UTRECHT UNIVERSITY

MASTER THESIS

# A Security Assessment Model for Crypto Asset Safekeeping

*First Supervisor:*
Dr. R.L. Slinger JANSEN

*Author:*
Tim Braam

*Second Supervisor:*
Dr. F. Fabiano DALPIAZ

*External Supervisor:*
Henk Brink

*A thesis submitted in fulfillment of the requirements for the degree of Master of Science*

*in the*

Graduate School in Natural Sciences, Business Informatics

November 7, 2019

UTRECHT UNIVERSITY

# Abstract

Graduate School in Natural Sciences, Business Informatics
Master of Science

**A security assessment model for crypto asset safekeeping**

by Tim Braam

In this study we research crypto asset security by dissecting existing security systems, reviewing academic and grey literature and interviewing experts. We then propose a model on crypto asset security and employ it on well-knwown crypto asset safekeeping solutions. We validate the results with experts and elicit mass evaluation with our demonstrations and release to the public.

Keywords: *Cryptocurrency, Cryptocurrency security, Cryptocurrency exchange, Cryptocurrency custodian, Cryptocurrency wallet, Blockchain*

## Acknowledgements

A year ago I started this project, which at that time had a different subject that is, however, closely related to the current one. It is the second time I am writing a thesis, the first being for my bachelor, but the first time I enjoyed doing so. I would like to thank dr. Slinger Jansen for letting and helping me write about a relatively uncharted subject I was passionate about. I would also like to thank my external supervisor, Henk Brink, for believing in the project and supporting me every step of the way. Another huge pillar of support has been my girlfriend and her family, my family-in-law and especially my father-in-law helping me with whatever they could think of. And finally, my own family and friends, thank you all for listening to my blockchain rambling that may have taken up one too many an hour.

# Contents

# List of Figures

# List of Tables

# Chapter 1

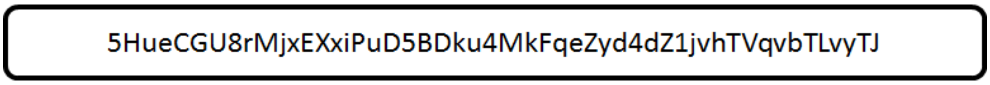
# Introduction

On 9 January 2009 Satoshi Nakamoto implemented and released the first bitcoin code. The code was released as open source. It would be the first "cryptocurrency", which is a form of electronic cash. Fast forward to the present and the first cryptocurrency has become popular and valuable. With it thousands of new cryptocurrencies have sprouted, with a different degree of popularity and success.

Bitcoin, and other cryptocurrencies, rely on another technology that was first introduced with bitcoin called blockchain [63]. A blockchain is a list of records which are linked to each other using cryptographic methods. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data [63]. The most important characteristic of a blockchain is that it is a permanent way of recording that is resistant to modification.

Cryptocurrencies are decentralized, meaning that there is no central authority. Instead cryptocurrencies utilize the blockchain's distributed ledger technology maintained through general consensus. Simply said, the ledger is what most of its users agree on. The ledger keeps an overview of addresses and the number of cryptocurrencies they are entitled to. Because cryptocurrencies are decentralized, they are not bound by borders and can be sent and received around the globe.

Cryptocurrencies are "stored" in "wallets". The term wallet refers to its physical counterpart that is also used to store currency, however they function differently. "Wallets" do not actually hold any currency, the ledger records how much cryptocurrency has been sent **a)** to your address and **b)** from your address, the difference between those amounts is your balance. That balance cannot be negative. Cryptocurrency wallets are pieces of software capable of interacting with one or multiple blockchains. When creating a wallet, a private key is created. From the private key a public key is derived. In turn the public key (along with a checksum and information about the network) is transformed using a hash function to create an address which is public. Because of cryptography, reversing that process is nigh impossible. A private key is a digital signature when creating a transaction on the blockchain. This signature confirms that the transaction comes from the user and prevents the transaction from being altered after issuing. Most wallet services store your public and private keys meaning that whoever has access to your wallet service with your account has access to your crypto assets. When using a HD (deterministic) wallet [27, 84] users also receive ten words (a seed) that can be used to create multiple private keys. Addresses of HD wallets typically start with a 3 [27, 84]. Both public and private keys are long integer numbers, often represented using Wallet Input Format (WIF) which uses both letters and numbers. A sample private key is shown below [97].



5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ

Figure 1.1: A private key

In short; wallets do not actually "hold cryptocurrency" but often store private keys. Those private keys are a signature needed for transactions meaning they are what identifies assets to an owner. There are different kinds of wallets. Losing private keys means losing ownership of the assets. Now let us look at the ecosystem as a whole.

The cryptocurrency ecosystem is relatively young but is invested in immensely. At the time of writing the market cap is over $226 billion [1]. Most of that 226 billion is in the hands of companies established in the year 2009 or later. These companies do not have decades of experience in security. In addition, legislation has not caught up to the possibilities of blockchain and cryptocurrencies. A large amount of money guarded by startups inevitably attracts those with malicious intent. We are left with a risky young ecosystem where not only price fluctuations are extreme, but cryptocurrencies are stolen or lost every day.

Blockchain is one of the technological advancements that could impact our future. Some examples include: First of all, voting using blockchain [2], possible because the blockchain cannot be changed unless there is general consensus. This way citizens could vote fast, secure and from wherever without needing to visit a voting booth. The votes would be counted instantly and precisely. The second example is paying musicians every time their music is played instantly [3] around the globe, without needing a subscription, effectively cutting out the middlemen.

A risky young ecosystem, with great rewards and functionality is for many worth exploring. In this paper we will consider the nature of the cryptocurrency ecosystems as well as the most common threats and weaknesses. We then attempt to create a model that can help investors in determining the security of the environment they keep their investments in, and finally we demonstrate the model against some well-known providers of cryptocurrency safekeeping giving investors some stepping stones in this dangerous ecosystem.

In the next chapter we describe the context of crypto assets, wallets, legislation and crime. Chapter 4 expands on the research methods used, including a description of our literature review. In chapter 5 we describe the results from our interviews with experts. The actual model is constructed in chapter 6, where all maturity levels are discussed and created. We demonstrate the constructed model on some well-known providers of crypto asset safekeeping in chapter 7. Finally, we discuss the findings, validity, accuracy, practicality and further research in chapter 8 and finish with our conclusion in chpater 9.

[1] www.Coinmarketcap.com

[2] https://www.voteaustralia.org.au/blockchain_voting

[3] https://musicoin.org/

# Chapter 2

# Context

Pseudonymity is in the nature of blockchain and the cryptocurrencies that were built on it. Pseudonymity is a word derived from pseudonym, which means “false name”. Cryptocurrency holders hold their assets under a pseudonym, in the case of cryptocurrency that pseudonym is their public address. If your pseudonym is not linked to your legal identity you remain anonymous.

Because of this high measure of anonymity cryptocurrencies have been a popular target for hackers and social engineers. If they succeed in stealing an amount of cryptocurrency and manage to keep their legal identity from being linked to their public adresses they remain anonymous. Just in the first half of 2018, around US $1.1 billion in cryptocurrency was stolen [79]. Additionally, there are services and methods to obscure the transaction streams making them hard to trace [29]. It should be mentioned that some blockchains use technologies and methods to improve anonymity (E.g. zCash [2]).

Even if an address that holds stolen funds can be connected to a legal identity there are various legal issues that make it very hard to get stolen assets back to their rightful owner [7]. First of all, most stolen funds are not even reported because the lack of trust in retrieval by the original owner. And secondly, cryptoassets can easily cross borders. Before the relevant authorities are involved and evidence is gathered the assets are often moved. Because of these reasons reactive methods of securing cryptoassets are very unreliable.

Over the years numerous exchanges have been broken into [50, 94, 101], and thousands of users have lost their cryptocurrency. Often the human is the weakest link [54], and funds are stolen due to negligence on the user’s part. However, in some of the most notable heists, weak points in technology were used to gain access [72, 100]. A few examples made use of libraries in languages such as Javascript and Solidity, the programming language for smart contracts on the Ethereum blockchain. These libraries can be malicious or contain a small error that can be abused [37, 72, 81, 100]. 2-Factor authentication using SMS to identify a user on their mobile phone has also proven insufficient, as hackers gained access to the telecommunication network and rerouted the SMS to their phone instead [64]. This method is also vulnerable to social engineering [40, 54], hackers can impersonate you and ask for a new sim card at your cellular carrier store [3, 56].

Web wallets may use ads or analytics which can be abused by those with malicious intent. Software wallets rely on the safety of the environment in which they run, and cold wallets can be stolen, lost or destroyed. Web and mobile wallets often have no dedicated servers, which can cause critical downtimes [89] and is a general vulnerability [66].

## 2.1 Different wallet providers

We divide wallet providers in three categories; Virtual Currency Exchange Providers (VCEPs), Custodian Wallet Providers (CWPs) and Wallet Providers (WPs). VCEPs are online exchange platforms where cryptocurrencies can be traded against other cryptocurrencies or fiat currencies, examples of well-known VCEPs are Binance.com, Huobi.com and Coinbase.com. CWPs provide their clients with a safekeeping service where they hold their crypto assets for them. This service is often supplied with regular reports and analysis. Some examples of well-known CWPs are BitGo.com and Gemini.com. Finally, WPs provide their clients with a wallet in which they themselves can keep their crypto assets safe. Some examples of well known-wallets are Exodus and Edge.

The current ecosystem is attractive to investors because of the sharp rises in value, but there are dangers that are overlooked in the face of profit. When investing in crypto assets, for instance, investors need to use VCEPs to exchange fiat currency for cryptocurrency. VCEPs, because of their role as facilitators between owners of cryptocurrency, keep the private keys of their owners to themselves to facilitate transactions in a fast, secure and smooth fashion. Unfortunately, this means that a large amount of cryptocurrency is in the hands of a single party, which makes that party very attractive to hackers and social engineers or other malicious parties. In the current situation investing in cryptocurrency immediately puts your investments in a risky place, depending partly on the VCEP in question. Additional effort and knowledge is needed to send that investment elsewhere, to wallet provided by a CWP or a WP. And even then, an investor needs to be privy to the strengths and weaknesses of those CWPs and WPs in order to improve the security of their investments. Unfortunately, there does not exist a tool except for extensive investigation to help investors in that regard. Searching for “best wallet” or “most secure wallet” will result in unreliable blog posts based on a whim, or simply return the most popular ones.

## 2.2 Different cryptocurrencies

At the time of writing there are over 2400 cryptocurrencies. Those cryptocurrencies can roughly be categorized in three categories; Bitcoin, altcoins (alternative-coins) and within those altcoins there are stablecoins.

Bitcoin was the first cryptocurrency and by far the largest. At the time of writing, of the 226 billion invested in cryptocurrencies, 66% is invested in Bitcoin [1]. For most other currencies goes; when Bitcoin loses value other cryptocurrencies lose value. When Bitcoin gains value other cryptocurrencies gain value.

Altcoins are alternative (coins) to Bitcoin [16]. Sometimes they use (nearly) identical code but differ just in name. However, more often they distinguish themselves with a different business model and code. Altcoins can use different consensus algorithms, use different block sizes, hashing algorithms or block processing speed to name the most important ones. A consensus algorithm is needed when computing is distributed such as in a blockchain. Agents need to have a process to agree on the next block in a blockchain. The consensus algorithms currently used by different altcoins are proof of authority, proof of stake, proof of work and proof of space. Differences in block size have an impact on the amount of information that can be stored in a single block while block processing speed impacts the speed new blocks are processed. Faster block processing impacts the time needed for a transaction to be confirmed.

Stablecoins are cryptocurrencies that are pegged to a fiat currency such as the American dollar or the European Euro [51]. There are two kinds of stablecoins, those that are

[1] www.Coinmarketcap.com

redeemable in currency, commodities or fiat money are said to be backed while those that are tied to an algorithm are said to be seignorage-style (not backed) [51].

Different VCEPs, CWPs and WPs support different cryptocurrencies. In this paper we take on the different kinds of providers' point of view when investigating the amount of security of investments. We will not consider security from each cryptocurrency's point of view because of the immense scope and variety. However, our model should be generally applicable from the perspective of other cryptocurrencies as all of them need to be kept by the same providers.

## 2.3 Cryptocurrency governance

Cryptocurrencies are relatively young and so is their governance. Some countries have created legislation aimed at the cryptocurrency ecosystem, such as Japan, South Korea, the United States, Bermuda, Malta and the EU while others have not yet implemented specialized legislation. Even in the countries with specialized legislation the approach taken differs [1, 12, 87].

In this study we will take a high-level approach on governance, differentiating between countries with specialized legislation, countries with early generation specialized legislation and countries that have not yet implemented specialized legislation. We have chosen this level of approach due to the scale of governance variety, general applicability of the model and the limited time of existence of specialized governance.

# Chapter 3

# Research Method

In this research we will be making use of design science which is described as follows: *"Design science is fundamentally a problem-solving paradigm. It seeks to create innovations that define the ideas, practices, technical capabilities and products through which the analysis, design, implementation, management and use of information systems can be effectively and efficiently accomplished"* (von Alan et al., 2004). In this research the purpose will be to create an artifact which should help resolving a problem. As such it is design science research.

In this research we considered using the design science cycle by Wieringa [98] and the design science research methodology (DSRM) [69]. After consideration we have chosen to use the DSRM which is better suited to our research goal.

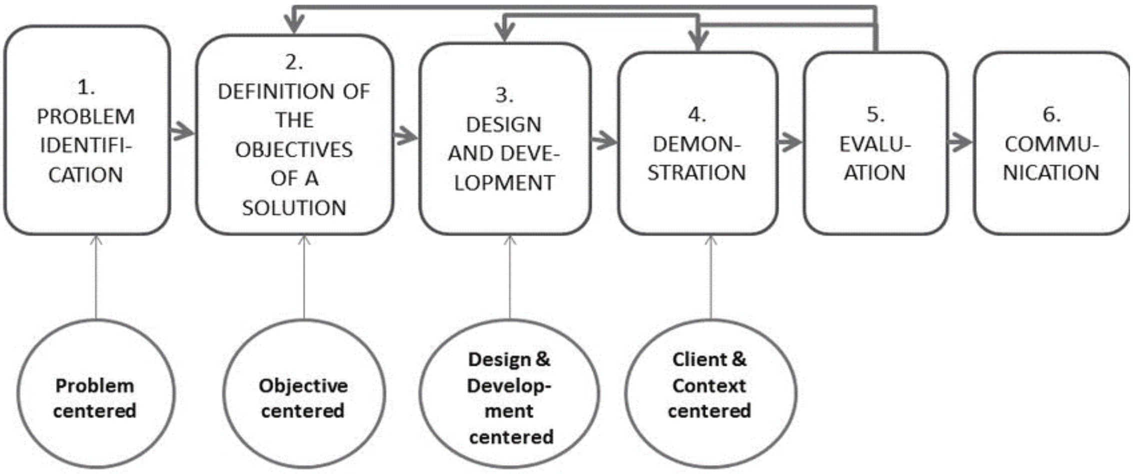

1. PROBLEM IDENTIFI-CATION
2. DEFINITION OF THE OBJECTIVES OF A SOLUTION
3. DESIGN AND DEVE-LOPMENT
4. DEMON-STRATION
5. EVALU-ATION
6. COMMU-NICATION
Problem centered
Objective centered
Design & Develop-ment centered
Client & Context centered

Figure 3.1: The DSRM process model

## 3.1 Problem identification and motivation

In this research we attempt to identify and solve a problem relevant to science, the KAS bank and our personal interest. With our personal interest piqued by the cryptocurrency ecosystem and the limited scientific coverage on that ecosystem we are mostly limited by problems relevant to the KAS bank.

Recently clients of the KAS bank, a custodian bank based in the Netherlands, have been interested in investing in cryptocurrencies. The KAS bank does not support cryptocurrency custody at the time of writing. Because of the interest of their clients in the ecosystems they may, however, start to do so in the future. In the meantime, the bank wants to start with being able to advise their clients on investments. As a custodian bank their service is mostly focused on secure stable investments.

Stability is not something inherent to cryptocurrencies, except for stablecoins pegged to fiat currencies. However, advising investors about security of their investments is possible. There are no frameworks to do so yet, with most searches returning blog posts without clear rationale. As described earlier in the context the ecosystem is known to be risky to investors. That is why in this paper we attempt to create a crypto asset safekeeping security assessment model to arm investors with when entering the ecosystem.

## 3.2 Define the objectives for a solution

After consultation with the KAS bank we have defined the objectives for a solution to the problems we have previously outlined. We hereby establish the following goals; **1)** our framework should be of practical use by investors in the ecosystem, **2)** information needed to use our framework should be gatherable within reasonable means, **3)** the framework should provide a clear, high-level overview of the offered security.

These objectives translate to the following research question: **How can we model the security of a crypto asset safekeeping provider?** With sub questions for our defined objectives.

- What are the design characteristics of a model that depicts the offered security by a crypto asset safekeeping provider?
- What is the scope of information we can use that is attainable by investors?
- What are the requirements of a usable crypto asset safeekeeping security assessment model?

We will answer these questions and abide by their answers in the rest of our research.

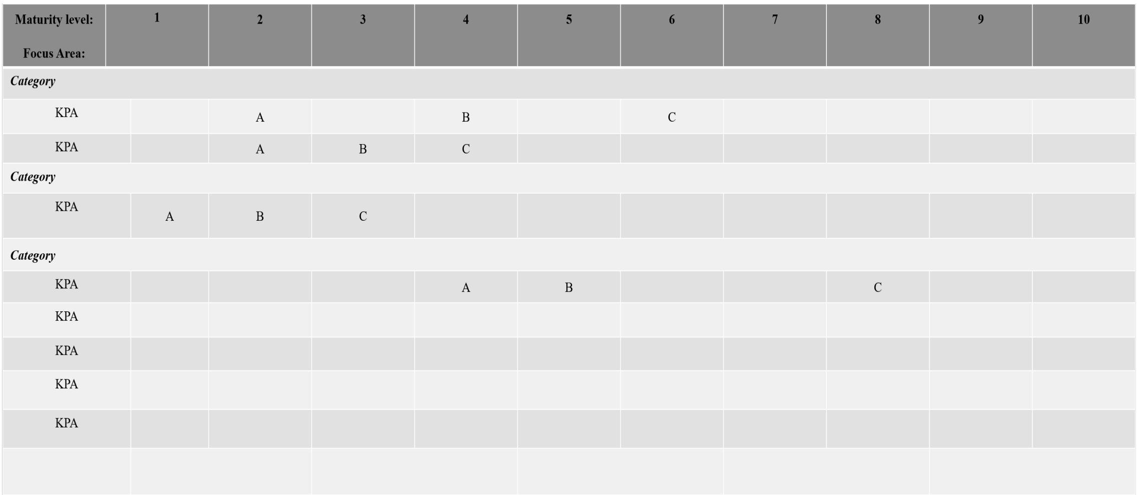
## 3.3 Design and development

### 3.3.1 Design

Design-wise we opted to use the Information Security Focus Area Maturity (ISFAM) pattern as proposed by Mijnhardt et al. [58]. The ISFAM model was developed to aid small and medium enterprises (SMEs) in making incremental improvement in information security. The ISFAM model is a focus area-oriented maturity model as proposed by Steenbergen et al. [95]. The rationale behind this decision is a) maturity is decided by the lowest level capability, an attribute shared by the reality of security engineering, b) it allows us to provide a model with an overview of the security offered in different process areas with different capabilities and c) it can provide developers with a set of requirements when developing a wallet service or increasing the security of one. Finally, the ISFAM model objective is similar to our own. The SMEs in the research by Mijnhardt et al. [58] are the exchange, custodian wallet and wallet providers in ours.

In focus area-oriented maturity models there are different levels measured by clusters of features called Key process Areas [59]. Key process areas in turn have capabilities as visualized in figure 2. Implemented capabilities are shown on different maturity levels with the characters A, B and C. More characters are addes when there are more capabilities.

Key process areas will be depicted on the Y-axis and maturity levels on the X-axis. In our model we will make use of 10 maturity levels, categorized in 5 safety classes. These 5 classes are unsafe, lacking, relatively safe, safer and optimized. The reason we use 10 maturity levels with 5 categories is that allows to distinguish implemented capabilities with greater accuracy. Implemented capabilities that both are a threshold for the unsafe class can now be depicted to have a larger or smaller impact than the other because of the two levels of maturity available to each class.



| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| *Category* | | | | | | | | | | |
| KPA | | A | | B | | C | | | | |
| KPA | | A | B | C | | | | | | |
| *Category* | | | | | | | | | | |
| KPA | A | B | C | | | | | | | |
| *Category* | | | | | | | | | | |
| KPA | | | | A | B | | | C | | |
| KPA | | | | | | | | | | |
| KPA | | | | | | | | | | |
| KPA | | | | | | | | | | |
| KPA | | | | | | | | | | |
| | | | | | | | | | | |

Figure 3.2: A maturity model with 10 maturity levels and example capabilities

### 3.3.2 Development

Development of an artifact in design science is a loop of developing and evaluating. [55]. These two steps are visualised below in the comprehensive framework by Hevner et al. [96] Information Systems Research Framework for Design Science. We have divided the first development process in four phases relying on foundations and methodologies from the knowledge base. In phase I we apply feature modelling, a technique we use to dissect information systems [21]. In phase II we use multiple literature reviews on different perspectives. We use the knowledge of the dissected features from phase I to aid us. Phase 3 and 4 are development phases. In phase 3 we consruct the backbone of our model, a list of candidate key process areas. In phase 4, using all of the information from phases I&II and the list of candidate key process areas we develop our artifact, the crypto asset security maturity assessment model.

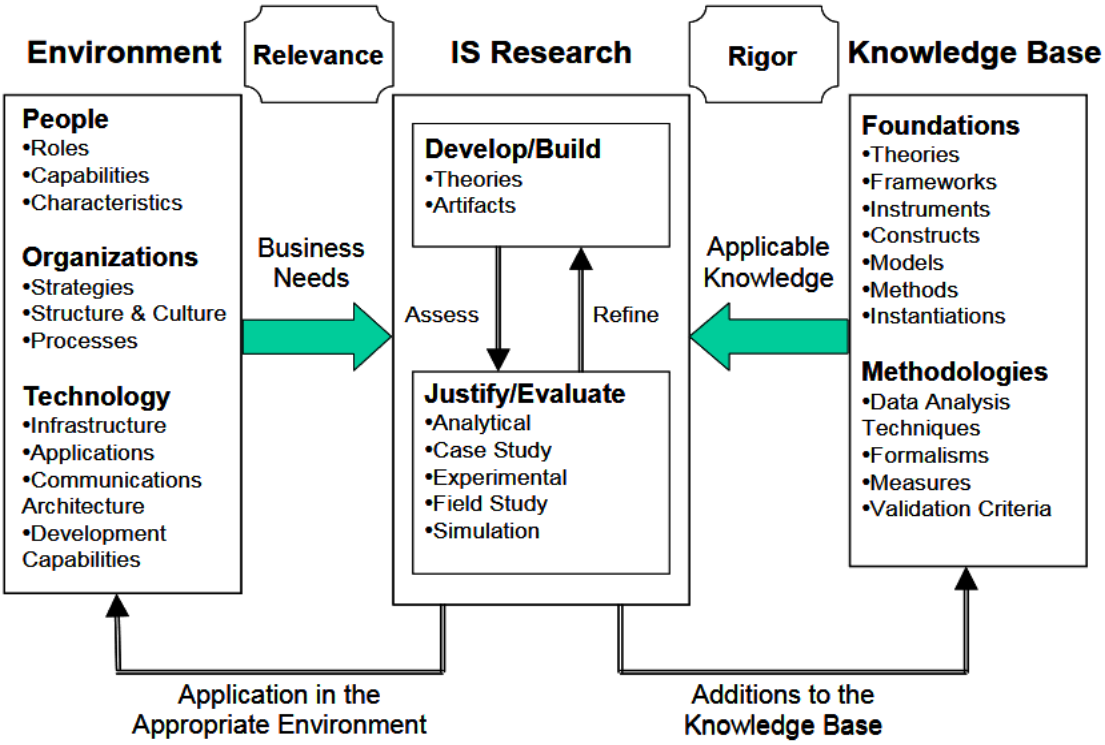


Figure 3.3: The Information Systems Research Framework

**Phase I: Feature modelling**

In phase 1 we use feature modelling in order to a) discover and b) learn about the different components that influence the security of crypto asset safekeeping providers. A simple example of a feature model [1] is shown below.

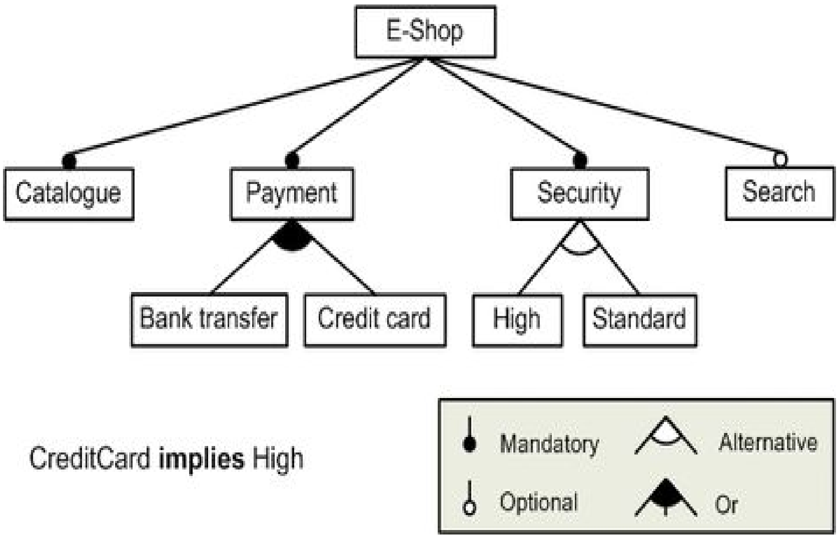


Figure 3.4: Example of a feature model concerning an e-shop

The E-shop, in this case, is the root feature. An e-shop has to have a catalogue, payment option and security in order to function. Explanation on the cardinality of feature models:

- Mandatory means that a child feature is required.
- Optional means that a child feature is optional.
- OR means that at least one, but all of them are also possible, child feature is required.
- Alternative means that one child feature is required and no more than one.

After learning about the different components, we decide if a) the component has a direct impact on security, b) information on the component can be retrieved with reasonable means and c) the provider has a large influence on the component.

The reason we inspect the impact on security is because some features may have a correlation with security but no (direct) causation. For example, let us consider the platform a crypto asset safekeeping service is based on. Is Linux safer than Windows, or are users using Linux generally more knowledgeable users than Windows users? Is Linux safer because Windows is being used more and as such malicious software is developed more for Windows? We attempt to collect factors that have a more direct impact on security without over-generalizing.

Availability of information on a component is required if we want the model to be usable by investors. If the information our model requires cannot be retrieved, the model is unusable. This means that we do not consider some parts of security such as internal security audits and staff training although these are important to running and keeping a service secure.

[1] commons.wikimedia.org/wiki/File:E-shopFM.jpg

Finally, the provider has to have a certain influence on the component it uses. Without influence there is nothing the provider can do to improve the security. For example, investing in cryptocurrency is risky because of the large rises and drops in value. That risk is not something that can be influenced by a crypto asset safekeeping provider.

### Phase II: Literature Research

We search for literature using four perspectives; general, technical, attacker and governance.

A general search on the subject we research provides us with the general knowledge needed to understand the ecosystem. The technical perspective keywords are derived from the feature models and what we learned in our initial general search allowing us to search for the technical details of components involved in crypto asset security. The third perspective focusses on attackers. We search for literature and grey literature on attacks on the security of crypto asset safekeeping providers. Past attacks provide us with valuable information on security such as vulnerabilities in security, the strength or weakness of different components and other practices that are actively abused. Finally, the fourth perspective, governance, is focused on the governance situation in countries and their legislation concerning cryptocurrencies. With the amount of anonymity native to the cryptocurrency ecosystem, the security provided by the government and legislation is a factor to investors. If there is no governance or legislation, providers of crypto asset safekeeping solutions could just run with the crypto assets they were supposed to keep safe after all. We study the level of governance and the legislation world-wide. We expect a large amount of our sources to be government papers and financial task force documentation, which is grey literature.

We use a structured literature review on search words derived from our feature models, which is the technical perspective. However, our other three perspectives do not allow for a structured literature review. The general perspective's purpose is mostly to describe the context of our research and the problem statement, both documented mostly by grey literature instead of academic literature. The attacker perspective is used in creating the security assessment model but is derived from grey literature that does not allow for a strictly structured literature review either. In order to deliver an applicable model without a structured literature review on two of the three perspectives we validate what we derive from grey literature with experts. The general perspective is not directly used in the construction of our model, but the fourth perspective, governance, is. We consider grey literature commissioned by governing bodies and financial task forces to be trustworthy enough to implement their information in our model.

Our general search concerns the main topics of blockchain, cryptocurrency, custody, wallets, security, crime, software and authentication. We use combinations of keywords as depicted in the table below (table 3.1). Query tables show the OR and AND operators. Queries are executed using every single search words and in combination with every search word with the operator AND. When a search words has an operator OR either one of the two search words is included in our query and not both. For example some search queries we executed that are depicted in table 3.1 are: Blockchain, Custody, (Blockchain OR Cryptocurrency) AND Custody, Wallets, (Blockchain OR Cryptocurrency OR Wallets) AND Custody and so on. We inspect the first 60 results (3 pages) generated by Google scholar and Google, as results on further pages are not related closely enough. We eliminate results from dubious sources such as blogs, forums and outdated material.

Information that is mentioned in multiple places is traced to the source or most descriptive source. For instance, when something important happens in the cryptocurrency ecosystem, and one of the dedicated news outlets publishes an article about it, other outlets will often publish a copy, or worse, an edited version. Sometimes we are forced to use a copy if, for example, the original is in Korean or Japanese.

| *Search words & Query* | Blockchain | Cryptocurrency | Custody | Wallets | Security | Crime | Software | Authentication |
|---|---|---|---|---|---|---|---|---|
| Blockchain | - | OR | AND | OR | AND | AND | AND | AND |
| Cryptocurrency | - | - | AND | AND | AND | AND | AND | AND |
| Custody | - | - | - | AND | AND | AND | AND | AND |
| Wallets | - | - | - | - | AND | AND | AND | AND |
| Security | - | - | - | - | - | AND | AND | AND |
| Crime | - | - | - | - | - | - | OR | OR |
| Software | - | - | - | - | - | - | - | AND |
| Authentication | - | - | - | - | - | - | - | - |

Table 3.1: General perspective queries

The literature review for our technical perspective uses search words derived from feature models (ch.4.1) and our general literature review. Search engines used are Google Scholar and Scopus. We only inspect the first two pages (40 results) as further pages are not related closely enough. Below is a table representing the queries. We eliminated results that a) did not describe the keyword we searched for, b) were related but not closely enough, c) described the same thing or d) were not published in a trusted place. Finally, we read the remaining research and used a forward and backward search on the literature cited in the research we considered useful in order to build the list of literature we use in this research.

| *Search words & Query* | Cryptography | Social Engineering | Encryption | Hashing | Mobile | Biometric | Digital Signature | Security | Standards |
|---|---|---|---|---|---|---|---|---|---|
| Cryptography | - | OR | OR | OR | AND | AND | OR | AND | AND |
| Social Engineering | | - | OR | OR | AND | AND | OR | AND | AND |
| Encryption | - | - | - | OR | AND | AND | OR | AND | AND |
| Hashing | - | - | - | - | AND | OR | OR | AND | AND |
| Mobile | - | - | - | - | | AND | OR | AND | AND |
| Biometric | - | - | - | - | - | | OR | AND | AND |
| Digital Signature | | - | - | - | - | - | | AND | AND |
| Security | - | - | - | - | - | - | - | - | AND |
| Standards | - | - | - | - | - | - | - | - | - |

Table 3.2: Technical perspective queries

Third, the literature search that focusses on attacks on services in the cryptocurrency ecosystem works in much the same way as our general literature review. We take a look at the first 60 results, eliminate doubles and those with a dubious source. We backtrack through sources of read articles to the original source if we can. In this review our purpose is to find the weak link that allowed the attackers to pull off their attack.

| *Search words & Query* | Cryptocurrency | Bitcoin | Stolen | Lost | Frozen |
|---|---|---|---|---|---|
| Cryptocurrency | - | OR | AND | AND | AND |
| Bitcoin | | - | AND | AND | AND |
| Stolen | - | - | - | OR | OR |
| Lost | - | - | - | - | OR |
| Frozen | - | - | - | - | |

Table 3.3: Attackers perspective queries

Finally, the fourth literature review focusses on governance. We use Google and focus on the first 60 results. We focus our search through governing bodies and specialized websites that we consider highly trusted. For instance, we search through the entire financial action task force (FATF) website, because it is an official global leader of anti-money laundering governance and legislation. Likewise, we study the contents of all of the reports released by Ciphertrace [2] , a website solely focused on reporting about the state of cryptocurrency legislation and governance. Other sources of information are other international and national financial taskforces.

| *Search words & Query* | Cryptocurrency | Legislation | Anti-money laundering | Financial task force | Governance |
|---|---|---|---|---|---|
| Cryptocurrency | - | AND | AND | AND | AND |
| Legislation | | - | AND | OR | OR |
| Anti-money laundering | - | - | - | AND | AND |
| Financial task force | - | - | - | - | OR |
| Governance | - | - | - | - | |

Table 3.4: Governance perspective queries

[2] Ciphertrace.com

#### Phase III. Key process discovery

KPAs or Key Process Areas are “A cluster of related practices in an area that, when implemented collectively, satisfies a set of goals considered important for making improvement in that area" [59]. In our model, the different KPAs will satisfy the goal of security.

Constructing our list of key process areas is spread out over the design and development, evaluation and communication phases of the DSRM that, like we explained before, are repeated multiple times in this research. When we discover a candidate key process area, we present the process area below the research that provided us with that insight. These tables look like this:

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Candidate key process area | [35, 53, 63, 97] | The category the ckpa belongs to | A short description on the ckpa. This description usually explains why we consider the process area important to security. |

Table 3.5: Example kpa candidacy

In the design and development phase a candidate key process area shortlist is created. At the beginning of this phase that list is empty. During this phase we constantly add clusters of related practices when we find them during feature modelling, general, technical and attacker literature review. These candidate key process areas may be added, changed or removed at any step in this phase. When we arrive at the end of the design and development phase the first time, we now have our first iteration of a candidate key process area shortlist.

We then construct an iteration of our model in the last step of the design and development phase, which we will describe in more detail later. Now that the design and development phase is concluded we start the next phase; evaluation. In this phase we talk with experts about the current model and the current candidate key process area shortlist. Experts are asked for **a)** their opinion on the current candidate key process areas and which ones to add, change or remove, **b)** the maturity levels and their assigned capabilities.

With the added, changed or removed candidate key process areas we then construct a new candidate key process area shortlist which we use in a new iteration of the model. At times in the DSRM process we communicate an iteration of that model to a larger audience and collect feedback. That feedback is used to once again add, change or remove candidate key process areas after which we end up with a new iteration of the CKPA shortlist. Although we drop the candidate in candidate key process area in the last iteration of the shortlist, which is included in this research, in reality the key process area shortlist is not perfect and will undergo more change in the future. This means the key process area shortlist will always remain a candidate list, and the process of adding, changing and removing continuous throughout this research.

#### Phase IV: Model construction

In the last phase we start constructing the crypto asset security maturity assessment model. We already specified the information security focus area maturity pattern we will use, the ten maturity levels and their 5 security classes. In phase 3 we have constructed a list of KPAs. These KPAs are entered in the focus area-oriented maturity model which now leaves us with deciding on the capabilities and their assigned maturity levels.

Implemented capabilities are assigned according to our literature review, multiple interviews with experts and mass feedback gathered in the communication phase of the

DSRM. The development step of the DSRM is revisited multiple times and the model constructed in this phase has had 11 relevant iterations at the time of writing, not counting iterations focused on layout or readability.

## 3.4 Demonstration

This step is about testing the artifact to solve the problem or several instances of it. In this case, the cryptoasset model will be used to measure the security of several popular virtual currency exchange providers, custodian wallet providers and wallet providers.

Demonstration is used to **a)** test the usability of the model, **b)** elicit feedback from stakeholders and **c)** prove the usefulness of the model.

We have stated earlier that the model should be usable by investors. If information required to use the model cannot be discovered with reasonable means and our description in doing so we need to adjust our model until it can. We add one condition to this restriction, which is that this restriction is not considered if the information required does not matter in acquiring a higher maturity level. For instance, if a technical KPA can structurally not be discovered for multiple providers of a certain kind but that kind of provider cannot acquire a higher level of maturity with or without that missing information.

Demonstrating our model can be used as an elicitation technique in order to gather meaningful feedback. Stakeholders, be they investors, developers or providers can agree or disagree and may be more inclined to provide feedback. In the later iterations of our model the model should be becoming increasingly accurate. We can then compare the results of our demonstration with the representation in other media. If that yields a relevant difference, we consider our goal of informing investors at least partially completed and the model useful.

## 3.5 Evaluation

Although evaluation is officially step 5 in the DSRM, we re-visit the construction, demonstration, evaluation and communication steps multiple times during this research.

Following each iteration of our constructed model we interview an expert on the subject. Depending on his or her opinion we return to the construction step. By communicating and publishing the model and our demonstration we provoke mass feedback.

## 3.6 Communication

Communicating this research will be done by releasing the model to the public, online for everyone to use. Feedback gathered on the website can be used as second evaluation and be incorporated in the final model. Steps 3-6 are repeated every iteration of the model.

Communicating is done in earlier stages by sending the model to experts and demonstrating the model to our peers.

# Chapter 4

# Model Development

## 4.1 Feature Modeling

In order to know what we should search for in literature and grey literature we must first understand what crypto asset safekeeping security consists of. To do this we start with dissecting crypto asset safekeeping methods using feature modelling. We have created multiple feature models of different safekeeping providers in order to determine what features are important. We then discard features that cannot be controlled by the Virtual Currency Exchange Providers (VCEPs), Custodian Wallet Providers (CWPs) and Wallet providers (WPs). The list of features that remain will be added to the search for literature.

We selected a range of existing security methods with increasing complexity. Below are the feature models we have constructed. All models except the last, most complex model, can be found in Appendix B. The most complex model will be textually described first, followed by its feature model (figure 4.1).

- A method using only pincode authentication. We modelled an existing software wallet requiring a pincode.
- A method using either a pincode or a fingerprint for authentication. In this case we have moddeled a software wallet on a mobile device which can be unlocked by either a pincode or fingerprint. The wallet itself does not require authentication.
- A method using 2-factor authentication with both a password and a pincode. In this case the password is needed to login a windows computer, the pincode is required to access the software wallet installed on the windows computer.
- A 2-factor authentication method using SMS as one of the two authentication factors.
- A wallet with an escrow multisignature setup requiring two out of three parties to approve transactions (Figure 4.1).

### 4.1.1 Escrow two out of three feature model

The online computer is protected by two step verification, one step being the windows password and the second a pin code for the online wallet service. The air gapped offline computer only requires a pin code for the wallet software and runs on windows. The mobile device requires a pin code or a fingerprint.

The online computer requires a password to log in. Windows passwords are hashed by two hash functions; LMHash and NTHash. LMHash is based on DES but provides less protection. NTHash is based on MD4. Now let us look at the pin code. Pin codes are usually between 4-8 numbers, and as such are more prone to brute force techniques simply because there are fewer options. As such hashing does not help much, even if you hash the pin code, those that know what hashing algorithm was used can still brute force the pin code simply because of its simplicity. So, if you want to be safe, the way to go is to encrypt the hashes with a private key that is stored in a different location from the hashes. Another way to go about this is neglecting the encryption and hashing altogether and be very sure that nobody is going to get access to the database.

The air-gapped offline computer is protected by a PIN code in the wallet software and runs windows. The difference here is that the PIN code is not required by Windows but by the wallet software. Additionally, the wallet in this case is software running on the local machine and not an online wallet service. As such the PIN code will not be stored in an online database, but locally. Because a PIN code set on wallet software serves to keep people out who already have access to the device, we can assume that not hashing or encrypting the PIN code when saving it locally is not a realistic option.

The mobile device can be unlocked by either entering a PIN code or by fingerprint. Because a mobile device should be unlockable when there is no internet connection PIN codes and fingerprint data is stored locally. The place where they are stored however, is different. Biometric data needs to be stored very securely because users cannot change their biometric data for the rest of their lives. As such, biometric data on mobile devices is stored securely in a Trusted Execution Environment (TEE) [85] which essentially is a separated and isolated area of hardware with in-and output protection running on a specialized OS. The fingerprint is hashed using device, user and time specific data.

Explanation on the cardinality of feature models: **1)** Mandatory means that a child feature is required, **2)** optional means that a child feature is optional, **3)** OR means that at least one, but all of them are also possible, child feature is required, **4)** alternative means that one child feature is required and no more than one.

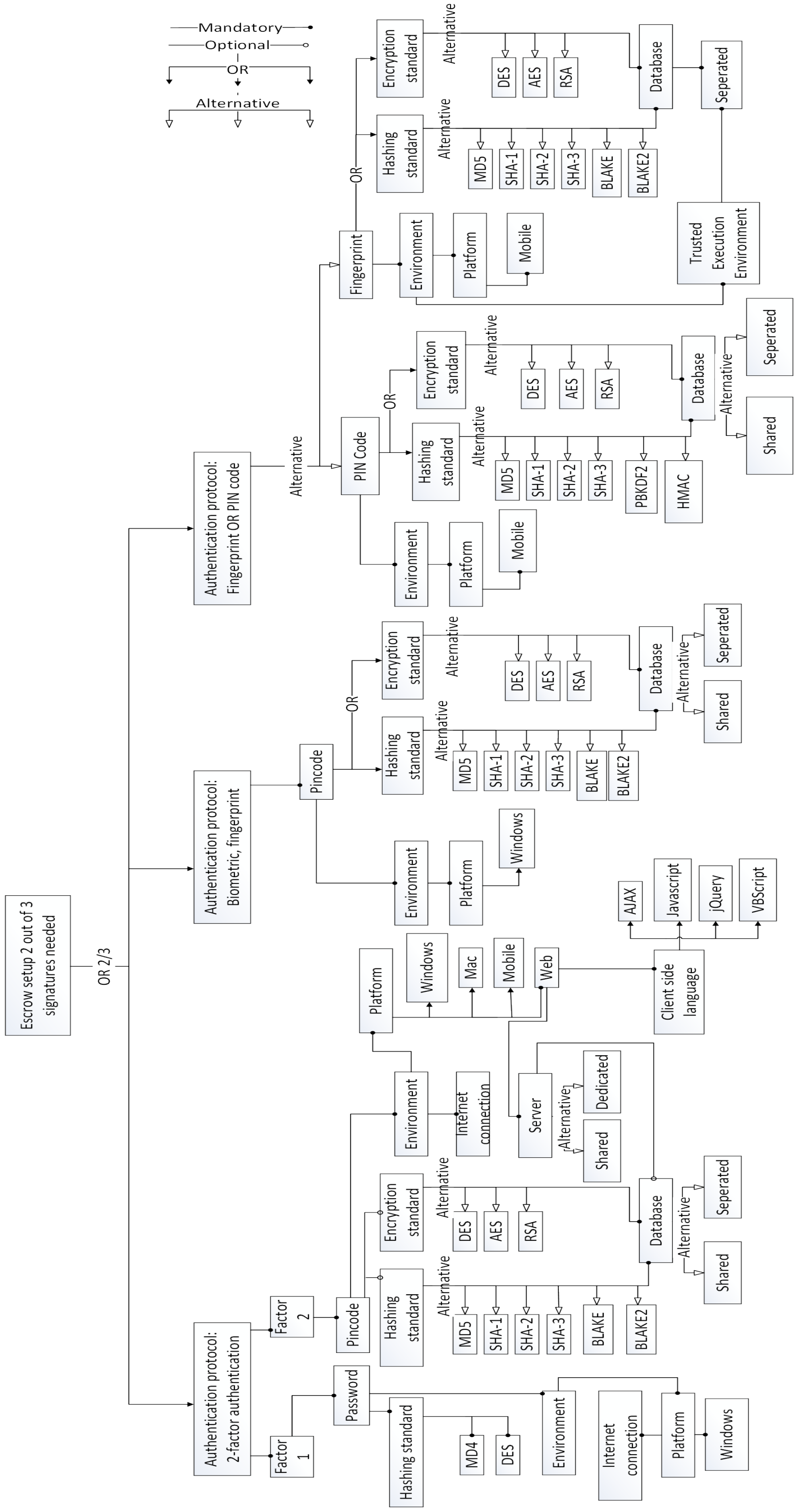


Figure 4.1: A complex crypto asset security setup using escrow 2 out of 3 feature model

After modelling the multisignature solution seen on the last page we have gathered a list of components required when securing a wallet solution. Table 4.1 shows the components we think we should research and which components we discard. We shortly describe the feature and the reason behind our action in the rationale column.

| *Feature* | *Action* | *Rationale* |
|---|---|---|
| Authentication protocol | Research | Authentication and identification protocols are indispensable to access control. |
| Encryption | Research | There are multiple encryption families with multiple encryption algorithms. Not all of them offer the same level of security. Providers often use encryption in their services. |
| Platform | Discard | There are multiple platforms (i.e. windows, mac, linux, mobile, web) wallets can run on. Platforms are customizable by users and do not translate into security directly. |
| Server | Research | All (online) services are hosted on a server. We should find out what the differences are. |
| Programming languages | Discard | Programming languages have different qualities. Programmers have different level of skills. Some programming languages are better suited to certain goals. Additionally inspecting code is impossible for investors due to lack of expertise and access to the actual code. As was the case with platform there are too many factors playing a role that judging on programming language would be overgeneralizing. |
| Hashing | Research | Hashing has different hashing families with different hashing algorithms varying in security just like encryption does. Which algorithms are secure and why? Moreover, which are less secure and why? |
| Digital signature | Research | Sometimes services use a digital signature when communicating. When are digital signatures used, which algorithms are there and how secure are they? |
| Database | Research | A Databases store important information that should be kept safe. What is secure database management and what isn't? |

Table 4.1: Discovered features

## 4.2 Literature Review

### 4.2.1 General perspective

The research goal in this study is the defining of a crypto asset safekeeping security maturity assessment model. Knowledge needed to do so, covers the fields of security engineering, cryptography, social and security hacking, blockchain, cryptocurrency and wallet soft-and hardware.

Security engineering is the specialized field of engineering that deals with the security aspect of the designing of systems [54]. The security aspects need to be able to withstand disruptions from sources ranging from malicious attacks to natural disasters. The information we are looking for from this specialized field of engineering are the security mechanisms and technologies used today and what sort of disruptions they are supposed to protect a system against.

Cryptography is the practice and study in ways of communicating securely [44]. Cryptography used to be based on encryption, conversion of readable text to nonsense. In the current day and age cryptographic methods are based on mathematical theories and designed around computational hardness assumptions. Where encryption was defeated by hand historically, nowadays these algorithms are solved by computers, which is why in turn the design of new algorithms is focused on not being solvable in a relevant timespan by those same computers. However, with computer technology advancing rapidly algorithms that may have once been safe, or still are, may be rendered useless before the computers of the future [93].

Hacking is the act of gaining access to systems. In this research we will pay attention to two categories; social hacking (also called social engineering) [40] and security hacking [37, 56, 64, 66, 72]. Security hacking is the use of bugs and exploits to gain access to a system, while social hacking uses psychology and clever tricks on humans to do the same. This information is needed to judge how secure security technologies are.

A blockchain is a growing list of blocks linked by cryptography. Each block contains a hash of the previous block, which is a cryptographic code used to map larger data, a timestamp and a certain amount of transaction data [44, 63]. Blockchains are what cryptocurrencies are built on, and the network wallets communicate with. In order to understand the ecosystem in which wallets operate we need knowledge of the blockchains they work on.

A cryptocurrency is a digital asset designed to work as a medium of exchange on a blockchain [63]. Cryptocurrencies are many and differentiate in the way they work and what they focus on. The idea behind cryptocurrencies is that they are completely decentralized in control, although many cryptocurrencies diverted from complete decentralization. Information on these cryptocurrencies is needed to know what exactly the nature is of the assets we are trying to protect.

Wallet soft-and hardware are the products and services to communicate and transfer cryptoassets on a blockchain [53]. There are five types of wallets: hardware wallets, paper wallets, desktop wallets, mobile wallets and web wallets [53]. They offer different kind of services and use different technologies to secure their products. They represent the current situation in cryptoasset security, which makes them essential in this research.

There are a few characteristics to cryptocurrency and investing in cryptocurrency that are unique to the ecosystem. These characteristics are often overlooked by those new to the ecosystem but are in fact very important.

The **first characteristic**, and the one that caught the eye of most investors in the first place, is the explosiveness of its value. In the chart below we can see the value of the best-known cryptocurrency, Bitcoin.

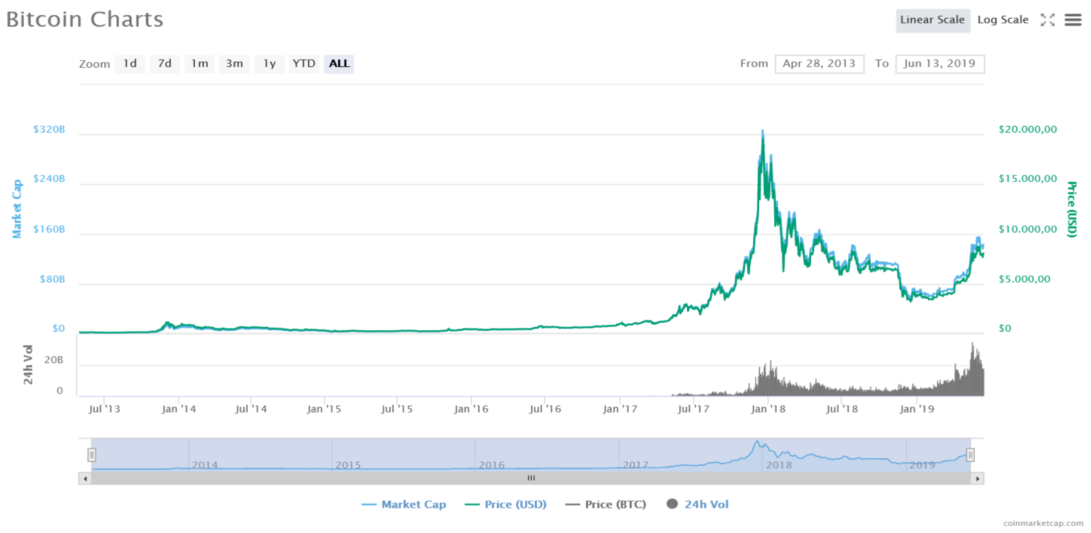


Figure 4.2: The value of Bitcoin (BTC) over its entire lifespan

Source: Coinmarketcap.com

Bitcoin rose in a couple of years from being worth nearly \$0, to a peak of \$19.710. Shortly after that peak, however, it dropped a staggering ∼\$13.000 to \$6.479 in mid-February, a drop in value of ∼77%. Although more gradually the cryptocurrency would continue to lose value until April.

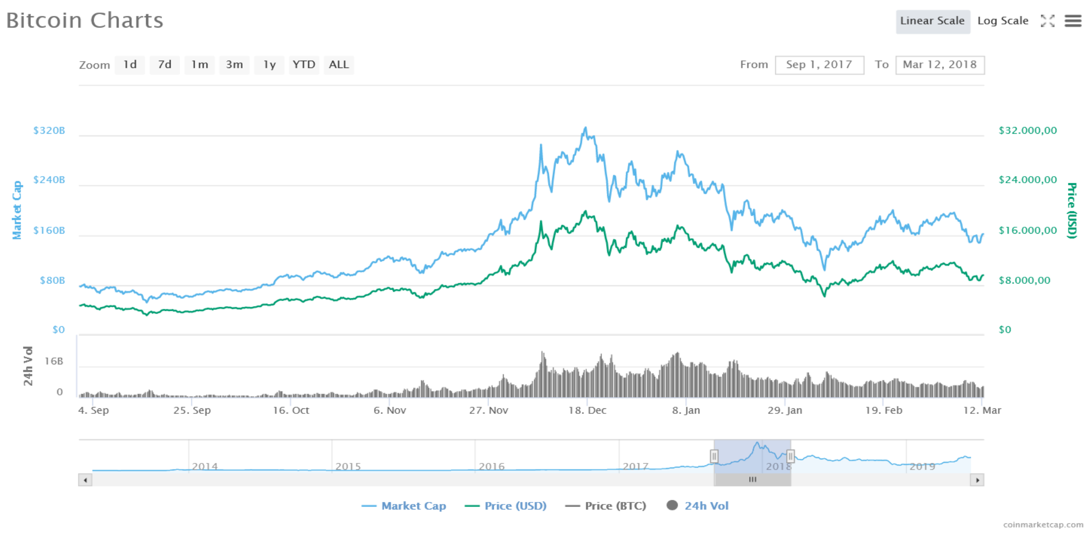


Figure 4.3: The largest drop in BTC history, December 2017 to February 2018

Source: Coinmarketcap.com

Although this drop in value is the largest to date, when you look at the percentages these rises and drops are nothing new to Bitcoin. In June 2011 Bitcoin was worth $32 but fell back to about $2 a few months later, a drop of 94%. Towards the end of 2013 Bitcoin rose to new heights when the value of a single Bitcoin was $1200. Due to China's conclusion that Bitcoin was not a currency, restrictions worldwide and the famous implosion of Mt Gox the price got in a slump bottoming out at $150 over 411 days which was a tumble of about 87%. Earlier that year, in April, Bitcoin rose to $260 in a matter of days, but managed to drop back to $45 in two days, a decline of 83% [24]. Although we only look at Bitcoin here, there are strong ties to other cryptocurrencies which are also subject to these rises and drops. The only types of cryptocurrencies not affected are so called "stablecoins" which are pegged to the value of a FIAT-currency such as the American dollar or the European Euro [73].

Money can be made by investing at the right moment, but the opposite is also true, and an investment may devaluate by half or more in just a couple of days or even hours. Because of this reason some investors have stop-loss orders in place [28]. Stop-loss orders trigger when a cryptocurrency drops to a certain price which can be specified by the investor. Not all exchanges allow for stop-loss orders, and other investors do not use them because they can also trigger when you do not want them to. In case of a flash crash caused by a bug a stop-loss may trigger, even though the value bounces back directly after, effectively losing investors' money. However, using stop-loss orders, or not, investors are dependent on the exchange they use. There have been cases in the past where exchanges froze the trading of certain cryptocurrencies during massive price rises or drops [57], or where a flash crash happened [15] triggering stop losses.

The **second characteristic** of cryptocurrencies are the exchanges they are traded on. We already mentioned the stop-loss dilemma and freezes that may happen on these platforms, but there are more characteristics unique to the trading platforms in the cryptocurrency ecosystem. Exchanges do not earn their revenue by investing in cryptocurrency themselves, although they have a very large amount of it because they control the cryptocurrency of all their users. This is not the case for decentralized exchanges, where users control their own private keys [9], however, there currently is only one real decentralized exchange. Exchanges earn most revenue by charging money on FIAT deposit and withdrawal, a transaction fee on every transaction, offering extended service or functions to PRO users and listing fees. Listing fees are paid by companies who would want to list their cryptocurrency for trade on an exchange. Listing fees on exchanges with higher trading volumes can ask for higher listing fees. However, because exchanges have control over the cryptocurrency of their users, they can artificially inflate the trading volume, allowing them to inflate their listing fees. In recent research by Bitwise [4] only 10 out of 83 exchanges did not artificially inflate their trading volume, those 10 accounts for 5% of the reported trading volume. The other 73 exchanges wash trade to some extent to inflate their trading volume and listing fees. Wash trading is buying or selling a stock for the express purpose of misleading the market and was banned in the Commodity Exchange act of 1936. Also included in that act was that brokers are not allowed to profit from wash trading, even if they are not involved themselves. However, no cryptocurrency exchanges have been fined or sued yet for wash trading. In conclusion, exchanges cannot and should not be trusted to the extent of regular brokers and exchanges as they are not (yet) regulated in the same way.

The **third characteristic** concerns the blockchain, the distributed ledger technology cryptocurrencies exist on. A blockchain, as the name suggests, is a chain of records called blocks. Blocks are linked to one another using cryptography. Each block contains a hash of the previous block as well as a timestamp and transaction data [44, 63]. As more transactions take place the chain grows longer and longer. The ledger is constantly synchronized between everyone who downloads it. Sometimes the community behind a blockchain may decide a change to the protocol is needed. Because blockchains are decentralized updates cannot happen in an instant. What happens is a fork, either a soft fork or a hard fork. When the protocol changes the nodes running the new rules will no longer accept blocks with the old rules. In the case of a soft fork nodes running the old rules will realize their blocks are not accepted anymore and update their protocol, in the end resulting in one blockchain while the older one is abandoned [11]. In the figure below a graphical representation is shown.

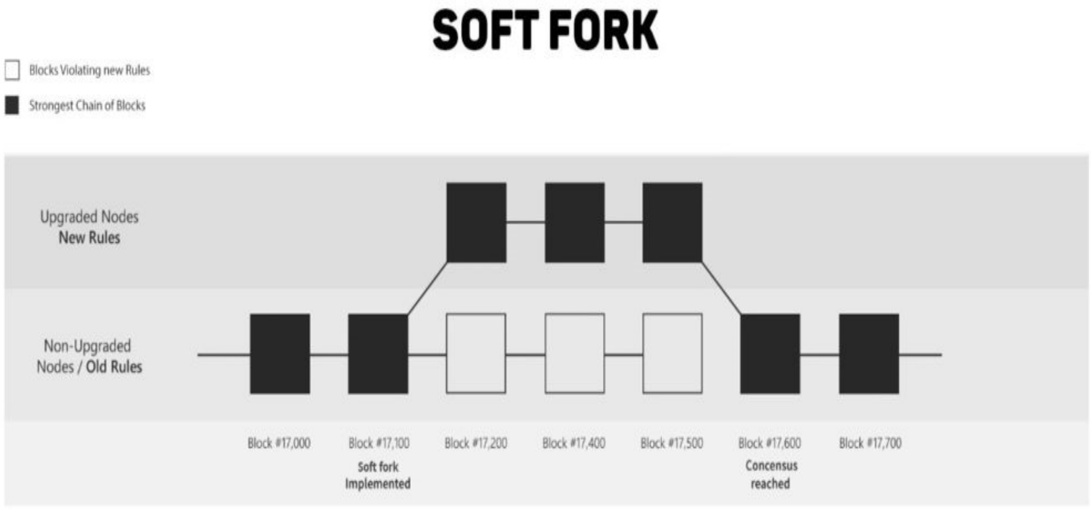


Figure 4.4: A soft fork

Source: https://applicature.com/wp-content/uploads/2018/11/a-soft-fork.jpg

Soft forks usually happen when the community behind the blockchain is in favor of one of the two versions of protocol. With insufficient support for the other, one of the two is abandoned. However, in some cases there are supporters for both versions of protocol. In this case neither of the chains are abandoned, this is called a hard fork. Figure 4.5 shows a graphical representation of a hard fork.

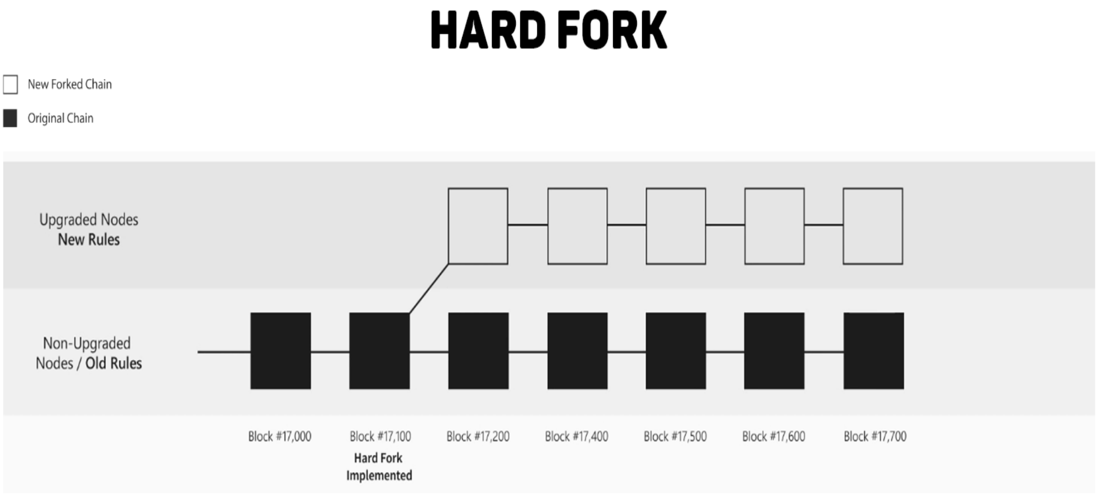


Figure 4.5: A hard fork

Source: https://qph.fs.quoracdn.net/main-qimg-05e3c26fc5eacd057de2661cb240133f

A hard fork results in a phenomenon that is unique to investing in cryptocurrencies. After a hard fork the cryptocurrency is split in two cryptocurrencies that may fluctuate in value independently [11]. Because both cryptocurrencies share blocks before the hard fork, anyone owning any cryptocurrency before said fork own the same amount of cryptocurrency on both chains after the fork. Although, because of independently fluctuating values, this does not mean that your investment has effectively doubled it does mean that your investment has split in two. Now, what is important to this characteristic to investors is that if they do not own the private keys to their cryptocurrencies the split-off currency may not be handed to them. This means that a part of your investment is effectively taken. When a hard fork is coming up it is important to control your own private keys. Parties who not grant the power over private keys (VCEPs, CWPs) to their users should alert and inform their users of the actions they as a company will take.

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Distribution of power | [4, 9, 11, 15, 28, 73] | Preventive | VCEPs are not regulated the way traditional brokers are (yet) and should not be trusted to the same extent. Additionally, both VCEPs and CWPs do not allow for control over your own private keys and may not hand over split-off currency, inform and alert investors in case of a hard fork and may freeze transactions or trigger stop losses. Parties who do not allow control over your own private keys are targets for hackers and insiders as they are the places where most of the cryptocurrency gathers in one place. Because of these reasons the distribution of power over the private keys is very important to the security of investments made in the cryptocurrency ecosystem. |

Table 4.2: CKPA distribution of power

## 4.3 Technical perspective

### 4.3.1 Authentication protocol

| *#* | *Title* | *Authors* | *Year* | *Source* | *Cites* | *Topic* |
|---|---|---|---|---|---|---|
| [99] | The memorability and security of passwords–some empirical results | Yan, J., Blackwell, A., Anderson, R., & Grant, A | 2000 | University of Cambridge, Computer Laboratory | 149 | Weakness of passwords |
| [25] | Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. | Bonneau, J., Bursztein, E., Caron, I., Jackson, R., & Williamson, M. | 2015 | Proceedings of the 24th international conference on world wide web (pp. 141-150). | 51 | Weakness of passwords, Weakness of security questions. |
| [48] | Shoulder surfing attack in graphical password authentication. | Lashkari, A. H., Farmand, S., Zakaria, D,. Bin, O,. & Saleh, D. | 2009 | arXiv preprint arXiv:0912,0951. | 113 | weakness of passwords, graphical password authentication, shoulder surfing. |
| [75] | Enhancing security and privacy in biometrics-based authentication systems. | Ratha, N. K., Connell, J. H., & Bolle, R. M. | 2001 | IBM systems Journal, 40(3), 614-634. | 1793 | Weakness of passwords, strengths and weaknesses of different biometric authentication protocols. |
| [49] | Security weaknesses and improvements of a fingerprint -based remote user authentication scheme using smart cards. | Yang, H. K., & An, Y. H. | 2012 | International Journal of Advancements in Computing Technology, 4(1), 15-23. | 256 | Fingerprint authentication, biometric authentication |
| [80] | Independent one-time passwords. | Rubin, A. D. | 1996 | computing Systems, 9(1), 15-27. | 123 | One-time passwords |
| [65] | Comparing passwords, tokens, and biometrics for user authentication. | O'Gorman, L. | 2003 | Proceedings of the IEEE, 91(12), 2021-2040. | 772 | Authentication protocols |
| [91] | Face recognition on consumer devices: Reflections on replay attacks. | Smith, D. F., Wiliem, A., & Lovell, B. C. | 2015 | IEEE Transactions on Information Forensics and Security, 10(4), 736-745. | 65 | Face recognition, biometric authentication, replay attacks |
| [42] | Biometrics: a tool for information security. | Jain, A. K., Ross, A., & Pankanti, S. | 2006 | IEEE transactions on information forensics and security, 1(2), 125-143. | 1145 | Biometrics, multibiometrics |
| [31] | How iris recognition works. | Daugman, J. | 2009 | The essential guide to image processing (pp. 715-739). | 4451 | Iris recognition, biometrics |
| [68] | Preliminary study on iris recognition system: Tissues of body organs in iridology. | Othman, Z., & Prabuwono, A. S. | 2010 | 2010 IEEE EMBS Conference on Biomedical Engineering & Sciences (IECBES 2010) (pp. 978-1). | 16 | Iris recognition, iris data and medical information |
| [26] | Biometric authentication. | Braghin, C. | 2000 | University of Helsinki, Department of Computer Science. | 17 | Biometrics, biometric authentication protocols |
| [13] | Location-based kerberos authentication protocol. | Abdelmajid, N. T., Hossain, M. A., Shepherd, S., & Mahmoud, K. | 2010 | Computing (SocialCom), 2010 IEEE Second International Conference on (pp. 1099-1104). IEEE. | 21 | Location based authentication, kerberos |
| [41] | Legal and ethical implications of GPS vulnerabilities. | Iqbal, M. U., & Lim, S. | 2008 | J. Int'l Com. L. & Tech., 3, 178. | 24 | Location based authentication, GPS vulnerabilities |
| [74] | Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. | Rabkin, A. | 2008 | Proceedings of the 4th symposium on Usable privacy and security (pp. 13-23). ACM. | 217 | Security question authentication |

Table 4.3: literature list of the technical perspective - authentication

Authentication is the first step in access control. Authentication protocols can be divided in three main categories: "something you know", "something you have" and "something you are".

The best known and most used authentication protocols are the password and PIN-code authentication protocols. These authentication options belong to the something you know category. A password is a word you enter in order to gain access to something. A PIN code is a number. PIN codes are weaker to brute force attacks because they limit users to using only numbers, which reduces the pool of possible entries [99]. However, because brute force attacks are very basic most services protect against them by limiting the amount of times you can enter your password. Passwords that are stored can be stolen, entering passwords anywhere is not resistant against a variety of technological and psychological attacks such as the man-in-the-middle attack or simple shoulder surfing [99]. Additionally, humans often find it hard to remember passwords and as such use very simple passwords [99].

As mentioned before, static passwords are not resistant to methods like wiretapping. Hashed passwords are but are still vulnerable to man-in-the-middle attacks [25]. Another weakness that is often abused is the need for a "forgot your password" option because humans tend to forget their passwords. These forgot my password options often rely on a secret question, or just send a link to your e-mail. Secret questions often are only few and have been known to be prone to datamining techniques [25]. A link to your e-mail means that if someone with malicious intent has control of your e-mail address that he or she has access to any sites, services or software that use this kind of forgot your password option [25].

Finally, we humans tend to reuse the same (often simple) password. This means that if one of the services we use the password for is compromised, every service the same password is used on is in danger [48].

Fingerprint authentication is the first protocol that uses biometric data that we will discuss. All biometric authentication protocols belong to the "something you are" category. Fingerprints are much more secure than passwords. They are very hard to be stolen and can almost not be lost [75]. They are very hard to forge, cannot be shared, easy to use and just as fast or faster as passwords. However, in the case that a fingerprint is compromised this means you lost that fingerprint for the rest of your life, as you cannot change your fingerprint and only have 10 fingers [75].

Fingerprints cannot be guessed, or brute forced. Fingerprints are still vulnerable to some kinds of man-in-the-middle attacks. For instance, the masquerade attack is when a service pretends to be another service to ask for your fingerprint and then saves it. Intercepting traffic between the user and a trusted service is still possible as well, however usually fingerprint scanners, and every other biometric scan, run on secured hardware to prevent these attacks [49]. Another problem is the fact that hardware errors cannot be solved by users. If the hardware that you are using does not recognize legitimate fingerprints suddenly there is not much that can be done [65].

Face recognition, like fingerprint authentication, uses biometric data. It is very fast, but not nearly as secure as fingerprint authentication. Hardware in the possession of the public is not yet good enough. Additionally, a face may change with diet or age. A person only has one face, which means that if it is stolen you cannot use another. A large amount of the public has his or her face on the internet somewhere. As such the protocol is very vulnerable to replay attacks, where a photo of the face is used to authenticate [91]. Face recognition also suffers under different conditions of face position, illumination, accoutrements and the complexity of a human's face and its different expressions [42].

Irises, like fingerprints, can vary immensely and as such are very reliable for authentication. Irises are internal organs but are visible from the outside, they are protected from the environment so well that they remain very stable. Compared to any other biometric authentication protocol, irises can vary the most, and are the most stable over time. Additionally, as a small planar object it is relatively insensitive to angle, pose or illumination and the small variation that does occur can be easily reversed [31]. There are downsides, however. The iris contains so much information that even body constitution, genetically inherited tendencies and weaknesses, health level and transitions in it during someone's life can be deduced from it. As such a powerful container of information it should be valued very highly, which also makes it a lot worse to lose [68].

Voice recognition, like face recognition, only works well on a very small sample group. Like face recognition it suffers due to limited consumer hardware, maybe even more because the public usually values the quality of their camera above the quality of their microphone. Additionally, a voice's pitch may change due to a user's mood, whim, age and environment. As such, it does pose less of a problem when lost. However, it is the easiest biometric feature to steal [26], as recording someone can be done relatively easily without being noticed.

Tokens are small hardware products used to authenticate a user. Tokens are one-time passwords using hardware and belong to the something you have category together with one-time passwords using software. They are expensive to the party that orders them, are often lost and usually only authenticate the user only when initiating the connection. This means that the connection can still be hijacked afterwards [80]. Tokens are very tamper resistant and employ special hardware that disable the token when a certain threshold of incorrect passwords is reached, or the token is tampered with (unprofessionally). Like biometric authentication there is not much the user can do in case of hardware failure. Additionally, because tokens are lost often there are cases of fake renewal petitions [65]. Because tokens are physical, they can be reverse engineered, cloned and spoofed. This however, is not easy and requires extensive knowledge [70].

One-time passwords, using software instead of hardware, think of authenticator apps on your phone, can be considered quite safe. The software generating the passwords often employs protection that makes it very hard to tamper with. However, there is one major vulnerability and that is the fact that the user or admin still needs a way to initiate the software and generate the password or list of passwords. When initiated from a compromised system, in case the list is stolen or the list is lost problems arise [80].

Another method of authentication is using GPS coordinates. This is probably one of the most insecure methods of authentication. An upside is that it is very fast. Those with malicious intent can go to the authorized locations, edit or spoof the GPS signal. Should not be used as a standalone authentication protocol and even in multi factor authentication does not provide that much of an increase in security [13,41].

Finally, one of the most used and weakest authentication protocols in existence are security questions. There are two kinds of security questions, the first are questions regarding sensitive information such as social security number, bank account or ATM pin codes. The second are personal questions about family history, pets or mother's maiden name. This kind of authentication shifts the responsibility of coming up with something secure to the designers of the questions. In addition, because the question determines what the answer should be this method is very vulnerable to all kinds of data mining and psychological attacks [74]. As we mentioned when we discussed the use of passwords, this authentication protocol is one of the greater weaknesses of a lot of authentication methods.

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Authentication protocol | [13,25,26,31,41, 42,48,49,65,68,70, 74,75,80,91,99] | Technical | An Authentication protocol is adamant to access control. Those with access have full control over cryptocurrency on exchanges, custodians and some wallets depending on if those wallets have the private keys of their users saved or not. There are various methods of authentication including passwords, pin codes, fingerprints, iris scans, face recognition, voice recognition, gps location and security questions. |

Table 4.4: CKPA authentication protocol

### 4.3.2 Encryption

| # | Title | Authors | Year | Source | Cites | Topic |
|---|---|---|---|---|---|---|
| [22] | Differential Cryptanalysis of the Data Encryption Standard. | Biham, E., & Shamir, A | 2009 | Springer Science & Business Media. | 1409 | The data encryption standard (DES) |
| [30] | The design of Rijndael: AES - the advanced encryption standard. Berlin: Springer. | Daemen, J., & Rijmen, V. | 2011 | Springer Science & Business Media. | 4854 | The advanced encryption standard (AES) |
| [77] | A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. doi:10.21236/ada606588 | Rivest, R. L., Shamir, A.,& Adleman, L. | 1978 | Communications of the ACM, 21(2), 120-126. | 20468 | RSA public key encryption |
| [14] | A Comparison of the 3DES and AES Encryption Standards. | Aleisa, N. | 2015 | International Journal of Security and Its Applications, 9(7), 241-246. | 23 | DES and 3DES |
| [34] | Quantum computation and Shor's factoring algorithm. | Ekert, A., & Jozsa, R. | 1996 | Reviews of Modern Physics, 68(3), 733. | 1647 | Quantum computation and possibilities |

Table 4.5: literature list of the technical perspective – encryption

Encryption is the process of encoding a message or information in such a way that only those that are authorized can access it. We will study and discuss the various standards of encryption in this section.

The first, and oldest standard is the Data Encryption Standard which was developed by IBM in the early seventies. In 1977 it was selected as an official standard for the United States, and as such was widely used. However, because of its small 56-bit key size it is no longer considered safe to use [22]. A more modern variant of DES is 3DES which basically employs the cipher three times. Although more secure, it was breached using consumer hardware in 2015 [14]. It is known to be one of the slowest encryption standards. It does have a strong point however, it is very fast when used with legacy soft and hardware because it is based on DES [14].

DES was superseded by the Advanced Encryption Standard (AES) which was developed in 2001 and is to this day considered safe. There have been some theoretic attacks but nothing with any practical use yet [30].

The last algorithm we studied is Rivest-Shamir-Adleman (RSA) which is known to be one of the slower encryption algorithms but has other uses. Because it is so slow it is not often used as an encryption algorithm but rather to decrypt shared keys in symmetric key cryptography which is used to encrypt the bulk [77]. RSA keys come in different bit sizes, and anything below 512 bits is known to be unsafe although it may cost a large amount of CPU power. RSA keys typically are between 1024 and 4096 bits which still makes them very secure [23]. However, many have voiced their doubts on the strength of these keys when quantum computing makes its entrance 73.

| Candidate key process area | References | Category | Rationale |
|---|---|---|---|
| Encyption | [6, 14, 22, 23, 30, 34, 77] | Technical | Encryption is another tool used in access control. With encryption messages and information can be encoded in such a way that only those with the right key or cipher can access it. However, encryption comes in different algorithms with varying levels of security. |

Table 4.6: CKPA encryption

### 4.3.3 Digital Signature

| *#* | *Title* | *Authors* | *Year* | *Source* | *Cites* | *Topic* |
|---|---|---|---|---|---|---|
| [77] | A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. doi:10.21236/ada606588 | Rivest, R. L., Shamir, A., & Adleman, L | 1978 | Communications of the ACM, 21(2), 120-126. | 20468 | RSA public key encryption |
| [62] | Digital Signature Standard. | Boneh D. | 2011 | Encyclopedia of cryptography and security. Springer Science & Business Media. | 508 | The digital signature standard (DSS) |
| [43] | The Elliptic Curve Digital Signature Algorithm (ECDSA). | Johnson, D., Menezes, A., & Vanstone, S. | 2001 | International Journal of Information Security, 1(1), 36-63 | 1236 | The elliptical curve signature algorithm (ECDSA) |

Table 4.7: literature list of the technical perspective – digital signature

Digital signatures are used to verify the authenticity of digital messages or documents, and that the message or document was not tampered with. RSA is used as a digital signature scheme as well as encryption. The up and down-sides are the same as they were when using the scheme for encryption.

DSS (Digital signature Standard) is based on DSA (Digital Signature Algorithm). DSA, like RSA is safe when using keys with enough bits and unsafe when using a small number of bits. DSA is signed with a random key, but if the key or a part of it is reused, leaked or predicable the whole signature key may be compromised. This characteristic is shared by ECDSA [62]. Also, like RSA, the algorithm may not be resistant to quantum computing.

ECDSA (Elliptical Curve Digital Signature Algorithm) is a variant of DSA using elliptic-curve cryptography. However, it needs less bits for the same security level as DSA. It suffers the same vulnerability in that its random signature key needs to be kept secret. Implementing the algorithm correctly should keep it so [43].

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Digital signature | [43, 62, 77] | Technical | Digital signatures function much like signatures in the real world. Their purpose is to prove that whoever is who he says he is, and that the information he sends has not been tampered with. In theory a hacker could alter information even if it has been encrypted. By adding a digital signature this would invalidate the digital signature, alerting stakeholders that their information has been tampered with. As is the case with encryption there are multiple algorithms used for digital signatures. Some are more secure than others. |

Table 4.8: CKPA digital signature

### 4.3.4 Hashing function

| # | *Title* | *Authors* | *Year* | *Source* | *Cites* | *Topic* |
|---|---|---|---|---|---|---|
| [76] | The MD5 Message-Digest Algorithm. | Rivest, R. | 1992 | MIT Laboratory for Computer Science. | 5546 | The MD5 hashing algorithm. |
| [33] | US Secure Hash Algorithm 1 (SHA1) | Eastlake, D., and P. Jones. | 2001 | The internet society | 1112 | The US secure Hash algorithm (SHA1) |
| [36] | "Security Analysis of SHA-256 and Sisters." Selected Areas. | Gilbert, Henri, and Helena Handschuh. | 2004 | International workshop on selected areas in cryptography (pp. 175-193). Springer, Berlin, Heidelberg. | 226 | Security of the SHA-2 family |
| [20] | Keccak specifications. | Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. | 2009 | Submission to nist (round 2), 320-337. | 91 | Specifications of the Keccak family of hashing algorithms. |
| [92] | MD5 considered harmful today, creating a rogue CA certificate. | Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A. K., Molnar, D., Osvik, D. A., & de Weger, B | 2008 | 25th Annual Chaos Communication Congress (No. EPFL-CONF-164547). | 125 | Weaknesses of MD5 (and older) hashing algorithm |
| [32] | Flickr's API signature forgery vulnerability. | Duong, T., & Rizzo, J. | 2009 | Tech. Rep | 16 | Example of an attack abusing weaknesses of MD5 |
| [18] | BLAKE2: simpler, smaller, fast as MD5. | Aumasson, J. P., Neves, S., Wilcox-O'Hearn, Z., & Winnerlein, C. | 2013 | International Conference on Applied Cryptography and Network Security (pp. 119-135). Springer, Berlin, Heidelberg. | 149 | Specifications of BLAKE 2 |

Table 4.9: literature list of the technical perspective – hashing

Hash functions are used to map data of arbitrary size on data of a fixed size. Values returned by a hash function are called hashes. Hash functions can be used to easily check if data maps to a given hash code, but that data cannot be constructed using the hash code. This is very useful when considering integrity of communication. In the past there have been competitions for the SHA-1, SHA-2 and SHA-3 hashing standards. The hash functions or family of hash functions that could be considered the best at that time won those competitions. When we talk about a hashing standard, we mean the hashing function that won the competition for that standard.

One of the earlier functions is MD5 (Message-Digest Algorithm 5). It was very widely used at the time and is still used by a lot of legacy software. MD5 is a hash function producing a 128-bit hash value and was designed to replace MD4 in 1991 (which replaced MD3 and so on) [76]. A basic requirement for cryptographic hash functions is that it is computationally infeasible to find two distinct messages which hash to the same value. With MD5 this can be done in seconds on a normal computer, meaning it is considered compromised and should not be used on any sensitive data [92].

SHA-1 (US Secure Hash Algorithm 1) is a cryptographic hash function that takes an input and produces a 160-bit or 20-byte hash value [33]. Since 2005 SHA-1 is no longer considered safe against attackers with sufficient funds. Considering computers have only gotten stronger since then attackers may not even need that much funds anymore [88].

SHA-2 (US Secure Hash Algorithm 2) is a family of hash functions with hash values that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 [36]. SHA-224, SHA-256, SHA-384 and SHA-512 are prone to length extension attacks and therefore insecure for some applications. It is recommended to switch to SHA-3 or SHA-512/224 or SHA-512/256 [32]. Finally, SHA-3 (US Secure

Hash Algorithm 3) is internally very different from SHA-1 and SHA-2 which are a lot like MD5. SHA-3 is based on the Keccak cryptographic family. It is the newest standard and comes in varying bit sizes just like SHA-2 [20].

Two other notable hashing functions are BLAKE and BLAKE2. BLAKE was submitted to the competition for the SHA-3 standard, it lost to the current SHA-3 standard Keccak [17] in the finals but should still be considered more secure than SHA-2.Blake 2 is supposed to be faster than MD5, SHA-1, SHA-2 and SHA-3 on 64-bit architectures while boasting security higher than SHA-2 and on par with SHA-3 [18].

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Hashing function | [17, 20, 32, 33, 76, 82, 88, 92] | Technical | Hash functions map data of arbitrary size on data of a fixed size and is mostly used to validate the integrity of communication. There are various hash functions with varying levels of security. |

Table 4.10: CKPA hashing function

### 4.3.5 Social hacking or social engineering

| *#* | *Title* | *Authors* | *Year* | *Source* | *Cites* | *Topic* |
|---|---|---|---|---|---|---|
| [52] | Social engineering: The neglected human factor for information security management. | Luo, X., Brody, R., Seazzu, A., & Burd, S. | 2011 | Information Resources Management Journal (IRMJ), 24(3), 1-8. | 80 | Social engineering, instruction |
| [67] | The vishing guide. | Ollmann, G. | 2007 | http://www. infosecwriters. com /text resources/pdf/IBM ISS vishing guide GOllmann. pdf, IBM, Tech. Rep. | 9 | Vishing, instruction |
| [46] | Advanced social engineering attacks. | Krombholz, K., Hobel, H., Huber, M., & Weippl, E. | 2015 | Journal of Information Security and applications, 22, 113-122. | 239 | Social engineering, instruction |
| [61] | A taxonomy for social engineering attacks. | Ivaturi, K., & Janczewski, L. | 2011 | International Conference on Information Resources Management (pp. 1-12). Centre for Information Technology, Organizations, and People. | 91 | Social engineering attacks |

Table 4.11: literature list of the technical perspective – Instruction

Social hacking, or social engineering, is the psychological manipulation of people into revealing their confidential information or gaining access to it. We will now shortly discuss the most important techniques and their characteristics.

The first technique is called pretexting and is often defined as follows; “Pretexting is the act of creating and using a contrived scenario to persuade a potential victim to voluntarily reveal information or perform actions [52].” Think of someone posing as security, a helpdesk employee, a company’s administrator and such, asking their target for confidential information such as passwords, email addresses, phone numbers and bank accounts.

The second technique, phishing, is the most popular technique these days and is defined: “Phishing, is a two-time scam technique of fraudulently obtaining private information. Typically, the attacker sends a masqueraded e-mail that appears to originate from a legitimate business, such as a bank or credit card company, requesting “verification” of information and warning of some significant consequences if it is not in accordance with the request [52].” Think of e-mails from Apple, Google, Microsoft, your bank or your work with an attached file or link with an interesting name. People tend to click the link or open the attached file because the name triggers their curiosity without checking the e-mail address it was sent from. Really good phishing e-mails or letters are almost identical to the original.

Vishing is like phishing but uses the phone. “Vishing is the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward. The term “vishing” is derived from a combination of “voice” and “phishing ” [67]. Examples here are calls from Microsoft or Apple from an Indian or African caller (Vishing is a popular means of income in those countries) who tells you there is something wrong with your computer. This problem can be fixed by going to a site they provide or downloading some software. Sometimes they will use a robot caller, where you need to press numbers because this adds a measure of fake security for some people.

One of the most dangerous techniques is called spear-phishing. “Spear-phishing attacks are highly targeted messages carried out after initial data-mining [46].” Criminals will contact their target with pre data-mined information, which they can smartly leverage in such a way that they are hard to distinguish from legitimate. Examples are e-mails from work, the bank, or something else you frequently receive e-mails from, on the exact time or date that you would expect such an e-mail looking precisely the same as the legitimate version. The danger is in this likeliness, as even the most careful people do not double check every e-mail they receive.

A lesser-known technique is water holing, which can be defined as follows; “Describes a targeted attack where the attackers compromise a website that is likely to be of interest to the chosen victim. The attackers then wait at the waterhole for their victim [46].” Examples of water holing are when those with malicious intent for instance compromise an e-mail provider or a website’s database. They then lie in wait until they find their targets.

The next technique, called baiting, requires storage media which is the ‘bait’. “Baiting is an attack during which a malware-infected storage medium is left in a location where it is likely to be found by the targeted victims [46].” Criminals will leave CD’s or USB’s with titles that may bait their target into inserting the media into their device, which will compromise it.

The next attack makes use of the psychological phenomenon called “quid pro quo” which means give and take. “The attacker presents himself as a person in a perceived position of authority which influences the victim to ask more questions instead of the attacker. The orchestration of such an attack usually spans three stages which are sabotage, advertising and assisting [61].” This is different from phishing in the sense that the criminal often offers something, like a professor, IT service desk or the police, who offer assistance, money or a free pen or chocolate bar, in exchange for some information. In the past studies have proven that humans are very susceptible to small rewards in return for valuable information.

And finally, the simplest of techniques; “Tailgating simply means following a person with authorized entry into a secure area, basically riding on coattails (Long, 2008). The act may be considered to be legal or illegal depending on the circumstance but in general this term has a negative connotation and is used to describe an illegal act [61].” Someone with malicious intent may just follow or walk in between real employees and gain entry to a company that way.

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Instruction | [46, 52, 61, 67, 83, 87, 90] | Preventive | Instruction is one of the few effective ways to deal with social engineering threats. Social engineering relies on psychological tricks that abuse the way the human brain tends to function and make decisions. All the automated security in the world does not help if the user himself (unknowingly) grants access to those with malicious intent. |

Table 4.12: CKPA instruction

## 4.4 Attacker perspective

In this section we look at the vulnerabilities that have been abused in the past, to learn from them.

One of the first, and largest, cryptocurrency heists in history was the first Mt Gox Heist in 2011. Most likely criminals were able to gain entry to the system by compromising the personal computer of an auditor working for the company [6]. The second time was because before 2011 the private keys of some of the hot wallets belonging to the company were unencrypted and stored in their database. Those files were stolen either by an insider, or by a hacker who gained access [6]. This happened to Bitfloor in 2012 as well. In 2016 hackers gained access to one of the servers of Gatecoin by overloading the server and forcing it to restart, the wallet files on the server were unencrypted.

Webhosts proved to be another point of failure in 2012, when hackers gained access to the server of Bitcoinica in 2012 through the webhost [38]. Something similar happened to Vicurex in 2013, when hackers used a ruby-on-rails attack to gain access to the VPS control system of Vicurex. With these login credentials they managed to gain the trust of the helpdesk of the web server, which complied to their request of resetting the login credentials to the server [8]. Bitcoinica was unfortunately not spared, because hackers managed to abuse the “forgot your password” option of the admin login to the server to break in a second time [39].

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Webhost | [6, 8, 38, 39] | Preventive | Webhosts can prove to be a point of entry for some websites and their databases. A webhost can be well protected against attacks such as DDoS, provide continuous uptime, employ professional well-trained staff and strict protocols when it comes to security. Another webhost may not provide these things, or to a lesser extent which has a negative impact on security. |

Table 4.13: CKPA webhost

In 2014 Cryptorush was one of the first exchanges to break down due to a bug in a shady altcoin, which allowed users to withdraw funds they did not have [78]. Something similar happened to Poloniex in 2014, although the bug this time was on the exchange’s side. Users could make multiple withdrawals at the same time [78]. The Geth platform was also victim to an abused bug. “Geth is one of the most popular clients for running the Ethereum node. Its JSON-RPC interface allows users—and thieves—to remotely access the Ethereum blockchain and node functionalities, including the ability to send transactions from any account which has been unlocked before sending a transaction. Once unlocked, however, the port stays opened for the entire session. The unwitting victims had opened their JSON-RPC port 8545 to the outside world, allowing hackers to breach their Ethereum wallets [1].” Another instance of a bug causing a lot of damage happened in 2018. The parity wallet service functioned like a smart contract. Then a bug in the smart contract was triggered, effectively freezing 150 million in Ethereum [81].

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Active devvelopment | [1,6,8,38,39,78,81] | Preventive, technical, trust | Active development is very important when it comes to keeping up with the latest technology, and fixing bugs before they can be abused. |
| Open source | [1,6,8,38,39,78,81] | Preventive, trust | When developing as open source the idea is that more eyes are always better when it comes to prevent, locate and fix bugs and vulnerabilities |

Table 4.14: CKPA active development & CKPA open source

In 2014 the CEO of Bitpay was phished into giving his e-mail credentials. With these credentials the attacker sends out requests for Bitcoin to his own address. [90] Another case of (spear) phishing is that of Bitstamp in 2015. An email to a system administrator about a membership form was opened, this malicious file downloaded malware and breached the computer. Ultimately this allowed the attackers access to two wallet files stored on the server [83].

In 2015, one or more hot wallets belonging to Bitstamp were compromised. The attackers were able to compromise the wallets presumably because the company re-used the random value in its ECDSA hashing algorithm [82].

A notable vulnerability is the Bitcoin Gold attack of 2018. “BitCoin Gold was compromised by a “51 percent attack” in which the hackers apparently employed rented computers to achieve this previously theoretical type of cyberattack. These attacks occur when one entity gains control over more than 51% of the network hash-rate. Then, the successful attacker can not only prevent valid transactions from occurring but also reverse previously completed transactions on the blockchain. This degree of control even enables a single coin to be spent twice from the same origin—a so-called double-spend attack like the thefts that occurred on Bitcoin Gold. This attack netted thieves in excess of $18 million. Possibly the blame for the Bitcoin Gold trouble lies with the fact that it uses the Proof of Work (PoW) consensus protocol of Bitcoin in a small pool to create distributed trustless consensus [1]”.

Javascript cryptography is something we have seen discussed in several places as well. Websites that use Javascript to handle cryptography and secure login and other confidential services, should be handled with care. Although the cryptography of Javascript can be sound, Javascript cannot be delivered to the user without trusting the server. This means that, techniques like water holing would still be effective [72]. Another problem in Javascript which is discussed often are the npm packages used. In theory it’s very hard to check the dependencies of widely used npm packages. Some may depend on other npm packages, which in turn depend on other packages. In the end one of these packages may be compromised, allowing someone to load their malicious code on widely used websites [37].

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Javascript cryptography | [37,72] | Technical | Using Javascript cryptography undermines the security it is supposed to provide. |

Table 4.15: CKPA javascript cryptography

In 2018 1.7$ billion dollars in cryptocurrencies were stolen and scammed [87]. Of that 1.7 billion hackers stole 950 million from cryptocurrency exchanges and infrastructure which is 3.7x more than in 2017. Of those 950 million most were stolen by inside jobs and scams rather than hacks on exchanges and wallets. Apparently, the new breed of cybercriminals finds it easier to make use of unwitting investors and users than attacking hardened security systems.

Ciphertrace, a company specialized in tracking cryptocurrency theft and money laundering has publicized a list of the 10 biggest crypto threats at the moment, we will discuss the crimes in the list relevant to security shortly [87].

1. **Sim swapping:** An identity theft technique that takes over a victim's mobile device to steal credentials and break into wallets or exchange accounts to steal cryptocurrency. The crime at number one of this list makes use of the vulnerability in 2FA using SMS. By Sim swapping criminals can receive these SMS messages instead of the actual recipient.

4. **Next-Generation Crypto Mixers:** Money laundering services that promise to exchange tainted tokens for freshly mined crypto, but in reality, cleanse cryptocurrency through exchanges. Crypto Mixers will not be allowed in countries with more regulation and legislation.

5. **Shadow Money Service Businesses:** Unlicensed Money Service Businesses (MSBs) banking cryptocurrency without the knowledge of host financial institutions, and thus exposing banks to unknown risk. With the risk that the service goes bankrupt and users lose their money. This is another reason why users should always control their own cryptocurrency.

9. **Email Extortion and Bomb Threats:** Cyber-extortionists stepped up mass-customized phishing emails campaigns using old passwords and spouse names in 2018. Bomb threat extortion scams demanding bitcoin spiked in December. These threats make use of phishing techniques. It also points out that it is important to protect your user data on the internet.

10. **Crypto Robbing Ransomware:** Cyber-extortionists began distributing new malware that empties cryptocurrency wallets and steals private keys while holding user data hostage. With these new kinds of crypto robbing ransomware, it is even more important to protect your device.

From what we have read on the vulnerabilities and crimes concerning cryptocurrency in this day and age it seems very important to protect your user data on the internet. Problems arise when they know: 1) if, and how much, cryptocurrency is owned, 2) phone number, 3) e-mail address, 4) ip-adress, 5) residential address, 6) first name, 7) last name, 8) date of birth and other personal information.

Users are considerably safer when it comes to social hacking and security hacking techniques, such as spear-phishing, sim-swapping and bomb threats. This responsibility is one shared by the user, but also by cryptocurrency exchanges wallets and custodians. They should protect your data as much as they can. From the vulnerabilities we have learned that encryption and hashing of data on servers is important, but those two are already CKPA's. We have also learned that webhosts can be a weakness. We have also learned that regulation and legislation is important when it comes to security, but we will further analyze and discuss the regulation and legislation in the next section.

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Secure database management | [6, 71, 87, 90] | Technical | The balance between security and usability in databases has been a problem for a long time. Making a database watertight makes it nigh unusable, while maximizing t usability will result in a vulnerable database. When it comes to information as sensitive as user data, public and private keys and wallet.dat files the security needs to be on the more secure side. This can be achieved by other proposed key process areas such as encryption, authentication protocols, hashing and digital signatures. But also depends on how the database is managed, structured and layered. |

Table 4.16: CKPA secure database management

The problem with databases is, however, as is described by Ross J. Anderson [71]; "By their nature large databases will never be free of abuse by breaches of security; if a large system is designed for ease of access it becomes insecure; if made watertight it becomes impossible to use". We have established that a database is hard to protect. If user data is so hard to protect, not collecting it at all is the best way to protect your users.

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Collection of user data | [6, 71, 87, 90] | Preventive | Collection of user data is about the extent of the KYC protocol in place. VCEPs in some countries are legally obligated to have an extensive KYC protocol. CWPs and WPs are not. User data such as name, address, phone number and e-mail address in combination with the fact that the user in question has cryptocurrency is very sensitive information. If databases cannot be made secure, collecting less user data is the only way to prevent this from happening. As such we consider extensive KYC protocols insecure, while no or little KYC is more secure. |

Table 4.17: Collection of user data

Another vulnerability we discussed was the 51% attack on Bitcoin Gold, and the bug in the shady altcoin of Cryptorush. Apparently, cryptocurrency exchanges should closely monitor the cryptocurrencies they support in order to avoid these attacks.

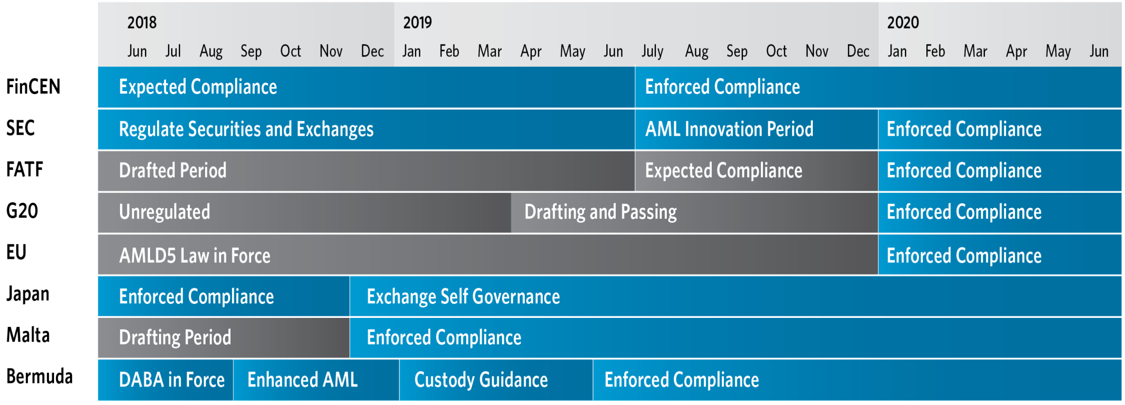
| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Monitoring of supported cryptocurrencies | [1, 78, 87] | Preventive | A lot of money in the cryptocurrency ecosystem is stolen by scams. Some of these scams make use of alt coins developed for that purpose or those that have been compromised. In order to protect the wallet itself and the users there should be competent monitoring of supported cryptocurrencies |

Table 4.18: CKPA monitoring of supported cryptocurrencies

Finally, we have learned from the literature that a large amount of the stolen money is due to inside jobs and hacks. This means that hackers focus on places where they can steal a large amount of cryptocurrency in one go. These places are exchanges and custodians who keep cryptocurrencies for multiple users. Wallet services, the software and hardware variants (not the hot wallets) have no control over their user's private keys, and as such, their cryptocurrency. This alerts us to a very important difference.

## 4.5 Governance perspective

Since the inception of cryptocurrencies legislation has been trying to catch up, and every year there have been important new rulesets for cryptocurrencies and companies handling them. Because legislation has a big impact on virtual currency exchange platforms (VCEPs) and custodian wallet providers (CWPs) we look at the different set of rules worldwide and what those rules mean to the public [5, 12, 86, 87].



Source: CipherTrace Cryptocurrency Anti-Money Laundering Report Q4 2018

Figure 4.6: AML legislation rollout 2018-2020

This year the fifth European Anti Money Laundering Directive (AMLD5) has been drafted and will start being enforced with complete enforced compliance in 2020. The fifth version increases its scope so that VCEPs and CWPs are now “obliged entities” and are now subject to the requirements of the AML legislation.

AMLD5 requires all member states of the European Union to enforce mandatory registration of VCEPs and CWPs and report any and all suspicious activity occurring on said platforms. The ruleset also includes much stricter rules in diligence when it comes to business relationships with clients from high-risk jurisdictions, which includes inquiring more information on the client, the sources of their funds and wealth.

Additionally, AMLD5 grants Financial Investigation Units (FIUs) access to information held by VCEPs and CWPs regardless of whether these entities have submitted suspicious reports or have requested investigation.

Second, AMLD5 states that member states should create a central database with user identities and wallet addresses. These databases should also grant direct access to FIUs. It is not clear how enforcement on this matter will take place and if this is possible. In the United States new AML legislation will be enforced starting in the third quarter of the year. In addition to the ruleset that will be enforce in the EU, the United States have included anonymizing services such as mixers and tumblers.

The United States’ Securities and Exchange Commission (SEC) is taking steps in regulation for ICOs as ICO-derived tokens can be seen as a form of securities. An example of this is EtherDelta, the SEC took regulatory actions against the company because of the way it used smart contracts. According to the SEC the company was using the blockchain to run an unregistered, and thus illegal, securities trading platform.

The Financial Action Task Force is a globally operating task force advising 36 member states and two regional organizations. It is one of the most influential voices globally when it comes to combating financial crimes. Although technically a policymaking body, the FATF also act as watchdogs in the progress of implementation of AML techniques in the member states. They also report on deficiencies of AML in countries and provide a bi-annual blacklist of high-risk countries.

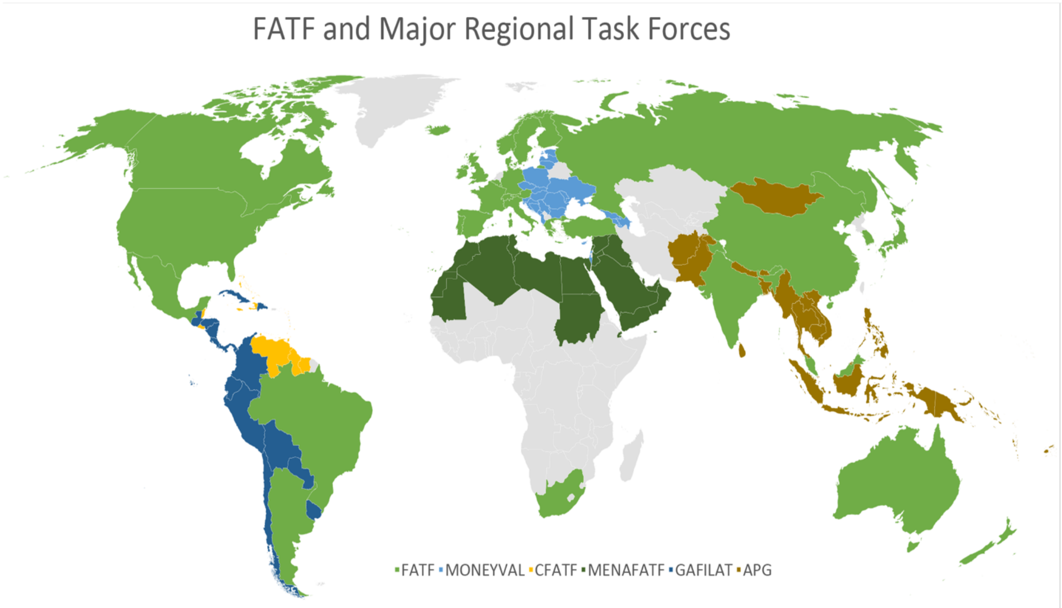

FATF and Major Regional Task Forces
▪FATF ▪MONEYVAL ▪CFATF ▪MENAFATF ▪GAFILAT ▪APG

Figure 4.7: Coverage of major financial task forces worldwide

With the new AMLD5 of the EU, G-20 member states have asked the FATF for recommendations on legislation comparable to AMLD5. Below is the map with the countries currently deemed to be high-risk by the FATF.

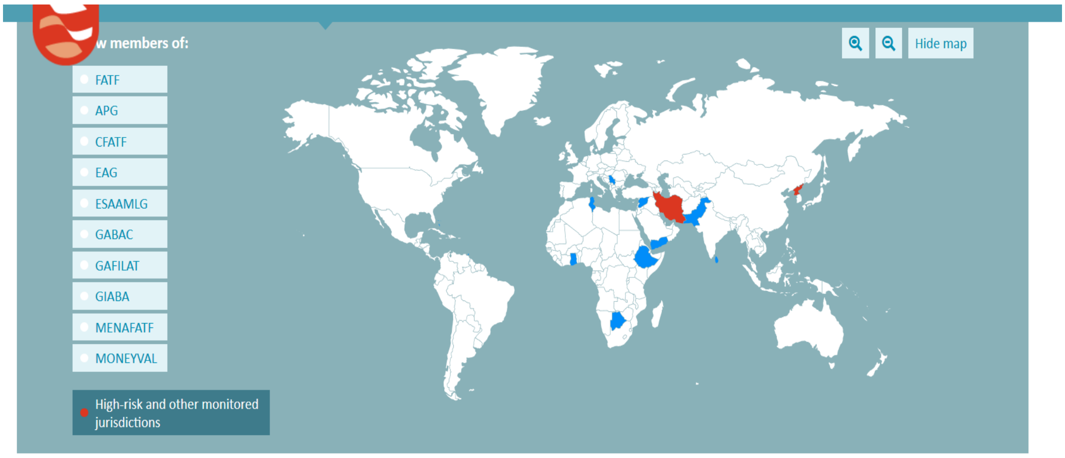


Figure 4.8: Countries on the FATF blacklist

| *FATF blacklisted countries 2019* | |
|---|---|
| Botswana | Syria |
| Ghana | Republic of Serbia |
| Ethiopia | Iran |
| Yemen | Pakistan |
| Tunisia | Sri Lanka |
| North Korea | |

Table 4.19: FATF blacklist 2019

Bermuda is taking steps to progress to a major crypto island. It has recently developed a regulatory framework with new cybersecurity rules, Digital Asset Business (DAB, client disclosure) rules, Digital Asset (DA) rules and a Digital Asset Business Code of Practice (DABCP). Additionally, Bermuda is the leader of the Caribbean Financial Action Task Force (CFATF). With its new regulatory framework Bermuda is one of the few countries in the world with comprehensive legislation including not only VCEPs and CWPs but also ICOs, payment service providers using digital assets and market makers/dealers/traders of digital assets.

Malta was the first country to implement a holistic regulatory framework for the blockchain and cryptocurrency space. It consists of 3 laws:

I. The Malta Digital Innovation Authority (MDIA) Act - Allows for the formation of the Malta Digital Innovation Authority, which focuses on not only regulation but also promoting the country's crypto economy.

II. The Innovative Technology Arrangements and Services Act (ITASA) - Provides legal clarity on many aspects of blockchain technology to help developers certify the quality and governance of blockchain technology used by companies who seek the approval of domestic operation.

III. The Virtual Financial Assets Act (VFAA) - Provides a regulatory structure for all entities that handle virtual financial assets, including Security Token Offerings (STOs). It includes a test to determine whether an offering constitutes a security.

Notably, this new regime imposes AML more strictly than AMLD5 does.

Canada is currently drafting its AML and KYC ruleset. The current ruleset does not impose AML rules on companies that do not do one of the following three activities:

i. Foreign exchange

ii. Money transferring

iii. Issuing/redeeming money orders or other similar instruments

This has created an environment in which some companies are being regulated while others are not. With the new AMLD5 coming into view Canada as part of the G-20 has requested the FATF for a more comprehensive ruleset, which should be implemented by 2020.

The United Kingdom has announced that it will implement AMLD5 but will go further. Part of the plan for tougher AML/CFT regime includes strict regulation of the following:

- Exchange services between different cryptoassets, to prevent anonymous 'layering' of funds to mask their origin
- Platforms that facilitate peer-to-peer exchange of cryptoassets, which could enable anonymous transfers of funds between individuals
- Cryptoasset ATMs, which could be used anonymously to purchase cryptoassets
- Non-custodian wallet providers that function similarly to custodian wallet providers

Japan has announced that it has granted the Japan Virtual Currency Exchange Association (JVCEA) the right to self-regulate and implement and enforce AML rules. The JVCEA is made up of all registered exchanges of Japan, in addition to five more companies that handle virtual currency related services such as wallet dealers.

Korea is home to the strictest AML and KYC rules in the world, but there are some controversies. For instance, the government banned the use of privacy-coins such as Monero, and yet South Koreans are the owners of 83% of Monero coins.

| *Candidate key process area* | *References* | *Category* | *Rationale* |
|---|---|---|---|
| Governance | [1, 5, 12, 73, 86, 87] | Governance & Legislation | Not every country in the world has the same quality of governance. Without proper governance companies in the cryptocurrency ecosystem are not regulated to the extent where investments could be considered secure. |
| Legislation | [1, 5, 12, 73, 86, 87] | Governance & Legislation | Legislation in most of the world is still catching up on legislation regarding the cryptocurrency ecosystem. There are a few countries where the legislation is advanced much further than others. There are also differences in the legislation. Even most of the newer legislation is mostly focused on VCEPs but not on CWPs and WPs. |

Table 4.20: CKPA governance & CKPA legislation

## 4.6 Candidate key process area shortlist

Below is the initial Candidate Key Process Area shortlist constructed based on potential key process areas we have discovered in our literature reviews. We started with feature modelling existing safekeeping solutions. With knowledge on safekeeping soltions we used those keywords to search for information on the parts that together make a safe-keeping solution as well as inspecting other perspectives of influence such as legislation and crime. Whenever we discovered a proess area in the literature list we constructed we added it to the candidate key process list (table 4.21). We will use this CKPA shortlist in our semi-structured interviews with professionals. After the interviews we will decide on the action and rating of the CKPAs.

| *#* | *CKPA* | *References* | *Category* | *Action* | *Rationale* | *Rating* |
|---|---|---|---|---|---|---|
| 1 | Authentication methods | [13,25,26,31,41, 42,48,49,65,68,74, 75,80,91,99] | Technical | tbd | Authentication protocols are one of the most important tools in access control. | tbd |
| 2 | Encryption | [14,22,23,30,34,77] | Technical | tbd | Literature suggests that encryption is important to keep files safe even when the server is breached | tbd |
| 3 | Digital signature | [43,62,77] | Technical | tbd | A digital signature is useful when communicating sensitive information. The algorithm used and the implementation influence how much security a digital signature can provide. | tbd |
| 4 | Hashing function | [18,20,32,33,36, 76,88,92] | Technical | tbd | Hashing, like encryption can increase security when implemented correctly. | tbd |
| 5 | Instruction | [46,52,61,67] | Preventive | tbd | One of the only, and certainly the most effective way of dealing with social engineering. | tbd |
| 6 | Active development | [1,78,81] | Technical & preventive | tbd | In order to solve bugs, and repair vulnerabilities development needs to be relatively active. | tbd |
| 7 | Open source | [1,6,8,38,39,78,81] | Trust | tbd | Open source increases the speed bugs and other mistakes can be detected and solved as well as increasing the trust. | tbd |
| 8 | Secure database management | [6,71] | Technical | tbd | Making databases secure while keeping them usable has proven to be a challenge to many. | tbd |
| 9 | Javascript cryptocurrency | [37,72] | Technical | tbd | tbd Using Javascript cryptography is inherently not secure. | |
| 10 | Collection of user data | [71] | Preventive | tbd | Lost user data can compromise the anonymity of users. Without anonymity users can come under attack of more dangerous techniques used by hackers and social engineers. | tbd |
| 11 | Webhost | [1] | Technical | tbd | A webhost hosts multiple websites and can grant admin rights over the websites it hosts. If their security protocol for doing so is not secure those with malicious intent may use a webhost to gain entry to one of the hosted websites such as a cryptocurrency exchange. | tbd |
| 12 | Monitoring of supported cryptocurrencies | [1,78] | Preventive | tbd | There are thousands of altcoins, some of them shady or bugged. | tbd |
| 13 | Distribution of power | [1,4,5,9,11,12,15, 28,73,86,87] | Distribution of power | tbd | Who controls the cryptocurrency is detrimental in keeping it secure. | tbd |
| 14 | Legislation | [1,5,12,73,86,87] | Governance & Legislation | tbd | Legislation is important to the whole ecosystem of cryptocurrencies. | tbd |
| 15 | Governance | [1,78,87] | Governance & Legislationl | tbd | Governance, like legislation, is very important to the ecosystem of cryptocurrency. | tbd |

Table 4.21: Collected CKPAs

# Chapter 5

# Expert Evaluation

Having constructed a list of candidate key process areas from literature we proceeded to validating that list with some experts in the fields of cryptocurrency, security and risk modelling. The list of CKPAs was used in the semi-structured interviews. In the interviews we discuss the CKPAs found in literature. The expert is asked how important he thinks the CKPA is, the way it should be measured and if he/she has other CKPA's he/she thinks should be added.

After discussing the CKPA with the expert we rate the CKPA. Rating is based on the opinion of the expert and found literature. CKPAs that are adamant to security are rated ++ for more important, important +, neutral +/-, less important - and unimportant –. Ratings are based on the direct importance of the CKPA on security. Although CKPAs with a – rating have a small direct impact on security, they may have an indirect one that is still not to be overlooked.

Finally, we decide what action we will take. CKPAs we nominated, discussed, rated and found to have a) an impact and b) are within the realm of measurability, are retained. CKPAs we have not discovered in literature but were suggested by experts are added. CKPAs that are found to a) have no impact or b) are unmeasurable are removed.

We have performed 8 interviews, 5 in which the expert stated that they do not possess the necessary knowledge on the combination of fields required to evaluate the model or had nothing to add to that iteration of the model. These interviews have been added to the mass evaluation instead of the expert evaluation. The interviews have been recorded. With the three experts that were proficient on the subject we kept in touch. Whenever we introduced a new iteration of the model they were asked for their opinion. We also had contact with the Korean Internet and Security Agiency which at the time of writing is the only government agiency that has audited crypto-asset providers on security. Unfortunately we ran into problems aside from the language barrier when the KISA was unable to release the list of qualities it judged providers on as it was classified at this moment. Finally, we also had little luck contacting international providers as their communication channels usually got us stuck in tech support but not in contact with someone knowledgeable on our subject.

The first expert we talked with had worked in security for over 10 years at ING, a large bank in the Netherlands. He had also been a member of the cryptocurrency team for 4 years, until the team was disbanded.

The second expert used to be a programmer but started working on wallet software and finally became a cryptocurrency consultant. At the time we spoke to him he had been in his current function of cryptocurrency consultant for three years.

The third, and final, expert used to be the head of strategy and the head of risk at ABN Amro, another big bank in the Netherlands. His expertise in strategy, risk modelling and management counted over 40 years and he had personally led some of the ABN Amro cryptocurrency teams.

Below is the CKPA shortlist with the added CKPA's communication and customer service under the category trust. Rationales have been updated with expert opinion and a rating on importance from all experts has been added.

| *#* | *CKPA* | *References* | *Category* | *Action* | *Rationale* | *Rating* |
|---|---|---|---|---|---|---|
| 1 | Authentication methods | [13, 25, 26, 31, 41, 42, 48, 49, 65, 68, 74, 75, 80, 91, 99] | Technical | Retain | Literature suggests that authentication is one of the most important factors of security. Experts agree. Authentication protocols are what access control hinges on. | ++ |
| 2 | Encryption | [14,22,23,30,34,77] | Technical | Retain | Literature suggests that encryption is important to keep files safe even when the server is breached. Important to have some encryption according to experts, but simply usually not the weakest link. | – |
| 3 | Digital signature | [43, 62, 77] | Technical | Retain | According to literature using a faulty or weak signature standard can be a vulnerability. All communication over the blockchain is usually signed with ECDSA. However not every service implements it correctly which hurts its safety. Like encryption and hashing less important than other categories simply because it usually is not the weakest link. | – |
| 4 | Hashing function | [18, 20, 32, 33, 36, 76, 88, 92] | Technical | Retain | Hashing, like encryption can increase security when done right. According to experts hashing is mostly used for passwords and seed phrases. Usually not the weakest link. | – |
| 5 | Instruction | [46, 52, 61, 67] | Preventive | Retain | One of the only ways to prevent social engineering. Experts agree with importance and lack of instruction on a lot of services. Important, but not as important as basic security. | + |
| 6 | Active development | [1, 78, 81] | Technical & preventive | Retain | In order to solve bugs, and repair vulnerabilities development needs to be up to date. Experts strongly agree, lack of development over a longer period could be compromised. | ++ |
| 7 | Open source | [1,6,8,38,39,78,81] | Trust | Retain | Literature suggests that open source can increase security and trust. Experts agree but add that the number of developers that commit should also be looked at. | + |
| 8 | Customer service | [87] | Trust | Add | Depends on the problem. Not usually very important when it comes to security but does help in optimizing a service and trust. | –– |
| 9 | Communication | [87] | Trust | Add | Without communication users can not know what the company is planning. Depends on the case if it has impact on security. Has impact on trust. | +/– |
| 10 | Javascript cryptography | [37, 72] | Technical | Remove | We have no way of knowing which web languages were implemented and in what manner. Neither do we possess the expertise to judge what security they offer precisely enough. | +/– |
| 11 | Secure database management | [6, 71] | Technical | Remove | There is no way to find out how a company manages their database without consulting the company. | ++ |
| 12 | Collection of user data | [71] | Preventive | Retain | Lost user data can be very dangerous to users. Experts agree and think it very important. Not only is it dangerous to users if information is lost, but also to build trust with userbase. | ++ |
| 13 | Webhost | [1] | Technical | Remove | No way to find out what webhost a service uses without consulting them. | + |
| 14 | Monitoring of supported cryptocurrencies | [1, 78] | Preventive | Remove | There are thousands of altcoins, further research needed. | – |
| 15 | Distribution of power | [1, 4, 5, 9, 11, 12, 15, 28, 73, 86, 87] | Distribution of power | Retain | Who controls the cryptocurrency is very important according to literature. Experts strongly agree. | ++ |
| 16 | Experimental | [60] | Experimental | Retain | Experimental security options can be added to increase security but may be in development or very specific. Process area allows for future developments in the field. Experts unsure about name of the category, but do not know what else to call it. | –– |
| 17 | Legislation | [1, 5, 12, 73, 86, 87] | Governance & Legislationl | Retain | Legislation is important to the whole ecosystem of cryptocurrencies. Experts strongly agree. | ++ |
| 18 | Governance | [1, 5, 12, 73, 86, 87] | Governance & Legislationl | Retain | Governance, like legislation, is very important to the ecosystem of cryptocurrency. Experts strongly agree, but think governance is slightly more important than legislation because legislation depends on governance. | ++ |
| 19 | Network transmission security | | Technical | Remove | Brought up by multiple experts. Wallets should transmit their information server side using the HTTPS protocol. Additionally, wallets should scan the legitimacy of digital certificate in the user library in order to secure the communication routes. This prevents Man in the Middle attacks. Removed because this information is not available to investigation without inside knowledge. | + |

Table 5.1: Collected CKPAs

# Chapter 6

# The crypto-asset safekeeping security maturity assessment model (CSSMAM)

Capabilities are generally categorized as: A = None/worst, B = Some/average, C = Complete/good. In some cases, however, this rule of thumb does not apply. We will explain the categorization in those cases.

## 6.1 Level one : Unsafe

Capabilities at the first level of maturity are governance A, active development A and authentication protocol A.

Governance A, the first capability level of governance concerns the countries that the Financial Action Task Force (FATF) has blacklisted. Countries on this blacklist are non-cooperative in the fight against money laundering and anti-terrorism financing [12]. Countries on this list are unlikely to act if a VCEP, CWP or WP takes part in illegal activities. As such we consider trusting companies based in these countries with crypto-assets to be extremely unwise. Countries currently on the FATF blacklist are Botswana, Ghana, Ethiopia, Yemen, Tunisia, Syria, Republic of Serbia, Iran, Pakistan, Sri Lanka and North Korea.

Active development A, the first capability of active development concerns the last time the provider has updated its service. A lot of crypto-assets have been lost or stolen over time due to bugs [1,6,8,38,39,78,81]. Without a team of developers actively developing and updating the service these bugs can be abused. We consider services that have had no updates longer than a year to be very unsafe.

Authentication protocol A is granted to any service with lacking or no authentication protocol in place. If a service has no authentication protocol any party with malicious intent may steal the crypto-assets if they somehow gain access to the device or private keys. We have also assigned location-based authentication to A. The party with malicious intent could steal any crypto-assets on location or spoof their location to match the investor's. Spoofing a GPS location is a simple trick [41].

## 6.2 Level two : Unsafe

The second maturity level has two capabilities assigned to it; authentication protocol B and Legislation A.

The authentication protocols we consider a little bit safer, but still unsafe, than those assigned to A are face recognition and voice recognition [26,42,65,75]. Face recognition is vulnerable to replay attacks [47,91]. A replay attack on facial recognition means that an unauthorized party unlocks the service by using a captured image of the face belonging to the investor. Some facial recognition software can be fooled this way. These pictures can often be found on the internet relatively easily. Additionally, face recognition technology can sometimes be fooled with a face that looks alike. Voice recognition suffers from the same problem as face recognition as the technology is just as vulnerable, or even more vulnerable to a replay attack. A voice may be harder to find on the internet but can be easily recorded. A high-quality recorded voice is hard for voice technology to discern from an actual voice. Voice recognition may sometimes incorrectly pass a voice not belonging to the owner.

Legislation A covers the same countries as governance A, countries without cryptocurrency legislation and blacklisted by the FATF [12]. Because there are no countries on the FATF blacklist who do have specialized cryptocurrency legislation the list of countries assigned to this capability is identical to the list of governance A. The countries are Botswana, Ghana, Ethiopia, Yemen, Tunisia, Syria, Republic of Serbia, Iran, Pakistan, Sri Lanka and North Korea. Legislation A has been assigned a maturity level higher that governance A because without governance legislation does not matter, making it slightly more important.

## 6.3 Level three : Lacking

Capabilities assigned to the third maturity level are active development B, communication A and governance B.

Active development B is assigned to a service if it has not been updated in the last six months to a year. This window of time is smaller than that belonging to active development A, which means there has been less time for technological advances to create bugs and for those with malicious intent to find existing bugs and abuse them. The time windows however, is still relatively large and any service that has not been update longer than half a year should be considered lacking in safety.

Capability A of communication is assigned to a service if the company or group of developers does not communicate at all. Without communication users have no way of knowing what the company is working on, if forks are supported or not, if a cryptocurrency is going to be delisted, when trading is stopped or frozen and so on. No communication is not only suspicious but also very risky to an investor which is why this capability was assigned to maturity level three.

Governance B covers the countries in the world where there is some governance allowing investors to make a case against a provider who duped, or otherwise disadvantaged them [12]. Governance however is still lacking to a certain degree which is why these countries do not belong to capability level C. Countries we consider having some degree of governance are most of the African, South American and middle American countries.

## 6.4 Level four : Lacking

Capabilities belonging to maturity level four are authentication protocol C, collection of user data A, legislation B and distribution of power A.

The authentication protocols we consider to be lacking in safety and belonging to capability C are; password, pin code, SMS and 2-factor authentication making use of two out of the three mentioned protocols [25, 45, 48, 65, 99]. The reason password belongs to C is because passwords are the most used method of authentication. People often use weak passwords that they use on multiple sites and have used for multiple years or keep in insecure places. Additionally, requiring a password for authentication means that the service also needs a "forgot your password" option which introduces another weakness. A way to reset the password is often sent to the users' e-mail address, which could be compromised. A pin code suffers from the same vulnerabilities as the password does but makes use of a smaller amount of possible characters making it more vulnerable even to brute force attacks. Brute force attacks guess every possible option until one works. Like passwords people tend to use pin codes in multiple places and pick pin codes they think are easy to remember like 1234 or 9876. Finally, SMS authentication is considered lacking in safety because SMS messages are sent to a mobile number, which is assigned to a SIM card. Because users sometimes lose their phones, SIM cards can often be replaced at mobile shops. This means that a party may take part in "SIM swapping" by presenting him or herself as someone else at such a mobile provider's shop in order to swap the SIM card. The malicious party will then receive the SMS messages intended for someone else. Sometimes the malicious party is, or works together with, the employee of the mobile providers shop making SIM swapping attempts easier. "SIM swapping" attacks are currently the most popular attack on crypto assets [87]. Because all three authentication methods above are lacking in security, we do not consider a 2-factor authentication option using two of the three methods that much safer that it should belong in a higher capability. Keep in mind that using 2-factor authentication may give the user a false sense of safety, which is a risk.

Collection of user data is differently categorized as other KPAs. Collection of user data A indicates that the service has an extensive Know Your Customer (KYC) protocol in place that needs to be completed before the user may make use of the service. Some services such as VCEPs in some countries may be obligated by new cryptocurrency legislation in their respective countries to have an extensive KYC protocol in place. The reason KYC protocols may be obligatory according to cryptocurrency legislation is so the exchanging of cryptocurrency to fiat currency can be traced to a legal identity. This way no person or party who has illegally obtained cryptocurrency can exchange that currency into fiat currency without the governing body being able to trace his or her legal identity. However, with VCEPs, CWPs and WPs often being relatively new companies who sometimes may be more interested in usability than the safety of their users' data we consider the extensive gathering of user data harmful. Data gathered may be lost, sold or spread to parties with malicious intent. Because of this reason we state that no KYC protocol is secure, while an extensive KYC protocol is not. Losing anonymity in the ecosystem of cryptocurrencies exposes investors to the more dangerous threats [46, 52, 61, 67]. Therefore, collection of user data A includes those services that make their users complete an extensive KYC protocol.

Legislation B is assigned to countries who do not have specialized legislation concerning crypto-assets (yet) [1, 12, 86, 87]. This capability is also assigned to providers who are not obliged to adhere to the specialized legislation in place. For instance, some legislation only concerns VCEPs but not CWPs or WPs. With a large amount of the countries in the world adhering to the recommendations on AML legislation by the FATF which will be released in 2020 almost every country in the world belongs to capability level B. Only countries that already have specialized crypto-asset legislation in place do not belong to this capability. Countries with specialized legislation in place are the United States, Bermuda, Malta, Japan, South Korea, Europe, the United Kingdom and Canada. The fact that the FATF will release its recommendation considering new AML legislation specialized for crypto-assets in 2020 does not mean that every country will implement the new legislation in 2020. Countries who do not have specialized crypto-asset legislation may not act against providers who dupe or otherwise disadvantage their users. This is a risk and the reason we have assigned legislation B to maturity level four.

Finally, distribution of power A is the last capability assigned to maturity level four. This capability, however, is one of the most important in the CSSMAM model [1,4,5,9,11,12,15,28,73,86,87]. Distribution of power A is assigned to all services who control the private keys of their users. This means that all exchanges that are not decentralized have this capability assigned to them. This also means that those exchanges cannot achieve a higher maturity level than four. The reason exchanges need the power over the private keys of their users is to be able to guarantee trades are completed in a timely manner or completed at all. However, if the provider controls an investor's private key, they control their crypto-assets. These providers keep a lot of those crypto-assets of multiple investors making them a prime target for parties with malicious intent. Additionally, providers controlling the private keys and thus crypto-assets of their clients may leverage them for personal gain by participating in pump and dump schemes, fake trading volumes or keep newly forked coins for themselves. Because of these risks we have decided that providers who control their clients' private keys can never be considered anything more than lacking in safety, maturity level four.

## 6.5 Level five : Relatively safe

Capabilities in level five consist of instruction A, customer service A, hashing A, encryption A, digital signature A, active development C, communication B and governance C.

Instruction A is assigned to services who do not attempt to teach and instruct their users on the threats, dangers and practices to safely invest in the cryptocurrency ecosystem. Uninformed users are much easier to rob or trick out of their crypto-assets by parties with malicious intent [46, 52, 61, 67]. Half of all the crypto-assets stolen in the US in the past year [1, 87] was stolen by social engineers. The most effective countermeasure to social engineering is repeated instruction. Threats and dangers may be forgotten by investors, or the threats and dangers themselves may change over time. For that reason, instruction should be repeated. Any service not instructing their users on the threats and dangers of investing in the ecosystem indirectly puts them at risk. This is the reason instruction A is assigned to maturity level five.

Capability A of customer service also belongs in maturity level five. Customer service A is assigned when a provider has no customer service in place at all. This means that whenever something goes awry investors have not a single option to ask for help. Furthermore, no customer service severely hurts trust in a provider.

Hashing A is the capability assigned to providers who either do not make use of a hashing algorithm or who use an outdated algorithm [33, 76]. The outdated algorithms who are assigned to this capability are the MD5 (and older, MD4, MD3 and so on) and SHA-1 families of algorithms. SHA-1 keys could be broken by a computer worth 30 million in 56 hours in 2005. 2005 Is a long time ago and improvements in computing power have been made constantly. We can safely assume that SHA-1 keys can be broken much faster nowadays. Breaking hashed information usually is not the easiest way of gaining access to crypto-assets, which is why even providers with no hashing or outdated algorithms can still achieve a maturity level of five.

Like hashing, encryption also has multiple families of algorithms which offer varying amounts of security [22]. Encryption A is assigned to providers who either do not make use of an encryption algorithm or use DES or RSA with less than 1024 bits. The Data Encryption Standard (DES) can be broken by brute force in under 26 hours, and the service is even offered online [1] . In 2010 an RSA key with 768 bits was broken in 2 years, with computing power increasing over the past 9 years we decided to flag any RSA key with less than 1024 breakable. As was the case with hashing, because other links are weaker a poor encryption algorithm can still belong to a provider with maturity level five.

The same principle is used when it comes to the digital signatures used. Digital signature A belongs to services who make use of an RSA key with less than 1024 bits.

Active development C further limits the time window in which an update should have taken place. Providers who have updated their service within the past three months are awarded active development C. Additional maturity levels may be earned by updating more often with updating daily belonging in maturity level nine or ten (optimal).

Communication B is awarded to providers who release an update from time to time. There is some communication on important news and updates, but communication has not been standardized nor is every issue addressed and explained. Lacking communication can still lead to unwanted and risky situations but does not directly hurt safety to a large amount, which is why the capability can be considered relatively safe, maturity level five.

Finally, governance C is the last capability belonging to maturity level five [1, 12, 86, 87]. Any country with a well-functioning governing body are granted this capability. We consider the governing bodies of Europe, the United States, Canada, the United Kingdom, Australia, New Zealand, South Korea, Singapore, Malta and Bermuda to function to this degree.

## 6.6 Level six : Relatively Safe

Capabilities assigned to maturity level six are the collection of user data B, distribution of power B, open source A and legislation C.

Collection of user data B is granted to providers who either have limited their KYC protocol and have not included proof of residency and proof of ID or allow users to make use of their service without KYC to a certain degree. This way users may stay anonymous unless they use too much of their real information in the KYC or want to use the service fully and fill in the KYC form. Services with these kinds of KYC protocols in place are not that bad, which is why this capability belongs in maturity level six.

Distribution of power B is granted to providers who let their clients control their own private keys. If the provider does not control the private keys, they cannot disappear with all the crypto assets, pump and dump using crypto-assets of their clients or lose everything in a hack or scam. This does mean that the user is now responsible for keeping their private keys safe, but because all users have their own private keys all crypto-assets are not pooled into one place. This means that it is a lot less interesting to hackers and social engineers.

Open source A is assigned when providers do not release their code as open source.

Advantages of open source are that more eyes can more often find bugs and weaknesses, and these are usually patched soon after discovery [87]. Software or services that are not open source may take a while to do so, or do not even know about the bug. Malicious insiders may create backdoors as well. However, this does not necessarily mean

[1] https://crack.sh/

that anything not open source is not safe necessarily which is why this capability belongs to relatively safe, maturity level six.

Finally, legislation C is the last capability of maturity level six. Countries granted this capability do have specialized legislation but are not pushing the standards. Countries that belong to this select group are Europe, the United Kingdom and Canada.

## 6.7 Level seven : Safe

Capabilities in maturity level seven are collection of user data C, instruction B, digital signature B, authentication protocol D, open source B, communication C, experimental security options A and customer service B.

Collection of user data C is granted when a service has no KYC protocol at all. When no data is gathered, there is no data to be lost, stolen or sold. This way their clients keep anonymous and thus safer. Maturity levels up to 8 can be granted, with 9 and ten only if the company or service goes out of their way to keep their clients' data even safer.

Instruction B is a capability assigned to the providers who put some effort in instructing and teaching their customers about the potential threats of the cryptocurrency ecosystem. The instructions are not extensive however, or not repeated very often. A little can still help a lot, especially when it concerns the safekeeping of private keys or seed phrases, for example.

Digital signature B means that a provider uses digital signature algorithms that are currently considered safe. These algorithms are RSA keys with more than 2048 bits, Digital Signature Algorithm (DSA) and Elliptical Curve Digital Signature Algorithm (ECDSA) [43, 62, 77]. Additional maturity levels are granted to providers who make use of ECDSA, which is more modern than DSA and can be just as safe with less bits used. When using DSA the company or service should make very sure the random key k is kept secret. Using the same value twice, using a predictable value or leaking even a bit of the random key k can undermine security. This issue also effects ECDSA. If the key is kept safe both DSA and ECDSA are safe.

Authentication protocol D is assigned when a provider makes use of 2-factor authentication [49] with the exception of the following combinations; password/pin & location, password/pin & voice recognition, password/pin & SMS, password/pin & security question, SMS & location, SMS & voice recognition, SMS & security question, security question & location, security question & voice recognition and security question & face recognition. 2 Factor-authentication is the combination of two authentication methods, which does make authentication a lot safer. However, when making use of two methods both lacking in security 2 factor authentication still is not that safe. Because of this reason we excluded the combinations above.

When a provider is partly open source, or completely open source but with a small amount of people that commit to the project we assign open source B. Partly open source still has the added benefit of more eyes that find and solve more problems, sooner. However, the trust bonus that is gained when a service is completely open source so users can see what the company or group of developers is doing exactly is not earned. When the service has a small amount of active developers, we also do not grant the highest capability, because the added benefit of being open source is limited. Communication C is assigned when the provider communicates about updates, decisions and other things about the cryptocurrency ecosystem in a regulated and timely manner. The communication also needs to be published in relevant channels.

Experimental security options are a process area meant to grant providers with distinctive security options maturity levels to distinguish them from their peers who do not. Capability A is granted to any provider who does not employ experimental, new or distinguishing security options. Because providers can be safe enough without making use of distinguishing security methods this capability is assigned to maturity level seven.

Finally, the last capability in maturity level seven is customer service B. This capability can be earned by providing customer service to some degree. Clients can contact the company or group of developers and ask for help if necessary. However, the whole process cannot be called fast, effective or very professional and problems are not resolved often enough.

## 6.8 Level eight : Safe

Capabilities in maturity level eight are hashing B and Encryption B.

Hashing B is assigned when the family of hashing algorithms that are used to hash data is SHA-2, BLAKE or equivalent in terms of security [17, 36]. Although not to most secure algorithms available at the time of writing, all these algorithms are considered safe.

Encryption B is granted when the family of encryption algorithms used is AES 128/AES 256 or equivalent [30]. This encryption algorithm is currently used by the NSA to encrypt secret information, which means it should be safe enough for a wallet provider.

## 6.9 Level nine : Optimal

The capabilities assigned to level nine are legislation D, instruction C, authentication protocol E, customer service C, experimental security options B, open source B and communication D. Legislation D is granted only to countries that have the most modern legislation specialized for cryptocurrency. The countries that have that kind of legislation at the time of writing are Malta, Bermuda, the United States, Japan and South Korea. All of them have a different approach, but it is too early to determine which functions better than others [1, 12, 86, 87].

Instruction C means that a provider instructs its clients on the threats in the cryptocurrency ecosystem and repeats that instruction from time to time. Instructions may include, but are not limited to, a) keeping the seed phrase safe, b) recognizing scams, c) double checking website address and d) verifying communication. Additional maturity levels can be granted when a provider optimizes instruction of clients further.

Authentication protocol E is assigned to providers with the strictest of authentication protocols. Authentication should use 2, or more, factor authentication. One of the authentication methods should be considered very secure. Methods we consider that secure are iris recognition, fingerprint recognition, one-time password (token) and one-time password (software). Mobile devices can be considered tokens if the provider limits its service to that device only. Our rationale is that mobile devices are not often left lying around as PCs or laptops are because they are usually kept on the body. They often require additional authentication and can be deactivated or reset from a distance when stolen. Services in authentication protocol E can distinguish themselves further by offering additional authentication options.

Customer service C is assigned to providers who have optimized their customer service. The service should be fast and professional, a large amount of problems should be solved. The customer service should be carried out by professionals and not be outsourced to a generic customer service company. Outsourcing to a company specialized in the field is fine, however.

Experimental security options B is reserved only to the providers that have implemented cutting edge technology, protocols or otherwise experimental methods [60] to secure their services. Examples of currently experimental security methods are decoy wallets. Decoy wallets pretend to be the main wallet when a service is opened, but a secret handling is needed to reveal the main wallet. This way, when robbed or held up at gunpoint only the decoy wallet may be lost or stolen.

Open source C is granted when a service is entirely open source. Being entirely open source means that every part of the service can be inspected by the public, revealing that the company or group of developers behind it is not doing anything unwanted. Additionally, bugs and other problematics can be found and resolved earlier. There needs to be an active group of reasonable size of developers.

The final capability D of communication is assigned to providers who have optimized their communication. The most popular outlets are used effectively and regularly. Users can ask questions and are answered within a reasonable time frame. Decisions are explained carefully, and their users are sometimes even included in the process. Other methods of communication such as roadmaps, AMA's and interviews with developers can also help optimizing communication.

## 6.10 Level ten : Optimal

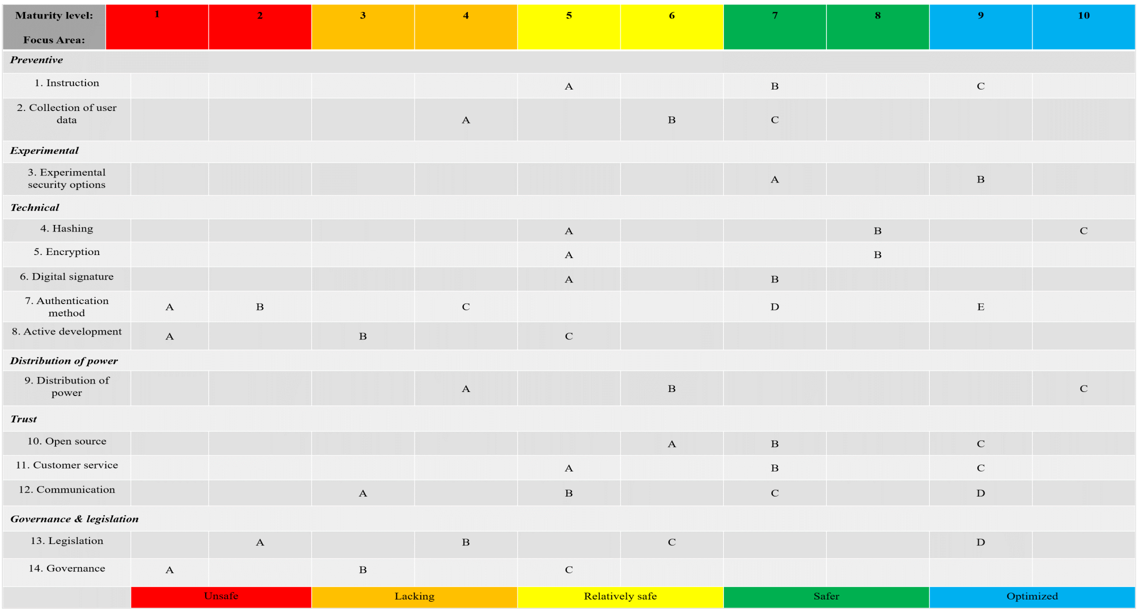
The final maturity level only has two capabilities; hashing C and distribution of power C.

There are two families of hashing algorithms that are considered quantum-proof, and as such the best possible algorithms for the future. These two families are SHA-3 and BLAKE2. Any provider using one of these two families or equivalent has optimized their hashing to such a degree that they have earned hashing C, maturity level 10.

Distribution of power C is assigned to those providers that allow their clients to divide power over their private keys to be split across multiple parties and devices. For instance, 2 out of 3, 3 out of 5 or signing transactions using an offline device. Some providers provide their users with the services of a specialized signing company who can serve as a third party in 2 out of 3.

## 6.11 Mass evaluation of the crypto asset safekeeping security maturity assessment model

As a second, and hopefully, continuous evaluation method we make use of mass validation by publishing the model online and asking for feedback from everyone interested. The model is currently published online at www.howsafeismycrypto.com. We try eliciting feedback out of **a)** my fellow students during, and after, presentations **b)** the interviewed experts by communicating the model back to them and **c)** providers the model has been demonstrated on. At the time of writing we have had 8 e-mails resulting in a couple of adaptations to the model.
The current iteration of the CSSMAM can be found below.



| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure 6.1: The crypto asset safekeeping security maturity assessment model

# Chapter 7

# Demonstration

After developing the model, we now demonstrate it on the largest providers of virtual currency exchange, custodian wallets and wallets. Tables with descriptions on every inspected key process area and the filled in model belonging to that service can be found in appendix B.

## 7.1 Largest VCEPs by volume

| *#* | *Top 5 VCEPs* | *Maturity level* | *Maturity score* | *Rationale* |
|---|---|---|---|---|
| 1 | Binance | 4 | 90 | Binance scores high on most process areas and is a good example for other exchanges. However, it still supports SMS as a 2-FA function. |
| 2 | Digifinex.com | 4 | 83 | Digifinex does not score particularly high on most process areas and has room for improvement everywhere. However, it does not score low anywhere either which is shown in the maturity level. |
| 3 | BitMax.io | 4 | 82 | Bitmax, like Digifinex does well across the board, but has a lot of room for improvement as well. |
| 4 | OKEx.com | 2 | 69 | OKEx scores low, security of their customers, customer support and trust does not seem to be a high priority, avoid. |
| 5 | Dobiexchange.com | 2 | 68 | Like OKEx, dobiexchange has put little effort in the security and protection of their customers. |

Table 7.1: Top VCEPs

In order to determine which VCEPs are the largest we look at the trading volume reported on coinmarketcap.com [10]. Note that we have discovered before that the trading volume reported on a large part of the top ranking VCEPs is probably false [4], but without possessing verified statistics we have no choice but to make use of the trading volume. Reported volume on exchanges may rise or drop explosively, so we look at the 30-day reported adjusted trading volume. Review tables and filled in models belonging to the top VCEPs can be found in appendix B.

The first VCEP we look at is Binance, the largest VCEP by trading volume. Binance was founded in 2017 in China but was moved to Japan before China banned cryptocurrency trading. Binance is currently based in Tokyo, Japan. Japan is ahead of most countries when it comes to AML legislation concerning crypto assets. The governing body of Japan can be trusted as well.

Binance does put some effort into instructing its users on possible threats. On every visit of the website and logging in users are prompted to double-check the websites' address. When registering as a new user there are some extra instructions on safety that need to be read and checked off, before the user can continue. The next step is setting up 2-FA, which is strongly recommended. Unfortunately, Binance does allow 2-FA using SMS, which is known to be abused by hackers using SIM swapping. Whenever visiting a user's profile, a security recommendation is shown.

Binance is relatively lenient when it comes to its KYC protocol. Without any proof of identity or residency users can withdraw up to 2 Bitcoin every 24 hours, which may seem like a small amount but keep in mind that at time of writing 1 Bitcoin is worth more than $10.000. If a user wants to be able to withdraw more than 2 Bitcoin every 24 hours there is an extensive KYC protocol that requires your first name, last name, date of birth, country, city and postal code. In addition, a proof of identity and a proof of residency are required. When it comes to cutting edge and experimental security solutions, we did not encounter any.

As VCEPs usually are not open source we have no way of finding out what standards are used for hashing, encryption and digital signatures. In addition, as a VCEP Binance controls your private keys, which means you can lose your investments whenever Binance is hacked from the in or –outside, does some economically stupid things or just decides to take off. Not to mention that users may not receive new currencies after a hard fork, may lose their investments when a coin they have is delisted from the website altogether and may have their capital used in pump and dump practices. Authentication on Binance is done by e-mail address and password. 2-FA is optional, but so strongly recommended we doubt many users would skip setting it up. Unfortunately, 2-FA allows using SMS, which is known to be weak to SIM swapping.

Binance is updated regularly and does very well in communication. It uses Telegram, Facebook, Twitter, Reddit, Instagram and Medium to communicate with its users. Except for communication the help desk has a reputation for being fast and resolving most problems. Users without exceptional problems can consult the extensive FAQ.

Binance, as the largest VCEP in the world does a lot of things very well. Their instruction, communication and customer support are excellent. Unfortunately, the bottleneck is the authentication method, although they do force users to use 2-FA they allow users to use SMS. With SIM swapping becoming such a popular method of stealing crypto assets, we believe this is no longer a method that should be used. Binance, according to our model can be considered lacking in security with a maturity level of 4. We also, however, include a maturity score which is a total of maturity levels reached in every category which can be used to distinguish providers with the same maturity level. Binance, because it does score very well in a large amount of the categories has earned itself a maturity score of 90, which is very high.

The second VCEP is OKEx.com, founded in 2017 in Malta which is known for its modern legislation on digital assets. The governing body of Malta can be trusted. OKex does a lot worse than Binance, however. There is notably hardly any instruction on threats and security for users when signing up, logging in or visiting your user profile when using OKEx. The exchange requires extensive KYC, without complying trading on their platform is not possible. There do not seem to be any special or experimental security options in place.

Like most, if not every, VCEP OKex is not open source and the hashing, encryption and digital signature standards they likely use to some extent are not known to us. In addition, as was the case with Binance, and will be with every other VCEP, OKex controls your private keys. This means you can lose your investments whenever OKex is hacked from the in or –outside, does some economically stupid things or just decides to take off. Not to mention that users may not receive new currencies after a hard fork, may lose their investments when a coin they have is delisted from the website altogether and may have their capital used in pump and dump practices.

Authentication is done by e-mail and password. 2-FA is possible, but users are not prompted to set it up unless they visit the tab in their profile. When setting up 2-FA, OKex does allow SMS to be used, which is known to be weak to SIM swapping.

Okex is updated regularly and communicates about its updates on the website. The helpdesk of Okex seems especially poor. There is no FAQ to be found, and although there are OKex Facebook and Twitter account they are not linked to from the website, which may indicate they are not official. We consider OKex to be unsafe, with a maturity level of 2 and a maturity score of 69. Not instructing users at all and only using authentication by e-mail and password is very unsafe. The company has barely any redeemable qualities, as customer service and communication can be considered lacking as well. Users can not use the exchange without complying to the extensive KYC protocol either.

The third VCEP is DigiFinex, founded in 2017 in the Seychelles, but currently headquartered in Singapore. Modern legislation on cryptocurrencies in Singapore is underway but not yet implemented at the time of writing. The governing body in Singapore can be trusted.

DigiFinex puts a decent amount of effort in instructing its user base, there are some instructions on safety on login and registration as well as repeated security tips when you visit the user profile. Like Binance DigiFinex allows users to use the exchange and withdraw money without adhering to their KYC protocol. The amount is half of that of Binance, however, with 1 Bitcoin every 24 hours.

As was the case with the other VCEPs there does not seem to be any experimental or cutting-edge security features in place. Neither do we have any way to discern the hashing, encryption and digital signature protocols that are used to protect user data. As is the case with every VCEP the power over private keys is in the hands of DigiFinex and the code is not open source.

DigiFinex does very well when it comes to the authentication protocol. Authentication is done by e-mail and password, after which a one-time password will be sent to the e-mail on every login. In addition, 2 factor-authentication is strongly recommended. The 2 factor-authentication used by DigiFinex does not support SMS, which is important.

The communication is decent, with the company using the websites' notice board, Facebook, twitter and Telegram but the customer service could be better. The only way of contact seems to be through a ticket option and the customer service does not link to the communication channels. According to our model DigiFinex can be considered relatively safe with a maturity level of 5 and a maturity score of 83. DigiFinex does not do amazing things in any category, but scores decent in every category.

The fourth VCEP by corrected trading volume is Dobiexchange.com, an exchange based in Hong Kong, China. We had trouble researching the founding year, country the company is based in and their address which hurts our trust.

Dobi fails to instruct their users on threats, does not allow users to make use of their services without extensive KYC and has very poor customer service. The only option of communication is an e-mail address which was hard to find on the website. Like other VCEPs we have no way of finding out which technical standards are being used for hashing, encryption and Digital Signature. Also, like other VCEPs Dobi controls their users' private keys. The authentication protocol cannot be called very strong either. It is done by e-mail and password with 2 factor authentication being optional, but not recommended by Dobi. The one thing they do correctly is not supporting SMS when using 2-fa, but only authenticator.

Dobiexchange is unsafe with a maturity level of 2 and a maturity score of 68 which indicates that there are a lot of categories they scored very poorly in.

The fifth and final VCEP by trading volume is Bitmax.io which is based in Switzerland where both legislation and governance are all right. Bitmax does unfortunately forget to instruct their users on any security threat. This is one of the categories they could easily improve in. Bitmax allows their users to make use of the exchange and withdraw up to 2 Bitcoin every 24 hours, just like Binance. 2 Factor-authentication is required for everything, and Bitmax does not support 2-FA by SMS which is a big plus. Like all VCEPs Bitmax controls the private keys of their users, Bitmax is not open source and do not release statements regarding the use of security protocols. Communication of Bitmax is fine, but customer service is kind of lacking. The company only sports a ticket option for users with problems in addition to a FAQ.

All in all, Bitmax does well enough in every category to receive a relatively safe maturity level of 5, with a maturity score of 82.

## 7.2 Top Custodian Wallet Providers (CWPs)

| *#* | *Top 5 VCEPs* | *Maturity level* | *Maturity score* | *Rationale* |
|---|---|---|---|---|
| 1 | BitGo | 4 | 99 | BitGo does very well for a custodian wallet provider who does provide its services to individual investors. BitGo makes an effort in instructing their users and uses all the modern standards. They are partly open source as well which helps both in trust as in development. However, they keep their clients' private keys. Clients pay them for that service, which is why they are custodian wallet providers. We cannot grant a service any maturity level higher than 4 without users controlling their own private keys. |
| 2 | Xapo | 2 | 77 | Xapo offers its services to individual investors as well but puts in very little effort. There is no instruction, nor are they open source. There is extensive KYC and they even allow their clients to login using Facebook or Google. People forget to logout of their Facebook or Google services on public computers all the time. Extremely unsafe. |

Table 7.2: Top CWPs

The custodian wallet providers are selected by reputation from websites proficient in the cryptocurrency ecosystem [10]. The completed review tables and filled in models belonging to the CWPs we look at can be found in appendix B.

BitGo supports custody of over 100 different cryptocurrencies and has been in business since 2013. We selected the company because it is one of the best known, and oldest, CWPs in the business. Xapo is another very old CWP founded in 2013. The company is based in Zürich Switzerland and it allegedly holds 7% of the world's circulating Bitcoin in its Swiss vaults [10]. Xapo only offers a Bitcoin wallet.

When analyzing the custodian wallet providers, we ran into a large problem. Most custodians are not open to the general public but only to institutional investors, which we are not. Without access we cannot analyze the security measures in place. As such we can only analyze the custodian wallet providers who also offer their services to individual investors.

BitGo is one of the oldest CWPs in the business. Founded in 2013 in California, USA the company has been around for a long time and it shows. BitGo does not neglect instructing their users. When registering there is advanced feedback on the strength of the chosen password and how long it would take to brute force it. When users make a back-up key there is advanced instruction and variety in choices. If a user so chooses to keep their own back-up key, the key is downloaded in pdf which removes some security risks such as screen capturing and key loggers. Users are instructed what to do with their keys and backups keys if they choose to keep them themselves. BitGo does not require any KYC at all. Sure, they want to know an e-mail address and a username, but nobody forces users to use their legal names. BitGo makes use of modern technical standards. They use SHA-512 (part of the SHA-2 standard) which is secure, and AES-128 for encryption which is considered very strong.

BitGo uses Elliptical Curve Digital Signature Algorithms (ECDSA) which is considered secure if you use it correctly. Authentication is done by 2-factor authentication, with one of them being an authenticator (token) as a minimum but security can be increased even further. Communication is fine but customer support is a bit lacking, with an extensive FAQ but only a ticket option to report problems. BitGo is partly open source, which does help in finding bugs sooner but not completely open source which does not net them the trust bonus a completely open source provider would earn.

Finally, when making use of the custodian service BitGo controls their users' private keys. This does mean they are vulnerable to the company going out of business, or them being hacked from either the in or –outside.

In conclusion, BitGo does many things well but in the end does not allow users to control their own private keys, which is the point of a custodian service after all. However, this does introduce very real risks in the ecosystem of cryptocurrency, risks we cannot ignore. As such we consider BitGo relatively safe with a maturity level of 4 and a maturity score of 99.

The second custodian wallet provider which also offers their services to individuals is Xapo. Founded in 2013 in Zurich, Switzerland, Xapo is considered one of the oldest and largest custodians holding allegedly over 7% of all Bitcoin. We think those Bitcoin may belong to their institutional investors mostly, because their individual custodian service seems lacking.

Xapo does not offer any instruction to their users, KYC is extensive and required. Xapo is not transparant nor open source, so we could not retrieve information on the hashing, encryption and digital signature algorithms we assume are in place. Authentication seems to be especially lax, logging in can be done by e-maill and password or even with facebook or google which we must admit have not seen anywhere before. At least they do communicate clearly on Twitter and Facebook, but their customer service does not seem to be all that impressive either with only a ticket option and an FAQ.

As such we can only assign a maturity level of 2 to Xapo, with a maturity score of 77. A CW should not allow login by facebook or google under any circumstances. E-mail and password is not very secure either. As of 15-8-2019 Xapo's custody services have been acquired by Coinbase.

## 7.3 Top wallet providers

| *#* | *Top WPs* | *Maturity level* | *Maturity score* | *Rationale* |
|---|---|---|---|---|
| 1 | Trezor | 8 | 119 | Trezor is an impressive piece of technology. They instruct their users, provide a hardware product of the highest grade, use all the modern techniques and standards and are open source to boot. Trezor does not require any personal information from their users. Keep in mind that Trezor does not come free. |
| 2 | Ledger | 7 | 117 | Ledger is very alike Trezor, and a hardware wallet. However, the big difference with Trezor is that Ledger's bootloader is not open source. This hurts their trust a little bit |
| 3 | Greenadress | 6 | 117 | Greenadress does recently well in most important process areas. Their communication, customer service and authentication protocol firmly keep them at maturity level six. |
| 4 | Electrum | 6 | 115 | Electrum was granted a maturity level of 6 which is impressive for a software wallet. The wallet is open source and does not require personal information from their users. They do not enforce 2-factor authentication, although their security options are highly secure if chosen. |
| 5 | Edge | 5 | 118 | Edge does a lot of thing well. Their ideas about security, their discussions about their choices on security options are all top notch. They use the latest standards. Authentication protocol could be better, but like other mobile wallets they use the users' mobile device as a unique identifier (token). Edge could be several maturity levels higher if not for the complete lack of instruction for their users. |
| 6 | Coinomi | 4 | 102 | Coinomi is average. Technical they are up-to-date. Communication and customer service are minimal. Authentication protocol only requires a password or pin code which is bad. Fortunately, they use a mobile device as unique identifier (token) but even then, only a password or pin code is not very secure. |
| 7 | Armory | 1 | 100 | Armory is a special case. It is both one of the best wallets, while also being one of the worst. Technically nobody does better. Armory even lets you choose the own size of AES encryption. They also offer various experimental security features such as vaults and the offline signing of transactions which can be divided across multiple parties and devices. However, their main problem is that the wallet has not had an update in the past year. As such it should be avoided. Customer service and communication ever since the product was discontinued and made open source has been bad too. |
| 8 | Bitcoin Core | 1 | 92 | Bitcoin Core is a very basic wallet client. Being basic it lacks functionality to make it secure. There is no authentication protocol which is its worst quality. |
| 9 | Exodus | 1 | 90 | Exodus has invested in usability and design instead of security. There is no authentication protocol. Communication and customer service are decent however. A very basic service with great looks. |

Table 7.3: Top wallet providers

Wallet providers provide software or hardware so you can store your own cryptocurrency. We will look at the most popular solutions in a few different categories; hardware wallets, software wallets, web wallets and mobile wallets. All completed reviews and filled in models can be found in appendix B.

Hardware wallets are physical devices that need to be bought. They are made to be secure even on an infected computer or when physically stolen. The two best known and most used hardware wallets are Trezor and Ledger, we will look at both.

Software wallets require the user to download them to their desktop. They store your private keys on your machine, which does make them depend on the security of that machine. In this section we look at four different software wallets that are rather different. First, we look at two of the most popular wallets; Exodus and Electrum. The third candidate is one of the oldest wallets; Bitcoin Core and the last wallet is Armory, a wallet built specifically to be secure.

Web or online wallets run in the cloud and are often quick and easy to use. We looked at two web wallets; greenadress.io and blockchain.info, but greenadress.io discontinued its web wallet while blockchain.info has extended its web wallet to be an exchange. We reviewed greenadress.io as a mobile wallet instead and chose to drop blockchain.info from reviewing because it lacked features that distinguished it in any way from the exchanges we already reviewed. At this moment, there are no popular web wallets in existence anymore.

Mobile wallets are apps for your smartphone, which means the private keys are stored on your mobile device (except when using the Ledger app in combination with the Ledger hardware device). The three mobile apps we will review are two of the most used mobile wallets; Edge and Coinomi in addition to greenadress.io which used to be the most popular web wallet.

We start with looking at Ledger and Trezor, both hardware wallets are very secure and operate in much the same way. We will describe both here because their strengths are often shared and their differences small.

Both hardware wallets have extensive instruction on safety and threats, and what to do to recover the wallet. They both do not require any form of KYC, and both make use of the latest hardware that should be resistant to any tampering from the outside. Technically both wallet providers are very alike as well, the hashing standard used is SHA-256 (SHA-2 family), the encryption algorithm being used is AES-256 and the digital signature algorithm is ECDSA. All these protocols are currently considered secure. Both Ledger and Trezor allow their users full control over their private keys, have an extensive FAQ, ticket option and active communication over social media such as Facebook, Twitter and Telegram. Ledger is based in Paris, France while Trezor is based in Prague, Czech Republic. Both countries are part of the EU where the legislation on cryptocurrency is modern and will be even better at the end of this year. Governance in both countries can be trusted. The differences are minimal; Trezor is entirely open source, while Ledger is only partly open source. The reason behind this is that Ledger does not publicize their bootloader code because it is used that their hardware was not tampered with on delivery. Trezor uses holographic stickers instead, but we consider that less secure than Ledgers solution. However, not being entirely open source hurts the trust in Ledger. Both hardware act as a token themselves and are additionally protected by PIN. Ledger only requires a PIN code of 4 digits, while Trezor requires 9 which is a little safer. An additional password is needed when connecting the device to a computer.

At the end of the day both hardware wallets are very secure and much alike, but between the two Trezor scores just a little bit better with a maturity level of 8 and a maturity score of 119, while ledger has a maturity level of 7 and a maturity score of 117.

The software wallets we chose to demonstrate the CSSMAM on vary more than Ledger and Trezor. The first software wallet we examined is Exodus. Exodus distinguishes itself with its sleek design and clear interface. The wallet focusses itself on usability and design rather than security. There is no instruction on threats in the cryptocurrency ecosystem, there is no authentication protocol and no encryption because there are no passwords or other user data to encrypt. We could not even find an option to set a password. Like all WPs exodus at least allows users control over their own private keys. Exodus also does well on communication and active development. Communication is done using multiple social media outlets such as Facebook, Twitter and Slack. The wallet is updated every two weeks. Exodus is based in the United States, where both legislation and governance considering cryptocurrency are one of the best.

In conclusion, Exodus focusses on usability and design rather than security. Their business plan depends on the number of users, which they attract with said usability and design. Investors are not protected nor informed. Exodus is not open source. Exodus has a maturity level of 1 and a maturity score of 81.

The next wallet provider is Electrum, one of the oldest wallets in existence. It was released in November 2011. Electrum is very different from Exodus, focusing on security and functionality rather than usability. When downloading Electrum there are various warnings regarding the source of the download. There is a PGP signature included in order to check the download. Users are instructed on the use of their seed key, how to keep it safe and where to keep it. In order to double-check if users have written down their seed phrase it is asked of them again, users can not copy the seed phrase. Unfortunately, the seed phrase is entered by keyboard, which makes it susceptible to key loggers. Electrum has no KYC, it allows full control over your private keys and even offers a third-party signing service. The seed phrase is hashed using SHA-256, which is secure. Passwords and private keys are encrypted using AES-256 which is also very secure. The authentication protocol depends on the kind of wallet you want to create. Multisig, 2-factor authentication wallets are possible but if a user so chooses, he could create a wallet with only a password. This is not recommended however, which is why we grant Electrum capability C here. Communication is only done through Twitter, but communication is extensive, clear and released regularly. A weaker point is their customer service which is minimal, barely earning capability B. Electrum is updated regularly, however, and entirely open source. The open source project is registered in the United States where both legislation and governance considering the cryptocurrency ecosystem is one of the best in the world.

Although it may take a little getting used to Electrum, we consider it very safe. The wallet is open source, updated and the company is non-profit. Authentication can be done well, but it depends on the user and is not enforced. The technical standards are all modern. Electrum was granted a maturity level of 6 and a maturity score of 115.

The next wallet provider is Bitcoin Core, the oldest wallet in existence released together with the Bitcoin code. The wallet is also a full node and verifies every transaction fully. The wallet functionality is very basic. The wallet does not provide instructions, nor does it require a password or ask for user information. As we mentioned, the wallet is very basic. This is both a good thing and a bad one. It provides the basic functionality and does that as it should. The wallet is open source and non-profit, updated regularly and allows users complete control over their private keys. The wallet however, does not have an authentication protocol nor support seed keys. As such there is no encryption or hashing of anything. There is no customer support to speak of and communication is sporadic. The head developer with the domain belonging to Bitcoin Core registered to his name is Martti Malmi a Finnish developer. Governance and legislation in Finland can be trusted.

Bitcoin Core as a wallet is not secure, it is however still very usable for anyone willing to run a full node or verify transactions. Bitcoin core has a maturity level of 1 with a maturity score of 92.

The final software wallet we use our model on is Armory, a wallet renowned for focusing on security. Armory offers advanced instruction to its users on all its safety functionalities, the methods of saving the seed phrase and how to back up your wallet. It does not require KYC. As the wallet that is renowned for its security, Armory offers users to choose what number of bits the AES algorithm uses with more bits taking longer to load but also incredible security. Armory even offers settings to run the wallet over the TOR-network for anonymity. The SHA-256 algorithm is used for hashing the seed phrase. Authentication is done using just a password normally, but Amory allows for an offline signing set-up where a transaction needs to be signed from a computer not connected to the internet. Additionally, Armory is fully open source and non-profit. All of this is top notch; however, Armory was developed by Armories technology incorporated who discontinued the development and handed the project over to the community. The community has not released an update of Armory in the last year. Communication and customer support are minimal too.

In conclusion, Armory may have been the most secure wallet there was with some experimental security techniques and lots of functionalities. Unfortunately, the work on the wallet has been discontinued which hurts its security a lot and the provider can no longer be trusted to be safe. Requiring only a password for authentication is weak as well. Armory has a maturity level of 1, with a maturity score of 100.

The first of the mobile wallets is edge. Using a mobile device, the wallet attempts to combine security and usability. Their choices of security and authentication are explained and discussed in blog posts and seem to be thought about deeply. However, they neglect to instruct their users in order to protect them against threats that are not technical by default. Edge has chosen to encrypt and hide the master keys at any time in the secure part of the users' smartphone so it cannot be stolen by key loggers or screen loggers. Like all WPs Edge allows users full control over their private keys. Edge is fully open source with good communication and a dedicated customer support line during work hours. Edge is updated once a month and based in the United States where both legislation and governance are good. Edge uses a username and password combination for login. Usernames are slightly safer than e-mail addresses because those may be found online. When reclogging in within an hour only a pin code is needed. 2-FA is optional but recommended. Edge uses Scrypt to hash seed phrases which is secure and AES-256 to encrypt which is also very secure.

Edge seems expertly constructed with a good combination of security and usability. They make use of the most modern technologies and support their users with good customer support and strong communication. However, they seem to forget that users can protect themselves too if they know how, which is one of their only weak points hurting their maturity level. Edge has a maturity level of 5 and a maturity score of 118.

The second mobile wallet is Coinomi. Coinomi has instruction on what to do with your master seed and how to keep it safe, with instruction on what could happen if you do not. Users are prompted to re-enter the master seed they receive in order to make sure they wrote it down. Coinomi does not allow users to type in the master seed however, which protects it against keylogging but not screen logging. There is no KYC to be found. Technically everything appears to be sound. Coinomi uses SHA-256 to hash seed phrases and AES-256 to encrypt anything else. Coinomi is not open source however, which hurts trust in the application. Authentication wise Coinomi could do better, only a password is required when logging in although the application does allow to replace that with a PIN (unsafe) or a fingerprint (safer). No 2-Fa option. Customer support is minimal, with only a ticket option to those with problems. Communication is decent, using the app store and their website. And finally, the company is based in the European part of Cyprus where legislation and governance can be trusted.

Concluding, Coinomi does relatively well in most process area's but could improve a few. Customer support is minimal and using only a password or pin code as authentication is weak security, even though it is a mobile wallet which requires the mobile device as well. Coinomi has a maturity level of 4 with a maturity score of 102.

The last wallet provider we inspect is Greenadress, once one of the most used web wallets, which now has moved their service to mobile devices. Greenadress is based in Malta, which can be considered one of the safest countries in the world when it comes to cryptocurrency legislation and governance. The move to mobile does imply that security on mobile devices is better, and that greenadress cares about security. Greenadress instructs their users a bit on the importance of the master seed and how to keep it safe but could do more. KYC is non-existent. As was the case with Coinomi the seed phrase needs to be re-entered in order to make sure users have it written down, but the words are not typed out but clicked on instead in order to avoid key logging, but this method is still vulnerable to screen logging. Greenadress allows for a PGP signature on every official e-mail to verify its legitimacy. Technically Greenadress seems up to date, with SHA-256 for hashing and AES-256 for encryption, both very secure. Greenadress is completely open source and allows users to divide ownership of private keys over multiple users or devices if users so want it. Customer service could be better, with the main channel being an e-mail address. Communication is decent, with updates on the website and on the official Twitter channel. The service is updated once a month. The authentication protocol requires 2-FA but supports SMS and e-mail which are not that safe. It is however, an improvement from only requiring a PIN code or password.

In conclusion, Greenadress does well in most process areas but supporting SMS in 2 factor-authentication really hurts them. Greenadress has a maturity level of 6 with a maturity score of 117.

# Chapter 8

# Discussion

In this chapter we discuss the process, results and limitations of this research. We start with major findings and then continue to a discussion on the validity of the literature review, model creation and model evaluations. We then analyze the practicality and the accumulation of necessary information to use our model in order to answer our research questions and finally end with some suggestions for further research.

## 8.1 Major Findings

In this research we have investigated the safekeeping of crypto assets. We have investigated the technologies used in these systems, studied the attacks on them, learned about governance and legislation on the matter and evaluated our findings with experts. This has led to a framework that can inform investors on security of their crypto assets. We hope it can be used to increase ecosystem maturity and decrease criminal opportunities. Below are some of our major findings, and the influence that our research has on them.

- This research combines the fields of cryptocurrency and blockchain with security, governance and risk assessment. A combination necessary not only to consult users on investing in the cryptocurrency ecosystem more securely, but also for writing legislation, developing secure wallets and risk assessments.
- Security is determined by its lowest denominator, be that technology, legislation or humans themselves. Our framework provides a high-level overview of these influences in security and is as such the only transparent and complete security assessment framework in existence.
- The variance in our security assessment lays bare the immaturity of the ecosystems and the risks that come with investing in it, but also provides any party within it with a framework that can be used to improve it. We further expand on this in chapter 8.4 practicality.

When demonstrating our model it becomes clear that popularity is not an indicator of security. Some providers are clearly insecure but are still used by a large amount of investors.

## 8.2 Model Validity

### 8.2.1 Validity of literature review

We have carried out a specialized literature review from 4 perspectives. The structured review for the technical perspective was carried out with search words discovered using feature modelling. With some forward and backward searches, we have established a literature library on all the technologies that are used.

The literature review that was performed for the governance and legislation perspective was carried out by focusing on a small group of trusted and descriptive sources that together fulfill the need for information in this perspective. We have focused our investigation on the international organizations of which only a few exist who decide on the governance and legislation concerning money laundering and as such also digital assets such as cryptocurrencies.

The last perspective that was used in model creation, the attacker perspective, is necessary to point out the weak points of existing systems, technologies and even humans. However, these attackers do not document their methods, successes and failures. Research is based on retrospective analysis, historical breaches and preventive methods.

### 8.2.2 Validity of model creation

We have combined technological, legal and attacker perspectives into a framework on security. When we did so, we elected the Information Security Focus Area Maturity pattern by Mijnhardt et al. [58], which shares an important quality with the reality of security. The level, of maturity and in this case security, is determined by its lowest denominator. A system is only as secure as its most insecure link.

However, although the model style is a good fit, there are parts that are lost in translation. For instance, a capability used in ISFAM models acts as a threshold for a certain maturity level. However, if the highest threshold of a certain key process area is at maturity level 4 out of 10, does it mean that no system can have a higher maturity level than 4? The answer is no, whenever a threshold is passed additional security levels may be granted to match maturity level until the next bottleneck is reached, or additional maturity levels may be granted on a beforehand specified scale.

Key process areas were elicited from our earlier literature reviews and expert opinion. Capabilities of these key process areas were assigned using the same literature review and then evaluated with experts and adapted during the demonstration phase.

### 8.2.3 Validity of model evaluation and adaption

We have evaluated the model through demonstration, expert evaluation and mass evaluation. The model was constructed using knowledge gained from literature reviews and the expertise of experts in the concerning fields. That model, before demonstration, was evaluated by experts using semi-structured interviews. After each (big) iteration previously interviewed experts were informed of the change and asked for their opinion. Finally, the model was applied to 16 safekeeping providers of three kinds; 1) virtual currency exchange providers, 2) custodian wallet providers and 3) wallet providers. Results of these demonstrations were communicated to a) providers and b) the public. Feedback from both sources was incorporated in the next iteration of the model.

Unfortunately, the combination of fields that our model brings together is not something that an abundance of people in the Netherlands specialize in. As such, the expert feedback pool is relatively small. That is why the demonstration, communication and mass validation is important.

## 8.3 Model Accuracy

In this research we have investigated security of cryptocurrency safekeeping. The perspective we have used is that of an investor. Finally, we chose to use the ISFAM pattern by Mijnhardt et al. [58] for our security assessment model. We now expand on the consequences and limitations of those decisions.

The problem Mijnhardt et al. [58] had with their ISFAM model was that it is rigid. Some focus areas and capabilities were not applicable or out of place because of organizational characteristics. We suffer from the same problem, although the characteristics of security solutions by providers of wallets arguably differ less than the small medium enterprises Mijnhardt et al. constructed their model for. Additionally, we have attempted to alleviate this rigidness by adding the experimental security focus area. This focus area functions much like the Situational Factors that Bekkers et. al [19] incorporated.

There are almost 3000 different cryptocurrencies[1]. Safekeeping providers do not support all of them. Most only support a few(i.e. Coinbase pro[2], a well-known VCEP, supports 53 different cyrptocurrencies[3]). However, our model does not differentiate providers by the cryptocurrencies they support. As such investors may use our model on their provider, or look at the top providers we have reviewed, only to find out they do not support the cryptocurrencies they own. Furthermore, a lot of those cryptocurrencies have different use cases. For example, stablecoins are mostly used to transfer money between different services or currencies as they are pegged to a fiat currency [73]. Other cryptocurrencies such as Bitcoin, are more interesting as a long-term investment, transactions using Bitcoin are relatively slow and expensive compared to other cryptocurrencies, but the currency does often rise in value explosively [24, 63]. Thus, logically stablecoins are used more often in transactions, while Bitcoin is more often bought and then left alone for a long time. Because of these different use cases using a more usable safekeeping provider who provides a stable exchange platform with additional other services could be more enticing than a very secure provider. Those different use cases are not considered in our model.

We have divided safekeeping providers in virtual currency exchange providers, custodian wallet providers and wallet providers. This division is made on the distribution of power, a VCEP keeps a large amount of their users' assets online, digitally and in one place. A custodian wallet provider also controls their users' private keys, but usually keep them offline, divided and insured. A WP lets users control their own private keys. However, there are differences between these providers in: 1) which cryptocurrencies they support, 2) whether they insure the funds they are keeping, 3) usability, 4) exchanging options (fiat currencies, cryptocurrencies, payment methods), 5) minimum or maximum funds, 6) insurance and much more [53, 66]. So even when a service has attained a certain maturity level there may be other factors to consider instead.

The Information Security Focus Area Maturity (ISFAM) pattern by Mijnhardt et al. [58] allows clear thresholds for maturity levels, but when the highest-level capability is reached does that mean the service should be stuck on the maturity level of that highest capability? Ideally every key process area would have capabilities assigned to every maturity level for accuracy. Nevertheless, some of the highest capabilities are assigned to some relatively low maturity level because of their importance as thresholds. For instance, gov-

[1] Coinmarketcap.com

[2] pro.coinbase.com

[3] Coinmarketcap.com/exchanges/coinbase-pro/

ernance capability C is assigned to maturity level 5. A well-functioning governing body is just too important. Does that mean that no service can attain a higher level than maturity level 5? No, maturity levels are assigned according to safety class or to match the lowest maturity level of other key process areas. However, either option means that some accuracy is lost.

When it comes to cryptocurrency governance and legislation, we have taken a relatively general, high-level, approach. This approach results in a difference between model and reality. Governing bodies are categorized as unsafe, lacking and safe, but there are many differences to countries within one of those categories. Our categorization when it comes to legislation suffers much the same problem, although there is one more category that belongs to countries with optimized legislation. However, because legislation is relatively young because cryptocurrencies are relatively young it is hard to categorize unproven legislation any different than we did.

In our method we stated that our model should be usable by investors themselves, as such we have disregarded key process areas that are impossible to assess to outsiders. For instance, how secure a service is definitely depends on internal security practices concerning coding, company access control and internal security instruction. We do not consider these factors because 1) we do not have access to them, 2) an average investor would not know where to find the information. Additionally, even if a company would inform us of their internal practices concerning security, we have no way to double-check that information. Do note that we have made open source a key practice area in order to partly combat this lack of information, with a threshold for being open source that companies that are not cannot surpass. This way we count on the community to review code and such, although even being open source does not mean that internal security is tight. Finally, quality of implementation of process areas that we do consider cannot be tested. For instance, we assign the highest capability to the digital signature key process area if a provider uses ECDSA. However, if that provider does not implement ECDSA correctly by reusing a random key or using a predictable one, security provided by that digital signature is lower than what we assigned it [43].

Finally, we have had to take a certain standpoint when it comes to some security tradeoffs. One such tradeoff came up in our research and can serve as an example. The bootloader code by Ledger is not released as open-source. They do not release this bootloader code in order to be able to verify the integrity of their products when users received them. Because Ledger is not completely open source, we have not granted Ledger the open-source capability but the partly open-source capability instead. Now, Trezor, is completely open-source. They try to protect the integrity of their devices with a holographic sticker on the boxes of their devices. Arguably that method is less secure than that of Ledger, but because we do not consider this problem specifically in our model, Trezor receives a higher maturity level than Ledger does.

## 8.4 Practicality

Unfortunately, there are no available statistics on the number of users per wallet provider. However, we did find a study by Statista[4] in 2019 about the percentage of users that use a certain wallet type. The study was performed in the Netherlands, where cryptocurrency owners were asked what kind of wallet-type they used. Options were; **a)** online wallet

[4] www.Statista.com

(web wallet, VCEP), **b)** software wallet, **c)** hardware wallet or d) other. The results of this study can be seen below in fig. 8.1.

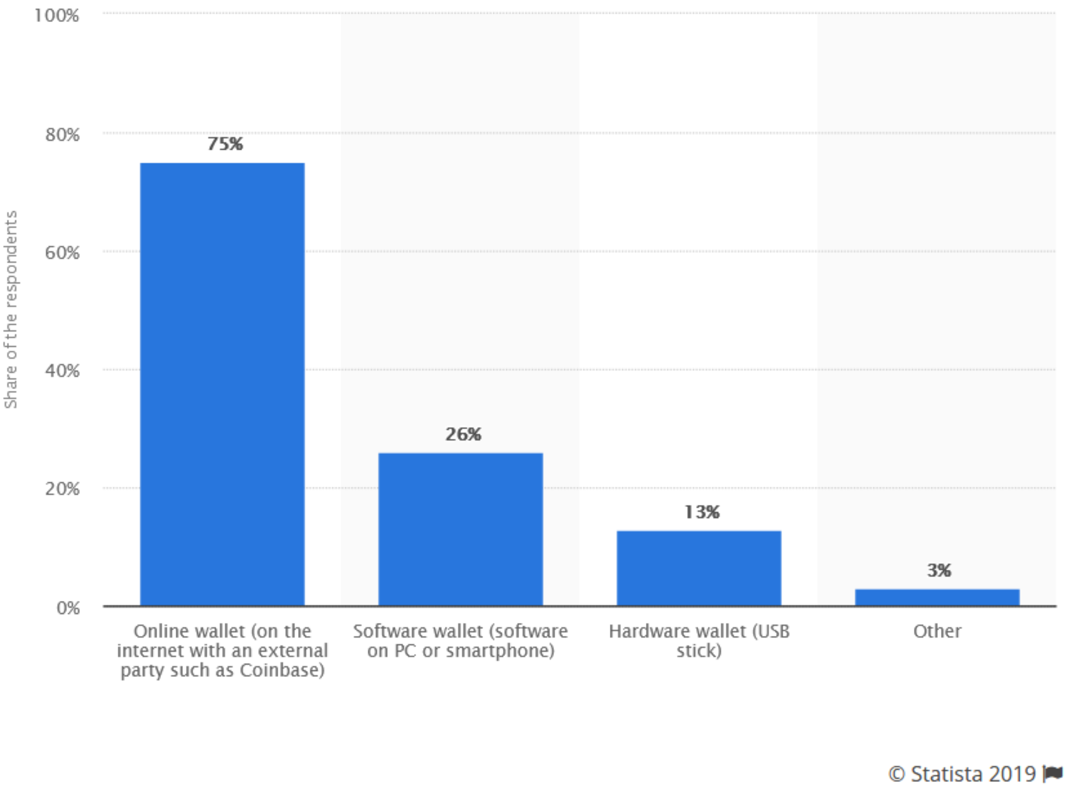


Figure 8.1: Percentage of users per wallet type (Exceeds 100% because of multiple answering options)

Source: www.statista.com/statistics/819039/cryptocurrency-wallets-used-in-the-netherlands-by-type/

Although we have chosen to divide providers differently, we can categorize the providers we demonstrated our model on in hardware, software/mobile and web wallets. That categorization is displayed in table 8.1 below.

| *#* | *Hardware wallets* | *Maturity level* | *Wallet type* | *Average maturity level* | *7.5* | *Max. maturity* | *8* |
|---|---|---|---|---|---|---|---|
| 1 | Trezor | 8 | Hardware | | | | |
| 2 | Ledger | 7 | Hardware | | | | |
| *#* | *Mobile & software wallets* | *Maturity level* | *Wallet type* | *Average maturity level* | *3.25* | *Max. maturity* | *6* |
| 3 | Greenadress | 6 | Mobile | | | | |
| 4 | Edge | 5 | Mobile | | | | |
| 5 | Coinomi | 4 | Mobile | | | | |
| 6 | Xapo | 2 | Mobile | | | | |
| 7 | Electrum | 6 | Software | | | | |
| 8 | Armory | 1 | Software | | | | |
| 9 | Bitcoin core | 1 | Software | | | | |
| 10 | Exodus | 1 | Software | | | | |
| *#* | *Web wallets* | *Maturity level* | *Wallet type* | *Average maturity level* | *3.33* | *Max. maturity* | *4* |
| 11 | BitGo | 4 | Web | | | | |
| 12 | Binance | 4 | Web | | | | |
| 13 | Digifinex | 4 | Web | | | | |
| 14 | BitMax | 4 | Web | | | | |
| 15 | OKEx | 2 | Web | | | | |
| 16 | Dobiexchange | 2 | Web | | | | |

Table 8.1: Providers, maturity levels and wallet type

According to the statistics provided by Statista 75% of all cryptocurrency owners use web wallets. According to our model 6 of the most popular web wallets have an average maturity level of 3.33, with a maximum maturity of 4. Mobile and software wallets, used by 26% of all users, have an average maturity level of 3.25, although the software kinds do lower the average by a lot. They have a maximum maturity of 6. Finally, hardware wallets used by 13% of users have an average maturity level of 7.5 and a maximum maturity of 8.

Now let us assume that all these users would use our model. 75% of all users could potentially move from 3.33 to 8 which is an increase of 240% if their concern would be security. Hardware wallets however, cost money. The best free option is one of the software wallets, greenadress or Electrum have a maturity level of 6 which would still be an increase of 180%.

The range in security between software wallets ranges from 1-6, which is a large range. With our model investors could potentially move to the software wallets that offer better security.

Still, these percentages only exist in a vacuum in which we only consider security, which is unrealistic. Users do not only consider security when deciding which wallet they use. Factors such as knowledge, usability and supported cryptocurrencies are very important when deciding on which wallet provider to use. But with 40 million wallets owned worldwide and steadily increasing, as can be seen in figure 8.2 below, even advising a small percentage could increase overall security significantly. This satisfies practical potential and our research question regarding usability.

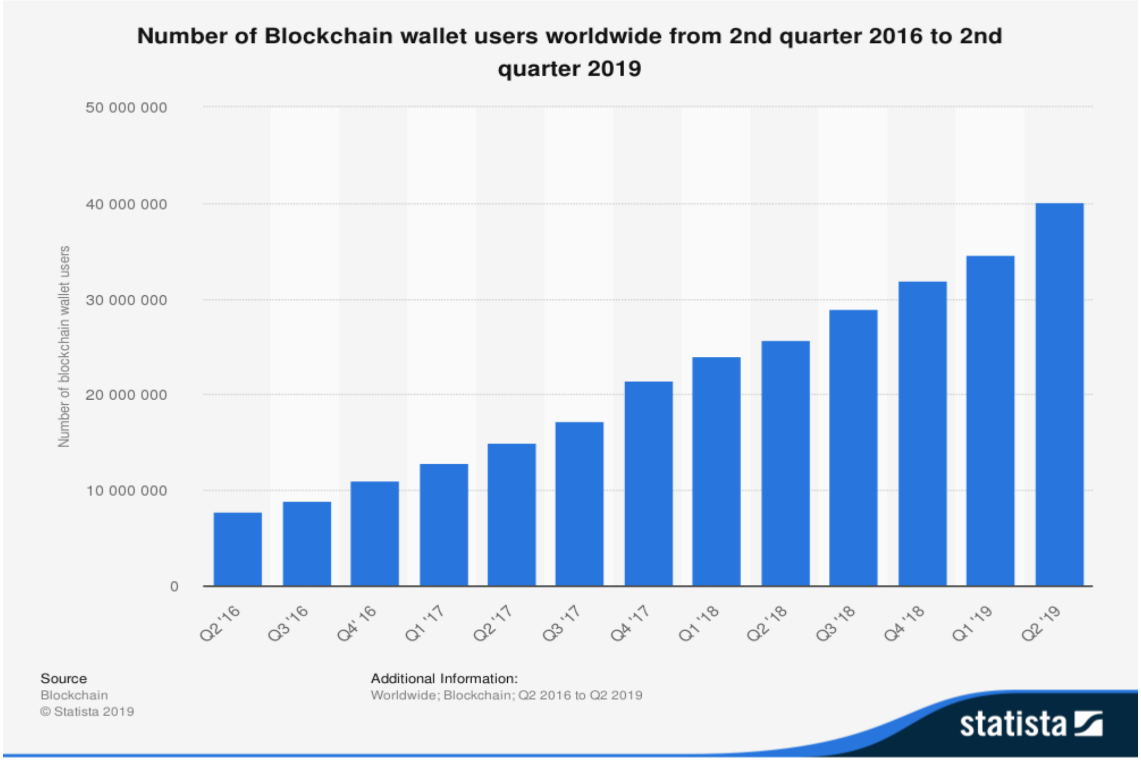


Figure 8.2: Number of cryptocurrency wallets

Source: www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

## 8.5 Accumulation of information

Let us look at the different key process areas and where the data can be retrieved from needed to assess them correctly.

| *#* | *KPA* | *Category* | *Data accumulation* |
|---|---|---|---|
| 1 | Authentication methods | Technical | Investors would need to create an account on the service and look at the authentication protocols that have been put in place by the provider. |
| 2 | Encryption | Technical | This key process area depends on the service either being open source or releasing a statement on the encryption protocol that is used. A google search is the most effective method to search for the used encryption in combination with the standards we have listed. If the used encryption cannot be found assign the first capability A. |
| 3 | Digital signature | Technical | Alike to encryption |
| 4 | Hashing function | Technical | Alike to digital signature and encryption. |
| 5 | Instruction | Preventive | Investors would need to create an account on the service and look for hints, tips or otherwise provided information on security. Look at a) amount of detail, b) comprehensibility and c) repetition |
| 6 | Active development | Technical (preventive) | Look at the download page, playstore page, github or update information on social media. Look at how far apart the updates are and when the service was last updated. |
| 7 | Open source | Trust | A google search will reveal the needed information. |
| 8 | Customer service | Trust | Search for websites who provider ratings and read through the comments. Keep in mind that there should be enough feedback before considering what is found. Other sources where customer service is discussed are social media channels. Finally, testing the customer service is a possibility. |
| 9 | Communication | Trust | Look at listed communication media. Look at a) amount of detail, b) comprehensibility, c) communication interval |
| 10 | Collection of user data | Preventive | Investors would need to create an account on the service and look at the information they need to provide before the service can be used. |
| 11 | Distribution of power | Distribution of power | Generally, exchanges and custodians always have control over your private key. There are however a few exceptions. Whenever the service notifies investors to securely save private keys and warns them that without it they lose the control over their crypto assets, they control their own private keys. In every other situation, investors do not own their own private keys. |
| 12 | Experimental | Experimental | Experiment security options is a flexible key process area that can be used to assign additional maturity levels whenever a service does something new or very different that our model does not cover. |
| 13 | Legislation | Governance & Legislation | Legislation can be studied on government websites which makes it easy to find. However, legislation may be complex and thus hard to understand. |
| 14 | Governance | Governance & Legislation | The functioning of governing bodies is described by some international organizations such as the FATF. Simply visit the website. |

Table 8.2: KPAs and how to accumulate the necessary information to correctly asses them

Most of the key process areas as can be seen above can be found with a google search or through a small number of trusted websites. The only category that could prove complex is the technical category. However, we have considered this fact in our framework. Even without information on technicalities a provider can reach maturity level 5. Gaining more maturity levels requires a combination of key process areas that need the company to share the way their business operates. We consider this level of investigation to be possible for an investor. As such we consider our final goal satisfied and the corresponding research question answered.

## 8.6 Suggestions for future research

First, there are key process areas that are generalized because of scope limitations in this research. As such, future research could focus on any of the key process areas. Further research could improve knowledge, adapt, change or add capabilities or key process areas and increase the accuracy of the model.

We have constructed this model from, and for, an investor's perspective. With additional research this model could be adapted to the perspective of a developer, corporate risk analyst or even attacker. That way it could be used as a framework for developing secure crypto asset safekeeping services. Moreover, it could be used to calculate risk when investing in a certain cryptocurrency[5] or using a certain safekeeping provider.

Further research could also increase accuracy and add important key process areas that we have discarded, if the researchers could gain information about the inner practices and workings of providers. However, that inside knowledge is not available to investors themselves which removes the possibility for investors to use the model themselves.

One of the key process areas is the experimental security options key process area. It was meant partly to assign maturity levels to exceptional security options and partly in order to make the model more future proof and less rigid and functions much like the Situational Factors introduced by Bekkers et. al [19]. Although we already discussed the option for further research in the existing key process area, future proofing the model is something else.

[5] https://coinmarketcap.com/all/views/all/

# Chapter 9

# Conclusion

The ecosystem of cryptocurrencies is relatively new and undiscovered, especially when it comes to academics. In this research we have dissected the systems that are supposed to keep investors' crypto assets safe and secure. We have studied the components of these systems, not neglecting to include the human, governance and attacker perspectives in addition to the technical components. The undocumented nature of some of these perspectives have made it hard for us to structure our literature searches, instead leaning on expert opinion. Experts, that, unfortunately, are scarce worldwide, not to mention in the Netherlands.

Nevertheless, we have attempted to create a framework that satisfies the objectives of a solution that we have established beforehand. Let us look at these objectives once more; 1) our framework should be of practical use by investors in the ecosystem, 2) information needed to use our framework should be gatherable within reasonable means, 3) the framework should provide a clear, high-level overview of the offered security. The third objective, a clear, high-level overview has been satisfied by using the capability maturity style. The model can be depicted on a single page and the maturity level indicates the weakest link in security. A characteristic that translates to reality, where parties with malicious intent focus on these weak links.

We have discussed our goals and sub research questions and consider them fulfilled. In this research we phave presented our answer to the research question we set: How can we model the security of a crypto asset safekeeping provider? We analyzed the strengths and weaknesses, model accuracy and model validity and outlined the possibilities for future research.

# Bibliography

[1] CipherTrace. (n.d.). Q2. https://info.ciphertrace.com/crypto-aml-report-q218, 2018. [].

[2] Privacy Considerations for Official Zcash Software & Third-Party Wallets. . https://z.cash/support/security/privacy-security-recommendations/, 2018. [Online; accessed: November 14, 2018 ].

[3] Bitcoin Investor Sues AT & T for $224 Million after Mobile-Linked Theft. https://www.ccn.com/bitcoin-investor-sues-att-for-224-million-after-mobile-linked-\theft/, 2018, August 15. [Online; accessed: September 20, 2018 ].

[4] Out of Top 10 Exchanges, Only Binance, Bitfinex Do Not Fake Volume. https://bitcoinist.com/binance-bitfinex-not-fake-volume/, 2018, December 19. [Online; accessed: June 13, 2019].

[5] SEC Charges EtherDelta Founder With Operating an Unregistered Exchange. https://www.sec.gov/news/press-release/2018-258, 2018, November 08. [Online; accessed: December 16, 2018 ].

[6] The History of the Mt Gox Hack: Bitcoin's Biggest Heist. https://blockonomi.com/mt-gox-hack/, 2018, November 19. [Online; accessed: November 13, 2019].

[7] If Your Bitcoin is Stolen, There's Only a 20% Chance You'll Get it Back. https://www.ccn.com/if-your-bitcoin-is-stolen-theres-only-a-20-chance-youll-ever-get\-it-back/, 2018, October 19. [Online; accessed: November 14, 2018 ].

[8] 30 Cryptocurrency Exchange Hacks - A Comprehensive List. https://coiniq.com/cryptocurrency-exchange-hacks/, 2019, February 06. [Online; accessed: September 20, 2018 ].

[9] 3 Reasons Why You Should Care about Decentralized Exchanges. https://blockgeeks.com/guides/decentralized-exchanges/, n.d. [Online; accessed: June 13, 2019 ].

[10] Cryptocurrency Exchange Rankings. https://coinmarketcap.com/rankings/exchanges/, n.d. [Online; accessed: May 18, 2019 ].

[11] Hard Fork vs Soft Fork. https://www.coindesk.com/information/hard-fork-vs-soft-fork, n.d. [Online; accessed: May 17, 2019 ].

[12] The Financial Action Task Force. http://www.fatf-gafi.org/, n.d. [Online; accessed: November 18, 2018].

[13] Nabih T Abdelmajid, M Alamgir Hossain, Simon Shepherd, and Khaled Mahmoud. Location-based kerberos authentication protocol. In *2010 IEEE Second International Conference on Social Computing*, pages 1099–1104. IEEE, 2010.

[14] Noura Aleisa. A comparison of the 3des and aes encryption standards. *International Journal of Security and Its Applications*, 9(7):241–246, 2015.

[15] A. Alexandre. Margin Lenders on Poloniex Lost $13.5 Million Due to Flash Crash. https://cointelegraph.com/news/margin-lenders-on-poloniex-lost-135-million-due-to-flash-crash, 2019, June 07. [Online; accessed: June 13, 2018 ].

[16] Partz H. Huillet M. Suberg W. Frost L. & Pirus B Alexandre A., Zmudzinski A. Latest News on Altcoin. https://cointelegraph.com/tags/altcoin, 2018, May 2. [Online; accessed: May 11, 2019].

[17] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C-W Phan. Sha-3 proposal blake. *Submission to NIST*, 92, 2008.

[18] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. Blake2: simpler, smaller, fast as md5. In *International Conference on Applied Cryptography and Network Security*, pages 119–135. Springer, 2013.

[19] Willem Bekkers, Inge van de Weerd, Sjaak Brinkkemper, and Alain Mahieu. The influence of situational factors in software product management: an empirical study. In *2008 Second International Workshop on Software Product Management*, pages 41–48. IEEE, 2008.

[20] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak specifications. *Submission to nist (round 2)*, pages 320–337, 2009.

[21] Rafael Bidarra and Willem F Bronsvoort. Semantic feature modelling. *Computer-Aided Design*, 32(3):201–225, 2000.

[22] Eli Biham and Adi Shamir. *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.

[23] J. Bijl. Certificates abused in the wild. https://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/, 2011, November 21. [Online; accessed: October 05, 2018 ].

[24] C. Blenkinsop. The Biggest Rises and Falls of Bitcoin, Explained. https://cointelegraph.com/explained/the-biggest-rises-and-falls-of-bitcoin-explained, 2019, May 15. [Online; accessed: May 19, 2019].

[25] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In *Proceedings of the 24th international conference on world wide web*, pages 141–150. International World Wide Web Conferences Steering Committee, 2015.

[26] Chiara Braghin. Biometric authentication. *University of Helsinki, Department of Computer Science*, 2000.

[27] V. Buterin. Bitcoin Multisig Wallet: The Future of Bitcoin. https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504/, 2014, March 13. [Online; accessed: September 21, 2018 ].

[28] J. Chen. Stop-Loss Order. https://www.investopedia.com/terms/s/stop-lossorder.asp, 2019, March 12. [Online; accessed: April 27, 2019 ].

[29] Usman W. Chohan. The Cryptocurrency Tumblers: Risks, Legality and Oversight . https://ssrn.com/abstract=3080361, November 30, 2017. [Online; accessed: September 20, 2018 ].

[30] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[31] John Daugman. How iris recognition works. In *The essential guide to image processing*, pages 715–739. Elsevier, 2009.

[32] Thai Duong and Juliano Rizzo. Flickr's api signature forgery vulnerability. *Tech. Rep.*, 2009.

[33] Donald Eastlake and Paul Jones. Us secure hash algorithm 1 (sha1), 2001.

[34] Artur Ekert and Richard Jozsa. Quantum computation and shor's factoring algorithm. *Reviews of Modern Physics*, 68(3):733, 1996.

[35] & Salone A. G., Brown J. Cryptocurrency Wallet Guide: A Step-By-Step Tutorial. . https://blockgeeks.com/guides/cryptocurrency-wallet-guide/, 2017, January 01. [Online; accessed: September 20, 2018].

[36] Henri Gilbert and Helena Handschuh. Security analysis of sha-256 and sisters. In *International workshop on selected areas in cryptography*, pages 175–193. Springer, 2003.

[37] D. Gilbertson. I'm harvesting credit card numbers and passwords from your site. Here's how. https://hackernoon.com/im-harvesting-credit-card-numbers-and-passwords-from-your-site-\here-s-how-9a8cb347c5b5, 2018, January 06. [Online; accessed: September 20, 2018].

[38] D Goodin. Bitcoins worth $228,000 stolen from customers of hacked Webhost. https://arstechnica.com/information-technology/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost/, 2012, March 02. [Online; accessed: November 13, 2019 ].

[39] D Goodin. Bitcoins worth $87,000 plundered in brazen server breach. . https://arstechnica.com/uncategorized/2012/05/bitcoins-worth-87000-plundered/, 2012, May 02. [Online; accessed: SNovember 13, 2019].

[40] S. Granger. Social Engineering Fundamentals, Part I: Hacker Tactics | Symantec Connect. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics, 2001, December 18. [Online; accessed: September 20, 2018].

[41] Muhammad Usman Iqbal and Samsung Lim. Legal and ethical implications of gps vulnerabilities. *J. Int'l Com. L. & Tech.*, 3:178, 2008.

[42] Anil K Jain, Arun Ross, and Sharath Pankanti. Biometrics: a tool for information security. *IEEE transactions on information forensics and security*, 1(2):125–143, 2006.

[43] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[44] Jonathan Katz, Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[45] Jae-Jung Kim and Seng-Phil Hong. A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, 7(1):187–198, 2011.

[46] K Krombholz, H Hobel, M Huber, and E Weippl. " advanced social engineering attacks"; journal of information security and applications, 22 (2015), s. 113-122.

[47] P. Kulche. Gezichtsherkenning op smartphone niet altijd veilig. https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken, 2019, January 03. [Online; accessed: January 08, 2018 ].

[48] Arash Habibi Lashkari, Samaneh Farmand, Dr Zakaria, Omar Bin, Dr Saleh, et al. Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951*, 2009.

[49] JK Lee, SR Ryu, and KY Yoo. Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters*, 38(12):554–555, 2002.

[50] & Navaratnam S. Lee J., Yang H. South Korean cryptocurrency exchange to file for bankruptcy after... https://www.reuters.com/article/us-bitcoin-exchange-southkorea/south-korean-cryptocurrency-exchange-to-file-for-bankruptcy-after\-hacking-idUSKBN1ED0NJ, 2017, December 19. [Online; accessed: September 20, 2018].

[51] B. Leighton. What is a stablecoin and how does it work - Coininsider. https://www.coininsider.com/stablecoins/, 2018, February 2018. [Online; accessed: May 11, 2019].

[52] Xin Luo, Richard Brody, Alessandro Seazzu, and Stephen Burd. Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*, 24(3):1–8, 2011.

[53] M. All Cryptocurrency Wallet Types, Explained. https://hobowithalaptop.com/crypto-wallets, 2018, May 11. [Online; accessed: September 20, 2018].

[54] Logan O Mailloux, Cheryl Garrison, Rick Dove, and Ryan C Biondo. Guidance for working group maintenance of the systems engineering body of knowledge (sebok) with systems security engineering example. In *INCOSE International Symposium*, volume 25, pages 1004–1019. Wiley Online Library, 2015.

[55] Salvatore T March and Gerald F Smith. Design and natural science research on information technology. *Decision support systems*, 15(4):251–266, 1995.

[56] M. Matsumura. I got my cryptos hacked, so you don't have to – Evercoin Blog. https://blog.evercoin.com/securing-your-cryptocurrency-cec5703a63a6, 2017, August 21. [Online; accessed: September 20, 2018].

[57] G. McFarlane. Millions Gone? Broker Takes Fire for Bitcoin Cash Freeze. https://www.coindesk.com/millions-gone-broker-takes-fire-bitcoin-cash-trading-freeze, 2017, November 20. [Online; accessed: February 11, 2019 ].

[58] Frederik Mijnhardt, Thijs Baars, and Marco Spruit. Organizational characteristics influencing sme information security maturity. *Journal of Computer Information Systems*, 56(2):106–115, 2016.

[59] Maturity Model. A systems engineering capability maturity modelsm, version 1.1. 1995.

[60] Malte Möser, Ittay Eyal, and Emin Gün Sirer. Bitcoin covenants. In *International Conference on Financial Cryptography and Data Security*, pages 126–141. Springer, 2016.

[61] Francois Mouton, Louise Leenen, and Hein S Venter. Social engineering attack examples, templates and scenarios. *Computers & Security*, 59:186–209, 2016.

[62] David Naccache, David M'RaÏhi, Serge Vaudenay, and Dan Raphaeli. Can dsa be improved?—complexity trade-offs with the digital signature standard—. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 77–85. Springer, 1994.

[63] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[64] L. H. Newman. A Cell Network Flaw Lets Hackers Drain Bank Accounts. Here's How to Fix It. https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/, 2017, June 03. [Online; accessed: September 20, 2018].

[65] Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[66] O. Ohayon. The sad state of crypto custody. https://techcrunch.com/2018/02/01/the-sad-state-of-crypto-custody/, 2018, February 01. [Online; accessed: September 20, 2018].

[67] G. Ollmann. The vishing guide. http://www.infosecwriters.com/textresources/pdf/IBM, 2007. [ ].

[68] Zuraini Othman and Anton Satria Prabuwono. Preliminary study on iris recognition system: Tissues of body organs in iridology. In *2010 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, pages 115–119. IEEE, 2010.

[69] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[70] Pedro Peris-Lopez, Julio C Hernandez-Castro, Juan ME Tapiador, Tieyan Li, and Jan CA van der Lubbe. Weaknesses in two recent lightweight rfid authentication protocols. In *International Conference on Information Security and Cryptology*, pages 383–392. Springer, 2009.

[71] H. Porter. Nine sacked for breaching core ID card database | Henry Porter. . https://www.theguardian.com/commentisfree/henryporter/2009/aug/10/id-card-database-breach, 2009, August 10. [Online; accessed: February 1, 2019].

[72] T. Ptacek. Javascript Cryptography Considered Harmful. https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2011/august/javascript-cryptography-considered-harmful/, 2011, August 29. [Online; accessed: September 20, 2018].

[73] D. Quirk. What are Stablecoins? A guide to Fiat-Pegged Cryptocurrencies. https://medium.com/altcoin-magazine/stablecoin-a-guide-to-fiat-pegged-cryptocurrencies-feae3e0b77c8, 2019, February 2019. [Online; accessed: February 20, 2018 ].

[74] Ariel Rabkin. Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In *Proceedings of the 4th symposium on Usable privacy and security*, pages 13–23. ACM, 2008.

[75] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3):614–634, 2001.

[76] Ronald Rivest. The md5 message-digest algorithm. 1992.

[77] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[78] & Rizzo P. Rizzo, P. Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack. https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack, 2014, March 06. [Online; accessed: November 13, 2019].

[79] K. Rooney. $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy\-to-do.html, 2018, June 07. [Online; accessed: November 14, 2018 ].

[80] Aviel D Rubin. Independent one-time passwords. *computing Systems*, 9(1):15–27, 1996.

[81] J. Russell. A major vulnerability has frozen hundreds of millions of dollars of Ethereum. https://techcrunch.com/2017/11/07/a-major-vulnerability-has-frozen-hundreds-of-millions-of-dollars\-of-ethereum/, 2017, November 07. [Online; accessed: September 20, 2018 ].

[82] Higgins S. Bitstamp Claims $5 Million Lost in Hot Wallet Hack. https://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack, 2015, January 08. [Online; accessed: SNovember 13, 2019 ].

[83] Higgins S. Details of $5 Million Bitstamp Hack Revealed. https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange, 2015, July 03. [Online; accessed: November 13, 2019 ].

[84] Khatwani S. What are HD Wallets? (Deterministic Wallet). . https://coinsutra.com/hd-wallets-deterministic-wallet/, 2017, July 31. [Online; accessed: September 20, 2018 ].

[85] Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah. Trusted execution environment: what it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 57–64. IEEE, 2015.

[86] A. Schlabach. Cryptocurrency Anti-Money Laundering Report – Q3 2018. . https://ciphertrace.com/pr-crypto-aml-report-2018q3/, 2018, October 10. [Online; accessed: January 19, 2019 ].

[87] A. Schlabach. Cryptocurrency Anti-Money Laundering Report – Q4 2018. https://ciphertrace.com/crypto-aml-report-2018q4/, n.d. [Online; accessed: February 14, 2019 ].

[88] B. Schneier. Schneier on Security. https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html, 2005, February 18. [Online; accessed: November 05, 2018 ].

[89] L. Shen. Bitcoin Exchange Kraken Goes Down for 40 Hours, Drawing Mt. Gox Comparisons. https://finance.yahoo.com/news/bitcoin-exchange-kraken-goes-down-231315587.html, 2018, January 12. [Online; accessed: September 20, 2018].

[90] E. Smart. BitPay CEO Scammed for Over $1.8 Million in Bitcoin. https://cointelegraph.com/news/bitpay-hacked-for-over-18-million-in-bitcoins, 2019, February 12. [Online; accessed: November 13, 2019].

[91] Daniel F Smith, Arnold Wiliem, and Brian C Lovell. Face recognition on consumer devices: Reflections on replay attacks. *IEEE Transactions on Information Forensics and Security*, 10(4):736–745, 2015.

[92] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen K Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger. Md5 considered harmful today, creating a rogue ca certificate. In *25th Annual Chaos Communication Congress*, number CONF, 2008.

[93] R. Stubbs. Quantum Computing and its Impact on Cryptography. https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography, 2018, April 29. [Online; accessed: November 14, 2018 ].

[94] J. A. Stucky. Behind the Biggest Bitcoin Heist in History: Inside the Implosion of Mt. Gox. https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion\-of-mt-gox, 2016, May 19. [Online; accessed: September 20, 2018 ].

[95] Marlies Van Steenbergen, Rik Bos, Sjaak Brinkkemper, Inge Van De Weerd, and Willem Bekkers. The design of focus area maturity models. In *International Conference on Design Science Research in Information Systems*, pages 317–332. Springer, 2010.

[96] R Hevner Von Alan, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, 28(1):75–105, 2004.

[97] W. Why Do I Need a Public and Private Key on the Blockchain? . https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76, 2017, January 30. [Online; accessed September 20, 2018].

[98] Roel Wieringa. Design science as nested problem solving. In *Proceedings of the 4th international conference on design science research in information systems and technology*, page 8. ACM, 2009.

[99] Jianxin Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. The memorability and security of passwords–some empirical results. Technical report, University of Cambridge, Computer Laboratory, 2000.

[100] W. Zhao. Ether Reported Stolen Due to Parity Wallet Breach. https://www.coindesk.com/30-million-ether-reported-stolen-parity-wallet-breach/, 2017, July 20. [Online; accessed: September 20, 2018 ].

[101] W. Zhao. Crypto Exchange Zaif Hacked In $60 Million, 6,000 Bitcoin Theft. https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft/, 2018, September 20. [Online; accessed: September 20, 2018 ].

# Appendix A

Below the maturity model question list can be found.

| *#* | *Question* | *Category* | *Answer* |
|---|---|---|---|
| 1 | Uses location based validation | Authentiation protocol | Yes/No |
| 2 | Uses password | Authentiation protocol | Yes/No |
| 3 | Uses pincode | Authentiation protocol | Yes/No |
| 4 | Uses fingerprint recognition | Authentiation protocol | Yes/No |
| 5 | Uses iris recognition | Authentiation protocol | Yes/No |
| 6 | Uses security question | Authentiation protocol | Yes/No |
| 7 | Uses face recognition | Authentiation protocol | Yes/No |
| 8 | Uses voice recognition | Authentiation protocol | Yes/No |
| 9 | Uses SMS | Authentiation protocol | Yes/No |
| 10 | Uses one time password (Token) | Authentiation protocol | Yes/No |
| 11 | Uses one time password (Software) | Authentiation protocol | Yes/No |
| 12 | Uses Data encryption standard or equivalent | Encryption | Yes/No |
| 13 | Uses advanced encryption standard or equivalent | Encryption | Yes/No |
| 14 | Uses Rivest-Shamir-Adleman or equivalent for encryption | Encryption | Yes/No |
| 15 | Uses Rivest-Shamir-Adleman for digital signature | Digital signature | Yes/No |
| 16 | Uses digital signature standard | Digital signature | Yes/No |
| 17 | Uses elliptical digital signature standard | Digital signature | Yes/No |
| 18 | Uses MD5 or equivalent or older algorirthms | Hashing | Yes/No |
| 19 | Uses SHA-1 or equivalent | Hashing | Yes/No |
| 20 | Uses SHA-2 or equivalent | Hashing | Yes/No |
| 21 | Uses SHA-3 or equivalent | Hashing | Yes/No |
| 22 | No instruction on the dangers of social engineering | Instruction | Yes/No |
| 23 | Some instruction and repetition on the dangers of social engineering | Instruction | Yes/No |
| 24 | Instruction and repetition on the dangers of social engineering | Instruction | Yes/No |
| 25 | No development | Active development | Yes/No |
| 26 | Updated in the last 6 months | Active development | Yes/No |
| 27 | Updated every month | Active development | Yes/No |
| 28 | Open Source | Open Source | Yes/No |
| 29 | Lists all affiliates | Communication | Yes/No |
| 30 | Public API | Open Source | Yes/No |
| 31 | First name required | Collection of user data | Yes/No |
| 32 | Last name required | Collection of user data | Yes/No |
| 33 | Address required | OCollection of user data | Yes/No |
| 34 | E-mail required | Collection of user data | Yes/No |
| 35 | Phone number required | Collection of user data | Yes/No |
| 36 | Proof of residency required | Collection of user data | Yes/No |
| 37 | Proof of identity required | Collection of user data | Yes/No |
| 38 | Service controls private keys | Distribution of power | Yes/No |
| 39 | User controls private keys | Distribution of power | Yes/No |
| 40 | Multiple parties control private keys | Distribution of power | Yes/No |
| 41 | Uses experimental security options | Experimental security options | Yes/No |
| 42 | Experimental security option adds little security | Experimental security options | Yes/No |
| 43 | Experimental security option adds some security | Experimental security options | Yes/No |
| 44 | Experimental security option adds a lot security | Experimental security options | Yes/No |
| 45 | Is based in Botswana, Ghana, Ethiopia, Yemen, Tunisia, Syria, Republic of Serbia, Iran, Pakistan, Sri Lanka or North Korea | Governance & Legislation | Yes/No |
| 46 | Is based in the United States, Bermuda, Malta, Japan, South Korea, Europe, the United Kingdom or Canada | Governance & Legislation | Yes/No |
| 47 | Never communicated with users | Communication | Yes/No |
| 48 | Communicated with users last 6 months | Communication | Yes/No |
| 49 | Communicated with users this month | Communication | Yes/No |
| 50 | Released a roadmap | Communication | Yes/No |
| 51 | Has no customer service | Customer service | Yes/No |
| 52 | Has lacking customer service | Customer service | Yes/No |
| 53 | Has good customer service | Customer service | Yes/No |

Table A.1: Maturity model question list

# Appendix B

Feature models

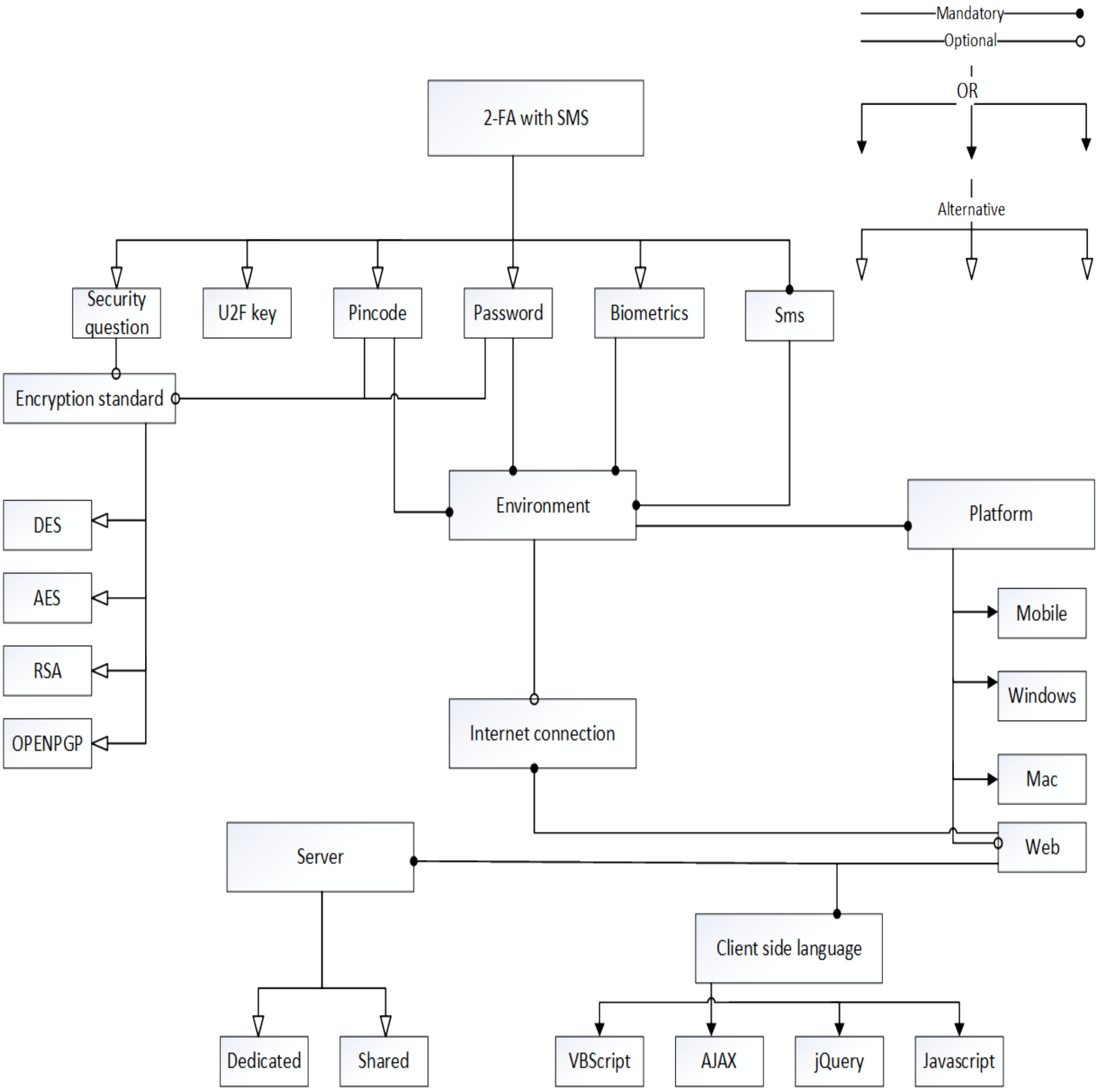


Figure B.1: 2-FA authentication using SMS feature model

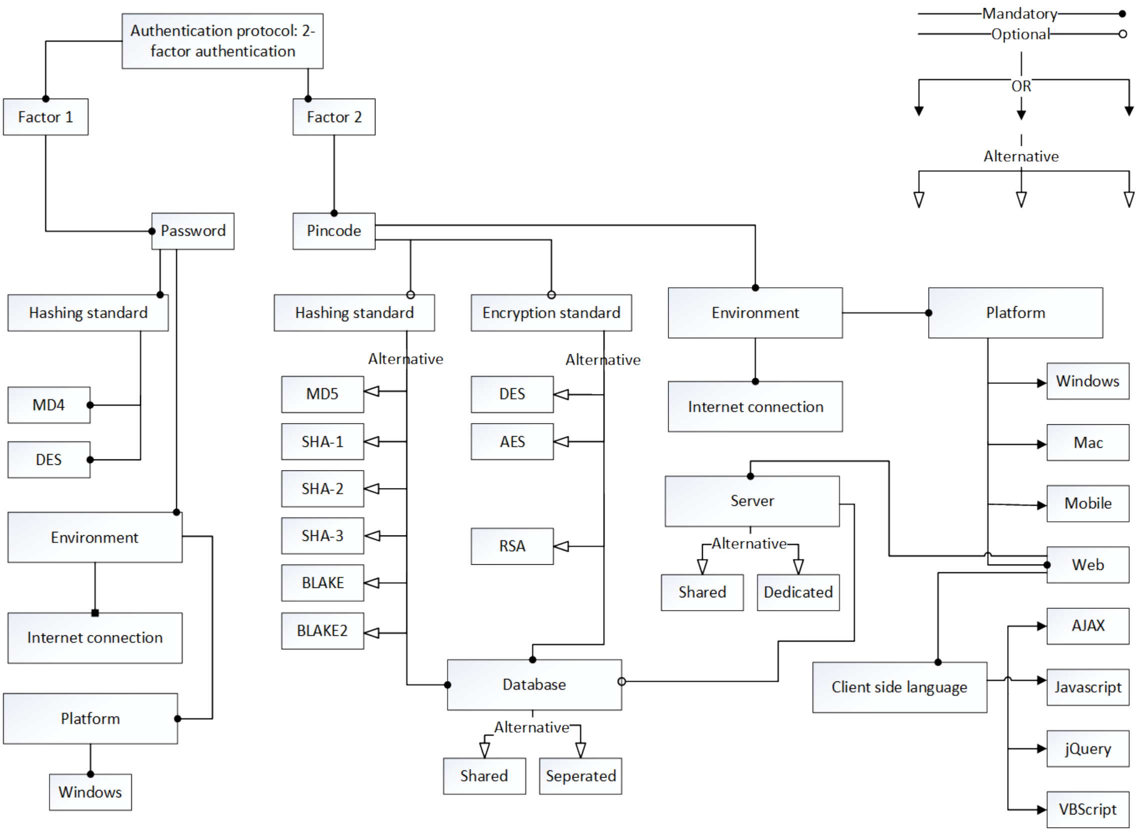


Figure B.2: 2-factor authentication feature model

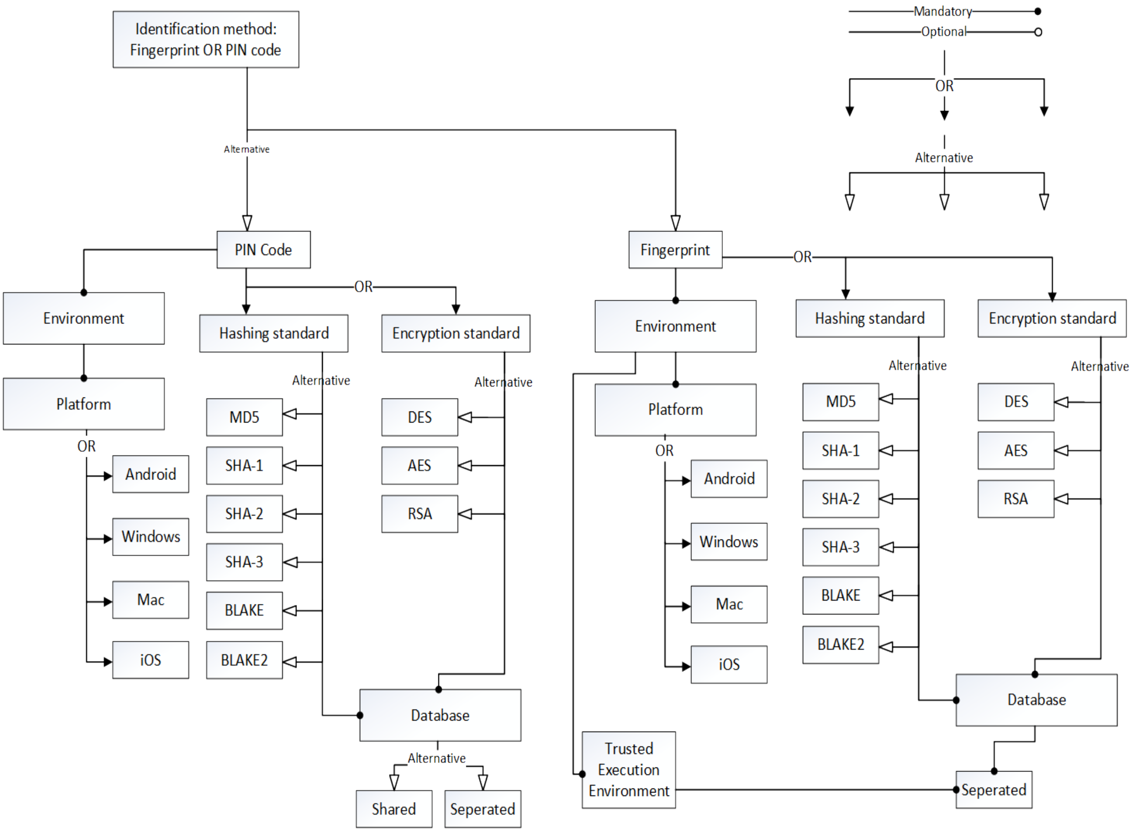


Figure B.3: Identification method fingerpint or PINcode

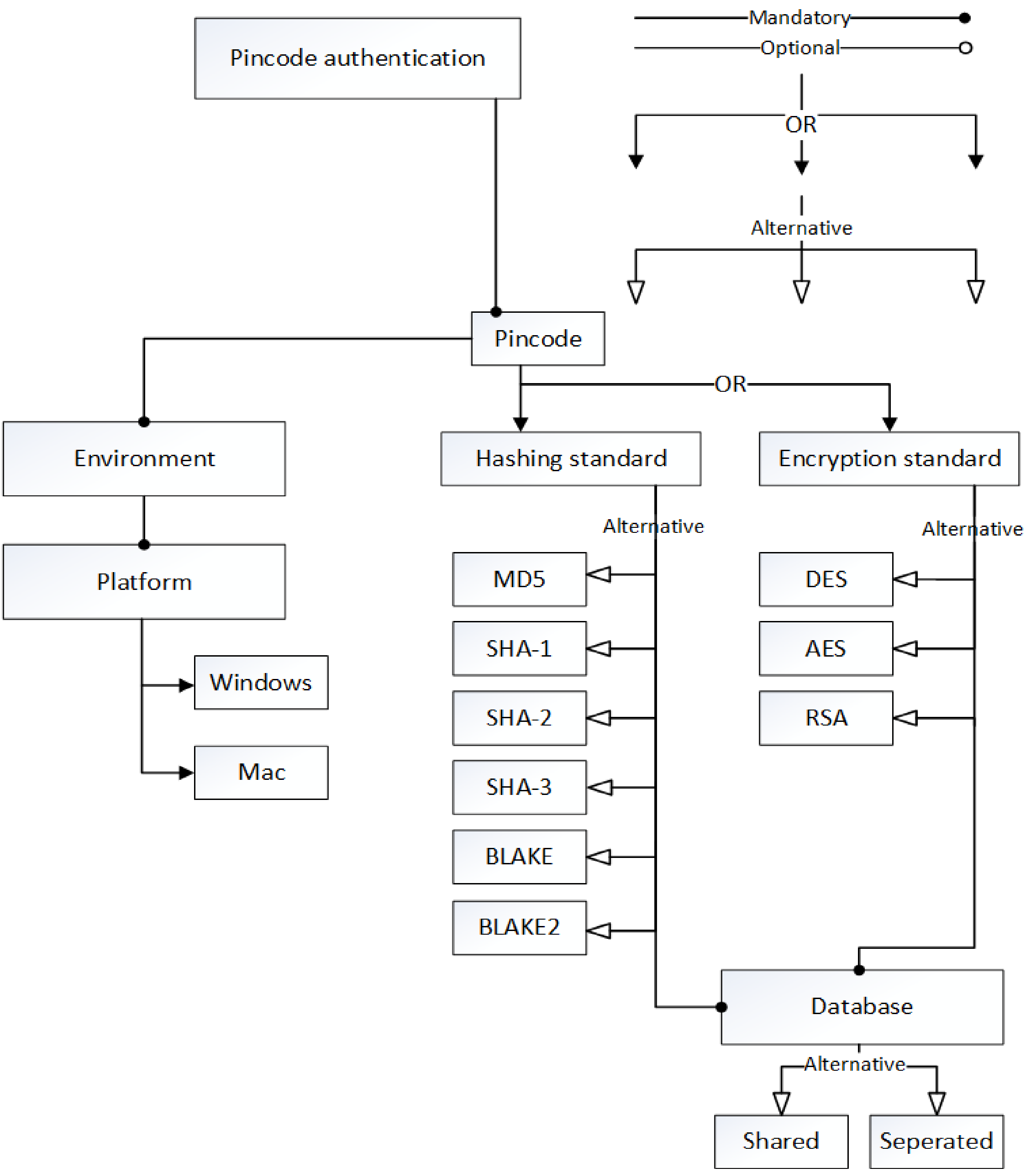


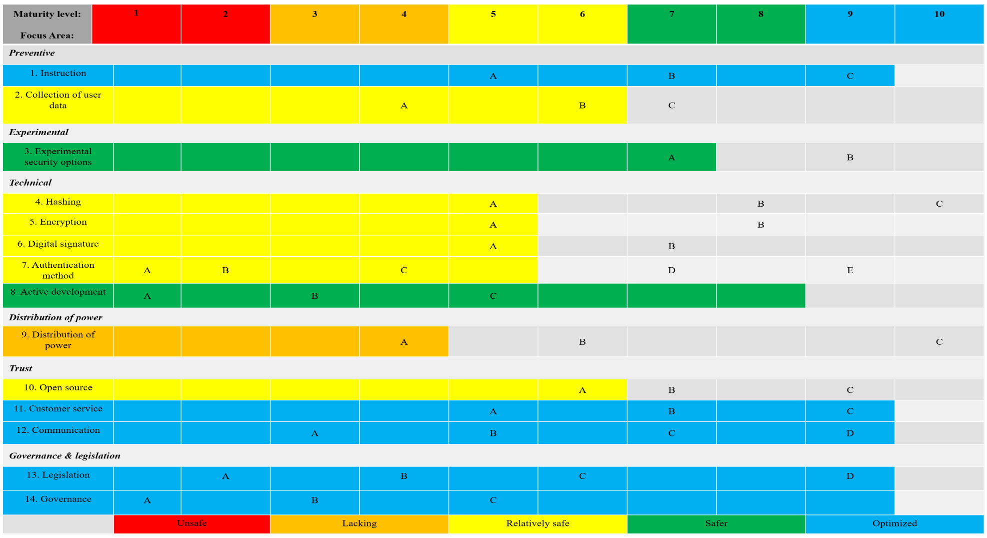
Figure B.4: Pincode verification feature model

# Appendix C

Below are the tables with description of all investigated key process areas, their assigned capability level and the description of the current situation. Below every table is the filled in model that belongs to the service that has been reviewed.

| *Data: #1 Binance* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Users are prompted to check the website's address before every login. On registration users receive some extra instruction they need to check off before being able to continue. Afterwards users are strongly recommended to activate 2-FA using either SMS or Authenticator, there is also an option to skip this step. Security recommendations are shown above your profile every time you login. | C |
| Collection of user data | Preventive | Without KYC you are allowed to withdraw up to 2BTC every 24 hours. This may seem as if that is not a lot but BTC are the most valuable cryptocurrency and represent on time of writing about $18.000. If you want to be able to withdraw up to 100BTC a day the exchange requires extensive KYC including first name, last name, date of birth, address, postal code, city and coutary. It also needs proof of ID and a picture of the users face in combination with a legal letter. | B |
| Experimental security options | Experimental | Binance offers no experimental, cutting edge security options. | A |
| Hashing | Technical | Data not available | A |
| Encryption | Technical | Data not available | A |
| Digital Signature | Technical | Data not available | A |
| Authentication method | Technical | Authentication is done by a combination of e-mail and password. However, users are strongly prompted to enable 2-FA using either SMS or authenticator when they register, there is an option to skip this step but it is depicted in a corner in a very small font. | C |
| Active development | Technical | Binance is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | Binance controls the private keys, users do not. | A |
| Open source | Trust | Binance is not open source. | A |
| Customer service | Trust | Extensive FAQ, specialized twitter account, fast help and barely any negative reviews on the internet | C |
| Communication | Trust | Regular updates on facebook, twitter, telegram, blog. | D |
| Legislation | Governance & legislation | Company is based in Tokyo, Japan which has advanced legislation. | C |
| Governance | Governance & legislation | Company is based in Tokyo, Japan. Governance in Japan is optimized. | C |
| Maturity level | | Extensive repeated instruction. No KYC up to 2btc/24h. 2-FA, but unfortunately supports SMS. Customer service and communication are extensive and intuitive. Japan is known to be a frontrunner in the cryptocurrency ecosystem | 4 |
| Maturity score | | | 93 |

Table C.1: Binance review

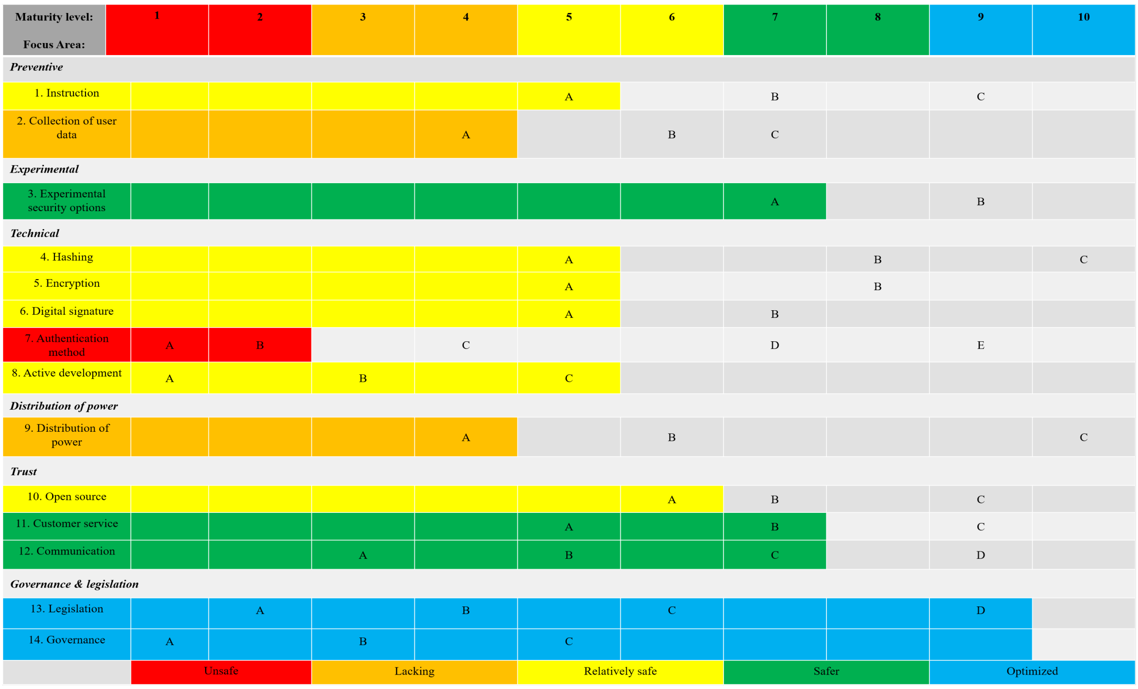


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.1: Binance Model

| *Data: # 2 OKEx.com* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Barely any instruction on registration, only on how to trade. | A |
| Collection of user data | Preventive | Extensive KYC, can't trade without it. | A |
| Experimental security options | Experimental | OKEx offers no experimental, cutting edge security options. | A |
| Hashing | Technical | Data not available | A |
| Encryption | Technical | Data not available | A |
| Digital Signature | Technical | Data not available | A |
| Authentication method | Technical | Authentication is done by a combination of e-mail and password. Users can enable 2-FA by either SMS or Authenticator. You are only prompted to enable either when you visit the account safety tab. | B |
| Active development | Technical | OKEx is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | OKEx controls the private keys, users do not. | A |
| Open source | Trust | OKEx is not open source. | A |
| Customer service | Trust | No FAQ, There are facebook and twitter accounts names OKEx support, but they are not linked to from the website and have very few likes/follows. Ticket seems like the main/only way of contacting them. | B |
| Communication | Trust | Regular updates on facebook, twitter. | C |
| Legislation | Governance & legislation | OKex is based in Malta. The legislation concerning cryptocurrencies in Malta is optimized. | C |
| Governance | Governance & legislation | OKex is based in Malta. Governance in Malta can be considered good. | C |
| Maturity level | | Barely any instruction. Extensive KYC. Lacking authentication protocol. Lacking customer service. Legislation is not up-to-date. Governance in Kuala Lumpur is decent. | 2 |
| Maturity score | | | 69 |

Table C.2: Okex.com review

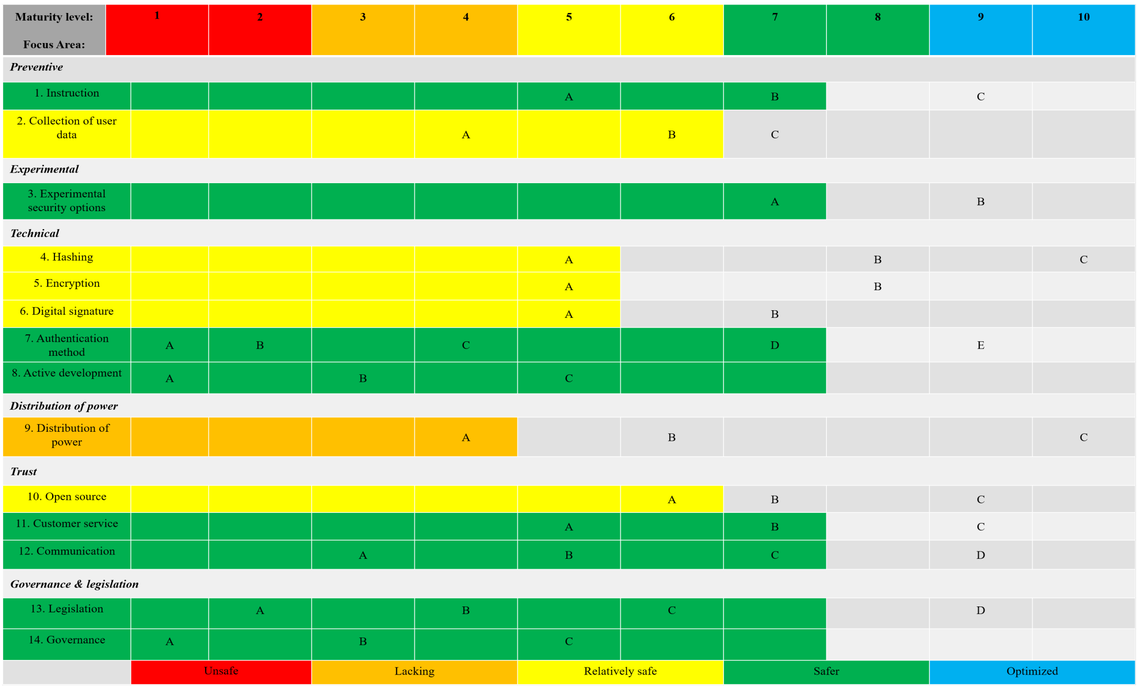


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.2: Okex Model

| *Data: #3 DigiFinex.com* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Some instruction, when you go to user profile there are repeated hints on security. | B |
| Collection of user data | Preventive | Can withdraw up to 1BTC ($9.000) per 24 hours. In order to withdraw more there is extensive KYC. | B |
| Experimental security options | Experimental | Digifinex offers no experimental, cutting edge security options. | A |
| Hashing | Technical | Data not available | A |
| Encryption | Technical | Data not available | A |
| Digital Signature | Technical | Data not available | A |
| Authentication method | Technical | Authentication is done by e-mail, password and OTP e-mail codes on every login. 2-FA is strongly recommended and does only support Authenticator and no SMS. | D |
| Active development | Technical | Digifinex is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | Digifinex controls the private keys, users do not. | A |
| Open source | Trust | OKEx is not open source. | A |
| Customer service | Trust | There is a FAQ. Help center does not link to Twitter, Facebook or other social media options. Only a ticket option available. | B |
| Communication | Trust | Regular updates on facebook, twitter, Telegram and notice board. | C |
| Legislation | Governance & legislation | Company is based in Singapore, Signapore where the legislation on the cryptocurrency ecosystem is good but not optimal (yet). | C |
| Governance | Governance & legislation | Company is based in Singapore, Singapore where governance is considered good. | C |
| Maturity level | | Instructs users, but could do better. Allows users to make use of the exchange without extensive KYC to an extent. Secure authentication protocol. Customer service seems decent. Singapore has no up-to-date legislation yet, but will have one in the near future. | 4 |
| Maturity score | | | 83 |

Table C.3: DigiFinex.com review

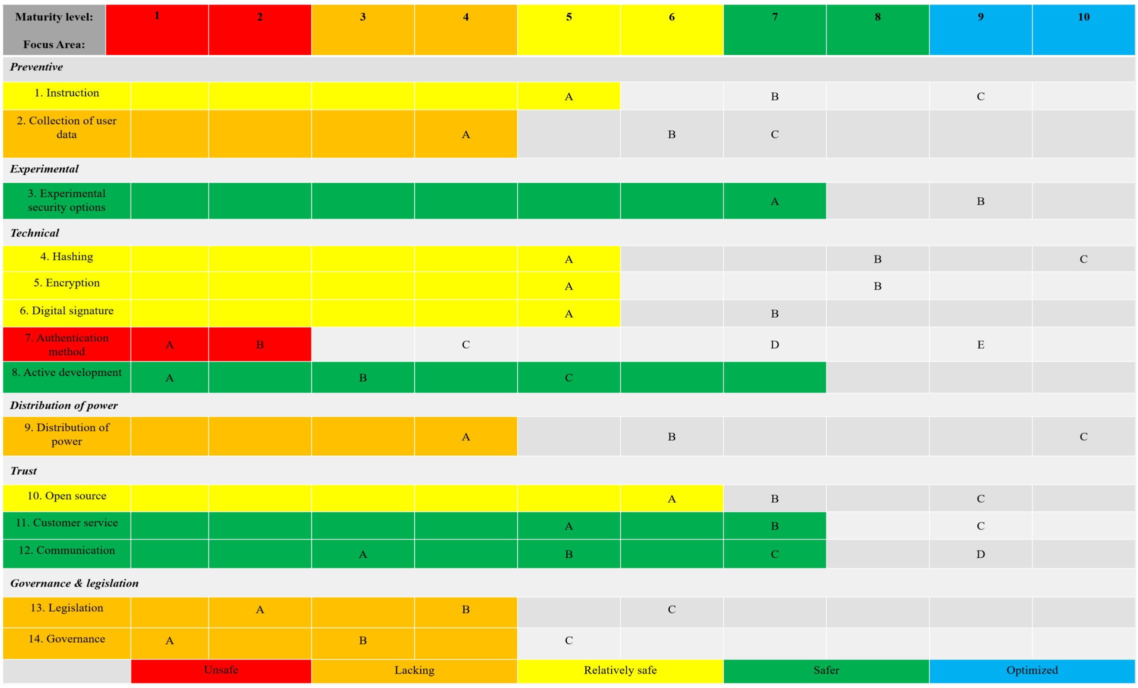


| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| *Preventive* | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| *Experimental* | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| *Technical* | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| *Distribution of power* | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| *Trust* | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| *Governance & legislation* | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.3: Digifinex Model

| *Data: # 4 DOBI exchange.com* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | No instruction on registration, no repeated instruction. | A |
| Collection of user data | Preventive | Extensive KYC | A |
| Experimental security options | Experimental | DOBI exchange offers no experimental, cutting edge security options. | A |
| Hashing | Technical | Data not available | A |
| Encryption | Technical | Data not available | A |
| Digital Signature | Technical | Data not available | A |
| Authentication method | Technical | Authentication is done by e-mail, password 2-FA is optional and does only support Authenticator and no SMS. | B |
| Active development | Technical | DOBI is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | DOBI controls the private keys, users do not. | A |
| Open source | Trust | DOBI is not open source. | A |
| Customer service | Trust | There is a small FAQ. Help is hidden somewhere at the bottom and redirects back to the FAQ. Not even a ticket option, just an e-mail address. | B |
| Communication | Trust | Regular updates on facebook, twitter, Telegram and notice board. | C |
| Legislation | Governance & legislation | Company is based in Hongkong, China where the legislation on the cryptocurrency ecosystem is not yet up-to-date. Country is not mentioned on the website, only on social media. No address. | B |
| Governance | Governance & legislation | Company is based in China, where governance is all right. | B |
| Maturity level | | No instruction for users. Extensive KYC. Lacking authentication protocol. Lacking customer support. No address. | 2 |
| Maturity score | | | 68 |

Table C.4: DOBI exchange.com review

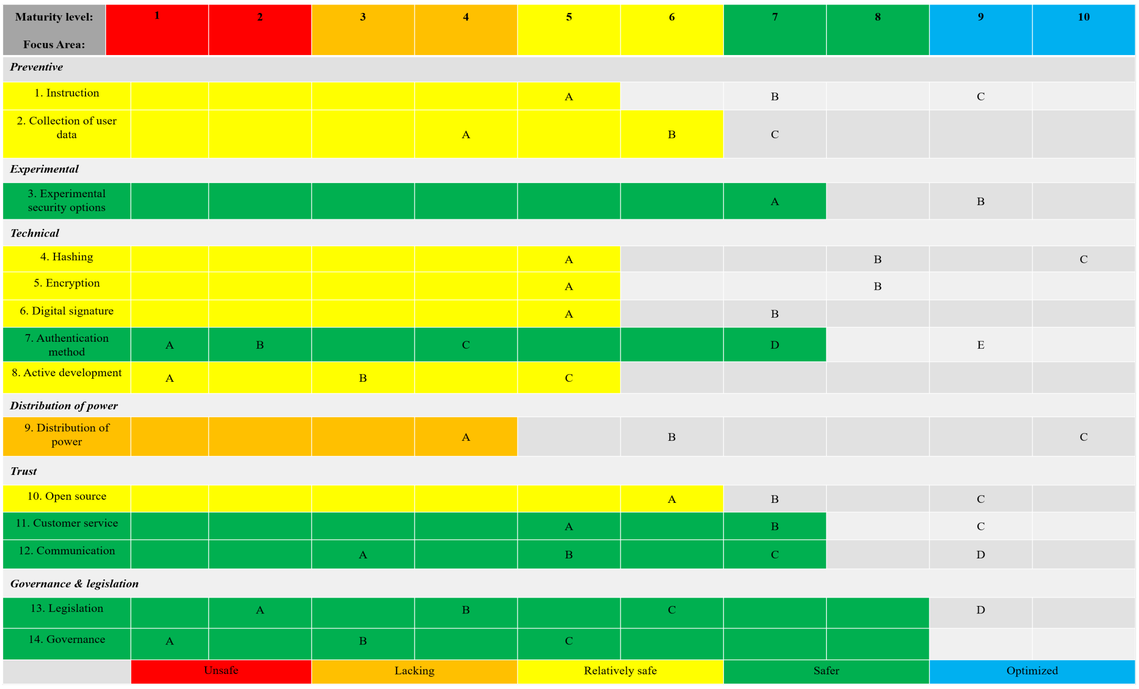


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.4: Dobi exchange Model

| *Data: # 5 Bitmax.io* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | No instruction on registration, no repeated instruction. | A |
| Collection of user data | Preventive | Can withdraw up to 2BTC ($18.000) per 24 hours. In order to withdraw more there is extensive KYC | B |
| Experimental security options | Experimental | Bitmax offers no experimental, cutting edge security options. | A |
| Hashing | Technical | Data not available | A |
| Encryption | Technical | Data not available | A |
| Digital Signature | Technical | Data not available | A |
| Authentication method | Technical | Authentication is done by e-mail, password. 2-FA is required for withdrawals, changes of password and other security settings and only support authenticator. | D |
| Active development | Technical | Bitmax is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | Bitmax controls the private keys, users do not. | A |
| Open source | Trust | Bitmax is not open source. | A |
| Customer service | Trust | There is a FAQ. Help center does not link to Twitter, Facebook or other social media options. Only a ticket option available. | B |
| Communication | Trust | Regular updates on facebook, twitter, Telegram and notice board. | C |
| Legislation | Governance & legislation | Company is based in Switzerland a country that adheres to the EU AML laws. | C |
| Governance | Governance & legislation | Company is based in Switzerland where governance is considered good. | C |
| Maturity level | | Could definitely instruct their users on safety more. Most technical details are unknown to outsiders. Has control over their users private keys, so a target for hacks and insiders. Customer service could be increased. Allows use of exchange without KYC, relatively safe authentication protocol. | 4 |
| Maturity score | | | 82 |

Table C.5: Bitmax review

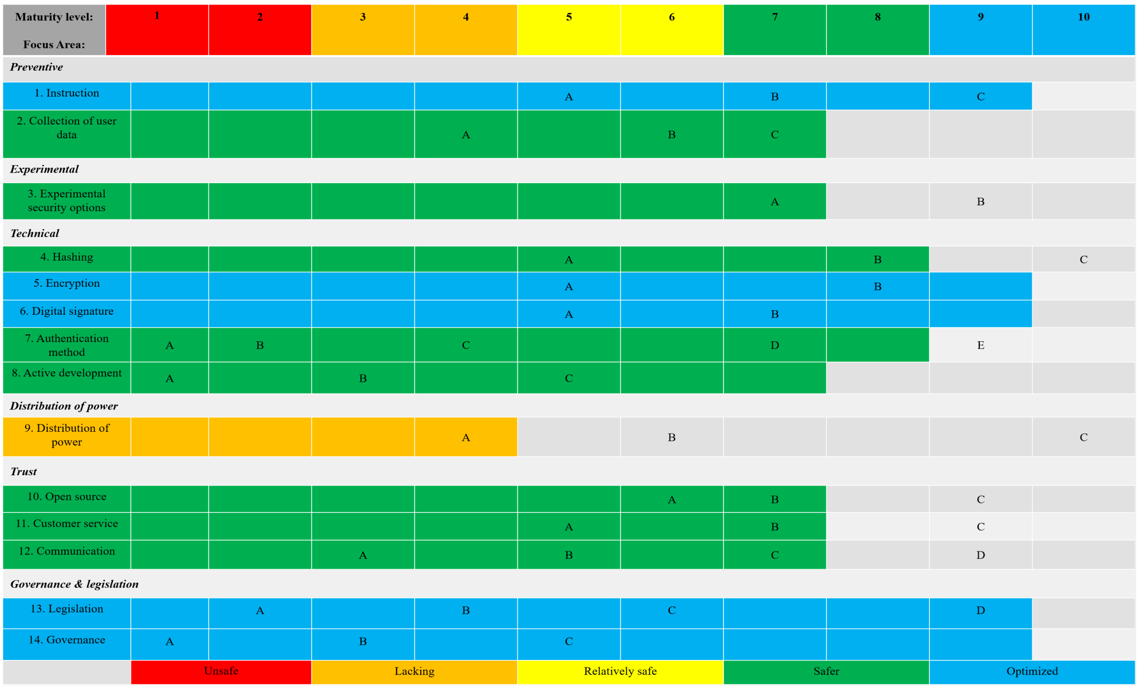


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.5: Bitmax Model

| *Data: # 6 BitGo* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Users receive immediate feedback on the strength of their passwords. Users are prompted with different choices when creating a backup key, users are instructed on the differences in security. If an user chooses to keep their own private and backup key they are shared via pdf. There are extensive instructions on safety in the key pdf. Users are prompted to save their keys securely, offline. | C |
| Collection of user data | Preventive | There is no extensive KYC. You can use the wallet without providing address, legal ID or photo ID. You are prompted to give your name and e-mail address, but since users do not need to verify this it is possible to use the service more or less anonymously. | C |
| Experimental security options | Experimental | BitGo offers no experimental, cutting edge security options. | A |
| Hashing | Technical | BitGo uses SHA-512 when generating master keys. SHA-512 is part of the SHA-2 family | B |
| Encryption | Technical | BitGo encrypts user data using json web encryption (AES-128 [108]) | B |
| Digital Signature | Technical | BitGo uses ECDSA. | B |
| Authentication method | Technical | Authentication is done by e-mail, password and Authenticator (token). This is the minimum. | D |
| Active development | Technical | Bitmax is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | When making use of the BitGo custody service they have control over your private keys. | A |
| Open source | Trust | BitGo is not entirely open source, but has a github with a public SDK and API. | B |
| Customer service | Trust | Extensive FAQ. Ticket option. | B |
| Communication | Trust | Regular updates on Twitter, some blogposts. | C |
| Legislation | Governance & legislation | Company is based in California, USA. Legislation in the USA is good. | C |
| Governance | Governance & legislation | Company is based in California, USA. Governance in the USA is good. | C |
| Maturity level | | | 4 |
| Maturity score | | | 99 |

Table C.6: BitGo review

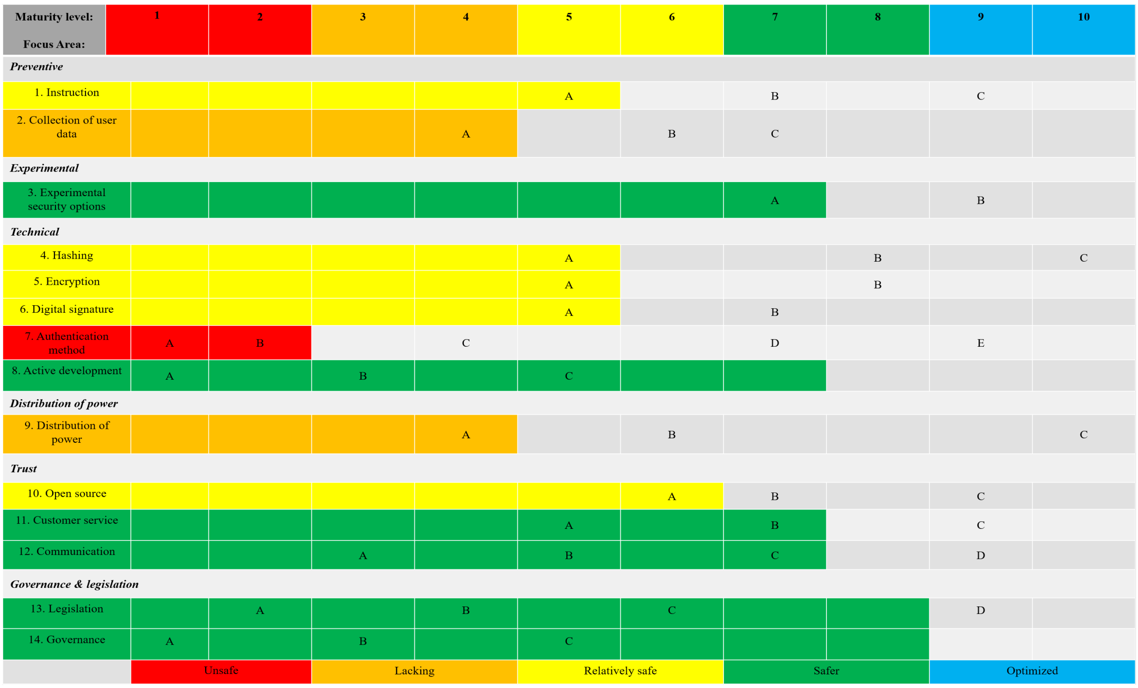


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.6: BitGo Model

| *Data: #7 Xapo* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Hardly any instruction on safety. | A |
| Collection of user data | Preventive | Extensive KYC, need ID and photo. | A |
| Experimental security options | Experimental | Xapo does not use experimental security options. | A |
| Hashing | Technical | Data unavailable. | A |
| Encryption | Technical | Data unavailable. | A |
| Digital Signature | Technical | Data unavailable. | A |
| Authentication method | Technical | Authentication is done by e-mail, password and PINcode. You can even log in by using facebook or google. | B |
| Active development | Technical | Xapo is monitored continuously and updated regularly. | C |
| Distribution of power | Distribution of power | When making use of the Xapo custody service they have control over your private keys. | A |
| Open source | Trust | Xapo is not open source. | A |
| Customer service | Trust | Extensive FAQ. Ticket option. | B |
| Communication | Trust | Regular updates on Twitter, some blogposts. | C |
| Legislation | Governance & legislation | Company is based in Zurich Switzerland. Legislation in Switzerland is good. | C |
| Governance | Governance & legislation | Company is based in Zurich Switzerland. Governance in Switzerland is good. | C |
| Maturity level | | | 2 |
| Maturity score | | | 77 |

Table C.7: Xapo review

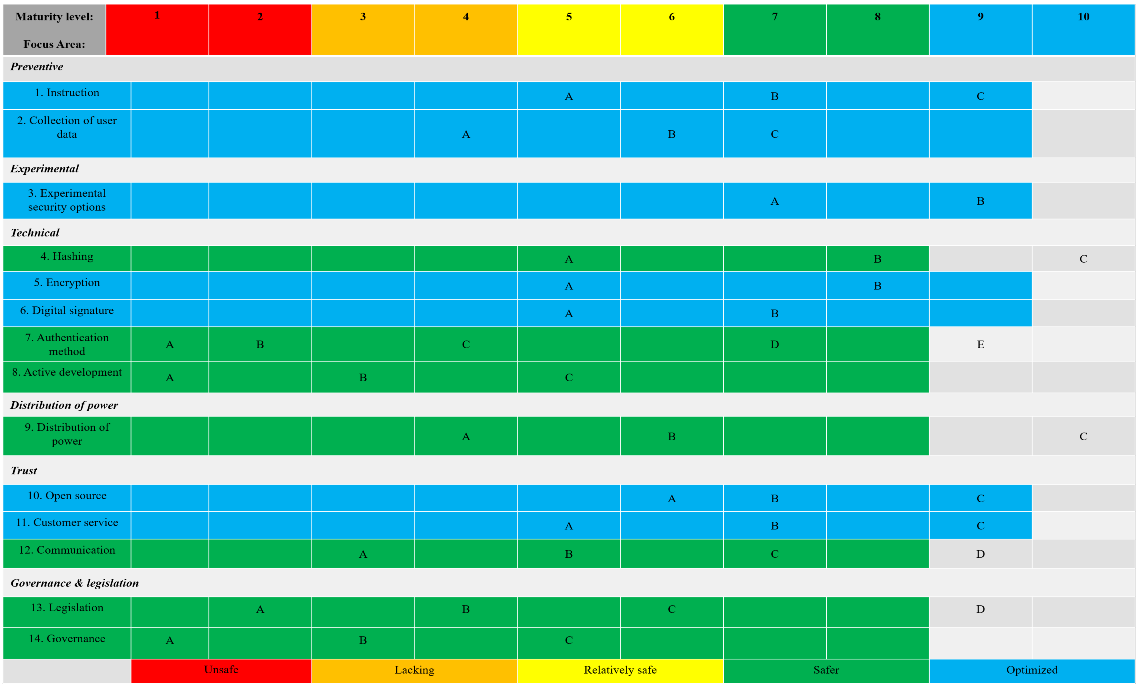


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.7: Xapo Model

| *Data: #8 Trezor* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Instruction on what the hologprahic sticker should look like, instruction on making a pin code, instruction on what to do with the seeds to recover the wallet if anything happens. | C |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | The hardware itself is purely specialized equipment. | B |
| Hashing | Technical | Trezor uses SHA-256. | B |
| Encryption | Technical | Trezor uses AES-256. | C |
| Digital Signature | Technical | Trezor uses ECDSA. | C |
| Authentication method | Technical | Trezor requires users to have the physical device. The device needs a 9 digit pin code. A password is needed when connecting to a computer. | D |
| Active development | Technical | Trezor is developed actively and any weaknesses are fixed as soon as possible. | C |
| Distribution of power | Distribution of power | Trezor allows users full control over their private keys. | C |
| Open source | Trust | Trezor is open source. | C |
| Customer service | Trust | Extensive FAQ. Ticket option. Community support. Active on Reddit, Facebook, Twitter and GitHub. | C |
| Communication | Trust | Regular updates on Twitter, Facebook and website. | C |
| Legislation | Governance & legislation | SatoshiLabs is based in Prague, Czech replublic. Legislation in the EU is good. | C |
| Governance | Governance & legislation | SatoshiLabs is based in Prague, Czech replublic. Governance in the EU is good. | C |
| Maturity level | | | 8 |
| Maturity score | | | 119 |

Table C.8: Trezor review

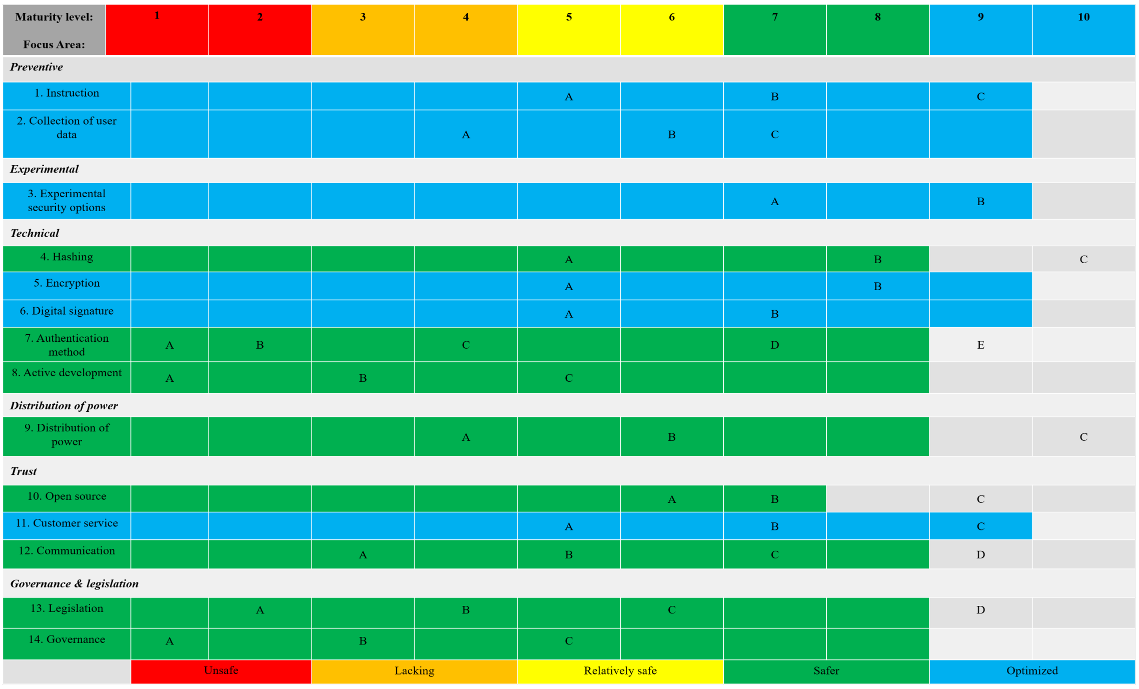


| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| *Preventive* | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| *Experimental* | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| *Technical* | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| *Distribution of power* | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| *Trust* | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| *Governance & legislation* | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.8: Trezor Model

| *Data: # 9 Ledger* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Instruction on making a pin code, instruction on what to do with the seeds to recover the wallet if anything happens. | C |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Although pushing the boundaries of tech, there is nothing we can really call experimental. | A |
| Hashing | Technical | Ledger uses SHA-256. | B |
| Encryption | Technical | Ledger uses AES-256. | C |
| Digital Signature | Technical | Ledger uses ECDSA. | C |
| Authentication method | Technical | Ledger requires users to have the physical device. The device needs a 4-8 pin code. Additionally a password is needed when connecting to a computer. | D |
| Active development | Technical | Ledger is developed actively and any weaknesses are fixed as soon as possible. | C |
| Distribution of power | Distribution of power | Ledger allows users full control over their private keys. | C |
| Open source | Trust | Ledger is partly open source, but the bootloader is not. | B |
| Customer service | Trust | Extensive FAQ. Ticket option. Community support. Active on Reddit, Facebook, Twitter and GitHub. Active customer support on Twitter during work hours. | C |
| Communication | Trust | Regular updates on Twitter, Facebook and website. | C |
| Legislation | Governance & legislation | Ledger is based in Paris, France. Legislation in the EU is good. | C |
| Governance | Governance & legislation | Ledger is based in Paris, France. Governance in the EU is good. | C |
| Maturity level | | | 7 |
| Maturity score | | | 117 |

Table C.9: Ledger review

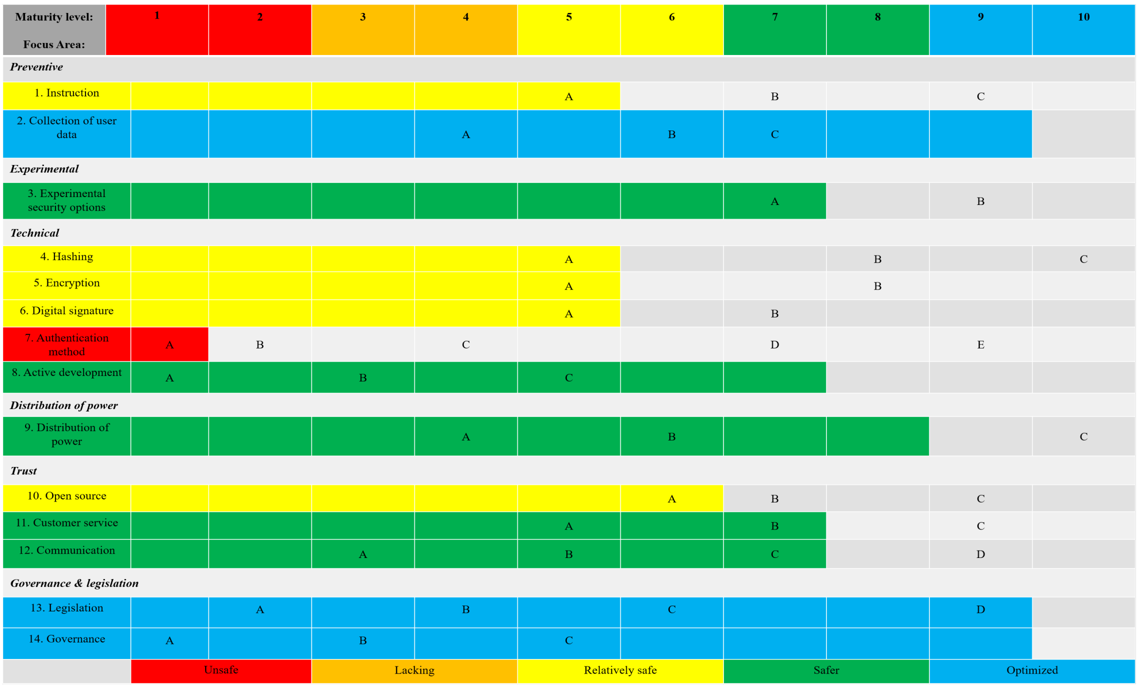


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.9: Ledger Model

| *Data: #10 Exodus* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | No Instruction without looking for it hard. When taking a look at your private keys there is a warning. | A |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Nothing experimental. | A |
| Hashing | Technical | Exodus does not hash anything, there are no security options. | A |
| Encryption | Technical | Exodus does not encrypt anything. | A |
| Digital Signature | Technical | Exodus uses ECDSA. | C |
| Authentication method | Technical | There is no authentication. | A |
| Active development | Technical | Exodus is updated once every two weeks. | C |
| Distribution of power | Distribution of power | Exodus allows users full control over their private keys. | C |
| Open source | Trust | Exodus is not open source. | A |
| Customer service | Trust | Extensive FAQ. Ticket option. Active on Facebook, Twitter and Slack. | B |
| Communication | Trust | Regular updates on Twitter, Facebook and website.. | C |
| Legislation | Governance & legislation | Exodus movement inc. is based in the US. Legislation in the US is top notch. | D |
| Governance | Governance & legislation | Exodus movement inc. is based in the US. Governance in the US is top notch. | C |
| Maturity level | | | 1 |
| Maturity score | | | 90 |

Table C.10: Exodus review

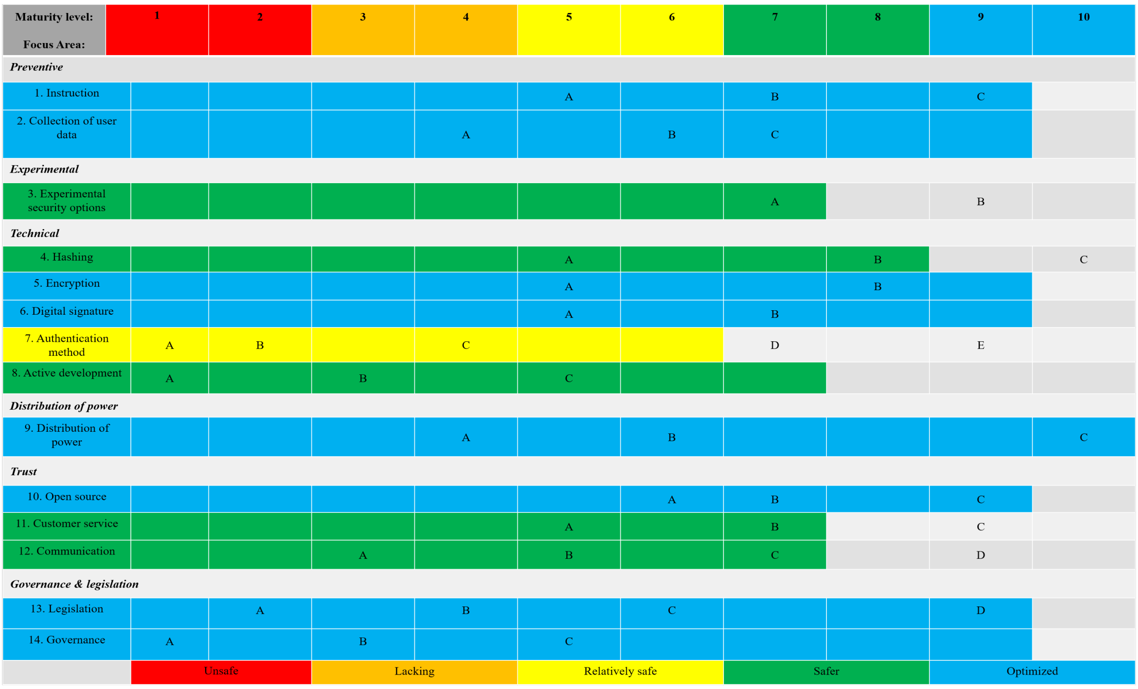


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.10: Exodus Model

| *Data: #11 Electrum* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Instructions to only download from a single source, warnings about older versions. Digital signature in PGP format included to verify download. Seed is not copyable, need to re-enter it, instruction on safekeeping. Instruction on password creation. | C |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | A lot of instruction and safety measures, but nothing experimental. | A |
| Hashing | Technical | Seed keys are hashed using SHA-256. | B |
| Encryption | Technical | Electrum encrypts seeds and private keys using AES-256. | C |
| Digital Signature | Technical | Electrum uses ECDSA. | C |
| Authentication method | Technical | 2 factor or even multisig. 2-FA using an authenticator. | C |
| Active development | Technical | Electrum receives a major update every 3 months, with smaller updates in between. | C |
| Distribution of power | Distribution of power | Electrum allows users full control over their private keys. | C |
| Open source | Trust | Electrum is open source. | C |
| Customer service | Trust | Extensive FAQ, help through Twitter. | B |
| Communication | Trust | Regular updates on Twitter, GitHub and website. | C |
| Legislation | Governance & legislation | Electrum is based in the US. Legislation in the US is good. | C |
| Governance | Governance & legislation | Electrum is based in the US. Governance in the US is good. | C |
| Maturity level | | | 6 |
| Maturity score | | | 115 |

Table C.11: Electrum review

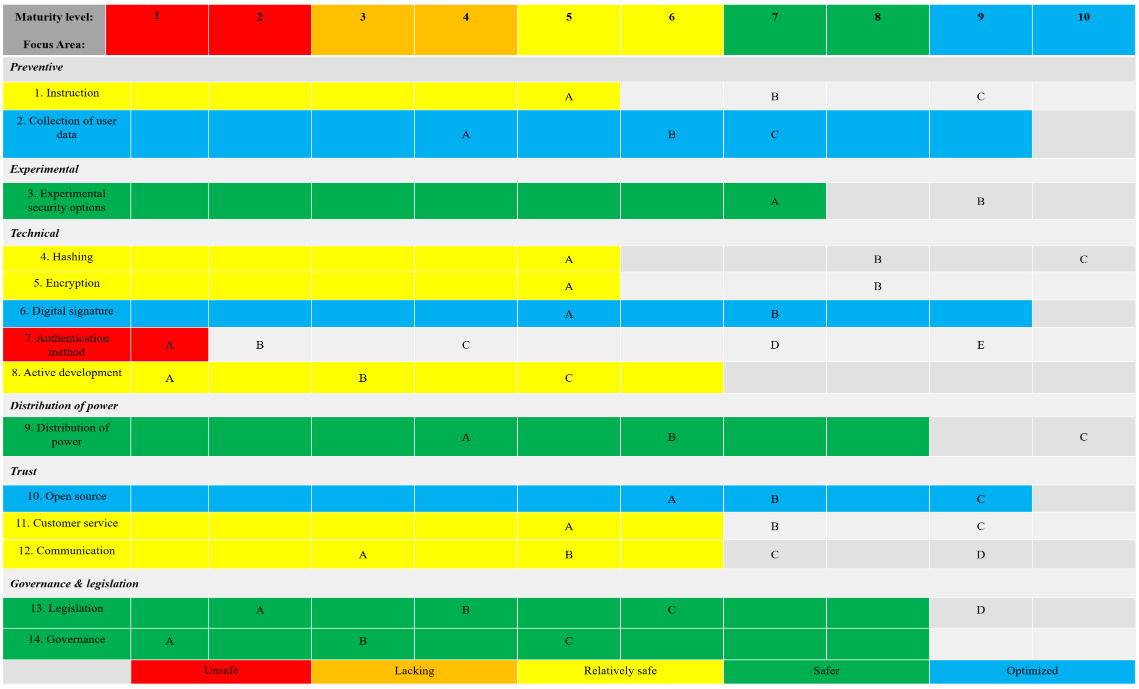


| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| *Preventive* | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| *Experimental* | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| *Technical* | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| *Distribution of power* | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| *Trust* | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| *Governance & legislation* | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.11: Electrum Model

| *Data: #12 Bitcoin Core* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | No instructions on safety. | A |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Nothing. | A |
| Hashing | Technical | No hashing | A |
| Encryption | Technical | No encryption | A |
| Digital Signature | Technical | Bitcoin core uses ECDSA. | C |
| Authentication method | Technical | No authentication. | A |
| Active development | Technical | Bitcoin core receives a major update every 2 months, with smaller updates in between. | C |
| Distribution of power | Distribution of power | Bitcoin core allows users full control over their private keys. | C |
| Open source | Trust | Bitcoin core is open source. | C |
| Customer service | Trust | No specialized FAQ, referred to general forums | B |
| Communication | Trust | Some updates on Twitter and RSS feed. | B |
| Legislation | Governance & legislation | Bitcoin core is developed purely open source, but the domain is in hands of Martti Malmi who is Finnish. Legislation in the EU is good. | C |
| Governance | Governance & legislation | Bitcoin core is developed purely open source, but the domain is in hands of Martti Malmi who is Finnish. Governance in the EU is good. | C |
| Maturity level | | | 1 |
| Maturity score | | | 92 |

Table C.12: Bitcoin Core review

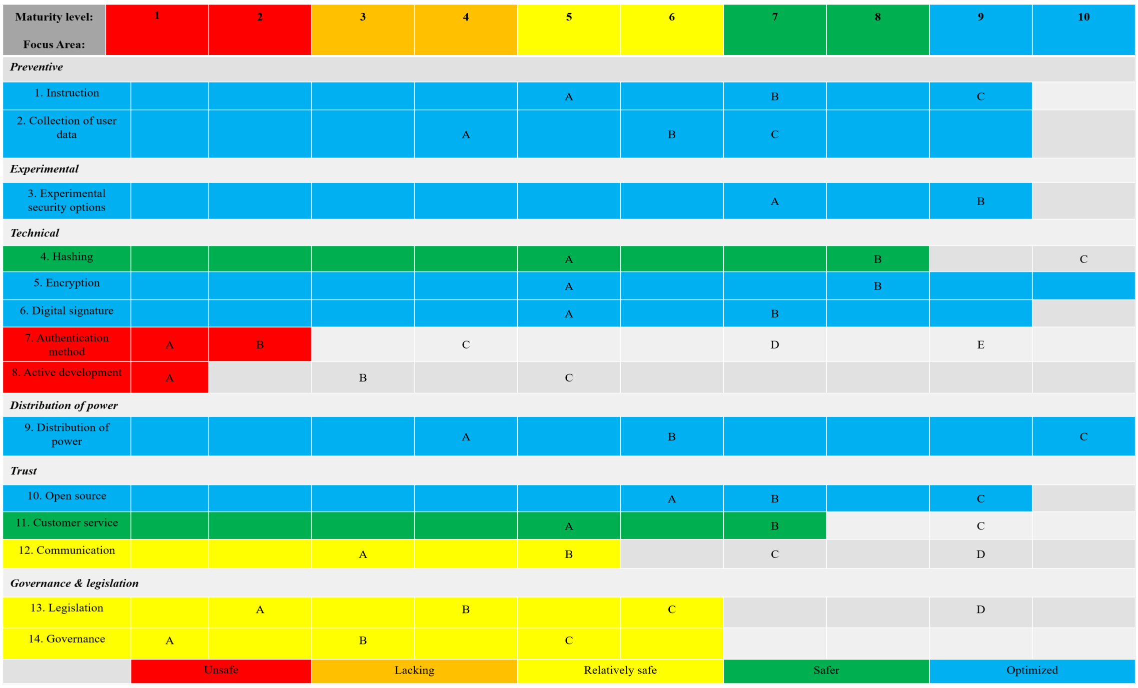


| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| *Preventive* | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| *Experimental* | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| *Technical* | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| *Distribution of power* | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| *Trust* | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| *Governance & legislation* | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.12: Bitcoin core Model

| *Data: #13 Armory* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Advanced instruction on all safety options, methods of saving the passphrase and backing up your wallet. | C |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Encryption can be selected on the time and space you wish it to be. Longer times and more space means better encryption. Wallets can be made watch only, so they do not store private keys but can be used to verify transactions. Amory allows for settings to use Armory over the Tor-Network. | B |
| Hashing | Technical | Armory uses SHA-256. | B |
| Encryption | Technical | Armory uses AES with varying bit size depending on what the user wants. | C |
| Digital Signature | Technical | Armory uses ECDSA. | C |
| Authentication method | Technical | Typically just a password, but Armory allows for multisig wallets spread over multiple devices and offline signing of transactions. | C |
| Active development | Technical | Armory has last been updated over a year ago. | A |
| Distribution of power | Distribution of power | Armory allows users full control over their private keys. | C |
| Open source | Trust | Armory is open source. | C |
| Customer service | Trust | An FAQ a bit on the small side. There is no e-mail, only an IRC channel. | B |
| Communication | Trust | Updates on the website | B |
| Legislation | Governance & legislation | Armory technologies inc. is a company based in the US. However they discontinued their work on armory, which is now in the hands of the community. | C |
| Governance | Governance & legislation | Armory technologies inc. is a company based in the US. However they discontinued their work on armory, which is now in the hands of the community. | C |
| Maturity level | | | 1 |
| Maturity score | | | 100 |

Table C.13: Armory review

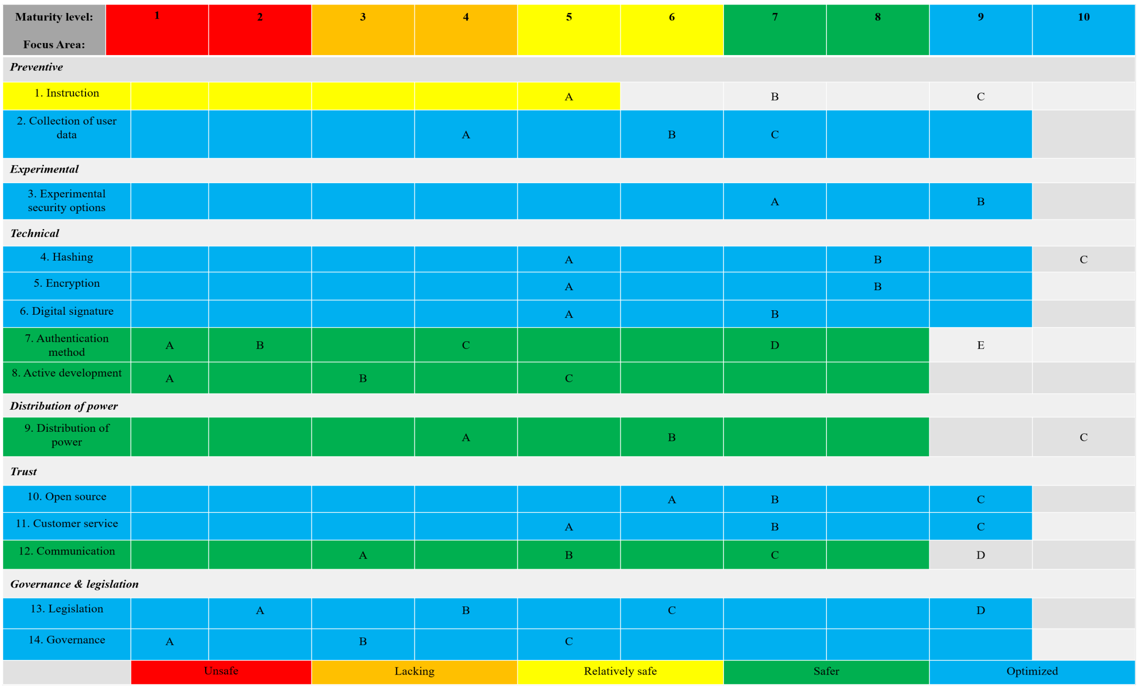


| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.13: Armory Model

| *Data:#14 Edge* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Hardly any instruction. | A |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Hiding of master private keys at any time. | B |
| Hashing | Technical | Edge uses Scrypt. | C |
| Encryption | Technical | Edge uses AES-256. | C |
| Digital Signature | Technical | Edge uses ECDSA. | C |
| Authentication method | Technical | Edge uses an username & password combination, and a PINcode to relogin within an hour of signing out. Optional 2-FA. Of course the mobile device is needed as well. | C |
| Active development | Technical | Edge is updated once a month. | C |
| Distribution of power | Distribution of power | Edge allows users full control over their private keys. | C |
| Open source | Trust | Edge is open source. | C |
| Customer service | Trust | No FAQ in app, but dedicated support via telephone. | C |
| Communication | Trust | Updates on the google play store and on the website. | C |
| Legislation | Governance & legislation | Edge is based in California, in the United States where legislation can be considered good. | C |
| Governance | Governance & legislation | Edge is based in California, in the United States where governance can be considered good. | C |
| Maturity level | | | 5 |
| Maturity score | | | 118 |

Table C.14: Edge review

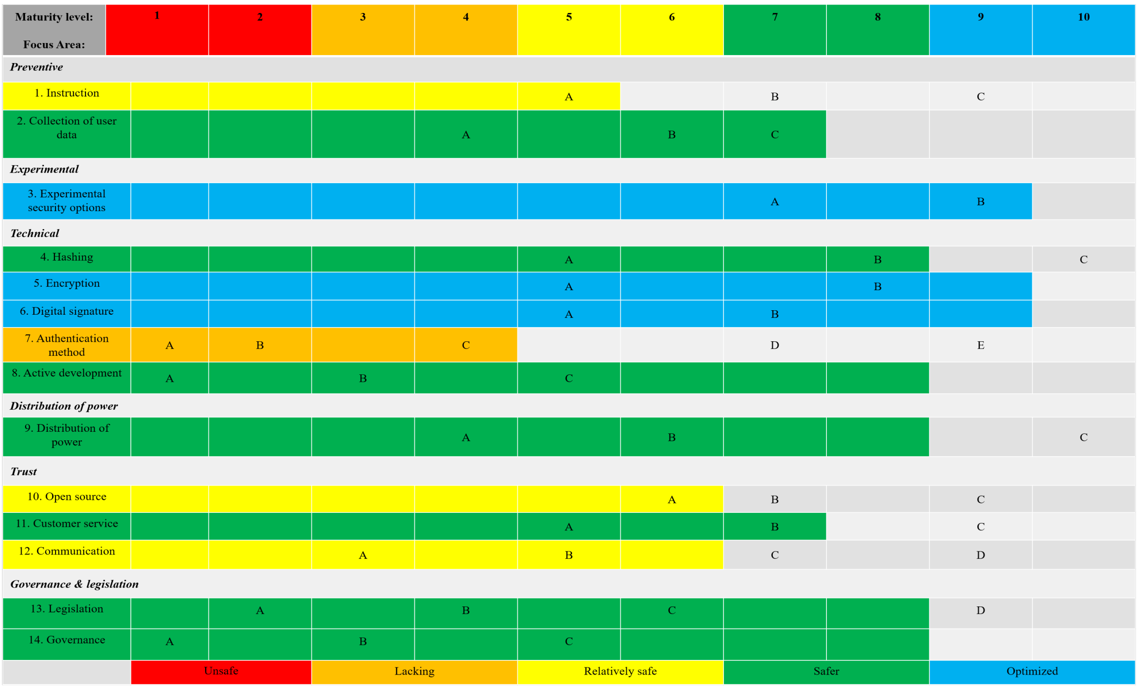


| **Maturity level:**<br>**Focus Area:** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.14: Edge Model

| *Data: #15 Coinomi* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Instruction on keeping your master seed, what to do with it and what happens when you lose it. | A |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Users are prompted to save their master seed, then re-enter it to make sure they have it saved. However, re-entering is not done by keyboard but by clicking the words which are placed on the screen which avoids the master seed being key-logged. Still vulnerable to screen logging however | B |
| Hashing | Technical | Coinomi uses SHA-256 according to BIP39 to hash the master seed. | B |
| Encryption | Technical | Coinomi uses AES-256. | C |
| Digital Signature | Technical | Coinomi uses ECDSA. | C |
| Authentication method | Technical | A password is used. Optional to replace with PIN or fingerprint. | C |
| Active development | Technical | Coinomi is updated once a month. | C |
| Distribution of power | Distribution of power | Coinomi allows users full control over their private keys. | C |
| Open source | Trust | Coinomi does not seem to be open source, debatable. | B |
| Customer service | Trust | No FAQ in app, but dedicated support via telephone. | B |
| Communication | Trust | Updates on the google play store and on the website. | B |
| Legislation | Governance & legislation | Coinomi is based in the EU-part of Cyprus, which has good legislation. | C |
| Governance | Governance & legislation | Coinomi is based in the EU-part of Cyprus, which has good governance. | C |
| Maturity level | | | 4 |
| Maturity score | | | 102 |

Table C.15: Coinomi review

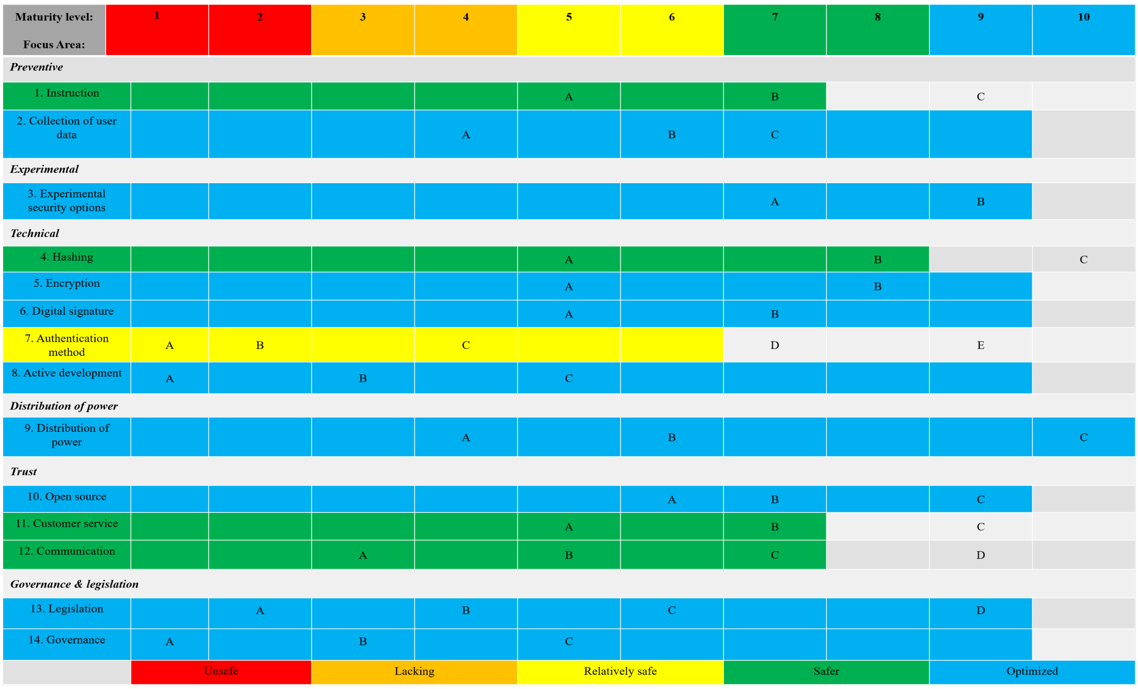


| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Preventive*** | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| ***Experimental*** | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| ***Technical*** | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| ***Distribution of power*** | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| ***Trust*** | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| ***Governance & legislation*** | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.15: Coinomi Model

| *Data: #16 Greenadress* | *Category* | *Description* | *Capability level* |
|---|---|---|---|
| Instruction | Preventive | Some instruction on writing down the master seed and keeping it safe. | B |
| Collection of user data | Preventive | No KYC at all. | C |
| Experimental security options | Experimental | Master seed is entered using randomly generated on screen words you need to touch. Optional PGP support for any e-mails. | B |
| Hashing | Technical | Greenadress uses SHA-256 according to BIP39 to hash the master seed. | B |
| Encryption | Technical | Greenadress uses AES-256. | C |
| Digital Signature | Technical | Greenadress uses ECDSA. | C |
| Authentication method | Technical | Greenadress requires 2-FA, but supports e-mail and SMS in addition to authenticator and calls. | C |
| Active development | Technical | Greenadress is updated once a month. | C |
| Distribution of power | Distribution of power | Greenadress allows users full control over their private keys, and supports multisig. | D |
| Open source | Trust | Greenadress is an open source. | C |
| Customer service | Trust | No FAQ in app but FAQ on website, Twitter and e-mail. | B |
| Communication | Trust | Updates on the google play store and on the website. | C |
| Legislation | Governance & legislation | Greenadress is based in Malta, which has good legislation. | D |
| Governance | Governance & legislation | Greenadress is based in Malta, which has good governance. | C |
| Maturity level | | | 6 |
| Maturity score | | | 127 |

Table C.16: Greenadress review



| Maturity level:<br>Focus Area: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| *Preventive* | | | | | | | | | | |
| 1. Instruction | | | | | A | | B | | C | |
| 2. Collection of user data | | | | A | | B | C | | | |
| *Experimental* | | | | | | | | | | |
| 3. Experimental security options | | | | | | | A | | B | |
| *Technical* | | | | | | | | | | |
| 4. Hashing | | | | | A | | | B | | C |
| 5. Encryption | | | | | A | | | B | | |
| 6. Digital signature | | | | | A | | B | | | |
| 7. Authentication method | A | B | | C | | | D | | E | |
| 8. Active development | A | | B | | C | | | | | |
| *Distribution of power* | | | | | | | | | | |
| 9. Distribution of power | | | | A | | B | | | | C |
| *Trust* | | | | | | | | | | |
| 10. Open source | | | | | | A | B | | C | |
| 11. Customer service | | | | | A | | B | | C | |
| 12. Communication | | | A | | B | | C | | D | |
| *Governance & legislation* | | | | | | | | | | |
| 13. Legislation | | A | | B | | C | | | D | |
| 14. Governance | A | | B | | C | | | | | |
| | Unsafe | | Lacking | | Relatively safe | | Safer | | Optimized | |

Figure C.16: Greenadress Model