



**University of
Zurich**^{UZH}

Analytic Study on Android-based Crypto-Currency Wallets

*Atif Ghulam Nabi
Zurich, Switzerland
Student ID: 15-709-116*

Supervisor: Sina Rafati Niya, Prof. Burkhard Stiller
Date of Submission: May 31, 2018

Abstract

Cryptocurrencies have emerged as an important financial ecosystem relying on a secure distributed ledger based on blockchain technology and mining the transactions. Blockchain technology is disrupting society by enabling new kinds of disintermediated digital platforms [1]. The process of mining adds records of past transactions to the distributed ledger known as Blockchain, allowing users to reach secure, robust consensus for each transaction[2]. By using a cryptocurrency, users are able to exchange value digitally without third party oversight. The main interfaces to connect to BC and leverage the cryptocurrency ecosystem for regular users are web pages and mobile applications. The goal of this report on one hand is to evaluate at least three CC wallets such as Ethereum wallet[3], CoinBlesk[4], and a recently implemented wallet for Bazo BC[5] considering the technical and theoretical aspects. On the other hand, the focus is to propose a new wallet with comprehensive functionality for a new BC based on Proof of Space. To this end, an analytic study was conducted for android-based cryptocurrency wallets and a new set of requirements are proposed in this report with advanced security features to achieve high performance in terms of fast transaction handling, secure connections, scalability, and reliability.

Acknowledgments

I would like to express special thanks to my supervisors Sina Rafati and Prof. Dr. Burkhard Stiller, the head of the Communication Systems Group at the University of Zurich, for making this report possible.

Contents

Abstract	i
Acknowledgments	ii
Contents	iii
1 Introduction	1
1.1 Types of Cryptocurrency wallets:	2
2 Android Based Wallets	5
2.1 Ethereum Wallet	5
2.2 Enjin Wallet	8
2.3 Trust - Ethereum & ERC20 Wallet	10
2.4 Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	12
2.5 Coinbase - Buy Bitcoin & more. Secure Wallet.	13
2.6 Coins.ph Wallet	15
2.7 A Progressive Web App (PWA)-based Mobile Wallet for Bazo	16
2.8 CoinBlesk 4.0	19
3 Requirements for New Wallet	23
3.1 BurstCoin as an example	23
3.2 SpaceMint	24
3.3 Chia Wallet	25
3.4 Functional Requirements for New Wallet	25

3.5 Advanced Features 27

3.6 Security Requirements: 27

3.7 Reliability & Quality Requirements 28

4 Future Work 31

4.1 QuarkChain 31

4.2 Flutter Framework 31

4.3 Prototypes of the envisioned application should be developed. 32

Bibliography 33

List of Figures 35

Chapter 1

Introduction

A cryptocurrency wallet is a software program that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance. A wallet can contain multiple public and private key pairs. If you want to use Bitcoin or any other cryptocurrency, you will need to have a digital wallet. Every piece of cryptocurrency has a private key. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency[6]. As of January 2018, there are over thirteen hundred cryptocurrencies; the first and best known is bitcoin[7].

When choosing a wallet, the owner must keep in mind who is supposed to have access to (a copy of) the private keys and thus has potentially access to the cryptocurrency. Just like with a bank, the user needs to trust the provider to keep the cryptocurrency safe. Trust was misplaced in the case of the Mt. Gox exchange, who 'lost' most of their clients' bitcoins. Downloading a cryptocurrency wallet from a wallet provider to a computer or phone does not automatically mean that the owner is the only one who has a copy of the private keys. For example, with Coinbase[8], it is possible to install a wallet on a phone and to also have access to the same wallet through their website. The software can also have known or unknown vulnerabilities[9]. For receiving cryptocurrency, access to the receiving wallet is not needed. The sending party only needs to know the destination address. Anyone can send cryptocurrency to an address. Only the one who has the private key of the corresponding address can use it[10].

It's advisable to keep just small amounts of currency for everyday use online, on your computer or mobile. The majority of your crypto-coins should be stored in a highly secure environment. Choose a cold or offline storage options or an USB for backup. This ensures that your wallet can be recovered even if your computer fails or is lost or stolen.

It is important to have a backup for security reasons, no matter what wallet you are using, to avoid the loss of digital assets. There are many examples, people lose their wallets but if they don't have backup they lose the digital funds. A backup of a wallet can come in different forms like:

- A (encrypted) file like wallet.dat or wallet.bin which contains all the private keys.

- A mnemonic sentence from which the root key can be generated, from which all the private keys can be recreated. Preferably these words could be remembered or written down and stored on other physical locations.
- A private key like: KxSRZnttMtVhe17SX5FhPqWpKAEgMT9T3R6Eferj3sx5frM6obqA

When the private keys and the backup are lost then that cryptocurrency is lost forever. When using a webwallet, the private keys are managed by the provider. When owning cryptocurrency, those trusted with managing the private keys should be carefully selected. An (encrypted) copy of the wallet should be kept in a trusted place. Preferably off-line. Some people 'write' their mnemonic sentence or private key on metal, because it is robust[11].

To enhance the levels of security. It is recommended to keep your software up to date so that you have the latest security enhancements available. You should regularly update not only your wallet software but also the software on your computer or mobile. Add extra security e.g. two factor verification, make sure it's google authentication as supposed to text messages because people can easily clone your phone. Google authentication is a good safety feature when it comes to 2-step verification.

1.1 Types of Cryptocurrency wallets:

A few questions come into mind before selecting a wallet:

1. Do you need a wallet for everyday purchases or just buying and holding digital currency?
2. Do you plan to use several currencies or one single currency?
3. Do you require access to your digital wallet from anywhere or only from home?

There is a need to ponder over these questions, make a list of requirements and then choose a most suitable wallet. The type of wallet you should use really depends on your level of activity and level of security with which you want to handle your cryptocurrency. It also depends on how frequently you use your funds and how much you want to store on any particular wallet.

There are difference types of cryptocurrency wallets available in the market to manage the digital assets[12].

Desktop: wallets are downloaded and installed on a PC or laptop. They are only accessible from the single computer in which they are downloaded. You can easily download it, and it offers pretty good security; however, the downfall is you could only use it on your desktop. If the PC gets a victim of virus, hacker may easily access your private and public keys.

Web Wallets (aka Hot/Online/Hosted/Cloud Wallets): wallets run on the cloud and are accessible from any computing device in any location. These wallets are basically web services and are accessible through web/internet-based browsers such as Google Chrome, Firefox, and IE are called web-based Bitcoin wallets. They are also called "hosted wallets" because you store your bitcoins on the servers of the agency which you have chosen as your online wallet. The wallets in which private keys are stored online and which are connected 24/7 to the internet are called hot wallets. While they are more convenient to access, online wallets store your private keys online. There are security issues, people can hack your password, they can clone your phone.

Mobile Wallets: wallets run on an app on your phone and are useful because they can be used anywhere including retail stores. Mobile wallets are usually much smaller and simpler than desktop. They can be used anywhere around the world, some of them are quite secure, some of them have multi signature access, a lot of them have backup features. You never keep cryptocurrency on your phone, what you have is actually the keys, a mnemonic stores your private key and that key unlock your phone to see your digital assets.

Hardware/Cold Storage Wallets: These wallets differ from the software wallets in that they store a user's private key on a hardware device like a USB. Although hardware wallets make transactions online, they are stored offline which delivers increased security. It offers security and you can access it like your physical wallet.

Paper: wallets are easy to use and provide a very high level of security. While the term paper wallet can simply refer to a physical copy or printout to your public and private keys, it can also refer to a piece of software that it used to securely generate a pair of keys which are then printed.

Hot vs. cold wallets: Hot wallets are connected to the internet while cold wallets are not. With a hot wallet cryptocurrency can be spent at any time. A cold wallet has to be 'connected' to the internet first. As long as something is connected to the internet, it is vulnerable to an attack. The short version is that software wallets (where the device is turned on or the wallet software is running) are considered hot wallets. A (not connected) hardware wallet is considered a cold wallet.

Deep Cold Storage: is the process of storing cryptocurrencies in cold wallets that were never connected to the Internet or any kind of network. Additionally, the private keys associated with this system are generated offline.

Deterministic wallet: with a deterministic wallet a single key can be used to generate an entire tree of key pairs. This single key serves as the "root" of the tree. The generated mnemonic sentence or word seed is simply a more human-readable way of expressing the key used as the root, as it can be algorithmically converted into the root private key. That single root key is not replacing all other private keys, but rather is being used to generate them. All the addresses still have different private keys, but they can all be restored by that single root key. A mnemonic sentence is considered secure. It creates a 512-bit seed from any given mnemonic.

Non-deterministic wallet: in a non-deterministic wallet, each key is randomly generated on its own accord, and they are not seeded from a common key. Therefore, any backups of the wallet must store each and every single private key used as an address.

Chapter 2

Android Based Wallets

The main focus of this study is to compare and analyze android based cryptocurrency wallets in order to propose a set of requirements for a new wallet based Proof of Space.

Following cryptocurrency wallets will be analyzed for studying the theoretical and practical aspects in order to propose new requirements:

1. Ethereum Wallet
2. CoinBlesk
3. Bazo BC
4. Other popular android based-wallets

2.1 Ethereum Wallet

Ethereum is a decentralized platform that runs smart contracts, applications run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middleman or counterparty risk. The **Ethereum Wallet** is a gateway to decentralized applications on the Ethereum blockchain. It allows you to hold and secure ether and other crypto-assets built on Ethereum, as well as write, deploy and use smart contracts[13].

Ethereum team recommends using official clients, like Mist or Geth. They both are desktop wallets.

- Mist Ethereum Wallet: GUI, Official, Full Node, App, Supports ETH, Generic Token Interface, Generic Contract Interface

- Geth (go implementation): Command Line, Official
- There is another secure wallet, called Parity (Rust implementation - GUI + CLI). It is developed using the sophisticated and cutting-edge Rust programming language.

The official Ethereum Wallet, sometimes also called the Ethereum Mist Wallet, is a feature that is built into the Ethereum platform. Designed by the team behind Ethereum, the Wallet is integrated into the Mist web browser. This browser is an application that, while still under development, can be used to connect to the main Ethereum network and interact with other Ethereum applications. The Ethereum Wallet is free to download and use, although it will cost you some time and space on your hard drive to download the blockchain. You will most likely need to pay transaction fees in order to send ether over the network, although there is a built in flexibility feature to give you some control over fees in relation to transaction priority. You will have to understand and agree with the security and legal warnings before using the official Mist Ethereum desktop wallet as shown in the following figure.

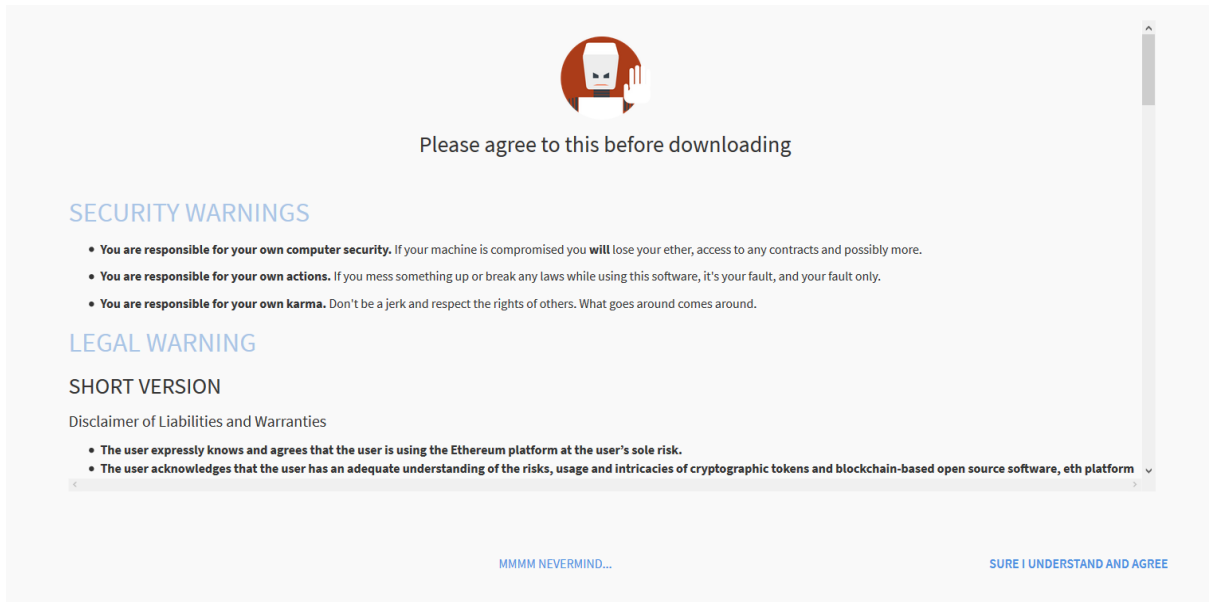


Figure 2.1: Term and Conditions for Ethereum Wallet

Ethereum is a young project, and many elements of the Ethereum platform are still under development. A lot of the existing infrastructure that enables users to interact with Ethereum is designed primarily for developers and those with a fairly advanced technical skillset. Fortunately, however, the official Ethereum Wallet does come with a simple graphical user interface (GUI) and it's not too difficult to get it up and running.



Figure 2.2: Ethereum Configuration

Pros	Cons
Easy to purchase ether with US dollars or bitcoin, or directly through the application.	Documentation is not easily accessible, it's not easy to understand how it works.
Because the developers behind Ethereum created this wallet, it's widely considered to be one of the most secure wallets for storing ether.	Sometime slow or freezing when contracts have a high update rate. (The DAO during first weeks is a good example)
Holds ether and other digital assets issued on the Ethereum platform.	To install the wallet, users need to download the entire Ethereum blockchain, which can take a long time and requires significant storage space.
Complete control over your passwords, private keys and funds without relying on any third-party software.	Non-mobile computer only (Windows, Linux, Mac). Only available as a desktop client.

How secure is the Ethereum Wallet?

The Ethereum Wallet is widely considered to be one of the most secure digital wallets for storing ether. Because your personal wallet is stored on your computer, you're in complete control of your private keys and your funds. This also means that if you lose your password or private keys, you may not be able to recover your wallet or its contents. It's a good idea to write down your password and keys and store them in a secure physical location.

However, regardless of the tool you use to create an account/wallet; you should always safely store all of the necessary information in multiple places. Multiple places mean multiple physical locations. If your house burns down, that computer and piece of paper are both gone. For example: on your computer, on a USB at your house and a safety deposit box, and written on a piece of paper at your office[14].

As the main focus is Android-based Ethereum wallet. The following primary features will be considered to study the popular Android Wallets:

- **Private keys** - Wallets where you control your private keys.
- **Ease of use** - Elegant UI for ease of use.
- **Development community** - Active development community.
- **Backup & security** - Backup and restore features.
- **Cutting-edge & Innovative features** - such fees calculating technologies, segregated witness, patch 32 address etc.
- **Compatibility** - Compatible with different operating systems.

We will look into the features of following popular android based cryptocurrency wallets.

- **Enjin Wallet**
- **Trust - Ethereum & ERC20 Wallet**
- **Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum**
- **Coinbase**
- **Coins.ph**

2.2 Enjin Wallet

The Enjin Smart Wallet is claimed to be a world's most secure cryptocurrency wallet available for Android — supporting BTC, ETH, LTC, ENJ and all ERC-20 tokens by default. It features a Smart UI that evolves on the fly to suit your specific needs, and employs innovative security measures to turn your smart phone into a hardware-like secure wallet. The Enjin Wallet never holds or has any access to your funds—you remain in total control of your private keys. You can always restore your wallet or funds on any device with your recovery 12 word passphrase[15].

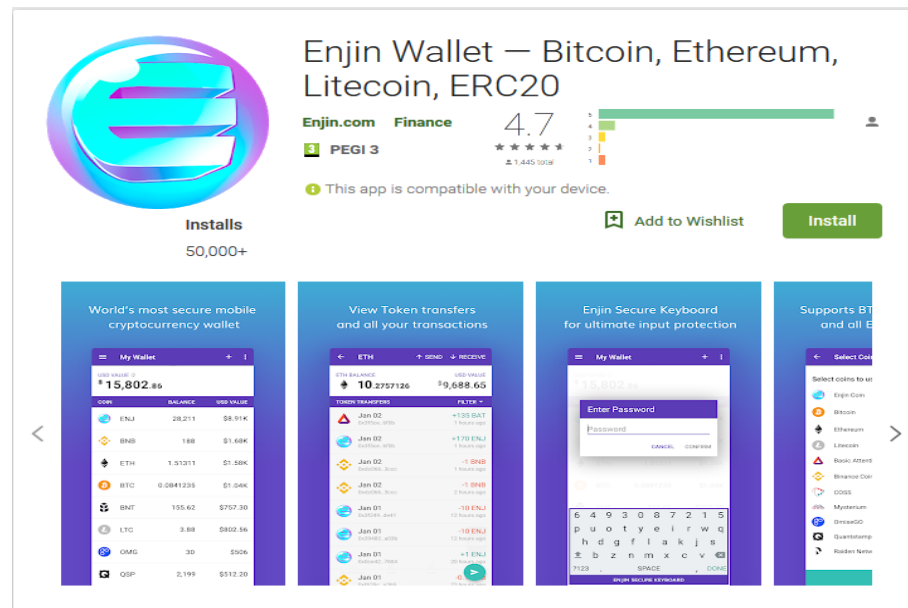


Figure 2.3: Enjin Wallet

Security Innovations

- **Enjin Secure Keyboard:** Designed to prevent any form of data sniffing or keyloggers, featuring an option to randomize keys for the ultimate level of input protection.
- **Rule of Two Encryption:** Two independent layers of cryptography protect the key-store and confidential data. Hardware 256 AES encryption is employed on the lower level and software encryption is utilised at the application layer.
- **Memory encryption:** Data is held in encrypted memory and any important values are deleted from system memory.
- **Screenshot & video blocking:** Secure window layout at the OS level stops any screen recording attempts.

Smart by Design, Simple by Choice

- **Smart UI:** Seamless and blazing-fast user interface evolves on the fly to suit your specific needs.
- **A wallet for any coin you own:** Supports Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Enjin Coin (ENJ) and all ERC-20 tokens. Other Altcoins will be supported soon.
- **Detailed transaction info:** View all the important details for all your transactions instantly.
- **Custom fees and limits:** Transaction fees are calculated dynamically, for optimal sending. Alternatively, you can set your own custom fees and limits.

Additional Features

- Multi-Currency values
- Multi-Lingual (31 languages)
- QR Scanner
- Import from most major wallets
- ETH Transaction filters

12 words and a pen

In case your device gets lost, you can secure your wallet and coins with just 12 words written on paper. The master phrase can restore your wallet and funds on any other device.

No ads. No tracking. Always free. Always private.

A free wallet with no ads or privacy concerns. That's our promise.

2.3 Trust - Ethereum & ERC20 Wallet

Trust Wallet is a secure mobile Ethereum wallet that supports Ethereum and ERC20, ERC223 tokens. It provides a fully security audited system to send, receive and store digital assets. With Trust Wallet you have complete control over your private keys that are only stored on your device. Trust Browser is a full-fledged Web3 browser that allows you to interact with decentralized applications (DApp) directly from the app. Meticulously crafted tool that provides a seamless, simple and secure connection between you, Ethereum network, and any decentralized application (DApp). Integrated interface that is fully optimized for mobile so you can enjoy the content designed specifically for your device.[16]

Salient Features of Trust - Ethereum wallet

- Participate in any ERC20 or ERC223 based ICO or airdrop. Configure gas price, gas limit and data/message in a simple and easy-to-understand way
- Gain a peace of mind with military grade security. Trust Wallet was fully audited by a leading security firm that ensured safety and integrity of the application
- Take the full advantage of Ethereum platform. Send, receive, store and track Ethereum (ETH), Ethereum Classic (ETC), Callisto (CLO) and over 30,000 supported ERC20 tokens, including EOS, OmiseGO, Qtum, Kyber Network, EOS, Bat, TenXPay and Augur
- Maintain control of your digital assets by storing your private keys on your own device. With Trust Wallets server-free infrastructure only you can access your funds

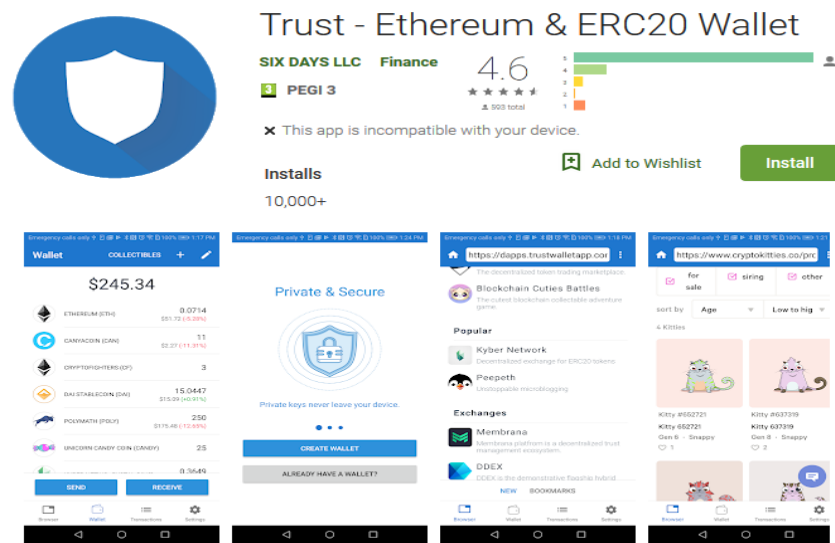


Figure 2.4: Trust - Ethereum & ERC20 Wallet

- Protect your crypto funds by enabling additional level of security - pin and biometrics. With that feature turned on, even if a mobile device is unlocked, the app will require separate authentication in order to access the funds
- Check balance, history, and other transaction details
- Backup and restore your wallet from a highly encrypted file in less than 30 seconds
- Access any cold storage wallet - Trezor, Ledger, KeepKey etc. - with Trust's "watch" function without exposing your private key in a "view-only" mode. Monitor performance of your digital assets while keeping keys in a safe and secure location
- See how much your tokens and coins are worth! Monitor real-time value of your digital portfolio and individual assets in your native currency
- Enjoy the simplicity of intuitive interface that was created specifically for a mobile device. You won't see your app crashing or lagging because our UI was built using native Android components and technologies

Trust - Ethereum Wallet for Android has been designed from the ground up to provide the best possible cryptocurrency experience on your Android device with following features:

Wallet: send and request ether, ERC20 and ERC223 tokens

Watch: add an address and get notified when it is active

DApp Browser: use decentralized applications to instantly buy, sell Ethereum and ERC20 and ERC223 tokens, collect digital assets such as cryptokitties and more

Push notifications: get notified of when transactions happen on your address

Transactions: see detailed information about transactions, full history, price of your portfolio

Send & Receive: easily send and receive assets via QR code or copy/paste

Security: set a passcode to protect the app to add another level of encryption

Additional Features

- DApp browser - explore "browser" tab to learn more and buy your first Cryptokitty
- Watch arbitrary address without the private key/keystore
- Lock screen with 6-digit pin
- Pending transactions show in transaction list
- Slicker UI on transaction list
- Collectables
- Bookmarks for dApp browser
- Mnemonic phrase

2.4 Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum

Blockchain Wallet strive to make using bitcoin and ether as simple and seamless as possible. Securely store your funds, exchange BTC, ETH & BCH, and instantly transact with anyone in the world. Access your existing wallet on your Android device or create a new one. It's free and takes just a few seconds[17].

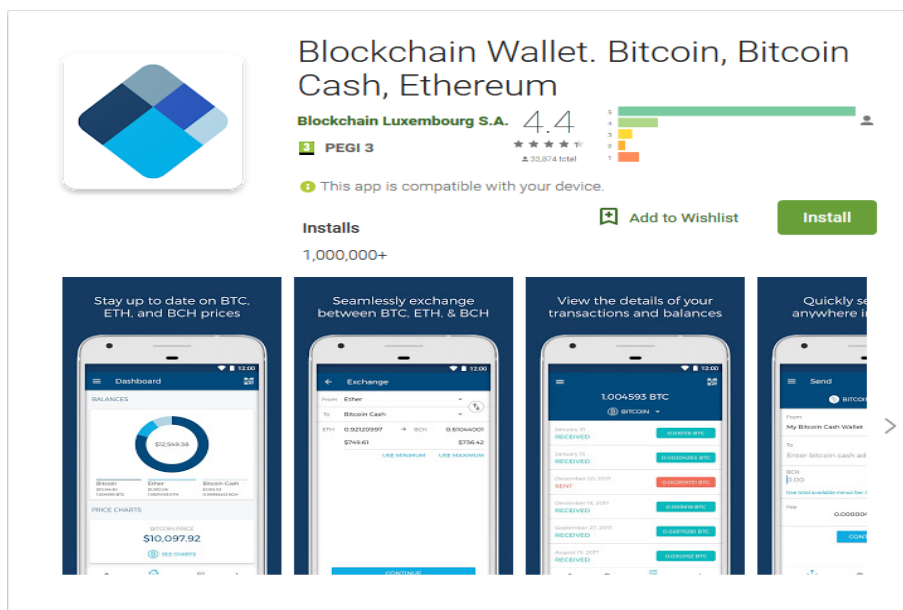


Figure 2.5: Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum

Main Features:

Ease of use

- Send and receive bitcoin, ether, and Bitcoin Cash instantly with anyone in the world
- Seamlessly exchange between bitcoin, ether, and Bitcoin Cash

Peace of mind

- You are the only one who has access to your funds

- You stay in control

High security

- A security center to help protect your funds from unauthorized access
- Advanced Two-Factor Authentication keeps the bad guys out
- Successfully completed security audits by world-class researchers
- PIN Protection

More features:

- Hierarchical deterministic address architecture
- Simplified backup and recovery with a 12 word backup phrase
- Server-side entropy for maximum randomness
- 20+ currency conversion rates
- 18 languages
- Dynamic fees
- Paper Wallet import
- Spending from watch-only addresses
- TOR blocking
- Open source
- QR Code Support

What's New

Notification Touch-Up - Rather than choosing to flood your phone with SMS messages when you buy or receive bitcoin, you can now opt to get push notifications instead.

2.5 Coinbase - Buy Bitcoin & more. Secure Wallet.

Coinbase is a private company based in San Francisco that provides web and mobile digital currency services. Coinbase offers to buy and securely store bitcoin, bitcoin cash, ethereum, and litecoin, offering the most complete services for btc, eth, and ltc on both web and mobile. It makes easy to securely buy, use, and store digital currency[18].

Highlights of Coinbase

- Buy and sell digital currency: You can easily buy and sell digital currency like bitcoin, bitcoin cash, ether, and litecoin directly from your Coinbase account without having to leave the app.
- Connect bank account: You can easily deposit or withdraw money, and buy or sell bitcoin with your linked bank account.
- Connect credit and debit cards: You can instantly buy bitcoin, bitcoin cash, ether, and litecoin with your linked credit cards in 32 countries.
- Connect PayPal: You can instantly sell bitcoin, bitcoin cash, ether, and litecoin with your linked PayPal account in US.

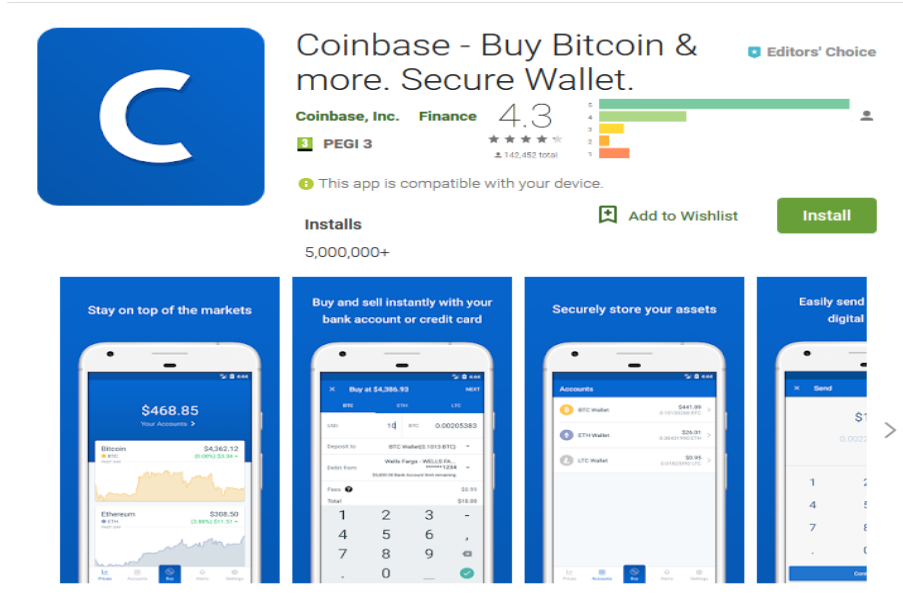


Figure 2.6: Coinbase Wallet

- Merchant services - accepted by over 38,000 businesses such as Dell, Expedia, and Overstock.
- Web and mobile - You can open your bitcoin, bitcoin cash, ethereum, and litecoin wallet and fully manage it on both web and mobile, and access your bitcoin, bitcoin cash, ether, and litecoin any time.

Coinbase Bitcoin Wallet for Android has been designed from the ground up to provide the best possible digital currency experience on your Android device with following features:

- Wallet: send and request bitcoin, bitcoin cash, ether, and litecoin instantly by name, email, or digital currency address
- Buy & sell: instantly convert your local currency into or out of bitcoin, bitcoin cash, ether, and litecoin
- Price charts: Track real time and historical bitcoin, bitcoin cash, ether, and litecoin price with price charts functionality.
- Price alerts: Get notified of changes in bitcoin, bitcoin cash, ether, and litecoin price on the go with our new price alerts functionality.
- Send & request: easily send and request money from any of your Google contacts, or send and request via NFC, QR code
- Security: set a passcode to protect the app and remotely disable your phone's access if lost or stolen

2.6 Coins.ph Wallet

Coins.ph is the easiest way to send money, buy load, pay bills and shop online. It was founded in 2014 by Silicon Valley entrepreneurs Ron Hose and Runar Petursson, Coins is Southeast Asia's leading mobile blockchain-enabled platform that enables anyone, including those without bank accounts, to easily access financial services directly from their phone. Using Coins, customers have access to a mobile wallet and services such as remittances, air-time, bill payments, and online shopping at over 100,000 merchants who accept digital currency. Operating in the Philippines and Thailand, Coins' mission is to increase financial inclusion by delivering financial services directly to people through their mobile phones. It offers following features to customers[19]

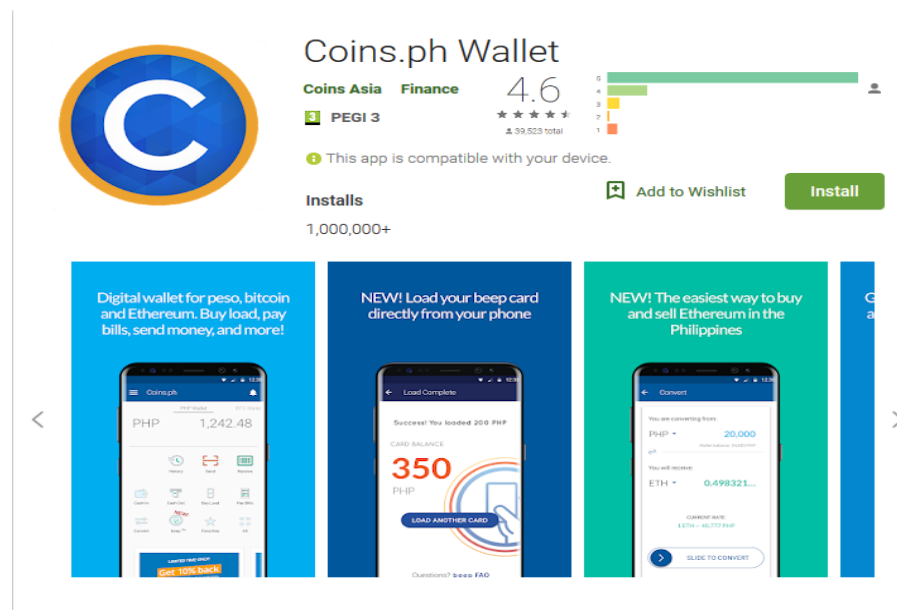


Figure 2.7: Coins.ph

Loading

- Load your beepTM card with Coins.ph
- It's instant, available 24/7, and has no fees!

Buy and Sell Ethereum

- Best Ethereum wallet in the Philippines
- Instantly buy, sell, send and receive Ethereum

Buy Load

- Get a 10% rebate instantly when you load any Smart, Talk n Text, Globe, TM, or Sun prepaid phone
- Choose from 70+ load promos for all major Philippines providers
- Buy international load for prepaid phones in 150 countries
- Save your favorite numbers to easily load next time

Pay Bills

- Pay Meralco, Smart, Sun, PLDT, Globe, and 80+ other billers all in one place
- Get a 5 PHP rebate every time you pay a unique bill

- Get an extra 100 PHP for every 5 unique bill payments you make each week

Cash In and Cash Out at 33,000+ Locations

- Instant cash in at any 7-Eleven, Cebuana, or M-Lhuillier nationwide
- 30+ major banks
- 5,000+ cash pickup locations
- 450 ATMs for instant cardless cash-out
- Door-to-door delivery

Send and Receive Cash

- Send money to any major bank or padala remittance center in the Philippines
- Person-to-person transfers are FREE
- Make and share payments instantly with your Facebook friends
- Transfer money to GCash and Smart Money mobile wallets
- Send fun holiday Red Envelopes (ang paos) to your friends and loved ones

Buy and Sell Bitcoin

- Send and receive funds from any Bitcoin wallet
- Pay online at Overstock, Newegg, Expedia, Microsoft, and 70,000+ other merchants accepting Bitcoin
- Buy and sell Bitcoin instantly in-app

Buy Game Credits

- Purchase game credits for Blizzard, Cherry, EX Cash, Game Club, Garena Shells, Level Up!, Steam Wallet, WarpPortal (Ragnarok Journey) and zGold-MOLPoints

Shop Online

- Buy eGiftCards from 120+ merchants delivered instantly via SMS and e-mail.

2.7 A Progressive Web App (PWA)-based Mobile Wallet for Bazo

Bazo is a cryptocurrency, developed by the Communication Systems Group of the University of Zurich. Bazo is a cryptocurrency developed at the University of Zurich. The currency was tailored to the use case of the financial service provider which acts as a central institution that is able to create new coins and accounts. This makes the currency private, since an invitation needs to be used to participate. The financial service provider developed a bonus program that incentivizes customers to use its credit cards by issuing virtual points for every conducted purchase with these cards. The virtual points can in turn be used to buy gift cards and coupons from registered partners on a centralized marketplace ordered by the service provider[20].

A Progressive Web Application (PWA), is a web application that has various characteristics that are usually found within native applications. They leverage the accessibility from the web but have various enhancements to give them a user experience that is closer to native mobile applications[21].

This differs from various popular cryptocurrencies such as Bitcoin and Ethereum which

2.7. A PROGRESSIVE WEB APP (PWA)-BASED MOBILE WALLET FOR BAZO17

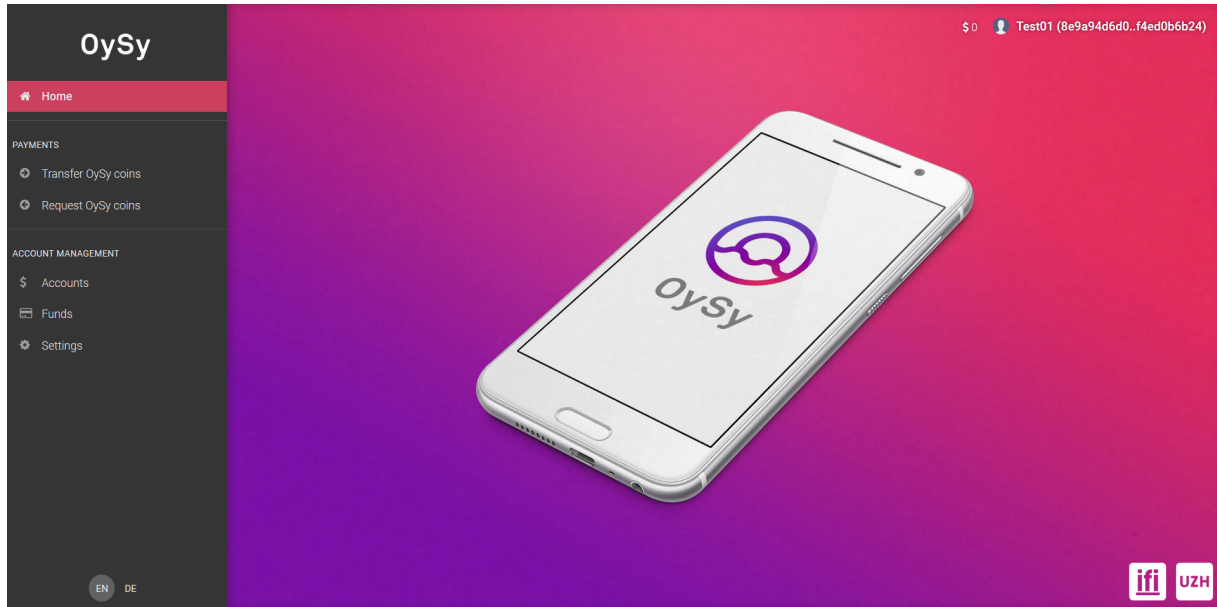


Figure 2.8: A Progressive Web App (PWA)-based Mobile Wallet for Bazo

are both open to the public. As part of the initial development efforts for Bazo, a full client application was created. With this application it is possible to issue transactions. However, in order to participate in the Bazo network, peers have to obtain a complete copy of the Blockchain.

Although the architecture for Coinblesk[22] is substantially different from the approach with Bazo, parts of the user interface are reused for the Bazo Wallet.

Salient Features of Bazo Wallet:

The developed Wallet application is enables the following operations.

- Requesting funds from other users. This is achieved by sending transaction data between users over multiple ways, such as NFC, BTLE, QR Code and Links.
- Sending funds to users.
- Inspecting account state such as e.g. balance.
- Linking account details to the Bazo Block Explorer, thus directing the user to it for further details.
- Requesting new Bazo coins from the traditional bonus points.
- Querying transaction value of a cash register in an existing POS system
- Operations with the currency are possible in a trustless way using the application.
- All operations requiring the users private key should be safe and run completely in the browser.

- It should not be necessary to send the key over a network or expose it in any other way.

Most of the features described above match with the functionality of myetherwallet.com, a web-based wallet for the Ethereum cryptocurrency, except for the ways of transferring transaction data.

Design

Due to Progressive Web Applications having native elements, PWAs can be a solution for providing a unified experience for multiple operating systems, targeting both mobile and desktop devices. All operations need to be made in the browser. Since no backend application should be leveraged, the Web app needs to be able to sign transactions in the browser. All further communication with the Bazo network is done over web interfaces. This led to the design of a RESTful web interface for the Bazo light client with following operations:

Querying account state: This endpoint should return all necessary information about the account's state such as balance, the transaction counter and information if the account has root access.

Preparing transactions: By supplying fee, transaction value, target and source address to this endpoint, the API will prepare the transaction hash and return it to the client to calculate the signature.

Distributing transactions in the peer-to-peer network: This endpoint can be used to post a transaction hash and signature. The API will then distribute the transaction in the peer-to-peer network.

In order to explore further possibilities on how to extend the browser support for native APIs a Proof of Concept was designed. The PoC is targeted to the Android platform, since NFC support is still fairly limited on iOS devices at the time of the design. This means that with Core NFC, a technology by Apple, only communication with passive NFC Tags is supported. Since the support for WebNFC is limited to Android devices, the functionality for writing and reading the transaction data is visible only to the users that have activated advanced options.

NFC Bridge

Due to limited browser support for Native APIs such as webNFC, a prototype was discussed and implemented. The prototype involved a native Android application that should enable the web application to forward transaction information to NFC capable devices using the Android Beam technology.

Payer control with the Bazo currency has a mixed image. The user has the control to create transactions at terms he prefers, for example, the user can set the fee he is willing to spend on the transaction. However, the clearance of the transaction highly depends on the network.

Security, as in the definition, should be given for all transactions signed by the user. From a technical point of view, the Wallet can be considered secure, as that it is not possible to steal a private key or manipulate transactions which would result in the loss of funds for the user.

Universality is not a strength of the Bazo currency. Since the Wallet is not compatible with other payment systems or applications, only users in the system can exchange funds. Since Bazo is a newly created cryptocurrency, there is no user base and users would have to be convinced to join the system.

There are some limitations of Bazo wallet:

Trust It is an objective of many cryptocurrencies to be as independent from third parties as possible. This should allow that assets can be traded in a trustless way. Since the application is designed as a Signing-Only Client, there needs to exist a certain amount of trust between the user of such a Wallet and the server he relies on.

Phishing Another risk is introduced with the unified data model of transaction data, since this points to the URL of the Bazo Wallet. One could trick a user into using a web application that looks like the Bazo Wallet, but has the single purpose of stealing the private key. This is a serious risk in cases where the user does not realize that the URL does not belong to the actual Wallet.

2.8 CoinBlesk 4.0

Coinblesk is a mobile bitcoin payment solution developed at the University of Zurich. It consists of a mobile android application and a central server providing payment services. While originally intended to be used as a payment system for a cafeteria, it has seen many improvements over the last years and can now be used as a general purpose bitcoin wallet and payment solution. Coinblesk supports trust-less, zero-confirmation transactions and mobile payments over Near Field Communication (NFC) and bluetooth, making it a great fit for a point-of-sale system. However, the increasing transaction fees become a problem in such a scenario, as they make up a large portion of each payment.

The first version of **CoinBlesk 1.0** ran in a client-server architecture, where the client was mostly a thin RESTful service consumer and the server was responsible for all communication with the Bitcoin network. Since the server could spend the money without the client's permission various legal issues arose from this approach.

CoinBlesk 2.0 addressed the above issues and introduced a new concept working with multisig Bitcoin addresses which brought more responsibilities to the client. Both versions of CoinBlesk worked only in combination with NFC. Furthermore, clients need to trust the server with both versions.

CoinBlesk 3.0 introduces a generic abstraction to handle any kind of communication channel, simplifies the CoinBlesk protocol further and improves it in a way that no more client trust is required. All improvements are based on top of the Bitcoin protocol and

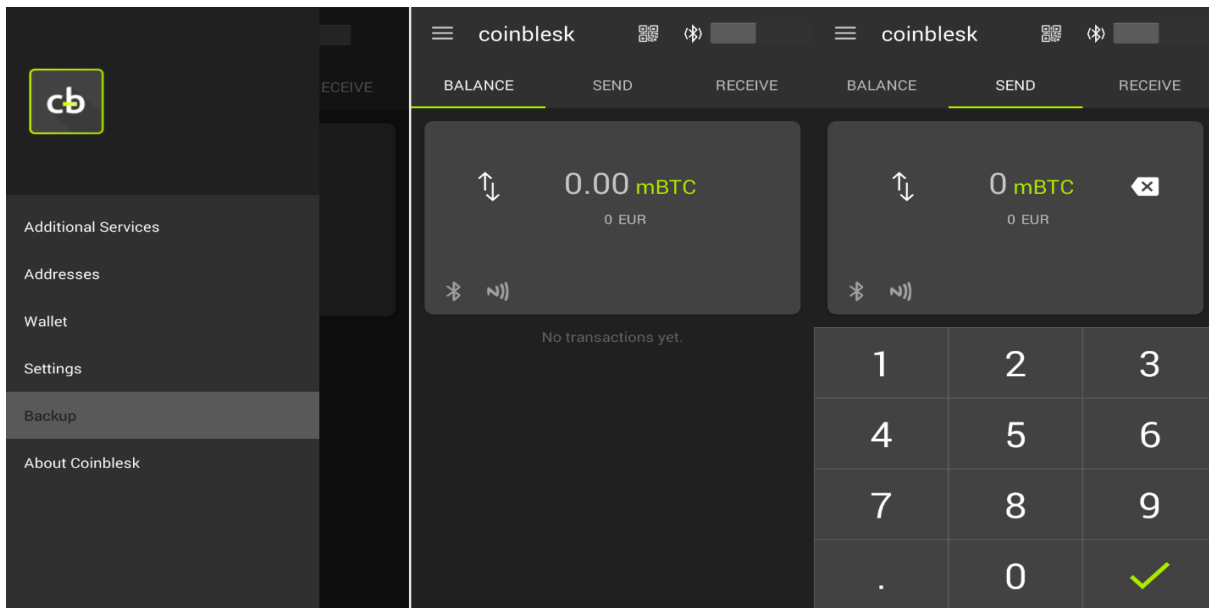


Figure 2.9: CoinBlesk 4.0

integrate transparently with the system. The proposed design keeps its compliance with Swiss banking laws and offers a better protection to clients without a negative impact on usability.

Major disadvantages were found related to transaction fees in the 3.0 version of CoinBlesk which are highlighted below.

Transaction Fees The user has to pay a transaction fee for each payment made with Coinblesk. This cost can be a significant, especially for smaller purchases: a minimal transaction between two Coinblesk user currently costs at least USD 1.52.

Security When transactions are made between Coinblesk users, the resulting unspent transaction outputs (UTXO) can be immediately spent again. Due to the currently missing malleability fixes in the bitcoin protocol, this makes those chained transactions unsafe.

Fixed transaction fees Currently Coinblesk uses a fixed hard-coded fee for transactions. However, the required fee for a fast block inclusion is dynamic and can change at any time. Requesting this fee from an external service would be the better option.

Outdated Codebase Coinblesk has seen many iterations over the last years. This has left the codebase in a sub-optimal state. There are outdated library dependencies and unused or untested code paths. Additionally, some unit tests are nondeterministic as they rely on a given execution order. Also development setup and deployment are non-trivial, as a specific application server is needed.

CoinBlesk version 4.0 addresses the issues mentioned above by providing the following features.

Micro-payment channels:

CoinBlesk introduces micropayment channel to decrease the costs and processing time.

In the initial step of creating a micropayment channel, the sending entity transfers some funds to an address that both the sender and receiver control. These types of addresses are known as MultiSig addresses. A n-of-m MultiSig address needs n out of m signatures to be spendable. In the case of a micropayment channel, a 2-of-2 address is used, meaning that neither the sender nor the receiver can spend the money on their own. However, there must be some mechanism that allows him to get that money back eventually. Otherwise the money might be lost forever, should the receiver disappear. It would also be possible for the receiver to extort money from the sender by threatening to not sign any transactions from the newly created address.

There are several ways to avoid this scenario. One solution is to use a **refund transaction** as the process is shown in following figure.

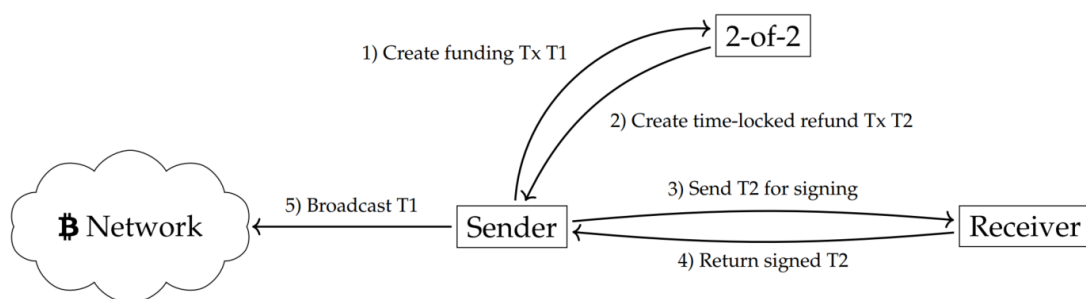


Figure 2.10: Refund Transaction

Initially, a funding transaction T1 is created by the sender (1), which he keeps secret. He then creates a refund transaction which connects to the funding transaction and sends all coins in the 2-of-2 MultiSig address back to himself (2). This refund transaction additionally has a time lock, which prevents a broadcast before some time in the future. This is possible by using the **nLockTime** field in a transaction. The refund transaction is then sent to the receiver (3), who signs it and sends it back to the sender (4). Now the sender owns a transaction which gives him the guarantee that he will eventually get back his money, should the receiver stop collaborating. In the worst case he has to wait until the lock time is reached. Knowing this, he can then safely broadcast T1 to the network, locking some money in the MultiSig address (5) and completing the setup.

Key Exchange: A user sends his public key to the server, which will then respond with his own user specific public key. This is equivalent to the old system and acts as a registration process. The key exchange has to be done once per user.

Time locked Address: After the initial key exchange, the user creates a new bitcoin address. This address is a 2-of-2 MultiSig address that requires both signatures from the exchanged keys. It is also defined by a user-chosen lock-time, a timestamp set in the future, after which the client is able to spend funds in the address without the involvement of the server. This lock-time gives the user the guarantee that he will eventually be able to retrieve his funds in case of an uncooperative server.

Funding of Address: In order to make any payments, the user must load some funds into one of his time-locked addresses. The method of funding is left to the user. He can use any wallet or bitcoin exchange provider or be funded by a different Coinblesk user. After a funding transaction was made, he must wait for at least one block for the transaction to be confirmed.

Virtual Payment to Coinblesk User: A user that has received micropayments can use his virtual balance to directly transfer funds to other Coinblesk users. This is a very cheap and efficient way to transfer coins, as it is a simple database change and does not involve any bitcoin related operations.

Server Operations:

Closing of Channels The server can close a payment channel at any time. This is done by broadcasting the latest saved channel transaction to the network and locking the user's account until the transaction is mined in a block.

Increasing/Decreasing Pot Size The server administrator might choose to increase the pot size for more liquidity in the system. Likewise, coins can be taken out from the pot if they are needed elsewhere.

Trust Coinblesk 4.0 adds some required trust back to the system. When a user sends some funds over a micropayment channel, he trusts the server to forward that money to the receiver at some point in the future. Likewise, the receiver trusts the server to receive a payout of his virtual balance from the server. Trust between Coinblesk users is not required.

Improvements in bitcoin 4.0 regarding protocol

Following section describes the improvement in protocol and communication.

- **Near Field Communication**

Near Field Communication (in short NFC) is a short range wireless technology. It allows devices to communicate within 10cm distance. The technology is based on the RFID standard. NFC can be used in combination with passive tags that don't require any external power source. Its theoretical transmission rate of 100-800Kbit/s makes it only usable for small data transfers.

- **Peer-to-Peer Mode**

This mode allows two NFC devices to communicate with each other. Both devices are active and communicate using a logical link control protocol.

- **Read/Write Mode**

This mode allows an active NFC device to read data from or write data to a passive device (e.g., a NFC tag). The data exchanged has to follow the rules described in the NFC Data Exchange Format (in short NDEF).

- **NFC Card Emulation Mode**

This mode allows a passive device to emulate an NFC smart card. The device in NFC Card emulation mode cannot initiate the communication, it can only reply to request made by the active device interacting with it.

Chapter 3

Requirements for New Wallet

Proof-of-space (PoSpace), also called proof-of-capacity (PoC), is a means of showing that one has a legitimate interest in a service (such as sending an email) by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider. The concept was formulated by Dziembowski[23] in 2015 and independently by Ateniese[24]. Proofs of space are very similar to proofs of work, except that instead of computation, storage is used. Proof-of-space is related to, but also considerably different from, memory-hard functions and proofs of retrievability.

After the release of Bitcoin, alternatives to its PoW mining mechanism were researched and PoSpace was studied in the context of cryptocurrencies. Proofs of space are seen as a fairer and greener alternative due to the general-purpose nature of storage and the lower energy cost required by storage. Several theoretical and practical implementations of PoSpace have been released and discussed, such as SpaceMint and Burstcoin.

3.1 BurstCoin as an example

PoSpace has been used in the Burstcoin cryptocurrency founded in August 2014. Burstcoin claims to have a green algorithm that favors smaller miners by design, making transaction costs cheaper and the network more decentralized[25]. The goal of depending on smaller miners was most typified by the original Android app to mine Burstcoin. However, by December 2017, the estimated network size approached 157,000 terabytes and the average mining payoff was 21 burst per week per terabyte, so participants with disk space measured in gigabytes are no longer likely to receive significant payback from mining. It's an open source project.

BurstCoin offers following features:

Ease of use

- Send and receive Burstcoins instantly with anyone in the world
- It's safe, simple, and fast

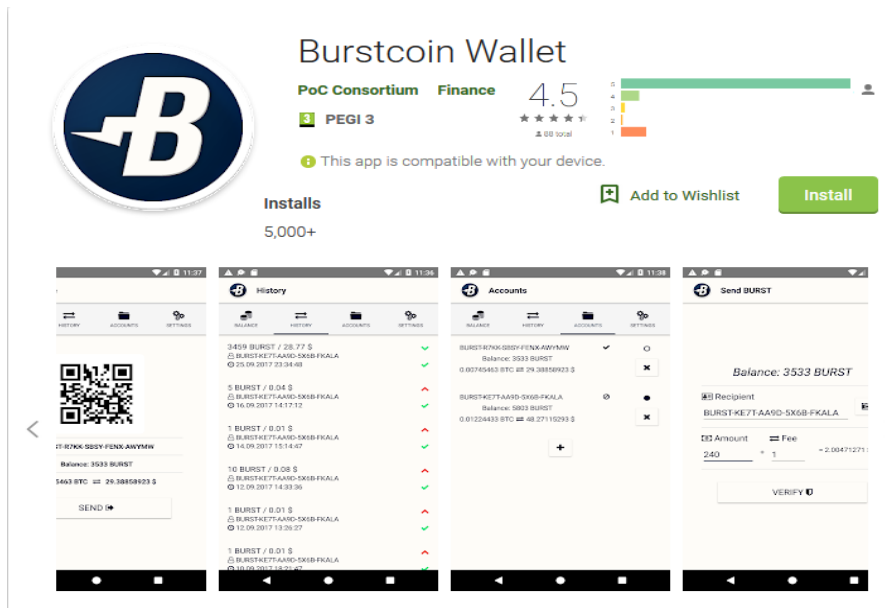


Figure 3.1: BurstCoin Wallet

High security

- Random Seed Generation
- PIN Protection

Main Features:

- * Watch only addresses
- * Currency conversion
- * Client-side encryption and decryption
- * QR code support
- * Secure and easy passphrase generation
- * Support for 15 languages
- * Support for over 30 currencies

They don't use proof of capacity as means of mining, they use distributed storage?

3.2 SpaceMint

SpaceMint is a cryptocurrency that replaces energy-intensive computation underlying most of today's cryptocurrencies by "proof of space". Once set up, SpaceMint consumes very little energy, which will motivate regular users to participate in the mining process thereby truly decentralizing control over the currency.[26]

In Spacemint, once a miner has dedicated and initialized some space, participating in the mining process is very cheap. A new block is added to the chain every fixed period of time, and in every period a miner just has to make a small number of lookups to the stored space to check if she "wins", and thus can efficiently add the next block to the chain and

get the mining reward. In this paper, we detail the construction of Spacemint, analyze its security and game-theoretic properties, and study its performance. Our prototype shows that it takes approximately 25 seconds to prove over a terabyte of space, and it takes a fraction of a second to verify the proof[27].

3.3 Chia Wallet

Ram Cohen invented torrenting. Now he's building a cryptocurrency called Chia that doesn't waste electricity like Bitcoin, and top investors are lining up. Chia has just raised a \$3.395 million seed round led by AngelList's Naval Ravikant and joined by Andreessen Horowitz, Greylock and more. The money will help the startup build out its Chia coin and blockchain powered by proofs of space and time instead of Bitcoin's energy-sucking proofs of work, which it plans to launch in Q1 2019[28].

3.4 Functional Requirements for New Wallet

Requirements are criteria that are necessary to meet project objectives. Typically, they outline how the product or solution will address the needs of the product and/or its users. Requirements documents can be high-level, as it's likely the product will change and evolve as new information and learnings become available.

The purpose of the project is to develop a state of the art cryptocurrency wallet based on proof of space. It will enhance the security for managing cryptocurrency coins with a highly secure and easy to use wallet. It will streamline the current business process for trading existing cryptocurrency coins along with supporting the new emerging coins based on proof of space by introducing new features. The newly developed will be an initial version of product. The underlying infrastructure will be different as compared to Coinblesk or other available wallets based on Proof of Work. However, the existing features can also be used from the previous versions of CoinBlesk or open source projects. A highly secure and elegant user interface is the main object of the project. It should be compliant technically with the PoSpace, newly developed APIs and protocols.

Functional requirements are described in the following section.

Requesting & Sending funds from other users. This is achieved by sending transaction data between users over multiple ways, such as NFC, BTLE and QR Code. It should allow to send funds to users on the same network as well as sending funds to users on other networks instantly in-app. You should easily buy and sell digital currency directly from your wallet account without having to leave the app with an intention to provide a seamless customer experience.

Shop Online Pay online to all merchants who are accepting cryptocurrency.

Watch only addresses A watch-only address is a public bitcoin addresse you've imported into your wallet. This is a cool, useful feature if you want to monitor activity

at a particular bitcoin address. You can import any existing coin address (e.g. 1PRxCERNys1jWEBnbG3Ad1e2s3uQzpasGX) into your wallet as a watch-only address, which will incorporate all of its incoming and outgoing transactions into your live transaction feed.

Linking account details to the Block Explorer, directing the user to it for further details.

Currency conversion There should be a feature to display the latest conversion rates for different cryptocurrencies. Application should allow to seamlessly exchange between bitcoin, ether, and other popular currencies.

Client-side encryption and decryption Client side encryption means only you have access to your wallet. Server should not store your coins. The wallet can be encrypted on android device with your personal password. The private password acts as a decryption key to both lock and unlock the wallet —it shouldn't be accessed without the password.

QR code support There should a QR code support to easily transfer funds and share public keys with other users as it was developed in the CoinBlesk application.

Secure and easy passphrase generation Security is especially important because if the coins are stolen, there is often no recourse. Online transactions cannot be reversed on blockchain network. A passphrase is similar to a password in usage, but is generally longer for added security.

Multi language Support Both English and German language should be supported in the initial version of wallet.

Multi-Currency Support Application should support conversion of popular cryptocurrencies for buying and selling coins. It should support Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), and all ERC-20 or ERC-223 tokens. Other popular currencies should also be supported.

CoinBlesk Salient Features This newly developed cryptocurrency wallet should contain the Coinblesk competitive features e.g. Near Field Communication, Bluetooth LE, Micro-payment channel, Time locked Addresses, Refund Transactions etc.

Dynamic Fees work to detect changes in network volume and will raise or lower transaction fees accordingly. This means that the same transaction may require a higher fee during a period of network congestion, or a lower fee if sent during a period of decreased activity. Alternatively, you can set your own custom fees and limits.

Funds Management check balance, full history, price of your portfolio, and other transaction details. Monitor real-time value of your digital portfolio and individual assets in your native currency.

Paper Wallet It should allow to import the paper wallet. There can also be an option to print your private keys in a paper wallet by sending a file through Email.

Notification Touch-Up - Rather than choosing to flood your phone with messages when you buy or receive bitcoin, you should be able to opt to get push notifications instead.

Mnemonic Sentence In case your device gets lost, you can secure your wallet and coins with just 12 words written on paper. The master phrase can restore your wallet and funds on any other device.

3.5 Advanced Features

- **Connect bank account:** It should allow to easily deposit or withdraw money, and buy or sell bitcoin with your linked bank account.
- **Connect PayPal:** There can be an option to instantly sell cryptocurrency coins with your linked PayPal account.
- **Connect credit and debit cards:** You should be able to instantly buy bitcoin, bitcoin cash, ether, and litecoin with your linked credit cards
- **Omnichannel integration** in the future to attract more customers. It is a multichannel approach to sales that seeks to provide the customer with a seamless shopping experience whether the customer is shopping online from a desktop, web or mobile device.
- **Price charts & alerts:** Track real time and historical cryptocurrency prices with price charts functionality. There can be a functionality to get notification of changes in cryptocurrency price on the go with the new price alerts.
- There can be an option to access any cold storage wallet for example Trezor, Ledger etc. - with a function without exposing your private key in a view-only mode. It would also be helpful to monitor performance of digital assets while keeping keys in a safe and secure location.

3.6 Security Requirements:

All operations requiring the users private key should be safe and run completely in the app with security. It should not be necessary to send the key over a network or expose it in any other way. MultiSig has already been introduced in the Bitcoin Core, it adds more trust and security in the system for end users in micropayment channels. It will enhance the security to spend cryptocurrencies. High security of application is primary objective. It should provide peace of mind that a user is the only one who has access to his funds. A user controls his funds without involvement of central authority.

- **Level 1:** It should integrate advanced Two-Factor Authentication to keep the malicious users out.
- **Level 2:** Protect your crypto funds by enabling additional level of security - 6-digit pin and biometrics. With that feature turned on, even if a mobile device is unlocked, the app will require separate authentication in order to access the funds.

- Level 3: Block all the TOR requests. This option blocks IP addresses coming from the Tor network from accessing your account. Tor is an anonymizing tool that is often used by hackers, although many privacy enthusiasts also use Tor for non-malicious purposes.
- Rule of Two Encryption: Two independent layers of cryptography to protect the keystore and confidential data[29].
- Memory encryption: Data should be held in encrypted memory and any important values must be deleted from the system memory.
- Hierarchical deterministic address architecture. All HD wallets use 12-word master seed keys. Each time this seed is appended by a counter at the end and is used to derive seemingly unlimited new Bitcoin addresses hierarchically and sequentially.
- Application should offer a feature for a simplified backup and recovery with a 12-word backup phrase or using a highly encrypted file.
- Secure Keyboard: Designed to prevent any form of data sniffing or keyloggers, featuring an option to randomize keys for the ultimate level of input protection.
- Remote Access: It should disable android phone's access remotely.
- Screenshot & video blocking: Secure window layout should be developed at the OS level to stop any screen recording attempts.
- There should be security audit on the application by a competitive security auditor to ensure the safety and integrity of the application.
- An online security center or support to help protect the funds from unauthorized access with an emergency response.

3.7 Reliability & Quality Requirements

- It should be available instantly, 24/7, without incurring fees from users. The newly developed wallet should instantly offer the services to buy, sell, send and receive cryptocurrency coins.
- There should be a simple and intuitive interface using the latest UI elements for android device.
- There should not be any app crashing or lagging in the application. It is recommended to build the UI using native Android components and technologies.
- In order to make sure the transparency and enhance trust, source code should be kept open source.
- Smart UI: Seamless and blazing-fast user interface evolves on the fly to suit the customer specific needs.

- Users can focus on objects and read necessary text. App installs and runs without crashing. App maintains high performance. There should be maximum test coverage for the written code to make sure the high quality and smooth experience for customers.
- No ads, no tracking. Always free and secure.

Features	Enjin Wallet	Trust - Ethereum	Blockchain Wallet	Coinbase	Coins.ph	CoinBlesk	BurstCoin	MBM Wallet
Requesting & Sending funds	✓	✓	✓	✓	✓	✓	✓	✓
Watch only addresses	✗	✗	✓	✗	✗	✗	✓	✓
QR Support	✓	✓	✓	✓	✓	✓	✓	✓
Shop Online	✓	✗	✗	✓	✓	✓	✗	✓
Game Credits	✓	✗	✗	✗	✓	✗	✗	✓
Micropayment Channel	✗	✗	✗	✗	✗	✓	✓	✓
Dynamic Fees	✓	✗	✓	✗	✗	✗	✓	✓
Connect credit and debit cards	✗	✗	✓	✓	✓	✗	✓	✓
Rule of Two Encryption	✓	✗	✗	✗	✗	✗	✗	✓
Memory encryption	✓	✗	✗	✗	✗	✗	✗	✓
Advanced Two-Factor Authentication	✓	✗	✓	✓	✓	✗	✗	✓
Smart & Sleek UI	✓	✓	✓	✗	✓	✗	✗	✓
Omnichannel integration	✗	✗	✗	✗	✗	✗	✗	✓
Secure Key-board	✓	✗	✗	✗	✗	✗	✗	✓
Screenshot & video blocking	✓	✗	✗	✗	✗	✗	✗	✓
Price charts	✗	✗	✗	✓	✗	✗	✗	✓
Open Source	✗	✓	✓	✗	✗	✓	✓	✓
Segregated Witness	✗	✗	✗	✗	✗	✗	✗	✓

This table highlights a comparison of android wallets studied in this report with a newly proposed wallet.

Chapter 4

Future Work

There is need to explore and find the potential of latest tools and technologies in future work. A few examples are discussed in this section.

4.1 QuarkChain

The QuarkChain Network introduces a novel sharding-based blockchain architecture that aims to meet the global commercial standard. Visa claims 56,000 Transactions per second (TPS), Alipay claims 200,000 TPS. QuarkChain wants to bring the number of transactions per second to go beyond the moon with not just 10,000, no, not even 100,000 but yes, 1 MILLION transactions per second. The real challenge with blockchain scalability isn't getting the number of transactions per second up, it's doing this whilst maintaining an acceptable level of decentralization and security for the blockchain. When it comes to decentralization, QuarkChain has implemented several innovative features such as an ASIC-resistant Proof-of-Work (PoW) algorithm so that QuarkChain essentially operates as a hybrid PoW blockchain[30]. It is required to explore such other technologies for high scalability and advanced security.

4.2 Flutter Framework

Flutter is an open-source mobile application development SDK created by Google. It is used to develop applications for Android and iOS, as well as being the primary method of creating applications for Google Fuchsia. Its preview release Beta 3 (v0.3.2) was published in May 2018. UI design in Flutter involves assembling and/or creating various widgets. A widget in Flutter represents an immutable description of part of the user interface; all graphics, including text, shapes, and animations are created using widgets.

More complex widgets can be created by combining many simpler ones. The Flutter framework contains two sets of widgets which conform to specific design languages. Material

Design widgets implement Google's design language of the same name, and Cupertino widgets imitate Apple's iOS design[31].

There are also other competitors in the market like ReactNative, Xamrin. It is claimed that Flutter provides support for android and iphone without any bridge or third party APIs to access native components. A further study is required to understand the full potential of Flutter framework for using native components and leverage the framework for developing a single codebase.

4.3 Prototypes of the envisioned application should be developed.

Software prototyping is the activity of creating prototypes of software applications, i.e., incomplete versions of the software program are developed. A prototype typically simulates only a few aspects of, and may be completely different from, the final product. The next step after collecting and finalizing the requirements, should be validation of requirements through prototypes to realize the concept of future product.

Bibliography

- [1] Juri-Mattila-.pdf, <http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf>
- [2] IEEE, <https://ieeexplore.ieee.org/document/7906988/>
- [3] Ethereum Wallet, <https://www.ethereum.org/>
- [4] <https://ercim-news.ercim.eu/en110/special/coinblesk-a-real-time-bitcoin-based-payment-approach-and-app>.
- [5] A Progressive Web App (PWA)-based Mobile Wallet for Bazo, <https://files.ifi.uzh.ch/CSG/staff/bocek/extern/theses/BA-Jan-von-der-Assen.pdf>
- [6] Wat is cryptocurrency? <https://cryptostart.nl/introductie-in-cryptocurrency/>
- [7] What is cryptocurrency, how does it work and why do we use it?, <https://www.telegraph.co.uk/technology/0/cryptocurrency/>
- [8] Coinbase, <https://www.coinbase.com>
- [9] CCN, <https://www.ccn.com/15-year-old-hacks-hardware-crypto-wallet-ledger/>
- [10] CCN, <https://www.ccn.com/15-year-old-hacks-hardware-crypto-wallet-ledger/>
- [11] COINALERT, <http://coinalert.eu/2015017743-Cryo+Card+Review+Nearly+Indestructible+Bitcoin+Cold+Storage.html>
- [12] coindesk, <https://www.coindesk.com/information/how-to-store-your-bitcoins/>
- [13] ethereum, <https://www.ethereum.org/>
- [14] StackExchange, <https://ethereum.stackexchange.com/questions/1239/what-is-the-recommended-way-to-safely-store-ether>
- [15] Google Play, <https://play.google.com/store/apps/details?id=com.enjin.mobile.wallet>

- [16] Google Play, <https://play.google.com/store/apps/details?id=com.wallet.crypto.trustapp>
- [17] Google Play, <https://play.google.com/store/apps/details?id=piuk.blockchain.android>
- [18] Google Play, <https://play.google.com/store/apps/details?id=com.coinbase.android>
- [19] Google Play, <https://play.google.com/store/apps/details?id=asia.coins.mobile>
- [20] Bazo - A Cryptocurrency from Scratch, <https://files.ifi.uzh.ch/CSG/staff/bocek/extern/theses/BA-Livio-Sgier.pdf>
- [21] A Progressive Web App (PWA)-based Mobile Wallet for Bazo, <https://files.ifi.uzh.ch/CSG/staff/bocek/extern/theses/BA-Jan-von-der-Assen.pdf>
- [22] Transaction Fee Reduction in Coinblesk, <https://files.ifi.uzh.ch/CSG/staff/bocek/extern/theses/MA-Sebastian-Stephan.pdf>
- [23] Cryptology ePrint Archive: Report 2013/796, <https://eprint.iacr.org/2013/796>
- [24] Proofs of Space: When Space is of the Essence, <https://eprint.iacr.org/2013/805.pdf>
- [25] Burstcoin - An Energy Efficient Cryptocurrency, <https://ecoin4dummies.com/2017/12/28/burstcoin-energy-efficient-cryptocurrency/>
- [26] SpaceMint: A Cryptocurrency Based on Proofs of Space, <https://dc1.mit.edu/research/spacemint-cryptocurrency-mining>
- [27] Spacemint: A Cryptocurrency Based on Proofs of Space, <https://pdfs.semanticscholar.org/f217/9075332a2f5517edc16fd23a74d59d80ff63.pdf>
- [28] BitTorrent inventor announces eco-friendly bitcoin competitor Chia, <https://techcrunch.com/2017/11/08/chia-network-cryptocurrency/>
- [29] Wikipedia, https://en.wikipedia.org/wiki/Multiple_encryption
- [30] QuarkChain, <https://hackernoon.com/quarkchain-is-this-new-crypto-blockchain-pure-quackery-or-pure-genius-d7fd275102de>
- [31] Flutter, <https://flutter.io/>

List of Figures

2.1	Term and Conditions for Ethereum Wallet	6
2.2	Ethereum Configuration	7
2.3	Enjin Wallet	9
2.4	Trust - Ethereum & ERC20 Wallet	11
2.5	Blockchain Wallet. Bitcoin, Bitcoin Cash, Ethereum	12
2.6	Coinbase Wallet	14
2.7	Coins.ph	15
2.8	A Progressive Web App (PWA)-based Mobile Wallet for Bazo	17
2.9	CoinBlesk 4.0	20
2.10	Refund Transaction	21
3.1	BurstCoin Wallet	24