CryptoEscrow:
Mais segurança em negociações P2P

Motivação

As criptomoedas permitem a transferência direta de valores entre quaisquer pessoas no mundo sem depender de grandes bancos ou outras instituições financeiras. Embora isso abra um potencial enorme para mercados *P2P*, existem problemas que impedem que estes sejam explorados em sua plena potencialidade.
Um deles é a questão da confiança mútua entre as partes envolvidas em uma negociação: como garantir que cada pessoa irá cumprir com sua parte no acordo? Em uma troca de *crypto* por real (R$), por exemplo, como garantir que o comprador de *crypto* envie os reais (R$) para o vendedor e que o vendedor transfira as *cryptos* prometidas ao receber o dinheiro? Geralmente, uma das partes precisa ceder e confiar na boa índole/reputação da outra: em uma negociação de *crypto*, geralmente os vendedores exigem o pagamento em *FIAT* antes de transferir as moedas, como forma de proteção. Por um lado, há compradores que não se sentem nem um pouco seguros com essa abordagem; por outro, vendedores estão sempre receosos com a possibilidade de golpes, e muitos acabam exigindo documentos, *selfies* e outras provas na tentativa de evitá-los, tornando os seus serviços tão invasivos quanto os de exchanges centralizadas convencionais.

Hipótese

Se houvesse um ambiente em que tanto compradores quanto vendedores se sentissem mais seguros para negociar, tendo contrapartidas que minimizem a chance de golpes e que incentivem o comportamento honesto na negociação, todo o mercado *P2P* seria beneficiado, e as pessoas ficariam cada vez menos refém de grandes instituições centralizadas que raramente se importam com a privacidade e liberdade financeira dos seus usuários.

Proposta

Criar uma plataforma descentralizada e gerenciada por contratos inteligentes que estabeleça regras claras de conduta para negociações em *crypto* e que promova o comportamento honesto das partes:

1. Vendedores poderão criar um perfil para listar seus produtos e serviços incluindo informações para contato e quaisquer outros detalhes relevantes. Esses dados serão associados ao endereço de carteira utilizado pelo vendedor na plataforma, então, para melhorar sua privacidade, o vendedor poderá reservar uma carteira apenas para este fim.
2. Os dados de perfil dos vendedores serão armazenados em uma rede descentralizada, pública, imutável e resistente à censura: *IPFS + FileCoin*.
3. Estatísticas sobre o número total de negócios, negócios cancelados, concluídos e disputados serão armazenadas diretamente na *blockchain* — seja na rede *Ethereum*, na *Binance Smart Chain* e/ou outra compatível —, e ficarão disponíveis no perfil do vendedor.
4. Potenciais compradores poderão navegar pela lista de produtos/serviços e poderão entrar em contato com os vendedores para tirar dúvidas, esclarecer detalhes, etc.
5. Ambas as partes (comprador e vendedor) deverão realizar um depósito de segurança — pago em moeda base da rede, como *ETH* na *Ethereum* e *BNB* na *Binance Smart Chain* — exigido como garantia de que estes tenham *skin in the game* e estejam dispostos a negociar de forma honesta, sob a pena de perda de recursos financeiros em caso de disputas.
6. Um comprador poderá abrir uma negociação com um vendedor por meio de uma opção disponível diretamente no perfil desse vendedor. O comprador deverá realizar o depósito de segurança previamente acordado com o vendedor, depósito o qual será recolhido e armazenado sob custódia pelo contrato inteligente.
7. Logo em seguida, o vendedor deverá também realizar um depósito de valor igual àquele efetivado pelo comprador. Além do depósito de segurança, o vendedor deverá incluir, na mesma transação, uma pequena taxa automaticamente cobrada pela plataforma, a título de taxa de serviço.
8. Após 30 minutos, caso o vendedor ainda não tenha efetivado o depósito de segurança, o comprador terá a opção de cancelar a negociação, recuperando o depósito de segurança inicialmente colocado sob custódia no contrato inteligente.
9. O contrato inteligente irá automaticamente detectar quando ambas as partes efetuarem o depósito de segurança, instruindo ao comprador que cumpra com a sua parte do acordo.

10. Se a negociação ocorrer bem, o comprador deverá sinalizar o fato diretamente ao contrato inteligente, que fará a devolução dos depósitos de segurança para ambas as partes, diretamente em suas carteiras.
11. Qualquer uma das partes poderá solicitar mediação caso se sinta lesada pela outra. Isso vale tanto para um comprador que cumpriu sua parte no acordo mas não recebeu a contrapartida esperada do vendedor, quanto para um vendedor que se sinta prejudicado por um comprador inativo ou que tenha agido de forma contrária à acordada.
12. Em caso de disputa, as partes serão instruídas a contactar um árbitro da plataforma que irá trabalhar para resolver o conflito da melhor forma possível.
13. Ao solicitar mediação, uma taxa de mediação será cobrada sobre ambos os depósitos de segurança e repassada diretamente ao árbitro quando este concluir sua decisão. Isso cria o incentivo para que ambas as partes colaborem entre si e só recorram à mediação se estritamente necessário.
14. Caso ambas as partes cheguem a um acordo, o árbitro acionará uma opção no contrato inteligente para liberar os valores em custódia — já descontadas as taxas de mediação — para ambas as partes, encerrando o caso.
15. Se for comprovada a má-fé de alguma das partes, o árbitro poderá acionar uma opção no contrato inteligente para direcionar o valor remanescente do depósito de segurança da parte ofensora para a parte ofendida, encerrando o caso.