HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

GRADUATION THESIS

A Model for Synthetic Crypto Assets

TRINH TRUNG KIEN
kien.tt1760034@sis.hust.edu.vn

Major: Information Technology
Specialization: Blockchain

Supervisor: Ph.D. Thanh-Chung Dao _____

Signature

Department: Computer Engineering

School: School of Information and Communications Technology

HANOI, 08/2022

ACKNOWLEDGMENT

First of all, I would like to acknowledge and express my deepest gratitude to my supervisor, Ph.D. Thanh-Chung Dao, who directly instruct me and make this work possible. His guidance and advice carry me through all the stages of modeling, implementing the project, and composing this thesis.

I would also like to give special thanks to all the teachers that have taught me in those last five years, especially those in the SOICT at Hanoi University of Science and Technology. Their dedicated guidance and support provide me with profound knowledge and enable me to have a better understanding of the computer science field.

Finally, I want to show my appreciation to all of my friends, and my family for always supporting me. Their love and support walk me through hardships and make me believe in myself.

ABSTRACT

New opportunities and challenges are rising as we shift towards a decentralized economy. Trillions of dollars of traditional assets, including physical goods, precious metals, stocks, bonds, derivatives, and real estate have not yet been reflexed in digital business models. Blockchain, as a trustless and transparent platform, enable numerous innovative financial activities. Tokenization of traditional assets democratizes certain aspects of the macroeconomy and increases the playing field for the decentralized finance which we are building by adding resources that we have been using into the blockchain. Tokenization lowers the minimum investment threshold, minimizes administrative burden, increases liquidity, offers interoperability, and allows real-time traceability and validation.

The majority of projects focused on tokenizing the currencies, to represent the currencies on the public ledger. Some projects including Mirror attempt to tokenize traditional assets in general. Their design can be categorized into two main classes. In the first case, tokens issued exist on the chain, while the real assets on the back of which the tokens are issued continued to exist in the "off-chain" world. In the second case, asset tokenization involves the creation of asset tokens through the issuance of tokens that are native to the blockchain, built directly on-chain, and living exclusively on the distributed ledger. While the first approach raises concern about security, the cost to store huge amounts of assets off-chain, and the transparency of the issuer, the second approach are vulnerable to design choices and the volatility of the market.

In this work, we use an over-collateralization leverage loan model, which uses the second approach to address the tokenization problem. The model is designed to ensure that it can contain the pegging mechanism to reflex the value of assets, as well as guarantee that every issued token has enough assets on the back. Open problems and future orientations are also discussed for researchers to work on, to decentralize the traditional finance system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Definition
Address	An wallet address or address is a string of letters and numbers from which cryptocurrencies or NFTs can be sent to and from.
AML	Anti-Money Laundering
contraction	Contraction in supply refers to fall in the quantity supplied of a commodity only due to a fall in its price
CosmWasm	Cosmwasm is a library providing all modular code needed for building a contract on Cosmos
DeFi	Decentralized Finance
EI	Employment Insurance
Expansion	Expansion of supply refers to rise in the quantity supplied of a commodity only due to a rise in its price
IBC	The Inter-Blockchain Communication protocol
ICO	An initial coin offering (ICO) is the cryptocurrency industry's equivalent of an initial public offering (IPO)
KYC	Knowing Your Customers
Liability	The fact that someone is legally responsible for something.
MiFID	The Markets in Financial Instruments Directive (2004/39/EC)
pre-IPO	A pre-IPO placement is a sale of large blocks of stock in a company in advance of its listing on a public exchange.

Abbreviation	Definition
QTM	Quantity Theory of Money
SAG	Synthetic Assets Governance tokens allow the process of voting and making decisions in our system
SCA	Synthetic Crypto Assets represent tokens in our system whose value is pegged to real-world assets such as gold, bonds, and stocks.
Smart Contract	A program stored on a blockchain that run when predetermined conditions are met.
Stablecoin	Stablecoins are cryptocurrencies the value of which is pegged, or tied, to that of another currency, commodity, or financial instrument
VAT	Value-added tax
Whitelist	A whitelist (allowlist) is a cybersecurity strategy that approves a list of email addresses, IP addresses, domain names or applications, while denying all others

CHAPTER 1. INTRODUCTION

In this section, we introduce the overview picture of the blockchain industry, what has been achieved and what needs to be improved. With the ultimate goals of decentralizing how the world operates, and creating a more trusted, transparent, and egalitarian society, this work focuses on studying and modulizing the asset tokenization problem.

1.1 Motivation

Since the existence of Bitcoin [1] and cryptocurrency, it is been argued that blockchain could transform the way financial services companies do business. Go beyond the application as a digital currency, blockchain allows people to build any kind of logic and business which requires the trusted and decentralized nature of blockchain [2]. Even though many great applications and models have been built and blockchain and received approvals from many users and businesses, blockchain is still quite siloed and does not affect the actual business outside the world except for speculative purposes.

One of the most crucial tasks in making blockchain wildly accepted is to reflex the value of traditional assets into the blockchain. Due to the isolated nature of blockchain, what has been built on a blockchain simply just stays on that blockchain. Tokenizing the traditional assets, including currencies, gold, oil, and stocks can create a bridge between what exists in the real world with thriving economic activities and businesses which have been being built on blockchain.

Currencies are types of assets that received the majority of the attention of many projects. Stablecoins are created to reflex the value of a token or a coin to the value of the existing traditional currency. There has recently been an explosion in the number of stablecoin projects announced, especially following the crash in Bitcoin prices in early 2018 [3]. There are over a hundred stablecoins in existence or in progress, with the top three projects now representing a market capitalization of over $100B [3]. The explantation of the success of many stablecoins projects is the need for a currency on the blockchain, which contains the functions of money for people to transfer, store and use as a unit of account.

Money is supposed to have three functions: a store of value, a unit of account, and a medium of exchange [4]. Stability is the key for all those three functions. If people store their wealth in an asset, their wealth will fluctuate according to the value of that asset. A volatile asset is a poor unit of account. It is so inconvenient

to value the price of something based on assets that constantly change price. Every time the values of assets or units of accounts change, the prices must be adjusted correspondingly. Finally, a currency price needs to be predictable to be considered as a medium of exchange. No one will accept payments in Bitcoin if they are unsure that the next day, the price could drop a half. Stability is the key to all three functions of money.

Traditional money assets such as USD, EUR, and JPY achieve stability through the micro and macroeconomics adjustment of the banks and the governments. On the other hand, in the blockchain, stablecoins usually follow a mechanism to adjust the supply when the price deviates from the peg and can be categorized into four main classes. Many stablecoins keep a fully collateralized reserve of pegged assets and allow users to expand the supply when the price is too high and redeem when the price gets too low. The second way to maintain stability is to pair the pegged coin with a secondary coin, which absorbs the volatility of the first. Some other currencies simply use an algorithmic approach to adjust the supply of stablecoins when there are fluctuations. The last category uses leveraged loans, which utilized components of all the above classes to achieve stability.

Even though there are some successful projects, the majority of stablecoins failed “tragically”. The blockchain industry has witnessed many “death spiral” stablecoins collapses which make their value go to zero. Some are successfully and still pegged to currency outside, but because it is issued by the third company makes people doubt their “decentralized nature”. Many billions of market cap stable coins are under investigation whether they have enough collateral for redemption. The stablecoins design often works in a calm market scenario, but when there are significant fluctuations in the price of the assets, it is extremely vulnerable due to bad design and people’s emotional behavior. In the case of a dual coin system, it often fails because the system is naturally built on users’ beliefs. Some algorithmic stablecoin designs can peg the value of the token to the currency, but they do not contain all the vital functions of money. On the other hand, stablecoins using reserve pegged assets as token’s collateral model often work, but it raises concern about how transparent and decentralized they are and how the third party a huge amount of collateral.

The existence of stablecoins has made blockchain much more accessible to many users. However, a wide area of the financial industry remains closed and inaccessible, only experimenting with private blockchains which restrict access to specific parties. Indeed, access to financial assets such as stocks, bonds are derivatives remains a challenge for most of the world outside of developed countries.

It is not easy for an average person to possess an asset they believe in because of high entry costs, liquidation constrain,s and geographical barriers. By tokenizing these kinds of assets, the blockchain could create a globally accessible, transparent, and censorship resistance financial system and bring the blockchain's mass adoption one step closer.

1.2 Research Objectives

As mentioned in 1.1, most of the existing projects on tokenizing assets focus on stablecoins. This research aims to tokenize broader types of assets. We call the tokenized assets Synthetic Crypto Assets (SCA). By tokenizing assets including stocks, bonds, real estate, and precious metals, SCA has the potential to decentralize finance and make access of all shape and form accessible to everyone from anywhere in the world. There are three main orientations of what SCA can do.

Witnessed the success and failure of the predecessor projects, SCA utilized the leveraged loans mechanism to reflex the value of asset on-chain, and also to ensure the liability that every token existing on the blockchain is backed up by amounts of other assets in form of cryptocurrency that has the value at least equal to the value of the tokenized asset. In short, the mechanism can be described as follow. Users can either possess a tokenized asset by trading or minting new tokens. If users want to mint new tokens, they need to lock an amount of collateral to issue some tokens on-chain. They can do anything with the tokens they have just borrowed, but if they want to get back the amount of collateral they have locked, they need to return the number of tokens that they issued. This process combined with the liquidation process for under-collateralized users' positions will ensure the operability of the system and enable users to own traditional assets on the blockchain.

This design of asset tokenization solves the centralization and security of the design which used the reserve of pegged assets by providing collateral in form of cryptocurrency and also resolves the trust contingent problems that exist on many algorithmic and dual coin models. By over-collateralizing, the system guarantees that every issued token is backed up by at least the value of the collateral. When the market is unstable, the liquidation process will make sure the value of tokens issued on-chain does not exceed the value of collaterals locked by the system.

The major contributions of this paper can be summarized as follows:

- Synthesizes and analyzes previous studies on tokenizing assets, especially stablecoins.
- Study the problem for tokenizing a more general type of assets beyond creating

stablecoins. The model aims to bring traditional assets including stocks, precious metals, and real estate into the blockchain.

- Provide leverage loan model and mathematical formulation for tokenizing assets problem. The model ensures the liability of the system and also provides an incentive scheme for users to peg the price of tokens to the value of assets off-chain.
- Perform numerical simulations on the liquidation process to evaluate the risk the system will take in an unstable market condition.

1.3 Organization of Thesis

The rest of this paper will be structured as follow. In chapter two, we summarized the important concepts of blockchain, and analyze the existing design of stablecoins. We also introduced the related economic knowledge, and study about the compliance of tokenizing assets. In chapter three, we present our leverage loan design model and formulate the process. The incentive theory scheme will also be discussed in this chapter to illustrate how the model will work using the profound economic theory. Next, in chapter four, we perform numerical simulations to evaluate the risk the system will have to take when there are significant changes in the price of assets. Finally, in chapter five, we summarize what our model has solved, and address the concerns that we need to continue working on. We also provide a few suggestions for future work that can be expanded using this model.

CHAPTER 2. BACKGROUND

In this chapter, we briefly introduce the blockchain, its characteristics, and its applications. A number of famous cryptocurrency projects along with many applications that are built on blockchain are presented to demonstrate how the blockchain is developing. The related work to our asset tokenization problem synthesized and analyzed demonstrates different approaches in modeling and how they succeed and fail. The chapter also provided related economical theory and the regulatory framework that needs to be considered when implementing an asset tokenization project.

2.1 Background of Blockchain

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events, maintained and shared by a community, using cryptography to ensure the security of transmission and access, to achieve data consistency, tamper-proof, and transparency. The name of blockchain originates from its structure, blocks, and chains, where individual records, called blocks, are linked together in a series to form a blockchain. A typical blockchain stores data in the units of blocks, in which each block contains the cryptographic hash of the prior block. The very first block of a blockchain is called the “genesis block”, which is created by the blockchain creator.

When a new block is created, it receives a hash, or encrypted number, that includes the timestamp, information from the previous block, and transaction data. In Bitcoin, this information is encrypted using SHA-256 algorithm [5]. That block is closed when its information is verified by miners using proof-of-work consensus, and a new one will be created with the hash of the previous block. An amount of Bitcoin is rewarded to the miners whose machine verified the hash.

What makes blockchain stands out for being a more secure and transparent type of database is because of its tamper-proof and double-spending prevention capability. The double spending problem is the problem that a potential flaw in which the same digital cash can be spent more than once [6]. In the traditional database, a trusted third party is required to ensure that a transaction does not double-spend the coin. The third-party checks every transaction for double-spending. After each transaction, the coin must be returned to the central mint to issue a new coin, and only the coins that originate from the mint are trusted not to be double-spend. However, this design requires a trusted mint authority, which is vulnerable to data tampering, since a key person within a third party can change data and gain

monetary benefits.

In the case of Bitcoin, a chain of transactions is computed to prevent these issues. Blockchain is aware of all transaction that has ever been made. Whenever a new block is added to the blockchain, the nodes need to perform validity checks on all new transactions, and when it reaches the consensus by the parties, the new block will be added to the chain. The longest chain is considered an honest version with the most compute resources. To change or modify the data of such chains, an attacker needs to create a new version or branch of the chain with the modified data. That newly created chain will be accepted by the participants only if it is the longest chain, which requires the attacker to have the compute resource exceed the summation of all other nodes. This design would minimize the above profound issue in digital cash: "Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one". [1]

It is nearly impossible to hack or attack the entire system based on blockchain due to the distributed nature of this technology. The blockchain contains a certain and verifiable record of every single transaction ever made. Once the information is recorded on the blockchain after passing the validity check and reaching the consensus by the parties, the data can not be erased or changed. For example, if Alice signs and makes a transaction to pay Bob $100, the participants of the network first will check the validation of the transaction that whether Alice has enough $100 to pay Bob. If the transaction is valid, the parties will communicate and reach a consensus to write the transaction of Alice on the blockchain or not. Modifying a past block, an attacker would have to redo the proof-of-work and all blocks after it, which requires he has to have to compute power over 51% of the network.

Everyone that has internet access can retrieve all the transactions that have ever been made on the blockchain. To use a basic analogy, it is easy to steal a bike kept inside a secluded place than to steal it from the marketplace, being observed by thousands of people.

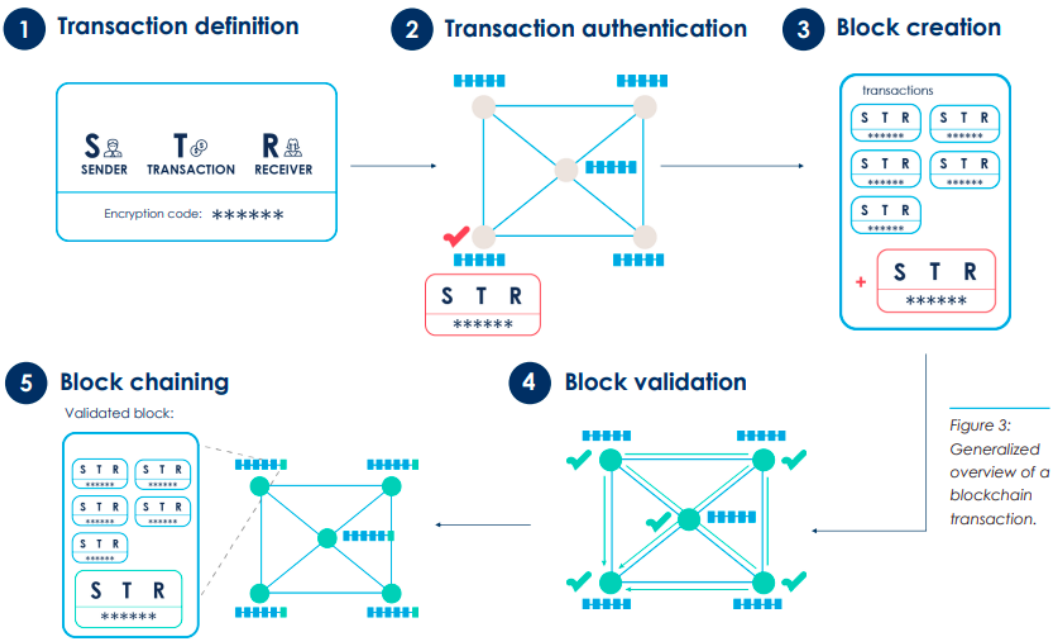

Figure 2.1: Blockchain network diagram [2]

2.1.1 Characteristic of blockchain

Compare to a traditional distributed database, blockchain reflects the following characteristics. Blockchain is a permanent and unalterable network. Blockchain technology functions through a collection of nodes/validators, where each node has a copy of the digital ledger. A transaction can only be added to the network if it is valid and the majority of the nodes agree on that. This means without the approval of a majority of the participants, no one can add any transaction blocks to the ledger. A block of transactions on the blockchain contains the cryptographic hash of the prior block. That means if anyone attempts to change the transaction at a block, that would consequently make the entire following blocks invalid, and that person has to outpace the majority of nodes to write new data to the blockchain and make it valid. Hence, it is nearly impossible for a person to attempt to change the data that has been stored on the blockchain.

Blockchain is a decentralized network since there is no central governing authority that is responsible for all the decisions of what will happens on the blockchain. Instead, a group of nodes makes decisions and maintain the network. Each and every node has the same copy of the ledger and participates in the validation. In a blockchain world, no node will get any sort of special treatment or favors from the network. Everyone will have to follow the standard procedure to add new blocks to the network. Since blockchain removes central authority and completely behaves based on logic and decisions made by participants, it is fault-tolerant and self-functioning. There is no need to worry about the management risk or data

censorship. Users have full control over their properties and they do not have to trust a third party to manage their assets and act as the middle man for their transactions.

The process of making decisions on the blockchain instead using a consensus algorithm. Consensus is a decision-making algorithm for the group of nodes active on the networks to reach an agreement quickly and faster and for smooth functioning of the system. Nodes might not have to trust each other, but they can trust the algorithm that runs at the core of the network to make decisions. All the participants agree to the validity of the records before they can proceed to add new blocks to the network. After being approved by the majority of nodes, a node can simply add, update or delete information on the network. Every record is updated simultaneously and the process of synchronous propagates quickly in the network. Hence, it is impossible to make any change without approval from the network's participants.

Blockchain gets faster settlement than traditional centralized systems. For example, banking systems can take days to finalize all settlements, which can be corrupted easily. In the blockchain case, as long as the transaction is valid, the process of transferring assets between two users can take less than a second.

2.1.2 Scenarios applicable to blockchain

The integrated application of blockchain technology plays an important role in new technological innovations and industrial changes. Even though it can be applicable in a wide range of applications, it is technically decentralized and difficult to tamper with, making it highly applicable within a limited number of scenarios. It has broad prospects in the fields of a new database, digital currency, mutual trust, strong business related".

Firstly, the application scenario is from the needs of the database. The blockchain is essentially a new type of tamper-proof timestamp database [7]. It is extremely applicable for organizations that want to store and manage an unforgeable, and tamper-proof database, which will reduce the maintenance cost and the risk of deception. In the future, the Internet, artificial intelligence, and the Internet of Things will generate massive data, and the existing centralized data storage will face huge challenges. Edge storage computing based on blockchain technology is expected to become the future solution.

Secondly, digital currency has become the main orientation in the development of the digital economy [1] [7] [8]. Compared with physical currency, digital money has lower store costs, convenient use, nearly zero low circulation cost, better integration, and anti-counterfeiting and management. Many successful cryptocurrency projects

using the underlying blockchain technology have brought massive innovation to the new technological economy.

Thirdly, it needs to be a cross-subject, multi-party application scenario. The tamper-proof and decentralized nature of storing data allows blockchain to ensure mutual trust between businesses. Many businesses nowadays still have to maintain a different version of books to agree on business logic. However, the data is often not shared, and the business logic is not uniform, resulting in the "Reconciliation Failure" phenomenon. In contrast, by applying blockchain, data consistency can be achieved easily and each entity in the blockchain can have a complete exact copy version of the book, avoiding complex processes. Many blockchains are programable, allowing businesses to define a set of logic that can not be changed so that the operation flow can be performed much quicker and more reliable [7] [8]. Blockchain can be considered as an "intermediate machine" that removes the untrusted issues between businesses, the data consistency problem of maintaining data between many parties, and high operation costs. In Ethereum, much great business logic has been built and renovated in how blockchain technology work. People now can go to the DeFi application to trade assets without actually knowing each other, or many businesses have created a DAO voting mechanism for deciding its future development [9] [10].

Finally, the blockchain can be customized as a private blockchain, allowing entities to decide who can enter and access the network. The normal public blockchain allows any node to join, and it does not restrict the dissemination of information. For some particular use cases, businesses may want the information to stay private inside the cooperation, and the transaction and consensus mechanism is limited to a certain extent. For example, a group of key members in a company can create a private blockchain to maintain and ensure the consistency of the data, but they want to keep those data secret for their own purposes.

2.1.3 Cryptocurrency

Bitcoin and Digital Currencies One of the most intrinsic and famous applications of blockchain is Bitcoin, which is introduced in 2008 by Nakamoto [1]. In 2017, the price of Bitcoin increase significantly, which made Bitcoin famous to broader groups of society. Bitcoin, as described in the whitepaper, is a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. The bitcoin serves as the electronic cash system through a shared public ledger that lives on the blockchain.

All the confirmed transactions are included in the blockchain, and it allows Bitcoin wallets to calculate their spendable balance so that new transactions can be verified thereby ensuring that they are actually owned by the spender. The integrity and the chronological order of the blockchain are enforced with cryptography, by hashing the information of all transactions of the previous block, and timestamp using the SHA-256 algorithm. A transaction is a transfer of value between Bitcoin wallets that gets included in the blockchain. Bitcoin wallets are a pair of a public key and a private key, which are used to sign transactions, providing mathematical proof that the owner of the transferring wallet authorized the transaction. All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through the process called mining. Mining is a distributed consensus system that is used to confirm pending transactions by including them in the blockchain. It enforces a chronological order in the blockchain, proves the proof-of-work of the participating nodes, and allows different computers to agree on the state of the system. This process allows blockchain to be tamper-proof and prevents the double spending problem. In order for a block to be confirmed, all the transactions inside that block must fit very strict cryptographic rules that will be verified by the network. Modifying data of any past block will change the hash of the block, hence will invalidate all the subsequent blocks.

Bitcoin is a hard cap of 21 million tokens, which makes it scarce. It serves as a fundamental and fairly easy use case for transferring value over the internet. The user can do no more than receive, store, or send units of Bitcoins. In theory, we can program on Bitcoin, but its limited programming language and design are incapable of implementing complex computational logic into Bitcoin transactions. Bitcoin, in other words, is the most famous application of the first blockchain generation, which was built to address a specific problem only.

Ethereum and smart contracts Blockchain technology can be used to create applications that go beyond just enabling a digital currency. Thus, in 2013, five years after the birth of Bitcoin, a group of visionaries around Vitalik Buterin created Ethereum, which is considered the second generation of blockchain [7]. While Bitcoin was created as an alternative to national currencies and thus applied to be a medium of exchange and store of value, Ethereum was intended as a platform to facilitate immutable, programmatic contracts and applications via its own currency. Besides having the native means of payment like Bitcoin, Ethereum allows storing data and executable code on the blockchain via the concept of the smart contract.

Smart contracts are programs that contain pre-determined terms condition, which

is immutably deployed on the blockchain. Ethereum, taken as the whole, can be viewed as a transaction-based state machine: we begin with a genesis state and incrementally execute transactions to morph it into some current state. By allowing running smart contract on the Ethereum network, the tremendous range of applications that required trust, transparency, and security has been deployed on Ethereum and shaped how the cryptocurrency field operate.

Many tokens build on top of Ethereum using the ERC20 standard allows party and corporation to issue their business model, NFT using the ERC721 standard changes people's perspective about art and ownership [11]. Many models revolutionize how cryptocurrency operates, Defi created a whole financial service on the blockchain [9].

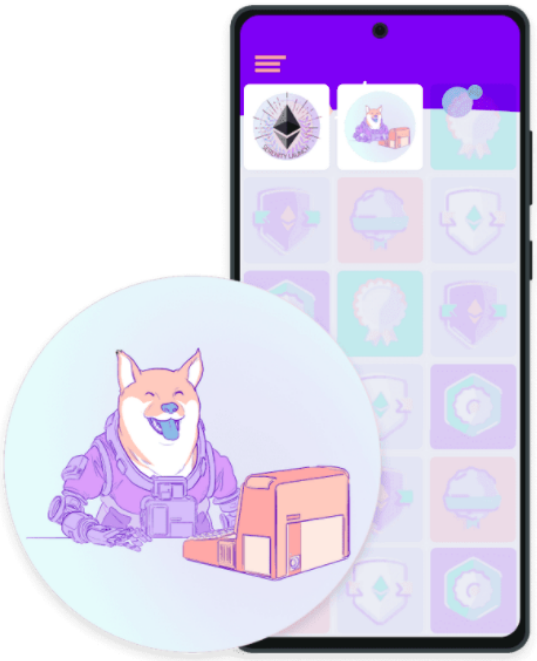

Figure 2.2: Non-fungible Token [11]

Because of their decentralized nature, a set of self-interacting sets of logic smart contracts are also called decentralized applications (dApps). Because it inherits the transparent, tamper-proof, and consistency of blockchain, smart contracts can be used to create services that require trust and transparency. In contrast to smart contracts, much of traditional software is often entirely invisible to customers. Users have to trust that companies' programs do what they promise to do. Smart contracts remove that ambiguity and create trusted applications that can be witnessed, examined, and used by anyone in the world.

Cosmos The success of Bitcoin and Ethereum has created tremendous economic activity in the blockchain. However, these blockchains have suffered from a number of drawbacks, including their gross energy inefficiency, poor or limited performance, and immature governance mechanisms. For example, Bitcoin can only handle 7 transactions per second, the Ethereum network is able to handle around 30 transactions per second. In comparison, Visa handles around 1,700 transactions per second while claiming to be able to scale to 24,000 [12]. Bitcoin and Ethereum (1.0) currently both use Proof-of-work as the consensus mechanism, which has been criticized for its tremendous energy consumption for the mining process. More importantly, these blockchains can not really communicate with each other. With an increasing number of users using blockchain products, it is vital to create a blockchain architecture that solves this problem.

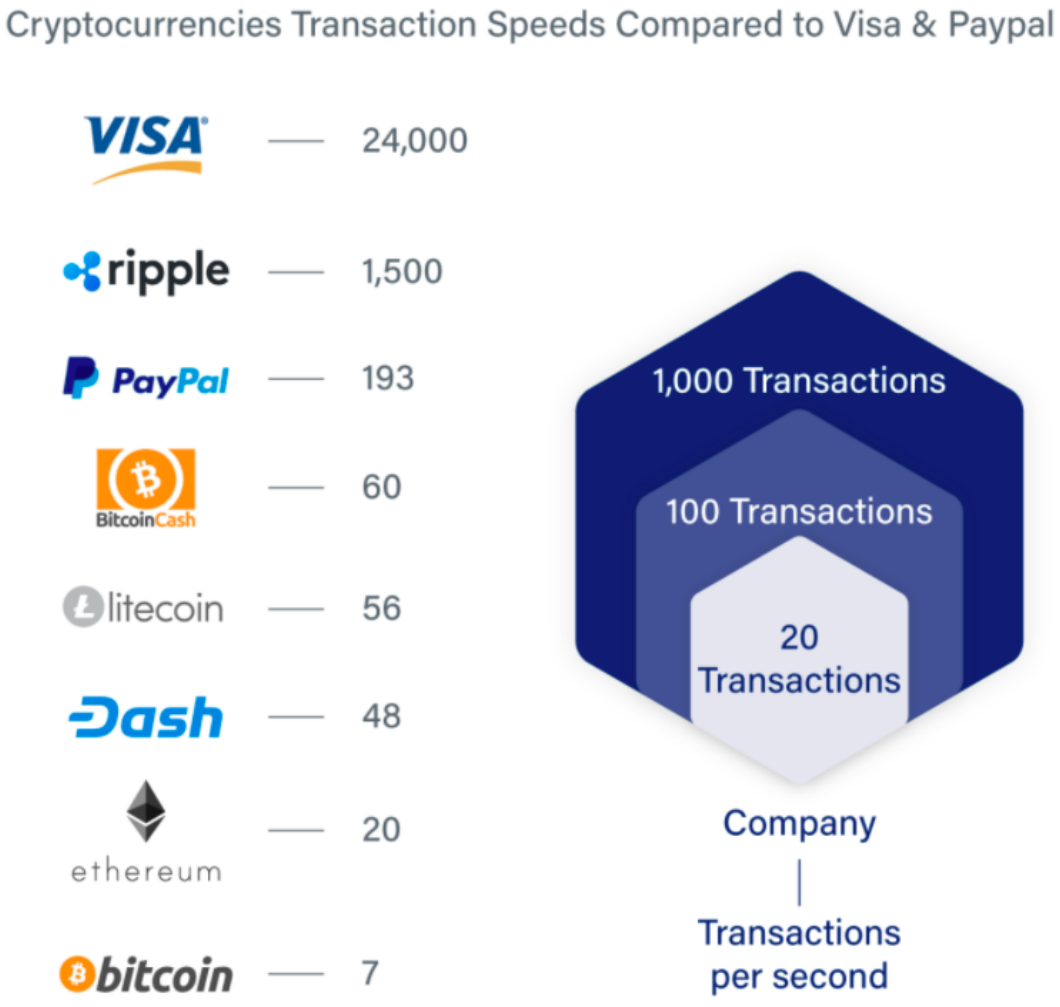

Figure 2.3: Scalability Comparision[12]

Cosmos, considered one of the third-generation blockchains, is a network of many independent blockchains, called zones [8]. The zones are powered by classical

Byzantine fault-tolerant (BFT) consensus algorithms, Tendermint. Unlike smart contracts which are built on a specific blockchain, application-specific blockchain is customized to operate a single application in a specific chain. On EVM, smart contracts inherit the underlying consensus mechanism, state-machine replication engine for distributed nodes, and distributed database of the Ethereum blockchain. This ensures the security and the infrastructure of Ethereum will be passed on to a smart contract, however, it limits the flexibility for developers. It is unprofitable to build a smart contract that handles the logic of a game which a huge user base or create an order-book trading platform type because of expensive transaction costs and the limited amount of transactions Ethereum can handle in a second.

Cosmos allows developers to create an application-specific blockchain, which means the application can have customed consensus mechanism, block time, and native currency. Cosmos offers great flexibility for developers to create a blockchain with the underlying components required for a chain. For example, a game company can create a custom blockchain with low block time and small transaction fees to handle many transactions per second. This design seems to be inapplicable in the case of Ethereum.

Blockchain in Cosmos's networks of blockchain can transfer value between each other, which makes the cosmos extremely scalable. First and second-generation blockchain is siloed and acts as a self-operating network. Cosmos, on the other hand, connects the blockchains in its networks together via Inter-Blockchain Communication Protocol IBC. According to Metcalfe's law, the value of a telecommunications network is proportional to the square of the number of connected users of the system (n2) [13]. Hence, we can the potential scalability of Cosmos is extremely promising.

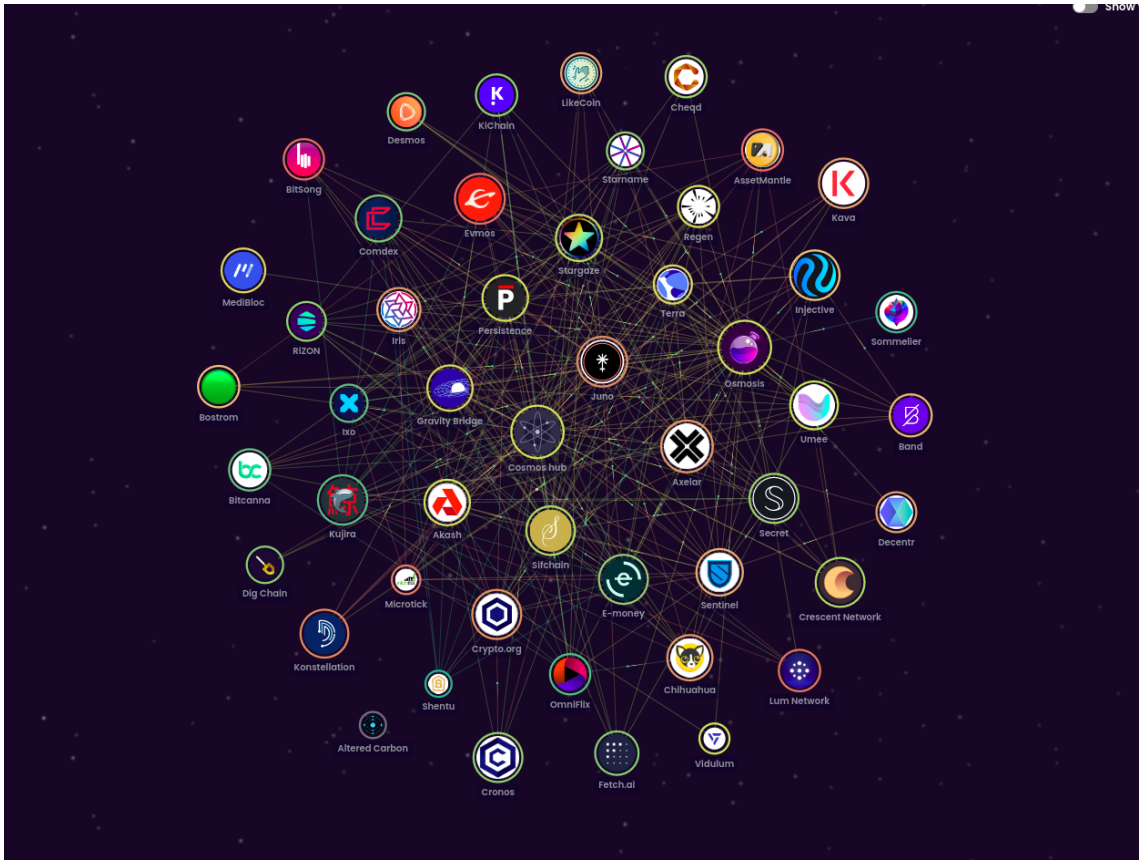

Figure 2.4: IBC Mapzone [14]

In the above figure, we can see the number of projects that have been deployed on the Cosmos ecosystem. Many projects famous and successful projects including Cosmos Hub, Osmosis, Terra, Juno, and Cronos are reshaping how a program should be deployed and worked on the blockchain. The number of connections will increase exponentially based on the number of projects, and the scalability of the networks is limitless.

2.1.4 DeFi

The traditional financial systems are still heavily on intermediaries such as banks, payment service providers, or investment funds. Even though those systems handle billions of transactions per day, and affect virtually almost everyone on earth, it concerns many issues including lack of transparency, low latency, unnecessary paperwork, hard to access, and high maintenance cost. Blockchain enables the potential to remove those issues and open a global ecosystem of finance. Decentralize Finance, in short the DeFi, aims to develop and operate the financial market sector in a decentralized way without the reliance on third parties. Let's imagine if a financial service is built on top of a transparent, trustless blockchain network.

Smart contracts offer flexible solutions for industries such as logistics, education, health care, and financial services. Since the existence of programmable blockchain,

main applications have enabled core financial functions such as payment (stablecoin) [10], credit (lending/borrowing) [10], as well as more complex functions such as derivatives (leverage, swap) and trading with crypto assets (decentralized exchanges) [15]. Those financial primitives are the backbone of Decentralized Finance (DeFi). Those primitives reflex virtually all the people's needs for using and storing money. Tremendous applications can be built using those primitives to create a thriving, endless, and smooth digital economy.

It is impressive what has been created in a short time since the deployment of Ethereum in 2015. The number of DeFi projects is increasing, and reshaping how the financial system operates. In theory, anything we can imagine can be programmable. In Ethereum alone, a thriving ecosystem of DeFi applications gradually makes the digital economy widely accepted.

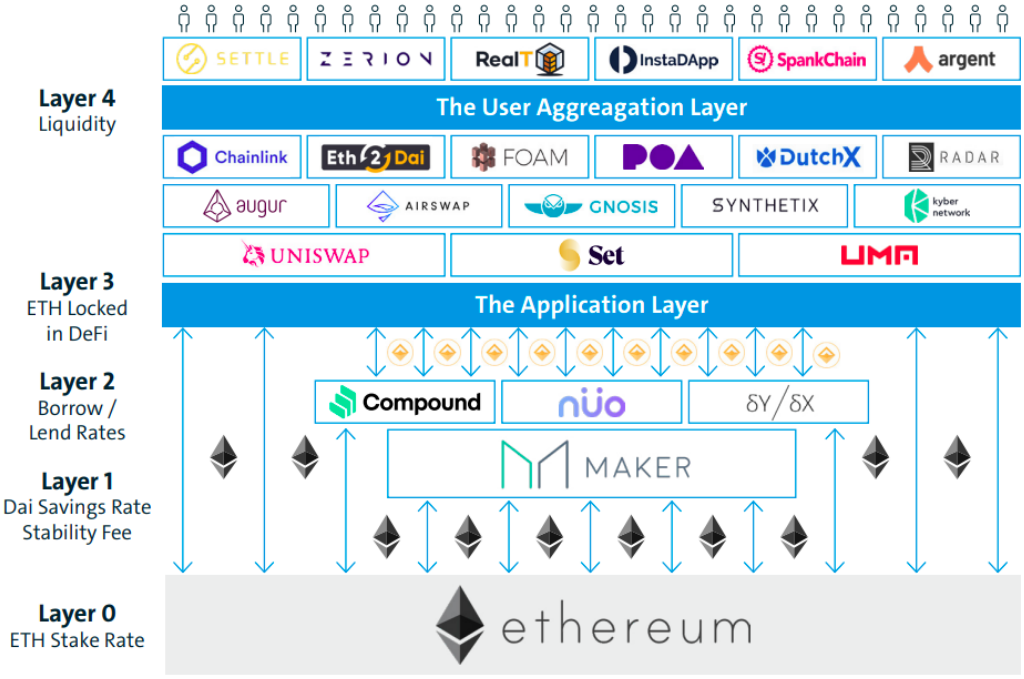

Figure 2.5: DeFi Stack [9]

The DeFi is built on top of the blockchain, which is called layer 0 [1] [7]. Blockchain provides trust and security for its living projects. Above this layer 0 is layer 1, where basic financial functions such as stablecoins to the reflex value of currency are built. The next level, layer 2, provides users with slightly more advanced functionality, such as Lending and Borrowing. Layer 3 is built on top and inherits the products of these two layers, offering more complex financial services such as decentralized exchanges including Uniswap, or market prediction like Augur. Finally, layer 4 provides user-friendly apps that contain similar functions

to what we are using from the traditional finance app offers: storing and sending money, investing in assets, and leverage trading.

The ultimate vision does not stop here. It is great that the DeFi has been mirroring what financial services already existed in real life, but the potential for growth is extremely huge. Technical improvements will be made, and ideas and innovations will be reflex and built on the profound trustless interpolatable blockchain.

2.2 Related Works

The vital question in tokenizing assets is to identify what assets are to be tokenized. The majority of existing works aim to create a token that reflexes the value of the currency, some of which focus on a broader type of assets. In this research, we focus on analyzing one of the focused types of asset, stablecoins peg to USD, since USD is considered the strongest currency, and how a project such as Mirror moves one step further for the more generalized problems, tokenizing any kind of assets [16].

When the price of stablecoins deviates from the peg, all of them need some kind of mechanism to adjust the price. Even though there are many kinds of models to adjust the price, most of them use the quantity theory of money as the core idea to adjust the price of tokens. They contract the supply when the price gets too low and expand the supply when the price is higher than the peg price. Most stablecoins are designed to create an incentive model so that rational, self-interested users will act to restore the peg when prices get diverge. Some use pure algorithmic models to adjust the supply and the user's balance will fluctuate accordingly to the deviation of the price. Other stablecoins issues a secondary token to absorb the volatility of the first, and still others depend on a centralized third party to adjust the supply.

2.2.1 Reserve of pegged assets

One of the most intrinsic mechanisms is by creating a fully collateralized system backed by the pegged asset, and allowing users to expand the supply when the price is too high and redeem when the price is too low. Arbitrageurs, self-interested users will earn profit while helping main the peg. By having the third party issue the new tokens and maintaining the collateral, the expansion and contraction of the supply can be easily operated as follow. When the price of stablecoins is traded above the peg, the issuer allows users to issue new tokens by putting an amount of asset and receive back the tokens which have greater value. For example, if a stablecoin pegged to USD is being traded at the price of $1.1, the arbitrager can go to the issuer, deposit $1 as collateral and receive a token with the value of $1, hence earning 10% in profit. In this process, the issuer will mint new tokens, hence

expanding the supply. On the other hand, when the price of the stablecoin on-chain is under the peg price, the issuer has the liability to ensure that users can redeem the stablecoins they are owning for the equivalent amount of collateral. For example, if the price of the stablecoin drop to $0.9, the user will go to the issuer to redeem back the actual value of the stablecoins, which is $1. That amount of token will be burned and withdrawn from circulation, hence contracting the supply.

The majority of stablecoins in circulation today use this mechanism or a very similar one because of its simplicity and liability. By Jul of 2022, the three biggest stablecoins namely Tether (USDT) [17], USD Coin (USDC) [18], and Binance USD (BUSD) [19] with a total market cap of over $100B use the reserve model to issue their tokens [20]. Some other notable examples of this design include TrueUSD [21], Paxos [22], and many others.

It is easy to expand the supply when the demand is high, but the hassle when price drops causes a lot of concern to users. Even though the model has proved to work and be successful, it is not totally foolproof. In the event of a panic sale, the price of stablecoins can drop significantly. For example, in May of 2022, following the collapse of LUNAUSDT, the price of Tether(USDT) dropped to $0.95. The model proves to work, in the next few days, the price return to its peg. The strong stablecoins projects need to be liable to have enough collateral for redemption when those events happened.

The main problem to allow users to redeem for collateral is storing large amounts of collateral at some physical location. Since it is expensive and requires security to protect the huge amounts of collateral, for example over $50B in the case of Tether, most stablecoins rely on one central location such as the bank. This leads to other issues: centralization and financial legacy. Imagine if the third party holds all the collateral and runs away, the circulating stablecoins will have no value. USD Coin (USDC) gets around this problem by storing money in a network of banks rather than a single one. And the last problem is its ability to scale. Storing and keeping safe a large value of assets is inconvenient and risky.

Some stablecoins including Binance USD are fully collateralized, but some variations only keep a portion of collateral corresponding to the value of the circulating supply. Tether is no longer fully collateralized, they also have the right to deny people to redeem. Some variations use a central authority to mint new tokens, they release newly minted tokens in waves. Facebook's Libra allows only a set of validators to mint or redeem coins, instead of all users. This reduces the overhead of performing many small transactions but comes with a cost of delayed adjustment.

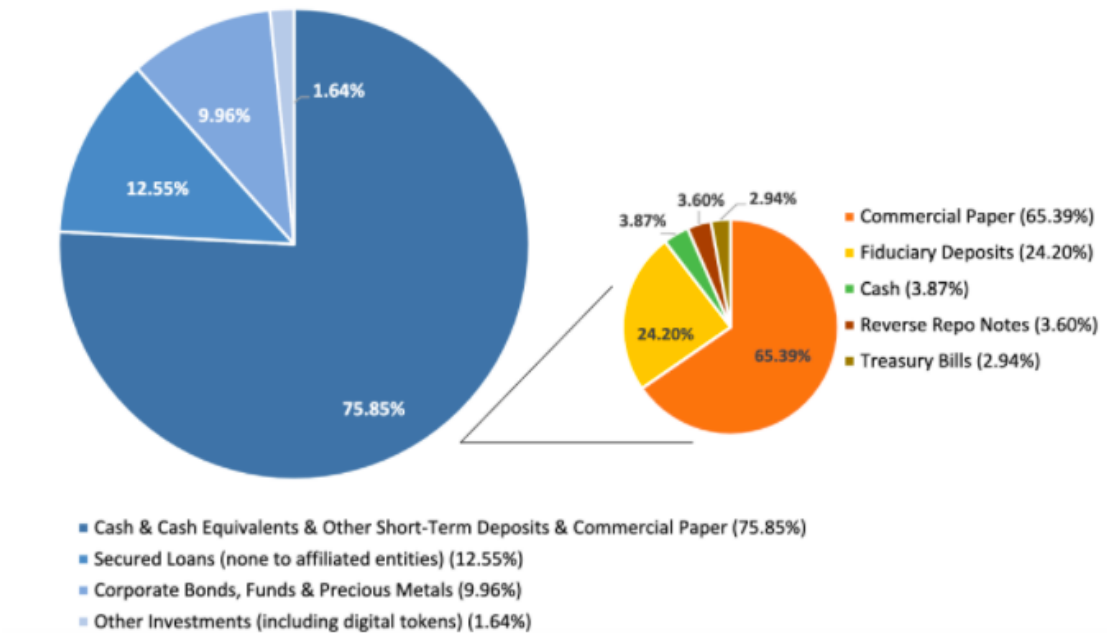

Figure 2.6: Tether Treasury Breakdown [23]

A variation of this model is an under-collateralized model. The remaining collateral can be used to invest in other digital tokens, buy bonds, or store precious metals. In the above figure, Tether only keeps 75.85% of users' collateral in form of cash, cash equivalent, short term deposit, and commercial paper. That means the user might not be able to fully redeem 1 USDT for $1 dollar.

2.2.2 Dual coins

Another way is to pair the pegged coin with a secondary coin which absorbs the vitality of the first. When the price of the stablecoin drop below the peg, a secondary coin is exchanged at a premium in exchange for the stablecoin. The number of stablecoins the system receives after the auction is then burned to reduce the supply. When the price is above the peg, the system simply provides some kind of mechanism to expand the supply. One of the most recent and famous examples of this design is Terra Classic. Terra Classic is a stablecoins platform, which aims to create a system with LUNA as the platform token to absorb volatility and many stable currencies including USD, JPY, KRW, and EUR [24]. For example, when the price of USDT, which is pegged to USD, goes below $1, the arbitrager can exchange less than 1 USDT for a $1 value of Luna and vice versa. The amount of token the system receives after the auction will be burned or put on reserve accordingly to adjust the supply of the stablecoin and incentivize Luna token holders.

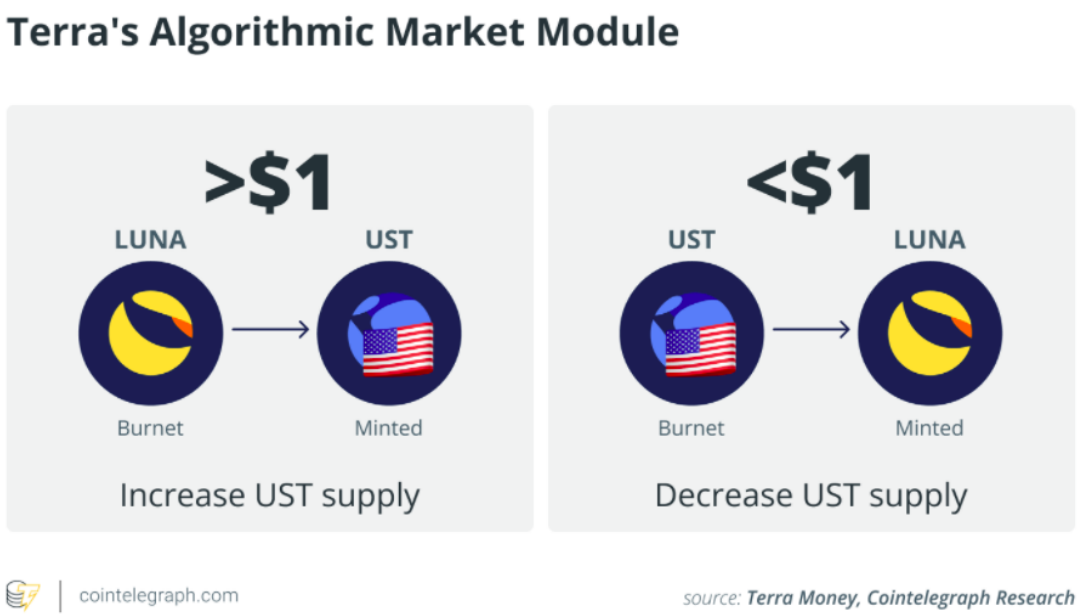

Figure 2.7: Terra Stability Mechanism [25]

However, history proves that this kind of design often fails catastrophically. In May of 2022, Terra Classic collapsed has wiped out more than $100B out of the crypto market, bringing the value of a USTC token, formerly UST near to $0 [26]. Since many users want to redeem UST, they use the mechanism to exchange UST for LUNA. Before the collapse, the total supply of LUNA was 345M. After the crash, the price goes up to 6.5T until the validators decide to halt the network and stop the mint burn mechanism. The price of LUNA drops from around $100 to $0.00001 in just a few days. This is considered one of the biggest crashes in cryptocurrency history.

There are some main concerns with this type of design. One is that the system is built on trust. When trust is gone, the value of the system is often gone dramatically. When the holders of the stablecoins do not believe that their value will remain in the future, there is no incentive to buy and hold the secondary token to ensure the ability to absorb the volatility of the primary one. Or simply in some “black swan” events, the price of the secondary token can fluctuate significantly, which will unstable the absorption ability of the secondary one. In the downtrend, people will be reluctant to buy and wait for a better time for their investment. Since there is no collateral backing if people do not buy the secondary token and retain its value, if the price of stablecoins drops, it often drops in a catastrophic way. The death spiral is a term for the collapse of the dual coin system, when the price of a primary coin drops and brings the price of the secondary coins down, and the decrease in the price of the secondary coins makes it harder for the primary token

holder to redeem the token, which make people insecure and sell the primary coins, and the loop goes on. The other concern is that the secondary token often meets the SEC's definition of security. Basis failed to launch, and Carbon also changed from a dual coin system to a fiat-backed system, for undisclosed reasons, possibly due to regulatory hurdles. The Basis proposed a triple coin system, which is a variation of the dual coin system [27]. The Basic Design contains stablecoins (or the Basis), bond tokens, and share tokens. If Basis is trading for more than $1, the blockchain creates and distributes new Basis by protocol-determined priority to holders of bond tokens and share tokens. If the Basis is being traded under $1, auctions to sell bond tokens for Basis are created to take coins out of circulation. Since 1 bond tokens cost less than 1 Basis, bondholders have the potential to redeem for 1 Basis when Basis demand increases and a newly created Basis is created to expand supply. The bondholders absorb the volatility and are prioritized to receive Basis during expansion time.

2.2.3 Algorithmic

Some other stablecoins use pure algorithmic approaches to control the supply of the stablecoin. One of the most famous examples of this type of design is Ampleforth, previously named Fragments [28]. When the value of Ampleforth changes, its token holders will have their balance adjusted proportionally to how the price deviates. For example, when the price of Ampleforth increase from $1 to $1.1, all user's balances will be inflated by 10%. On the other hand, when the price declines, Ampleforth holder's balances will be decreased accordingly. Instead of using reserved pegged assets or secondary coins to absorb the volatility, the balance of users will change proportionally to the price fluctuation. This design makes Ampleforth a stable unit of value since when the price deviates, the supply of Ampleforth will be adjusted accordingly and make it stable at the price of $1. However, holding Ampleforth is no different than holding non-pegged tokens, since the balances of holders will be adjusted accordingly and the value of Ampleforth users hold fluctuates when the price changes.

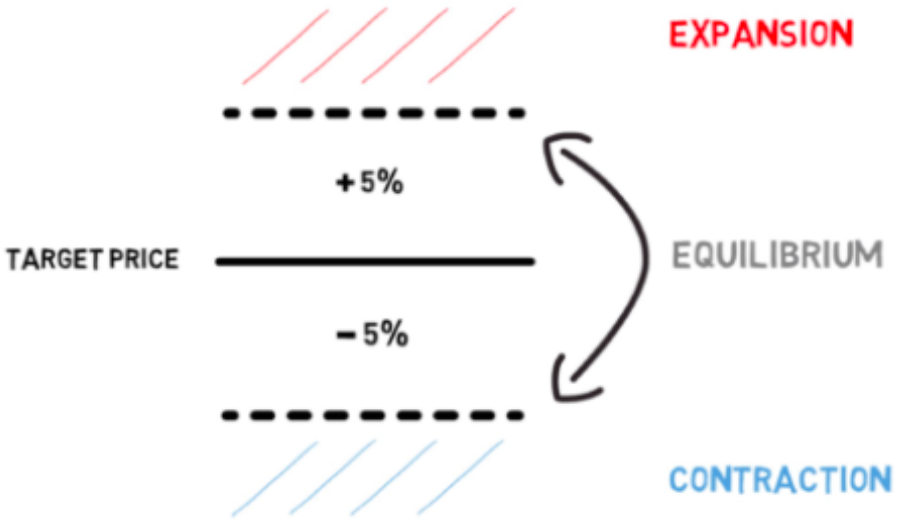

Figure 2.8: Ample Forth Stability Mechanism [29]

The above figure illustrates if there is an increment in price, the supply will expand and vice versa.

2.2.4 Leverage Loan

The last type of stablecoin design is leveraged loans, which utilize and take advantage of all the above classes. Instead of providing collateral in form of real-world assets, the leveraged loan model requires users to over-collateralize assets in form of cryptocurrency in return for stablecoins. To receive back the collateral amount, users need to pay back the stablecoins they are owing the system. One of the most successful examples of this approach is DAI [10]. To issue or mint new DAI tokens, a stablecoin pegged to USD, users need to lock up collateral in form of Ethereum or other crypto assets. The value of collateral users need to lock up to mint new stablecoins must be over a Minimum Collateral Ratio (MCR) times the value of newly minted tokens. For example, if a user wants to mint 10 DAI with the MCR at 150%, which is worth $10, they need to collateralize at least the $15 amount of cryptocurrency asset. If a user wants to get back their collateral back, they need to pay the debt, in this case, 10 DAI back to the system. The received amount of DAI will be burned to contract the supply.

In the downturn of the market, when the price of collateral drops below MCRx the DAI borrowed, the user's debt position will be automatically liquidated, and the collateral is used to auction and buy back and burn the amount of DAI that is currently unbacked by collateral. Any remaining collateral after subtracting the liquidation fee is returned back to the collateral debt position owner. DAI handles

the case when the price of the collateral drops suddenly and significantly by minting a secondary coin, MKR. It is estimated that the system has to mint new MKR tokens, which are the government tokens, to cover the loss when the price of collateral assets suddenly drops by over 33%. It rarely happens, but when it does, the MKR token holders are diluted.

When the price of DAI decreases, users are incentivized to buy DAI and unlock their collateral since it is cheaper for them to pay the debt. This consequently reduces the supply of DAI and restores the peg. When borrowing a new DAI, the user needs to pay for stability fee. If the price of DAI kept being traded underwater, the MKR token holders can vote to increase the stability fee, hence encouraging users to close the debt position and contract the DAI supply.

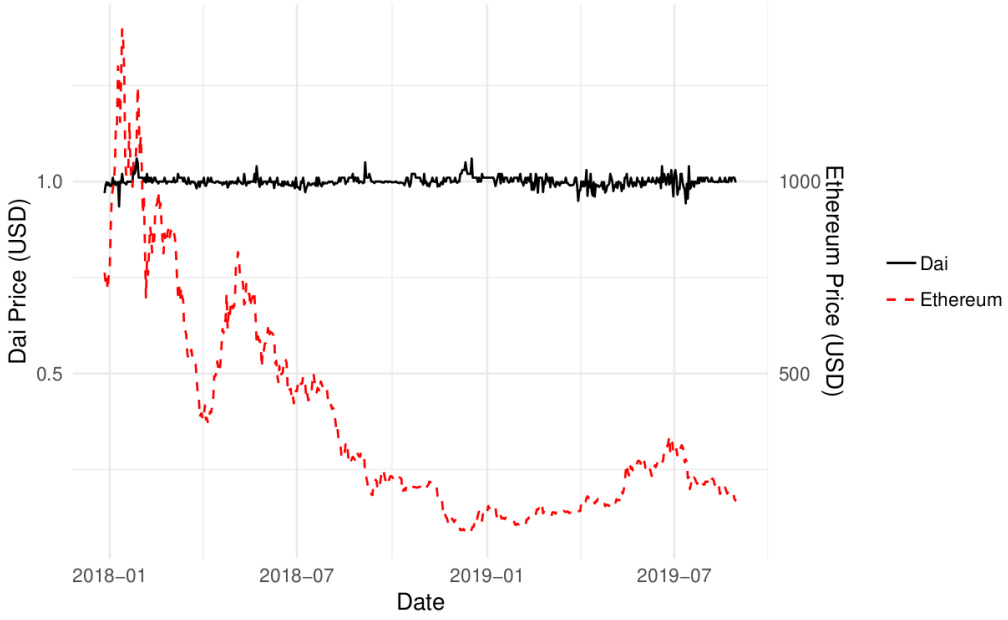

Figure 2.9: DAI remains relatively price stable despite the decline in ETH price [3]

DAI is one of the successful models that does not use fiat-backed assets. Since its launch in 2018, DAI, using ETH as the main collateral asset, experienced many market fluctuations, but the price of DAI has been still traded at the price of $1. Even when the price of ETH dropped by around 90 percent in 2018, DAI has managed to only deviate around 2% of its pegged value.

2.3 The quantity theory of money

The quantity theory of money (QTM) refers to the proposition that changes in the quantity or supply of money lead to changes in the price level. History has shown that the market rise and falls, and people often make un-rational and

emotional choices in an economy. When the economy is raising, people have more money and they want to buy more goods, causing the price of goods to rise, which in turn increases the demand for higher wages, which means people will have even more money. This inflationary spiral happened to Germany in the 1920s, Brazil in the 1980s, and Argentina in the 1990s. On the other hand, when the economy falls, people make less money and are afraid to buy goods, which causes the price of goods to decline and drives people to spend more thrifty and make the price falls even more, and so on. This is known as the deflationary spiral, money loses its value, and it almost occurred during the global recession of 2008. In both of these situations, the quantity theory of money is the main method being used by the central banks to cut off these destructive loops.

The quantity theory of money, in general idea, can be summarized as follow. The general price level of goods and services is proportional to the money supply in an economy. If the amount of money in an economy doubles, price levels will double as a consequence. And vice versa, when the amount of money in an economy reduces in half, the price also reduces in half also. For example, there is a "basket of goods" with a predefined price of $10. If we double the supply, in the long run, the same basket of goods would cost 20$. While the amount of money in circulation has doubled, the actual value of the basket of goods stayed the same. That means that people are willing to pay twice as before to get the same amount of basket of goods, and money has devalued. The same principle applies in the reverse. Using this concept, the central banks can control the price by controlling the supply of money.

High prices mean that the demand is high, and people are willing to spend more money. To prevent inflation and keep money from losing its value, they simply restrict people to spend by withdrawing money from circulation. Similarly, in the events of deflation, expanding the money supply will encourage people to spend more money and devalue the value of money. There are many means and methods that are used by central banks to achieve this, but there are two main actions that the central banks will do at a high-level picture:

- **Expanding the money supply** When the price of goods is going down, and the value of money is going up, they can expand the supply to devalue the value of money and increase the price level of goods
- **Contracting the money supply** When the price of goods is going up, and the value of money is decreasing, they contract the money supply to increase the value of money and drag the price of goods to acceptance levels.

2.4 Monetary Policy

The economy fluctuates over time, which requires central banks to conduct monetary policy to achieve price stability (low and stable inflation) to control the overall money supply and incentivize economic growth. Monetary policy in short is the control of the circulating money supply in an economy [30]. Depending on the level of growth or stagnation within the economy, monetary policies either expand or contract the quantity of money available in an economy. In an economic boom, a contractionary policy increases interest rates and limits the outstanding money supply to slow growth and decrease inflation, in which money devalues and the price of goods and services increases. In contrast, in a recession, expansionary policy incentivizes economic activity by lowering the interest rate and putting more money into the open market. Saving becomes less attractive, and borrowing money is cheaper during normal times, hence consumer spending and borrowing increase.

The goals of money are to fight against volatility and target a small level of inflation to stimulate economic growth. In an expansion, business activities and the job market are more vibrant, which drives higher demand for employment. The domestic currency also becomes cheaper than its foreign exchange when there is an increase in the money supply. There are many methods that are used by the central banks to control the supply of money. Interest rate as discussed above is often used to achieve a macroeconomic effect. In the open market operations, they issue bonds to adjust the balance of reserve and to manipulate the short-term interest rates. The other way is to adjust the reserve requirements, which are the funds that the banks must retain as a proportion of the deposits made by their customers to ensure that they can meet their liabilities. For example, by lowering reserve requirements, banks can spend more money from users' collateral to offer loans or buy other assets. Increasing this rate restricts the free money the bank can useless and slows growth.

One additional tool used by governments and not central banks is fiscal policy. In the U.S, while the Federal Reserve can influence the supply of money, The U.S. Treasury Department can create new money, implement new taxes and apply it directly or indirectly to the economy. In the COVID-19 pandemic, both monetary policy and fiscal tools were deployed by the U.S government and the Federal Reserve to fight against unemployment, and high inflation. [31]

2.4.1 Compliance

Asset tokenization opens a huge range of benefits compared to the existing traditional finance system. Automation, transparency, liquidity enhancement, cross-

border nature, and fractional ownership is what asset tokenization offers to change how economical finance operates. At the same time, the application of tokenization and blockchain, in general, raises important risks stemming from the business model and the decentralized character of the technology itself.

The Crypto industry is no longer for early adopters and speculative traders, but for the people and investors who seek investment opportunities and use the blockchain in their daily life. The existing financial system contains regulations around assets for several reasons. The regulation provides protection for users' funds and investments, prevents fraudulent activities, and capitalizes cash flows.

Assets Regulatory Classification

Tokenization increases the number and diverse many types of assets on the blockchain. Bitcoin, stablecoin, and stock assets are created with different purposes and hence need to be treated differently. Although the classification of digital assets is complex, the proper taxonomy is crucial since we need to imply regulation in different types of assets. For example, gold is considered a commodity, and stocks in considered security assets. Securities and commodities operate under different laws and are regulated by different agencies. For example, the Securities and Exchange Commission (SEC) regulates securities under the Securities Act of 1933 [32]. On the other hand, the Commodity Futures Trading Commission regulates commodity markets under the Commodity Exchange Act of 1936 [33]. Therefore, when creating assets that are unlike any known existing assets, there should have a framework that decides to regulate them the same way as other assets or regulate them under a completely new category.

Over the years, many efforts have been put into the classification of tokenized assets. FINMA for instance divides tokens into the three following categories [34]:

- **Payment tokens**. These tokens are defined as a payment, exchange, or currency tokens, which intend to provide many of the same functions as the existing currencies, such as the USD or EUR.
- **Security tokens**. People buy securities as a form of investment. For example, stocks and bonds are famous types of securities. A security token is subject to the laws that govern securities since it derives its value from the underlying asset in the real world. **Utility tokens**. Utility tokens are not created to be an investment, but their main purpose is to access digitally an application or service by means of a blockchain-based infrastructure.

As FINMA states, hybrid tokens are also possible. For example, a token can be

both the utility and payment for example. In our design specifically, the tokenized assets often fall under the securities category. Hence, besides the implementation, the choices for assets to list and the necessary compliance need to be considered carefully.

Regulatory Challenges

The lack of regulatory clarity for tokenized assets remains an obstacle to the wider implementation of this new asset class. Since the existence of many non-compliant Initial Coin Offering, many jurisdictions with active tokenized markets create a new regulation standard for this special kind of asset. The purpose of such a standard is to identify how tokens can comply with the regulation in the respective jurisdictions. Most of them inherited the existing standard for traditional assets, hence a need for a hybrid token structure with off-chain and on-chain components is obvious. For example, in 2019, the European Securities and Markets Authority highlights that some crypto-assets, especially the securities type, are likely to qualify MiFID financial instruments, and need to comply with the full set of EI financial securities rules.

The entities owning a portfolio of assets also should be classified as a collective investment scheme. This requires another set of approvals and compliance related to investment funds. This raises the question of qualified custodians for digital assets, who are responsible for holding client assets.

The other issue that the regulator considers is property rights, which represent legal ownership of an asset in a way that is recognizable in court. However, some experts argued that the investors would want to own a part of the project rather than actually own the actual asset in the real world.

Compliance on Blockchain

The innovation of tokenized assets promises to enable markets without borders. However, it raises concerns about fraudulent behavior, from terrorist financing to money laundering. At a minimum, securities type of token needs to meet the Anti-Money Laundering (AML) requirements, which is a framework of laws and policies aiming to prevent and identify financial crime. AML often start with KYC - Knowing Your Customers and will then continue to monitor and report suspicious behavior. Regulation framework varies between different countries. For instance, in Europe, every country has its own legislation. That makes a general framework for AML requirements complex and expensive to come to general compliance.

It is crucial for cryptocurrency to research and comply with the current existing regulation. Even though regulation may not be currently imposed on the blockchain,

many organizations and governments are designing such a framework. For example. Many of the non-compliant ICOs with innovative business models, but lack compliance, are under the investigation of the regulator.

Another problem that has not yet been well regulated is how to address the policy of the different regions. The cross-border nature of cryptocurrency enables various applications, but also raises the concern of how the governments can control and imply tax on them. Holding securities tokens should be considered holding stocks or bonds in real life. Should the government apply VAT to the assets that are backed by commodities? Or should they imply capital taxes on real estate assets? Each different region under different jurisdiction deploys a different strategy for taxation. Coming to a standard takes time and requires the synergy of authorities.

Compliance on Tokenization Process

It is complicated to build a fully compliant system since the regulatory rules are in the development process. However, there are a few methods we can implement in the system to fulfill the AML obligations. KYC users: Since possessing some kind of assets require the identification of users, for example, the U.S stock may be limited in some region. The issuer needs to provide attestations of the investor's identity. Each type of asset requires different requirements, such as age, and nationality. This process allows further application of other regulatory rules. Set ownership and transfer restrictions: The model can set who can hold the token, how it can be transferred and the maximum number of tokens an investor can hold. For example, the system can disclose customer information, such as the sender's and the recipient's names, and geographical address when performing a transaction worth more than $10,000. For our specific system, in which the tokenized assets often fall under the securities category, the need of implementing the regulatory method of such a system to comply with the regulatory framework is extremely vital.

CHAPTER 3. Our model for Synthetic Crypto Assets

In this chapter, we discuss about the design of the model and its implementation details. The role of the government token and the incentive scheme are also discussed here.

3.1 Overview

3.1.1 Leverage Loan Design

This chapter presents the design of tokenizing any kind of traditional asset. The asset can be stocks, real estate, precious metals or anything that need to be tokenized. Unlike the case of currency, the price of traditional assets can be volatile in a short period of time. For example, the price of stocks can fluctuate significantly within a day, so we need to utilize the existing approach for stablecoins and modify it for our needs. We leveraged one of the most successful and decentralized designs of stablecoins, leveraged loans, and tailor the needed ingredient.

In the example of DAI, the assets used in the model can be compromised into two main types of assets. The primary one is stablecoins, in which the model attempt to stabilize the price, and the collateral one, is cryptocurrency assets, which act as an asset to absorb the volatility of the system. The price of collateral assets, mostly ETH in the case of DAI, often fluctuates compare to the stablecoins. Users need to provide mortgages to issue new stablecoins. Of course, if the users lock another kind of stable asset compared to the issuing stablecoins, their position will less likely to get liquidated. But there is no incentive for them to do that since they can have much more money in circulation if they just use their collateral normally. Users who mint new DAI often is the believer in the Ethereum ecosystem, and they will believe that in the future, their locked collateral will increase in value and they want to issue new DAI for their own purpose.

Our problem addresses the problem in a slightly different way. In the case of many volatile assets, for example, APPL, the more volatile the two types of assets are, the riskier it will be for the user. The model leveraged the existing successful stablecoins as the collateral and aims to ensure the liability of the system and peg the price of the other volatile assets. Of course, we can use any kind of cryptocurrency as the collateral, but for better protection of the users and the longevity of the system, we are focusing on stablecoins as the collateral in this version. The problems the model needs to solve are nearly the same as the case of stablecoins. The design needs to ensure that every circulating token on-chain is backed up by the corresponding amount of collateral and to create the incentive

scheme for the price of the token to follow the peg, the price of token off-chain.

3.1.2 Design flow

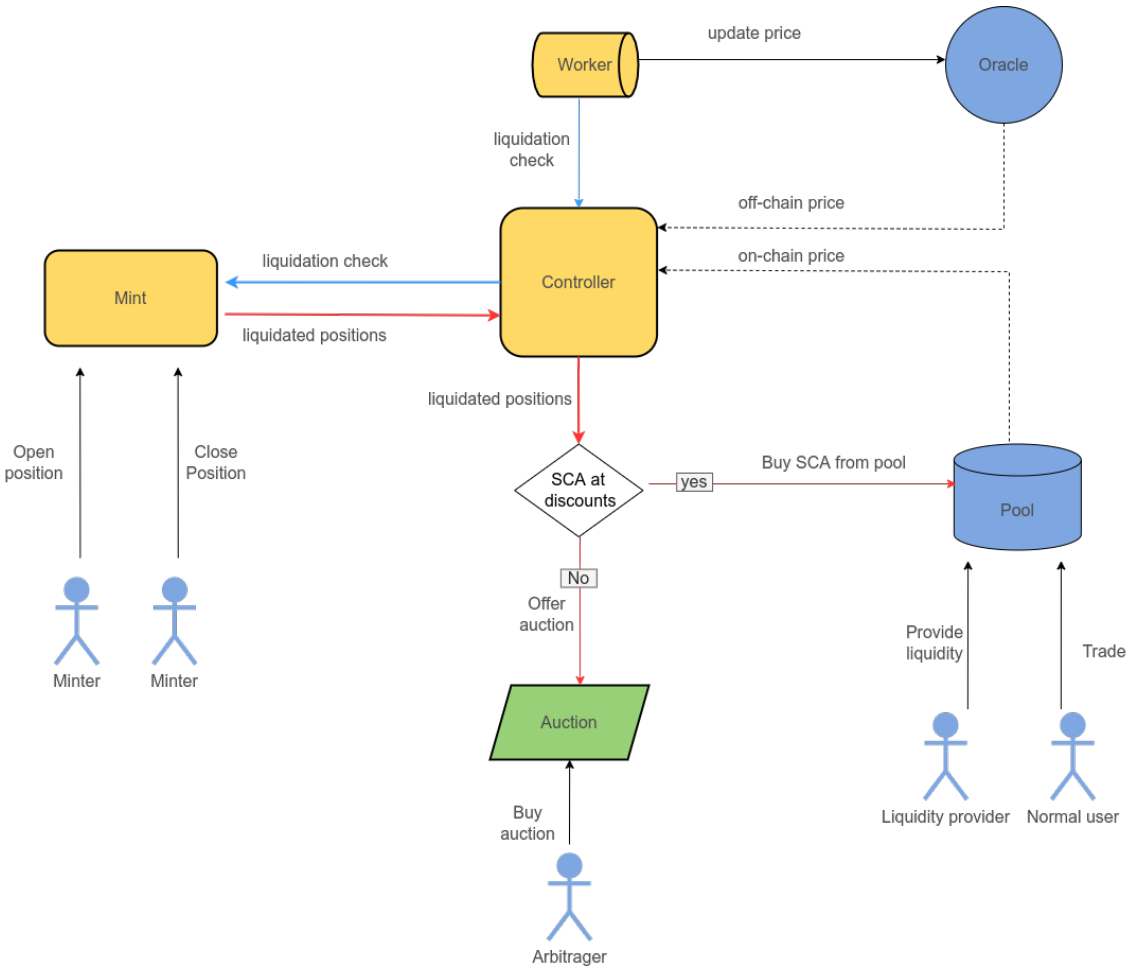

Figure 3.1: Synthetic Crypto Assets Model

There are four types of users who contribute to peg the price of the asset and ensure the liability of the system.

- **Minters** are users who open a new collateral debt position in order to issue new SCA tokens. They lock up the number of stablecoins at the minimum collateral rate (MCR) to receive back the corresponding amount of SCA tokens. After minting new tokens, they are in a debt position, and are required to return back the amount of issued SCA or their collateral will get liquidated.
- **Liquidity providers** provide pair of assets for trading between SCA and the stablecoin. In this model, we provide the pair between the SCA and a stablecoin, since it commonly has the highest trade volume. Implementing new pair will have the same impact since the market and the arbitrager will ensure that the price level between pairs remains correct.
- **Normal users** are the ones who will buy and sell SCA tokens on the open

market. For example, if a user who lives in Asia wants to buy APPL stocks, he can do so by trading on the pair normally or issuing a new token (being the minter).

- **Arbitragers** can be either normal users or minters. When they see the price of SCA on-chain and its asset price off-chain deviate, he can simply buy when the price on-chain is lower than the price off-chain, or mint a new token when the price on-chain is higher than the price off-chain and close the position when the price gets back to the peg.

The design includes the following components. When users want to mint new tokens, they deposit collateral into the Mint module to mint new SCA tokens. In order to issue new tokenized assets SCA for users, the Mint module needs to acknowledge the price of the asset on-chain and the price of the asset off-chain. The price information is taken from the Oracle module. Following the traditional Defi design, the Pair module of SCA and a stablecoin allows users to provide liquidity and perform trading. The Controller is in charge of watching and performing liquidation on the user's under-collateral position. If the user position gets liquidated, the Controller will use user collateral to buy back and burn the SCA on the Auction.

In the following sections, we will analyze important steps in this design. Besides two main types of assets, the tokenized assets SCA and the collateral stablecoin, we introduce the governance token SAG to maintain the model. The governance token holders can decide what assets to tokenize and what kind of crypto assets to collateralize. After defining what kind of assets will be included in the model, we need to find a way for the blockchain to acknowledge the price of the asset on-chain and off-chain. Then, we will focus on the Mint mechanism, and how minters can issue new tokens. Finally, after the user has been in a position, how does the system handle when the user's position is under-collateral by performing liquidation and auction.

3.2 Peg

One of the most salient choices for this design is choosing what kind of assets to tokenize. While any kind of asset is tokenizable in theory, we categorize assets into two main classes:

- **Physical assets**: This would include types of goods or assets that exist as physical entities. It can be precious metals, commodities, real estate, and paintings.
- **Abstract assets**: These are the type of assets that exist based on human agreements, such as stocks, bonds, and derivatives.

Choosing what kind of assets to tokenize needs to be performed with caution. Some assets are extremely volatile, their price can fluctuate significantly in a short time. For example, the price of a random unpopular stock can change more than 100% within a single day. Some assets are unsafe to possess. In 2020 alone, over 170 companies have been delisted from the US stock exchanges.

Our aim at first is to tokenize "well-known" assets, which prove to last over history. Our suggestion is to tokenize physical assets including gold and real estate, common commodities such as rice, meat or abstract assets like popular stocks and bonds. The additional assets will be proposed by the SAG stakers, and if the votes pass the thresh hold, they will be added to the system.

Implementing decentralized oracles raise several issues, but the most important problem is the possibility for the voters to profit by coordinating a false price vote. There are some approaches to address this kind of problem. We can limit the vote of users who own a huge portion of SAG or choosing the right rewarding and slashing mechanism can vastly decrease the odds of such coordination.

3.3 Price information

3.3.1 Price off-chain

Blockchain is siloed and does not acknowledge the information about the world outside. However, in our problem, the system needs to know the price of the asset off-chain in order to operate. The simplest approach is to create a job that constantly updates the price base on the data provided by the maintainer or from some other source. However, this approach creates the single point of failure of the system and makes the system vulnerable to corruption since the maintainer can easily change the price for their own good. Hence, we need a more decentralized approach the update the price information off-chain to the blockchain.

In this design, we design a voting mechanism to update the price. The SAG stakers, as the contributors to the system, reserve the right to vote and update the price of the SCA tokens. Before the update time, each SAG stakers can submit a vote on the price of an asset that he believes is true to the system.

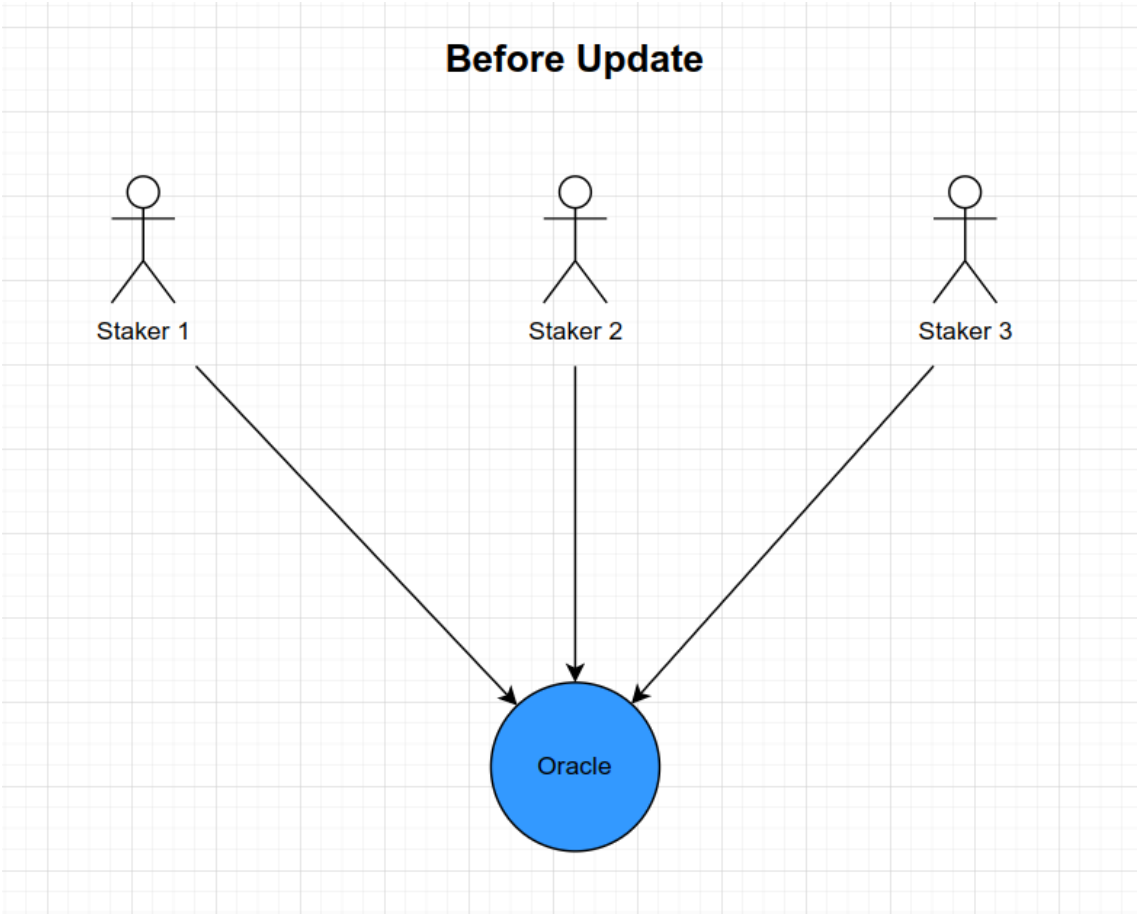

Figure 3.2: Voting process

After a time interval, at the update time, the vote is tallied by taking the weighted medians as the true price. Some amount of SAG is rewarded to those who voted within 1 standard deviation of the true price. The others who voted outside are punished by slashing some amount of their stakes.

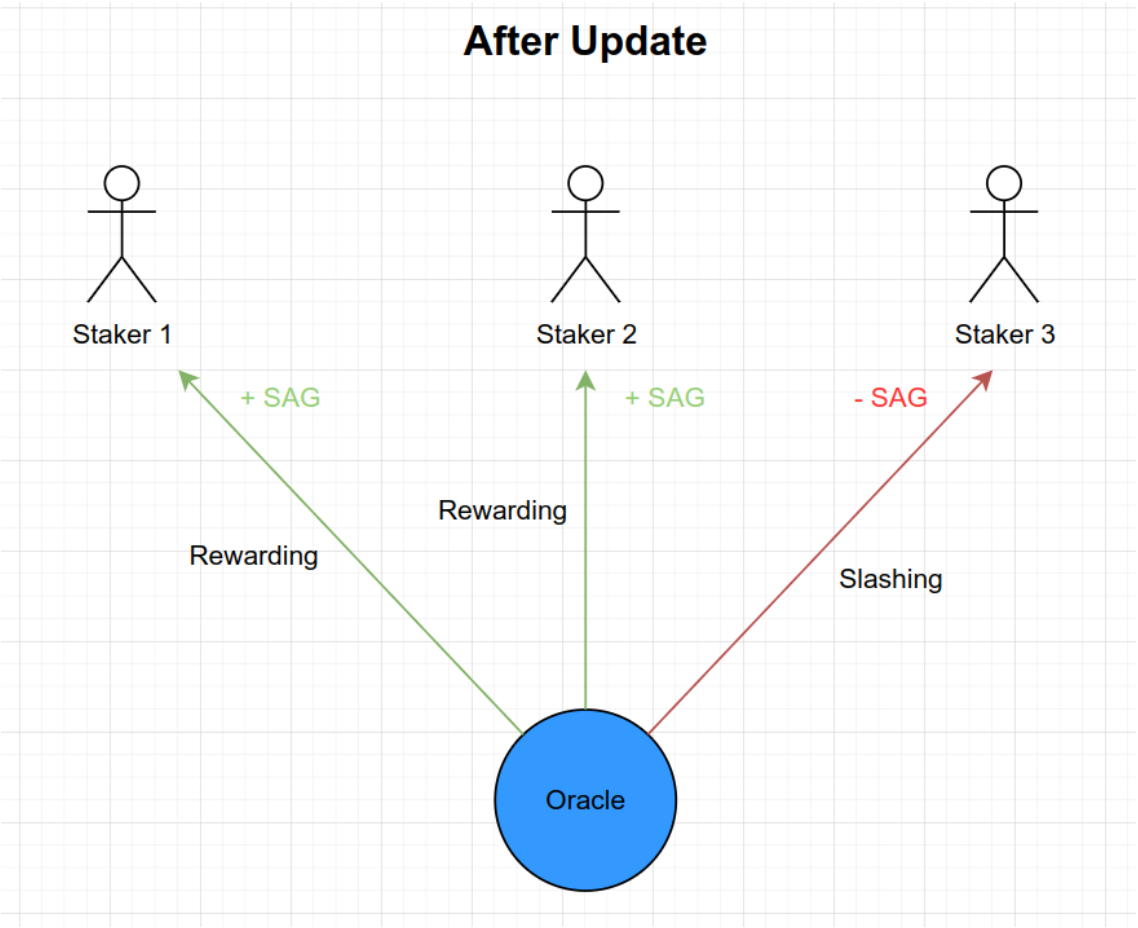

Figure 3.3: Rewarding and Slashing

3.3.2 Price on-chain

When the assets are tokenized on-chain, they can be traded in many open Defi markets and centralized platforms. There are two ways to get the price off-chain. The first one is the price of the tokenized assets on-chain can be updated via the same voting mechanism as above. Users will collect and vote the price of the assets on-chain and submit it along with the price of assets off-chain. However, in this design, we are going to get the price directly from the trading pair itself. Since our system initially implements one trading pair between the SCA tokens and a stablecoin that is pegged to USD, it removes the overhead and the risk when using the decentralized oracle. If the SCA tokens are being traded on multiple platforms, the arbitrager will make sure it gets its price stay at the same level.

The price of token on-chain in this design will be the exact same pricing model of Uniswap [15]. Liquidity providers put a pair of assets as the reserve to allow people to trade in return for receiving trading fees. The amount of reserve of two assets in a pair is called x and y. When a user makes a trade, the amount of token she spends and the amount of token he gains follow the pricing formation, $x * y = k$.

k is a constant during one trade.

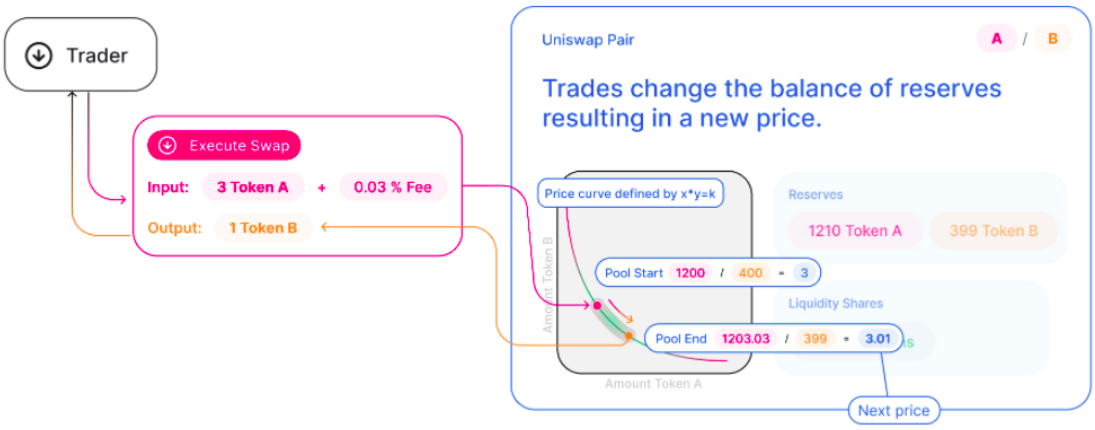

Figure 3.4: Uniswap Pricing [35]

3.4 Minting mechanism

After getting the price information, a user now can open a debt position and mint a new token. When a user wants to mint new tokens, they need to lock at least the amount of collateral with the value of new-minted tokens off-chain times the minimum collateral ratio. The system will mint an equivalent amount of SCA tokens and transfer it back to the minter. When the user does not want to use the SCA anymore and wants to redeem their collateral, he can close the position by repaying the amount of borrowed SCA and receiving back the collateral.

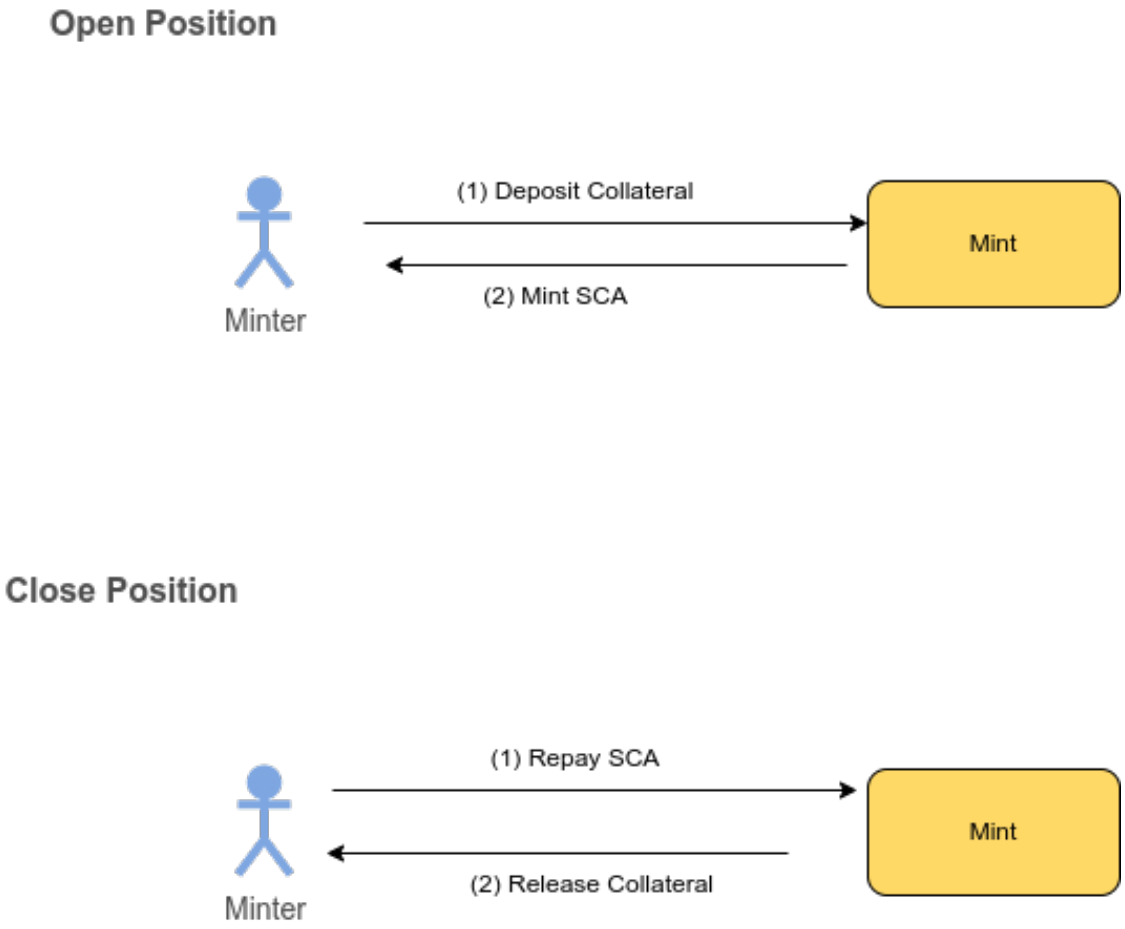

Figure 3.5: Minting

To formulate the idea, we discuss clarifying the minting process in more detail. Let sX is the tokenized asset, and sC is the collateral stablecoin. The Minting module acknowledges the off-chain price of sX and sC compared to USD, which is sX^p and sC^p respectively. The minimum collateral rate, MCR is initially set by the contract's deployer and later adjusted by the community. When a user wants to issue new X tokens, they need to provide the amount of collateral $||sC||$ they want to lock, and the collateral ratio CR they want to put position in. The amount of asset $||sX||$ they will be received after the mint process can be calculated as follow:

$$CR >= MCR \tag{3.1}$$

$$||sX|| = \frac{||sC|| \times sC^p}{MCR \times sX^p} \tag{3.2}$$

After opening a new position, the user borrowed an$||sX||$ amount. The user can do whatever they like with the borrowed amount of $||X||$ tokens, including trading, staking, holding, etc... In order to claim back the locked amount of collateral

$||sC||$, he or she needs to return back the borrowed $||sX||$. The constraint requires users to provide a collateral ratio amount CR greater than the minimum collateral rate MCR. For example, a user wants to issue new $sTSLA$ tokens by locking $sUSD$ collateral. For example, the TSLA stock currently has a price of $776, and $sUSD$ is being traded at $1. The system requires the MCR at 150%, so the user needs to provide the CR at least 150%. If a user wants to use 1000 $sUSD$ as locked collateral at CR of 200%, he will receive is: $\frac{1000\times1}{2\times776} = 0.64$ amount of $||sTSLA||$. Note here that since $||sTSLA||$ token is tokenized, it can be divided into smaller fractions, and small investors can own just a fraction of $||sTSLA||$. For example, in the case of Bitcoin, 1 Bitcoin is fractionated into 100000000 Satoshi, which is the smallest unit of Bitcoin.

3.5 Liquidation

Finally, to ensure the liability of the system, which means that all user's positions are being collateralized by the value of the number of stablecoins that are worth at least the minimum collateral ratio times the actual value of the borrowed tokenized asset in the real world, we introduce the liquidation mechanism. Liquidation happens when the circulating borrowed assets are being under-collateralized.

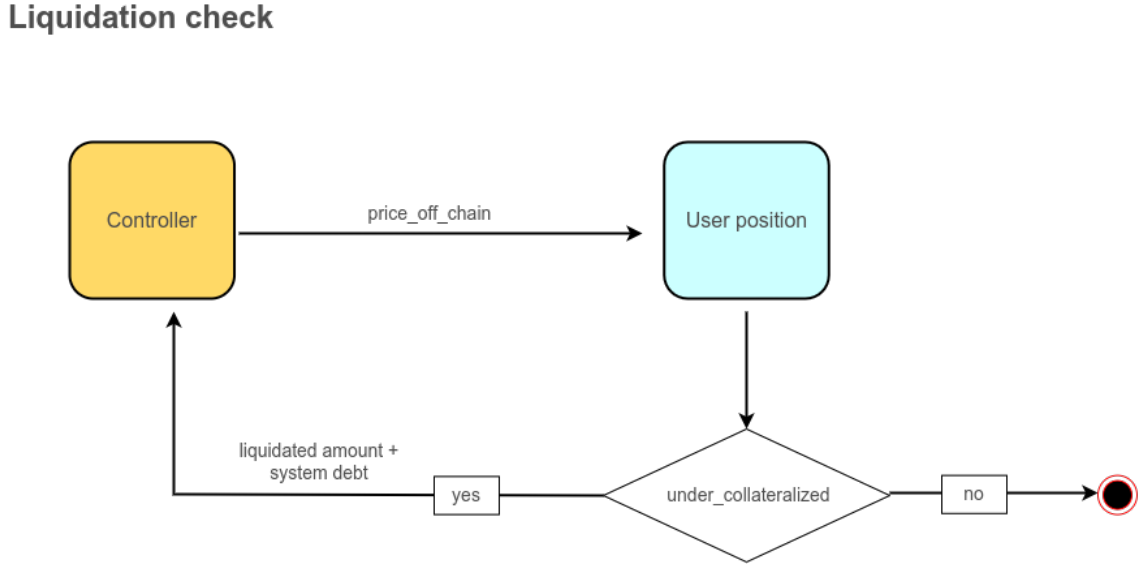

Figure 3.6: Liquidation Check

In the working flow of the system, in each time interval, the controller performs liquidation checks on all the active positions. If a position is spotted as under-collateralized, a liquidated amount of collateral will be transferred to the controller to perform buyback and burn a corresponding amount of system debt. If the position is qualified, then nothing will happen.

After a user has opened his position, lets α be the number of tokens that he

borrowed or the debt that he is owing the system. In order to borrow α tokens, the user needs to provide an amount of collateral β at the minimum collateral rate MCR. The user position also contains the premium rate Pr, which is the rate that will be used in auctions in order to incentivize to buy back the liquidated collateral.

The user's position needs to satisfy the following constrains to stay active:

$$\alpha \times sX^p \times MCR \leq \beta \tag{3.3}$$

$$\alpha > 0 \tag{3.4}$$

$$\beta > 0 \tag{3.5}$$

The constrain (3.3) ensures each user's position is being collateralized by an amount of collateral that has a value equal to at least the value of borrowed tokens times the minimum collateral rate. The constrain (3.4) and (3.5) remove the position which has no debt or no collateral left. In each time interval, the system will update price information from the oracle and examine positions' liquidation status. Let $sX^p_{t_i}$ is the price at time interval t_i, and $sX^p_{t_{i+1}}$ is the price of the asset at time interval t_{i+1}. Assuming that at the time t_i with the price of $sX^p_{t_i}$, the user position is about the get liquidated. The threshold can be expressed as follow:

$$\alpha \times sX^p_{t_i} \times MCR = \beta \tag{3.6}$$

There are two scenarios that happen at the time of t_{i+1}. The first one is at that time, the price of the tokenized asset is smaller than its price at the time of t_i. That would not violate constrain (3.3), and user position will remain safe. The second scenario is when the price of the asset increase, the user position will be partially liquidated. An amount of user collateral $d\beta$ will be used to buy back and burn the corresponding amount $d\alpha$ of SCA tokens at a premium. The amount of $d\beta$ and $d\alpha$ needs to satisfy the following constrains.

$$(\alpha - d\alpha) \times sX^p_{t_{i+1}} \times MCR = \beta - d\beta \tag{3.7}$$

$$d\alpha = \frac{d\beta \times Pr}{sX^p_{t_{i+1}}} \tag{3.8}$$

When the user position is under-collateral, an amount of $d\beta$ collateral will be withdrawn from the user position to perform auction. Equation (3.7) ensures that after performing buy back and burn, the user position is healthy, which satisfies the constrain (3.3). In equation (3.8), to incentivize users to sell their SCA tokens for the liquidated collateral, the auctions offer to buy user tokens at a premium rate Pr. Substitute the value of $d\alpha$ from constrain (3.8) to constrain (3.7), we can calculate the amount of $d\beta$ needed to perform buy back and burn:

$$(\alpha_i - \frac{d\beta \times Pr}{sX^p_{t_{i+1}}}) \times sX^p_{t_{i+1}} \times MCR = \beta - d\beta \tag{3.9}$$

Simplify the equation, we get:

$$d\beta = \frac{\alpha_i \times sX^p_{t_{i+1}} \times MCR - \beta}{MCR \times Pr - 1} \tag{3.10}$$

After getting the price of $d\beta$, by combining with (3.8), we can easily calculate the amount of $d\alpha$ that the system needs to buy back and burn.

However, the price of tokenized assets can change significantly in one interval, and there are cases when the user's collateral amount can not cover the amount of $d\beta$ needed to perform buyback and burn. In the following equation, the thresh hold of the maximum price at time interval $t_{t_{i+1}}$ for a self-liquidation position can be calculated under the following constrain:

$$\frac{\alpha_i \times sX^p_{t_{i+1}} \times MCR - \beta}{MCR \times Pr - 1} \leq \beta \tag{3.11}$$

The constrain (3.11) shows that in order for the system can use only the user's collateral to perform buy back and burn, the amount of collateral $d\beta$ needed to put into the auction needs to be smaller than the current amount of collateral the user is owning β. Shorten the constrain (3.11), we get a simpler version:

$$\alpha_i \times sX^p_{t_{i+1}} \times MCR \leq \beta \times MCR \times Pr \tag{3.12}$$

Combining this constrain with the constrain (3.3), we get the thresh hold of price changes for self-liquidation between a time interval as follow:

$$\frac{sX^p_{t_{i+1}}}{sX^p_{t_i}} \leq MCR \times Pr \tag{3.13}$$

According to equation (3.7) and (3.10), the amount of $d\alpha$ will be greater of constrain (3.13) get violated. However, we actually just need to buyback and burn an amount of α, so we can come up to the final equation to calculate the amount of collateral $d\beta$ as follow:

$$d\beta = \begin{cases} \frac{\alpha_i \times sX^p_{t_{i+1}} \times MCR - \beta}{MCR \times Pr - 1} & \text{if } sX^p_{t_{i+1}} \leq sX^p_{t_i} \times MCR \times Pr \\ \alpha \times sX^p_{t_{i+1}} \times Pr, & \text{if } sX^p_{t_{i+1}} \geq sX^p_{t_i} \times MCR \times Pr \end{cases} \tag{3.14}$$

3.6 Controller

Suppose that there are n opening positions. The total liquidated amounts of users' positions $||sC^l|| = \sum_{i=1}^{n} d\beta$ will be transferred to the controller to buy back and burn the amount of system debts $||sX^l|| = \sum_{i=1}^{n} d\alpha$. The controller is responsible for deciding to perform actions or perform direct buy back and burn to withdraw an amount Sa of system debts of assets from circulation.

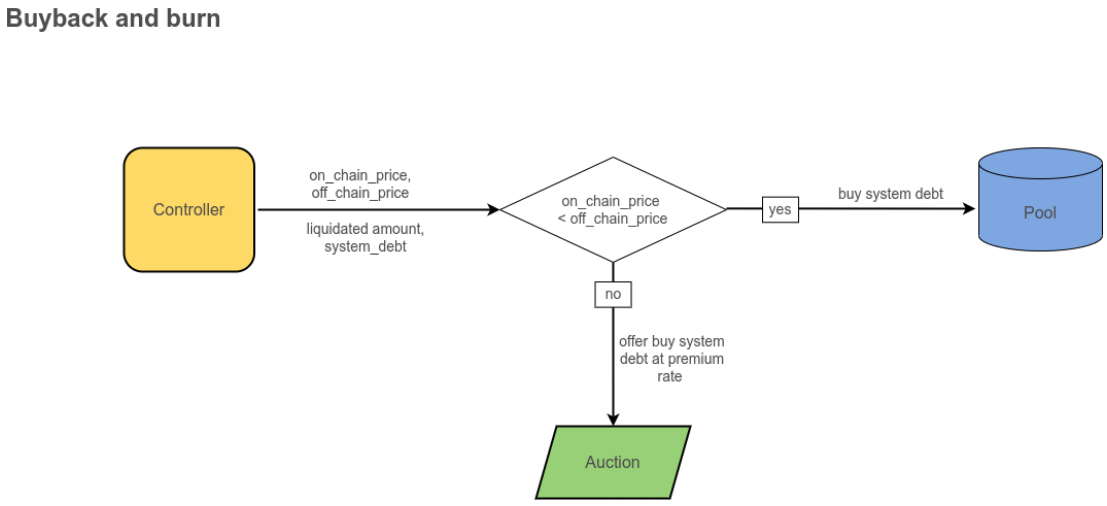

Figure 3.7: Controller

The price of SCA tokens on-chain and the price of corresponding assets off-chain may differ. The deviation of price can be classified into two main events. First, in the discount event, when the price off-chain is higher than the price on-chain. In reverse, we say that token is trading at a premium of the price on-chain is higher than the price off-chain. The controller then will decide to perform the corresponding actions based on these events.

- If tokens are being traded at discount, the system directly buys $||sX^l||$ tokens at the pool's pair price. The remaining amount of the collateral will be used to buy the SAG tokens and burn them in order to incentive SAG's holders.
- If tokens are being traded at a premium, the system will perform an auction to

buy from the user an amount of $||sX^l||$ tokens at a system's auction premium rate sPr. This premium rate represents how higher the system offers to buy back the SCA tokens from the users in the auction compare to its on-chain price.

3.7 Mechanism Derivation

In this section, we will discuss how the model acts in times of market volatility and how users will act upon them. After deciding what assets to tokenize, there are two vital concerns we will discuss in order for the model to work, which are the liability and the pegging ability.

3.7.1 Liability

Market rise and fall. Many assets tokenized model seems to work in a calm market, but seems to fail when the market volatiles significantly. And when they fail, they often fail tragically. We have witnessed many collapses, for example, NuBits, Basis Cash, Iron Finance, and Terra/Luna.The common idea in these designs is their systems are built on trust, rather than actual collateral. In the other words, they need a strong contingent of users who, even in the downturn, believe in the liability that the tokenized assets they hold can remain its value and the redemption ability is preserved event in bad market events. But people's rational decisions are vulnerable to frenzies and panics, so the system with no collateral backing often does not work. For example, in the case of TerraLuna which uses the dual coin mechanism, the system uses its native token Luna to absorb the volatility of the stablecoins. If the price of stablecoin goes below the peg, users can simply go to the system and exchange the underpriced stablecoins for the corresponding amount of Luna, but at the peg price. The same strategy applies in reverse, when the price of a stablecoin is being traded above the peg, the arbitrager can exchange an amount of Luna for the corresponding amount of the stablecoin at the peg price. The design success in the market boom, but in a downturn, when the trust is gone, the death spiral occurs. In the case of Luna, when the whole market falls, the price of Luna falls also. People panic about the liability of the system since the total market cap of stablecoins is nearly as big as the market cap of Luna. If the price keeps going down, the redemption ability weakens, and the value of circulating stablecoins might decrease as well. So people start to sell Terra's stablecoins, which drives the price of Luna even down further and causes panic since there is no actual guarantee of collateral or assets for the amount of token they own. The loop kept going on and have created one of the biggest crash in crypto history.

In a simpler design, stablecoins use reserved assets backing, which means that each stablecoins in circulation is backed by the corresponding assets in real life. The model works because of its simplicity, liability, and real collateral, not based on truth. Even though this kind of model has not yet reached decentralization and transparency, we cannot deny the benefit and the applications it has brought to the blockchain, which was siloed to the world. Many successful projects such as Tether, Binance USD,and USD Coin have made blockchain widely accessible to a much more people.

Our model attempts to solve the liability issue and aims to decentralize the model. Since cryptocurrency has developed and reached the point too big to fail, providing collaterals as forms of cryptocurrency ensures the value of the system. By over-collateralization, the system ensures that each and every circulating tokenized asset is backed by at least an amount of the value of its corresponding price. In the case of market volatilization, the liquidation steps in to ensure that if the value of a user's collateral is not enough, the system will do its job to buy back and burn the needed amount of tokenized assets to make the user's position legit. That self-functioning process will solve the liability issue of this kind of problem.

3.7.2 Pegging Mechanism

After the system is ensured by the liability, the second issue we need to address is to reflex the value of tokenized assets on-chain. There are three market scenarios for the difference in prices of the assets:

- **Normal**: SCA tokens on-chain are being traded around its peg
- **Premium**: SCA tokens are being traded at a higher price than their value off-chain
- **Discount**: SCA tokens are being traded at a lower price than their price off-chain.

The pegging mechanism is built on the profound theory, the quantity theory of money. Considering two scenarios we need to adjust the price, premium, and discount events. In premium events, SCA tokens' price on-chain price is higher than their value off-chain. According to the quantity theory of money, to lower the price, we need to increase or expand its supply. On the other hand, we need to contract its supply to increase the price of SCA tokens when it is being traded at discount.

Here are how users' rational choices might be during each event:

- In premium, they expect the price of SCA tokens will go lower in the near future. People also have incentives to sell the token and wait to buy at cheaper prices. The minters might consider this as an opportunity to borrow tokens since they can quickly pay them back at a lower price. This will expand the supply and will drive the price of the tokens down.
- In discount, the users that are in positions might want to close their position since they can buy them at discount. This will contract the supply. Also, the normal buyers might see this as an opportunity to own the token at the discount, so they will buy more and put the price back to the peg.

3.7.3 The governance token SAG

This section describes how the governance token can strengthen the liability of the systems in extremely volatile times. We introduced the SAG tokens as the government token, which are used for the community to submit their votes to update the price of an asset, propose to add a new asset to be tokenized, and change the parameters such as the minimum collateral rate or the auction premium rate of the system.

However, in extreme market conditions, SAG tokens can be used as the last line of defense against volatility. In these events, SAG absorbs the fluctuation of the market, hence the SAG holders get diluted. They fight against sudden volatility and are rewarded with the mechanism of the system. The SAG token stakes get a portion of the trading fee from the pools, and the SAG tokens often being buyback and burn when there is high demand for the SCA tokens.

Analyzing equation (3.13), the risk occurs if, between two adjacent intervals, the price of an asset increases by an amount more than $MCR \times Pr - 1$. For example, if a tokenized asset has the MCR at 150%, the premium rate at 105%, the price need to increase an amount of 57.5% between two intervals to put the system at risk of having to mint new SAG to cover up for the insufficient amount of collateral. This rarely happens since the interval are often set at a small time frame, such as 1 minute.

CHAPTER 4. NUMERICAL RESULTS

As we discuss in 3.7.1, liability is one of the most important factors of this tokenized assets model. In this design, the liability is ensured via the liquidation process. In short, the liquidation mechanism has the responsibility to ensure that each and every existing collateral debt position, which are the positions that the minters open by locking their collateral to borrow tokenized assets from the system, are "heathy". A "healthy position" is the position that satisfies the constrain (3.3), (3.4), (3.5). At each time interval, the system will check and validate all users' positions. If any positions are under-collateralized, the liquidation process will occur. In this chapter, we will provide simulation processes on the LocalTerra blockchain to perform the evaluation process on how the liquidation occurs and how risky it is when changing the parameters.

4.1 Simulation Scenario

In this scenario, we focus on evaluating the risk the system will take when the liquidation process occurs. At the time of t_i, a user position is currently at the blink of getting liquidated and can be formulated as an equation (3.6). The user can increase the amount of collateral to make his position back to safety. A safety position is the position that satisfies the constrain (3.3), (3.4) and (3.5). Assuming that the user does not provide more collateral, the value of MCR remains unchanged, the risk occurs when in extremely hyped market conditions when the price of the assets soars up in just one interval. In the next interval t_{i+1}, the price of tokenized asset $sX^p_{t_{i+1}}$ has increased, the user's position will get liquidated, and the amount $d\beta$ that the system will used to buy back and burn a sufficient amount of debt will be calculated using equation (3.14). A liquidating position is considered to be no risk to the system if it satisfied the constrain (3.11), which means that it has the self-liquidated ability. The liquidation position that violates constrain (3.11) will require the system to mint more SAG governance tokens to cover up the insufficient amounts of collateral.

The liquidation parameters can be summarized as follow:

Table 4.1: Liquidation parameters

Parameter	Annotation
t_i	The time interval in which the user's position are about to get liquidated
t_{i+1}	The time interval in which the user's position get liquidated
$sX^p_{t_i}$	The price of the tokenize asset at time interval t_i
$sX^p_{t_{i+1}}$	The price at time interval of t_{i+1}, which is greater than $sX^p_{t_i}$
MCR	The minimum collateral rate
Pr	The premium rate of the position
β	The position's collateral at the time t
α	The position's debt at the time t
$d\beta$	The liquidated collateral amount at time $t+1$

4.2 Risk endurance capacity

Risk endurance capacity of the system measures how the system can absorb price changes without the need of minting the governance tokens. When we have to mint the governance tokens to cover the liquidated amount of a user position, the system is being put at risk since the governance tokens holders getting diluted. If more and more tokens are printed, its circulating supply increases and hence devalues its price. A healthy position can perform self-liquidation, which means using the user's own collateral to perform buyback and burn. A poor design and unwise choice of parameters will put a lot of burden on the last defense of the system.

The percents of price change dX^p of prices between two time interval t_i and t_{i+1} can be defined as follow:

$$dX^p = \frac{sX^p_{t_{i+1}} - sX^p_{t_i}}{sX^p_{t_i}} \tag{4.1}$$

We named the product of MCR and Pr as the liquidation rate Lr. Combine these parameters with constrain (3.6), (3.10), we get the following equation to calculate the percentage between the amount need to perform liquidation $d\beta$ and the current amount of user collateral β as follow:

$$\frac{d\beta}{\beta} = \frac{dX^p}{Lr - 1} \tag{4.2}$$

Continuing the constrain (4.2), we define the risk endurance threshold of the system, which is the max percentage of price changes dX^p_{max} as the following constrain:

$$\frac{dX^p_{max}}{Lr - 1} = 1 \tag{4.3}$$

The simulation results will use the liquidation rate Lr as the parameters, which varies from 110% to 200% to define the risk endurance threshold as the following figure:

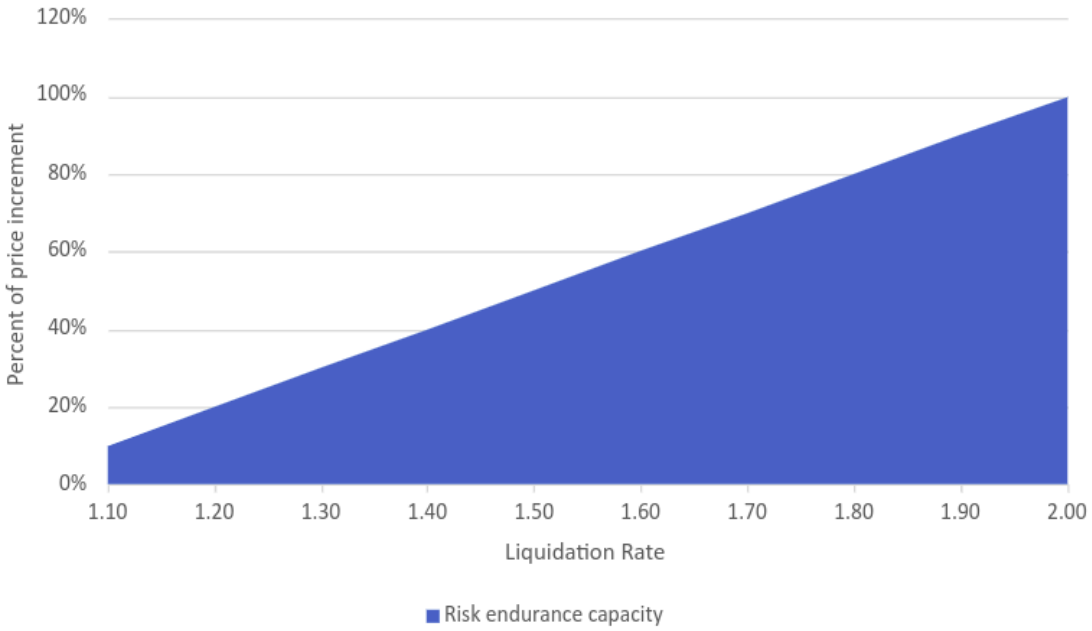

Figure 4.1: Risk endurance threshold

The chart shows the relation between the liquidation rate and the risk endurance capacity of the system. On the horizontal axis, the evaluate the different values of liquidation rates, which range from 1.1 to 2.0. When there are price changes between two intervals, if it stays inside the risk endurance capacity, the self-liquidation process occurs. If the price changes exceed the risk endurance hold, a new government token is required to be minted to perform buyback and burn.

As we can see, the higher the liquidation rate is, the higher the risk endurance capacity the system can provide. At the liquidation rate of 1.1, an increase in the price of over 10% will put the system at risk. Similarly, if the liquidation rate is set at 2.0, the price increment can range from 0% to 100% without putting the risk on the government tokens.

The choices for determining the liquidation rate, which includes the MCR and the Pr, need to be well aware of the community. If we tokenize an extremely volatile asset, the liquidation rate should be set higher than a normal asset. We recommend 150% as the suitable liquidation rate, but we allow the community to decide. We define a thresh hold for setting the liquidation rate at 110%, since lowering the liquidation would put a significant potential risk to our system.

The interval is set at a small timeframe. In our system, we deliberately choose the time interval of 5 minutes to balance the transaction costs and the performance of the system. The risk we analyze above is the risk of price changes between two adjacent intervals, which means that in 5 minutes, the price increases by 50% at the liquidation rate of 1.5, and the system will liquidate all of the user's remaining collateral.

The user's position state after update always satisfies the constraint (3.3), (3.4) and (3.5) of the above liquidation process. The risk here only occurs between two update times, so another way to reduce the risk of the system is to lower the time interval frame.

4.3 Liquidation Percents

In this section, we perform numerical simulations to calculate the percent of a liquidated amount compared to the remaining collateral of a user's position based on price changes between two adjacent time intervals and the MCR parameters.

Using the equation (3.14), we can calculate the liquidation percent compare to the current amount collateral of the position. Results of simulation on the parameters of price changes $d\beta$ from 0% to 50% and the variations of liquidation rate Lr between 10% to 100% returns the following result:

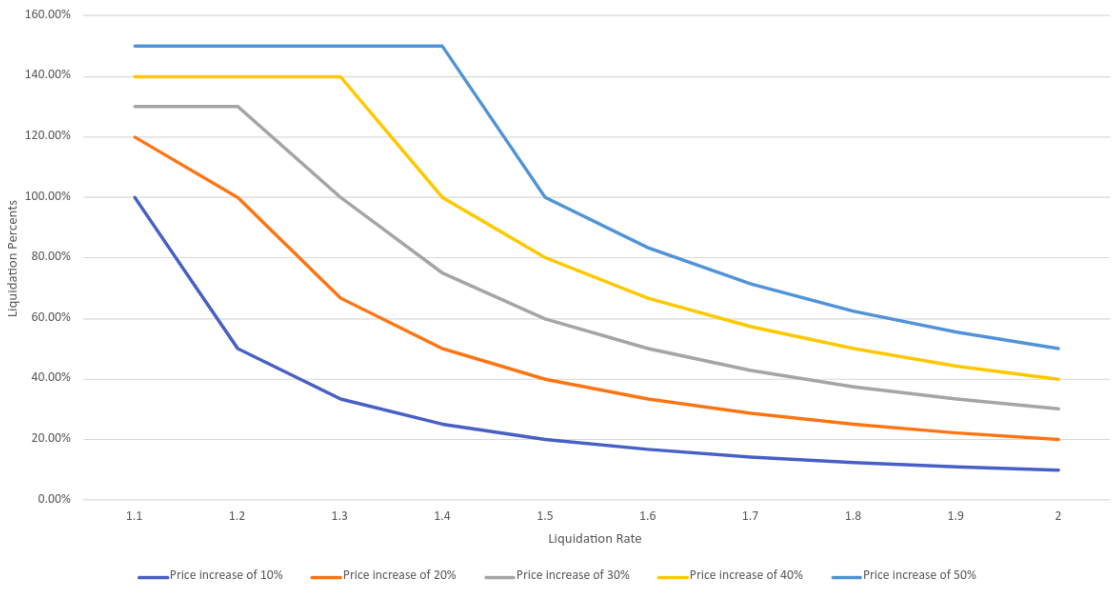

Figure 4.2: Liquidation percents of collateral percent of increase in price

The above figure illustrates the liquidation percent compared to the user's remaining collateral when there are price changes at each liquidation rate. In the horizontal axis, we examine the liquidation rate from 1.10 to 2.00, and the scenarios of price

changes including the increment of price between two intervals from 10% to 50%.

The figure shows that the lower the liquidation rate we set, the higher the liquidation percentages there are. For example, if a position has a liquidation rate of 1.1, it is extremely vulnerable to price changes. For example, if a user has an amount of collateral of 100$, when the price increase by 10%, the user's position will totally get liquidated. When the price increase by 30%, the system need to use 130$ to ensure the buyback and burn process, hence it is required to cover up 30$ for the user position.

At the liquidation rate of 1.5, the liquidation percent is one when the price increase by 50%. The more the liquidation rate increase, the lower the corresponding liquidation percent compare to price changes. If we set the liquidation rate at 200%, the user position only gets liquidated in half.

We can also see that if the price change passes the liquidation thresh hold, the liquidation percent is always equal to the price change. For example, if the price at the latter interval increases by 50%, the position with a liquidation rate smaller than 1.5 always gets liquidated with the liquidation percent of 150%. The position will be closed after this update.

APPL Price	Debt	Size	Collateral Ratio
165	606	150000	150.02%
172	533	137304	149.77%
163	533	137304	158.04%
185	419	116098	149.77%
190	385	109464	149.64%

Figure 4.3: Simulation data

In the above figure, we perform a simulation on the Localterra blockchain. The user opens a position with a collateral size of $150000 when the price of Apple's stock (APPL) is at $165 with an initial collateral ratio of the minimum collateral ratio, 150%. The system always ensures that when the price change, the collateral ratio, which is equal to size divided by debt, will always be greater than the minimum collateral ratio MCR. The size and the debt of a user position will be reduced accordingly to the liquidated amount.

CHAPTER 5. CONCLUSIONS

In this chapter, we summarize what problems the thesis has solved and the remaining problems that we need to address. We also provide our suggestions for future works, which researchers can use to utilize the models and customize them for their special needs.

5.1 Summary

This work focuses on analyzing the model and examining the effect of the external factors on the system. Many related works and researches have been investigated to choose the most suitable design. Some design proves to work, but remains centralization and management risk concerns, some can grow fast but are vulnerable to people's emotions. Some designs do not fully reflex the value of assets. In this work, we proposed the leverage loan design, which utilizes all the components of the other design. The model minimizes the liability issue and acts on behalf of the community. We discussed the pegging mechanism, the liability protection process, and its detailed implementation.

In short, the model can be summarized as follows. The model enables the creation of blockchain-based tokens that can be traded, stored, and transferred in the digital world. These tokens exist on the chain to reflex the value of the real-world assets. The ultimate goal of this model is to create a layer of asset-based that enables and stimulates the development of decentralized finance. By bringing the existing asset into the blockchain, tokenization can add liquidity and create a secondary market, allowing fractional ownership, offering greater interoperability, and removing the administrative burden and geographical barriers. Using the over-collateralized model, the user needs to lock an excess amount of collateral in return to mint new tokens. The liquidation and auction process is studied and examined to ensure the liability of the system, which means that every existing token is backed by an excess amount of collateral.

We implement the contracts on the Terra blockchain associated with the user interface to illustrate the main features of the model. The simulation is run to examine the risk the system will have to take when there are price changes. The code is usable in any blockchain of the Cosmos, which is the network that allows the interpolation of many blockchains. Cosmos is chosen because of its scalability and efficiency.

Even though the model utilized the existing design and is quite similar to the

successful example of DAI, it is not completely failproof and there remain some open problems that we need to address.

First of all, since the tokenized assets of the model may fall into the regulatory securities category, the compliance of the model needs to be researched and studied thoroughly. For example, the whitelisted and KYC process is required to comply with the Anti-Money Laundering, which we have discussed in section 2.4.1. Secondly, the incentive scheme for the holders of governance tokens has not been discussed in this work. The model should provide an appropriate incentivization for users for them to vote more actively, and preserve the value of the system. Thirdly, other mechanisms should be considered to reduce the volatility of the token price. Finally, researchers and developers can customize and provide more functionality for this model, which will be discussed in the following section.

5.2 Suggestion for Future Works

In this section, we introduced suggestions for future works that can be extended for this model.

5.2.1 Mint Collateral Diversification

Currently, the model accepted only stablecoins as a form of collateral. However, any cryptocurrency can be used as collateral. But higher volatile a cryptocurrency is, the more risk the system will take when using it as collateral. The market rises and falls, and we believe that there needs to be a thoughtful examination of the choices for collateral. For example, besides stablecoins, cryptocurrencies such as Bitcoin or Ethereum can be considered because they have market capitalizations and prove to be more stable than other tokens.

The choices of collateral can be further improved by allowing users to put many collaterals for backing a tokenized asset. This allows user to diversify their investment, and also reduce the risk of volatility. For example, instead of providing 100% amount of collateral in form of stablecoin, the users now can provide stablecoin, BTC, and ETH with the percent of value 50%, 25%, and 25% respectively.

5.2.2 Whitelisted

Whitelisted is a process similar to KYC. The model now can serve as a private model, which limits access to the tokenized assets. This process can ensure compliance, or especially design to meet the need of businesses and organizations. For example, a small group of investors might be a predefined number of investors having the ownership of a piece of land. The system then can allow the asset creator to whitelist addresses, or even apply the KYC process. Then, only the user who is on the

whitelist can access to own, trade, and sell tokens.

5.2.3 pre-IPO Assets

Initial Public Offering (IPO), is a process of offering shares of private cooperation to the public in a new stock issuance for the first time. An IPO allows a company to raise capital from investors. In the traditional finance system, the process of trading before the IPO, which is called pre-IPO allows private sales before the initial listing. However, the buyers are often the big organizations who are willing to buy significant stakes in the firm. This prevents small inventors from being able to perform these types of transactions.

A customized model for this type of asset can be enabled and allows individual investors have equal rights to access that pre-IPO event. The number of shares will be hard-capped, and during the pre-listing phase, the pre-listing price of the tokenized assets will have a fixed value, which is set by the issuer of the token. After the asset is listed, the oracle will be enabled to get the price of the actual asset. The opportunity now becomes available for everyone.

REFERENCE

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2018.

[2] "Blockchain powering internet of value," 2020. **url**: https://blockchainlab.com/pdf/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf.

[3] A. Moin, "A classification framework for stablecoin designs," 2019. **url**: https://assets.website-files.com/5d80307810123f5ffbb34d6e/5e6176a18436bc4204f4db36_stablecoin.pdf.

[4] F. D. Graham, "The primary functions of money and their consummation in monetary policy," *The American economic review*, **jourvol** 30, **number** 1, **pages** 1–16, 1940.

[5] W. E. M. Penny Pritzker, *Secure hash standard*. **url**: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf (**urlseen** 01/07/2022).

[6] U. W. Chohan, "The double spending problem and cryptocurrencies," *Available at SSRN 3090174*, 2021.

[7] G. Wood, "A secure decentralised generalised transaction ledger," 2022.

[8] E. B. Jae Kwon, *A network of distributed ledgers*. **url**: https://v1.cosmos.network/resources/whitepaper (**urlseen** 01/08/2022).

[9] D. A. P. Julian Grigo Patrick Hansen, *Decentralized finance (defi) – a new fintech revolution?* **url**: https://www.bitkom.org/sites/default/files/2020-07/200729_whitepaper_decentralized-finance.pdf (**urlseen** 01/08/2022).

[10] *The maker protocol: Makerdao's multi-collateral dai (mcd) system*, 2015. **url**: https://makerdao.com/en/whitepaper/ (**urlseen** 01/08/2022).

[11] *Non-fungible tokens (nft)*. **url**: https://ethereum.org/en/nft/ (**urlseen** 01/08/2022).

[12] *A deep dive into blockchain scalability*, 2020. **url**: https://crypto.com/university/blockchain-scalability (**urlseen** 01/08/2022).

[13] J. Hendler **and** J. Golbeck, "Metcalfe's law, web 2.0, and the semantic web," *Journal of Web Semantics*, **jourvol** 6, **number** 1, **pages** 14–20, 2008.

[14] *Ibc map zone*. **url**: https://mapofzones.com (**urlseen** 01/08/2022).

[15] D. R. Hayden Adams Noah Zinsmeister, *Uniswap v2 core*, 2020. **url**: https://uniswap.org/whitepaper.pdf.

[16] *Mirror: Reflecting asset value on-chain*. **url**: https://docsend.com/view/kcsm42mqiyu5t6ej (**urlseen** 01/08/2022).

[17] "Tether: Fiat currencies on the bitcoin blockchain," **url**: https://whitepaper.io/document/6/tether-whitepaper.

[18] "Centre," **url**: https://api-new.whitepaper.io/documents/pdf?id=HJX1cRBSO.

[19] *Binance usd*. **url**: https://www.binance.com/en/blog/futures/busd-all-you-need-to-know-about-the-stablecoin-421499824684903051 (**urlseen** 01/08/2022).

[20] T. Berners-Lee, *Top stablecoin tokens by market capitalization*. **url**: https://coinmarketcap.com/view/stablecoin/ (**urlseen** 31/07/2021).

[21] *Trueusd: A regulated and tokenized version of the us dollar*, 2019. **url**: https://trueusd.com/pdf/TUSD_WhitePaper.pdf (**urlseen** 01/08/2022).

[22] B. C. Cascarilla, *Pax gold*, 2019. **url**: https://paxos.com/wp-content/uploads/2019/09/PAX-Gold-Whitepaper.pdf (**urlseen** 01/08/2022).

[23] *Tether's first reserve breakdown shows token 49% backed by unspecified commercial paper*, May, 2021. **url**: https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/ (**urlseen** 01/08/2022).

[24] D. Kwon, *Terra money: Stability and adoption*, 2019. **url**: https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf (**urlseen** 01/08/2022).

[25] *Can terra blockchain sustain its growth? research report digs deeper*, Apr, 2021. **url**: https://cointelegraph.com/news/can-terra-blockchain-sustain-its-growth-research-report-digs-deeper (**urlseen** 01/08/2022).

[26] *The fall of terra*. **url**: https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/ (**urlseen** 01/08/2022).

[27] L. D. Nader Al-Naji Josh Chen, *Basis: A price-stable cryptocurrency with an algorithmic central bank*, 2018. **url**: https://www.basis.io/basis_whitepaper_en.pdf (**urlseen** 01/08/2022).

[28] M. R. C. Evan Kuo Brandon Iles, *Ampleforth: A new synthetic commodity*, 2019. **url**: https://api-new.whitepaper.io/documents/pdf?id=H1uqo9Tew (**urlseen** 01/08/2022).

[29] *How does ampleforth work? **AMPL** explained*, 2020. **url**: https://finematics.com/ampleforth-explained/ (**urlseen** 01/08/2022).

[30] *Monetary policy and central banking*, 2022. **url**: https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/20/Monetary-Policy-and-Central-Banking (**urlseen** 01/08/2022).

[31] *Supervisory and regulatory actions in response to covid-19*. **url**: https://www.federalreserve.gov/supervisory-regulatory-action-response-covid-19.htm (**urlseen** 01/08/2022).

[32] W. O. Douglas **and** G. E. Bates, "The federal securities act of 1933," *Yale LJ*, **jourvol** 43, **page** 171, 1933.

[33] J. W. Markham, *Commodity exchange act (1936)*. **url**: https://www.encyclopedia.com/history/united-states-and-canada/us-history/commodity-exchange-act.

[34] Finma, *Developments in fintech*. **url**: https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/.

[35] *Uniswap docs*. **url**: https://docs.uniswap.org/protocol/V2/concepts/core-concepts/swaps (**urlseen** 01/08/2022).