Staked WBTC Whitepaper

Version 1.0

Abstract

Staked WBTC (stWBTC) is a platform that enables users to participate in the decentralized finance (DeFi) ecosystem using WBTC. Users can deposit their WBTC into the DAO's smart contracts and receive stWBTC token, a representation of the WBTC staked on the platform, in return.

Staked WBTC would be utilized towards various yield generating strategies which includes, but not limited to, liquidity pools, yield aggregators, yield optimizers, via customized smart contracts deployed by the protocol.

stWBTC is a rebased token and holders of the token will be able to observe an increase in the quantity held every 24 hours. A wrapping solution for the token will also be made available to holders of stWBTC, to wrap the token into wstWBTC. wstWBTC is a standard ERC-20 token which quantity received by the user will decrease as time progresses to signify the share of the ever growing asset pool.

User depicted yields for both stWBTC and wstWBTC tokens will be net of protocol operation fees.

stWBTC strategies will be evaluated in accordance with a risk based approach in order to mitigate the risk of any loss of deposited tokens and if the yield is worth the associated risk. Continued assessments and monitoring will be performed to ascertain that risks are addressed timely in order to adapt to a changing market condition.

Generated yield will be in WBTC, rewards from strategies will be sold to purchase WBTC to re-enter into the strategies on a timely basis.

1. Introduction

This whitepaper outlines the technical architecture, economic model of stWBTC.

BTC being the father of all cryptocurrencies has been widely regarded as digital gold due to its limited quantity, and has been sought after by holders to expand its utility to other blockchain ecosystems.

WBTC is the pioneering wrapped version of BTC being bridged from its native blockchain to the Ethereum ecosystem, this has made it a trusted asset in Decentralized Finance due to the relation to Bitcoin.

Unlike Delegated Proof-of-Stake coins, WBTC is not able to draw any yield from staking nodes. Hence, stWBTC would provide an alternative solution to provide holders of BTC or WBTC to generate a yield whilst holding on to them for a long term.

2. Technical Architecture

Staked WBTC will be used to supply into risk assessed strategies generating a yield and returned to users via rebased mechanism for stWBTC and asset pool for wstWBTC. These returns will be generating yield as long as strategies are in place, yield rates may vary due to the change in strategies returns and duration of deployment of staked WBTC.

stWBTC is a rebase token, which will be rebased every 24 hours to accurately represent yields generated from the assessed strategies. Generated yield will be sold to purchase WBTC to be redeployed into the strategies. Users may redeem WBTC with stWBTC and the protocol will unwind the strategies placed into liquid WBTC for the user.

wstWBTC is a wrapped version of the stWBTC, which serves as an alternative token to grant its holder a utility to other protocols which are not compatible with rebase tokens.
wstWBTC is a time sensitive token which will be minted in unproportionally to stWBTC, a lower amount is wstWBTC will be minted per stWBTC as time progresses to represent the User's share of the total asset pool. As yields from prior periods are not to be shared to users who enter in a later period. Users may redeem WBTC with wstWBTC and the protocol will unwind the strategies placed into liquid WBTC for the user.
Generated yield will be sold to purchase WBTC to be redeployed into the strategies. Users may redeem WBTC with stWBTC and the protocol will unwind the strategies placed into liquid WBTC for the user.
Protocol will deploy and maintain all relevant smart contracts on the Ethereum blockchain and will implement the core logic and functionality of the platform. Protocol will govern all smart contract parameters, such as but not limited to, fees, rewards, strategies and upgrades.

2.1 Smart Contracts

Customized smart contracts deployed on supported chain:

- **stWBTC Token Contract**: Represents stWBTC on Ethereum and supported blockchains.
- **wstWBTC Token Contract**: Represents wstWBTC on other Ethereum and supported blockchains.
- **Vault/Pool Contract**: Staked WBTC asset pool on Ethereum and supported blockchains.
- **Strategy Contract**: Deployment of Staked WBTC onto strategies.
- **Chief Contract**: Authorization of changes to protocol contracts.

3. Token Standards

stWBTC is a standard ERC-20 token and the associated smart contract(s) are compatible across most EVM compatible blockchains.

wstWBTC is a rebase token and the associated smart contract(s) are compatible across most EVM compatible blockchains.

4. Use Cases

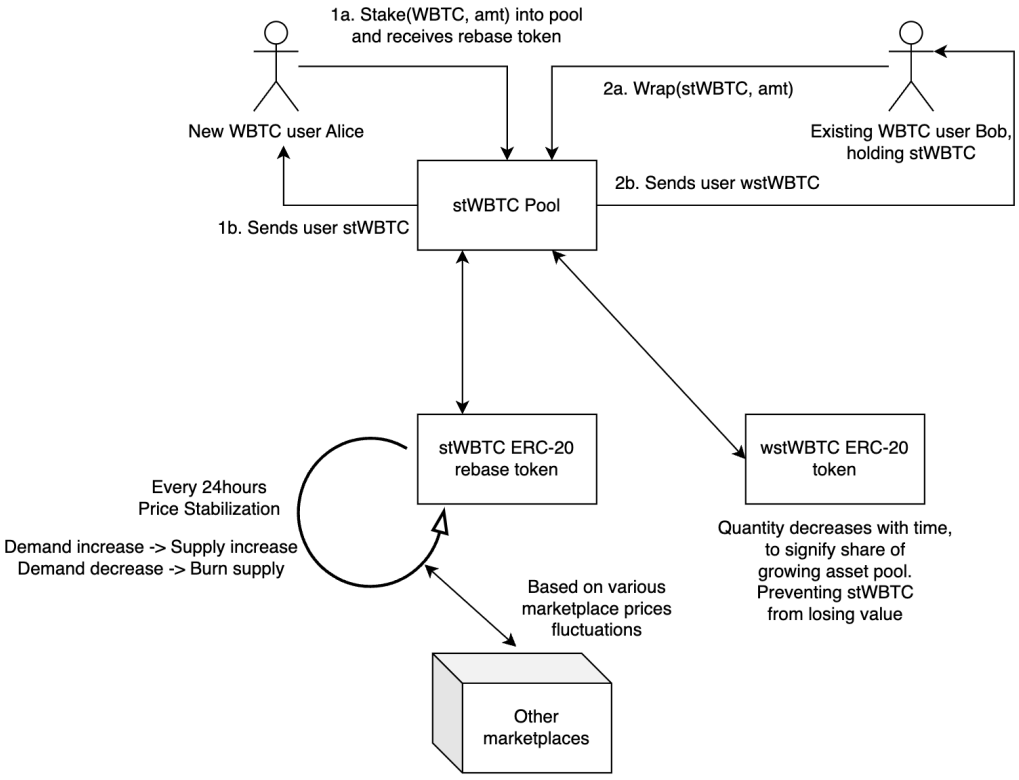

Figure 1: User Stake deposit flow

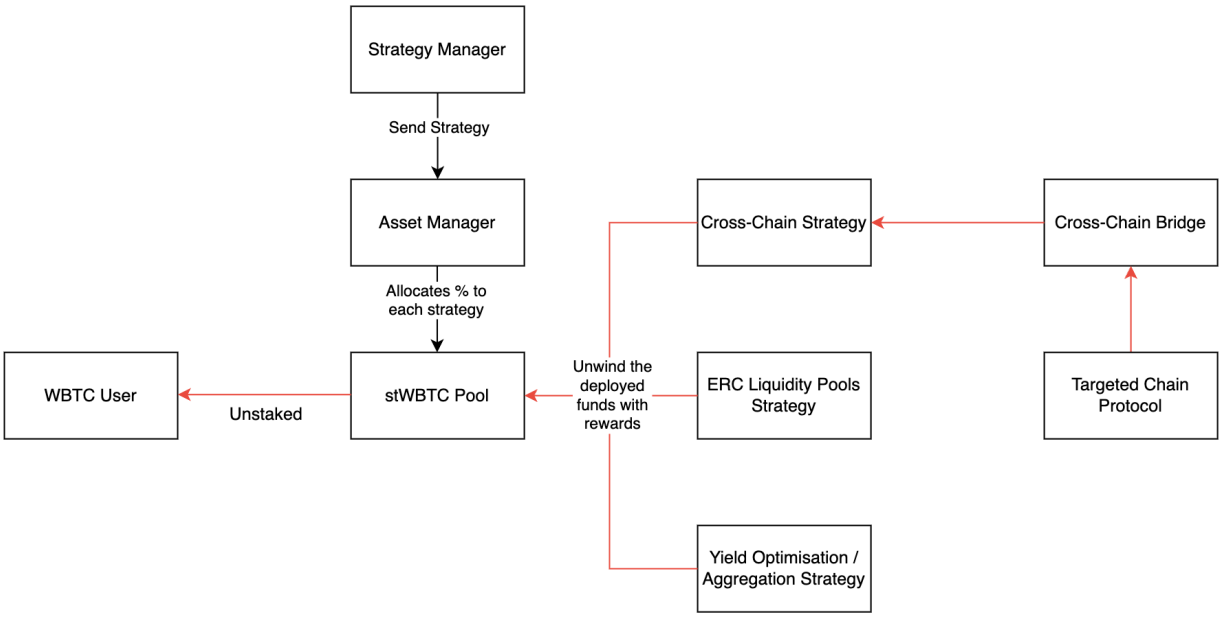

Figure 2: User unstake flow

4.1 Liquidity Pools

Liquidity pools are decentralized exchange swaps on Ethereum and other blockchains which provide yield via transaction fees and platform reward tokens.

Risks involved are smart contract integrity risk and impermanent loss.

4.1.1 Smart Contract Integrity Risk

Smart Contracts are designed to serve its required function. A single contract can be designed to serve all functions required to run the protocol, but that would lead to poor gas efficiency. Hence, multiple smart contracts are designed to only perform the required functions when requested to mitigate redundancy and be more gas efficient.

This is where risk is assessed, whether the smart contracts are designed to its function, no hidden functions are coded to cause detriments to its users and attack vectors by bad actors are prevented.

4.1.2 Impermanent Losses

Impermanent losses is a unique concept to decentralized finance. It is simply the difference between the liquidity provided to a liquidity pool at the entry and exit points. Due to the design and structure of a liquidity pool, 2 token types exist in each pool with different proportions.

These proportions would determine the price of the assets at any given point of time. As arbitrageurs are required to maintain that asset prices remain fairly similar across all blockchains and exchanges. The proportion of liquidity provided in the liquidity pools is bound to be different between entry and exit points leading to impermanent losses.

4.2 Yield Farming

Yield farming is a generalized term for yield farming activities and strategies, Liquidity Pool provisioning is also a subset of yield farming. Other activities include secondary layer protocols such as yield aggregation and optimization protocols to be incorporated into the strategies. With an added layer above the primary protocol, brings complexity and added risks. Such protocol viability, team behavior, smart contract integrity and processes and operations.

4.2.1 Yield Aggregation

Yield aggregation is a secondary layer protocol which consolidates yield from other primary protocols into a single source for users to access conveniently.

4.2.2 Yield Optimization

Yield optimization is a secondary layer protocol which targets single or multiple primary protocols by owning its governance tokens for a boosted yield which normal users may not have access to.

4.3 Governance

Governance for stWBTC will have participation from the community via ownership of Governance Tokens. Tokens will be distributed to the community via participation of protocol strategies as rewards.

Governance Tokens will provide holders with a voice on decisions and matters in relation to the strategies and operations of the protocol via a voting system.

Refer to protocol published roadmap for the initialization of the rewards distributions.

5. Economic Model

5.1 Tokenomics

stWBTC

- Total Supply: 21,000,000
    - Based on total amount of BTC able to be minted

wstWBTC

- Total Supply: 21,000,000
    - Based on total amount of stWBTC able to be minted

Governance Token (Subjected to changes)

- Total Supply: 1,000,000
    - Treasury Use: 200,000
    - Investors: 300,000
    - Partnerships: 100,000
    - Community Rewards: 400,000

5.2 Protocol Fees

Protocol fees are fees drawn from yield generated from various strategies, this is to ensure that the protocol is financially viable and able to provide funding to various counterparties in forms of blockchain transaction fees, service provider fees and other miscellaneous fees.

The amount drawn will be subjected to market conditions and utilisation of the protocol, amounts drawn will always be below total yield rate from total strategies and not from initial amounts staked from users.

5.2.1 Service Providers

Service providers are individuals or collectives providing support for protocols, utilising these services would cost the protocol. The benefits should outweigh the costs are it should provide greater efficiency and security on various aspects of the protocol. Such service providers could be, but not limited to:

- Smart Contract Auditors
- Decentralized Price Oracles
- Automation Services
- Governance Facilitator

5.2.2.1 Smart Contract Auditors

Smart Contract Auditors are external service providers who provide a secondary layer of review of smart contracts and identifies potential lapses and weaknesses, and advises the protocol to make changes to strengthen its security. They offer reports to the protocol to be available to the public as a form of assurance that the protocol is of a certain quality and risk vectors have been mitigated.

5.2.2.2 Decentralized Oracle Price

Price oracles are price references in which the protocol draws its data from, traditional price references were based on a single source which was risky and prone to price manipulation. Hence, a decentralized price oracle is required to ensure that protocol is mitigated from price manipulations. And also a timely update or current market prices accurately.

5.2.2.3 Automation Services

Automation Services are service providers who are granted limited access to parameters or functions of the protocols to ensure that the changes and upgrades are queued and uploaded for updates on a timely basis.

5.2.2.4 Governance Facilitator

Governance Facilitators are individuals or a collective who would assist to facilitate the governance of a protocol by proposing changes, managing the community or keeping users up to date with the workings of the protocol.