UNIVERSITY OF LJUBLJANA
SCHOOL OF ECONOMICS AND BUSINESS

MASTER'S THESIS

LENDING PROTOCOL IN SOLANA BLOCKCHAIN TECHNOLOGY

Ljubljana, january 2023

ROK HRIBAR

AUTHORSHIP STATEMENT

The undersigned Rok Hribar, a student at the University of Ljubljana, School of Economics and Business, (hereafter: SEB LU), author of this written final work of studies with the title ‘Lending protocol in Solana blockchain technology', prepared under the supervision of Matej Marinč, Ph.D.

DECLARE

1. this written final work of studies to be based on the results of my own research;
2. the printed form of this written final work of studies to be identical to its electronic form;
3. the text of this written final work of studies to be language-edited and technically in adherence with the SEB LU’s Technical Guidelines for Written Works, which means that I cited and/or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU’s Technical Guidelines for Written Works;
4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offense and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;
5. to be aware of the consequences a proven plagiarism charge based on this written final work could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;
6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;
7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained the permission of the Ethics Committee;
8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;
9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically, and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;
10. my consent to the publication of my personal data, included in this written final work of studies and in this declaration when this written final work of studies is published.

Ljubljana, January 13rd, 2023 Author’s signature: Rok Hribar

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

sl. – slovene
AML – (sl. Proti pranje denarja); Anti-money laundering
BFT – (sl. Bizantinska toleranca napak); Byzantine faul tolerance
CPI – (sl. Skozi-programski poziv); Cross-program invocation
DAO – (sl. Decentralizirana avtonomna organizacija); Decentralized Autonomous Organization
DAPP – (sl. Decentralizirana aplikacija); Decentralized Application
DEFI – (sl. Decentralizirane finance); Decentralized Finance
DESOC – (sl. Decentralizirana družba); Decentralized Society

DEX – (sl. Decentralizirana borza); Decentralized Exchange

DLT – (sl. Distribuirana verižna tehnologija); Distributed Ledger Technology

ECB – (sl. Evropska centralna banka); European Central Bank

EU – (sl. Evropska unija); European Union

EURIBOR – (sl. Evropska medbančna obrestna mera); Euro Interbank Offered rate

FED – (sl. Federalni sistem rezerv); Federal Reserve System

FMC – (sl. Financiranje skozi kreiranje denarja); Financing Through Money Creation

IOU – (sl. Dolgujem ti); I owe you

KYC – (sl. Poznaj svojega uporabnika); Know Your Customer

LIBOR – (sl. Londonska medbančna obrestna mera); London Interbank Offered rate

LP – (sl. Likvidni bazen); Liquidity Pool

NFT – (sl. Ne ponareljiv žeton); Non-fungible Token

P2P – (sl. Od uporabnika do uporabnika); Peer-to-peer

pBFT – (sl. Praktična bizantinska toleranca napak); Practical Byzantine faul tolerance

PDA – (sl. Programsko izpeljan naslov); Program Derived Addresses

PLF – (sl. Protokol za posojilna sredstva); Protocol for Loanable Funds

PoH – (sl. Dokaz o zgodovini); Proof of History

PoS – (sl. Dokaz o deležu); Proof of Stake

PoW – (sl. Dokaz o delu); Proof of Work

SBT – (sl. Token privezan na posameznika); Soulbound Token

SEC – (sl. Komisija za vrednostne papirje in borze); Securities and Exchange Commission

SOFR – (sl. Stopnja zavarovanega financiranja čez noč); Secured Overnight Financing Rate

SSI – (sl. Samoupravna identiteta); Self-Sovereign Identity

TPS – (sl. Transakcije na sekundo); Transactions per second

TRADFI – (sl. Tradicionalne finance); Traditional Finance

TVL – (sl. Celotna zaklenjena vrednost); Total Value Locked

US – (sl. Združene države); United States

ZKP – (sl. Dokaz brez znanja); Zero knowledge proof

INTRODUCTION

The inspiration for this master's thesis is the fact that decentralized finance (DeFi) lending protocols are on the rise and have as of March 29, 2022, over 55 billion US dollars of total value locked worldwide (Statista, 2022). In this thesis, I will perform a thorough analysis of the traditional finance (TradFi) world and of the upcoming DeFi world powered by blockchain technology. The main objective of this thesis is to see if merging the traditional finance world with blockchain technology is feasible, viable, and scalable in the long run. In view of this, I will tackle the design and implementation of a traditional money lending protocol with the blockchain technology Solana.

To thoroughly understand the problem that I will be solving we first need to look at lending in traditional finance. Greenbaum, Thakor, and Boot (2019) defined a bank loan as »Simply put, it is the purchase of an asset (the borrower's indebtedness) that is typically an illiquid and highly customized financial claim against the borrower's future cash flows«. Meaning, that loans are of illiquid nature and can be highly customized which requires thorough screening and due diligence of the borrower so that banking institutions can offer them the best loan terms and minimize the risk of default. In essence, screening and monitoring prevent moral hazard problem and adverse selection problem (Marinč, 2022). Furthermore, banking institutions act as financial intermediaries to finance real economic activities like financing corporate growth (Aramonte, Doerr, Huang, & Schrimpf, 2022). In economic theory, banking institutions collect deposits and later lend out the collected deposits in a form of a loan. However, the banking institutions are not solely financial intermediaries as they do not issue loans only from deposits, but rather provide financing through money creation. This means they create new money at the point of making a loan constrained by their profitability and solvency requirements (Jakab & Kumhof, 2015). This is important for this thesis as it outlines that the money lent out in TradFi is not fully constrained by the amount of deposits, but by the regulatory profitability and solvency requirements.

In the DeFi world, there are already some paradigms for on-chain lending. The biggest market capitalizations have so-called overcollateralized lending paradigms such as Maker and Aave protocols which have a market capitalization of 1,71 billion and 1,62 billion U.S. dollars respectively (Statista, 2022). In such a paradigm, the borrower overcollateralizes the loan with one token and withdraws another token. For example, the borrower puts the Ethereum token as collateral and in exchange withdraws stablecoins of lower value such as USDT (stablecoins are tokens pegged to fiat currencies). This is because, in the DeFi world, loans are not used for financing real economic activities but rather for collateralizing already owned crypto assets and with acquired stablecoins acquiring more crypto assets. Overcollateralized protocols are thus most often used for margin trading (Future Learn, 2021). This means these crypto-collateralized loans cannot be used for real-world activities as the borrower cannot enter the position of net debt (Gudgeon, Werner, Perez, & Knottenbelt, 2020). Overcollateralization in this case is done as the crypto assets are extremely volatile and pro-cyclical (Aramonte et al., 2022).

The purpose of this master’s thesis is to propose a paradigm that would issue loans in which the borrower could enter the position of net debt and this debt would then finance real economic activities. One paradigm is the paradigm of prime brokerage and the other is an identity-based approach. In prime brokerage, the protocol lends money, but remains in control of the funds and offers only limited actions to the borrower (Baker, 2022). In this master thesis, I will design, implement, and analyze an identity-based approach. In the DeFi world, the traditional banking loan that I will be implementing is denoted as an undercollateralized identity-based loan (Baker, 2022). In the identity approach, loans are issued based on the real-world identity of an individual, whose information is stored on the blockchain. This means that I will assess creditworthiness based on either borrower’s cash flow or his credit score. Undercollateralization means that the borrower can enter a position of net debt. Since all actors on the blockchain in DeFi are pseudo-anonymous, by far the biggest problem that needs to be solved will be how to successfully solve moral hazard problem and adverse selection problem through blockchain technology.

The goal of the master's thesis is to see if blockchain technology can be successfully implemented in the traditional financial system. To check this, I will design and develop an undercollateralized identity-based lending protocol in a blockchain technology called Solana. I have chosen Solana as it is a blockchain technology, which is finally scalable enough to be used for big enterprise-level DeFi applications (Yakovenko, 2021). After implementing the protocol, I will answer two main research questions:

1. Can an undercollateralized identity-based lending protocol be successfully implemented with blockchain technology?
2. Can the adverse selection and moral hazard problem be solved in the blockchain implementation of the bank lending protocol?

To design and implement the bank lending protocol in blockchain technology, I need to have a good understanding of the underlying theory of bank lending protocols and the underlying technology with which such a protocol will be built – which is the Solana blockchain. Through extensive research, I will get a good understanding of already existing traditional bank lending protocols and DeFi lending protocols. Moving on, I will get a good grasp and understanding of the Solana blockchain through documentation about the technology such as the official documentation and Solana’s whitepaper. I will also need to acquire knowledge about the underlying technologies with which the Solana blockchain applications are built, such as the Rust programming language and its supporting tools. When designing a bank lending protocol, I will need to define the bank lending elements. I will account for all the elements that the traditional lending protocols have until now, like fixed and variable interest rates, various interest rate models, collateralization, and so on.

The structure starts with the theory of traditional finance, blockchain technology, and decentralized finance. It then continues with designing the protocol, implementing it, and lastly also analyzing it.

1 TRADITIONAL FINANCE

The concept of money originated as a need for a medium of exchange. In most simple terms, it originated from people having a different number of resources, for instance, some farmers had a surplus of straw for their cattle while others had a deficit. To trade with each other, the earliest form of market exchange was peer-to-peer or also known as barter. The items traded needed to be of similar value for the exchange to happen. However, this kind of system was thus highly inefficient as it was difficult to find items whose value would match exactly. This is where the money came in as a medium of exchange and a store of value (Harvey, 2021). Though, when one had insufficient funds at the juncture of making the trade, he could ask other people for money. Thus, a mutual agreement was achieved between the buyer and other people for the borrowed money to be repaid later. This action is denoted as lending and has been an integral part of human society for thousands of years (Harvey, 2021). The first evidence of loans took place in Mesopotamia approximately five thousand years ago. At the core of lending is the concept of trust and the promise of repayment. Furthermore, the term *credit* comes from mid-16th century French, which means to believe and trust (Xu & Vadgama, 2022). The lender lends money and in return expects to be repaid and earn interest. Lending has developed since its beginnings, but the fundamentals stand. On the retail level, it offers people an option to buy a commodity and pay it back later. On the corporate and economic level, it fuels corporate and economic growth and cultivates forward-looking commercial activities (Xu & Vadgama, 2022). The lending market is now formed of many different instruments some of which are mortgages, lines of credit, and government bonds. The global debt markets are estimated to be 305 trillion USD in 2022 (Campos, 2022).

However, not all loans are of the same quality. Credit rating agencies give loans a rating. Banks repackage bad loans with good loans and sell them to capital market investors. This is called securitization and is an act of converting an untraded debt claim into a traded security. Banks do this by issuing claims against it and then selling these claims (Greenbaum, Thakor, and Boot, 2019). Unfortunately, this was exploited, and the financial crisis followed in 2008. Because the world's economy is thus highly dependent on banking, this is a heavily regulated industry and banks need to comply with regulations. Traditional finance (henceforth TradFi) also encompasses the stock market, where stocks of public companies are bought and sold. The profit made is then called capital gains. This sector is also highly regulated as there were a lot of manipulations in the past. An example of this is insider trading – where information asymmetry allowed individuals to acquire large profits. Traders on the stock market can also loan money from the trading platform and acquire larger returns. This notion is called margin trading which is a form of lending (Fernando, 2022). Moving forward we look in-depth at how banks operate concerning three key economic theories - the financial intermediation theory of banking, the fractional reserve theory of banking, and lastly the credit creation theory of banking.

1.1 Operations of a bank

According to the *financial intermediation theory of banking,* banks are at their core financial intermediaries (FIs). This means they are entities that intermediate between providers and users of financial capital (Greenbaum, Thakor, & Boot, 2019). FIs are classified into two groups: depository financial institutions and non-depository financial institutions. Banks are classified as depository financial institutions because commercial banks take people's deposits and loan them at a certain interest rate. The deposits are thought of as excess liquidity – the money that depositors do not need right now. On the other hand, loans are given to entities that require money right now. The banks pay an interest rate to the depositors for providing this excess liquidity and charge borrowers a certain interest rate for using the excess liquidity. Banks are then able to profit from the interest rate spread (1), which is the delta between interest paid and interest received. The bank lending protocol is the one that determines the interest rate of the borrowed funds, the covenants, and all the other terms of the loan and is as such the most important part of the bank's business model as lending has always been bank's primary source of income (Greenbaum, Thakor, & Boot, 2019). On the other hand, non-depository financial institutions acquire funding through capital markets.

$$\Delta i = i_b - i_s \tag{1}$$

In the equation (1), Δi is the interest rate spread, i_b is the borrowing interest rate and i_s is the saving interest rate. However, banks operate in a wide industry, and apart from lending they provide various other financial services. They offer underwriting services, brokerage services, and payment processing services. On top of that, they also offer fees within their financial products such as mobile or online banking applications. They also hold a variety of earning assets, such as mortgages and working capital (Greenbaum, Thakor, and Boot, 2019). Apart from commercial banks, every country has a central bank that is charged with managing the money supply and thus enforcing monetary policy. The central banks also function as lenders of last resort and by doing so they protect the integrity of the financial system. When talking about monetary policy, central banks look to stabilize economic activity. For example, if there is high inflation, the central bank will increase interest rates and thus restrain the growth of money. Decreasing the growth of money lowers the number of loans made by commercial banks and drives up interest rates (Greenbaum, Thakor, and Boot, 2019).

Banks are in a heavily regulated industry and therefore need to adhere to and comply with regulations. Commercial banks' liquidity is constrained through a *fractional reserve theory of banking* and solvency requirements from the central bank. This means they need to maintain reserve requirements set by the central bank to store liquidity in the case of a bank run. During a bank run, depositors demand their money all at once, which leads to bank failure (Johnston, 2021). The *fractional reserve theory of banking* describes a system where banks loan out a certain amount of deposits that they have on their balance sheets. This in turn expands the economy by freeing capital for lending. Banks are required to keep on hand a certain amount of the cash that the depositors give them, which are known as the bank's reserves. Such depository institutions must report their transaction accounts, savings deposits, and other reservable obligations to the central bank. Some banks are not required to hold reserves, but all are paid an interest rate on the reserves called interest rate on excess reserves (IOER) as an incentive to keep excess reserves. When estimating the impact of the reserve requirement on the economy, the money multiplier equation (2) is used.

$$\text{Money Multiplier} = \frac{1}{r} \tag{2}$$

Where r is required reserve ratio. Equation (2) provides an estimate for the amount of money created with the fractional reserve system with a known fractional reserve ratio. Given the deposits in a system, one can estimate the impact on the money supply (Kagan, 2022).

1.2 Money creation

In the previous sub-chapter, we discussed how bank lending works. We have looked at the *financial intermediation theory of banking,* where banks are merely FIs that collect deposits and then lend out those deposits. Then we have looked at the *fractional reserve theory of banking,* where banks are creating money through systemic interaction (Werner, 2014). However, there is one theory we have not looked at and that is the *credit creation theory of banking.* This theory states that each bank has the power to create money 'out of nothing' when extending credit. Richard A. Werner wrote a paper in which he described how he conducted an empirical test, where money was borrowed from the bank while its internal records were being monitored. He argues that according to that research this latest money creation theory holds (Werner, 2014). When a bank issues a loan, it extends its balance sheet by increasing its assets (loans receivable) and its liability (borrower's deposits) at the same time (Lindner, 2015). Put simply, at the time of making a loan a matching deposit is created in the borrower's bank account, therefore, creating new money (McLeay, Radia and Thomas, 2014). This theory states that the amount of credit is not limited by deposits or savings. Deposits are created by the bank when issuing loans. The amount of credit depends on banks' ability and willingness to provide credit and on borrowers' willingness to increase their debts (Lindner, 2015). The money creation model predicts pro-cyclical bank leverage and not countercyclical bank leverage, this means that during a downturn it predicts a bigger role for credit rationing compared to price rationing. In simpler terms, this means that in a downturn restraining issuance of credit has a bigger role compared to increasing the prices of commodities. In turn, this financing model yields changes to bank lending that are much larger and faster (Jakab & Kumhof, 2015).

In conclusion, in the FI theory of banking, banks are seen as barter institutions between depositors and borrowers. However, *money creation theory claims* that there are no pre-existing loanable funds in the real world and that such FI institutions don't exist. The money creation model also states that no deposit multiplier mechanism hinders banks' ability to create money. It notes that the main constraint is banks' expectations concerning their profitability and solvency. Although, the regulation also constrains bank activities to maintain financial system stability (McLeay, Radia and Thomas, 2014). Therefore, the money creation model sees banks as fundamentally monetary institutions (Jakab & Kumhof, 2015).

1.3 Adverse selection problem and screening

The adverse selection problem and the moral hazard problem are two of the biggest problems when it comes to lending. Loans are assets for banks. Therefore, both problems are prevented by the bank functions on the asset side of the banks' balance sheet. An adverse selection problem abounds when there is information asymmetry between the two sides of the party. Information asymmetry occurs when there is one side more informed than the other. When talking about a loan for a project in a business, the borrower has more information about that specific project and their business compared to the lender. Therefore, the lender cannot manage risk properly such as providing a loan with a good (lower) interest rate or *vice-versa*. This means the lender cannot adjust the interest rate to the quality of the company or project (Greenbaum, Thakor, and Boot, 2019). The adverse selection problem is solved by screening. Screening refers to the *ex-ante* gathering of information about the company and is thought of as one of the competitive advantages of the bank. Because the banks screen the companies, they gather information about different sectors and can thus better assess credit risk. Through this information gathering, they gather industry knowledge and can thus better assess the creditworthiness of the companies. The banks also screen the borrower and depending on the information acquired determine what kind of loan they should issue at what kind of interest rate. The banks thus also acquire local industry knowledge and can better determine the loan terms. All this comes down to banks' ability to issue loans at much lower interest rates than for example non-depositary FI, which do not have as much industry-specific knowledge (Marinč, 2022).

In terms of retail online banking, screening is even more important. In retail online or mobile banking, a customer can take out a loan through an application. This would not be possible without screening. The lender (in this case the bank) has enough information about the customer, which enables them to have enough information about his financial status to issue a loan. In this case, the bank would issue a loan to its long-term client, with whom they have years of financial experience. This is also referred to as know your customer or KYC (Rao, 2014).

1.4 Moral hazard problem and monitoring

After the loan is issued the borrower can take actions that damage the interests of the lender. This is called the moral hazard problem. An example of the moral hazard problem occurs when a borrower borrows a loan for a project, but then at once uses it for a different riskier project. By doing this, they trick the lender and mislead the bank. The borrower essentially increases the risk of a loan immediately after they borrow.

Banks tackle this information asymmetry by monitoring. Monitoring refers to the *ex-post* gathering of information about the borrower. For example, banks monitor their borrowers by continuously examining the borrower's business and financial health. Depending on the loan agreement, they can also intervene in the operating strategy of the business when applicable. Similarly, venture capitalists (which are a form of non-depository FIs) use a threat to transfer control of the company. This is so that entrepreneurs' and investors' incentives do not diverge too far from each other (Greenbaum, Thakor, and Boot, 2019).

1.5 Bank lending protocol in traditional finance

1.5.1 Elements of bank lending protocol

Bank loan agreements have a lot of elements that need to be agreed upon before issuing a loan. The first one is the amount being loaned out, often referred to as the principal of the loan. Here is important that not too big of an amount is loaned out as the required interest on the loan would be too high for the borrower to pay interest payments and the loan would need to be refinanced. Loan refinancing means that another loan would be needed to pay off the outstanding loan (Wamala, 2021). The second element is the pricing formula or the interest rate of the loan, this can be either a floating or fixed interest rate in TradFi. In the case that the interest rate is floating, it could be "prime-plus" (e.g. prime rate plus 0.5 %) or "times-prime" (e.g., prime rate times 1.1). The interest rate could also be at a "transaction rate" where the bank agrees to a fixed markup over a current money rate (e.g. T-bill). The third element is the term of the loan or the maturity. This refers to the duration of the loan, during which the loan would be paid back. There are three different maturities of a loan: short-term (less than 1 year), intermediate-term (1-5 years), and long-term (more than 5 years) (Greenbaum, Thakor, and Boot, 2019).

Another section of a loan agreement is the conditions precedent section which includes requirements that the borrower needs to satisfy before the bank can legally issue a loan. These conditions can be specific business transactions like sale deals going through or events that must occur beforehand like a board approval. The loan agreement also has a warranties section which consists of information about the borrower's creditworthiness and legal status. When the loan is executed, the borrower is held accountable for the accuracy and the truth of the information provided. The borrower signs that the assets and collateral are owned by him and that he is not involved in any litigation. The bank would also want to know the purpose of the loan. Here agreement is reached between the lender and the borrower on what the loan will be used for. An element of bank loans is also any additional fees associated with the loan. Such as the application fee, processing fee, origination fee, annual fee, late fee, prepayment fee, etc. (Pritchard, 2021). In the case of "transaction rate" pricing, there is also a closing fee when the loan is issued. This fee may be 0.25-0.375 % or even higher in a non-competitive environment. A payment guarantee is also an element of the banking loan like a personal guarantee or co-signing the loan with a high net-worth individual or a family member. Banks can also take something for collateral such as real estate, vehicles, or inventory (Scottish Enterprises, 2022). Debt covenants also represent a section in a bank loan agreement. This is how banks make sure you use the money for the purpose of the loan as the borrower agrees with the bank that certain activities will or will not be carried out (Hayes, 2022). Essentially, covenants make sure that borrowers adhere to the warranties – actions that they signed they would undertake. In an event of inappropriate business development which do not respect the agreed-upon warranties, the bank has the right to accelerate the loan. It creates an event of default, and the bank can require premature repayment (Greenbaum, Thakor, and Boot, 2019).

1.5.2 Assessing creditworthiness

Creditworthiness is the lender's (bank) estimation of how likely you are to default on your debt and not repay your obligations. Essentially, how worthy are you to get new credit. In retail banking, creditworthiness is based on a lot of factors. In the case of US, creditworthiness is determined based on the individual's repayment history, credit score, and credit report. The credit report outlines how much debt an individual carries, including past defaults and bankruptcies. Individuals' credit score measures their creditworthiness on a numerical scale where a high score means high creditworthiness. Another factor that plays a role is payment history, as loans are usually not issued to people whose payment history shows late and missed payments or overall financial irresponsibility. The higher individual's credit score in turn means better interest rates, fewer costs, and even better terms and conditions on your loan. Individuals' employment eligibility and insurance premiums are also affected (Dhir, 2021). In the EU, your monthly income also carries a big weight when determining your credit score. In Slovenia, banks determine an individual's creditworthiness by looking at SISBON's credit rating (Banka Slovenije, 2022). There are a handful of assessments of borrowers' creditworthiness, but they are all based on multiplying the value of certain financial indicators by their weight of significance (Caplinska, 2020).

Creditworthiness is also denoted as credit risk or default risk. In the case that a borrower defaults on a loan or a lease, it causes the bank to lose the principal along with any potential interest earned. Banks management determines loan-loss provisions, a pool of allowance for loan and lease losses (Wagner, 2021). Furthermore, credit-rating agencies determine the creditworthiness of sovereign nations, local and state governments, and corporations. However, after the 2008 financial crisis, they received a lot of criticism as they gave good ratings to bad mortgage-backed securities. A conflict of interest arose as the issuers of these securities paid agencies for a good rating; thus, these agencies were reluctant to give low ratings so that they would continue to receive payments. These ratings are used for structured finance transactions such as beforehand mentioned mortgage-backed securities and collateralized debt obligations. The agencies also rate bonds from emerging and developing countries, it thus helps them as the governments of these countries are then able to sell bonds and obtain financing from Word Bank and the International Monetary Fund (IMF). Corporations that want to issue securities need to find a rating agency to rate their debt (CFI Team, 2022).

1.5.3 Interest rates of bank lending protocol

Interest rates are one of the most crucial elements of bank lending as their entire business model evolves around them. Interest income poses the highest percentage of revenue streams for the bank (Wagner, 2021). However, before we discuss interest rates in banking, we must first deep dive into their background to see how they are set. Interest rates are usually calculated as a market reference rate plus an interest rate spread. Market reference rate or benchmark rate can differ from country to country. In the US the most common market reference rate is the federal funds rate, in the UK, it is the LIBOR rate, and, in the EU, it is the EURIBOR rate. This is also the interest rate that commercial banks charge on money lent to another bank to keep their reserve requirement. The reserve requirement is the smallest amount of a bank's deposits that need to be held in cash and not loaned out to the borrowers. This requirement is set by the central bank, in the case of the US that is the Federal Reserve System or FED. Similarly, they also set the federal funds rate with which they help to stabilize the economy and enforce their monetary policy. Banking institutions are viewed as the second most creditworthy entities in the economy, right after the governments. Thus because of the lowest default risk, interest rates on loans are the lowest. The second lowest interest rate is called the prime rate. This is the rate for customers with high creditworthiness like large corporations or high net-worth individuals. If the benchmark rate increases, so do the prime rate and the retail interest rate that the individuals borrow in retail banking (CFI Team, 2020a).

There are two kinds of interest rates – floating and fixed interest rates. A floating interest rate is a variable interest rate that changes over the term of the loan. Conversely, the fixed interest rate stays constant throughout the term of the loan. The reference rate for floating interest rates is normally the prime rate or SOFR (in the past it was LIBOR). Floating interest rate debt is normally cheaper than fixed interest rate debt as it is generally perceived that the interest rates will rise over time. However, floating interest rate debt can be more expensive than fixed interest rate in the case that the yield curve is inverted (CFI Team, 2020b). Yield curve is a line that plots interest rates of bonds with equal credit quality but different maturities. Normally, interest rate should increase with bigger maturities, however in an inverted yield interest rate decrease with bigger maturities.

One of the most important risks that banks need to manage and be aware of is the interest rate risk. Interest rate risk is the management of the spread between interest paid on deposits and received on loans over time (Chen, 2021). When interest rates fall, the deposit interest rates increase faster than rates on fixed-rate loans. This is because assets and liabilities have an unequal duration (Greenbaum, Thakor, and Boot, 2019). In this case, deposits are typically short-term investments and fixed rates are long-term investments. To eliminate the interest rate risk, one could equalize the durations of assets and liabilities. However, by doing so the bank would need to renounce any premium embedded in the yield curve (Greenbaum, Thakor, and Boot, 2019). That is why interest rate risk is hedged using interest rate derivatives such as interest rate futures, swaps, and options (Chen, 2021).

1.5.4 Liquidity of bank lending protocol

The liquidity of bank lending has already been discussed in earlier chapters. In the banks as FI theory, the liquidity is constrained by the sum of the depositor's funds in the liquidity pool. The fractional reserve banking theory adds on top of that, as the liquidity is constrained by the reserve requirements, but it is higher as they can borrow money from other banks at the benchmark rate to achieve those requirements. However, since funding rates are a lot lower than the benchmark rates, it is cheaper for banks to maintain their reserve ratio through deposits from new customers (Johnston, 2021). Funding rates are the interest rates that the banks are paying their depositors for loaning out their money (RBA, 2022). When we discussed banks as money creators, the liquidity for loans is constrained by banks' solvency and profitability preferences. The reserve requirements in that theory are not binding to the bank's ability to lend. Banks first issue the loan and then worry about the reserve requirements. Yet, banks are constrained by regulatory capital requirements. These have been implemented to make sure that banks maintain certain ratios such as a certain capital-to-assets ratio (Johnston, 2021).

Greenbaum, Thakor, and Boot (2019) have defined liquidity risk as *"the risk of being unable to satisfy claims without impairment to its financial or reputational capital"*. An example of liquidity risk is when the bank does not have access to funds that it needs, and it thus incurs costs. Liquidity risk is connected also to credit risk as the sudden need for liquidity could force the bank to sell its asset at a lower price and impair its solvency. The same could be said for interest rate risks and liquidity risks. Let's assume that interest rates increase, this could cause a bank run as depositors could withdraw their money and earn higher interest on their deposits elsewhere. Regulatory reserve requirements in a way also help prevent liquidity risk as they force banks to preserve minimum excess liquidity. The banks need to maintain reserve requirements to store liquidity in the case of a bank run. During a bank run, depositors demand their money all at once, leading to bank failure (Johnston, 2021). Liquidity risk can be managed to an extent. The bank can improve its liquidity by investing more in liquid loans and keeping more cash on hand, although at expense of profits as it cannot lend this money out. An alternative way is to reduce withdrawal risk, which is to minimize the chances of a bank running by taking necessary precautions and adhering to the necessary principles. Another way is to preserve access to as many funding markets as possible. The last way is for the bank to mitigate liquidity risk by turning to the lender of last resort which are the central banks (Greenbaum, Thakor, and Boot, 2019). Big banks lend to a big portion of the economy, meaning that if they default, they have a high chance of getting bailed out as their collapse could have massive consequences on the economy.

2 BLOCKCHAIN TECHNOLOGY

The fundamental ideas about blockchain technology appeared in a paper written by Lamport, Shostak and Pease (1982). They described a consensus model for reaching an agreement on a network of computers. Furthermore, in 1991, an electronic ledger was used for digitally signing documents in a way that could be proven that none of the signed document's contents had been changed. The above two concepts were merged in an attempt of creating a peer-to-peer (P2P) electronic cash by the name of Bitcoin in 2008 by a person under the alias of Satoshi Nakamoto. His implementation at the time marked one of the many implementations of electronic cash, but it became the most well-known. This mass adoption was contributed to the perks of the underlying blockchain technology (Yaga, 2018). Blockchain technology is a distributed ledger technology (DLT), meaning that it allows for digital information to be recorded and distributed, but not edited, altered, or deleted. Put in very simple terms, it enables efficient and secure storage of data with added features like immutability. The biggest technological challenge in P2P money transfer is the double money spending problem (Singhal, Dhameja & Panda, 2018). In the terms of digital money, this problem is solved with a central intermediary like a bank which keeps records of all transactions and makes sure the same dollar cannot be spent twice. However, the implementation of distributed ledger technology takes the approach of recording and transferring information in ledgers across all nodes of the system. The nodes synchronize between themselves and always have the latest and newest versions. Thus, the blockchain-distributed database is stored on many different nodes in a network that do not share the same geographical location. Each node carries the up-to-date database, and the user can directly check if the transaction was executed or that there was not an attempt of using the same money more than once (Rajšp, 2020).

Blockchain networks can be categorized based on their permission model into two categories – permissionless and permissioned blockchains. In permissionless blockchain networks, everyone can publish new data to the ledger, without needing permission from any authority. Anybody can also freely download them, and anybody can read or write to the ledger. Since it is open to the public, malicious users may be tempted to publish data to the blockchain with the intention to subvert the system. This is prevented by the consensus algorithms which we will discuss in-depth in later sub-chapters. In the permissioned blockchain networks, the users who publish new data must be authorized by some authority (either centralized or decentralized). Only authorized users can issue transactions. Permissioned blockchain decides who can have the access to the blockchain and who cannot. For instance, everybody can read the blockchain, but only authorized users can write to it or vice-versa. Permissioned blockchains, therefore, do not enforce consensus algorithms as only trusted or authorized users can use them. Therefore, they are protected separately. Consensus models which are employed in permissioned blockchain networks are therefore faster and less computationally expensive. Permissioned blockchain networks are often used by organizations that need to control and protect their blockchain. In these models, a single entity controls the blockchain and its users need to have trust in that entity. Furthermore, the users of these systems are not anonymous, and they can be identified, which means that they are thus disincentivized to commit fraud or behave as bad actors (Yaga, 2018).

2.1 Role of blockchain technology in traditional finance

When blockchain technology came about, it was praised as a solution to fix the supply chains, healthcare systems, and even democracy. However, it dominated the financial sector as the characteristic of the technology and thus derived benefits that tackled the problems that financial institutions face. Blockchain in finance was first introduced with the introduction of Bitcoin which was first minted right after the financial crisis on the 3rd of January 2009 as a P2P means of payment. However, at first, there were some experiments and pilot programs conducted to implement blockchain in the financial services and banking industry. These implementations fell short as it was found that in some cases centralized solutions could provide similar functionalities with lower costs and without a burden of an initial investment (Harvard Law, 2022). Yet, with time characteristics of the technology grew in popularity among the public, and the technology was thus continuously improved and worked on.

A key role of blockchain technology in TradFi is the decentralization role. Blockchain technology enables transactions without central intermediaries, currencies whose value is not controlled (with fiscal and monetary policies), and data that is private and secure. This aspect enables blockchain solutions to provide funds and liquidity for anyone from anyone, to transfer money across borders in seconds, and essentially to bank the unbanked (Harvard Law, 2022). Furthermore, blockchain's immutability and traceability serve as anti-money laundering (AML) functionalities. That is because no transaction on the blockchain can be altered, deleted, or reversed. Similarly, depending on the blockchain, all transactions are public and thus everyone can trace where the funds came from. Furthermore, its decentralized data storage and anonymousness ensure data security and privacy (AWS, 2022). Moreover, in the case of Solana, its advanced blockchain architecture enables cheaper and faster transactions thus reducing the cost and time of transactions and services (Yakovenko, 2021).

Blockchain technology is changing the way assets are transferred, stored, and accounted for. Blockchain-based currencies are being developed by companies and even countries. However, since TradFI is heavily regulated for good reasons, we come to a big question of how to regulate emerging blockchain-based currencies. To ensure financial stability this is being actively worked on by the Securities and Exchange Commission (SEC), FED, and other government officials. FED has outlined safety and soundness expectations concerning crypto asset-related issues (FED, 2021).

2.2 Functionality of blockchain technology

Blockchain guarantees the security of data and enforces trust without the need for a trusted third party. A blockchain-distributed database is shared between the nodes of a computer network. These nodes add new blocks of information to the chain and cross-reference with each other to agree upon the latest version of the blockchain. For a hacker to change a block on the chain it would be cost-prohibitive as he would need to alter more than half of the nodes on the network. This would be fruitless as it would immensely affect the blockchain which would not go unnoticed. Furthermore, the hacks could be reverted quickly through a process called forking (Hayes, 2022).

Many underlying elements achieve blockchain functionality such as cryptographic hash functions, transactions, addresses, blocks, and consensus models. Cryptographic hash functions are an important component of blockchain technology. Hashing is applying a method of the cryptographic hash function to data, which in turn calculates a unique output based on the input data we have provided. Changing the input data just slightly will result in a completely different output. Cryptographic hash functions have three important security properties. They are preimage resistant – this means that it is impossible to calculate the correct input value given an output value. They are second preimage resistant – meaning it is not possible to find an input that hashes to a specific output. Thirdly, they are collision resistant – this means that two inputs cannot ever hash to the same output (Yaga, 2018).

Transactions represent an interaction between parties. Cryptocurrencies, for example, they represent a transfer of funds between two parties on the blockchain network. Transactions are stored as data in a block on the chain and each of these blocks can store zero or more transactions. Blockchain technology also uses asymmetric-key cryptography or public key cryptography. It uses a pair of keys such as a public key and a private key which are mathematically related to each other. Many times, it is referred to as a public-private keypair. The public key is made public when doing the transaction but without the expense of security. On the other hand, the private key must remain secret to retain cryptographic protection. The mathematical relationship between the two keys does not enable the private key to be determined based on the public key. The private keys of a user are used to digitally sign transactions as only he has this key and thus nobody can sign on his behalf. This enables a trusting relationship between users who either do not know or do not trust each other. Such cryptography can be very computationally expensive, and the alternative is the use of a single secret key. It is important for the individual to store their private keys as losing them, makes them unable to access their bought digital assets. This is where wallets come in which store private keys, provide a better user experience when confirming transactions and provide the ability to calculate how many digital assets a user has. Blockchain networks also use addresses and address derivation. The address is a string derived from using a hash function on the user's public key. Addresses are then later used as the "to" and "from" endpoints in a transaction (Yaga, 2018). When the transaction is approved by the two parties, it is sent to the nodes within the blockchain network as a candidate transaction. The nodes differ from each other as they could be publishing or non-publishing nodes. Once the transaction is validated by nodes it is then distributed amongst other nodes and added to the queue of the publishing node for it to add to the blockchain. The publishing node then adds the transaction by adding a block to the blockchain. A block is structured by a block header and block data. The first contains metadata for the specific block and the former contains a list of transactions, ledger events, and any other data. The transactions are checked for validity and authenticity – such as that the transactions were signed by the private key of the holder of digital assets. The block metadata structure differs between specific blockchains, but it normally consists of a timestamp, a hash value, a nonce value, and a previous block header's hash value (Yaga, 2018).

2.3 Blockchain consensus algorithms

How to reach a consensus among nodes that do not trust each other and whom we do not trust is a transformation of the Byzantine Generals Problem which was first defined by Lamport, Shostak and Pease (1982). In this problem, a group of generals whom each commands a portion of the Byzantine army circle the city which they want to attack. The said attack would fail if only some generals attack the city. The generals need to communicate and reach a consensus on whether attack or not. But some generals might be traitors which could send different decisions to different generals. In this situation, generals do not trust each other and thus reaching an agreement in such an environment is a challenge. Similarly, it is a problem in blockchains where there are distributed nodes without a central node which ensures that ledgers on those nodes are the same. The mentioned nodes do not trust other nodes. Therefore, we need protocols and approaches to reach a consensus in the blockchain (Zheng, 2018).

Byzantine fault tolerance (BFT) is a category of algorithms that are focused on solving the Byzantine General's Problem. Their purpose is to solve the consensus problem, so the nodes are not allowed to approve random data (Bach, Mihaljević & Žagar, 2018). BFT is the property of a system that can resist the class of failures derived from the Byzantine Generals' Problem. The goal of each blockchain is to defend itself from byzantine faults. A properly implemented system tolerant of byzantine faults should be able to provide services, assuming that the majority of nodes are fair. Due to the decentralized nature of the blockchain and the value of the data stored in databases, dishonest users have large economic initiatives to cause Byzantine errors in the system, which inevitably leads to the need to create a system tolerant of Byzantine errors (Zheng, 2018). In the absence of tolerance for Byzantine errors, any dishonest user can submit and confirm fraudulent transactions, which negates the key benefits of blockchain technology. The first breakthrough in the solution of the Byzantine general's problem was the introduction of a consensus algorithm called the practical Byzantine fault tolerance (pBFT), and in the area of blockchain, an algorithm called proof of work (PoW) in the Bitcoin system (Rajšp, 2020).

Practical Byzantine Fault Tolerance (pBFT) is one of the optimizations of the BFT concept introduced by Miguel Castro and Barbara Liskov. For the pBFT model to work, the assumption is that the number of malicious nodes in the network cannot be equal to or greater than *n* total nodes in one vulnerability window. The pBFT model works in three phases and focuses primarily on providing a practical replica of the Byzantine machine of the current state that allows for Byzantine errors (unfair nodes) by assuming that faults and manipulated messages are propagated by specific and independent nodes. All nodes in the system communicate with each other, and the aim is that all fair nodes agree on the state of the system and check that the message sent was not manipulated in between (Rajšp, 2020).

2.3.1 Proof of work

Proof of work (PoW) is the method most popular for reaching consensus on the Bitcoin blockchain network. Users who want to validate a data block and add it to the chain must prove that they have performed "work" and essentially used a certain amount of processing power by solving a mathematical puzzle like finding a correct hash value that is less than the target value (Yaga, 2018). This is a computationally intensive process but checking whether the solution is valid is easy which enables other nodes to easily validate any proposed next blocks. Publishing nodes make slight changes to their block header like changing the nonce and trying to find a hash that meets the requirement. A mathematical problem that every publishing node faces is finding a hash value for the data in the block that starts with a specified number of leading zeros. This hash value is called the signature and they need it if they want to add the data block to the chain. Several leading zeros required are defined in each specific blockchain and adding a new block is not possible if it does not contain enough leading zeros. The number of zeros specified is called the difficulty level and determines how challenging the solution of the puzzle is. By increasing the number of leading zeros, the difficulty level increases as there are fewer possible solutions because any solution must be less than the difficulty level. The available computing power increases with time and with it also the puzzle's difficulty (Yaga, 2018).

When the difficulty target is adjusted it ensures that no entity can take over the block production, but in turn, the puzzle is more computationally expensive. Due to increased workloads for computers, there is a move to add publishing nodes to areas with a surplus supply of cheap electricity. Publishing nodes in this context are also called miners. An important aspect of this model is that more performed "work" does not increase the likelihood of solving puzzles as the puzzles are independent. What this means is that when a miner receives a completed and valid block from another miner, they need to discard their current work and start building off the newly received block as the publishing node will be building off the new block. For many PoW blockchain networks, the publishing nodes organize in pools where they work together and split the reward which incentivizes them to do the work. This means that the work can be distributed between two or more nodes in a pool and share workload and rewards. In practice, this means that each publishing node takes an equal amount of the nonce value range to tests. Dividing the work among more machines, yields better results, as the rewards are more consistent (Yaga, 2018).

The use of this difficult puzzle helps to prevent the Sybil Attack. This is a computer security attack in which an attacker creates many nodes to gain influence and control. The PoW model prevents this by having the focus of network influence being the amount of computational power combined with chances. The computational power costs money and more hardware increase the likelihood, but it does not guarantee it (Yaga, 2018).

2.3.2 Proof of stake

The proof of stake (PoS) algorithm is designed in such a way that it overcomes the computational extensiveness of the PoW algorithm in the process of mining (Baliga, 2020). The PoS model comes from the idea that the more stake a user has invested in the system, the more likely they will want the system to succeed, and the less likely they will want to sabotage it (Yaga, 2018). Stake, therefore, represents the user's share or the amount of cryptocurrencies, which represents the amount of ownership, that the user has in the system. Normally, once cryptocurrencies are staked, the staked cryptocurrency is not able to be spent. PoS blockchain network uses the user's stake as a determining factor when publishing new blocks. Therefore, the more staked cryptocurrency a user has, the higher the likelihood of the user publishing a new block. Since this model uses fewer resources like time, electricity, and processing power than PoW, these systems are designed so all the cryptocurrencies are already on the open market. This is contrary to before where cryptocurrency was being "mined" or generated at a constant pace in exchange for doing the "work" in the PoW consensus algorithm. In such a system, the incentive to mine is therefore the transaction fees paid (Yaga, 2020). Ethereum blockchain moved from PoW to PoS at the time of writing this thesis.

There are four different methods of how the blockchain network can use stakes. Random selection of staked users is when the block publisher is determined at random. The blockchain network will look at all the users with stakes and choose the likelihood of the user being chosen would be the same as their stake. In the case of a multi-round voting system, the process is more complex. The blockchain network selects several users with stakes to create new proposed blocks. Then all staked users will cast a vote for a proposed block. There might be many rounds of voting before a new block is decided upon. This approach allows for all the stake users to have a voice in the block selection process. Another method is a coin age system where stake cryptocurrency has an age property. The longer the user stakes its currencies the higher the likelihood of being chosen as a block publisher. The age is then reset, and the user has a cooldown period before it can be used again. This enables the users with more stake to publish more blocks but not to dominate the system as their age counter resets and they need to endure the cooldown time. To prevent the hoarding of cryptocurrencies there are set maximum limits. Another system is the delegate system, where users vote for nodes to become publishing nodes and create blocks on their behalf. Their voting power is held to the stake, meaning that the larger the stake, the larger the voting power. The most voted nodes become publishing nodes and can validate blocks. The threat of losing publishing nodes' status is constant as this system is incredibly competitive as the established published nodes can also be voted for removal. This incentivizes them to not act against the system. Normally, network users vote for delegates who take part in the governance of the blockchain – meaning they propose new changes and improvements, which will be voted on by blockchain network users. In PoS, wealthy individuals might stake more of digital assets and earn more in return but acquiring control of a system is cost-prohibitive (Yaga, 2022).

2.3.3 Proof of history

In the blockchain, any source of time, such as an atomic clock, is seen as an outside third party. With network delays and relativistic effects, most clocks have slight delays (Pierro & Tonelli, 2022). Proof of History (PoH) is a consensus algorithm presented in Solana's whitepaper (Yakovenko, 2022). It uses a sequence of computations that provides a way to cryptographically verify that an event has occurred before or after another event. It is essentially a cryptographic clock (Tyson, 2022). A cryptographically secure function such as SHA-56 is used so the output cannot be predicted from the input (Shoup, 2022). The function is run every time a new transaction is recorded on the network, and it uses its previous output as the current input. It then periodically records the current output and how many times it's been called. The output is then recomputed and verified by external computers ran in parallel by checking each sequence segment on a separate core. The data is timestamped into the sequence by appending the data into the state of the function. State, index, and data provide a timestamp and a guarantee that the data was created sometime before the next hash was generated in the sequence. Furthermore, this process enables horizontal scaling as multiple generators can synchronize with each other (Yakovenko, 2022).

Put simply, a cryptographic hash function is run on a random starting value and the hash output of that function is then used as an input for the next same function. This is done periodically and the *hashN* represents the actual hash output where *N* is the current index at the current time *T*. As long as the hash function chosen is collision-resistant, this set of hashes can only be computed in sequence by a single computer thread. As there is no way to predict what the hash value would be at index 400 without running the algorithm 400 times. Thus, we can say that time has passed from index 0 and index 400. In a practical example, one event's hash value could be at index 100 and the other could be at index 500, this means we can trust that real-time passed between these indices and therefore these two events (Yakovenko, 2022). The sequence of hashes can thus also record that some data was created before a particular hash index was generated. We can use this timestamp for events. The use of the "combine" function, combines the data with the current hash at the current index. The data can be a unique hash of arbitrary event data. The "combine" function could be any operation that is collision-resistant. The next generated hash is the timestamp of data, as it could have been generated after that specific piece of data was inserted (Yakovenko, 2022). Although the amount of time that has passed seems very inexact and the amount of computation required to verify such a proof of history is very high (Shoup, 2022).

PoH consensus algorithm is used in the Solana system, where a single Leader also denoted as a PoH generator, receives the transactions. The PoH generator checks the transaction hash, it checks if the account balance is enough to pay the transaction fee, and assembles all the valid transactions to generate the PoH sequence. All the invalid transactions (e.q. if there is insufficient balance) are dropped. Since the PoH generator is a single entity, the system achieves decentralization through an algorithm that elects a new Leader after a certain number of blocks. The PoH generator executes transactions and publishes them with a signature of the final state to nodes called Verifiers. Verifiers can split the transactions between each other and thus verify the transactions in parallel. PoH sequences can thus be easily verified by multi-core computers (Verifiers) compared to the time required for the Leader to generate them. If a malicious PoH generator is detected by a two-thirds majority of the Verifiers, the PoH generator loses its role, and an election is performed to pick up the position of the malicious PoH generator. State generation is dependent on a single machine thus the speed of the system will scale with Moore's Law. Meaning that the better the underlying computing hardware, the higher the TPS of Solana's system. Solana believes that it can achieve a theoretical speed of 710 000 TPS in the future (Pierro & Tonelli, 2022).

2.4 Solana blockchain technology

Solana's blockchain design strives to solve the blockchain trilemma. A concept that explains that no blockchain can have all three – scalability, security, and decentralization (Shilina, 2022). It is a blockchain network that brings tremendous improvement to the performance of traditional blockchain and makes scalable enterprise applications possible (Li, Wang, Kong, Zheng, & Luo, 2020). Yakovenko first outlined the Solana blockchain in a white paper with a theoretical speed of 50 000 TPS (Yakovenko, 2022). Many innovations play a role in achieving a high TPS rate, but the use of the PoH consensus algorithm plays a significant role. Key innovation also introduced by the Solana team is the Tower BFT which is a PoH-optimized version of pBFT. In their implementation of pBFT, they use PoH as the network clock which provides exponentially increasing time-outs to be used in pBFT. These can be computed and enforced already in the PoH function (Duffy, 2022). The list of technical innovations introduced by the Solana Team can be seen in Appendix 2.

In functionality, Solana resembles Ethereum – both keep the core principles of Bitcoin but they drastically expand their capabilities by introducing smart contracts. Smart contracts allow for specifying the business logic on top of the blockchain infrastructure (Frankenfield, 2021). Solana is much more user-friendly compared to other networks. It features low transaction fees, fast confirmation speed, and high performance. Solana offers a static near-zero fee for all transactions regardless of the amount paid. Furthermore, the transactions can be bundled together which in turn reduces the fee even more. On the other hand, Ethereum transaction fees are variable. They are a subject of network congestion and the complexity of invoked smart contracts. Similarities and differences between Solana, Ethereum, and Bitcoin can be seen in Table 1.

Table 1: Comparison of Solana, Ethereum, and Bitcoin.

	Solana	**Ethereum**	**Bitcoin**
Theoretical TPS	50000 TPS	15 TPS	7 TPS
Actual TPS	3139 TPS	15 TPS	7 TPS
Transaction Fee	0.00001 USD	10 USD	~ 1 USD
Transaction Finality	0.6 (1 block)	8 min (30 blocks)	1 hour (6 blocks)
Consensus Algorithm	PoS and PoH	PoW[1]	PoW
Scalability with hardware	Yes	No	No
Supports smart contract	Yes	Yes	No
Difficulty of development	High	Low	No smart contracts.
Support for concurrency	Yes	No	No

Adapted from Bodziony, Jemioło, Kluza & Ogiela (2021).

To conclude, Solana's unique architecture consisting of Proof of Stake, Proof of History, and an optimized BFT algorithm makes scalability native to the blockchain. Solana's theoretical TPS is higher than that of Visa and Mastercard which can be seen in Table 2 (Yakovenko, 2022).

Table 2: Comparison of Solana, Visa, and Mastercard.

	Solana	**Visa**	**Mastercard**
Theoretical TPS	50000 TPS	24000 TPS	5000 TPS
Actual TPS	3139 TPS	3941 TPS	2486 TPS
Transaction Fee/Provision	0.00001 USD	0,2 – 1,75 %	0,2 – 2,2 %

Adapted from Solana Explorer (2022); Rajšp (2021).

Solana's extremely fast, low-cost, and highly scalable blockchain makes it an ideal technology for decentralized finance. Key issues that prevented the wide adoption of other blockchains were scalability and performance problems, but Solana's advances showed that it is possible to improve those aspects by innovating on data structure, processes, and algorithms. This is by improving various time-consuming algorithms while not forgetting

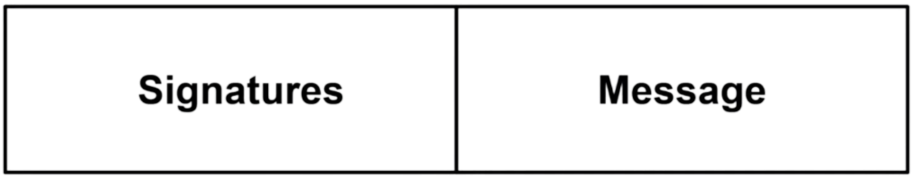
[1] At the time of writing this thesis, the Ethereum blockchain transitioned from a PoW consensus algorithm to a cheaper and more energy-efficient PoS consensus algorithm (Ethereum, 2022).

security enforcement (Li & others, 2022). Because of these features, it only makes sense to leverage Solana blockchain technology for the implementation of a decentralized bank lending protocol in this master's thesis.

2.4.1 Solana technology smart contract life cycle

This chapter seeks to analyze Solana's smart contract life cycle at a high level. Smart contracts are essentially just programs. A chunk of code that enables some action to be performed once specific criteria are met. However, as such, they are crucial as, without them, the decentralized finance world would not be possible. Transactions are created on the client side. They are combined of signatures and messages as it is shown on Figure 1. Signatures are an array of the user’s private keys made for the transaction. The message is a payload of information that we send to our smart contract (Solana Team, 2022a).

Figure 1: Structure of the Transaction object

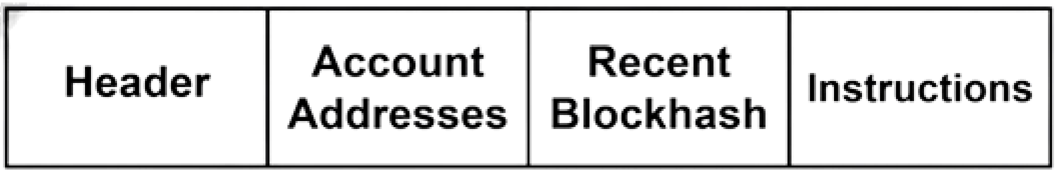


Signatures	Message

Source: Solana Team (2022a).

On Figure 2 it is shown that the message is comprised of the header which holds the data (like the number of signatures, accounts, etc.) that is associated with the transaction. The account address is an array of accounts that we are interacting with. The recent block hash is the hash of the last observed blockchain ledger that made the transaction. Instruction is an array of data used by smart contracts to complete the transaction. It is essentially where developers' smart contract logic is stored so that Solana processes it and knows what to do.

Figure 2: Structure of the Message object

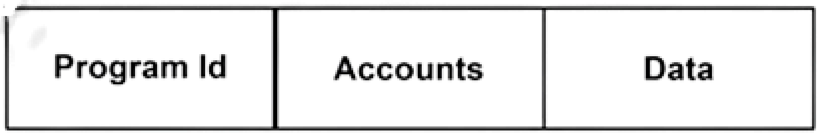


Header	Account Addresses	Recent Blockhash	Instructions

Source: Solana Team (2022a).

Figure 3 shows that instructions have three fields. A program id is the id of the smart contract we save on a Solana Network. Accounts are an array of accounts that contain state information for the user. They keep track of the state on a Solana Program, which is stored on the blockchain similar to a file on a hard drive. Accounts have a lot of fields such as who the signer is and the rent that needs to be paid for our program to live on the Solana Network. Data is a byte array that the program will use to handle each transaction.

Figure 3: Structure of the Instructions object



Source: Solana Team (2022a).

As mentioned, Solana Program Data in Figure 3 is stored in a separate buffer account. This architecture in turn enables a feature that Ethereum blockchain does not have. The architecture enables upgrading of our smart contracts and redeploying them to the Solana Network. Upgrading a smart contract means that we can add new features and capabilities to our existing smart contract. This means that the code for smart contracts can be changed but the existing data is preserved. In a blockchain technology like Ethereum, an existing smart contract cannot be easily redeployed to the network as the acquired data like users would be deleted, thus we are limited to the functionality of the smart contract that was developed and deployed at the start.

2.4.2 Solana technology stack

Rust programming language differentiates from other C-family of programming languages. It encompasses memory management language features like borrowing, referencing, and ownership. These security features force developers to handle data allocations when developing the software. Although it increases the development time of the developer, it makes the software fast at runtime as it does not need to recheck conditions when the program is already running. Because of its security and speed, it is used for writing software like operating systems, and web servers, or in our case, it is used for Solana blockchain technology. The program also uses traits, lifetimes, and concurrency which makes it even more powerful (Rust Team, 2022a). Since there is no point in rewriting reusable code, developers import code from other developers to reuse generic logic. Packages of generic code are called crates in Rust and are managed by the Cargo package manager. Cargo manages the dependencies of our program. The dependencies are other packages of code that our code depends on. It ensures that the program uses specific versions of our dependencies because otherwise, the dependencies could have new changes which could crash our program. Cargo also manages the crates so they cannot be deleted in any way (Rust Team, 2022b). Anchor framework is a new library that offers us a much simpler development of smart contracts on Solana. It offers a set of reusable functions, which help us greatly while working with the Solana blockchain. For example, we are not required to serialize and deserialize data as Anchor handles that part for us. Furthermore, it also offers a set of commands for initializing, testing, and deploying our project (Rust Team, 2022c).

This chapter performed a technological deep dive into the blockchain technology itself and its early use cases in the traditional financial system. It discusses blockchain technology functionalities and different approaches for reaching consensus of the latest information. Furthermore, it also compares different blockchains between themselves and outlines why Solana blockchain technology native scalability makes it attractive for developing scalable DeFi solutions. The chapter also discusses Solana's programming model which will be useful for understanding the implementation of our software solution in-depth.

3 DECENTRALIZED FINANCE

Decentralized finance (henceforth DeFi) is an ecosystem of blockchain financial applications without any third-party or central administration intervention (Leeway Hertz, 2022). The total value locked (TVL) in DeFi was approximately 230 billion USD on March 29th 2022. On Ethereum, blockchain lending represented 47,4 billion USD in TVL, decentralized exchanges (DEXes) 24,95 billion, assets 17,19 billion, derivatives 2,21 billion, and payments 1,89 billion USD, respectively (Statista, 2022). Having said that, the DeFi ecosystem is no stranger to asset management applications, insurance, and the like (Leeway Hertz, 2022). DeFi technologies provide an alternative to traditional financial approaches. They are based on a public blockchain on which transactions are recorded and where smart contracts operate. Smart contracts are at the core of the system, and they are essentially just programs that are executed once the transaction is initiated (IOSCO, 2022). Once initiated the smart contracts execute through the blockchain network and change for example the balance of crypto assets in the user's wallet. However, smart contracts are at the core of DeFi and without them, DeFi would not be possible. They are self-executing programs that require no intermediary oversight, and which run only once all predetermined conditions are met. Smart contracts are written by developers, meaning that they allow for all kinds of functionality such as implementing lending, trading, and derivatives, to say the least. DeFi offers financial services to anyone who has an internet connection (Leeway Hertz, 2022).

DeFi products and services are created with smart contracts, which operate in a stack of technologies that interact with each other. On each of the stacks, products and services are offered. The technology stack of DeFi can be separated into five major layers: settlement, asset, protocol, application, and aggregation layer. The foundational layer, the layer on which all blockchains are, is the settlement layer (also called Layer 1). The blockchain layer features consensus algorithms as the ultimate source of truth for the validity of the transaction and other means which agree on the order in which transactions will be settled (Dionysopoulos et al., 2022). The asset layer consists of different types of tokens with different functionalities such as governance, utility, non-fungible tokens (NFTs), coins, and so on. These assets or tokens are created through standardized smart contract specifications such as ERC-20 or ERC-721 standards for the Ethereum blockchain. The protocol layer or smart contract layer is where financial use cases are created (IOSCO, 2022). It encompasses DeFi protocols or services such as exchanges, lending, and derivatives … Here independent smart contracts live that dictate the rules of the protocol. The application layer consists of a standard internet user interface. This interface consists of for example wallets such as MetaMask in Ethereum blockchain and Phantom in the Solana blockchain. They enable a user-friendly way to sign transactions (Dionysopoulos et al., 2022). The application layer also consists of protocol-specific interfaces like websites, applications, and bots. All these layers encompass on-chain functionalities, but when an application requires outside data such as exchange rate information it is provided by oracles. Data that is acquired from outside of the blockchain ecosystem is denoted as off-chain data.

3.1 Benefits and drawbacks of decentralized finance

Because of the blockchain functionality and its characteristics, DeFi offers many benefits. The benefit that stands out the most is permissionlessness as it enables access to capital and markets to all people with an internet connection. Another benefit is decentralization. In TradFi each transaction is validated by a third party like for example a bank. In DeFi each transaction is rather verified by multiple nodes. Furthermore, banks need a lot of time to process certain transactions and they would even not execute some of them. May it be because the transaction started after hours or because they have flagged a transaction. However, in the blockchain network, a transaction can be conducted between any P2P without authentication by the central agency (Zheng, 2018). Blockchain technology offers immutability and persistence as the data stored on the blockchain cannot be changed. The only way one could do that, would be if the hacker altered 51 % of the nodes on the network which would take unacquirable resources and would be rendered useless as the hacks could be reverted quickly by forking to the past unaltered version of the blockchain (Hayes, 2022). Blockchain offers anonymity, each user interacts with the blockchain network with a generated address. The user's private information is no longer kept by the bank. Furthermore, the technology empowers the users and allows them to control their information and information about their transactions (Gupta, 2020). The blockchain also offers auditability since each transaction on the blockchain is validated and timestamped. Therefore, users can easily verify and trace previous records about the user by accessing the blockchain ledger (Zheng, 2018). Another benefit of blockchain technology is its availability. Blockchain technology enables users to transact whenever and wherever they are. With its constant uptime, it enables users to perform transactions without being geographically or time constrained. This is contrary to TradFi where banks only process payments in a geographical area where they have branches. They however support cross-border payments, but they usually take longer and come with more constraints. Furthermore, banks only process payments during their business hours.

There is still one layer that we did not mention when we discussed the technology stack of DeFi. And that is the aggregation layer. The aggregation layer combines application layers of different protocols of the same type into a single interface. A practical example of this is the aggregation of interest rates when it comes to lending. One could see on which protocol the interest rate is the highest and invest their money there (Dionysopoulos et al., 2022). However, this layer brings us to a minor example of composability but a major benefit for DeFi. Composability or money Legos allows developers and users to treat DeFi primitives as independent financial building blocks with which other financial services can be built (Saengchote, 2022). The system's building blocks can freely interact with one another and form new services.

The benefits of DeFi do not come without drawbacks. Since DeFi technology is still at its beginnings, it is therefore immature and has yet to be fully stress-tested at scale over an extended period (Vistra, 2022). In the case of Bitcoin and Ethereum blockchain technology, transactions proved to be expensive at times of congestion. In the case of Solana blockchain technology, occasional network outages were present. Contrary to traditional financial systems, DeFi systems offer services anytime and anywhere. In DeFi, all actors are also pseudo-anonymous, which enables privacy but restricts KYC. This is because we are unable to do due diligence on the actor as it is done in traditional banking. As trust between the actors is not established, DeFi services operate with high leverage (Vistra, 2022). As some blockchain technologies are public, so is their smart contract code which specifies how the protocol will behave. Lack of legal framework, lack of KYC, public protocol code, pseudo-anonymity and constant uptime make DeFi an ideal system for hacks and other types of exploit attacks.

To conclude, DeFi allows a cheaper and more robust approach to data privacy and transparency, it allows for 24-hour financial services and decentralization. In the case of Solana, DeFi applications also offer cheaper, more efficient, and faster transactions. Transactions on the blockchain are also public and everyone can see who the sender and the receiver were for the specific transactions (granted if the specific blockchain and platform support that) (Hayes, 2022). Moreover, blockchain technology enables instant asset traceability, meaning that it is easy to follow where the assets went. Furthermore, transactions can also be automated securely with smart contracts. For example, a smart contract specifies that a transaction is triggered only once all conditions are met (IBM, 2022).

3.2 Stablecoins

Cryptocurrencies in the context of DeFi do not serve as an effective unit of account and it thus hinders their ability to be widely used as a medium of exchange, which is one of the basic functions of money (Dionysopoulos et al., 2022). We will discuss the reasons for this in the next chapter, but for now, it is enough to know that crypto assets' value is extremely volatile which translates to high exchange-rate volatility. Considering this, a new digital currency (or a type of token) emerged known as stablecoins. Stablecoins aims to counter the volatility of cryptocurrencies and establish a blockchain-native unit of account without sacrificing the most vital characteristics of DeFi, which are composability and programmability (Dionysopoulos et al., 2022).

Stablecoins are cryptocurrencies that are pegged to another currency, commodity, or financial instrument. We can categorize them based on their degree of centralization and the mechanism they use for maintaining their peg. In terms of centralization, we identify centralized stablecoins (otherwise known as custodians) and decentralized (non-custodian) stablecoins. Centralized stablecoins are maintained by centralized entities which maintain off-chain collateral which is backing the stablecoin. The collateral usually represents money or money equivalents, and the stablecoin is just an on-chain representation of the value of this collateral. The characteristics of such stablecoins are that they are efficient, and censorship-prone, they have a single point of failure but lack transparency and auditability. However, they are deployed on open blockchains and are still composable, programable, and accessible. These types of coins also introduce holders to counterparty risk since they are essentially IOUs. On the other hand, there are decentralized stablecoins, which rely on on-chain collateral and smart contract-backed algorithms which maintain their peg. In TradFi they could be thought of as risk-transfer instruments such as collateralized debt obligations. This means that they are in turn less capital-efficient, but transparent, censorship-resistant, and accessible (Dionysopoulos et al., 2022).

Stablecoins differ in terms of the mechanism with which they achieve their peg. We know reserve-backed, collateral-backed, algorithmic, and mixed approaches. Centralized stablecoins are often reserve-backed, whereas decentralized stablecoins rely on an algorithm or on-chain collaterals. Collateral-backed stablecoins are oftentimes pegged to fiat currencies like the USD (cryptocurrency USDT). This type is called fiat-collateralized stablecoins. As such they are less volatile compared to normal cryptocurrencies making them a medium of exchange and thus, they play a major part in DeFi and lending. Furthermore, they empower DeFis composability (Saengchote, 2022). Stablecoins manage to remain pegged to a currency by maintaining a reserve. Crypto-collateralized stablecoins maintain a reserve of other cryptocurrencies. As the reserve of cryptocurrencies may be highly volatile, these kinds of stablecoins are oftentimes over-collateralized. The last type of stablecoins is algorithmic stablecoins which do not necessarily have reserves. They however peg the value by controlling the supply through a computer algorithm (Hayes, 2022).

3.3 Crypto assets

Crypto assets (also referred to as cryptocurrencies, digital assets, or non-stablecoins) encompass a large and diverse group of tokens. We will not discuss them too much in-depth as the purpose of this thesis is not to get a throughout knowledge about each cryptocurrency but to focus on lending in DeFi. First, we can isolate platform-native cryptocurrencies used for transaction purposes or as a store of value. Under this group fall the first generation of cryptocurrencies such as the first cryptocurrency Bitcoin, Litecoin, Ripple, and more. These cryptocurrencies are built on non-smart contract platforms and most of them are based on PoW blockchains. At first, enthusiasts hoped that these cryptocurrencies could replace fiat currencies as a transaction medium, but PoW ledgers had proven to be slow and expensive when it comes to confirming transactions (Makarov, 2022). The second generation of cryptocurrencies solved this problem and even led the way for smart contracts. Here we are talking about Ethereum decentralized platform which constituted smart contracts and thus allowed developers to write their customized transactions. But because the adoption of DeFi skyrocketed, the Ethereum blockchain could not support the number of microtransactions. This is where the third generation of cryptocurrency networks came in, such as Cardano which tried to optimize this process (Rajšp, 2019).

However, all of these cryptocurrencies are just tokens residing on the asset layer of the DeFi technological stack. A process called tokenization also enables real-world assets to be presented on-chain such as currencies, securities, real estate, etc. These assets become tokens on the chain and their holder would thus have ownership over them. They could be traded or hedged against. Utility tokens enable user access to a product or a service, but they are used only in a closed ecosystem and are not designed for investment purposes. They are normally issued to raise financial resources for the further development of blockchain applications (Civiero, 2020). However, there are governance tokens which are a kind of utility tokens that give voters voting power on the next features of the protocol. Governance will be discussed in later chapters. There are also security tokens which are digital assets that represent transferred ownership rights or asset value to a blockchain token. Security tokens are created using before mentioned tokenization in which the investment criteria are selected. The information is then entered into the blockchain which in turn creates a token. They are not available to retail investors, but many institutions are working to develop and offer them. The SEC must approve security tokens before issuance (Majaski, 2022). There are also non-fungible tokens (NFTs) which represent a unique token that another digital asset cannot replace. The data can be associated with either a digital or physical asset. Furthermore, it can represent texts, drawings, images, etc. Because each token is uniquely identifiable, NFTs differ from cryptocurrencies. However, they can also be bought and sold, and are seen as a form of digital art (Makarov, 2022).

3.4 Lending in decentralized finance

Before we research lending in DeFi we must first understand the driving forces behind the DeFi ecosystem development – the crypto ethos. This ethos also introduce limitations and problems which are outlined in this chapter.

3.4.1 Crypto ethos

Any services and products in the DeFi world are looked at for how well they adhere to various aspects of crypto ethos. There are four key crypto ethos: decentralization, composability, permissionless, and sovereignty. Decentralization means to what extent can the system be controlled by a few dominant parties. Decentralization is at the core of DeFi as removing central intermediaries (like a bank in TradFi) is the driving force behind creating a new financial system – DeFi (Baker, 2022). Decentralization branches into three separate axes: architectural decentralization, political decentralization, and logical decentralization. Architectural decentralization means how many physical computers is the system made up of. Furthermore, it looks also into how many of those computers can the system tolerate breaking down at any single time. Moving on we have political decentralization which explores how many individuals or organizations control the computers that the system is made up of. Lastly, there is logical decentralization which seeks to analyze if the interface and data structures of the system look like a single monolithic object or an amorphous swarm. In other words, if the system, including providers and users, is cut in half, will both halves continue to fully operate as independent units (Buterin, 2017).

The next crypto ethos is composability, which explores how easy is it to integrate the DeFi service with other protocols. For example, stablecoins are an essential building block that DeFi services leverage as stablecoins represent a single unit of money. Moreover, there is also the permissionlessness aspect which looks at how reliant is the system on gatekeeping or third-party authorities. On the spectrum of permissionlessness aspect, the more permissionless a protocol is the better, meaning that there are no third parties who censor and keep people out of the protocol. In a permissionless blockchain, the public validates transaction information through consensus algorithms. Last is sovereignty which focuses on how much control a user has over their identity (Baker, 2022). This aspect goes hand in hand with data privacy as the user wants to be in control of his data and his credentials. Sovereignty is achieved in the latest's blockchains by users opening an account without any identity verification. Users are essentially pseudo-anonymous as their account is only stored as an address to which funds can be sent. This means that nothing is preventing them from taking out a loan, transferring funds to their bank account, and then opening a new account and repeating the process. This action is called Sybil borrowing and will be discussed in-depth in the following chapter.

To conclude, crypto ethos is highly important in the DeFi world as it can be seen as an ideology of the DeFi system and as a design and implementation guideline. They give excellent insight into why certain protocols are designed and implemented in a certain way. Crypto ethos will be discussed in detail for each mechanism of the lending protocol.

3.4.2 Sybil borrowing

Sybil borrowing is an act of taking out loans on behalf of anonymous or disposable entities and then defaulting without an impact on creditworthiness. Before globalization and modern record-keeping, Sybil borrowers were common in the real world. For instance, in 18th-century Europe it was possible to accrue unpaid debt in England, then flee to France and begin again under a new name (Vause, 2021). However, this evasion comes with difficulty and personal sacrifices. In the case of DeFi, users are essentially pseudo-anonymous as they can open an account without any identity verification. This goes back to the sovereignty aspect of the crypto ethos. But this means that nothing is preventing them from taking out a loan, transferring the funds to their bank account, and then opening a new account and repeating the process. This means that Sybil's borrowing can essentially be performed as easily as in a few clicks without repercussions like fleeing the country and starting a new life. Sybil's borrowing essentially boils down to the question *"Why should not I take the money and run?"* (Baker, 2022).

In TradFi Sybil borrowing is prevented as penalties for defaulting are sufficiently harsh that few consider doing so voluntarily. Some of these are ruined credit scores, increased future borrowing rates, or even denials of credit that would follow. Furthermore, banks perform thorough screening and monitoring to minimize credit risk. In the DeFi world, minimizing credit risk through credit scores is not optimal as it goes against the sovereignty aspect of the crypto ethos. Since the protocol needs to have identifying information about the borrower. Furthermore, the concept of a credit score presumes a well-defined entity to which that credit score is assigned. In DeFi accounts are not well-defined entities but rather an address. The protocols that will aim to provide loans to retail customers will need to solve the issue of identity in addition to that of credit risk (Baker, 2022).

3.4.3 Economic problem

There are already various approaches that solve Sybil's borrowing. The most popular approach is the over-collateralization approach which does not come without its faults. Overcollateralized protocols represent the vast majority of the DeFi lending market. These protocol approaches will be discussed in-depth in later chapters, for now, it is enough to understand that to get a loan in this kind of protocol one needs to put up a collateral of higher value. In this case, the Sybil borrowing is solved through financial incentives as a form of economic security: users will not default, because they will lose money. Every fully collateralized debt position maintains a promise: if there is a choice between giving up the collateral or the loan, the borrower prefers to preserve access to the higher-value collateral (Baker, 2022). As crypto assets are very volatile, the collateral value fluctuates heavily. The user is incentivized to put more for collateral, otherwise, it is liquidated through liquidation auctions, where other participants are rewarded by acquiring the collateral for buying out their debt position. As the underlying collateral has a higher value than the value of the loan (Gudgeon et al., 2020).

However, this approach does not come without one major economic problem. In TradFi, lending gives people more money than they have, to buy a commodity like a house or a car. At the corporate and macro levels, lending in TradFi is an engine of corporate and economic growth. However, because the borrower in overcollateralized approach cannot enter the position of net debt there is a big economic problem. A position of net debt is where you get more money out of the protocol than you put in. Essentially, the overcollateralized approach negatively affects the borrower's liquidity. Since corporations through this approach cannot enter the position of net debt, they cannot use overcollateralized lending protocol to grow and expand through debt financing like loans. In TradFi, corporations can enter the position of net debt as trust is established through due diligence, but in DeFi all actors are pseudo-anonymous and KYC is therefore extremely limited. Inability of DeFi overcollateralized lending protocols to enable loan financing and facilitate growth is the core problem of this thesis. Before this problem is resolved DeFi system will not be able to replace TradFi system.

3.5 Lending protocols in decentralized finance

The existing implementations of lending protocols in DeFi are quite different from bank lending in TradFi. At the time of writing this thesis, the leading decentralized lending protocols are Maker, Aave, and Compound with total value locked (TVL) of 8 billion, 3,2 billion, and 2,13 billion respectively (Defi Pulse, 2022). These protocols have outstanding loans of around 10 billion USD (Mayr, 2022). However, these protocols are so-called overcollateralized loans, in which the borrower puts crypto assets of a bigger value than the value of the loan they are taking out. Therefore, the borrower cannot enter a position of net debt but rather a so-called collateralized debt position (CDP). This is done as loans in the DeFi world are not used for economic growth, but rather for leveraged trading. These kinds of instruments are also denoted as Protocols for Loanable Funds (PLFs), which implement lending in a decentralized way without a central intermediary like a bank (Gudgeon et al., 2020). We will look into overcollateralized loans extensively in the following sub-chapter. Overcollateralized lending protocols exist as it is hard to establish trust and perform screening and monitoring of the lender like a bank does in the TradFi world since anyone can open a DeFi account which is inherently anonymous. However, there exist implementations of bank lending protocols which are called undercollateralized lending protocols. To my knowledge, this thesis is one of the first academic papers that outlines different lending protocol approaches in DeFi.

In the following sub-chapters we will discuss different overcollateralized and undercollateralized lending protocols as follows below:

- crypto asset overcollateralized,
- third-party collateralized (with underwriters),
- prime brokerage,
- asset collateralized and
- identity collateralized.

Protocols will be discussed based on how they perform in three key aspects: economic, business, and crypto aspects. The following sub-chapter seeks to analyze how each protocol prevents Sybil's borrowing concerning crypto ethos. Moreover, the business and scalability aspects of each protocol will also be outlined. The economic aspects of each protocol will be discussed such as the security guarantees for the borrower to not default, the effects on borrowers' liquidity, borrowers' identity, and what the credit obtained can be used for.

Explanation of key aspects regarding DeFi lending can be seen in Table 3 whereas comparison of different DeFi lending protocols based on these aspects can be seen in Table 4.

Table 4 showcases that each lending protocol fulfills two aspects but falls short in fulfilling the third. For instance, overcollateralized lending protocols are not complex in the business aspect and they adhere to the crypto ethos, but they fail on the economic aspect as the effect on the borrower liquidity is negative. Prime brokerage also fall short on the economic aspect as the credit can be used only for specific use cases. Third party lending protocols does not adhere to the crypto ethos as the permissionlessness is low. That is because due diligence of the borrower is performed off chain by third parties and only entities with permission from third parties can access the protocol to borrow money. In asset collateralized protocol the effect on borrower liquidity is negative as well. Lastly, there is identity approach which is the goal of this thesis. In identity collateralized approach the effect on the borrower liquidity is positive and it does fulfill crypto aspects, but the approach itself is complex.

Table 3: Explanation of aspects of DeFi lending

	Name	***Explanation***
Economic Aspects	*Security Guarantee*	How does the lending mechanism prevent Sybil borrowing?
	Effect on Borrower Liquidity	Does the borrower’s access to liquid capital increase or decrease?
	Borrower Identity	Who or what is ultimately responsible for repaying the loan?
	Uses of Credit	How broad is the range of uses for credit obtained?
Business Aspects	*System complexity*	How many “moving parts” are required to facilitate a single loan?
	Network Effects	How strongly does utility depend on the number and quality of participants?
	Quality Driver	What is the key aspect that governs the value of the service to the borrower?
	Scales with	Which type of participant is most critical for building a strong ecosystem?
Crypto Aspects	*Decentralization*	To what extent can the system be controlled by a few dominant parties?
	Composability	How easy is it to integrate the service with other protocols?
	Permissionless	How reliant is the system on gatekeeping or third-party authorities?
	Self-sovereignty	How much control does the borrower have over their identity?

Adapted from Baker (2022).

Table 4: Comparison of different DeFi lending protocols

Lending mechanisms	***Economic Aspects***				***Business Aspects***				***Crypto Aspects***			
	Security Guarantee	*Effect on Borrower Liquidity*	*Borrower Identity*	*Uses of Credit*	*System complexity*	*Network Effects*	*Quality Driver*	*Scales with*	*Decentralization*	*Composability*	*Permissionless*	*Self-sovereignty*
Overcollateralized	Economic	Negative	Address	General-purpose	Low	Low	Depth of Lending pool	Investors (TVL)	High	High	High	High
Prime Brokerage	Algorithmic	Positive	Address	Specific-purpose	Mid	High	Uses of capital	Partnerships	Mid-low	Low	High	High
Third-party	Sociolegal	Positive	Entity	General-purpose	High	Mid	Cost of capital	Underwriters	High	High	Low	Mid-low
Asset Collateralized	Economic	Negative	Address	General-purpose	Mid	Low	Cost of capital	Tokenization	High	High	High	High
Identity Collateralized	Sociolegal	Positive	Address	General-purpose	High	Low	Cost of capital	Credit data	High	High	High	High

Adapted from Baker (2022).

3.5.1 Crypto asset overcollateralized

In DeFi, lenders receive an interest rate on the money lent out and the borrowers need to pay an interest rate on the money borrowed. Contrary to the DeFi's definition of P2P transfers, lending is a pool-to-peer activity. People with excess liquidity deposit or stake their money into the liquidity pool (LP) from which loans are then given out. For every unit of stablecoins lent, the lenders get a platform-specific token on which they then earn interest. However, this token does not only give them just interest it also gives them governance over the proposed changes to the protocol as the protocol is decentralized (Chiu, Ozdenoren, Yuan, & Zhang, 2022).

Because of ledger-based features like anonymity, it is hard to assess the creditworthiness of the borrower as you do not have information about the person's credit rating or income. This information asymmetry makes credit risk (the risk of not getting a loan paid back) extremely high and it thus enables Sybil borrowing. Current lending protocols solve this by taking crypto assets as collateral and in exchange issuing loans of crypto-backed stablecoins. This is because, in the decentralized finance world, loans are not used for financing real economic activities but rather for collateralizing already owned crypto assets and with acquired stablecoins acquiring more crypto assets. Implemented lending protocols are most often used for margin trading (Future Learn, 2022). Thus, these crypto-collateralized loans cannot be used for real-world activities as the borrower cannot enter the position of net debt. Because the borrower collateralizes the loan with assets of similar or bigger value as he will borrow. Furthermore, the borrower oftentimes needs to overcollateralize his loan to around 150 % of the value of the loan he takes out. This is because crypto assets are highly volatile. Moreover, to ensure lender protection, platforms set a liquidation ratio of example 110 % relative to the borrowed amount. When the value of the collateral falls below the liquidation ratio the collateral is sold on the market at a discount, the lender is repaid, and the position is closed (Gudgeon et al., 2020). As the loans are issued by underlying crypto collateral, DeFi lending is inherently procyclical, amplifying boom-bust cycles. In the bull market, the collateral appreciates, meaning that the borrower can borrow more. While in the bear market the collateral depreciates, lowering the amount one can borrow and thus amplifying the drop (Aramonte et al., 2022).

Interest rates of DeFi bank lending protocols are determined based on the supply and demand of the market. In other words, the market utilization. In times of high utilization, when the supply is low and demand is high, the interest rate increases. Since the interest rates as a function of utilization are set programmatically through a smart contract, everyone can see the platform's interest rate implementations on the public blockchain. For example Compound's interest rate model is a kinked interest rate model (Saengchote, 2020). In essence, there are three main interest rate models: linear, non-linear, and kinked. In Table 5 below, we can see what kind of interest rate model each over-collateralized protocol implements. However, the interest rates are not independent, it has been shown that the

Compound Protocol's interest rates move first and Aave and dYdX follow (Gudgeon et al., 2020).

Table 5: Elements of overcollateralized DeFi Protocols

Overcollateralized Protocols	**Interest Rate Model**	**Fixed Interest Rate**	**Variable Interest Rate**	**Governance Token**	**Interest-bearing Derivative Token**	**Additional Functionalities**
Compound	Kinked	NO	YES	YES	YES	-
Aave	Kinked	YES	YES	YES	YES	Swap rates, flash loans
dYdX	Non-linear	NO	YES	NO	NO	DEX, flash loans

Adapted from (Gudgeon et al., 2020).

To conclude, Sybil's borrowing is prevented using economic incentive – the over-collateralization of the loan. Users will never default on the loan as the value of the collateralization is higher than the value of the loan. Unfortunately, this means that this protocol fails in achieving the economic aspect of the TradFi loans. The borrower cannot borrow against their future cashflows as the loan needs to be fully collateralized upfront. Furthermore, the capital inefficiency of the collateral is often idle and unproductive (Baker, 2022). On the other hand, overcollateralized lending does achieve all the aspects of crypto ethos. Anybody can lend to, borrow from, or build atop the protocol, without the requirements for identifying information or third-party gatekeepers (Baker, 2022).

3.5.2 Third party collateralized (with underwriters)

Overcollateralized lending dominates the DeFi lending market, but so-called undercollateralized lending is growing rapidly. The third-party collateralized lending protocols represent the first undercollateralized approach. Undercollateralized lending does not require borrowers to provide collateral of value bigger than the value of a loan, it requires them to put the collateral of value far less or even nothing in the case of uncollateralized lending (Baker, 2022).

The top three lending protocols in the third-party collateralized lending protocols are Maple, TrueFi, and Goldfinch – which currently services around 1,3 billion USD in outstanding loans (Mayr, 2022). These protocols slightly differ in design and functionality, but common points remain which is that creditworthiness is determined off-chain by third-party entities. Borrowers enter the platform and submit a loan request on-chain to initiate the borrowing process. In the case of Maple finance, the loan request is then performed by pool delegates who conduct off-chain due diligence on the borrowers. This consists of an assessment of the borrower's reputation, management background, business strategy, and financial records (Mayr, 2022). Pool delegates are simply institutional investors in the Maple finance ecosystem that create and manage pools of capital used to finance loans. Finally, these pool delegates agree on loan terms directly with the borrowers, who also sign a master loan agreement during onboarding which enables off-chain legal recourse in the event of default. In the case of TrueFi, borrowers also need to sign a master loan agreement on sign-up. After that, they go through an off-chain loan evaluation process which is managed directly by TrueFi underwriters. In this process, they receive an on-chain credit score, which considers both on- and off-chain data. Once this process is finished the borrowers are whitelisted and can apply for loans. However, TrueFi minimizes credit risk so that it allows borrowers with a minimum of 10 million USD in assets (TrueFi, 2022). Similarly in Goldfinch, the borrowers also need to be approved by auditors which conduct off-chain checks like Maple and TrueFi. Only then can the borrower apply for a loan (Goldfinch, 2021). The main drawbacks of this approach are that due diligence and loan underwriting is done off-chain (meaning they are centralized) and that default protection is low. However, these protocols allow only businesses to get a loan and they thus fail to serve retail customers.

Sybil borrowing is prevented through an off-chain legal entity that screens and monitors the borrower just like in TradFi. However, these protocol services only corporate institutions. Since there is an off-chain legal entity present this fails to comply with the permissionlessness aspect of the crypto ethos. At the same time, real information is provided off-chain from the borrowers to the underwriters which means it does not comply with self-sovereignty as the borrower is not in control of their data and credentials.

3.5.3 Prime brokerage

Decentralized prime brokerages are essentially a DeFi implementation of TradFi prime brokerages which banks offer to hedge funds. Prime brokerage in TradFi encompasses a bundle of services that investment banks and other big financial institutions offer to other financial institutions like hedge funds. Some of the services provided are cash management, accessing research, and finding new investors. Banks essentially offer a mechanism to institutions, which allows them to outsource investment activities and focus more on investment goals and strategy. Financial institutions are also bounded by a minimum account size to be able to transact with prime brokerages (Chen, 2022).

Prime brokerage in DeFi is to leverage and rely on the notion of "code is law". Credit risk is mitigated by simulating undercollateralization in a closed system by restricting the use of funds. This is contrary to how it is done in overcollateralized protocols which enforce over-collateralization in an open system. A protocol can provide undercollateralized lending but remains in full control of the loan lent out. This can be thought of as *"borrowing in a bubble"*, where credit risk is prevented algorithmically by the underlying smart contract as the protocol will not let you spend funds in a way that you could default (Baker, 2022). Decentralized prime brokerage is a result of defining boundaries on what the borrower can and cannot do and executing transactions on-chain. This kind of protocol can implement the necessary restrictions through access control. For example, it only allows the funds to be transferred to a restricted wallet, which only allows a well-defined set of commands and smart contract interactions. Restrictions can also be more specific like whitelisting of allowed function calls per smart contract. The key is to ensure that loans can be able to put to good use and that they cannot be transformed into a freely tradable token in an unrestricted, self-custodial wallet (Baker, 2022). Examples of this approach are Oxygen Protocol, DeltaPrime, and Gearbox. For example, loans in Oxygen Protocol can be used for yield generation and margin trading.

Prime brokerage mechanisms prevent Sybil's borrowing programmatically. The underlying smart contracts and ecosystem prevent the borrower to use funds in a way that he could default. However, since this is a closed ecosystem that prevents the funds to be used elsewhere it violates the composability aspect of crypto ethos. Furthermore, with it, decentralization also suffers as the protocol is driven by underlying partnerships which need to be acquired through a centralized entity.

3.5.4 Asset collateralized and tokenization

DeFi lending protocols can also be asset collateralized. Here we differentiate between real-world asset-collateralized loans and digital asset-collateralized loans. Real-world asset collateralized loans are represented on-chain via a process called tokenization. Tokenization is an expansion of blockchain technology that allows real-world assets to be present as tokens on-chain which improves their liquidity – meaning that they can be sold, bought, or traded on blockchains. Blockchain guarantees that once you buy tokens representing an asset, no single authority can erase or change your ownership — your ownership of that asset remains entirely immutable (Cryptopedia Staff, 2021). In asset-collateralized lending protocols, real-world assets are represented on-chain via non-fungible tokens (NFTs). Non-fungibility means that the token is unique and cannot be replaced by any other token. As the name suggests in these lending protocols, credit risk is mitigated with tokenized real-world assets put as collateral. This is similar to mortgages in TradFi where your house is put as collateral and is seized in the case of default. The challenge in this approach lies in the liquidity or even more precisely in the illiquidity of the underlying asset. This is also the case in TradFi, although tokenization makes asset liquid, and thus it enables it to be traded on-chain. Furthermore, NFT tokenization enables fractional ownership of the asset. This means that not only can the underlying collateral be sold on the global open market where there can be many buyers, but its ownership could also be fractionalized (Hedera, 2022). This protocol is promising as it could eliminate a lot of friction that is present when taking a mortgage in the TradFi world (Crypto Chain Capital, 2021).

Digital asset-backed loans are NFT-backed loans. As such, in both asset-collateralized lending protocols, the collateralized asset is a digital asset, but the underlying asset is either a real-world asset or a crypto asset. Since digital assets are crypto-native such as NFTs, they are already expressed on-chain, and using them to settle default is easy. However, here asset illiquidity concern is valid as many NFT artworks are volatile and can likely lose market liquidity. This makes them a poor choice for collateral (Crypto Chain Capital, 2021). There exist mixed approaches which combine asset collateralized and prime brokerage protocols. For example, in the Lendefi protocol, the borrower borrows liquidity to purchase a digital asset. The same digital asset is then used as collateral locked in a smart contract which liquidates the asset if the borrower fails to meet their debt obligations collateral (Crypto Chain Capital, 2021).

This undercollateralized approach tackles Sybil's borrowing by requiring real-world or digital asset collateral. Since both collaterals are represented on-chain the protocol is composable and the effect on the borrower cash flow is positive, even though the underlying collateral can be illiquid (Crypto Chain Capital, 2021).

3.5.5 Identity collateralized

Identity in DeFi is an extremely hard problem to solve. This is because one of the crypto ethos (the driving forces behind DeFi) is self-sovereignty. Self-sovereignty empowers the user to be in control of their data, instead of it being in the hands of a third-party intermediary. Therefore, DeFi borrowers are reluctant to share their data to a protocol for it to assess their creditworthiness. This is exactly what we have seen in previous protocols, especially the over-collateralization mechanism where the loans were even over-collateralized as the participants were anonymous and thus had no reason to trust each other since Sybil's borrowing could not be prevented. However, this can be solved through zero-knowledge proofs (ZKP) which will be discussed in detail. These proofs enable the lender to validate or deny a statement without receiving the actual information. The DeFi world is also challenged by the ability of unlimited virtual identities since the borrower can quickly switch wallets in case of default. There are many proposed solutions for this where wallets are tied to users' real-world identities on-chain in a pseudonymous way through ZKPs. The following chapters will take a look at self-sovereign identity (SSI) and soul-bound tokens (SBT) which tie a user's identity to an on-chain account (Crypto Chain Capital, 2022).

DeFi on-chain identities are likely inevitable, but their implementation is very complex. Some DeFi financial applications offer on-chain identity by leveraging a variety of historical on-chain activities. Such as historical loan repayment, yield farming, trading activity, governance, participation, etc. In TradFi this would represent the credit report and credit score of an individual. This data could compound quickly as all transactions are recorded in DeFi and there are no such things as unrecorded cash transactions like in TradFi. Furthermore, DeFi composability enables this data to be reused across different DeFi financial services. Examples of such protocols are LedgerScore, Credmark, easyfi, link, etc. (Crypto Chain Capital, 2022). Since to my knowledge, there does not yet exist a successful implementation of an identity-based protocol that would leverage DeFi credit scores, this protocol is the focus of this thesis.

4 DESIGNING THE PROTOCOL

This chapter looks into designing the lending protocol with respect to problems in DeFi lending which we identified in the previous chapters. First the problems are discussed individually on a high level and then the mechanism is described at the end of the chapter.

4.1 Solving the economic problem

We have identified that a lending protocol with the biggest total value locked in DeFi is the overcollateralized approach. However, this approach does not serve as an engine of economic growth as is the case with lending in TradFi. This is because community behind the development and use of DeFi greatly values crypto ethos – which is decentralization, composability, permissionless, and self-sovereignty. However, since self-sovereignty is important, it constrains the use of data about an individual, and therefore all accounts in DeFi are pseudo-anonymous. This lack of trust yields over-collateralization approaches, which do not fuel the economy as the borrower cannot enter the position of net debt. This means that the value of the collateral is higher than the value of the loan. This economic problem is solved by developing an undercollateralized approach in which the value of the collateral is lower than the value of the loan. However, this means that in the undercollateralized approach the credit risk is higher and the Sybil borrowing is possible. In this thesis, we will offset the credit risk difference by mapping to TradFi by securely acquiring information about the borrower through on-chain identity. Doing this will minimize credit risk and enable better loan terms for the borrower.

4.2 Solving the Sybil (trust) problem

Since all actors on public blockchains are pseudo anonymous by default there is a big problem of trusting the borrower to repay and not run off with the lender's money (Sybil borrowing). This chapter outlines different approaches to prevent Sybil borrowing and still preserve the driving forces behind DeFi ecosystem – crypto ethos.

4.2.1 Zero-knowledge proofs

Zero-knowledge proof (ZKP) was proposed in 1989 by Goldwasser, Micali, and Rackoff (1989). In the context of cryptography, a ZKP is a technique by which one party (prover) can through cryptographic commitment prove to another party (verifier) that they know some data or a secret without conveying any information apart from the fact that they know the secret. This is useful in terms of blockchain as we do not want to reveal information about a person as we would like to maintain his anonymity (Li & Nejad, 2020). Furthermore, through ZKP we can prove that a given statement is true, without conveying any additional information apart from the fact that the statement is true (Xie, Holmes & Dagher, 2020). There are two kinds of ZKP depending on if there is challenge-response interaction: interactive and non-interactive. In an interactive ZKP, the prover and verifier engage in at minimum three rounds of communication exchange. In this kind of protocol, the verifier can submit challenges to the prover. The prover then replies with responses that reinforce the validity of the prover's original statement. In non-interactive ZKPs there is no challenge-response interaction, although there is sometimes a common reference string shared in advance by both parties (Lesavre, Varin, Mell, Davidson, & Shook, 2019). A ZKP produces proof that is sent to the verifier. For a specific statement the resulting proof must satisfy the three properties to be considered secure:

- *Completeness*: If the statement is true, then the proof will convince the verifier that the statement is true with overwhelming probability.
- *Soundness*: If the statement is false, then the probability that P can convince the verifier that the statement is true is negligible.
- *Zero*-knowledge: If the statement is true, then the verifier learns nothing about the proof besides the fact that the statement is true.

The prover cannot convince the verifier of a false assertion because of the soundness property. For example, if the prover cheats with a probability of 1 / 3, then the ZKP may need to be repeated n times so the soundness error is reduced from 1 / 3 to (1 / 3)^n. The zero-knowledge property can be either statistical or computational. When the verifier is assumed to have unlimited computational resources but learns no additional information from the protocol, then the protocol is assumed to achieve statistical zero knowledge. When the zero-knowledge property holds some assumption about the verifier's computational power, then the protocol achieves computational zero knowledge (Lesavre et al., 2019). ZKPs scalability and cost rely on the succinctness of the proof, which measures the required storage size of the proof, proving time, and verification time. When talking about blockchain, the verification time is typically the most important and proving time the least important consideration. When implementing a trusted setup phase, a significant initial cost is required but it then enables verification of the proof to require fewer resources as it allows the statement to be proven again by verifying with limited time and resources (Lesavre et al., 2019).

4.2.2 Self-sovereign identity

Self-sovereign identity (SSI) concept has originally been proposed by Christoper Allen. The concept stands on the notion that an identity subject has control over their digital identity and their related credentials hence it is called self-sovereignty. By leveraging SSI credit risk can be assessed, Sybil borrowing can be prevented, and the self-sovereignty aspect of crypto ethos can be maintained. SSI allows an identity holder to transact with another without allowing them to observe content. This means that SSI removes the need for a central trusted authority (van Bokkem, 2019). Alongside message encryption, data can be shared in a minimalist way through zero-knowledge proofs (ZKP). ZKPs are widely used in SSI solutions and are being applied to DeFI in the form of cryptocurrencies (one example is Zcash which keeps all your transactions and financial information private and in your control). Another use of ZKPs is to solve Ethereum scalability issues where transactions are validated based on the underlying math of ZKPs and not by validators (one approach to this is zkSync) (Kroon, 2021). Each SSI solution can be perceived by analyzing the principles or properties that were described by Allen and Cameron van Bokkem (2022). The principles and their interpretations are gathered in Table 6 below.

Table 6: Principles of SSI

Principle	Interpretation
Existence	*Users must have an independent existence*
Control	*Users must control their identities.*
Access	*Users must have access to their own data.*
Transparency	*Systems and algorithms must be transparent.*
Persistence	*Identities must be long-lived*
Portability	*Information and services about identity must be transportable.*
Interoperability	*Identities should be as widely usable as possible.*
Consent	*Users must agree to the use of their identity.*
Minimalization	*Disclosure of claims must be minimized.*
Protection	*The rights of users must be protected.*
Provable	*Claims must be shown to hold true.*

Adapted from van Bokkem (2022); Shuaib (2020).

4.2.3 Decentralized society and soul-bound tokens

Another way to solve the Sybil problem and to achieve lending as an economic engine in DeFi (undercollateralized lending) through identity is through the use of so-called soulbound tokens (SBTs) represented by Vitalik Buterin the founder of Ethereum and other authors in the white paper by the title of *Decentralized Society: Finding Web3's Soul* (Weyl, Ohlhaver, & Buterin, 2022). In essence, SBTs represent publicly visible, non-transferable (but possible revocable-by-the-issuer) tokens that represent non-transferable identity and reputation tokens. Web3 social identity with rich social composability through SBTs could tackle problems in web3 such as wealth concentration and financial attacks on governance. This kind of use case and the concept of a derived richer pluralistic ecosystem is denoted as a Decentralized Society (DeSoc). In DeSoc SBTs represent commitments, credentials, and affiliations which would be issued by other wallets that attest to these social relations (Weyl, Ohlhaver, & Buterin, 2022).

The use of SBTs is not entirely limited to lending but is in the context of this master's thesis particularly useful as SBTs can encapsulate an individual's or entity's credit score on-chain. Since credit and undercollateralized lending are built directly on top of reputation. An ecosystem of SBTs could enable censorship-resistant, bottom-up alternatives to top-down commercial and social credit systems. SBTs could represent education credentials, work history, and rental contracts that would serve as a persistent record of credit-relevant history. Loans and credit lines would be represented as non-transferable but revocable SBTs among other SBTs in a user's wallet until the loan would be repaid. SBT's non-transferability prevents transferring outstanding loans while the ecosystem of SBTs prevents Sybil borrowing as the borrower would lack SBTs to acquire a meaningful loan the next time. SBTs would birth the open-source lending markets and thus the correlation between SBTs and repayment risk would emerge, yielding better lending algorithms. These algorithms would better predict creditworthiness and thus reduce the role of centralized credit-scoring infrastructure as the algorithm would be improved based on all the default risk data in the system. Since SBTs represent membership across social groups, community lending may partake in a "lend-it-and-help-it" approach – which would combine working capital with human capital for greater return and lower credit risk (Weyl, Ohlhaver, & Buterin, 2022).

4.2.4 Adverse selection problem and screening

Since the records of transactions are immutable and stored on a ledger, we can acquire all information about the transactions of the borrower. This means that we are not constrained by the requirement that the borrower needs to be our client before asking for a loan as it is done now in TradFi. Banks get information about a person by looking at their past transactions at this specific bank. This means that other banks do not have this data and because of that they cannot assess the creditworthiness of the borrower. This concept is often referred to as know your customer (KYC). In terms of our solution, this means that anybody anywhere would be able to obtain a loan if it would be assumed that they are creditworthy. This goes exactly with the decentralization aspect of the blockchain as the central entity would be cut out and the banking would be provided for the unbanked (Sánchez, 2020). However, just information about past transactions is not enough to issue credit. That is why this service needs to determine creditworthiness through identity. That means that we require a blockchain identity provider which would give us information about the person's credit score and/or monthly income. In this process, no data exchanges hand as it would be done through ZKPs which just checks that certain thresholds are met.

4.2.5 Moral hazard problem and monitoring

The moral hazard problem is a hard problem to solve in DeFi as the person can quickly take the loan out of their wallet and transfer it to their bank account (so-called Sybil borrowing). By doing this we cannot monitor them and see what the loan was used for. One solution for real-world loans is tokenization. Real-world assets are tokenized and then used as collateral when getting a loan. When a borrower defaults on a loan, the platform then takes ownership of the collateral. There are many benefits to tokenization. The underlying real-world assets represented by tokens gain liquidity as the assets are available to a much larger audience, which yields increased market liquidity and removal of liquidity premium. Tokenized assets can be freely exchangeable online, and they allow investors to acquire fractional ownership of a token's underlying asset. As such crypto tokens can contribute to the liquidity of existing markets and provide a broader investment opportunity to investors. Tokenization also offers faster and cheaper transactions as it allows investors to bypass market intermediaries and other middlemen which are involved in the TradFi asset management process. This means that it reduces the transaction costs and processing times of each transaction. Furthermore, crypto tokens can be traded 24/7 around the globe. DeFi also enables transparency and provability of the asset. Users can easily trace tokens' provenance and transaction history in a cryptographically verifiable way. Transactions are automatically recorded on the blockchain, whose immutability and transparency guarantee the authenticity of each token's state history (Cryptopedia Staff, 2021). Another solution is that we monitor the transactions of our borrowers. However, this is only possible when the loan is used on-chain.

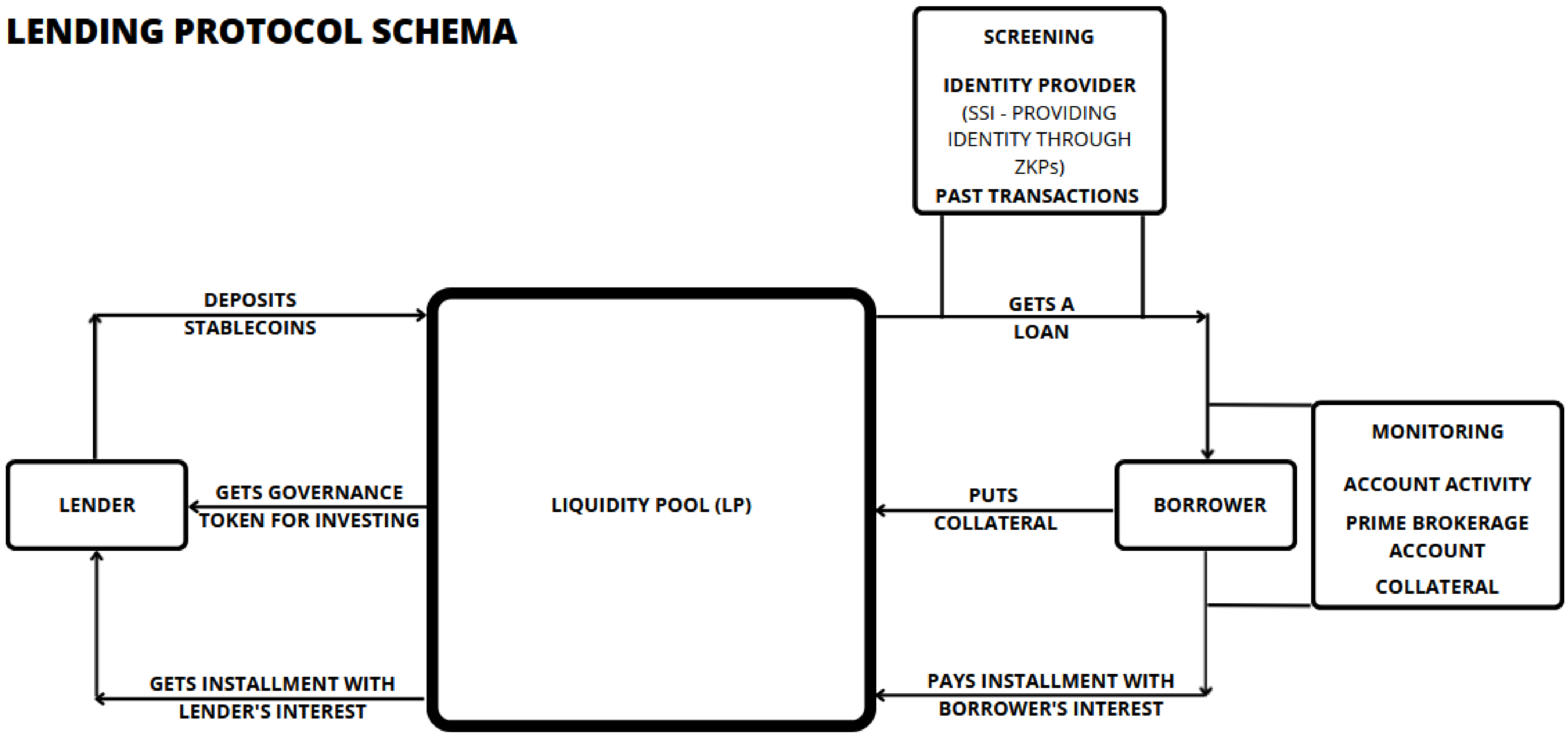
4.3 Centralization problem – governance system

Blockchain's inherent pseudonymous and permissionless structure has implications for the governance of DeFi applications. DeFi applications avoid placing trust in any centralized actor or institutions, instead, they experiment with new organizational forms. These forms are called decentralized autonomous organizations (DAO), which spread control over decisions among stakeholders by issuing special governance tokens. These tokens give holders the power to propose changes to the protocol and vote on them. This is because the system cannot function without human intervention and the rules governing the blockchain and any upgrades to the system must be agreed upon. These rules form the governance of the system and represent the interest of its different stakeholders (Makarov, 2022).

All stakeholders want the protocol to grow, but there are different incentives between them. For example, token holders and validators want high fees for transactions while users and developers want them to be low. To achieve a compromise, the control over decisions is spread among stakeholders through governance tokens. On the blockchain, all activity is governed by smart contracts and noted on the blockchain. Normally, one governance token equals one vote. New proposals to the protocol are decided on by a predefined majority rule. Holders of governance tokens have an interest in the success of the platform as the protocols give them a share of the transaction fees because they hold governance tokens. Governance in DeFi is transparent and verifiable as it is backed by a public smart contract code that is trusted by anyone. However, because this kind of decision-making is dispersed, and the stakes are small it can be inefficient. Therefore, stakeholders might not be incentivized to learn about how it works as there is a little trade-off for them. This would lead to stakeholders refraining to vote. There is also an issue of stakeholders with large stakes gaining control and imposing their preferences on the system (Makarov, 2022). However, the history of corporate governance shows that economic invectives for managers or investors are not sufficient to deter bad actors if the financial gains are high. Fiduciary duties holding corporate agents accountable play a critical role in the enforcement of governance rules. The threat of punishment creates disincentives for fraudulent behavior, whereas just losing money from fraud does not have the same effect. Therefore, the pseudonymous nature of blockchain systems makes it difficult to hold bad actors accountable for their actions in the way that corporate governance does (Makarov, 2022).

4.4 Lending protocol schema

Figure 4: Lending protocol schema



Source: own work.

4.4.1 Lending mechanism and liquidity pool

The lending mechanism of a lending protocol in DeFi is similar to one in TradFi and is portrayed in Figure 4. Actors with excess liquidity called lenders deposit stablecoins in a liquidity pool (LP) which holds money from all other lenders. Lenders get in exchange a governance token, which gives them the ability to vote on future proposed changes to the protocol. They also get a protocol native interest-bearing token on which they get interested at specified lenders' interest rates for providing liquidity. The LP holds all the liquidity from the lenders and its underlying smart contracts determine who gets a loan. This decision is done through screening instruments like identity screening of the borrower and based on past transactions of the account. The identity provider provides a self-sovereign identity of the borrower through zero-knowledge proofs. On the other side, the borrower applies for a loan through a platform application where he chooses the loan terms. Loan terms can be a principal amount, interest rate, payment regime, etc. Once screening is done, the borrower's loan request is fulfilled, and he gets issued a loan at the borrower's interest rate in stablecoins. The borrower pays instalments with a predetermined borrower's interest rate, whereas the lender gets paid instalments at the lender's interest rate which is lower than the borrower's one. The interest rate premium is collected to maintain the reserve ratio and for fuelling the future growth of the protocol.

4.4.2 Interest rate model

The interest rate of the protocol is a linear interest rate model. This means that the interest rate is set as a linear function of the utilization of our liquidity pool. This means that the more funds that are lent out, the higher the utilization and the higher the corresponding interest rate. This is so it becomes more attractive (a lower borrowing rate) to get a loan in times of excess liquidity. In this model interest rates are determined algorithmically depending on the utilization of the pool. The borrowing interest rate is denoted by the below equation (3).

$$Borrowing\ Interest\ Rate = \alpha + \beta U \tag{3}$$

Where α is some specified constant and β is a slope coefficient of the responsiveness of the borrowing interest rate to the utilization rate. Utilization rate of our liquidity pool (assets lent versus total assets) is denoted as U. The saving interest rate is denoted by the following equation (4).

$$Saving\ Interest\ Rate = (\alpha + \beta U)U \tag{4}$$

Here we can see that the borrowing interest rate is multiplied by the utilization, which in turn ensures that the interest rate spread is positive. This spread can be then used for reserves.

5 IMPLEMENTING THE PROTOCOL

The protocol implemented in this master's thesis serves as a proof of concept (POC). Meaning, that the protocol is only implemented to an extent so that we can in later chapters analyze and discuss its feasibility and viability. Furthermore, POC as such is not a production-ready application meant to handle many users. Having said that the application and its implementation is publicly available at Hribar (2022). As this is a POC and because of resource constraints this protocol was developed with some compromises. For the purposes of showing the protocol feasibility there is no need to implement governance of the protocol as governance handles which future features will be implemented in the protocol and thus falls outside of the scope of this application. At the same time some other compromises needed to be made. On-chain credit rating providers are still under development and thus cannot be leveraged for monitoring. Similarly, identity providers are far too complex to implement with Solana technology with the limited resources at hand.

5.1 Architecture of the application

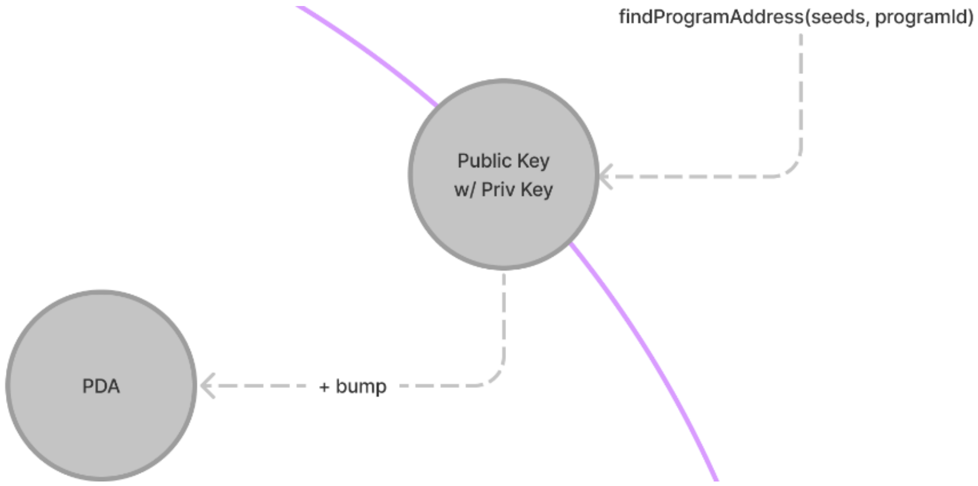
A type of application that will be developed in this master thesis is denoted as a web application, more precisely a web3 application. Web3 (also known as web 3.0) encompasses a new idea of the World Wide Web which incorporates blockchain technologies, token-based economics, and crypto ethos such as decentralization and self-sovereignty (Worldcoin, 2022). Because these applications are decentralized, they are many times referred to as decentralized applications (dApps). In simple terms dApp's architecture consists of frontend and blockchain backend. Additionally, we require a wallet to interact with the dApp. In our case our blockchain is the Solana blockchain and the corresponding wallet is the Phantom wallet. The Solana blockchain holds the smart contracts that perform some operation when called (like borrowing funds in our example) and then write the transaction to the blockchain. In our case we will use the Rust programming language coupled with the Anchor Framework to write the smart contracts. The wallet in DeFi stores private keys which represent the sequences that give you access to the cryptocurrencies that you hold (Coinbase, 2022). Apart from providing safety and accessibility of your cryptocurrencies it also lets users digitally sign the transaction with their own private key. This makes it an integral part of a DeFi application as it provides an ability to sign transactions. However, usually one wallet connects to only one blockchain (either Solana or Ethereum). Finally, the frontend of our dApp is written in JavaScript, CSS, and HTML. We will leverage the React Framework which lets us write all three in a more structured way and we will also use TypeScript to enable types to our JavaScript programming language to prevent bugs.

5.2 Implementing lending

When implementing lending we first need to create a unique liquidity pool in which all the liquidity will be stored. In Solana the liquidity pool is represented by an "account". However, since our liquidity pool needs to be controlled by a specific program, we need to create

Program Derived Addresses (PDAs). By doing this the programs can then programmatically sign for certain addresses without the need of a private key (Solana Cookbook, 2022). PDAs are essential for developing programs on Solana and serve as the foundation for Cross-Program Invocation (CPI). CPIs allow for the programs to call each other and are enabled by Solana runtime. Calling between programs is achieved by one program invoking an instruction of the other. An example of this would be a client creating a transaction that modifies two accounts (Solana Team, 2022b). PDAs are technically not created, but rather found. On Figure 5 we can see that by invoking a function *findProgramAddress* with seeds and *programId* we are trying to see if the generated public key lies on the ed25519 elliptic curve which is a part of elliptic-curve cryptography (ECC). By running our *programId* and seeds through a sha256 hash function, the hash function would sometimes generate a public key which is already in use. In those cases, we also provide a *bump* which enables us to alter our input by a little. This process gives us a deterministic way of deriving the same PDA over and over again (Solana Cookbook, 2022).

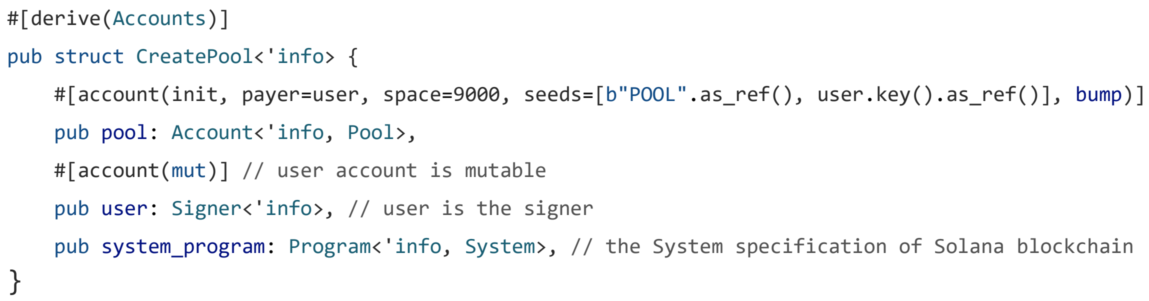
Figure 5: ed2559 Elliptic Curve



Source: Solana Cookbook (2022).

In code defining a PDA would look similarly to *Figure 6* where we initialized the pool with the seed *POOL* and a default *bump* which maps to 255.

Figure 6: Defining the account structure for the CreatePool smart contract



```
#[derive(Accounts)]
pub struct CreatePool<'info> {
    #[account(init, payer=user, space=9000, seeds=[b"POOL".as_ref(), user.key().as_ref()], bump)]
    pub pool: Account<'info, Pool>,
    #[account(mut)] // user account is mutable
    pub user: Signer<'info>, // user is the signer
    pub system_program: Program<'info, System>, // the System specification of Solana blockchain
}
```

Source: Own work.

Now that the pool has been initialized the lender can fund the pool, providing liquidity and thus get interest on the money lend out. In below Figure 7 we have created a *fund_pool* smart contract which takes *ctx (context)* and *amount* as input parameters. We have then transferred the *amount* defined from the users account to the pools account.

Figure 7: Fund pool smart contract

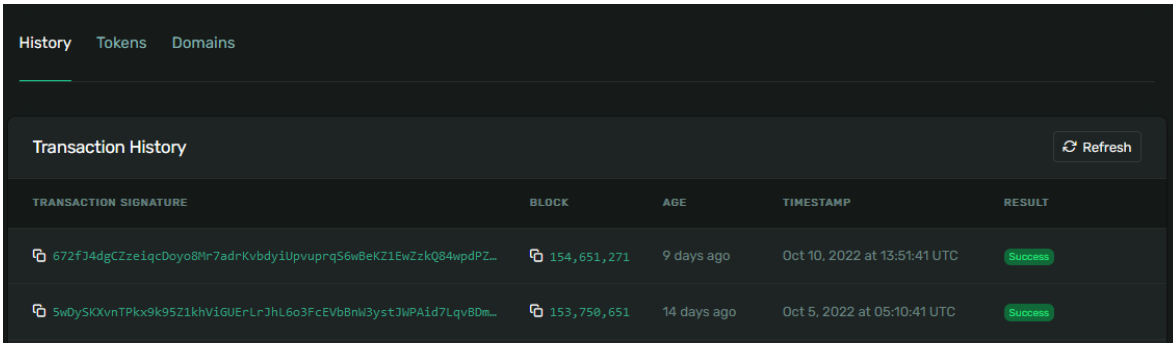
```
pub fn fund_pool(ctx: Context<FundPool>, amount: u64) -> ProgramResult {
    let ix = anchor_lang::solana_program::system_instruction::transfer(
        &ctx.accounts.user.key(),
        &ctx.accounts.pool.key(),
        amount
    );
    msg!("funded liqudity pool on the chain");
    msg!("{}", ctx.accounts.pool.amount_hold);

    anchor_lang::solana_program::program::invoke(
        &ix,
        &[
            ctx.accounts.user.to_account_info(),
            ctx.accounts.pool.to_account_info()
        ]
    );
    (&mut ctx.accounts.pool).amount_hold += amount;
    Ok(())
}
```

Source: Own work.

5.3 Implementing screening and monitoring

Since Solana is a public blockchain this means that everyone has access about the wallet's transactions history. Figure 8 represents a way of how we can monitor what the funds of the loan are being used for through Solana Explorer.

Figure 8: Account details retrieved from Solana Explorer



Transaction History

TRANSACTION SIGNATURE	BLOCK	AGE	TIMESTAMP	RESULT
672fJ4dgCZzeiqcDoyo8Mr7adrKvbdyiUpvuprqS6wBeKZ1EwZzkQ84wpdPZ…	154,651,271	9 days ago	Oct 10, 2022 at 13:51:41 UTC	Success
5wDySKXvnTPkx9k95Z1khViGUErLrJhL6o3FcEVbBnW3ystJWPAid7LqvBDm…	153,750,651	14 days ago	Oct 5, 2022 at 05:10:41 UTC	Success

Source: Solana Explorer (2022).

6 ANALYZING AND DISCUSSING THE PROTOCOL

The following subchapters seek to analyze whether our implementation of the undercollateralized lending protocol makes sense in the real world. We will discuss its feasibility, viability, and scalability. Furthermore, we are going to look at these aspects with respect to two of the most important problems that banks face when issuing loans – the moral hazard and the adverse selection problem.

6.1 Feasibility

Solana blockchain enables us to build DeFi applications atop of it without worrying about fraud or liquidity issues. Those issues are handled directly with the Solana network or any other suitable blockchain. Many financial service applications can be built that offer more features than traditional banking apps. In our case, we managed to build a lending protocol to lend funds. Furthermore, it is easier to get started building DeFi applications as you can use existing open-source libraries and frameworks and launch a minimum viable product without spending much on development costs. In essence, you can create a smart contract that implements the business logic, deploy it, and then test the market with less effort (Procoders, 2022). We have implemented the loan issuing platform with a frontend and a decentralized blockchain backend. This is not how it is done now with banks that have a centralized server backend. However, solving the adverse selection and moral hazard problem is a big feat in the blockchain implementation of the lending protocol. Since decentralized finance strives to provide financial services for anyone anywhere without third party intermediation, it is hard to acquire information about the user. However, a compromise will need to be reached and a third party or in-house implementation of identity provider will need to be implemented. This is so we can assess the creditworthiness of a borrower. Another problem is the monitoring part, as of right now a user can transfer all the funds from his wallet to his bank account. This poses a huge moral hazard problem as we do not know what the loan is used for.

6.2 Viability

DeFi environment offers viable opportunities for development of DeFi services and products. It is an open technology that can be great assistance in the development of a new era of financial solutions. Its significance grows as more and more decentralized applications are developed each day. However, DeFi is still in its early stages of development. Meaning that it is unregulated and riddled with mishaps, hacks, and scams. Current legislation is based on the concept of distinct financial jurisdictions – each of them having their own set of laws and rules. But DeFi offers an ability to conduct border-less transactions which raises problems on how to regulate it (Diwan, 2022). In our case we have delved into online lending which is already offered with some restrictions by other banks. Therefore, I see no reasons why this solution would not be viable from consumer standpoint.

6.3 Scalability

Lending protocol has been built with the blockchain technology Solana which does not come without its faults. Solana blockchain is still in beta and has suffered a handful of major network outages since its launch in 2020 (Seeking Alpha, 2022). In fact, three of the major outages occurred only this year. There are different reasons for outages such as misconfigured nodes, bugs in Solana's code, and network getting overwhelmed by artificial traffic from bots. At each of these outages the network goes offline for a couple of hours and normally the validators are the ones that restore the network by participating in finding consensus. However, these kind of network outages have not gone unnoticed, and it is a major cause of concern to its founder, developers, and users. Solana's own founder admitted that network outages are Solana's biggest challenge and finding a solution for it has been made a number one priority of the Solana team. Having said that these kinds of hacks are not new to DeFi world. Solana based DeFi protocol Mango Markets lost over 100 million US dollars in the attack, which has led to a drop of TVL on Solana by 24 %. In raw numbers, twenty-four hours following the attack the TVL on Solana dropped from 1,32 billion US dollars to 985 million US dollars. However, these kinds of attacks are not limited to only Solana, they are also present on Ethereum, which also suffered an outage in November 2021. Solana is known for growing very fast, and it is often said that it has sacrificed efficiency and security in favor of doing so. In others L1 protocols like Cardano, such hacks are less common as everything is peer-reviewed. However, Solana blockchain technology enables us to offer financial services twenty-four hours a day, seven days a week if we do not account for occasional downtime. This is contrary to TradFi financial services which are offered only in working hours (that includes digital services). This means that blockchains take out the time and resource constrain of TradFi. In conclusion, Solana blockchain is new with its shortcoming, but it is being actively worked on and improved to provide a stable network that will be able to offer financial services at all times. With Solana blockchain being improved I firmly believe that it is a scalable solution for DeFi application as it is able to handle volatility of use by itself.

CONCLUSION

In this master's thesis I have first looked into lending in the traditional finance and then at the lending ecosystem of the decentralized finance. I have identified and discussed the driving forces behind the development of the decentralized finance and denoted them as crypto ethos which consist of decentralization, self-sovereignty, permissionless, and composability. Furthermore, I have assessed the impact of crypto ethos on lending with which we are familiar in traditional finance. Moreover, I have designed, implemented, and analyzed a proof of concept of an undercollateralized lending protocol developed with Solana blockchain technology.

First, let's answer the research questions which we have set in the introduction of the master's thesis. The first research question states if the undercollateralized identity-based lending protocol can be successfully implemented with blockchain technology. We were able to implement a proof of concept of a lending protocol with the use of the Solana blockchain technology. However, in the Solana ecosystem, we were unable to identify an identity provider which we can use to perform thorough screening and due diligence of the borrower. This indicates that the Solana ecosystem might be too young to support an on-chain identity solution, but developed enough that it makes it possible to implement a lending protocol without screening.

The first research question is strongly intertwined with the second as it questions if the adverse selection and the moral hazard problem can be solved in the undercollateralized lending protocol. Since DeFi is entirely held online and because of crypto ethos such as decentralization and self-sovereignty this is a far more complex issue. Decentralization aspect strives to achieve a financial system without a central intermediary and authority like a central bank whereas self-sovereignty strives for the user to be in control of their data. Self-sovereignty aspect makes all the actors (such as the lenders and the borrowers) who are represented online on a public DeFi blockchain as pseudo-anonymous. This means that it is hard to solve the adverse selection problem as the self-sovereignty aspect restricts us to gather the data of the customer and perform screening effectively. Fortunately, in theory, we have identified a compromise between self-sovereignty and the need to perform screening of the borrowers to offer them the best possible interest rate. We have identified that we can use a self-sovereign identity on-chain which allows us to verify and screen if the user meets certain requirements through the use of zero-knowledge proofs. Zero-knowledge proofs allow us to prove the truth of the statement based on mathematical algorithms without observing the contents of the statement. With this solution we can properly screen the borrower while preserving the self-sovereignty aspect. In my opinion, screening without observing the contents should be adequate to solve the adverse selection problem. On the other hand, solving the moral hazard problem is more complex, but one way to do it is to monitor the transaction history of the borrower, however this brings us to a new problem. Because all the actors are represented online as pseudo-anonymous, they could just transfer the money to their bank account and run without repercussions – this represents Sybil borrowing. To solve this problem, we need to go back to on-chain identity which would prevent Sybil borrowing as we would be able to acquire the information required to track down the borrower and enforce repercussions. Another solution to the Sybil borrowing could be a closed wallet allowing for only verifiable payments, so the user could not transfer the money to their bank account.

We have identified that there is a big issue of trust between the participants when it comes to undercollateralized lending in DeFi. However, I believe that on-chain identity, on-chain credit score rating and enforceable legal framework would enable undercollateralized lending in DeFi and prevent Sybil borrowing. Furthermore, I believe that through the process of real-asset tokenization and underlying regulatory framework supporting and enforcing it, such lending can already be achieved now on the Ethereum blockchain. Real-asset tokenization allows for the assets and its ownership to be represented on-chain. Furthermore, a regulatory framework that would help the transfer of ownership of the asset in the case of default would portray an economic disincentive for Sybil borrowing.

To conclude, DeFi and its underlying technology does not come without its shortcomings. But since it is being rapidly worked on and invested in, it looks like that its faults could be addressed, and compromises achieved. Even more so as it is in very early stages of development compared to the traditional financial system. Having said that, this thesis to my knowledge represents one of the first academic work that outlines and discusses different lending protocols in the DeFi lending ecosystem. My master's thesis contributes to the understanding of lending in the DeFi system and the principles of the developer community behind it. Furthermore, it outlines and presents a handful of solutions on how to implement undercollateralized lending in DeFi so that it can fuel economic growth and thus enable widespread adoption. We have concluded that rightly implemented identity with the regulatory framework supporting and enforcing it is crucial for the implementation of lending as economic engine and thus to DeFi as a whole. However, this approach is very complex. Finally, the purpose of this master’s thesis research is to research lending in DeFi like it is now and propose solutions so that production-ready undercollateralized lending can be developed and leveraged in the real economy. I believe that once undercollateralized protocol is implemented and economy of scale is achieved the interest rate on loans in such a protocol would be lower compared to interest rates on loans in the traditional finance. Moreover, it would be accompanied with greater accessibility of the financial services on the retail as well as on the corporate level. Furthermore, cheap debt would pose economic incentives to corporations as their cost of funds would decrease and consequently profit margin would increase.

REFERENCES

1. Aramonte, S., Doerr, S., Huang, W., & Schrimpf, A. (2022). *DeFi lending: intermediation without information?* (No. 57). Bank for International Settlements. https://www.bis.org/publ/bisbull57.pdf
2. AWS. (2022). Decentralization in blockchain. Retrieved September 7, 2022 from https://aws.amazon.com/blockchain/decentralization-in-blockchain/
3. Bach, L. M., Mihaljević , B. & Žagar, M. (2018). Comparative Analysis of Blockchain Consensus Algorithms. International Convention on Information and Communication Technology, Electronics and Microelectronics, 41, 1545–1550
4. Baker, L. (2022). *Paradigms for On-Chain Credit.* Retrieved September 7, 2022 from https://jumpcrypto.com/paradigms-for-on-chain-credit/

5. Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, *4*(1), 14. https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf
6. Banka Slovenije (2022). *Sisbon.* Retrieved September 7, 2022 from https://sisbon.si/
7. Bodziony, N., Jemioło, P., Kluza, K., & Ogiela, M. R. (2021). Blockchain-based address alias system. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1280-1296. https://www.mdpi.com/0718-1876/16/5/72
8. Buterin, V. (2017). *The Meaning of Decentralization*. Retrieved September 7, 2022 from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
9. Campos, R. (2022). *China, U.S. lead rise in global debt to record high $305 trillion - IIF*. Retrieved September 7, 2022 from https://www.reuters.com/markets/europe/china-us-lead-rise-global-debt-record-high-305-trillion-iif-2022-05-18/
10. Caplinska, A., & Tvaronavičienė, M. (2020). Creditworthiness place in credit theory and methods of its evaluation. *Entrepreneurship and sustainability issues*, *7*(3), 2542. https://jssidoi.org/jesi/uploads/articles/27/Caplinska_Creditworthiness_place_in_Credit_Theory_and_methods_of_its_evaluation.pdf
11. CFI Team. (2020a). *Prime Rate*. Retrieved September 7, 2022 from https://corporatefinanceinstitute.com/resources/knowledge/finance/prime-rate/
12. CFI Team. (2020b). *Floating Interest Rate*. Retrieved September 7, 2022 from https://corporatefinanceinstitute.com/resources/knowledge/finance/floating-interest-rate-variable/
13. CFI Team (2022). *Rating agency.* Retrieved September 7, 2022 from https://corporatefinanceinstitute.com/resources/knowledge/finance/rating-agency/
14. Chen, J. (2021). *Interest Rate Risk Definition and Impact on Bond Prices.* Retrieved September 7, 2022 from https://www.investopedia.com/terms/i/interestraterisk.asp
15. Chen, J. (2022). *Prime Brokerage*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/p/primebrokerage.asp
16. Chiu, J., Ozdenoren, E., Yuan, K., & Zhang, S. (2022). *On the Inherent Fragility of DeFi Lending*. Retrieved September 7, 2022 from https://www.snb.ch/n/mmr/reference/sem_2022_06_03_chiu/source/sem_2022_06_03_chiu.n.pdf
17. Civiero, M. (2020). *Crypto-assets and decentralized finance.* Retrieved September 7, 2022 from https://thesis.unipd.it/handle/20.500.12608/23293Coinbase (2022). *What is a crypto wallet?* Retrieved September 7, 2022 from https://www.coinbase.com/learn/crypto-basics/what-is-a-crypto-wallet
18. Crypto Chain Capital. (2021). The Current State of Undercollateralized DeFi Lending — 2021. Retrieved September 7, 2022 from https://medium.com/coinmonks/the-current-state-of-undercollateralized-defi-lending-2021-1f84e14527b5
19. Cryptopedia Staff. (2022). *What Is Tokenization in Blockchain?* Retrieved September 7, 2022 from https://www.gemini.com/cryptopedia/what-is-tokenization-definition-crypto-token#section-the-benefits-of-tokenization

20. Defi Pulse. (2022). *The Decentralized Finance Leaderboard*. Retrieved September 7, 2022 from https://www.defipulse.com/
21. Dhir, R. (2021). *Creditworthiness.* Retrieved September 7, 2022 from https://www.investopedia.com/terms/c/credit-worthiness.asp
22. Dionysopoulos, L., Giaglis, G., Kostopoulos, N., Damvakeraki, T., Anania, A., Moré, Í., Pawłowski, M., Niemerg, M., Joshi, A., Baró, M., Karasek-Wojciechowicz, I., Loesch, S., Szegö, D., Charalambous, M. & Ntouzgou, A. (2022). Decentralised Finance (DeFi). Retrieved September 7, 2022 from https://www.researchgate.net/publication/362860081_Decentralised_Finance_DeFi
23. Diwan, P. (2022). *DeFi: Defying the Normal.* Retrieved September 7, 2022 from https://pdiwan.medium.com/defi-defying-the-normal-249fc4e6afbf
24. Duffy, F., Bendechache, M., & Tal, I. (2021). Can Solana's high throughput be an enabler for IoT?. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 615-621). IEEE.
25. Ethereum. (2022). *The Merge.* Retrieved September 7, 2022 from https://ethereum.org/en/upgrades/merge/
26. FED. (2021). *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps* Retrieved September 7, 2022 from https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211123a1.pdf
27. Fernando, J. (2022). *Margin and Margin Trading Explained Plus Advantages and Disadvantages*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/m/margin.asp
28. Future Learn. (2021). *Why borrow and lend in DeFi?* Retrieved September 7, 2022 from https://www.futurelearn.com/info/courses/defi-exploring-decentralised-finance-with-blockchain-technologies/0/steps/256206
29. Frankenfield, J. (2022). *Smart Contracts*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/s/smart-contracts.asp
30. Goldfinch Team. (2021). *Goldfinch whitepaper.* Retrieved September 7, 2022 from https://uploads-ssl.webflow.com/62d551692d521b4de38892f5/631146fe9e4d2b0ecc6a3b97_goldfinch_whitepaper.pdf
31. Goldwasser, S., Micali, S., & Rackoff, C. (2019). The knowledge complexity of interactive proof-systems. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali* (pp. 203-225). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.8132&rep=rep1&type=pdf
32. Greenbaum, S. I., Thakor, A. V., & Boot, A. (2019). *Contemporary financial intermediation*. Academic Press. https://www.arnoudboot.nl/publication/595/contemporary_financial_intermediation_with_s.i._greenbaum_and_a.v._thakor_elsevier_4th_edition_2019./download
33. Gudgeon, L., Werner, S., Perez, D., & Knottenbelt, W. J. (2020, October). Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. In *Proceedings of the*

2nd ACM Conference on Advances in Financial Technologies (pp. 92-112) https://arxiv.org/pdf/2006.13922.pdf

34. Gupta, S., Sinha, S., & Bhushan, B. (2020, April). Emergence of blockchain technology: Fundamentals, working and its various implementations. In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3569577
35. Harvard Law. (2022). *Blockchain in the Banking Sector: A Review of the Landscape and Opportunities,* Retrieved September 7, 2022 from https://corpgov.law.harvard.edu/2022/01/28/blockchain-in-the-banking-sector-a-review-of-the-landscape-and-opportunities/
36. Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the Future of Finance*. John Wiley & Sons. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711777
37. Hayes, A. (2022a). *What is Blockchain?* Retrieved September 7, 2022 from https://www.investopedia.com/terms/b/blockchain.asp
38. Hayes, A. (2022b). *Covenant*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/c/covenant.asp
39. Hayes, A. (2022c). *Stablecoin*, Retrieved September 7, 2022 from https://www.investopedia.com/terms/s/stablecoin.asp
40. Hayes, A. (2022d). *Lender of Last Resort*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/l/lenderoflastresort.asp
41. Hedera. (2022). *What is asset tokenization?* Retrieved September 7, 2022 from https://hedera.com/learning/tokens/what-is-asset-tokenization
42. Hribar, R. (2022). *Lending protocol implementation.* Retrieved September 7, 2022 from https://github.com/rhribar/lending-protocol
43. IBM. (2022). *Benefits of blockchain*. Retrieved September 7, 2022 from https://www.ibm.com/topics/benefits-of-blockchain
44. IOSCO (2022). *IOSCO DECENTRALIZED FINANCE REPORT*. Retrieved September 7, 2022 from https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf
45. Jakab, Z., & Kumhof, M. (2015). Banks are not intermediaries of loanable funds–and why this matters. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612050
46. Johnston, M. (2021). *Why Banks Don't Need Your Money to Make Loans*. Retrieved September 7, 2022 from https://www.investopedia.com/articles/investing/022416/why-banks-dont-need-your-money-make-loans.asp
47. Kagan, J. (2022). *Fractional Reserve Banking: What It Is and How It Works*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/f/fractionalreservebanking.asp
48. Kroon, H. (2022). *Introducing Self-Sovereign Identity and Identity as Collateral in Decentralized Finance.* https://repository.tudelft.nl/islandora/object/uuid%3A5728bcf1-265a-49d0-b3f5-b6653c315b1d
49. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. Retrieved September 7, 2022 from https://lamport.azurewebsites.net/pubs/byz.pdf

50. Leeway Hertz. (2022). *How does Defi Lending Work?*, Retrieved September 7, 2022 from https://www.leewayhertz.com/how-defi-lending-works/
51. Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2019). A taxonomic approach to understanding emerging blockchain identity management systems. *arXiv preprint arXiv:1908.00929*. https://arxiv.org/ftp/arxiv/papers/1908/1908.00929.pdf
52. Li, W. & Nejad. M. (2020). Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. Retrieved September 7, 2022 from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9210529
53. Li, X., Wang, X., Kong, T., Zheng, J., and Luo, M. (2022). *From Bitcoin to Solana – Innovating Blockchain towards Enterprise Application.* Retrieved September 7, 2022 from https://arxiv.org/ftp/arxiv/papers/2207/2207.05240.pdf
54. Lindner, F. (2013). *Does saving increase the supply of credit? A critique of loanable funds theory* (No. 120). IMK Working Paper. http://wer.worldeconomicsassociation.org/files/WEA-WER-4-Lindner.pdf
55. Majaski, C. (2022). *Cryptocurrency Security Token.*. Retrieved September 7, 2022 from https://www.investopedia.com/terms/s/security-token.asp
56. Makarov, I., & Schoar, A. (2022). *Cryptocurrencies and Decentralized Finance (DeFi)* (No. w30006). National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w30006/w30006.pdf
57. Marinč, M. (2022). *Introduction to Banking.* Lecture, Banking Management, School of Economics and Business, University of Ljubljana.
58. Mayr, P. (2022). *Exploring Un(der)collateralized Lending in DeFi.* Retrieved September 7, 2022 from https://www.cherry.xyz/writing/exploring-uncollateralized-lending-in-defi
59. McLeay, M., Radia, A., & Thomas, R. (2014). Money creation in the modern economy. *Bank of England Quarterly Bulletin*, Q1. https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/money-creation-in-the-modern-economy.pdf?la=en&hash=9A8788FD44A62D8BB927123544205CE476E01654
60. Pierro, G. A., & Tonelli, R. (2022, March). Can Solana be the Solution to the Blockchain Scalability Problem?. In *2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)* (pp. 1219-1226). IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9825807
61. Pritchard, J. (2021). *Learn How Loans Work Before You Borrow*. Retrieved September 7, 2022 from https://www.thebalance.com/how-loans-work-315449
62. Procoders. (2022). *How to Create a DeFi App – Guide of Successful DeFi Project Developing.* Retrieved September 7, 2022 from https://seekingalpha.com/article/4546458-solana-one-hack-too-many
63. Rajšp, G. (2020). *Analiza tehnologije veriženja podatkovnih blokov in alternativnih uporab na področju denarnih transakcij: magistrska naloga*. http://www.cek.ef.uni-lj.si/magister/rajsp3742-B.pdf

64. Rao, R. S. (2014). The Role of Retail Banking In Indian Economy. *International Journal of Engineering Research and General Science*, *2*(2), 152-158. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.428.9298&rep=rep1&type=pdf
65. RBA. (2022). *Why Banks Don't Need Your Money to Make Loans*. Retrieved September 7, 2022 from https://www.rba.gov.au/education/resources/explainers/banks-funding-costs-and-lending-rates.html
66. Rust Team. (2022a). *The Rust Programming Language*. Retrieved September 7, 2022 from https://doc.rust-lang.org/book/
67. Rust Team. (2022b). *More About Cargo and Crates.io.* Retrieved September 7, 2022 from https://doc.rust-lang.org/book/ch14-00-more-about-cargo.html
68. Rust Team. (2022c). The *Anchor Book*. Retrieved September 7, 2022 from https://book.anchor-lang.com/
69. Saengchote, K. (2022). *Decentralized lending and its users: Insights from Compound. Available at SSRN 3925344.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3925344
70. Sánchez, D. C. (2019). *Zero-knowledge proof-of-identity: Sybil-resistant, anonymous authentication on permissionless blockchains and incentive compatible, strictly dominant cryptocurrencies. arXiv preprint arXiv:1905.09093.* https://eprint.iacr.org/2019/546.pdf
71. Scottish Enterprises. (2022). *How banks make lending decisions?.* Retrieved September 7, 2022 from https://www.scottish-enterprise.com/learning-zone/business-guides/components-folder/business-guides-listing/how-banks-make-lending-decisions
72. Seeking Alpha (2022). *Solana: One hack too many.* Retrieved September 7, 2022 from https://seekingalpha.com/article/4546458-solana-one-hack-too-many
73. Shilina. (2022). *What is Solana, and how does it work?* Retrieved September 7, 2022 from https://cointelegraph.com/news/what-is-solana-and-how-does-it-work
74. Shoup, V. (2022). *Proof of history: what is it good for?* Retrieved September 7, 2022 from https://www.shoup.net/papers/poh.pdf
75. Shuaib, M., Alam, S., Alam, M. S., & Nasir, M. S. (2021). Self-sovereign identity for healthcare using blockchain. *Materials Today: Proceedings*. https://reader.elsevier.com/reader/sd/pii/S2214785321021027?token=87E4ED9D2D9EEA05F092F9C7919438B01E5270B7D8CCDF66D0CC6DA4FEB4738CF736EF1E30811746B4B1B86201498AC7&originRegion=eu-west-1&originCreation=20221003182507
76. Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning Blockchain: A Beginner's guide to building Blockchain solutions*. Apress. https://books.google.si/books/about/Beginning_Blockchain.html?id=fEpjDwAAQBAJ&printsec=frontcover&source=kp_read_button&hl=en&redir_esc=y#v=onepage&q&f=false
77. Solana Team (2022a). *Transactions.* Retrieved September 7, 2022 from https://docs.solana.com/developing/programming-model/transactions

78. Solana Team (2022b). *Cross-program invocations.* Retrieved September 7, 2022 from https://docs.solana.com/developing/programming-model/calling-between-programs#cross-program-invocations
79. Solana Cookbook (2022). *Generating PDAs.* Retrieved September 7, 2022 from https://solanacookbook.com/core-concepts/pdas.html#generating-pdas
80. Solana Explorer. (2022). *Solana Explorer.* Retrieved September 7, 2022 from https://explorer.solana.com/
81. Statista. (2022). Decentralized Finance (DeFi). Retrieved September 7, 2022 from https://www-statista-com.nukweb.nuk.uni-lj.si/study/103482/decentralized-finance-defi/
82. TrueFi Team. (2020). *TrueFi whitepaper.* Retrieved September 7, 2022 from https://blog.trusttoken.com/introducing-truefi-the-defi-protocol-for-uncollateralized-lending-9bfd6594a48
83. Tyson, M. (2022). *Solana blockchain and the Proof of History*. Retrieved September 7, 2022 from https://www.infoworld.com/article/3666736/solana-blockchain-and-the-proof-of-history.html
84. Van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv preprint arXiv:1904.12816*. https://arxiv.org/pdf/1904.12816.pdf
85. Vause, E. (2021). *The Art of Making Debts*. Retrieved September 7, 2022 from https://publicdomainreview.org/essay/the-art-of-making-debts
86. Vistra (2022). *Decentralised finance: Understanding the benefits, risks and challenges of DeFi*. Retrieved September 7, 2022 from https://www.vistra.com/insights/decentralised-finance-understanding-benefits-risks-and-challenges-defi
87. Wagner, H. (2021). *Analyzing a bank's financial statements.* Retrieved September 7, 2022 from https://www.investopedia.com/articles/stocks/07/bankfinancials.asp
88. Wamala, Y. (2021). *What Does It Mean to Refinance a Loan?.* Retrieved September 7, 2022 from https://www.valuepenguin.com/loans/refinancing-a-loan-what-it-means
89. Werner, R. A. (2014). Can banks individually create money out of nothing?—The theories and the empirical evidence. *International Review of Financial Analysis*, *36*, 1-19. https://www.researchgate.net/publication/265909749_Can_Banks_Individually_Create_Money_Out_of_Nothing_-_The_Theories_and_the_Empirical_Evidence
90. Weyl, E. G., Ohlhaver, P., & Buterin, V. (2022). *Decentralized Society: Finding Web3's Soul. Available at SSRN 4105763*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763
91. Worldcoin (2022). *Is Web 3.0 The Future Of The Internet?* Retrieved January 25, 2023 from https://worldcoin.org/articles/what-is-web-3
92. Xie, Y., Holmes, J.; & Dagher, G. (2020). ZeroLender: Trustless Peer-to-Peer Bitcoin Lending Platform. *CODASPY '20: Proceedings of the Tenth ACM Conference on Data*

and Application Security and Privacy, 247-258. https://doi.org/10.1145/3374664.3375735

93. Xu, J., & Vadgama, N. (2022). From banks to DeFi: the evolution of the lending market. In *Enabling the Internet of Value* (pp. 53-66). Springer, Cham. https://arxiv.org/abs/2104.00970
94. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*. https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf
95. Yakovenko, A. (2022). *Solana: A new architecture for a high performance blockchain v0.8.13*. Retrieved September 7, 2022 from https://solana.com/solana-whitepaper.pdf
96. Yakovenko, A. (2021). *Solana (SOL): Scaling Crypto to the Masses*. Retrieved September 7, 2022 from https://www.gemini.com/cryptopedia/solana-blockchain
97. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375. https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf

APPENDICES

Appendix 1: Abstract in Slovene

V magistrskem delu smo preučili posojilodajalstvo v obstoječem finančnem sistemu, tehnologijo veriženja blokov in na njej baziran decentralizirani finančni sistem. Magistrsko delo predstavlja akademsko delo, ki podrobno preuči in razčleni posojilodajalne protokole v decentraliziranih financah. Močno prevladujejo tako imenovani preko zavarovani protokoli, identificirali pa smo še ostale, tradicionalnem posojanju bolj podobne protokole, t.i. pod zavarovane protokole. Med njimi spadajo posojila zavarovana s strani tretje osebe, posojila v borznem posredništvu, posojila zavarovana z digitalnimi sredstvi, ter posojila zavarovana z identiteto. V tradicionalnem sistemu smo identificirali, da se posojila na makro ravni izdajajo za financiranje rasti podjetji in rasti ekonomije. Banke imajo dovolj informacij o podjetjih katere financirajo, in hkrati imajo možnost nadzorovanja uporabe posojil. Medtem pa v decentraliziranih financah ni mogoče takšno financiranje. Omenili smo da v decentraliziranih financah močno prevladujejo t.i. preko zavarovani posojilodajalni protokoli, kjer posojilojemalec zavaruje posojilo z večjo denarno vrednostjo kot pa je posojilo samo, saj se v decentraliziranem finančnem sistemu posojila uporabljajo za pridobivanje sredstev za kopičenje kripto sredstev na borzah (*ang.* margin trading). Med preučevanjem teh dveh različnih finančnih sistemov je glavna identificirana razlika torej v uporabnosti posojil. Ta problem smo v magistrski nalogi označili za ekonomski problem, ki ga pod zavarovani protokoli poskušajo rešiti.

Decentralizirani finančni sistem se razvija na podlagi načel, kot so decentraliziranost, samostojnost, samoupravnost, in sestavljivost. Zaradi načela samoupravnosti, so vsi uporabniki v decentraliziranem finančnem sistemu pseudo anonimni. To omogoča uporabo finančnega sistema tudi tistim, ki tradicionalnega sistema ne morejo uporabljati. Vendar pseudoanonimnost onemogoči predhodni pregled uporabnikov, ki zaprosijo za posojilo. Ker je decentraliziran finančni sistem v celoti digitalen in uporabniki pseudoanonimni, bi uporabniki lahko denar le vzeli in ne plačali nazaj. Takšno ravnanje je Sybilovo sposojanje. Če hočemo rešiti ekonomski problem in Sybilovo sposojanje, potrebujemo identiteto. Potreben je kompromis med načeli decentraliziranih financ in ekonomskimi iniciativami. Eden izmed kompromisov je uporaba dokazov brez znanja (*ang.* zero knowledge proofs), ki s pomočjo matematičnega dokaza omogoči identiteto brez deljenja dejanskih informacij.

V magistrskem delu smo razvili in nato analizirali pod zavarovani protokol, ki temelji na identiteti in zato velja med najbolj kompleksne posojilne protokole. Razvili smo ga na tehnologiji veriženja blokov Solana, katera nam omogoča razvijanje kompleksnih aplikacij v decentraliziranih financah. Sposobnost posojilojemalcev in uporabo posojila za kredit smo preverili s pomočjo identitete in preteklih transakcij. Ugotovili smo, da je protokol možno razviti s pomočjo ponudnikov identitete in ponudnikov kreditne sposobnosti. Magistrska naloga in razvit protokol močno pripomore k razvoju decentraliziranih financ k nadomestitvi tradicionalnih financ. Naloga je napisana v upanju, da bo v prihodnosti nekoga vodila pri vpeljevanju decentraliziranega posojilodajalskega protokola v ekonomijo. Tako bo le-ta služil za cenejše financiranje rasti realnega gospodarstva.

Appendix 2: Solana Innovations

Innovation	**Description**
Proof of History (PoH)	*A clock before consensus*
Tower BFT	*PoH-optimised version of pBFT*
Turbine	*Block propagation protocol*
Gulf Stream	*Mempool-less transaction forwarding protocol*
Sealevel	*Parallel smart contracts run-time*
Pipelining	*Transaction Processing Unit for validation optimization*
Cloudbreak	*Horizontally Scaled Account Database*
Replicators	*Distributed ledger store*

Source: Duffy (2022).