Pagamentos Automatizados Programáveis em Carteiras Auto-Custodiadas: Uma Exploração Técnica

Ana Julia Bittencourt Fogaça[1], **Saulo Popov Zambiasi**[2]

[1]Universidade do Sul de Santa Catarina (UNISUL)
Tubarão - SC - Brasil

[2]Universidade do Sul de Santa Catarina (UNISUL)
Florianópolis - SC - Brasil

anajuliabit@gmail.com, saulopz@gmail.com

Abstract.

Resumo. *(provisório) À medida que a tecnologia blockchain continua a ganhar adoção, percebe-se um crescimento na demanda por funcionalidades que viabilizem sua aplicação em situações reais. No âmbito deste artigo técnico, nos inspiramos na recente publicação da Visa como premissa para a exploração da implementação de pagamentos programáveis automatizados em carteiras de auto custódia. Adentramos na esfera do conceito de Abstração de Contas e propomos uma execução codificada em Solidity com o propósito de habilitar pagamentos recorrentes originados diretamente de carteiras sob controle do usuário. Por meio desta sondagem, nosso intuito primordial é fornecer perspectivas elucidativas e orientações pragmáticas relativas à implementação de pagamentos automáticos no contexto das finanças descentralizadas.*

RESUMO

Sim, nem precisa fazer nada aqui por enquanto. Só vamos ver mais pro final.

1. Introdução

A tecnologia blockchain, primeiramente introduzida por Satoshi Nakamoto em 2008, é identificada como uma megatendência computacional capaz de revolucionar múltiplos setores industriais[World Economic Forum]. As características distintas de segurança, transparência e rastreabilidade inerentes à blockchain têm incentivado uma ampla gama de setores a explorar seu uso na reestruturação de suas operações fundamentais. A aplicabilidade dessa tecnologia ultrapassa o domínio das criptomoedas, abarcando setores como pagamentos, gerenciamento de identidade, saúde, eleições governamentais e outros[Pu and Lam 2021].

Com a divulgação do *whitepaper* Ethereum em 2014, um marco significativo foi estabelecido no desenvolvimento da tecnologia blockchain[Buterin 2014]. Distinto do Bitcoin, que foi originalmente idealizado como um sistema de pagamento digital, Ethereum introduziu uma funcionalidade inovadora na tecnologia blockchain: os contratos inteligentes (*smart contracts*). Esta inovação foi concebida para se valer dos atributos da blockchain, implementando automaticamente os termos acordados entre duas partes ao formalizar um contrato em um ambiente desprovido de confiança,

uma característica que levou à denominação de *smart contract* para esse código de software[Pinna et al. 2019]. No entanto, apesar do seu grande potencial, a complexidade associada à aplicação prática da tecnologia é um dos obstáculos para a sua adoção em larga escala[Sadhya and Sadhya 2018]. Para utilizar de forma segura os aplicativos descentralizados (DApps) - aplicativos que substituem o sistema de back-end por contratos inteligentes, os usuários precisam possuir conhecimentos técnicos em criptografia para manter sua chave privada segura[Antonopoulos and Wood 2018].

Em face deste desafio, o presente estudo pretende explorar tecnicamente a ERC-4337[Buterin et al. 2021], também conhecida como *Account Abstraction (AA)*, para a execução de pagamentos automáticos em carteiras auto-custodiadas. A ERC-4337 apresenta uma inovação substancial, proporcionando maior flexibilidade no processo de validação de transações e permitindo autorizações personalizadas, que não necessitam necessariamente de uma assinatura criptográfica. Esta capacidade tem o potencial de aprimorar consideravelmente a experiência do usuário no ecossistema Ethereum[Coyle 2023]. Esta pesquisa procurará entender este recurso em profundidade e propor uma implementação prática para habilitar pagamentos automáticos em carteiras auto-custodiadas. O objetivo é oferecer uma visão esclarecedora e orientações pragmáticas relacionadas à implementação de pagamentos que possam servir como referência para futuras aplicações. A pesquisa foi inspirada por um estudo conduzido pela Visa, empresa líder em soluções de pagamento. A Visa propôs a ideia de realizar pagamentos automáticos na blockchain sem a necessidade de revelar chaves privadas utilizando os benefícios da ERC-4337[Andrew Beams and Kumaresan 2023]. No entanto, os detalhes técnicos ou o código-fonte para tal implementação não foram disponibilizados.

A estrutura deste artigo é a seguinte: após esta introdução, procederemos com uma revisão bibliográfica detalhada, começando por um overview do Ethereum, abordando elementos da linguagem de programação Solidity, da Ethereum Virtual Machine (EVM) e da ERC-4337. Na seção de desenvolvimento, analisaremos o estudo da Visa e proporemos uma implementação em Solidity para habilitar pagamentos automáticos programáveis em carteiras autogerenciadas. Concluiremos com uma discussão sobre as implicações e possíveis aplicações desta nova funcionalidade nas blockchains, revelando oportunidades inovadoras no campo dos pagamentos.

2. Revisão Bibliográfica

2.1. Ethereum

A compreensão clara das diferenças entre os dois tipos de contas no Ethereum é fundamental para um entendimento completo do funcionamento dos contrato inteligentes. No Ethereum, existem essencialmente duas categorias distintas de contas: as contas de propriedade externa (*externally owned accounts* - EOAs) e as contas de contrato (*contract accounts*). As EOAs, podem ser criadas e controladas por meio de carteiras como a MetaMask. Essas contas possuem uma chave privada que concede controle sobre o acesso aos fundos ou contratos associados. Em contraste, as contas de contrato apresentam características distintas das EOAs. Uma conta de contrato abriga o código de um contrato inteligente, uma funcionalidade ausente em uma simples EOA. Além disso, uma conta de contrato não possui uma chave privada. Em vez disso, é controlada pela lógica incorporada no código do contrato inteligente [Antonopoulos and Wood 2018].

As contas de contrato possuem endereços, semelhantes às EOAs, e também são capazes de enviar e receber Ether. No entanto, quando uma transação é destinada a um endereço de contrato, ocorre a execução desse contrato na *Ethereum Virtual Machine* (EVM), utilizando a transação e os dados da transação como entrada. Além do Ether, as transações podem conter dados que especificam qual função específica do contrato deve ser ativada e quais parâmetros devem ser fornecidos a essa função [Antonopoulos and Wood 2018]. Enquanto as EOAs permitem que os usuários tenham controle direto sobre seus fundos e contratos, utilizando suas chaves privadas para autorizar transações, as contas de contrato possibilitam a implementação de lógica programável e automatizada por meio do código do *smart contract*.

Com a compreensão das diferenças entre contas de propriedade externa (EOAs) e contas de contrato, podemos agora explorar as aplicações descentralizadas (DApps) em maior detalhe. Essas aplicações substituem a infraestrutura tradicional de back-end por smart contracts que operam em blockchains como o Ethereum. Atualmente, o campo mais consolidado no contexto das DApps é o das finanças descentralizadas. No entanto, a complexidade inerente ao uso das DApps tem sido um obstáculo para a adoção em massa dessas aplicações.

Para enfrentar os desafios intrínsecos mencionados, são realizados esforços contínuos para aprimorar e simplificar a experiência do usuário no ambiente do Ethereum. Como o Ethereum é uma rede descentralizada e de código aberto, a comunidade constantemente formula propostas de melhoria conhecidas como *Ethereum Improvement Proposals* (EIPs). Uma proposta relevante para nossa discussão é a EIP-4337 [Buterin et al. 2021].

A EIP-4337, também conhecida como Account Abstraction (AA), introduz uma inovação radical no modelo convencional de contas no Ethereum, sugerindo a utilização de smart contracts no lugar das tradicionais EOAs. Essa proposta tem o potencial de abrir novos casos de uso na plataforma.

Ao proporcionar maior flexibilidade no processo de validação de transações, a Account Abstraction (AA) desencadeia uma série de novas capacidades, destacando-se a possibilidade de autorização personalizada sem a obrigatoriedade do uso de ECDSA, assim como nas EOAs. Isso permite a adaptação da lógica de autorização de acordo com necessidades específicas [World Economic Forum]. Esse caso de uso específico que será o foco central deste artigo. Através da EIP-4337, podemos estabelecer regras de validação que não dependem necessariamente da assinatura do proprietário da conta, o que representa uma inovação para as blockchains. Até então, a autorização de transações era exclusivamente baseada na atomicidade das assinaturas criptográficas, exigindo que a aprovação ocorresse instantaneamente, sem a possibilidade de pré-aprovação.

2.2. Account Abstraction

Account Abstraction é um conceito que vem sendo explorado para aumentar a flexibilidade e funcionalidade das contas na rede Ethereum.

Esse conceito sugere um desenvolvimento transformador na maneira como essas contas funcionam, propondo que todas as contas na rede Ethereum tenham a potencialidade de operar como Contas de Contrato. Isso implica que cada conta poderia abrigar sua própria lógica de operação, conduzindo a um grau de personalização e funcionali-

dade sem precedentes. Por exemplo, uma conta poderia ser programada para gerenciar transações de uma maneira específica ou para se defender contra certos tipos de ataques.

3. Desenvolvimento

3.1. Análise publicação da Visa

text

O texto abaixo precisa de referência

Em sua recente contribuição para a expansão do campo de pagamentos automáticos programáveis em carteiras auto-custodiadas via blockchain, a Visa apresentou revelações significativas numa publicação técnica intitulada ”Autopayments via Account Abstraction”. As próximas linhas fornecem uma síntese das conclusões primárias e propostas emergentes desta publicação.

Na sua abordagem, a Visa introduz um mecanismo inovador que simplifica a possibilidade do usuário de executar autopagamentos, prescindindo do uso da chave privada associada à sua identidade. O intuito subjacente é viabilizar autopagamentos para comerciantes sem a necessidade de expor a chave privada do usuário a qualquer servidor de terceiros. Como alternativa, um contrato inteligente é capacitado para processar um autopagamento em nome do usuário para o comerciante destinatário, sem a exigência da chave privada do usuário.

O modelo concebido pela Visa concede ao contrato inteligente a autoridade de conduzir pagamentos automáticos aos comerciantes associados ao usuário, estando sempre condicionado à ratificação deste último. Esta ratificação pode ser obtida através do fornecimento de dados que o contrato inteligente está autorizado a utilizar para realizar os autopagamentos em representação do usuário. Em essência, o usuário pode pré-autorizar a transação, habilitando o contrato inteligente a processar o pagamento em seu nome quando uma solicitação é encaminhada pelo comerciante. A Visa sugere ainda que o usuário possa compilar uma lista de permissões, onde poderá pré-autorizar transações com pagadores predeterminados, como comerciantes, outros usuários, entre outros.

Na monografia técnica mencionada, a Visa recorreu a um conceito recente e a uma das principais propostas de desenvolvedores do Ethereum conhecida como Abstração de Conta para investigar a implementação de contratos inteligentes que viabilizem pagamentos programáveis automáticos. Propuseram uma inovadora solução para uma aplicação real de pagamentos automáticos, demonstrando como estruturar um contrato inteligente para uma carteira autogerida capaz de retirar fundos automaticamente, sem necessitar da participação ativa do usuário em cada instante para instruir e realizar pagamentos numa blockchain.

3.2. Abordagem da solução

Demonstração de como os pagamentos automáticos podem ser implementados usando contratos inteligentes de pagamento automático pré-aprovados escritos em Solidity.

3.3. Implementação técnica

Explicação dos passos técnicos necessários para configurar contas delegáveis em carteiras auto-custodiadas. Visão sobre o fluxo de transação e interação entre o contrato inteligente

de pagamento automático e as carteiras controladas pelo usuário.

3.4. Vantagens e Potenciais Aplicações

: Discussão dos benefícios e vantagens oferecidos pela solução proposta para pagamentos automáticos. Exploração de casos de uso potenciais além de pagamentos recorrentes, como serviços de recuperação de conta de terceiros e gestão de ativos.

4. Conclusão

text

Nem tente escrever conclusão ainda. Uma porque isso é só pra TCC II

~~Reflexão sobre a importância dos pagamentos programáveis e o potencial para inovações futuras no espaço blockchain. Pesquisa Futura e Considerações Identificação de possíveis áreas para futuras pesquisas e desenvolvimento na automatização de pagamentos em carteiras de auto-gestão. Discussão sobre possíveis desafios e considerações a serem tratados na implementação de pagamentos automáticos em escala.~~

Referências

Andrew Beams, Catherine Gu, S. R. M. M. and Kumaresan, R. (2023). Auto payments for self-custodial wallets.

Antonopoulos, A. and Wood, G. (2018). *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media.

Buterin, V. (2014). Ethereum white paper.

Buterin, V., Weiss, Y., Gazso, K., Patel, N., Tirosh, D., Nacson, S., and Hess, T. (2021). Erc-4337: Account abstraction using alt mempool. Ethereum Improvement Proposals.

Coyle, K. (2023). Account abstraction: Use cases, technical overview, and security considerations.

Pinna, A., Ibba, S., Baralla, G., Tonelli, R., and Marchesi, M. (2019). A massive analysis of ethereum smart contracts empirical study and code metrics. *IEEE Access*, 7:78194–78213.

Pu, S. and Lam, J. S. L. (2021). Blockchain adoptions in the maritime industry: a conceptual framework. *Maritime Policy & Management*, 48(6):777–794.

Sadhya, V. and Sadhya, H. (2018). Barriers to adoption of blockchain technology.

World Economic Forum. Deep shift - technology tipping points and societal impact. `http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf`.