BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INTELLIGENT SYSTEMS
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

SECURITY AND PRIVACY ORIENTED-SURVEY OF FINANCIAL APPLICATIONS UTILIZING BLOCKCHAIN

PRŮZKUM FINANČNÍCH APLIKACÍ VYUŽÍVAJÍCÍ BLOCKCHAIN Z POHLEDU BEZPEČENOSTI A SOUKROMÍ

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR Mgr. HANA KŘÍŽOVÁ
AUTOR PRÁCE

SUPERVISOR Ing. IVAN HOMOLIAK, Ph.D.
VEDOUCÍ PRÁCE

BRNO 2021

Brno University of Technology
Faculty of Information Technology

Department of Intelligent Systems (DITS) Academic year 2020/2021

Bachelor's Thesis Specification

23162

Student:	**Křížová Hana, Mgr.**
Programme:	Information Technology
Title:	**Security and Privacy Oriented-Survey of Financial Applications Utilizing Blockchain**
Category:	Security

Assignment:

1. Get familiar with principles of the blockchains, their consensus protocols, smart contracts, and related security threats.
2. Study existing financial-oriented applications of blockchains and identify most common categories.
3. Analyze security and privacy threats specific to particular categories and visualize them by vulnerability/threat/defense graphs.
4. Identify the most secure and private solutions within each category and propose recommendations about their correct usage.
5. Embed your categorization into existing Security Reference Architecture for Blockchains.

Recommended literature:

- Homoliak, I., Venugopalan, S., Hum, Q., Reijsbergen, D., Schumi, R., & Szalachowski, P. (2019). The security reference architecture for blockchains: Towards a standardized model for studying vulnerabilities, threats, and defenses. *arXiv preprint arXiv:1910.09775*.
- Bonneau, Joseph, et al. "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies." *2015 IEEE symposium on security and privacy*. IEEE, 2015.
- Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* 151.2014 (2014): 1-32.
- Wang, Wenbo, et al. "A survey on consensus mechanisms and mining strategy management in blockchain networks." *IEEE Access* 7 (2019): 22328-22370.

Requirements for the first semester:

- Items 1 and 2

Detailed formal requirements can be found at https://www.fit.vut.cz/study/theses/

Supervisor:	**Homoliak Ivan, Ing., Ph.D.**
Head of Department:	Hanáček Petr, doc. Dr. Ing.
Beginning of work:	November 1, 2020
Submission deadline:	May 12, 2021
Approval date:	November 11, 2020

Abstract

This bachelor's thesis focuses on blockchain applications in the field of finance and banking, which are also called decentralized finance (DeFi). Blockchain for finance is a significant technology that changes the current system settings. In the thesis, real and potential blockchain applications from the field of finance and banking are presented. Their differences and benefits compared to the current applications controlled centrally are shown. This bachelor thesis mainly focuses on the identification of security threats resulting from the transition to blockchain and suggests their potential solutions.

Abstrakt

Tato bakalářská práce se soustřeďuje na finanční aplikace vystavěné na blockchainu, kterým se také říká decentralizované finance (DeFi). Blockchain pro oblast finančnictví představuje zásadní technologii měnící dosavadní nastavení systému. V této práci jsou představeny reálné, ale také potencionální blockchainové aplikace z oblasti finančnictví a bankovnictví. Jsou ukázány jejich rozdíly a přínosy oproti dosavadním aplikacím, které jsou řízeny centrálním způsobem. Tato bakalářská práce se především soustřeďuje na identifikaci bezpečnostních hrozeb plynoucí z přechodu na blockchain a navrhuje jejich potencionální řešení.

Keywords

blockchain, smart contracts, decentralized finance (DeFi), security, Oracle attack, Censorship attack

Klíčová slova

blockchain, smart contracts, decentralizované finance (DeFi), bezpečnost, Oracle útok, Cenzorní útok

Reference

KŘÍŽOVÁ, Hana. *Security and Privacy Oriented-Survey of Financial Applications Utilizing Blockchain.* Brno, 2021. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Ing. Ivan Homoliak, Ph.D.

Security and Privacy Oriented-Survey of Financial Applications Utilizing Blockchain

Declaration

I hereby declare that this Bachelor's thesis was prepared as an original work by the author under the supervision of Ing. Ivan Homoliak, Ph.D. I have listed all the literary sources, publications and other sources, which were used during the preparation of this thesis.

. . . .
Hana Křížová
May 4, 2021

Acknowledgements

I would like to thank my supervisor Ing. Ivan Homoliak, Ph.D. for his thorough guidance, valuable advice, and time spent on consultations.

Contents

List of Figures

Chapter 1

Introduction

Despite blockchain being a technological invention, it has its economic roots in the Austrian school, a school of economic thought founded in 19. century by Carl Menger, an Austrian economist. In his book *"Principles of Economics"* [68], he laid the foundations for a new economic approach called the Austrian School of economics.

The Austrian School of economics emphasizes the individual and her decision making - which is a pivotal component of economy. To satisfy desires, the individual chooses what she is going to buy or which services she will use. The economy is thus the result of these individual decisions and reflects individuals' desires and attitudes [22]. Any state intervention in the economy is considered undesirable, and it leads to market distortion. According to the theory, the state plays a minimal role in economy.

The Austrian School of economics refers to the economic background of blockchain. Technological foundations of blockchain are laid in the *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (hereinafter the White paper) written by Satoshi Nakamoto [72].

We live in a world of massive state interventions into the economy. These interventions are frequently reasoned by "good faith". However, they have reverse impacts (inflation, currency devaluation). Therefore, there is a huge desire to establish a new monetary and financial system without interventions, fully independent and fair. It is not surprising that Bitcoin was launched in 2009, a year after the beginning of the Great Recession when many people lost their faith in the current monetary system.

After the success of Bitcoin, blockchain has emerged in other areas such as finance and banking. Financial applications that are built on blockchain are called decentralized finance (hereinafter DeFi). In 2020, the financial volume within DeFi applications was 600m USD. As of March 2021, the total financial volume of DeFi applications reached 41 billion USD. Therefore, DeFi represents a growing financial area, where many investors are fleeing. Unfortunately, this area is facing severe attacks. Moreover, this year, U.K.'s Financial Conduct Authority (hereinafter FCA) has issued a notice warning investors about the high-risk of cryptocurrencies and Defi applications. This thesis aims to categorize financial applications, identify vulnerabilities at the application layer for each category of financial applications and suggest a potential defense.

1.1 Organization

The second chapter briefly introduces the historical background of blockchain and smart contracts. In the third chapter, blockchain technology is explained, particularly its key features, principles, and consensus protocols. The fourth chapter introduces decentralized finance in general. It shows its advantages and disadvantages compared to the current financial system. In the fifth chapter, we establish eight categories of financial applications built on blockchain, which are subject to our analysis. For each category, we describe its benefits resulting from the introduction of the blockchain. In the sixth chapter, for each financial application, its vulnerability is identified, and we propose a potential defense for the presented vulnerability. In the last chapter, we summarize our findings concerning the most common security risks and present current challenges.

Chapter 2

History of blockchain

Before the White paper was released by Satoshi Nakamoto [72], the first ideas regarding blockchain had been already presented. The first reference was made in 1976 when the concept of distributed systems was firstly introduced in *“New Directions in Cryptography“* [40]. Later, there were presented works in the area of timestamp [50], electronic cash [30], hashcash [6], which contributed to the establishment of blockchain technology. However, the game-changer was a work called *“Bitcoin Peer-to-Peer electronic cash system“* [72] published by mysterious Satoshi Nakamoto (anonymous person or group) in 2008. Foundations of an electronic monetary system based on blockchain were laid. One year later the first open software Bitcoin was launched. Since that time there has been plenty of attempts to create new cryptocurrencies and blockchain applications.

2.1 Smart Contracts

Smart contracts were introduced by Nick Szabo [89] as a computerized transaction protocol that executes the terms of a legal contract among a few parties. Despite the original definition, the smart contract now serves as a method for building decentralized applications on blockchains, which are in the scope of this work. For example, one can implement decentralized applications such as auctions or escrow services based on smart contracts. Decentralized applications that are closely related to the financial industry are also referred to as Decentralized Finance.

Chapter 3

Blockchain

Blockchain is a decentralized and distributed system keeping records of transactions created by participants. It stores data and records their movements in a distributed environment. Sometimes blockchain is described as a database shared by participants and recording their transactions [8]. In this context, the transaction represents a data record broadcasted to the blockchain.

Blockchain presents a peer-to-peer system where each of the participants keeps a copy of the database (records of transactions among participants). Based on predetermined conditions, new transactions are added to the chain. There is no superior authority that would grant permission to transaction performance [8].

Blockchain is an append-only ledger whose data are unlikely to be changed. It is based on the write-once ready-many (WORM) approach. This approach also causes that blockchain length grows continuously [62].

3.1 Blockchain Features

Decentralization

Decentralization is an essential element of blockchain. Blockchain presents a peer-to-peer system where authentications are carried out between participants. There is no central entity that validates transactions between participants. The decision-making process is transferred from one superior entity to the participants. This approach minimizes security risk coming from single-point failure [94].

Robustness

The great number of participants communicating peer-to-peer manner represents significant unlikeness of blockchain's fail. Unlike to centralized system where one endpoint holds and stores all data, participants of the blockchain (nodes) keep records of transactions. Therefore, in the event of a failure of one node, the stored data are not lost because they are available on the other nodes [94]. This feature is also described as blockchain availability. Blockchain is fully available to its participants, unlike centralized or cloud applications [54].

Transparency and Auditability

The newly created block is inserted at the end of a chain of so-far-created blocks. Blocks chronologically follow each other and have their parent block. Therefore, blockchain allows tracing previous records and via displaying a history of records their verification. This feature helps to establish a credible system.

Immutability

Immutability derives from append-only characteristics. Due to its interconnection between blocks, blockchain does not allow any changes or post-deletion of previously created blocks. The block which was once created stays in the chain without any modification. It is another feature contributing to the credibility of the blockchain.

Censorship Resistance

The crucial deficiency of central systems is their subordination to one authority, which has the ultimate decision-making power. The central authority might exercise this power arbitrarily. Certain activities may be prohibited or censored. However, blockchain, due to its decentralized system, does not allow censorship and is censorship-resistant. Due to the elimination of central entities, validation is carried out among participants, and all valid transactions are directly inserted into the blockchain after their successful approval [54].

3.2 Architecture

Blockchain network consists of independent nodes that keep a copy of the database. Node is an individual player who is capable of communicating with other nodes. If a node fails due to any reason (technical problems or hacker attack), stored data are still available to other nodes. Types of nodes can vary depending on the actions that they perform. See in Figure 3.1.

Consensus nodes

Consensus nodes are nodes with the most significant abilities. These nodes have the right to read, write, and append new transactions. They can also validate blockchain. Based on its validation process and writing skills, they can detect malicious behavior of nodes and prevent possible harm [54].

Validating nodes

Validating nodes, unlike consensus nodes, cannot write to the blockchain. Therefore, they can only detect malicious behavior, but they have no means of preventing harm [54].

Lightweight nodes

Lightweight nodes are nodes with limited privileges. They can read only some parts of the block (typically header) and validate a small number of transactions. For validation purposes, these nodes save the blockchain's header (or part of it) [54].

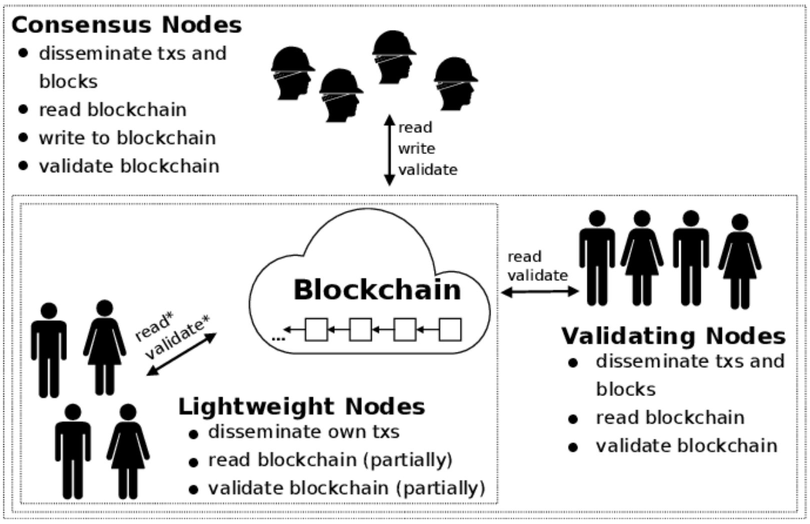


Figure 3.1: Types of nodes in blockchains [54].

3.3 Data Structures

Transaction

The transaction is described as a data record. It can vary according to blockchain purposes. It might be a record of money transfer or ownership transmission. Transaction(s) is/are formed into block.

Blocks

The structure of the block is described in Figure 3.2. Block consists of two parts block header and block body. Block header contains block version, a pointer to previous block's hash, timestamp, Nonce, Merkle tree root, and nBits. Block version determines validation rules that must be met. The nonce is an attribute used by the Proof of work protocol proving that the required amount of energy has been consumed. Merkle tree root represents a hash value of all transactions in the block and allows efficient verification of the transaction. nBits shows the current hashing target [94].

Block body contains the transaction counter and list of transactions. Block size determines the maximum number of transactions. As each block contains the hash of the previous one it reminds the shape of a chain and that is a reason for naming blockchain. The genesis block is the first block of the chain [94].

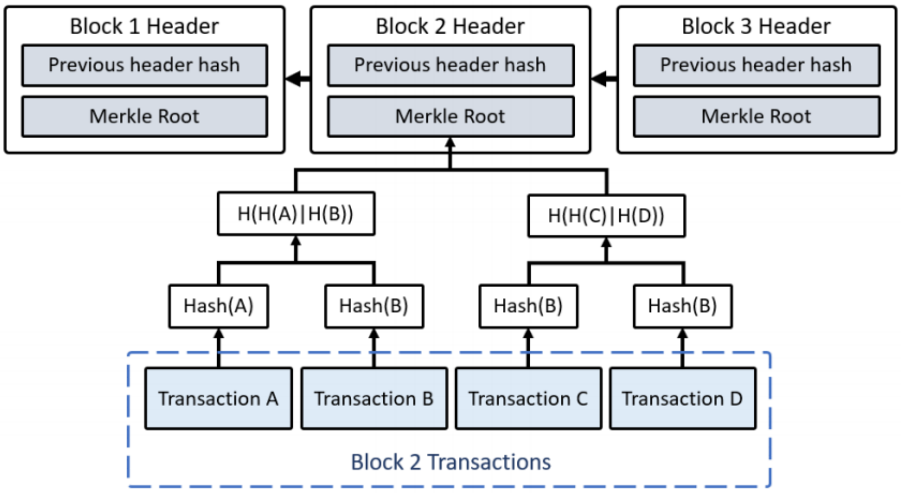


Figure 3.2: Merkle root [31].

3.4 Blockchain life cycle

After the transaction is created by any node, a message regarding the new transaction is broadcasted to all peers who further gossip the message throughout the blockchain network and it starts block mining. Once the block is mined, the newly mined block is broadcasted to all other miners and waits for its acceptance by other nodes. When validity is acknowledged, the block is added to the chain. Acceptance must be carried out in all nodes and based on the consensus of participants. This process is an essential mechanism of blockchain. Unlike current systems, where decisions are made, and transactions are approved by the central authority, blockchain is based on consensus among all participants. There are several algorithms on how to reach a consensus [18].

3.5 Consensus algorithms

Proof of work (hereinafter PoW)

PoW is a method requiring a complicated computational process. Nodes calculate a hash value of the constantly changing block header. It is called a hash puzzle (finding the desired hash). The calculation is being carried out by nodes until the required hash is found. When a node finds the required value, other nodes confirm the correctness of values [94]. Transactions must be validated for anti-fraud purposes. Then a new block can be incorporated into the blockchain.

To achieve desirable value, miners spend a considerable amount of powerful computational resources. A way to avoid a huge amount of resource loss is mining pools. Miners join into groups called “pools“ where they share resources. The mining pool has higher chances of successful mining. The mining pool is administrated by a manager who receives potential reward and allocates it among participants according to the amount of work spent with finding a block. PoW algorithm is applied in Bitcoin or Ethereum [94].

Proof of Stake (hereinafter PoS)

PoS tries to save external resources in contrast to PoW. PoS prefers nodes that own the most currencies because it is believed that nodes with lots of currencies are more trustable and unlikely cause any harm to the blockchain. However, this method supports the dominance of rich nodes and complicates the entrance for freshmen with a lower reserve of currencies. It builds a suitable environment only for rich nodes. Therefore, modification is deemed necessary. This method must be completed with other sets of rules which would randomize the final choice. Other rules might be hash number or size of stake [94]. Examples of PoS protocols are Chains of Activity [9] or Ouroboros [59].

Delegated proof of State (hereinafter DPoS)

DPoS is a method based on the voting system. Likewise PoS, DPoS prefers nodes with a higher stake. However, nodes are voting for their delegation, which later validates transactions and allows the addition of a block into the chain. This method is not directly democratic like PoS but representative democratic. Based on validating activity, nodes gain a higher reputation helping them in being re-elected [94].

Practical Byzantine Fault Tolerance (hereinafter PBFT)

PBFT presumes situations such as a malicious node or the sending of inconsistent information. Determination of a new block is divided into three parts pre-prepared, prepared, and commit. PBFT supposes 1/3 of votes can be malicious. Therefore, moving to another stage is possible if 2/3 votes of all nodes are received [94]. Examples of synchronous protocols are BFT-SMaRt [11], Tendermint [20], Byzantine Paxos [25], BChain [41]. Asynchronous protocols are SINTRA [24] and HoneyBadgerBFT [69].

3.6 Ethereum

Ethereum is an open-source platform for the creation and administration of individual blockchain decentralized apps - also known as Dapps. It can be described as an infrastructure for running Dapps. It incorporates important blockchain functionalities. Ethereum is fully decentralized and runs on a vast number of independent computers. Ethereum was introduced by Vitalik Buterin in 2013 [21], and one year later it was launched by a Swiss company Ethereum Switzerland. Ethereum has its currency Ether (ETH). It also has its programming language Solidity used for the creation of smart contracts.

3.7 Smart contract

Legally contract is a binding agreement between parties. Smart determines self-execution [18]. Therefore, the smart contract means automation of contract enforcement without any middleman. Smart contract controls that required conditions are met, and after their fulfillment, the desired transaction can be carried out. It might be understood as the implementation of business logic. According to its founder Nick Szabo [89], a computer scientist and legal scholar: *"A smart contract is an electronic transaction protocol that executes terms of a contract.*" Smart contract is embedded in Ethereum.

3.8 Types of blockchain

Types of blockchain can be distinguished according to the way the new node enters the consensus protocol. We describe three different types of blockchains in the following.

Permissioned

Blockchain membership must be approved by the central authority. Therefore, blockchain can only be accessed by those who are allowed to access it. Hence, the important aspect of this category is that the identity of nodes is known. The node which received authorized permission may join the consensus protocol and has the right to read, access, and write information on the blockchain. Usually, nodes have equal consensus power within this category [54].

Permissionless

On the contrary, the permissionless blockchain is publicly available, and anyone can join the consensus protocol without the need for approval. However, malicious behavior of nodes is anticipated, and the blockchain sets rules to detect it and eliminate it [54]. Permissionless blockchain might keep its users anonymous as there is no duty to identify participants.

Semi-Permissionless

Permission for joining the consensus protocol is required. However, there is no centralized authority that grants it, any consensus node can do so [54].

Chapter 4

Decentralized finance

The current financial world has been managed by superior entities that heavily influence its shape and consume its resources. The system is called centralized finance (hereinafter CeFi). Blockchain brings a new concept that can significantly change the architecture of the current financial system. It is called decentralized finance (hereinafter DeFi).

DeFi includes financial services based on blockchain architecture, cryptography, and smart contracts. Financial services and applications can be carried out directly between participants without the approval of central authorities or the presence of third parties. DeFi contributes to significant cost savings for external services, facilitates service delivery, and transfers decision-making processes from the central level to the participants. Therefore, DeFi brings greater transparency and overall openness. The purpose of DeFi is to create a new financial ecosystem which will be independent, fair, and accessible to everyone [27].

4.1 Advantages of DeFi

Full control

CeFi applications are based on a custodial model. Financial institutions exercise full custody over clients' funds, and the client has no other choice than to trust them. Furthermore, this custody is usually subject to charges. Compared to DeFi, clients have full control over their assets and are free to decide how to dispose of them. Blockchain creates a safe financial environment among participants who do not trust each other but can interact without third entities [96].

Accessibility and higher democracy

Access to CeFi applications is considerably limited. Possible clients must fulfill several entry conditions to reach financial services. Some of these conditions may cause significant barriers, preventing public access to financial services. Blockchain, on the contrary, is boundless. Financial services based on the blockchain can be offered more widely. DeFi allows anyone to utilize financial services without censoring or blocking access by a third party [96]. Therefore, blockchain contributes to greater democratization of the financial industry and facilitates access to financial services for everyone.

Lower expenses

The removal of intermediaries significantly reduces the additional costs. This cut contributes to lower costs of financial services reflecting the final price of financial products. Therefore, utilizing blockchain leads to wider customer accessibility and greater democratization of financial services.

Data security

In the case of CeFi, all customers' data are saved in a single point which might fail due to attack or technical problems. Failure of a single point is devastating for both providers of financial services and customers. The data breach is usually irreversible. Utilizing blockchain, the risk of a data breach is considerably lower because each node holds a copy of the blockchain.

Transparency

Based on its characteristics (append-only transaction, chronological order, and cryptographic principles), blockchain allows tracing previous records and via displaying a history of records their verification. A participant can easily audit all activities that have occurred on the blockchain network and can rely on the credibility of these records [96]. This characteristic contributes to building a stable and credible financial system.

4.2 Disadvantages of DeFi

Legal environment

Despite living in a digitalized society, many legal systems do not cover this topic and are not ready for new disputes. Therefore, enforcement of claims arising from a new digital society is difficult and often has no legal support. Due to the mentioned legal problem application of blockchain might face skepticism and reluctance. The legal environment should respond flexibly to new challenges related to the blockchain. Otherwise, it hinders the technological development of society.

Money Laundering and Terrorist Funding

Blockchain is frequently criticized for its possibility of abuse regarding drug dealing, blackmailing, money laundering, and terrorist funding. To manage the fight against these illegal activities, it is necessary to introduce identity management that would identify and verify participants. Identity management would help in tracing financial flow and would lead to minimizing money laundering. However, the current legal system does not cover this area. Therefore, measures adopted by blockchain have no effect [48]. Another problem related to identity management is the inconsistency of rules, institutions fail to agree on uniform rules for identity identification and verification that would be applied uniformly.

Costs

Although the blockchain via eliminating third entities leads to cost reduction, on the contrary, transaction costs are increasing. The increase lies in transaction fees that have risen considerably [96]. Increasing transaction costs lead to more expensive transactions, which is not worth in the case of small transactions. Cost increase results in slowing down of DeFi applications global spread and use [57].

Governance

Another issue of blockchain impacting DeFi is problematic governance. Governance refers to processes involving creating, updating, or abandoning rules of a system. Many changes into protocol design require a hard fork, and thus all nodes should update the latest version of the protocol software. The problem occurs if nodes fail to agree on the update of blockchain and one group of nodes follows the previous protocol, and the other group follows the new version. Therefore, the hard fork leads to a branching of the blockchain, which is not desirable.

Chapter 5

Financial applications utilizing blockchain

5.1 Derivatives

The purpose of financial derivatives is to spread the risk associated with investing. Financial derivatives are often used for hedging and speculative investments. The origins of financial derivatives are as old as the market itself [96].

Derivatives derive their value from the value of monitored assets such as bonds, stocks, or currencies [96]. The goal of implementation financial derivatives on a blockchain is to establish an independent and fair financial environment, eliminate third parties that often negatively influence the market, and consequently reduce costs.

Unlike CeFi applications, which rely on a risk management system, blockchain applications in the area of derivatives are often collateralized to hedge risk [96]. However, collateral risk hedging is inefficient as the trader has to deposit large assets. This method of hedging can lead to the low popularity of blockchain applications.

Derivatives can be settled physically when the underlying asset is transferred between parties. However, the most common settlement is cash settlement, when the price difference of the underlying asset is paid. Derivatives can be traded via Automated market maker or order book model (Decentralized exchanges) [96].

An example of a blockchain application that provides various derivatives is Synthetix. Synthetix is built on Ethereum and uses the smart contract as its counterparty. Therefore, it is similar to an Automated market maker. Synthetix enables bets on crypto assets, stocks, bonds, currencies, and other assets in the form of tokens. Synthetix tracks the price movement of assets via a decentralized oracle system (price oracle). Tokens can be used to bet on price increase or decrease of underlying assets. Synthetix users lock up collateral to create a synthetic asset which enables exchanging one synthetic asset for another [19]. The price is not set according to to supply and demand as in the order book model, but according to price oracle. The principle is explained in Figure 5.1.

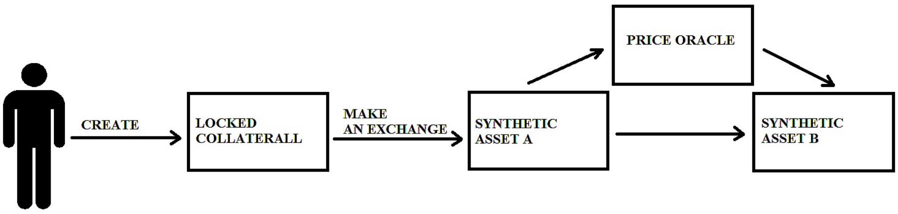


Figure 5.1: Synthetix exchange [10].

Examples of derivatives are:

Futures

Futures are a type of obligation where one party undertakes to buy or sell a specific asset at an agreed price and on a particular day in the future. Sometimes it is referred to as a futures contract. For example, Party A undertakes to purchase one hundred bitcoins from Party B on 31 December. If parties agreed that the price of one bitcoin would be $ 100, and the price of bitcoin rises to $ 150 at the time of enforceability of the contract, a net profit of Party A is $ 5,000 (difference in bitcoin price * quantity of purchased bitcoins). However, if the bitcoin price decreased, Party B would make a profit. Nevertheless, due to the high price volatility of cryptocurrencies, it is difficult to determine the price and both parties are exposed to significant risks. Therefore, this type of derivatives is not very widespread in DeFi [96].

Perpetual Swap

Perpetual swap is similar to futures, but with the difference that it has no expiry date. It means that there is no date in the future at which the contract expires or must be settled [35]. Traders open their derivative position and bet on a drop or increase of the value of an asset. If traders believe that the value of an asset will rise, they open a long position. Contrary, they open short position [35].

The trader opens or closes derivative positions based on current price developments of monitored assets. The perpetual swap allows traders a quick and flexible response to actual price fluctuation [96]. For example, if a trader has made a misjudgment about the price of a particular asset, she may close her position immediately, thus avoiding a significant loss. However, if the same happened to her in the futures contract, she would have to wait until the settlement date, which could bring her a devastating loss.

When traders open their derivative position, they will be charged funding fees. The purpose of funding fees is to keep contract prices consistent with the underlying asset. Perpetual swaps due to their timelessness have no convergence mechanism and funding fees are a tool to incentivize this convergence. The final price of perpetual swap contracts consists, among other things, of funding fees penalizing or rewarding traders, depending on the nature of their position (long or short). For example, if the contract price is too high, long positions will pay short positions a fee [38]. Perpetual swaps are provided by eg. BitMex [16].

Options

Options are a type of commitment between the seller and the buyer to fulfill an obligation. The buyer decides on the timing of the fulfillment. However, the buyer bears the risk of reducing the value of the obligation in the event of later enforcement [96]. An example of a blockchain application providing an option is Ledgerx [78].

5.2 Identity management and KYC

KYC means “know your customer“, and it refers to a policy that deals with verification of identity to avoid money laundering, terrorist funding, or identity theft. KYC is widely applied in the financial sector. Each financial institution follows its KYC policy to detect fraudulent transactions.

Unfortunately, there is no global standard for the KYC, which leads to a lower capability to collaborate on identity verification. Nowadays, customers’ identity is verified by financial institutions individually. For example, for each opening bank account, the client must undergo the verification process again. For both parties (client and financial institutions), the KYC is a time-consuming and expensive procedure [75].

Unlike the current situation, in the KYC Blockchain application, the client shares her private information only once. KYC Blockchain application contains a database of clients’ information shared among nodes. If the client allows it, her information is made available to the concerned node [75]. See in Figure 5.2.

One of the first pioneers in the area of KYC is the project Decentralized Identifiers (hereinafter DIDs). DIDs create a digital identity of any person, organization, or subject and enables their KYC verification. DIDs are represented by URI that links a DID subject with a DID document. URI is a simple text string consisting of scheme identifier, method, and method-specific identifier. DID subject can be any entity (person, group, or thing) identified by a DID and described by a DID document that contains data such as cryptographic public keys [81]. DID identification is incorporated in the Hyperledger Indy [56] project, the most developed project in the field of identity management. Unfortunately, the difficulty of this project is the involvement of a centralized entity, which produces verifiable credentials.

However, the above-mentioned concept is not widespread due to its incompatibility with other applications. Each application uses its KYC and is reluctant to accept other KYC rules. Other projects on KYC Blockchain applications are KYC-Chain [29], Cambridge Blockchain [26], SelfKey [86], and Civic [32].

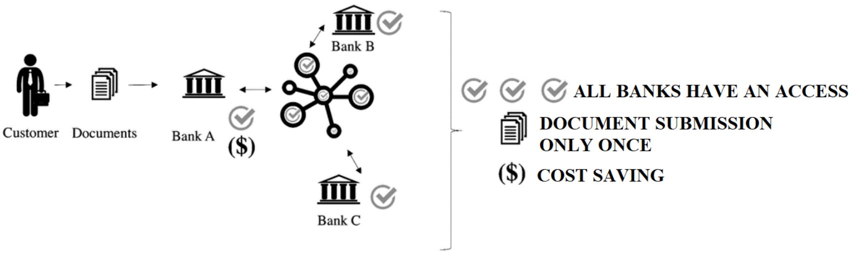


Figure 5.2: KYC on Blockchain [71].

5.3 Prediction markets

A prediction market is a market where participants bet on the outcome of the predicted events. Examples of such events are *“The price of BTC will exceed 70 000 dollars before the end of 2021“*, or *“Donald Trump will be president in 2024.“* Successful predictions are monetarized. Prediction-making lies in a method called the *“wisdom of the crowd“* where predictions coming from a group of untrained individuals are more accurate than the one from trained professionals [47].

Prediction markets had already existed before the introduction of blockchain. However, prediction markets were managed in a centralized way. The crucial moment in the prediction market is the occurrence of an expected event and its reporting. In the case of CeFi, reports are announced by a central entity. See in Figure 5.3. Unfortunately, CeFi has no means to ensure wise, impartial judge, whom all participants in the market trust [79]. Therefore, the risk that reports might not be accurate is high. A way to avoid misleading or tampered reports is the blockchain, where the outcome comes from participants themselves. See in Figure 5.4. Since blockchain joins lots of participants, the possibilities for influencing are considerably low [79]. Based on reports that a monitored event has occurred, the smart contract stipulates who correctly predicted and who would be rewarded.

A popular blockchain application in the area of the prediction market is Augur. In Augur anyone is entitled to create a market predicting the real event. Users of Augur can freely join any prediction market and bet. The crucial element in Augur is the reputation token which is needed for reporting results of predicted events. Determination of the outcome is based on a consensus of market reporters. Reputation token is not stable and may be gained or lost depending on the accuracy of predicted events [79]. Other examples of applications regarding the prediction market are Stox [87], or Gnosis [49].

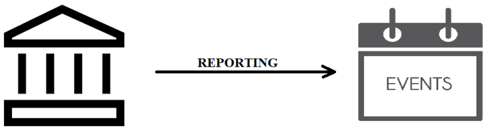


Figure 5.3: CeFi in prediction market.

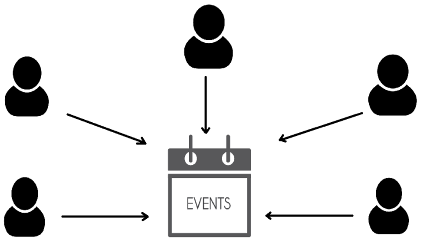


Figure 5.4: DeFi in prediction market.

5.4 Stablecoin

The value of cryptocurrencies, in general, is still very volatile and is subject to daily deep price fluctuation. It is a target of speculative traders who play with the hype of demand. However, high price fluctuation is not attractive for serious investors who want to hold cryptocurrencies for an extended period. Stablecoin solves the problem [77].

The stablecoin is a cryptocurrency that aims to stabilize its price and purchase power [77]. A stable exchange rate and no volatility are pivotal characteristics of stablecoin. The stablecoin performs two crucial functions: payments and asset management. The stablecoin serves as a payment and transfer tool between cryptocurrencies and real-world currencies. Due to its stability, stablecoin is a means for saving the value in the volatile market of cryptocurrencies [1].

The stablecoin is divided into two categories custodial and non-custodial. Custodial stablecoins are pegged to collateral assets such as fiat currencies, bonds, or commodities [60]. See in Figure 5.5. These assets are usually off-chain stored. Custodial stablecoins are further classified into Reserve Fund and Fractional Reserve Fund. In the case of the Reserve Fund, the reserve ratio reaches 100%. Each stablecoin is backed by a unit of the reserve asset managed by the custodian. Unlike the Reserve Fund, the Fractional Reserve Fund holds only certain percentage of reserve assets. The principle of the Fractional Reserve Fund is similar to commercial bank deposits [60]. Examples of custodial stablecoins are Tether [90], TrueUSD(TUSD) [93], or Binance [12].

Non-custodial stablecoins are algorithmically backed by collateral. The issuance of new coins depends on many factors, such as the value of other cryptocurrencies or developments in financial markets. These factors are controlled in smart contracts, which also decide on the issuance of new coins after their fulfillment. Therefore, the peg is related to the financial market and its development [46]. Unlike the custodial stablecoins third-party participation is excluded [60]. See in Figure 5.6. An example of non-custodial stablecoin is DAI [67].

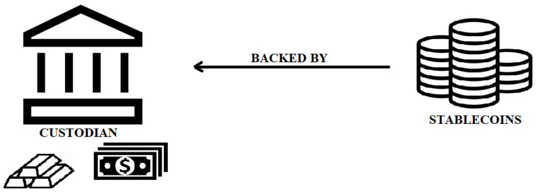


Figure 5.5: Custodial stablecoins.

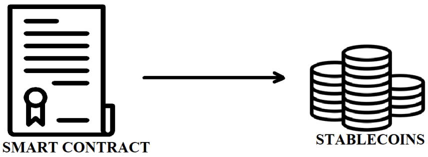


Figure 5.6: Non-custodial stablecoins.

5.5 Cryptocurrency Exchanges

There are three types of cryptocurrency exchanges: Centralized exchanges, Decentralized exchanges, and Automated market makers.

Centralized exchanges

Centralized exchanges are platforms where traders are enabled to buy, sell and exchange cryptocurrencies against other cryptocurrencies or fiat currencies. Transactions are under the full control of the owners of the exchange. Traders deposit their funds directly on the exchanges, and then exchanges assume the responsibility for the execution of a transaction. Traders do not have access to their private keys and must trust the owners in the execution of transactions [2]. The most popular centralized exchanges platform is Binance. Binance was founded by Changpeng Zhao in 2017 and has had one of the largest trading volumes. It carries out more than 1,400,000 transactions per second [12]. Other examples are Huobi Global [55], Bybit [23], BitMEX [16], or OKEx [74].

Decentralized exchanges

Decentralized exchanges (hereinafter DEX) operate without a central authority. Traders have full control over their crypto assets. Transactions on decentralized exchanges are carried out by smart contracts and atomic swaps. A trader (a token owner), who wants to make an exchange of her assets, sets up a selling order where specifies the number of units, the cost of the token, and the time for bidding. A trader makes her selling order available for other traders who submit bids. After the time is up, the transaction is carried out [14]. Examples of decentralized exchanges are Binance DEX [12], Dydx [42], or Sushiswap [88].

Automated market makers

Traditionally, the market consists of subjects (a purchaser and a vendor) who trade with each other (peer-to-peer transaction). The purchaser tries to buy an asset for the lowest price possible, and the vendor tries to sell the asset for the highest price possible. The price of the asset is a result of the clash depending on the market influence of these subjects. This concept is called the order book model. In the order book model, market creation is caused by the clash between the purchaser and the vendor [45].

Unlike the order book model, an automated market maker (hereinafter AMM) can create a market without the existence of a second counterparty substituted by the smart contract. The trade is carried out between party and smart contract (peer-to-contract transaction) based on a set mathematical formula. The formula defines the price of a demanded asset [15]. The AMM belongs to an intra-chain decentralized exchange protocol.

In connection with the Automated market maker, it is necessary to describe a liquidity pool. The liquidity pool substitutes the second counterparty, and it is a tool facilitating decentralized trading and providing liquidity. The liquidity pool consists of tokens locked in the smart contract. The market is created by the addition of an equal value of two tokens into a pool. A liquidity provider, a creator of the liquidity pool, sets the initial asset price and receives LP tokens according to the quantity of provided liquidity. Assets price is derived from the ratio of the tokens in the liquidity pool [45]. See in Figure 5.7.

Sometimes an impermanent loss occurs in the liquidity pool. The impermanent loss is a consequence of the price difference between real-world price and price set in the liquidity pool. The impermanent loss occurs when the ratio between the two tokens is set, but suddenly price of one token changes. The loss is called impermanent until the price settles according to real-world price. The impermanent loss might be common for volatile cryptocurrency. This situation opens a door for speculative trading [15].

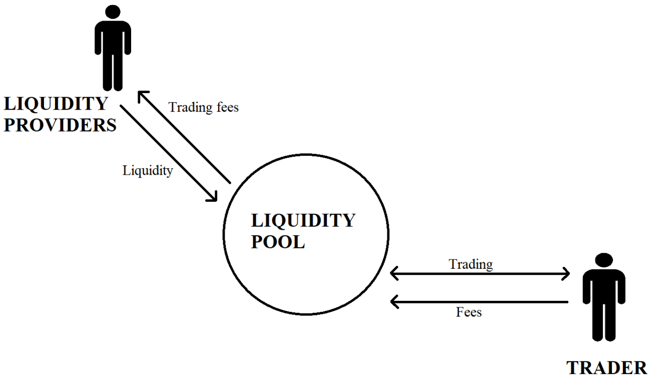


Figure 5.7: Liquidity pool.

Examples of exchanges are:

Uniswap The Uniswap is an automated liquidity protocol build on Ethereum. The Uniswap provides liquidity pools managed by smart contracts that allow token swap, addition, and removal of liquidity. Asset price is determined by the mathematical formula: $x * y = k$. Variables x and y represent the quantity of token A and token B available in a liquidity pool, and k is a constant value. The higher addition of token A is, the higher the removal of token B must be carried out [3].

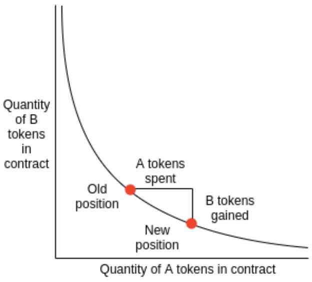


Figure 5.8: Uniswap formula [82].

Balancer Like Uniswap, the Balancer is an automated liquidity protocol build on Ethereum. However, the Balancer supports a higher amount of assets (up to eight) in one liquidity pool. More types of assets in one liquidity pool are profitable for users because they can freely distribute the risk arising from price fluctuation. Another difference is trading fees. In the case of the Balancer, trading fees are set by the liquidity pool creator. Uniswap charges a flat fee of 0.30% per trade. The last significant difference between the Balancer and the Uniswap lies in the weighting of LP assets. In the case of the Balancer, weighting is arbitrary. The Uniswap weights assets in ratio 1:1 [91].

Bancor The Bancor is a blockchain protocol providing the Dynamic Automated Market Maker (hereinafter DAMM). It is a new type of automated market maker liquidity pool integrated with Chainlink price oracles helping to determine the correct price. Integration with a decentralized price oracle should mitigate an impermanent loss. The Bancor derives its name from the name of a supra-national reserve currency, which was introduced at the Bretton Woods conference in 1944 by John Maynard Keynes, an English economist. The Bancor enables direct token conversion with other tokens on different blockchains, without the presence of a counterparty. Token conversion flow is managed by the Bancor Network smart contracts [64].

SET SET is a protocol built on Ethereum providing strategic asset management and automatically executes such a strategy. It can be described as a robot advisor in the world of DeFi. SET offers several investment strategies (or sets) which are tokenized. Users purchase tokens representing assets traded according to the chosen strategy [4]. It is possible to cash out tokens into Ethereum. The protocol is transparent, so users are familiarized with the procedure for dealing with their assets. There are four main strategies approaches trend trading, inverse, range-bound, and buy and hold.

The trend trading approach constitutes its strategy on statistical and market sentiment analysis of an asset's momentum. The range-bound approach is a strategy monitoring the price fluctuation of a particular asset and creates its investment strategy accordingly. The inverse approach monitors a particular asset for 20 days and, based on its price development within the period, decides on their purchase or sale. The buy-and-hold approach holds a portfolio of BTC and Ethereum in a certain ratio. According to price fluctuation, the portfolio is adjusted [4].

5.6 Credit and lending

The lending industry governed in a centralized manner suffers from several flaws. Loans are usually provided by entities deciding based on their criteria to whom they will grant a loan. Unfortunately, these entities often do not follow the set criteria themselves and circumvent them. An example is the Great Recession of 2008 when mortgages were provided to people who were not entitled to them. The system of trust placed in these entities has completely failed. It is also linked to the high level of corruption and fraud that occurs in the sector [70]. Unfortunately, loans are not always provided on the basis of careful risk management, but rather based on connections. The last flaw of the current lending industry is a large bureaucracy. The customer must submit an enormous quantity of documents to fulfill set criteria. Furthermore, the approval process takes a long time and may not always respond effectively to the customer's current needs. The lending industry consequently becomes very inefficient and inflexible.

Blockchain offers a fresh opportunity to create a fairer lending environment by excluding third parties and establishing a direct link between the creditor and the debtor. On the basis of precisely given conditions set in smart contracts and uniformly applied, blockchain makes lending easier, smoother, and more efficient [70]. See in Figure 5.9. Blockchain also increases the certainty of which entities are eligible for a loan and thus prevents fraud.

DeFi application usually enables role duality. The client can exercise both roles - a debtor and a creditor. This option enables more efficient management of assets, as the user can respond quickly and flexibly to her current financial situation.

Examples of blockchain applications in the field of loans include Salt Lending [85], which provides cash loans backed by digital assets, Celsius network [28], which also provides cash loans backed by cryptocurrencies, Liquid mortgage, focused on providing mortgages, Wetrust [97], providing loans based on social capital and personal trust networks. Lendroid is another example of a blockchain application used for lending and borrowing cryptocurrencies [36]. It creates a decentralized system of nodes that may act as creditor or debtor. Based on clear conditions set in smart contract lending or borrowing is a self-executing process [63].

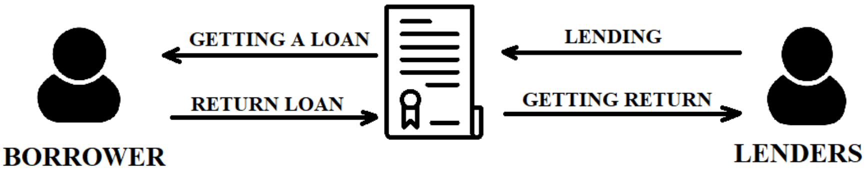


Figure 5.9: Lending in blockchain.

5.7 Payments

The current payment system is controlled by monopoly companies that manage worldwide payment flow. Since these companies are mainly monopolies, high operating costs are charged. Payments carried out via blockchain eliminates the cost and facilitates fast and secure cross-border payments with real-time verification and without clearing. The blockchain also establishes a direct connection between payer and payee.

In connection with payments, it is necessary to mention wallets which is an interface that manages cryptocurrency private keys. The wallet consists of two unique keys: the public key and the private key. The purpose of the private key is to authenticate asset ownership and encrypt the wallet [65]. Therefore, the private key must be kept secret. Contrary, the purpose of the public key is to identify the wallet and to receive funds [65]. The wallet fulfills one of the crucial characteristics of a blockchain, which is full custody over assets. The owner via wallet controls and manages her assets without the participation of a third entity.

There are different types of wallets. It differs according to the method of storing and accessing private keys. Examples of wallets are:

Keys in local storage

It is an unencrypted form of private key storing. Plaintext form of the private key is stored on the local storage of a machine [53]. Examples of wallets using the unencrypted form are Bitcoin Core or MyEtherWallet.

Password-Protected Wallet

It is an encrypted form of private key storing. The user must submit her specific password to encrypt the private key [53]. Examples of wallets supporting this functionality are Bitcoin Wallet, Bitcoin Core, or Electrum Wallet.

Password-Derived Wallet

It is a type of wallet that computes its private keys. It is also called brain wallets or hierarchical deterministic wallets [53]. It starts with a single key pair as the master keypair, from which all future keys are calculated. Examples of these wallets are Electrum, Armory Secure Wallet, or Daedalus Wallet.

Hardware Storage Wallets

A hardware storage wallet provides storage of the private key in a secure hardware device. It is also called cold storage, where private keys are isolated from the Internet. Cold storage mitigates the risks of an online attack. On the contrary, there is a risk of theft of hardware wallets. However, it is almost impossible extraction of private keys from a stolen hardware wallet. Private keys stored on the hardware wallet are protected by a PIN and an optional passphrase [53]. Examples are Trezor, Ledger, KeepKey, or BitLox.

Split Control - Threshold Cryptography

The core idea of threshold Cryptography lies in splitting the private key into several parties acting as transaction approvers. A minimum number of approvers who must collaborate is set to retrieve the private key [53].

Split Control - Multi-Signature Wallets

A multi-signature wallet is a wallet owned by two or more users. Transaction of the wallet must be signed by the required number of signatures. In the case of a 2-3 wallet, there are three owners, and two signatures to sign a transaction are required [53]. Examples are Lockboxes of Armory Secure Wallet and Electrum Wallet.

Hosted Wallets

Hosted Wallets are not true wallets. They only offer an online interface for interaction between the user and the blockchain. The user can display transaction history or manage crypto-tokens. However, there is no private key storage. The private key is stored on the server, so the wallet does not have full control over the private key [53].

Server-Side Wallets

It is a wallet whose key is stored on the server, and the wallet has full control over the private key. Therefore, it is the opposite of hosted wallets. A server-side wallet is similar to the custodial model in CeFi applications that takes full care of a client's account [53]. An example of such a wallet is Coinbase.

Client-Side Wallets

Client-Side Wallets enables two-Factor authentication. The first authentication is carried out against the server based on the knowledge of a password. The second one is carried out again against the server but through one of the options consisting of Google Authenticator, YubiKey, SMS, and email [53]. An example of such a wallet is Blockchain Wallet.

Despite the above-mentioned positives, payments based on blockchain technology face technical difficulties, particularly transaction speed and transaction costs. To eliminate these deficiencies, the second layer of blockchain was introduced. Integration of the second layer helps with the offloading transaction. Within the second layer, blockchain transactions are carried out independently of the first layer. The second layer does not interrupt the blockchain technology and is built on top of an existing blockchain system [76].

One of the first attempts to create the second layer is the Bitcoin Lightning Network that consists of state channels where blockchain transactions are performed. The Bitcoin Lightning Network reports its performance to the main (root) layer [76].

5.8 Insurance

The current insurance system is hierarchical and includes several redundant levels. Blockchain establishes a direct connection between entities and simplifies the system using smart contracts. The most probable insurance-rated use cases are the KYC use case, Automated underwriting and claims handling, and fraud detection.

The KYC use case

Like the above-mentioned KYC blockchain applications, the KYC use case in the field of insurance should be used to identify and verify clients. The main goal is to simplify identification and verification procedures for clients and insurance companies. The client shares her private information only once [66]. KYC blockchain application contains a database of client's information shared among nodes. Based on the client's consent, her information is made available to the concerned node. Blockchain increases efficiency and speeds up procedures.

Automated underwriting and claims handling

Another use case in the field of insurance concerns automation of the premiums payment and the settlement of complaints. See in Figure 5.10. Based on data from an oracle, the smart contract decides on the payment of the premium or its termination. However, this concept is too theoretical, and its main drawback is the absence of a reliable data feed [66]. Dynamis has tried to link its blockchain application with a social network system that would decide on the payment of unemployment insurance [37]. When a person becomes unemployed, it is recorded, and the smart contract decides on issue insurance payments. However, it is a very theoretical use case, and it is still under development.

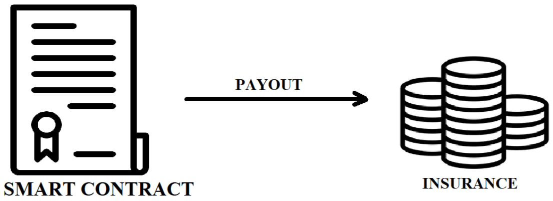


Figure 5.10: Automated underwriting and claims handling in insurance.

Fraud detection

In this case, blockchain should detect fraud. The mechanism lies in sharing fraudulent claims with other institutions to help classify bad behavior patterns. However, it is necessary to create a coordinated effort among institutions [66]. Blockchain would avoid multiple claims regarding the same accident because accidents would be reported only once. Nevertheless, it is again a very theoretical model, which has not been available in practice. Its main drawbacks are reluctance among insurance companies and the inability to share personal information.

Chapter 6

Security and privacy threats related to financial applications utilizing blockchain

6.1 Derivatives

Reliable determination of prices is a key element in creating a stable and credible blockchain application in the area of financial derivatives. Therefore, it is necessary to avoid any price manipulation that leads to market distortion. Oracle attacks are usually used to manipulate the price. However, there are two types of attacks under the term oracle attack, namely market manipulation and oracle manipulation [96]. See in Figure 6.1.

Market manipulation is a type of attack that intentionally distorts the market environment, artificially influences supply and demand, from which an attacker eventually benefits [96]. It is, for example, triggered by artificially created arbitrage, which is involved in the rapid and mass process of borrowing, exchanging, and storing a large number of tokens. Based on these artificially induced processes, the price of assets is manipulated. If the price of the attacked asset serves as the underlying asset then the attack may cause a snowball effect leading to a massive impact on the market [52].

One possible way to minimize this attack is to introduce the Funding Fee mechanism used in Bitmex. The introduction of the Funding Fee could reduce the volume of financial operations [52]. A potential attack would thus become more expensive and the number of costs associated with the attack could discourage the attacker.

The purpose of the Funding Fee is to keep contract prices consistent with the underlying asset. It is called a convergence mechanism. Funding fees penalize or reward traders, depending on the nature of their position (long or short). Funding fees are periodically paid for (or earn) when a trader has an open position. These are possible scenarios: If a trader has a long position and funding is negative, a trader will be paid for having her position open [92]. If a trader has a long position and funding is positive, a trader will be paying the shorts. If a trader has a short position and funding is positive, a trader will be paid for her position. If a trader has a short position and funding is negative, a trader will be paying the longs [34]. A high financial penalty could thus deter an attacker from a possible attack.

Another way to minimize market manipulation is an introduction of decentralized oracle networks such as Chainlink to provide and verify price information [52]. Chainlink provides real-world data to smart contracts on the blockchain. Smart contracts evaluate given data and automatically initiate execution when certain conditions are met.

The second type of oracle attack is an oracle manipulation [96]. See in Figure 6.1. In the case of centralized oracles, the risk lies in the single authority that feeds price information. It is difficult to ensure wise, impartial authority, whom all participants in the market trust. The authority may intentionally supply manipulated data. The solution is a conversion to a decentralized oracle.

Unfortunately, even a decentralized oracle can face troubles with malicious data feed. One way to mitigate the false data feed is by aggregating data feeds from multiple resources and using a reputation system for their verification [96].

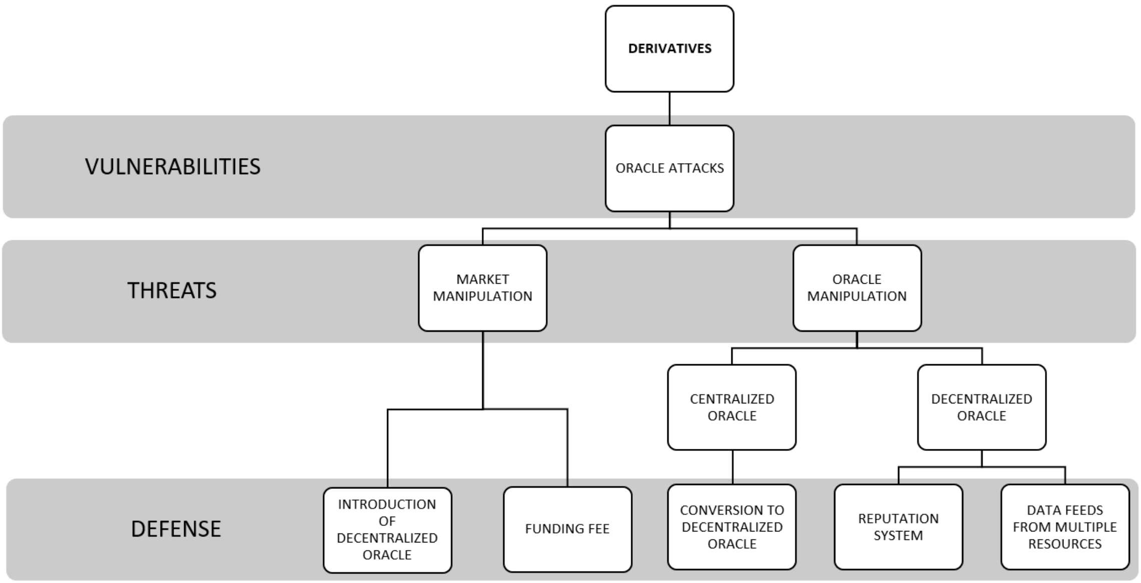


Figure 6.1: Vulnerabilities, threats, and defenses of Derivatives part 1.

Due to the on-chain characteristic of some blockchain applications, there is a risk of a front-running attack. See in Figure 6.2. The name front running attack comes from the days of paper stocks. At that time, if a participant learned that a large purchase of certain shares were approaching, she tried to buy this stock first and then sell them at the highest market price. This principle is similar in blockchain when transactions are overridden by malicious transactions containing a higher fee [54]. Front-runners obtain information on transactions from the mempool (the pool of unconfirmed transactions). The attack is caused due to the possibility that anyone can start validating blocks and sending transactions.

One possible solution is to introduce a transaction counter set in the smart contract. The transaction counter is incremented by one if a state-modifying transaction occurs in the smart contract[33]. The value of the transaction counter is sent together with the transaction. If the transaction counter's value is not equal to the specified value, the transaction reverts. For a better understanding, if the buyer requests to buy assets at a certain price, a transaction counter is set. If the contract owner updates the price of the asset, the transaction counter is incremented by one. If the current transaction counter does not equal to original transaction counter set by the buyer, the buyer's transaction is reverted. The transaction counter is checked in the smart contract.

Another solution is a limit in the form of a gas price. Ethereum allows checking the gas cost for the transaction. It is checked whether the gas cost is less than or equal to max gas price[39] preventing preferential transaction behavior. A potential solution is also the injective protocol funded by Binance Labs. The protocol lies in proof of elapsed time, where the user proves that she has spent a certain amount of time by solving verifiable delay functions (VDF's) [39]. The idea is that the one who started the VDF solution process first will have the best chance of completing the transaction.

Another proposal is a commitment scheme, where the name and public bid are published at the first step and text is published afterward. It could be also a solution for this type of attack [54]. See in Figure 6.1.

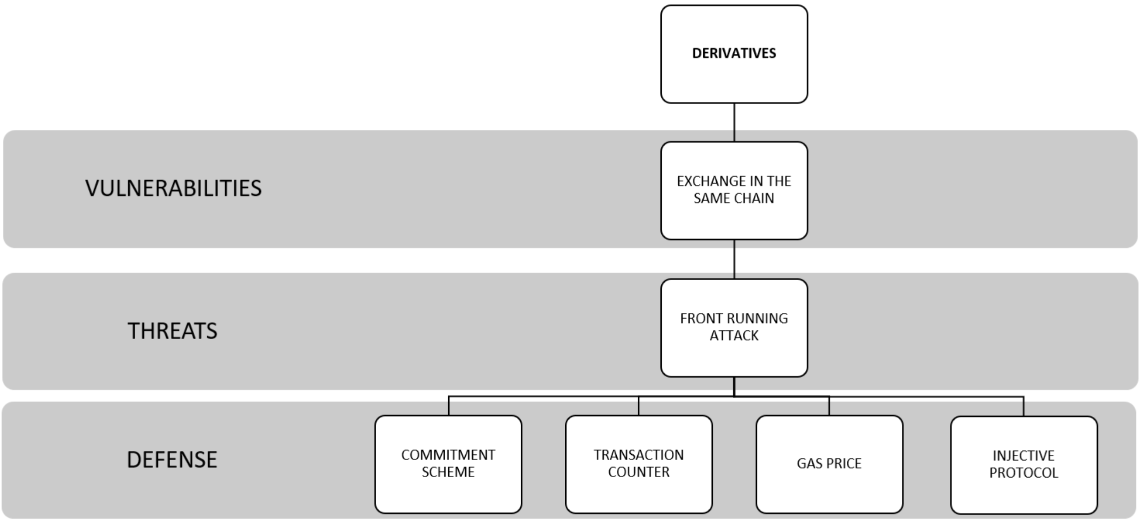


Figure 6.2: Vulnerabilities, threats, and defenses of Derivatives part 2.

6.2 Identity management and KYC

The core issue related to KYC applications is coming from the nature of stored data. Data stored on the KYC blockchain application and shared among nodes concerns sensitive personal information such as name, address, occupation, etc. Therefore, the protection of data integrity must be an essential part of the KYC blockchain application. It must be avoided that the malicious node seizes sensitive data.

The solution for this problem could be data stored off-chain. See in Figure 6.3. Blockchain would keep only hashes of such data. It would be more difficult for an attacker to access this data. However, off-chain data storage is not a flawless solution, and it opens a door for new security threats such as censorship attacks and availability issues [54].

The risk of a censorship attack arises when third parties are involved in the blockchain. These entities decide on writing their transactions to the blockchain and thus can prioritize certain transactions over others. The censorship attack could be mitigated via on-chain censorship resolution [54].

The availability issue arises when a new block is created, and it is uncertain whether all the data of the new block has been published on the network. If all data is not available, it is not possible to determine whether it contains a malicious transaction [5]. The availability issue could be mitigated by converting to fully on-chain systems or partially replicated decentralized file systems [54]. See in Figure 6.3.

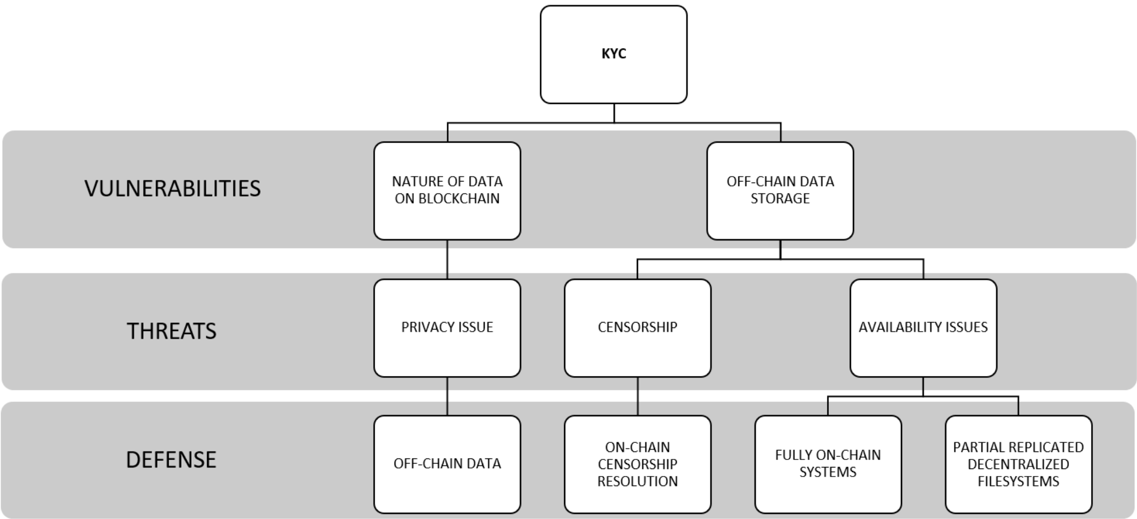


Figure 6.3: Vulnerabilities, threats, and defenses of KYC part 1 [54].

Since the KYC blockchain application contains sensitive data, it is necessary to consider what type of blockchain will be applied in terms of accessibility. When anyone can start validating blocks and sending transactions, the risk of an overriding transaction by malicious transaction containing a higher fee rises [54] - it is called a front-running attack. There are several ways to mitigate the front-running attack. See in Figure 6.4. For example: transaction counter, gas price, a commitment scheme, or injective protocol. Their principles are explained in Section 6.1.

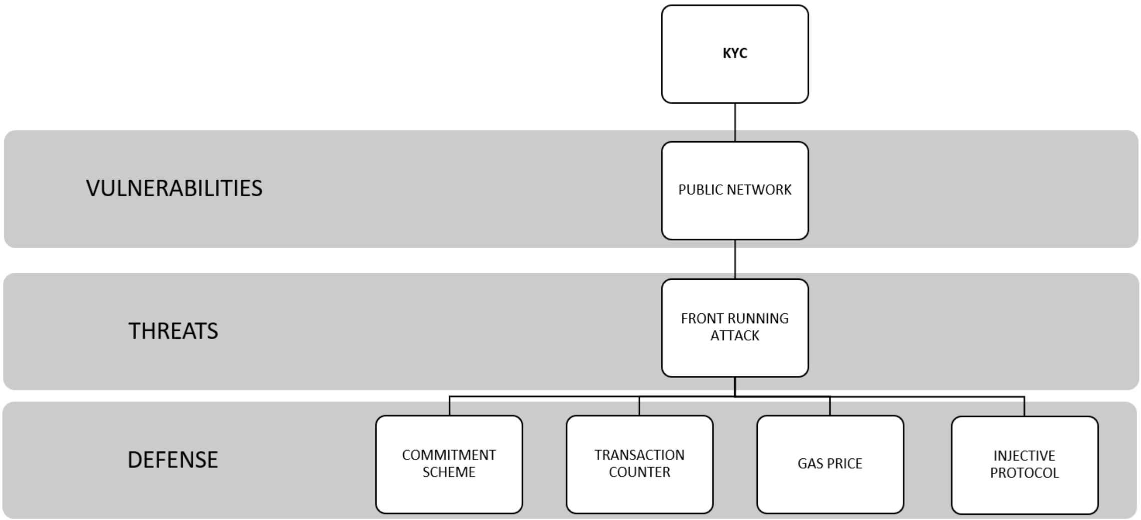


Figure 6.4: Vulnerabilities, threats, and defenses of KYC part 2 [54].

6.3 Prediction markets

The critical point of the prediction market is the reporting process when the outcome must be reported truthfully. Based on the outcome, it is decided who was guessing correctly and consequently would receive a financial reward. Therefore, the vulnerability lies in the interests of reporters during the reporting process of decisive events. See in Figure 6.5. Reporters themselves might be participants in the prediction market and might desire specific outcomes from which they would benefit [54].

Blockchain applications related to the prediction market should focus in detail on the reputation of reporters and monitor it, as this is an essential element of the prediction market. Any manipulation with outcomes, or illegal cooperation among reporters must be eliminated. A way to achieve it is positive motivation or reward for honest reporters. Reporters for their honestly delivered and correct reports should be rewarded. Another mechanism to supervise the honesty of reporters is the introduction of the KYC into the prediction market. In the case of manipulation with reports, the KYC can determine the identity of a dishonest reporter and make her accountable for her misbehavior [54].

In its design, the prediction market presumes a great number of members, which is essential for market creation and proper reporting. If the participants of the prediction market are few, it is easy to manipulate the market. A malicious user may create several accounts and trade with herself. Honest participants would join her prediction market maliciously created and would be manipulated [7]. A possible solution is to involve validators who would check the correct market settings. However, this is not a flawless solution because it is difficult to ensure credibility of validators [7]. The reputation of validators would have to be monitored. Validators should be prevented from participating in the prediction market, which would have to be financially compensated.

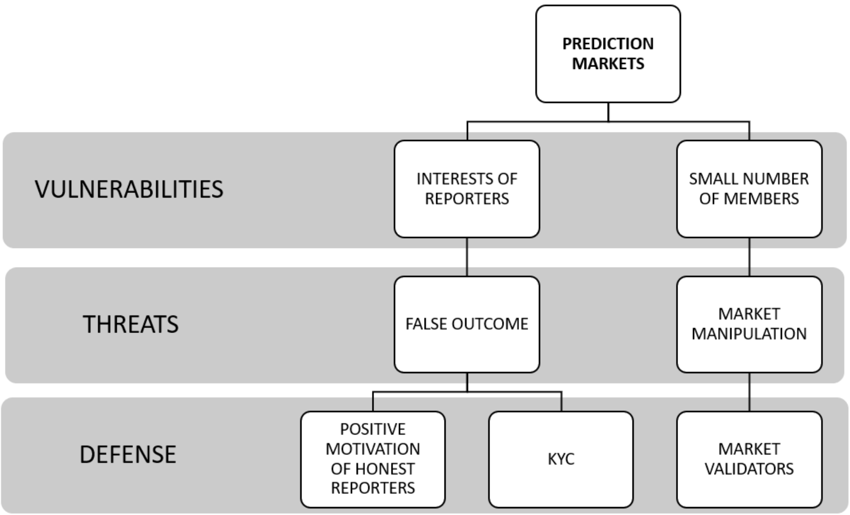


Figure 6.5: Vulnerabilities, threats, and defenses of Prediction markets.

6.4 Stablecoin

In the case of stablecoins, attacks are conducted primarily to disrupt their stability, which is a pivotal element of stablecoins. If stablecoin experiences a price fluctuation similar to other cryptocurrencies, its reputation will be severely damaged, and the market will stop trusting it. Therefore, it is necessary to minimize any speculative attacks on its value that lead to price fluctuations.

In the case of non-custodial stablecoins, an attack on the stability of a stablecoin value can occur when the attacker bets heavily on the stablecoin drop, triggering spiraling liquidations and affecting the market. See in Figure 6.6. For this type of attack, short squeeze-like trades are used. Moreover, the attack might be supported by bribing miners to freeze top-ups [61]. After the attack, new higher stablecoin prices are set, from which the attacker profits. Attackers do not only benefit from the price fluctuation of stablecoins, but also from the prices of other cryptocurrencies as they are negatively correlated with stablecoins. Usually, attackers open their positions in other cryptocurrencies in advance. This attack leads to a price fluctuation of stablecoin, which has a long-term negative impact on the demand for stablecoin and a loss of its credibility [61]. This type of attack is also called the Soros-Like Attack because it is similar to the attack that George Soros made on the British pound in 1992.

A way to prevent speculative attacks affecting the stability of stablecoin is a connection with another decentralized oracle, such as Chainlink, that would verify the price. The oracle would serve as price corrections avoiding price fluctuations. [61]. See in Figure 6.6.

As the issuance of new stablecoins is decided in the smart contracts based on many factors, such as the current state of the financial markets, there may be an overproduction of stablecoins, which causes inflation. It is, therefore, necessary to incorporate into smart contracts conditions monitoring the number of already-issued stablecoins.

The weak point of custodial stablecoins is the management of reserve assets. To establish credible custodial stablecoin, the number of reserve assets must correspond to the declared reserve ratio. A company providing custodial stablecoin must hold a declared amount of assets that back stablecoin. If the amount of reserve assets does not correspond to the set ratio, stablecoin is overestimated, and users are deceived. The way to prevent these manipulations could be through regular audits carried out by an independent and credible institution that oversees the state of the reserve funds. However, if this solution is not sufficient, non-custodial stablecoins should be applied. See in Figure 6.6.

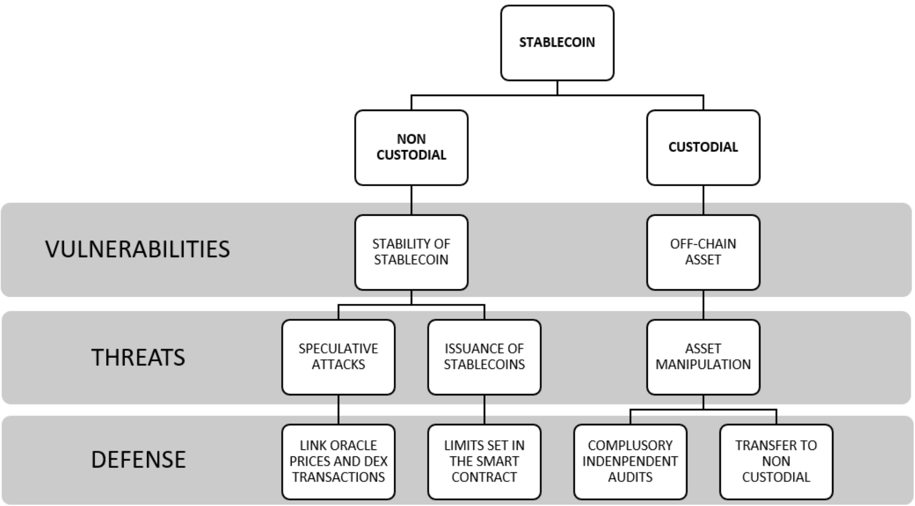


Figure 6.6: Vulnerabilities, threats, and defenses of Stablecoin.

6.5 Centralized exchange

In the case of a centralized exchange, the vulnerability lies in a single point of failure, because all data are stored on the server. See in Figure 6.7. The server can fail due to various reasons (technical problems or attacks). Due to the single-point failure, all stored data might be lost or stolen. Reliable providers cannot be exposed to such a risk of a data breach. Therefore, it is recommended to convert centralized exchange into Decentralized exchange (DEX) [54].

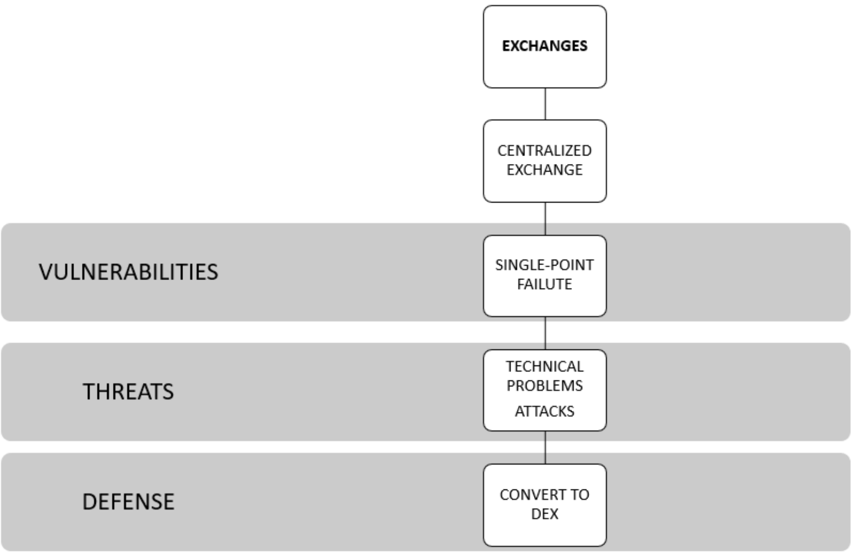


Figure 6.7: Vulnerabilities, threats, and defenses of Centralized exchange [54].

6.6 Decentralized exchange

In determining vulnerabilities in decentralized exchanges, I followed *“the Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses“* [54]. The main vulnerability in the case of decentralized exchanges joining several blockchains primarily lies in time clashes. See in Figure 6.8. Each blockchain may determine a different time to finality that could lead to overturning each other. Therefore, it is necessary to set clear rules preventing such situations. A solution for finding synchronization in finality could be an implementation of the set of confirmations that would validate finality [54]. Based on confirmations coming from all joined blockchain, the finality would be acknowledged.

However, the implementation of confirmations leads to a new problem regarding delays. As confirmation scheme requires more time for transaction execution, delays could occur. The solution for delays could be an off-chain exchange where an update is carried out only once, after determining finality. The other manner to prevent delays is punishing intentional delaying [54].

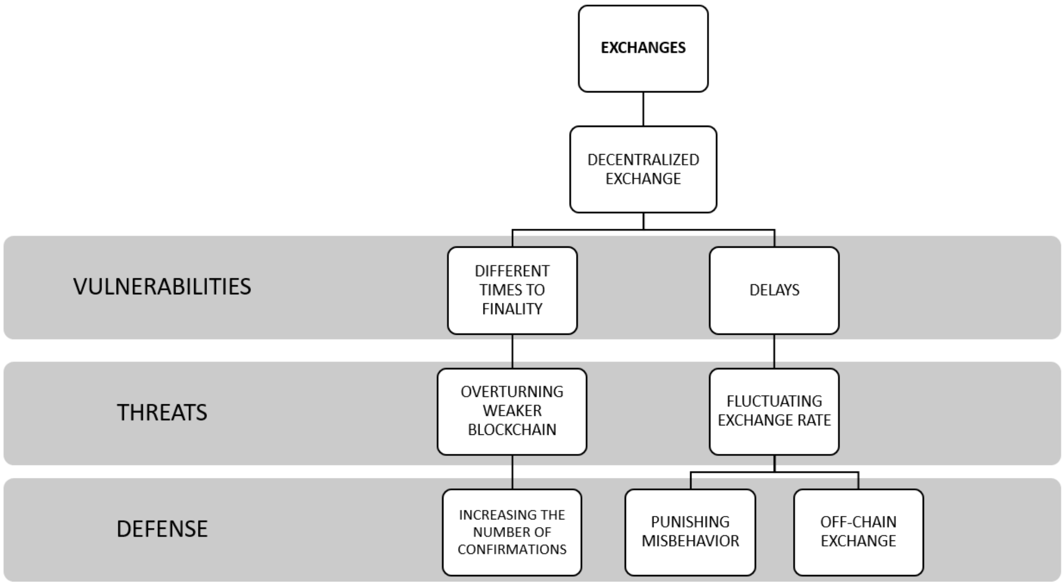

EXCHANGES
DECENTRALIZED EXCHANGE
VULNERABILITIES
DIFFERENT TIMES TO FINALITY
DELAYS
THREATS
OVERTURNING WEAKER BLOCKCHAIN
FLUCTUATING EXCHANGE RATE
DEFENSE
INCREASING THE NUMBER OF CONFIRMATIONS
PUNISHING MISBEHAVIOR
OFF-CHAIN EXCHANGE

Figure 6.8: Vulnerabilities, threats, and defenses of Decentralized exchange [54].

6.7 Automated market maker

The automated market maker is a specific case of decentralized exchange where transactions are executed in one blockchain (on-chain). Due to the on-chain characteristic of blockchain applications, there is a risk of a front-running attack. The risk of an overriding transaction by malicious transaction containing a higher fee rises. The attack is caused due to the possibility that anyone can start validating blocks and sending transactions [54]. There are several ways to mitigate the front-running attack. See in Figure 6.9. For example: transaction counter, gas price, a commitment scheme, or injective protocol. Their principles are explained in Section 6.1.

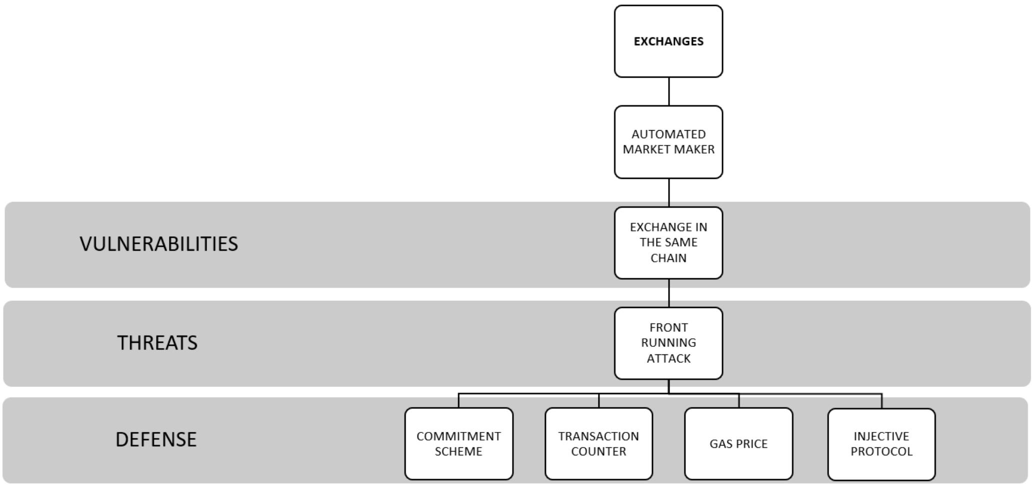


Figure 6.9: Vulnerabilities, threats, and defenses of Automated market maker part 1.

Concerning the absence of a counterparty, the AMM uses price oracles for price determination. Therefore, the main target of attacks is price manipulation and related market manipulation. For those purposes, oracle attacks are usually applied. However, there are two types of attacks under the term oracle attack, namely market manipulation and oracle manipulation [96]. See in Figure 6.10.

Market manipulation is a type of attack that intentionally distorts the market environment, disturbs the price by artificially influencing supply and demand [96]. An example is a launch of an arbitrage, which is involved in the rapid and mass process of borrowing, exchanging, and storing a large number of tokens. Based on these artificially induced processes, the price of assets is manipulated. [52].

One possible way to mitigate this attack is to introduce the Funding Fee mechanism which is used in Bitmex. The introduction of the Funding Fee could reduce the volume of financial operations [52]. A potential attack would thus become more expensive and the number of costs associated with the attack could discourage the attacker. The funding fee is explained in more detail in Section 6.1.

Another way to minimize market manipulation is to implement decentralized Oracle networks, such as Chainlink, that provide and verify price information [52].

The second type of oracle attack is an oracle manipulation [96]. See in Figure 6.10. The manipulation of an oracle differs according to a centralized or decentralized oracle. In the case of the centralized oracle, the risk lies in a single authority that provides price information. Centralized oracles can not ensure impartial and credible authority who provides reliable data. Therefore, the only solution is a conversion to a decentralized oracle. Unfortunately, the decentralized oracles also face difficulties with reliable data feed. Ways to mitigate the false data feed are by aggregating data feeds from multiple resources, or using a reputation system for their verification [96].

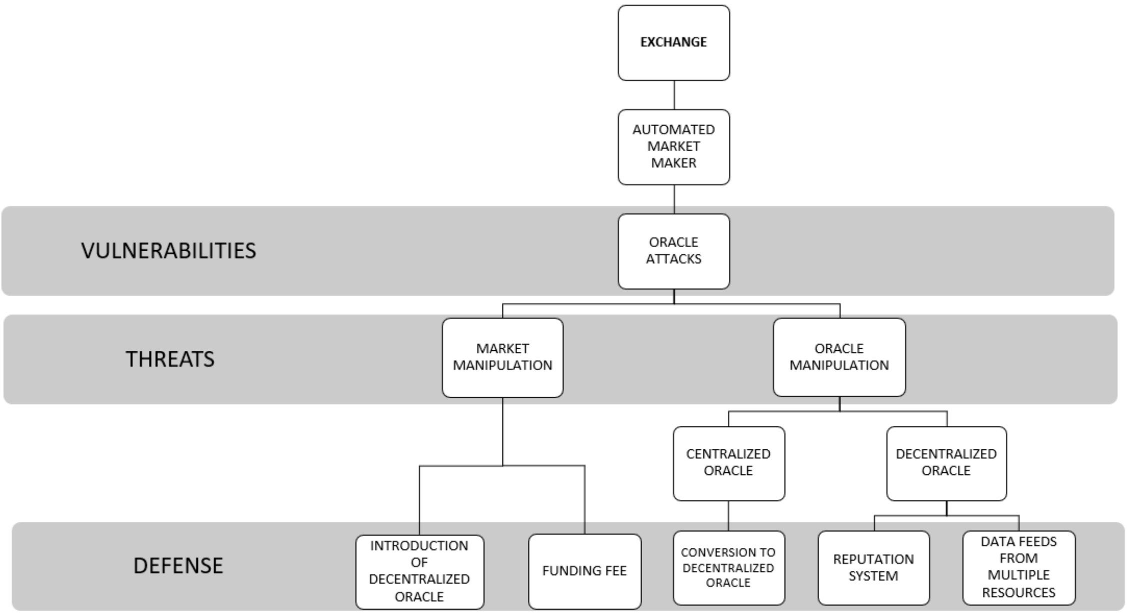


Figure 6.10: Vulnerabilities, threats, and defenses of Automated market maker part 2.

6.8 Credit and lending

Lending systems have been facing flash loan attacks recently. See in Figure 6.11. Flash loans are types of loans executed by smart contracts and do not require to provide any collateral. Therefore, these loans are considered to be unsecured. However, a flash loan must be repaid in the same transaction [13]. It is stipulated that the loans are repaid in full by the time the transaction has been completed. If the loan is not repaid, the smart contract will automatically roll back the transaction as if it never happened.

Within the period between providing the loan and repaying it, the user can do anything with the loan. Therefore, the crucial part of flash loans is the time between borrowing and repaying the loan. Within this period, it is possible to handle the loan diversely. Mainly, flash loans can be used for arbitrage (taking advantage of price discrepancies across different exchanges), collateral swaps, or lower transaction fees [13].

Two large flash loan attacks have been reported recently. Both are related to price manipulation. The first type of attack is based on the possibility of constantly repeated trades (borrow, swap, deposit) of a large number of tokens. In the interval between borrowing and returning, the attacker can use the amount for other trades. If these trades occur repeatedly in a short time and involve a huge number of tokens, it results in price manipulation, because individual trades affect the value of other assets and cryptocurrencies [13]. If these assets serve as a basis for determining the price of another asset, it spins a spiral that has devastating effects on the market. Flash loans are not a cause of the attack but provide funding to execute an attack that manipulates the price.

The second attack lies in the deceiving of a lender. The lender believes that the value of the provided loan has been repaid to her. The attack resides in temporary price manipulation of the stablecoin, which was used to repay the loan. With borrowed money from the flash loan, the attacker bought a huge portion of stablecoins. However, the purchase due to its volume doubled the price of stablecoins. The attacker then returned overvalued stablecoins within the flash loan [13]. After settling the correct price of stablecoin, the lender finds that she has not received the original value provided in the flash loan.

These attacks can be expected to increase in the future. Unfortunately, there is no clear solution to prevent these attacks. One way to mitigate flash loan attacks would be an introduction of market-based price oracles [80]. The correct price would be set according to a weighted average of prices extracted from the last X blocks either. This mechanism would help detect large price fluctuations that would indicate malicious price manipulation.

However, the introduction of an oracle to validate the correct asset price opens a door for oracle attacks which threaten both centralized and decentralized oracles. Oracle attacks were described in detail in Section 6.1.

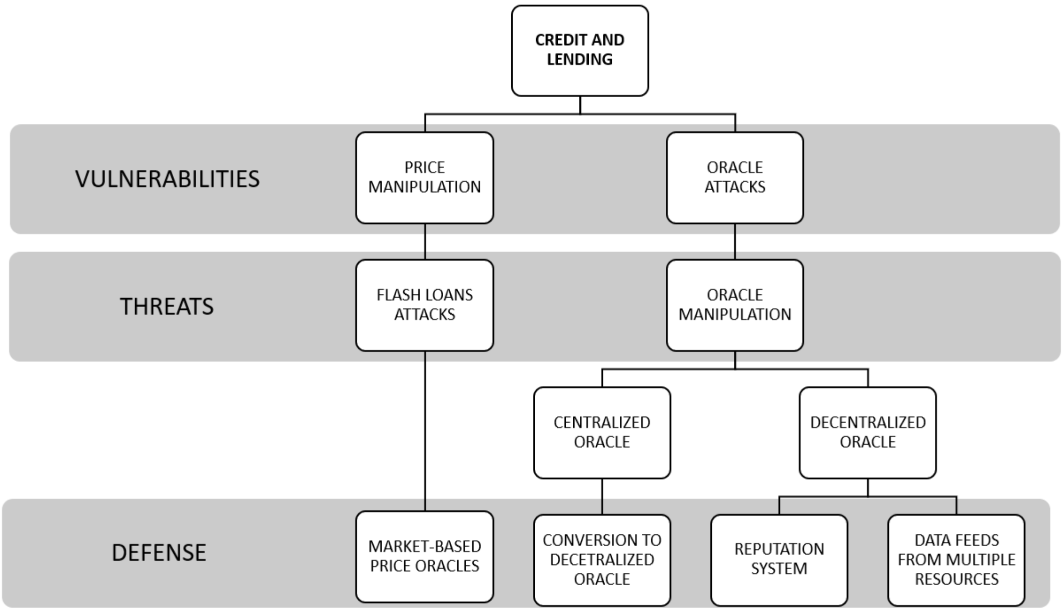


Figure 6.11: Vulnerabilities, threats, and defenses of Credit and lending.

6.9 Payments

In determining vulnerabilities in payments, I followed *"the Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses"* [54]. Attacks on wallets are divided according to their types. The first type of wallet is a self-sovereign wallet that stores the private key locally and directly interacts with the blockchain platform via keys. Serious security risk arises from the storage of the private key. See in Figure 6.12. If an attacker finds a location to store the private key, access to the wallet is open. Typical threats come from malware or keyloggers focusing on stealing keys. Potential protection against this type of attack could be the introduction of multi-factor authentication or conversion to a hardware wallet [54].

The second type of wallet is hosted wallets which are further distinguished into a client-side wallet and a server-side wallet. The division is made based on an entity that controls private keys. In the case of the server-side wallet, the private key is stored on the server and is managed by the hosted wallet. The owner, therefore, has no direct access to her private key. However, in the case of the client-side wallet, the private key is managed directly by the owner, herself. The owner exercises full control over her private key [54].

In the case of a server-side wallet, the vulnerability lies in a single point of failure, because the private key is stored on the server. See in Figure 6.12. The server can fail due to various reasons (technical problems or attacks), and consequently, the stored private key might be lost or stolen. The way to prevent this failure is to convert to a self-sovereign wallet where private keys are stored locally [54].

In the case of client-side wallets, there is a problem with the storage of keys and the online interface provided by a third party. Like in the case of self-sovereign wallets, potential threats are malware or keyloggers focusing on private keys theft. See in Figure 6.12. A suitable solution would be an implementation of hardware wallets [54]. Conversion to the hardware wallet is also recommended in the case of an online interface provided by a third party.

The interface might maliciously manipulate clients and consequently got the private key from them.

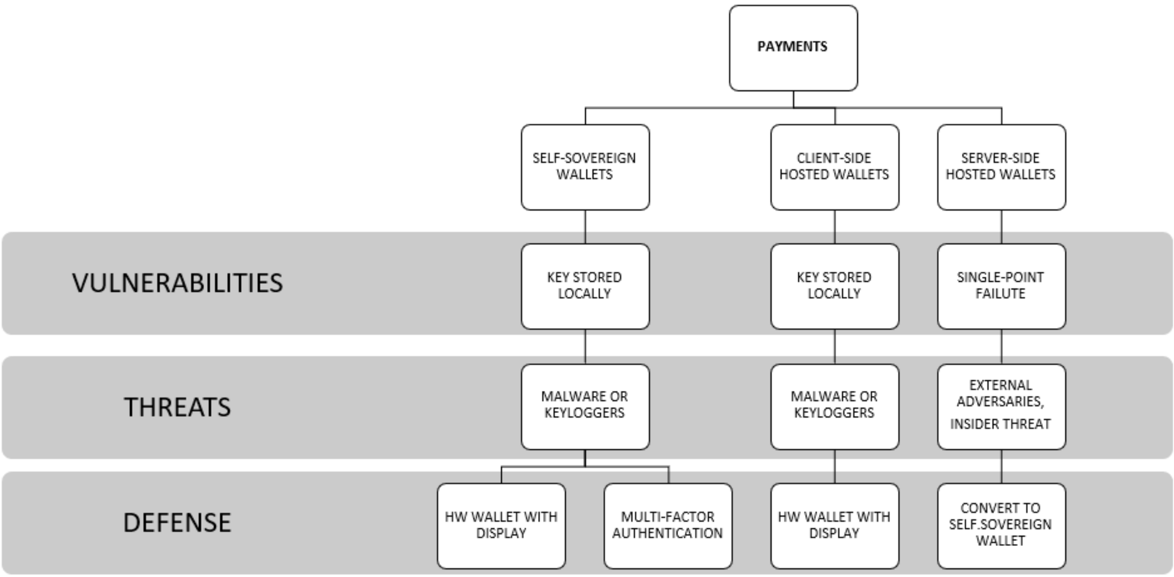


Figure 6.12: Vulnerabilities, threats, and defenses of Payments [54].

6.10 Insurance

Like KYC, a critical point of insurance is the nature of the data stored on the blockchain. See in Figure 6.13. The data stored on the blockchain and shared between nodes often concerns sensitive personal information about health status, property relations. A possible solution to the privacy issue could be off-chain data storage. However, off-chain data storage opens a door for new security threats such as censorship attacks and availability issues.

As the blockchain involves third entities, the risk of a censorship attack is considerably high. These entities decide to write their transactions to the blockchain and thus can prioritize certain transactions over others. The censorship attack could be mitigated via on-chain censorship resolution [54]. See in Figure 6.13.

The availability issue is coming from uncertainty whether all the data of the new block has been published on the network. All data must be available. Based on incomplete data, it is not possible to determine whether a new block contains a malicious transaction [5]. The availability issue could be mitigated by converting to fully on-chain systems or partially replicated decentralized file systems [54]. See in Figure 6.13.

Another vulnerable point of insurance is data feed. See in Figure 6.13. Data regarding a person's state of health or other personal matters are crucial for deciding on issuing insurance payments. Therefore, provided data must be complete and true. If the submission of reliable data is not ensured, there is a high risk of falsifying data, and it opens room for fraud regarding premiums. The way to prevent these attacks is to incorporate KYC that would identify and verify clients' identities. Based on KYC verification, a potential attacker would be accountable for such acts. Submitted data could also be verified by a credible entity. However, this solution is very similar to the current insurance setting, and it contradicts the idea of decentralized system.

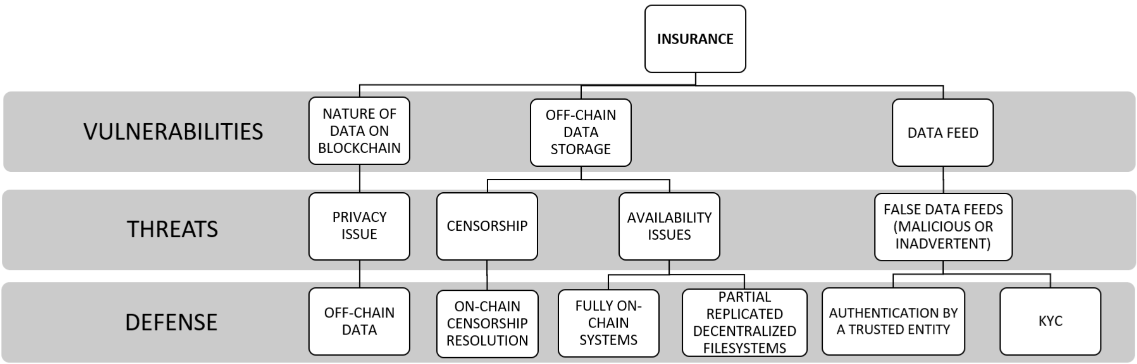

INSURANCE
VULNERABILITIES
NATURE OF DATA ON BLOCKCHAIN
OFF-CHAIN DATA STORAGE
DATA FEED
THREATS
PRIVACY ISSUE
CENSORSHIP
AVAILABILITY ISSUES
FALSE DATA FEEDS (MALICIOUS OR INADVERTENT)
DEFENSE
OFF-CHAIN DATA
ON-CHAIN CENSORSHIP RESOLUTION
FULLY ON-CHAIN SYSTEMS
PARTIAL REPLICATED DECENTRALIZED FILESYSTEMS
AUTHENTICATION BY A TRUSTED ENTITY
KYC

Figure 6.13: Vulnerabilities, threats, and defenses of Insurance.

Chapter 7

Security risks and current challenges of financial applications utilizing blockchain in general

In this chapter, we will present findings regarding the main areas of security risks arising out of DeFi applications and the most common attacks on the application layer. We will also present the current state and challenges of each DeFi application.

7.1 Main areas of security risks associated with DeFi

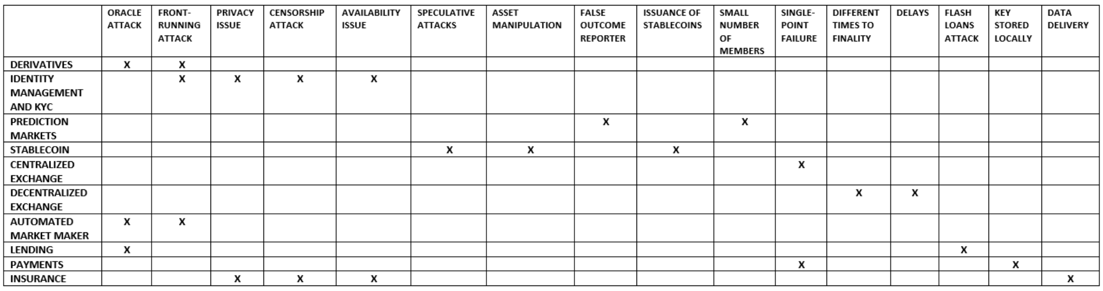
In general, security risks on DeFi applications can be divided into two main areas, **attacks of a financial nature** and **attacks arising out of the blockchain design**.

As DeFi applications are in the field of finance and banking, the main target of attacks is the manipulation of the price affecting the entire market, from which the attackers benefit. Oracle attacks, speculative attacks, or flash loan attacks are most often used to manipulate price and market. The launch of massive financial operations affecting the price of various assets is a typical feature of these attacks. As attackers are aware of the negative correlations between assets, they invest or open their derivative position in advance from which they later benefit. In general, a possible solution could be the implementation of a decentralized price oracle such as Chainlink, which will help with the correct pricing of assets. The price of the asset would be based on a weighted average of prices extracted from the last X blocks. It is also proposed to include fees similar to the funding fee in Bitmex making a potential attack more expensive.

The second group of security risks is arising out of the design of the blockchain. The crucial attacks are censorship attacks and front-running attacks. In front-running attacks, transactions are overridden by malicious transactions containing a higher fee, because transactions with higher fees are preferred. We propose various methods to mitigate these attacks, such as transaction counter, gas price, a commitment scheme, or injective protocol. The censorship attack is caused by the involvement of third centralized parties in the blockchain, which can decide on writing their transactions in the blockchain. It creates a risk of prioritizing certain transactions over others. The proposed solution is on-chain resolution.

7.2 The most common security risks associated with DeFi based on this survey

All attacks for each of the DeFi applications are displayed in Figure 7.1. Based on this table the most common security risks across DeFi applications include oracle attacks and front-running attacks. Other significant risks associated with DeFi applications are censorship attacks. As some DeFi applications deal with highly sensitive data of their clients, such as personal data, financial condition, or health status, privacy issues represent a serious risk. The last common attack based on Figure 7.1 is an availability issue which is associated with uncertainty as to whether all the data of the new block has been published on the network.
Overview of DeFi applications sorted by type of attacks:



	ORACLE ATTACK	FRONT-RUNNING ATTACK	PRIVACY ISSUE	CENSORSHIP ATTACK	AVAILABILITY ISSUE	SPECULATIVE ATTACKS	ASSET MANIPULATION	FALSE OUTCOME REPORTER	ISSUANCE OF STABLECOINS	SMALL NUMBER OF MEMBERS	SINGLE-POINT FAILURE	DIFFERENT TIMES TO FINALITY	DELAYS	FLASH LOANS ATTACK	KEY STORED LOCALLY	DATA DELIVERY
DERIVATIVES	X	X														
IDENTITY MANAGEMENT AND KYC		X	X	X	X											
PREDICTION MARKETS								X		X						
STABLECOIN						X	X		X							
CENTRALIZED EXCHANGE											X					
DECENTRALIZED EXCHANGE												X	X			
AUTOMATED MARKET MAKER	X	X														
LENDING	X													X		
PAYMENTS											X				X	
INSURANCE			X	X	X											X

Figure 7.1: Vulnerabilities and threats of DeFi applications.

7.3 Current state and challenges of financial applications utilizing blockchain

7.3.1 Derivatives

The most fundamental problem of blockchain applications in the area of financial derivatives is the oracle attack manipulating the price of assets. This manipulation results in manipulation of the entire market, in which significant financial losses occur. Synthetix has also experienced these attacks and last year recorded losses amounting to 37 million dollars. Therefore, Synthetix is investing heavily in its security and has decided on the incorporation of Chainlink, a decentralized oracle, to mitigate these attacks. Integration has been made recently, thus it is not possible to assess its impacts.

7.3.2 Identity management and KYC

The biggest obstacle in KYC blockchain is the reluctance to unify conditions so a single KYC with a unique database can be established across various entities. There is no global standard, and companies or institutions have no interest in creating one. Therefore, all mentioned projects are only local and can not reach global impact. Nevertheless, the first attempts to create a uniform KYC are slowly emerging and are initiated by companies providing blockchain applications. There is an integration of Blockpass, KYC and AML screening software, and Chainlink, a decentralized oracle, leading to the creation of on-chain KYC. It is anticipated that the integration will bring an automated on-chain KYC suitable for blockchain applications. In particular, KYC will be used in identity verification and cryptographical signature to meet AML regulation [95].

7.3.3 Prediction markets

Currently, well-known blockchain applications providing the prediction market are Augur, Stox, and Gnosis. All applications are based on Ethereum and are barrier-free. It means that a user may establish and participate in any predicted event. Augur mainly uses a decentralized oracle, but the user may add a centralized one. In the case of Gnosis and Stox, the user can choose between a centralized or decentralized oracle for each event. Only Augur and Stox offer an opportunity to initiate dispute proceedings in case of disagreement with the oracle decision. Each of the applications has its tokens, but only Stox requires these tokens for betting [47]. Based on the above-mentioned features, Agur is considered to be the most appropriate application (fully decentralized and resolution system [44].

7.3.4 Stablecoin

Tether (USDT), custodial stablecoin, is considered to be a digital dollar equivalent and is the most popular stablecoins. Tether fluctuates slightly around $1 per one USDT [46]. However, there is a lack of evidence regarding reserve assets. Tether does not provide reliable information that its stablecoin is backed by a declared amount of dollars. Therefore, there are many doubts about its credibility. Some court proceedings on possible fraud have been initiated [58]. Tether has been facing also several severe attacks manipulating its price.

Nowadays, stablecoin is very popular in Venezuela. Given the local regime, it is one of the few ways to invest effectively and preserve the value of assets. In Venezuela, it is easy to carry out an exchange between bitcoin and stablecoin. Moreover, stablecoin does not contradict the anti-dollar policy. Therefore, it has become a useful investment tool [17].

7.3.5 Cryptocurrency Exchanges

Nowadays, there are plenty of cryptocurrency exchanges on the market. Therefore, it is not easy to determine and recommend the most secure exchange platforms. In the area of centralized exchanges, Binance and Coinbase are considered to be widely used and stable exchanges. Coinbase is praised for its intuitive look and offering multiple ways to purchase cryptocurrency. From a security point of view, Coinbase provides 2FA verification and biometric fingerprint logins. It also offers and insurance for hot storage if Coinbase is breached [43]. On the other hand, Binance is popular for its low fees and a huge selection of transaction types. From a security point of view, Binance also provides 2FA verification. Binance offers FDIC-insured USD balances [43]. In general, reliable applications should provide two-factor authentication. Clients should also monitor the history of attacks and a track record for safeguarding users' data. All these factors should be met [73].

Automated market makers face several attacks manipulating the asset price. Based on these attacks, some AMMs have started to integrate decentralized price oracles to provide and verify correct price information.

7.3.6 Credit and lending

As it was mentioned in Section 6.8, the lending industry is facing massive flash loan attacks, which have devastating financial consequences. As this type of attack highlights system deficiencies related to decentralized finance, the reputation of blockchain applications in the lending industry is damaged, and its popularity is declining. However, OpenZeppelin, a cryptocurrency software, and security firm, has created Defender - a software suite for decentralized finance (DeFi) projects attempting to fight against flash loan attacks and other exploits. Defender contains alerts to warn of market manipulation, and automated scripts to respond to these attacks [51]. As the Defender has been recently launched, it is not possible to assess its impact on flash loan attacks.

7.3.7 Payments

Nowadays, there are different types of wallets on the market. However, there is no exact recommendation which wallet is the safest. It depends on the user, the cost, the purpose of the wallet, and the degree of risk that the user is willing to bear. Nevertheless, Electrum is considered to be the safest wallet from hot wallets based on two-factor authentication. In Electrum wallet private keys are stored with a password. Electrum also has a special measure to protect users in case of loss or theft of the device that Electrum is installed on [84]. Trezor is considered to be the safest wallet from hardware wallets. Trezor gained this reputation due to its multi-factor authentication [83].

7.3.8 Insurance

Although many projects are promising revolutionary changes in the insurance industry, and expecting a rapid increase, we have not noticed global implementation so far. These proclamations are made only on paper, and big corporations are reluctant to make the first step. The biggest deficiency is the absence of a reliable data feed that would be connected to the blockchain.

Chapter 8

Conclusion

As part of this bachelor's thesis, we have created eight categories of financial applications built on blockchain, which we subjected to analysis. These financial applications are Derivatives, Stablecoins, Identity management, and KYC, Prediction markets, Cryptocurrency Exchanges, Credit and Lending, Payments, and Insurance. After a thorough study of the design of individual financial applications and careful examination of already occurred attacks, for each category of financial applications, we identify crucial vulnerabilities that cause different threats. For each of these vulnerabilities, we have proposed a solution that could mitigate or eliminate these attacks. As we are in the field of finance, among the most common vulnerabilities are oracle attacks, which include price manipulation, and market manipulation. Attackers intentionally cause heavy price fluctuations, from which they subsequently benefit. Attackers in DeFi applications are highly sophisticated. They understand the technology of blockchain, as well as the financial implications they cause. Another common issue is the vulnerability of centralized entities that are involved in a blockchain. As DeFi applications increasingly attract new investors, it can be assumed that similar attacks will rise in the future.

Bibliography

[1] Adachi, M., Cominetta, M., Kaufmann, C. and Kraaij, A. van der. *A regulatory and financial stability perspective on global stablecoins* [online]. Ecb.europa.eu [cit. 2020-10-17]. Available at: `https://www.ecb.europa.eu//pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202005_1~3e9ac10eb1.en.html#toc2`.

[2] Adamik, F. and Kosta, S. SmartExchange: Decentralised Trustless Cryptocurrency Exchange. In: Abramowicz, W. and Paschke, A., ed. *Business Information Systems Workshops*. Jan 2019, p. 356–367. DOI: 10.1007/978-3-030-04849-5-32. ISBN 978-3-030-04848-8.

[3] Adams, H., Keefer, R., Zinsmeister, N., Robinson, D. and Salem, M. *Uniswap v3 Core* [online]. uniswap.org, Mar 2021 [cit. 2021-04-15]. Available at: `https://uniswap.org/whitepaper-v3.pdf`.

[4] admin. *TokenSet Protocol – Automated Crypto Asset Management* [online]. defipicks.com, December 2019 [cit. 2020-10-20]. Available at: `http://defipicks.com/2019/12/03/tokenset-protocol-what-are-token-sets/`.

[5] Al Bassam, M. *What Is Data Availability?: CoinMarketCap* [online]. coinmarketcap.com, Nov 2020 [cit. 2020-11-20]. Available at: `https://coinmarketcap.com/alexandria/article/what-is-data-availability`.

[6] Back, A. *Hashcash - A Denial of Service Counter-Measure* [online]. August 2002 [cit. 2020-09-28]. Available at: `http://www.hashcash.org/papers/hashcash.pdf`.

[7] Baker, P. *Binance Research: Design Flaws Make Augur Vulnerable To Attack* [online]. cryptobriefing.com, Apr 2019 [cit. 2020-10-08]. Available at: `https://cryptobriefing.com/binance-augur-flaw/`.

[8] Bashir, I. *Mastering Blockchain*. 1st ed. Packt Publishing, Mar 2017. ISBN 9781787125445.

[9] Bentov, I., Gabizon, A. and Mizrahi, A. *Cryptocurrencies without Proof of Work* [online]. 2014 [cit. 2020-10-04]. Available at: `http://arxiv.org/abs/1406.5694`.

[10] Berenzon, D. *Synthetic Assets in DeFi: Use Cases & Opportunities* [online]. Defiprime, Sep 2019 [cit. 2020-10-17]. Available at: `https://defiprime.com/synthetic-assets-defi`.

[11] Bessani, A., Sousa, J. and Alchieri, E. *State machine replication for the masses with BFT-SMART* [online]. Jun 2014 [cit. 2020-10-04]. DOI: 10.1109/DSN.2014.43. Available at: `https://www.di.fc.ul.pt/~bessani/publications/dsn14-bftsmart.pdf`.

[12] Binance. *Buy & sell Crypto in minutes* [online]. Binance.com [cit. 2021-03-15]. Available at: https://www.binance.com/en.

[13] Binance Academy. *What Are Flash Loans in DeFi?* [online]. Binance Academy, Oct 2020 [cit. 2020-12-14]. Available at: https://academy.binance.com/en/articles/what-are-flash-loans-in-defi.

[14] Binance Academy. *What Is a Decentralized Exchange (DEX)?* [online]. Binance Academy, Feb 2021 [cit. 2021-03-03]. Available at: https://academy.binance.com/en/articles/what-is-a-decentralized-exchange-dex.

[15] Binance Academy. *What Is an Automated Market Maker (AMM)?* [online]. Binance Academy, April 2021 [cit. 2021-04-28]. Available at: https://academy.binance.com/en/articles/what-is-an-automated-market-maker-amm.

[16] Bitmex. *Bitmex The Next Generation of Bitcoin Trading Products* [online]. Bitmex.com [cit. 2021-01-14]. Available at: https://www.bitmex.com/.

[17] Bitspark Hong Kong. *The case for stablecoins in Venezuela* [online]. disruptionbanking.com, Jul 2019 [cit. 2020-10-15]. Available at: https://disruptionbanking.com/2019/07/24/the-case-for-stablecoins-in-venezuela/.

[18] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: IEEE. *2015 IEEE Symposium on Security and Privacy*. 2015, vol. 2015, p. 104–121. DOI: 10.1109/SP.2015.14. ISBN 978-1-4673-6949-7.

[19] Brooks, S., Jurisevic, A., Spain, M. and Warwick, K. *Synthetix white paper* [online]. synthetix.io, Jun 2018 [cit. 2020-10-15]. Available at: https://www.synthetix.io/uploads/synthetix_whitepaper.pdf.

[20] Buchman, E., Kwon, J. and Milosevic, Z. *The latest gossip on BFT consensus* [online]. Jul 2018 [cit. 2020-10-07]. Available at: http://arxiv.org/abs/1807.04938.

[21] Buterin, V. *Ethereum Whitepaper* [online]. ethereum.org, Feb 2021 [cit. 2021-03-03]. Available at: https://ethereum.org/en/whitepaper/.

[22] Butler, E. *Austrian Economics: A Primer* [online]. Ludwig von Mises Institute, Jan 2009 [cit. 2020-10-29]. Available at: http://www.hayek.sk/wp-content/uploads/2012/12/austrian-primer-text.pdf.

[23] Bybit. *Bybit Cryptocurrency Exchange Platform* [online]. Bybit.com [cit. 2021-01-14]. Available at: https://www.bybit.com/en-US/.

[24] Cachin, C. and Poritz, J. Secure INtrusion-Tolerant Replication on the Internet. In: IEEE, ed. *Proceedings International Conference on Dependable Systems and Networks*. 2002, p. 167–176. DOI: 10.1109/DSN.2002.1028897. ISBN 0-7695-1101-5.

[25] Cachin, C. *Yet Another Visit to Paxos* [online]. IBM Research - Zurich, Jul 2010 [cit. 2020-10-07]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.295.5410&rep=rep1&type=pdf.

[26] Cambridge Blockchain. *Cambridge Blockchain* [online]. Cambridge-blockchain.com [cit. 2021-01-14]. Available at: https://www.cambridge-blockchain.com/.

[27] Casino, F., Dasaklis, T. K. and Patsakis, C. *A systematic literature review of blockchain-based applications: Current status, classification and open issues* [online]. 2019 [cit. 2020-10-21]. DOI: https://doi.org/10.1016/j.tele.2018.11.006. ISSN 0736-5853. Available at: https://www.sciencedirect.com/science/article/pii/S0736585318306324.

[28] Celsius. *Celsius Whitepaper* [online]. Celsius network, April 2018 [cit. 2020-12-18]. Available at: https://celsius.network/wp-content/uploads/2018/04/celsius_whitepaper-march21.pdf.

[29] Chain, K. *Individual and Corporate KYC* [online]. Kyc-chain.com [cit. 2021-03-15]. Available at: https://kyc-chain.com/.

[30] Chaum, D., Fiat, A. and Naor, M. Untraceable Electronic Cash. In: Advances in Cryptology — CRYPTO' 88. *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings.* Springer, 1988, vol. 403, p. 319–327. Lecture Notes in Computer Science. DOI: 10.1007/0-387-34799-2-25. ISBN 978-0-387-34799-8.

[31] Chen, Y.-C., Chou, Y.-P. and Chou, Y.-C. *An Image Authentication Scheme Using Merkle Tree Mechanisms* [online]. Jul 2019 [cit. 2020-10-04]. DOI: 10.3390/fi11070149. ISSN 1999-5903. Available at: https://www.mdpi.com/1999-5903/11/7/149.

[32] Civic. *Identity Verification by Civic* [online]. Civic.com [cit. 2021-04-08]. Available at: https://www.civic.com/identity-verification/.

[33] Coverdale, C. *Solidity: Transaction-ordering attacks* [online]. Medium, Mar 2018 [cit. 2020-11-10]. Available at: https://medium.com/coinmonks/solidity-transaction-ordering-attacks-1193a014884e.

[34] CreditTag Crypto. *BitMEX Fees Explained - How Much Are You Paying?* [online]. credittag.io, Apr 2020 [cit. 2020-11-06]. Available at: https://www.credittag.io/bitmex-fees-explained/.

[35] CryptoCompare. *What are Bitcoin Perpetual Swaps and How to Trade Them* [online]. cryptocompare.com, Apr 2020 [cit. 2020-10-17]. Available at: https://www.cryptocompare.com/exchanges/guides/what-are-bitcoin-perpetual-swaps-and-how-to-trade-them/.

[36] Daley, S. *Buy your dream home with a blockchain mortgage: 11 companies using DLT for lending and credit* [online]. builtin.com, Oct 2019 [cit. 2020-11-20]. Available at: https://builtin.com/blockchain/lending-loans-borrowing-mortgages.

[37] Daley, S. *Nine companies using blockchain to revolutionize insurance* [online]. builtin.com, march 2019 [cit. 2020-11-06]. Available at: https://builtin.com/blockchain/blockchain-insurance-companies.

[38] Defi Rate. *Crypto Funding Rates 2021* [online]. Https://defirate.com/ [cit. 2021-02-05]. Available at: https://defirate.com/funding/.

[39] DericEcourcy. *Protecting Against Front-Running and Transaction Reordering* [online]. forum.openzeppelin.com, Sep 2019 [cit. 2021-03-05]. Available at: `https://forum.openzeppelin.com/t/protecting-against-front-running-and-transaction-reordering/1314`.

[40] Diffie, W. and Hellman, M. New directions in Cryptography. *IEEE transactions on Information Theory*. 1st ed. IEEE Transactions on Information Theory. 1976, vol. 22, no. 6, p. 644–654.

[41] Duan, S., Meling, H., Peisert, S. and Zhang, H. BChain: A Practical Byzantine Agreement Protocol with Fault Diagnosis. In: Aguilera, M., Querzoni, L. and Shapiro, M., ed. *Lecture Notes in Computer Science*. December 2014. DOI: 10.1007/978-3-319-14472-6-7. ISBN 978-3-319-14471-9.

[42] dYdX. *DYdX* [online]. Dydx.exchange [cit. 2020-10-16]. Available at: `https://dydx.exchange/`.

[43] Elliott, J. *Binance vs. Coinbase: Which Should You Choose?* [online]. investopedia.com, May 2021 [cit. 2021-05-03]. Available at: `https://www.investopedia.com/binance-vs-coinbase-5120852`.

[44] Esan, J. and Alexandre, A. *5 Crypto Prediction Markets to Pay Attention to in 2021* [online]. BeInCrypto, Feb 2021 [cit. 2021-03-02]. Available at: `https://beincrypto.com/crypto-prediction-markets-to-pay-attention-to-in-2021/`.

[45] Finematics. *How Do Liquidity Pools Work? DeFi Explained* [online]. finematics.medium.com, Jul 2020 [cit. 2020-11-02]. Available at: `https://finematics.medium.com/how-do-liquidity-pools-work-defi-explained-6d3418ea71fa`.

[46] Fire Labs Team. *Everything You Need to Know About Stablecoins* [online]. 4irelabs.com, August 2020 [cit. 2020-10-27]. Available at: `https://4irelabs.com/articles/stablecoins/`.

[47] Fröberg, E., Ingre, G. and Knudsen, S. *Blockchain and prediction markets: An analysis of three organizations implementing prediction markets using blockchain technology, and the future of blockchain prediction market* [online]. kth.diva-portal.org, 2018 [cit. 2020-11-03]. Available at: `http://kth.diva-portal.org/smash/get/diva2:1306764/FULLTEXT01.pdf`.

[48] GetID. *The 2021 Guide to AML and KYC for Crypto Exchanges & Wallets* [online]. getid.ee, April 2021 [cit. 2021-04-21]. Available at: `https://getid.ee/aml-kyc-crypto-exchanges-wallets/`.

[49] Gnosis. *Gnosis* [online]. Gnosis.io [cit. 2021-04-08]. Available at: `https://gnosis.io/`.

[50] Haber, S. and Stornetta, W. S. *How to Time-Stamp a Digital Document*. 1991. DOI: 10.1007/BF00196791.

[51] Harper, C. *Defender Gives DeFi Teams a Weapon Against Flash Loan Attacks* [online]. CoinDesk, Mar 2021 [cit. 2021-03-25]. Available at: `https://www.coindesk.com/openzeppelin-defender-solution-defi-flash-loan-attacks`.

[52] Hashed. *Synthetix: the Most Progressive Experiment on the Synthetic Token and the Protocol Economy* [online]. Hashed Team Blog, Jul 2020 [cit. 2020-12-14]. Available at: https://medium.com/hashed-official/synthetix-the-most-progressive-experiment-on-the-synthetic-token-and-the-protocol-economy-f60f943786cd.

[53] Homoliak, I., Breitenbacher, D., Hujňák, O., Hartel, P., Binder, A. et al. *SmartOTPs: An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets.* Oct 2020. DOI: 10.1145/3419614.3423257.

[54] Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R. et al. The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Communications Surveys & Tutorials* [online]. Institute of Electrical and Electronics Engineers (IEEE). 2021, vol. 23, no. 1, p. 341–390, [cit. 2021-03-05]. DOI: 10.1109/comst.2020.3033665. ISSN 2373-745X. Available at: http://dx.doi.org/10.1109/COMST.2020.3033665.

[55] Huobi Global. *Huobi Global* [online]. Huobi.com [cit. 2021-01-14]. Available at: https://www.huobi.com/en-us/.

[56] Hyperledger. *Hyperledger* [online]. Hyperledger.org [cit. 2021-03-15]. Available at: https://www.hyperledger.org/.

[57] Kaminska, I. *Blockchain officially confirmed as slower and more expensive* [online]. Financial Times, May 2019 [cit. 2020-10-13]. Available at: https://www.ft.com/content/fe5b17e1-4040-3249-b473-f3c998c67de9.

[58] Keely, A. *Lawyer for Bitfinex, Tether says firms are almost finished producing documents sought by NYAG.* [online]. theblockcrypto.com, Jan 2021 [cit. 2021-02-11]. Available at: https://www.theblockcrypto.com/linked/91855/bitfinex-tether-nyag-documents-court.

[59] Kiayias, A., Russell, A., David, B. and Oliynykov, R. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In: Katz, J. and Shacham, H., ed. *Advances in Cryptology – CRYPTO 2017.* Jul 2017, p. 357–388. DOI: 10.1007/978-3-319-63688-7-12. ISBN 978-3-319-63687-0.

[60] Klages Mundt, A., Harz, D., Gudgeon, L., Liu, J.-Y. and Minca, A. *Stablecoins 2.0* [online]. ACM, Oct 2020 [cit. 2020-11-27]. DOI: 10.1145/3419614.3423261. Available at: http://dx.doi.org/10.1145/3419614.3423261.

[61] Klages Mundt, A. and Minca, A. *(In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks.* Cryptography and Security, june 2019.

[62] Kuperberg, M. *Enabling Deletion in Append-Only Blockchains (Short Summary / Work in Progress)* [online]. May 2020 [cit. 2020-09-28]. Available at: https://arxiv.org/pdf/2005.06026.pdf.

[63] Lendroid. *Lendroid* [online]. Lendroid.com [cit. 2021-03-15]. Available at: https://lendroid.com/.

[64] Levi, Y. and Cohen, M. J. *Overview of the Bancor Network Architecture and its core entities* [online]. Bancor.network [cit. 2021-02-10]. Available at: https://docs.bancor.network/network-architecture/overview.

[65] Lielacher, A. *Private Keys: The Keys to Your Crypto: CoinMarketCap* [online]. coinmarketcap.com, november 2020 [cit. 2020-12-10]. Available at: `https://coinmarketcap.com/alexandria/article/private-keys-the-keys-to-your-crypto`.

[66] Lorenz, J.-T., Münstermann, B., Higginson, M., Olesen, P. B., Bohlken, N. et al. *Blockchain in insurance – opportunity or threat?* [online]. McKinsey&Company, Jul 2016 [cit. 2020-09-28]. Available at: `https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat`.

[67] Makerdao. *A better, smarter currency* [online]. Makerdao.com [cit. 2021-03-15]. Available at: `https://makerdao.com/en/`.

[68] Menger, C., Dingwall, J. and Hoselitz, B. *Principles of Economics*. 1st ed. Terra Libertas, 2011. Classic reprint series. ISBN 9781908089083.

[69] Miller, A., Xia, Y., Croman, K., Shi, E. and Song, D. *The Honey Badger of BFT Protocols*. Oct 2016. DOI: 10.1145/2976749.2978399.

[70] Mire, S. *Blockchain In Lending: 6 Possible Use Cases* [online]. Disruptor Daily, Mar 2019 [cit. 2020-10-17]. Available at: `https://www.disruptordaily.com/blockchain-use-cases-lending/`.

[71] Musienko, Y. *Blockchain for Know Your Customer (KYC): Use Cases - Merehead 5366* [online]. Merehead, Nov 2019 [cit. 2020-11-06]. Available at: `https://merehead.com/blog/blockchain-for-know-your-customer-kyc-use-cases/`.

[72] Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system* [online]. bitcoin.org, Mar 2009 [cit. 2020-10-08]. Available at: `http://www.bitcoin.org/bitcoin.pdf`.

[73] Observer Content Studio. *Best Crypto Exchanges: Top 5 Cryptocurrency Trading Platforms of 2021* [online]. Observer, Mar 2021 [cit. 2021-03-25]. Available at: `https://observer.com/2021/03/best-crypto-exchanges/`.

[74] Okex. *Okex The cryptocurrency exchange with the most option* [online]. Okex.com [cit. 2021-01-14]. Available at: `https://www.okex.com/`.

[75] Ostern, N. and Riedel, J. *Know-Your-Customer (KYC) Requirements for Initial Coin Offerings* [online]. December 2020 [cit. 2020-12-28]. DOI: 10.1007/s12599-020-00677-6. Available at: `https://link.springer.com/article/10.1007/s12599-020-00677-6`.

[76] Paszke, A. *Layer 2* [online]. Binance Academy, Jan 2020 [cit. 2020-11-02]. Available at: `https://academy.binance.com/en/glossary/layer-2`.

[77] Pernice, I., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H. et al. *Monetary Stabilization in Cryptocurrencies – Design Approaches and Open Questions* [online]. Jun 2019 [cit. 2020-11-04]. DOI: 10.1109/CVCBT.2019.00011. Available at: `https://arxiv.org/pdf/1905.11905.pdf`.

[78] Peters, K. *LedgerX* [online]. Investopedia, Apr 2021 [cit. 2021-02-10]. Available at: `https://www.investopedia.com/terms/l/ledgerx.asp`.

[79] Peterson, J. and Krug, J. *Augur: a decentralized, open-source platform for prediction markets* [online]. 2015 [cit. 2020-10-20]. Available at: http://arxiv.org/abs/1501.01042.

[80] Qureshi, H. *Flash Loans: Why Flash Attacks will be the New Normal* [online]. Medium, Feb 2021 [cit. 2021-03-06]. Available at: https://medium.com/dragonfly-research/flash-loans-why-flash-attacks-will-be-the-new-normal-5144e23ac75a.

[81] Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R. et al. *Decentralized Identifiers (DIDs) v1.0* [online]. w3.org, April 2021 [cit. 2020-04-30]. Available at: https://www.w3.org/TR/did-core/.

[82] Reimi, M. *Understanding Uniswap: a beginner's guide and review* [online]. holdex.io, Sep 2020 [cit. 2020-10-08]. Available at: https://holdex.io/x/uniswap/understanding-uniswap-a-beginners-guide-and-review.

[83] Rosenberg, E. *Best Bitcoin Wallets of 2021* [online]. thebalance.com, Feb 2021 [cit. 2021-03-11]. Available at: https://www.thebalance.com/best-bitcoin-wallets-4160642.

[84] S., A. *Complete Electrum Wallet Review: How to use Electrum?* [online]. bitdegree.org, Jan 2021 [cit. 2021-03-11]. Available at: https://www.bitdegree.org/crypto/electrum-wallet-review.

[85] SALT. *Loans Backed By Crypto* [online]. Saltlending.com [cit. 2021-04-08]. Available at: https://saltlending.com/.

[86] Selfkey. *Selfkey* [online]. Selfkey.org [cit. 2021-04-08]. Available at: https://selfkey.org/.

[87] Stox. *The blockchain prediction markets platform* [online]. Stox.com [cit. 2021-04-08]. Available at: https://www.stox.com/.

[88] Sushi. *Be a DeFi Chef with Sushi* [online]. Https://sushi.com/ [cit. 2020-10-16]. Available at: https://sushi.com/.

[89] Szabo, N. *The idea of smart contracts.* 1997.

[90] Tether. *Tether: Fiat currencies on the Bitcoin blockchain* [online]. Tether.to [cit. 2021-03-15]. Available at: https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

[91] Token Terminal. *ELI5: What is Balancer?* [online]. Medium, Apr 2020 [cit. 2020-11-06]. Available at: https://medium.com/token-terminal/eli5-what-is-balancer-labs-16c8cfe092d9.

[92] Trading Apps. *BitMEX Fees Explained: Complete Crypto Margin Trading Fee Guide* [online]. Tradingapps.org [cit. 2021-02-07]. Available at: https://tradingapps.org/bitmex-fees-explained/.

[93] TrustToken. *The TrueCurrency Liquidity Fund is Now Open* [online]. trusttoken.com, September 2020 [cit. 2020-10-17]. Available at: https://blog.trusttoken.com/the-truecurrency-liquidity-fund-is-now-open-3cd0e8dd890c.

[94] Wang, H., Zheng, Z., Xie, S., Dai, H.-N. and Chen, X. Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services.* 1st ed. october 2018, vol. 14, no. 4, p. 352 – 375. DOI: 10.1504/IJWGS.2018.10016848.

[95] Warner, M. *The Importance of On-Chain KYC* [online]. blockpass.org, Jan 2021 [cit. 2021-03-03]. Available at: `https://www.blockpass.org/2021/01/23/the-importance-of-on-chain-kyc/`.

[96] Werner, S., Perez, D., Gudgeon, L., Klages Mundt, A., Harz, D. et al. *SoK: Decentralized Finance (DeFi)* [online]. arXiv, Jan 2021 [cit. 2021-02-07]. Available at: `https://arxiv.org/abs/2101.08778`.

[97] WeTrust. *WeTrust Identity* [online]. Wetrust.io [cit. 2021-04-08]. Available at: `https://www.wetrust.io/`.

Appendix A

Contents of the included storage media

- thesis — source code in LaTeX, PDF file and pictures