Exploring Stablecoins:

A HOLISTIC ANALYSIS OF USE, POTENTIAL, AND IMPLICATIONS

MASTER'S THESIS (CAEFO1041E) – MSc IN APPLIED ECONOMICS AND FINANCE

CHRISTOFFER KYLLEBÆK (S128478) & EMIL GALLOV RASMUSSEN (S127933)

SUPERVISOR: PETER BOGETOFT

Date of submission: 15th of May 2023
Pages: 119
Total Pages: 142
Number of Characters: 236,517

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Abstract

Stablecoins are crypto-assets run on a blockchain that aim to peg their value to legal tender currency to remain stable in price. This study analyzes the use, possibilities, and implications of stablecoins from a holistic perspective considering financial, technological, and political factors that may influence them. We find that holding stablecoins comes with considerable risks as they may not be as stable as their name suggests as they have instability properties and can fail. Since stablecoins are crypto-currencies, a comprehensive analysis of how blockchain technology impacts them is also conducted to find that stablecoin transactions will have difficulties on the base layer blockchain with transaction throughput. However, using a Layer2-scaling solution, stablecoins transactions can be competitive with alternative transaction methods. Extensive adoption of stablecoins can have macroeconomic implications and threaten monetary policy transmission. Thus, policy-makers may be incentivized to regulate them. The example used in the thesis to illustrate a comprehensive regulatory framework is MiCA, introduced by the European Union. Under MiCA, Stablecoins will soon need to be fully backed by a liquid reserve while transaction volumes will be limited. On top of regulating stablecoins, some central banks are considering a competing digital currency that could threaten the use of stablecoins. We argue that while stablecoins have considerable difficulties to be characterized as money. Stablecoins, in the proper context, still have some features that can make them a better alternative to traditional means of payment. Introducing a central bank digital currencies can only challenge stablecoins in some respects.

Contents

1 Introduction

The 31 of October 2008 marks a special day in the history of finance as it was the day the pseudonym Satoshi Nakamoto published the first whitepaper for the cryptocurrency Bitcoin. Since that day, crypto-currencies like Bitcoin have been on everybody's lips due to their highly volatile nature and the possibility of earning a high return on such assets. However, possible high returns are not the only exciting feature of crypto-currencies, as their foundation is built on the revolutionizing blockchain technology. A technology best described as a shared database that can ensure trust, transparency, security, and transaction traceability without intermediaries or central authorities.

While cryptocurrencies have gained significant attention, their volatile nature has prevented mainstream adoption and utilization similar to money. In response to this issue, stablecoins emerged as a solution for individuals who wanted to hold crypto-assets on a blockchain network without exposure to extreme price volatility by referencing the price of a legal tender currency.

As they are currently mainly used as a safe haven for crypto investors who want to keep their assets on the blockchain, stablecoins are yet to fulfill their potential outside of the crypto-ecosystem as an alternative to traditional means of payments. Though small adoptions have been made in some areas, stablecoins may face significant challenges and require further exploration to understand how stablecoins should be used and their potential.
This study explores this matter by looking at several factors that may impact how stablecoins are used and how they may be used in the future.

2 Research Questions and Scientific Contribution

The phenomenon of stablecoins is a new area of study in finance and economics, where previous studies of stablecoins have aimed to uncover the topic from a single, delimited perspective. This project seeks to provide a comprehensive understanding and assessment of the concept. Therefore, the contribution to the scientific field of study is the holistic approach to stablecoins, where we assess the phenomenon based on the sum of all the analyzed factors explored. The contribution thus lies in evaluating stablecoins from an application perspective, where the project will consider the macroeconomic, financial, and technological challenges they may face.

Thus, this study aims to:

Provide a holistic assessment of the use, possibilities, and implications of stablecoin from a financial, technological, and political perspective.

To provide this assessment the following research questions will be answered:

- What are stablecoins?
- How do decentralized blockchains enable safe stablecoin transactions?
- What are the financial risks of holding stablecoins?
- What technological factors impact the use of stablecoins?
- What are the motivations of regulating stablecoins and how may policy-makers regulate them?
- Are stablecoins money?
- What do stablecoins offer that is unique to traditional means of payment?
- Will stablecoins survive an introduction of a central bank digital currency?

3 Methodology

3.1 Philosophy of Science

Though stablecoins are a relatively new phenomenon, various scientific contributions have already been made. Many of these contributions have taken a positivistic approach to the subject by seeking to verify certain traits of stablecoins through induction. Others have taken a more critical rationalistic approach where the aim of the study has been to falsify a hypothesis regarding stablecoins. Since many contributions are now in place, a general assessment of the phenomena is needed to understand stablecoins in a greater context. Because of this, a holistic perspective concerning relevant topics within the field of study is used. Here, subjects of stablecoins will be stated and discussed in relation to each other for a better comprehension of the phenomena.

A general assessment of such a complex topic as stablecoins and their role within society requires a broad perspective. The philosophy of science can be characterized pragmatic in the sense that multiple approaches are utilized to give insights into the field of study (Lewis & Thornhill, 2012). As the research questions are not pointing toward one scientific position, such as positivism, the research of the subject will take multiple approaches. The emphasis is on the practical implications of using stablecoins on an individual and societal level.

The philosophy of science can be described by looking the ontology, epistemology, and axiology of the study. Ontology is the study of what reality is and epistemology is the question of how knowledge can be defined and what we can know about reality (Presskorn-Thygesen, 2021). Finally, axiology describes what role of the researchers' values should be in the study (Saunders et al., 2012).

The ontology of philosophy is external but with multiple perspectives to answer the research question. For the research, both observable phenomena, such as market prices and subjective opinions, will be necessary to interpret the data available. In interpreting phenomena, the thesis will take on both subjective and objective points of view.

3.2 Research Design and Structure

A research design consisting of three parts has been chosen to provide a holistic perspective on the use and potential of stablecoins. Here, the first part involves a comprehensive introduction to the

fundamental concepts of the subject, the second is an analysis of relevant factors of stablecoins, and the third is a holistic discussion based on the analysis. The first two parts create the foundation for a qualified discussion of the three questions in the third part. The following figure represents the research design:

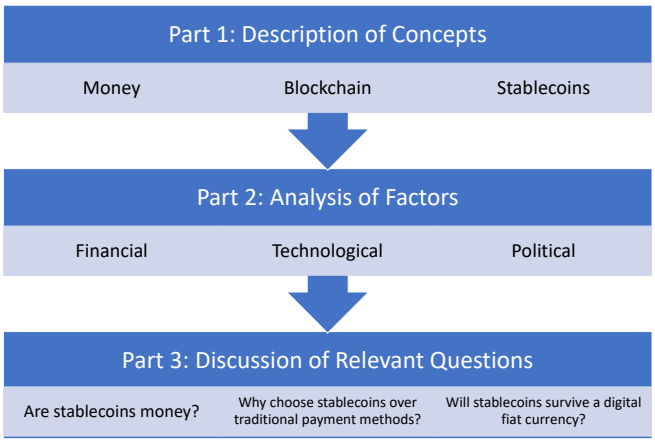


Figure 1: Research Design. Source: Own Creation

Before initiating the analysis, it is necessary to define some concepts that will be utilized later in the project. For this reason, the first part of the thesis will consist of an introduction to the fundamental concepts of the subject. This part includes a theoretical section on what money is and the different types of money, a comprehensive but necessary presentation of the blockchain technology that stablecoins are based on, and a characterization of stablecoins and their features.

The analysis will build on the concepts presented in the first section, focusing on three specific areas. First, stablecoins will be analyzed from a financial perspective focusing on stability, the risk of default, and the risk of storing them. Second, with the concepts presented in the blockchain section, there will be an analysis of the possibilities for scaling the technology and the technical factors that affect the use of stablecoins. Third, as external factors can also affect stablecoins, we will examine the macroeconomic consequences that a widespread adoption of stablecoins can have. Finally, after identifying the negative externalities that stablecoins can bring, we will look at the opportunities for policymakers to regulate stablecoins and the options available for governments to create a competing product.

For a general assessment of stablecoins, three key questions will be raised based on the analysis's conclusion. The first question will be a theoretical discussion of whether stablecoins can be classified as money and which flaws, they have in the theoretical context of money. The next question will focus on the application of stablecoins. Specifically, we will examine the reasons for choosing to use stablecoins as a means of payment over traditional methods. The last question will be forward-looking and examine the future of stablecoins concerning a possible introduction of a central bank digital currency.

3.3 Data Collection

This thesis utilizes primarily secondary data to address the research questions. The choice of this type of data is due to the scope of the research question and to ensure a broad and nuanced understanding of stablecoins. Given the exploratory nature of the project, the advantages of utilizing secondary data include that it requires fewer resources and potentially has a higher quality than empirical data collection (Saunders et al., 2012). Furthermore, secondary data allows for the possibility of making unforeseen discoveries that otherwise may have been overlooked through own empirical research (Saunders et al., 2012).

Concerns about relying heavily on secondary data include losing control over data quality. As the scope of the project is extensive, it would be challenging to ensure the quality of all sources as the thesis considers several topics that require a high degree of expertise. Furthermore, the collected sources may have biases depending on the sender and the intention of creating the data.

Therefore, it is essential to include an assessment of the validity and reliability of the secondary data. The sources utilized in the thesis can be categorized into five distinct types: books and academic journals, industry and government reports, news articles, market data (such as prices and capitalization), and internet blogs specifically focused on blockchain and crypto-assets. We will briefly discuss both validity and reliability regarding the five types.

First, regarding books and academic journals, it has been assessed that there should not be significant issues with reliability or validity. The issue of reliability and validity is considered unproblematic because of the author’s academic qualifications within the studied subject. Most of the academic journals included have undergone peer-review, but it is important to state due to the

topic's novelty, all journals included have not been peer-reviewed. It can be argued that this may cause minor issues regarding the reliability and validity of the journals used. However, these sources have been considered reliable and valid enough to add context and value to the research.

Sources characterized as industry and government reports predominantly refer to publications from official institutions such as the International Monetary Fund, the European Union, and the US Federal Reserve. It also includes reports on relevant subjects published by private institutions, e.g., law and consulting firms. These sources can be biased because the author may have other interests than being objective. However, given the sender's expertise, the sources should have adequate reliability and validity in a proper context.

News articles are utilized to provide external context, such as reactions to introductions of new regulations in the area, and provide an understanding of discourses and consensus in the population regarding the subject. As blockchain and crypto-assets can be a tremendously complex subjects for conventional journalists to comprehend fully, there may be some concerns with the validity of these sources. However, since these sources do not serve in the context of explaining concepts in blockchain, this is not considered an issue.

Quantitative secondary data regarding market prices are primarily collected from Coinmarketcap, Statista, and Glassnode with all three being some of the most used platforms for market price-monitoring crypto-assets. The reliability of such data is high as there can only be minor errors in measuring the changes in prices and measures alike. Quantitative secondary data regarding the Ethereum blockchain is primarily drawn from Etherscan, one of the primary providers of data for the Ethereum blockchain. In general, there are no issues with the validity and reliability of this data source type.

Internet blogs focused on blockchain and crypto-assets represent the potentially most controversial secondary data source utilized in the thesis. This is because many of the contributors of such sources are anonymous. Because of this, these sources call for a high degree of caution. Though there are particular challenges in meeting credibility, validity, and reliability standards, such data and sources are necessary to include when the subject concerns blockchain and crypto-assets like

stablecoins. The reason is that blockchain is built on open-source principles that allow for contributions from anyone. Furthermore, the pace of developments within this technological area is too high for new information to be shared through conventional academic journals. As a result, the culture within the blockchain community is that updates and relevant insights are posted directly on specific online blogs. Despite this type of data source requiring significant quality control, it is essential to include it in any study related to blockchain.

3.4 Limitations

The study aims to provide a holistic and explorative approach to the researched subject. Because of this, the limitations and scope of the project were not clearly defined at the beginning of the research. This was an active choice as a scope too narrow would prevent a general and nuanced assessment of stablecoins. However, space limitation dictates that some elements of the subject have been left out purposely.

Overall, the project will only consider crypto-assets that are run on a permissionless blockchain network referencing the price of a legal tender currency. These assets will be referenced as stablecoins throughout the project. This implies that the term stablecoin will not include private settlement coins used on private networks, e.g., JPM Coins. It also implies that crypto-assets pegged to assets other than legal tender currencies of a country are also excluded. Another limitation is that only current stablecoins are included in the project, so Meta's possible introduction of Libra will not be part of the thesis.

A crucial part of the study is investigating blockchain's impact on stablecoins. Blockchain networks can vary in many aspects and certainly in the ones included in the analysis. Since it would be too comprehensive to include all blockchain networks, it has been decided only to consider the most used and representative blockchain, Ethereum.
We do not set further limitations regarding crypto-assets fulfilling the requirements listed earlier. However, because of the limitation of the Ethereum blockchain network, the main focus will be on the most capitalized ERC-20[1] stablecoins.

[1] ERC-20 is a standard for fungible tokens created on the Etheruem blockchain. The term shall be clarified later on in the thesis.

Since the analysis aims to cover many aspects of stablecoins, it would be impossible to go into detail to the same degree as a thesis focusing on only one. This reflects why a literature review of stability is chosen over a self-conducted empirical analysis. The technology part will also include elements that could have been studied in more detail to a degree where it could have been a thesis in itself. In terms of analyzing from a regulatory perspective, it would be impossible to consider the regulations of every country, and we have thus chosen what we find to be the most relevant regulatory framework, MiCA.

These shortfalls in the analysis can be subject to criticism but are necessary compromises to fulfill the thesis's objective of giving an overall assessment of stablecoins.

4 Review of Concepts

4.1 Theory of Money

To understand stablecoins as an entity in a larger context, it is essential to make clear what money is. Understanding the nature of money will make it easier to evaluate the shortcomings of stable-coins when compared to traditional means of exchange. In this first concept review, we will study the properties of money and describe two critical terms of money that will be utilized throughout this project.

4.1.1 Properties of Money

A common way to describe money is by describing the three properties it must possess (Anderson, 2019). The three properties are: A unit of account, a medium of exchange, and a store of value.

First, money must be a unit of account. This means that the unit must be acknowledged by a broad consensus to be worth something. Typically, people view their local currency as a unit of value. In this way, money is used to value goods or assets. For example, a person living in the Eurozone will value goods in Euros. He will clearly know how many Euros a cup of coffee, a pizza, or a particular house is worth. Not that the value estimation is necessarily correct, but the point is that the person will use the currency as a measure of value. In the same way, debt and obligations can easily be settled by this medium. For example, suppose one owes another person ‘1000’. In that case, the borrower cannot repay him with 1000 stones but instead typically with the local currency

such as euro, dollar, or pound (even if the stones have a higher value than the currency). Thus, money creates a common base for prices.

Second, money is a medium of exchange, meaning that it allows people to avoid bartering. For example, a farmer does not need to trade the corn he produces for other products he may need. Instead, the farmer can sell the corn on the market and then get money to shop for the needed products. To be a medium of exchange, money must be fungible, meaning that one unit of money must be the same value as another unit of the same money. Again, this is another reason why stones cannot be money since no stone is the same, and one could argue that two stones would not have an identical value. A central principle used in this thesis when defining money is the 'No Questions Asked'-principle presented by Gorton & Zhang (2021). NQA-principle means that when doing a transaction, the taker of the money will accept the payment without asking questions or inspecting the money received.

Third, money is a store of value. Money must maintain its value over time. Again, take the example of the farmer earlier and imagine that corn was a unit value and a medium of exchange. Here, the problem is that the corn itself depreciates when it molders over time, meaning that the farmer can only save the corn for a limited amount of time if he wants to use it. Moreover, the money must also be able to be stored safely.

4.1.2 Fiat Money

Fiat Money is currency issued by the government. Instead of being backed by a commodity or reserve, it is solely backed by the government issuing the money. Central banks typically control this type of money, and it is the only legal tender currency that central banks can issue. In simpler terms, fiat money refers to paper money and coins that are not backed by physical commodities. Because it has no backing, it is inconvertible and cannot be redeemed at the central bank for any asset. The value of fiat money is derived from the belief and trust that the entity has a value that can be realized through its utilization as a medium of exchange and unit of account in society.

Many central banks have moved from representative money to a fiat currency which is best exemplified by the ending of the gold standard in the US (Ghizoni et al., 1971). Such transformation

can give central banks more control of the economy and earn the government seigniorage profits when issuing new money.

4.1.3 Representative Money

Representative money is a form of money where the value of the money represents an intention to pay with an underlying asset or financial instrument. This implies that the money on issue is backed by an asset or a pool of assets that can be redeemed. In many countries, the legal tender was a representative currency typically backed by precious metals such as gold. Up until 1971, the US dollar was directly convertible for a certain amount of gold in the United States (Anderson, 2019). Though many central banks have moved away from issuing representative money, most payments today are made with representative money issued by commercial banks in the form of bank checks or credit cards.

Money held in commercial bank accounts will be referred to as commercial bank money. It consists primarily of deposit balances that can be transferred electronically or by paper checks. This type of money differs from fiat currency as the value is backed by the commercial bank instead of the government. This is because the cash clients deposit is not safe kept but invested or lent out to other clients. Hence, the cash becomes an asset for the bank, and the bank account opened is a liability for the bank. Commercial banks can then create new money by issuing loans to the bank accounts (Sveriges Riksbank, 2023.). Account holders have the right to withdraw the cash but can also transfer the money using cards or checks without withdrawing the fiat currency deposited (Selgin, n.d.).

4.2 Decentralized Blockchains

Decentralized blockchains are the foundational platforms that enable stablecoins' existence. To comprehend the technologies that execute and govern stablecoin transactions, we will now examine the key concepts of one of the largest decentralized blockchains, Ethereum.

4.2.1 Digital Money and the Foundation for Distributed Ledger Technology

Physical cash payments have one of the benefits of being anonymous to the extent that two parties can engage in a transaction for a service or good without any information about either the payer or the recipient being needed for the transaction to succeed. Once physical cash has been spent, the payer is unable to spend the same note or coin again as it is no longer in their possession. If one

were to perform this scenario online using digital cash, an issue arises as nothing stops the payer from performing two transactions on the same cash note. This is known as the double-spending problem.

Currently, the use of debit and credit cards relies on banks to serve as intermediaries to ensure a safe payment transaction, stopping the double-spending problem. As an intermediary is overseeing the transaction, it is not truly anonymous. Moreover, if a dispute between the two parties involved occurs after the time of the transaction, the intermediary, the bank, would often have the power to reverse the transaction, which contrasts with a physical cash settlement.
If one were to replicate a physical cash transaction between two parties using digital cash without the intervention of an intermediary, a decentralized system of operation would need to be to solve the double-spending problem.

Such a decentralized ledger is referred to as a permissionless distributed ledger technology, commonly known as blockchain. It is permissionless as it allows anyone to add a transaction to the ledger, and the ledger's state is open for the public to see all transactions and balances. This, of course, has certain privacy implications, as no one wishes to publicly display their account balance with their identity. However, we will see in the following sections how cryptography is used to create pseudo-identities so that a person is only identified if the individual chooses to reveal the address of their public account.

4.2.2 Fungible Tokens

Stablecoins are cryptocurrencies that do not have their own blockchain but rather exist on blockchains as fungible tokens. Using smart contracts, a concept that will be elaborated on in the coming sections, tokens can be created. Tokens can represent a variety of functions, such as currency, asset ownership, access right, voting rights, identity documentation, utility functions, and many more (Antonopoulos & Wood, 2018). These tokens will exist on the blockchain, where ownership of a token is able to be transferred through smart contracts clearing the transfer (if that function is enabled in the smart contract creating the token).

The two main ways of telling apart the characteristics of a token is whether a token is distinguishable from other tokens. In the crypto space, this concept is referred to as fungibility. Fungible

tokens (FTs) are simply tokens that are interchangeable with other units of tokens without change in value or function. Non-fungible tokens (NFTs), on the other hand, represent tokens referring to a specific and unique asset or item (Antonopoulos & Wood, 2018).

To better streamline token creation (tokenization through smart contracts and help ensure format compatibility with exchanges, where tokens are often traded, blockchains supporting smart contracts will often have token standards. Token standards are smart contract code templates that simplify the tokenization process. Examples of this are the Ethereum Request for Comments standards. The two most utilized standards for Ethereum tokens are the ERC20 standard for fungible tokens, i.e., stablecoins, and the ERC721 standard for non-fungible tokens (ethereum.org, 2023b).

4.2.3 Permissionless Distributed Ledger Technologies (Decentralized Blockchains) in Layers

To provide a simpler overview of the mechanisms that enable secure transactions, accounting, economics, and much more within a decentralized blockchain, let the blockchain architecture be structured into layers, as seen in the illustration below. By following this structure, we will learn all the intricacies of a blockchain. It should be noted that the "Infrastructure Layer" will have its own chapter, as the components of the layer will be elaborated through the "Execution layer" and "Network Propagation Layer".

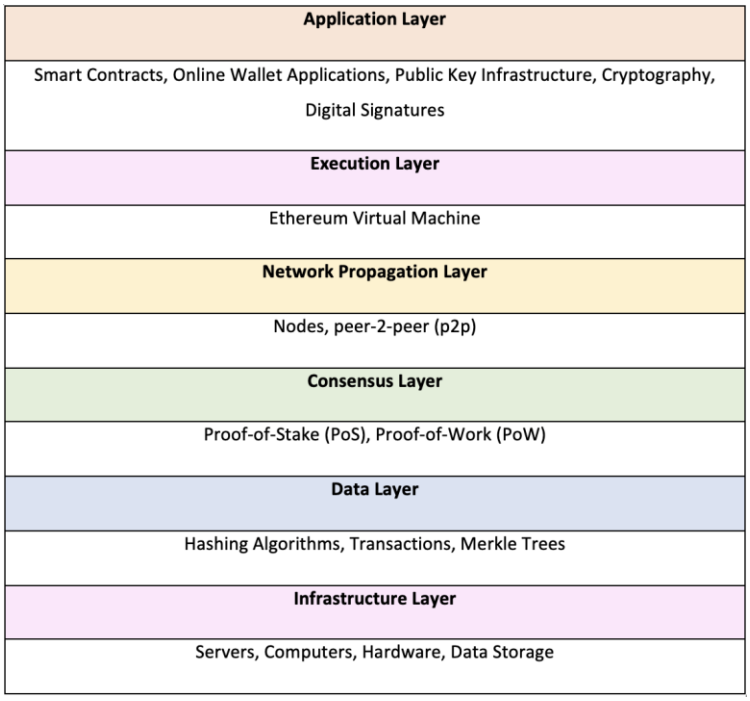


Figure 2: Layered Structure of a Decentralized Blockchain. Own Creation

To understand the layered structure chronologically, we will be following an example of a stable-coin transaction between Alice and Bob.

Bob owns a local pizzeria where Alice often eats. Bob has complained to Alice that now that his customers are increasingly making cashless payments, the cost of credit and debit card payments are cutting into his profit margin, as the costs of these card transactions are carried by the merchant and not the card user. Furthermore, Bob had two instances last week where customers, who had paid with their credit card using the tap-and-go function had called their card provider, and denied having ordered and paid for this pizza. Even though the card provider, Visa, had covered the cost of the pizzas, this would mean someone had acted dishonestly in the transaction.

Alice understands Bob's frustrations and wants to support a local business. Alice is an individual proficient in blockchain technologies and helps Bob set up a digital wallet which can be thought of as a bank account for cryptocurrencies. Alice then pays Bob 10 Tether (USDT), a stablecoin designed to hold the same value as the US dollar.
The transaction is completed using the Ethereum main net, where Alice carries the transaction cost of 0.0026 ETH, the cryptocurrency native to the Ethereum blockchain, which is equivalent to 4.93 USD. After 36 seconds, Bob received the 10 USDT in his wallet, and Alice received her pizza. After 16 minutes, Alice informs Bob that now sufficient blocks have been accepted to the Ethereum blockchain so that it would be computationally infeasible for the transaction to reverse. Everything mentioned in this example with be elaborated on in later sections.

4.2.4 The Application Layer - Smart Contracts and the Ethereum Virtual Machine

The term smart contracts were first coined by Nick Szabo, (1996), a pioneer within computer science and cryptography. Szabo (1996) described smart contracts as *"A set of promises, specified in digital form, including protocols within which the parties perform on these promises"* (Szabo, 1996). In essence, a smart contract in one of its simplest forms could, as an example, be: Inserting coins into a laundromat. In this case, the promise is that once the customer (party 1) inserts a certain number of coins, the laundromat (party 2) will perform a laundry wash. The laundromat

will be programmed to perform this command beforehand and will only do so when the pre-specified criteria are met.

The first-generation blockchain Bitcoin was used solely to document the state of transactions in the local currency (BTC) through a public ledger. Once a transaction is sent, the Bitcoin protocol executes a smart contract, I.e., A set of digital commands that carries out the transaction. In today's world, many blockchains are designed to run standardized smart contracts, not only carrying out transactions in the native currency of the blockchain but also on a wide assortment of other services or assets that have been digitalized. The most used blockchain protocol to carry out such smart contracts of a universal nature is the Ethereum Virtual Machine (EVM) (Antonopoulos & Wood, 2018)**.** The EVM carries out commands specified by smart contracts that are activated by a transfer of ETH in a concept called gas, which is more thoroughly explained later. To sum up, concerning our example of the laundromat: A payment is made in ETH to the EVM, which executes the smart contract through a computational command. This part happens at the Execution layer, which is elaborated on in its chapter.

4.2.4.1 Wallet Creation and Public Key Infrastructure

Decentralized blockchains function with a publicly distributed ledger, meaning that all transactions can be seen by everyone and added to by everyone. In practice, transactions can be added to the ledger that has not been agreed to by the other party. To ensure both security and privacy on a transactional level, digital cryptography is an integral part of blockchain technology. In the case of most cryptocurrencies, asymmetrical encryption, called Public Key Infrastructure (PKI), is applied to all transactions to verify the transaction's validity.

In simple terms, PKI is used for executing transactions on a blockchain and relies on two elements: a public key and a secret key. The public and secret key serves the purpose of securely exchanging information on the blockchain (Lipton & Treccani, 2022). Once a public and secret key pair has been created and connected to the blockchain protocol through an access link, this will serve as a digital wallet.

Recall our interaction with Alice and Bob. Alice helps Bob generate a digital wallet, by creating a secret and public key pair. The public key will in layman's terms be Bob's account number for receiving transactions, whereas the secret key will be his password for sending transactions. It is important that only Bob knows his secret key, as the holder of the secret key will be able to send transactions.

A secret key is first randomly generated as a string of 256 bits in binary code. An example of a binary secret key could be:

0100110100000110101110011101100101000001000010000001000011111111
1000111001011110010011001101010111011010100000100111100011100000
1011001111011100101010101011011010001111101010111111101101110100
1010010000011011110011111010110111110011100111100010011001110011

This string of bits should be interpreted as some random number between 1 and 2^{256}.
For convenience a secret key can be expressed in hexadecimal, which is another way of expressing the number. Hexadecimal numbers are with letters A to F and numbers 0 to 9 as below, giving us a private key of 64 characters:

4d06b9d9410810ff8e5e4cd5da8278e0b3dcaab68fabfb74a41bcfadf39e2673

Once a secret key has been generated, a public key is derived from it. Different cryptocurrencies will use different algorithms for cryptographic encoding, so to simplify the Elliptical curve digital signature algorithm has been chosen for illustrative purposes as it is used for both, the Bitcoin, and Ethereum public key infrastructure.

4.2.4.2 ECDSA Elliptical Curve Digital Signature Algorithm

The ECDSA is an elliptical curve function, that can be expressed visually as a graph that exists on an incredibly large field of coordinates. Here the secret key is multiplied by a starting point expressed as x and y coordinate on the elliptical curve called a generator point. When multiplying a number in this case our secret key, with the coordinates of the generator point on the elliptical curve. In elliptical curve mathematics, this result will be equal to adding G with itself $G + G +$

G ... ... n times where n is the unique number of the secret key (Antonopoulos & Wood, 2018). Below is a representation of the processes is illustrated:

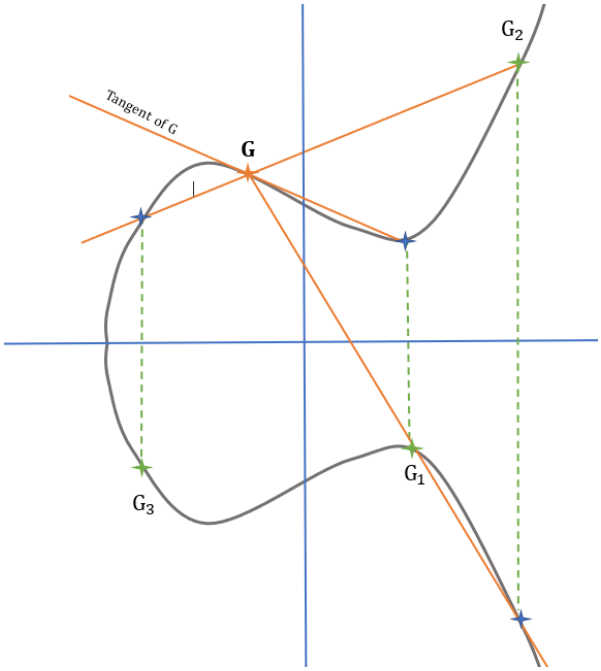


Figure 3:Public Key Generation, Where G is Added to Itself Sk Number of Times on Curve. Source: Own Creation

Looking at the illustration above, adding G to itself once will give the point equal to where the tangent of G intercepts on the Elliptical curve. The next starting point will be the point on the dimension below. Call this point G1. Now the next point is represented as the intercept of a line running between point G and G1 on the elliptical curve, where the point in the dimension above will represent point G2 and so on, repeated the number of times of the secret key.

The final addition point on the graph will represent our public key and can be shared with the world. The ECDSA standard is applied in most decentralized blockchains for public key infrastructure and uses "secp256k1" as the input parameters for deriving the public key from the ECDSA. These input parameters and the ECDSA formula can be found in the Appendix I.

As the secret key is an integer containing 256bits and G an (x,y) coordinate on the elliptic curve, each point containing 256 bits, we are left with an x and y coordinate on the curve, containing the public key giving us a size of the public key as 512 bits.

The nature of the public key function is such that the public key can easily be calculated if the secret key and generator point are given. However, the secret key is infeasible to calculate with

modern computing power, with only the public key and the generator point given, as they are not integers but instead coordinates on the elliptical curve. Thus, the secret key cannot be extracted by isolating in an equation. This kind of function is called a trap door function and secures the encryption mechanism for the Public Key Infrastructure.

In summation, the PKI is the foundation that ensures that no one else than the holder of the secret key can send messages or transactions from the corresponding public key address, nor can anyone obtain the currency received from that public address. Modern digital wallet platforms will have this entire secret and public key generation process built into the code of the application so that a random secret key is generated and displayed only to the user of the application. The public key generated will be a 128-character string in hexadecimal:

04a0d157a185b63c9531ff0e22f17b9a5bd70e9c89f7ad28bec40fe1a97c9fe1d5
494f9d3104338f86991c79aa524b866027968b9f04b3aa346ca71d38edfe2672

Now a public key should theoretically be ready to send and receive transactions. Many blockchains will, however, use different ways of displaying public keys. The Ethereum blockchain uses an address format for wallets called an externally owned address, which is essentially written like a smart contract in the code language Vyper or Solidity that the Ethereum Virtual Machine can interpret in binary code. The digital wallet acts like a smart contract, meaning a user will interact with it through a transaction. An Ethereum address besides the encoding is created with an extra security measure where the public key is run through a trapdoor sha256 hash function called Keccak-256, here the last 40 characters of the hash are added an 0x at the front giving a total of 42 characters in hexadecimal like illustrated below (ethereum.org, 2023a):

14ee76fa49938541242a7b16121a9cf621e40264db397753a3f59208f57c185e

With the corresponding Ethereum wallet address:

$$\mathbf{0}x\mathbf{121}a\mathbf{9}cf\mathbf{621}e\mathbf{40264}db\mathbf{397753}a\mathbf{3}f\mathbf{59208}f\mathbf{57}c\mathbf{185}e$$

Recall our interaction with Alice and Bob. Bob has now entered his secret key through the ECDSA. Using cryptographic mathematics, he is left with a secret key, a public key, and a digital wallet address compatible with the Ethereum blockchain. This address that Bob has created is written like a smart contract, where Bob will now be able to receive funds and send funds in his digital wallet.

Hashing algorithms are essential for transaction security and keeping the blockchain unchangeable. A look into how exactly how and why hashing algorithms are used in blockchains will be explored in the following section.

4.2.4.3 Hashing Algorithms

In the context of blockchain and distributed ledger technologies, PKI ensures that the holder of the secret key can generate the corresponding public key. Transactions sent on the blockchain can contain messages of any length. The variation in length makes the messages impractical for computers to interpret. To account for this issue, hashing algorithms are utilized.

A hashing algorithm is a trapdoor function that will take an arbitrary length input and provide an output of a fixed length called a hash or digest. Attempts to reverse the function to generate the input using the output hash will be computationally infeasible. Most blockchains today use a variation of the Secure Hashing Algorithm, SHA-256, where 256 refers to the 256 bits output that the algorithm produces. As bits are binary and will either be a 0 or a 1, this mathematically gives 2^{256} possible combinations for the SHA-256, which is an incredibly large number.
Most often the hash output will be expressed in 64 hexadecimal characters like that of a secret key. An example of the usage could be:

SHA-256 input: **Learning cryptography is easy**
SHA-256 output: **eecd9a63e48580d6946b4e715496b8ea920fc29ae3a827d54cf51ecede83ceca**

Typing the above message into any sha256 calculator will always yield the same output as the output above and corresponds to the determinism property of the hashing algorithm. The important feature that hashing algorithms such as the sha256 holds is non-correlation (Antonopoulos & Wood, 2018). Non-correlation can be explained by making a tiny change to the input

message, such as replacing the capital letter ‘L’ with a lowercase ‘l’, we get a radically different hash, that cannot be correlated to the previous input, as is illustrated below:

SHA-256 input: **learning cryptography is easy**
SHA-256 output: **c57da6e9c6ec561b1e5f65f2c7a53fd898d0f3d20151e4c07b51552399f08f36**

Finally, a main property of hashing functions is that the hash generated should be collision protected, meaning that it should be infeasible to generate the same hash output with two different message inputs (Antonopoulos & Wood, 2018). Below we will see how hashing algorithms are used together with the ECDSA, secret, and public keys, to secure and verify digital transactions.

Now that Bob has a digital wallet, Alice sends him 10 USDT from her digital wallet. Alice uses her secret key to generate a digital signature, which Bob will be able to verify using Alice’s public key once he has received the funds of 10 USDT. We will see later how this verification process works.

4.2.4.4 Digital signatures and transaction verification.

In the greater context of the distributed ledger, anyone can add transactions to the ledger. As this is the case there needs to be a way of proving that this transaction was in fact agreed upon by the sender of the payment. This is achieved with digital signatures, that the receiver can verify as valid or invalid.

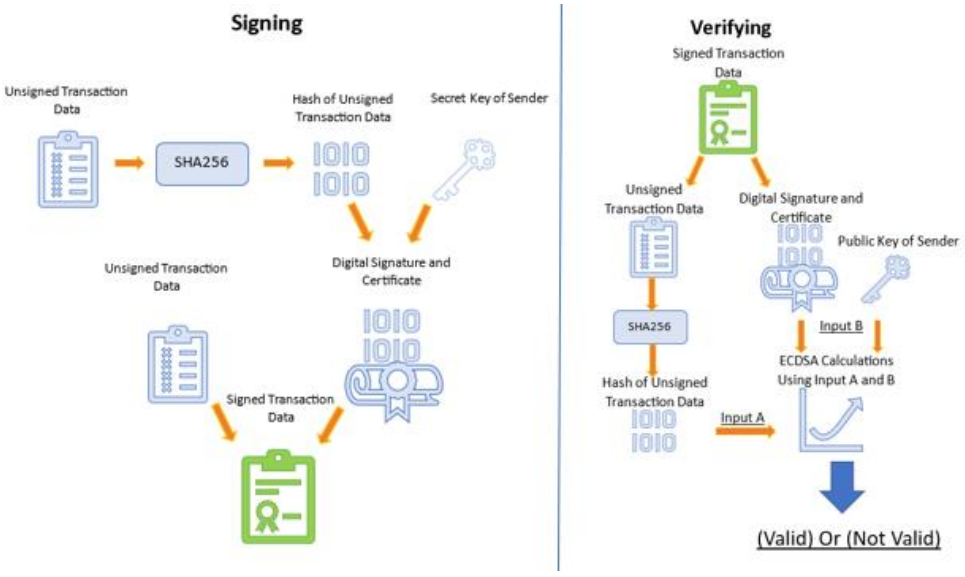


Figure 4: Digital Signing and Verifying Transaction Data. Source: Own Creation

From the illustration, we can see how using the secret key, and a hash function, will enable the sender to sign the transaction digitally. This digital signature will enable a recipient to verify the validity of the transaction with the corresponding public key. This process is known as asymmetrical encryption and is how trustless transactions are carried out on a permissionless ledger. The asymmetric encryption used by the blockchain-recorded digitally signed transactions requires a few more security steps, including elliptical curve cryptography calculations. For simplicity, this process has been left out but can be found in Appendix III.

This concludes the functions interacting in the Application Layer of a permissionless decentralized blockchain. To sum up, digital wallets that interact with blockchains and smart contracts rely on public key infrastructure consisting of secret and public keys. These keys and hashing algorithms enable users to safely send transactions from a public address without revealing anything else about themselves. A recipient can then verify the transaction's validity from the digital signature attached to the transaction by using the public key from the sender. In the next section, we will see how the transaction is carried out on the blockchain.

4.2.5 Execution Layer

4.2.5.1 The Ethereum Virtual Machine, a Publicly Distributed Computer.

A virtual machine carries out transactions performed on newer generations of blockchains. An introduction to the Ethereum Virtual Machine (EVM) will be made to better grasp this concept.

As the name might indicate, the EVM is not one physical computer. Instead, the EVM can be considered a distributed mesh network of computers that are all processing an agreed sequence of commands.

Recall or example. Alice sends the transaction to the EVM: "Send 10 USDT from Alice to Bob". The EVM will process this transaction by first checking that Alice has 10 USDT in her digital wallet, if yes, the EVM will carry out the transaction by crediting Alice 10 USDT and debiting Bob 10 USDT. If Alice, however, does not have the funds to carry out the transaction, the EVM will see it, and refuse the command, resulting in a failed transaction.

As computing power is never free, virtual machines like the EVM will require a fee for executing a command, also known as a "gas fee," which can be considered the transaction fee. As complex commands require more computations, the gas fee will proportionally increase with the complexity. Steps of computations are measured in "gas units," so the accumulation of "gas units" involved in a transactional command will then be noted as the "gas cost." The price of gas units is denoted in the cryptocurrency native to the blockchain that the virtual machine operates on. In this case, for the EVM running on Ethereum, the gas fee is paid in Ether (ETH). This concept will be elaborated further in the analysis.

The structuring of a transaction carried out by the EVM can be illustrated as the following, where values are hypothetical for illustration purposes.

Structure of a Tether Stablecoin Transaction Command Carried Out by the EVM
Function selector: **Tether token (USDT)** *(Informs the EVM that the value transferred is USDT)*
Nonce: **24** **(***The sequence number of transactions from Alice's wallet to prevent double-spending the transaction)*
Gas price: **40 Gwei (***The price per unit of gas that the sender is willing to pay (demand estimated))*
Gas limit: **65,000 (***The maximum units of gas the sender is willing to let the EVM use to execute the transaction)*
Recipients address: **0x121a9cf621e40264db397753a3f59208f57c185e (***Bob's wallet address)*
Value: **10 (***The amount to send to the recipient, (function selector determined the unit))*
Data payload: **From Alice to Bob as payment for pizza (***Variable length message attached to transaction)*
Digital signature certificate: **Digital signature components for verification (***Digital signature that can be checked against Alice's public address for verification (see Appendix III for details))*

Figure 5: Structure of Transaction Inputs for a Stablecoin Transaction on Ethereum. Source: Own Contribution (Antonopoulos & Wood, 2018)

Alice now sends Bob 10 USDT, which is structured like the table above, inputs like Nonce, Gas price, Gas limit, and digital signature certificate are automatically filled in by the wallet software on Alice's digital wallet. The transaction is now broadcasted to the network and carried out by the EVM.

When sending transactions and messages over blockchain networks, the data is broadcasted and passed along in the network by connected “nodes” acting as “peers” to one another. We will see in the coming section how this process works.

4.2.6 The Network Propagation Layer

4.2.6.1 Broadcasting transactions on the peer-to-peer network.

When sending transactions and messages over blockchain networks, the data is broadcasted and passed along in the network by connected “nodes” acting as peers. As decentralized blockchains are permissionless, everyone can become a node by downloading and running the blockchain protocol. Once a digital wallet connects to a blockchain network, it becomes a client to a server, meaning it will request information that the server will provide. These nodes can perform different tasks such as executing transactions (EVM), recording transactions (storage), verifying transactions, creating blocks, validating blocks, and, most important of all, propagating information and data. The EVM is essentially a mesh network of nodes, where individual nodes lend out their computers to sequentially run the commands sent to the EVM.

On a permissionless (public) distributed ledger, nodes run as a network referred to as Peer-to-Peer (p2p). The p2p term means that the nodes on the network are all peers to one another, implying that no node holds more power than another (Antonopoulos, 2017). All nodes on a P2P network are not directly connected to one another, but instead, one node is connected to an array of nodes, which are all connected to a different array of nodes, and so on.

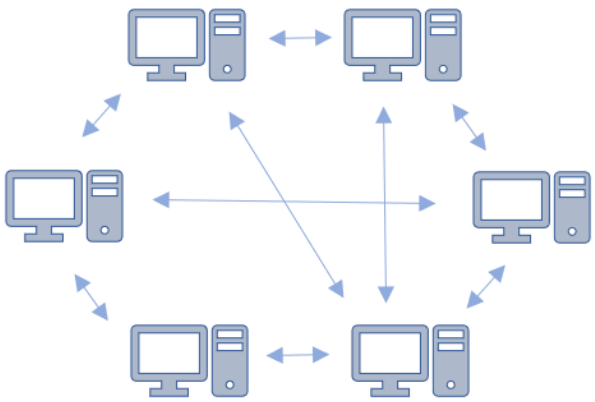


Figure 6: Illustration of peer-to-peer (p2p) network of nodes. Source: Own Illustration

Often when referring to a node, what is referred to, is a full blockchain node that has a full copy of the entire blockchain and the corresponding transactions in each block stored in its memory. The node will constantly update and add new blocks to the blockchain independently of other nodes and broadcast its version of the blockchain to the network for consensus (Antonopoulos, 2017). For a decentralized permissionless blockchain, this feature ensures that the network has a certain level of resilience against attacks or failures, as the network can endure if one or even many nodes fail.

Full nodes play a crucial role in verifying that transactions are valid in accordance with the blockchain protocol. The protocol is a set of rules encoded into the network, meaning if one node is discovered to broadcast false information, it will be ignored by the network to preserve the integrity of the blockchain (Lipton & Treccani, 2022).

Once a transaction is created through a wallet, it is received by a full node on the p2p network. The node will then verify if the transaction is in accordance with the blockchain protocol, which can vary depending on the network, most often this involves that the data structure is correct and that the input referencing the monetary output has not already been spent in a previous transaction (Antonopoulos, 2017). If the transaction is valid, the node will add the transaction to its mempool, a localized pool of unconfirmed transactions, and propagate the transaction to neighboring nodes. These neighboring nodes will then repeat this process independently, ensuring that a fraudulent node will be detected and isolated if found. When a transaction is placed in the mempool, it is in essence, ready to be added to the blockchain and confirmed by the consensus mechanism native to the blockchain protocol of that network.

Alice's 10 USDT transaction to Bob has been executed and spread throughout the network of interconnected nodes. It now awaits being finalized by being included on a block attached to the blockchain; here, it will be visible to everyone and un-reversible.

To sum up this blockchain layer, the data propagation layer is a network of computers all running the blockchain protocol. The nodes will execute, receive, check, and spread transactions to their neighboring nodes at rapid speeds so that, in a short period of time, the entire network will be

aware of a transaction. Now transactions are executed and broadcasted to the network in the previous three layers, and this, however, does not mean that they are final and immutable yet. Transactions are not final before they are confirmed on a block in the blockchain. We will in the next section, see how blockchains are governed through consensus mechanisms and how blocks and blockchains are assembled.

4.2.7 Consensus Layer

4.2.7.1 Proof-of-Stake

A consensus mechanism is a protocol that ensures agreement on the state of transactions between the nodes. The consensus mechanisms implemented to govern larger decentralized blockchains like Ethereum are called Proof-of-Stake (PoS). Another known consensus mechanism is the Proof-of-Work-Mechanism which is explained in Appendix IV.

PoS has a consensus mechanism consisting of so-called validator nodes responsible for transaction execution, block creation, and block validation. These nodes have a full copy of the blockchain (full nodes) stored on their hard disk. On the Ethereum PoS protocol, a full node is then required to insert a "stake" of 32 ETH into a smart contract to become a validator. This stake will serve as collateral, incentivizing the node to act honestly, as dishonest behavior will be punished, with the node losing some of its stake and the right to be a validator. This enforcement is known as "slashing." As Blockchain consensus mechanisms can be seen as a democratic attestation to the true state of transactions, balances, and accounts, posting a 32 ETH stake to become a validator can be seen as providing identity and receiving the right to cast one vote to the perceived state.

To visualize block creation and PoS consensus mechanisms, we will describe how it works in practice on Ethereum. The PoS Consensus mechanism starts every "epoch" consisting of 32 blocks, each assigned to a time slot. The roles that a number of nodes will carry out in the upcoming epoch are assigned in the two epochs preceding the upcoming epoch by a pseudo-randomized process.

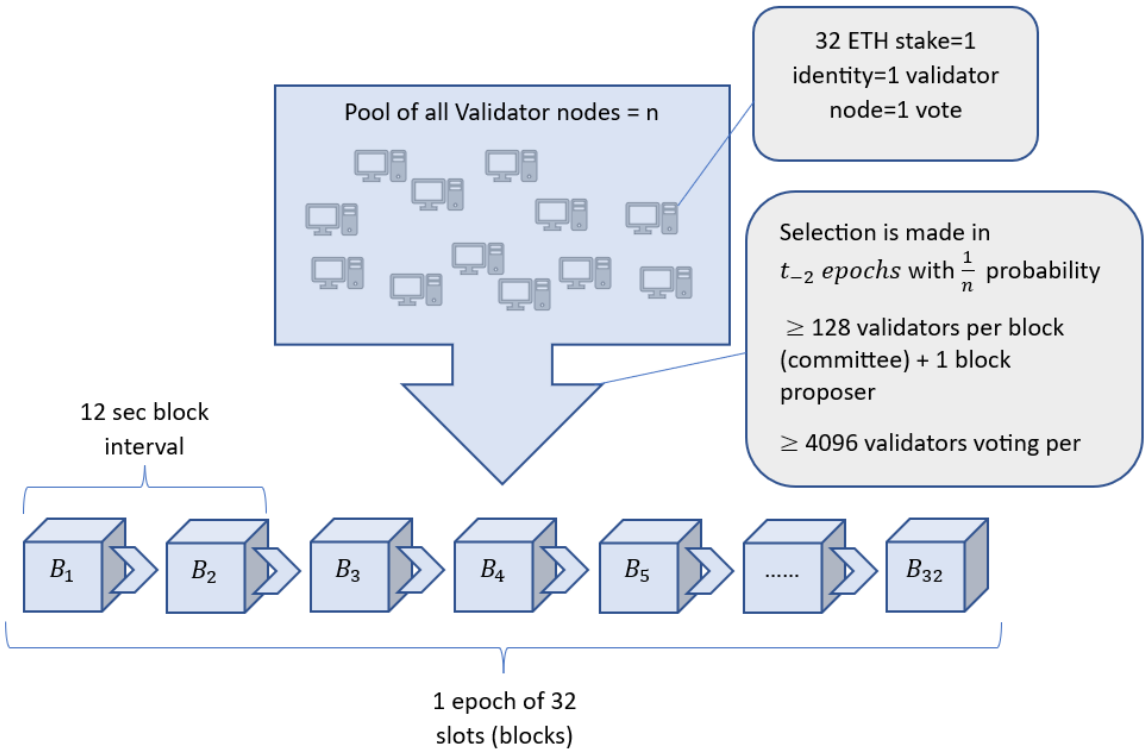


Figure 7: Role Assignment to Blocks in an Epoch. Source: Own creation

32 validators are chosen to each create a block in an assigned timeslot of 12 seconds so that an Epoch makes up 6 minutes at 24 seconds. These validators are called block proposers. More than 128 different validators are assigned to each of the 32 blocks to independently verify and vote if the proposed block is valid.

4.2.7.2 Block Proposal and Structure of the Blockchain.

Each block will have an appointed validator node construct a candidate block which will be the next block to be added to the blockchain. But, first, the node will gather all the transactions in its mempool into a Merkle tree, as illustrated below:

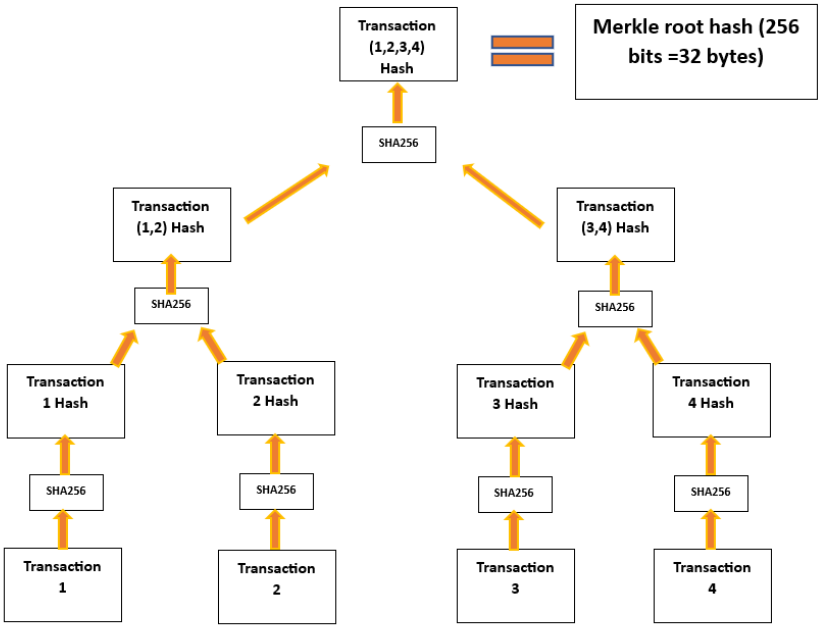


Figure 8: Merkle Tree of Hashed Transactions. Source: Own creation

Each transaction is hashed together on the leaves of the Merkle tree, and the result will be a single hash called the Merkle root hash. This is included in a Block Header along with a timestamp and the hash of the previous Block Header, as illustrated below.

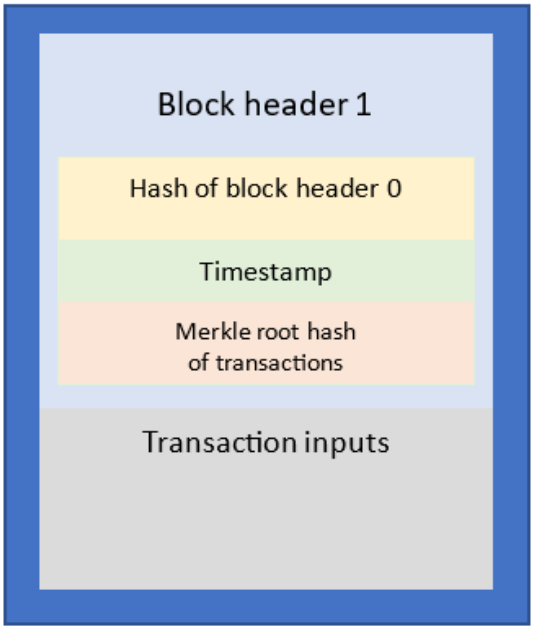


Figure 9: Layout of Block Inputs. Source: own creation

Depending on the consensus mechanism that the given blockchain uses, information in the block header will vary. All information in the block header is hashed, and the block is propagated out via the p2p network on the propagation layer, where validator nodes on the block's committee will validate its accuracy.

4.2.7.3 Block Validation of the Validator Committee

When validator nodes on the committee of this block receive the proposed block, they independently validate two things:

First, that using the hash of the last block (parent block) in each of their copy of the blockchain, hashed together with the block header inputs from the proposed block, will give the same hash result as what is provided by the block proposer.

Second, the validator nodes on the committee will independently re-execute the transactions from the proposed block to see if they are valid (Ethereum.org, 2023). If valid, the validator nodes will attest to the proposed block's validity by signing it and adding it to their local blockchain copy, equivalent to casting a vote. On the other hand, they will not add the proposed block if found invalid, equivalent to casting a vote on the previous block. Here a local consensus is said to be reached if a 51% majority of the validator nodes on the committee votes for the proposed block.

They will now begin broadcasting the block to each local neighborhood on the p2p network. Soon after that, the entire network of nodes will have added the block to their copy of the blockchain, and once 66.67% of the network of nodes agree on the newly added block, we will have reached global consensus. This is reached after around 2.5 epochs or 16 minutes (80 blocks) (Ethereum.org, 2023).

Now the next block in the epoch is created, and this new block proposer will use the hash of this block in its block header for the next block as its parent block, as the next block uses the hash from the previous block in the hashing input for the next block. This means that the hash would no longer be the same if one were to make even the slightest change in any inputs from a previous block.

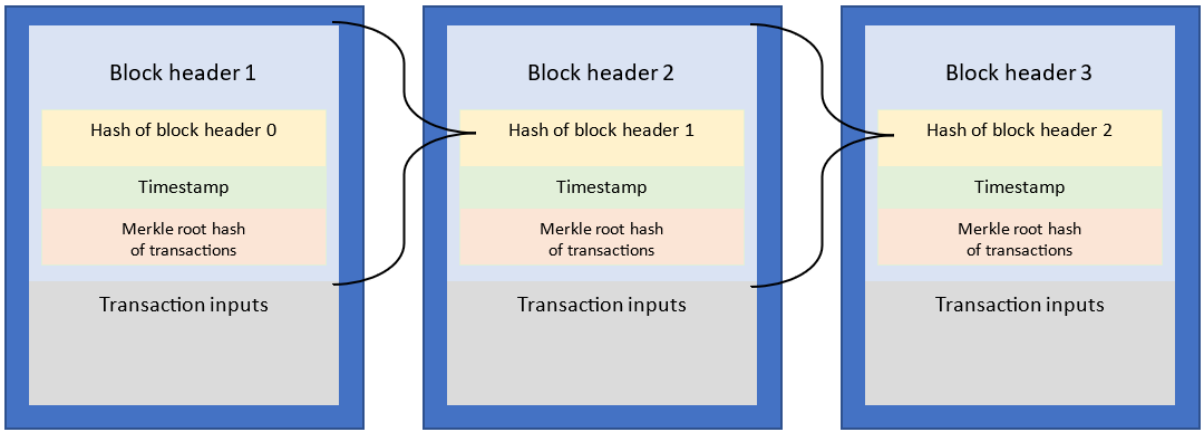


Figure 10: Blockchain Linked by Previous Hash. Source: Own creation

If the hashes of the blocks on the blockchain were not to match, it would invalidate all the subsequent blocks. On the other hand, a matching chain of hashes will provide a theoretical immutability guarantee of transactions, which fundamentally provides the chain links for the blocks.

4.2.7.4 Latency and Forks

As new blocks are created at a fixed block interval every 12 seconds on the Ethereum blockchain, slow internet speed (latency) can limit how fast new blockchains are propagated out on the p2p network. As a result, a block that should have been the fourth block in the epoch has now become the third, thereby using the same parent hash as the actual planned third block. This can result in conflicting views on the perceived order of blocks in the blockchain, also commonly called a fork, as illustrated below.

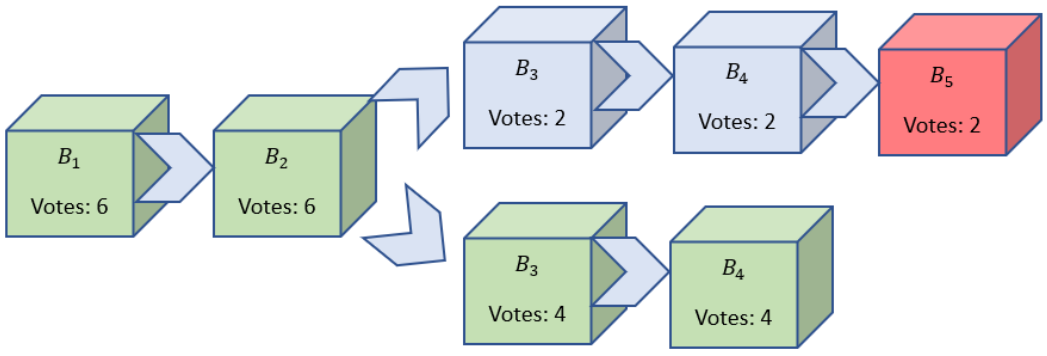


Figure 11: Blockchain Fork (Heaviest Block in Validator Votes Win). Source: Own Illustration.

Recall that validator nodes will attach a signature when voting for a block and adding it to its blockchain. The PoS Ethereum protocol nodes will always adopt the block with the most validator signatures attached. As each vote represents an individual 32 ETH stake, the block with the most votes is where most of the validator network capital has been invested (Buterin et al., 2020).
This is contrary to the PoW blockchain protocol used by Bitcoin, where "mining" nodes always adopt the longest chain, as it would have the most amount of computational Proof-of-Work attached to it (for further explanation, see Appendix IV).

As for who is allowed to create a new block differs in what consensus mechanism is used for the blockchain. The two most adopted consensus mechanisms are currently, Proof-of-Work and Proof-of-Stake, which are the consensus mechanisms governing Bitcoin and the later Ethereum. Ethereum switched from PoW to PoS as of September 15th, 2022. Several other consensus mechanisms are being developed and used, perhaps with higher efficiency than the two mentioned, but for the time being, PoW and PoS are the prevalent two. As the thesis will focus on the Ethereum blockchain, Proof-of-Stake will be the consensus mechanism in scope. A detailed description of the Proof-of-Work consensus protocol used in Bitcoin can, however, be found in Appendix IV.

4.2.7.5 Validator Node Incentives

As seen in the above chapters, many functions are required for a decentralized blockchain to run reliably and honestly. As blockchains often transfer tokens of value, nodes executing transactions and recording the total state of transactions and balances might be motivated to attempt to cheat for financial gain. For decentralized blockchains, this game theoretical problem of dishonest or faulty nodes is known as the "Byzantine generals problem," where the consensus and incentive system employed in PoS and PoW are theoretical solutions to said problem.

The incentives for validating on the Ethereum blockchain are rooted in how new ETH is issued. For every block created, newly minted ETH is paid to the validator nodes as compensation for their services. Whereas PoW requires miner nodes to spend copious amounts of computational power amounting to large electricity bills, PoS requires no more than simple computations.
As a result, the block rewards paid to validators are in accordance with each function executed correctly. The validators are only rewarded if the block is adopted onto the global consensus

blockchain. Each action below carried out timely and correctly will qualify the validator for a block reward (Buterin, 2022) (ethereum.org, 2023d).

A. Reward factor: **14** "Reward for the attestation getting included at all."
B. Reward factor: **26** "Reward for the attestation specifying the correct epoch checkpoint."
C. Reward factor: **14** "Reward for the attestation specifying the correct chain head."
D. Reward factor: **2** "Reward for correctly participating in sync committee signatures."
E. Reward factor: **8** "Reward for proposing block."

The numbers in each assignment represent a block reward factor in accordance with the role that the validator played in the validation of the block. Hence, the max block reward factor would be 64. If an action is executed incorrectly, the reward will be negative.
The rewards earned by a validator attesting to a block are found as a function of:

$$Validator\ Reward = Effective\ Balance * \left(\frac{Base\ Reward\ Factor}{(Base\ Rewards\ per\ Epoch * \sqrt{Total\ ETH\ staked})}\right)$$

Where the Effective balance is the amount that a validator has left of their stake. The base reward factor is the sum of base reward factors executed correctly. The base rewards per epoch is a constant fixed at 4.

This will yield a maximum base reward of:

$$\text{Maximum Base Reward} = 32 * \left(\frac{64}{4 * \sqrt{17{,}915{,}429}}\right) = 0.121\ \text{ETH}$$

And a minimum base reward of:

$$\text{Minimum Base Reward (Penalty)} = 32 * \left(\frac{-64}{4 * \sqrt{17{,}915{,}429}}\right) = -0.121\ \text{ETH}$$

If a validator attempts to cheat the system by creating or voting for more than one block, the validator will be slashed and penalized -1 ETH immediately. They will be penalized an additional

amount of ETH in a parameter increasing proportionally to the number of slashed validators found until the stake is released after 36 days. If a coordinated attack is attempted, the attacker will risk losing the 32 ETH stake and will only gain control momentarily (Buterin, 2022) (Buterin et al., 2020).

As block rewards are now less than the PoW-based consensus mechanism, it has consequently led the Ethereum blockchain to change from an inflationary localized blockchain economy to a deflationary economy. Currently (April 2023), the deflation rate since the switch from PoW to PoS has been -0.18%, 537,959 ETH has been burned, and only 403,407 ETH has been minted (Ultrasound.money, 2023).

Summing up the consensus layer, it can be said that decentralized Proof-of-Stake blockchains are using the Proof-of-Stake consensus to solve the game theoretical “Byzantine generals’ problem” by economically incentivizing validator nodes to stay honest, as the rewards of such behavior will outweigh the risk of having their stake slashed.

4.3 Introduction to Stablecoins

The birth of Bitcoin in 2009 marked a significant development in the financial landscape, offering an alternative to traditional fiat currencies such as the US dollar. The principles of blockchain technology supporting Bitcoin represented a revolutionary breakthrough, introducing several new features through blockchain technology. However, as a medium of exchange, cryptocurrencies suffered from a significant flaw: their highly volatile nature, with prices fluctuating frequently and rapidly. To tackle this issue, stablecoins emerged as a solution designed to provide stability by fixing their value to another asset, also known as pegging. As a result of their ability to hold a stable price, stablecoins are a more practical medium of exchange than unbacked crypto-assets like Bitcoin or Ethereum.

Stablecoins come in various forms, typically pegged to fiat currencies like the US dollar or assets like gold. The peg is central to the definition of stablecoin as this determines the asset that the price of a stablecoin should represent. If a stablecoin loses its peg permanently, it can be deemed a failed stablecoin. To avoid a loss of their peg, stablecoins are designed in different ways to accommodate events that may pose a risk to their peg.

4.3.1 Types of Stablecoins

Stablecoins can have different designs and protocols that enable them to be stable relative to a legal tender currency. Based on their design and backing, Stablecoins can be classified into three main categories: asset-backed, crypto-collateralized, and algorithmic (Burke, 2023). In this sub-section, we will provide an overview of each type of stablecoin and examine some of the most notable stablecoins in each of the three categories.

4.3.1.1 Asset-Backed Stablecoins (Off-Chain Collateralization)

Off-chain asset-backed stablecoins represent the most prevalent form of stablecoins, with the three largest stablecoins by capitalization belonging to this category (Dark et al., 2022). The idea of this design is that the stablecoin issuer holds assets in reserve that are equivalent in value to the tokens in circulation. Furthermore, these assets are typically safe and highly liquid to handle potential bank runs (Dark et al., 2022). Hence, the peg is maintained by holders' ability to redeem a token for the value of the peg at any time. This type of stablecoin can be further divided into two subtypes depending on the type of asset in reserve. Fiat-backed (or tokenized) stablecoins are a subtype

where the reserve is typically kept in the same fiat currency that the stablecoin represents (Burke, 2023). The other subtype is commodity-backed stablecoins, characterized by collateralization in physical assets such as gold or oil. We shall now study the two most capitalized stablecoins in the market, which are also fiat-backed, Tether and USD Coin.

4.3.1.1.1 Tether

Tether, the stablecoin with the highest market capitalization globally, is supported by a reserve of liquid assets and is owned by iFinex Inc. This Hong Kong-registered company initially introduced it as "RealCoin" in 2014 (Frankenfield, 2023).

A Tether token is minted after an equivalent amount of fiat currency has been deposited in Tether's reserves. Tether requires a minimum deposit of 100.000 US Dollars and charges a fee of 0.1% for the exchange. The exact requirements apply for withdrawals meaning a holder must redeem 100.000 USDT and pay a fee of 0.1% of the redeemed amount (Tether, 2023).

Though Tether is the highest capitalized stablecoin, it has received significant criticism for reserve management. Tether did not undergo auditing in the first four years, creating a lack of transparency regarding the reserve's value and composition (Burke, 2023). The absence of transparency led the New York Attorney General to accuse iFinex Inc. of hiding an $850 million loss by covering it with a minimum of $700 million from the cash reserves (Burke, 2023).

In the settlement, it was revealed that Tether only had 2.9 percent of its backing in cash. Since then, Tether has improved the transparency of its reserves by uploading reserve balances, the composition of reserves, and audit reports, to its website for public display. An illustration of the most recent reserve composition is shown below:

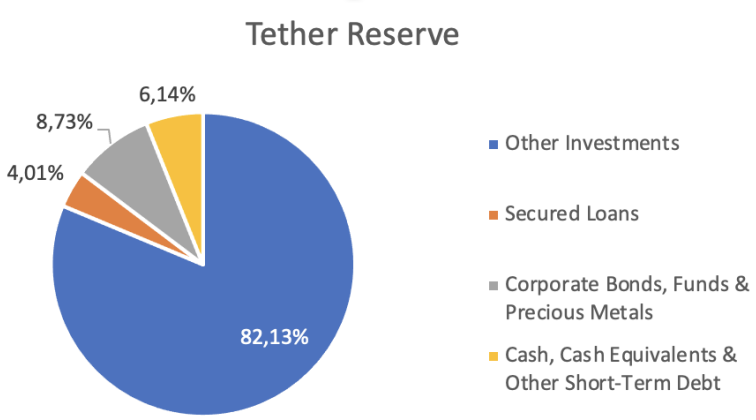


Figure 12: Tether Reserve Composition. Source: tether.com

As of December 31st, 2022, most of the reserves, specifically 82.13%, were assets denoted as "Cash & Cash Equivalents & Other Short-Term Deposits & Commercial Paper." Notably, of this reserve percentage, only 9.66% represents cash or bank deposits (Tether, 2022).

4.3.1.1.2 USD Coin

In 2021, Circle Internet Financial Ltd & Coinbase Global Inc. led a joint venture that created USD Coin, the second-largest stablecoin in 2023, by capitalization. Like Tether, USDC maintains its peg to the dollar through a reserve of assets. However, USD Coin's difference lies in its governance model, wherein Circle's strategy prioritizes compliance with regulatory standards. Notably, Circle has announced its commitment to comply with full-reserve banking regulations, with the support of federal institutions such as the US Federal Reserve and the US Treasury (Burke, 2023). Moreover, Circle safeguards its reserves by storing assets in designated accounts, which prevents any usage of reserve funds for loans or liquidity issues the company may face. As of March 2, 2023, the reserves of USDC amount to $43.2 billion, including $11.4 billion in cash and $31.9 billion in a short-dated US treasury portfolio. These reserves are held in custody at the New York Bank Mellon and are managed by BlackRock (Circle, 2023).

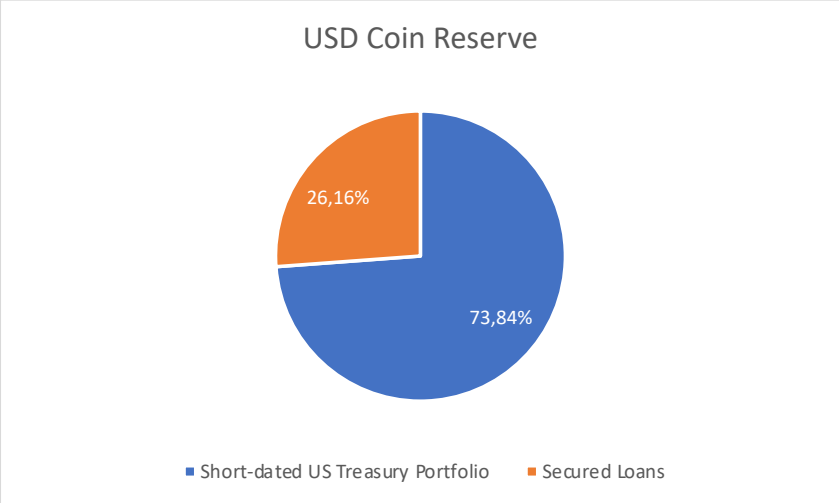


Figure 13: USD Coin Reserve. Source: Circle

4.3.1.2 Crypto-collateralized stablecoins

Crypto-collateralized stablecoins are a type of digital currency that relies on a reserve of other crypto-assets on a blockchain network. Given the highly volatile nature of these underlying assets, a crucial feature of such stablecoins is the implementation of over-collateralization to maintain the stablecoin's peg to a specific value. The over-collateralization of crypto-assets is necessary to support the stablecoin, which safeguards against potential fluctuations in the value of the underlying crypto-assets (Kahya et al., 2022). It is worth noting that crypto-collateralized stablecoins may be supported by either a single crypto-asset or multiple crypto-assets, depending on the design of the stablecoin in question. While off-chain assets may be safer collateral compared to crypto-assets, having on-chain assets in reserve can give clear advantages in terms of decentralization. This is because assets are on-chain, and reserves do not need to be governed by a company or traditional entities. This subsection will focus on the most capitalized crypto-collateralized stablecoins in circulation, DAI from MakerDAO.

4.3.1.2.1 DAI USD

The MakerDAO system is a two-coin system consisting of the stablecoin DAI and a coin to govern the DAI called MKR Token. To issue DAI, users must lock up collateral in a “Maker collateral vault”. Here, the loaner puts in crypto-collateral such as Ether and gets a loan on DAI. This collateral remains in escrow until the user returns the DAI. When the collateral is returned, the tokens are burned. The system is designed so the user will need to over-collateralize the DAI loaned with at least 150% of the value in the Maker collateral vault. This limit is known as the liquidation ratio.

If the value of the collateral in the vault drops to under 150%, the vault is automatically liquidated, and the user will pay a 13% penalty fee of the returned liquidated collateral (MakerDAO, 2023). The liquidation is done by auctioning off the collateral in the system. In this way, the system incentivizes users to constantly keep their vault over-collateralized, necessary when the assets are as volatile as crypto-assets.

To open a vault, users must pay a stability fee, a form of interest rate. The stability fee stabilizes the DAI price as a lower stability fee encourages more users to open a vault and vice versa. This fee is set by the owners of MKR tokens, who act as governors of the stablecoin. The owners of the MKR tokens also control the types of assets that can go into the Maker vaults. They are incentivized to keep the DAI continuously over-collateralized since new MKR tokens are issued to pay off any excess debt if the collateral auction and the stability fees fail to do. MKR tokens get burned through surplus auctions, where excess profits from stability fees get sold for MKR tokens.

MKR token holders are thus incentivized to create stability for the value of their tokens to grow. The DAI stablecoin is further stabilized through external arbitrageurs called "Market Maker Keepers", who will buy DAI when the price is below the peg and sells when it is over (MakerDAO, 2023). Users open Maker Vaults for two main reasons; firstly, opening a vault gives the user a more liquid asset in DAI to trade with while still holding on to their crypto-asset. Secondly, the MakerDAO system also allows leveraging a position in a crypto-asset. For example, an investor holds ETH and believes the price increase. The investor can then open a vault where he puts in the ETH and receive DAI to invest in more ETH.

The design of the MakerDAO system ensures a more decentralized system where smart contracts are encoded, the functions that autonomously handle the day-to-day management of the reserves instead of a company.

4.3.1.3 Algorithmic Stablecoins

The central aspect of algorithmic stablecoins that differentiates them from the other two types is that they are non-collateralized, meaning they have no backing of assets. Instead of an asset reserve, algorithmic stablecoins build on algorithms and smart contracts that govern the supply of tokens similarly to central banks (Burke, 2023). Practically, the number of coins is reduced if the

price goes below the peg, and supply increases if the price goes over. In this way, the supply is always managed to keep up with the demand to secure the 1:1 peg. Algorithmic stablecoins are often governed in a two-coin system, with one coin holding the peg and the other functioning as a volatility absorber (Burke, 2023). In their natural form, algorithmic stablecoins can be compared to fiat currency as none are backed by a reserve. Thus, the value and peg rely on the trust of the system, which could easily be more fragile in the case of an algorithmic stablecoin protocol compared to a central bank system of a state. In the coming section, we will study the case of TerraUSD – an algorithmic stablecoin that managed to hold its peg to the dollar for more than a year but eventually crashed.

4.3.1.3.1 TerraUSD

Terra is a protocol that runs two cryptocurrency tokens – TerraUSD and Luna. The former is designed to be a stablecoin pegged to the US dollar, while the latter is a form of governing coin with a different design and purpose compared to the MKR token of MakerDAO. The system uses arbitrage mechanisms to stabilize by trading the two tokens between each other. If the TerraUSD is above its peg, owners of Luna can buy TerraUSD with Luna tokens for 1 dollar creating arbitrage opportunities. Reversely, when TerraUSD drops below 1 dollar, the owners can exchange TerraUSD for 1 dollar worth of Luna. During this process, a percentage of the swapped coin gets burned while the coin received is minted.

By doing this, Terra automatically regulates the supply of TerraUSD to ensure it matches the demand for TerraUSD relative to the value of 1 dollar. Consequently, holders of Luna benefit from a demand for TerraUSD as the supply of Luna will diminish with a higher supply of TerraUSD. This mechanism incentivizes Luna holders to keep TerraUSD stable since increases in minted Terra will increase the value of Luna tokens (Burke, 2023).

TerraUSD and Luna run on the Terra blockchain, and the coins were designed to be used within the Terra ecosystem. The percentage kept when transferring coins is used to develop this system, which includes applications for decentralized finance.

4.3.2 Primary Use-Cases

Currently, stablecoins play a crucial role in the crypto-ecosystem by serving as a bridge between conventional currencies and crypto-assets, with over 75 percent of trades on major crypto exchanges involving stablecoins in 2022 (Dark et al., 2022). In addition to their function as a medium

of exchange within the crypto-ecosystem, stablecoins also serve as a secure store of value for cryptocurrencies. Investors in volatile cryptocurrencies can mitigate waiting times and trading fees of exchanging their cryptocurrencies for fiat currency by keeping their value on-chain in stablecoins instead (Burke, 2023).

Stablecoins are also used on so-called decentralized finance platforms such as crypto banks. These platforms can act as an intermediary between lenders and borrowers. As stablecoins are in demand in the crypto-ecosystem, holders can earn up to 12% in annual percentage yield though lending can be illegal in some areas (Burke, 2023).

Two other cases are international remittances and the use of smart contracts in transactions. Since blockchain technology allows people to make transactions with each other without a bank account stablecoins are utilized for cross-border payments and especially remittances. Here stablecoins are an alternative to companies such as Western Union for foreign workers who wire money home to their families. Blockchain technology can here cut out the fees of having an intermediary overseeing the transactions as the technology ensures trust between the trading parties.

4.3.3 Holding Stablecoins

As explained in the review of blockchain, crypto-assets such as stablecoins are stored in a digital wallet. In terms of stablecoin storage, holders generally have two options when it comes to the digital wallet. First, they can generate their digital wallet, where only the owner of the wallet knows the secret key that enables sending transactions. For an individual who has yet to gain advanced knowledge of blockchain technology, crypto wallets can be challenging to engage with regarding transactions and security.

Another way of storing stablecoins is through a centralized crypto exchange. This implies that holders have their wallets with the exchange. As for convenience, holding stablecoin assets on exchanges is a more user-friendly and relatively secure way of interacting with the blockchain. The deciding difference is that the user does not directly control the interaction with their assets. Instead, when a user sends a transaction, it will be a request to the exchange to credit the account the transactional amount and debit the receiver. The transaction will be carried out by the exchange

interacting with the blockchain protocol, as only the exchange will know the secret key to the corresponding account.

4.3.4 Acquiring and Withdrawing Stablecoins

Stablecoins have long been a stable intermediary for investors looking to liquidate an investment in a more unstable cryptocurrency. In such a case, swapping a volatile crypto-currency to a stable-coin at the marked spot rate can be executed with the counterparty being another blockchain user on a decentralized exchange. Here smart contracts will serve as autonomous intermediaries to reduce counterparty risk. Centralized exchanges are a more traditional way of executing a swap, where the exchange will serve as the counterparty. Buying Stablecoins, or any other cryptocurrency using fiat currencies, is usually only available on centralized exchanges. Buying stablecoins on a centralized exchange is nearly identical to exchanging currency in a bank. What can be costly is withdrawing stablecoins to fiat currency (Dark et al., 2022). Below is a table of Tether and USD Coin's withdrawal fees at some of the largest exchanges:

Exchange	Tether (in USDT)	USD Coin (in USDC)
Coinbase		
Withdrawal Fee	**1%**	**1%**
Minimum Withdrawal	**<0.1**	**<0.1**
Binance		
Withdrawal Fee	**7**	**7**
Minimum Withdrawal	**50**	**50**
Kraken		
Withdrawal Fee	**3.55**	**3.55**
Minimum Withdrawal (inc. Fee)	**7.11**	**7.11**

Figure 14: Withdrawal Fees and Minimum Withdrawal. Source: Coinbase (n.d.), Binance (n.d.) & Kraken (n.d.)

4.3.5 Stablecoin market

Along with the stablecoins mentioned in the previous section, more than a thousand distinct stablecoins are in circulation. Since the introduction of the first stablecoin, the market of stablecoins has been more or less growing ever since. Since 2017, Tether has been the superior coin measured in market capitalization, followed by the two other asset-backed stablecoins, USD Coin and Binance USD. The capitalization of a coin is the number of tokens on issue times the market value in a fiat currency. Since stablecoins with a peg to the dollar typically are worth 1 dollar, market capitalization is an excellent measure of the popularity of each coin.

The developments of the total market capitalization of the ten largest stablecoins reveal stablecoin's significant gain in popularity. From January 2020 to June 2022, the total market capitalization has grown by over 2,700 percent. Though the total market capitalization has grown significantly on average over the past years, it took a notable hit at the start of 2022. This drop is in line with the general fall in prices of non-backed crypto-currencies such as Bitcoin during the start of 2022, again underlining that the primary use of stablecoins is within the crypto-ecosystem.

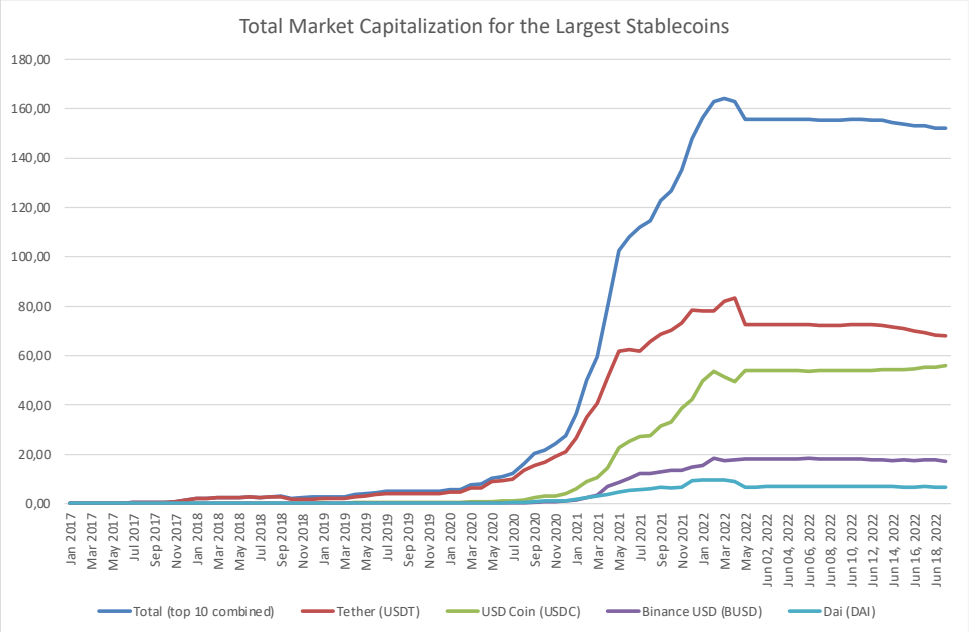


Figure 15: Total Market Capitalization for the Largest Stablecoins Source: Statista (2023)

Tether has been the largest capitalized stablecoin on the market, with capitalization at times accounting for more than half of the total capitalization. Since 2021, USDC Coin has also gained significant market share and accounts for more than a third of the total capitalization in the market in June 2022. As of May 2022, Tether, USD Coin, Binance USD, and DAI account for 97.2% of the total market capitalization (CoinCapMarket, 2023). Of these four tokens, only DAI is to only one not backed by conventional assets like fiat currencies hinting towards a preference for asset-backed stablecoins. This can hint towards a preference for stablecoins backed by a reserve of liquid assets.

5 Analysis

5.1 Financial Factors

Like most assets, holding stablecoins comes with risks of losing value. In the first part of the analysis, we shall investigate the risks of holding stablecoins from a financial point of view. We will first study the stability of the stablecoins, i.e., how well a stablecoin manages to hold its peg, and which factors will determine potential instability. The analysis will be conducted through a literature review on stablecoins stability to get a clear nuanced comprehension of the subject. After the review, we will look at how a stablecoin may lose its peg permanently, which ultimately determines if a token has a value, and finally consider past stablecoin failures.

5.1.1 Stability Analysis

The most significant feature of a stablecoin is its ability to remain stable relative to its peg. Here price stability is critical for a stablecoin to be a store of value. By exploring the historical prices of the four largest ERC-20 stablecoins over the past five years, we will see that the mean of the prices is very close to 1 dollar. However, it is also evident that some volatility does exist and that stablecoins cannot constantly hold its dollar peg.

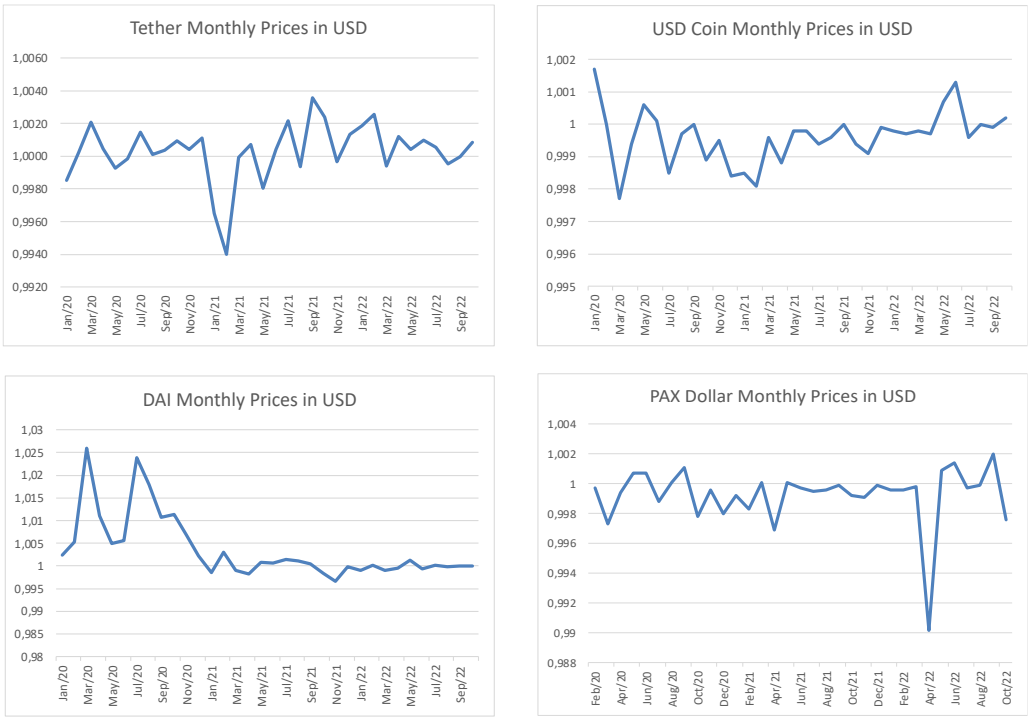


Figure 16: Developments in Prices. Source: Statista (2022)

The variance of prices is different from coin to coin. This may indicate that stablecoins are less stable than their name suggests. To assess the stability of stablecoins, we will now do a literature review of previous findings regarding the general stability and risks to the stability. Here, we will dive into how price-volatile stablecoins are and what may influence volatility. In this review, we have chosen to split the field of stablecoin stability into smaller topics, where we will go over some of the most significant contributions within each topic. The scientific field of stablecoin stability is relatively new, and thus different methodologies have been applied to identify instability and its reasons. Hence, each review will contain information on the methodology applied and the study's conclusions.

5.1.1.1 How Stable Are Stablecoins?

Looking at historical prices, it is easy to conclude that stablecoins are unstable to some degree. But what about the stability in relative terms? Is the volatility of prices so insignificant that it is still fair to conclude that stablecoins are stable? Baur & Hoang (2021) research this by analyzing the stability of the top six largest stablecoins measured by capitalization at the end of 2019, along with the gold-backed stablecoin DGX and the EUR-pegged stablecoin EURS. The sample consists of 5-minute intraday prices of all eight stablecoins from October 31, 2018, until December 26, 2019. Intraday prices are the prices of stablecoin observed every fifth minute 24/7 in the sample period. The study defines two types of stability: absolute stability and relative stability. The former type of stability is defined as zero variance of returns allowing for insignificant variations, while the latter form of stability is defined as a lower variation in returns compared to other assets. In their study, Baur & Hoang (2021) use Bitcoin, fiat currencies, stocks, and gold as benchmarks for relative stability.

When testing for absolute stability Baur & Hoang (2021) use a chi-square test to test for zero variation of return for each stablecoin. Formally:

$$H_0: \sigma_{sc} = 0$$

In the test they allow for 0.1% daily standard deviation to be able to calculate test statistics. Hence, the null hypothesis is more accurately:

$$H_0: \sigma_{sc} \leq \sigma_0 = 0.1\%$$

With the test statistic given as:

$$T = \frac{(N-1)*\sigma_{SC}^2}{\sigma_0^2} \sim \chi_{N-1}^2,$$

where N is the number of observations.

The results of the test show that the null hypothesis can be rejected on a 1% significance level for all stablecoins in the sample. This implies that none of the stablecoins in the sample can be categorized as absolute stable. The results of the test are reported below:

	USDT	USDC	TUSD	PAX	GUSD	SAI
Test statistics	7,720.10***	7,418.79***	5,578.44***	5,414.17***	40,599.44***	83,171.32***
N	421	421	421	421	421	421
p-value	0.00	0.00	0.00	0.00	0.00	0.00

Figure 17: Test Statistics the Chi-Sqaured Test. Source: Baur & Hoang (2021)

A GARCH-test is also proposed as an alternative test. Here, the results are in line with the chi-square test.

Concluding that stablecoins do not show indications of being stable in absolute terms, Baur & Hoang (2021) move on to test for relative stability, meaning that the stablecoins in the sample cannot show a higher standard deviation than the benchmark assets. The test is conducted with an F-test with the null hypothesis:

$$H_0: \sigma_{sc} \leq \sigma_{benchmark}$$

They find that all stablecoins have higher variance than fiat currencies[2] but in general, have a lower variance than Bitcoin. Moreover, Baur & Hoang (2021) also discover that the stablecoins with the highest market capitalization in the sample have lower volatility than gold and stocks.

[2] Fiat currencies are represented by the Euro (EUR) and the dollar index (USDX). The indices are measurements of the value of a currency relative to a basket of other major currencies.

Establishing that stablecoins may show signs of instability, Baur & Hoang (2021) move on to investigate potential sources of stablecoin instability by testing the correlation of return and volatility with other assets like Bitcoin. Volatility is estimated using a T-GARCH(1) model with daily returns. Tests of correlation between returns put evidence towards an interconnection with Bitcoin. At the five-minute frequency, all stablecoin returns exhibit a relatively high correlation with Bitcoin returns. Going from five-minute frequency return to hourly or daily returns, the correlation coefficients with Bitcoin get weaker for all stablecoins but Tether. The correlation coefficient increases from 0.10 to 0.33 when increasing the frequency from 5 minutes to 24 hours. The volatility of many stablecoins, including USD Coin and Tether, is also significantly correlated with Bitcoin volatility. Because of this, Baur & Hoang (2021) give further evidence to the conclusion that stablecoins are not stable, since they provide the argument that a stable asset should not co-move with an unstable and volatile asset such as Bitcoin.

5.1.1.2 The impact of stablecoins design on stability

The research conducted by Bauer & Hoang (2021) is noteworthy for stablecoin holders, as the maintenance of price stability is arguably the most important characteristic of this form of crypto-assets. But what if one were to hold a stablecoin regardless of the lack of absolute stability? Are some designs of stablecoins better to accommodate stability? Jarno and Kołodziejczyk (2021) test if the design of stablecoins influences the ability to hold a stable peg. The dataset used in the study contains daily prices of 20 different stablecoins from the day each coin got introduced until September 25, 2019. For the analysis, the stablecoins in the sample are split into three different categories similar to the division made in the introduction earlier in the paper: tokenized funds, collateralized (on-chain), and algorithmic. 'Tokenised funds' in the sample include fiat backed stablecoins like Tether and USD coin. In contrast, the type 'collateralized funds' is equivalent to what we previously introduced as crypto-collateralized funds, including DAI.

The volatility measure chosen is the standard deviation of daily logarithmic rates of return corrected for autocorrelation based on the estimate of the autocorrelation function (ACF)[3]. Formally stated:

[3] ACF defines how the correlation between any two values of the times series changes as their separation changes (Box, Jenkins & Reinsel, 1994).

$$s^2 = \frac{n_{eff}}{n(n_{eff}-1)} \sum_{t=1}^{n} (i_t - \bar{\imath})^2,$$

Where n is a number of observations for a given stablecoin and n_{eff} is an effective number of observations based on the estimate of ACF-function[4]. i_t is the logarithmic rate of return on day t:

$$i_t = \log\left(\frac{p_t}{p_{t-1}}\right)$$

Name	Peg	Volatility (in p.p.)	Type
Paxos	USD	0.457619	tokenised funds
USD Coin	USD	0.552184	tokenised funds
StableUSD (Stably)	USD	0.640032	tokenised funds
TrueUSD	USD	0.770574	tokenised funds
Gemini Dollar	USD	1.194509	tokenised funds
Dai	USD	1.48214	collateralised (on-chain)
Stasis Euro	EUR	1.510869	tokenised funds
Tether	USD	2.165575	tokenised funds
Terra	SDR	3.956304	algorithmic
Aurora	USD	6.762596	collateralised (on-chain)
PHI	USD	7.334355	collateralised (on-chain)
BitShares	USD	7.444987	collateralised (on-chain)
NuBits	USD	8.58101	algorithmic
Moneytoken (IMT)	USD	9.119281	collateralised (on-chain)
Steem	USD	10.03096	algorithmic
BridgeCoin (SweetBridge)	USD	10.41627	collateralised (off-chain)
MinexCoin	USD	10.49871	collateralised (on-chain)
Alchemint	USD	11.82065	collateralised (on-chain)
White Standard	USD	15.04977	tokenised funds
bitUSD	USD	16.01225	collateralised (on-chain)

Figure 18: Ranking of the Stablecoin based on volatility. Source: Jarno & Kolodziejczyk (2021)

The results of the study show that not all stablecoins in the sample show the same volatility as the stablecoin with the lowest volatility (Paxos) has a daily standard deviation of return of 0.4576 in percentage points, while the one with the highest (bitUSD) has a daily volatility of 16.0123 percentage points. Regarding the type of stablecoin, the five best-performing stablecoins measured on daily volatility all belong to the 'tokenized funds' type. Dai is the best-performing stablecoin that is not fiat or asset-backed, with Terra being the best-performing algorithmic stablecoin. ACF estimates show that the average volatility of tokenized funds is lower than the other groups.

[4] $\widehat{n_{eff}} = \frac{n-2n_c-1+n_c(n_c+1)/n}{1+2\sum_{k=1}^{n_c} r_k^2}$, where n_c is the maximum lag and r_k are elements of autocorrelation function estimate.

Standard deviations of the algorithmic and collateralized stablecoins are close to each other, with the volatility of algorithmic stablecoin being a little lower:

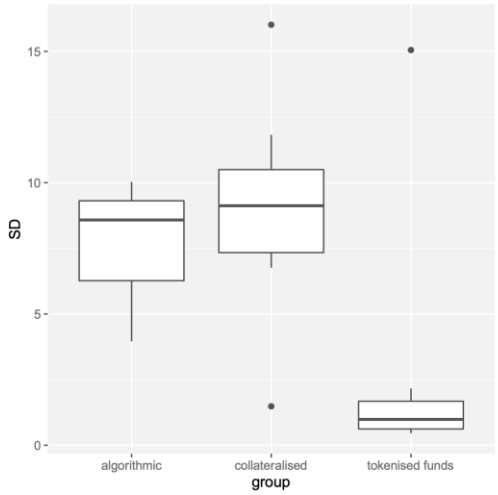


Figure 19: Standard Deviation Boxplot Based on ACF-Estimates. Source: Jarno and Kolodziejczyk (2021)

While the individual volatilities indicate that some stablecoins are more volatile than others, a formal test is needed to test for differences in standard deviation for the three groups. Therefore, a Kruskal-Wallis H and bootstrap F-statistic are calculated to test the differences for the groups. The Kruskal-Wallis test indicates that at least two of the three groups do not come from the same distribution regarding the measured volatility. Moreover, results of the bootstrap F-test also evince that the mean of the standard deviation of daily returns of at least two groups are different. Post-hoc tests[5] are then conducted to find significant differences in the distribution of the standard deviation of returns for the three groups.

The results of the tests are reported below:

Test	Tested Groups	Value of the Test Statistic	*p*-Value
Pairwise Wilcoxon–Mann–Whitney U test with Holm correction	collateralised—algorithmic	-	0.600
	tokenised funds—algorithmic	-	0.170
	tokenised funds—collateralised	-	0.033
Dunn test (*p*-values adjusted with Benjamini–Hochberg method)	collateralised—algorithmic	−0.3662335	0.714
	tokenised funds—algorithmic	1.5500663	0.182
	tokenised funds—collateralised	2.6621153	0.023

Figure 20: Results of the Post Hoc-Tests. Source: Jarno and Kolodziejczyk (2021)

[5] Tests are Pairwise Wilcoxon-Mann-Whitney U test with Holm correction and Dunn test. Authors do not provide a formal description of the tests, thus we shall refrain from paraphrasing them from other sources.

A non-parametric multiple contrast test is then conducted[6]. The results of the test imply that we can conclude two things. Tokenized funds generally have lower values of standard deviation compared to collateralized stablecoins. Moreover, it is concluded that tokenized funds tend to have lower values of standard deviation of daily returns compared to both collateralized and algorithmic stablecoins. Because of this, Jarno and Kołodziejczyk (2021) find that different designs of stablecoins do not deliver equally on the promise of stability in price, with stablecoins backed by liquid assets being superior.

5.1.1.3 Bitcoin's influence on Stability

As revealed earlier, stablecoins play a significant role in the trading of Bitcoin. The interconnectivity of stablecoins and Bitcoin raises a natural question of whether the price volatility of Bitcoins affects the stability of stablecoins. Grobys et al. (2021) investigate the volatility processes of stablecoins and how they may be interdependent with the volatility of Bitcoin. The data used in the analysis consists of prices of Bitcoin and the five biggest stablecoins measured by market capitalization on November 22, 2020. The stablecoins are Tether, USD Coin, DAI, Binance USD, and TrueUSD, where all available daily prices have been collected for each stablecoin. The study can roughly be split into two parts: first, an investigation of the volatility processes of stablecoins, and second, an analysis of stablecoin's interdependencies with Bitcoins volatility. To model the probability density functions of the stablecoins, Grobys et al. (2021) compute annualized realized daily volatilities for each stablecoin in the following way[7]:

$$\sigma_{i,t} = \sqrt{T}\sqrt{\left(\ln\left(\frac{HIGH_{i,t}}{CLOSE_{i,t}}\right) * \ln\left(\frac{HIGH_{i,t}}{OPEN_{i,t}}\right) + \ln\left(\frac{LOW_{i,t}}{CLOSE_{i,t}}\right) * \ln\left(\frac{LOW_{i,t}}{OPEN_{i,t}}\right)\right)},$$

where $\sigma_{i,t}$ is the annualized volatility of cryptocurrency i. $HIGH_{i,t}$ and $LOW_{i,t}$ denote respectively the highest and lowest price of cryptocurrency i on day t. $OPEN_{i,t}$ and $CLOSE_{i,t}$ denote the

[6] The specifications of the test are tedious and space consuming. Details about the test can be found in the study. DOI: 10.3390/jrfm14020042

[7] The volatility estimator based of Rogers and Satchell (1991). Prices of volatile assets are often described as a Brownian motion with drift $\sigma B_t + ct$ with constants σ and c being unknown. Using the estimator proposed we can obtain an unbiased estimate of σ without knowing the drift, c.

opening and closing price of cryptocurrency i on day t. T is set to 365 since all cryptocurrencies in the data are traded all year 24/7.

Unsurprisingly, Bitcoin is found to exhibit the highest average volatility of 53%, while the stablecoins are in the range between 17% and 27%. Furthermore, outliers are observed for all cryptocurrencies as all have significantly high kurtosis values relative to a thin-tailed normal distribution, with values ranging from 15.5 to 175.4. Taking this into consideration, all cryptocurrencies in the dataset have significantly fat tails.

Grobys et al. (2021) then investigate the volatility processes of the six cryptocurrencies by modeling the realized volatility using power laws. The method used is too complicated and tedious to be within this project's scope. Nevertheless, the power laws used are:

$$P(X > x) = p(x) = Cx^{-a},$$

where $C = (\alpha - 1)x_{MIN}^{\alpha-1}$ and $x \in \{\mathbb{R}_+ \,|x_{MIN} \leq x < \infty\}$ with x_{MIN} being the minimum value of realized volatility that bends the power law and $a \in \{\mathbb{R}_+ \,|\alpha > 1\}$ is the magnitude of the tail exponent.

Through this modeling, Grobys et al. (2021) conclude that the mean of Bitcoin's volatility is stable. This implies that if the sample size is large enough, the mean of realized volatility will converge toward its true value. This means that the mean of Bitcoin's realized volatility is informative. However, this is not the case for stablecoins, where it is found that the true mean of the realized volatilities is impossible to observe when the sample size is finite. Because of this, Grobys et al. (2021) conclude that *"... Bitcoin volatility is stable in the statistical sense that a theoretical variance exists*" (Grobys et al., 2021, p. 211). On the other hand, in terms of stablecoins, it is concluded that "…the volatilities of stablecoins are statistically unstable due to infinite theoretical variances" (Grobys et al., 2021, p. 211).

Next, Grobys et al. (2021) test if the volatility of Bitcoin has a spill-over effect on the stablecoins. To test whether the volatilities of Bitcoin and the stablecoins show contemporaneous effects, the following OLS model is estimated:

$$btc_t = c + b_1 btc_{t-1} + \sum_{i=1}^{5} h_i stablecoin_{i,t} + \sum_{i=1}^{5} s_i stablecoin_{i,t-1} + u_t,$$

,

where btc_t is the natural logarithm to the realized annualized daily volatility of bitcoin in time t and $stablecoin_{i,t}$ is the natural logarithm to realized annualized daily volatility of stablecoin i in time t.

To test if the stablecoins and Bitcoin exhibit contemporaneous effects a Wald test is conducted. Formally stated:

$$H\_0: h_1 = h_2 = \cdots = h_5 = 0$$
$$H\_1: at\ least\ one\ h_i \neq 0, i = \{1, 2, \dots, 5\}.$$

The test returns a p-value of 0, which is why it is concluded that the volatility of stablecoins and Bitcoin co-moves simultaneously.

Same test is also done for the lagged parameters:

$$H_0: s_1 = s_2 = \cdots = s_5 = 0$$
$$H_1: at\ least\ one\ s_i \neq 0, i = \{1, 2, \dots, 5\}.$$

Here, the test statistic does not exceed the 95% critical value and it is hence concluded that stablecoin volatility does not have any spill-over effects on Bitcoin volatility.

Grobys et al. (2021) then conclude the study by testing if Bitcoin volatility has spill-over effects on stablecoin volatility by estimating a system of regressions using the Seemingly Unrelated Regression estimation technique. The volatility of each stablecoin is regressed on its lagged value, and the volatility of Bitcoin in the same period and with one lagged:

$$usdt_t = a_{1,1}usdt_{t-1} + a_{1,2}\, btc_t + a_{1,3}\, btc_{t-1} + e_{1,t}$$
$$usdc_t = a_{2,1}usdc_{t-1} + a_{2,2}btc_t + a_{2,3}btc_{t-1} + e_{2,t}$$
$$dai_t = a_{3,1}dai_{t-1} + a_{3,2}btc_t + a_{3,3}btc_{t-1} + e_{3,t}$$
$$busd_t = a_{4,1}busd_{t-1} + a_{4,2}btc_t + a_{4,3}btc_{t-1} + e_{4,t}$$
$$tusd_t = a_{5,1}tusd_{t-1} + a_{5,2}btc_t + a_{5,3}btc_{t-1} + e_{5,t}$$

Regression estimates show that all parameters for Bitcoin volatility in the same period ($a_{i,2}, i = \{1, 2, \dots, 5\}$) are significant on a 1% level and ranges between 0,42 and 0,50 for the five stablecoins. Intuitively, when Bitcoin volatility increases by 1%, the volatility of Tether increases on average by 0.50% contemporaneously. Considering the previous tests, this is not a shocking result which is why it is more interesting to consider the parameters for the lagged bitcoin volatility. Here, all estimates are negative, with only the parameter for DAI being insignificant. To test if the Bitcoin volatility is Granger-causal for stablecoin volatility, the following test is conducted:

$$H_0: a_{1,3} = a_{2,3} = \cdots = a_{5,3} = 0$$
$$H_1: at\ least\ one\ a_{i,3} \neq 0, i = \{1, 2, \dots, 5\}\ .$$

Again, using the Wald test statistic, it is concluded that the test statistic obtained of 176.14 is larger than the critical value of 11.07 and that Bitcoin volatility has a Granger-causal effect on the volatility of the stablecoins included in the test. This implies that if Bitcoin volatility increases, the volatility of stablecoin will, on average, decrease the next day and vice versa.

5.1.1.4 The Impact of Systematic Risk on Stability

Non-diversifiable risk is always a concern when holding assets that can be volatile in price or value. A prime example of this is the stock market during economic recessions, where infamous events like the Wall Street Crash of 1929 or the financial crisis of 2007 saw the stock market drop significantly in value, causing significant increases in price volatility (Jeger et al., 2021). In terms of cryptocurrencies, Bitcoin has shown great exposure to global economic events like the emergence of the COVID-19 pandemic led to price drops of 50% (Jeger et al., 2021). Having these

effects in mind, it should be reasonable to question whether stablecoins are able to hold their peg during times of economic crisis. Jeger, Rodrigues, Scheid & Stiller (2021) set out to analyze the implications of the COVID-19 pandemic on stablecoin stability. The dataset analyzed consists of daily closing prices, closing market capitalization, and trading volume of Tether, USD Coin, Digix Gold, Paxos Gold, DAI, and Synthetix USD in the period November 19, 2019, to May 1, 2020. For the analysis, Jeger et al. (2021) first define the volatility of stablecoins in the following way:

Let $X_1, \dots, X_T$ be a discrete time series where T is the number of prices for a stablecoin. The logarithmic returns of the stablecoin r_t is: $r_t = lnX_t - lnX_{t-1}$ where $1 < t \leq T$. Here Jeger et al. (2021) define the mean log-return at time $t \leq T$ for period length, n, smaller or equal to T as:

$$\mu_t = \frac{1}{n} \sum_{i=t-n+1}^{t} r_t$$

And the volatility of the time series is then defined as:

$$\sigma_t = \sqrt{\frac{1}{n-1} \sum_{i=t-n+1}^{t} (r_t - \mu_t)^2}$$

Jeger et al. (2021) identify that the prementioned volatility estimator has some weaknesses when it comes to explaining short-term changes in volatility. An Exponentially Weighted Moving Average (EWMA) estimator is chosen instead to accommodate these changes in volatility:

$$\sigma_{t,\lambda} = \sqrt{(1-\lambda) r_{t-1}^2 + \lambda \sigma_{t-1,\lambda}^2},$$

where λ is an arbitrarily chosen decay factor set to 0.94 and r_t is the log returns. With this estimator recent events gets a higher weight and disappears exponentially over time.
Moreover, Jeger et al. (2021) as measure for stability introduces a stablecoin exchange rate (SX):

$$X_t = \frac{S_t}{P_t}$$

Here S_t is the value of the asset at time t and P_t is the value of the peg at time t. The interpretation of the measurement is intuitive – if the rate drops below 1, holders of fiat-backed stablecoin are incentivized to redeem the token since they can profit from redeeming and then repurchase the stablecoin on an exchange. Thus, the SX-rate represents the rate at which stablecoins can be redeemed. For instability measurement, the EWMA estimator is applied to the logged returns of the SX-rate (SX Rate Daily Log-return EWMA Volatility).

With this methodology, Jeger et al. (2021) find that with 7-day averages of SX-rates, Tether and USD Coins peg is maintained within 1% of their peg during the sample period, while the other stablecoins were off by multiple percentage points. Jeger et al. (2021) mark March 12, 2020, as the day the stock market crashed and compare the rates from before and after. Interestingly, DAI and the gold-pegged stablecoins, Digix Gold and Paxos Gold, generally have 7-day average SX-rates below 1 before and above 1 after the crash. Synthetix USD is almost exclusively below 1 in the sample period.

Furthermore, excluding USD Coin, a significant jump in SX Rate Daily Log-return EWMA volatility is observed for all stablecoins. It is assumed that the increase in volatility for DAI is due to the design because of the high number of automatic liquidations due to significant drops in the value of the crypto-collateral. Tether has the highest relative volatility increase, mainly because of the low volatility before the crash. Synthetix USD has the highest absolute increase in volatility of nearly 30%. The two gold-backed saw relatively low increases in volatility after the market crash but, in general, were significantly more volatile than their fiat-backed counterparts. The analysis concludes that the two fiat-backed stablecoins, Tether and USD Coin, were the best-performing stablecoins during the pandemic, where both gained popularity and kept stability. Hence it is concluded that in times of economic instability, off-chain backed stablecoins are superior to on-chain collateralized stablecoins.

5.1.1.5 The Interconnection of Stability

Grobys et al. (2021) conclude that some spill-over effects exist between Bitcoin volatility and the volatility of stablecoins, pointing toward an interconnection. If Bitcoin volatility can affect stablecoins, what about the effects of volatility between the stablecoins? Can the volatility of one stablecoin affect another? Tanh, Hong, Pham, Cong & Anh (2022) study exactly this question. The dataset analyzed is based on daily prices of Tether, USD Coin, Paxos Standard, TrueUSD, and DAI from November 23, 2019, to April 1, 2021. Tanh et al. (2022) use two measures for stability. The first measure (measure 1) is the deviation of the stablecoin's closing price compared to the nominal value of the pegged asset:

$$M1\_i_t = ClosePrice_t - 1$$

The second measure (measure 2) is a realized volatility measure:

$$M2\_i_t = \sqrt{\frac{(\ln High_t - \ln Low_t)^2}{4\ln 2}},$$

where $High_t$ and Low_t represents respectively the highest price and lowest price of stablecoin i on day t.

Applying both measures to the daily prices of the five stablecoins show moderate stability with episodes of significant deviations from nominal price and high price volatility. Measure 1 exposes DAI to have the highest range of deviation from the nominal value, with the highest price being 9% higher than the nominal price and the lowest price 3.5% under the nominal value. Taking the average $M2\_i_t$ of all the stablecoins also reveal DAI to have the highest realized volatility on average hinting that the DAI value may be more unstable compared to the other stablecoins in the sample. The values of the two measurements are also being tested for correlation. Here the $M1\_Tehter$ is negatively correlated to all other values of $M1$ while the other stablecoins are positively correlated to each other. For the second measure all stablecoins are positively correlated meaning that the volatilities of the stablecoins are positively related. These relationships are investigated further through a vector autoregressive model (VAR) to estimate the impulse responses of the stablecoins stability measures. The VAR(p) model is:

$$Y_t = \sum_{i=1}^{p} A_i Y_{t-i} + \epsilon_t (1),$$

where the model is run for both measure 1 and 2. A contains the coefficient matrix and Y_t is the vector including all the variables where $M2$ for Bitcoin is added in the regressions.
The vector Y_t is:

$$\begin{pmatrix} BitcoinMeasure(2)_t \\ Tetherstabilitymeasure_t \\ USDcoinstabilitymeasure_t \\ TrueUSDstabilitymeasure \\ PaxosStandardstabilitymeasure_t \\ DAIstabilitymeasure_t \end{pmatrix}$$

Lag length is set to 5 based on the Akaike Information Criterion, the Schwarz Criterion, the Hannan Quinn Criterion, and sequential likelihood-ratio test statistic.

Impulse responses of the VAR-model for measure 1 reveal that increases in $M1\_Tether$ decreases the $M1$ for the other stablecoins hinting that investors may exchange their Tether to other stablecoins when the price is above the peg. Reversely, when the $M1$ of USD Coin goes up, the $M1$ of all the other smaller capitalized stablecoins (including DAI) increases as well. For the smaller-cap stablecoins no significant evidence is found that changes in the $M1$ drives the the $M1$ of any other stablecoin.

The measure 2 model impulse responses show that an increase in Tether market price volatility raises the market price volatility significantly for every other stablecoin in the sample. The market price volatility of USD Coin is also observed to be driving the market price volatility of the smaller capitalized stablecoins. However, the reverse effect is insignificant for the smaller capitalized stablecoins. This again points to investors exchanging their Tether when the market price fluctuates for smaller capitalization stablecoins.

5.1.1.6 Discussion of the Literature Review

While this review gives insights into the behavior of stablecoin stability and price volatility, we shall not give any final verdict on the exact behavior. Regardless of the joint consensus that the stability of stablecoins has flaws, several issues arise if one should define stablecoin stability based

on this review. First, the five studies included are only a sample of the total number of contributions within the field. Because of this, studies that may conflict with the findings included in this review may have been overlooked. Including more studies could also have given further insights into the parameters causing instability.

Another area for improvement is the time of the sample data. Though all studies have been published within the past three years, the study with the latest sample data had its last observation in April 2021. This can be a problem as we can observe significant changes in volatility by looking at changes in historical prices from 2021 and onwards. This change is not appropriately captured in the review, which is why new studies may distort our conclusions. Since the field of study is relatively new, no methodology paradigm regarding the measurement of stablecoin stability is yet in place. Hence, we cannot disclose whether some of the studies are failing when measuring stability. With different measurement approaches, we cannot tell if one method is superior to the others and how they may have limitations in different contexts.

5.1.1.7 Main Findings of the Literature Review

In this literature review, we have reviewed some of the most significant findings of stablecoin stability available within the field of study. The review has focused on five studies that each contribute to the features of stability and price volatility of stablecoins. All five studies contribute different methodologies in measuring the price volatility of stablecoins. Datasets of the four are relatively aligned regarding sample dates spanning from the introduction of Tether in 2015 to April 2021. Over 20 different stablecoins are represented in the review, with the larger capitalized stablecoins Tether, USD Coin, and Dai (SAI) represented in all four studies. While the methodology and purpose of contribution to the field of study differ among the five, the individual findings are not in serious conflict. Because of this, we can extract some good insights about the price volatility of stablecoins:

- The most obvious insight is that stablecoins cannot hold their peg at all times completely. Variations of price returns exist; hence, no stablecoin can be categorized as absolute stable (Baur & Hoang, 2021) (Tanh et al., 2022).
- In relative terms, stablecoins also fail to be stable when compared with fiat currency indices as a benchmark. Promising for stablecoins is that it found to be less volatile than Bitcoin

and stocks on a daily basis which gives a foundation to label stablecoins as relatively stable but with underlying factors that can cause instability (Baur & Hoang, 2021).

- One of these factors may be the design of the stablecoin as some categories of stablecoins have shown significantly less volatility than others. Regarding stability relative to design, Jarno and Kołodziejczyk (2021) find that off-chain backed stablecoins such as Tether and USD Coin are best at providing stability.
- Based on the events of the COVID-19 pandemic, we can also assume that during times of economic crisis with fluctuations in the stock and crypto market, off-chain backed stablecoins are also superior to other types of stablecoins in terms of stability but that stablecoins, in general, saw an increase in volatility (Jeger et al., 2021).
- The fluctuations in Bitcoin prices also influence the stability of stablecoins (Tanh et al., 2022) (Grobys et al., 2021) (Baur & Hoang, 2021) (Jeger et al., 2021). Grobys et al. (2021) find Granger-causality between the volatility of Bitcoin and stablecoins, meaning that an increase (decrease) in the volatility of Bitcoin has negative (positive) spillover effects on stablecoin volatility.
- Bitcoins are not the only crypto-asset that can influence the stability of stablecoins, as Tanh et al. (2022) find that the stability of larger capitalized stablecoins (Tether and USD Coin) drives the stability of lower capitalized stablecoins.

5.1.2 The Risk of Default

Stablecoin are held to store value and not to yield a return, thus we can assume that they only have a value for the holder if the token can keep its peg. Due to this assumption, stablecoins can roughly only take two values in the long run – either the value of one token is equivalent to the value of the pegged asset, or it is worth nothing. Because the value can take this binary form, stablecoins can fail, meaning that the holder of stablecoins can lose 100% of the value in the position. We will now study two mechanisms that can make a stablecoin lose its peg.

5.1.2.1 Bank Runs

When studying stablecoin a serious risk is the risk of a stable losing its peg permanently. In such a case the crypto-currency can end up being worth close to nothing. For asset-backed stablecoins the most typical way to lose the peg is runs on the reserve. In the world of banking, there is a phenomenon where bank clients become concerned about the safety of their deposits, leading them to withdraw their funds. This can pose a risk to the bank, as it may not have enough reserves to

accommodate the large volume of withdrawals, resulting in bankruptcy. Such an event is known as a bank run (Diamond & Dybvig, 1983). An analogy can be made to stablecoins backed by a reserve. Doubts about an issuer's ability to redeem all tokens in circulation may cause stablecoin holders to redeem their tokens, potentially collapsing the stablecoin's value if the issuer cannot accommodate all redemption requests. Such events can be sparked if holders get signals that the reserve does not have sufficient assets or that it is too illiquid to accommodate mass redemptions.

5.1.2.2 The TerraLuna-crash and Risk of Permanent De-pegging of Algorithmic Stablecoins

On May 7th, 2022, the price of Terra lost its peg to the US dollar making the market capitalization of TerraUSD plummet from 18 billion US Dollars to under 100 million US Dollars within a month (coinmarketcap, n.d.). The crash has been deemed as one of the worst events in the history of stablecoins and may be a testimony to why investors should be cautious when getting into stablecoin trading. As of now it remains unclear whether it was an organized attack or a mass selling by individuals that caused the token to ultimately lose it peg (Burke, 2023).

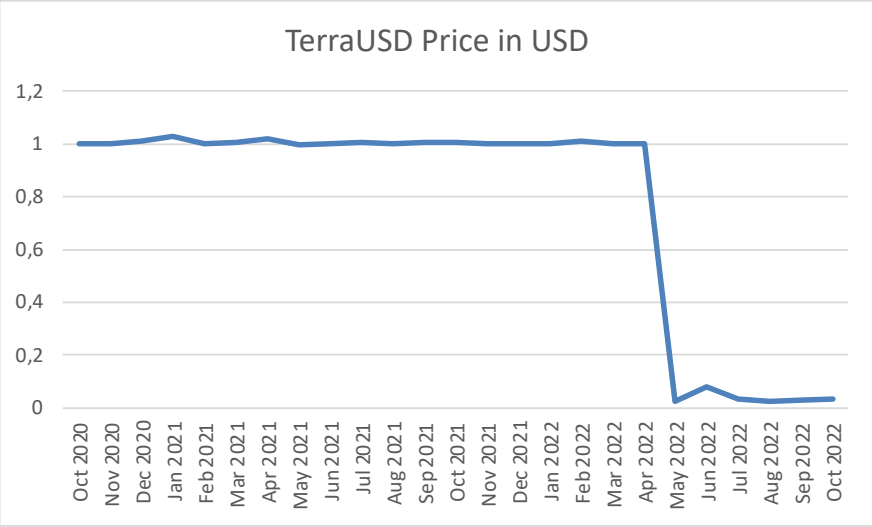


Figure 21: Price Developments of TerraUSD. Source: Statista (2023)

Many had argued before the crash that the design and protocols of the token were imperfect. A common criticism is that algorithmic stablecoins rely on arbitrage as a stabilizer which historically has been unreliable and fragile (Burke, 2023). In addition, J.P. Koning (2021) argues that algorithmic stablecoins have a circular relationship between two agents with conflicting interests that can cause permanent de-pegging.

The relationship can be described by this example. Roughly for algorithmic stablecoins we can identify the holders as two types of agents. First are the agents who hold the token as a store of value and as a medium of exchange (we will call them **A**). And second, we have the agents who seek a return by exchanging Terra for Luna when the price of TerraUSD goes below the peg (we will call them **B**). When the peg is lost, **B** exchanges TerraUSD, which is now worth less than 1 dollar, for Luna, worth 1 dollar, to make a return. **A** will not do anything because he is only interested in the stability of TerraUSD and believes that **B** will ensure stability by trading TerraUSD for Luna. This relation can describe the equilibrium of the stability of algorithmic stablecoins. However, this can be a fragile equilibrium if the beliefs in each other start to change as **A** stops using TerraUSD if they do not believe that **B** supports the stability by trading, and **B** will not support the stability if **A** are not using TerraUSD. A breakage of this equilibrium can then make the de-pegging permanent.

This implies that a breakage of the equilibrium will be a self-enforcing negative feedback loop, as both agents will lose further trust in the system leading the stablecoin to ultimately fail.

5.1.2.3 Failing Coins

The case of TerraUSD is not the only case of a failing stablecoin. In a study by Mizrach (2023) looks at all ERC-20 stablecoin projects on the Ethereum mainnet. The study identifies 65 active and inactive stablecoins that are among the top 5000 most capitalized. Inactive or failed stablecoins are categorized as projects where the trading volume has fallen below 1% of its peak quarterly volume. In the hazard function below the survivor probabilities is plotted.

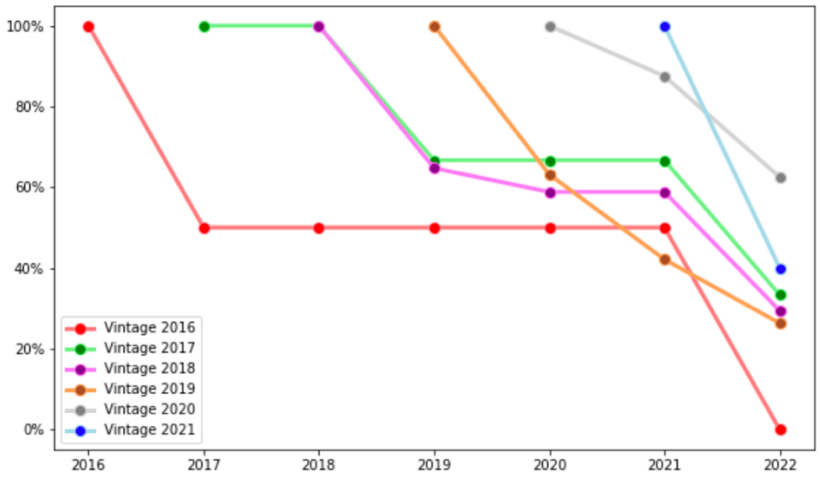


Figure 22: Hazard Function. Source: Mizrach (2021)

In 2016, two stablecoins reached the mainnet with both being deemed as failed projects by 2022. Both stablecoins were backed by gold. Six got introduced in 2017 with two still active in 2022 including Tether. In 2018, 17 new stablecoin projects ended on the mainnet with DAI, Paxos and USD Coin being some of them. By 2022, 12 of them failed. The same trend is observed for the remaining years where newly introduced projects fail within a year or two. In total between 2016 and 2022 only 24 of the 65 stablecoins are still active, creating a failure rate of 63%. From the hazard function we can conclude that stablecoin are considerably in danger of failing within the first year but stablecoin projects with a longer lifetime also risk failing.

5.1.3 Storage Risks

Certain risks also come from the storage method. As mentioned earlier stablecoin holders have the possibility to store stablecoin on their own digital wallet or with an exchange. In terms of holding stablecoins with their own secret key, risks of losing the assets can be boiled down to the holder's own management of securing of the assets. This includes losing access to the wallets e.g., by forgetting access details or distributing the secret keys to others. Since transactions are irreversible and pseudo-anonymous, individuals who have gained access to the wallet can transfer the funds to their own wallets without getting exposed.

For digital wallets held with exchanges such risks are reduced as the exchange is managing the secret key to the digital wallet. However, giving away control over a wallet to the exchange carries a certain risk. As the stablecoin are now held with a third-party holders take the risk of losing the tokens if the exchange gets hacked or goes bankrupt. A recent example of this risk was users that held their assets at the exchange FTX lost them when the exchange went bankrupt on November 11. 2022. FTX had lent customer funds to the company Alameda Research to pay off debts that Alameda Research had outstanding due to a series of failed bets involving the stablecoin TerraUSD. As a mass hiatus of the exchange ensued, and as FTX did not have the funds required to pay its customers the funds promised in their accounts, the funds were lost in the bankruptcy (Chow, 2022).

5.1.4 Summary of Financial Factors

In this first part of the analysis, we have gained significant insights into some of the risks of holding stablecoins. First, a literature review was conducted to understand the stability of stablecoins. It

was clear that stablecoins are not absolute stable, meaning that historical prices of stablecoins do vary (Hoang & Baur, 2021). However, stablecoins prices are found to have less variation than benchmark assets such as Bitcoin and stock indices (Hoang & Baur, 2021). The instability of stablecoins can arise from several factors. One of the most significant factors for the instability was the behavior of the Bitcoin price. The design of the stablecoin also plays a part in the stability where fiat-backed stablecoins were found to be the superior design for accommodating instability. Capitalization is also a factor since larger capitalized stablecoins drive the volatility of the smaller ones.

Not only can stablecoins be volatile in price, but they can also be worth nothing if they fail. Stablecoins with a reserve of assets can default in the event of a mass redemption of tokens. Such bank runs can happen if the holders get signals that the reserve value does not correspond to the value of the tokens in circulation or if the reserve assets are illiquid. For algorithmic stablecoins, we saw that holders' beliefs about each other maintain the peg. This equilibrium can easily break if the holders have reasons to change their beliefs, as seen with the crash of TerraUSD. TerraUSD is far from the only stablecoin to crash. Mizrach (2021) finds that stablecoins on the Ethereum mainnet have a failure rate of 63%, with many failing within the first years of existence.

Holders of stablecoins will also need to consider where to store the tokens, as storage possibilities come with different risks. A holder can either hold them on a digital wallet with full access to the secret key or with an exchange where the exchange is the only one with access to it. If holders choose to hold the tokens with their self-created digital wallet, they are exposed to the risks of making mistakes that can lead to losing tokens. Since digital can be challenging for holders without the necessary knowledge, this can be a significant risk. Due to this risk, many holders have their stablecoins with an exchange which is often a more accessible and convenient way of handling crypto-assets. Here, other risks arise as the holders do not have full access to their accounts; they are exposed to the risk of the exchange going bankrupt. A risk that is not insignificant from a historical perspective with the crash of FTX, where many crypto-asset holders lost their funds.

5.2 Technological Factors

At this moment, the primary utilization of stablecoin transactions is to serve as an intermediary for crypto investments. As a result, most stablecoins-related transactions are executed through exchange-based accounts (Mizrach, 2021). Enabling the transaction to stay off-chain between a trader as one party and a centralized exchange as the counterparty for a fixed exchange fee.
In the coming section, we will focus on the blockchain-based technology factors impacting stablecoin transactions for businesses and consumers, assuming both parties have their own digital wallet address, not held at an exchange. This analysis aims to gain insight into blockchain-related technological factors enabling scalable, fast, reliable, cheap, and secure transactions and how significant gradual demand increases might prevent stablecoin transactions from being so.

Much of the analysis will focus on the Ethereum main net and Ethereum-compatible solutions, as the Ethereum blockchain is the largest stablecoin transaction facilitator. Visa, the largest automated-clearing-house payment processor in the world, processed 226 billion transactions in 2021, corresponding to 7,166 transactions per second (de Best, 2023). To explore the possibilities of using stablecoins for payment like automated-clearing-house transactions and, in turn, bank-wire transactions. Let us explore how transaction traffic equal to 10% of Visa (716 TPS) would affect stablecoin transactions on Ethereum.

5.2.1 Issues with Capacity and Transaction Costs on Ethereum

5.2.1.1 Introduction to Stablecoin Gas Cost Fee

On the Ethereum blockchain, stablecoins run as ERC20 tokens where the transaction fee is synonymous with a gas fee and denoted in Gwei (giga-Wei), which is equal to 0.000000001 ETH (ethereum.org, 2023). The reason behind calling it a gas fee is that the EVM (Ethereum virtual machine) can run all computer programs of a general-purpose computer, also known as being Turing-complete, where every computational step requires one unit of gas, known as the gas cost. Therefore, the determinant of the gas fee for the transaction is determined by (ethereum.org, 2023):

$$\text{Stablecoin Gas Fee} = \text{Gas Cost} * \text{Gas Price}$$

The units of gas used for an operation will depend on the transaction's complexity. For example, an ETH transaction will have a total gas cost of 21,000 gas which is fixed, as the computational inputs for an ETH transaction are standardized. However, sending an ERC-20 token, such as a stablecoin, will require the EVM to compute extra steps, as their smart contracts are more complex. These additional steps result in a higher gas cost. The expected gas cost of sending a stablecoin is between 40,000 and 70,000 (etherscan.io/token, 2023).

5.2.1.2 Ethereum Block Capacity

To reiterate from the blockchain section, a new block is created every 12 seconds on the Ethereum (block interval), and the gas cost capacity of a block is 30 million gas units, with a benchmark of 15 million gas units. Assuming that a stablecoin transaction is 65,000[8] gas units and no partial transactions can exist, we can calculate the maximum stablecoin transaction per block:

$$\left(\frac{15{,}000{,}000}{65{,}000}\right) \approx 230 \text{ Transactions per block}$$

Dividing transactions per block with the block interval we obtain stablecoin transactions per second:

$$\frac{230}{12} \approx 19 \text{ Stablecoin Transactions Per Second}$$

This is the long-run network limit, as a pricing algorithm will ensure that transactions per second will converge to this number shown in the next section. This figure is also optimistic as the calculation assumes stablecoin transfers as the only transfers being processed by the network. Other activities, such as token swaps, are also being processed by the EVM, which as a minimum, has a gas cost more than double in size. Thus, it would be optimistic to say that the Ethereum main net can process about 19 stablecoin transactions per second at the current benchmark capacity.

[8] Conservative assumption to enable analysis of capacity and fees.
In reality stablecoin gas cost will vary depending on the complexity of the coin's smart contract.

5.2.1.3 Stablecoin Gas Price

From the gas cost section, we estimated the gas cost of a stablecoin transaction to be 65,000 gas units.

$$\text{Stablecoin Gas Fee} = 65{,}000 * \text{Gas Price}$$

The second part of the gas fee is the gas price. Gas price can be split into two components, base fee, and priority fee. The base fee is determined by the supply of block capacity and demand for transactional block inclusion. The supply and demand function is a tool to minimize network congestion. This implies that the base fee is burned after a transaction. The priority fee is intended as a tip for the validator nodes to prioritize fast block inclusion.

$$\text{Gas Price} = (\text{Base Fee} + \text{Priority Fee})$$

The base fee is determined by the last block's gas cost, compared to its benchmarked limit of 15,000,000 gas; conversely if the gas cost of the previous block has been more than the target size the base fee would increase to decrease demand.

Gas Used in Last Block	Effect on Next Block
$> 15,000,000$	↑ Base Fee ↓ Demand
$= 15,000,000$	Base Fee Demand
$< 15,000,000$	↓ Base fee ↑ Demand

Figure 23: Relation Between Base Fee and Demand. Source: Own Creation

The maximum increase and decrease per block are 12.5% on the base fee, which is reached at the capacity limit of 30 million gas or 0 gas. Such an increase can continue for each block maxing out the block capacity, increasing base fee exponentially until demand falls or rises to the capacity benchmark of 15 million gas (ethereum.org, 2023a).

5.2.1.4 Stablecoin Gas Fee

Based on the assumption from the past section, we can estimate the transaction fee (gas fee) associated with a stablecoin transaction on the Ethereum mainnet. It should be noted that the base fee and priority fee are automatically expressed as gas price in digital wallet applications. Summarized, the gas fee can be illustrated as (ethereum.org, 2023a):

$$Gas\ Fee = Gas\ Cost * (\ Base\ Fee + Priority\ Fee)$$

At the time of writing, a stablecoin transaction with a conservative gas cost estimate of gas is 4.93 USD. Using data from Etherscan, the highest this figure has been on 1st May 2022, where the average for the day was 87$ for a stablecoin transaction with a gas cost of 65,000. To find the stablecoin gas fee in US Dollar, the following equation is used:

$$\text{Stablecoin Transaction Fee} = (\text{ETH/USD Price}) * \text{Gas Fee}_{\text{ETH}} * 65{,}000_{\text{Gas}}$$

Based on this function we can illustrate the change in gas fee over time:

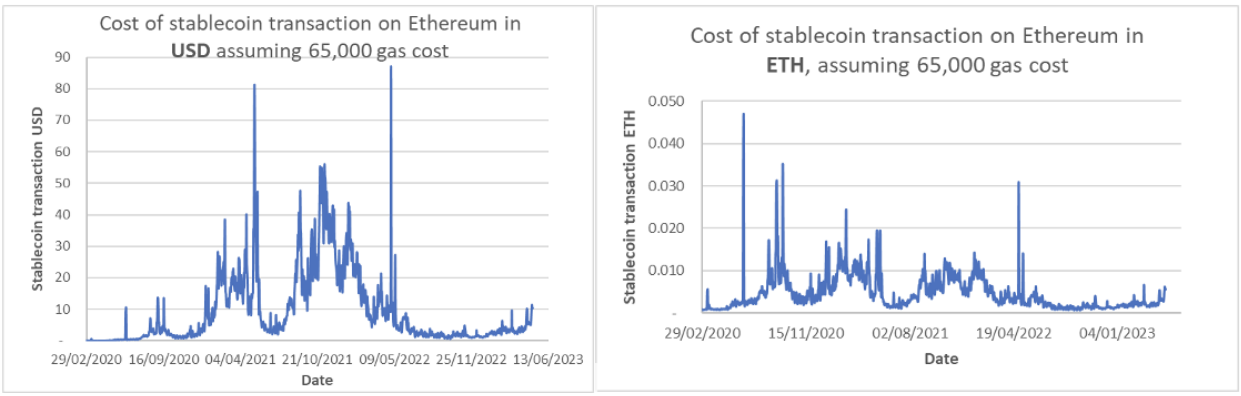


Figure 24: Cost of Stablecoin Transaction. Source: Etherscan

Summary statistics in the period 01/01/2019-04/05/2023 for the cost of a stablecoin transition assuming gas cost of 65,000 was:

Mean	**6.82 $**
Median	**2.25 $**
Minimum	**0.08 $**
Maximum	**87.18 $**

With transaction costs as high as seen from the summary statistics, it is far-fetched to imagine that Ethereum would be a reliable and cheap option for smaller retail payments. Much of these costs

are attributed to the block size not matching the transaction demand, however, some degree of the high transaction costs can also be attributed to the price development of ETH/USD, as can be seen by the spike in 2021 on the left graph.

As we learned in the previous section, the current block capacity only enables 19 TPS, so if a blockchain like Ethereum were to handle just 10% of the traffic that Visa does (716 TPS), block capacity would max out immediately. As a result, transaction costs would increase exponentially by a factor of: $Stablecoin\ gas\ fee\ *\ (1 + 12.5\%)$ per block (12 seconds) until demand stabilized to the 19 TPS benchmark.

One method of solving this issue is increasing the block capacity and frequency of block intervals, as was done in September 2022 when Ethereum switched to PoS. This is, however, a slow and costly process where demand catches up fast. Furthermore, frequent changes to the fundamental structure of a blockchain in the name of scalability also come with an increased risk of something not working correctly, which could have fatal consequences for both security and decentralization. Compromising on decentralization and security could likely be a risk for the capital tied up in the blockchain. This balancing act of scaling, decentralization, and security is commonly known as the scaling trilemma (blockchain trilemma) and was theorized by Vitalik Buterin, the co-founder of Ethereum (Hafid et al., 2020). More about the "Scaling Trilemma" can be seen in Appendix VI.

5.2.2 Scaling capacity on Layer2

In the following chapters, we will see how scaling solutions on Layer2 can maximize the blockchain capacity and throughput (transactions per second) and consequently enable a decrease in the costs of transactions without the risk of compromising on security and decentralization. Based on the previous estimates for transaction cost and capacity, such an initiative will be necessary for stablecoins on Ethereum to be competitive with traditional transaction means.

5.2.2.1 Categorizing blockchain scaling into layers

Scaling efforts of blockchains are often categorized into layers: 0, 1, and 2 to quickly identify how the change impacts the foundational principles that make up the blockchain.

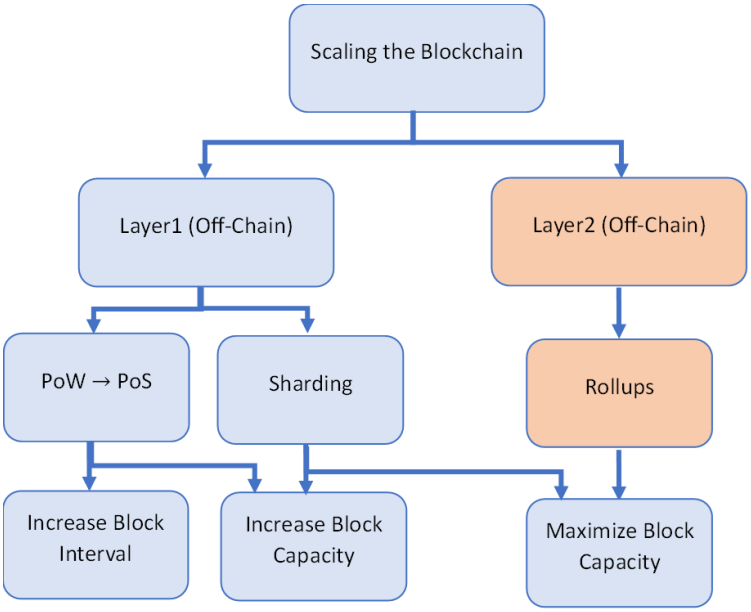


Figure 25: Scaling the Blockchain. Source: Own Creation

The three layers are defined as:

Layer0: Protocols concerning themselves with Layer0 address bandwidth usage optimization and increasing network communication abilities (Lipton & Treccani, 2022).

Layer1 (base layer): This is the layer where the blockchain is run, also called the base layer. Scaling methods in this layer can be seen as horizontal scaling. Layer 1 protocol changes include but are not limited to changes in consensus algorithm, block size or frequency interval changes, and computational sharding (See Appendix VII) **(Lipton & Treccani, 2022)**.

Layer2: Protocols concerning Layer2 can either be built atop the Layer1 protocol, thereby benefiting from the security features of the Layer1 protocol, thereby often being referred to as vertical scaling. Such solutions include optimistic rollups, zero-knowledge rollups, and state channels. Layer2 can also include separate blockchains that are compatible with the Layer1 chain; such solutions include sidechains and plasma chains (ethereum.org, 2023c).

5.2.2.2 Defining Relevant Layer2-Solutions

A critical matter of fact about Layer2 solutions and blockchain technologies, in general, is that there is not necessarily one perfect option. The optimal solution depends on the purpose for which

it is used. The focus of this analysis will be on rollup solutions. The reason for this choice is that Rollups are the only scaling solutions with full transaction data availability so that the validity of transactions can be verified independently on the Layer1 blockchain.

Sidechains and plasma-sidechains might only offer this transaction data availability on their own blockchain and will instead have "checkpoints" of the state of balances on the Layer1 blockchain. This implies a risk of compromising the integrity of transactions if the chosen sidechain or plasma-sidechain does not have a sufficiently secure consensus layer. Furthermore, sidechains and plasma-sidechains will also have their own token for sending payments, which is considered a complication in the scope of analysis, with ETH being the primary means of paying for transactions. In the following sections analysis of Layer2 scaling solutions and their impact and potential for scaling will be applied to better understand the scalability gains and risks involved with rollups. In turn, this will allow us to explore the possibilities of using stablecoins as a means of payment comparable to automated-clearing-house transactions and, in turn, bank-wire transactions.
In the coming sections, events referring to blockchains such as Ethereum will be referred to as Layer1 (L1), and scaling methods such as rollups will be generalized as Layer2 (L2).

5.2.2.3 Rollups: A Data Available Layer2-Solution

Rollups are new concepts that have only existed since about 2019, whereas actual functional use has picked up in the past two years. Rollups function by moving the computation of transactions off-chain and then submitting the transaction data (calldata) in bulk (batches) to Layer1 afterward. The calldata takes up less storage space (capacity), thereby increasing the number of actual transactions that are submitted to the Layer1 Blockchain. The state of the accounts and balances on the rollup network are Merkelized into Merkle trees, where a hash of the Merkle root, called a state root, is also stored on-chain in a Layer1 smart contract connecting Layer1 to Layer2 (Buterin Vitalik, 2021). The processes involved with Layer2 scaling on rollups is illustrated below:

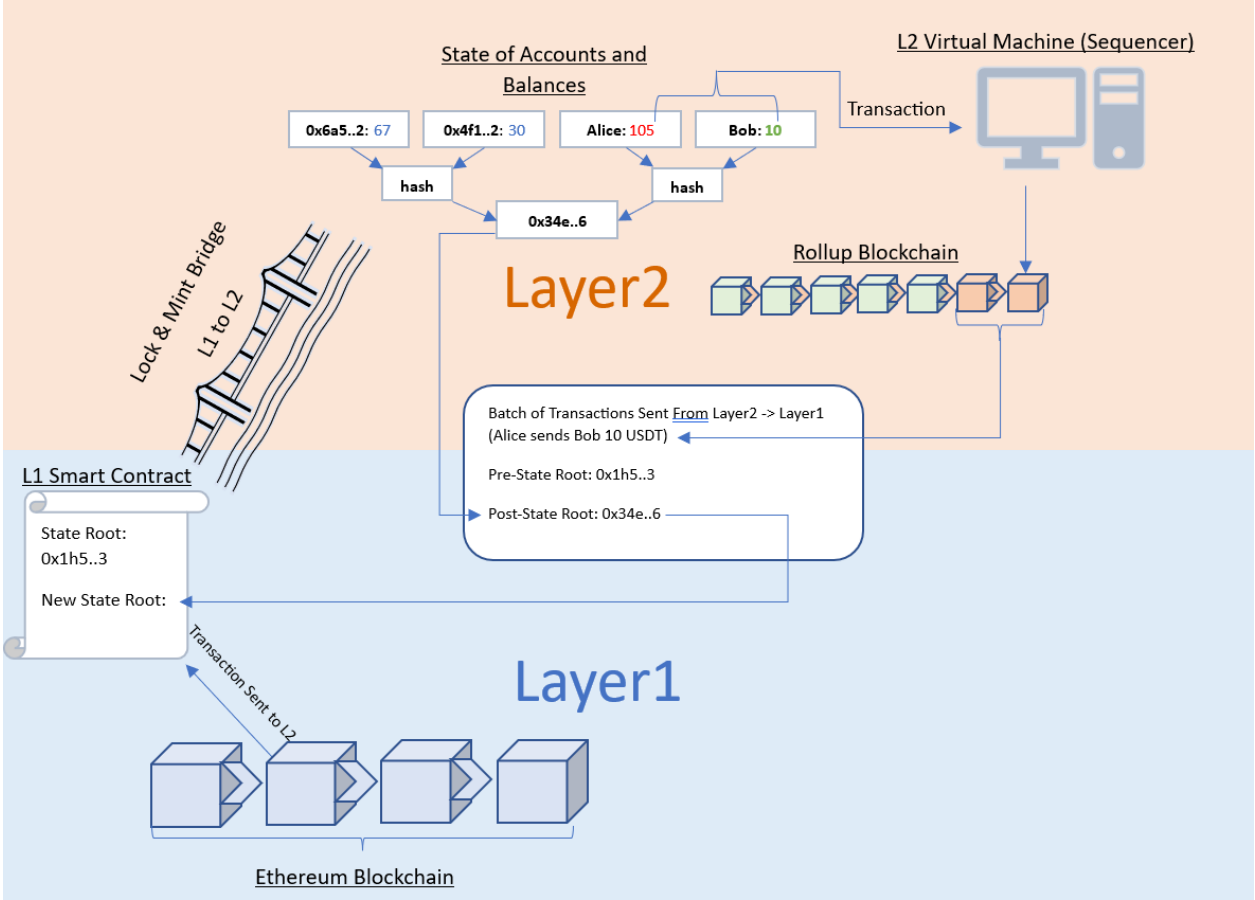


Figure 26: Rollup Transaction Operation Scheme. Source: Own Creation

Each 'leaf' represents a user's balance, and an index represents its position in the Merkle tree. Past balance updates can therefore be proven by recreating the state from the state root and indexing the account. However, past transactions cannot be altered, as the new state root is updated with each batch of transactions executed off-chain, hashed with the previous state root, and submitted to Layer1, which gives us an equivalent immutability guarantee as that of the blockchain.

Currently, the two dominant rollup solutions being developed and used are zero-knowledge rollups and optimistic rollups. One real-world application of each two rollup solutions is chosen for perspective, where both examples are Ethereum Virtual Machine compatible for easy comparison.

5.2.2.4 Zero-Knowledge Rollup Technology

Sending token funds as stablecoins through a zero-knowledge rollup (ZKR) will mean that the transactional computations will be executed by a virtual machine off-chain, by the hand of Layer2 operators called sequencers, which are often a centralized entity due to the complexity of the computational work. After the transactions are executed, the sequencer will generate a cryptographic zero-knowledge proof, which is submitted with the batch of the calldata (transaction data) to an on-chain smart contract connecting the ZKR to Layer1 for recording (ethereum.org, 2023d).

The calldata, coupled with the zero-knowledge proof of validity (ZK-Proof), can be independently verified by validators on Layer1 without revealing the content of the transactions themselves. Similar to a digital signature, verifying the ZK-Proof will then return 'is valid' or 'is not valid,' i.e., the name zero-knowledge (ethereum.org, 2023d).

Zero-knowledge rollups use a lock-and-mint bridge to move funds from L1 and L2 (Appendix V). Funds can be withdrawn from a ZKR to Layer1 as fast as it takes to send a transaction to a burn address; on L2, the balance will then be restored on Layer1 by the bridge smart contract.

5.2.2.4.1 ZKR Scalability of Transaction Capacity

When looking at the transaction capacity of rollups, it is essential to keep in mind how many transactions per second (TPS) the network can scale is limited to the Layer1 blockchain atop which it is built. This measure does not represent transaction speed by instead the throughput capacity. Essentially this implies that the hypothetical TPS gain comes from the storage space that the calldata and ZK-Proofs from the ZKR will occupy, which might otherwise be used for storing uncompressed transactions. Using estimates from Buterin (2021), we can illustrate the byte sizes of compressed calldata from transactions as:

Zero-knowledge rollup Storage space vs Ethereum	**L2**	**L1**
Token specification approx. ~	4.00	4.00 Bytes
Nonce	0.00	3.00 Bytes
Gas price approx. ~	0.50	8.00 Bytes
Gas approx. ~	0.50	3.00 Bytes
To address	4.00	21.00 Bytes
value approx. ~	3.00	9.00 Bytes
From address	4.00	0.00 Bytes
Signature n/a. since ZK-proof serves same purpose	0.00	68.00 Bytes
Transaction data	16.00	116.00 Bytes

Figure 27: ZKR Storage Space Compared to Layer1. Source: Own Contribution based on Xangle (2022) & Buterin (2021)

Transaction data of stablecoin transfers can be compressed from 116 bytes of data to a rough estimate of around 16 bytes by switching from L1 to L2. The real compression gain here is attributed to 68 bytes of data digital signature certificates.

After the Ethereum Berlin update, 1 byte of non-zero calldata has a gas cost of 16 (Wood, 2022). Stablecoin transaction calldata on ZKR is, therefore, 256 gas. The gas cost from proof of validity is fixed no matter the number of transactions. However, the estimates of the actual gas cost depend on the complexity of the code when executing the proof. Sources suggest the gas cost is between 500,000-1,500,000 gas. For simplicity, the gas cost of the zkSNARK generated by the Layer2 solution zkSync is used (Wu, 2019; Xangle, 2022; zksync.io, 2022a). Formally:

Gas Cost for ZK-Proof (zkSNARK): $\sim \mathbf{800,000}\ \boldsymbol{Gas}$

Gas Cost per stablecoin transaction in a batch: $16\ \text{Bytes} * 16\ \text{Gas Cost} \sim \mathbf{256\ Gas}$

We can then calculate the theoretical capacity gain from executing transactions off-chain using ZKR as:

$$\frac{\left(\frac{15{,}000{,}000 - 800{,}000}{256}\right)}{12} \approx \mathbf{4,622}\ \boldsymbol{Stablecoin\ Transactions\ Per\ Second}$$

Thereby scaling the Layer1 Ethereum throughput of 19 TPS by 24,226%.

It is important to note that this figure is a theoretical capacity of stablecoin throughput achievable by a ZKR. It is meant to give a benchmark to compare with other alternative Layer2 scaling solutions. This capacity will only ever be hypothetical at the current state as it is infeasible to account for all other non-stablecoin-related transactions concurrently being transferred on both Layer1 and Layer2.

5.2.2.4.2 ZKR Transaction Fee Structure

The costs involved in stablecoin transactions on a ZKR are comprised of two components, the first being the off-chain computations carried out by the sequencer, i.e., executing transactions, aggregating them into blocks on Layer2, and generating the ZK-Proof (zksync.io, 2022b). The second cost component is the on-chain cost of sending the ZK-Proof along with the transaction inputs to the L1 cost, which is the largest cost by magnitude.

As generating the ZK-Proof can take up to several minutes, gas prices can potentially fluctuate significantly (Burger, 2022). In order not to charge ZKR users retroactively with the actual cost transaction calldata, the sequencer carries will, in some cases, carry the cost (zksync.io, 2022b). ZKRs mediate this cost by using a demand-based algorithm, pricing the transaction upfront depending on past proof verification pricing, the type of token transfer (stablecoins are more expensive to send than ETH), and Layer2 network congestion.

The fees from a stablecoin transaction on ZKR should, with the costs involved with the transaction for L1 and L2, be estimated as approximately:

$$\text{L2 Fee} = \text{Execution Fee} + \text{Prover Cost} \approx 0.001\text{USD (zksync.io, 2022b)}$$

$$\text{L1 Fee} = \left(\frac{\text{ZKproof}}{\text{Batch Size}} + \text{L1 Bytes per User Operation} * \text{L1 Gas Cost}\right) * \text{L1 Gas Fee} * \text{ ETH/USD Price}$$

$$\text{ZKR Stablecoin Transaction Fee} = \text{L2 Fee} + \text{L1 Fee}$$

The estimates are based on the figures described in the previous section. What is important to note is that as Ethereum gas prices increase, so does this transaction fee. Recall that gas prices were demand controlled to stay at the block capacity benchmark of 15,000,000 gas units. This implies that if gas prices are to increase by a factor of 10, the fees of the ZKR will grow at a similar rate. As the gas fee paid for transaction execution on Layer2, is a fraction of the transaction execution on Layer1, the total transaction fee will be made up almost entirely of Layer1 calldata storage cost.

5.2.2.4.3 ZKR Security and Decentralization

On a ZKR, the methods for calculating a ZK-Proof of validity vary. However, the most known proof of validity is a Succinct Non-interactive ARgument of Knowledge, or zkSNARK. Other ZK-proofs, like zkPLONK's and zkSTARK's, are also used (Burger, 2022). The complex calculations in computing a zkSNARK are out of the scope of this thesis, but the computations involve cryptographic proof of the transaction data coupled with a batch root, a pre-state root, and a post-state root.

Of the two Layer2 scaling solutions chosen for this analysis, ZKR shows the most significant promise in the security of transactions. This is attributed to the ZK-proofs generated, which are independently verified at Layer1 against the pre-state and post-state of accounts and balances.
The only genuine concern would be the high degree of centralization, where censorship by a rogue sequencer could either single out an address, refuse to execute transactions from it, or stop executing transactions altogether. As a security measure, ZKRs have a built-in function that allows anyone to submit transactions to the Layer1 smart contract. This function enables users to manually bridge back to Layer1 at the exact cost as a transaction on Ethereum, comparable to using an emergency exit (ethereum.org, 2023d).

5.2.2.4.4 ZKR Transaction Speed and Finality

Transaction speeds can be tricky to estimate when using Layer2 scaling, as it is all a matter of when one would consider a transaction final. To further explore transaction finality of a ZKR transaction, it can be split into four stages with the prefix ZKR for Zero-knowledge rollup, or L1 indicating where the stage takes effect:

Let us say that Alice sends Bob 10 USDT on a ZKR.

1. ZKR ≈ instant: Transaction execution, block inclusion & proof generation: Here, the transaction will be carried out instantly and be included in a block. Alice will receive a receipt of the payment and fee; Bob will see the 10 USDT added to his ZKR wallet.

2. ZKR ≈ 1-20 minutes: Proof generation is complete, and the batch of transactions from the ZKR is then submitted to Ethereum smart contract.

3. L1≈ 12-36 seconds: The zkSNARK proof is verified by validator nodes on Ethereum (Layer1) and has been included in the transaction data on a block as calldata.

4. L1 ≈ 16 minutes: 2,5 epochs of 32 slots (blocks) have passed, and the transaction data is now considered finalized and immutable.

This gives us a total time for transaction finalization of around **36.5 minutes**. After which a transaction will be considered immutable.

5.2.2.5 Optimistic Rollups

Whereas zero-knowledge rollups rely on computational proof of valid transactions, optimistic rollups (ORs) function with the predisposed assumption that the calldata from transactions processed in Layer2 submitted to Layer1 is correct. This assumption of reliable computation is what gives this sort of rollup the name "optimistic rollup." ORs are contrary to zero-knowledge rollups, fully compatible with smart contract coding on Layer1. At the time of writing, this makes them the largest rollup on a user basis for stablecoin transactions, as ZKRs in the past needed more time to encode the smart contract of each token and application (Gluchowski, 2019).

5.2.2.5.1 Operators and Fraud Proofs

The operator aggregating and executing transactions on optimistic rollups is referred to as the sequencer and is more than likely a centralized entity. ORs operate under the assumption that verifiers will continuously check and verify that the state change is in accordance with the previous state, thereby holding the sequencer accountable.

The sequencer will aggregate transactions sent on the Layer2 network into a block on the Layer2 after execution. Larger aggregates of transactions' calldata are then rolled up into batches sent to the rollup smart contract on Layer1. The calldata submitted to Layer1 will contain a batch root hash, pre-state root hash, post-state root hash, transaction inputs, and the ECDSA digital signature of each transaction.Once the calldata block is submitted to the optimistic rollup smart contract, a challenge period begins for a limited time, usually a week, where anyone can challenge the validity of the transactions carried out in the calldata block (ethereum.org, 2023b). If a challenge occurs, the optimistic rollup protocol will re-execute the disputed transaction through a smart contract, this time on Layer1. If the challenger is correct, the operator/sequencer will have its stake slashed.

5.2.2.5.2 OR Scalability of Transaction Capacity

Recall the ECDSA for executing and signing transactions with private and secret keys. As optimistic rollups publish transaction data directly onto Layer1 without a ZK-Proof of validity, there needs to be proof that the transaction was carried out by the intended sender so that the transaction can be reconstructed if doubt occurs. To accomplish this, the digital signature applied to the

transaction on Layer2 must be included in the transaction data published on Layer1. Currently, such a signature makes up approximately 81% of the total calldata needed for storage per transaction (Xangle, 2022)(Buterin, 2021). As seen with ZKR, we can illustrate the byte sizes of compressed calldata from transactions as:

Optimistic rollup storage space vs Ethereum	L2	L1	
Token specification approx. ~	4.00	4.00	Bytes
Nonce	0.00	3.00	Bytes
Gas price approx. ~	0.50	8.00	Bytes
Gas approx. ~	0.50	3.00	Bytes
To address	4.00	21.00	Bytes
value approx. ~	3.00	9.00	Bytes
From address	4.00	0.00	Bytes
Signature n/a. since ZK-proof serves same purpose	68.00	68.00	Bytes
Transaction data	84.00	116.00	Bytes

Figure 28: OR Storage Space Compared to Layer 1. Source: Own Contribution based on Xangle (2022) & Buterin (2021)

84 bytes per transaction is quite an increase compared to the 16 bytes of transaction data that a ZKR will include per transaction. Besides the transaction data submitted in batches, a hash of batch root, the batch root being the root of all the transactions in the batch summarized into a Merkle tree on the OR, is added along with a hash of pre- and post-state root. The compression abilities to publish the hash of these roots can vary, so for simplicity, let us use an estimate from Optimism, one of the largest ORs by platform users. Here the batch root hash, pre-state root hash, post state root hash, and a transaction to the smart contract on Layer1, carry a gas cost of approximately 280,000 gas (Xangle, 2022).

We can then estimate the TPS of OR:

Gas Cost for publishing one batch: $\sim \mathbf{280,000}\ \boldsymbol{Gas}$

Gas Cost per stablecoin in a batch: 84 Bytes $*$ 16 Gas Cost $\sim \mathbf{1,344}\ \boldsymbol{Gas}$

$$\frac{\left(\frac{15{,}000{,}000 - 280{,}000}{1344}\right)}{12} \approx \mathbf{912}\ \boldsymbol{Stablecoin\ Transactions\ Per\ Second}$$

This is scaling the original Ethereum throughput of 4,700%, which is a substantial increase. Once again, this is a theoretical transaction throughput, where the actuality will have to account for Layer1 capacity being utilized for other computations. This throughput might increase significantly with signature aggregation through BLS signatures. So instead of verifying the validity of each digital signature for every transaction, only one digital signature will prove the validity of the entire batch.

5.2.2.5.3 OR Transaction Fee Structure

Optimistic rollups will have their own gas prices, which will be benchmarked after demand, but because the block interval on ORs will be significantly higher than on L1, it will likely never increase to a point where it will have a substantial influence on the total OR fee, for reference Optimism one of the largest OR solutions have benchmarked the gas price at 0.001 Gwei (Optimism, 2023). We can thus define the OR Fee Structure:

Execution Fee: Being the product of gas used for a transaction multiplied by the OR's gas price.

$$\text{Execution Fee} \approx \sim\text{Fixed L2 Gas Cost} * \sim\text{Fixed L2 Gas Price}$$

Layer2 Fee: Being the product of the execution fee multiplied by the ETH in USD

$$\text{L2 Fee} = \text{Execution Fee} * \text{ETH/USD Price}$$

Layer1 Fee: The cost of storing transaction data on Layer1 in USD.

$$\text{L1 Fee} = \left(\frac{\text{Fixed Gas Cost of Batch}}{\text{Batch Size}} + \text{L1 Bytes per User Operation} * \text{L1 Gas Cost}\right) * \text{L1 Gas Fee} * \text{ETH/USD Price}$$

OR Transaction Fee: The cost of sending a stablecoin transaction on OR is the sum of L1 and L2 fees.

$$\text{OR Stablecoin Transaction Fee} = \text{L2 Fee} + \text{L1 Fee}$$

We will see later how the L1 fee far outweighs the L2 fee. This makes data compression efforts the most valuable tool in decreasing transaction costs for ORs.

5.2.2.5.4 OR Security and Decentralization

ORs rely on an optimistic assumption of honest transaction executing from the sequencer and honest user transactions. While this enables fast transaction times, as batches can be sent to Layer1 at a higher rate than for ZKRs, there is no guarantee that the transactions were executed correctly. The reason is that this requires a validator to verify all transaction data and create Fraud-Proofs if mistakes were made, which might, in theory, not always be the case.

One significant risk associated with ORs using a centralized sequencer system is relying on Layer2 block production to withdraw funds. User withdrawal back to Layer1 is dependent on a withdrawal transaction on the OR. After the challenge period is finalized, the funds will be available for extraction on Layer1 (l2beat.com, 2023). In the scenario that a sequencer is faulty or, for some other reason, stops producing blocks, users will be unable to send transactions or withdraw their funds. However, having data availability on Layer1 enables a new sequencer node to recreate the last state of the rollup and continue producing blocks (ethereum.org, 2023c). Another centralization-related risk is the purposeful censorship of a user by a malicious sequencer; users can submit their transactions to Layer1 smart contract as a defense. After a certain time, the sequencer will be forced to include the transaction or risk not being able to produce valid blocks (ethereum.org, 2023c).

5.2.2.5.5 OR Transaction Speed & Finality

The finality of OR stablecoin transactions can, like ZKR transactions, be split into four stages, with the prefix OR for Optimistic rollup or L1 for Layer1 indicating where the stage takes effect. Furthermore, as ORs operate with fraud proofs affecting transactions retroactively, we will also categorize finality into soft transaction finality and hard confirmation finality, as seen below.
Let us again say that Alice sends Bob 10 USDT on an OR.

1. OR ≈ Instant: Transaction execution, block inclusion: Here, the transaction will be carried out instantly and be included in a block. Alan will receive a receipt of the payment and fee; Bella will see the 10 USDT added to her OR wallet.

2. OR ≈ 0-5 minutes: Block is included in a rollup batch and sent to the Layer1 smart contract.

3. L1 Soft Transaction Finality ≈ 12-36 seconds: Validators have included the transaction data in a block as calldata.

4a. L1 < 7 days: Verifier disputes transaction validity and displays fraud-proof, in which case the transaction is executed on Layer1 and is finalized here.

4b. L1 Hard Transaction Finality ≈ 7 days: The challenge period is over, and the transaction is finalized and immutable.
This gives us a soft transaction finality of ≈ 5 minutes and a hard finality of ≈ 7 days.

5.2.2.6 Future Scalability Implementations Affecting Ethereum and Rollup Solutions

Over the coming years, EIP-4488 (Ethereum improvement proposal) is expected to implement Proto-Dank sharding to the Ethereum blockchain, the first of many sharding efforts applied to Ethereum (ethereum.org, 2023a). In short, Proto-Dank sharding will introduce "blobs" that rollups can post transaction calldata in, which will be attached to the blocks on the blockchain. The data written in the blobs will be downloaded on each full node on the p2p network but will, however, not be accessible to the EVM, thereby not counting against the gas capacity of each block. Furthermore, as OR only need the data to be available for approximately seven days, as for the case of the challenge period for fraud-proof generation in Optimistic rollups, the blobs can and will be deleted from the full nodes on Layer1 after 1-3 months (ethereum.org, 2023a).

The transaction data posted by rollups in each blob will have a cryptographic commitment fitted to it in the form of a polynomial function, where the function's inputs can be evaluated against the function and verified by each validator node. If the transaction data is changed later, the inputs will no longer yield the same result, giving us a similar effect of hashing one Merkle root to the hash of a previous Merkle root, like the process of a ZK-proof.

As data recording on Layer1 makes up most of the transaction fee from L2, such methods might decrease fees significantly. More importantly, the transaction throughput of rollup solutions will not be bound to the Ethereum gas capacity, which could move theoretical throughput upwards of 100,00 transactions per second within just a few years (ethereum.org, 2023a). This would be a

throughput that can potentially be higher than that of automated clearing houses such as Mastercard and Visa, currently having a max throughput of 24,000 TPS (Visa, 2023).

5.2.2.7 Conclusion Layer2

From the past sections, we can conclude that rollup Layer2 solutions are a valuable tool to enable scaling transactional throughput of stablecoin transactions to a level where it should at least, in theory, be able to handle more than 10% of the transaction traffic of Visa. Layer2 rollups can do this with minimal risks of compromising on transactional integrity, where it seems the security of ZKR would be more likely to be preferred over ORs due to fraudulent activity from a sequencer not being possible.

In the coming section, we will illustrate how demand-related factors impact stablecoins transactions executed both on-chain on Layer1 and off-chain on Layer2.

5.2.2.8 Capacity and Transaction Cost Drivers Exemplified

The past sections analyzed more of the theoretical underlying technological functions affecting the blockchain-related economics of stablecoin transactions on the Layer1 blockchain Ethereum and data available scaling solutions as Layer2 rollups. These technological functions can now be applied to a data set to gain additional insight into how demand-related factors interact with stablecoin transactions.

The goal of this analysis is not necessarily to gain precise knowledge about the current state of prices stablecoin transaction costs, as this would only serve as a cross-sectional image that would not be relevant soon after that, given the volatile history of blockchains. Instead, the goal is to have a broader perspective and understand the limits and opportunities of stablecoins for transactional functions other than serving as an investment medium for speculation in volatile crypto-currencies. As previously established, stablecoin transaction fees will be a function of several demand-dependent variables. However, to summarize, they can be decomposed to:

Stablecoin Transaction Ethereum Fee:

$$\approx \text{ETH/USD Price} * \text{Gas Cost} * \text{Gas Price}$$

Stablecoin Zero-Knowledge Rollup Fee:

$$\approx \sim\text{ZKR Execution Fee} + \left(\frac{\text{ZKProof Gas Cost}}{(\text{batch size})} + \text{L1 bytes per User Operation} * \text{L1 gas cost}\right) * \text{Gas Price} * \text{ETH/USD Price}$$

Where,

$$\text{ZKR Execution Fee} \approx (\sim\text{Execution fee}_{\text{USD}} + \sim\text{Prover cost}_{\text{USD}})$$

Stablecoin Optimistic Rollup Fee

$$\approx \sim\text{OR Execution Fee} * \text{ETH/USD Price} + \left(\frac{\text{Fixed Gas Cost of Batch}}{\text{Batch Size}} + \text{L1 Bytes per User Operation} * \text{L1 gas cost}\right) * \text{Gas Price} * \text{ETH / USD Price}$$

Where,

$$\text{OR execution fee} \approx \sim\text{fixed L2 Gas Cost of Transaction} * \sim\text{fixed L2 Gas Price} * \text{ETH/USD Price}$$

Here the two most impactful variables are L1 gas prices on the blockchain and the price of ETH/USD. Both these variables are demand sensitive, so a mass adoption of stablecoins as a means of payment should influence the user reliability of stablecoin transaction fees.
The graph below conceptualizes the ETH/USD price development's isolated effect on stablecoins transaction costs by holding the gas prices fixed at the Q1 2023 median of 0.00000002888 ETH so that gas fees are fixed at 0.001876984 ETH, corresponding to our conservative assumption of 65,000 gas cost for a stablecoin transaction. The breakdown of the input variables used can be found in Appendix VIII. For context, the ETH/USD price is currently between 1800-1900 USD. Formally[9]:

$$\Delta\,\text{Stablecoin Transaction Costs Ethereum} = (\Delta\,\text{ETH/USD Price} * \text{Gas Cost} * \text{Gas Price})$$

$$\Delta\,\text{Stablecoin Transaction Cost L2} = (\Delta\,\text{ETH/USD Price} * \text{L2 Execution Fee}) + (\Delta\,\text{ETH/USD Price} * \text{Gas Cost} * \text{Gas Price})$$

[9] The blue text in the formula indicates that variables are fixed.

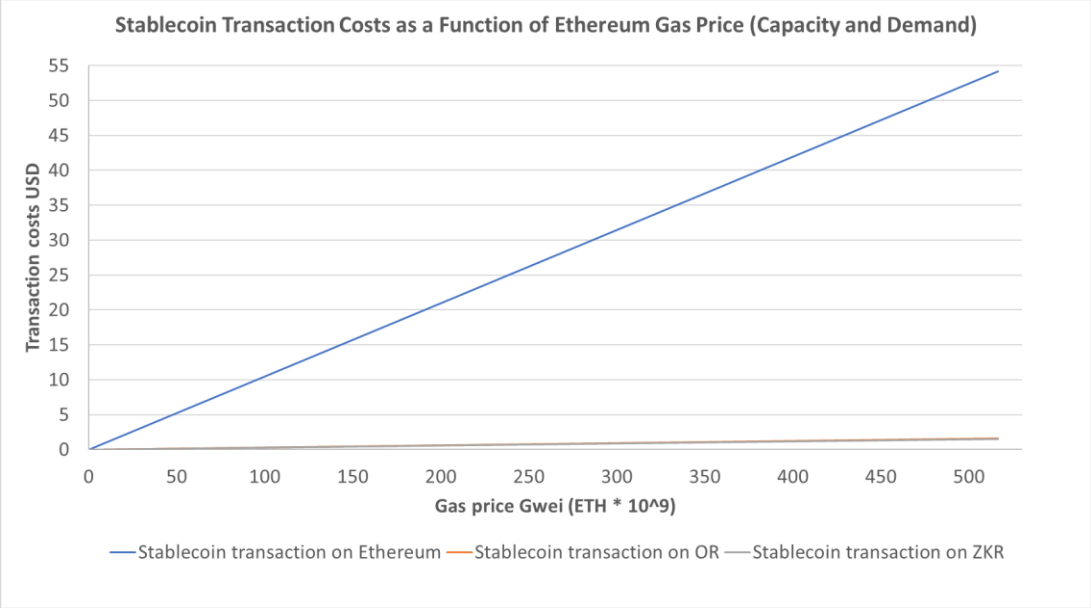


Figure 29: Stablecoin Transaction Costs as a Function of Ethereum Gas Price. Source: Own illustration, Own Estimates from assumptions (Etherscan.io, 2023b, 2023a)

From the graph, we can conclude that though the ETH/USD price will have a substantial effect on transaction costs on Ethereum, it would be significantly less influenced on the Layer2 solutions. The second variable impacting transaction costs to perhaps the most significant degree is L1 network congestion, i.e., how many require transaction inclusion on the blockchain. Below, the graph conceptualizes the isolated effect of capacity demand on stablecoin transaction costs which is measurable by the gas price. Here the ETH/USD price is held fixed to the Q1 2023 arithmetic price average of 1590.19 USD, along with the transaction fees for Layer2 off-chain execution fees. Again stated formally:

$$\Delta \text{ Stablecoin Transaction Costs Ethereum} = (\text{ETH/USD Price} * \text{Gas Cost} * \Delta\text{Gas Price})$$

$$\Delta \text{ Stablecoin Transaction Cost L2} = (\text{ETH/USD Price} * \text{L2 Execution Fee}) + (\text{ETH/USD Price} * \text{Gas Cost} * \Delta\text{Gas Price})$$

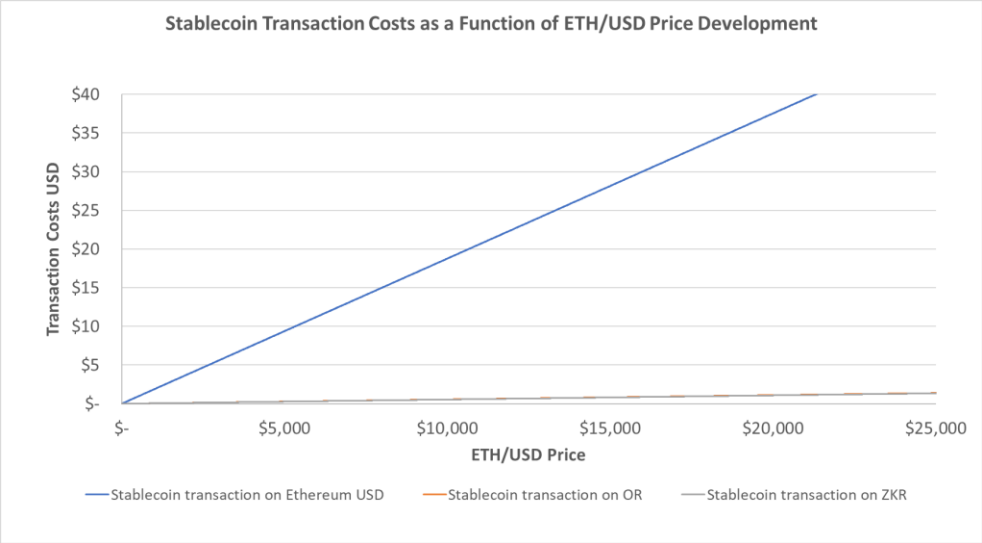


Figure 30: Stablecoin Transaction Costs as a Function of ETH/USD Price Development. Source: Own illustration, Own estimates from assumptions (Etherscan.io, 2023b, 2023a)

Gas prices are directly correlated with block inclusion demand, as gas price will increase or decrease for the next block proportionally with how far the last block's gas demand was from the benchmark. This will have a direct causal effect on the stablecoin transaction fee in ETH.
The effect that ETH/USD Prices and gas prices would have on one another has not been analyzed, but the correlation from 15/09/2022 to 04/05/2023 between the two variables was 0.515. Furthermore, as the current ETH supply is shrinking by approximately 0.5% yearly, then by the law of demand, ETH/USD price, ceteris paribus, is expected to rise. In the period before the implementation of PoS in Ethereum, the supply of ETH was increasing. In the period after implementation of PoS from 15/09/2022 to 04/05/2023, the correlation between ETH supply and ETH/USD price was -0.531.

If ETH/USD prices were to have any causal effect on gas price relative to the dollar cost, one would expect that future stablecoin transaction costs on Ethereum would rise in the long run. Whereas the effective ETH cost of gas price might not necessarily, as deflation would have an inverse effect of blockchain localized gas pricing.

In the next section, we will, through assumptions and estimates made, compare how stablecoin transactions sent through Layer1 and Layer2, match up against automated clearing houses and bank-wire transfer payments.

5.2.2.9 Comparison of Decentralized Stablecoin Payments to Traditional Payment Systems

Assuming that stablecoins can be accepted as a medium of exchange equivalent to digital debit-credit card payments and legal tenders such as cash, a side-by-side comparison can be illustrated as seen below. Estimates are based on the minimum and maximum expected transaction costs of stablecoin transactions on Ethereum and Ethereum-compatible rollups for Q1 2023 to give a rough idea of comparability for use case functions.

100$ Equivalent US Domestic transaction:

	Plat-form	**TPS (capacity)[10]**	**Exp. Sender fee[11]**	**Exp. recipient fee**	**Transaction verification proof**	**Transaction finality**
Cash	n/a	Instant	Free	Free	Instant	n/a
Wire transfer	Swift	n/a	26$	13$	Instant	~ 0-3 days
ACH	Visa	~7,166[12]	Free	2.1$ (2%+0.1$)	Instant	~ 0-3 days
Layer1 blockchain	Ethe-reum	~19*	~1.41-11.99$*	Free	Instant	~ 16 min
Layer2 OR	n/a	~ 912*	~0.04 - 0.35$*	Free	Instant	~ 7 days
Layer2 ZKR	n/a	~4,622*	~0.04 - 0.34$*	Free	Instant	~ 36 min

Figure 31: Comparison of a Transaction Worth $100. Source: Own Contribution & (AFP, 2022; Burger, 2022; Etherscan.io, 2023a, 2023b; Goldberg, 2022; optimis-tic.etherscan.io, 2023; Snyder, 2023; Worldbank.org, 2022; Xangle, 2022; zksync.io, 2022b)

Conversion fees and exchange rates aside, looking at the raw transaction estimates of a 100$ equivalent transfer of value, stablecoins transactions completed on Layer 2 technologies match up quite decently against ACHs like Visa or Mastercard. There are, however, some striking differences and caveats that raise questions for discussion.

[10] *The TPS for Layer 1 and Layer 2 is the using the theoretical long-run limit for optimal block capacity on the Ethereum blockchain.
[11] *Based on the Min and Max expected transaction costs using assumptions coupled with daily ETH/USD and gas prices on the Ethereum blockchain
[12] The TPS for visa, is calculated as the average of global transactions in 2021

Starting with capacity, the sheer volume that an ACH like Visa can handle is theoretically 24,000 TPS (Visa, 2023). So here, even if the entirety of the long-run block capacity limit on the stablecoin market leader platform, Ethereum, were used for ZK-rollups, it would not be able to handle the 7166 TPS that Visa on average handled in 2021 at this current moment. However, it is far stretched to imagine that adoption of stablecoins as a retail payment would be adopted fast enough for this to be an issue. With adoptions like Dank-sharding and constant developments of compression capabilities, it is considered realistic to realize a theoretical throughput comparable to that of Visa within just a few years.

Secondly, in traditional payment methods, debit and credit card payments, most of the transaction fee will depend on the transaction amount in fiat currency. Debit and credit card transactions are structured as a fixed fee from the card issuer plus a fixed coefficient multiplied by the variable, the amount transferred in the transaction. It can be stated as follows:

$$\text{Debitcard Transaction Fee} = \text{ACH Fixed Fee} + \text{Bank Fee Rate} * \text{Transaction Amount}$$

Though stablecoin transactions sent and received on Layer2 will be competitive and perhaps even cheaper in total cost, consumers are not incentivized to use stablecoins for purposes such as retail shopping. This is due to the transaction fees being distributed to the sending party (consumers). Merchants would be highly incentivized to accept stablecoin payments. However, they would be hard pressed to find anyone willing in a domestic scenario, as it would not make sense for customers to pay with stablecoins in such a case.

However, when traveling abroad, most banks and ACHs will demand a fee for exchange rate uncertainty and payment routing between the transaction and final bank clearing, which in most cases are 1-3 days(Snyder, 2023) (World Bank, 2022).
An example of consumers beneficiating from using stablecoin could be if a European traveled to the USA in the first quarter of 2023. Using a debit-credit card from Visa or Mastercard will often yield a transaction of around 3% (Snyder, 2023). If compared to using a layer2 rollup, where

stablecoins are used as payment instead, consumers and merchants would benefit from decreased fees.

Wire transfer payments are seemingly the clearest use case for decentralized stablecoin payments. Wire payments have been known in many countries to be an expensive yet safe way of sending payments.

Another case for stablecoins is in international remittance payments. The World Bank estimates the global cost of remittance payments of 500$ was 6.3% in Q3 2022 (World Bank, 2022).

	Worldwide remittance	
	Exp. Sender fee	**Exp. Recipient fee**
Bank payment	31.5$ (6.3%)	Free (depending on if costs are split the parties)
Layer 1 blockchain	~1.41-11.99$*	Free
Layer 2 OR	~0.04 - 0.35$*	Free
Layer 2 ZKR	~0.04 - 0.34$*	Free

Figure 32: Fees of Remittance Transfers of $500. Source: Own Contribution & World Bank (2022)

In comparison, there is a strong incentive to adopt stablecoin payments to send cheap cross-border payments. A final and perhaps most efficient use case of stablecoins would be for firms conducting several cross-border bank transactions, such as charities. Because blockchain technologies do not discriminate the transactional amount, a 1,000,000$ stablecoin transaction will come at the exact cost of a $1 transaction.

5.2.2.9.1 Security and Transaction Finality Comparison

One of the key discussion topics of alternative transaction systems is trusting the security, reliability, and finality of transactions. A side-by-side comparison of the different payment methods is illustrated below.

	Platform	Transaction verification proof	Transaction finality	Transaction reversibility before finality	Transaction reversibility after finality
Cash	n/a	Instant	n/a	n/a	n/a
Wire transfer	Swift	Instant	~ 0-3 days	Easy	Difficult
ACH	Visa	Instant	~ 0-3 days	Easy	Difficult
Layer1 blockchain	Ethereum	Instant	~ 16 min	Difficult	Infeasible
Layer 2 OR	n/a	Instant	~ 7 days	Difficult	Infeasible
Layer 2 ZKR	n/a	Instant	~ 36 min	Difficult	Infeasible

Figure 33: Security, Reliability and Finality of Payment Methods. Source: Own Contribution & AFP, 2022; Burger, 2022; Etherscan.io, 2023a, 2023b; Goldberg, 2022; optimis-tic.etherscan.io, 2023; Snyder, 2023; Worldbank.org, 2022; Xangle, 2022; zksync.io, 2022b)

The reversibility of bank payments can be considered relatively easy as they are not carried out immediately, perhaps days later, unless the recipient account is under the same bank (Danmarks Nationalbank, 2018). Furthermore, the reversibility of physical debit card transactions is considered easy in most developed countries with the new debit card “tap & go” function, giving the impression of a trusted transaction without providing proof of identity in the form of a pin code. Therefore, were a transactor to call their card provider or bank and tell them that they did not engage in this transaction, it would be annulled in most cases, as the investigation cost would often be higher than the transaction itself for smaller amounts. If a transaction has been cleared using traditional payment methods, only the bank can reverse it, which is deemed difficult unless a dishonest actor has a trusted position with the bank.

On the contrary, reversing a simple stablecoin payment on either the Layer1 or Layer2 blockchain network before finality would firstly require a high degree of computer proficiency, coupled with a trusted position in the execution layer and consensus layer of the given blockchain network. Such

an action would be extremely difficult and resource intensive. Secondly, it would serve against the transactors' best interest as they would stand to lose their trusted positions and economic resources staked. Finally, attempting to reverse transactions after global consensus finality on a blockchain would be computationally infeasible due to the blockchain's immutability guarantee.

Stablecoins have long served as transitional currency for actors speculating in volatile cryptocurrencies. However, within the last year's realizations of scaling an established decentralized blockchain like Ethereum through Layer2 rollups, transactions of stable cryptocurrencies can now be realized at a fraction of the cost previously, with hardly any security compromises. This enables stablecoin transactions to be carried out with comparable transaction speeds and costs.

As concluded from the Blockchain and Scalability sections, Ethereum, as a decentralized blockchain protocol, has extraordinary security measures that make it seemingly economically unprofitable to attempt dishonest behavior. However secure as the Proof-of-Stake consensus mechanism may seem, it has only seen real stress testing in the past six months. Therefore, questions could be raised about potential weaknesses the PoS protocol might have that are yet to be explored, contrary to an established consensus mechanism like the PoW protocol. One thing that certainly plays in Ethereum's favor regarding security is the significant amount of capital invested in its local currency ETH. High ETH capitalization would make it very unlikely for an attacking actor to acquire more than 50% of stakes in an attempt to extract block transactions for personal gain.

5.2.3 Summary of Technological Factors

Using stablecoins for everyday retail purchases would require gas cost demand for block capacity that large blockchains like Ethereum cannot meet. As a result, gas prices nominated in ETH have been rising to points where the cost of small transactions conducted on the blockchain could be more than the transactional amount. Changing the block capacity to meet said demand only happens in small increments, as great scaling efforts will risk compromising the security and decentralization of the blockchain.

The most gas-cost-intensive action on blockchains is transaction execution by the virtual machine (recall the execution layer). Therefore, moving the execution layer of transactions off-chain to Layer2, will enable leverage of the capacity of each block on a blockchain like Ethereum. This is

because the blockchain consensus layer will only serve the purpose of validating the correctness of the transaction data and storing it safely on the blockchain.

In analyzing the Layer2 scaling solutions: Zero-knowledge and Optimistic rollups (ZKR and OR). Each rollup technology was dissected and analyzed to determine how their use would impact stablecoin transactions. The theoretical transaction throughput on the Ethereum blockchain can be scaled from 19 stablecoin transactions per second (TPS) to 4622 TPS and 912 TPS for ZKRs and ORs, respectively. Each rollup offers instant verification of the executed transaction, but they differ in finality times. ZKRs will have finality in around 36.5 minutes, ORs will have soft finality after around 5 minutes, and hard finality in around 7 days. As for the risk of holding funds on each rollup, ZKRs appear to have a slight edge over ORs. ZKRs rely on zero-knowledge proofs, which are computationally infeasible to falsify. Due to both technologies' early stages, new implementations to both Layer1 and Layer2 might change these estimates and results in the coming year.

By estimating the stablecoin transaction fee formulas for both blockchain Layer1 and Layer2, it was illustrated that the two cost drivers, ETH/USD price and ETH gas prices, each impacted stablecoin transaction costs on both layers when holding all other variables fixed. With economic reasoning and these two graphs in mind, it could be deduced that if demand for ETH remained unchanged, the relative transaction costs in USD would increase over time due to ETH supply being deflationary. As stablecoins are pegged to fiat currencies like USD, this would mean an expected increase in future transaction costs. These transaction costs are likely to periodically decrease with capacity expansions and technological advancements in the capacity and technological advancements within the blockchain space until demand catches up again.

Lastly, estimated stablecoin transaction costs when conducted on Layer1 and Layer2 were calculated for Q1 2023. These estimates were compared to traditional payment systems such as ACH and wire payments to illustrate the areas where stablecoin payments were competitive. The comparison intentionally omitted vital cost components, such as bridging and exchange costs, to only compare technological differences and not the barriers of entry to each system. What is worth

highlighting from this comparison is mainly stablecoins transactions, outperforming traditional payment systems in the areas of cross-border payments and payments of large transaction amounts. As for speed and transaction finality, both blockchain and traditional systems will each have advantages in particular scenarios.

5.3 Political Factors

This part of the analysis will turn to the political and economic implications that stablecoins may be exposed to. The rising capitalization of stablecoins have been subject to much debate especially in how they should be used in a macroeconomic context. In this part we shall study how a rise in unregulated stablecoin use may bring negative externalities to economies and which efforts policymakers can make to regulate them in an optimal way.

5.3.1 Macroeconomic Implications

The growing interest in stablecoins may bring negative or unprecedented externalities to the economy of countries. This is an important aspect to consider when assessing the implementation of stablecoins, as not only can stablecoin holders be affected by unintended economic consequences of a growing adoption of stablecoins. Therefore, policymakers may need to regulate the use of stablecoins and other crypto-asset to control economic growth and stability. This poses a risk for holders of stablecoins, since regulation might limit the possibilities of utilization. Thus, we shall now study the macroeconomic implications of stablecoins on both a global scale and a more local perspective. To grasp the economic implication, we will first study the instruments that policymakers have to regulate the economy and hereafter turn to how stablecoin may set some of these instruments out of effect.

5.3.1.1 Monetary Policy

To ensure overall economic growth, countries, or economic unions such as the European Union have monetary policy instruments to control the money supply. The money supply in an economy is a significant factor for output, inflation rate, exchange rate, and unemployment rate. A central bank typically operates with three essential tools: ' open market operations' (OMO), the discount rate, and reserve requirements. Central banks can use OMO to manipulate the money supply within an economy by buying or selling bonds in the bonds market (Blanchard, 2017). If the central bank wants to increase the money supply in the economy, it will buy bonds. By buying bonds, the central bank takes money out of the economy and increases the money supply, Also known as an expansionary open market operation.

Conversely, the central bank can sell bonds and, in this way, decrease the supply of money, which is called a contractionary open market operation. Along with OMO, central banks can control the money supply through the discount rate. When the money supply in a country is too high- often characterized by a high inflation rate. Central banks may adopt a contractionary monetary policy by increasing the discount rate. By raising the discount rate, agents within the economy will have less incentive to hold cash, and the money supply will go down. Assuming that money is non-neutral in the economy, the output can increase by lowering the discount rate.

5.3.1.2 Implications of Stablecoins on Monetary Policy Transmission

We have previously studied the dominance of asset-backed stablecoins pegged to the US dollar measured in market capitalization. Four of the five biggest stablecoins have some liquid backing and are all pegged to the US dollar. This dominance can be a problem for economies outside of the US. The accessibility of crypto-transfers through blockchain networks proves attractive for countries with weak financial infrastructure. Here, both transaction speed and cost may be less than transferring through conventional methods.

5.3.1.2.1 Adoption of Crypto-currencies in Emerging Markets and Developing Countries

One of the more extreme examples was when El Salvador, in 2021, made Bitcoin a legal tender within the country (Arslanian et al., 2021). The policy implementation was criticized by global economic institutions such as IMF, while the World Bank initially refused to help. One of the primary motivations for this move was the improved efficiency of international remittances that Bitcoin can provide. In 2021, personal remittances accounted for over a quarter of the country's GDP making money transfers from workers in foreign countries instrumental for the economy (World Bank, n.d.). Additional motivation for El Salvador to adopt Bitcoin is that approximately 70 percent of the population does not have access to a bank account (Arslanian et al., 2021). Here, the promises of financial democratization of decentralized finance have proven intriguing, where the population can access financial services directly on their mobile phone or other devices with a network connection.

5.3.1.2.2 Dollarization

Another reason for El Salvador to adopt Bitcoin was the high reliance on the US dollar in the economy (Arslanian et al., 2021). Exactly this dependence on the dollar or other major fiat currencies is known throughout the world where countries have huge reserves in foreign currency or even

use it as a primary medium of exchange (Blanchard, 2017). Dollarization is the phenomenon when countries use the dollar as a substitution for local currency or in addition to it. It can happen through policy to handle uncontrollable inflation, or it can be adopted over time by market participants making the dollar a 'de facto' official currency.

Though the adoption of foreign currency can be helpful to ensure economic stability in the short term there are certain caveats to be aware of. By adopting the US dollar as a legal tender in a country the policymakers are giving up significant control of the monetary policy within the country. This means that the economy is giving up its ability to control the supply of money and effectively handing over the control to the US Federal Reserve. Obviously, this can be problematic as the American central bank has a primary interest in the American economy and thus interest rates set by them could out of line with the needs of a dollarized economy.

In a report by World Economic Forum (2022), the concern of global fiat-backed stablecoins' effect on dollarization is raised. As studied earlier in the paper in this assessment, a key property of money is its ability to store value. In countries with high inflation rates individuals will be tempted to hold their liquid assets in a more stable currency such as the dollar. For countries with a less developed financial system, the introduction of stablecoins may gain them easier access to hold other currencies besides the local one (Feyen et al., 2021). With a heavy adoption of a stablecoin backed by a foreign currency, local policy-makers may gradually lose monetary control subconsciously while the economy gets impacted by misaligned monetary policy.

5.3.1.2.3 Impact on Larger Economies

The high concentration of dollar-pegged stablecoins in the market should also raise concerns for developed economies. Economies outside the US borders could fear that the features of the technology and concepts behind cryptocurrencies and stablecoins will encourage people to adopt stablecoins despite having a stable local currency. In this case, some of the same consequences for monetary policy can also occur. Though the adoption of dollar-pegged stablecoins should not affect the ability to do monetary policy in the United States, some negative externalities could still arise. With the growing market capitalization trends of fiat-backed stablecoins, an increase in the reserve backing the stablecoin should also be expected. With the reserve building up, chances of expansionary monetary effects increase if high amounts of stablecoins are redeemed too quickly.

Redemption of stablecoins will typically happen if holders cannot sell their stablecoins in exchange for a value corresponding to the peg.

An unforeseeable side effect of asset-backed stablecoin issuers contributing to inflation might also raise concerns from policy-makers. Such inflationary effects might be attributed to stablecoin issuers minting an equivalent amount of stablecoin currency as is in their reserves. However, as we previously learned, the currency in stablecoin-issuers reserves is not necessarily removed from the economy. Some significant percentages of the issuers' holdings are invested in various assets, contributing to a double-spending impact on the economy effectively giving the stablecoin users the same possibility to create representative as commercial banks.

5.3.2 Market Integrity and Money Laundering

In traditional money transfers, it has been the job of banks and financial institutions to ensure that funds have not been gained through criminal or dishonest offenses. As a tool to enable such assurances, two legal protocols have been set in place, known as “Know Your Customer” (KYC) and “Anti-Money Laundering” (AML). KYC is conducted when a client plans to get financial services from a bank or financial institution. Here, the clients must provide the institution with the necessary information, such as proof of identification. AML is a set of regulations and procedures to ensure that illicit funds do not appear legal through transfers to legal institutions (Montevirgen, n.d.).

As unregulated crypto-asset trade can create money laundering possibilities, policy-makers must set policies to regulate such actions. Though stablecoin transfers are decentralized from conventional financial institutions, it is necessary to set standards for entities that provide crypto-assets for currency exchange services. These standards include crypto-exchanges but also issuers of stablecoins. For example, in the case of Tether, a user who wishes to deposit cash or redeem tokens must pay a verification fee for Tether to verify the user’s identity (Tether, n.d.). It may be that both issuers and other exchange providers have verification processes in place, but it does not mean that they comply with the same standard of KYC and AML that traditional transfers do. Hence, policy-makers must set clear regulatory frameworks to accommodate the risk of money laundering that stablecoin transactions possess.

5.3.3 Regulation of Stablecoins

Several regulatory concerns arise with the increasing popularity of stablecoins, as previously presented. Since crypto-currencies, including stablecoins, are a relatively new phenomenon in the world economy, governments and international organizations are still developing regulations for issuing and using stablecoins. Since international regulation is not in place, we shall study recent developments and considerations for regulating stablecoins. Due to space limitations, the focus will be on the EU regulatory framework "Markets in Crypto-Assets". The intention of this section is not to state all laws and legislative proposals regarding stablecoins but instead to understand how regulations may develop and how they may limit the opportunities of stablecoins.

5.3.3.1 The Markets in Crypto-Asset Framework

On the 20th of April 2023, the Parliament of the European Union passed the Markets in Crypto Act (MiCA), making it the most comprehensive regulatory framework for digital assets such as stablecoins to date (Browne, 2023). The act is expected to come into effect within the European Union in 2024. Since the framework is the first of a kind in terms of scope and ambition, countries outside of the EU are expected to make regulatory actions inspired by the MiCA framework (Zhang et al., 2022).

Actors affected within the stablecoin-ecosystem can be defined as the issuers of the stablecoin, crypto-asset service providers, and persons who are or wish to engage in stablecoin trading on authorized crypto-asset service providers (Clifford Chance, 2022). All stablecoins are not met with the same regulations and requirements. In the proposal made by the Council of the European Union, stablecoins are not categorized in the same way as presented earlier by Burke (2023). Instead, MiCA distinct between crypto-assets and defines three different classifications in the following way:

1. **Electronic Money Tokens (EMT):**

   A category of crypto-assets "…*that aim at stabilising their value by referencing only one official currency*" (Council of the European Union, 2022, p. 13). Their primary purpose is to be used as a means of payment while sustaining a stable value. The way of obtaining stability is through a reserve of the same currency that the crypto-asset is representing, e.g., if a stablecoin is pegged to the Euro, it should only be backed by a reserve of Euros (King, 2022). EMTs do not necessarily need to be in Euros, but the most important thing is that the currency that the EMT is representing should have a reserve of the same currency. A simplification in Euro of

EMT is that 1 EMT is worth 1 Euro backed by 1 Euro. Compared to the definition of stablecoins earlier presented, only a part of the stablecoins in the 'asset-backed'-categorization can fit within the EMT definition. Thus, all 'on-chain collateralized' and 'algorithmic' stablecoins do not meet the criteria of EMT along with 'asset-backed' stablecoins with a reserve of commodities such as gold. On the other hand, fiat-backed stablecoins like Tether, USD Coin, and Binance USD may all very well qualify to be an EMT.

2. Asset-Referenced Tokens (ART)

The second category is defined as crypto-assets that "*aim at maintaining a stable value by referencing to any other value or right, or combination thereof, including one or several official currencies*" (Council of the European Union, 2022, p. 13). Like EMT, Asset-Referenced Tokens can also be pegged to a fiat currency, i.e., one ART representing the value of a dollar is worth one dollar. The difference between the two is the composition of the reserve backing the crypto-asset. The reserve of an ART can consist of more than one fiat currency, one or more crypto-asset(s), or one or more other asset(s). A simple definition is that an ART is a crypto-currency that tries to hold a stable peg to a fiat currency by holding a reserve that includes assets other than the fiat currency it represents. Commodity-backed stablecoins and on-chain crypto-collateralized stablecoins could qualify for this definition.

3. All Other Crypto-Assets

Crypto-asset not falling under the two first definition belongs to the 'all other crypto-asset'-categorization. Crypto-assets that do not fall under the categories of Burke (2023), including crypto-currencies without a peg, e.g., Bitcoin and Ether, are also included in this category. The classification does not apply to most non-fungible tokens (NFT) types.

5.3.3.1.1 Implications For Issuers of All Crypto-Assets

Regardless of crypto-asset type, all issuers of crypto-assets launched after MiCA is in effect should comply with three major conditions. These conditions are obligatory for selling tokens to EU citizens or getting listed on an EU exchange (King, 2022):

1. The issuer must register an entity.
2. The issuer must publish a whitepaper explaining the project.

3. The issuer must submit the whitepaper to the National Competent Authority in the country of which the issuer is registered and not have it rejected.

An essential aspect of the regulation is that this only applies to new projects launched after MiCA is in effect. This means that stablecoins already offered are not affected by this new regulation. Nevertheless, issuers of stablecoins already offered should not disregard this new regulation, as MiCA could expand to set similar conditions for these projects (King, 2022).

The whitepaper must contain all relevant information about key persons involved in the project along with details in the economic model and the technology that the project relies on (e.g., what consensus mechanism is used). Moreover, the issuer's responsibilities should be stated, as well as the rights of the buyers of the assets. To a certain degree, all stablecoins mentioned in this paper comply with these conditions for a whitepaper. However, one should know that under MiCA the whitepaper is a legally binding document and not just a detailed description of the project.
Smaller projects that lie outside the scope of this thesis, like ones with a total value of less than 1 million EUR, do not need to comply with the third condition. On the other hand, a project can be deemed 'significant' if it is too extraordinary in terms of size. Implicitly, the project is no longer regulated nationally but by a European regulator. These projects should meet criteria such as "*large customer base, a high market capitalization, or a high number of transactions*" (Council of the European Union, 2022, p. 29). The exact thresholds for these criteria are not clarified in the proposal. King (2022) however estimates among the criteria that the total value of tokens issued should be greater than 1 billion EUR. For reference, the six largest stablecoins measured on market capitalization have a market cap of well over 1 billion EUR. Due to the risk such projects can impose on monetary policy transmission and financial stability, they will be met by even more stringent regulation. Regulation implies EU interference with the issuing company's risk management policies and internal remuneration. As a result, new stablecoin projects that aim to compete with the market's incumbents face greater regulation and monitoring than their established competitors.

5.3.3.1.2 Regulations for Stablecoins (EMT and ART)

Since EMTs and ARTs have their value backed by a reserve, these assets can pose a greater risk to the financial and macroeconomic concerns stated earlier in the analysis. Thus, issuers of

stablecoins must hold a liquid reserve equivalent to the value of tokens currently in circulation (King, 2022). This is a crucial part of MiCA that is non-negotiable and will be monitored and audited frequently once the regulation is in place. Furthermore, with this regulation, algorithmic stablecoins are banned within the EU as they, per definition, do not have a liquid reserve (Legal Nodes, 2023). Moreover, it is not allowed to grant interest to users for holding ARTs or EMTs (Council of the European Union, 2022).

5.3.3.1.3 Specific Regulations for Issuers of EMT

For EMT, specific regulations apply on top of the aforementioned. These specific regulations are generally more stringent than the rules of ART. Regulation only apply to EMTs offered within the EU. However, if an EMT references a union currency, it is automatically deemed to be offered in the EU. Furthermore, the issuance of EMT is only allowed through EU credit institutions and electronic money institutions authorized by the E-money directive. So, in order to qualify for admission to EMT trading an issuance within the EU, an issuer must be licensed as a credit institution. Another entry barrier for EMT-issuers is the 350.000 EUR initial capital requirement. Issuers of EMT will also need to keep their corporate capital at a ratio of 3% of the total reserves that backs the tokens on issue. Besides the capital requirements, issuers will be subject to strict rules regarding safeguarding the funds received for tokens.

To accommodate risks of dollarization in the EU, EMTs denominated in a currency that is not an official EU currency are only allowed to have an average daily transfer volume of 1 million EUR (Beck et al., 2022). This volume cap does not apply to all types of transactions, only when the EMT is "*used as a means of exchange*" (Council of the European Union, 2022, p.45). This gives some breathing space for heavily traded stablecoins such as Tether but most likely limits their abilities relative to traditional means of payment or transaction.

5.3.3.1.4 Specific Rules for Issuers of ART

ART is less regulated compared to EMT but do still have some specific rules that issuers need to comply with. Issuers of course need to comply with the rules stated earlier for all crypto-assets. Other than that, there is no requirement for initial capital, however corporate capital must be 2% of the reserve value or 350.000 EUR (depends on which is higher) (Zhang et al., 2022). Reserves must also be audited every six months to ensure that the issuer is compliant with the non-negotiable

condition that value of reserves should be equivalent to value of tokens in circulation. Must inform of transactions outside of the issuance of coins and transactions on exchanges. To reduce ART to become a store of value, it is not allowed to grant interest to users for holding ART (Council of the European Union, 2022).

5.3.3.1.5 Right of Redemption

A fundamental aspect of MiCA is the right of redemption that secures holders of runs on the stablecoin and enforces financial stability. The right of redemption applies to both EMT and ART and implies in its basic form that holders of stablecoins must be able to redeem their tokens free of charge (Ali & Piazzi, 2022). Still, the right of redemption differs from EMT to ART. EMT holders are "*…always provided with a claim on the electronic money institution and have a contractual right to redeem their electronic money at any moment against an official currency of a country at par value with that currency*" (Council of the European Union, 2022, p. 14). Thus, holders of EMT have a claim and can always redeem their tokens for a value equivalent to the holding, which is provided by the non-negotiable liquid reserve requirement.

For ART, holders do not have a direct claim. However, ART issuers "*…should provide a permanent redemption right to the holders of the asset-referenced tokens, in the sense that holders are entitled to request from the issuer the redemption of the asset-referenced token at any moment.*" (Council of the European Union, 2022, p. 28). Here, the issuer can either fulfill the redemption by refunding in fiat currency equivalent to the value of the redeemed amount of tokens or delivering back assets of the reserve corresponding to the value. For ART, issuers must provide explicit information on the process and redemption methods in the whitepaper.

5.3.3.1.6 Right of Withdrawal

Retail token holders have the right to withdraw their purchase of crypto-assets from the issuer within 14 days. Analogously with the right of redemption, the holder must be able to withdraw and get funds refunded without having to provide an explanation or incur any costs (European Parliament, 2023). Once a token is listed on an exchange, the right of withdrawal will no longer apply (King, 2022). Hence, issuers can end up in a situation where they have raised vast amounts in the pre-sale of a coin before entering the market and then end up in a situation where significant amounts of tokens are returned shortly after. This can pose a new risk for new issuers and may be a motivation to have significantly higher start-up capital compared to earlier initiated

projects. Below is a comprehensive comparison of the differences in regulation between ARTs and EMTs, to sum up the regulations stated above.

Classification	**EMT**	**ART**
Definition	Reserve of a single fiat currrency	Reserve of other assets or more than one single fiat currency
Examples of stablecoins that may qualify	Tether & USD Coin	DAI & PAX Gold
Who can issue?	Authorised credit institution or e-money institution	Entitys complying with the obligatory MiCA conditions
Initial Capital Requirement?	Initial capital requirement of 350.000 EUR	No
Threshold of daily transaction volume value	200 million EUR (1 million for tokens not referencing a EU currency)	200 million EUR
Requirement of corporate capital?	3% of reserve value	2% of reserve value or 350.000 EUR (the highest)
Monitoring of reserve	Stringent rules comlying with the EBA	Audit every sixth month
Rights of redemption	Yes	Yes
Direct claim by holders against issuers?	Yes	No

Figure 34: Comparison of Regulation of ERT & ART. Source: Own Creation

5.3.3.1.7 Crypto-Asset Service Providers (CASPs)

In regulating stablecoins, professional entities that provide services concerning crypto-currencies in the EU play a key role. Such entities are named Crypto-Asset Service Providers (CASPs) in MiCA and are defined as a "… *legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis, and are allowed to provide crypto-asset services*" (Council of the European Parliament, 2022, p. 57). Crypto-asset services include (Council of the European Parliament, 2022):

- Custody and administration of crypto-assets on behalf of third parties:
- Operation of a trading platform for crypto-assets:
- Exchange of crypto-assets for funds
- Exchange of crypto-assets for other crypto-assets
- Execution of orders for crypto-assets on behalf of third parties
- Placing of crypto-assets
- Providing transfer services for crypto-assets on behalf of third parties

In general, CASPs must be authorized in the EU and have a legal address within one of the member states to provide crypto-asset services as described above. An implication of this is that CASPs must have a registered office in the EU, with one of the directors of the CASP being a resident of one of the EU countries (Ali & Piazzi, 2022). This does not apply to already registered entities such as credit institutions and investment firms. CASPs also have a general obligation to act "*honestly, fairly, and professionally in the best interest of their clients*" (Council of the European Parliament, 2022, p. 36) to ensure market integrity, financial stability, and consumer protection. Because of this marketing efforts of CASPs must not be misleading or unfair (Ali & Piazzi, 2022). Furthermore, CASPs are obligated to inform their customers about the environmental impact of the consensus mechanism[13].

Like crypto-asset issuers, CASPs are also met with a corporate capital requirement. The requirement depends on the service type provided but will be a minimum 50,000 EUR for all CASPs. Crypto exchanges will need to have capital of 150,000 EUR, while CASPs offering crypto-for-crypto or crypto-for-funds exchanges and custody services will need to have 125,000 EUR in capital. CASPs that provide other services will only need 50,000 EUR (Ali & Piazzi, 2022).
CASPs will also need to take serious measures in safekeeping the ownership rights of their client. CASPs are in no way entitled to use the crypto-assets held for their own account and are required to keep them separate from accounts used to hold funds belonging to the CASP.

Significant for MiCA are the regulations for the governance of CASPs. Members of the management of a CASP must have a good reputation and be assessed to have sufficient knowledge and skills within the field of operation (Ali & Piazzi, 2022). Management of CASPs is also required to "*... assess and periodically review the effectiveness of the policies arrangements and procedures put in place to comply with the obligations*" (Council of the European Parliament, 2022, p. 200). Besides being transparent with the compliance of MiCA, CASPs will also need to be transparent with complaints received (Ali & Piazzi, 2022).

[13] Primarily refers to PoW. PoS uses around 0.01% of the energy that PoW consumes. For reference see Appendix VI.

The European Securities and Market Authority (ESMA) will update a register of non-compliant entities providing crypto-asset services. This register will be updated regularly and is available to the public on the ESMA website (Council of the European Council, 2022). Importantly, this law will not apply to transactions without a service provider. Therefore, it will be possible to circumvent the regulations by doing person-to-person transactions through self-hosted wallets, such as personal digital wallets where the user administers the secret key without interference from intermediaries (European Parliament, 2023).

5.3.4 Central Bank Digital Currency

The growing interest in privately issued digital assets, such as crypto-currencies like Bitcoins, Ether, and various stablecoins, has seen central banks develop innovative ways to gain better control of digital currencies. As of now, 87 countries worldwide, accounting for more than 90 percent of the world's GDP, are exploring the possibility of implementing a digital currency issued by the central bank (McKinsey & Company, 2023). The term "Central Bank Digital Currency" (CBDC) defines the appearance of a centralized digital currency system. CBDC is a digital central bank-issued and operated fiat currency not pegged to any physical asset or commodity. In the same way as fiat currency, CBDC is a liability of the central bank available to the public. In most countries, a full-scale implementation of CBDC is yet to be seen, but developments within the field should not be underestimated. In Europe, CBDC achieved recognition in October 2021 when the European Central Bank initiated an investigation of an eventual European CBDC (ECB, n.d.). This section investigates the incentives behind a CBDC, proposed approaches, and how CBDC may differ from stablecoins.

5.3.4.1 Motivation for CBDC

The rapid rise in the development of CBDSs worldwide is not to be underestimated. Let us dive deeper into why many central banks consider implementing a CBDC. CBDCs possess many of the same traits as stablecoins but are more centralized by nature. An introduction of CBDC can, first of all, be a digital alternative to crypto-currencies. As mentioned earlier in the paper, stablecoins can have negative consequences on a macroeconomic level if their regulation remains unchanged. A report on CBDC published by the US Federal Reserve states: "*In our rapidly digitizing economy, the proliferation of private digital money could present risks to both individual users and the financial system as a whole. A U.S. CBDC could mitigate some of these risks while supporting private-sector innovation.*" (US Fed, 2022, p. 14-15). Central banks recognize the need for

innovation in transactions but fear the consequences of private agents mitigating the issuing of digital money.

In most countries, cash is the only central bank money available to the general public (US Fed, 2022). The use of cash as payment has decreased dramatically over the past years, especially in Europe, where it has decreased by one-third between 2014 and 2021 (McKinsey & Company, 2023). Due to this development, individuals now use digital payment methods with higher credit or liquidity risks than CBDCs would have. Creating a CBDC will allow central banks to give the public access to central bank money, increasing the use of central bank money in payments and transactions. With higher use of digital fiat currency, central banks can provide a more inclusive system where people without bank accounts can make online transactions and cross-border payments.

5.3.4.2 Types of CBDCs

There is no clear-cut definition of a Central Bank Digital Currency other than what the name suggests. Thus, the design CBDCs can vary significantly from central bank to central bank, depending on the needs of the country's economy. Schär (2021) identifies three significant design dimensions for CBDC:

- Centralized vs. Decentralized:

  Which type of technology is used? How much control does the central bank have?
- Retail vs. wholesale:

  Is the digital currency for public to buy goods with or is it only for selected companies as form of settlement coin?
- Token-/object vs. account based:

  How is the token held? Can it be stored on private wallets or only with authorized banks?

To comprehend how CBDCs may threaten stablecoins, we will now investigate some use cases of CBDCs. Since many projects are far from finished, we will first focus on China, that have implemented a CBDC, and then move on to the suggested frameworks for Australia, which is still in an investigation and development phase.

e-CNY

In 2019, China launched its first pilot for its central bank digital currency, “digital Renminbi” or e-CNY (Conrad, 2022). During the past years, e-CNY-pilots have been slowly rolled out in larger cities all over China. e-CNY is issued by China's central bank, the People’s Bank of China (PBOC), and is designed to have the same value as its physical cash counterpart Yuan. The digital currency is intended for retail payments for businesses and consumers. Unlike most stablecoins, e-CNY does not run on distributed ledger technology or blockchain. The PBOC argues that the reason for the rejection of blockchain technology is due to its disability to handle the transaction volume they expect (Chorzempa, 2021). Just as physical currency is not distributed directly from the central bank to the consumer, neither is e-CNY. The e-CNY ecosystem is built on a “two tier-system” where commercial banks are a form of intermediate link between the consumers and the PBOC.

To hold e-CNY, users must have a digital wallet applicable to the digital currency. These wallets function similarly to bank accounts and are only available in larger banks in China (Deutsche Bank, 2021). When the user has set up a digital wallet in the bank, she can use the e-CNY as payment. Holding e-CNY in a digital wallet does not earn any interest and can thus be equated with having cash in a physical wallet. These retail payments will be handled by the bank where the wallet is set up and other banks and payment services similar to Visa or Mastercard payments (ACH). With this structure, most responsibility is given to the banking institutions that need to comply with regulations in terms of privacy, AML protocols, and KYC.

In general, the ecosystem is comparable to the money ecosystem seen in most countries where financial institutions play a significant role in distributing money. A key difference for e-CNY is of course its digital nature that can allow public institutions to gain more control and information regarding transactions and flows of money in China.

eAUD

The Reserve Bank of Australia (RBA) is exploring the possibilities of a central bank digital currency in Australia through a pilot project called eAUD. The pilot project consists of a CBDC platform that will run on the Ethereum platform on a permissioned network (Quorum). Prior research on digital currencies in Australia has revealed that a use case for retail payments is not currently

suitable for the Australian economy. Instead, RBA has found CBDC to have potential within wholesale due to smart contracts' advantages to payments and transactions. Like the e-CNY, the eAUD will be a liability of RBA and be worth the same as an Australian Dollar. Nevertheless, similarly to e-CNY, holding eAUD will not earn the holder any interest (RBA, 2022).

The ecosystem is created via four types of agents: RBA, 'use case providers', KYC providers, and end-users. Central in the pilot are so-called 'use case providers' who are market participants approved by RBA for the pilot. The use case providers can access the eAUD platform through the Application Programming Interface (API) and smart contracts (recall Application layer). This platform will manage the balances and transactions of eAUD. Use case providers are then responsible for developing platforms to distribute the eAUD to the end user. Finally, before end-users can hold eAUD, they must engage with a KYC platform created by the use case providers or an independent KYC provider (RBA, 2022).

The holding structure of eAUD is still to be determined, but three approaches are currently being discussed depending on the role the use case providers should play in the system. In the first approach, eAUD is a direct liability of the central bank to the end-user, where the end-user has the individual holding on the ledger. Here, the end-user has complete control over the secret key. In the second approach, eAUD is also a direct liability of RBA to the end user, but here, the use case providers control the individual holdings on behalf of the end user. Finally, in the last approach, the eAUD will be liable to the use case provider who holds a combined pool on behalf of users with an indirect claim on eAUD for the users (RBA, 2022).

5.3.4.3 How are CBDCs Different from Stablecoins?

Comparing stablecoins to central bank digital currency can be difficult because none of the entities are fully defined. Moreover, both stablecoins and CBDC vary significantly in design and purpose. While CBDC can be perceived as a way for central banks to compete with privately issued crypto-assets, they pose a solution to different problems.

The most glaring difference between stablecoins and CBDCs lies with the issuer and the backing of the token. Stablecoins are backed by either a reserve of assets or an algorithm, and CBDC is fiat

currency with a government backing it. Since CBDC is issued on par with traditional fiat currency, the value will always correspond directly to the value of cash. Consequently, CBDC has no volatility in value relative to the currency it is referencing. Moreover, CBDCs cannot be classified as crypto as they, per definition, are controlled by a central bank, meaning that they are centralized. Stablecoins are decentralized and have no central regulator. Unlike stablecoins, CBDC cannot engage with smart contracts on public permissionless networks, which implies that they cannot engage with decentralized financial services.

5.3.5 Summary of Political Factors

Using stablecoin in an economy can have several negative macroeconomic consequences for developed and developing countries. Most notable is the consequences that stablecoins can have on monetary policy transmission. Within lies the risk of dollarization that can undermine local monetary policy transmission. Both developed and developing countries can be victims of this. However, developing countries may have greater incentives to implement stablecoins in their financial system as the system may be underdeveloped. Asset-backed stablecoins can also influence a country's money supply if high volumes of tokens are redeemed simultaneously, which can lead to inflation. The decentralized system that blockchain provides also challenges market integrity, where it can be feared that stablecoins can be utilized in money laundering and financing terrorism.

Because of these risks, policy-makers will want to limit stablecoins in some respects. We have analyzed that policy-makers in the EU have introduced a local regulatory framework for stablecoins. Here, we looked at the “Markets in Crypto-Assets”-framework (MiCA) of the European Union to understand how stablecoin will be regulated within the union. If this legislation sets a precedent in other countries, it can have several implications for stablecoins. First and foremost, stablecoins will need a liquid reserve equivalent to the value of tokens in circulation to comply with the legislation, meaning that algorithmic stablecoins could be banned. In addition, issuers of stablecoins with a backing of the same fiat currency that it is referencing (EMT) will have to comply with very stringent rules, and they will need to be authorized financial institutions. Stablecoins with a different reserve composition will have less stringent rules but will still be impacted by the legislation. Notable for MiCA, is the regulation of trading volume, where all types of stablecoins will be capped when used as “a medium of exchange,” with the trading volume of stablecoins referencing foreign currency being limited the most.

In many countries, central banks are either implementing or discovering the possibilities of implementing a digital fiat currency or “Central Bank Digital Currency” (CBDC). Among the motivations for such an implementation is the wish to offer an alternative to privately issued stablecoins. One of the most significant CBDC projects is the e-CNY in China, where the system is designed especially for retail payments. Here, the CBDC is distributed from the Peoples' Bank of China to commercial banks where users can hold them. The Reserve Bank of Australia is currently piloting a CBDC focusing on wholesale transactions. Unlike e-CNY, the holding and distribution system is still under development, underlining the differences CBDC can have in design. While one of the main motivations of a CBDC implementation may be to reduce the use of stablecoins, it is vital to notice that the two have significant differences. One of the major differences is in the backing, where a CBDC is a fiat currency, and reserves or algorithms are backing stablecoins. Another key difference is in technology, where CBDCs can run on blockchain but only private ledger system, which disables them from interacting in the crypto-ecosystem.

6 Discussion

6.1 Are stablecoins money?

We have previously studied the three properties of money, which now enables us to discuss whether stablecoins can be characterized as money and the problems of such characterization. It must be a store of value, a medium exchange, and a unit of account. We shall now discuss the three properties concerning stablecoins to establish how they compare to money.

6.1.1 Stablecoins as a Store of Value

Based on the analysis three factors that can have implications for stablecoin to be a store of value: The first is the ability to maintain the peg. The critical thing differentiating stablecoins from other crypto-assets is the price stability that they seek to maintain. If a stablecoin loses its peg, like in the case of TerraUSD, the stablecoin makes a lousy store of value. Through our literature review on stability, we have discovered that stablecoins cannot always maintain their peg and that we can falsify that stablecoins are stable in absolute terms (Baur & Hoang, 2021). However, the large capitalized stablecoins can still be categorized as relatively stable as historical prices have minor variances and lower volatility compared to assets other than fiat currency. Furthermore, the design of the stablecoin plays a role in stability, where we have seen that algorithmic stablecoin performs the worst regarding stability. Hence, not all stablecoins should be reckoned as a good store of value especially considering the large number of stablecoin projects that fail (Mizrach, 2023).
Incoming regulatory frameworks may also help stablecoins, in general, to become a better store of value. The MiCA framework in the EU will require higher standards for new stablecoin projects that can help stablecoins in general to be a better store of value. It will be required for all stablecoins to have a reserve of assets meaning that the most unstable design type, algorithmic stablecoins, will be banned for issuers and exchanges to sell. Furthermore, will the requirements of having a reserve value equivalent to the value of tokens on issue, along with the right of redemption, ensure that stablecoins can be perceived as a safe store of value.

The second factor is the asset that stablecoin references. Stablecoins referencing other assets that can be used as a store of value, like the US dollar, should have no problem with this property. However, if the stablecoin is pegged to a heavily depreciating currency such as the Argentinian peso, it would make a worse store of value.

The third factor is the storage possibilities of stablecoins. Storage possibilities of stablecoins can be done in two ways. The first is by holding a personal wallet, and the second is by holding the funds at an exchange. Storing stablecoins in a personal digital wallet enables users to interact directly with their stablecoin assets on the decentralized blockchains without intermediaries through the application layer. Furthermore, extraordinary cryptographic tools have made it virtually infeasible to access these assets through brute-force attacks. Implicitly, the security of an end user's assets is directly correlated with their steps to ensure the safe storage of their secret key and wallet passwords. A comparable example of this is for a person to have their assets in a secure vault at home, where if the key to the vault is placed carelessly, it will compromise the safety of the assets inside the vault.
Storing stablecoins at an exchange will mean surrendering direct control of funds to the exchange by allowing them to hold the secret key to the wallet. The stablecoin assets will be presented to the user as an "I owe you" (IOU) balance. The security of funds held on an exchange carries a risk related to the exchange fulfilling its promise of funds when needed. With the MiCA-act introduced, this risk can be significantly reduced as legislation requires exchanges and other crypto-asset service providers (CASPs) to take serious measures in safekeeping the stablecoins of the holders.

6.1.2 Stablecoins as a Medium of Exchange

Stablecoins are already functioning as a medium of exchange in the crypto-ecosystem where volatile crypto-asset are exchanged for stablecoins and vice versa. Therefore, this is the only market where stablecoins are entirely a medium of exchange. However, transactions outside of the crypto-ecosystem, including retail use, are still minimal, which can be due to several factors. Based on the analysis, we can also identify four factors behind this. The first factor is the short time that stablecoins have existed.

The first stablecoin was introduced less than ten years ago, which is a short time considering traditional ways of transaction. Companies and private actors are already significantly invested in traditional and may not consider the benefits of stablecoin to outweigh the costs of implementing stablecoins in transactions. Possible adopters may also be a victim of bounded rationality. They may not be able to comprehend the abilities of stablecoins or even be aware of stablecoins as a possibility of transacting.

The second reason is network effects. Stablecoins are used in the crypto-ecosystem because all agents have a place for storing and infrastructure to transfer stablecoins. However, exchanging fiat currency for stablecoins is costly, so it will be necessary to know that it is usable as payment. Hence, the implementation of stablecoins outside of the crypto-ecosystem is trapped in an equilibrium where it is not worth considering the implementation of stablecoins before others do.

Third is the complexity of the technology behind stablecoins. As we have discovered, blockchain technology is rooted in many complex concepts. The same can, be argued with centralized transaction systems entities such as digital bank accounts and credit cards. The critical difference in the need for knowledge about the system is the aspect of centralization. Users of centralized systems can learn the system to a low degree as the system is ultimately backed by a government through regulation. For blockchain, there is a higher degree of need to understand the security and safekeeping of assets. The system behind transaction costs and how they may change differs from traditional ones and can be difficult to grasp without a thorough introduction.

Fourth is the development of regulation. Many market actors may previously have been reluctant to engage with stablecoins due to regulatory risks that could undermine the value of stablecoins. With frameworks for regulation slowly flourishing, possible adopters will soon know the limits of stablecoins in a legal context. Because of this, the adoption of stablecoins may thrive under regulation. However, regulation may also limit stablecoins' ability to be a medium of exchange. Due to the risk of losing monetary policy transmission and dollarization, regulating bodies may adopt a framework similar to MiCA and limit daily transaction volume. Significantly, even stricter regulation regarding stablecoins that is not referencing a local currency can have several implications for stablecoins as a medium of exchange. A regulation like this will limit the emergence of a global stablecoin that could act as an international unit of account, where one token will become a default option when dealing with stable crypto-assets. Another aspect of such regulation will also limit the ability to become a medium of exchange as international transfers will become limited if many governments regulate stablecoins that reference a foreign currency.

6.1.3 Stablecoins as a Unit of Account

For stablecoins, the financial crypto-asset is often backed by other assets so that it is stable, unlike other volatile crypto-assets, e.g., Bitcoin or ETH. As a result, a stablecoin can be a safer store of

value and is, therefore, closer to being utilized as money. Hence, stablecoins are a compromise between traditional money and crypto-currencies. The unique advantages and features that stablecoin transactions functionally offer compared to traditional transaction systems can essentially be boiled down to the advantages of permissionless distributed ledger technologies. In answering this discussion, we will highlight some key aspects of blockchain technology that may make stablecoin superior to traditional money in the proper context.

6.1.4 Stablecoins and the NQA-Principle

An interesting approach to analyzing stablecoins as a form of money is through the NQA-principle (Gorton & Zhang, 2021). For money to fulfill the NQA-principle, it requires that all trade parties accept a form of payment without asking any questions or conducting due diligence on the value. When analyzing this principle, it would be feasible to compare it with other types of money. Money such as bank deposits is accepted because it is too costly to perform due diligence on the backing of the short-term debt that the bank is issuing. In addition, the less transparent or opaque the bank's assets are, the higher the cost of information, making the money more likely to be accepted. This acceptance is based on the fact that the bank's assets are regulated, and the receiver knows that the bank must comply with particular regulations to pay the debt.

For stablecoins, such regulation needs to be put in place, meaning that the backing of the stablecoin can be unreliable. In this case, it is profitable for the receiver to gain information about the backing before accepting. As an example, imagine a person receiving money through a bank transfer. Before the transfer, the receiver would never gain information about the bank from which the money is sent or the reserves it holds. Nevertheless, suppose a person would receive an amount of Tether in exchange for another asset. In that case, he might want to gain information about the protocols of the token, i.e., questions about how the Tether is backed, the composition of the reserve, and which measurements are in place in case of a run. This makes for an inefficient form of money. To combat this, stablecoin issuers must be extremely careful in explaining their protocols efficiently and transparently to minimize the costs of gaining information. This inefficiency could be helped by incoming MiCA regulation regarding the safekeeping of reserves, but a general trust and reliability of the backing be money years out in the future.

6.2 Why Use Stablecoins?

For stablecoins, the financial crypto-asset is often backed by other assets so that it is stable, unlike other volatile crypto-assets, e.g., Bitcoin or ETH. As a result, a stablecoin can be a safer store of value and is, therefore, closer to being utilized as money. Hence, stablecoins are a compromise between traditional money and crypto-currencies. The unique advantages and features that stablecoin transactions functionally offer compared to traditional transaction systems can essentially be boiled down to the advantages of permissionless distributed ledger technologies. In answering this discussion, we will highlight some key aspects of blockchain technology that may make stablecoin superior to traditional money in the proper context.

Programmable

As stablecoins are created through smart contracts minting them as a token existing on the desired blockchain, they are programmable assets by definition. This comes with opportunities that traditional payment systems cannot offer. One of them is the ability for a user to interact directly with a smart contract on the blockchain using a blockchain transaction. An example of this could be an autonomous hotel. To gain access to a room, one would have to send 100 Tether to the smart contract of the corresponding room. The smart contract would unlock the door, and the customer would gain access to the room where a key card would be inside so that that access could be gained repeatedly. Once the number of nights paid for has passed, the smart contract would have been programmed to revoke access to the key card. This feature decreases counterparty risks as the smart contract will serve as an intermediary, ensuring that both parties fulfil their promises.

Private

In recent years there has been an increased focus on securing the privacy of digital personal information, best depicted with the GDPR legislation introduced in the EU. However, privacy in transactions is lacking in most digital scenarios by today's standards. This can be argued as positive since it has contributed substantially to the fight against money laundering, rendering it more challenging to benefit from criminal activities. An opposing argument could also be made that whatever a person spends their money on is not the business of big data consumer analysis companies, insurance companies, and other third parties. Instead, it is the business of the two parties engaging in the transaction and their business only. In everyday retail purchases, one should not have to

reveal personal data to complete a purchase, just like a person does not have to reveal personal data when paying with cash. Using decentralized blockchains enables consumers to stay pseudonymous in transactions through their wallet address and only reveal their identity if they are required or voluntarily choose to do so. Here stablecoins enable this functionality of said decentralized blockchain without making too impactful changes to the medium of exchange, as they are purposefully kept to the same value as the currency they imitate.

Trustless

Decentralized blockchains are built as systems where one does not need a trusted intermediary to carry out a transaction. Their game-theoretical incentive structure is in the consensus layer built to detect and defer fraudulent transactions. This same consensus layer provides an immutability guarantee of transactions. For better or worse, once a transaction is recorded on the blockchain, it cannot be annulled or altered. This feature can be argued to benefit businesses rather than consumers. For example, consumers will no longer be able to annul payments with their bank for disputed transactions. It could also be argued that the judicial system's role is solving such disputes, not bank intermediaries.

Permissionless

Decentralized blockchains are permissionless. This comes with the benefit that anyone with an internet connection and a computer or smartphone can hold a digital wallet address that can serve the purpose of a bank account. In remote areas in less developed parts of the world, digital KYC can be less common, and banks can be few and far between. A functional alternative to send and receive a stable currency, like a stablecoin, is valuable to parts of the world with a financial sector not up to par with the developed world. Additionally, in countries where governments and centralized entities of power would use their position to censor transactions, stablecoins, as a stable asset that stores value, can be effectively used as a medium of exchange. As stablecoins exist on permissionless blockchains, they can be a reliable alternative to circumventing censorship. Thus, stablecoins and blockchain technology can create a more inclusive financial system where people are not required to have a bank account to perform transactions.

Borderless

A stablecoin, as a concept, will only have a relationship with the currency to which it is pegged. This relationship will have no implications for the technical functionality transactions. As stablecoins exist on decentralized blockchains that rely on p2p networks, the blockchain is as borderless as the internet. A transaction executed and recorded on a blockchain will not discriminate between being a cross-border transaction or a domestic transaction, nor will the transactional amount play any role in the transaction fee. By design, most blockchains will have their transaction fees decided by demand for block inclusion to keep the network traffic within the bounds of the network (block) capacity. This comes with the downside of less reliability in predicting future transaction costs. The upside is, however, a more fair and transparent fee structure compared to traditional means of digital payments, as blockchains are open source. At this point, transaction costs of cross-border payments using traditional means of payment, such are bank payments routing, will often require money to pass through several banks to get to its destination. This inefficiency is costly in both time and monetary fees, without even accounting for the additional costs of currency exchange fees. Using stablecoin transactions will only expose the sender to the transaction cost and the receiver to the spot rate exchange fee of the currency.

6.3 Can Stablecoins Co-Exist with CBDCs?

6.3.1 Decentralization May Be Stablecoin's Raison d'Être.

As we have seen from the design dimensions of CBDCs, central banks must choose the degree of centralization for the digital currency. CBDCs will arguably never become as decentralized as stablecoins that run on pseudo-anonymous permissionless networks. It would likely never be in a central bank's interest to issue money it cannot control to some degree. Imagine that creating a digital currency could help criminal activity by providing money as anonymous as cash but with better transaction options. Berentsen and Schär (2018) present a hypothetical example of an introduction of an anonymous CBDC made by the US Federal Reserve called "Fedcoin." Such an introduction would have huge reputational risk if such money were utilized in money laundering or financing terrorism. At the same time, banks would wonder why they should comply with AML/KYC regulations.

Because of these risks, it is seen as a fair assumption that CBDC will be somewhat centralized. The platform that a CBDC would rely on, might be with technology invented before the blockchain

or distributed ledger technology as for the case e-CNY. Alternatively, a CBDC with a DLT framework might share some features of decentralized blockchains but will differ in other aspects. A CBDC constellation using DLT would most likely entail a permissioned blockchain where one would have to register with personal information allowing the creation of a wallet address which is then attached to the KYC registration with a centralized entity. This way, the appearance of transactions and addresses would be as in a permissionless DLT, as users will have privacy through pseudonymity towards other users on CBDC-based DLT. This privacy will, however, not exist with the authority governing the DLT and the KYC register. Contrary to the traditional banking system, the complete transaction history of any user could be perfectly recreated with the click of one button. Hence, many existing users of stablecoins might not be intrigued by a CBDC as such an entity would not cover the ideological need for privacy in transactions that made them start using crypto-currencies in the first place.

Such a CBDC permissioned blockchain could solve many of the same inefficiencies highlighted for decentralized blockchains, such as borderless transactions, programmable money through smart contracts, and fees identical no matter the transactional amount sent. CBDC on a permissioned blockchain would also not have the same issues with capacity. As the decentralization of the consensus layer would not be of any concern, transactions could be handled by specialized supercomputers, thereby being able to scale the blockchain to instant transactions without the need for Layer2 scaling. However, with a centralized consensus layer, an immutability guarantee can never exist. Transaction history can be altered on a preceding block, and an identical chain can be built alongside the current one to be the new blockchain going forward. Such a scenario would make the central bank the de facto hegemonic power of the entire permissioned blockchain ecosystem on which the CBDC exists, which carries the risk of censorship for users.

CBDC May Be Superior in Retail and Wholesale

One foreseeable development of stablecoins could be their use in retail payments. As we have seen in the analysis, stablecoins can be a superior option to commercial bank money regarding transaction speed and costs in some cases. However, a CBDC may be equally fast, cheap, and the better option for the ordinary consumer or business, as seen in the context of the analyzed risk of stablecoins previously in the project.

First, stablecoins can be a risky asset to hold. Not only can the value of a position be volatile due to several external reasons, but it can also end up being worth nothing due to counterparty risk. For consumers who want to hold value in the form of money for retail purposes, a CBDC will undoubtedly be a safer and preferred choice. Since CBDC is issued as fiat money on par with physical bills, holders will not be exposed to the volatility of value relative to the national currency. Furthermore, money issued by a government would arguably have a lower default risk than money issued by private companies.

Another factor is the transaction costs. We have seen that the costs of transactions with stablecoins can be variable and fluctuate depending on the demand for block inclusion and the price of the local crypto-currency in USD. For a CBDC, it can be argued that it would be in the central bank's best interest to offer low and transparent transaction costs that should not be a concern for the users. Eichengreen and Viswanath-Natraj (2022) argue that the central bank could bear transaction costs through seigniorage profits, arguably making CBDC more competitive than stablecoins and other payment systems such as PayPal or Visa.

Dollar-pegged stablecoins dominate the stablecoin market in terms of capitalization and popularity. These dollar-pegged stablecoins with high capitalization also prove to be the most stable in terms of price volatility, which is why one could argue that these are the only ones to have some of the prerequisites to compete with CBDC in such an area. Consumers and companies with domestic transactions outside the United States will then be exposed to the risks of holding stablecoins and exchange rate risks, which domestic CBDCs effectively mitigate.

The novelty of the privately issued form of money that is stablecoins may also cause unpredicted regulations in the future that can limit the utilization of stablecoins for commercial use even further. However, with CBDC, consumers and firms will have considerably lower regulation risk. Furthermore, CBDCs may make compliance with KYC/AML regulations easier than stablecoins and reduce the chances of inadvertently participating in criminal activities.

Stablecoins Will Keep Their Relevance in the Crypto-Ecosystem.

Stablecoins distinguish themselves from CBDCs by existing on decentralized, permissionless blockchains rather than the possible scenario of a CBDC using centralized permissioned blockchains. The primary function of serving as a stable medium for crypto-currency trading that stablecoins currently fulfill on decentralized exchanges will remain the same. For this to be a scenario threatening stablecoin's position, it would require the interconnectivity (bridging) of a CBDC asset to a decentralized blockchain. On centralized blockchains, CBDCs could be challenging the position of stablecoins through simple debiting and crediting two addresses held by an on a centralized exchange. This might be the use case for many newcomers to the crypto space.

In contrast, many existing investors with ideological investment in the decentralized blockchain space would prefer stablecoin assets that exist within it. As for stablecoins' role as a means of payment for goods and services, their feature of being private and censorship-resistant will remain valuable to individuals if a scenario with the risk of government entities attempting to censor, block, or exclude transactions occurs. As was the intended ideology of Satoshi Nakamoto and other blockchain founders with decentralized, permissionless blockchains.

It All Comes Down to Regulation

As mentioned earlier, Gorton & Zhang (2021) see two possibilities for policy-makers when handling the risks of stablecoins. Either they regulate stablecoins to a degree where they transform stablecoin from private money to public money with regulation much in line with MiCA or introduce a CBDC and tax private stablecoins out of existence. While we cannot rule out a scenario where the two entities co-exist, it is worth speculating on the next steps of stablecoin regulation should a CBDC be introduced. As a CBDC can fulfill some of the same needs as a stablecoin, politicians may assess that stablecoins are too risky compared to the additional benefits they bring to society with a CBDC in place. Besides managing the risk of the crypto-asset, limiting stablecoins would also give more control of monetary policy and market integrity to the central bank and government. The argument here is that an introduction of CBDC may become a slippery slope towards even stricter regulations for their use and issuance where we end up with only CBDC as an option.

7 Conclusion

Stablecoins are crypto-assets running on a blockchain network that maintains a stable value by referencing a legal tender currency. Three stablecoin types exist: asset-backed backed, crypto-collateralized, and algorithmic. The crypto-asset has seen a significant increase in total market capitalization over the past years, with the four largest capitalized being Tether, USD Coin, Binance USD, and DAI. The primary utilization for stablecoins is as a tool to hold crypto-assets on-chain without being exposed to price fluctuations. However, they are also used in other contexts, such as remittances.

One of the most significant features of stablecoins compared to other crypto-asset types is their ability to hold a stable value relative to a legal tender currency. However, this thesis finds that stablecoins have certain flaws regarding stability. A literature review on the stability of stablecoins shows evidence that stablecoins cannot be categorized as absolute stable, implying that some variation in historical prices exists. Instead, stablecoins are relatively stable as the variation of historical prices is smaller than benchmark assets like Bitcoins. The instability stems from factors like the price of Bitcoin, the design of the stablecoin, and capitalization. Overall, we find larger capitalized asset-backed stablecoins like Tether and USD Coin to perform best regarding price stability.
Besides instability, holding stablecoins also comes with other risks. Holders' lack of trust in the issuer or other holders can ultimately cause a stablecoin to fail, making it worthless. Such failures are not unlikely to happen as stablecoins on the Ethereum mainnet have a failure rate of 63%, with TerraUSD being the largest capitalized stablecoin to fail. Storage of stablecoins also comes with caveats, as holders risk personal mistakes when storing the crypto-assets in their self-created digital wallet. Such risks are reduced when holding stablecoin with an exchange, but other risks arise as holders can lose their assets if the exchange goes bankrupt.

Although constantly improving, decentralized blockchains are limited in how much they can scale without compromising on decentralization and security. From analysis, it was estimated that the current Ethereum mainnet capacity for stablecoin transactions, had a long-run limit of around 19 Transactions Per Second. As the stablecoin transaction costs are largely influenced by network congestion, it could be concluded that sending payments on Ethereum would lead to

expensive and unpredictable costs. Offloading transaction execution to Layer2 Rollups enables scaling of theoretical Ethereum transaction throughput to an estimated 912 and 4,622 TPS for Optimistic and Zero-Knowledge Rollups, respectively, by way of only recording compressed transaction data. The resulting decrease in stablecoin transaction costs from the scalability gains of rollups is an estimated 97% less than the Ethereum Layer1 blockchain. The two most significant influences of relative transaction cost in USD were the demand for block inclusion on Layer1 and the ETH price in USD. The latter is ceteris paribus, expected to rise in the future, attributed to deflation in Ethereum's local blockchain currency ETH. With the scalability gains from Layer2 Rollups, it could be concluded that stablecoin transactions are competitive with traditional payment methods in some use cases.

With the possibility to optimize transactions per second and transaction fees by Layer2 scaling, stablecoins can be an alternative to traditional money. However, extensive adoption of stablecoins in society can have substantial macroeconomic consequences. As most significant stablecoins are referencing the US-Dollar, stablecoins threaten monetary transmission since an extensive adoption may have dollarization effects. Dollarization is a significant risk for developing countries as such countries will be more incentivized to adopt blockchain technology in transactions due to insufficient financial infrastructure. Furthermore, asset-backed stablecoins can also influence the money supply if, in the event of a mass redemption, causing inflation to rise.
Due to these risks, policy-makers may find it necessary to regulate stablecoins. Here, we have studied one of the first and most comprehensive regulatory frameworks for stablecoins developed by the European Union, MiCA. In MiCA, issuers of a stablecoin backed by a reserve of assets face stringent rules to comply with, while algorithmic stablecoins are banned. Most notably, the issuers are required to hold liquid reserves with a value corresponding to the tokens in circulation along with a limit of daily transfer volume of the stablecoin.
Other than regulations policy-makers also have the choice of introducing a central bank digital currency that may have some of the same traits as a stablecoin which perhaps can pose a threat to the adoption of stablecoins outside of the crypto-ecosystem.

In the discussion, it is argued that stablecoins may have problems regarding the properties of money. Based on the analysis, stablecoins can have specific issues as a store of value and

medium of exchange. Through the analysis, we have found that stablecoins have certain issues with stability and risk of default that makes them a worse store of value than fiat currencies though possible incoming regulation may help. As a medium of exchange, Layer2 scalability can enable stablecoins to be used outside of the crypto-ecosystem for retail and remittance payments. However, regulation capping the daily transaction volume of such payments may limit such purposes. Stablecoins will also have issues fulfilling the "No-Questions-Asked"-Principle, as receivers of stablecoins may need to conduct due diligence on the received stablecoin before accepting it as a means of payment making them inefficient as money.

Though stablecoins may not be characterized as money, they still have some features that can make them relevant outside of crypto-exchange. These features come from blockchain technology. The distributed ledger technology of blockchain ensures that transactions are secure without any intermediary overseeing the transfer. A larger adoption could thus create a more inclusive financial system where bank accounts are not a necessity for money wiring. Stablecoin transfers may also provide more privacy, fairness, and transparency in transactions, no matter the situation.

Lastly, a central bank digital currency may offer some of the same features that make stablecoins unique to traditional means of payment. However, a CBDC will be much more centralized in design, implying that the two should not be confused with one another. An introduction of a CBDC is likely to solve many of the same payment inefficiencies that stablecoins do. However, CBDCs may be a slippery slope regarding centralized power and transaction censorship. Stablecoin is, therefore, likely to be relevant for those who still desire decentralized means of payment.

8 Bibliography

1. AFP. (2022). Payments Cost Benchmarking Survey Comprehensive Results. www.AFPonline.org

2. Ali A. & Piazzi P. (2022 November 23). EU's Proposed Legislation Regulating Cryptoassets MiCA Heralds New Era of Regulatory Scrutiny | Skadden Arps Slate Meagher & Flom LLP. Skadden. Retrieved April 7 2023 from https://www.skadden.com/insights/publications/2022/11/eus-proposed-legislation

3. Anderson T. J. (2019). Money Without Boundaries: How Blockchain Will Facilitate the Denationalization of Money. John Wiley & Sons.

4. Andreas M. Antonopoulos. (2018 September 30). Bitcoin Q&A: Why Permissioned Blockchains Fail. Andreas M. Antonopoulos. https://www.youtube.com/watch?v=GEQzlJ_WL-E

5. Anthony Lewis. (2018). The Basics of Bitcoins and Blockchains. Mango Publishing Group.

6. Antonopoulos A. M. (2017). Mastering bitcoin: Programming the open blockchain (2.). O'reilly.

7. Antonopoulos A. M. & Wood G. (2018). Mastering Ethereum Building smart contracts and DAPPS. www.EBooksWorld.ir

8. Arner D. Auer R. & Frost J. (202 C.E.). Stablecoins: risks potential and regulation. Bank for International Settlements No. 905. https://www.bis.org/publ/work905.htm

9. Arslanian H. Donovan R. Blumenfeld M. & Zamore A. (2021). El Salvador's law: a meaningful test for Bitcoin. PricewaterhouseCoopers; PricewaterhouseCoopers. Retrieved March 6 2023 from https://www.pwc.com/gx/en/financial-services/pdf/el-salvadors-law-a-meaningful-test-for-bitcoin.pdf

10. Beck B. Schimke J. C. Hörauf M. & Scholl P. (2022 December 14). EU Markets in Crypto-Assets (MiCA) Regulation Expected to Enter into Force in Early 2023 | Perspectives & Events | Mayer Brown. Mayer Brown. Retrieved April 8 2023 from https://www.mayerbrown.com/en/perspectives-events/publications/2022/12/eu-markets-in-crypto-assets-mica-regulation-expected-to-enter-into-force-in-early-2023

11. Benson J. (2022 April 13). BlackRock to Handle Circle's USDC Cash Reserves as Part of $400M Funding Round. Decrypt. https://decrypt.co/97795/blackrock-handle-circle-usdc-cash-reserves-400m-funding-round

12. Berentsen A. & Schär F. (2018). The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies. Federal Reserve Bank of St Louis Review 100(2) 97–106. https://doi.org/10.20955/r.2018.97-106

13. bitcoinenergyconsumption.com. (2023). Bitcoin Energy Consumption Index. Bitcoinenergyconsumption.Com. http://bitcoinenergyconsumption.com/

14. Blanchard O. (2017). Macroeconomics. (7. ed. Global ed.). Pearson Education Limited.

15. Board of Governors of the Federal Reserve System. (2022). Money and Payments: The U.S.Dollar in the Age of Digital Transformation. In US Federal Reserve. Retrieved April 10 2023 from https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

16. Box G.E.P. Jenkins G.M. and Reinsel G.C. (1994) Time Series Analysis; Forecasting and Control. 3rd Edition Prentice Hall Englewood Cliff New Jersey.

17. Browne R. (2023 April 20). EU lawmakers approve world's first comprehensive framework for crypto regulation. CNBC. Retrieved April 2 2023 from https://www.cnbc.com/2023/04/20/eu-lawmakers-approve-worlds-first-comprehensive-crypto-regulation.html

18. Burger E. (2022). Decentralized Speed: Advances in Zero Knowledge Proofs. In a16zcrypto. https://a16zcrypto.com/content/article/decentralized-speed-advances-in-zero-knowledge-proofs/

19. Burke M. E. (2023). From Tether to Terra: The Current Stablecoin Ecosystem and the Failure of Regulators. Fordham Journal of Corporate & Financial Law 28(1) 99.

20. Buterin Vitalik. (2021). An Incomplete Guide to Rollups. https://vitalik.ca/general/2021/01/05/rollup.html

21. Buterin V. (2022a). Serenity Design Rationale. https://notes.ethereum.org/@vbuterin/serenity_design_rationale?type=view

22. Buterin V. (2022b). Paths toward single-slot finality. https://notes.ethereum.org/@vbuterin/single_slot_finality

23. Buterin V. Hernandez D. Kamphefner T. Pham K. Qiao Z. Ryan D. Sin J. Wang Y. & Zhang Y. X. (2020). Combining GHOST and Casper. http://arxiv.org/abs/2003.03052

24. Center for Innovative Finance & Schär F. (2021 May 19). CBDC and Stablecoins - Bitcoin Blockchain and Cryptoassets [Video]. YouTube. Retrieved April 2 2023 from https://www.youtube.com/watch?v=NmT9Rcfh_a0

25. Chand Arjun. (2022). What Are Blockchain Bridges And How Can We Classify Them? https://blog.li.fi/what-are-blockchain-bridges-and-how-can-we-classify-them-560dc6ec05fa

26. Chorzempa M. (2021). China the United States and central bank digital currencies: how important is it to be first? China Economic Journal 14(1) 102–115. https://doi.org/10.1080/17538963.2020.1870278

27. Chow A. R. (2022). Where Did FTX's Missing $8 Billion Go? Crypto Investigators Offer New Clues. In Time Magasine. https://time.com/6243086/ftx-where-did-money-go/

28. Circle | USDC Payments Treasury Management & Developer Tools. (n.d.). Circle. https://www.circle.com/

29. Clifford Chance. (2022). CRYPTO REGULATION: THE INTRODUCTION OF MICA INTO THE EU REGULATORY LANDSCAPE. In Clifford Chance. Retrieved April 7 2023 from https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/12/crypto-regulation-the-introduction-of-mica-into-the-eu-regulatory-landscape.pdf

30. CoinCapMarket. (n.d.). CoinCapMarket. Retrieved March 5 2023 from https://coinmarketcap.com/

31. coinwarz.com. (2023). Bitcoin Hashrate Chart. https://www.coinwarz.com/mining/bitcoin/hashrate-chart

32. Conrad J. (2022 November 8). China's Digital Yuan Works Just Like Cash—With Added Surveillance. WIRED. Retrieved March 15 2023 from https://www.wired.com/story/chinas-digital-yuan-ecny-works-just-like-cash-surveillance/

33. Council of the European Union. (2022 June 30). Digital finance: agreement reached on European crypto-assets regulation (MiCA) [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

34. Crypto-assets: green light to new rules for tracing transfers in the EU | News | European Parliament. (2023 April 20). Retrieved April 25 2023 from https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu

35. Danmarks Nationalbank. (2018). CLEARING AND SETTLEMENT OF RETAIL PAYMENTS. In www.nationalbanken.dk

36. Dark Rogerson & Wallis. (2022). Stablecoins: Market Developments Risks and Regulation. In Reserve Bank of Australia. Reserve Bank of Australia. https://www.rba.gov.au/publications/bulletin/2022/dec/stablecoins-market-developments-risks-and-regulation.html

37. de Best R. (2023). Number of purchase transactions on global general purpose card brands American Express Diners/Discover JCB Mastercard UnionPay and Visa from 2014 to 2021. https://www.statista.com/statistics/261327/number-of-per-card-credit-card-transactions-worldwide-by-brand-as-of-2011/

38. De Vries A. (2023). Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin. Patterns 4(1) 100633. https://doi.org/10.1016/j.patter.2022.100633

39. de Vries A. Gallersdörfer U. Klaaßen L. & Stoll C. (2022). Revisiting Bitcoin's carbon footprint. Joule 6(3) 498–502. https://doi.org/10.1016/j.joule.2022.02.005

40. Diamond Douglas W. and Philip H. Dybvig. "Bank Runs Deposit Insurance and Liquidity." Journal of Political Economy vol. 91 no. 3 1983 pp. 401–19. JSTOR http://www.jstor.org/stable/1837095.

41. Digital yuan: what is it and how does it work? (2021 January 14). Deutsche Bank. Retrieved March 21 2023 from https://www.db.com/news/detail/20210714-digital-yuan-what-is-it-and-how-does-it-work

42. Dr. Wood G. (2022). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.

43. Eichengreen B. & Viswanath-Natraj G. (2022). Stablecoins and Central Bank Digital Currencies: Policy and Regulatory Challenges. Asian Economic Papers 21(1) 29–46. https://doi.org/10.1162/asep_a_00843

44. Elrom E. (2019). The Blockchain Developer. In The Blockchain Developer. Apress. https://doi.org/10.1007/978-1-4842-4847-8

45. Ethereum.org. (2023 January 12). PROOF-OF-STAKE (POS). Https://Ethereum.Org/En/Developers/Docs/Consensus-Mechanisms/Pos/#:~:Text=Proof%2Dof%2Dstake%20(PoS)%20underlies%20Ethereum's%20consensus%20mechanismProof%2Dof%2Dwork%20architecture.

46. ethereum.org. (2023a). Danksharding. https://ethereum.org/en/roadmap/danksharding/

47. ethereum.org. (2023b). ETHEREUM ACCOUNTS. Https://Ethereum.Org/En/Developers/Docs/Accounts/#:~:Text=come%20from%20Alice.-Account%20creationBe%20encrypted%20with%20a%20password.&text=The%20public%20key%20is%20generatedIn%20a%20new%20tab)%E2%86%97.

48. ethereum.org. (2023c). Gas and Fees.

49. ethereum.org. (2023d). Optimistic rollups.

50. ethereum.org. (2023e). PROOF-OF-STAKE REWARDS AND PENALTIES. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/

51. ethereum.org. (2023f). Scaling. https://ethereum.org/en/developers/docs/scaling/

52. ethereum.org. (2023g). TOKEN STANDARDS. Https://Ethereum.Org/En/Developers/Docs/Standards/Tokens/.

53. ethereum.org. (2023h). ZERO-KNOWLEDGE ROLLUPS. Https://Ethereum.Org/En/Developers/Docs/Scaling/Zk-Rollups/. https://ethereum.org/en/developers/docs/scaling/zk-rollups/

54. ethereumenergyconsumption.com. (2023). Ethereum Energy Consumption Index. ethereumenergyconsumption.com

55. Etherscan.io. (2023a). Ether Daily Price (USD) Chart. https://etherscan.io/chart/etherprice

56. Etherscan.io. (2023b). Ether Supply Growth Chart. https://etherscan.io/chart/ethersupplygrowth

57. Etherscan.io. (2023c). Ethereum Average Gas Price Chart. https://etherscan.io/chart/gasprice

58. etherscan.io/token. (2023). Token Tether USD. https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7

59. European Central Bank. (n.d.). Digital euro. Retrieved March 5 2023 from https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html#know

60. Feyen E. Frost J. Natarajan H. & Rice T. (2021). What does digital money mean for emerging market and developing economies? In Bank for International Transfers (BIS Working Papers No 973). Bank For International Transfers. https://www.bis.org/publ/work973.pdf

61. Frankenfield J. (2023). Tether (USDT): Meaning and Uses for Tethering Crypto Explained. In Investopedia. Retrieved February 25 2023 from https://www.investopedia.com/terms/t/tether-usdt.asp

62. General Secretariat of the Council. (2022). Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 (MiCA): - Letter to the Chair of the European Parliament Committee on Economic and Monetary Affairs. In Council of the European Parliament (2020/0265 (COD)). Council of the European Parliament. Retrieved April 2 2023 from https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf

63. Ghizoni B. S. K. (n.d.). Nixon Ends Convertibility of U.S. Dollars to Gold and Announces Wage/Price Controls. Federal Reserve History. https://www.federalreservehistory.org/essays/gold-convertibility-ends

64. Gluchowski A. (2019). Optimistic vs. ZK Rollup: Deep Dive. Matter Labs. https://blog.matter-labs.io/optimistic-vs-zk-rollup-deep-dive-ea141e71e075

65. Goldberg M. (2022). How much are wire transfer fees? https://www.bankrate.com/banking/wire-transfer-fees/

66. Gorton G. & Zhang J. Y. (2021). Taming Wildcat Stablecoins. Social Science Research Network. https://doi.org/10.2139/ssrn.3888752

67. Grobys K. Junttila J. Kolari J. W. & Sapkota N. (2021). On the stability of stablecoins. Journal of Empirical Finance 64 207–223. https://doi.org/10.1016/j.jempfin.2021.09.002

68. Hafid A. Hafid A. S. & Samih M. (2020). Scaling Blockchains: A Comprehensive Survey. IEEE Access 8 125244–125262. https://doi.org/10.1109/ACCESS.2020.3007251

69. Hoang L. T. & Baur D. G. (2021). How stable are stablecoins? European Journal of Finance 1–17. https://doi.org/10.1080/1351847x.2021.1949369

70. https://btc.com/stats/diff. (n.d.). Difficulty .

71. Imam P. (2020). De-dollarization in Zimbabwe: What lessons can be learned from other sub-Saharan countries? International Journal of Finance & Economics. https://doi.org/10.1002/ijfe.2177

72. International Monetary Fund. (2020). Digital Money Across Borders: Macro-Financial Implications. In International Monetary Fund (No. 2020/050). https://www.imf.org/en/Publications/Policy-Papers/Issues/2020/10/17/Digital-Money-Across-Borders-Macro-Financial-Implications-49823

73. Jarno K. & Kołodziejczyk H. (2021). Does the Design of Stablecoins Impact Their Volatility? Journal of Risk and Financial Management 14(2) 42. https://doi.org/10.3390/jrfm14020042

74. Jeger C. Rodrigues B. Scheid E. J. & Stiller B. (2020). Analysis of Stablecoins during the Global COVID-19 Pandemic. https://doi.org/10.1109/bcca50787.2020.9274450

75. Kahya A. Krishnamachari B. & Yun S. (2021). Reducing the Volatility of Cryptocurrencies--A Survey of Stablecoins. arXiv preprint arXiv:2103.01340.

76. King R. (2022 June 26). How EU Crypto Regulation Will Affect You: Everything you Need to Know About MiCA - Dusk. Dusk. Retrieved April 6 2023 from https://dusk.network/news/how-eu-crypto-regulation-will-affect-you-everything-you-need-to-know-about-mica

77. Koning J. (2021). Algorithmic Stablecoins. AIER. https://www.aier.org/article/algorithmic-stablecoins/

78. l2beat.com. (2023). Risk analysis. Https://L2beat.Com/Scaling/Projects/Optimism#risks.

79. Legal Nodes Team. (2023 February 23). The EU Markets in Crypto-Assets (MiCA) Regulation Explained. Legal Nodes. Retrieved April 6 2023 from https://legalnodes.com/article/mica-regulation-explained#more-rules-for-token-issuance-processes

80. Lipton A. & Treccani A. (2022). Blockchain and distributed ledgers: mathematics technology and economics. World Scientific Publishing Co. Pte. Ltd. .

81. Mizrach B. (2021). Stablecoins: Survivorship Transactions Costs and Exchange Microstructure. Social Science Research Network. https://doi.org/10.2139/ssrn.3835219

82. Mizrach B. (2023). Stablecoins: Survivorship Transactions Costs and Exchange Microstructure. https://www.kaggle.com/bigquery/ethereum-blockchain;

83. Montevirgen K. (n.d.). Anti-Money Laundering (AML) Definition | Britannica Money. In Britannica. Retrieved March 29 2023 from https://www.britannica.com/money/anti-money-laundering-aml

84. n/a. (2022). (Almost) Everything about Rollup. Https://Mirror.Xyz/Msfew.Eth/WQJaOcFkpTOZLns8MBQaCS4OepRoaZ7uoctnLAnalVw.

85. Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

86. Optimism. (2020). OVM Deep Dive. Optimism PBC Blog. https://medium.com/ethereum-optimism/ovm-deep-dive-a300d1085f52

87. Optimism. (2023). Transaction fees on L2. Https://Community.Optimism.Io/. https://community.optimism.io/docs/developers/build/transaction-fees/#

88. optimistic.etherscan.io. (2023). Transaction Details. https://optimistic.etherscan.io/tx/0x57a12c6d47a79f695acfcaf80c894c739be6d107c0808b0bed6b9e5867a317eb

89. Personal remittances received (% of GDP) - El Salvador. (n.d.). World Bank Open Data. Retrieved March 5 2023 from https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=SV

90. Pomerantz Ori. (2022). SHORT ABIS FOR CALLDATA OPTIMIZATION. In https://ethereum.org/en/developers.

91. Presskorn-Thygesen T. (2022). Erhvervsøkonomisk videnskabsteori. Samfundslitteratur.

92. Pymnts. (2022 January 17). In Winning DeFi Circle's USDC Shows It Can Be the No. 1 Stablecoin. PYMNTS.com. https://www.pymnts.com/cryptocurrency/2022/winning-defi-circle-usdc-shows-it-can-be-top-stablecoin/

93. RBA. (2022). Australian CBDC Pilot for Digital Finance Innovation: Whitepaper. In Reserve Bank of Australia. Reserve Bank of Australia. Retrieved April 14 2023 from https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/pdf/australian-cbdc-pilot-for-digital-finance-innovation-white-paper.pdf

94. Riksbank S. (2023). What is money? Sveriges Riksbank. https://www.riksbank.se/en-gb/payments--cash/what-is-money/

95. Saunders M. Lewis P. & Thornhill A. (2012). Research methods for business students: 6th ed. Pearson.

96. Selgin G. A. (n.d.). Bank | Definition History Types Examples & Facts. In Encyclopedia Britannica. https://www.britannica.com/topic/bank/Commercial-banks

97. Snyder I. (2023). Foreign Transaction Fee: What is it? How does it work? https://www.valuepenguin.com/credit-card-foreign-transaction-fees#:~:text=Visa%20and%20Mastercard%20both%20chargeis%20applied%20to%20all%20transactions.

98. Standards for Efficient Cryptography. (2010). SEC 2: Recommended Elliptic Curve Domain Parameters.

99. Szabo N. (1996). Smart Contracts: Building Blocks for Digital Markets. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.h…1/10

100. Tether. (2023 January 13). Tether | Design Branding & Advertising. https://tether.com/
101. Thanh B. N. Hong T. Pham H. P. Cong T. & Anh T. T. DO. (2022). Are the stabilities of stablecoins connected? Journal of Industrial and Business Economics. https://doi.org/10.1007/s40812-022-00207-3

102. The Maker Protocol White Paper | Feb 2020. (n.d.). MakerDAO. Retrieved February 20 2023 from https://makerdao.com/en/whitepaper/#abstract

103. U.S. Energy Information Administration. (2021). INTERNATIONAL Electricity. https://www.eia.gov/international/data/world/electricity/electricity-consumption?pd=2&p=0000002&u=0&f=A&v=mapbubble&a=-&i=none&vo=value&&t=C&g=00000000000000000000000000000000000000000000001&l=249-ruvvvvvfvtvnvv1vrvvvvfvvvvvvfvv-vou20evvvvvvvvvvnvvvs0008&s=315532800000&e=1609459200000

104. ultrasound.money. (2023). SUPPLY GROWTH. https://ultrasound.money/

105. Visa. (2023). Security and reliability. Https://Usa.Visa.Com/Run-Your-Business/Small-Business-Tools/Retail.Html.

106. WEF. (2022). The Macroeconomic Impact of Cryptocurrency and Stablecoins. In World Economic Forum. World Economic Forum. https://www.weforum.org/whitepapers/the-macroeconomic-impact-of-cryptocurrency-and-stablecoins/

107. Wei W. (2018). The impact of Tether grants on Bitcoin. Economics Letters 171 19–22. https://doi.org/10.1016/j.econlet.2018.07.001

108. What is central bank digital currency (CBDC)? (2023 March 1). McKinsey & Company. Retrieved March 4 2023 from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-central-bank-digital-currency-cbdc

109. World Bank. (2022). World bank Remittance prices worldwide Quarterly 2022. 43.

110. Worldbank.org. (2022). Sending money from UNITED STATES to UKRAINE. https://remittanceprices.worldbank.org/corridor/United%20States/Ukraine

111. Wu K. (2019). ZK Rollup & Optimistic Rollup (En). https://kimiwu.medium.com/zk-rollup-optimistic-rollup-70c01295231b

112. Xangle. (2022). Would Optimistic Rollup Remain as a Viable Candidate Even After ZK Rollup Is Fully Developed? https://xangle.io/en/insight/research/635254a312965190a302f559

113. Zhang K. Morgan P. J. & McLaughlin J. M. (2022 November 15). MiCA – Overview of the New EU Crypto-Asset Regulatory Framework (Part 1). K&L Gates. Retrieved April 5 2023 from https://www.klgates.com/MiCA-Overview-of-the-new-EU-crypto-asset-regulatory-framework-Part-1-11-15-2022

114. zksync.io. (2022a). Technology. Https://Docs.Zksync.Io/Userdocs/Tech/#congested-Mainnet.

115. zksync.io. (2022b). Tokens & Fees. Https://Docs.Zksync.Io/Userdocs/Tokens/#fee-Costs. [Original source: https://studycrumb.com/alphabetizer]

9 Appendix

Appendix I: Smart contract creation and execution on Ethereum

Creating a smart contract is done by first programming what command the smart contract is to carry out, Ethereum programmers mainly use the code language "Solidity" or "Vyper". Once encoded to its function, the smart contract code is sent as a message via an Ethereum transaction to the Ethereum address 0x0000000000000000000000000000000000000000, also called the zero address (Antonopoulos & Wood, 2018). This address serves the purpose of simply validating (PoS consensus) the smart contract so that it exists as a transaction on a block of the blockchain, had this been a public ledger using PoW, the contract would instead have been mined onto a block. Once sent to the zero address, the smart contract will now have an address of its own. This address will appear as a public key address, but smart contracts do not have a secret-public key pair such as an externally owned address (EOA), i.e., a digital wallet would have. This address now functions as a smart contract on which the owner of the smart contract can execute and interact with the code programmed into it by executing a transaction to the address in ETH.

Appendix II: ECDSA inputs and Public key derivation.

Inputs used for elliptical curve cryptography when deriving a public key using the Elliptical Curve Digital Signature Algorithm. (Standards for Efficient Cryptography, 2010):

$secp256k1$: $T = (p, a, b, G, n, h)$

where the definitions of the constants for $secp256k1$ *are*:

The field F modulo p F_p:

$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

where p has to be a positive prime number

Elliptical curve function $E(F_P)$: $y^2 = x^3 + ax + b$ *is defined by*

a

$= 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000$

b

$= 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000000\ 00000007$

Ellitical curve function becomes: $y^2 = x^3 + 7$

This means that in order for a point to exist on the curve

$it\ must\ satisfy\colon\ (x^3 + 7 - y^2)\ modulo\ p = 0$

$G\ is\ the\ generator\ point\ used\ for\ public\ key\ generation\ and\ is\ fixed\ for\ secp256k1$ $on\ the\ Elliptical\ curve\ at\ point$ (Lipton & Treccani, 2022):

$\boldsymbol{G(x, y)}$

$\boldsymbol{G_x} =$

$79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798$

$\boldsymbol{G_y} =$

$483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4d8$

$The\ order\ n\ of\ G\ and\ its\ cofactor\ h\ (cofactor\ meaning\ the\ amount\ of\ cyclic\ subgroups)(n =$ $number\ of\ point\ within\ the\ subgroup\ )$ (Standards for Efficient Cryptography, 2010)

$n =$

FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE

BAAEDCE6 AF48A03B BFD25E8C D0364141

$h = 01$

To generate a public key, let public key be P, let secret key be a random integer s and G be the generator point as shown above.

$Public\ key\ function\colon\ P = s * G = (x, y)$

As s is an integer containing 256bits and G an (x,y) coordinate on the elliptic curve each point containing 256 bits, this multiplication is the same as adding G to itself s number of times(Antonopoulos & Wood, 2018). We are left with an x and y coordinate on the curve, containing P giving us a size of P as 512 bits.

The nature of the public key function is such that P can easily be calculated if s and G are given. However, s is infeasible to calculate with modern computing power, with only the P and G given, as they are not integers but instead coordinates on the Elliptical Curve and can therefore not simply extract s by division. This completes the encryption mechanism for the Public Key Infrastructure.

Appendix III Digital signature scheme of transactions with the use of SHA256 and ECDSA

ECDSA is again used, and the process can be described as the following formula for the digital signature (Antonopoulos & Wood, 2018).

$ds = q^{-1}(sha256(T) + r_x * s)\ mod\ (p)$

$ds: is\ the\ digital\ signature\ produced\ by\ the\ formula$

$q: is\ a\ randomly\ generated\ temporary\ secret\ key\ which\ is\ inverted$

$sha256(T): is\ the\ sha256\ hash\ of\ transaction\ in\ question$

$r_x: is\ the\ x\ coordinate\ of\ a\ public\ key\ Q\ generated\ from\ the\ temporary\ secret\ key\ q$

$s: is\ the\ secret\ key\ of\ the\ of\ the\ sender$

$p: is\ the\ field\ that\ the\ ECDSA\ operates, also\ called\ the\ prime\ order\ of\ the\ curve$

Once the digital signature is obtained, it is sent with a certificate which includes, $r_x\ and\ sha256(T)$. The receiver can then verify the validity of the digital signature with automated calculation, the steps involved uses the inverse of ds, along with the r_x value to obtain the temporary public key Q can be shown as (Antonopoulos & Wood, 2018):

$u_1 = sha256(T) * ds^{-1}\ mod\ (p)$

$u_2 = r_x * ds^{-1}\ mod\ (p)$

$The\ point\ Q\ on\ the\ EC\ is\ given\ by: Q = u_1 * G + u_2 * P$

Where $Q\ is\ the\ temporary\ public\ key\ used\ for\ verification$

$G\ is\ the\ fixed\ generator\ point\ set\ by\ \boldsymbol{secp256k1}$

$P\ is\ the\ public\ key\ of\ the\ sender$

If the x coordinate of the point Q is = r_x then the signature is valid(Antonopoulos & Wood, 2018).

Appendix IV: Proof-of-Work consensus mechanism and mining.

PoW became the first conceptualized consensus mechanism in blockchain technologies with the creation of bitcoin. It works by having **mining nodes** volunteer computing power to hash the block header to a number smaller than the target algorithmically generated by the network called the target bits.

These target bits are made up of two components, a **coefficient** and an **exponent**. At the time of writing the target bits for a block on the bitcoin blockchain is (given in hexadecimal numbers) 0x1706023e where 0x17 is the exponent, and the coefficient is 0x06023e.

The formula for the difficulty target on bitcoin protocol is given as (Antonopoulos, 2017):

$Target\ bits = coefficient * 2^{(8*(exponent-3))}$

Inserting the values gives us:

$Target\ bits = 0x06023e * 2^{0x08*(0x17-0x03)}$

$Target\ bits = 0x06023e * 2^{0x08*(0x17-0x03)}$

If we write this in decimal format it translates to the number:

$Target\ bits = 393790 * 2^{8*(20)}$

$Target\ bits =$
575,524,729,764,536,260,159,429,050,
275,345,090,310,309,676,098,519,040

$Target\ bits_{hex} =$

$6023e000000000000000000$

0000000000000000000000

Mining nodes will now use a variable called a **“**Nonce**”** that they will hash together with the fixed inputs of block header, such as the hash of the previous block, timestamp, and the Merkle root of the transactions included in the block, to find 64-character hexadecimal number smaller than the target.

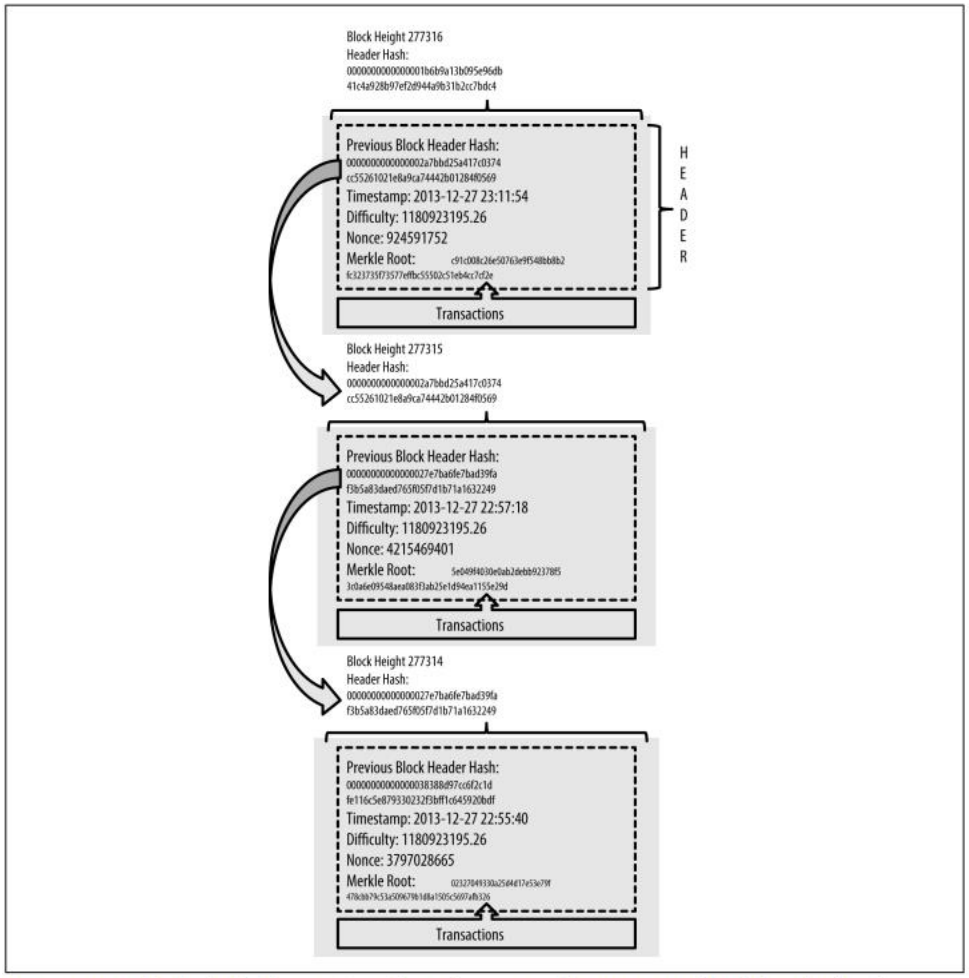


Figure 9-1. Blocks linked in a chain by reference to the previous block header hash

Source: (Antonopoulos, 2017)

$sha256(fixed\ inputs + nonce) <$

$0000000000000000006023e00000000$

$0000000000000000000000000000000000$

Recall that as the Sha256 algorithm is a one-way function where any change in the input will change the output in an unpredictable manner. Therefore, mining nodes will have no choice but to run through all possible solutions of the nonce starting from the number 1, until they have found a hash output smaller than the difficult target.

On the bitcoin blockchain this difficulty target changes every 2016 blocks, so that desired hash rate (time to solve the target bits), is 10 minutes. As the hash rate increases, the target bits as a number will decrease, as the lower the target bits are the harder it will be to find a number lower than it out of 2^{256} possibilities.

Incentives for mining.

When a mining node is successful in finding a suitable candidate block, it is rewarded with the transaction fees from the transactions on the block, as well as the coinbase transaction.

The coinbase transaction can be seen as the cryptocurrency minting process, where the new coins on the blockchain are created with the new block and paid out to the miner for them to spend in the localized economy. Some blockchains, such as Bitcoin, have a deflationary function coded into the protocol. The first coinbase transaction on the Bitcoin protocol was 50 BTC and has been set to reduce by 50% for every 210,000 stacked on the blockchain (Antonopoulos, 2017). At the time of writing, the current block is 782,904. The coinbase transaction has therefore been reduced by 50% three times and is, therefore, 6.25 BTC. This gives us a total amount of BTC that can ever be created is asymptotically 21 million BTC.

The coinbase transaction is a vital incentive and driver behind Proof-of-work consensus, as mining will increasingly demand more computing power, and, therefore more energy.

Confirmations, forking and consensus.

Full nodes will always look to adopt the longest blockchain they receive, which in essence, means that there might temporarily be conflicting versions of a blockchain on the p2p network regarding what blocks have been added to the chain recently. This is due to the network being p2p and that the newly found blocks are not propagated to the entire network immediately but rather to the interconnected nodes of the mining node that created the block.

If multiple solutions are found, mining nodes will build on the block solution they receive first but keep a copy of the alternative block solution. This is known as a fork. When the next block is solved, the solution on which that block has been built must be the prevailing solution, as it has had the most computing power spent on it to solve the next block. As this new block is propagated out to the network, all nodes working on a chain with a losing solution will stop working on it and adopt the alternative solution. The losing block is thereby **orphaned**, and all transactions in the block that are not included in the alternative solution are sent back to the mempool.

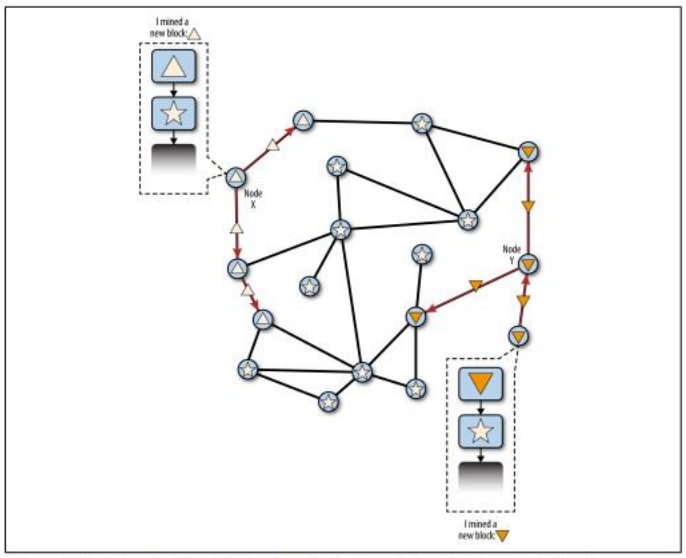


Figure 10-3. Visualization of a blockchain fork event: two blocks found simultaneously

Source: (Antonopoulos, 2017)

In theory, this means that just because a block has one or even two **confirmations** (blocks build on top of it), there is still a probability that a chain on the network is equally long. These two chains will then compete for as long as it would take for one chain to be at least one block ahead. Once a longer chain is propagated and has reached far enough out to the network, the probability of catching up to a longer chain drops exponentially as no miner node will be working on the shorter chain. (Antonopoulos, 2017).

51% attack.

Security-wise, PoW has one downfall, as it can be the subject of a 51% attack. Such an attack would entail one entity controlling 51% of the nodes mining the network. This entity could then, in theory, alter transactions on current blocks and expend the energy to have it recorded on all subsequent blocks to catch up and surpass the honest blockchain, thereby reaching consensus by having expended the largest proof-of-work (Nakamoto, 2008).

Appendix V: Bridging: A prerequisite for the interconnectivity of token transactions between Layer1 and Layer2.

While Layer2 solutions in most use cases share similarities with the Layer1 blockchain on which they are compatible, it is essential to keep in mind that when a Layer2 solution is used, assets are sent through another network computation wise, the asset is just noted to have swapped hands on Layer1. As this is the case, if an asset exists on Layer1 and an individual wish to transfer the

asset through a Layer2 network (this could be for several reasons such as lower fees, faster transaction speed, etc.), the asset would need to be transferred to the Layer2 networks. Transferring assets between networks uses a concept called a bridge; this bridge can be seen as a transaction between networks. Three kinds of bridging methods are most common for token transfers, such as stablecoins (Chand Arjun, 2022).

Burn and mint bridge: Burns the tokens on the origin network and mints an equal number of tokens on the destination network.

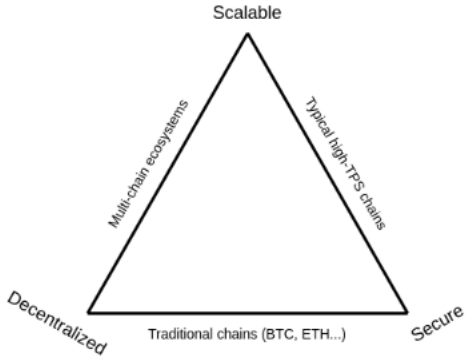
Lock and mint bridge: Tokens are locked up at the origin network held by a smart contract, equal number of tokens are minted at the destination network. Once tokens are returned over the bridge to the origin network, the smart contract will release the locked tokens and burn the tokens on the destination network.

Atomic swap bridge: Swapping tokens on the origin network to other tokens on the destination network.

Using one or several of these types of bridges allows users of stablecoins and other cryptocurrencies to easily swap from one network to another in times of high network congestion. In contrast, previously, Tokens were locked to the network in which they were created. Bridges can therefore be seen as the tool that truly allows for the mobility and interchangeability of stablecoins.

Appendix VI: Scalability trilemma of decentralized blockchains

Increasing transaction processing speed and scaling the blockchain network without compromising security or decentralization is an ongoing battle in the decentralized blockchain space. A popular illustration of this point at issue is the scalability trilemma first proposed by Ethereum co-founder Vitalik Buterin.



Source: (Buterin, 2021)

Where it is unattainable, or at the very least, severely difficult, to excel in 2 factors without con promising on one. What makes up the trilemma is:

Scalability: Concerns about how many transactions the network can handle and what the costs and speed associated with transactions are.

Security: Concerns security of the network, in the sense that it is resilient to attacks, that transactions are immutable (non-reversible), double-spending, and other fraudulent actions are infeasible.

Decentralization: Concerns if the network if or not the network is controlled by one or a few entities (Hafid et al., 2020).

The first decentralized blockchain technologies relied on PoW consensus to attain a high level of decentralization and security a description of PoW can be found in the in the Appenidx. PoW is an ideal system with seemingly few flaws security-wise besides the 51% attack, the consensus mechanism does however fall short in its scalability prospects to compete with modern payment systems. Bitcoin, the largest PoW consensus protocol, had as of March 31st, a hash rate corresponding to electricity consumption of 100.18 TWh yearly, in ccomparison it is more than 2.5 times the Annual electricity consumption of the entire country of Denmark (38 TWh in 2021) (U.S. Energy Information Administration, 2021)(bitcoinenergyconsumption.com, 2023). The second largest blockchain platform using PoW based consensus mechanism, was Ethereum.

As mentioned, Ethereum switched from PoW to PoS as the consensus mechanism governing the blockchain in an event called “The Merge” on the 15th of September 2022. In two days, the estimated annual energy consumption decreased by 99.99% from 77.774 TWh pre-merger to 0.013 TWh post-merger(ethereumenergyconsumption.com, 2023).

The Ethereum merger was part of a greater scaling plan for the Ethereum main net to achieve more reliable transaction speeds and reduced costs associated with them. In the context of the blockchain trilemma, the switch from PoW to PoS has raised questions about Ethereum potentially compromising on decentralization, as the minimum stake of ETH required to validate is 32ETH which at the time of writing is the equivalent of 67,661 USD. Furthermore, the probability of being chosen to stake will increase as there is no limit to how many Validator nodes an individual can run if they have the capital. This barrier to entry has made way for staking pools, where participants pool together ETH to reach the 32 ETH needed to validate, where the

transaction fees and block rewards earned from validating are then split proportionately between the staking pool participants.

In effect, this is comparable to mining pools that exist in PoW protocols; the key difference is just that each participant is volunteering computing power, thereby making them direct participants in the network, whereas in PoS only one computer will validate, i.e., a less decentralized approach.

Appendix VII: Increasing transaction capacity through sharding.

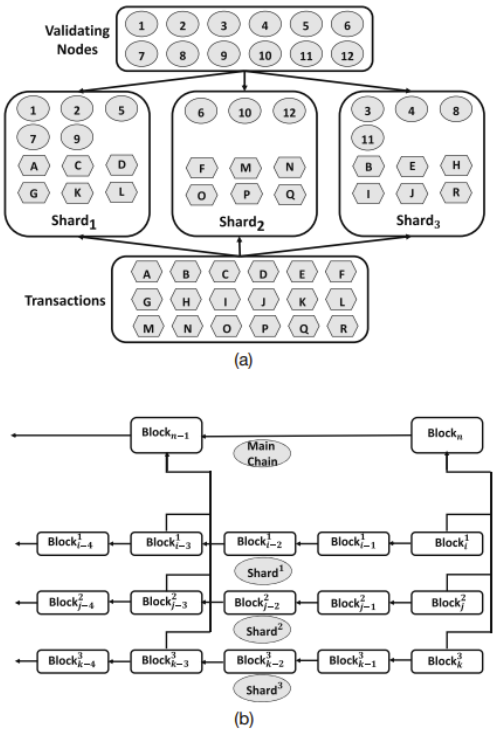
Every block (slot) is 12 seconds, the gas cost capacity is benchmarked at 15 million gas, 1 stablecoin transaction estimated to 65,000 gas.

$$\left(\frac{15{,}000{,}000}{65{,}000}\right) = 230\ stablecoin\ transactions\ per\ block\ (no\ half\ transactions\ can\ exist)$$

$$\frac{230}{12} = 19\ Stablecoin\ transactions\ per\ second\ is\ the\ long\ run\ network\ limit$$

This is optimistic as the calculation assumes stablecoin transfers as the only transfers being processed by the network, as Defi operations such as token swaps are also being processed by the EVM, which has a gas cost more than double in size as a minimum. It would be optimistic to say that the Ethereum main net can process about 20 stablecoin transactions per second at the current benchmark capacity. As the Ethereum main net is the preferred blockchain protocol for running smart contract-based applications and tokens such as NFTs, the network, as a result, has enormous amounts of capital tied up in it.

One proposed method for future Layer1 scaling of transactions is through a concept called sharding. As was reviewed in the “Blockchain” section, decentralized permissionless ledgers such as Bitcoin and Ethereum rely on all full nodes agreeing to the current state of the ledger. As the size of the ledger grows, this will eventually create problems as storing the ledger as would take up large amounts of computer memory.



Source: (Lipton & Treccani, 2022)

Sharding relieves this problem by splitting the network layer of nodes up into smaller fractions called shards. In practice, this means that transactions would be assigned to one of the shards in the network for processing parallel to the mainchain, thereby creating many smaller blockchain ledgers. The state of these smaller blockchain ledgers is then reported back to the mainchain periodically to receive a state of the entire network ledger(Lipton & Treccani, 2022). In short is like having many smaller blockchains within a blockchain, which drastically increase network capacity and speed while simultaneously decreasing transaction costs.

For the Ethereum network, plans have been set into effect to first implement a sharding technique called Dank-sharding, sometime in the coming years, which coupled with Layer2 rollups, will enable transactions per second to reach above 100,000. This is the first step on the roadmap toward complete sharding of the blockchain.

Appendix VIII: Assumptions made for enabling comparisons.

Wire transfers domestic

Expected sender fee US industry average: 26$ (Goldberg, 2022)

Expected receiver fee US industry average: 13$ (Goldberg, 2022)

Platform: Swift as USA is part of the swift agreement.

Layer1 Ethereum

L1 gas cost of sending stablecoin transaction: 65,000 gas (conservative assumption can vary between 40,000-70,000)(etherscan.io/token, 2023)

Layer2 ZKR

ZKR Execution and ZK-prover fee: 0.01$ (zksync.io, 2022a)

Batch size: 500 stablecoin transactions (conservative assumption, but is variable depending on ZKR)

ZK-proof verification gas cost: 800,000 gas (Wu, 2019; Xangle, 2022)

L1 Size of transaction data as calldata: 16 bytes (Buterin Vitalik, 2021)

L1 Gas cost of transaction data as calldata: 16*16=256 gas (Dr. Wood, 2022)

Layer2 OR

OR gas cost of stablecoin transaction: 65,000 gas (conservative assumption can vary between 40,000-70,000)(etherscan.io/token, 2023)

OR gas price: 0.001 Gwei (Optimism, 2023; optimistic.etherscan.io, 2023)

OR execution fee: 65,000*0.001=65 Gwei

Batch size: 500 stablecoin transactions (conservative assumption, but is variable depending on ZKR)

Storage and replacement costs of: Pre-state root, post-state root, batch root ≈ fixed gas cost: 280,000 gas (Xangle, 2022)

L1 Size of transaction data as calldata: 84 bytes

L1 Gas cost of transaction data as calldata: 84*16=1344 gas (Dr. Wood, 2022)

Estimates L1+L2:

The estimates are based on:

ETH/USD average daily prices from Q1 2023 01/01/2023-30/04/2023.(Etherscan.io, 2023a)

Ethereum gas average daily prices in Wei from Q1 2023 01/01/2023-30/04/2023 (Etherscan.io, 2023c)

ETH supply growth (Etherscan.io, 2023b).

Estimates

Visa TPS calculations are attached in Excel (de Best, 2023)