Wrapped Dogecoin

A multi-institutional framework for tokenizing Dogecoin

Whitepaper v0.1
Jan 6th 2023

Bluepepper
BitGo Inc

Abstract

With the rise in popularity of ERC20, digital tokens in the Ethereum ecosystem have emerged as an important asset class. These tokens have all the advantages that blockchains and Ethereum have to offer in terms of transparency in total number of coins, owners, minting, fast confirmation times, transaction details and smart contract execution. Tokens on the Ethereum blockchain can serve several different functions; this paper will specifically focus on asset backed or wrapped tokens. The prices of these tokens reflect the price of the asset backing them and hence they can also be called "stable coins". Asset backed tokens are usually done in two different ways:

- **Algorithmic** - This is a mechanism followed by some tokens on Ethereum where demand and supply are controlled by smart contracts in order to keep the price of the token in line with a fiat currency. Some examples of this are Dai, Basis, Carbon, and NuBits

- **Centralized** - Assets are stored with an organization which publishes proof of reserves. This is the case with Tether, True USD, USDC (USD), Digix (gold), Globcoin (a mix of fiat currencies), and AAA reserve (governmental bonds)

Wrapped Dogecoin follows the centralized model, but instead of relying entirely on one institution, they rely on a consortium of institutions performing different roles in the network. This whitepaper proposes a framework for issuing asset backed tokens by addressing challenges with scalability, trust, regulation, and governance. The wrapped token will be an ERC20 token backed by Dogecoin (DOGE) and will be appropriately named, "Wrapped Dogecoin" (wDoge). Unlike centralized solutions (USD), wDoge will be fully accounted for and proof of reserves posted on the Dogecoin chain.

There is no additional secondary utility/payment token required to use wDoge, and no transfer fees other than blockchain fees. wDoge uses a simple federated governance model and strives to promote usability.

Use Cases

Tokenization

The act of tokenizing assets can:

- Increase speed of transactions
  Ethereum blocks are created every ~15 seconds and it is possible to have a fair deal of confidence in the irrevocability of a transaction in less than 5 minutes. This speed is faster than transacting natively compared to many other assets including Dogecoin, gold, and fiat currencies
- Reduce the number of intermediaries
  One of the key benefits of assets on a blockchain is their ability to be transacted without intermediaries. This can be done through atomic swaps, decentralized exchange protocols, and lightning/raiden style channels.
- Enhance security
  Tokenization enables users to have full control of private keys of the asset. Users who do not want to hold keys can reduce counterparty risk by moving it from exchanges to a security-focused custodian.
- Usability
  The ERC20 standard has been adopted by a large number of institutions and products. This provides users with a variety of exchanges, wallets, and Dapps to use while handling their tokenized asset. They also have the ability to move tokens quickly, 24/7.
- Improve Transparency
  The total number of tokens, token creation transactions, token removal transactions, number of token holders, and rules for transfers can be seen on a public block explorer by anyone. This level of transparency is not usually available for assets like fiat currencies, commodities, and stock.

Liquidity on decentralized exchanges and dapps

Most decentralized exchanges do not offer Dogecoin/Token trades. A Wrapped Dogecoin can bridge this gap and provide more liquidity on decentralized exchanges. In addition, other decentralized applications/protocols (like funds, lending payments) will also benefit from having access to greater liquidity that a Dogecoin token can bring. wDoge brings the ease of creation of smart contracts to Dogecoin.

Interoperability between cryptocurrencies

As we see an expansion in the number of cryptocurrencies today, each one focuses on some aspect of monetary exchange. Some such aspects are transactional throughput, privacy, cheap transaction fees, smart contract ability, and decentralization of nodes/miners. The wrapped framework would make it easy to represent any other cryptocurrency, such as Dogecoin, on Ethereum and thereby enhance it with all the capabilities of the Ethereum blockchain. One such use case is the ability for initial coin offerings (ICOs) to be directly funded and mint tokens on deposits of Wrapped Dogecoin tokens. In the future, centralized exchanges and other institutions which accept cryptocurrencies would not need to maintain multiple cryptocurrency nodes and instead could just develop on Ethereum.

On chain ways to enforce policies

Tokenization also provides a way to enforce policies on chain. On chain policy enforcement makes rules more transparent and doesn't rely on one single party to enforce them. Based on the type of asset, there could be a need to enforce rules on asset transfer or trade

Common Issues

Trust

Asset backed tokens usually involve trust in the institution(s) holding the asset. This goes against the ethos of cryptocurrencies which seeks to minimize need for trust in operations. Some key questions to answer here are:

- Is the asset holder authorized in the existing legal framework to hold the asset?
- Can the custodian create an arbitrary amount of tokens?
- How does the custodian prove possession of the asset under custody?

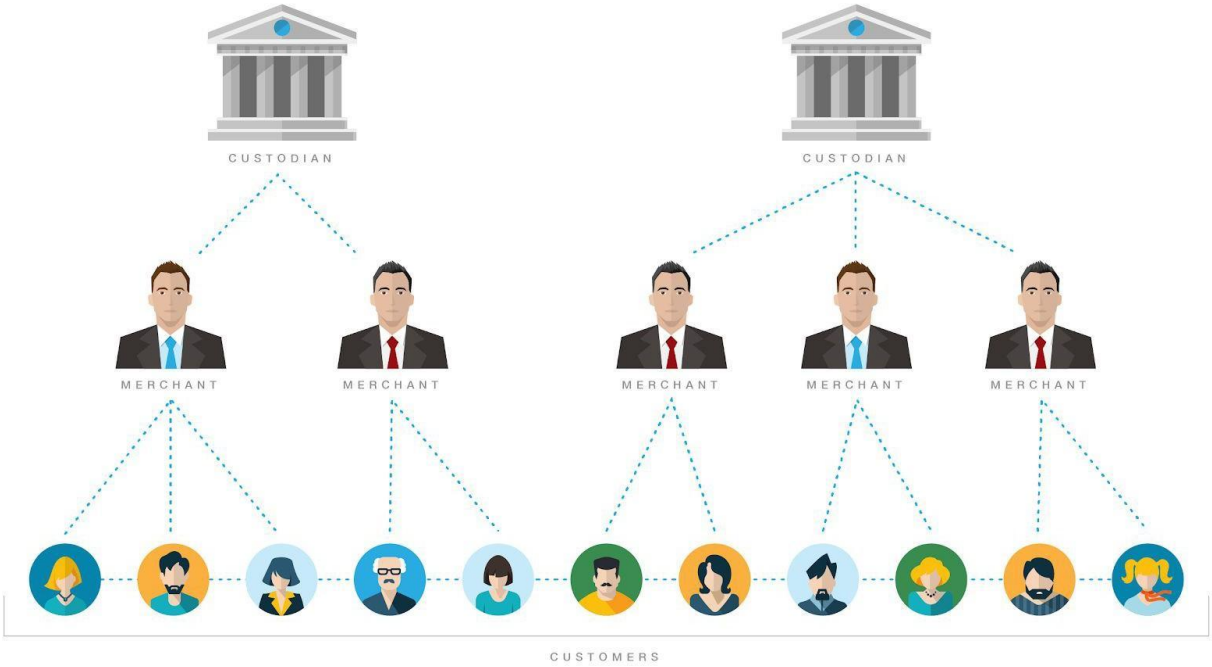
Regulation

Custodians of asset backed tokens need to be licensed to hold the asset. This license may vary based on the asset and geographical jurisdiction of the custodian. Custodians must also prove reserves regularly given that a lack of 1:1 backing would undermine the whole system. KYC and AML restrictions also apply to users engaging in asset backed tokens. These restrictions need to be enforced at the time of purchase, redemption, or transfer of tokens.

Governance

When there are multiple stakeholders in the system, there is a governance challenge with how to handle changes made to the token. Most asset backed tokens are entirely reliant on the asset custodian to make changes to the rules/smart contract governing the token. Usually in the case of ICOs, the issuer of the token has full control of protocol changes. There have been some cases like decentralized autonomous initial coin offerings (DAICOs) where users have voting rights, but they face the challenge of a low voter turnout [1].

Implementation and Technology



Key Roles

- Custodian - The institution or party who holds the asset. In the case of wDoge, this will be played by BitGo [2]. Custodians hold the keys to mint tokens.
- Merchant - The institution or party to which wrapped tokens will be minted to and burnt from. Merchants play a key role in distribution of the wrapped token. In the case of wDoge, this will be played initially by Bluepepper [3]. Each merchant holds a key to initiate minting of new wrapped tokens and burning of wrapped tokens.
- User - The holders of the wrapped token. Users can use wrapped tokens to transfer and transact like any other ERC20 token in the Ethereum ecosystem.
- wDoge DAO member - Contract changes and addition/removal of custodians and merchants will be controlled by a multi-signature contract. Holders of the keys to the multi-sig contract will be held by institutions as part of the wDoge DAO.

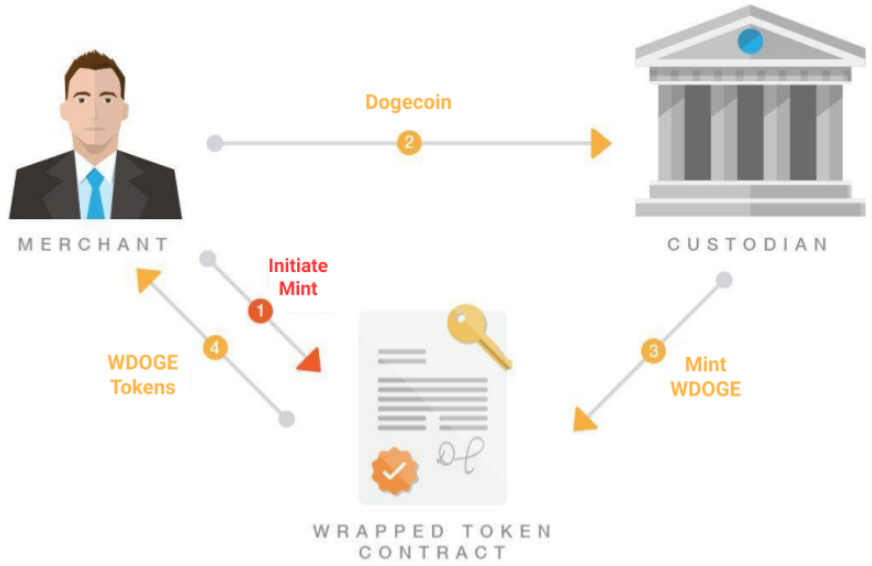
Custodians exchange assets for Wrapped Dogecoin with merchants. This is done through two different types of transactions; minting (creation of Wrapped Dogecoins) and burning (reducing supply of Wrapped Dogecoins). These transactions will be available publicly and can be viewed by anyone through a block explorer. After the initial exchange, merchants aim to maintain a buffer of Wrapped Dogecoins so that they can exchange it with users. The two-step minting process helps reduce the time it takes for users to get Wrapped Dogecoins, as minting and burning are more time consuming processes.

Custodian wallet setup

Custodians are expected to have a pooled wallet for all merchants. The wallet will use multi-signature with all keys controlled by the custodian. The wallet will only be able to send to the whitelisted merchant address on chain. All minting and burning transactions are expected to be done within 48 hours of submission to the custodian. Note that in case of multiple custodians, a single wallet might not have enough funds to redeem all pending Wrapped Dogecoins.

Minting

Minting refers to the process of creating new Wrapped Dogecoins. Minting in the wrapped framework has to be done by a custodian, but needs to be “initiated” by a merchant. It is important to note that minting does not involve the user. It is a set of transactions done between the merchant and the custodian.



Sequence of minting events for wDoge

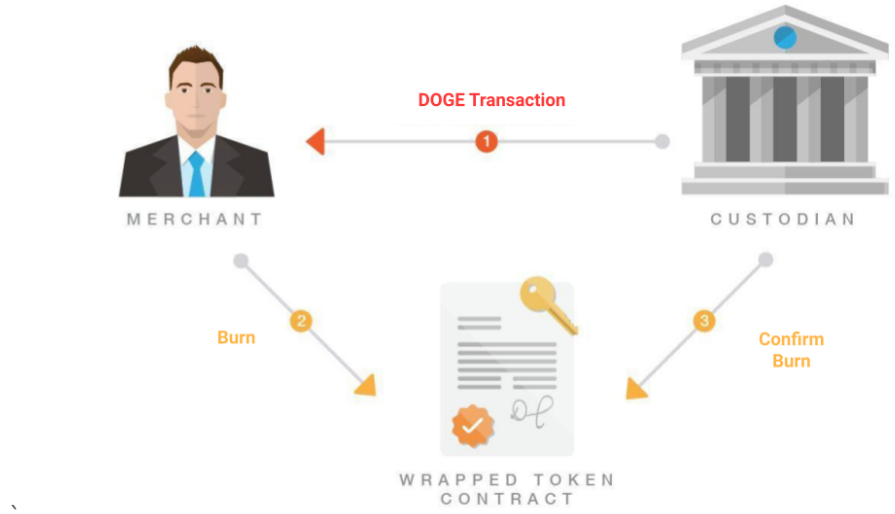
- Merchant initiates a transaction to authorize the custodian to mint X wDoge to the merchant’s address on the Ethereum chain.
- The merchant sends the custodian X Dogecoin.
- Custodian waits for 60 confirmations of the Dogecoin transaction
- Custodian creates a transaction to mint X new wDoge tokens on the Ethereum chain

Sequence of events for users to receive wDoge tokens

- User requests Wrapped Dogecoins from a merchant
- The merchant does the required AML, KYC procedures and gets identification information from the user
- The user and merchant perform an atomic swap, or use a trusted exchange with the merchant receiving Dogecoin and the user receiving wDoge

Burning

Burning refers to the action of redeeming Dogecoins for wDoge tokens. Only merchant addresses can burn Wrapped Dogecoins. In order to do so, the 'burn' function is called in the contract with the amount of tokens to be burnt on the Ethereum chain. By doing so, the amount is deducted from the merchant's wDoge balance (on chain) and the supply of wDoge is reduced.



Sequence of events for burning wDoge tokens

- The merchant creates a burn transaction, burning X wDoge tokens
- Custodian waits for 25 block confirmations of the ETH transaction
- Custodian releases X wDoge to the merchants Dogecoin address
- Custodian makes an ethereum transaction marking the burn request as completed

Sequence of events for users to receive Dogecoin

- User requests the redemption of tokens from a merchant
- The merchant does the required AML, KYC procedures and gets identification information from user
- The user and merchant perform an atomic swap, or use a trusted exchange where the user receives Dogecoin and the merchant receives wDoge tokens

Governance

The Wrapped Dogecoin contract is governed by a multisig contract in which signatures are required from DAO members in order to add/remove members. All custodians and merchants will be DAO members, but other institutions can also be included as a member without having a custodian or merchant role. An “M of N” signature signature will be used in the contract where M is the required number of signatures in the multisig contract and N is the total number of members. The values of M and N will be decided mutually between members keeping in mind security as well as the ease of adding/removing members.

Atomic Swap

Atomic swaps can be used between merchants and users in order to exchange wDoge and DOGE. If the user would like to receive wDoges or Dogecoins more quickly, a trusted method of exchange could also be done through the merchants.

Once KYC is completed, the steps for users to atomically swap Dogecoin for wDoge with the merchant are:

- User generates a secret and a hash of it is provided to the merchant off chain. The user and the merchant also agree on other swapping details such as receive addresses (ETH and Dogecoin)
- The user creates a Dogecoin HTLC (Hashed Time Lock Contract) using the merchant’s Dogecoin address, user’s refund address, secret hash, and expiration time. This is used to create a P2SH address which the user funds with X Dogecoins
- After 60 confirmations, the merchant will create an HTLC contract on Ethereum, by using the user’s Ethereum address, merchant’s refund address, secret hash, and expiration time. The merchant then transfers X wDoge to the atomic swap contract.
- The user reveals the secret in order to move X wDoge from the atomic swap contract to the user’s Ethereum address
- The merchant uses the secret in order to move Dogecoin funds from the P2SH address
- If the user does not claim the wDoge within the expiration time, the transaction does not go through and the user can claim the DOGE back

Some important things to note here:

- In order to deploy the atomic swap contract and send wDoge to it, there are transaction fees involved. Hence, the user will have to pay an atomic swap fee before initiating a swap.
- Atomic swaps take time and multiple transactions on both the Dogecoin and ETH chain. The user may have the option of doing a trusted swap in which Dogecoin is transferred to the merchant address and after 60 confirmations on the Dogecoin network, the merchant sends wDoge to the user. This involves trust in the merchant, but it is quicker and cheaper.

wDoge vs Atomic Swaps

Atomic swaps can be performed without wDoge for users which only want to perform a Dogecoin-ETH trade. However, it is important to note that wDoge provides a representation of Dogecoin on the ETH chain, which is required for DAPPs and the ecosystem to interact with. A few other tradeoffs to consider while comparing atomic swaps with wDoge:

- They require price discovery to be done by whoever does the atomic swap. In wrapped tokens price discovery only needs to be done while trading on a decentralized exchange after having already obtained wDoge.
- Requires atomic swap technology to be supported by existing wallets and decentralized exchanges. Wrapped Dogecoin will be available for use in any ERC20 supported wallet.
- They are really slow because every transactions is as slow as multiple confirmations on the ETH chain and then the Dogecoin chain (as opposed to wDoge, where the initial minting/tokenization is slow but after creation it's easily tradable on the ETH chain)
- Doing an atomic swap on a decentralized exchange requires a separate deposit and an atomic swap fee as well. This is inconvenient each time users want to swap currencies.

Fees

Transfers of wDoge between users will have no cost apart from network fees. There are three ways in which different parties in the network can earn fees:

- Custodian fees: This is taken by the custodian at the time when a merchant mints or burns wrapped tokens.
- Merchant fees: This is taken by the merchant who the user exchanges wrapped tokens with for the asset.

Legal Binding

Contract between custodians and merchants

The process of minting and burning tokens does not involve the user and is between trusted institutions. Merchants are required to hold the identity information of the user securely.
Custodians are required to publish details of assets under custody quarterly and perform minting/burning duties in a timely manner. Failure to meet these criteria can lead to removal from the network.

It is to be noted that there can be multiple custodians in the network, but this comes at the cost of increasing the risk involved in the network. A model where custodianship is shared by different institutions holding keys to a multi-sig wallet is also possible in the future. Though operationally, minting/burning/auditing would require more coordination and time. A security breach among any of the custodians would cause the loss of trust and could lead to mass withdrawals. A security breach with a merchant is much less severe as all outstanding tokens will still be backed up by custodians, but instead could lead to a loss of KYC/AML user data.

Trust model

In some sense custodians are trusted in the wrapped framework, as assets could be stolen or they might not honour the one-to-one backing. However, the wrapped framework aims to minimize this trust in a few ways:

- Quarterly audits will be conducted by external third parties to verify that all Wrapped Dogecoins minted have an equal amount of asset stored among all custodians. In the case of wDoge, proof of reserves can be shown by publishing signatures from the addresses which Dogecoin is stored in.
- Custodians will not be able to mint tokens on their own, but would instead require the initiation of a merchant in order to do so. Hence creation of new tokens involves both the custodian and the merchant.
- The user is insulated from interacting with the custodian through a set of merchant institutions. An individual merchant does not need to be trusted, but instead all merchants together would need to be.
- Existing credibility of the institutions involved is at stake for all the institutions involved with the framework.

Transparency

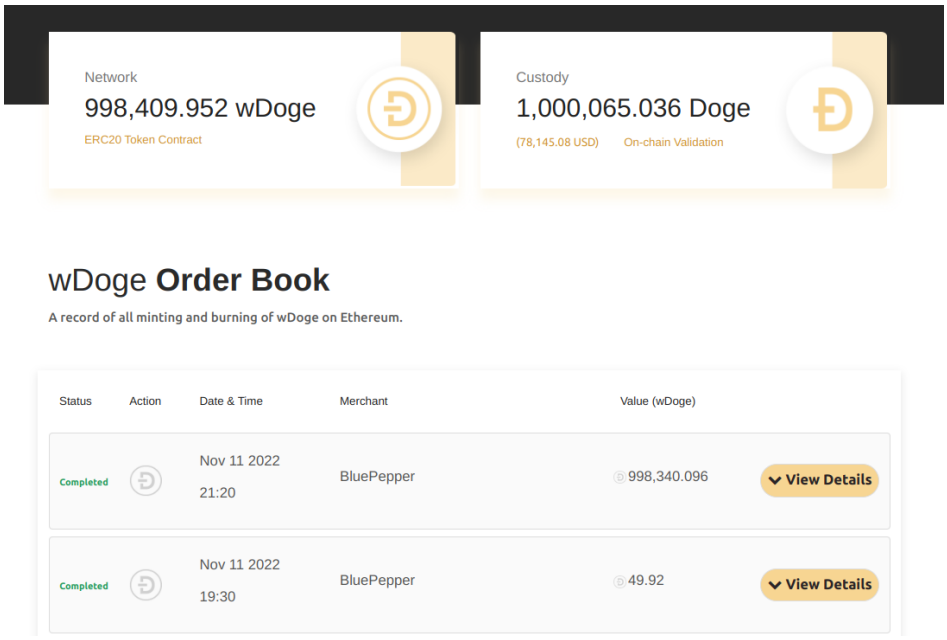
There will be full transparency in the functioning of the wrapped token. All key details of the network will be reflected in a dashboard, some of which are:

- Names and details of institutions performing different roles in the network
- Status of mint and burn orders (pending, processing, canceled, complete)
- Total amount of Dogecoins stored by custodians
- Total amount of wDoge in the network (Will be the same or slightly lower than Dogecoins

stored)

- Quarterly audits in the form of transactions which prove that the custodian has the keys to the Dogecoin
- Merchant and Custodians ethereum addresses
- The Dogecoin address associated with each merchant, controlled by the custodian
- Links to the open source token contract code / deployed contract on a block explorer

An example of what the dashboard might look like:



Conclusion

Through Wrapped Dogecoin, we propose a solution to make Dogecoin interchangeable and representable on the Ethereum chain. Global liquidity, increased fractional ownership, smart contract programmability and reduction in transaction fees are some of the key benefits of tokenization. All transactions, contracts and audits will be publicly viewable to maintain transparency and enable trust in the network. The framework also provides a way in which multiple institutions in the cryptocurrency space can perform different roles to get past common issues faced by asset backed tokens.

Glossary

Custodian - The institution or party who holds the asset. In the case of wDoge, this will be played by BitGo. Custodians hold the keys to mint tokens.

Merchant - The institution or party to which Wrapped Dogecoin will be minted to and burnt from. Merchants play a key role in distribution of the wrapped token. In the case of wDoge, this will be played initially by Bluepepper. Each merchant holds a key to approve minting of new wrapped tokens and burn wrapped tokens.

User - The holders of the Wrapped Dogecoin. Users can use Wrapped Dogecoin to transfer and transact like any other ERC20 token in the ethereum ecosystem.

KYC (Know your customer) - FINCEN and OFAC Required Guidelines pursuant to which institutions must seek information in order to confirm that customers are not subject to OFAC sanctions, violate any Bank Secrecy Act rules or are otherwise potentially engaged in money laundering activities.

AML (Anti money laundering) - Rules and regulations enforced by regulatory authorities (including the Department of Treasury in the US) to target and combat illicit source of funds which may be laundered.

wDoge (Wrapped Dogecoin) - An ERC20 token on ethereum backed 1:1 by Dogecoin.

References

[1] - https://cointelegraph.com/explained/what-is-a-daico-explained
[2] - https://www.bitgo.com
[3] - https://www.bluepepper.io/