White paper: *Project Stabilitas*

Description

The goal of blockchain technologies is to allow the efficient exchange of value. Blockchain technology allows the issuance of tokens which represent real world assets.

The ability to have stablecoins representing real currencies allows general users to use them to efficiently swap these tokens with real world assets in e-shops and crypto communities.

Project Stabilitas aims to tokenize real world assets such as USDc, EURc, or gold with smart contracts.

The cybersecurity offered by smart contracts ensures that there is no counterparty-risk and that the usage of the *Stabilitas* protocol is safe for general use.

Goals of *Stabilitas* protocol

- Provide a means for anyone to issue any amount asset-backed tokens at the market level
- Create AMM pools and increase liquidity with increased usage
- Provide a means for holders of the tokens to receive the currency from the reserve at the market level
- Ensure that the protocol is resilient against market manipulation

Dictionary

stCurrency is currency issued by *Stabilitas* protocol ie: stCHF, stUSD, stEUR, stCZK, stHUF

BaseCurrency is the DAO-approved deposit token, such as USDc, EURc. The BaseCurrency must not be a volatile asset such as bitcoin. The BaseCurrency must be fully backed by the underlying asset

Base points are standard financial expressions for the size of the fees. 1 basis point is 0,01%

How to achieve the goals?

The protocol is dependent on decentralized oracles who provide following price calculations:

- **CBPrice**: BaseCurrency/stCurrency prices from official data sources, for example European Central Bank quotes
- **VWAPPrice**: VWAP price of the AMM BaseCurrency/stCurrency pool is calculated by pool smart contract or by the oracle
- **CurrentPrice**: Most recent price from AMM BaseCurrency/stCurrency pool

Additional variables manageable by the DAO are:

- **ProtocolFee**: Protocol fees expressed in basis points (N*0,01%)
- **LiquidityProgramFee**: Fee expressed in basis points
- **NegativeFee**: If the current price is better for the user then the quote from the central bank, then the user pays a negative fee. Negative fee is expressed in basis points
- **ExitFee**: If a user wants to remove assets from the reserve, the exit fee may be applied
- **StopPriceTop**: If the current market price is above the last central bank price, the protocol will not release any funds. (Funds may still be traded by the AMM)
- **StopPriceLow**: If the current market price is below the last central bank price plus percentage, the protocol will not release any funds. (Funds may still be traded by the AMM)

Depending on the maturity of *Stabilitas* protocol, the free-market price discovery will be moved.

Examples of market simulation

BaseCurrency:	USDc	Stop price:	2%
stCurrency:	stCZK		
ProtocolFee:	0.01%	Protocol maturity configuration:	
LiquidityProgramFee:	0,3%	CBPrice:	0%
NegativeFee:	0,3%	VWAPPrice:	100%
ExitFee:	0,1%	CurrentPrice:	0%

Example #1

Use Case: *Deposit reserves above CBPrice*

CBPrice: 22,102 stCZK/USDc

VWAPPrice: 22,536 stCZK/USDc

CurrentPrice**:** 22,386 stCZK/USDc

User wants to swap $100,000 to stCZK. Obtainable assets: 22.536*100,000=2,253,600 stCZK

StopPriceTop is 22.54404. VWAPPrice < StopPriceTop, CurrentPrice < StopPriceTop, user can perform deposit of USDc and withdrawal of stCZK.

CurrentPrice >= CBPrice with increased reserves action, so **NegativeFee** is 0.

User pays 0,01%+0,3% = 100,000*1.0031=100,310 USDc, from which 300 USDc goes to increase stCZK/USDc LP position. User receives 2,253,600 stCZK

Example #2

Use Case: *Withdraw reserves above CBPrice*

CBPrice: 22,102 stCZK/USDc

VWAPPrice: 22,536 stCZK/USDc

CurrentPrice**:** 22,386 stCZK/USDc

User wants to swap 2,239,936.38 stCZK to USDc.

StopPriceTop is 22.54404. VWAPPrice < StopPriceTop, CurrentPrice < StopPriceTop, user can perform deposit of stCZK and withdrawal of USDc.

CurrentPrice >= CBPrice with decreased reserves action, so **NegativeFee** is 0,3%.

User pays 0,01%+0,3%+0,3% = 2,239,936.38*1.0061=2,253,600 stCZK, from which 6719,81 stCZK goes to increase stCZK/USDc LP position and 0,3% stays in reserves. User receives 99,393.70 USDc

Difference between 100,000 and 99,393.70 from deposit and withdrawal from example 1 and example 2 is kept in the reserve increase and AMM LP increase.

Example #3

BaseCurrency:	USDc	NegativeFee:	0,01%
stCurrency:	stCHF	ExitFee:	0,1%
AMM Liquidity token 1:	100 000 000 USDc	Stop price:	10%
AMM Liquidity token 2:	90 000 000 stCHF		
Reserves:	300 000 000 USDc	Protocol maturity configuration:	
Reserves coverage:	102%	CBPrice:	0%
ProtocolFee:	0.01%	VWAPPrice:	0%
LiquidityProgramFee:	0,0%	CurrentPrice:	100%

Use Case: *Very mature market - AMM reserves higher than 100 000 000 USDc*

CurrentPrice: 1,11 stCHF/ USDc

The smart contract will allow users to deposit reserves at current AMM price and receive stCHF.

The smart contract will allow users to withdraw reserves at 0,11% fee.

DAO

Some central banks might not like this protocol because blockchain technologies do not allow any privacy. The general users might be tagged with their accounts and at that point their full history of transactions, their incomes, investments and any other earnings will become public and non deletable. Options for users is to use multi accounts, and it is their decision to go public, but some governments or politicians might not be willing to make open monetary systems a preferable direction.

That's why the protocol must be secured with smart contracts where not even the DAO can cheat the protocol - allow any withdrawals of tokens without depositing reserves at the current rate.

The DAO must be resistant to local legislative unfavorability. That's why the DAO should be established in a trusted financial zone such as Switzerland or UAE.

Risks

- Market manipulation to drain the reserves

  The main purpose of the variables in the protocol are to prevent the drain of reserves. The VWAP price ensures the arbitrage opportunities for the real world market disable onchain price manipulation.

- DAO takeover by market manipulator

  The DAO must be decentralized and decisions must be done in a fair manner. DAO tokens should be issued to active participants. Price oracle multisig parties are executives of the DAO. DAO will be managed by the Vote Coin protocol. Variable setup is done using multisig wallets owned by the DAO executives.

- Price oracle stops the data feed or becomes centralized

  The DAO must ensure the oracle feeds are high quality and decentralized.

- Reserves do not fully covers the issuance

Reserves may not be fully covered, but the selection of stablecoins to cover the reserves will ensure that reserves are much higher than the reserves of central banks.

- Terrorist financing, money laundering

The freeze and clawback functionality will be used and any dispute by the authorities will be processed according to valid legislation.

Copyright

Ludovit Scholtz

Versioning of the document

1-22-2023 Document created

1-23-2023 Document Edited

1-23-2023 Example 3 added, DAO section added