DePix

A discreet way to enter the digital world.

Contents

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

v 2.3, August 21, 2024, Last update: August 23, 2024.

Abstract

DePix is a token pegged to the Brazilian Real (BRL) at a 1:1 ratio, operating on the Liquid network. Although this parity is standard, operational limitations may affect conversion in large volumes, challenges that can be mitigated by "Banking Nodes" and diversification of collateral. The risks are quite limited, and DePix offers significant advantages in terms of sovereignty and privacy, especially in confidential Bitcoin operations. In addition to its link to the Real, **DePix** stands out as an innovative **Transient Tactful Token (3T)**: 1) **Transient** – its use is temporary, serving as an intermediary between the Real (fiat world) and Bitcoin (digital world), without the intention of being held long-term due to the risk of collateral inflation and custody risk. 2) **Tactful** – discreet, leveraging the confidential transaction infrastructure of the Liquid network or other networks with similar characteristics, enhancing privacy in transactions, particularly in conversions to assets like Bitcoin.

1 Motivation

Bitcoin has attracted the attention of attackers and external agents since its inception [1][9], who strive to make life difficult for the average user. This attention intensifies with the increase in its value and transaction volume. Typically, these attackers exploit weaknesses in the "legacy fiat system" [2], where, being a centralized and outdated system, security and privacy are limited.

The main vulnerable point of Bitcoin has been its connection to the traditional fiat system [3]. However, this vulnerability stems more from the limitations of the legacy system itself than from any intrinsic flaw in Bitcoin. In Brazil, this fiat system was consolidated with the introduction of the "PIX" payment system in late 2020 [4], which facilitates bank transfers quickly, cheaply, and in a standardized manner. Although PIX offers significant benefits, it also poses challenges to privacy and individual sovereignty, centralizing and making financial surveillance instantaneous. For those seeking greater financial autonomy, the challenge arises in transferring value between the digital world (Bitcoin) and the fiat system, a conversion still necessary since Bitcoin is not widely accepted in everyday transactions.

To address this challenge, the **DePix** token was created with the aim of enhancing privacy and security for those who wish to accumulate Bitcoin without being subjected to constant surveillance and external threats. It is important to note that DePix aims to *improve* privacy, not to solve all problems miraculously. The token is designed to provide greater sovereignty and privacy to individual users, due to its intrinsic characteristics detailed later in this document. Despite its great utility, it is still not suitable for large-scale operations.

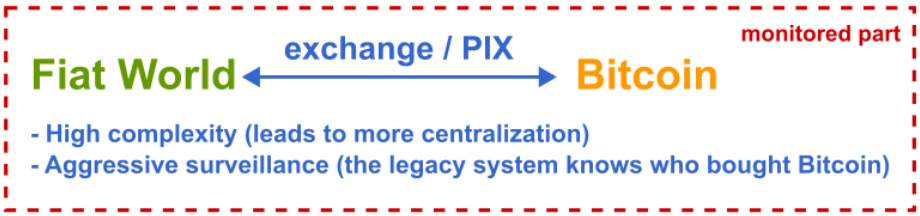
1.1 Entry and exit from the digital world

Since Bitcoin does not have a 1:1 relationship with any fiat currency, any entity that wants to provide this exchange must maintain some sort of "order book." This system is generally complex and involves creating and executing orders, listings, among other challenges. It should also be noted that, in addition to maintaining a complex system, this system needs to be centralized since conversion to fiat currency involves using a bank account and transfers within the PIX system or some local banking system.

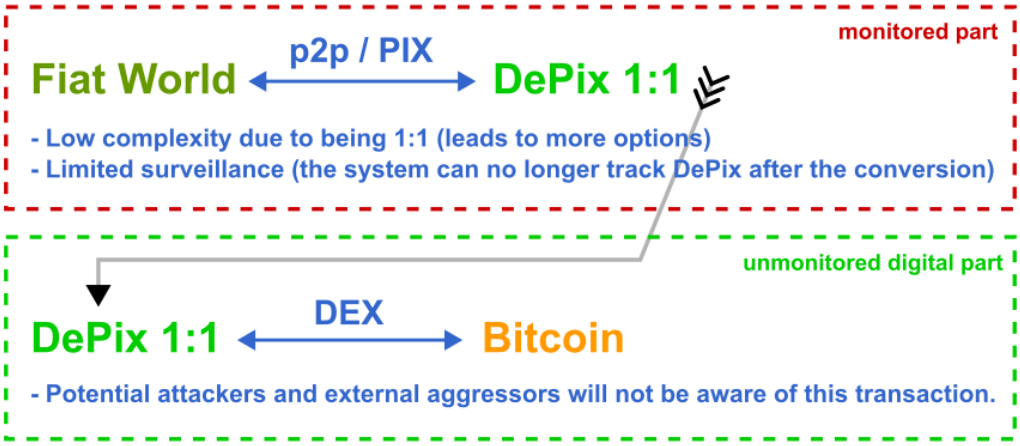
With the advent of technologies like Atomic Swap [5] and decentralized and semi-decentralized exchanges such as SideSwap [6], which allow the exchange between two or more digital tokens without the need for a central intermediary, direct exchange for Bitcoin at the entry point is no longer necessary. The entry point from the fiat world to the digital world no longer needs to be complex: the creation of a token pegged 1:1 to the fiat world makes entry systems, which need to be centralized, much simpler. With more simplicity, more interested parties emerge to provide such a service, and the entire process becomes more decentralized. Instead of individuals relying on a few exchanges capable of performing the exchange, they have a much wider range of options to enter the digital world. Once in the digital world, individuals can then seek more decentralized and confidential solutions to perform the digital operation they want (so-called "crypto/crypto").

In summary: a more indirect exchange between fiat currency and Bitcoin, through an intermediary like DePix, can make the entire process simpler, more decentralized, more private, and more secure.

Before DePix:



With DePix:



2 Specification

DePix is a token pegged to the Brazilian Real (BRL) at a 1:1 ratio, representing Brazil's official currency. Under normal circumstances, 1 DePix can be exchanged for 1 Real and vice versa. However, the use of the term "normally" reflects the token's limitations, which may hinder or restrict this conversion, especially in large-volume transactions. Despite these limitations, DePix offers a valuable solution for those seeking greater sovereignty and privacy, being particularly useful in contexts such as confidential Bitcoin buying and selling.

In addition to its interchangeability with the Real, DePix is classified as a **Transient Tactful Token (3T)**, which implies two main characteristics:

2.1 Transient

The token is not intended for savings, meaning it has a transient nature (typically between the Real and Bitcoin) and is not recommended for medium- to long-term wealth retention. Firstly, because the Real, which backs DePix, is already subject to significant inflation, making its accumulation disadvantageous. Furthermore, due to the centralized nature and associated custody risks, it may become unfeasible to convert DePix into Reais in the medium to long term.

2.2 Tactful

In the sense of being "discreet," the DePix token operates on the Liquid network, a platform that supports confidential transactions. This means that when using DePix for transactions, specific details such as transferred amounts and the identities of the parties involved are concealed. This feature is particularly advantageous for users who value privacy, as it allows transfers without exposing sensitive information. Additionally, the token's discreet nature makes it an attractive choice for operations that require maximum confidentiality, such as strategic negotiations or sensitive financial movements. The implementation of advanced privacy helps protect against financial surveillance and data analysis, ensuring an extra layer of security for users.

Future plans include adding more second- or third-layer protocols to the Bitcoin network, such as Taproot assets and RGB tokens. The main feature of a 3T Token is its issuance on privacy networks to ensure end-user privacy and protect "Banking Nodes" and "Token Issuers."

2.3 Technical specification

Currently, DePix operates on the Liquid network. It is an asset with a precision of 8 decimal places. ***ATTENTION:*** *the token on the Polygon network has been discontinued.*

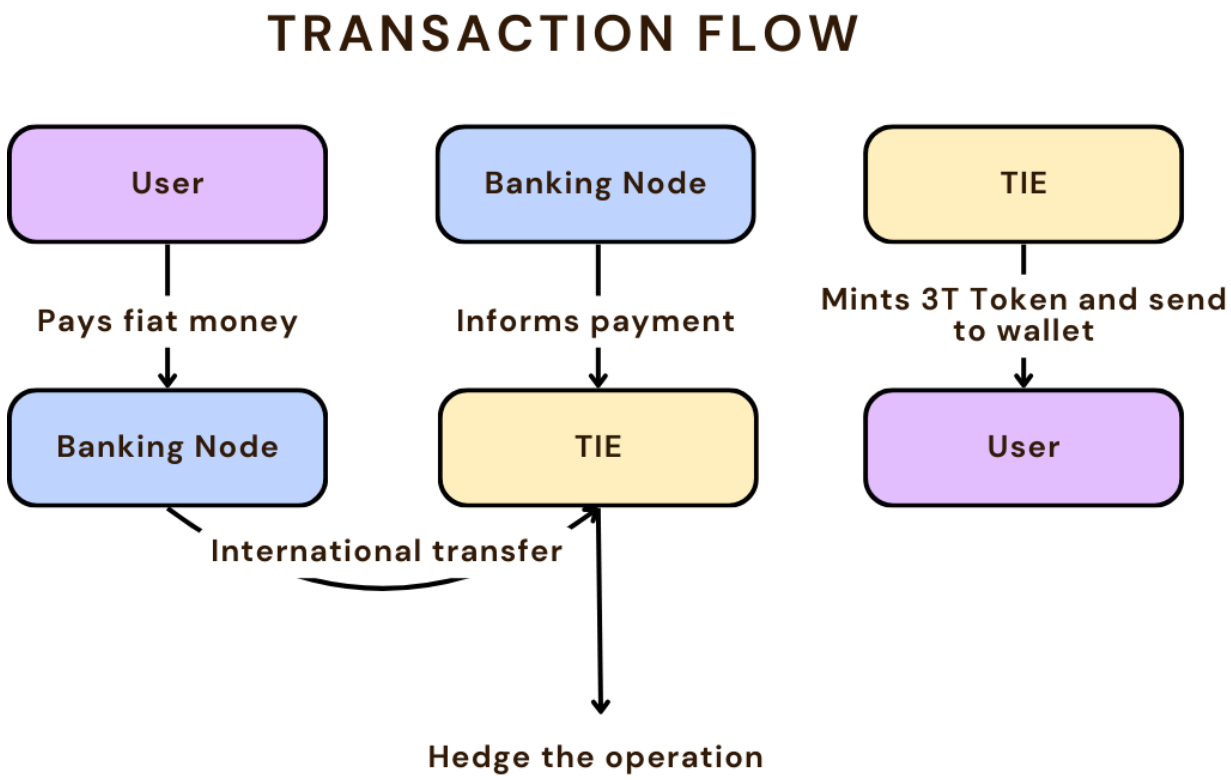
An always-updated list of the networks on which the token operates and a more precise specification, such as asset ID, circulating value, and other relevant information about the token, can be found on the official DePix website: `https://depix.info` or on Github `https://github.com`

/eulen-repo/DePix — This information will not be included in this whitepaper due to the difficulty of updating and distributing it.

The Liquid network was chosen as the first and main network for the following reasons:

- It is a network based on the Bitcoin token, thus adding value to Bitcoin itself.
- It has the concept of "confidential transactions," which significantly improves user privacy.
- On-chain transaction fees are currently low (2024).
- The network has the potential to support second layers (such as Lightning Network) for future scalability.
- On-chain transactions are relatively fast.

2.4 Transaction Flow



1. User: The user initiates the process by paying fiat money to the Banking Node.
2. Banking Node: Upon receiving the payment, the Banking Node informs the TIE (Token Issuer Entity) that the payment has been received.
3. TIE: The TIE issues the 3T Token and sends it to the user's wallet address.
4. Banking Node: The Banking Node then makes an international transfer to the TIE's bank account.
5. TIE: Finally, the TIE secures the operation with the money received in the bank account.

This visualization describes the simplified process of 3T Token issuance and management, ensuring transparency and understanding of each step involved.

3 Risks & risk mitigation

3.1 Legal risks

During the transition period, DePix's collateral in Reais is held in a fiat bank account. While there are some risks, such as judicial blockades or information requests, these risks are similar to those faced by traditional exchanges. Effective ways to minimize these challenges are demonstrated later.

3.1.1 Adverse Scenarios and Jurisdictional Issues

The 3T Token is designed to operate effectively in adverse scenarios, including countries with political and economic instability, such as Brazil, Argentina, Mexico, Nigeria, China, among others. To ensure the token's stability and usability, robust mechanisms and strategic measures have been implemented. Additionally, Tokens Issuers Entities are encouraged to be incorporated in jurisdictions that offer strong property rights and favorable regulatory environments for cryptocurrencies, such as Switzerland, the Bahamas, and Seychelles, mitigating legal and regulatory risks.

3.2 Operational risks

In addition to legal risks, there are some operational risks such as: operational errors or system errors (transfer exceeding or below the value transferred via PIX); refund requests by the end user or any intermediary (MED [7]); among others.

3.3 Mitigating the risks

To reduce legal risks, it is important to adopt good compliance practices, such as the Know Your Customer (KYC) process, which helps to understand the financial capacity of users and ensure that the volume traded is appropriate when entering and exiting the digital world to fiat. Additionally, working with smaller volumes can help mitigate risks, as high-risk operations generally involve large amounts that are outside the original purpose of the project, which is to promote more freedom, privacy, and sovereignty to individuals.

For end users of DePix, who may eventually face difficulties converting DePix to Reais, it is advisable to make smaller transactions and avoid holding large amounts of DePix in custody for long periods. DePix was designed to be used transiently, facilitating exchanges but not as a savings tool. Therefore, it is advisable to convert DePix into Bitcoin, another token of your choice, or Reais as quickly as possible, and for larger operations, divide the operation into smaller steps.

We always reinforce the recommendation not to save DePix for long periods or large quantities. *Remember: DePix has a transient utility, and only Bitcoin is a reliable and secure digital token, despite price fluctuation risks. If you do not want to be exposed to Bitcoin's volatility, we recommend converting your DePix to Reais as quickly as possible.*

3.3.1 Banking Nodes

Banking Nodes are entities that handle the inflow and outflow of money for the 3T Token within the local national fiat financial system. These nodes are crucial for ensuring smooth transactions and maintaining network trust. The more banking nodes the system has, the more decentralized and less custodial risk there is.

The *Banking Node* API can be connected to the *Token Issuer* (TIE) API for automatic processing and minting/burning of the token.

1. Responsibilities of a Banking Node
    - Process payments for the 3T Token.
    - Maintain collateral in Reais, Bitcoin, USD, or Gold to guarantee obligations.
    - Comply with local regulatory requirements (IRS, Central Bank, cryptocurrency licenses, etc.).
    - Identify and remove malicious agents to preserve network integrity.
    - Ensure robust operations to mitigate risks associated with adverse scenarios.

3.3.2 Collateral diversification

The 3T Token employs a multi-layered parity mechanism to ensure stability and parity with the local currency. For each token issued, there is a corresponding balance in a bank account. This ensures direct parity with the local currency.

To protect against legal uncertainty in unstable jurisdictions, the token issuer can employ international hedge strategies in secure forex jurisdictions. This provides an additional layer of security and ensures parity.

To further enhance security and prevent the issuer from acting as a malicious agent, parity will evolve in the future to an automated digital contract (*smart contract*) using advanced technology such as the Niti protocol [10]. Bitcoin will serve as collateral, ensuring a robust and decentralized parity mechanism.

4 Practical Use Cases

- **Token Exchange**: The 3T Token can be used in transactions with various other tokens such as Bitcoin, offering users different investment options.
- **Tax Management**: With privacy features, users can manage capital gains more efficiently, facilitating tax compliance.
- **Online Payments**: The 3T Token can be used for payments on websites and services, with an emphasis on transaction security and privacy.
- **Developer Integration**: Developers can incorporate the 3T Token into digital wallets, expanding payment possibilities in their applications.
- **Receiving Reais without a bank account in Brazil**: A *Banking Node* can offer an API for generating QR Codes for deposits via PIX that will be converted to DePix and sent to the final business or service, giving them the freedom to convert it to any other token or local currency. This facilitates receiving Reais by foreign websites in Brazil, for example.
- **P2P Transactions**: Users can conduct peer-to-peer transactions without the need for traditional financial institutions, strengthening privacy and financial inclusion.

These examples show how the 3T Token can be applied in different contexts, enhancing privacy, security, and accessibility in the digital environment.

5 Conclusion

DePix presents itself as an innovative solution for individuals seeking greater privacy and financial sovereignty when navigating between the traditional fiat system and the digital world of cryptocurrencies. Although the token has limitations, especially in large volumes and long-term holdings, it offers a practical tool for discreet and confidential operations, particularly in converting fiat currencies into digital assets such as Bitcoin.

However, it is essential that users are aware of the risks and adopt best practices to mitigate potential legal and operational issues. DePix is not a one-size-fits-all solution for privacy issues, but it is an important step in the right direction, especially in a world where financial surveillance is increasingly present. The ongoing implementation of improvements and collateral diversification will further strengthen the ecosystem, providing a robust tool for those seeking greater financial autonomy in the future.

Finally, the evolution of DePix as a 3T Token and the exploration of new technologies such as Taproot and RGB tokens indicate a continued commitment to innovation and user privacy protection. This whitepaper serves as a guide to understanding the fundamentals of DePix, its functionalities, and its risks, helping to prepare users for a smoother transition to the digital world.

6 Glossary

- **Atomic Swap**: Technology that allows the direct exchange of cryptocurrencies between two parties without the need for a centralized intermediary.
- **Banking Node**: Entities that handle the inflow and outflow of money for the 3T Token within the local national fiat financial system, ensuring smooth transactions and maintaining trust in the network.
- **Bitcoin**: The first decentralized cryptocurrency, created in 2008 by an individual or group under the pseudonym Satoshi Nakamoto. It operates without a central bank or single administrator.
- **BRL (Reais)**: The acronym for the Brazilian Real, the official currency of Brazil.
- **Compliance**: Adherence to laws, regulations, standards, and ethical practices required in a specific sector.
- **Confidential Transactions**: A technology that hides the amount being transferred, ensuring that only the parties involved know the transaction amount while allowing the network to verify that the sum of inputs and outputs in a transaction is equal, preventing double spending.
- **Cripto/cripto**: Refers to transactions conducted between different cryptocurrencies without the need for conversion to a fiat currency.
- **Custody**: The safekeeping of assets, such as money or cryptocurrencies, by an entity responsible for protecting and managing these assets.
- **DePix**: A digital token that represents the Brazilian Real (BRL) at a 1:1 ratio, aimed at improving privacy in financial transactions.
- **DEX**: A Decentralized Exchange (DEX) is a peer-to-peer marketplace where cryptocurrency transactions occur directly between users without the need for an intermediary.
- **Exchange**: A platform or marketplace where cryptocurrencies and digital tokens are bought, sold, or exchanged for other assets, such as fiat currencies or other cryptocurrencies.
- **Fiat / fiat currency**: Currency issued by a government, such as the Brazilian Real (BRL), the US Dollar (USD), etc., which has no intrinsic value but is accepted as a means of payment due to trust in the issuing entity.
- **KYC (Know Your Customer)**: A process of verifying the identity of customers, required by financial institutions to prevent fraud, money laundering, and other illegal activities.
- **Lightning Network**: A second-layer solution on the Bitcoin blockchain that facilitates faster and cheaper transactions, particularly for micropayments.
- **Liquid**: A blockchain network that supports confidential transactions and is based on Bitcoin, offering increased privacy and transaction speed.
- **PCT Token**: Same as **Token 3T**. PCT stands for Privacy-Centric Token.
- **PIX**: An instant and integrated payment system created by the Central Bank of Brazil, allowing fast and free money transfers between bank accounts.
- **RGB Tokens**: A second-layer protocol on the Bitcoin blockchain that allows the issuance of tokens with greater privacy and flexibility.
- **SideSwap**: A semi-decentralized exchange that allows cryptocurrency exchanges directly between users without the need for a centralized entity.
- **Smart Contracts**: Self-executing programs on a blockchain that automate the execution of contracts when certain conditions are met.
- **Tactful**: In the context of the DePix token, it refers to the characteristic of being discreet and confidential, offering greater privacy in transactions.
- **Taproot**: An upgrade on the Bitcoin blockchain that improves transaction privacy and efficiency by allowing multiple complex transactions to be grouped into a single one.
- **TIE (Token Issuer Entity)**: The entity responsible for minting and managing the 3T Token. The TIE operates in a secure jurisdiction to protect against arbitrary judicial decisions and totalitarian attacks. For DePix, the company Eulen.app acts as the Token Issuer.

- **Token**: A "token" is a digital unit of value issued on a blockchain that can represent assets, rights, or utilities.
- **Token 3T (Transient Tactful Token)**: A novel term first mentioned in this paper. A type of digital token that is transient and discreet, not intended for savings, but useful for transactions requiring privacy.
- **Transient**: Characteristic of something that is temporary or short-lived, not intended to be held long-term.

7 References

- [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.