Imperial College London

MEng Individual Project

Imperial College London

Department of Computing

DeFi Synthetic Assets: Systematization of Platforms and Data Insights

Author:
Tyler Danno

Supervisor:
Dr. Arthur Gervais

Second Marker:
Dr. Dalal Alrajeh

June 22, 2022

Abstract

Speculation on the price of assets plays a big part within the cryptocurrency industry, and similar to in any other market, there is a wide variety of means to do so. Synthetic assets were introduced to the digital asset space as one of these means in 2018, with the creation of the Synthetix protocol on the Ethereum blockchain. The assets fall under the financial instrument class of derivatives, with their value being derived from any underlying asset. Over the past years, many more synthetic asset platforms have been built to achieve similar goals, trying to address critical problems that occur in existing ones. To do so, they differ slightly in how their protocols are implemented, such as the synthetic asset minting and contract liquidation processes, as well as their method of tracking the value of the underlying asset.

This project will attempt to use the contrasting protocol features to categorize and systematize both the different types of protocol that are currently running within the Decentralised Finance (DeFi) space, as well as providing detail as to the wide range of synthetic assets that are available through them. The different benefits and risks of the various protocol design features will be documented alongside this. It provides some analysis of trends over time within the changing configurations and mechanisms of the platforms. The trends that were managed to be identified are aspects within the collateralization and liquidation mechanisms. It will then go on to provide data insights on the various platforms metrics available that can be used to evaluate protocol. The main protocols that will be investigated will be those with the highest Total Locked Value (TLV) in their smart contracts, hence identifying the largest platforms. The platforms investigated in this paper are Synthetix, Universal Market Access (UMA), Mirror, and Linear.finance.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Synthetic assets are not a type of financial instrument that is native to the cryptocurrency world. As a financial derivative, they allow the holder to gain custom exposure to price movements on either a singular or group of underlying assets. The contracts include no physical exchange of the assets, meaning neither party in the transaction must own them. The synthetic asset can derive its value from assets such as commodities, currencies, stocks or bonds. Common types of derivates include options, futures and swaps.

The DeFi sector aims to bring many elements of the traditional, centralised financial sector onto blockchain technology, eliminating the need for intermediaries in transactions. This allows for many benefits; higher transparency though the blockchain ledger, the ability for tokenization, and greater efficiency overall are amongst many others. With the DeFi sector incorporating an increasing number of centralised finance elements as it grows, it was only natural that a means of trading derivatives on the blockchain was developed.

In 2017 various platforms were built on Ethereum in order to offer derivatives trading through cryptocurrencies, addressing different areas within the derivatives landscape. dYdX is a decentralized exchange platform that was built at this time for margin trading of cryptocurrencies, allowing individuals to trade with leverage in order to increase their exposure. Synthetix was built in the same period, addressing the lack of being able to gain exposure to traditional assets while remaining within the cryptocurrency space, developing the first synthetic asset platform. Later on in 2018, the UMA Protocol was developed to offer access to synthetic assets in a different way.

Cryptocurrency-based synthetic assets are a tokenized way to provide exposure to real-world assets, without needing to leave the cryptocurrency system. They offer holders all the benefits of decentralization, as they are available to all users through the use of secured smart contracts, collateral pools and oracles (or substitutes to these last two in some cases). The key mechanisms of the synthetic asset smart contracts are the following: data/price retrieval, liquidation process, price pegging, asset synthesis and asset destruction.

The two Ethereum-based protocols mentioned, Synthetix and UMA, will be the two main platforms that will be analysed initially, as they provide a thorough insight into the generic structures of most synthetic asset protocols. Many newer protocols (such as Mirror Protocol and Linear Finance) approach the synthetic asset creation process with similar mechanics to Synthetix, however none yet have followed UMA in its alternate approach. The two platforms offer two different types of synthetic asset services, which in essence can be broken down into the following:

1. **Asset replication** (Synthetix, Mirror, Linear Finance) – the synthetic asset tracks the price of an existing underlying asset in some way, simply providing exposure to it on the blockchain. The smart contracts for each asset involved are pre-written and approved before being made available on the platform. The protocol uses the process of staking to create pools of collateral that act as counterparties to trades. This will be explained further in the Background section of the report.

2. **Direct creation** (UMA) – the platform facilitates individuals to create customizable synthetic assets, using any retrievable data value to derive price (e.g. Total Value Locked in a protocol, weighted combination of assets to create a synthetic index). The smart contracts

are written and agreed upon by two counterparties, who have opposite motives/expectation on the value of the newly created synthetic asset, hence the trade is taken against the other party.

After establishing the fundamentals of how these two types of synthetic asset platforms operate, further investigation will be performed into how newer platforms have adapted their approaches in how they offer synthetic assets.

1.2 Contributions

This paper will aim to make the following contributions:

1. **Synthetic Asset Platform Categorization and Systematization.** The paper provides a framework for the mechanisms of the two main types of synthetic platforms currently available within the DeFi ecosystem. Both types will be investigated and the benefits and risks associated with the design features of each will be assessed.

2. **On-chain Data Analysis.** The different design features of the various platforms will be evaluated using a number of metrics, to provide insights into data trends over the span of the platform lives.

3. **Trend Identification.** The combined results of the past protocol design changes as well as the data analysis will be used to provide further insights into the synthetic asset platform space as a whole, identifying any trends or patterns within the platforms investigated.

1.3 Project Aim

The aim of this project will be to systematize the mechanisms in which the different DeFi synthetic asset platforms operate. Having categorized the different platforms into two types, liquidity pool-based platforms and direct counterparty-based ones, I will begin to investigate further into the different platform design choices within each category, and the consequences of such choices. The platforms that will be investigated include:

- Synthetix
- UMA
- Mirror Protocol
- Linear.finance

This selection of platforms aims to cover both the range of structures within the synthetic asset platform space, as well as the range of synthetic asset classes they offer. The platforms selected represent over 82% of all TVL within synthetic asset platforms at the time of writing. Some offer multiple of the following asset classes, and some focus on a singular one out of the following: cryptocurrencies, forex, commodities, indexes (both traditional and cryptocurrency-related), yield bearing tokens and more exotic products.

The variations that will be investigated within each platform include: price retrieval, collateralization process, asset minting and burning, liquidation process and user rewards. Some of these will be touched upon in the background, however a thorough analysis of the smart contracts of each the stated platforms must be completed in order to compare platform design choices. Within these attributes, the following design decisions (amongst others) will be compared: permitted collateral asset type, minimum collateralization ratio, and choice of oracle (or oracle-like system).

The main objective is to systematize the mechanisms of the various platforms, comparing which ones are designed in similar ways in some areas while also identifying key differences at a qualitative level. Then in order to determine the effects of the different choices, where possible on-chain data will be collected for each platform and analysed.

The original goal of the paper was to provide some form of recommendation in the case of building a new synthetic asset platform, as to the features to include as well as the features to avoid when designing it. The recommendation would form its basis from the results of the on-chain data analysis of the various platforms, and encourage promising growth potential for the platform while maintaining the upmost security.

However, by the end of the investigation, the conclusion was made that there currently is not enough data yet relating to synthetic asset platforms to justify a recommendation for any one platform decision over another. Within the asset replication category of synthetic asset platforms, only one platform has been running for over 2 years, and that is Synthetix. Even with the 4 year standing it has, over this period there have been countless adaptations and changes to the protocol, to the point that any data collected for a specific platform design choice/configuration would only span a few months, and there are no platforms with a large enough trading volume or TVL that have the same design choices to compare data with effectively.

On the matter of direct creation synthetic asset platforms, there is only one platform that had sufficient TVL and use cases to investigate, and that is UMA. However, due to the clear differences in use cases for the platform that will be explained, and the inability to directly compare a lot of the assets traded on UMA with those on asset replication platforms, no direct comparison in data has been made between the two separate categories of synthetic asset platforms.

All being said, there is still a lot to gain by investigating the limited synthetic asset platform data that is available, so the data investigation section of this report has been written to try and provide insights into interesting trends or patterns within the synthetic asset space.

1.4 Ethics

The only ethics issue relevant from an ethics checklist is within the Misuse section. Specifically, "Does your project have the potential for terrorist or criminal abuse e.g. infrastructural vulnerability studies, cybersecurity related project?" The reason this is the case, is that any platform vulnerabilities, expressed through identifying risks of certain design choices, may be used by malicious actors in order to perform an attack against other platforms that may have been designed in the same way.

However, the fact that the attacks and exploits that will be investigated within the paper will only be the historically largest ones, they will have already been documented elsewhere, and hence these actors will not gain any new information from the assessment of them. On top of this, platforms that experience these types of attacks tend to quickly update their platform with the required measures to avoid such attacks in the future.

Chapter 2

Background

2.1 Blockchain

Blockchain is a technology that implements a specific type of database, storing data in blocks which are then chained together using the hash-codes of the blocks. The blockchain is stored on a peer-to-peer network of computers, which can often be scattered across the globe. This means that a blockchain is decentralized and distributed, compared to a centralized network such as the banking payment system, which requires intermediaries to process transactions. A specific blockchain platform can either fall into the categories of public or private [4] - a public blockchain maintains a distributed ledger that has its history available to view for all participants, whereas for a private one this is not the case.

Data within the blockchain is stored as transactions, which are grouped into blocks, and then cryptographic hashes are used along with timestamps in order to link these blocks together so that they maintain chronological order [5].

Due to the distributed nature of these ledgers, there must be some type of consensus mechanism in order to have all the participants, each of which is called a "node", agree on the correct blockchain history. There are a number of these consensus algorithms, and different blockchain platforms use different types. Certain nodes on the network are called "validators", and perform the consensus algorithm functions, ensuring the network remains immutable and secure, which keeps the blockchain safe from falsified information and hacks. These validators tend to be rewarded for this role through a portion of the transaction fees on the network [6].

The benefits of blockchain technology include immutability, security and transparency of the transaction history. Decentralization of data storage also ensures that data can always be recovered when lost on one node. For these reasons there are many use cases for blockchain technology, one of the largest currently being a decentralized currency system - cryptocurrencies. They offer some advantages such as the ability to process payments, as well as easy access to free financial accounts (in the form of digital wallets), in both cases removing the need for third party intermediaries. This can be particularly useful for citizens of developing countries, where it can sometimes be hard to get access to centralized bank accounts.

Blockchain can also be used by businesses, in order to benefit from similar features. Traditionally paper-heavy processes can be made faster and more efficient through the removal of intermediaries, as well as the ability for blockchain to store documents along with transaction details. Hence there is no need to manually align multiple companies' ledgers. The use cases for the technology within industries range from supply chain traceability to automatic underwriting and claims settlement in insurance. The automation of business processes on a blockchain is achieved through the use of "smart contracts" on certain blockchain platforms.

2.2 Smart Contracts

Smart contracts are programs stored on a blockchain platform that can either be interacted with directly, or run automatically when predetermined conditions are met. The automatic execution of agreements between participants means that everyone can be certain of the outcome of the agreement, without any intermediary company's involvement. This is due to the fact that the terms of the contract between the parties is written directly into lines of code.

Every interaction with a smart contract is recorded on the blockchain as a transaction. The most widely used blockchain platform that uses smart contracts is called Ethereum. In order to use a coded smart contract, it first must be deployed to a blockchain on which it'll be used. At this point it is assigned an Ethereum address, at which it can be accessed by other addresses [7]. These smart contracts can be used to create new tokens on the smart contract's blockchain, or link them together in order to build whole platforms to accomplish more complex tasks.

There are many other blockchains other than Ethereum that support smart contracts, boasting cheaper and faster transactions. Some of the synthetic asset platforms that will be investigated in the final report will be situated on these alternate blockchains, such as Mirror protocol, which is situated on the Terra blockchain.

2.3 Gas Costs

Every single transaction that is used to interact with a smart contract deployed on a blockchain incurs a transaction fee. These transaction fees vary both with the complexity of the transaction taking place, as well as the volume of transactions being made at that point in time on the network. This is due to the fact that there is limited space within each block for the number of transactions that can be recorded.

Miners and validators are rewarded with these transaction fees. On Ethereum, these transaction fees are paid in a unit called gas. These are priced in a subunit of Ether, called Gwei, which are equal to $1\text{x}10^{-9}$ ETH. The more complex a transaction is, the more space that transaction takes up in a block when recorded on the blockchain - for this reason, more complex transactions require higher gas fees in order to complete [8].

When creating a transaction by interacting with a smart contract, the transaction sender has choice as to how much gas they are willing to pay. As a result of supply and demand, miners are incentivised to accept transactions at higher gas fees [9]. Choosing to pay lower gas fees means your transaction is more likely to take longer to complete, and may even get dropped (and therefore not recorded on the blockchain) at times of high network volume.

For the reasons explained above, there is a trade-off with the cost willing to be paid for the transaction, the complexity of the transaction and the probability that the transaction will be finalized.

2.4 Decentralised Finance (DeFi)

Decentralised Finance is a blockchain based financial infrastructure and is one of the main applications of smart contracts within the cryptocurrency industry. The sector takes processes that are traditionally completed within centralised finance, and replicates them using series of smart contracts. The use of smart contracts in this way removes the necessity for intermediaries such as banks or financial institutions, providing the decentralised version of the sector with properties such as higher efficiency, accessibility and transparency compared to its traditional centralised counterpart.

With DeFi being such a rapidly expanding sector, growing from $25 billion [10] in Total Locked Value (TLV) in DeFi at the beginning of 2021 to over $90 billion at the beginning of 2022, new projects and platforms are constantly being added to it. The majority of DeFi platforms are built upon Ethereum, due to it being the first blockchain to integrate smart contracts, however the main components that operate within DeFi are the following:

1. **Decentralized Exchange (DEX)** platforms are one of the most prominent components within DeFi, using peer-to-peer protocols to exchange various fiat currencies or other cryptocurrencies for alternate cryptocurrencies. Unlike in the traditional finance world, these transactions are handled automatically via smart contracts, rather than being officiated by banks, brokers, or any other kind of intermediary. DEXs can be split into two categories; order book-based and Automated Market Makers (AMMs)[11]. Order book-based platforms operate similarly to centralized exchanges, where opposite position trades on an order book are matched and then executed on-chain. AMMs emerged in order to solve the illiquidity problem faced on order-based DEXs, using liquidity pools [12] to implement peer-to-contract trading rather than peer-to-peer trading. One of the most successful AMM-based exchanges is the Ethereum-based Uniswap [13].

2. **Lending and Borrowing** platforms allow individuals to take loans, deposit and earn interest on their on their digital assets, offering different APYs for different tokens. As more often than not, the parties on either side of the lending/borrowing transaction don't know each other's identities, there are no credit checks for these actions that would be required at a bank. In order to mitigate the risks this brings to the platform and to lenders, borrowers must put down more collateral in the form of some crypto-asset than their loan is worth (this must be more than the platform's collateralization ratio demands) [14]. This collateral would then be transferred to lenders if the loans are not repaid. In order to maintain the position, the borrower must ensure that the value of their collateral remains above the stated collateralization ratio, otherwise their position will be liquidated. This concept will be explored further later in the report. The largest names within the Lending and Borrowing sector of DeFi include MakerDAO and Aave [15].

3. **Automated Investing** platforms in their essence resemble what a mutual fund does, but on the blockchain. They allocate investor's funds across the cryptocurrency market, without the investor needing to actively do anything themselves. Instead of having portfolio managers making the decisions as to where to allocate funds, all decision making is through on-chain data analysis, and the outcomes of the analysis are implemented automatically. The smart contract algorithms involved tend to allocate capital across a variety of lending and borrowing platforms, maximizing the interest earnings potential by splitting them into different lending pools. An example of a DeFi platform that does exactly this is Yearn.finance.

4. **Derivatives Trading** platforms give individuals the ability to gain access to more complicated financial instruments, such as futures and options on cryptocurrencies. They also allow the use of leverage through margin trading. Like DEXs, all transactions are automated by smart contracts. The focus of this paper will be on the synthetic assets area within DeFi derivatives trading platforms. Synthetic asset platforms allow users to expose themselves to the price movements of traditional securities such as currencies and commodities without ever having to leave the cryptocurrency system (compared to the requirement of selling crypto-assets into fiat currency before being able to trade through a centralised broker). They also allow for custom exposure to trends/patterns not exclusive to financial assets, provided there is some sort of reference metric. They enable this through a variety of mechanisms, depending on how the protocol is built. Some use an innovative combination of a number of ideas that are fundamental for many DeFi platforms; liquidity pools and oracles.

2.5 Liquidity Pools

In order to understand the underlying mechanisms of how synthetic assets are able to be created and traded, we must first understand the system that many of these platforms are built upon, which is the concept of liquidity pools. A centralized exchange settles trades based upon an order book, matching opposing positions together with a matching engine [16] in order to fill both sides of the trade and absolve any associated price risk that the exchange might hold otherwise. Centralized market makers provide liquidity to the markets on these exchanges, meaning users are not required to wait for another counterparty to facilitate their trade.

Trying to implement this order book system on a blockchain can result in slow and expensive transactions. This is due to the order book system relying heavily on market makers to "make markets" on certain assets, who are constantly creating and cancelling orders [17] in order to set prices that balance supply and demand [18]. The number of transactions that would be required in order to replicate this process would accumulate extremely expensive gas fees, nullifying any market maker profits. However, without these market makers the system becomes extremely illiquid and mostly un-usable. Liquidity pool-based exchanges offer a solution to this, a peer-to-contract based system rather than peer-to-peer matching of orders.

Liquidity pools are collections of funds in the form of tokens that are locked in a smart contract, used to facilitate a number of activities (such as trading and lending) by providing liquidity. In their basic form, a single liquidity pool tends to hold two tokens, with each pool creating a new market for that particular pair of tokens. The funds within the liquidity pools are provided by participants called liquidity providers.

2.5.1 Liquidity Providers

When a liquidity provider adds their tokens to a pool, they add an equal value of the pair of tokens, according to the current price of both assets. As a reward for providing liquidity (as they can no longer actively use this capital as it has been locked into the smart contract), they earn Liquidity Provider (LP) tokens [19] in proportion to how much liquidity they supplied to the pool. Holding these tokens grants the owner a portion of the transaction fees that are collected when other users interact with the pool. In order to reclaim their liquidity from the pool, they must burn their LP tokens.

2.5.2 Pool Trading

Each token swap (trade) that happens in a liquidity pool leads to a price adjustment within the pool, which is determined by a pricing algorithm. This algorithm can vary in how it adjusts prices across different liquidity pool protocols, and is called an Automated Market Maker (AMM). A basic example of one of these algorithms is the constant product market maker algorithm that is used by Uniswap [20].

$$x * y = k$$

x - token X quantity
y - token Y quantity
k - constant

The algorithm ensures that the ratio between the two supplied token quantities remains equal. This means that trades in the pool must not change the product k of the balances of each token. The result of the price curve that this equation creates means that the ratio of the tokens dictates the price. For example, if someone buys ETH from a USDC/ETH pool, they will be reducing the supply of ETH in the pool and adding to the supply of USDC, which results in an increase in the price of ETH and decrease in the supply of USDC. In this way, the user is executing the trade against the liquidity in the pool, rather than having the counterpart be an individual. The extent to which the price moves all depends on the size of the trade being made – the larger the trade in proportion to the size of the pool, the greater the change in price.

This formula means that larger trades will execute at an exponentially worse rates than smaller ones [21], but also means that the liquidity pool can theoretically facilitate any size trade up to the size of the pool. Larger pools can accommodate far bigger trades without moving the price too much.

The fact that the relative price of the two tokens can only be changed in the pool via trading, arbitrage opportunities are created due to divergences between the price in the pool and the price found on other exchanges. This ensures that prices within the protocol always trend towards the agreed market price.

2.6 Oracles

Another concept that must be understood before tackling synthetic asset platforms, is that of the use of oracles in blockchain and DeFi. They act as on-chain data sources for blockchain applications, bringing both real-time data from outside of the blockchain world as well as on-chain data onto decentralized applications for reference. Most often, this data is in the form of asset prices. Although the oracles are not producing the data themselves, they consist of layers that verify data from real-world events, and then submit the collected data to smart contracts on-chain.

Oracles can be centralized or decentralized, with centralized oracles functioning as a single entity providing external data to a smart contract. The disadvantages of using a centralized oracle stem from the same reasons as for the traditional financial system – a single point of failure. This makes the oracle less secure and more vulnerable to corruption and attacks of malicious data being fed to the smart contract. Decentralized oracles reply on multiple sources in order to improve credibility of data. As centralized oracles go against the ethos of DeFi applications, decentralized oracles are the standard for the sector [22].

It is extremely important for oracles to have reliable data and very little latency, as this data is fed directly into smart contracts, which then function and make decisions based off this, hence they hold hierarchical power in the chain of execution of smart contracts. Some of the largest oracle development platforms currently are Chainlink and Band Protocol [23].

2.7 Synthetic Assets

Synthetic assets in the traditional finance world refer to a collection of assets that mimic the same value as another asset, combining derivatives such as options, futures and swaps. This provides the owner of the synthetic asset custom exposure to the underlying, without having to hold the asset itself. For example, a synthetic call (long on a futures position as well as purchasing a put option) allows for the unlimited profit potential and limited loss of a regular call option, without the restriction of having to choose a strike price [24].

The synthetic asset platforms that will be investigated in this paper bring this concept into DeFi. On top of not requiring the user to leave the cryptocurrency industry to speculate on these types of assets through a broker, the benefits of synthetic assets can be categorized into the below:

1. **Ease of access.** Derivatives trading in the centralized finance world is often associated with long, bureaucratic processes in order to be granted permission to trade these assets – only a select few investors are given access. Open-source protocols such as Synthetix and Mirror allow synthetic assets to be minted by anyone, hence investors of any location or jurisdiction are given exposure to the price of traditional assets and cryptocurrencies without having to hold the asset themselves. This provides a favourable alternative for foreign investors experiencing barriers to entry [25].

2. **Tokenization.** These DeFi synthetic assets are tokenized, meaning they can be held, sent or received through compatible cryptocurrency wallets, enabling borderless transfers. The fact that all transactions related to them are stored on a blockchain also provides the benefit of a more transparent ownership history of the assets.

3. **Increased liquidity.** DeFi is operational 24/7 (excluding platform downtimes), in contrast to many traditional markets, which are specific to certain days and hours. The ability to trade synthetic assets on their platforms at any hour of the day is a big advantage compared to traditional markets such as equities. In traditional finance, traders are often bound to the platform/broker that they opened a trading position with. The fact that many DeFi synthetic assets are tradeable not only on the platform they are minted on, but many other exchanges as well, means that traders can benefit from far greater liquidity.

4. **Creation of new assets.** Special synthetic asset platforms such as UMA allow users to create their own custom synthetics to trade, providing that there is a quantifiable value being used to calculate the price of the asset.

5. **Counterparty risk.** Another added benefit is the fact that you are trading against a liquidity pool when dealing with synthetic assets, rather than a centralized party such as a broker or a bank. When trading with centralized entities, they tend to require clauses that allow them to control your trading as they deem fit. This can lead to cases of individual traders winding up with larger losses than price dictates at the time, or left unable to realize their profits because these parties have stepped in. A perfect example of this was the 2020/2021 reddit-fuelled GME situation, where many investors were unable to sell specific securities due to restrictions imposed by brokers such as Robinhood [26].

Although DeFi synthetic assets have many benefits over their counterpart in the traditional finance system, they have some drawbacks as well. Most specific to synthetic assets, is the fact that they never grant ownership of the underlying asset, meaning that although this eases the process of trading them, holders cannot claim any benefits such as shareholder rights and dividends within the equity asset class. More general to DeFi, despite being powerful, scaling issues with blockchains such as Ethereum [27] can lead to delays in transaction processing ad high transaction fees (however this is being improved with the Ethereum 2.0 protocol improvement [28]).

Some other blockchains try to address this problem, however the vast majority of DeFi applications are still running on Ethereum. DeFi can also be vulnerable to hacks and exploits, common for technologies still in their preliminary stages, and many have been documented since the time of its beginning. As of September 2021, hacks in the DeFi system accounted for nearly 76% [29] of all major hacks worldwide that year.

2.7.1 Types

The synthetic assets offered in the DeFi space can be boiled down to two main types, under which all current platform products fall. The distinguishment between the two will make it easier to systematize the different platforms later on in the paper, as currently there are no platforms that offer both types of products, only one or the other. The two types are as follows:

1. **Asset Replication.** This type of synthetic asset aims to duplicate or mirror an already-existing asset, whether that is in the traditional world, or in crypto. Synthetix is an example of a platform that offers these types of assets. They solve the problem of cross-platform usability, such as the accessibility of stocks.

2. **Direct Creation.** This type on the other hand does not require a pre-existing asset to mirror. The platforms that offer these allow users to create their own tokens, based off their own chosen metric – not necessarily a traditional or crypto asset. Some examples of what a user could create is a synthetic index with their own customized weightings of assets, or the capitalization of cash flow, such as hashrate tokens. UMA is an example of one of the platforms that offer these. They allow users to create customized financial contracts between counterparties without the need for an expensive centralized intermediary.

Chapter 3

Synthetic Asset Platforms

3.1 Main Mechanisms

The main operating mechanisms that are essential to how the synthetic asset platform functions can be summarized into:

- Staking and Minting
- Burning (destruction)
- Liquidation
- Pricing

3.1.1 Staking and Minting

The way that users are able to create these synthetic assets uses similar mechanisms to that of the lending/borrowing sector of DeFi. In order so that synthetic assets can be minted (created), they must have some sort of asset backing them, providing them with value (this is separate to their underlying asset that they derive their price from). In order to have this, users must provide their own collateral to the smart contracts involved, similar to the process for loans, and once locked in this enables the issuance of the synthetic assets. This process of locking collateral into the smart contract is called staking.

Due to the volatility of prices within the cryptocurrency industry, the value of the assets that the user has staked can vary wildly within a short period of time. For this reason, the amount of collateral that must be provided by the user wishing to mint must be greater than that of which they are trying to mint. This ensures synthetic assets are backed by sufficient collateral to absorb large price shocks. This phenomenon is known as *over-collateralization*, and the minimum ratio of the value of the staked assets to the value of the minted assets is called the *collateralization ratio*. It provides various credit risk management properties for the opposite party (either liquidity pool or direct counterparty). Different platforms require different collateralization ratios, and these often change over time as well.

3.1.2 Burning

In order for individuals who have staked assets and minted synthetics to close their position and retrieve their collateral, realizing any profits or losses on their trade, they must go through a process which is known as burning the synthetic assets. Burning in the context of cryptocurrencies means to permanently remove a certain number of tokens from circulation [30]. In practice, this is usually accomplished by having a designated wallet that is known as a burn address. The tokens can never be retrieved from this wallet, as it cannot be used for transactions other than receiving the tokens [31].

3.1.3 Liquidation

Liquidation is the process of closing the positions that become under-collateralized due to changes in price movements. A position becomes under-collateralized when it's collateralization ratio falls below the threshold that the platform has set. At this point, this position becomes 'risky' to the platform as the value of the asset that is backing the synthetic asset is decreasing, which could mean that if left to continue, when the holder of the synthetic asset goes to redeem it for the collateral, there may not be enough to pay them back, which may cause a chain of settlement problems.

The platforms want to avoid this issue as much as possible, due to the huge liquidity problems the scenario could potentially cause. They do so by both disincentivising stakers from allowing their collateralization ratio to drop that far, as well as incentivizing other parties, known as liquidators [32], to handle the fall-out if they do. Before liquidators are permitted to become involved with an under-collateralized position, there is usually a period where the synthetic asset holder is given the opportunity to correct the collateralization ratio.

In the case where this is not completed, the role of the liquidators is to allocate their own capital/assets to fix the under-collateralized position. When they do this, they burn their own synthetic assets, which unlocks some of the collateral provided by the initial holder. In order to disincentivize position holders from letting themselves become under-collateralized in the first place, as well as to incentivize liquidators to perform this function, this newly unlocked collateral is sent to the liquidator, as a reward [33]. The lost collateral is the penalty placed on the initial synthetic asset minter. The amounts gained and lost respectively are determined by the liquidation penalty.

3.1.4 Pricing

One of the most important parts of how synthetic asset platforms operate, and one of the traits that sets the two different types of platforms apart the most, is the way in which the assets on the platform derive their price from the underlying asset. The pricing mechanism is used in two ways, the first being to quote the price of the synthetic assets, and the second being the provision of price indications for debt monitoring, as required for identifying under-collateralized positions.

Some platforms use oracles for this procedure; however others do not trust the security of oracles, hence they have their own "priceless" [34] methods. The oracle-based platforms are able to provide live price streams for each of their assets, but due to the nature of how the other type of platform decides on price, they cannot.

3.2 Platform Types

The types of synthetic asset platforms currently running on DeFi can be summarized into two types mentioned earlier, based upon how they implement the various mechanisms described in the section above; *asset replication* platforms and *direct creation* platforms. The paper will first cover the far more common type of synthetic asset platform, the asset replication platforms that use oracles and liquidity pools, by investigating Synthetix, Mirror Protocol and Linear Finance. It will dig into each of the platform's mechanisms, systematizing the different approaches to the aspects of asset replication protocols. Then it will cover the direct creation type of protocol that uses "priceless" methods, and does not rely on oracles, by investigating UMA.

3.3 Asset Replication Protocols Initial Evaluations

Asset replication protocols allow users to speculate on the price of traditional assets, not available in the cryptocurrency world normally. The synthetic assets used to do this track the price of the traditional asset or a cryptocurrency. Asset replication platforms, through the use of liquidity pools and oracles, are able to replicate the price movements and the position pay-outs as a normal trading broker would.

These platforms tend to be composed of a few key components; staking capability, minting capability, burning capability, and a synthetic asset exchange, where minted synthetic assets can be swapped for other synthetic assets. The best way to demonstrate these different aspects is to perform an initial analysis on how one platform works, and then build from there. The Synthetix platform was chosen for the initial analysis, for the reason that it was the first synthetic asset platform built in DeFi and still maintains the highest Total Value Locked (TVL) in smart contracts out of any asset replication platform.

3.3.1 Synthetix

Synthetix was the first synthetic asset platform built in DeFi, and was developed on Ethereum using a number of concepts already existing within the space to allow for this novel idea of creating synthetic assets on-chain, effectively using liquidity pools as the counterparty for trades. The name Synthetix has given synthetic assets on their platform is Synths, and they can be recognised by the 's' prefix on their individual token names (e.g. sBTC). Every Synth is an ERC-20 token [35], enabling them to be easily transferred between compatible wallets.

The Synthetix protocol has two main components to their system; Mintr and Synthetix.Exchange. The protocol uses a proprietary token they issued named SNX as the cryptocurrency that underlies much of the platform. In order to begin minting synthetic assets, one must purchase SNX. They can then stake these SNX on Mintr in order to mint sUSD, a dollar-pegged synthetic asset that can then be used to exchange with other Synths on Synthetix.Exchange. The asset classes of the Synths they offer include fiat currencies, commodities, cryptocurrencies, inverse tokens (short tokens), cryptocurrency indexes and equities.

Unlike the multi-liquidity pool system that many DEXs use, Synthetix only has one central liquidity pool. From now on, the Synthetix liquidity pool will be referred to as the debt pool, in accordance with Synthetix documentation [36]. Whenever a user stakes SNX to mint sUSD, they incur a 'debt', which can increase and decrease based on both exchange rates and the supply of Synths in the network. In order to unlock their SNX and exit the system, they must pay back the debt by burning Synths. The proportion of debt that each individual holds relative to the entire debt pool is stored by the protocol.

SNX stakers act as a pooled counterparty to all Synth exchanges, hence they are taking on the risk of the overall debt in the system. By incurring this risk, they enable trading on Synthetix.Exchange, and so are rewarded by the right to earn trading fees (typically 0.3%) generated by exchange. The protocol also has an inflationary monetary (SNX) policy [36] that rewards SNX stakers. It should be stated that stakers can only claim their rewards if they remain above the target collateralization ratio, explained in Section 3.4.3.

The conversion to any of the other Synths from sUSD (that is minted when staking SNX) can be used to speculate on price movements in various different markets can be done through the Synthetix.Exchange. When converting from sUSD to any other Synth, the source Synth (sUSD in this case) is burned, reducing the wallet address's sUSD balance and updating the total supply of sUSD. The conversion amount is established (using the exchange rate found by the oracles, and the trading fee is added) and issued by the specific Synth contract, with the wallet address being updated with the new Synth. The total supply of that Synth is updated as well.

No counterparty is required to exchange, as the system converts the debt from one Synth to another, allowing for infinite liquidity (up to the size of the debt pool). Therefore, no debt change is required to be recorded against the debt pool (just from the act of converting, not as prices change), as the same value is burned from the source Synth and minted from the destination Synth [36]. The total debt in the pool will now update going forward based upon the new supplies of Synths and their running exchange rates.

The value of all synthetic assets in the system are determined by a variety of oracles, using an algorithm that forms an aggregate value for each asset.

Synthetix.Exchange is not the only place that one can obtain Synths, as some of them trade on the open market, such as on Uniswap or Curve. For traders to be able to take profits from trading consistently, they require not only liquidity but also stability between the Synth's and the underlying price. This is because they can incur high costs if the Synth's price drifts away from its underlying. The Synth price peg is maintained by arbitrage in the market; the stakers have created debt by minting Synths, so if the peg drops they can profit by buying sUSD back below par and burning it to reduce their debt, as the system always values 1 sUSD as $1 USD. The protocol also uses secondary measures such as incentivising liquidity providers on certain Synth pools on Uniswap and Curve in order to more closely maintain the peg. Other platforms perform similar operations with external AMMs for the same reason of maintaining a correct price peg.

3.3.2 Mirror Protocol

Mirror Protocol is the second platform whose mechanisms will be investigated in this paper. The Mirror platform is relatively younger than Synthetix, with its genesis date being in December 2020. Although many of the aspects of Mirror seem similar to Synthetix at a high level, when investigated further at a smart contract level the differences become clear.

Situated on the Terra blockchain, rather than Ethereum as Synthetix is, Mirror boasted lower transaction fees when interacting with smart contracts, as well as faster finality of transactions. The reason past tense is being used here, is due to the crash of the Terra network in May 2022 [107] along with the decoupling of its native stable currency UST from the dollar (and the crash of LUNA, Terra's other native token). Mirror Protocol was heavily designed around the use of UST on its platform as the stablecoin, so once that crashed in price, the stability of the platform completely degraded and this resulted in over a 99% decrease in the TVL of the platform. This is due to both the decrease in value of the main coin held on the platform, as well as the huge number of stakers that pulled out of the system after this.

The vast majority of synthetic assets that Mirror offered, mAssets, were synthetic versions of equities and indices, offering a wide range of stock market exposure across the globe. Unlike Synthetix, Mirror did not offer any synthetic assets relating to commodities or forex currencies, however they did offer a number of synthetic cryptocurrencies, such as mBTC and mETH.

3.3.3 Linear Finance

Linear Finance is the final asset replication platform that will have its mechanisms investigated. Built and deployed around the same time as Mirror Protocol, in January 2021, Linear Finance is the only synthetic asset platform that is a cross-chain protocol, being situated primarily on Ethereum but also operating on Binance Smart Chain, with plans for future integrations with other EVM-compatible chains.

The native stablecoin used by Linear Finance on its exchange is called lUSD, and it is obtainable in a similar way as sUSD on Synthetix, by staking capital. The asset that it allows as its main collateral type is LINA, again a token native to Linear Finance. Users "build" (equivalent to mint) lUSD by staking LINA, which can then be used on Linear.Exchange to trade with any of Linear's Liquids, which are the equivalent of Synths and mAssets on Synthetix and Mirror. Similar to Synthetix and Mirror, users can stake LINA for rewards in the form of a portion of exchange fees as well as an inflationary monetary policy on LINA.

Although Linear.Exchange offers fewer Liquids than Synthetix offers Synths, they fall into the same mixture of categories including forex currencies, commodities and cryptocurrencies (however no indices).

3.4 Asset Replication Protocol Design Choices

Through inspecting the main operating mechanisms of the most prominent platforms within the DeFi synthetic asset space, we are able to identify their key differences in design choices and systematize the operations behind the current synthetic asset platforms available today.

The design choices made on the asset replication platforms have been categorized in the following way, encapsulating the main differences in implementation of the platform functions:

1. Collateral type
2. Collateralization ratio
3. User rewards
4. Liquidation mechanism
5. Inverse/short implementation

3.4.1 Collateral Type

The chosen token or list of tokens that platforms allow you to provide as collateral has a big impact on various other aspects of the platform. The main differences between platforms in this design choice is whether the collateral tokens are confined to stablecoins, or other tokens that have far more volatility in their prices. For example, Synthetix used to only allow users to stake one type of collateral on their staking platform, their own native token SNX, however more recently they began allowing people to use ETH as collateral. Mirror on the other hand allows users to stake Terra's native stablecoin UST, Terra's native token Luna or any of Mirror's synthetic mAssets that you may have minted before. Linear Finance, similar to Synthetix, only allows staking of their native token LINA in order to mint lUSD on their Build platform.

Comparing the price history of SNX and LINA to a stablecoin such as Tether's USDt, it is clear to see that the volatility of the first two is far greater than that of a functional stablecoin. Staking on a synthetic asset platform cannot be a completely passive process, where an individual can stake one day and then not look at their position for a long period of time. This is due to the user being responsible for ensuring that their collateral remains above the target collateralization ratio, otherwise they risk losing their staking rewards, and if not corrected in a suitable timespan they risk being liquidated and facing a penalty resulting in capital loss.

The change in their collateralization ratio is due to the ratio of their collateral value to that of the portion of debt they have obtained in the overall system, for example from minting sUSD when staking SNX on Synthetix. This ratio depends both on the price of the debt and how that changes over the staking period, but also the price of the collateral itself. Using a collateral type that has a lower volatility, such as USDt, reduces the risk of liquidation of your position, as there is only volatility within the debt half of the equation. Said equation is shown later in equation 3.1. Using a stablecoin as collateral means that the P_c variable in the equation is relatively fixed (compared to an asset like SNX or ETH).

It is important to note that just because a platform offers a stablecoin as means of providing collateral for staking, this does not necessarily make that protocol safer. Mirror Protocol is a perfect example of this – although they offered collateral staking in UST, the decoupling and eventual collapse of the price of UST, leaving it no longer pegged to the dollar and resulting in the collapse of the Terra network, left users with gigantic losses as all of their assets related to Terra network tumbled in price, leading to mass liquidations on the Mirror platform, which it currently has not recovered from.

	Synthetix	Mirror	Linear Finance
Collateral Type	SNX, ETH	UST, aUST, LUNA	LINA

Table 3.1: Collateral type allowed on different platforms.

3.4.2 Collateralization Ratio

The chosen collateralization ratio for synthetic asset platforms has a sizeable impact on how attractive it is to users. Over-collateralization is key for allowing these platforms to operate, ensuring that the value of debt in the system will not fall below the value of staked capital. However, there is a design choice to be made in terms of how overcollateralized the platforms want their users' positions to be.

The main trade-off in this decision is that between capital efficiency on the platform and risk of platform failure in a flash market crash. Setting the collateralization ratio to be high provides more assurances that the debt level will always remain lower than the staked capital, however it can greatly reduce capital efficiency on the platform. When Synthetix first began in 2018, their target collateralization ratio was at 800%, meaning that for every $800 for SNX that you would stake on the platform, you would be able to mint $100 sUSD, which could then be traded or swapped on their synth exchange for other synthetic assets.

A user's collateralization ratio can be calculated in the following way:

$$r_t = \frac{P_c Q_c}{\sum_{i=1}^{n} P_{mi} Q_{mi}} \tag{3.1}$$

And in order to prevent liquidation:

$$r_t \geq r_{liq} \tag{3.2}$$

Where:
r_t - collateralization ratio
r_{liq} - liquidation threshold
P_c - price of collateral asset
P_m - price of minted asset
Q_c - quantity of collateral asset
Q_m - quantity of minted asset
n - number of different minted assets

An example of some collateralization ratio calculations and how the value changes with changes in asset prices are provided in Appendix A.1.

For an individual trying to decide whether the benefits of participating in the DeFi world of synthetic asset trading, compared to their traditional bank or broker, the required value of collateral may seem exceptionally high, especially given that many brokers offer provisions for undercollateralized and leveraged trading. If the user is required to deposit 8x or more collateral to trade the same value position, they may feel disincentivized to trade with the platform. When factoring in that your collateral value may decrease towards the liquidation threshold, meaning it is recommended to have capital on the side as well as in the position, that can be used to increase the collateralization ratio again to avoid liquidation in certain cases, it becomes clear that there are big issues with capital efficiency when the collateralization ratio chosen is too high.

On the other hand, if the platform lowers the collateralization ratio too much, they are at a greater risk of potentially having to halt trading on the platform in event of the debt value rising to be greater than the collateral value, which would not only demonstrate the instability of the platform, discouraging individuals to use it, but also could lead to great losses of platform fund capital, if this is required to be used to pay off some of the outstanding platform debt. In the case of platforms that use their protocol (non-stable) native token as means of collateral, this could too see huge drops in value if platform trading volume decreases, triggering a whole new risk of mass liquidations.

Over time, as could be expected given the situation above, we have seen a general decrease across the board in required collateralization ratios on synthetic asset platforms. Synthetix initiated its platform with 800% target collateralization ratio, then eventually decreased it to 700% in 2020, then to 600% and 500% in 2021, to 400% in 2022 and it is now sitting at 300%. Mirror Protocol's genesis contract began with a different approach, requiring only a target collateralization ratio of 150%, however they assigned multipliers for different types of collateral asset. These multipliers where higher for more volatile assets, for example LUNA or their governance token MIR (before it was delisted as a collateral type) acting as a collateral premium. The multiplier for these tokens was set to be 1.33 (i.e. the target collateralization ratio for these assets is 200%), whereas that for UST was 1. Linear Finance has maintained a target collateralization ratio of 500% since its genesis.

Target Collateralization Ratio vs Liquidation Threshold

One of the aspects of collateralization ratios that hasn't been mentioned yet is the difference between a platform's **target collateralization ratio**, which is what I have been referencing up to this point, and the **liquidation threshold**. The target collateralization ratio is the value that the positions must be initially overcollateralized to, hence the importance when minting, however positions don't tend to be liquidated at this value, instead this is at the lower value that is the liquidation threshold. In order to incentivize users to maintain their collateralization ratio above the target ratio, platforms tend to only allow users to collect staking and fee rewards if they keep their ratio above this value. If it falls below, they will forfeit the rewards gained over that reward staking period. This gives them an opportunity and a further reason to correct their collateralization ratio before it reaches a point where their position requires liquidation. The fewer liquidations on the platform, the more stable it can be viewed, as it shows that the overall value of the debt stays well under that of the collateral, especially with a high collateralization ratio.

One interesting observation, visible in Table 3.2 is that while both other platforms have a target ratio that is different to its liquidation threshold, Mirror's target ratio is the same as its liquidation threshold, meaning that as long as the account is not flagged for liquidation, rewards are being earned.

Lock-up Period

Some platforms in their early stages will require users to agree to lock up their capital for a certain period of time if they want to stake it. This period can range from weeks to months all the way up to one year (the longest period observed through research of platforms). The platform's motivation behind this is to try to ensure that there will be sufficient staked capital when initially growing their platform in order that it can handle an increasing number of trades. They will earn rewards over this time period, however this adds another element of risk to stakers, due to the fact that if there is a crash in market prices over the course of that year, which is not uncommon in that time frame within cryptocurrency markets, they will not be able to pull out of the staking position and sell their tokens in order to try and readjust their portfolio and preserve some capital.

	Synthetix	Mirror	Linear Finance
Target Ratio	300%	150%	500%
Liq. Threshold	150%	150%	200%
Asset Weighting	no	yes	no

Table 3.2: Collateralization ratio for different platforms.

Opening New Positions

The general equation for determining how many tokens are minted when opening a new position on an asset can be found by rearranging equation 3.1 for a singular asset:

$$Q_m = \frac{P_c Q_c}{r_0 P_m} \tag{3.3}$$

Where r_0 is the initial chosen collateralization ratio, and all other variables have the same meaning as in equation 3.1. r_0 is a chosen value, that must be greater than r_{target} - the target collateralization ratio. The greater the value of r_0 chosen, and hence the further away from the target collateralization ratio, the lower the chance of liquidation of the position due to collateral asset and minted asset price fluctuations.

Depositing/Withdrawing Collateral from Position

A user who holds a collateralized position already can add collateral to improve their collateralization ratio r_t, or withdraw collateral up to the r_{target}. Q'_c is positive if adding to the position, and negative if withdrawing from the position.

The equation for this process is as follows:

$$Q_m + Q'_m = \frac{P_c(Q_c + Q'_c}{r_{target} P_m} \tag{3.4}$$

If the user is withdrawing from the position, they will receive $Q'_c - fee_{protocol}$ into their account.

Minting/Burning Assets

The general equation for determining the minimum amount of collateral that must be held in the position after a mint/burn is:

$$Q_c \geq \frac{r_{target} P_m (Q_m + Q'_m)}{P_c} \tag{3.5}$$

Where Q'_m is the quantity of newly minted tokens (which is negative if referring to newly burned tokens), and Q_m is the quantity of the asset that is already minted and held in the position.

3.4.3 Rewards

Staking rewards and offering a share of platform trading fees are the main incentive for users to provide liquidity to these platforms. Platforms stop providing rewards to users who hold positions under a certain collateralization ratio called the target collateralization ratio, usually set to be higher than the liquidation threshold. Setting it higher is in order to give a chance for liquidity providers to burn some of their chosen asset in order to correct the position before their account gets flagged for liquidation. Users receive a portion of the total rewards for the platform or their pool based on the ratio of the capital they have staked, to the total value of staked assets on the platform or that pool.

Rewards on all of the platforms investigated are not collected automatically by stakers. Instead, there are defined staking reward periods (typically 1-2 weeks), over which rewards build up for individuals with staked collateral. These rewards are offered through inflationary token mechanisms of their native tokens, as well as receiving a portion of the trading fees on the platform. At the end of each period, users have a set amount of time, (again, typically 1-2 weeks) in which they can claim the rewards they have accumulated on their account over that period. If the rewards are not claimed by the staker by the end of this claiming period, the rewards tend to be lost by the user and distributed through the platform to other stakers, or they are transferred to a fund linked to the platform, used for proposals suggested and voted on within the governance element of the platform.

The way in which rewards can be claimed varies by platform, with the main platform design choice being whether claiming is immediate or requires a lock-up period. Platforms that use immediate claiming allow users to build up rewards over a reward staking period, and then once that period is over they can withdraw the reward assets directly to their wallet. Synthetix is one of the platforms that allows users to immediately withdraw their rewards, and Mirror follows a similar methodology.

Other platforms, such as Linear Finance require a vesting period after the staking rewards period is over, in which time the rewards cannot be withdrawn. Out of the platforms investigated, 1 year tends to be the standard time required for a lock-up. Similar to the risks associated with staking lock-up periods, this may lead to capital losses if the value of the asset being rewarded decreases over time, however Linear Finance offers a service to reduce the impact of this risk. Their platform not only uses the value of collateral and debt to calculate their collateralization ratio, but also includes the value of the distributed rewards locked-up on an individual's account in this. This means that they can use this locked-up capital to mint more assets, giving utility to the rewards capital even if they can't withdraw it directly at first.

	Synthetix	Mirror	Linear Finance
Reward Assets	SNX	MIR	LINA, lUSD, BUSD
Claiming Period	1 week	1 weeks	2 weeks
Vesting Period	none	none	1 year

Table 3.3: Rewards information of different platforms.

Asset Weighting

Asset weighting is a unique feature that Mirror implemented, providing different rewards weightings for different synthetic asset pools. This means that staking in some pools will lead to a higher APY in terms of rewards than others. In this way, they are able incentivize users to stake on certain pools, increasing demand for the tokens in these pools. For example, the weighting on the MIR pools is 3x greater than that of the synthetic mAsset pools on Mirror, which is again 3x greater than the weighting on newly white-listed mAssets. This leads to a 9x difference in rewards for users, just depending on which pool they stake in. Although Synthetix does not have a weighting system implemented on their platform, they do occasionally provide additional incentives for providing liquidity for specific Synths through their AMM partners, by providing them with capital to increase rewards on the staking pools there.

3.4.4 Liquidation Mechanism

The way in which platforms deal with user staked positions that have fallen under their required collateralization ratio and has a sizeable effect on the stability of the protocol. The protocol must ensure that the position is liquidated before the value of the collateral falls underneath that of the debt the user must repay.

Once a position has been flagged for liquidation, there are two distinct liquidation mechanisms that are used in the chosen platforms evaluated. There are some variations within those two in terms of how they are implemented within the platform, and how users interact with the related smart contracts. These two mechanisms are the auction liquidation and the fixed spread liquidation [37].

Auction liquidations typically consist of two phases; the first in which liquidators submit increasing bids to repay the full debt associated with the now-undercollateralized position, and the second in which the liquidators submit decreasing bids relating to the amount of collateral they are willing to accept for paying that full debt. Mirror is an example of a platform that uses auction liquidations[38].

Fixed spread liquidations consist of a single atomic operation, where the position that requires liquidating can be liquidated in a single operation, and the debt is repaid all at once for a portion of the collateral without the requirement of process such as an auction or multiple operators. In fixed spread liquidation, the liquidator receives the collateral at a fixed discounted rate, providing them with the incentive to perform the operation.

Fixed spread liquidation models require lower overall transaction costs due to being able to avoid a long auction process, where many individuals are sending many transactions to complete the process. They also allow for the use of flash loans, decreasing the liquidator's risk caused by exposure to the currency being used for the liquidation [37]. Both Synthetix and Linear Finance use a fixed-spread liquidation system.

Since the genesis date of Synthetix, the first synthetic asset protocol, we have seen an interesting shift in the fixed-spread liquidation mechanisms on platforms. Over the last few years, the standard changed in two ways:

1. *Flagged account protection period.* When a position falls under the threshold, there is a period in which the platforms allow the owner of the undercollateralized position a certain amount of time to correct their position, before it is opened up for liquidators to take advantage of. This time period was as long as 2 weeks when Synthetix first implemented their liquidation mechanism, and was dropped to 3 days later in 2020. Compared to now though, this time period currently ranges from 12h on Synthetix, to a more flexible 72h on Linear Finance. Before its collapse, Mirror was still using an immediate liquidation method, with no protection period. The effect of this on the platform is that users tend to choose an initial collateralization ratio far above the liquidation threshold, as they know they will not be given a chance to correct it if it falls below. It is clear from this to see that the average allowed correction period is decreasing over time.

2. *Liquidation profit distribution.* Whereas liquidation profits used to be credited immediately and directly to the liquidator, the trend of liquidation systems is moving away from this. This older method increased the chance of *cascading liquidations*, where the selling of large amounts of liquidated capital for profit during a market crash leads to a further decrease in these collateral prices, leading to further liquidations and so on. To prevent this type of

destabilization of the protocol and significant losses for Synth holders, Synthetix overhauled their liquidation mechanism with an adaptation to SIP-148[39][40] in May 2022. Now, liquidated capital (SNX) is not sent directly to liquidators, but is distributed between all other stakers, after a 12 month period in escrow. Instead, users who flag accounts for liquidation and users that perform the liquidations receive a (configurable) flat fee that is currently 10 and 20 SNX, respectively. Linear follows a similar technique, where liquidated capital is distributed between stakers (25%) and the Linear fund (75%).

Variable Penalty

In Synthetix's overhaul, they also added some variability in the penalty faced by a user who is liquidated. Once your account has been flagged for liquidation, you can either burn sUSD to increase your collateralization ratio above 300%, which will lead to you not being liquidated, or one of two things will happen. Either the individual does what is called a self-liquidation, where you use your own SNX to pay off the debt, and the user is subject to a 20% penalty on the staked SNX, or another user will liquidate the position, leading to a 30% penalty. This provides incentives to users with under-collateralized positions to liquidate them themselves rather than waiting for a separate individual to do it.

	Synthetix	Mirror	Linear Finance
Liq. Type	Fixed Spread	Auction	Fixed Spread
Flagged Protection Period	12h	none	72h
Variable Penalty	yes	no	no

Table 3.4: Liquidation mechanism information of different platforms.

3.4.5 Inverse/Short Implementation

Within synthetic asset platform trading, although there is no order book and therefore long and short positions are not directly matched and executed, for the system to offer the same services as a traditional trading, as well as to aim for a net neutral platform position, they must offer means to take part in short trades as well. A short position on an asset is one that increases in value when the price of the asset decreases.

It is actually beneficial for platforms to try to balance the number of long positions with short positions taken on the platform, as it means that stakers will not be the ones suffering losses when minted asset price increase, but the longs will pay off the shorts and vice versa. The reason stakers would be able to more passively earn staking rewards while not having to worry so much about collateralization ratio is that if each asset in the debt pool makes up for an equal amount of longs and shorts, changes in minted asset prices would not lead to a difference in the value of debt in the pool, as they do when it is weighted to one side or another.

In traditional finance, short positions are implemented by a trader borrowing an asset from a broker and immediately selling it, with the expectation that the price will decline, so they can buy it back at a later date, return it to the broker and keep the difference in price as profit. As they are borrowing the asset, there is an interest rate they must pay over the duration of the trade, meaning that their overall profit is the price difference minus the interest paid [41].

On synthetic asset platforms this is not as simple, as there is no physical shares or commodity that is being exchanged, just a change in the debt ratio held by the platform once assets are minted. Given this fact, there are two ways in which synthetic asset platforms offer this service. The first is similar to the traditional way of implementing short positions, aptly named *traditional short*, and the alternative is called a *ranged inverse token*.

1. *Traditional Short.* A short position is opened by minting the desired asset for shorting, then the smart contract automatically sells this into stablecoin form and this is locked in the contract. When closing the position, the locked stablecoin is used to purchase the asset back, and the asset is automatically burned in order to regain the initial margin put in by the user (along with any profits or losses) [42]. Mirror and Linear Finance both used this type of short on their platforms (Linear is in the process of implementing this).

2. *Ranged Inverse Token.* The second method of implementing shorts is not via borrowing and repaying but via their own tokens. These "inverse" tokens are only currently available on Synthetix, and are initiated on the platform with an entry point, an upper price limit and a lower price limit. Its entry point is the price of the asset when the inverse token contract is initiated, the upper and lower limits are decided through voting by the Synthetix governance protocol before being listed. The naming convention for these tokens is to use an 'i' as the prefix to the asset instead of the usual long position 's', so the ranged inverse token for BTC is called iBTC.

Ranged Inverse Token Example

An example of how an inverse Synthetix token iBTC works is as follows [43]:
- Price of BTC when iBTC is added to the system/entry point: $5000
- Chosen upper limit: $7500
- Chosen lower limit: $2500

A user buys iBTC when it is first listed. If the price of BTC decreases to $4500, the inverse token increases in value by roughly 10%, and vice versa if the price of BTC increases. If the iBTC price increases to $7500, or decreases to $2500, the iSynth is frozen, and any temporary price changes after this do not reflect in the price of iBTC. Synthetix core contributors will then look to redeploy the inverse token as soon as possible, with a new entry point, upper limit and lower limit.

Ranged Inverse Token Leverage

The reason for the requirement of the upper and lower limits for the inverse token is due to the fact that by design, the further the price of BTC goes from its entry point, the more effective leverage is applied to that inverse position. This is shown in the following example:

Working on from the example above, if iBTC was at $3500 (hence BTC price has increased), moving towards its lower limit of $2500, then $1 of iBTC purchased at this point generates a price movement of $1.86 of price for every $1 that BTC moves, due to $6500/$3500 = 1.857. Clearly, the further the iBTC price moves away from its entry point, the more leverage is taken on.

Another way to view this is if iBTC is at $3500, BTC is at $6500, and BTC price decreases again to $5000, iBTC price will also move back to $5000. This is a 23% decrease in the price of BTC, but relates to a 43% increase in the price of iBTC from $3500.

Taking this to an extreme, if BTC price increases to $9999, this means that iBTC price would be $1. At this point, buyers of iBTC take on roughly 10,000x leverage compared to at entry, as every 1:10,000 movement in BTC you get a 1:1 movement in iBTC. The risk that is associated with high leverage trades means that it is necessary for the protocol to implement these upper and lower limits.

	Synthetix	Mirror	Linear Finance
Inverse/Short Implem.	Ranged Inverse	Traditional	Traditional

Table 3.5: Inverse/short implementations on different platforms.

3.4.6 Governance

Finally, an element of synthetic asset platforms that provides an extremely important role in protocol changes and ensuring that the stability of the protocol is maintained and constantly improved upon, is the governance. Platform governance is not specific to synthetic asset platforms, and is implemented in roughly the same way across different DeFi platforms, so the decision was made not to thoroughly investigate these parts of the platforms selected.

In order to make an amendment to the protocol, due to the fact that there is no central authority or body making decisions on it, a proposal must be submitted to the governance protocol. A voting system is implemented on each platform, allowing owners of the governance token to lock these into a specific governance smart contract, which then provides them with voting power proportional to the value of their locked governance tokens to the value of the all tokens locked for this proposal. Governance tokens can be obtained either by buying them directly on an exchange, or earning them as rewards for staking and participating in the platform itself. There are also voting rewards for those that participate in these proposals.

3.4.7 Platform Choices Table

	Synthetix	Mirror	Linear Finance
Collateral Type	SNX, ETH	UST, aUST, LUNA	LINA
Target Ratio	300%	150%	500%
Liq. Threshold	150%	150%	200%
Asset Weighting	no	yes	no
Reward Assets	SNX	MIR	LINA, lUSD, BUSD
Claiming Period	1 week	1 weeks	2 weeks
Vesting Period	none	none	1 year
Liq. Type	Fixed Spread	Auction	Fixed Spread
Flagged Protection Period	12h	none	72h
Variable Penalty	yes	no	no
Inverse/Short Implem.	Ranged Inverse	Traditional	Traditional

Table 3.6: Compilation of all platform design choice tables.

3.5 Direct Creation Protocols (UMA)

Where asset replication protocols offer a wide range of traditional asset classes that they have derived their synthetic products from, users must trade within the specified set they have available. UMA, also built upon Ethereum, allows the user a far higher degree of freedom when it comes to customization of the synthetic asset.

Unlike Synthetix, UMA does not make use of liquidity pools in order to operate. Instead, they have individuals design the smart contracts for the tokens they want through their platform, publish them, and then any other users can participate in the smart contract by depositing collateral. These users will act as counterparties to each other, one taking each side of the effective position created by the new synthetic asset.

Apart from the counterparty situation, the main fact that distinguishes UMA from platforms like Synthetix, is the fact that UMA doesn't use live price feeds. UMA believes that oracles are inherently insecure, as has been demonstrated by numerous flash loan attacks[44] and cases of oracle front-running across many different DeFi platforms. This leads them to want to use oracles as little as possible, and certainly not using their live price feeds to constantly be evaluating prices and collateral (due to temporary price spikes/dumps that are the result of attacks on the oracles, which can cause otherwise unwarranted liquidations).

"Priceless" contracts instead use other mechanisms to incentivize counterparties to properly collateralize their position [34]. This includes a liquidation and dispute process that rewards parties for identifying and liquidating under-collateralized positions. Unless a dispute is opened against a position, it is assumed to be solvent and properly collateralized. Price requests are only used when a liquidation is disputed. In this way they are only used as a backstop when disputes cannot be handled by mechanisms in the contracts themselves.

UMA's platform is split into two main components; its Token Facility, which is the framework for creating synthetic asset contracts, and its Data Verification Mechanism (DVM) [45], which is the mechanism used in order to solve disputes and ensure properly collateralized positions. One of the main reasons UMA has been identified separately to Synthetix, Mirror Protocol and Linear Finance is due to the fact that the products offered by UMA Protocol are not limited to individual synthetic assets. The Optimistic Oracle it has built using DVM can be used for many other applications, and these are included in UMA's TVL – in fact the top few projects UMA has listed on its website in order of TVL are not synthetic assets at all. Due to the fact that the Optimistic Oracle is native to UMA, its applications will be mentioned in this paper as they still are part of the synthetic asset platform as a whole.

3.5.1 Token Facility

The token facility refers to the smart contract on UMA which allows for the creation of synthetic tokens. Anyone designing a token in the Token Facility must provide/meet three key characteristics [46]:

1. Price identifier – the metric that will be used to derive price of the synthetic asset.
2. Expiration date – the date of settlement of the contract.
3. Minimum collateralization requirement.

The individual or entity who creates the smart contract for the new synthetic token is called the Token Facility Owner. Collateral can be provided in the form of any of the pre-approved crypto-assets, such as DAI, or an individual can create a proposal on the governance module of UMA, and hope that UMA token holders vote to approve this new collateral currency [46]. The same goes for using a new price identifier – this must first be approved by UMA token holders via a voting process.

Once the smart contract has been published by the Token Facility Owner, any other user who likes the idea of taking the other side of this trade can participate by depositing their own collateral to the contract. This entity is called the Token Sponsor. The two entities are now counterparties to each other in the trade. On top of this, any other user that thinks that the new synthetic token would be valuable (agrees with the position that the Token Facility Owner took), can deposit their collateral in order to issue tokens themselves (given there is also an interested counterparty). It is recommended to over-collateralize the position to reassure anyone taking the other position of your trade that the tokens are fully backed, and won't be liquidated before the expiration date.

3.5.2 Data Verification Mechanism (DVM)

The lack of using live price feeds from oracles means that the valuation and liquidation process that is necessary for synthetic assets must be accomplished in some other way in UMA. The mechanism they have built is underpinned by the use of their native token, the UMA token. This is used by holders for voting on both price requests that stem from the mechanism, as well as general governance issues on the platform.

Apart from the attacks on oracles mentioned previously, oracles can be very insecure in certain situations, especially ones that take off-chain data and move it on-chain. This is because there must be some relatively central source of data that is being fed to the oracle. If someone was to create a synthetic asset that derives its price from this oracle, they would have motivation to go to that price source and potentially bribe it, in order to corrupt it to swing the price of their synthetic asset in their direction for profit. The amount of money that the data source would require in order to manipulate their data is called the "Cost of Corruption (CoC)" [47], and the profit that the individual would make after taking this into account is called the "Profit from Corruption (PfC)".

UMA's DVM uses a simple economic framework to evaluate oracles, designing a mechanism to ensure that the cost of corrupting the DVM will exceed the potential profit, which eliminates the economic incentives for corrupting the DVM. This takes place in three steps:

1. Create a system to measure the CoC
2. Create a system to measure the PfC
3. Design a mechanism to keep CoC $>$ PfC

In order to measure the cost of corruption, the DVM uses a Schelling-Point style voting system, using the UMA tokens as a means of proportional vote. Token holders are asked to vote on price requests by contracts using the DVM. They are paid a reward for honest voting, and are penalized otherwise – the 'honesty' is determined by the majority vote. As long as there is an honest majority, voters will vote correctly, meaning that the CoC is the cost to buy 51% of the voting UMA tokens [47].

In order to measure PfC on the system, the PfC of each individual contract is summed up. PfC of a singular contract is the maximum profit that an attacker could make if they had full control of the DVM, including the price it returns to the contract. This value is specific to each contract – each smart contract registered with DVM is responsible for computing its own PfC values, and allowing others to read the function that calculates it. PfC is reported to the DVM system whenever fees are paid, as the fee amount is a function of the PfC value. The DVM then sums all individual PfCs into a system-wide PfC value.

A variable-fee policy is what is used to enforce the CoC $>$ PfC mechanism. Keeping the cost of 51% of the participating UMA voting tokens above the system-wide PfC is what is required to enforce this. This means that the total market cap of the participating voting tokens must be $>$ 200% of the system-wide PfC.

The system charges a periodic fee on all contracts proportional to each contract's contribution to the system-wide PfC, with larger contracts paying proportionally larger fees. These fees are used to perform 'buybacks' of the UMA token [48], which are then burned, reducing the token's supply and increasing its value, which in turn increases the market cap and the CoC. The fee amount also varies depending on how close the market price of the token is to the minimum price needed to secure the system.

3.5.3 Price Requests

When a contract owner wants to find out the price of their contract, they must submit a price request to the DVM. This begins the voting process, where token holders are asked to vote on the value of a price identifier (from a predetermined data source) at some historic timestamp, a process which takes 2-4 days to settle. The statistical mode of the voting process is the price used to settle the price request. On top of the periodic fee mentioned earlier, a flat fee is paid on every price request, in order to pay for the DVM service. This mechanism is designed so that prices are not requested often, only when they need to be, such as at settlement of the contract on the expiration date, or in a dispute on liquidation of a position.

Appendix diagrams B.1 and B.2, pulled from UMA's website[1], help to visualize the processes behind UMA's DVM and Optimistic Oracle.

3.5.4 Liquidations

Token sponsors can deposit more collateral to their position at any time, in order to avoid liquidation. They may also want to withdraw collateral if the position has moved in their favour, as long as the resulting position still has its collateral above the UMA-defined global collateralization ratio (GCR) [49].

UMA protocol, like Synthetix, rewards individuals who look for and correctly identify under-collateralized positions. Liquidator individuals can determine whether a token sponsor's position is properly collateralized based off the off-chain price feed they reference. If they believe it to be under-collateralized, they can open a liquidation request. Anyone can dispute a liquidation within its "liveness period" [49].

The liquidator submits synthetic tokens to the contract to post a liquidation bond which is pre-defined before the synthetic contract is launched. It is used for the following:

1. To back the liquidator's belief that the position should be liquidated.
2. To indicate the size of the position to be liquidated.
3. To close the sponsor's position.
4. To cover the cost of calling the DVM if liquidation is disputed.

If the liquidation is not disputed, the bond is returned to the liquidator along with a reward, however they will lose a portion of the collateral if their liquidation is disputed and found to be not valid.

If someone disputes the liquidation, this individual must also post a bond. Once raised, a price request is made to the DVM, which returns the value of the price identifier at the time of liquidation. If the token sponsor was undercollateralized, the dispute is resolved with the liquidator receiving all of the token sponsor's collateral for the position. The disputer will also lose their bond.

If the price returned by the DVM shows that the token sponsor was sufficiently collateralized at the time of liquidation, the disputer receives back their dispute bond along with a dispute reward. The liquidator receives collateral equalling the value of tokens they wanted to liquidate, minus the improper liquidation reward and the dispute reward. The token sponsor receives any remaining collateral and a reward for improper liquidation.

Table 3.7 demonstrates the different pay-outs [49]:

Scenario	Token Sponsor	Liquidator	Disputer
Liquidation not disputed	0	Token Sponsor's collateral + Liquidator bond	0
Token Sponsor over-collateralized	Token Sponsor's collateral - Value of tokens + Improper liquidation reward	Value of tokens - Dispute reward - Improper liquidation reward	Dispute bond + Dispute reward
Token Sponsor under-collateralized	0	Token Sponsor's collateral + Dispute bond + Liquidator bond	0

Table 3.7: Pay-outs for different scenarios in DVM liquidations.

Unlike Synthetix, where liquidation is an almost automatic process once it has begun, due to the fact that the ability to liquidate a position is determined by a live price feed rather than DVM, liquidators in the DVM put themselves at risk of losing capital if their liquidation is unjust.

It is worth noting that it is possible to create tokens though UMA's Token Facility that are "non-liquidatable", meaning that there is no risk of liquidation on either side of the counterparty trade, and collateral does not need to be managed closely. To be able to provide this type of product, these tokens have configurable capped up-side and down-side pay-outs.

3.5.5 Token Example

Through their Token Facility UMA allows for the creation of exotic synthetic assets that previously either did not exist on the blockchain or did not exist at all. An example of one of these tokens is the uGAS token – a synthetic futures contract that varies with the price of gas on the Ethereum network. The contract settles at the 30-day median gas price at the end of each month [50].

In this case, the expiration date of each uGAS token is the end of each month (uGAS-JAN21 expires on Feb 1st), and the reference index is the 30-day median gas price. The token can be used to simply speculate on the price of gas, or hedge against the holder's gas costs each month. For example, an individual who takes part in yield farming may carry out many transactions each month, accumulating high gas costs over the period. They may have an amount they expect to pay based off previous transaction volumes and gas costs, and budget their portfolio accordingly.

Normally, if gas costs increase, this individual would have to just accept that their yield farming profits will be lower that month. However, if this individual goes long the uGAS token for that month, they are able to hedge the increased cost of the gas they are paying with the profits realised from uGAS at the end of the month, allowing them to mitigate the gas cost risk they previously had.

This is just one of the many innovative examples of tokens that have been created with the UMA protocol.

3.5.6 Token Facility: Types of Products

There are 5 different types of tokens [51] that can be designed and implemented using UMA's Token Facility, each offering a slightly different use case [52]:

1. Key Performance Indicator (KPI) Options
2. Success Tokens
3. Range Tokens
4. Call/Put Options
5. Long Short Pair (LSP) Tokens

KPI Options

KPI Options are tokens that are used to perform "smart airdrops". An airdrop is when a cryptocurrency project sends free coins or tokens to wallet addresses in order to promote the awareness of a new currency or their platform [53]. The aspect of KPI options that differs from a normal airdrop is that they pay out more rewards if a project's KPI reaches a predetermined target before the token's expiry date. This is done in order to further align the interests of the holders of tokens of this new platform with the interests of the protocol.

The motivation behind creating a token like this is that traditional airdrops of tokens can act as a great fuel for network growth, but they can also result in increased sell pressure on the new token, as many users who sign up for these airdrops sell immediately for the free profit, rather than holding and benefiting more if the protocol succeeds.

Some examples of the Key Performance Indicators that can be used for the token are TVL (options pay out more if a specific TVL is hit), Trading Volume (options pay out more as trading volume increases) and DAU (options pay out more as unique number of addresses transacting with the protocols smart contracts increases).

Success Tokens

Success Tokens are a way of allowing DAOs to raise funds without requiring to offer token discounts upfront. A common way for DAOs to raise funds is to approach venture capitalist investors asking for capital, which they provide in return for a discounted price of the protocol's tokens.

For each token that an investor buys, they receive a bonus call option as well. Both the token and the call option are locked into the smart contract until the expiry date. The advantage to the investor is that the call option may increase the pay-out of the token to the investor, but only if the price of the token in question has increased over that time period. An appendix diagram pulled from UMA's Success Token documentation, Figure B.3, visualizes the pay-out of a Success Token [2].

In this way, not only does the DAO gain a strategic partner who profits even more now if the protocol and token succeed, but they have also increased their treasury compared to had they approached the investor with a discounted token sale. The investor has also given themselves increased exposure to their potential upside profits compared to buying discounted tokens.

Range Tokens

DAOs may have restrictions on when their tokens can be sold, but they may need capital at the moment. Range tokens allow DAOs to borrow funds using their native token as collateral, without liquidation risk, allowing them to delay selling those tokens to a later date (betting on a higher price and therefore greater profit).

The tokens can be viewed as an equivalent to convertible debt, which allows companies to receive funding now without issuing any shares upfront. Once the token reaches maturity, if the debt is not paid, the holder of the range token is paid out with an equal amount of the native token collateral put down by the DAO. Unlike with other borrowing/lending protocols in DeFi, the advantage to the DAO is that their position cannot be liquidated. For this reason, there is a cap on the number of tokens that can be given to the range token holder.

The holder of the range token has a similar exposure to being short a put option, where they have exposure to the downside of a token below a certain price. In order to compensate this exposure, the holder is also given a call option for the token price, and a minimum number of tokens is given to the range holder at expiry no matter how much the token rallies.

At the time of expiry of the token, the range token holder is given their native tokens, the amount of which is in a range of a minimum and maximum value. The range token holder also receives a constant payout in dollars between a specified price range on the token.

Due to this, range tokens are suited for individuals who are confident in the long term survival and success of a project, as they may be able to buy the range tokens on decline in token price and earn yield on their position while the token price is still in the range.

An appendix diagram, pulled from an article written on Medium by UMA, Figure B.4, visualizes the pay-out of a Range Token [3].

Call/Put Options

Call/Put Options offered by UMA replicate normal call/put options in traditional finance, though implemented through smart contracts. They can be used by DAOs to offer yield opportunities to individuals who own the tokens, as well as a form of leveraged exposure for speculators. The options are traded against the DAO's project token, allowing the DAO to create liquidity without the disadvantages of a discounted token sale outlined above.

The creation process for these options is permissionless, allowing the DAO issuing them a greater degree of control over the design process, as opposed to the high costs and less control experienced when creating custom options through a trading platform or bank. The option pay-out profile is the same as a traditional option.

LSP Tokens

Long Short Pair contracts allow for the creation of products that have a capped pay-out, and are non-liquidatable. There are a number of different contract templates, including binary pay-out options, linear pay-out, covered calls and range LSP, allowing for heavily customized products.

3.5.7 DVM/Optimistic Oracle: Integrations

One of UMA's main distinctions from the asset replication platforms, is the fact that although it can be used to create tokens as described in the previous section, it also offers its Optimistic Oracle up for use in other platforms, so that they can take advantage of the DVM. The reason they do this is that even when the Optimistic Oracle and DVM are used on other platforms, they still require UMA tokens to operate, leading to increased buying pressure for the token. From UMA's list of projects/products by TVL on their website[54], none of the top 3 entries are actually tokens created with the Token Facility. These top three projects are actually platforms in themselves, who chose instead of using oracles like Chainlink or Band Protocol to bring data onto their platform, they use UMA's Optimistic Oracle. UMA calls these projects "Integrations".

The first platform is called Across, which is a cross-chain bridge that is able to execute transactions between chains nearly instantaneously [55]. The Optimistic Oracle is used to provide proof that tokens have been deposited from one chain to a relayer[56] before funds are released to the second chain. The second platform is once called Sherlock[57], which describes itself as a risk management platform, designed to provide DeFi protocols with reliable coverage against smart contract exploits. Finally, the third integration with UMA is a decentralized betting platform called Polymarket[58], which uses the Optimistic Oracle to settle bets, and then smart contracts within the platform make the pay-outs based on the DVM result.

Chapter 4

Data Insights

In order to identify trends and patterns within the synthetic asset platform space, on-chain data relating to the platforms must be collected and analysed. Drawing conclusions between the difference in platform design decisions proves difficult due to two reasons. Firstly, data in this case is often limited by volume, with there not being enough transactional history on one platform to directly compare it to another that has sufficient data. Secondly, even where there is sufficient transactional volume, collected data on a specific platform design choice is often relevant only to a short time period of the platform's life, due to the fast paced nature of the cryptocurrency industry that leads to constant adjustment of the platform protocols to improve them.

The choice was made to not compare data between the two largest platforms, Synthetix and UMA, due to the vast differences in the products that they offer and their use-cases. Synthetix and other asset replication platforms are intended for individuals to speculate on prices of the specific assets that they offer. UMA on the other hand, whilst offering some products that allow an individual to gain custom exposure to a product they want to speculate on, focusses a lot more on different financing opportunities for much larger entities such as DAOs for other cryptocurrency projects. For this reason, the assets on asset replication platforms tend to be traded at a far greater frequency than many of those on UMA, which are marketed on their website as long-term financing options.

Another reason direct comparison of the platforms is too difficult is due to the concentration of trading around certain assets on the platform. Within asset replication platforms, many users trade the same set of pre-approved assets, leading to large trading volumes confined to a relatively small number of tokens. However, within direct creation platforms, such as UMA, trading volume tends to be spread across a larger number of assets and projects.

4.1 Data Collection Method

The choice of data collection method used was the decentralized indexing protocol The Graph, used for querying blockchain data. The protocol allows you to write GraphQL queries relating to the APIs for each platform that have pre-built schema. Elements of the schema are used in the queries to pull data. In order to be able to query data for a specific platform, a subgraph must be either used or created, that has the relevant platform data pre-indexed, allowing the queries to run much faster than taking the data directly from the EVM or respective blockchain. One of the main reasons for not directly taking data off their blockchains is due to the fact that the different platforms are situated on different blockchains - if they were all on Ethereum then the EVM approach would have been used.

Queries return .json files as output, and these in turn must be processed in order to obtain the data in a form that can be manipulated and plotted as a graph. In order to do this, MATLAB was used as the data processing tool.

4.1.1 Issues

There were some issues in the data collection process that led to only being able to obtain useful data for Synthetix. Although all three platforms out of Synthetix, Mirror and Linear Finance have

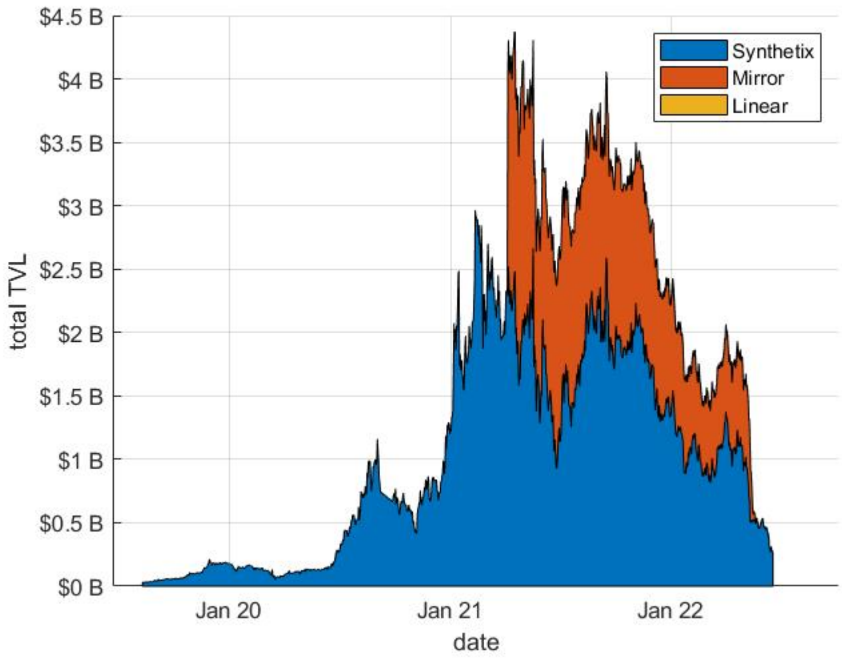

Figure 4.1: Graph of TVL over time for the chosen investigated platforms.

APIs for GraphQL queries, all written in the protocol documentation papers, not all performed the same function.

The API used for Synthetix was built bearing in mind that users may want to find historical aggregated statistics on the platform, hence there were no problems with data retrieval for Synthetix. Mirror's API on the other hand, although similar to Synthetix in the fact that its schema included elements that allowed the pulling of historical data easily, much of the data being pulled was incorrect. For example, total value staked on the platform was returning negative values, and other historical queries returned no data whatsoever. This could be due to the crash of the UST stablecoin and Terra network, leading to Mirror decide to stop maintaining the back-end that is used to handle the requests. Finally, Linear Finance does have a GraphQL API, but this is used only for developing applications alongside Linear's platform as well as querying information to do with these applications, hence it stores no historical data. Also, there would be very limited data that would be able to be retrieved from Linear, so it would not suit being compared to Synthetix even if the data was retrievable through GraphQL.

4.2 Asset Replication Platforms

4.2.1 Total Value Locked (TVL)

Figure 4.1 includes the TVL of each of the asset replication synthetic asset platforms investigated in this paper. Although essentially invisible, having the Linear Finance TVL incorporated into the data demonstrates why some of the other smaller synthetic asset platforms were not included in this paper. It is clear to see that the vast majority of synthetic asset platform activities took place on Synthetix and Mirror over the past few years. One element you might notice is that the mirror TVL drops down to almost zero before the end of the graph. This is due to the collapse in the Terra network and UST price that left almost no volume going through Mirror. From the TVL it is clear that Mirror was a successful protocol while it was running, capturing a very significant portion of the synthetic asset market from its infancy. It will be interesting to see going forward if a replacement for Mirror Protocol appears in the industry, or if the protocol tries to rebrand on a new network.

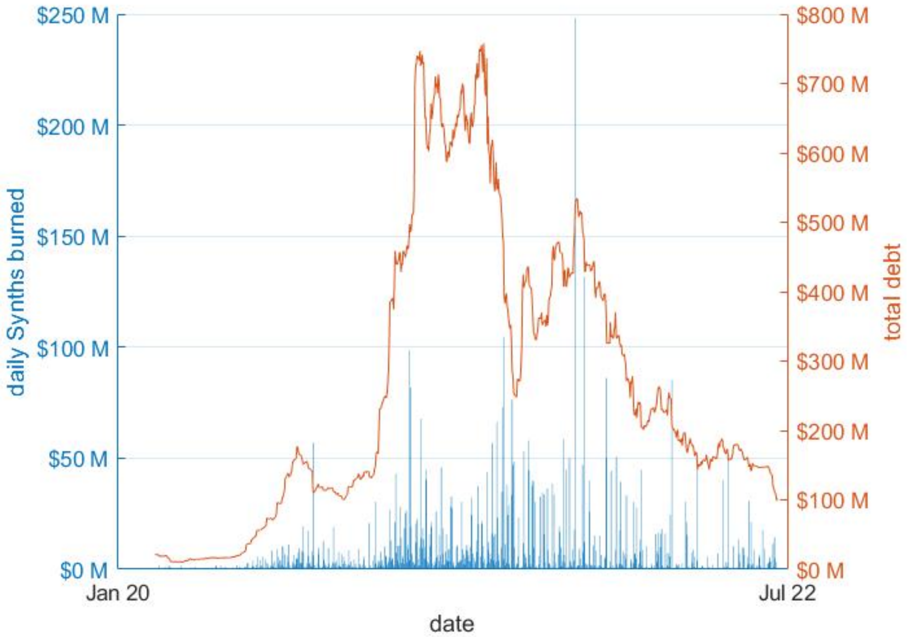

Figure 4.2: Graph of daily value of Synths burned against total system debt.

4.2.2 Daily Burned Synths

It is possible to see in Figure 4.2 that in most cases, when there is a sharp increase in burned assets, there is a visible decrease in total debt in the system, as expected, due to each burn of assets decreasing the total debt. What is also visible is that there is a far greater volume of Synths being burned during the years 2020 and 2021 compared to 2022, and this is also shown in the decrease in total debt since the start of 2021. This could be explained by the huge ramp-up in publicity that cryptocurrencies as a whole were receiving around the start of 2021, drawing many new users into crypto and DeFi.

Another interesting point is that there is a very similar relationship of burning data with the daily average price of SNX, visible in Figure 4.3. For each day that has a large value of Synths burned, there is a visible decrease in price of SNX.

The fact that they have very similar relationships is shown in Figure 4.4 of SNX price plotted along with the total debt in the Synthetix system.

This can be explained by the fact that when a liquidation occurs, the liquidator burns some of their capital in order to reduce the debt of the undercollateralized position. They then receive a portion of the SNX used as capital for the liquidated position as a reward. In many cases, this SNX is then sold to USD or stablecoin for profit by the liquidator. If there is a high volume of liquidations, there will be a high volume of Synths being burned, as well as high volumes of liquidator SNX rewards being sold, which can push the SNX price down.

The most obvious example of this is the data point showing the 11th June 2021, the date where the amount of Synths burned reached almost $250M. This was due to a very large wallet not managing their staked position and allowing their position to fall under the liquidation threshold of 200% at the time. This large liquidation led to a liquidator selling off the SNX as described, which pushed the price of SNX down, which led to more liquidations, and so on and so forth. The total value for liquidations on this day was $19.4M, and it led to a daily SNX price decrease of 14.8%.

This is an example of the concept of *cascading liquidations*. The new liquidation mechanism for Synthetix (adaptation of SIP-148) should mitigate this risk, as liquidators will no longer receive a portion of the liquidated SNX directly (which can be extremely large in big liquidations like the one mentioned), but will receive a far smaller flat fee and the rewards will be distributed to other stakers. The new reward vesting period of one year will help with this as well.

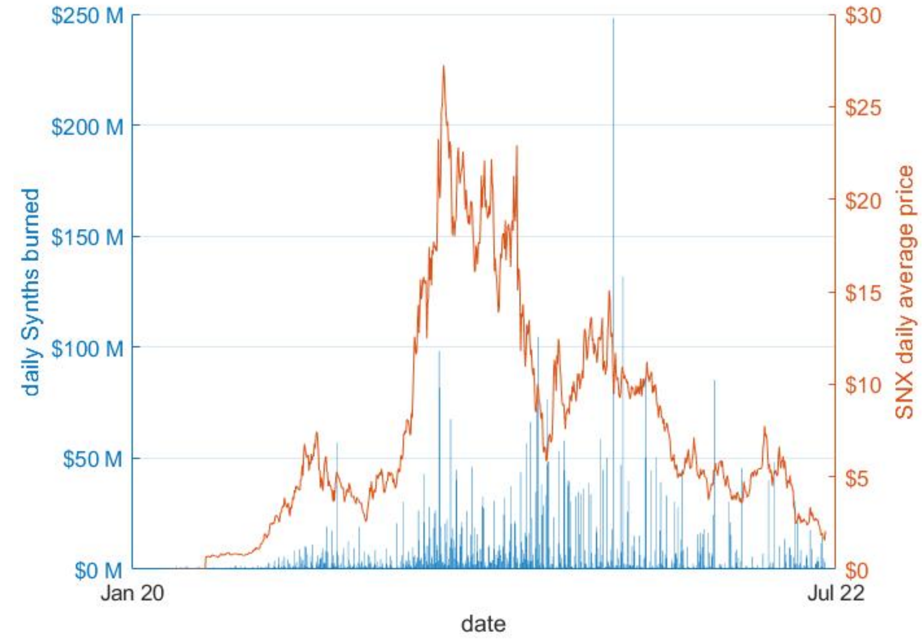

Figure 4.3: Graph of daily value of Synths burned against daily SNX price

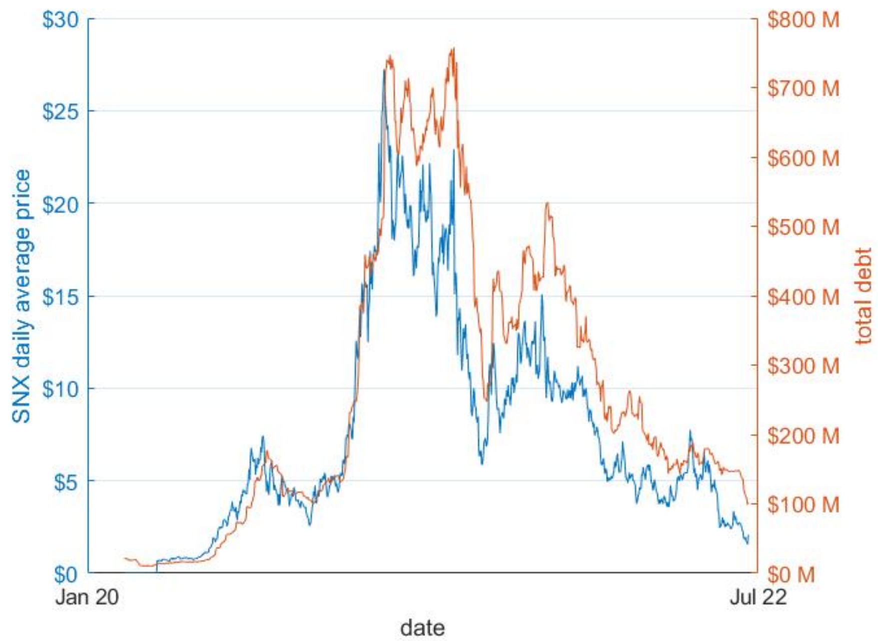

Figure 4.4: Graph of SNX daily average price compared with total system debt.

4.2.3 Daily Minted Synths

Similarly to previously but reversing the argument, it is clear to see in Figure 4.5 that on days with extremely high value of daily Synths minted, the total debt increases visibly. We have not seen a day with as large of a value in terms of daily minted Synths as we have seen for the maximum value of burned synths. The maximum value for daily Synths minted was found to be $153M.

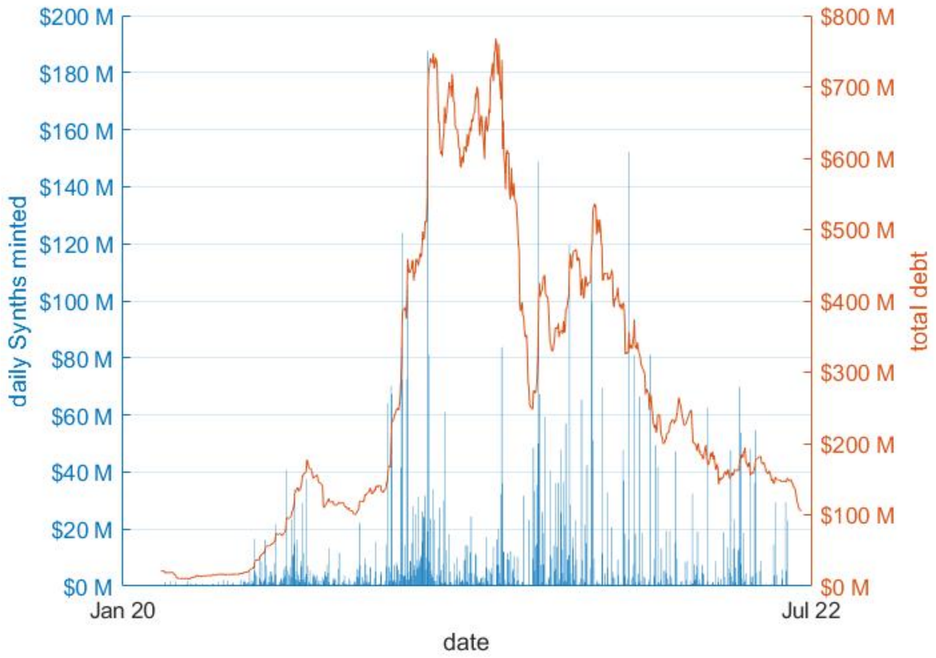

Figure 4.5: Graph of daily value of Synths minted against total system debt.

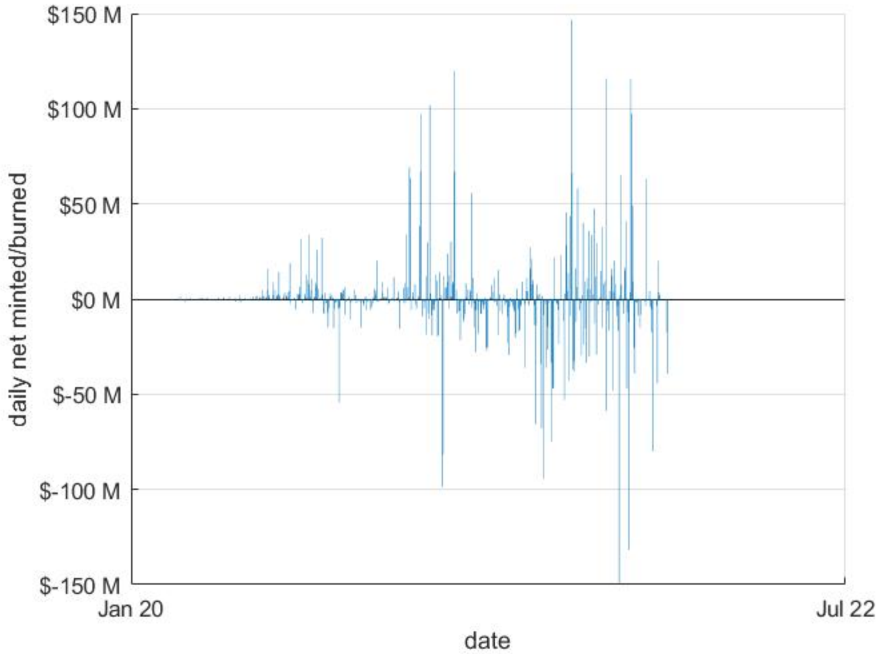

Figure 4.6: Graph of daily net mints or burns value in the Synthetix system.

4.2.4 Daily Synth Net Mint/Burn

Figure 4.6 shows the daily net outcome of all mints and burns in the system. If the value of daily Synths minted exceeds that of daily Synths burned, then the net minted/burned value is positive. In the opposite case, the net minted/burned value is negative, meaning there have been more burns than mints in terms of value on that day. Another way of viewing this statistic is the net change in debt in the system for that day. Worth mentioning is that the bar running off the bottom of the graph actually reads at -$248M. This is the date of June 11th 2021, when the cascading liquidations problem occurred.

4.2.5 Daily Active SNX Stakers

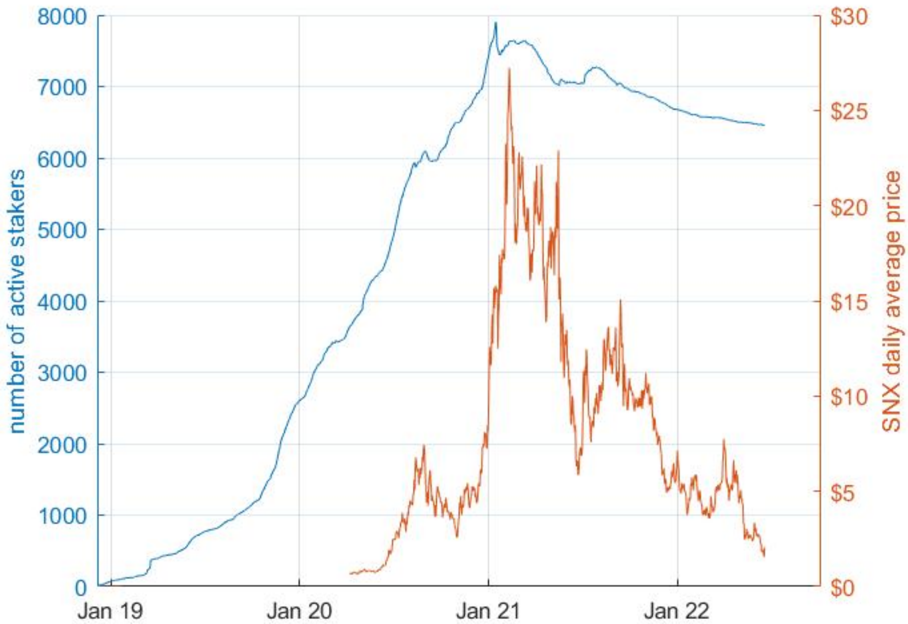

Figure 4.7: Graph of the number of daily active stakers against a graph of SNX price.

Figure 4.7 shows the relationship between daily active stakers, meaning the count of wallets that currently have SNX staked in a Synthetix smart contract, and the daily average price of SNX. The SNX token was only launched and subsequently introduced to the Synthetix ecosystem in February 2020, which is the reason there is no price data for SNX before that point.

The number of active stakers on the Synthetix platform increased steadily from January 2019 to around January 2021, at which point its value, along with the price of SNX (and many other cryptocurrency prices) peaked. While the price of SNX and the total debt in the system both decreased sharply after this, surprisingly the number of active stakers only had a slight downturn. Peaking at 7943, the number of active stakers only decreased by 18.2% to 6497, while the price of SNX over this time decreased by 90.1% (as of June 2022).

Although at first glance this seems like there must be quite a large number of individuals who have been actively managing their staked positions over this whole time, in reality this is not necessarily the case. The only way that a user that is marked as "active staker" by the protocol can be unmarked and taken off this list is by burning their minted sUSD and withdrawing all their staked SNX. If a staked position is just left unmanaged for a long period of time, what will happen is that each time the position falls underneath the liquidation threshold, someone will partially liquidate it until its collateralization ratio meets the target ratio again. This will happen time after time, taking away a portion of the total initial position value each time it is liquidated. This means that many of the wallets marked as "active stakers" may only hold very small positions of staked SNX due to repeated liquidations, and they may not even know they have SNX still staked on the platform at all.

4.3 Direct Creation Platforms

The data relating to UMA's different synthetic assets proves difficult to collate and compare, due to each token having configurable collateralization ratios, collateral types allowed and pay-out functions amongst other qualities. However, what can be done is combining the different types of current products listed on UMA's projects portal of their website[54], and collating their TVL data to see the distribution of how users are interacting with UMA. Doing this produces the chart in Figure 4.8.

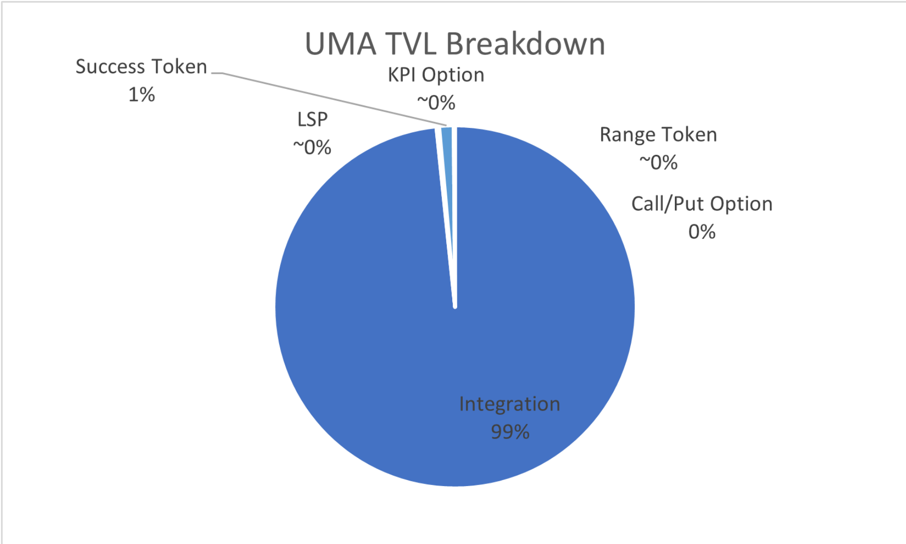

Figure 4.8: Pie chart of current TVL of different UMA projects.

It is clear to see that the vast majority of TVL registered by UMA is locked into the integration platforms partnered with UMA, as opposed to the tokens that can be built using the platform. These integrations account for $75.1m out of the $76.4m of overall TVL for UMA.

In order to get a better picture of the actual tokens that are being created with the Token Facility, we can remove the integration platforms TVL from the data, leaving us with the chart in Figure 4.9.

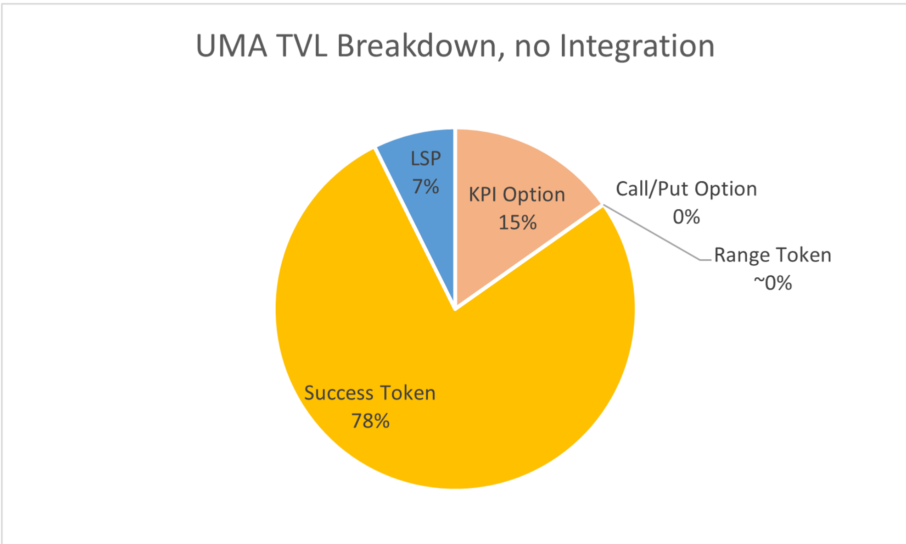

Figure 4.9: Pie chart of current TVL of different UMA projects, not including UMA's integration projects.

We now see a clearer picture of tokens being built. The TVL of all these tokens combined is $1.25M. Of the 16 synthetic asset tokens listed on UMA's project portal, we see that most of their TVL is confined to the Success Token product, valuing at $974k. The next highest TVL is in the KPI Options product, which consists of $191k of TVL. After that we have the Long-Short Pair Tokens, which have a combined TVL of $92k. The Range Tokens currently make up for only $217 of TVL, and there are no active Call/Put Option Tokens listed.

It is important to remember that many tokens built on UMA have expiry dates, and so this TVL data is just a snapshot of the assets that are currently live. UMA also allows you to view the data for their expired tokens, and this provides for an interesting insight. When including the TVL of tokens that are no longer active (bringing the total number of listed tokens to 74), with the TVL value being taken at the time of expiry, we see that historically the largest TVL for a Token Facility-built token is for a Range Token. This Range Token was the "UMA $4-$12 Range Token August 2021", meaning that it expired in the stated date. The TVL of this token at the time of expiry was $1.2M.

This shows a stark contrast to the current snapshot of TVL data, as Range Tokens make up for <1% of current TVL, but have clearly been a large portion of TVL in the past. This data tells us that due to the common quality of expiry dates within the space of tokens built with UMA, the distribution of TVL across the different products UMA offers can vary wildly depending on the date chosen for the snapshot.

Chapter 5

Conclusion

In this paper we investigate the four synthetic asset lending platforms that capture over 82% of all TVL within the synthetic asset platform space. The key mechanisms that allow these platforms to operate are studied and systematized, comprising of staking and collateralization, liquidation mechanisms, platform user rewards, and their implementations of short positions. The various different platform design choices and configurations are categorized and documented, also identifying any trends in platform changes over the past 4 years.

While there is limited data due to only two of the platforms having survived for over 2 years (as of June 2022), and the data from one of those platforms not being comparable to the other (asset replication vs direction creation platforms), some trends were able to be identified. We found that within asset replication platforms, collateralization ratios (both target ratios and liquidation thresholds) are decreasing as time goes on, in order to improve capital efficiency on the platforms, in an attempt to increase number of active users. We also found that platforms are trending towards longer escrow periods for rewards for liquidators, in order to reduce risk of cascading liquidations. Another mechanism being newly introduced to circumvent this risk is also not crediting collateral from liquidation directly to the liquidators, but distributing it between other stakers on the platform. Finally, we found that the amount of time allowed for a user to correct their collateral position if flagged for liquidation is decreasing from when synthetic asset platforms were first brought into DeFi.

5.1 Further Work

DeFi as a whole, and the synthetic asset platform space especially, are still very young and are constantly adapting as new risks are discovered. As time goes on and other synthetic asset platforms gain market share, it will be interesting to see what platform design choices they take forward from the current platforms, or what new mechanisms they introduce.

1. **New asset replication platforms.** Once these newer platforms have grown enough to be able to compare their data to platforms like Synthetix, this project should be revisited to analyse any new mechanisms or new trends developing in existing mechanism configurations.

2. **New direct creation platforms.** Currently there is only one synthetic asset direct creation platform operating in DeFi - UMA. Once other platforms appear that allow you to customize and build your own synthetic tokens, it will be important to systematize the differences between them, to provide a better understanding of the synthetic asset platform space as a whole.

3. **New Synthetix liquidation mechanism.** Synthetix's new liquidation mechanism implemented overhauls how liquidators get paid their rewards. This new mechanism, having only been implemented in May 2022 has not collated enough data (let alone any rewards in escrow being released yet) in order to compare the effect of liquidations on the system. Again, once enough liquidation data has been collected it will be useful to analyse the difference in impact on the system.

4. **Optimized fixed-spread liquidation mechanism impact on asset replication platforms.** It would be interesting to document the impact of using the optimal fixed-spread

liquidation mechanism (through simulations) as outlined in [37] specifically on synthetic asset platforms, and whether or not it can provide extra security against cascading liquidations.

Appendix A

Calculation Examples

A.1 Collateralization Ratio Example

In order to better understand the calculations behind staking in a pool and the profit or loss that can be incurred based on asset price changes, the following scenarios are described, greatly simplified in terms of number of participants. This scenario assumes a Synthetix target collateralization ratio of 500%.

Setup

Say a Synthetix user, Joe, has staked \$1000 worth of SNX to mint \$200 worth of sUSD, at a collateralization ratio of 500%. This leads to him owning \$200 worth of debt in the Synthetix debt pool. At the time that he staked his SNX, there are 3 other participants in the pool. These 3 individuals, A, B and C own \$400 worth of sBTC, \$400 worth of sETH and \$5000 sUSD respectively. Therefore the total debt in the Synthetix debt pool is worth \$6000, and Joe's share of the debt pool is \$200/\$6000 = 3.33%.

First Example

Say the price of sBTC increases by 50% on the next day, and all the other asset prices remain constant. Synthetic's debt pool now increases to \$6200 (Joe's \$200 in sUSD + A's **\$600** in sBTC + B's \$400 in sETH + C's \$5000 in sUSD). As Joe is still responsible for 3.33% of the debt, his debt owed will now be equal to \$206.46, despite only minting \$200 worth of assets. His new collateralization ratio is now calculated as follows: \$1000 SNX/\$206.46 debt = 484%. Joe now needs to add new collateral to his position in order to increase his collateralization ratio back to the target 500%.

Second Example

If instead the price of sBTC decreased by 25%, the debt pool has now decreased in value to \$5900 (Joe's \$200 in sUSD + A's **\$300** in sBTC + B's \$400 in sETH + C's \$5000 in sUSD). Joe is still responsible for 3.33% of the debt in the pool, hence his debt owed has now decresed to \$196.47, putting his collateralization ratio at: \$1000 SNX/\$196.47 debt = 509%. Joe can now either repay all of his debt for a \$3.53 profit, or he can mint an additional \$3.53 sUSD to reduce his collateralization ratio back to the original 500%.

Appendix B

UMA Diagrams

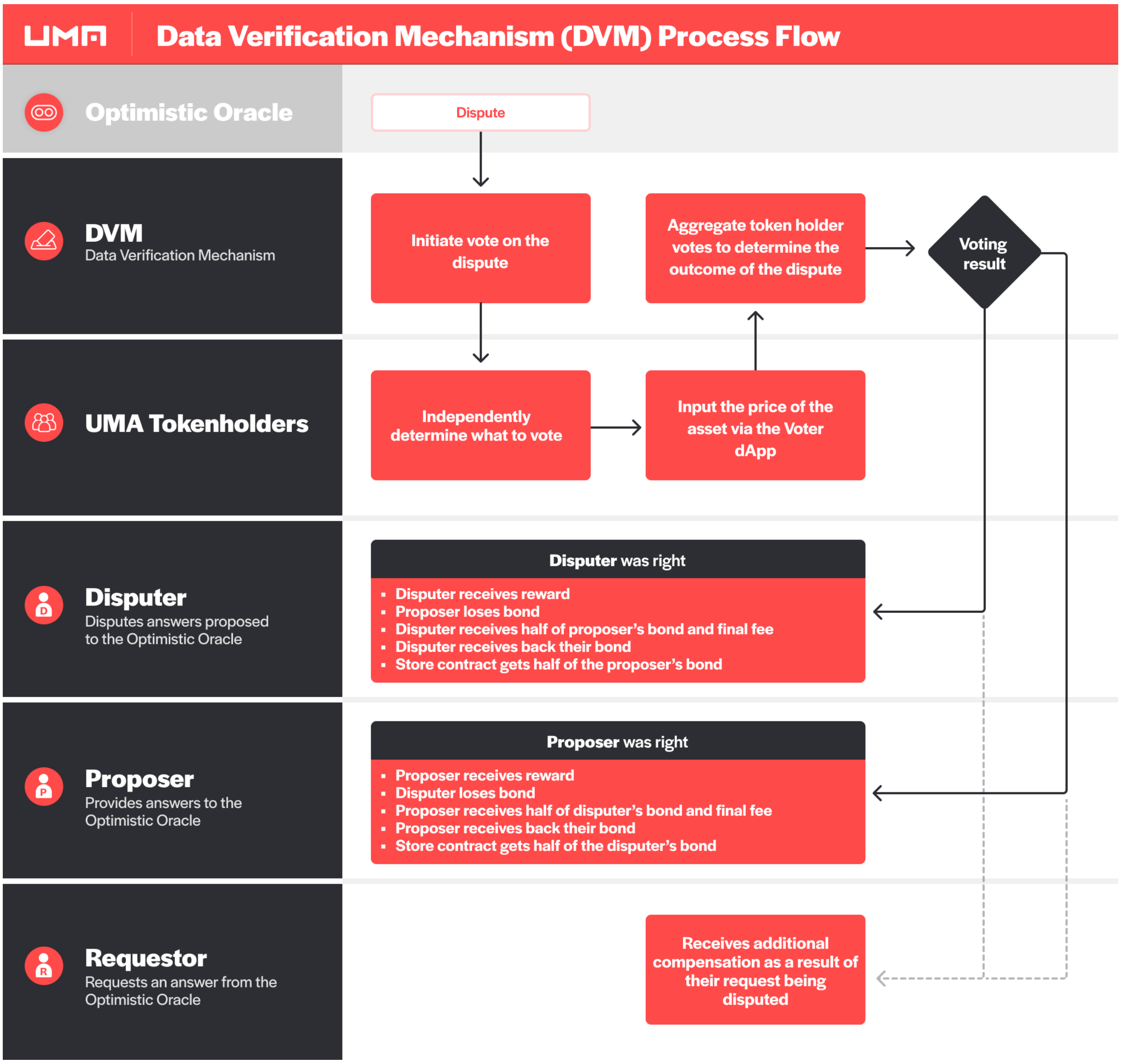

Figure B.1: Process flow of the UMA Data Verification Mechanism[1].

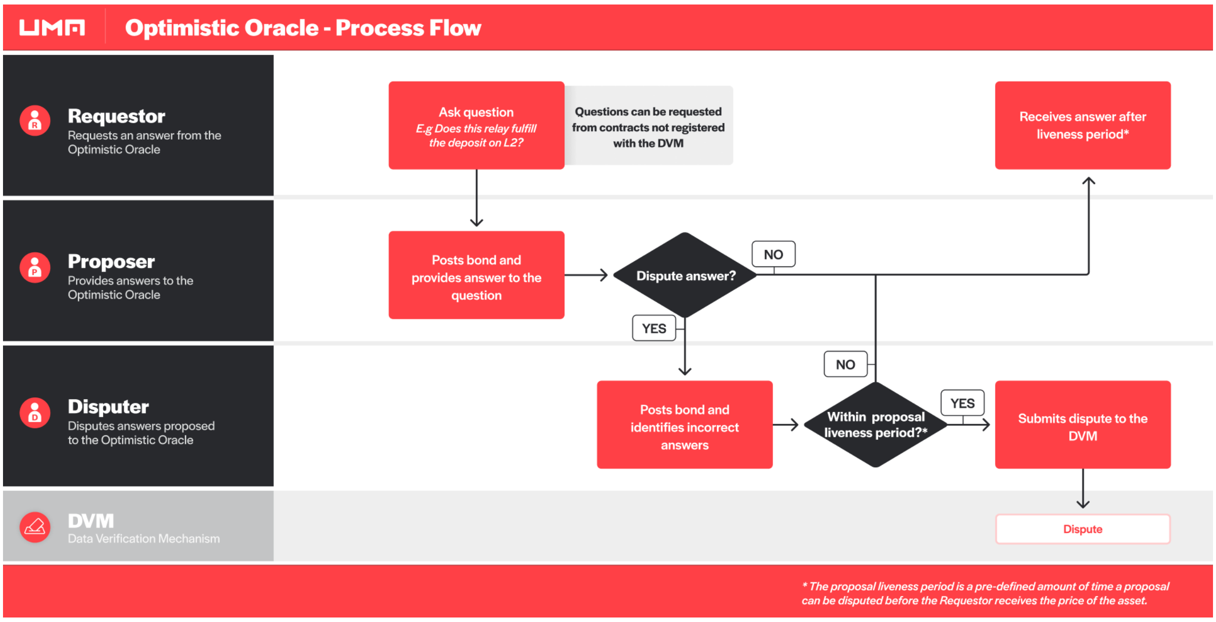

Figure B.2: Process flow of the UMA Optimistic Oracle[1].

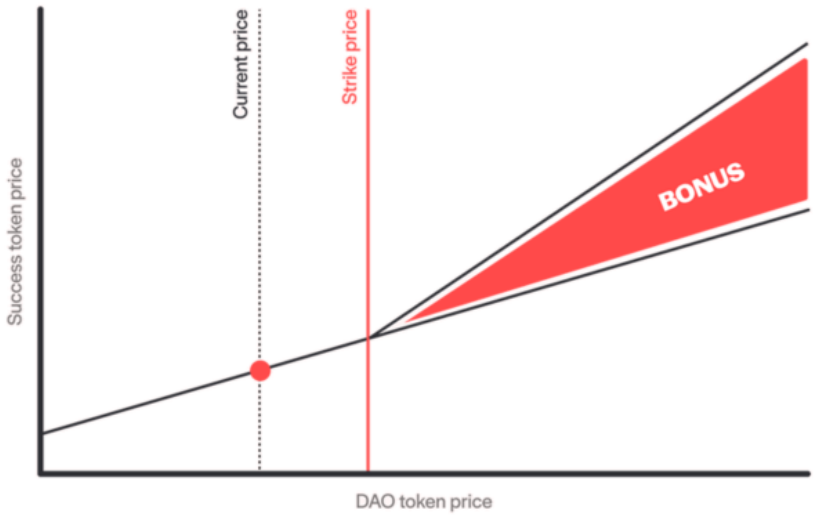

Figure B.3: Pay-out chart of the UMA Success Tokens[2].

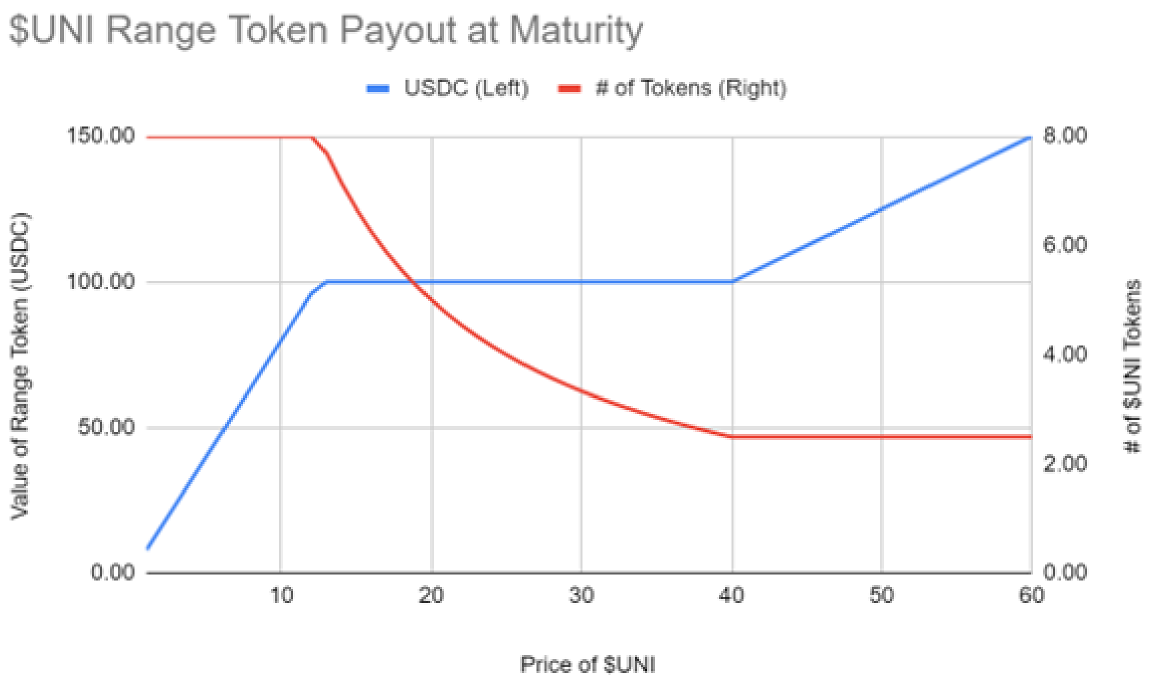

Figure B.4: Value of Range Token and token payout for different values of $UNI price at expiry with the following configurations: current price when the token was built is $25, the range low price is set to $12.50 and the range high price is set to $40.[3].

Bibliography

[1] UMA, “How does uma’s oracle work?” https://docs.umaproject.org/protocol-overview/how-does-umas-oracle-work.

[2] ——, “Success tokens,” https://umaproject.org/products/success-tokens.

[3] ——, “Treasury diversification with range tokens,” https://medium.com/uma-project/treasury-diversification-with-range-tokens-145d4b12614e.

[4] F. N.-A. Siamak Solat, Philippe Calvez, “Permissioned vs. permissionless blockchain: How and why there is only one right choice,” *ENGIE, Laboratory for Computer Science and Artificial Intelligence (CSAI)*, 2020.

[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[6] T. Roughgarden, “Transaction fee mechanism design,” 2021.

[7] Ethereum, “Deploying smart contracts,” https://ethereum.org/en/developers/docs/smart-contracts/deploying/.

[8] ——, “Gas and fees,” https://ethereum.org/en/developers/docs/gas.

[9] B. ArnaudLaurent, LuceBrotcorne, “Transaction fees optimization in the ethereum blockchain,” *SienceDirect*, 2021.

[10] D. Pulse, “Tvl in defis,” https://defipulse.com/.

[11] S. C.-Y. F. Jiahua Xu, Krzysztof Paruch, “Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols,” 2021.

[12] R. Whitaker, “A crypto investigator’s top 5 defi trends to watch,” https://www.linkedin.com/pulse/crypto-investigators-top-5-defi-trends-watch-robert-whitaker/.

[13] E. Dedezade, “Top decentralized exchanged (dexs) in 2021,” https://decrypt.co/73356/top-decentralized-exchanges-dex-uniswap-sushiswa.

[14] L. T. Michael Darlin, Georgios Palaiokrassas, “Debt-financed collateral and stability risks in the defi ecosystem,” 2022.

[15] I. Review, “Top six decentralized lending platforms,” https://identityreview.com/top-six-decentralized-lending-platforms/.

[16] Y. W. Lioba Heimbach, “Behavior of liquidity providers in decentralized exchanges,” 2021.

[17] S. US, “The speed of the equity markets,” https://www.sec.gov/marketstructure/data-highlight/speed-equity-markets.WzXWyWMzYW0.

[18] T. M. Fool, “Market makers,” https://www.fool.co.uk/investing-basics/how-the-stock-market-works/market-makers/.

[19] B. Council, “A complete guide of liquidity provider (lp) tokens,” https://www.blockchain-council.org/defi/liquidity-provider-tokens/.

[20] Uniswap, “Pools,” https://docs.uniswap.org/protocol/V2/concepts/core-concepts/pools.

[21] ——, “How uniswap works,” https://docs.uniswap.org/protocol/V2/concepts/protocol-overview/how-uniswap-works.

[22] J. Z. Bowen Liu, Pawel Szalachowski, “A first look into defi oracles,” *arXivLabs*, 2020.

[23] C. Anirudh Tiwari, “Defi oracles, explained,” https://cointelegraph.com/explained/defi-oracles-explained.

[24] I. Alan Farley, “Synthetic options,” https://www.investopedia.com/articles/optioninvestor/08/synthetic-options.asp.

[25] S. Neagle, “Synthetic stocks: The real deal, or just a fad?” https://www.finance-monthly.com/2021/08/synthetic-stocks-the-real-deal-or-just-a-fad/.

[26] A. Steiner, “Taking the long view on shorting: Market manipulation and gme,” *SLU Law Journal Online*, 2021.

[27] R. D. Sara Rouhani, “Performance analysis of ethereum transactions in private blockchain,” *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2017.

[28] L. B.-G. Mikel Cortes-Goicoechea, Luca Franceschini, “Resource analysis of ethereum 2.0 clients,” *2021 3rd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, 2021.

[29] Ciphertrace, “Cryptocurrency crime and anti-money laundering report,” https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/.

[30] C. Benedict George, “What does it mean to burn in crypto?” https://www.coindesk.com/learn/what-does-it-mean-to-burn-crypto/.

[31] N. Reiff, “Cryptocurrency burning,” https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/.

[32] N. J, “Liquidations in defi.” https://medium.com/defi-saver/liquidations-in-defi-how-they-happen-and-how-to-prevent-them-9caddd52de71.

[33] T. Schmidt, “Liquidators: The secret whales helping defi function.” https://medium.com/dragonfly-research/liquidators-the-secret-whales-helping-defi-function-acf132fbea5e.

[34] UMA, ““priceless” synthetic tokens,” https://medium.com/uma-project/priceless-synthetic-tokens-f28e6452c18b.

[35] Synthetix, “System synopsis,” https://docs.synthetix.io/synopsis/.

[36] ——, “Synthetix litepaper,” https://docs.synthetix.io/litepaper/synthetixexchange.

[37] P. G. P. J. A. G. Kaihua Qin, Liyi Zhou, “An empirical study of defi liquidations: Incentives, risks, and instabilities,” *ACM Internet Measurement Conference (IMC ’21),*, 2021.

[38] Mirror, “Mirrored assets (massets),” https://docs.mirror.finance/protocol/mirrored-assets-massets.

[39] Synthetix, “Sip-148,” https://sips.synthetix.io/sips/sip-148/.

[40] ——, “Synthetix new liquidation mechanism,” https://blog.synthetix.io/new-liquidation-mechanism/.

[41] J. D. Finnerty, “Short selling, death spiral convertibles, and the profitability of stock manipulation.”

[42] L. Finance, “Perpetual contract series launched,” https://medium.com/linear-finance/to-the-linear-community-a9a2cc36636d.

[43] Synthetix, "Tokens, inverse synths," https://docs.synthetix.io/tokens/inverse-isynths.

[44] B. L. A. G. Kaihua Qin, Liyi Zhou, "Attacking the defi ecosystem with flash loans for fun and profit."

[45] D. Krupta, "Uma review: Limitless defi," https://www.coinbureau.com/review/uma-token/.

[46] S. Brown, "A guide to creating a synthetic token on ethereum mainnet using uma," https://medium.com/@sean-uma/a-guide-to-creating-a-synthetic-token-on-ethereum-mainnet-using-uma-f15eede4f4e.

[47] UMA, "How uma solves the oracle problem," https://docs.umaproject.org/oracle/econ-architecture.

[48] ——, "Uma data verification mechanism: Adding economic guaranteed to blockchain oracles," https://github.com/UMAprotocol/whitepaper/blob/master/UMA-DVM-oracle-whitepaper.pdf.

[49] ——, "How expiring synthetic tokens work," https://docs.umaproject.org/synthetic-tokens/expiring-synthetic-tokens.

[50] Y. Finance, "Degenerative finance: ugas explained," https://medium.com/yam-finance/degenerative-finance-ugas-explained-458bedbc2f17.

[51] S. Protocol, "Luna and ust collapse: Debunking the lunatic conspiracy," https://medium.com/sentinel-protocol/part-1-debunking-the-lunatic-conspiracy-what-you-didnt-know-about-the-activities-behind-the-57227b75d5a6.

[52] UMA, "Uma products," https://umaproject.org/products.

[53] L. S. Martin Harrigan, "Airdrops and privacy: A case study in cross-blockchain analysis."

[54] UMA, "Uma projects," https://projects.umaproject.org/.

[55] Across, "Across docs," https://docs.across.to/v2/.

[56] ——, "Across overview," https://docs.across.to/v2/how-does-across-work/overview.

[57] Sherlock, "Sherlock docs," https://docs.sherlock.xyz/.

[58] PolyMarket, "Sherlock docs," https://docs.polymarket.com/.