DePix

Uma maneira de entrar discretamente no mundo digital.

Contents

Prof. Dr. Wilhelm Hans-Friedrich von Bergen <bergen@depix.info>

v 2.2, 21 de agosto de 2024

Abstract

DePix é um token lastreado no Real brasileiro (BRL) na proporção de 1:1, operando na rede Liquid. Embora essa paridade seja usual, limitações operacionais podem afetar a conversão em grandes volumes, desafios esses que podem ser mitigados por "Banking Nodes" e diversificação do lastro. Os riscos são bem limitados e o DePix oferece vantagens significativas em termos de soberania e privacidade, especialmente em operações confidenciais de Bitcoin. Além de sua ligação com o Real, o **DePix** se destaca como um inovador **Transient Tactful Token (3T)**: 1) **Transient** – seu uso é temporário, servindo como intermediário entre o Real (mundo fiduciário) e o Bitcoin (mundo digital), sem a intenção de ser guardado a longo prazo, dado o risco de inflação do próprio lastro e risco de custódia. 2) **Tactful** – discreto, aproveitando a infraestrutura de transações confidenciais da rede Liquid ou outras redes com características semelhantes, aprimorando a privacidade nas transações, particularmente na conversão para ativos como o Bitcoin.

1 Motivação

O **Bitcoin** tem atraído a atenção de atacantes e agentes externos desde a sua criação [1][9] que tentam a todo custo dificultar a vida do usuário comum. Essa atenção se intensifica cada vez mais com o aumento de seu valor e volume de transações. Geralmente, esses atacantes se beneficiam de fraquezas do "sistema fiduciário legado" [2] onde, por ser um sistema centralizado e ultrapassado, tem pouca segurança e privacidade.

O principal ponto vulnerável do Bitcoin tem sido sua ligação com o sistema fiduciário tradicional [3]. No entanto, essa vulnerabilidade decorre mais das limitações do próprio sistema legado do que de qualquer falha intrínseca do Bitcoin. No Brasil, esse sistema fiduciário se consolidou com a introdução do sistema de pagamentos "PIX" no final de 2020 [4], que facilita transferências bancárias de maneira rápida, barata e padronizada. Embora o PIX ofereça benefícios significativos, ele também traz desafios para a privacidade e a soberania individual, centralizando e tornando instantânea a vigilância financeira. Para aqueles que buscam maior autonomia financeira, o desafio surge ao transferir valor entre o mundo digital (Bitcoin) e o sistema fiduciário (Fiat), uma conversão ainda necessária, dado que o Bitcoin não é amplamente aceito em transações cotidianas.

Para enfrentar esse desafio, o token **DePix** foi criado com o objetivo de aprimorar a privacidade e segurança daqueles que desejam acumular Bitcoin sem estarem sujeitos a uma vigilância constante e perigos externos. Vale destacar que o DePix tem como finalidade *melhorar* a privacidade, e não resolver todos os problemas de forma milagrosa. O token foi projetado para proporcionar maior soberania e privacidade a usuários individuais, e devido a suas características intrínsecas, detalhadas posteriormente neste documento. Apesar de sua grande utilidade, ainda não é adequado para operações em larga escala.

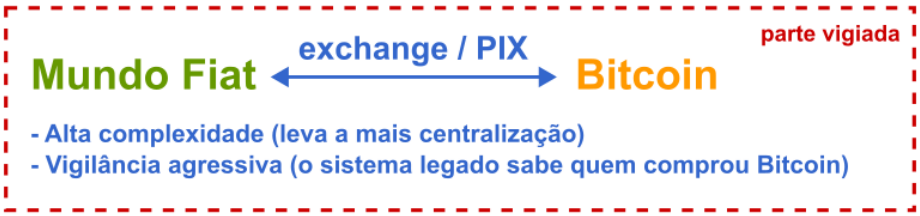
1.1 Entrada e saída do mundo digital

Como o Bitcoin não tem uma relação 1:1 com nenhuma moeda fiduciária, qualquer entidade que queira prover essa troca precisa manter alguma espécie de "livro de ordens". Esse sistema geralmente é complexo e envolve criação e execução de ordens, listagem, entre outros desafios. Note também que, além de manter um sistema complexo, esse sistema precisa ser centralizado, pois a conversão para moeda fiduciária envolve o uso de uma conta bancária e transferências no sistema PIX, ou em algum sistema bancário do país local.

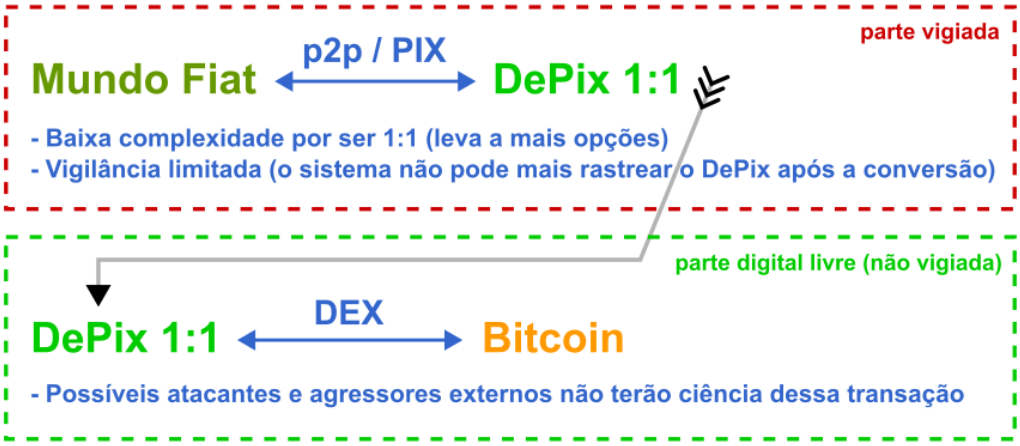
Com o surgimento de tecnologias como Atomic Swap [5] e exchanges descentralizadas e semi-descentralizadas tais como a SideSwap [6], por exemplo, que permitem a troca entre dois ou mais tokens digitais sem a necessidade de um intermediador central, não é mais necessário que exista uma troca direta para o Bitcoin logo na porta de entrada. A porta de entrada do mundo fiduciário para o mundo digital não precisa mais ser complexa: a criação de um token proporcional 1:1 ao mundo fiduciário torna os sistemas de entrada, aqueles que precisam ser centralizados, muito mais simples. Com mais simplicidade, mais interessados surgem para prover tal serviço e mais descentralizado se torna todo o processo. Ao invés do indivíduo ficar dependente de poucas exchanges capazes de realizar a troca, o indivíduo tem uma gama muito maior de opções para adentrar no mundo digital. Uma vez no mundo digital, o indivíduo então pode procurar soluções mais descentralizadas e confidenciais para fazer a operação digital que quiser (o chamado "cripto/cripto").

Em resumo: uma troca mais indireta entre a moeda fiduciária e o Bitcoin, passando por um intermediário como o DePix, pode tornar todo o processo mais simples, mais descentralizado, mais privado e mais seguro.

Antes do DePix:



Com DePix:



2 Especificação

DePix é um token lastreado no Real brasileiro (BRL) na proporção de 1:1, representando a moeda oficial do Brasil. Em circunstâncias normais, 1 DePix pode ser trocado por 1 Real e vice-versa. No entanto, o uso do termo "normalmente" reflete a limitações do token, que podem dificultar ou restringir essa conversão, especialmente em transações de grande volume. Apesar dessas limitações, o DePix oferece uma solução valiosa para aqueles que buscam maior soberania e privacidade, sendo especialmente útil em contextos como a compra e venda confidencial de Bitcoin.

Além de sua intercambialidade com o Real, o DePix é classificado como um **Transient Tactful Token (3T)**, o que implica em duas características principais:

2.1 Transient

O token não é destinado à poupança, ou seja, possui uma natureza transitória (tipicamente entre o Real e o Bitcoin) e não é recomendado para a retenção de riqueza a médio ou longo prazo. Primeiramente, porque o Real, que serve de lastro para o DePix, já é afetado por uma inflação significativa, tornando a sua acumulação desvantajosa. Além disso, devido à natureza centralizada e aos riscos associados à custódia, pode tornar-se inviável converter DePix em Reais no médio a longo prazo.

2.2 Tactful

No sentido de ser "discreto", o token DePix opera na rede Liquid, uma plataforma que suporta transações confidenciais. Isso implica que, ao utilizar o DePix para transações, os detalhes específicos como valores transferidos e identidades das partes envolvidas são ocultados. Essa característica é particularmente vantajosa para usuários que valorizam a privacidade, pois permite realizar transferências sem expor informações sensíveis. Além disso, a natureza discreta do token o torna uma escolha atraente para operações que requerem confidencialidade máxima, como negociações estratégicas ou movimentações financeiras sensíveis. A implementação de privacidade avançada ajuda a proteger contra vigilância financeira e análise de dados, garantindo uma camada extra de segurança para os usuários.

Planos futuros incluem a adição de mais protocolos de segunda ou terceira camada da rede Bitcoin, como ativos Taproot e tokens RGB. A principal característica de um Token 3T é sua emissão em redes de privacidade para garantir a privacidade dos usuários finais e a proteção dos "Banking Nodes" e "Token Issuers".

2.3 Especificação técnica

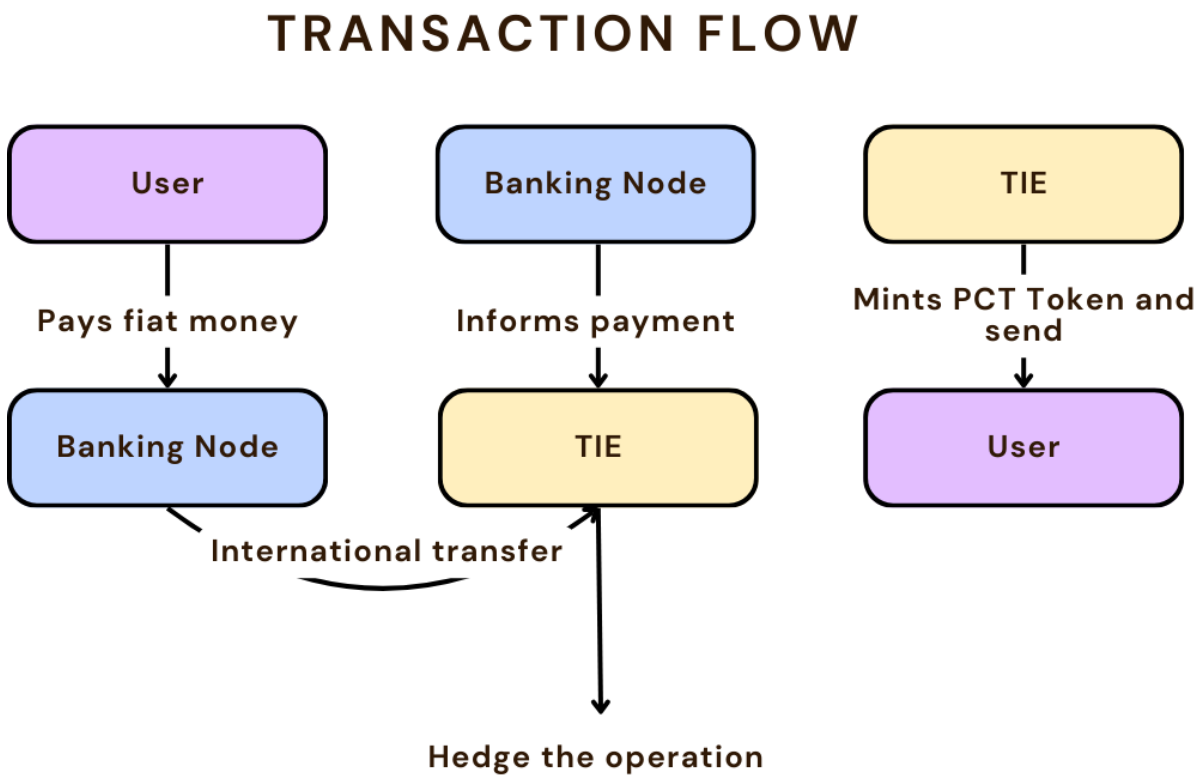
Atualmente o DePix funciona na rede Liquid. É um asset com precisão de 8 casas decimais. ***ATENÇÃO:*** *o token na rede Polygon foi descontinuado.*

Uma lista sempre atualizada das redes em que o token é operado e uma especificação mais precisa, como por exemplo o ID do asset, valor em circulação e outras informações relevantes sobre o token, podem ser encontrados no site oficial do DePix: `https://depix.info` ou no Github `https://github.com/eulen-repo/DePix` — Essas informações não serão colocadas neste whitepaper pela dificuldade de atualização e distribuição.

A rede Liquid foi escolhida como sendo a primeira e principal pelos seguintes motivos:

- É uma rede baseada no token Bitcoin, portanto de certa forma agrega valor ao próprio Bitcoin.
- Possui o conceito de "transações confidenciais" que melhora consideravelmente a privacidade do usuário.
- As taxas de transação on-chain são atualmente baixas (2024).
- A rede tem possibilidade de suportar segundas camadas (como Lightning Network) para uma escalabilidade futura.
- As transações on-chain são relativamente rápidas.

2.4 Fluxo de Transações



1. Usuário: O usuário inicia o processo pagando dinheiro fiduciário ao Banking Node.
2. Banking Node: Ao receber o pagamento, o Banking Node informa à TIE (Entidade Emissora de Tokens) que o pagamento foi recebido.
3. TIE: A TIE emite o Token 3T e o envia para o endereço da carteira do usuário.
4. Banking Node: O Banking Node então realiza uma transferência internacional para a conta bancária da TIE.
5. TIE: Por fim, a TIE protege a operação com o dinheiro recebido na conta bancária.

Esta visualização descreve o processo simplificado de emissão e gerenciamento de Tokens 3T, garantindo transparência e compreensão de cada etapa envolvida.

3 Riscos & mitigação dos riscos

3.1 Riscos legais

Durante o período de transição, o lastro do DePix em Reais são mantidos em uma conta bancária fiduciária. Embora existam alguns riscos, como bloqueios judiciais ou solicitações de informações, esses riscos são semelhantes aos enfrentados por exchanges tradicionais. Existem maneiras eficazes de minimizar esses desafios, conforme demonstrado mais adiante.

3.1.1 Cenários Adversos e Questões Jurisdicionais

O Token 3T é projetado para operar de forma eficaz em cenários adversos, incluindo países com instabilidade política e econômica, como Brasil, Argentina, México, Nigéria, China, entre outros. Para garantir a estabilidade e a usabilidade do token, mecanismos robustos e medidas estratégicas foram implementados. Além disso, os Banking Nodes são encorajados a serem incorporados em jurisdições que ofereçam direitos de propriedade sólidos e ambientes regulatórios favoráveis a criptomoedas, como Suíça, Bahamas e Seychelles, mitigando riscos legais e regulatórios.

3.2 Riscos operacionais

Além dos riscos legais, há alguns riscos operacionais tais como: erro operacional ou erro de sistema (transferência superior ou inferior ao valor transferido por PIX); pedido de estorno por parte do usuário final ou qualquer intermediário (MED [7]); dentre outros.

3.3 Mitigando os riscos

Para reduzir os riscos legais, é importante adotar boas práticas de compliance, como o processo de Know Your Costumer (KYC), que ajuda a entender a capacidade financeira dos usuários e garantir que o volume movimentado seja adequado, na entrada e saída do mundo digital ao fiduciário. Além disso, trabalhar com volumes menores pode contribuir para mitigar riscos, já que operações de alto risco geralmente envolvem grandes quantias que estão fora do propósito original do projeto, que é promover mais liberdade, privacidade e soberania ao indivíduo.

Para os usuários finais do DePix, que eventualmente podem enfrentar dificuldades para converter DePix em Reais, é recomendável realizar transações menores e evitar manter grandes quantidades de DePix em custódia por longos períodos. O DePix foi projetado para ser usado de forma transitória, facilitando trocas, mas não como uma ferramenta de poupança. Por isso, é aconselhável converter DePix em Bitcoin, outro token de sua preferência ou Reais o mais rapidamente possível e, para operações maiores, dividir a operação em etapas menores.

Reforçamos sempre a recomendação para que não se poupe DePix por longos períodos ou grande quantidade. *Lembre-se: o DePix tem uma utilidade transitória e apenas o Bitcoin é um token digital confiável e seguro, apesar dos riscos de flutuação de preço. Caso não queira estar exposto à volatilidade do Bitcoin, recomendamos que troque seu DePix por Reais o mais rápido possível.*

3.3.1 Banking Nodes

Os *Banking Nodes* são entidades que lidam com os processos de entrada e saída de dinheiro para o Token 3T dentro do sistema financeiro fiduciário nacional local. Esses nós são cruciais para garantir transações sem interrupções e manter a confiança na rede. Quanto mais nós bancários o sistema possuir, mais descentralizado e menor é o risco de custódia.

A API do *Banking Node* pode estar conectada com a API do *Emissor de Token* (TIE) para o processamento automático e a cunhagem/queima do token.

1. Responsabilidades de um Banking Node
    - Processar pagamentos para o Token 3T.
    - Manter colaterais em Reais, Bitcoin, USD ou Ouro para garantir obrigações.
    - Cumprir os requisitos regulatórios locais (IRS, Banco Central, licenças de criptomoedas, etc.).

- Identificar e remover agentes mal-intencionados para preservar a integridade da rede.
- Garantir operações robustas para mitigar os riscos associados a cenários adversos.

3.3.2 Diversificação de lastro

O Token 3T emprega um mecanismo de paridade em várias camadas para garantir estabilidade e paridade com a moeda local. Para cada token emitido há um saldo correspondente em uma conta bancária. Isso assegura a paridade direta com a moeda local.

Para proteger contra decisões judiciais arbitrárias por governos totalitários, o emissor do token pode empregar estratégias de *hedge internacional* em jurisdições forex seguras. Isso proporciona uma camada adicional de segurança e garante a paridade.

Para aumentar ainda mais a segurança e prevenir que o emissor aja como um agente mal-intencionado, a paridade evoluirá no futuro para um contrato digital automatizado (*smart contract*) usando tecnologia avançada como o protocolo Niti [10]. O Bitcoin servirá como colateral, garantindo um mecanismo de paridade robusto e descentralizado.

4 Casos de Uso Práticos

- **Troca por Outros Tokens**: O Token 3T pode ser utilizado em transações com diversos outros tokens como, por exemplo o Bitcoin, oferecendo aos usuários diferentes opções de investimento.
- **Gestão Fiscal**: Com recursos de privacidade, os usuários podem gerenciar ganhos de capital de forma mais eficiente, facilitando o cumprimento de obrigações fiscais.
- **Pagamentos Online**: O Token 3T pode ser utilizado para pagamentos em sites e serviços, com ênfase na segurança e privacidade das transações.
- **Integração para Desenvolvedores**: Desenvolvedores podem incorporar o Token 3T em carteiras digitais, ampliando as possibilidades de pagamento em seus aplicativos.
- **Recebimento de Reais sem a necessidade de uma conta bancária no Brasil**: Um *Banking Node* pode oferecer uma API de geração de QR Code para depósitos via PIX que serão convertidos para DePix e enviados ao comércio ou serviço final para que esse depois possa ter a liberdade para converter para qualquer outro token ou moeda local. Isso facilita o recebimento de Reais por sites estrangeiros no Brasil, por exemplo.
- **Transações P2P**: Usuários podem realizar transações peer-to-peer sem a necessidade de instituições financeiras tradicionais, fortalecendo a privacidade e a inclusão financeira.

Esses exemplos mostram como o Token 3T pode ser aplicado em diferentes contextos, aprimorando a privacidade, segurança e acessibilidade no ambiente digital.

5 Conclusão

O DePix se apresenta como uma solução inovadora para indivíduos que buscam maior privacidade e soberania financeira ao navegar entre o sistema fiduciário tradicional e o mundo digital das criptomoedas. Embora o token tenha limitações, especialmente em grandes volumes e retenções de longo prazo, ele oferece uma ferramenta prática para operações discretas e confidenciais, principalmente na conversão de moedas fiduciárias em ativos digitais como o Bitcoin.

No entanto, é fundamental que os usuários estejam cientes dos riscos e adotem as melhores práticas para mitigar possíveis problemas legais e operacionais. O DePix não é uma solução única para todas as questões de privacidade, mas é um passo importante na direção certa, especialmente em um mundo onde a vigilância financeira está cada vez mais presente. A implementação contínua de melhorias e a diversificação do lastro fortalecerão ainda mais o ecossistema, proporcionando uma ferramenta robusta para aqueles que buscam maior autonomia financeira no futuro.

Por fim, a evolução do DePix como um Token 3T e a exploração de novas tecnologias, como Taproot e tokens RGB, indicam um compromisso contínuo com a inovação e a proteção da privacidade dos usuários. Este whitepaper serve como um guia para a compreensão dos fundamentos do DePix, suas funcionalidades e seus riscos, ajudando a preparar os usuários para uma transição mais suave para o mundo digital.

6 Glossário

- **Atomic Swap**: Tecnologia que permite a troca direta de criptomoedas entre duas partes, sem a necessidade de um intermediário centralizado.
- **BRL (Reais)**: Sigla que representa o Real brasileiro, a moeda oficial do Brasil.
- **Bitcoin**: Primeira criptomoeda descentralizada, criada em 2008 por uma pessoa ou grupo sob o pseudônimo Satoshi Nakamoto. Funciona sem um banco central ou administrador único.
- **Compliance**: Conformidade com leis, regulamentos, normas e práticas éticas exigidas em um determinado setor.
- **Contratos Inteligentes (Smart Contracts)**: Programas autoexecutáveis em uma blockchain que automatizam a execução de contratos quando certas condições são atendidas.
- **Cripto/cripto**: Termo que se refere a transações realizadas entre diferentes criptomoedas, sem a necessidade de conversão para uma moeda fiduciária.
- **Custódia**: Guarda de ativos, como dinheiro ou criptomoedas, por uma entidade que detém a responsabilidade de proteger e gerenciar esses ativos.
- **DePix**: Token digital que representa o Real brasileiro (BRL) na proporção de 1:1, com o objetivo de melhorar a privacidade em transações financeiras.
- **DEX**: Uma Exchange Descentralizada (DEX) é um mercado peer-to-peer onde transações de criptomoedas ocorrem diretamente entre os usuários, sem a necessidade de um intermediário.
- **Exchange**: Plataforma ou mercado onde criptomoedas e tokens digitais são comprados, vendidos ou trocados por outros ativos, como moedas fiduciárias ou outras criptomoedas.
- **Fiat / fiduciário (Moeda Fiat)**: Moeda emitida por um governo, como o Real brasileiro (BRL), o dólar americano (USD), etc., que não tem valor intrínseco, mas é aceita como meio de pagamento devido à confiança na entidade que a emite.
- **KYC (Know Your Customer)**: Processo de verificação da identidade dos clientes, exigido por instituições financeiras para prevenir fraudes, lavagem de dinheiro e outras atividades ilegais.
- **Lightning Network**: Uma solução de segunda camada na blockchain do Bitcoin que facilita transações mais rápidas e baratas, particularmente para micropagamentos.
- **Liquid**: Rede de blockchain que suporta transações confidenciais e é baseada no Bitcoin, oferecendo maior privacidade e velocidade nas transações.
- **PCT Token**: É o mesmo que **Token 3T**. PCT é um acrônimo para Privacy-Centric Token.
- **PIX**: Sistema de pagamento instantâneo e integrado criado pelo Banco Central do Brasil, que permite transferências de dinheiro rápidas e gratuitas entre contas bancárias.
- **RGB Tokens**: Um protocolo de segunda camada na blockchain do Bitcoin que permite a emissão de tokens com maior privacidade e flexibilidade.
- **SideSwap**: Exchange semi-descentralizada que permite a troca de criptomoedas diretamente entre usuários sem a necessidade de uma entidade centralizada.
- **Taproot**: Um upgrade na blockchain do Bitcoin que melhora a privacidade e a eficiência das transações, permitindo que múltiplas transações complexas sejam agrupadas em uma única.
- **TIE (Token Issuer Entity)**: A Entidade Emissora de Tokens é a entidade responsável pela cunhagem e gerenciamento do Token 3T. A TIE opera em uma jurisdição segura para se proteger contra decisões judiciais arbitrárias e ataques totalitários. Para a DePix, a empresa Eulen.app atua como a Emissora de Tokens.
- **Token**: Um "token" é uma unidade digital de valor emitida em uma blockchain que pode representar ativos, direitos ou utilidades.
- **Token 3T (Transient Tactful Token)**: Termo inédito e citado neste paper pela 1a vez. Tipo de token digital que é transitório e discreto, não destinado à poupança, mas útil para transações que requerem privacidade.

- **Transações confidenciais**: Confidential Transactions escondem o valor sendo transferido, garantindo que apenas as partes envolvidas saibam o valor da transação. Isso é alcançado usando Pedersen Commitments [8], que permitem que o valor seja ocultado enquanto ainda possibilitam que a rede verifique que a soma das entradas e saídas em uma transação é igual, prevenindo assim o gasto duplo. CT também emprega fatores de ofuscação, que são números gerados aleatoriamente usados para obscurecer os valores das transações. Esses fatores garantem que o valor da transação seja visível apenas para o remetente e o destinatário, mantendo a privacidade em relação a observadores externos.
- **Transient**: Característica de algo que é temporário ou transitório, não destinado a ser mantido por longo prazo.
- **Tactful**: No contexto do token DePix, refere-se à característica de ser discreto e confidencial, oferecendo maior privacidade nas transações.

7 Referências

- [1] J. Yoonjae Chung, [[http://ijournals.in/wp-content/uploads/2020/09/IJSRC-8901-Justin-Yoonja
pdf][Cracking the Code: How the US Government

Tracks Bitcoin Transactions]] (archive), 2020.

- [2] RIVER LEARN, Understanding Fiat Currencies (archive).
- [3] W. Suberg, Bitcoin Exchange Bitfinex Exits Washington State In 24 Hours, Licence Problems Cited (archive), 2017.
- [4] WIKIPEDIA, PIX (archive), 2024.
- [5] THE INVESTOPEDIA TEAM, Atomic Swap: Definition, How It Works With Cryptocurrency Trade (archive), 2024.
- [6] SideSwap official website (https://sideswap.io/)
- [7] BANCO CENTRAL DO BRASIL, O que é e como funciona o Mecanismo Especial de Devolução (MED) (archive), 2023.
- [8] RARESKILLS What are Pedersen Commitments and How They Work (archive), 2024.
- [9] The Kyiv Independent News Moroccan man kidnapped, forced to transfer Bitcoin, then murdered in Kyiv, police say (archive), 2024.
- [10] I. Caleb, NITI : Non-custodial Interlinked Tokenization Infrastructure (archive), 2024.