-seguro-no-pais/. Acesso em 11 de outubro de 2023.