p2pix

Participantes: doiim & Quiver Trade

RELATÓRIO FINAL

1 Visão geral

Nosso protocolo para descentralização de *on-and-off-ramp* entre criptomoedas e dinheiro fiduciário brasileiro nasceu em setembro de 2022 durante o hackathon da Ethereum São Paulo num projeto que esteve entre os vencedores do evento.

Logo no começo de outubro iniciamos o processo de desenvolvimento com apoio do programa Lift Learning que nos apoiou com 5 engenheiros de software e 1 designer ligados à UnB que somaram esforços com o CTO, desenvolvedor blockchain e designer da doiim para criar o dApp p2pix em sua versão MVP. Na direção estratégica e plano de negócios são mais 3 board members doiim e 2 da Quiver Trade.

Seguindo agenda planejada anualmente pela Fenasbac conseguimos encaixar o final do Lift Learning em fevereiro de 2023 com o batch #2 do programa de aceleração Next Fintech que começou em março de 2023. Ou seja, chegamos em estágio pré-lançamento oficial da nossa aplicação descentralizadas, porque a publicação feita ao final do Lift Learning foi em testnets Ethereum e Polygon.

Como estamos rearranjando condutas, normas, contratos e parâmetros da web2 para criar um protocolo web3 esbarramos em um ponto de inflexão que é a falta do e2eID fornecido 100% pelo Banco Central do Brasil. Atualmente, o pagador que realiza transferências via Pix recebe seu comprovante direto do Bacen, mas o recebedor na outra ponta dessa transação tem seu 'recibo' gerado diretamente por sua instituição financeira e/ou iniciador de transação de pagamentos.

Entendemos que o 'coração' da ideia é que transferências já contam com Bacen como "oráculo" e é nele que pessoas brasileiras confiam. Nossa intenção é acelerar o processo de desintermediação entre cidadãos ou empresas que desejem acessar criptoativos direto via sistema nacional de pagamentos instantâneos via DeFi.

Todo esse contexto nos levou a abordar o programa Next sob duas perspectivas principais, tanto com mantenedores quanto mentores:

2 Plano de trabalho **Regulatório: Open Finance**

Conhecer o processo para 'se tornar' e manter um iniciador de transação de pagamentos ou uma instituição de pagamentos regulamentada no Brasil.

2.1 Objetivo

Saber a dificuldade e o provável tempo estimado para preencher todos trâmites legais ao se tornar ITP e depois IP.

2.2 Mentores envolvidos

Jihane Halabi, Marcelo Martins, Gustavo Costa Cunha e Keiji Sakai.

2.3 Sumarização dos resultados

Ao mesmo tempo que percebemos a alta complexidade para virar uma ITP no Brasil, também compreendemos que o prazo para que isso ocorra gira em torno de 2 anos, ou seja, dentro desse prazo a questão do e2eID já terá ~ possivelmente ~ sido resolvida pelo Bacen. Então seria um esforço empreendido sem retorno efetivo e não proporcionaria uma solução para lançarmos o p2pix ainda em 2023 (o que é nosso desejo).

No entanto, para aumentar número de casos de uso, é possível que avancemos na direção de transformar nosso protocolo em todos quatro tipos de IP (instituição de pagamento):

1. ITP (iniciador de transação de pagamento) responsável por disparar o comando do cliente pagador, mesmo sem deter a conta dele, e faz o recurso cair diretamente na conta do recebedor;
2. Credenciadora / Adquirente ('acquire') habilita estabelecimentos para aceitar transações de pagamento (Stone, Cielo, Rede, entre outras), pois faz processamento e liquidação do pagamento para o recebedor final (transacional) = faz parte do fluxo financeiro;
3. Emissor de moeda eletrônica (wallets / conta corrente ou 'conta de pagamento');
4. Emissor de pós-pago (cartão de crédito).

2.4 Feedbacks e ideias

Todas etapas deste plano de trabalho foram respondidas em congruência com as hipóteses levantadas lá em abril no ‘Plano de Trabalho’ estipulado no início do programa Next.

3 Plano de trabalho **Produto: descentralização e roadmap**

Saber o quanto vale a pena ter parceiros ao longo do caminho ou se é melhor acelerar o processo descentralizatório desde o começo.

3.1 Objetivos

Clarificar 'release plan' da evolução do p2pix.

3.2 Mentores envolvidos

Carlos Augusto de Oliveira, Courtnay Guimarães e João Paulo Pereira.

3.3 Sumarização dos resultados

Foi possível pensarmos por diferentes ângulos quais as implicações para o p2pix e também para seus parceiros para sub-iniciação de pagamento, iniciação de pagamento, instituição de pagamento, bem como evolução do Pix dentro do curto prazo.

3.4 Feedbacks e ideias

Algumas conversas demoraram a engrenar e o impacto de algumas mentorias só foi completamente entendido após discussões futuras com outras pessoas. Assim sendo, talvez faça sentido depois de transcorridas algumas conversas que se alinhe no checkpoint

entre fintech acelerada e equipe Next Fenasbac para que possa haver uma reunião, posterior às individuais, com mais de um mentor ao mesmo tempo junto com a empresa / startup integrante do programa de aceleração.

4 Projeto piloto **Finansystech / Celcoin**

Soluções modulares baseadas em blockchain com aplicabilidade no mundo real (...) que geram inclusão financeira e complementam o ecossistema do open finance (infraestrutura).

4.1 Proposta e Propósito

Tornar a solução viável para ser usada além das testnets nas quais o MVP teve seu deploy inicial (Goerli/Ethereum e Mumbai/Polygon). Ou seja, lançamento 'em produção' da v0.1 para usuários finais da solução p2pix.

4.2 Mantenedor / Parceiros Envolvidos

Por parte da Finansystech conversamos com Ana Carolina (analista e ponto focal), Danillo Branco (CEO), Daniel Campos (CTO), Caroline Geraldo (CPO), Igor Dantas Silva (PO), Gabriel Pereira (community manager). Além de Leandro Costa (desenvolvedor) da Celcoin.

4.3 Abordagem Técnica

A ideia é confiar no 'ITP as a Service' da infraestrutura ITP <> Pix, ou seja, não é confiar na ITP e sim na infraestrutura de ITPaaS.

O sandbox é uma collection JSON que é o demonstrativo FS/Celcoin mostrando fluxo open finance: e2eID é determinístico e aparece no webhook para o intermediador.

Houve concepção de caminho alternativo para controle de transação à assinatura via Finansystech/Celcoin usando chave API da FS/Celcoin para interagir com Chainlink Functions (rede ITPs para roadmap).

Motivos do porquê não é redundante na perspectiva de web3:

- API pode conversar com servidor via TLS;
- É imprescindível para interagir com blockchain, pois as EVMs (Ethereum Virtual Machines) são desconectadas da internet e só vão se comunicar em assinaturas de entidades previamente autorizadas no smart-contract.

Motivos do porquê é interessante utilizar essa solução, visto que é redundante apenas na web2. Em blockchain ainda não conseguimos interagir com APIs (são utilizados oráculos atuando na coleta de dados e informando os contratos-inteligentes);

- Foi sugerido um caso de uso de CCB tokenizada com pagamentos usando p2pix para liquidez;
- Seria possível usar ERC-20, mas o NFT ajuda a ter mais detalhes da transação. Por esse motivo foi optado pelo ERC-1155 para que as frações possam representar valores, multas ou prazos;
- A debênture seria o detentor do token (total ou parcial).

Após diversas discussões entre os times, foi decidido que a melhor forma para fazer essa 'chancela' seria assinar o retorno do open finance com a chave privada Finansystech que já é homologada:

- e2eID + chave destino + valor = validaria a transação sem precisar ter nenhum tipo de interação com API;
- chave RSA precisaria ser derivada para assinatura de curva elíptica; para isso, seria interessante fazer mudança com foco nos roll-ups e 2ª camada para futuro próximo;

Ficou a dúvida se resolveria replicar o endpoint existente hoje com retorno da assinatura ou chave-FS alimentando o Chainlink Functions. Esse movimento, basicamente seria pegar o retorno da requisição e assinar ele, mas pode ser interessante duplicar para não atrapalhar o fluxo atual (não precisa criar nada novo do lado FS).

Abaixo disponibilizamos o link do GitHub e dentro do README estão todos detalhes de como derivar um PrivateKey e usar isso para assinar mensagens. Protocolo p2pix autorizará chave-pública Finansystech/Celcoin a ser reconhecida dentro dos contratos inteligentes e acatar o que for informado por ela na mensagem assinada.

- https://github.com/doiim/p2pix-signature-schema

Como gerar wallet web3 que acionaria a chave para criar um smart-contract?

Via chave privada para assinar a mensagem que ~ *by the way* ~ não precisa ser on-chain para isso ser válida.

A única mudança significativa a se fazer no processo atual é derivar uma chave com curva elíptica, ou seja, criar estrutura parecida com APIs que já existem para assinar o retorno, seria um novo endpoint com as 'mesmas coisas'... mas assinado dessa nova forma, complacente com as necessidades da criptografia de um contrato inteligente. Ou para usar um pouco de "tecniquês": hash hexadecimal de 32 bytes).

Em outras palavras, seria o Open Finance brasileiro enriquecido com nova assinatura / chancela para formato de protocolo web3, tudo realizado nos moldes de API realizada em 'fase 3' do sistema financeiro aberto do Brasil porque precisamos apenas da iniciação de pagamento para funcionar como protocolo descentralizado na layer #01 de uma blockchain de rede pública.

Para quem entende melhor da desburocratização ao transitar informações consentidas pelos clientes, vamos no caminho da ITP ao invés de 'detentor de contas' via valor customizado:

1. *interaction id*;
2. chave destino Pix;
3. valor (*amount*);

Todas as três informações concatenadas e assinadas!

Sempre com máxima cautela para termos o mínimo de informação necessária sobre as pessoas gravadas em blockchain, por exemplo, se em algum momento no futuro do projeto for necessário guardar CPFs... estes serão hasheados para analisar junto com *client id*.

Futuro próximo... ideia original p2pix implementada na Finansystech:

- provável que isso ocorra no Q4 de 2023
    - próximo trimestre vai ser com foco na estabilização do novo produto FS;
    - até lá iniciativas com caráter de experimentação ficarão pausadas.

Plano de ação imediato = usaremos 'API Finansystech as is' como sub-iniciadores integrados ao oráculo da Chainlink Functions (solução em fase *beta*).

Assim, estaremos vinculados à FS direto, sem esforço de desenvolvimento dos nossos mantenedores. Para todos envolvidos, está claro que 'assinatura web3' só vai acontecer mais para o final do ano.

Para o 'demo day' do programa Next será sobre como usar assinatura e homologação... tudo explicado por tech-leaders Finansystech.

4.4 Sumarização dos resultados

Ao final das discussões, ficou claro que a Finansystech não pode alterar qualquer retorno ou criar integração no produto (para não regulamentados), pois o mesmo ainda está para ser lançado. Sabemos que o Smart Keys será lançado próximo à data do Demo Day do Next.

Para essa finalidade, listaremos a doiim como não-homologada no novo produto da Finansystech chamado Open Keys.

4.5 Visão de Futuro

Para doiim, esperamos solidificar parceria com Finansystech / Celcoin e contar com ajuda no processo de transformar o próprio p2pix em IP.

Iremos acompanhar o roll-out de soluções sobre account abstraction para tentar ter a melhor usabilidade disponível.

4.6 Feedbacks e ideias

Acreditamos que trazer tomadores de decisão para as rodadas de acompanhamento pode ser crucial para a celeridade do entendimento em relação àquilo que se quer construir.

Até conseguimos alguns 'bypass' graças a nossa presença e também do mantenedor em eventos do ecossistema de inovação financeiro brasileiro e pudemos cortar alguns caminhos por atalhos de ideias conjuntas, ainda assim o CTO do FS demorou muito para "entrar na jogada" e compreender nossa necessidade dentro do p2pix.

5 Projeto piloto **Mercado Bitcoin**

Soluções de infraestrutura para pagamentos inteligentes via stablecoins, operações financeiras na web3 como soluções de ponte entre o mundo real ou sistemas legados a blockchains e DLTs. Possibilidade de alguns casos de uso diferentes com Real Digital (CBDC brasileira) em breve.

5.1 Proposta e Propósito

Realizar uma POC que possa permitir ao p2pix ter sua 2ª stablecoin para on/off ramp entre cripto e moeda fiduciária. Depois de BRZ, agora também com MBRL.

5.2 Mantenedor / Parceiros Envolvidos

Reinaldo Rabelo (CEO), Fabrício Tota (Diretor de novos negócios), Lara Dal Soto (Product Manager e ponto focal), Lucas Pinsdorf (Produtos) e Débora Conconi (Novos negócios).

5.3 Abordagem Técnica

Estudamos a possibilidade de construir uma solução de ‘zero knowledge proof’, foi explorado o recurso de ZK badges da Sismo.

No futuro, provavelmente faremos prova de conceito usando selos atuais do próprio Mercado Bitcoin como "ouro, prata e bronze" ao invés de zero knowledge.

Aqui temos um resumo da discussão e escopo para construção do MVP e questões de compliance / AML:

- 'Whitelist' em apps descentralizados operando como corretoras (dEX): uma lista de endereços pré-aprovados que podem negociar, aumentando a segurança e reduzindo riscos de fraude e atividades ilícitas;
- Outra solução seria escalonamento via pontos de reputação
    - compra R$ 100 iniciais e depois R$ 1k (subindo aos poucos se não tiver KYC);
    - também é uma limitação técnica para evitar spam na rede;
- MB poderia atuar interferindo de forma automatizada nas reputações;
- ‘Merkel Tree’ implementada direto no smart-contract (usuários têm liberdade de transacionar se estiverem na mesma 'root' que os vendedores de criptomoedas)
- ‘Allowlist’ para transações com volume entre instituições também é algo importante que estamos considerando para OTCs.

Para o piloto específico entre doiim e Mercado Bitoin durante o programa de Aceleração Next, foi discutido, inicialmente, que o MBRL opera apenas na rede Stellar e que não é compatível com EVM. Por esse motivo não é possível usar essa solução no p2pix.

Para solucionar esse caso, o Mercado Bitcoin está trabalhando para realizar deploy do MBRL na rede pública Ethereum e assim poderemos usar o token dentro do p2pix.

No médio prazo também disponibilizaremos via Polygon com intuito de alcançar usuários menores e, posteriormente, na rede Arbitrum

5.4 Sumarização dos resultados

Possibilidade de piloto com lançamento do MBRL na Ethereum para promover uma segunda opção de token além do BRZ no p2pix.

5.5 Visão de Futuro

Aumentar o suporte de “sidechains” compatíveis com EVM (hoje rodamos o MVP em Ethereum e Polygon) para acompanhar a crescente maturidade na adoção de soluções em auto-custódia.

5.6 Feedbacks e ideias

Ainda que um pouco mais distante da rotina de trabalho intensa que tivemos com FS, ter essa interface com MB foi muito importante para entendermos caminhos possíveis sobre desintermediação entre moedas fiduciárias e criptoativos.

Ficamos muito satisfeitos em poder ter um segundo mantenedor nesse programa de aceleração junto com o time Fenasbac.