Introduction to DeFi

DeFi or Decentralized Finance is to enable different types of financial operations in the decentralized ecosystem. The financial operations can range from saving, borrowing, lending or any other type which a traditional bank would offer.

The concept of DeFi leverages all properties that are critical to a crypto currency which are as follows:

1. Permissionless
2. Censorship Resistant
3. Programmable
4. Transparent
5. Composability
6. Trustless

As in the traditional world, most of the financial transactions revolves around currencies which are stable. Similarly, the financial transactions on a DeFi revolves around cryptocurrencies. Since most of the traditional cryptocurrencies like Bitcoin, Ethereum, etc are highly volatile & cannot be considered as an ideal candidate for such transactions. Therefore, much of the concept revolves around stablecoin, a cryptocurrency backed by an entity or pegged to fiat currency like the dollar or using some sort of algorithmic price stabilization mechanism.

What is Stablecoin?

Stablecoins are the class of crypto assets created to address the issue of price volatility in typical cryptocurrencies. Due to the highly volatile nature of traditional cryptocurrencies, it becomes inconvenient to use them in a day-to-day financial transaction.

The low-price volatility in the stable coins is the result of the price stabilization mechanism that has been adopted. These stabilization mechanisms can be classified in two primary categories i.e., Pegged /Collateral & non-collateral.

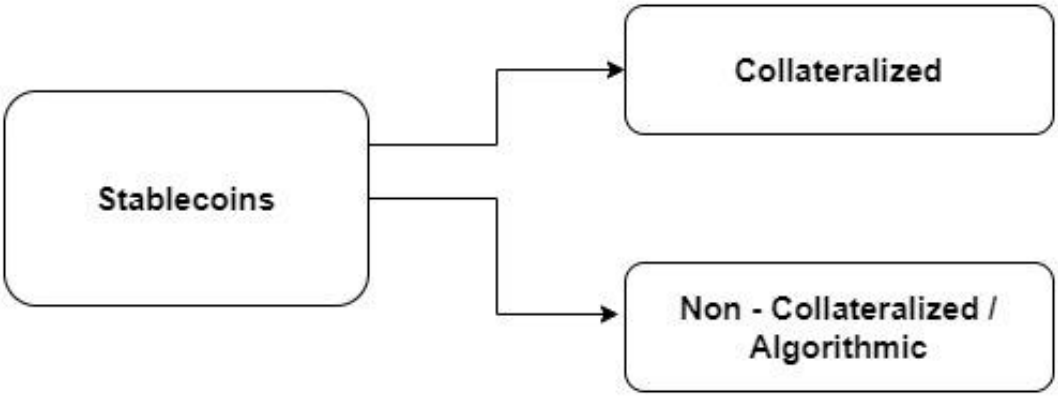

Fig: Types of Stablecoins

Pegged/Collateral Stablecoins

Pegged Stablecoins

Pegging is a way of controlling currency by trying it against another currency. This stabilization techniques are adopted by many countries to stabilize their currency by pegging it against a much stable currency for example USD (United States Dollar). These types of stable coins are pegged against fiat currencies or commodities (E.g.: Gold) or combination of both. Some stablecoins can also use a combination of different currencies. This provides insulation to stablecoin against shock to any one currency/commodity in the basket/group.

Pegging using a group of different currencies could also prove to be harmful if one of the currencies in the basket prove much more volatile than the rest. On the other hand, using a currency/ commodity has its own disadvantage in terms of scaling. To address this issue various indexes can be used such as SDR (Special Drawing Rights maintained by IMF) or CPI (Consumer Price Index), but it will have its own such problems as these indexes are less frequently calculated. Additionally, determining what currency should be in the basket and its corresponding weight is another complex task.

Collateral Stablecoins

Historically, fiat currencies often make use of collateral such as gold to ensure that the circulating currency has a redemption value. One of the many challenges the issuers face is to ensure that the currency never trades at any other price than the original redemption value. Using a fiat-currency or commodity as a collateral also raises the question of centralization as it would be under the control of a single entity or organization, hence defying one of the basic principles of decentralization. Additionally, the problem of storage and scaling will also arise as more the currency scales the more collateral is required

to maintain the original ratio of collateral to stablecoin.

One way to avoid these issues is to use cryptocurrency as a collateral. This has the advantage of decentralized operation and the potential for diverse backing assets. However, since cryptocurrencies are highly volatile makes it hard to use it to guarantee any type of redemption value. Additionally, stable coins backed by cryptocurrency needs to have an additional mechanism to manage large fluctuations in backed cryptocurrency's value.

Tether Stablecoin

Introduction

Tether is a collateralized stablecoin, each of the tether into circulation will maintain a one-to-one ratio with its fiat currency i.e.: one Tether UDST is one US dollar. The fiat currency reserve will be held in deposits by Hong Kong based Tether Limited.

As there exist a large array of assets and correspondingly even a larger medium that can be use as store-of-value, Tether believes Bitcoin blockchain as a better medium for transacting, store, and auditing of these assets. All Tethers are issued on Bitcoin blockchain via Omni Layer protocol, so they exist as a cryptocurrency tokens. Tethers are redeemable/exchangeable with the underlying fiat-currency or, if the holder prefers, the equivalent spot value of Bitcoin. Each Tether in circulation can be used to transact, transferred, spent, etc just like any other cryptocurrency.

Although Tether uses a much simpler approach to maintain the value of the stablecoin, but this approach is not purely decentralized since Tether Limited acts as a centralized third-party custodian of the reserve assets even though the Tether in circulation are decentralized tokens. Tether claims that at any point of time its reserve would hold fiat currency equal to or greater than number of Tethers in circulation. To establish trust & maintain transparency of this fact Tether uses

Proof of Reserve to report the status of their reserves in real-time on their website.

Issuance/ Redemption Process

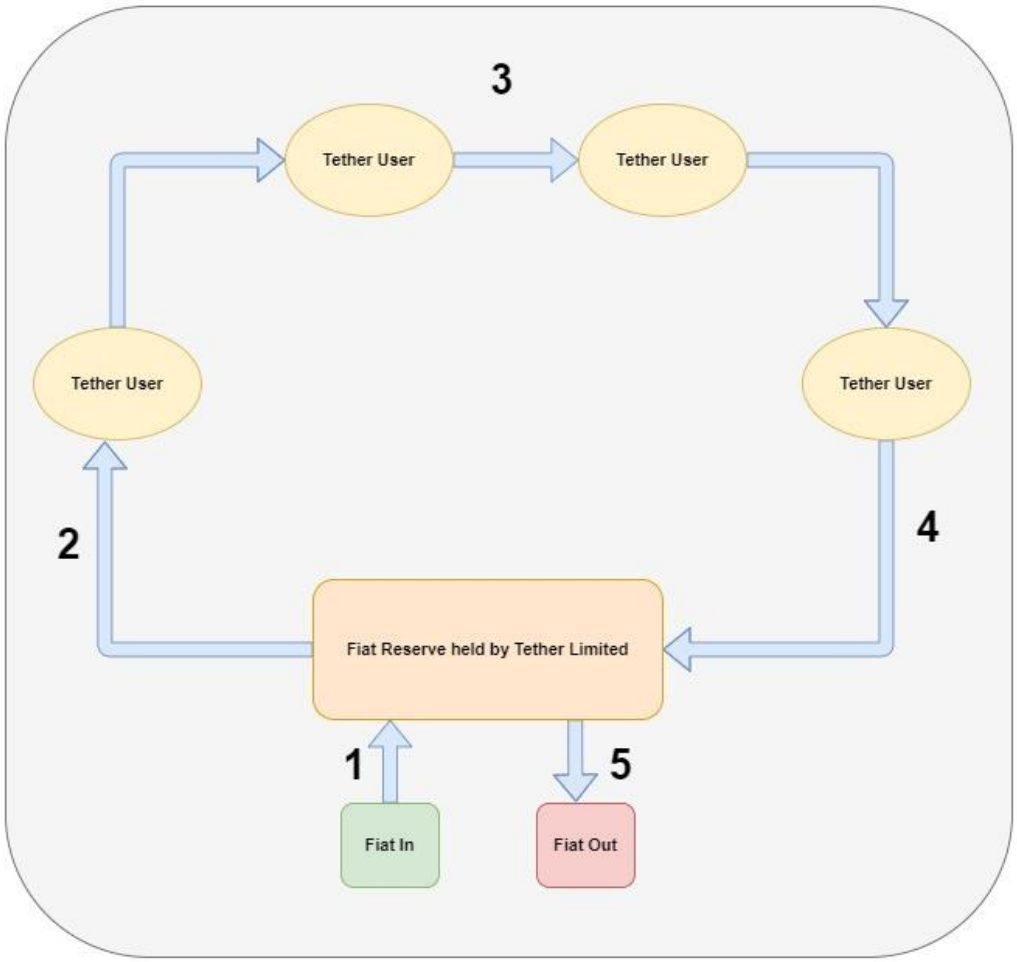

Fig: Tether Process Flow

The whole process from the issuance to redemption of Tether can be understood in the following steps:

- **Step 1**: User deposits fiat currency into Tether's bank account.
- **Step 2**: Tether Limited generates and credits the user's tether account. Tether enters in circulation. Amount of Tether deposited=Amount of fiat currency deposited by the user.
- **Step 3**: User utilizes the Tether to perform transfer or any other type of operation.

- **Step 4**: User deposits Tether with the Tether Limited for redemption.
- **Step 5**: Tether Limited destroys the Tether and send the fiat equivalent to user's bank account.

Any users can obtain Tether outside the above process via an exchange or another user. Once the Tether enters circulation it can be used freely for any type of financial transaction.

Tether Weakness & Resolutions

As mentioned before Tether's implementation cannot be considered as a fully trust less ecosystem. Since Tether Limited and the corresponding legacy banking institutions holding the asset reserve are the primary risk factors. Some of the other weaknesses are as follows:

- Tether could go bankrupt.
- Bank could go insolvent or freeze/confiscate the funds.
- Tether Limited creators could abscond with reserve funds.

In case of bankruptcy Tether Limited claims that the client funds would still be safe and hence all Tethers in circulation would sill be redeemable. Additionally, since the Tether is on Bitcoin blockchain individuals can store them directly through securing their own private keys.

Insolvency of banks or banks freezing funds are the risks associated with any tradition financial institutions or the exchange operators. However, the banks associated with Tether limited are confident of their business model. Furthermore, Tether limited are adding new banking partners in different jurisdictions to mitigate the risks.

DAI Stablecoin

DAI is another example of collateral stablecoins issued by MakerDAO, an Ethereum-based protocol. DAI seeks to maintain an exact ratio of one-to-one with US dollar.

MakerDAO first introduced in 2015, is a decentralized autonomous organization (DAO) built on Ethereum blockchain. Maker Protocol the underlying architecture of the DAI stable coin was launched in December 2017. DAI can be considered as truly decentralized stablecoin as DAI holds its assets into an Ethereum based smart contracts. These assets act as collateral & help in maintaining DIA's peg to the US dollar.

Initially MakerDAO supported only ether as a collateral but after further technology updates it can now support multiple cryptocurrencies like ether (ETH), basic attention token (BAT), USD coin (USDC), wrapped bitcoin (wBTC), compound (COMP) and many more thus mitigating user risk.
Additionally, DAI token holders act as a guarantor for DAI i.e., their MKR (MakerDAO's native governance token) can be liquidated if the system crashes. In return the DAI token holders earn interest on their DAI hence incentivizing the guarantor to ensure proper functioning of the system.

DAI Issuance

DAI is an ERC-20 token which can be purchased from any crypto exchanges. Additionally, DAI can be generated and borrowed by opening a Maker collateral vault through MakerDAO's Oasis Borrow dashboard and deposit Ethereum based assets as a collateral. Maker collateral vaults were previously referred to as collateral dept positions (CDPs) in prior versions of Maker protocol are essentially smart contracts that hold the collateral in escrow until the borrowed DAI has been returned.

Since the DAI is always over collateralized the value of collateral deposit must exceed the value of DAI borrowed.

Price Stabilization Mechanism

DAI balances out economic incentives using the concept of game theory to continuously maintain the value of 1$. In case the price of DAI falls below 1$ the system incentivizes users to increase the price and vice versa. This also results providing opportunities to users to make money due to price swings.

Since the DAI is always over collateralized the value of the collateral will always exceed the value of the DAI token in a predefined ratio. If the value of the collateral falls changing the ratio of collateral value to DAI, the collateral will be liquidated until the original ratio is achieved.

Non-Collateral Stable coins

The third type of stable coin deals with the volatility of the collateral/ pegged assets by not collateralizing the currency at all. The main disadvantage behind the pegged/collateral stable coin is its dependance on physical assets. The economy is continuously expanding and at a rate faster than it will soon outgrow to be backed amount of physical assets available. One such example is the US dropping the gold standard to achieve more flexibility that gold standard can provide. Similarly, the crypto economy is expected to expand beyond what can be collateralized with physical assets.

These type of stable coins hopes to achieve this stability with the help of algorithms hence these coins are also known as Algorithmic Stable Coins. This has many advantages such as following:

- No need to store collateral.
- Cheap to operate as it does not require to keep real assets at hand.

Additionally, if this type of stable coin works it can scale infinitely without need of any backing physical asset. However, there are some major uncertainties with this approach as follows:

- Algorithms used to maintain the stability are gamey, un-tested and there is no set approach to it. Several approaches have been tried which were unsuccessful yet (Terra, NuBits), others are still in development.
- The value of this type of currency largely relies on issuing mechanisms or the people's belief.
- One flaw in design or change in market sentiments can lead to a catastrophic fall which may be irrecoverable as there is no inherent redemption value.

Case Study: Terra Money

Introduction to Terra

Terra ecosystem was created in 2018. It is an opensource blockchain protocol for algorithmic stablecoins and several different financial applications. At the core, it has two basic principles which is to provide stability and promote adoption as a meaningful alternative to fiat-currencies to support different financial transactions and to store the digital currency as well.

Terra runs on Proof of Stake algorithm and is aimed to provide financial infrastructure so that different DApps could be created on it. Luna is the native token in the Terra ecosystem and represents mining power in the same way how a miner's hashing power represents the odds of generating a block in the bitcoin network.

Before we dive deep, the concept of depegging needs to be understood. A depegging event in terms of stable coin can be defined as point where the stable coin lost its predefined pegged value. For example, the point when UST value fell below 1$ can be considered as a depegging event.

Terra Money

Even though US dollar has dominated in international trades and forex operations terra recognized it is of no use for the domestic consumptions. This is because US dollar exhibits a significant amount of volatility when talking about consumption in a specific region.

It is because of this reason that terra launched a family of cryptocurrencies that are pegged to each of the world's major currencies i.e.: USD, EUR, CNY, JPY, GBP, KRW, and the IMF SDR (International Monetary Fund's Special Drawing Rights). TerraSDR is the flagship currency, given that it exhibits lowest volatility against any one fiat currency. It is because of this reason

TerraSDR is the currency in which transaction fees, miner rewards and stimulus grants will be denominated.

To maintain stability, it is important for all these different currencies to share liquidity among themselves. It is because of this the system support atomic swaps among Terra currencies at the applicable market exchange rate. This allows all the Terra currencies to share liquidity and macroeconomic fluctuations: a fall in demand in one currency can be consumed by another.

Stability Mechanism

Terra money follows the same rule of demand and supply to maintain its stability:

- When the price falls below the target price it keeps on reducing the money supply until it reaches its target price (Contraction).
- When the price increases above the target price the supply of money is increased until it reaches normalcy (Expansion).

Contracting the supply of money incurs cost to acquire money back from the market. Terra miners plays a vital role in this aspect and controlling the volatility of the currency. The miners absorb volatility in the Terra supply in the following way:

- The miners absorb the contraction cost through the dilution of mining power (LUNA). Or in other words the system mints and auctions more mining power to buy and burn back Terra.
- In long term miners are compensated with the increase in mining reward.

This entire process of burn-mint multi coin structure is known as Seigniorage algorithm where one coin is burned or minted (in this case Luna) to control the value of another.

In addition to this clever stability mechanism the founders of the Terraform Labs created the Luna Foundation Guard (LFG), a consortium which will help protect the peg with the help of reserves in bitcoin and other crypto assets. The idea was if the peg fell below 1$ (in case of UST) the bitcoin reserves will be sold to buy UST until the peg is regained. On the other hand, if the value goes above 1$ the LFG would sell the UST until it goes back to 1$, and the profits will be used to pad out the reserves.

Additionally, UST has a built-in arbitrage mechanism between UST & Luna token. Arbitrage can be referred to as a process of buying an asset from one exchange and selling it on another where price of the asset is much higher. This enables traders get profits with minimal risk.

In case of UST arbitrage works as follows: if UST slips to 99 cents, traders can profit by purchasing UST and exchanging it for Luna token profiting 1 cent per token. This also helps driving up the price of UST as it shrinks the overall supply. This can be also done other way around i.e., buying Luna and exchanging it for UST which will help increase the supply of UST and drive down the price.

Crash of TerraUSD 2022

TerraUSD (UST) launched in Fall 2020, is the version of Terra money which was pegged against USD and was supposed to always retain a value of $1. The crash of UST is intervened with that of LUNA token which fell from $116 in April 2022 to a fraction of penny at present.

To promote the traders to burn LUNA and create UST, the creators introduced the Anchor Protocol which was offering around 20% interest on loan. So, instead of keeping money and earning a nominal interest through traditional means the pitch was to convert the money to UST where it can earn 20% interest. Before, the de-peg happened

around $14 million (70% of toral UST supply) was deposited in this scheme.

On 7th May 2022 around $2 billion worth of UST was taken out of the Anchor Protocol. Around hundreds of millions worth UST was sold immediately after this. After these huge sell the price of UST fell further to around 90 cents. Traders tried to take advantage of this situation by selling UST to get $1 worth LUNA. However, due to the platform limitation that only allowed one hundred million worth of UST to be burned for LUNA per day cause the investors to panic and triggered massive sellout after which the UST could not retain its peg. Due to this the price of LUNA took a much worse hit as compared to UST i.e.: from under $120 to a fraction of penny.

The LFG made attempts to regain the UST peg. As reported the LFG's bitcoin reserves fell from 80,000 (about $2.2 billion) to just 313 ($9.2 million).

The remaining reserves of LFG are to be used to compensate the remaining users of the UST. The creators proposed to fork the blockchain to a new one with key features. However, its still doubtful to regain the confidence of the investors.

This crash led to around $17 billion worth crypto in UST and Luna been wiped out. What's more is that it raised more serious doubts related to stablecoins as a whole and specifically towards algorithmic ones. And lastly, this caught the much-needed attention of politicians and regulators who are pushing for stricter regulation to prevent anything like this from happening again.

	Teather (USDT)	DIA	USDC	Terra Classic (USTC)
Type	Collateralized	Collateralized	Collateralized	Algorithmic
Collateral	US Dollar	Cryptocurrencies (Ether, Basic Attention Token, USD Coin, wrapped Bitcoin, Compound)	US Dollar	N/A
Market Cap.	$67,742,498,406	$6,901,658,135	$51,593,989,076	$520,681,064
Stability Mechanism	1:1 Fiat to Coin Issuance	Over Collateralized, Liquidation of Collateral	fiat-collateralized (US Dollar)	Burn to Mint Concept, Luna token