Aokiji: Uma Carteira Digital Segura com Assinatura Limiar FROST para a Criptomoeda Nano

Diogo Gomes de Araújo, contact@diogoaraujo.com
Orientado cientificamente pelo Professor Doutor Paul Andrew Crocker

FACULDADE ENGENHARIA
Departamento de Informática

INTRODUÇÃO

Ao longo da última década, a tecnologia ***Blockchain*** tem revolucionado o mundo financeiro, permitindo um **registo de transações digitais seguro**, **transparente e descentralizado**. No entanto, por recorrer a chaves privadas guardadas exclusivamente pelo utilizador, existe um ponto único de falha. Para mitigar este risco, surgiram os **sistemas de assinatura limiar**, que permitem distribuir o **controlo da chave privada por vários utilizadores** de forma segura. Desta forma, evita-se a exposição da chave num único ponto, reduzindo significativamente a probabilidade de comprometimento ou roubo.

O presente projeto implementa, de raiz, um sistema de assinatura limiar baseado no protocolo ***Flexible Round-Optimized Schnorr Threshold (FROST)***, permitindo que grupos realizem **transações na criptomoeda Nano**, remotamente. Adicionalmente, desenvolve-se uma **carteira digital** que integra este sistema, tornando o seu uso mais simples e acessível ao utilizador.

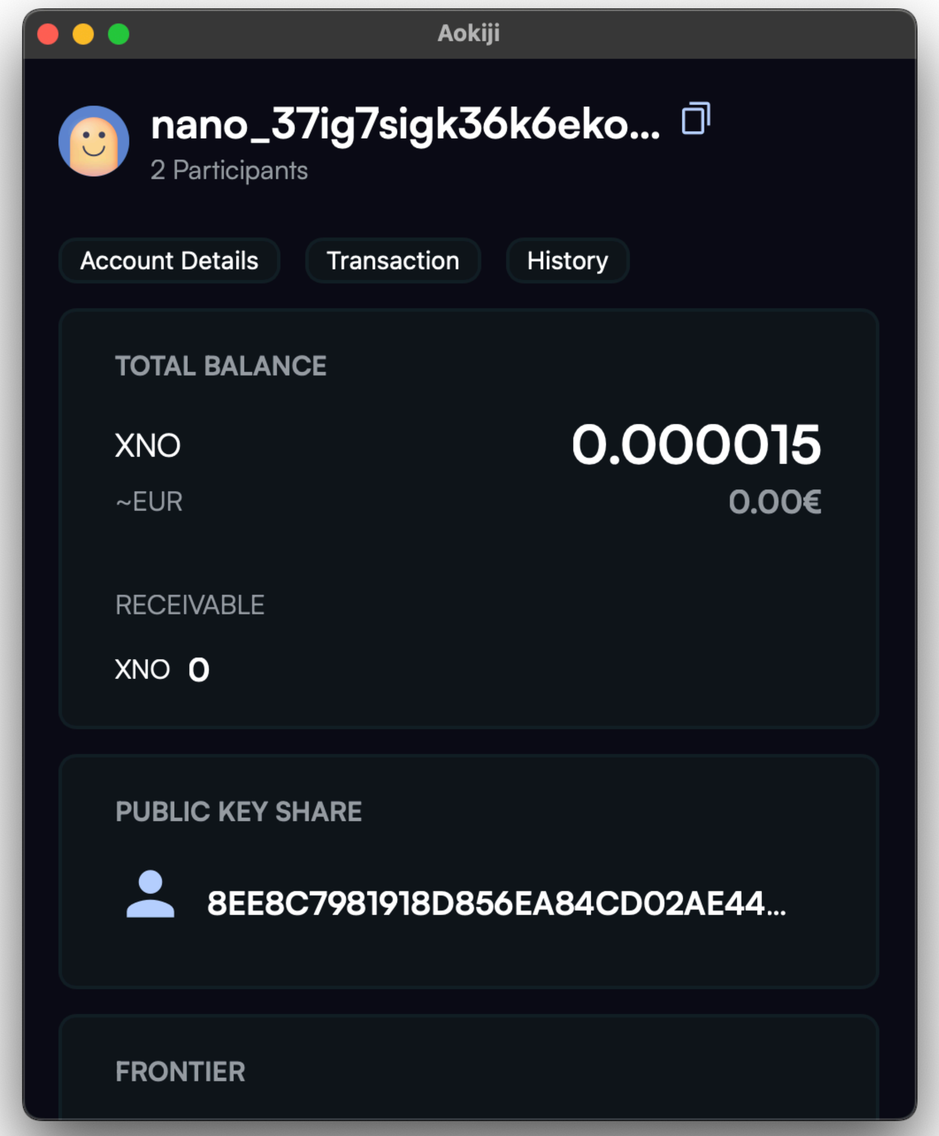
METODOLOGIA

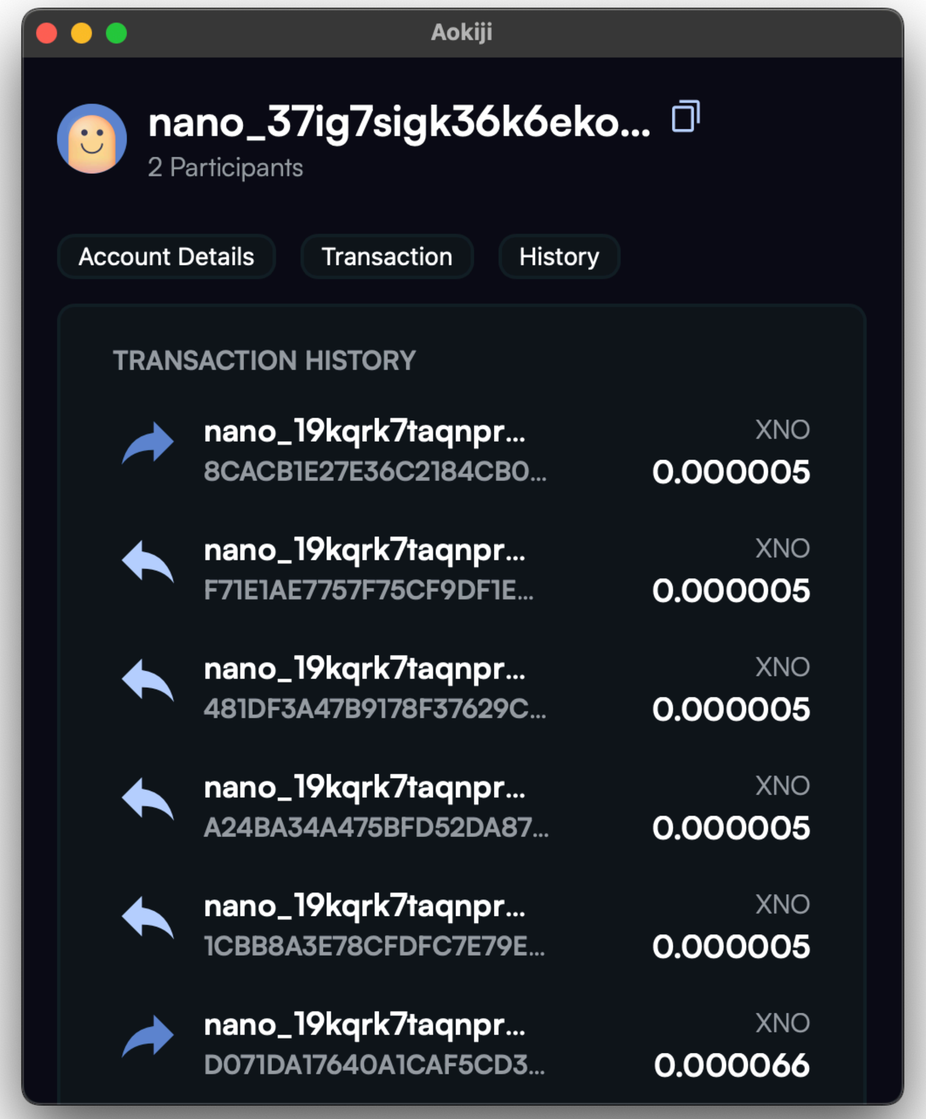
A metodologia adotada dividiu-se em três etapas principais:

1. **Estudo das tecnologias:** Foi realizada uma análise das tecnologias necessárias, nomeadamente Rust (pela segurança e performance), Dioxus (para a interface gráfica em Rust via WebAssembly), Dalek (para a criptografia de curvas elípticas) e os conceitos de criptografia necessários ao projeto.
2. **Desenvolvimento da biblioteca de contas em grupo:** Foi criada uma biblioteca em Rust que permite criar contas partilhadas na rede Nano e assinar transações de forma coletiva, recorrendo a protocolos threshold. Para facilitar a comunicação remota entre os participantes, foi utilizado o recurso a Sockets para troca de mensagens criptográficas seguras.
3. **Desenvolvimento da aplicação *desktop*:** Foi desenvolvida uma aplicação desktop em Rust, utilizando WebAssembly para componentes dinâmicos, permitindo aos utilizadores visualizar o saldo, o histórico de transações e assinar operações em grupo de forma intuitiva e segura.

RESULTADOS

Como resultado do trabalho desenvolvido, foi criada uma aplicação desktop funcional, desenvolvida em **Rust**, com **Dioxus e WebAssembly**, que permite **gerir contas partilhadas** na rede Nano de forma segura e intuitiva. A aplicação possibilita **visualizar o saldo**, **consultar o histórico de transações** e **realizar assinaturas em grupo**, conforme ilustrado nas figuras seguintes.





Adicionalmente, foi desenvolvida uma **biblioteca modular** que implementa o protocolo **FROST**, capaz de produzir assinaturas digitais válidas e **verificáveis na Blockchain da Nano**. Embora tenha sido integrada na aplicação para assinar transações na rede Nano, esta biblioteca foi concebida de forma **versátil** e pode ser **reutilizada** em outros contextos, incluindo outras criptomoedas ou sistemas que necessitem de assinaturas limiar seguras.

O código-fonte da aplicação e da biblioteca, bem como o executável para instalação, encontram-se disponíveis através dos seguintes códigos QR:

Aplicação

Biblioteca

CONCLUSÃO

O projeto demonstrou a viabilidade e segurança da utilização de assinaturas limiares na rede Nano, permitindo a gestão colaborativa de contas de forma intuitiva e segura. A implementação do protocolo FROST mostrou-se eficiente, reforçando a privacidade e a resiliência do sistema. A aplicação desenvolvida, aliada à biblioteca modular, oferece uma solução prática e inovadora, contribuindo para a adoção de tecnologias descentralizadas.

AGRADECIMENTOS

Gostaria de expressar o meu profundo agradecimento ao Professor Doutor Paul Crocker, por me dar a oportunidade de realizar este projeto e pelo valioso apoio prestado ao longo de todas as fases do trabalho. A sua orientação, disponibilidade e partilha de conhecimento foram fundamentais para o desenvolvimento e concretização desta investigação. Agradeço também à Universidade da Beira Interior, pelos recursos disponibilizados, e a todos os colegas e familiares que me apoiaram direta ou indiretamente nesta jornada.