Universität Zürich[UZH]

CAS Blockchain

Stable coins

What attempts have been taken to make cryptocurrencies less volatile? What attempts have been made to introduce stablecoins in Switzerland?

Tomasz Rybarczyk

29.11.2021

Table of Contents

1. INTRODUCTION

Few assets are as volatile as cryptocurrencies. The price of Bitcoin continually reaches new high levels followed by significant price drops of 50% or more. Almost all cryptocurrencies fluctuate wildly, making them attractive for investors but risky assets for those who want to use them for preserving value or just as a currency to pay for goods and services. Stablecoins are an attempt to provide an answer to the problem. They are a bridge between crypto and the real world. These cryptocurrencies run on blockchains seemingly tied to the value of government-backed currencies like the US Dollar or precious metals, such as silver or gold.

Stablecoins are generally used by crypto traders who want to keep their money invested on a crypto exchange, and easily go in and out of different crypto investments without paying high fees to cash out. They are also used for cash transactions between crypto businesses, and as a way to hold on to cryptocurrencies without the same risk of volatility. Almost all stablecoins are backed by companies or other organisations that claim to have every invested dollar backed by real currency or assets with the equivalent value, yet there is no way to know for sure what the companies are actually holding.

In this paper, I will describe different type of stablecoins, their most successful implementations and problems they are facing. Additionally, I will describe some stablecoin projects which failed spectacularly.

Most stablecoins are pegged to the USD or commodities like gold, so I will evaluate the need and various attempts to introduce stablecoins where the reference value is the Swiss Franc.

I will also present a proof of concept for the Swiss Franc based algorithmically crypto-collateralised stablecoin bitCHF, which I designed and implemented during the preparation for the CAS Blockchain at the University of Zurich in the year 2021. The prototype has been launched on the test blockchain and is accessible to anyone for test and evaluation, as the source code is public. All information about the prototype can be found on the following page: www.bitchf.ch.

2. TYPES OF STABLECOINS

Stablecoins are just cryptocurrencies on the blockchain ecosystem with their value pegged against some stable assets, such as precious metals, or fiat currencies, such as the US Dollar or Swiss Franc. It is possible to recognise stablecoins by the collateral structures backing them. Based on the underlying collateral structure, the following types of stablecoins can be distinguished: cash-collateralised stablecoins, commodity-collateralised stablecoins, crypto-collateralised stablecoins or algorithmic stablecoins.

An interesting aspect is how different types of stablecoins react to extensive sell-offs called “bank runs” or turbulent market situations like price drops of cryptocurrencies.

2.1. Cash collateralised Stablecoins

Cash-collateralised stablecoins are the foremost variant of stablecoins. They have the backing of a fiat currency, such as the US Dollar or Swiss Franc. Cash-collateralised stablecoins are the simplest stablecoin types with a 1:1 ratio backing. The 1:1 ratio implies that one stablecoin would be equal to one unit of currency, such as a

Dollar or one Swiss Franc. Every cash-backed stablecoin is supposed to have a real currency in a bank account to back it up.

Users can redeem their coins as the entity managing the stablecoin takes the corresponding amount of cash from their reserve and sends it to the user's bank account. At the same time, the equivalent amount of stablecoins are taken out of circulation or destroyed.

Theoretically, those types of stablecoins are safe in case of "bank runs", provided the issuer which is supposed to be holding backing assets really does it. The issuers of cash-collateralised stablecoins usually provide an opportunity to redeem them against the basis value. As long as the money is booked at the bank account of the issuer, there should be no problem. Holding the 1:1 value to the basis currency should also not be a problem because of obvious arbitrage opportunities. If the price of the stablecoin was noting significantly below the reference value, anybody could buy it cheaply, redeem against the basis value and complete an easy gain. If the price were above, anybody could create stablecoins using the underlying fiat currency and sell it with a win.

It is important to mention that even dramatic price drops of cryptocurrencies should not have a big influence on cash-collateralised stablecoins, so if 'stormy weather 'is expected on the cryptocurrency markets, it could be a good idea to use those kinds of stablecoins as a temporary 'safe haven'.

Buyers of those coins are, however, facing the issuer risk. Those kinds of protocols are not decentralised. Theoretically, the issuer could take the money and run away. It is also important to mention that there is not currently easily accessible cash-collateralised stablecoin issued by any central bank or by any important financial institution from the private sector. It seems as if these institutions believe that there is a conflict of interest between their business models and decentralised systems. It will be very interesting to observe the future developments of this matter.

2.2. Commodity-collateralised Stablecoins

Commodity-collateralised stablecoins have the backing of different types of interchangeable assets, such as precious metals, oil or real estate. The most common commodity used as collateral for commodity-backed stablecoins is gold. They make it possible for anyone in the world to invest in precious metals such as gold.

Generally, the issuers of such stablecoins usually promise to keep the amount of the basis value in their safe boxes or in their investment accounts in the form of financial instruments like futures.

The trust if the issuer is really keeping the amount of underlying commodity in their safe boxes is very important. 'Bank runs 'should not be a problem in such a case. They should also be resistant to price drops on the cryptocurrency markets and could be used as temporary 'safe havens'. The holder of those coins also face significant issuer risks.

2.3. Crypto-collateralised Stablecoins

Crypto-collateralised stablecoins are backed by other cryptocurrencies. Because the reserve cryptocurrency may also be prone to high volatility, the larger number of cryptocurrency tokens is maintained as a reserve for issuing a lower number of stablecoins.

For example, one Ether worth 2,000 USD may be held as reserves for issuing 1,000 USD worth of crypto-backed stablecoins, which results in a collateralisation level of 200%.

The challenge for crypto-collateralised stablecoins is to maintain the collateralisation level above 100%, even if a market faces significant price changes. Following the example, if the price of Ether dropped from 2,000 USD to 500 USD, the collateralisation level would fall under 100% to 50%, and thus issued stablecoins would no longer be backed by the required amount of cryptocurrency. It would not be possible to maintain the 1:1 exchange rate to the pegged currency in such a case. The overcollateralisation should make those kinds of coins resistant to 'bank runs'. In case a large number of people want to sell them and the price falls, it would create arbitrage opportunities for stable coin creators to buy those coins with a low price and redeem their collateral cheaply from the protocol.

Considering the high level of decentralisation where no one can take the collateral and run away, some consider those kinds of coins more safe than cash collateralised because there is no issuer risk.

There are, however, additional risks. The business logic of smart contracts controlling the protocols are complicated and the continuous target of hacker attacks. Such attacks have caused significant losses to various protocols and its users over the last few years. The following page provides an overview on the subject: https://rekt.news.

Price drops on cryptocurrency markets can also cause serious problems for crypto-collateralised stablecoin protocols. In the case of a significant price reduction of the collateral, many protocols attempt to liquidate that part of the collateral, which could cause the under-collateralisation of the protocol and burn stablecoins covered by it. The problem is that the collateral liquidation is usually performed with time-consuming activities, like auctions or sell-offs. During that time, the price of the collateral can sink further, causing the stablecoins to be uncovered and losses which need to be covered by someone if the reputation of the protocol should remain intact.

2.4. Algorithmic Stablecoins

Algorithmic or non-collateralised stablecoins do not have any assets or collateral backing them. They follow an algorithm for controlling the stablecoin supply. With the rise in demand, new stablecoins will be created to reduce the price to the normal level. In the event of considerably low demand, coins on the market are purchased up and destroyed in order to reduce circulating supply and increase the price. Basically, algorithmic stablecoins could offer stability according to the tenets of market supply and demand. In addition, it is also important to note that algorithmic stablecoins feature the highest level of decentralisation and independence. On the other hand, they require continual growth for ensuring success. There is no collateral or any guarantor involved with algorithmic and anyone can lose their money in the case of a 'bank run'.

I think that algorithmic stablecoins would suit central banks very well if any of them decide to play a bigger role in the crypto world. Central banks create money without collateral based on market supply and demand, and they are the guarantor by definition.

3. STABLECOIN IMPLEMENTATIONS

3.1. Tether USDT

Tether is the most known cash-collateralised cryptocurrency, whose tokens in circulation are supposed to be backed by an equivalent amount of USD. It is pegged to one USD. It was launched in 2014, and as of November 2021, USDT is the fourth-largest cryptocurrency by market capitalisation, worth more than 73 billion USD:

#	Coin		Price	1h	24h	7d	24h Volume	Mkt Cap
☆ 1	Bitcoin	BTC	$54,428.80	-0.6%	-8.2%	-4.5%	$41,060,872,468	$1,027,820,235,224
☆ 2	Ethereum	ETH	$4,078.83	-0.7%	-9.5%	2.1%	$29,391,505,714	$483,409,044,320
☆ 3	Binance Coin	BNB	$586.57	-1.2%	-8.9%	10.5%	$4,055,164,565	$98,624,776,481
☆ 4	Tether	USDT	$1.00	-0.4%	-0.1%	-0.2%	$99,910,621,690	$73,551,120,178

Tether is mostly used by crypto investors who want to avoid the extreme volatility of other cryptocurrencies while keeping value within the crypto market. There is a lot of controversy around Tether because of the lack of transparency. In April 2019, US authorities accused Tether's parent company of hiding an 850-million-USD loss. Eventually, the losses were covered while the company claimed that the missing amounts were not lost but were seized and safeguarded. The explanation does not seem to have any serious basis, but on the other hand, crypto-companies are learning fast that smooth cooperation between themselves and various authorities is crucial for their existence. No serious legal problems have been mentioned for other stablecoins recently launched with big market capitalisation like USDC or BUSD.

3.2. Digix Golds DGX

Digix Golds is the most common example of commodity-collateralised stablecoin. It is an ERC-20 token developed on the Ethereum blockchain with the backing of physical gold. It pegs one DGX against one gram of gold. The gold remains in reserve in Singapore while undergoing audits for a period of three months to ensure transparency. Users have the flexibility of redeeming physical bars of gold by visiting the reserve in Singapore.

3.3. DAI Stablecoin & MakerDAO

Dai is a crypto-collateralised stablecoin which aims to keep its value as close to one USD as possible through an automated system of smart contracts on the Ethereum blockchain. The protocol is described in detail in the white paper: https://makerdao.com/en/whitepaper or in the MakerDao documentation: https://docs.makerdao.com.

I provide the summary and the most important aspects of the protocol:

- The system consists of two tokens, MKR (governance token) and DAI (stable coin token). The MKR is distributed among investors, giving voting rights to holders if risk parameters of the system need to be adjusted or strategic decisions need to be made.
- A different type of collateral for DAI is accepted provided it is approved by the majority of MKR holders.
- The balance of collateral assuring the stability of the system is managed using collateral auctions where bidders compete with DAI for the outstanding collateral. One DAI must always be covered by at least one USD worth of collateral. If not, the deficit is booked in the system as debt.
- The debt is managed using debt auctions where bidders compete with decreasing 'amount requests' of MKR. MKR are newly minted in such a case and so the value of existing MKR tokens decreases. MKR holders want to avoid such a situation and try to provide the whole system with risk parameters which assure its stability.
- Profits earned via stability fees paid by DAI creators and liquidation penalties are distributed using surplus auctions where bidders compete with increasing amounts of MKR for DAIs earned by the protocol. MKR bought during the auction are burned and so the value of outstanding MKR tokens increases. It works like a share buyback program and MKR holders profit from it.
- For the creation of DAI and monitoring the quality of the collateral, prices are required for every type of the collateral. Oracles are used to input price information into the system.

The MakerDao protocol has proved to work fine even in difficult market conditions. Around 6 billion DAI have been created by now. It should be resistant to 'bunk runs 'as long relevant risk parameters are conservative enough. In the case of rapid price drops of underlying collateral, it is the owners of MKR governance tokens who pay for the losses, so it is in their interest to keep the whole system in balance. It is the only noncash-collateralised stablecoin, which is widely accepted by market participants. However, it should be mentioned that the protocol periodically faces serious problems.

The DAO was hacked in 2016 due to vulnerabilities in its code base and around 50 million USD worth of collateral was stolen. The Ethereum blockchain was eventually hard forked to restore the stolen funds, but not all parties agreed with this decision, which resulted in the network splitting into two distinct blockchains: Ethereum and Ethereum Classic.

This year on March 12, 2021, a massive crypto sell-off saw the price of ETH fall 43% from 194 USD to 111 USD. It was the largest ever loss in a single day. This sell-off triggered unintended consequences for the MakerDAO ecosystem. It sent the Maker system into chaos as 4.5 million USD worth of DAI was left unbacked by any collateral, and users lost millions.

The MakerDao problems show that the design and implementation of any kind of stablecoin protocol is a challenging undertaking and must be a subject of continuous monitoring and improvement.

3.4. Liquity

Liquity is another crypto-collateralised stablecoin pegged to the USD, which unlike DAI and MakerDao protocol is decentralised even further. No governance token enabling voting and adjustment of any risk parameters is involved in the system. All parameters are adjusted by the smart contract. The protocol is relatively new - launched in 2021 by a team operating from Switzerland. The stablecoin token LUSD has already accumulated almost 1 billion USD worth of value. The protocol is described in the detail on the following page: https://docs.liquity.org. I provide a summary:

- The system consists of two tokens LQTY (shareholder token) and LUSD (stable coin token). The LQTY is distributed among investors and front-end developers. It gives no voting rights or any other possibility to influence the protocol.

- Only Ether is currently accepted as collateral. Anybody can create LUSD using Ether as collateral. Creators pay the creation fee and can keep the stablecoin as long as they wish. There is no interest rate designed in the protocol.
- The 'liquidation level' for collateral is set to 110%. In the case of collateral liquidation, financial resources from the 'stability pool' are first used. There are no auctions or any other time-consuming mechanism involved in the liquidation process.
- Anybody can participate in the 'stability pool' and stake their LUSD. If the value of collateral of any stablecoin creator falls below 110%, the collateral is proportionally distributed among the 'stability pool' participants. The LUSD coins from the 'stability pool' are burned in return. The inception for 'stability pool' participants is to get collateral worth more than their LUSD coins which are burned. For example, they get Ether worth 1080 USD and only 1000 LUSD are burned. In the case of very fast price drops, 'stability pool' participants can also face losses. They can, for example, get Ether worth 900 USD and lose 1000 LUSD.
- The overall collateralisation level of the protocol is also monitored. If it falls under 150%, collateral of the creators which falls under the same level of 150% is liquidated, even before falling under the default 110%. Liquidity protocol creators call it 'emergency liquidations'.
- In the case the 'stability pool' is empty, the liquidated collateral is proportionally distributed among stablecoin creators. They get the liquidated collateral and the debt calculated in LUSD. The creators of LUSD are the saviours of the last resort for the protocol.
- On the other hand, in the case of high demand and the price of the LUSD notes above 1 USD, the protocol adjusts creation fees in order to increase or reduce the inceptions for creating the stablecoin.
- LUSD can always be redeemed against one USD worth of collateral. The protocol this way ensures that the price of LUSD will not significantly fall under the level of one USD. The collateral is taken from creators with the lowest collateralisation level. They face unexpected liquidation in the case of redemption.
- LQTY token can also be staked in the protocol. LQTY stakers participate in the redistribution of 'creation fees'. They get something like dividends.
- Inceptions for front-end developers are also designed in the protocol. Any front-end developer can register in the protocol, get a unique ID and use it while calling protocol functions. They get rewards paid in LQTY tokens in return, and thus can maximise revenues.

I find the liquidity protocol implementation very interesting because of the high level of decentralisation and inception mechanisms, especially the one for front-end developers. They are able to liquidate collateral much faster than MakerDao, but in the case of a 'bank run' or significant price drops of Ether, it is the stablecoin creators who are going to cover the losses. I wonder if they have all read the documentation and are aware of that fact.

3.5. Basis & BasisCash

Basis, originally called Basecoin, was the most well-funded stablecoin startup. It secured 133 million USD in funding to build an algorithmic stablecoin in the year 2018. Founders explained that the project would use code to maintain price stability for its token in the same way the U.S. Federal Reserve does for the dollar. Finally, the project was closed and money returned to investors because of US regulatory hurdles that could not be overcome.

The whitepaper of the project describes the idea in detail:

https://www.basis.io/basis_whitepaper_en.pdf

I provide the summary:

- Basecoin should be pegged to the USD.
- No collateral is involved or collected.
- If the price of the coin notes above one USD, new coins will be minted and distributed among project participants and investors. Many of them will sell newly created coins and so the price will fall.
- If the price of the coin notes significantly below one USD, bonds promising later conversion to the stablecoin will be sold at an attractive price. Stablecoins acquired during the sale of bonds will be burned. The price of the basecoin will rise as a result of reduced supply.

- There is not specific mechanism described as to how the protocol should maintain the price of the coin at exactly one USD level. Creators of the document hope that swings between the coin noting above and below one USD will be small after the reputation of the protocol is well established and eventually the pegged price will be maintained automatically.

Analysing the idea of basis stablecoin, I have the impression that perhaps some people who invest their money do not read the whitepapers, or maybe they read and do not understand it, or it could be that some of them clearly see unique opportunities for early adopters and investors, even if they understand the project is very likely to fail. I am sure this kind of protocol would work fine if the U.S. Federal Reserve or any other central bank were backing it. Without a guarantor of that kind, it is just a‘ Ponzi scheme’. Anybody would like to be involved in a creation of a protocol where the price stabilisation mechanism means printing dollars for yourself and selling them on the market.

Later in the year 2020, a team of anonymous developers made a so-called fork of a basis.io project and called it Basis Cash. The price of the BAC coin exploded to the level of almost 160 USD after launching and dropped below one USD shortly after. In November 2021, it was noting at a level of 0.04 USD with very few transactions per day registered on Etherscan. Anybody who had doubts whether the basis.io was not a good idea until then had clear market verification. On the whole, the BAC stablecoin is anything but stable.

3.6. Ampleforth

Ampleforth is another example of an algorithmic Stablecoin pegged to the USD. There is no collateral backing up the minted stablecoins. The software programmatically adjusts the supply of its AMPL cryptocurrency every 24 hours in a process called ‘rebasing’. If demand for AMPL tokens is high, and each AMPL token exceeds one USD, the supply increases. If demand is low, supply decreases. In practice, anyone who owns AMPL tokens will see the balance in their wallets change each day. This means that if anybody holds 1% of all AMPL tokens before a rebasing event, they would still hold the same percentage of coins after the rebasing.

The idea is very interesting and more fair than in the case of the basis protocol described in the former chapter. It is owners of stablecoin tokens who are rewarded in the case of increasing popularity of the coin, and it is also they who suffer losses when demand decreases. In the case of a ‘bank run’, owners of those coins will eventually lose most of their money, but they will also get rich if demand increases. With a market capitalisation of above 300 million USD as of November 2021, the protocol seems to be well accepted by market participants. The biggest advantage is its level of decentralisation. There is no collateral that can be stolen, so nobody can perform an ‘exit scam’ while taking the money and running.

The problem with the design is that AMPL is actually not a stablecoin but something like a share whose price rises or falls depending on the popularity of the system. The price stabilisation mechanism also does not seem to work well. The price of the coin was noting between 0.5 and 2 USD last year:

3.7. Frax and Iron

Finally, I would like to provide an example of a FRAX protocol, which is a combination of cash, crypto and algorithmic stablecoin. Accepted collateral is USDC, USD based cash-collateralised stable coin, and FXS, a

token which is a part of the protocol itself. The idea of self-collateralisation is very interesting indeed. The protocol is described in the whitepaper: https://docs.frax.finance/ in detail.

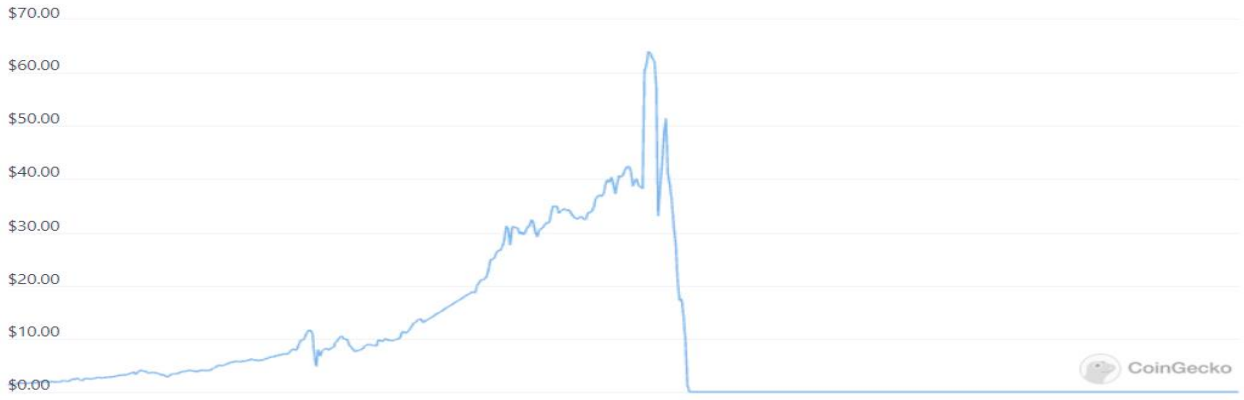
I provide a summary:

- The system consists of two tokens FXS (shareholder token) and FRAX (stablecoin token). The FXS is distributed among investors. It gives no voting rights or any other possibility to influence the protocol.
- The minting process uses a collateral ratio to create new tokens. In the case of a 50% collateral ratio, the individual would have to provide 0.5 USD worth of USDC and 0.5 USD worth of FXS to mint one FRAX. Delivered FXS is burned, which eventually increases its value.
- At any point in time, users can redeem one FRAX token for one USD worth of collateral. Assuming the collateral ratio is 50%, they can receive 0.5 USD worth of USDC and 0.5 USD worth of FXS for a single FRAX token. FXS tokens returned during redemption need to be newly minted, which is not a problem because FXS is part of the protocol and any required amount can be minted anytime.
- The protocol utilises arbitrageurs to safeguard its stable ratio against the USD. If the price of the FRAX token goes below one USD, anyone could buy it, redeem it and get USDC and FXS worth exactly one USD and generate revenue. The price of the FRAX token should rise in this case. If the price of FRAX goes above one USD, anybody could create it using collateral worth exactly one USD, sell it with a higher price on the market and generate an easy win. The price of the FRAX token should eventually fall to one USD level.

The idea of that FRAX protocol seems to be very clever. The FRAX token is easy to create, easy to redeem, and the described stability mechanism based on arbitrage possibilities should work fine because there are plenty of market participants waiting for them. The price of the FRAX token with market capitalisation of over 1 billion USD has been noting around one USD since it was launched. Finally, the price of the FXS token and its market capitalisation is constantly increasing and reached a level of 600 Mio USD as of November 2021.

This all looks like a success story, but there is one problem with the protocol. It works fine as long as everybody believes it will work fine. If its reputation is damaged because of any reason, users will first start to sell the FXS share token. The price of it will obviously fall, holders will also try to redeem FRAX tokens and save its collateral before it is too late. The problem is that part of the collateral is secured by FXS tokens which were burned during the creation process. FXS tokens will need to be newly minted before returned to FRAX owners. It will increase the amount on the market and create additional price pressure. The price of the FXS token would collapse if a 'bank run' occurs, and the FRAX token would only be worth as much as the underlying USDC collateral.

In fact, the scenario I described actually happened. TITAN together with IRON stablecoin is a protocol which is almost an exact copy of FRAX, and it faced a 'bank run' in June 2021. Its price reached a level of more than 60 USD as of 16 June 2021 and dropped to nearly zero USD one day after:



4. SWISS STABLECOINS IMPLEMENTATIONS

The Swiss Franc is a currency very much desired by investors. In the event of turbulence on international markets or crises of any kind, many funds are converted into Swiss Franc from other currencies. Obviously, it was just a matter of time until the creation of Swiss Franc based stablecoin. The situation is, however, complicated. Negative interest rates in Switzerland, currently -0.75% p.a., make creation of cash-collateralised

stablecoins unprofitable to its issuers. Owning a stablecoin with exactly one CHF is a winning business for the owner and a losing business for the issuer, provided the collateral collected in CHF is not exchanged to other assets. Exchanging CHF to other assets would increase the risk of the system and could cause regulatory issues. The negative interest rate environment may be the reason why two existing cash-collateralised CHF stablecoin implementations are not well established on the market. They cannot be bought on widely used exchanges, and I have the impression it is the intention of issuers to wait for interest rates that are more suitable for them.

Crypto-collateralised stablecoin projects, on the other hand, require a lot of resources with uncertain outcomes, and so there is currently not Swiss Franc based collateral stablecoin established on any crypto market. That kind of project would not only need a team of developers and analysts, but would also require taking legal issues into consideration right from the beginning.

The Swiss Financial Market Supervisory Authority FINMA published a supplement to its ICO guidelines outlining how it treats stablecoins under Swiss supervisory law:

https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf?la=de

Analysing FINMA's guideline one could have an impression that only cash-collateralised stablecoins fall under the definition of stablecoin, there are, however, other guidelines which need to be considered and require costly legal reviews.

The question if it is worth investing resources in the creation of a crypto-collateralised Swiss Franc based stablecoin has remained unanswered until now. The Swiss Franc is still considered a local currency, but it has proved to play a significant role in the global financial ecosystem over the last few years. Many market participants exchange currency to Swiss Francs in turbulent times in the 'real' world, and so I think many crypto market participants would do the same in a 'crypto' world.

4.1. Cryptofranc XCHF

The CryptoFranc (XCHF) is a cash-collateralised stablecoin bound to the Swiss Franc, issued by Bitcoin Suisse AG. It is implemented as an ERC-20 token on the Ethereum platform. Each XCHF token represents a claim of one Swiss Franc against the Bitcoin Suisse and is promised to be backed by a bank guarantee. There are only around two million XCHF tokens in circulation and their number is continually shrinking. Negative interest rates may be the reason why the issuer is not promoting its token.

4.2. Sygnum Bank DCHF

Sygnum, a regulated Swiss bank, announced in March 2020 the launch of a digital CHF Token (DCHF). For every settlement token minted in its customer accounts, Sygnum promises to hold the equivalent amount of CHF as collateral in the Swiss National Bank (SNB). The DCHF Token is also not traded on any major exchanges. It is not even possible to determine its current market capitalisation. Once again, negative interest rates are obviously the reason for its current lack of marketing and promotion.

5. BITCHF - PROOF OF CONCEPT

5.1. Introduction

BitCHF is a proof of concept for Swiss Franc based algorithmically crypto-collateralised stablecoin. The aim of bitCHF is to provide easily accessible, exchangeable and tradable crypto-currency which replicates the value of the Swiss Franc.

The stability of the exchange rate is provided with crypto-collateralisation and trading methods triggered algorithmically. The system is based on three types of financial instruments. The main token bitCHF is the crypto-currency. Share and convertible bonds are designed to provide investors with revenues and to control the price of the bitCHF currency as well. The price spread between buy and sell prices and small transaction fees provide additional collaterals to the system.

Collaterals backing up the value of the stable coin are collected with Ether. The protocol could be extended so some amount of collateral is exchanged to another USD or gold-backed stablecoin in order to reduce the risk of price drops of cryptocurrencies and the danger of under-collateralisation.

The prototype for bitCHF has been implemented in the Solidity programming language as an ERC20 token and launched on the Ethereum Rinkeby test blockchain. It is accessible to all and ready for evaluation:

5.2. System Architecture

5.2.1. Financial instruments

- bitCHF currency - crypto-currency which replicates the value of the Swiss Franc currency.

Designed as an exchangeable and tradable ERC20 token.

- bitCHF share - token for investors which periodically distributes dividends

Designed as an exchangeable and tradable ERC20 token. Shares may be sold during ICO. The holder of the share has the right to periodically collect dividends. The amount of the dividend is dependent on the collateralisation level.

- bitCHF convertible bond - asset designed to help control the price of the cryptocurrency

Designed as an exchangeable and tradable ERC20 token. If a significant price drop occurs, the contract sells bonds with a discounted price paid in bitCHF and the collected bitCHF coins are destroyed. When the price is back to the target value of 100%, the holder of the bond can convert the bond to bitCHF with the nominal value of 100% and gets some amount of shares as an additional reward.

5.2.2. Money Pools

All financial resources in the protocol are divided into money pools:

- Collaterals : 90% of all income

Financial resources backing up the value of the stable coin

- Investments

Financial resources collected during the ICO (Initial Coin Offering)

- Operations : 5% of all income

Financial resources securing the system maintenance and development of the protocol

- Dividends : 5% of all income

Financial resources paid back to the shareholders

5.2.3. Financial Incomes

- Selling, buying bitCHF with spread

The system is constantly selling bitCHF at a price of 102% of CHF. On the other hand, the system buys back bitCHF at a price lower than 98% of CHF. The spread between buy and sell price provides additional financial value to the system.

- Tax on dividends 20%

Dividends are paid in bitCHF, but collecting dividends are taxed with Ether (20% in the demo version). For example, the dividend money pool is not empty and dividends are distributed (once a week in the demo version). Let's say the shareholder is eligible for 100 bitCHF of dividends. They will have to pay 20 CHF (0.2 * 100) in Ether in order to collect the dividend.

- Tax on bonds conversion 20% of the gain

In the case that the price returns to 100% after a drop and the holder of a dividend is eligible for converting the bond to bitCHF and share, the tax of 20% in Ether is paid during the conversion process. For example, if the price drops to 90%, the user can buy a bond at a discounted price of 70%, which is 63% (0.7*90%). In the case that the price comes back to 100%, the bond holder earns 37%. The win is taxed at a rate of 7.4% (0.2 *37%) during the conversion process and is to be paid in Ether.

5.2.4. Price Stabilisation Methods

- Increasing price

The system is constantly selling bitCHF at a price of 102% CHF. Arbitrage possibilities ensure that the price does not significantly exceed the level of 102%.

- Falling price

Based on the Quantity Theory of Money, which ties long-run price levels to the supply and demand for money, the system reduces the amount of bitCHF in the case of price drops. The system monitors not only the price but also the trading volume. When the price drops, under 98% of CHF and the trading volume is relatively small,

the system buys bitCHF at a price 5% higher than the current market price using its collaterals. In the case of price drops accompanied by relatively big trading volume, the system sells convertible bonds. All bitCHF coins collected by the system are destroyed and so the supply of bitCHF is reduced, which causes a rise in the price. Trend monitoring methods from technical analysis like MACD (Moving Average Convergence Divergence), RSI (Relative Strength Index) or VPT (Volume Price Trend Indicator) could additionally be used to find the optimal number of coins to buy, number of offered convertible bonds and related price discounts. In the long run, when historical data are available, AI (Artificial Intelligence) algorithms can be implemented in order to find the best parameters.

5.3. External Interfaces

5.3.1. Blockchain Oracles

Blockchains and smart contracts cannot access off-chain data (data that is outside of the blockchain network). Third-party services called "blockchain oracles" usually provide smart contracts with external information. Essentially, they serve as bridges between blockchains and the outside world. For many contractual agreements, it is vital to have relevant information from the outside world to execute the agreement.

There are various types of oracles, which are vital within the blockchain ecosystem because they broaden the scope in which smart contracts can operate. Without blockchain oracles, smart contracts would have very limited use, as they would only have access to data from within their networks. Since smart contracts execute decisions based on data provided by oracles, they are key to a healthy blockchain ecosystem. The main challenge with designing oracles is that if the oracle is compromised, the smart contract relying on it is also compromised. This is often referred to as 'The Oracle Problem'.

5.3.2. Exchange Rate ETH/CHF

Chainlink Data Feeds have been used in order to add ETH/CHF into the protocol. It creates an easy way to connect smart contracts to the real-world market prices of assets. It provides ETH/USD and CHF/USD exchange rates so that the ETH/CHF exchange rate required by the bitCHF protocol can easily be calculated:

$$\frac{ETH/USD}{CHF/USD} = ETH/CHF$$

Using Chainlink Data Feeds eliminates the necessity of implementing one's own Blockchain Oracle, but it creates a strong dependency. If the Chainlink Data Feeds happens to be compromised, all protocols using it will face serious security issues and likely financial losses.

The list of all available exchange rates currently provided by the Chainlink Data Feeds:

https://docs.chain.link/docs/ethereum-addresses#mainnet

Chainlink also provides guidelines and tools for code integrations:

https://docs.chain.link/docs/get-the-latest-price

For the purpose of bitCHF protocol, the smart-contract Solidity integration mechanism provided by Chainlink has been used:

https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/blob/main/AggregatorV3Interface.sol

5.3.3. bitCHF price Information

The current price of the bitCHF stablecoin is crucial to the protocol. The price is used to activate a bond selling campaign in the case the price drops under an acceptable level or in order to trigger Bond conversions to bitCHF in the case the price reaches the one CHF level again.

Usually price information of the stablecoin is also provided by Blockchain Oracles and based on information from exchanges where the crypto-asset is traded. The bitCHF prototype has only been launched on the test Blockchain and so no price information from the exchanges is available.

For the purpose of testing, a price simulator has been implemented. The price changes every minute and oscillates between 97% and 103% of CHF.

5.4. Smart-Contract Implementation

BitCHF protocol has been implemented on the Ethereum Platform. Solidity has been used as a programming language. The source-code repository is public and accessible for anyone for review or inspiration:

https://github.com/stablecoinchf/CHF-Stablecoin_Solidity

The goal is not to provide a detailed analysis of the source code, so here I simply list the most important components of the system:

- Generic ERC20 Ethereum standard implementation. The code was developed by the OpenZeppelin organisation, which provides open-source solutions to build, automate, and operate decentralised applications:

  https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/blob/main/ERC20.sol

  ERC20 is the most widespread token standard for fungible assets. It defines the functions balanceOf, totalSupply, transfer, transferFrom, approve and allowance. It also has a few optional fields like the token name, symbol, and the number of decimal places with which it will be measured.
- StableCoin.sol - stable coin implementation of ERC20 Ethereum standard:

  https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/blob/main/StableCoin.sol
- BondCampaign.sol – smart contract responsible for managing convertible bond campaigns:

  https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/blob/main/BondCampaign.sol
- DividendCampaign.sol – smart contract responsible for managing dividend pay-outs:

  https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/blob/main/DividendCampaign.sol
- Prices.sol – library used to determine the ETH/CHF exchange rate and the price of the bitCHF stablecoin. It uses Chainlink Data Feeds to get exchange rates. The price of bitCHF cannot be determined because it is not traded on any exchange, and thus a price simulator has been implemented:

  CHF-Stablecoin_Solidity/Prices.sol at main · stablecoinchf/CHF-Stablecoin_Solidity (github.com)
- AggregatorV3Interface.sol – interface provided by Chainlink in order to use the Chainlink Data Feeds

  https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/blob/main/AggregatorV3Interface.sol
- SafeMath.sol – library provided by OpenZeppelin which ensures the security of mathematical operations.
- Unit tests:

  https://github.com/stablecoinchf/CHF-Stablecoin_Solidity/tree/main/tests

  Smart contracts are not upgradable or immutable. In some cases, they can be migrated to another version, but the migration process can be complicated, costly and risky. It is, therefore, very important to follow test-driven development principles while implementing any code in order to avoid costly bug-fixing procedures. Unit tests created during development of bitCHF can be executed on the web based development platform Remix: https://remix.ethereum.org/.

5.5. Smart-Contract Interface

The bitCHF Protocol implements the ERC20 Ethereum standard, which is the most widespread token standard for fungible assets. Additional functions have been implemented as an extension in order to provide bitCHF specific functionalities.

The list of bitCHF protocol functions provided as ERC20 standard implementation:

Function	Description
function totalSupply() external view returns (uint256)	Returns the amount of tokens in existence.
function balanceOf(address account) external view returns (uint256)	Returns the amount of tokens owned by the *account*.
function transfer(address recipient, uint256 amount) external payable returns (bool)	Moves *amount* tokens from the caller's account to the *recipient*.

function allowance(address owner, address spender) external view returns (uint256)	Returns the remaining number of tokens that the *spender* will be allowed to spend on behalf of the *owner* through the transferFrom() function. This is zero by default.
function approve(address spender, uint256 amount) external returns (bool)	Sets *amount* as the allowance of the *spender* over the caller's tokens.
function increaseAllowance(address spender, uint256 addedValue) public virtual returns (bool)	Atomically increases the allowance with *addedValue* granted to the *spender* by the caller. This is an alternative to the approve() function.
function decreaseAllowance(address spender, uint256 subtractedValue) public virtual returns (bool)	Atomically decreases the allowance with *subtractedValue* granted to the *spender* by the caller.
function transferFrom(address sender, address recipient, uint256 amount) external payable returns (bool)	Moves *amount* tokens from the *sender* to *recipient* using the allowance mechanism. The *amount* is then deducted from the caller's allowance.
function name() public view returns (string memory)	Returns the name of the token.
function symbol() public view returns (string memory)	Returns the symbol of the token, usually a shorter version of the name.

The list of bitCHF protocol functions provided as an extension to the ERC20 standard:

Function	Description
function buyCoin(uint amount) external payable returns (bool)	The function enables the purchase of the stablecoin against Ether.
function sellCoin(uint amount) external returns (bool)	The function enables the sale of the stablecoin. Ether is paid back in return.
function buyShare(uint amount) external payable returns (bool)	The function enables the purchase of the share token against Ether. One share and ten bitCHF are returned.
function isDividendAvailable() external view returns (bool)	Information if any dividends are available for shareholders. If it is so, they can call the getDividend() function and collect them.
function getDividend() external payable returns (bool)	The function allows shareholders to collect dividends if any are available.
function buyBond(uint amount) public returns (bool)	The function allows the purchase of convertible bonds if any are available, paying with bitCHF. Bonds are only available if the price of the bitCHF falls below the accepted level.
function convertBond() external payable returns (bool)	The function enables the conversion of bonds to bitCHF and the collection of share rewards in the case the price of bitCHF returns to one CHF.

function isBondHolder(address bondHolder) public view returns (bool)	The function returns the information if a user has any convertible bonds.
function getBondAmount(address bondHolder) public view returns (uint)	The function returns the number of convertible bonds in the possession of the user.
function isShareHolder(address shareHolder) public view returns (bool)	The function returns the information if a user has any shares.
function getShareAmount(address shareHolder) public view returns (uint)	The function returns the number of shares in the possession of the user.

5.6. bitCHF smart contract installation

The prototype of bitCHF has been launched on the Ethereum Rinkeby test Blockchain, and is accessible for everyone and ready for evaluation. Interaction with the smart contract on the Rinkeby test Blockchain does not require any financial resources. Test ether required on that Blockchain can be collected for free using following 'faucet', for example:

https://faucet.rinkeby.io/

The address of the smart-contract on the Rinkeby test Blockchain:

0x1076b9bFFC790fbcec10c32f7F67a76CE925BCbF

All bitCHF smart-contract activities can be followed on the Etherscan:

https://rinkeby.etherscan.io/address/0x1076b9bFFC790fbcec10c32f7F67a76CE925BCbF

5.7. bitCHF Front-End Implementation

The name 'smart contract' can be considered a misnomer. It is not a contract and it is only as smart as the source code implemented by the developer. The name is strongly misleading and confusing, but creates some kind of mystery around it, and so from the marketing point of view can be considered a huge success.

A smart contract is just a piece of code deployed on a decentralised platform providing functions which facilitate interactions with the platform. Smart contracts can be considered web-services, enabling interactions with decentralised ledgers. Implementation of user interfaces is not necessary. In many cases, projects provide just the smart contract and interface specifications, leaving front-end implementations to third parties. The advantage of that approach is obviously the fact that any front-end installation must be placed in the off-chain world and can be targeted by authorities or any legal actions. In an extreme case, front-end installations can be closed or mobile apps can be removed as a result of legal actions, while smart-contracts may stay installed 'forever' if they are designed so. No authorities or any other organisations can force them to be closed.

Web or app user interfaces play, however, an important role because all users cannot be expected to write code in order to interact with the smart contract installations. Smart contract user interfaces are called dApps (decentralised applications).

I have implemented a dApp which interacts with the bitCHF protocol on the Rinkeby test Blockchain in order to make testing of the protocol possible. The dApp provides an overview of all protocol and user balances of Ether, bitCHF, bonds and shares. It also facilitates the creation of bitCHF stablecoins, sells them back to the protocol, buys shares and convertible bonds and converts bonds back to the bitCHF if the price level allows it.

The dApp for bitCHF is accessible with the following URL:

https://stablecoinchf.github.io/dapp.html

The bitCHF dApp has been implemented using the JavaScript programming language. The source-code repository is public and accessible for anyone for review or inspiration:

https://github.com/stablecoinchf/CHF-Stablecoin_Front

The aim of the assignment is not to analyse the source code of dApp implementation. I will just mention that the interaction with the bitCHF smart contract has been implemented using open source web3.min.js library, which is currently the implementation standard:

```
<script type="text/javascript" src="./web3.min.js"></script>
```

An example of the source code using the web3 library, which interacts with the bitCHF smart contract and enables the purchase of the specific number of bitCHF coins (*noOfCoins*), provided the caller of the function has a sufficient amount of Ether to pay for the coins (*transactionPrice*) and to pay for gas fees (*gas: 3000000)* available in his account:

```
…
var transactionPrice = (priceCHFETH * coinPriceCHF * noOfCoins) * 10000000000;
noOfCoins = web3.utils.toWei(noOfCoins, 'ether');
await sc.methods.buyCoin(noOfCoins).send({ from: account, gas: 3000000, value: transactionPrice});
..
```

5.8. bitCHF Summary

The bitCHF prototype is an exercise implemented during the preparation for the CAS Blockchain at the University of Zurich in 2021.

The strength of the protocol is an easy way to create stablecoin. No complicated collateral management is required. There is no doubt that the design ensures that the price of the bitCHF token will not rise significantly above one CHF because of arbitrage possibilities. It is difficult to speculate if the stability algorithm would prevent a price drop below one CHF successfully. It should also be mentioned that price changes of the underlying collateral Ether can influence the collateralisation level and stability of the protocol. I suppose it is the kind of protocol which would work fine as long as enough people believe in it. In the case of a ‘bank run’ and drop of collateralisation level caused by decreasing Ether prices, the system would eventually fall apart.

6. SUMMARY

Overall, various types of stablecoins have been implemented in an attempt to make cryptocurrencies less volatile. Some of them, like Tether or DAI, are relatively successful with relatively large market capitalisation. Also, some of them, like Ampleforth, are particularly interesting but will probably play a minor role in the future. I have also described some projects like Basis.io or TITAN which failed because the design inaccuracies were painfully verified by market participants. Additionally, the reasons for the absence of well-established Swiss Franc based stablecoin have been analysed. Finally, with an attempt to implement the algorithmically crypto-collateralised stablecoin bitCHF on the Ethereum platform, I have described challenges of such a solution, and while making the source code public, I have provided some simple guidelines for such undertaking.

We live in a dynamic world that is changing at unprecedented speed. It takes years for changes which previously required decades. Thus, it is not impossible to predict the future. Decentralised finance and stablecoins as part of it will most probably play a major role in the transformation of the current financial system. Many financial institutions, authorities and regulators worry that stablecoins pose a risk to the financial system, so they slow down the overall transformation process. It may, however, be that we will see a stablecoin or some other kind of easily transferable digital money backed by a respectable institution like the central bank of a major country in the near future. In my opinion, the question is not if but when. Who will be the first? The answer may be surprising. It looks like China with their e-CNY is playing the long game and is several moves ahead of any other major economy. China’s immediate focus seems to be domestic. However, earlier this year, Huawei introduced into the African market a smartphone with a pre-installed e-CNY wallet. It appears that China’s secondary focus may very well be Africa, with an eye towards disrupting the global financial system. What will be their next steps if they succeed? Will institutions of developed countries react soon enough before they are overtaken? They will not be able to shut down the Chinese project as they did in case of Facebook’s Libra, which was another attempt at an easily accessible and transferrable crypto stablecoin pegged to the basket of currencies of major economies. There is no doubt that Libra had potential to change the current financial system dramatically.

On the whole, I am very curious how the financial landscape will look in the near future.

7. REFERENCES

MakerDao whitepaper : https://makerdao.com/en/whitepaper

MakerDao documentation : https://docs.makerdao.com

Liquity documentation : https://docs.liquity.org

Basis.io whitepaper : https://www.basis.io/basis_whitepaper_en.pdf

Chainlink Data Feeds documentation: https://docs.chain.link/docs

FINMA Stablecoin guidelines: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf?la=de