

Thomas Lian Ødegaard

Managing private keys in wallets for cryptocurrencies

An exploration of managing private keys in mobile applications

Bachelor's thesis in Web development

Supervisor: Gioele Barabucci and Peter Ruppel

May 2022

Thomas Lian Ødegaard

Managing private keys in wallets for cryptocurrencies

An exploration of managing private keys in mobile applications

Bachelor's thesis in Web development
Supervisor: Gioele Barabucci and Peter Ruppel
May 2022

Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

Abstract

Title: Managing private keys in wallets for cryptocurrencies

Date: 13.05.2022

Participants: Thomas Lian Ødegaard

Supervisor: Gioele Barabucci and Peter Ruppel

Employer: Norwegian University of Science and Technology in Gjøvik

Keywords: Web development, blockchain, private keys, secure storage, cryptocurrency wallets, mobile development

Number of pages: 33

Number of attachments: 4

This report investigates how users think about and interact with private keys when creating a cryptocurrency wallet. Often when people are creating a cryptocurrency wallet for the first time, they would backup their private key in something that could be seen as an unsecure way. One example is that one person took a print screen of the private key and stored it like they would store any picture taken with their phone. This project will look at what a person thinks about different types of generating and storing private keys in a web application and how a person backs up their private key when using a mobile device. This report can be used as a guide for further development of a wallet for cryptocurrencies, to see how the application should handle private keys and how the user handles a private key when they are presented one.

Sammendrag

Tittel: Håndtere private nøkler i lommebøker for kryptovaluta

Dato: 13.05.2022

Deltakere: Thomas Lian Ødegaard

Veileder: Gioele Barabucci og Peter Ruppel

Oppdragsgiver: Norges Teknisk-Naturvitenskapelige Universitet i Gjøvik

Stikkord: Webutvikling, blokkjede, private nøkler, sikker lagring, kryptovaluta lommebøker, mobilutvikling

Antall sider: 33

Antall vedlegg: 4

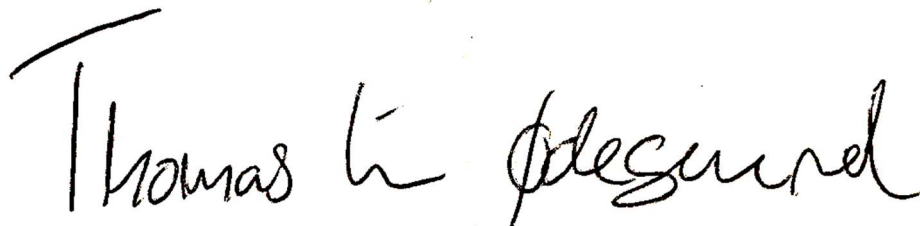
Denne rapporten undersøker hvordan brukere tenker om- og håndterer private nøkler ved opprettelse av en kryptovaluta lommebok. Mange som velger å lage en kryptovaluta lommebok for første gang, velger en usikker måte på å lagre den private nøkkelen. Et eksempel er at en person tok skjermdump av den private nøkkelen for å så lagre den samme plass som alle andre bilder tatt med mobiltelefonen. Dette prosjektet vil se på hva en person tenker om forskjellige typer generering- og lagring av private nøkler i en webapplikasjon og hvordan en person lagrer den private nøkkelen ved bruk av en mobiltelefon. Denne rapporten kan bli brukt som en guide for videre utvikling av lommebøker for kryptovaluta, for å se hvordan applikasjonen skal håndtere de private nøklene og hvordan en bruker lagrer den private nøkkelen når brukeren blir presentert en.

Preface

This thesis has been written during an exchange period at the Code University of Applied Sciences in Berlin, Germany. The exchange has been for the good of the result of the thesis. I have gotten a lot of different input from a lot of different people around the world, that are here in Berlin for the same reason as me.

I would like to thank my supervisors, Gioele Barabucci from NTNU and Peter Ruppel from CODE, for great feedback on questions, and for always questioning the choices I took. I would also like to thank Arthur Gousset at cLabs for all the input around cryptocurrencies and private keys. I could not have continued my bachelor without Mariusz Nowostawski that said yes to be my employer from NTNU. And a last thanks to Joakim P. Berg that helped me make the exchange to Berlin possible.

Berlin, 13. May 2022

A handwritten signature in black ink that reads "Thomas L. Pedersen". The signature is written in a cursive style with a large, sweeping initial 'T'.

Content

1	Introduction.....	1
2	Theory.....	2
2.1	Cryptocurrencies.....	2
2.1.1	Bitcoin.....	2
2.1.2	Ethereum.....	3
2.1.3	Power consumption.....	4
2.2	UN: Sustainable development goals.....	5
2.3	People’s motivations for using cryptocurrencies.....	5
2.3.1	The use of cryptocurrencies in countries with troubled economies.....	6
2.4	Local storage and cloud storage.....	7
2.5	Wallets.....	7
2.6	Private keys and existing Bitcoin users.....	8
2.7	Mobile first.....	8
2.7.1	Web application as a mobile application: Hybrid mobile applications.....	9
3	Methods.....	9
3.1	Planning.....	9
3.2	Qualitative interviews and user testing supported by a web application.....	11
3.2.1	Interviews (Part one of the qualitative interviews).....	11
3.2.2	User testing (Part two of the qualitative interviews).....	13
3.2.3	Prototyping.....	17
3.2.4	Programming.....	17
4	Results.....	18
4.1	Part 1: Interviews.....	18
4.1.1	Scenario 1.....	20
4.1.2	Scenario 2.....	20
4.1.3	Scenario 3.....	20
4.1.4	Scenario 4.....	21
4.1.5	Scenario 5.....	21
4.2	Part 2: User test.....	21
4.2.1	Test 1.1 – Generating a private key while registering for an account.....	22
4.2.2	Test 1.2 – Generating a private key.....	23
4.2.3	Test 2.1 – Recovering a private key with user login.....	24
4.2.4	Test 2.2 – Recovering a private key.....	25
5	Discussion.....	25

6	Conclusion	28
7	References.....	30
8	Attachments	33

1 Introduction

The popularity of cryptocurrencies and Bitcoin has been steadily climbing the last 12 years (Google Trends, 2022). Usually when creating a wallet on a public blockchain, someone gets a private key¹ that they are required to take care of. Losing the private key, means losing everything you own of valuables and coins on the blockchain the key was created. The funds are still in the wallet, but since the private key is lost, it is not possible to move the funds. There have been multiple stories of people “losing” their Bitcoins because they were not available to recover the private key. One story includes a man from the United Kingdom that accidentally threw his 7500 Bitcoin in 2013 (Kolirin, 2021), valuing around 328 million USD in the start of 2022 (Yahoo Finance, 2022). There was also a German programmer having his private key with 7002 Bitcoin on an encrypted hard drive. As he lost the password to decrypt the hard drive, he also lost the access to his Bitcoins (Onanuga, 2021), valuing about 306 million USD in the start of 2022 (Yahoo Finance, 2022). The computer skills of a programmer are assumed to be higher than average, which means losing a Bitcoin key can happen to everyone, even the best. Looking into solutions to manage a private key in wallets for cryptocurrencies could give an answer to which way would be best way to store a person’s private key. A survey shows that a big majority of the population does not know the basics of cryptocurrencies (Crypto Litteracy, 2021), which gives an assumption that a big portion of the population does not know how to store a private key correctly.

In countries such as Venezuela and El Salvador, citizens have made beneficial use of blockchain projects. Bitcoin is currently one of El Salvador official currencies, next to the US dollar (The Verge, 2021). While Venezuela created their own cryptocurrency called “Petro” (Ellsworth, 2021). It might give an assumption that persons with nationalities from countries that already uses cryptocurrencies, have a better understanding on storing their private keys.

In this project I will look at solutions to manage private keys in wallets for cryptocurrencies and how a person backs up their private key, using web development as a tool to guide the research.

¹ A private key is used to access the funds on a blockchain wallet. Can be compared to a password for a bank account.

2 Theory

2.1 Cryptocurrencies

“A cryptocurrency is a digital or virtual currency that is secured by cryptography” (Frankenfield, 2022). The cryptocurrencies chosen for this project are open source. Which means that the codebase of the blockchain is made publicly accessible for everyone to see, modify, and distribute (RedHat, 2019). This does however not mean that everyone can edit the code of open source blockchain projects, as there are teams reviewing and accepting changes to the codebase. So far there have been forks² of Bitcoin, where teams copy the code of Bitcoin to make another cryptocurrency with the same codebase with smaller changes. One example is a popular Bitcoin fork, Bitcoin Cash.

2.1.1 Bitcoin

Before Bitcoin was created, there was no way to make digital payments to each other without using a trusted third party. Bitcoin was in 2008 launched as a *“A Peer-to-Peer Electronic Cash System”* (Nakamoto, 2008). A Peer-to-Peer electronic cash system makes it possible for users of the system to create transactions on the network without the need of a middleman (ex. A bank). With non-reversible transactions people should be able to feel safer using the network, as it lowers the possibility of fraud.

Bitcoin is a chain of digital signatures, where multiple signatures are inserted into a block, creating a blockchain. The owner of a coin can digitally sign a hash of the previous transaction and use the public key of the next owner to add them to the end of the coin.

A block is mined through the Proof-of-Work (PoW) concept, where CPUs all over the world can join the network and mine blocks. As of this year (2022), mining Bitcoin is mostly done by application-specific integrated circuits (ASICs), which manages more calculations, resulting in finding a block much earlier than a CPU. PoW solves the problem in majority decision making. As PoW in the Bitcoin blockchain is set to one-CPU-one-vote. Most of the CPU power is controlling the longest chain, anyone trying to create a duplicate chain will be outperformed by all the CPUs in the honest chain. Every CPU that mines a block would in 2009 get 50 bitcoins to their public address. Today this amount has been reduced to 6,25 Bitcoin per block because of Bitcoin halvings (Conway, 2021).

² Someone copying the code from an open-source project to use it as a base for their own project.

The network is controlled by several nodes, the network is public and anyone with an internet connection can join with a node, assuming they have enough computer power and storage space. Every node is responsible to place new transactions into the next block and will always consider the longest chain to be the correct one.

Through the years since the launch of the blockchain it has gotten multiple upgrades. Some of which have been trying to fix the scalability problem in Bitcoin. One of them called Segregated Witness (SegWit), which efficiently rearranges the data in each block, making it possible to fit more transactions within one block which is currently at 1 MB (Cryptopedia, 2021).

2.1.2 Ethereum

Ethereum is a different type of cryptocurrency than Bitcoin, in the form of focusing more on smart contracts and decentralized applications (DApps) (Buterin, 2013). Ethereum contains a blockchain that allows anyone to write smart contracts and DApps using its Turing-complete programming language, with minimum lines of code.

In Ethereum you will find two types of accounts. Accounts controlled by private keys, which can send messages by creating and signing transactions. There is also contract accounts. A contract accounts is controlled by the code of the contract. The code of the contract activates every time it receives a message.

A transaction in Ethereum is a signed data package that stores a message, the message is sent from an externally owned account. It contains the recipient, the senders' signature, the amount of ether³ to transfer, a data field (optional), STARTGAS value (maximum number of computational steps the transaction execution is allowed to take) and a GASPRICE (the fee the sender pays per computational step) value.

A message is a virtual object and are used by contracts to send "messages" to other contracts. A message contains the sender, the recipient, the amount of ether to transfer alongside the message, a data field (optional) and a STARTGAS value. In the end, a message is similar to a transaction but produced by a contract, which means it is not produced by an external account.

³ Ether is the currency of Ethereum

The Ethereum contracts are written in a low-level, stack-based bytecode language called “Ethereum virtual machine code (EVM code).

The blockchain allows to create different types of applications, such as financial applications, semi-financial applications and online voting and decentralized governance. There is also possible to create tokens within the blockchain and financial derivatives and stable-value currencies (often referred to as “stable-coins”).

2.1.3 Power consumption

A controversial topic about cryptocurrencies is the amount of power they use. The estimated annual power consumption of Bitcoin by august 2021 was 94,5 TWh (The New York Times, 2021), which is more than what the whole country of Finland uses, which is a nation of about 5,5 million people. Globally, it is estimated that Bitcoin uses on a range from 40 to 75 percent renewable energy (The New York Times, 2021), however this means that the energy will be used on Bitcoin mining and not to power a home or charging an electric car.

An article from Domingo (2017) compares the power consumption of Bitcoin and the major card company Visa. Bitcoin and Visa are usually compared together, but this is an unfair comparison as Bitcoin is a currency as well as a form of payment, where Visa is only a form of payment. By using a Visa card, credit card information and banking information is sent across several databases and servers. To estimate the electricity consumption of Visa, someone would therefore need to include the power usage of the whole process, including the electricity consumption of banks.

To calculate the power usage of banks, Domingo (2017) assumed that there are around 30 000 banks around the world. Three values in the calculation of the power consumption of banks includes server costs, branches costs and ATM costs. There are however more to a bank than these categories, but it should give a good estimate. It is therefore estimated that in 2017 the total power consumption of banks is close to 100TWh a year.

This estimate is just a bit more than the total annual power consumption of Bitcoin. However other cryptocurrencies, such as Proof of Stake (PoS) based cryptocurrencies, have reported to be using less energy. Where Ethereum which plans to move from PoW to PoS, will lower the energy consumption by more than 99% (Kharif, et al., 2021). It might however affect the security of Ethereum.

By looking at the fork of Bitcoin, Bitcoin Cash, fork.lol⁴ has by 17.02.2022 reported that the hashrate of Bitcoin Cash is less than 1% of Bitcoin the last 7 days on average. If the Bitcoin Cash network uses the same efficient miners as Bitcoin, the total power consumption of Bitcoin Cash is therefore less than 1TWh. It will however be less secure as an attacker would need less hash rate to do an 51% attack of the network.

2.2 UN: Sustainable development goals

United Nations has developed several goals for sustainable development. Cryptocurrencies can be a crucial factor in reaching some of the goals. Here are some of the sustainable development goals where cryptocurrencies might be a key factor, however the impact of cryptocurrencies are not limited to this, and can also cover additional goals:

- 8. Decent work and economic growth. Goal 8.10 about giving the availability of banking and insurance services to everyone.
- 9. Industry, innovation, and infrastructure. Goal 9.3 about increasing the access of financial services for small industries, especially in developing countries.

2.3 People's motivations for using cryptocurrencies

Understanding people's motivation to using cryptocurrencies might help with learning how people store their private keys. A study done by Alqaryouti, et al. (2020) looked at "*users' knowledge and motivation on using cryptocurrency*". The participants were three people with engineering backgrounds, and have used crypto for 1,5 years, or more. The participants had a general understanding of the concept of a cryptocurrency, how mining worked and the meaning of market capitalization. The participants were asked about crypto wallets and the uses of crypto. Here as well a general understanding was shown and pointed out that there are multiple wallets out there. Cryptocurrencies can be used as described by the participants as: for e-commerce, as an investment or currency exchange.

In the report "Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency" (Prethus & O'Malley, 2017), it was done a quantitative survey. The survey got 135 answers in the period from June 2016 to August 2016. In the survey people were asked if they already were users of Bitcoin and got questions depending on what they answered. Users that were already using Bitcoin said that the "motivation to owning Bitcoin were curiosity and fascination about the technology". The users were not influenced by others, and therefore no

⁴ A website used to compare Bitcoin and Bitcoin Cash

trace of network effect. The non-users of Bitcoin said that requirements to start using it was stability, security, value, usefulness and easy of use. One person said “Vipps with Bitcoin = interesting” (Vipps is a Norwegian app used to make payments to other users or companies using the application, where you can send money from your bank account or credit card). However, some were not interested, and asked “why should anybody use this”. There was also discussed that “non-users wait for other non-users to start using the technology”.

Bashir, et al., (2016) did a report “What motivates people to use Bitcoin?”. 520 people participated in a survey, and the result shows that people with experience using Bitcoin generally have a positive attitude against the currency. People’s motivations to using Bitcoin were anonymity, borderless transactions and virtual money.

2.3.1 The use of cryptocurrencies in countries with troubled economies

Cifuentes (2019) did a report looking at Bitcoin in troubled economies, comparing Argentina and Venezuela, both countries have historically economic problems. Bitcoin is an important factor in the two countries because of the high inflation rate. People have been using Bitcoin as a store of value as it has less volatility than their native currency. In Argentina they had about 300% average yearly inflation between the years 1975 and 1990. A lot of people were storing their wealth in US dollars, but there was an exponential rise of the use of Bitcoin in 2015. It is estimated that 80 000 dollar worth of Bitcoin was used to buy and sell goods each day. However, the central bank of Argentina does not accept Bitcoin or any other cryptocurrencies as legal tender.

In the same report, it was shown that Venezuela were doing worse than Argentina. In 2018, there was an estimated inflation rate of 1 000 000%, making it the estimated highest hyperinflation in the world. A lot of citizens of Venezuela went to cryptocurrencies for their savings because of the high inflation rate. An exchange for trading Bitcoin “SurBitcoin” was launched in October 2014 as the first of its kind in Venezuela. Bitcoin raised as a transaction medium in Venezuela. Coinmap.org reported in November 2017, just 17 stores in Caracas accepting Bitcoin, while in March 2019 it was over 100. Bitcoin was also used to buy foreign goods that was not available in Venezuela, such as household supplies including toilet paper. It was reported that around 100 000 Venezuelans were mining Bitcoin around 2017, even when the authorities did a crackdown on mining farms in 2016 because of “energy theft and contraband”. 3rd of December 2017 the government of Venezuela launched their own cryptocurrency called “Petro”. The currency was supposed to help the financial problems in

Venezuela. However, people ended up using decentralized cryptocurrencies instead as Petro was decentralized and could easily be manipulated as the Venezuelan fiat currency.

2.4 Local storage and cloud storage

In the report *“Home is safer than the cloud!: privacy concerns for consumer cloud storage”* (Iulia, et al., 2011), a interview and an online survey was done to see what type of storage people use to save private files, sensitive data and passwords. The results shows that participants were using their email account for sensitive documents because “email feels like your private space”. Email was preferred over cloud storage because of the same reason. Participants were also using USB sticks for permanent storage. The participants were as well little willing to store a password list in the cloud, and 69% said that local storage is safer, while 31% said that the cloud is safer.

2.5 Wallets

A cryptocurrency wallet can be a place to securely store your cryptocurrencies. The procedure to create one depends on the type chosen, sometimes it can be as easy as one click. There are multiple of wallets to choose from, they all have positive and negative sides, and the choice often depends on the motivation of the user. Based on the Bitcoin wallet picker (Bitcoin.org, 2022), table 1 gives a general overview over the wallets to choose from.

Wallet type	Possibility to view private key?	User type	Free to obtain?
Mobile	Sometimes	New and experienced	Yes
Desktop	Sometimes	New and experienced	Yes
Hardware	Yes, but can be restricted	Experienced	No
Paper	Yes	Experienced	Yes, assuming someone already owns a piece of paper

Table 1: General overview of types of Bitcoin wallets.

2.6 Private keys and existing Bitcoin users

Two formats that are commonly used in the cryptocurrency space are Wallet Import Format (WIF) and Mnemonic. WIF is often found when creating and backing up a Bitcoin wallet and is usually a long string containing numbers and letters. Mnemonic is often found in Ethereum based wallet providers such as MetaMask and Trust Wallet and is often referred to as a seed phrase. Mnemonic contains an array of words that is used to recover a wallet containing multiple accounts. As a seed phrase can contain multiple wallets, it is also possible to extract the private key of one of the multiple accounts through a wallet provider such as MetaMask, to import only one wallet within another wallet provider or on another device (MetaMask Support, 2022).

It is good practice to back up the private key provided by the wallet provider. However, how a user backs up the private key can make them more vulnerable to losing their coins due to losing the private key or making the private key available to other people. A private key can usually be exported easily, depending on the wallet provider. And there is multiple ways one can back up their exported private key.

The study *“How do Bitcoin Users Manage Their Private Keys?”* (Lindqvist, et al., 2021) goes into how existing Bitcoin users manage their private keys. The study did a web survey and got 339 respondents. The result from the study shows that 46,6 % uses a hardware wallet for their Bitcoins followed by 17,4% who use a software mobile application. Next, the results shows that 88,2% creates a backup of the private key for their wallet. Later the study shows that 54,8% use a piece of paper for backing up the private key, followed by an external drive. From the backup, 59,9% of the respondents did not encrypt the backup, it is however noted that it is hard to encrypt backups done on a piece of paper. It is argued that existing Bitcoin users are security aware as a result of the web survey, and that Bitcoin users back up private keys to a higher degree than how often general user’s backup data. The research also calls for more ways private keys could be secured.

2.7 Mobile first

Mobile first is a term used when the mobile design is created first, and where the UX is optimized for mobile devices (Mullins, 2015). When developing for mobile first it is important that the market of the product will primarily use a mobile device to access the product. Mobiles are the only device a person keeps with oneself the entire day (Khanna, et al., 2017, p. 4) making it more reasonable to focus on mobile development.

There usage of mobile devices around the world are larger than the usage of desktop devices (statcounter, 2022), which arguments for developing for mobile first.

2.7.1 Web application as a mobile application: Hybrid mobile applications

Creating a native application can have a steep learning curve, and someone learning to create native mobile applications would need to learn at least one programming language for each platform. There is a term called WebView-based hybrid mobile applications, where a web developer can use HTML, CSS and JavaScript to create an installable application (similar to a native mobile app) to multiple platforms at once (Khanna, et al., 2017).

There are multiple platforms used to create web view based applications for mobile, one of them is Ionic (open source UI toolkit) that uses Capacitor, “*an open source cross-platform app runtime that allows web-based apps to run natively on iOS, Android, Electron and the web*” (Ionic, 2021). Ionic can be used with popular frameworks such as Angular, React and Vue.

3 Methods

3.1 Planning

The project was planned by using a mind map at mindmeister.com, a tool to create digital mind maps. As the research question was changed through the process of drafting the thesis, there was not a mind map created for the final research question. However, the mind map used did eventually lead to the final research question, as one of the written problems was based on insecurity around holding coins in exchanges instead of wallets (lack of backing up a private key).

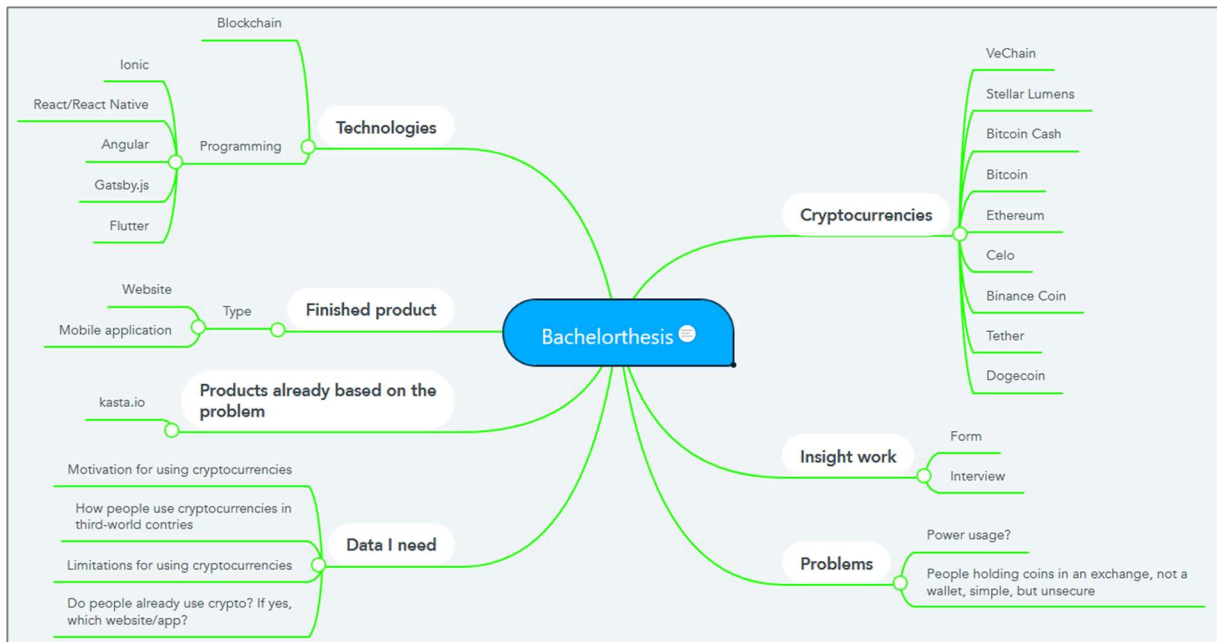


Figure 1 - Screenshot of mind map from mindmeister.com.

The timeframe and goals were set using a GANTT scheme template found in Microsoft Excel. Through the project, some of the goals were moved around as they had to be prioritized earlier or later in the project. One example was the development of the mobile application, as it was needed during the user testing process.

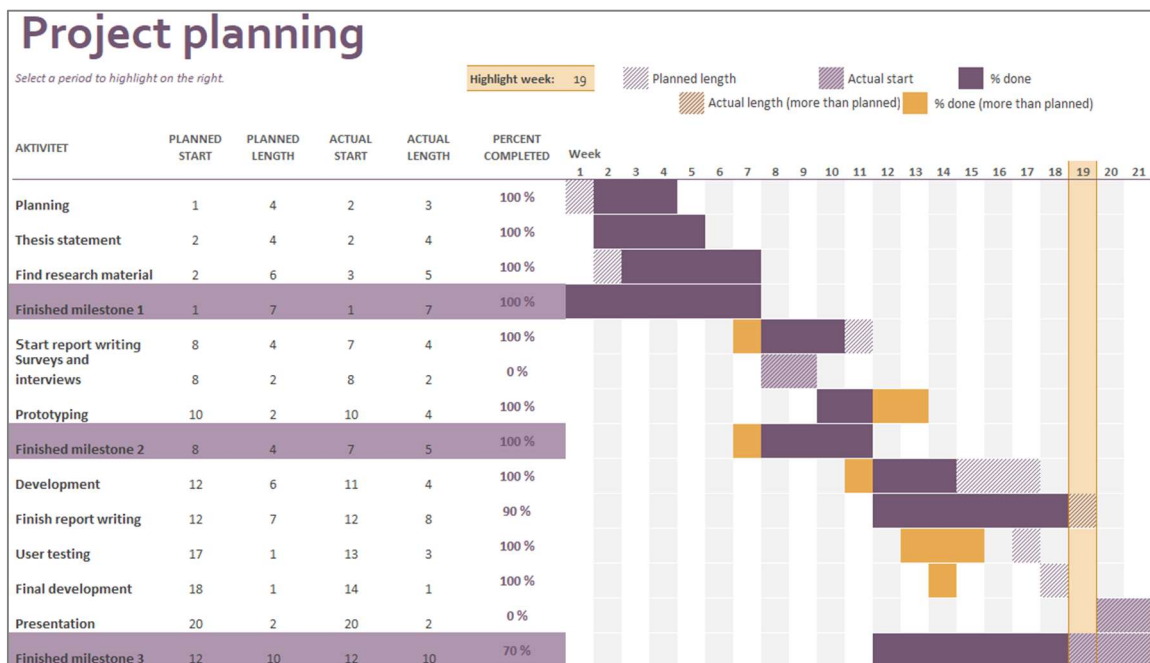


Figure 2 - GANTT scheme as of 11.05.2022. Created in Microsoft Excel.

In addition to the GANTT scheme, Google Calendar was used to have an overview of deadlines and daily working routines to keep track of when to work, and what to work with.

Using a calendar this way gave a more detailed planning of what to do and was more accessible to use from a smartphone.

3.2 Qualitative interviews and user testing supported by a web application

Interviews was set to get answers from a wide range of people, from different cultures and ages. The goal of the interviews was to get information that were not available from previously researched topics, and to give a clearer understanding to what someone sees as safe, and how different types of people would back up their private keys.

A total of eleven persons were interviewed and tested, all with a range of backgrounds. The goal was to get a general overview of persons with tech backgrounds and non-tech backgrounds to see what they do with private keys and if there is any difference in the way they see security, if there is any difference at all. The total time to take the interview and user test was about 40 minutes for non-tech participants, and about 25 minutes for participants with tech backgrounds.

Before doing interviews and user testing, the participant was asked to provide the following details:

- Age
- Nationality
- Education
- Previous experience with cryptocurrencies

Asking this type of questions gives an overall understanding of the person in the interview, for the interviewer and for a person that will be reading the interviews in a later time, as well as comparing the different participants. Age is to see if different generations have a better or worse understanding of the topic. Same goes for nationality, to see if other nationalities are more familiar with cryptocurrencies than other. Education to see what education equals better knowledge of the subject, and previous experience to see if it matters to have some previous knowledge to store a private key properly. At the same time as asking for education, the users will be asked if their education is technically based (Software engineer or similar) to see what a person familiar with the subject thinks what is the best practice.

3.2.1 Interviews (Part one of the qualitative interviews)

For the interview a diagram was created in Figma to demonstrate different scenarios to how a private key is created. Each scenario would be shown to the test subject, and they would say on a scale from 1-10 how secure the participant think this process is, where 1 is not secure at all, and 10 is very secure. The user was asked to say the reason for choosing the number for

each scenario. The user was shown one and one scenario; however, the user was allowed to go back to the previous scenarios if they changed their mind. The user was before the test asked if they know the difference of something created locally (on a device), or on a server (as someone was required to know the difference to finish the test). The user was explained the difference if they were unable to answer this question. In the end the user was asked which one they find the most secure, and why.

The test was created to give an understanding of what a user think is secure. A test subject would not be explained how a scenario would be secure. A hypothesis could therefore be that one participant would think that a scenario where you would not be able to lose your private key is the most secure, and another participant would think about security around how the private key is stored (example locally versus online). A last person would think of both security of storage and not to lose the private key. The goal is to see what type of persons would choose security in terms of losing their key, and the other in terms of where the private key is stored. However, a test subject could also come up with another scenario outside these two.

There were 5 possible scenarios (Figure 3 shows all scenarios from Figma.com):

1. The private key is generated on the server and stored in the database with the user's username and returned to the user device.
2. The private key is generated on the server and stored in the database with the user's username.
3. The private key is generated on the server and returned to the user device.
4. The private key is generated locally on the user device.
5. The private key is generated locally on the user device, and then stored in the database with the user's username.

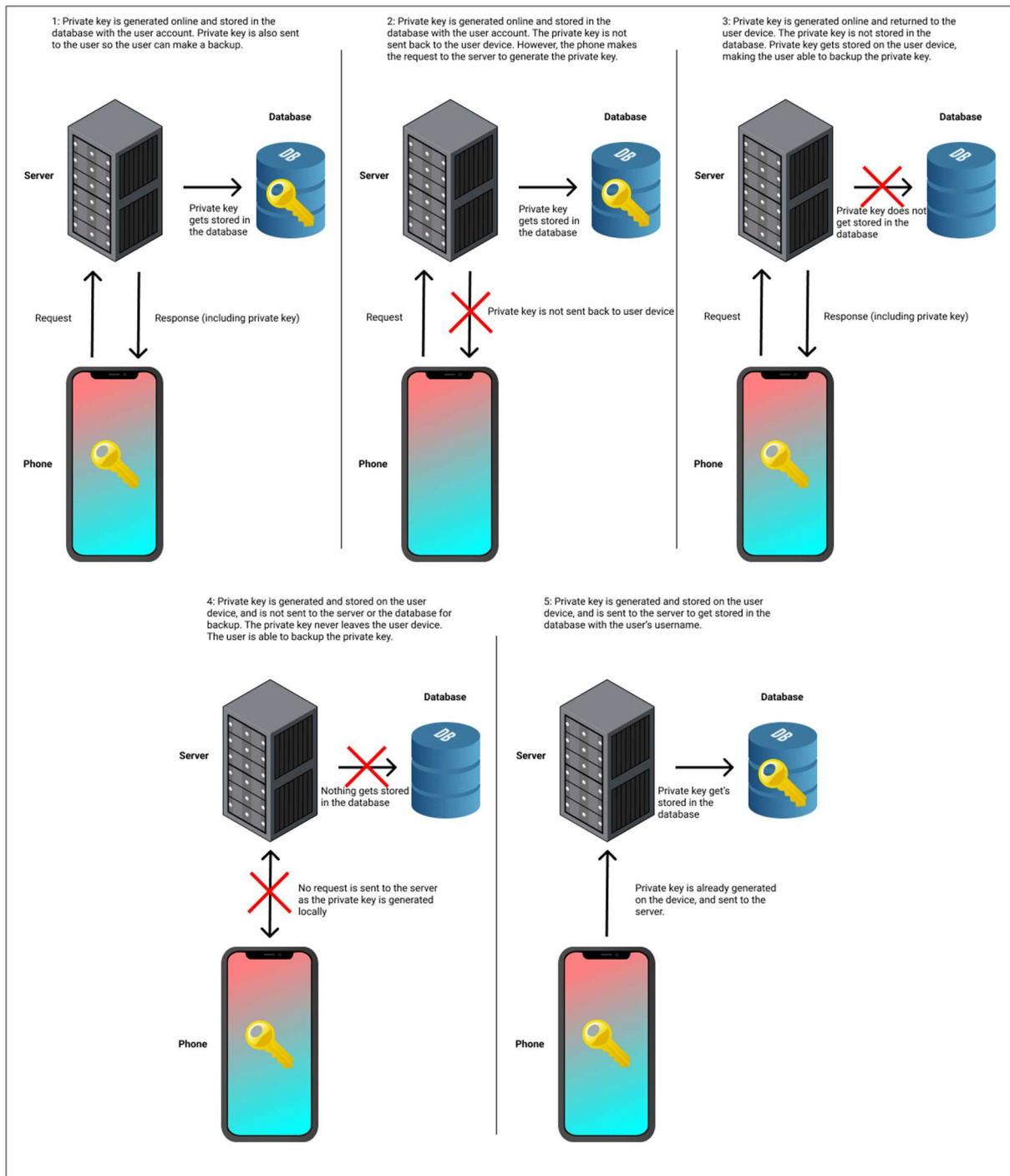


Figure 3 – All five diagrams created in Figma. Red cross indicates that the private key is not returned to the user device. Yellow key indicates where the key is stored.

3.2.2 User testing (Part two of the qualitative interviews)

For the user testing process there were two parts of a test that the user had to go through. Creating a wallet (Test 1.X) and recovering a wallet (Test 2.X). The test was a hybrid web application created to simulate the creation of a crypto wallet on a mobile device. Before starting the test, the user was told the difference between WIF and Mnemonic and told that

WIF is usually the standard for a Bitcoin wallet and Mnemonic is usually the standard for Ethereum. The user was told to explain an action before doing it, example clicking a button. The test was performed using the device of the participant. However, one test had to be done on a Windows Laptop in a Firefox browser using an iPhone 11 Pro in the browser inspect mode, a result of the app not loading in the browser of the device. The type of device used was written down in the test scheme. The user was shown how to make a print screen on the device and given a piece of paper and a pen in case they wanted to note something.

Test 1.X: There were created two types of tests for creating and backing up a wallet. Two for private keys using the WIF standard and two for the Mnemonic. The WIF test one (WIF 1.1), would be the same process of Mnemonic test one (Mnemonic 1.1). Same for test 1.2. A user would therefore randomly get one test from each, but not the same test number (example a user would get WIF 1.2 and Mnemonic 1.1, but never WIF 1.1 and Mnemonic 1.1).

Test 1.X is used to see how someone would backup their private key when creating a cryptocurrency wallet. There were different types of scenarios a user could do. In the application itself the user had the possibility to copy the key to clipboard, send the key to their email (test 1.1 only) or skipping backing up the key. There were also more possibilities as writing down the key on the given piece of paper, taking a screenshot of the private key, writing it down on their laptop if they have it nearby or any other scenario the test subject could think of. The test subject was open to do whatever they want to back up the given private key.

Here are the two scenarios (used for both WIF and Mnemonic):

- Test 1.1: The user creates an account for a crypto wallet. A simple registration form was used, where the user register with their email and a password. After registering the user is asked to back up their private key, skipping backing up the wallet or choosing to send the private key to their email. The private key is also stored with their account details in a database.
- Test 1.2: The user clicks a button to generate a crypto wallet. No information from the user is needed. Then the user gets a private key and can choose to back up their key or skip this part.

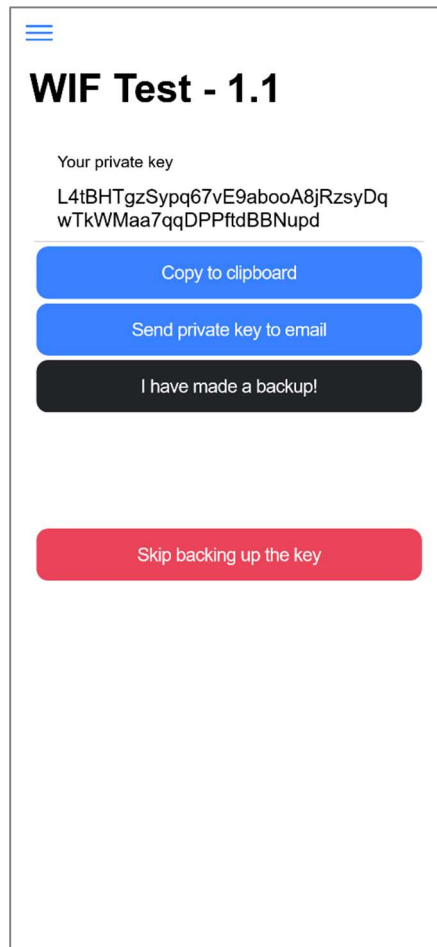


Figure 4 - How WIF test 1.1 was shown after registering for an account. Test 1.2 had a similar screen without "Send private key to email" button.

Test 2.X: The participant was told that they lost their device and would therefore need to restore their wallet on another device, using the private key they made a backup of if they did choose to make a backup. The test they did in the first part will match the number of the second part (if a user did WIF test 1.1 in the first part, they will use this data for the WIF test 2.1 in the second part).

Test 2.X was created to see if the way of backup is a sustainable way of creating a backup. A user could make a backup and would still not be able to recover their key because of errors with their backup. This could be something where a user could write a key down but forgetting a number or they stored the key in their notes and the file got corrupted somehow. As the time between making a backup and doing a recovery is less than 10 minutes in this test scenario, the chances of data corruption or losing a piece of paper is lower than if it was months or years between backup and recovery.

Here are the two scenarios for the second part of the user test (used for both WIF and Mnemonic):

- Test 2.1: The participant is presented a login form to recover their private key. Using the same email and password as in test 1.1. After they logged in, they are told that the service got hacked, and would need to use their private key to recover their wallet (as the private key is no longer available with their account details in the database as a result of the hack).
- Test 2.2: The participant is presented a form where they can insert a private key. The user is therefore required to have a backup of the private key generated in test 1.2.

After the user test was done, the participant were asked if they found anything confusing and how they think the process was.

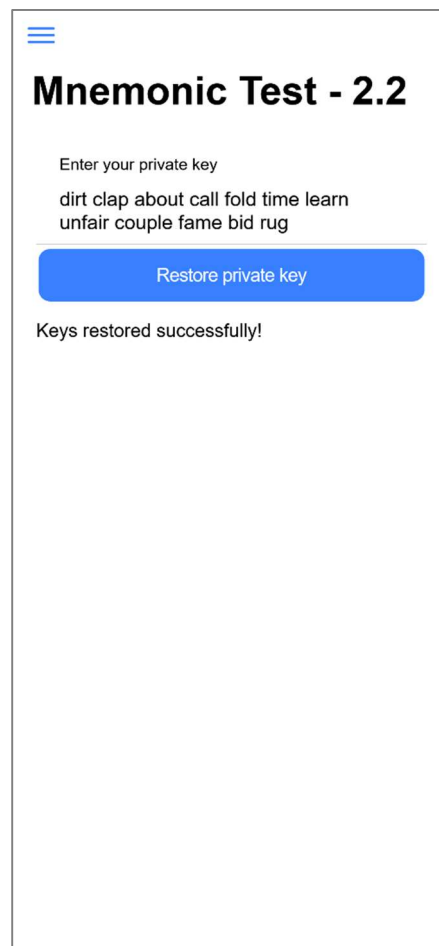


Figure 5 - How Mnemonic test 2.2 was shown after a user entered the right private key for their wallet.

To show the interaction of all participants, a map was created after all tests to see how the participants backup their private key. The interaction map was created in Figma.com.

3.2.2.1 Choosing the key standard

WIF and Mnemonic was chosen because they are the standard of the two most valuable coins as of 11.05.2022 (Bitcoin and Ethereum), looking at market capitalization (CoinMarketCap, 2022).

3.2.3 Prototyping

For the interview part, each of the 5 parts were created in Figma.com. The design of the first scenario, became the template for the next one. All templates were discussed and redesigned to make it as understandable for every person that would take the test, as they most likely would have different backgrounds.

Prototyping the user test application was done while making the application itself, using Ionic UI components as templates for how the application would end up looking. The overall goal was to create a neutral UI that would be like any other application with a register/login interface. The navigation to the different tests itself were sorted into a menu, and the user were not supposed to be affected by this menu as it is not part of the user test itself but should be used as a navigation to the different tests.

3.2.4 Programming

To create the full stack system, a front-end and back-end was needed. For the sake of the timeframe of the project, Google Cloud was chosen as it gives a ready to use backend to use with an Ionic application which makes it less time consuming than setting up a server and installing the required software. For front-end, Ionic was chosen as an application for iOS and Android. To keep track of the changes and different branches of the code, the version control system git was used, running it together with Github.com to have online backup and public view of the code.

Some of the code used in the backend and frontend of the application was intended to be used with the first research question, since the code works for the final research question it was reasonable to reuse the solution.

The backend consists of a NodeJS server running in Google Firebase. The server had multiple endpoints to get and store data:

- generateMnemonic – Used to generate a random mnemonic key and returning the key to the device making the request.
- generateWifKeys – Used to generate a Bitcoin keypair based of WIF and returning them to the device making the request.

See the backend part of the project at [Github.com](https://github.com)⁵.

Google Firebase was also used as the sign in system of the application, as it was an easy implementation with the Ionic framework.

For the sake of simplicity of this project, the public and private keys are generated in the backend even if the test shows that it is generated locally. Some of the scenarios were also simulated to make it appear like it is working as intended. Such as the generation of the mnemonic key, where the user is told that the key is saved in the database, when in reality it is not.

Ionic with Angular was used for the frontend with Ionic UI components which makes it easy to add UI components that fits mobile without doing a lot of work in HTML and CSS. To communicate with the backend, AngularFireFunctions was used, which is a Firebase client SDK for Angular (a module that can be added to Angular projects). The project was divided into four main folders:

- Components – Contains all reusable components such as the loading bar.
- Models – Contains the interfaces/models used in the project.
- Pages – All the different pages in the project that the user can navigate.
- Services – Used to communicate with the backend and store temporary data.

See the frontend part of the project at [Github.com](https://github.com)⁶.

4 Results

4.1 Part 1: Interviews

There was a wide range of answers from the interviews. The biggest contrast in answers were from people with tech background and people with non-tech backgrounds. Table 2 shows the results of the interviews. The average answers from people with tech backgrounds and non-tech backgrounds are added to show the contrast between the two.

⁵ <https://github.com/thomaslian/cryptoWalletFunctions>

⁶ <https://github.com/thomaslian/cryptoDemo>

Scenario	Total score	Average	Tech average	Non-tech average
1	52 (out of 110)	4,7	2,4	6,7
2	43 (out of 110)	3,9	2,2	5,3
3	62 (out of 110)	5,6	6,2	5,2
4	85 (out of 110)	7,7	8,8	6,8
5	65 (out of 110)	5,9	3,2	8,2

Table 2 - Results of all interviews done. Score indicates how secure the participants think the scenario is on a scale from 1 to 10.

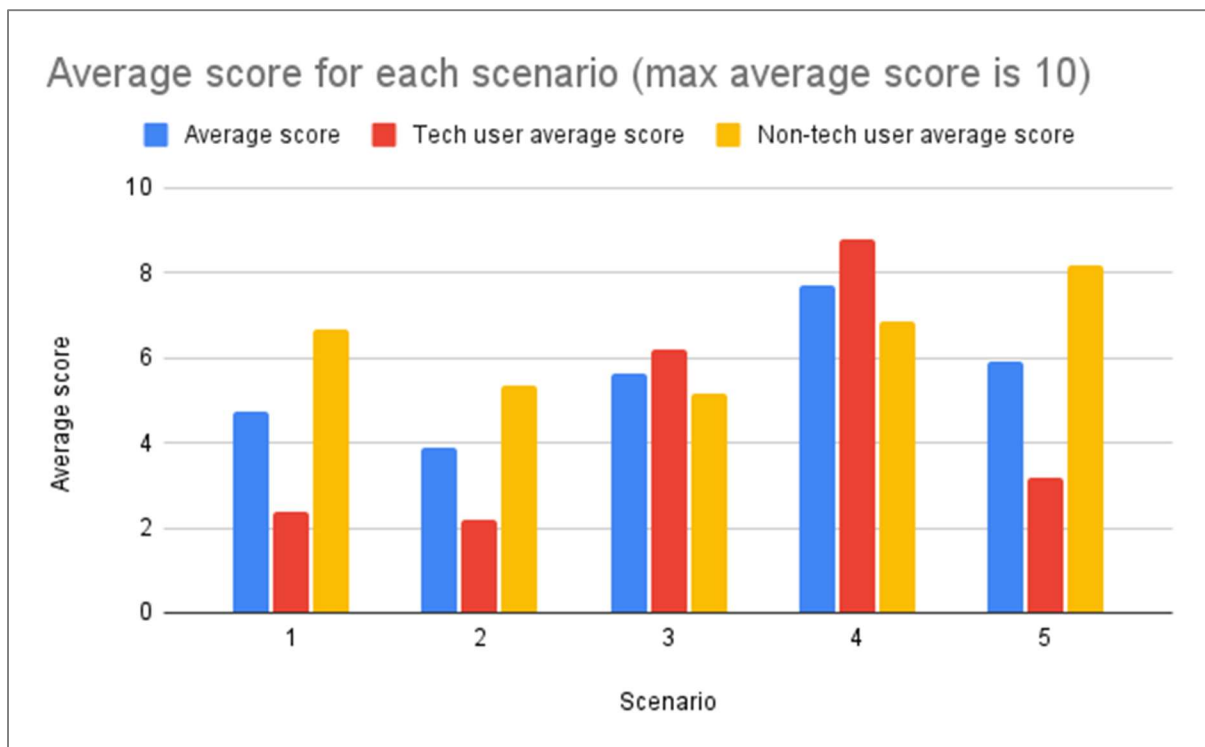


Figure 6 – Showing results from table 2, the average score, average score for participants with tech backgrounds and participants without tech backgrounds.

Table 2 shows the results from the interviews that was done. Total score indicates the sum of the score from all participants. Average is the average answer from all participants. Tech average shows the average answer from all participants with tech backgrounds, and non-tech average shows the average from all participants without tech average. The total possible score from one participant is 10, which makes the total possible score 110 from all the 11 participating participants.

One significant detail from the result in the interview is that non-tech people understand “secure” as how possible it is for them to lose the private key, while tech participants looked at the actual security of how the private key is stored. Which is also why it was important to

differentiate the two in the table. One example is participant 7 (non-tech), which said that scenario 5 is secure because "... it is created on the phone. Sounds safer that it is created on the phone. And you don't lose access to the key as it is in the database". However, participant 3 (non-tech) said "More secure than when the server is generating it. But not that secure because it is on the database.". Both participants are referring to scenario 1 and comparing them as they are similar. In scenario 1 the private key is generated in the server, while in scenario 5 it is generated on the phone. Both participants agree that scenario 5 is safer because it is generated on the phone. But have a more diverse answer about security when it comes to storing the private key on the database. Participant 7 says it is safe because you don't lose access to it, while participant 3 says that it is not secure because it is stored in a database, understanding the participant answer as there will be another point of failure storing it online, that is why it is not secure.

4.1.1 Scenario 1

The average score was 4,7 of 10, where participants with tech backgrounds rated the scenario as less secure than people with non-tech backgrounds. Most participants with tech backgrounds commented that it is easier for the database to be breached, and the private key might be leaked online. Some participants without tech background commented that the trust would depend on the application, if it is a known application or not. Other non-tech participants were not sure if it is safe when it is stored online, but because it is stored two places, it would make it more secure because it would make it harder for the participant to lose the private key.

4.1.2 Scenario 2

The average score was 3,9 of 10, where participants with tech backgrounds rated the scenario as less secure than people with non-tech background. Most participants agreed that it is safer to store the private key in only one location, however some participants were worried that the key is never sent back to the phone, meaning they would not be able to make a backup of the private key. Participants were overall more negative to this scenario than the first because they were not able to see the private key, as it would only in the database.

4.1.3 Scenario 3

In scenario 3 the average score was 5,6 of 10. Participants with tech backgrounds found this scenario to be more secure than participants without tech backgrounds. Where some participants agreed that it is safer to store the private key on the phone only, as one participant

pointed out “an attacker needs access to all devices” to access the private key. However, it is still generated on the server and an attacker might overview the system. Participants were also wondering if the private key needs to be generated on the server.

4.1.4 Scenario 4

Scenario 4 is the scenario with the highest average, scoring 7,7 of 10. Also, participants with tech backgrounds gives this scenario the highest average among all the scenarios. While non-tech participants give the scenario the second highest average. Participants pointed out that it is good that the private key is stored only on the phone, which makes the scenario decentralized. Another participant pointed out that the private key never leaves the device, which makes it more secure. However, some participants were worried that they would lose the private key if they lost their phone without making a backup.

4.1.5 Scenario 5

Scenario 5 scored the second highest average, 5,9 of 10. Participants with tech backgrounds found this scenario somewhat unsafe, while participants without tech backgrounds gave it the highest average among all scenarios, 8,2 of 10. Some of the participants compared the scenario to scenario 1, which is similar to this scenario, saying it is safer because the key is generated on the phone. Participants with tech backgrounds commented that the key is still stored in the database, which makes it less secure.

4.2 Part 2: User test

General feedback from the participants is that the application for the test was easy to understand, and it was understandable that the application was a demonstration to visualize how a real cryptocurrency wallet would generate and recover they private key. Both the standards WIF and Mnemonic was understandable, and it was easy to see the difference between both. Some participants found it easier to write down Mnemonic than WIF, which changed the way the participant backed up their key.

4.2.1 Test 1.1 – Generating a private key while registering for an account

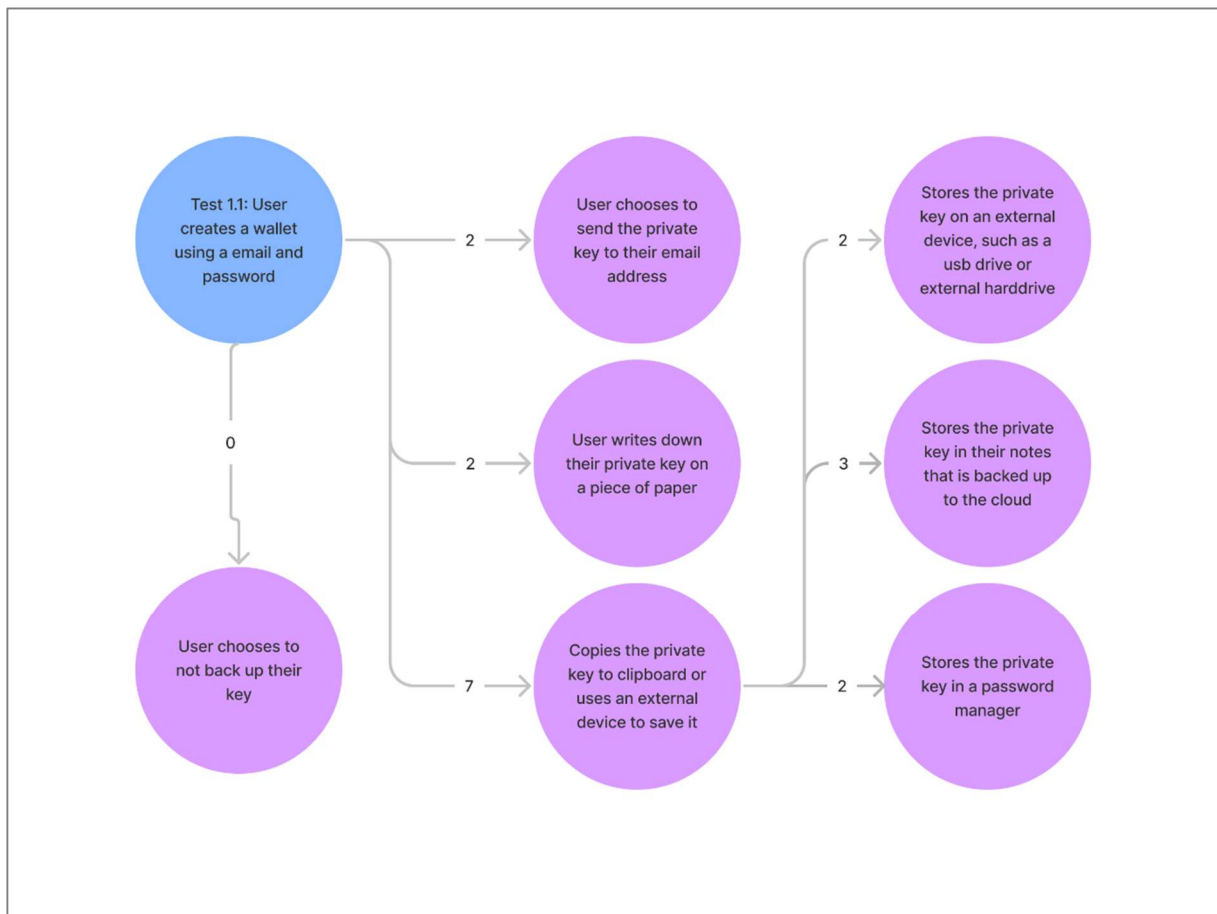


Figure 7 – User interaction map showing results from Test 1.1.

In test 1.1 all users backed up their private key in one way or another, even when told that the private key will be stored with their credentials online. Most users chose to save the private key to a text editor, like a notes app. There were participants that chose to store the private key in a password manager like LastPass, and to store it in plain text in a Word document on their computer. A couple of participants chose to write down the private key on a piece paper. No participants chose to store the private key on the same device without it being backed up to a cloud somehow. Test 1.1 was based on a user registering with their email to create an account, which gave the participant the option to send the private key to their own email account. A total of two users chose to send the private key to their email account.

4.2.2 Test 1.2 – Generating a private key

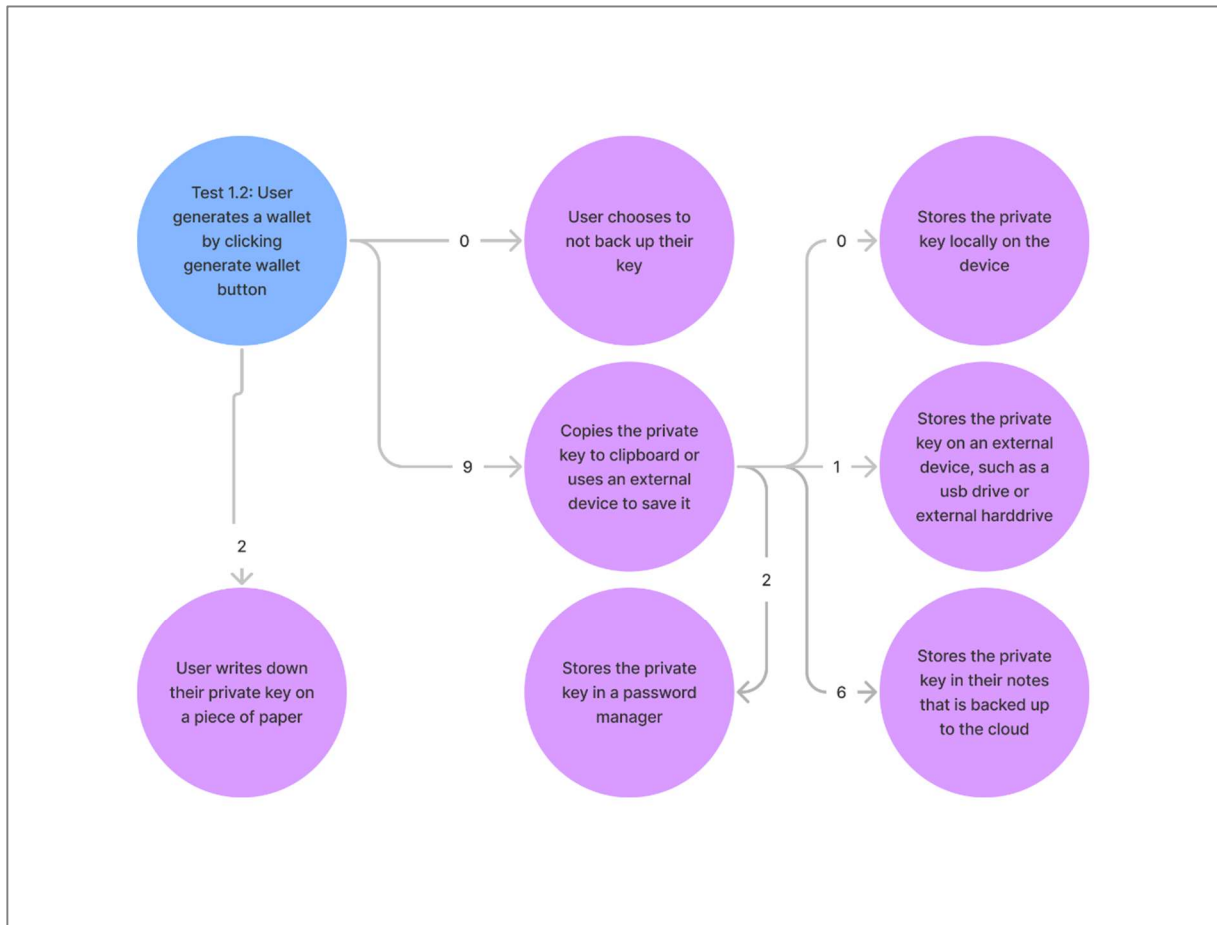


Figure 8 - User interaction map showing results from Test 1.2.

The participant would generally choose the same way to back up their private key as in test 1.1. However, some participants started test 1.1 with a Mnemonic private key and chose to write it down on a piece of paper. In test 1.2 they would get a WIF string and said that the string is too hard to write down and chose to save the key in the notes of the phones instead. Some users where unsure if the private key was backed up to the cloud when they saved the private key in the notes. In all situations, the participant found out that the notes are backed up in the cloud.

4.2.3 Test 2.1 – Recovering a private key with user login

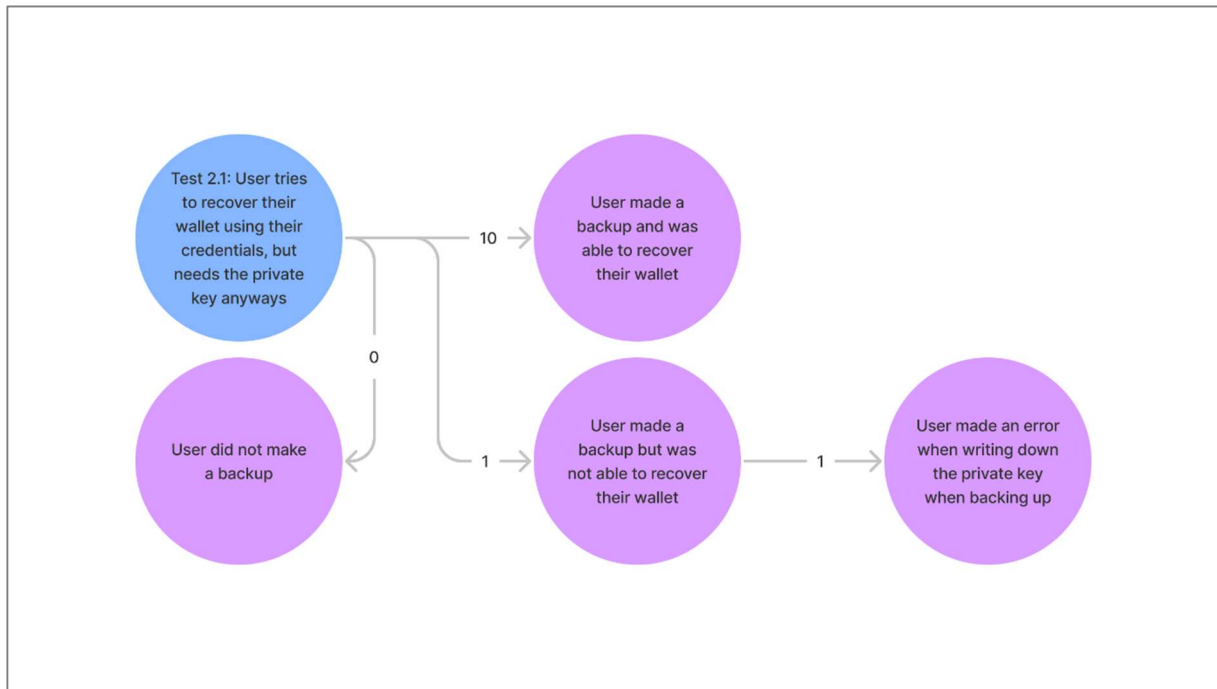


Figure 9 - User interaction map showing results from Test 2.1

All participants except for one were able to recover their wallet using the private key backup created in test 1.1. The error happened when the participant chose to write down the Mnemonic phrase in the text editor on their computer and spelled one of the words wrong. Another participant chose to back up a WIF private key by writing it down in test 1.1. When recovering the wallet, the participant tried to take a picture of the string that was written down and copy the string from the picture. The phone was unable to recognize the whole string, which made the user write the private key manually in the app, but successfully.

4.2.4 Test 2.2 – Recovering a private key

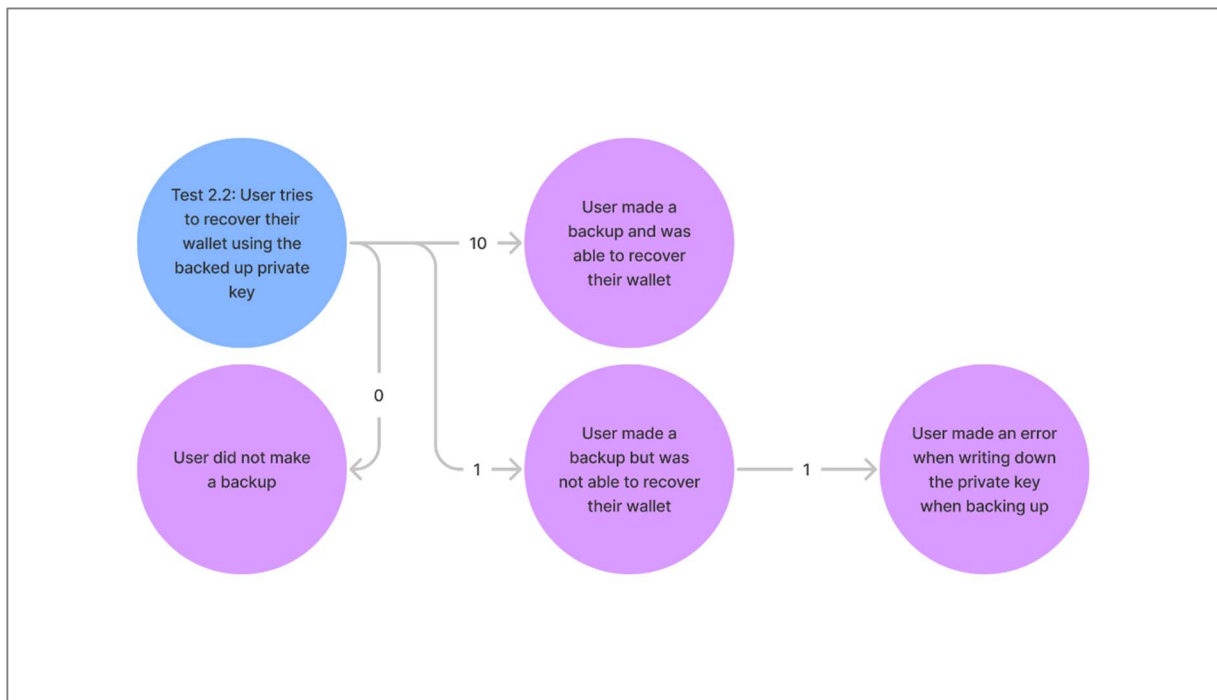


Figure 10 - User interaction map showing results from Test 2.2

From all participants, 1 participant were not able to recover their wallet in test 2.2, the others were successful. The error happened when the participant made a backup and wrote down their Mnemonic phrase on paper. When restoring the wallet, the participant realized they only wrote down 11 words, and not 12 as was used in this test. As all 12 words are needed to recover a wallet, the participant lost access to their wallet.

5 Discussion

The results shows that people think differently when creating their private key. People with tech backgrounds tend to choose what is safest based on their knowledge and experience as they are familiar with how a web application works and what vulnerabilities it might have. Most non tech people went for what is safest in form of not losing their private key, if it is stored multiple places, it might be safer, as the possibility of losing the key is lower.

An option would be to educate the user on how a private key can be stored and then storing the private key based on a small questioner in the app. However, based on the feedback from the participants of the user test, the user should still have the possibility to back up their private key later, even if they chose not when they created the wallet. If someone is not in possession of their private key, they might lose the access to their cryptocurrency at any point.

Giving the user the possibility of backing up their private key, might give the application more trustworthiness.

Even if the results might give an answer for what a user might think is the most secure option, in theory it might not actually be the case. However, choosing the most secure option in theory might affect usability and vice versa. Trying to find a balance between both usability and security might be a good option, giving the user an overall better experience. As the result shows that the average user would care about usability as well as security. It will also depend on the cryptocurrency wallet that is being made, as in some cases it would not make sense to have for example a user registration process. Making the service more in control of the private key than the user, might be a problem in case of a data breach where the private keys are leaked to an attacker. Having the service in control, might make the service owner liable for the loss of value in cryptocurrencies, while having only the user in control might not make the service owner liable.

In the theory chapter of this report (page 7), research said that 69% of users found local storage to be more secure. From the results of this report, it might be true for tech users. However, non tech users are leaning toward the opposite. It can be because of the way the question was asked, or simply because non tech users are more afraid of losing their data than the actual security of platform they are using. The result of this report calls for further research into this topic.

There might be a responsibility of the application around liability. An app without the possibility to back up their private key, might be seen as a payment app instead of a wallet app. Having the private key only stored server-side might give the application a payment app title instead of a wallet app. Which is another argument to give the user the option to back up their private key at any time if they want to.

As seen from the user test, some users found it easier to write down a Mnemonic seed phrase versus a WIF string. However, since Mnemonic is easier to backup, a user might not give too much attention to details. And as seen in the user test, participants did sometimes forget to write down a word of the seed phrase, giving Mnemonic a higher error rate when backing up because of user error. But a user often ended up backing up their WIF key in an easier way than Mnemonic, which might make the backup more vulnerable. Also, since the users did not choose to back up their WIF key the same way as their Mnemonic key, it might have similar error rates when backing up if a participant chose to do both the same way.

Through the interviews, the participants were asked about their nationality, to see if there is any difference in nationalities and the way they store private keys. In the theory chapter of this report (page 6), it was said that cryptocurrencies were widely used in Argentina and Venezuela because of the uncertainty of the government and inflation. The interviews of this report did not include any persons with those nationalities. For further research, it would be interesting to include persons from these countries to participate to see if there is a different understanding in storing and backing up private keys.

As cryptocurrencies are popular in countries with troubled economics (Cifuentes, 2019), there is not any data saying that people with nationalities from those countries have a better understanding in handling private keys. Participants of the user test were asked about their nationality to see if there is any connection being from different nationalities and knowledge about private keys, using the theory part to back up the claim. As there were not too many people with the same nationality in the interviews, there was not enough data to make any comparison.

Some persons chose to not participate in the interview because of its 40 minutes length. Trying to shorten the time of the interview could have given more persons to participate in the interview. The qualitative interview could also have been converted into a quantitative interview, where persons would use a multiple-choice form to answer the questions. Leaving the user-test left, with only about 20 minutes of time take to complete, which could be a lot more accessible for other persons. It has however interesting to see that people with non tech backgrounds spent up to 15 minutes longer to finish the total interview, than people that already have tech background. It could be the new environment of creating a cryptocurrency wallet and backing up their private key that made this time difference. There was also a lot more explaining done to people without tech backgrounds as some of the concepts were new to them.

As the first participant in the interview had a problem loading the test application to a phone, the test was done on a computer. The user chose to save the private key on an external storage unit, it makes this user test different than the others as no one else chose to do something similar. For further research it would be interesting to go in more depth into this topic, that a user might be more creative doing a backup of a private key on a computer than on a mobile device.

6 Conclusion

How to manage a private key could be a crucial step for the security of the user of the device. This report looked at what a user thinks is the safest way to store a private key in a mobile application, and how a user would manage and backup the private key themselves. The research is supposed to be the foundation to use in the creation of a cryptocurrency wallet application for mobile.

All tests were done in a matter that was understandable from the participant. Every participant said that they understood the processes they went through and understood at least the basics of storing something locally and online and what a cryptocurrency wallet is. Since a test took 40 minutes, some of the potential participants said no to taking the test as they did not have time to participate in an interview that was that long. Making the interviews shorter by splitting them up, and making the first part of the interview a quantitative one could have made it possible to get more participants and data.

The results from the interview and user test shows that a user have a basic understanding of the topic. One of the biggest differences in the interview part was that a participant with a tech background would often choose a more technical secure way than a participant without a tech background. It might be for the good and worse, as a user without a tech background cares more about not losing their private key than the actual security of it.

In the user-test the results were similar among the users. User found Mnemonic keys to be easier to back up because of the 12-word phrase, but Mnemonic also had the highest failure rate as a user did not pay a lot of attention to be sure they backed up all the words before proceeding. A user would also use an easier way of backing up their WIF key because of the complexity of the string, making their wallet more vulnerable. If a user chose to backup the two standards in the same way, they might have had the same amount of failure rate.

It is important to think about both usability and security when creating a web application. The most secure option could not be the best for the user, but it might also make the creator of the application liable to any losses if the private key is in the app creators' hands somehow.

Making the private key only generated and kept on the phone, might not make the application itself liable of any losses the user has, but would make it hard for the user if they lose their private key or if they change their phone without making a backup of the key. All users chose to back up their private key in the user test. However, some users chose to back up their private key to places which might not be the best way when thinking about security.

In the future, the way of storing private keys should be improved. The private key should be stored in a way that is secure enough to not be breached, while making it available for the user even if they choose to change their device. A private key could be encrypted with the account of the provider of the device that is being used (ex. Apple), and would be given to an application on request. There is also an improvement that could be done while a user is backing up their private key. Showing the user a small animation of a secure way of making the backup could make it more clear, or changing the standard of the private key to something that could eventually replace WIF or Mnemonic.

7 References

- Alqaryouti, O., Siyam, N., Alkashri, Z. & Shaalan, K., 2020. Users' Knowledge and Motivation on Using Cryptocurrency. In: *Information Systems*. Dubai: Springer, pp. 113-122.
- Bashir, M., Strickland, B. & Bohr, J., 2016. What Motivates People to Use Bitcoin?. In: *Social Informatics*. Bellevue: Springer, pp. 347-367.
- Bitcoin.org, 2022. *Choose your Bitcoin wallet*. [Online]
Available at: <https://bitcoin.org/en/choose-your-wallet>
- Buterin, V., 2013. *ethereum.org: Ethereum Whitepaper*. [Online]
Available at: <https://ethereum.org/en/whitepaper/>
- Cifuentes, A. F., 2019. Bitcoin in Troubled Economies: The Potential of Cryptocurrencies in Argentina and Venezuela. In: *Latin American Law Review*, no. 3. Bogotá: Universidad de los Andes, pp. 99-116.
- CoinMarketCap, 2022. *CoinMarketCap*. [Online]
Available at: <https://coinmarketcap.com/>
[Accessed 11 May 2022].
- Conway, L., 2021. *Investopedia*. [Online]
Available at: <https://www.investopedia.com/bitcoin-halving-4843769>
- Crypto Literacy, 2021. *98% Can't Pass Crypto Literacy Quiz*. [Online]
Available at: <https://cryptoliteracy.org/insights/98percent-cant-pass-crypto-literacy-quiz/>
- Cryptopedia, 2021. *Bitcoin Forks: Upgrades and Radical Blockchain Changes*. [Online]
Available at: <https://www.gemini.com/cryptopedia/bitcoin-fork-protocol-upgrades-blockchain-changes>
[Accessed 08 May 2022].
- Domingo, C., 2017. *The Bitcoin vs Visa Electricity Consumption Fallacy*. [Online]
Available at: <https://hackernoon.com/the-bitcoin-vs-visa-electricity-consumption-fallacy-8cf194987a50>
- Ellsworth, B., 2021. *As Venezuela's economy regresses, crypto fills the gaps*. [Online]
Available at: <https://www.reuters.com/technology/venezuelas-economy-regresses-crypto-fills-gaps-2021-06-22/>
- Frankenfield, J., 2022. *Investopedia: Cryptocurrency*. [Online]
Available at: <https://www.investopedia.com/terms/c/cryptocurrency.asp>
[Accessed 08 May 2022].
- Google Trends, 2022. *Google*. [Online]
Available at: <https://trends.google.com/trends/explore?date=all&q=cryptocurrency,bitcoin>
- Ionic, 2021. *Ionic: Glossary*. [Online]
Available at: <https://ionicframework.com/docs/reference/glossary#capacitor>
[Accessed 08 May 2022].

Iulia, I., Sachdeva, N., Kumaraguru, P. & Čapkun, S., 2011. *Home is safer than the cloud!: privacy concerns for consumer cloud storage*, New York: Association for Computing Machinery.

Khanna, R., Yusuf, S. & Phan, H., 2017. *Ionic: Hybrid Mobile App Development*. 1 ed. Birmingham: Packt Publishing Ltd..

Kharif, O., Mathis, W. & Saul, J., 2021. *Crypto's Energy Guzzling Sparks an Alternative That Merely Sips*. [Online]

Available at: <https://www.bloomberg.com/news/articles/2021-11-17/crypto-s-power-consumption-sparks-an-energy-efficient-alternative>

Kolirin, L., 2021. *Man who accidentally threw out a bitcoin fortune offers \$70 million for permission to dig it up*. [Online]

Available at: <https://edition.cnn.com/2021/01/15/uk/bitcoin-trash-landfill-gbr-scli-intl/index.html>

Lindqvist, G., Kävrestad, J., Modig, D. & Padyab, A., 2021. *How do Bitcoin Users Manage Their Private Keys?*, Skövde: s.n.

MetaMask Support, 2022. *User Guide: Secret Recovery Phrase, password, and private keys*. [Online]

Available at: <https://metamask.zendesk.com/hc/en-us/articles/4404722782107-User-Guide-Secret-Recovery-Phrase-password-and-private-keys>

Mullins, C., 2015. *Responsive, mobile app, mobile first: untangling the UX design web in practical experience*, New York: Association for Computing Machinery.

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*, s.l.: s.n.

Onanuga, T., 2021. *Bitcoin owner whose story went viral after he lost his wallet password says he has 'made peace' with potential \$220 million loss*. [Online]

Available at: <https://www.businessinsider.com/bitcoin-owner-who-lost-password-made-peace-potentially-huge-loss-2021-1?r=US&IR=T>

Presthuis, W. & O'Malley, N. O., 2017. *Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency (Pages 89-97)*, Barcelona: Procedia Computer Science.

RedHat, 2019. *RedHat: What is open source?*. [Online]

Available at: <https://www.redhat.com/en/topics/open-source/what-is-open-source>
[Accessed 08 May 2022].

statcounter, 2022. *Desktop vs Mobile vs Tablet Market Share Worldwide*. [Online]

Available at: <https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet>
[Accessed 11 May 2022].

The New York Times, 2021. *Bitcoin Uses More Electricity Than Many Countries. How Is That Possible?*. [Online]

Available at: <https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html>

[Accessed 08 May 2022].

The Verge, 2021. *El Salvador becomes first country to adopt Bitcoin as an official currency.* [Online]

Available at: <https://www.theverge.com/2021/9/7/22660457/el-salvador-bitcoin-legal-tender-currency-cryptocurrency-chivo-wallet>

Yahoo Finance, 2022. *Bitcoin USD (BTC-USD).* [Online]

Available at: <https://finance.yahoo.com/quote/BTC-USD/>

8 Attachments

Attachment 1: GANTT-scheme.

Attachment 2: Mind map.

Attachment 3: Diagrams from interviews made in Figma.

Attachment 4: User tests.

