Wrapped Tokens

A multi-institutional framework for tokenizing any asset

Whitepaper v0.1
Oct 5th 2018

Kyber Network
BitGo Inc
Republic Protocol

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, transactions 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 tokens follow 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 first wrapped token we launch will be an ERC20 token backed by Bitcoin (BTC) and will be appropriately named, "Wrapped BTC" (WBTC). Unlike centralized solutions (USD), WBTC will be fully accounted for and proof of reserves posted on the BTC chain.

There is no additional secondary utility/payment token required to use WBTC, and no transfer fees other than blockchain fees. WBTC 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 Bitcoin, 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

The majority of ERC20 trading in centralized exchanges today is done with BTC and not ETH. Most decentralized exchanges offer only ETH/Token and not BTC/Token trades. Wrapped tokens 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 BTC token can bring. WBTC brings the ease of creation of smart contracts to Bitcoin.

Benefits of fiat tokens

Tokens backed by fiat currencies offer a safe way for traders to keep their money in a cryptocurrency without having to worry about price fluctuations. This is particularly useful for traders on both centralized and decentralized exchanges where there is no direct way of transferring fiat currencies. Fiat currency backed tokens also promise a world in which a

cryptocurrency can replace traditional finance. Notably, it can be used in e-commerce by both buyer and seller without having to worry about conversion rates or taxes (buyers are required to pay capital gains tax calculated at the time of purchase in the US).

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 Bitcoin, 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 Bitcoin 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. Securities for example require whitelisting, holding periods, and identity management.

Common Issues

Scalability

As of January 2018, the maximum practical gas limit on Ethereum's mainnet topped out at 8,000,000 gas per block [1]. This limit is both hardware and software-bound. While there are several scalability solutions proposed, many require significant developer lift (state channels), or are too early in development for practical use (plasma, sharding). This is a problem for Dapps and users of the network because gas prices skyrocket during periods of contention (hot ICOs, CryptoKitties). Earlier this year in July, transactions caused by Chinese exchange Fcoin caused all time high transaction fees [2].

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?

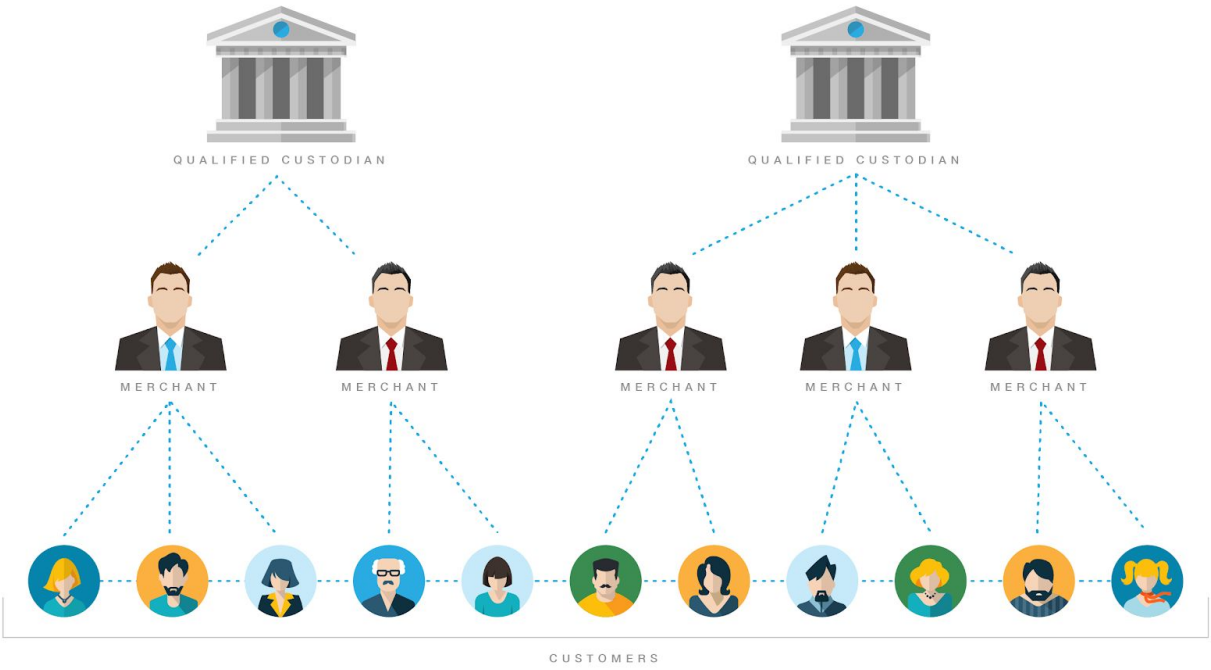
Regulation

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 [3].

Implementation and Technology



Key Roles

- Custodian - The institution or party who holds the asset. In the case of WBTC, this will be played by BitGo [4]. 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

WBTC, this will be played initially by Kyber [5] and Republic Protocol [6]. 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.
- WBTC 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 WBTC DAO.

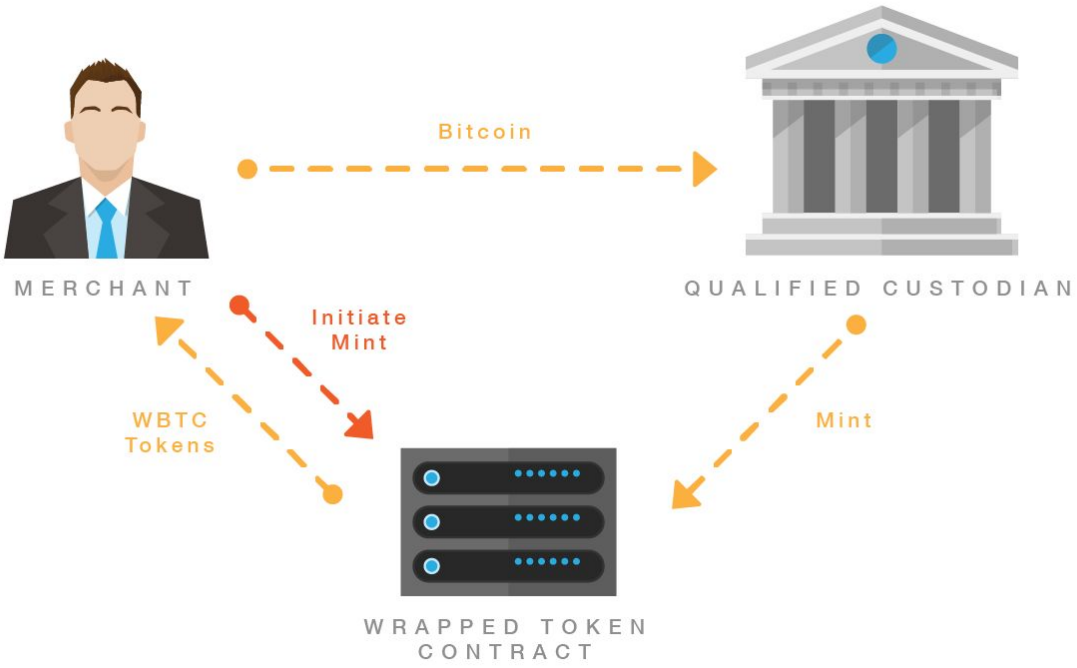
Custodians exchange assets for wrapped tokens with merchants. This is done through two different types of transactions; minting (creation of wrapped tokens) and burning (reducing supply of wrapped tokens). These transactions will be available publicly and can be viewed by anyone through a block explorer.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

Custodian cold wallet setup

Custodians are expected to have one pooled cold wallet for all merchants. The cold wallet will use multi-signature with all keys always offline and controlled by the custodian. The cold 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 cold wallet might not have enough funds to redeem all pending wrapped tokens.

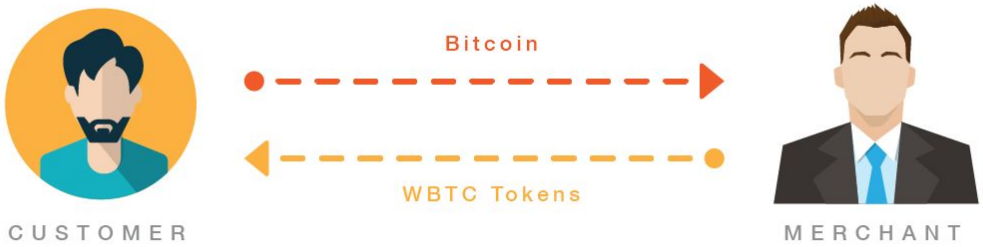
Minting

Minting refers to the process of creating new wrapped tokens. 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 WBTC

- Merchant initiates a transaction to authorize the custodian to mint X WBTC to the merchant's address on the Ethereum chain.
- The merchant sends the custodian X BTC.
- Custodian waits for 6 confirmations of the BTC transaction
- Custodian creates a transaction to mint X new WBTC tokens on the Ethereum chain

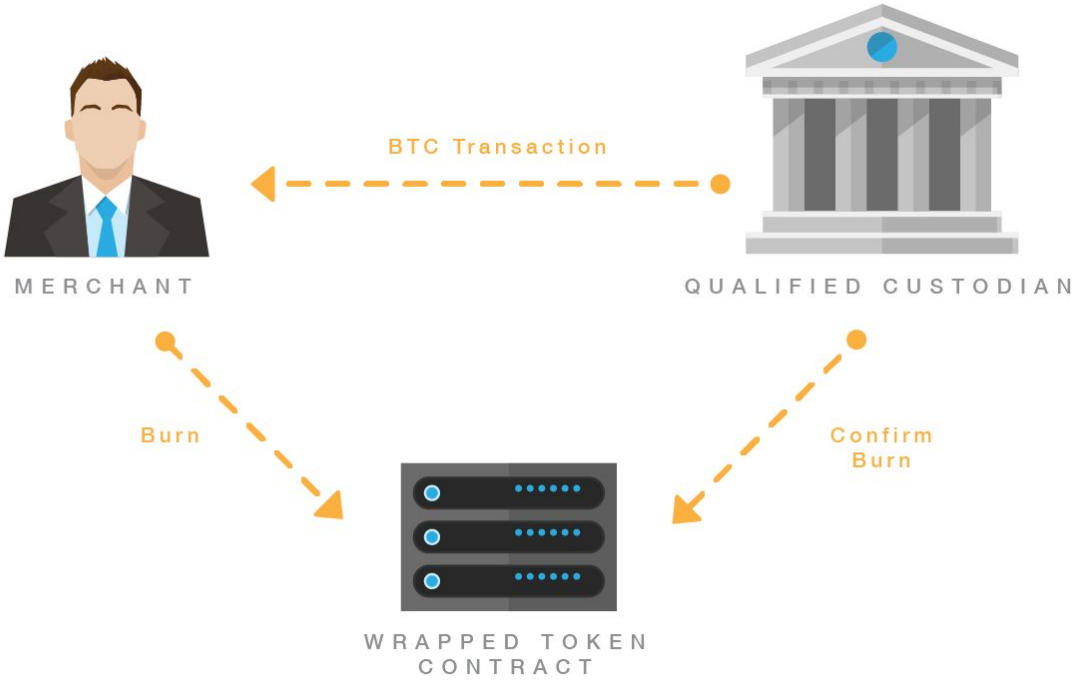


Sequence of events for users to receive WBTC tokens

- User requests wrapped tokens 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 Bitcoin and the user receiving WBTC

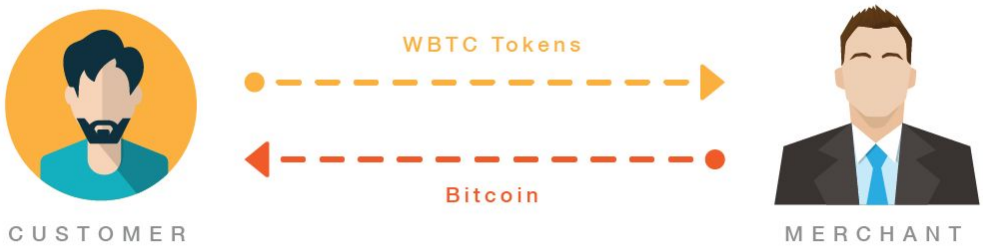
Burning

Burning refers to the action of redeeming BTC for WBTC tokens. Only merchant addresses can burn wrapped tokens. 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 WBTC balance (on chain) and the supply of WBTC is reduced.



Sequence of events for burning WBTC tokens

- The merchant creates a burn transaction, burning X WBTC tokens
- Custodian waits for 25 block confirmations of the ETH transaction
- Custodian releases X BTC from cold storage to the merchants Bitcoin address
- Custodian makes an ethereum transaction marking the burn request as completed



Sequence of events for users to receive Bitcoins

- 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 Bitcoin and the merchant receives WBTC tokens

On Chain transfer restrictions

Based on the token, there could be restrictions in place for the transfer of tokens. For WBTC, there will be no restrictions on transfers.

Governance

The wrapped token 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.

Side chain for wrapped tokens

Initially, WBTC will be launched on the Ethereum mainnet chain. The mainnet chain is easily accessible and usable as there are a network of exchanges, block explorers, wallets, and other Dapps on it. One of the key benefits of tokenization, is cheap transactional cost. But with gaining popularity of Ethereum and increased Dapp creation, transaction costs of wrapped tokens could rise to the point where it is not cheap to do so on the main chain. The collaboration of multiple institutions in the wrapped framework enables the ability to deploy a practical scalable solution to increase transactional throughput.

This can be done through the use of a pegged sidechain, using existing software (parity-bridge) run among DAO members. The chain will run on it's own proof of authority network [7] using the Aura consensus algorithm [8]. Blocks will be created every 4 seconds predictably and in a performant manner. Currently, there is already such a chain (Kovan testnet) and it has been in operation since March 2017. Wrapped tokens will be pegged between the main and side chain by creating a 2-way multi-sig wallet on mainnet and on the sidechain. Side chains provide much needed scalability on ethereum. Some benefits of a side chain for trading and transferring wrapped tokens are:

- Scaling with minimal development costs (same EVM)
- Dedicated, increased throughput - seperate blockchain on separate hardware and potential proof of authority (PoA) advantages (faster blocks)
- Easy to support in existing clients and wallets
- Chain is free from other "noisy neighbors"
- Minimal transactional cost (to prevent spam)

Validators (block generators) will be chosen from wrapped partners and other trusted parties who will be geographically distributed and represent several different domiciles / governments. Validators will also maintain the 2-way peg between the main and side chain. To peg the value of wrapped tokens on both chains, we propose a multi-signature contract to be used on the mainnet and the sidechain.

- To send from Ethereum mainnet to Ethereum sidechain:
    - Send from mainnet address to the federated mainnet multi-sig address
        - It is recommended to send the amount while calling the "sendToSidechain" method on the multi-sig address, specifying as the argument the destination address on the sidechain
        - If sent without a method, the destination address on the sidechain will be assumed to be the same as the source address
    - An event is generated on the mainnet to record the send
    - Federated signers "lock" tokens on mainnet
    - After a "confirmation period", multisig authorities on the sidechain can validate the send event on the mainnet and disburse the amount to the destination address on the sidechain, less transaction fees
- To send from ETH sidechain to ETH mainnet:
    - Identical (symmetric)

WBTC will be the first asset on the sidechain and will use a combination of these components working together to create an ecosystem:

- Node Software and Configuration
- Block Explorer
- Wallet Providers

- Block Validators
- Multi-sig Authorities

Incentivization

Transactions will be charged at the minimal starting gas price of 1 Gwei to cover running block validators and to prevent spam on the sidechain. Validators can also be incentivized off chain for each Dapp or have block rewards. Details of distribution/management of Ether on the sidechain are still to be determined.

Atomic Swap

Atomic swaps can be used between merchants and users in order to exchange WBTC and BTC. If the user would like to receive WBTC or BTC 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 BTC for WBTC 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 BTC)
- The user creates a Bitcoin HTLC (Hashed Time Lock Contract) using the merchant's Bitcoin address, user's refund address, secret hash, and expiration time. This is used to create a P2SH address which the user funds with X BTC
- After 6 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 WBTC to the atomic swap contract.
- The user reveals the secret in order to move X WBTC from the atomic swap contract to the user's Ethereum address
- The merchant uses the secret in order to move Bitcoin funds from the P2SH address
- If the user does not claim the WBTC within the expiration time, the transaction does not go through and the user can claim the BTC back

Some important things to note here:

- In order to deploy the atomic swap contract and send WBTC 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 BTC and ETH chain. The user may have the option of doing a trusted swap in which BTC is transferred to the

merchant address and after 6 confirmations on the bitcoin network, the merchant sends WBTC to the user. This involves trust in the merchant, but it is quicker and cheaper.

WBTC vs Atomic Swaps

Atomic swaps can be performed without WBTC for users which only want to perform a BTC-ETH trade. They can be done on a decentralized exchange outlined through a mechanism by the Komodo platform [9]. However, it is important to note that WBTC provides a representation of BTC 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 WBTC:

- 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 WBTC.
- Requires atomic swap technology to be supported by existing wallets and decentralized exchanges. Wrapped BTC 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 Bitcoin chain (as opposed to WBTC, 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 a atomic swap fee as well. This is inconvenient each time users want to swap currencies.

Fees

Transfers of WBTC 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.
- Sidechain transaction fees: This fee is predominantly aimed at preventing spam on the sidechain. This is shared equally among all institutions running nodes on the sidechain.

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 tokens minted have an equal amount of asset stored among all custodians. In the case of WBTC, proof of reserves can be shown by publishing signatures from the addresses which bitcoin 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.

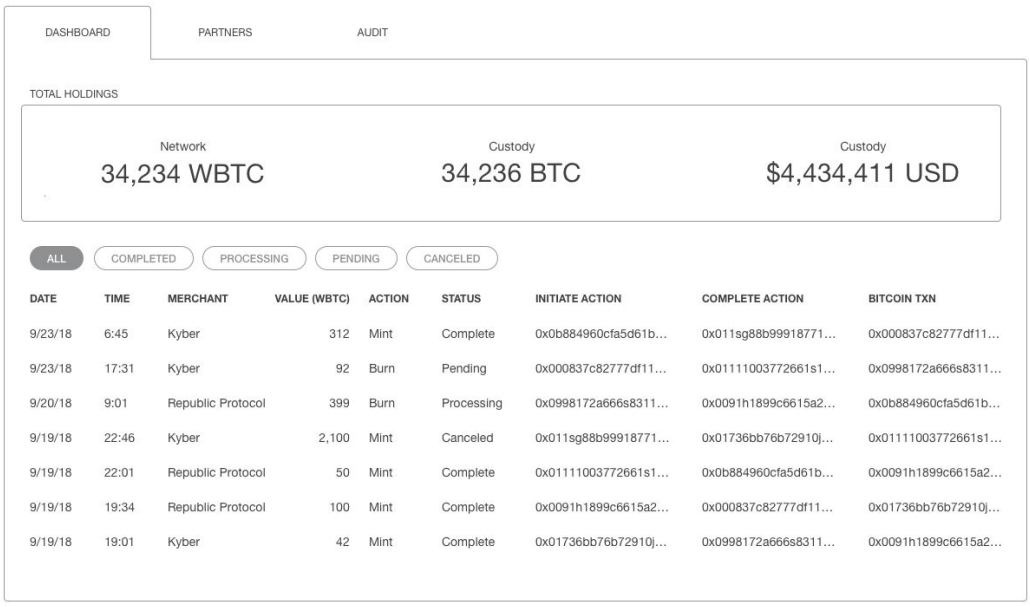
Transparency

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, cancelled, complete)
- Total amount of BTC stored by custodians
- Total amount of WBTC in the network (Will be the same or slightly lower than BTC stored)
- Quarterly audits in the form of transactions which prove that the custodian has the keys to the Bitcoin
- Merchant and Custodians ethereum addresses

- The Bitcoin 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 tokens, we propose a solution to make assets 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. WBTC will be the first such token, enabling Dapps easy access to Bitcoin. 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 WBTC, this will be played by BitGo. 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 WBTC, this will be played initially by Kyber and Republic Protocol. Each merchant holds a key to approve minting of new wrapped tokens and burn 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.

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.

WBTC (Wrapped Bitcoin) - An ERC20 token on ethereum backed 1:1 by Bitcoin.

References

[1] - https://etherscan.io/chart/gaslimit
[2] - https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/
[3] - https://cointelegraph.com/explained/what-is-a-daico-explained
[4] - https://www.bitgo.com
[5] - https://https://kyber.network
[6] - https://republicprotocol.com
[7] - https://paritytech.github.io/wiki/Proof-of-Authority-Chains
[8] - https://wiki.parity.io/Aura
[9] - https://komodoplatform.com/atomic-swaps/