Autonomous secure dollar (USSD) white paper

David Lee davidleechaum@proton.me

October 4, 2023

Abstract

The Autonomous Secure Dollar (USSD) is an open-source protocol designed for creating an autonomous ERC20 stablecoin. It is pegged to the US dollar and has a multiple times collateralization ratio, ensuring long-term stability. The USSD protocol only consists of cryptoassets and has no ties to any physical-world financial instruments such as banks or treasuries.

It has been designed to be censorship-resistant, ensuring that it can remain operational without interference.

Contents

1 Introduction

1.1 Concept of Autonomy and Safety

To make a significant contribution to the crypto economy's freedom and independence, a new secure and autonomous stablecoin is required to minimize the risks associated with centralization and crypto market volatility.

Existing stablecoins are susceptible to the following risks due to their strong connection to the traditional financial system, which is unpredictable:

1. Risks due to centralization:
   (a) Stable tokens can be banned/frozen, or the address can be blacklisted by authorized actors.
   (b) The creators of stablecoins can be influenced using legal or other means.
   (c) Some functions of stablecoin tokens might stop working if the project team stops supporting the project, such as collateral re-balancing or mint/redeem for centralized stables.
   (d) Collateral containing cash/treasuries or other stablecoins that include cash/treasuries can collapse due to various situations in the banking system or financial regulation issues.
2. Risks due to crypto market unpredictability and volatility:
   (a) A stablecoin might collapse if its internal business model operates incorrectly. Dependency on the internal business model makes its behavior much more unpredictable, for example:
      - For continuous support, a stablecoin project team needs funds. Thus, it needs revenue generation in some form. For USDT/USDC and other stablecoins backed by cash/treasures, it is the interest returned from deposits and treasury bond yields. For DAI and other stablecoins backed by crypto assets, the revenue is fees and commissions from lending and borrowing.
   (b) Collateral containing crypto assets can depreciate in value due to a decline in the crypto market. If the crypto market is down significantly, it can unpeg a crypto-backed stablecoin from USD.

The USSD stablecoin aims to avoid the risks associated with existing stablecoins by implementing the following features:

1. No methods for freezing, blacklisting, banning or pausing transfers are implemented in the smart-contract. The goal is to make the USSD stablecoin completely unstoppable.
2. USSD is a non-profit, long-term project that exists autonomously without any connection to physical entities. Only code is used, making it non-biased and secure.

Table 1: Comparison of stablecoin features

	USDT	**USDC**	**BUSD (USDP)**	**DAI**	**USSD**
Transparency	based on auditor reports[1]	by paper proof[2]	by paper proof [3]	by code[4]	by code
Source of collateral	short-term US treasuries, cash, etc.	short-term US treasuries, cash in US banks	short-term US treasuries, cash in US banks	crypto-backed (including USDC)	crypto-backed (including DAI)
Collateral ratio	claimed as 100%	100%	100%	~147%	~500+%
Regulatory status	Hong Kong entity	US entity	several entities	US entity	no entity
Centralization level of token management	team can freeze tokens	team can freeze tokens	team can freeze tokens	team can freeze collateral	no-one can freeze tokens
Project Management	centralized, manual	centralized, manual	centralized, manual	DAO managed, manual	autonomous
Business model	US treasuries yield	US treasuries yield	US treasuries yield	collateral service fees	non-profit

3. The architecture of the USSD stablecoin is designed to be autonomous. In the long-term, the operation of the USSD stablecoin would not be dependent on any person.

4. Since the USSD protocol operates independently of any business model, it eliminates the risks associated with the bankruptcy of such models.

5. USSD contains only cryptoassets with no connection to cash in banks or any other traditional financial instruments in the physical world, even low-risk ones.

6. USSD's collateral structure is designed to maintain a collateral to capitalization ratio of more than 10x.

7. The USSD smart contract is deployed on the Ethereum main network because it is the most common and trusted decentralized network that allows the building of a smart contract.

[1] https://tether.to/en/transparency/#reports
[2] https://www.circle.com/en/usdc#transparency
[3] https://paxos.com/busd-transparency/
[4] https://github.com/makerdao

Stablecoins with the largest market capitalization (like USDT / USDC / BUSD / USDP and others) are backed by dollar-evaluated collateral with a 1-to-1 ratio. Issuers of such stablecoins provide documents that are issued by trusted authorities (auditors). Nevertheless, we consider these proofs as paper-proof that contains risks due to their centralized nature, which could be affected by corruption, human mistakes, and political influence.

At the moment of writing, the DAI stablecoin is the largest, most secure, and widespread decentralized stablecoin in the market. DAI's collateral (crypto assets) is evaluated at a 147% ratio to its market capitalization. Nevertheless, DAI stablecoin collateral has some notable nuances that bring risks to it (and some of them have already been realized):

- DAI's collateral contains a major share of USDC stablecoin (74% of DAI's capitalization in April 2023), which is a cash/US treasuries-backed coin and is regulated by US financial authorities. This means collateral risks of the USDC are also valid for DAI (in March of 2023, DAI depegged from USD because USDC depegged too due to a bank issue, luckily the situation recovered later).
- USDC (a part of DAI's collateral) and some other stablecoins have an option of freezing funds (which makes them insecure).
- Both DAI and USDC have legal entities in the US and are obliged to comply with all regulator requirements, making them susceptible to influence.
- DAI contains a lending/borrowing protocol as a business model to support its existence, which makes the whole system more complicated, fragile, and dependent on the results of this business operating.

1.2 Timing

The period from 2022 to 2023 is regarded as a "crypto-fall" or "crypto-winter" time, during which the valuations of most crypto assets are low. Hopefully, this period will end soon, and the entire crypto market capitalization will increase by 3-5 times or more, as it has happened several times before. To achieve a high overcollateralization ratio, the USSD stablecoin was created during this time.

2 Collateral structure

The ideal crypto collateral structure should be robust enough to maintain a collateral factor of over 100% even in harsh scenarios, such as an overall crypto market downturn, a 70-90% depreciation of BTC/ETH, or even the complete depreciation of one of the crypto assets included as collateral. Due to the high volatility nature of crypto, we have decided to form a collateral structure that will:

1. Diversify using the most common and trusted crypto assets, namely BTC and ETH.

Table 2: Collateral buying proportions

	Collateral buy proportion	First flutter	Second flutter	Third flutter	Fourth flutter	Ultimate mode
DAI	25%	0.25x	0.35x	1x	0.8x	0.25x
wETH	25%	2x	4x	5x	6x	More 10x
wBTC	25%	2x	4x	5x	6x	More 10x
wBGL	25%	10x	20x	50x	100x	More 500x

2. Include DAI as part of the collateral to enhance usability and liquidity in USSD stablecoin. DAI was selected as the safe and decentralized stablecoin in the market at the time of USSD creation.

3. Use the most decentralized blockchain that supports smart-contracts, namely the Ethereum Mainnet.

4. Include a radical element in the collateral structure, namely the BGL (Bitgesell) coin, which is deflationary and has a small capitalization (at the time of writing). It was included in the collateral to overcome collateral fluctuations in the first period of USSD adoption and to increase collateral upside in the long run.

5. Have a flexible structure that changes with time and the market capitalization of the collateral. The overall goal of the model is to accumulate collateral amounts that are at least 100% of the DAI and more than 10 times the crypto assets (BTC and ETH).

Overview of the last two collateral component attributes.

BGL (Bitgesell) is a well-developed fork of Bitcoin with many parameters that remain the same, such as limited supply (21 million), but with the additional mechanics of burning 90% of the transaction fees and having block reward halving every year. It is running on its own blockchain, which is very similar to Bitcoin. The reasons for selecting BGL as a part of collateral are:

- Based on a proven code with similar blockchain safety as Bitcoin
- More coin scarcity in the long run compared to Bitcoin
- Small market cap that has significant upside potential

To grow and fix the share of DAI in the collateral structure, we have developed a roadmap for USSD collateral development (see Table 2). Once the share is fixed, the collateral structure will be locked forever to prevent any changes.

In the event of a decline in the USSD price, the algorithm for selling collateral to maintain the peg at 1 USD is as follows: DAI will be sold first, followed by wETH, then wBTC, and finally, wBGL.

3 USSD Supply management

USSD coin is 'initialized' with one-time minting of 1000 USSD, taking 1000 DAI as collateral. This 1000 USSD would allow to create a pool USSD/DAI to have initial liquidity. Uniswap V3 is selected as DEX of choice on Ethereum for being largest in volume and long-time reliable solution for on-chain swaps. As the pair is consisting of two stablecoins, the minimal fee tier (0.05%) is used. Initial liquidity equation at the whole price range would be:

$$P_{USSD} \cdot P_{DAI} = 1,$$

assuming equal price of USSD and DAI as a regular AMM curve that should fit the purpose of price discovery. Other curve variants, such as constant price () or Stableswap invariant (https://classic.curve.fi/files/stableswap-paper.pdf) serve different purposes (e.g. to prevent slippage when having a pool of stablecoins, even with significant different in their amounts).

The pool is used for price discovery of USSD, avoiding the necessity to use any off-chain oracles to keep USSD as autonomous as possible. For protection against flash-loan or liquidity manipulation geometric mean price oracle from Uniswap V3 is used (https://uniswap.org/whitepaper-v3.pdf):

$$P_{t1,t2} = 1.0001^{\frac{a_{t2}-a_{t1}}{t_2-t_1}},$$

where t2 and t1 are define interval in seconds, and at1, at2 define accumulator values. The length of the interval could be fine-tuned, making the assumed price less susceptible for short-term fluctuations (and liquidity/loan attacks), gaining some latency, but spending less gas overall on rebalancing operations.

The main way to obtain the USSD would be buying it on the USSD/DAI pool, this would increase the price of USSD in comparison to DAI. In such scenario, two outcomes are possible: the price is arbitraged back (and nothing changes to the supply) or USSD rebalances itself, minting USSD and selling it for DAI on the pool, expanding the total supply of USSD.

In the opposite scenario (price of USSD goes below 1 DAI), USSD contract would reduce supply, using stored collateral to buy USSD back and burn it, reducing total supply of USSD and bringing the peg back to 1 DAI.

4 Mint and redeem

At any given time, USSD can be minted using DAI as collateral at 1-to-1 ratio, expanding total USSD supply. This also can expand supply with larger amounts than current pool liquidity (so that USSD could be minted with no slippage).

Ability to mint USSD for DAI could serve as incentive to rebalance the coin when this is economically viable (covering the gas expenses). However, providing ability to mint or redeem USSD for collateral other than DAI (to which it aims to be pegged) could be exploited as getting a directional exposure

to the collateral component (e.g. mint for WETH and then redeem for WETH later would lead to profiting from short exposure if WETH price decreases).

To help USSD recover in negative scenarios (if USSD value falls below 1 DAI and there are less than 1 USD/DAI reserves per USSD): to refill the reserves by directly providing collateral to the USSD contract's address (at the expense of the agent performing that), and then triggering rebalance (optional) to reduce supply and repeg.

From the other side, implementing a redeeming method (e.g. redeem DAI for USSD) would de-incentivize calling rebalance, with more speculative arbitrage exposed, so direct redeem function is not included in the initial implementation of USSD.

5 Collateral rebalancing mechanics

The rebalance function is public and could be executed by anyone. This decision was made deliberately – providing less dependency on a single entity or project team supporting the calls for rebalancing.

In addition, rebalance also could be triggered before token transfer. If a price is exceeding some predefined threshold, the USSD would rebalance itself before any other transfer is done, providing it has an edge over other participants (who can try to front-run rebalancing).

Rebalancing is selling collateral and burning USSD for peg down recovery (supply contraction) and buying collateral components while minting USSD for peg up recovery (supply expansion).

The collateral has selling priority (order), which is: 1. DAI, 2. WETH, 3. WBTC, 4. WBGL.

The goal of having an order of collateral liquidation is to have more volatile assets be further in the queue, allowing them to be accumulated and grow in value, while keeping DAI as near-line reserves and serve as a protection buffer from speculative manipulation.

When expanding its supply, USSD would buy assets in non-linear fashion, the main metrics defining this would be total supply and collateralization factor of collateral components. If total supply is less than 50000 USSD, the collateral is DAI-only. After initial growth, the collateral buying is trying to achieve a collateral proportion defined as tiers (or 'flutters'), that are defined in table 2.

The current flutter level is determined as total collateralization level of USSD, e.g. first flutter is 0.25x + 2x + 2x + 10x = 14.25x. If collateralization factor is higher this value, then proportion is switched to the next flutter.

E.g., consider the following state of USSD and its collateral: USSD total supply: 750000

The collateral is bought in equal proportions, if the collateral factor is lower than the target collateral factor. In the example above, DAI would not be bought, as it's collateral factor of 0.385 is larger than target collateral factor of 0.25, and 1/3rd of the available buying power should be spent to buy in equal proportions WETH, WBTC, WBGL (if the threshold of target collateral

Table 3: Collateral state example

Collateral stored (price measured in USD)	Collateral factor	Target collateral factor
289000 DAI	0.385	0.25
125600 WETH	0.167	2
450000 WBTC	0.6	2
500000 WBGL	0.66	10
Total: 1364600/750000	1.812	14.25 (1^{st} flutter)

factor won't be reached, otherwise the appropriate buying amount for collateral component would be lower). As swapping and buying requires gas, if a portion to buy a collateral component is less than 5%, it is not bought (most probably it would be bought in the next operations).

Such mechanics also implies applying a cost-averaging accumulation of collateral assets. If a single asset depreciates, it's individual collateral factor decreases and amount to be bought increases.

Even if the collateral portion is higher than target collateral factor, no selling operations are performed during rebalancing.

Rebalancing is performed only if the relative proportion of tokens on the key USSD/DAI pool is skewed larger than a certain threshold value (1%), which is directly impacting swap price on the pool, inside a rebalance function there is no external calls (outside Uniswap's contracts and DAI transfer), and it's checked that amounts that are put into USSD/DAI pool make propotion closer to 1-to-1. Even if some collateral pricing is a bit mismatched (e.g. Uniswap V3 on-chain price oracle changes price once per block) the DAI that was accrued selling other collateral would stay as DAI collateral on the USSD contract.

The rebalancing amount is also multiplied by a 'safety buffer' (a value of 0.99), to take pool fees into account and to ensure that rebalance operations don't cross 1.0 USSD/DAI boundary to minimize arbitrage opportunities using USSD contract.

5.1 Collateral storage

The USSD contract acts itself as collateral holder. No other entity has access to USSD collateral except the contract's logic of collateral management, and DAI is also transferred during mint/redeem operations. In addition, at any moment, the collateral balances on the address of the USSD smart-contract serve as the proof of collateral presence and sufficiency. Collateral is not allocated in any other project (lending/borrowing platforms, investment vaults etc.) and is fully visible at all times.

USSD contract would provide and maintain allowances for itself, and collateral components (DAI, WETH, WBTC, WBGL) to Uniswap V3 router for swap operations.

Prices of collateral components are measured through a series of contracts

implementing simple oracle-like interface. There's some flexibility reserved at the time of writing related to the oracle implementations: there are numerous options available, such as using Chainlink public feeds (available for larger assets such as DAI, WBTC, WETH), measure TWAP price from Uniswap V3 pools, or other implementations. Oracle contract is assumed to return the price in USD (but that is just the naming of the function), in theory, it could be returning price in DAI. Various approaches to implementing price measurement have their own benefits and risks, and could be a part of further research.

6 Dependencies and deployment

This is a list of dependencies the USSD smart contract has for its implementation and functioning:

1. OpenZeppelin contracts-upgradeable library[5], that is thoroughly audited and widely used implementation of various useful libraries for access management, transparent proxy pattern and others. To reserve ability to patch possible bugs, the contract would be kept upgradeable (for a limited time, and then locked afterwards). There are two roles initially defined: one is standard DEFAULT_ADMIN role for managing upgradeability, and second is STABLE_CONTROL role, for managing collateral and several numerical parameters (rebalance minimal threshold, flutter ratios).

2. DAI stablecoin contract[6], as DAI is used as part of the collateral, and USSD tries to maintain its peg for DAI through Uniswap V3 pool rebalancing.

3. Uniswap V3 (universal V3 router[7] and pool contracts) Uniswap is used extensively by USSD to measure peg, collateral ratio, perform collateral buying and selling using swap routes (sometimes 2 or 3 pools in a swap chain). The pool swap path can be administered

Contracts for the USSD ERC20 token were deployed in two EVM-compatible blockchains:

1. Ethereum Mainnet (chain id 1): contract address 0x97D87327D8F168b0Ba317fd8B210d2B087f4b851;

2. BNB Chain (chain id 56): 0x19a23fEA27B1d845a334DFAADb5e54FAd7cdcE74. In addition, as DAI liquidity for BNB chain on Uniswap is not sufficient for USSD operation, USDT was used as a substitute (that may be changed in the future for the purposes described earlier).

[5] https://github.com/OpenZeppelin/openzeppelin-contracts-upgradeable
[6] https://etherscan.io/token/0x6b175474e89094c44da98b954eedeac495271d0f
[7] https://etherscan.io/address/0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45