

**Alpha**

**Multipurpose Cryptocurrency Wallet Google Chrome Extension**

**Department of Software Engineering**

**Capstone Project Phase A, 22-1-D-1**

**Supervisors**

Alexander Keselman

**Authors**

Alla Davydov317000669 [davydov.alla@gmail.com](mailto:davydov.alla@gmail.com)

Pavel Golikovski320636574 [pavel.golikovski@gmail.com](mailto:pavel.golikovski@gmail.com)

Table of Contents

[1 Abstract 4](#_Toc92466138)

[2 Introduction 4](#_Toc92466139)

[2.1 Motivation 4](#_Toc92466140)

[2.2 Overview 4](#_Toc92466141)

[2.3 Structure 5](#_Toc92466142)

[3 Background and Related Work 5](#_Toc92466143)

[3.1 Blockchain 5](#_Toc92466144)

[3.2 Mining 5](#_Toc92466145)

[3.2.1 Proof of Work 6](#_Toc92466146)

[3.3 Decentralization 6](#_Toc92466147)

[3.4 Ethereum Blockchain 6](#_Toc92466148)

[3.4.1 Gas 7](#_Toc92466149)

[3.4.2 Gas Limit 7](#_Toc92466150)

[3.5 Smart Contracts 8](#_Toc92466151)

[3.6 Cryptocurrency Wallets 8](#_Toc92466152)

[3.6.1 Custodial and Non-Custodial Wallets 8](#_Toc92466153)

[3.6.2 Hierarchical Deterministic (HD) Wallets 8](#_Toc92466154)

[3.6.3 Derivation Paths 9](#_Toc92466155)

[3.6.4 Mnemonic Phrases 9](#_Toc92466156)

[3.7 Decentralized Finances (DeFi) 9](#_Toc92466157)

[3.7.1 Infura 10](#_Toc92466158)

[3.7.2 Nods 10](#_Toc92466159)

[3.7.3 EVM 11](#_Toc92466160)

[3.8 Decentralized Lending and Borrowing 11](#_Toc92466161)

[3.8.1 Compound 12](#_Toc92466162)

[3.9 Decentralized Exchanges (DEX) 12](#_Toc92466163)

[3.9.1 Uniswap 13](#_Toc92466164)

[3.9.2 dYdX 13](#_Toc92466165)

[3.10 Aggregators 14](#_Toc92466166)

[3.11 Web3 14](#_Toc92466167)

[3.12 React 15](#_Toc92466168)

[3.12.1 Semantic UI 15](#_Toc92466169)

[4 Expected Achievements 16](#_Toc92466170)

[4.1 Product Infrastructure and Flow 16](#_Toc92466171)

[4.2 Success Criteria 16](#_Toc92466172)

[4.3 Unique Features 16](#_Toc92466173)

[5 Engineering Process 17](#_Toc92466174)

[5.1 Process 17](#_Toc92466175)

[5.1.1 Methodology 17](#_Toc92466176)

[5.1.2 Research 17](#_Toc92466177)

[5.1.3 Challenges 20](#_Toc92466178)

[5.2 Product 20](#_Toc92466179)

[5.2.1 Requirements 20](#_Toc92466180)

[5.2.2 Architecture 21](#_Toc92466181)

[5.2.3 API 21](#_Toc92466182)

[5.2.4 Flowcharts and Interface 23](#_Toc92466183)

[5.2.5 Deployment 29](#_Toc92466184)

[6 Evaluation and Verification Plan 30](#_Toc92466185)

[6.1 Testing 30](#_Toc92466186)

[6.2 Evaluation 31](#_Toc92466187)

[7 References 32](#_Toc92466188)

# Abstract

As of today, more and more decentralized financial services are being published to complement traditional financial practices. With that being said, many services come with many diverse user interfaces, varying user experiences and different learning curves.

In this project - **Alpha**, we want to assist novice and advanced Ethereum users alike to interface with the Ethereum Blockchain and DeFi services in a coherent and uniform manner by aggregating services such as Compound and Uniswap into a single local Google Chrome extension.

Using our browser extension users may manage their cryptocurrency assets in a built-in cryptowallet, perform transactions and use additional services such as Compound to borrow or lend money or convert it into other currency using Uniswap, *just like your own private banking service*, directly from within the extension.

Alpha incorporates external APIs that communicate with the Ethereum Blockchain via Smart Contracts to accomplish various financial operations, leveraging Blockchain’s inherent architecture to substitute centralized databases in order to provide security and verifiable actions.

Our main goal is to contribute to the DeFi ecosystem and to build a better financial landscape made possible by the Internet and the Ethereum Blockchain.

# Introduction

Traditional financial culture still mostly relies on centralized systems and third-party entities in order to perform monetary transactions that are inherently vulnerable. In turn, the centralized nature of such systems gave rise to the modern decentralized Blockchain technology.

## Motivation

As Blockchain technologies evolve and increasingly integrate with more and more aspects of our lives, it brings with it a myriad of new issues that are being solved by a magnitude of different developers and parties, which in turn offer a multitude of varying solutions.

In practice, this in itself becomes a strenuous **problem for the end user**.

## Overview

Publicly available decentralized finance (DeFi) applications (Dapps) tend to sacrifice user experience (UX) for unique visual fidelity. This forces users to learn to interact with new user interfaces (UI) and systems and creates user friction and unnecessary mental burden.

In this document we propose a browser extension for cryptocurrency owners that aggregates multiple DeFi services based on the extendible Ethereum blockchain technology (such as a wallet, exchanging, staking) into a simple, user-friendly and uniformly designed application.

## Structure

In this document we will further elaborate on the idea of the project and its general use cases, discuss the technologies we use, the way we approach design and our expectations.

# Background and Related Work

## Blockchain

A blockchain, is an ever-growing list of records, called blocks, that are linked through cryptographic means. Each block contains the cryptographic hash of the previous block, a timestamp, and transaction data. It is a database of transaction records that is distributed, verified and maintained by a decentralized network of computers around the world, which means it works like a peer-to-peer network.

Compared to a conventional centralized database, the information cannot be manipulated due to the built-in distributed structure of the blockchain and the confirmed guarantees from the partners. In other words, the timestamp proves that the transaction data existed when the block was posted to get into its hash. Blocks contain the hash of the previous block, forming a chain, with each additional block reinforcing the previous ones. Consequently, blockchains are resistant to modification of their data, because after being written, the data in any given block cannot be changed retroactively without changing all subsequent blocks. Whenever someone completes a transaction, it is sent to the network and computer algorithms determine the authenticity of the transaction. After the transaction is confirmed, this new transaction is linked to the previous transaction, forming a chain of transactions. This chain is simply called a blockchain.

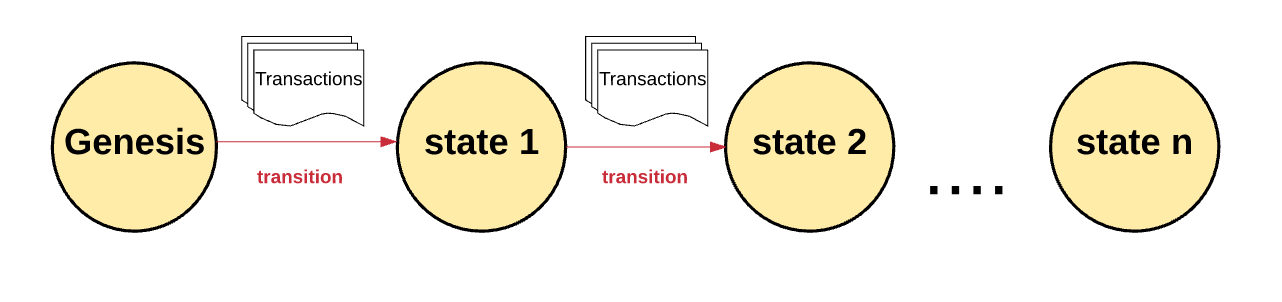


Figure : A very simplistic overview of the way blocks are chained in the system.



Figure : Blockchain transaction overview.

## Mining

In decentralized systems like Ethereum, we need to make sure everyone agrees on the order of transactions. Miners help with this by solving computationally complex block-building puzzles, protecting the network from attacks.

Mining is the process of creating a block of transactions that will be added to the Ethereum blockchain.

Ethereum miners - computers running software - use their time and computing power to process transactions and create blocks.

### **Proof of Work**

Any node on the network can declares itself as a miner can attempt to create and validate a block. Lots of miners from around the world try and create and validate blocks at the same time. Each miner provides a mathematical proof when submitting a block to the blockchain, and this proof acts as a guarantee: if the proof exists, the block must be valid.

For a block to be added to the main blockchain, the miner must prove it faster than any other competitor miner. The process of validating each block by having it miner provide a mathematical proof is known as a “proof of work”.

## Decentralization

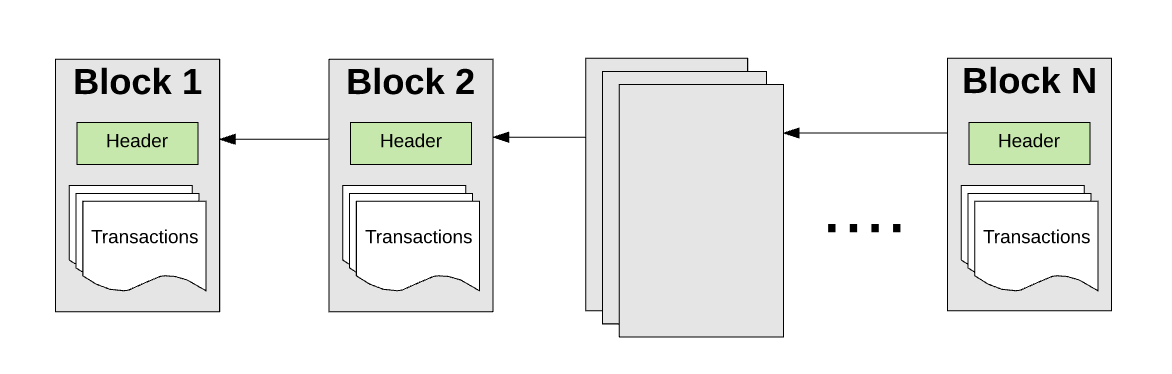
Most systems and services today are centralized. All data is stored in one object, and you must interact exclusively with this object to get the information you need. Centralized systems have served us well for many years, but they have several vulnerabilities such as being an easy target for potential hackers, updating a centralized system will stop the entire system, and shutting down at a centralized facility means no information is available. In a decentralized system, all data is distributed, so these vulnerabilities do not pose a threat. Also, in a decentralized system, no third party is required for interaction.

## Ethereum Blockchain

The Ethereum Blockchain is an open source, decentralized blockchain with smart contract functionality. Ether (ETH) is the cryptocurrency of the Ethereum network. It is the second largest cryptocurrency by market capitalization after Bitcoin.

Ethereum is the most actively developed blockchain protocol as of today. The network allows developers to build and deploy decentralized applications (Dapps).

They are also stored on the Ethereum blockchain along with transaction records.



Figure

Dapps are open-source software using smart contracts and do not need an intermediary to operate.

### **Gas**

Gas is required for the Ethereum network. It is the fuel that allows it to work just like a car needs gas to function.

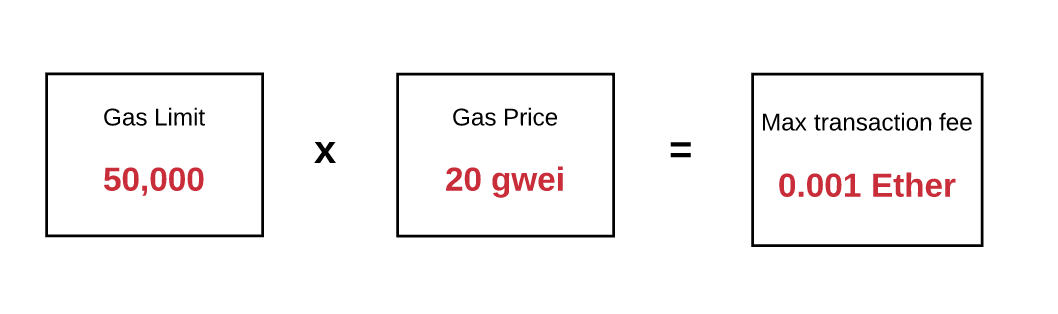
One very important concept in Ethereum is the concept of fees. Every computation that occurs as a result of a transaction on the Ethereum network incurs a fee. This fee is paid in a denomination called “gas”.

Gas is the unit used to measure the fees required for a particular computation. Gas price is the amount of Ether you are willing to spend on every unit of gas and is measured in “gwei”. “Wei” is the smallest unit of Ether, where Wei represents 1 Ether. One gwei is Wei.

### **Gas Limit**

With every transaction, a sender sets a *gas limit* and *gas price*. The product of gas price and gas limit represents the maximum amount of Wei that the sender is willing to pay for executing a transaction.

For example, a sender sets the gas limit to and gas price to gwei. This implies that the sender is willing to spend at most gwei = Ether to execute that transaction.



Figure

Where does that gas money go. All the money spent on gas by the sender is sent to the beneficiary address, which is typically the miner’s address. Since miners expending the effort to run computations and validate transactions, miners receive the gas fee as a reward.

It is also important to note, the sender is refunded for any unused gas at the end of the transactions, exchanged at the original rate.

Inversely, if the sender runs out of gas, none of the gas is refunded to the sender.

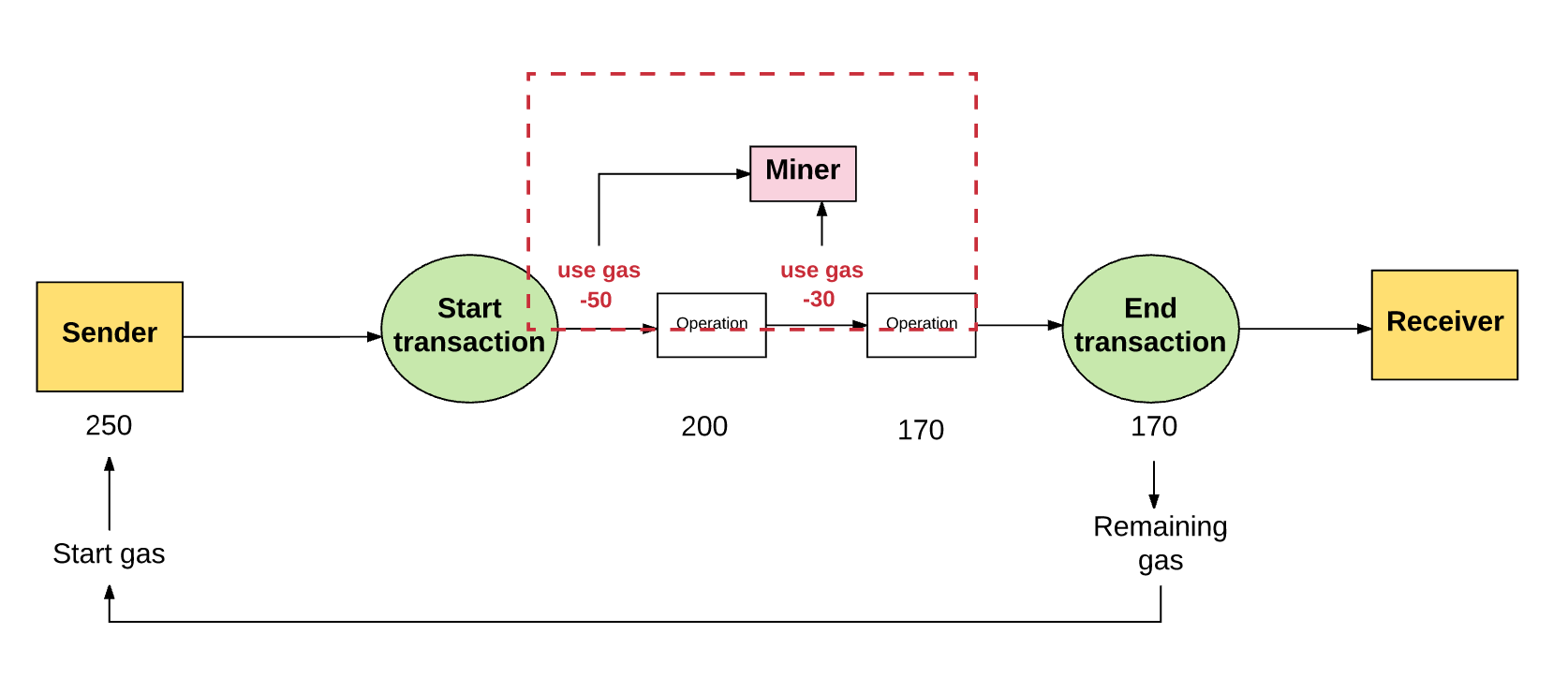


Figure : A flowchart depicting the way a transaction consumes gas.

## Smart Contracts

Smart contracts are code scripts that facilitate the exchange of money, stocks, content, or anything of value. Smart contracts are formed using the Ethereum Virtual Machine (EVM). When a smart contract runs on the blockchain it acts like a self-acting computer program, without censorship, downtime, or the influence of third parties.

A smart contract works automatically according to the terms and conditions defined in its specific protocol - when the conditions of the transaction are met (for example, a specific date or a predetermined share price), the contract is executed immediately and automatically. An “if and then” mechanism that does not require external intervention. Both parties to the contract remain anonymous, but the contract itself is in the public network log (Blockchain) and is completely transparent - anyone can check the contract and get all the existing information about it. Smart contracts are written in Solidity, so technical knowledge is required to read the actual contract, however the information is available to everyone.

## Cryptocurrency Wallets

A wallet is a user-friendly interface to the blockchain network. It manages your private keys, which are basically keys to the lock on your cryptocurrencies’ vault. Wallets allow you to receive, store and send cryptocurrencies.

### **Custodial and Non-Custodial Wallets**

There are two kinds of wallets, custodial and non-custodial wallets.

Custodial wallets are wallets where third-parties keep and maintain control over your cryptocurrencies on your behalf. Non-custodial wallets are wallets where you take full control and ownership of your cryptocurrencies.

### **Hierarchical Deterministic (HD) Wallets**

HD Wallets are the most advanced type of deterministic wallet. They contain keys in a tree structure, in which parent keys can produce children keys, which can produce grandchildren keys, and so on, infinitely. The cryptocurrency holder can use the tree structure to organize transactions by type of transaction or by entity involved, such as departments or subsidiaries.

Like simple deterministic wallets, all HD wallets are created from a single master root seed, usually represented by a mnemonic word sequence, which makes it easier for account holders to transcribe and store. But HD wallets also offer the option of creating public keys without having to access the corresponding private keys. This means they can be used on insecure servers or in a receive-only mode.

### **Derivation Paths**

If you use an HD wallet to store your crypto assets, you will encounter the phrase “derivation path.” Simply put, a derivation path defines a consistent method for generating the same set of accounts and wallets for a given private key even if you switch to another device or wallet provider.

To avoid confusion (e.g., using the same wallet address on multiple cryptocurrency networks), most popular cryptocurrency communities have established a conventional derivation path to be used exclusively by that cryptocurrency network. Some wallet providers have additional constraints, for example, on the Ethereum network, the Ledger and Ledger Live wallets use different derivation paths than the conventional Ethereum derivation path.

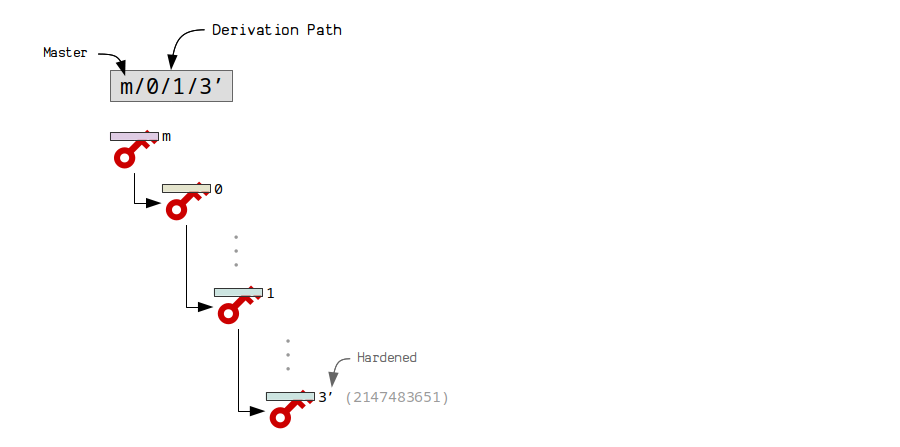


Figure : A derivation path includes a master key from which an infinite theoretical number of private keys can be derived.

### **Mnemonic Phrases**

*BIP39* or Bitcoin Improvement Proposal 39 is one of the many design ideas that was approved by an economic majority of the Bitcoin community and became a standard for many popular wallets.

BIP39 is the use of a mnemonic phrase – a group of easy to remember words – to serve as a back up to recover your wallet and coins in the event your wallet becomes compromised, lost, or destroyed. This is also known as a mnemonic seed, seed phrase, recovery phrase, wallet back up, master seed, etc.

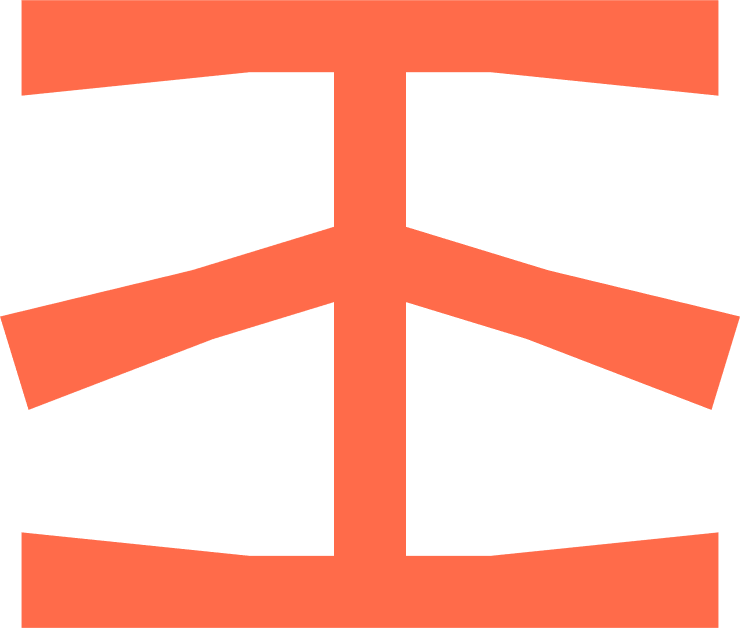
These words aren’t just any words. They are pulled from a specific list of 2048 words known as the BIP39 wordlist. Upon start up, wallets that utilize the BIP39 standard will provide the user with a 12–24-word phrase randomly chosen from the wordlist.

## Decentralized Finances (DeFi)

DeFi is currently one of the fastest growing sectors in the blockchain and cryptocurrency space. It is an ecosystem of decentralized applications (Dapps) that provide financial services built on distributed networks without any governing authority.

The DeFi sector is a collection of products and services that replace various institutions, including banking, insurance, bonds, and money markets. These financial services are delivered through decentralized applications (Dapps), allowing users to combine their services (such as borrowing, lending and trading) to unlock many possibilities.

### **Infura**

**** Across the Ethereum network, utilities are needed to lower the barrier to entry and make it easier to access Ethereum data. Among the most important of these are Infrastructure as a Service (IaaS) products. Leading the way is Infura, which offers developers, application development teams, and enterprises across industries a suite of tools to connect their applications to the Ethereum network and other decentralized platforms.

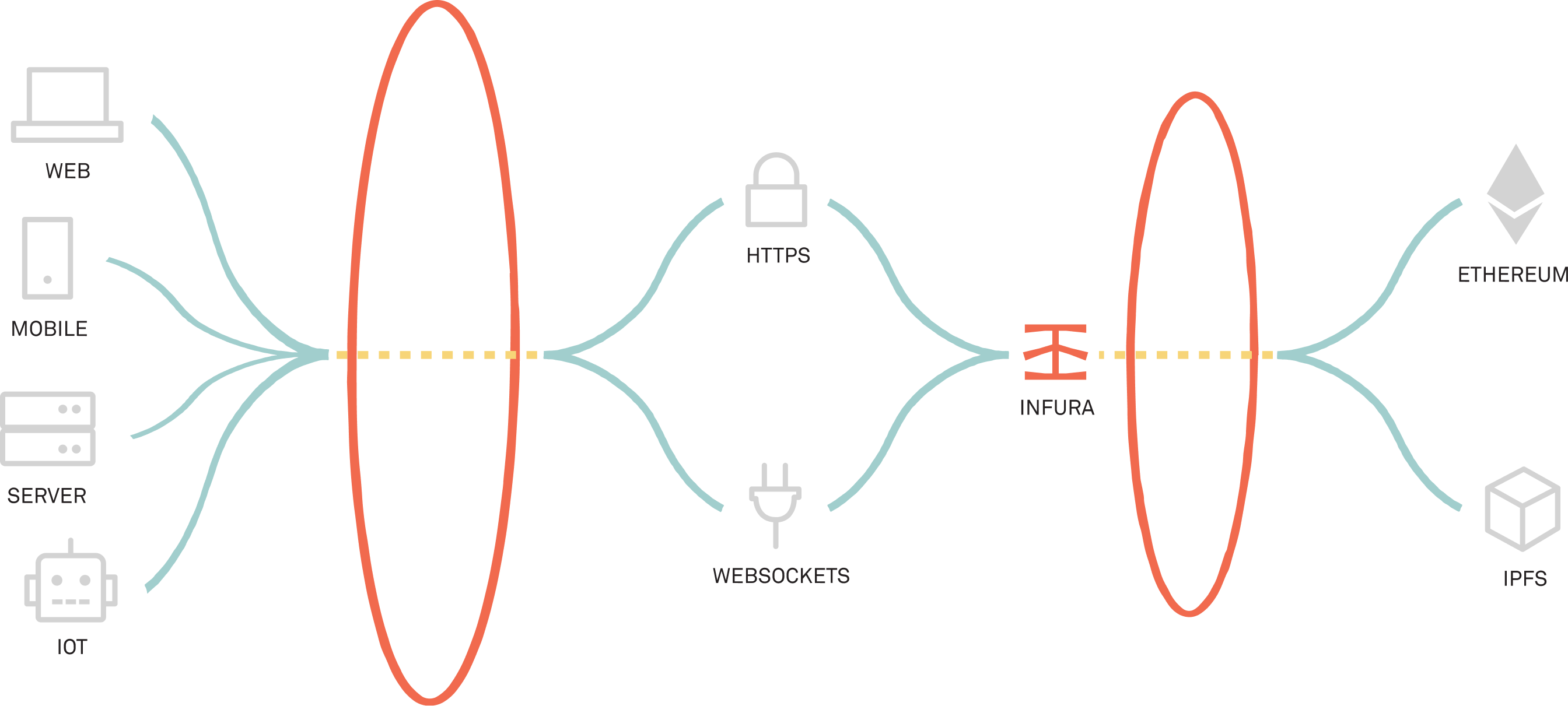


Figure : The Infura service is capable of interfacing between many technologies and the Ethereum Blockchain using HTTPS or Web Sockets.

Many of the most prominent Web3 projects - MetaMask, Aragon, Gnosis, our Alpha project and many more - use the Infura API to connect their applications to the Ethereum network. In doing so, Infura provides the fundamental infrastructure needed to handle both short-term spikes, which can often occur during token launches, and important long-term scaling solutions.  
Infura Transactions (ITX) are a simplified way to send Ethereum transactions. ITX handles all edge cases for transaction delivery and takes care of transaction mining, eliminating the need for developers to tackle the complexities of gas management.

### **Nods**

Real machines storing EVM state. Nodes interact with each other to propagate information about the EVM state and new state changes. Any user can also request code execution by submitting a code execution request from a node. The Ethereum network itself is a collection of all Ethereum nodes and their communications.

### **EVM**

The Ethereum Virtual Machine is a global virtual computer, the state of which is maintained and agreed upon by each participant in the Ethereum network. The Ethereum protocol itself exists solely to support the continuous, uninterrupted, and unchanging operation of this special state machine; It is the environment in which all Ethereum accounts and smart contracts live. For any given block on the chain, Ethereum has one and only one "canonical" state, and the EVM is what defines the rules for calculating the new allowed state from block to block.

## Decentralized Lending and Borrowing

One of the most common services offered by the financial industry is lending and borrowing.

In the DeFi world, there are no such barriers as intermediaries since banks are no longer needed. With enough collateral, anyone can have access to capital and do whatever they want, anyone can contribute to Compound's decentralized liquidity pool from which borrowers can borrow and repay at an algorithmically determined interest rate.

Rates are adjusted automatically based on supply and demand.

Entrepreneurs can borrow the capital they need to start a business by collateralizing the business, and families can get a mortgage on a house that would otherwise be too expensive for them, using the house as collateral.

On the other hand, accumulated wealth can be lent and become capital for creditors.

This system reduces the risk that borrowers will flee with borrowed funds.

### **Compound**

*Compound* is an algorithmic money market protocol on Ethereum where anyone can supply or borrow cryptocurrencies frictionlessly against collateral, lets users earn interest or borrow.



Compound acts as a pool of liquidity.

Providers provide assets to the pool and receive interest, and borrowers receive loans from this pool and pay interest on their debts.

The interest rates are calculated for each asset using algorithms that take into account the current supply and demand of that asset.

Essentially, Compound reduces lending / borrowing friction by allowing lenders / borrowers to interact directly with the protocol on interest rates without having to negotiate loan terms.

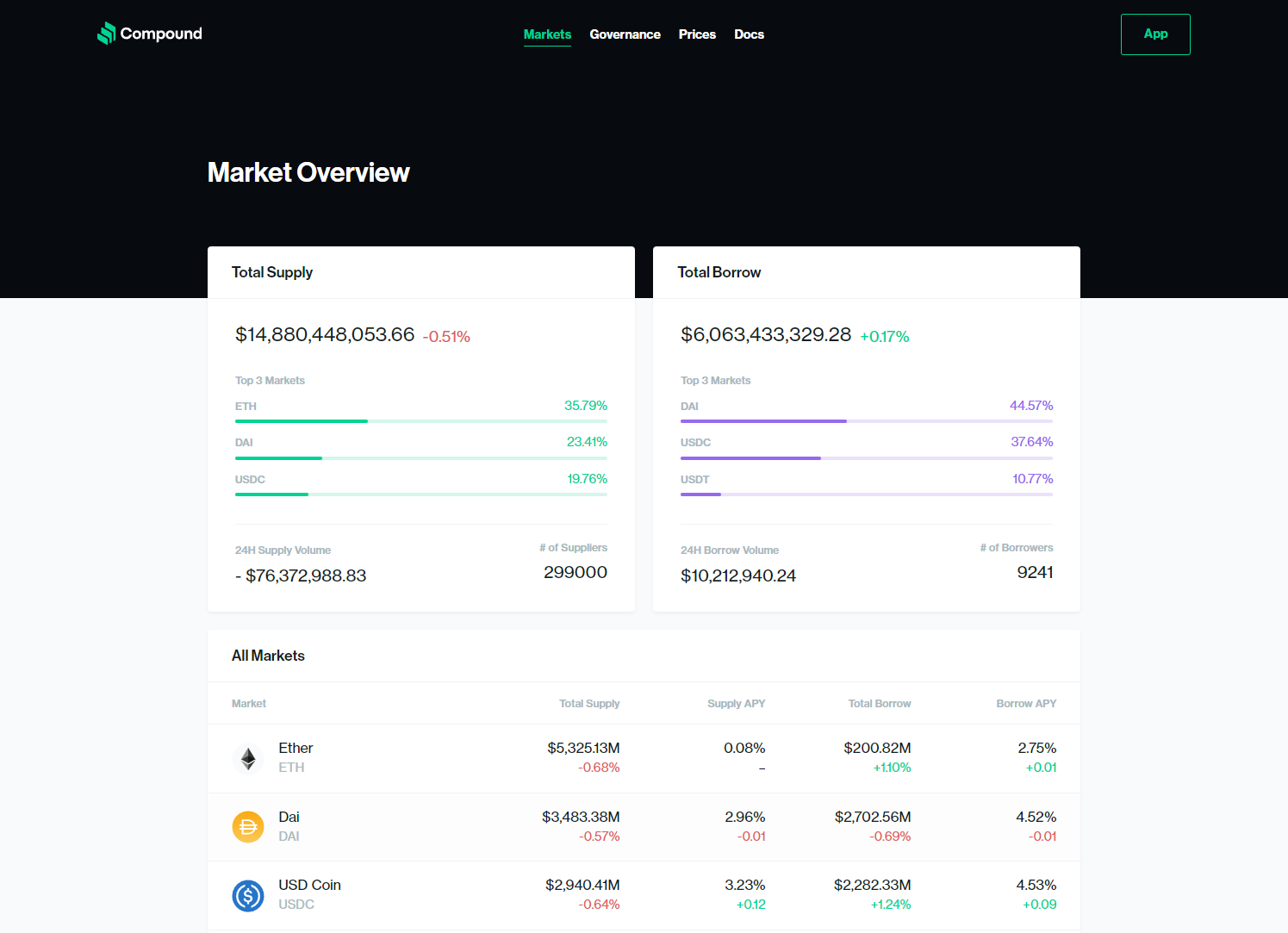


Figure : Compound web user interface.

## Decentralized Exchanges (DEX)

More and more people are aware of the risks and are turning to decentralized exchanges (DEX). Since users of centralized exchanges do not own their assets and there are cases of theft of registration data and, as a result, cryptocurrency.

DEX works using smart contracts and on-chain transactions to reduce or eliminate the need for an intermediary. Popular decentralized exchanges include Kyber Network, Uniswap, Dex.Blue, and dYdX.

Liquidity pools are essentially reserves of tokens in smart contracts, and users can instantly buy or sell tokens that are available in these pools. The token price is determined algorithmically and increases for large transactions. Liquidity pools can be used by several DEXs at once, which increases liquidity on each of these DEXs. Examples of DEXs based on liquidity pools are Kyber Network, Bancor and Uniswap.

In the case of DEX, users' assets can be stored in their own wallets.

### **Uniswap**

*Uniswap* Exchange is a decentralized token exchange protocol built on Ethereum that allows direct exchange of tokens without the need for a centralized exchange.



At Uniswap, you can simply exchange your tokens directly from your wallet.

All you have to do is send tokens from your wallet to the Uniswap smart contract address, and you will receive the desired token in return directly to your wallet. There is no order book, and the token exchange rate is determined algorithmically. All this is achieved through liquidity pools and an automatic market maker mechanism.

Liquidity pools are reserves of tokens that are in smart contracts.

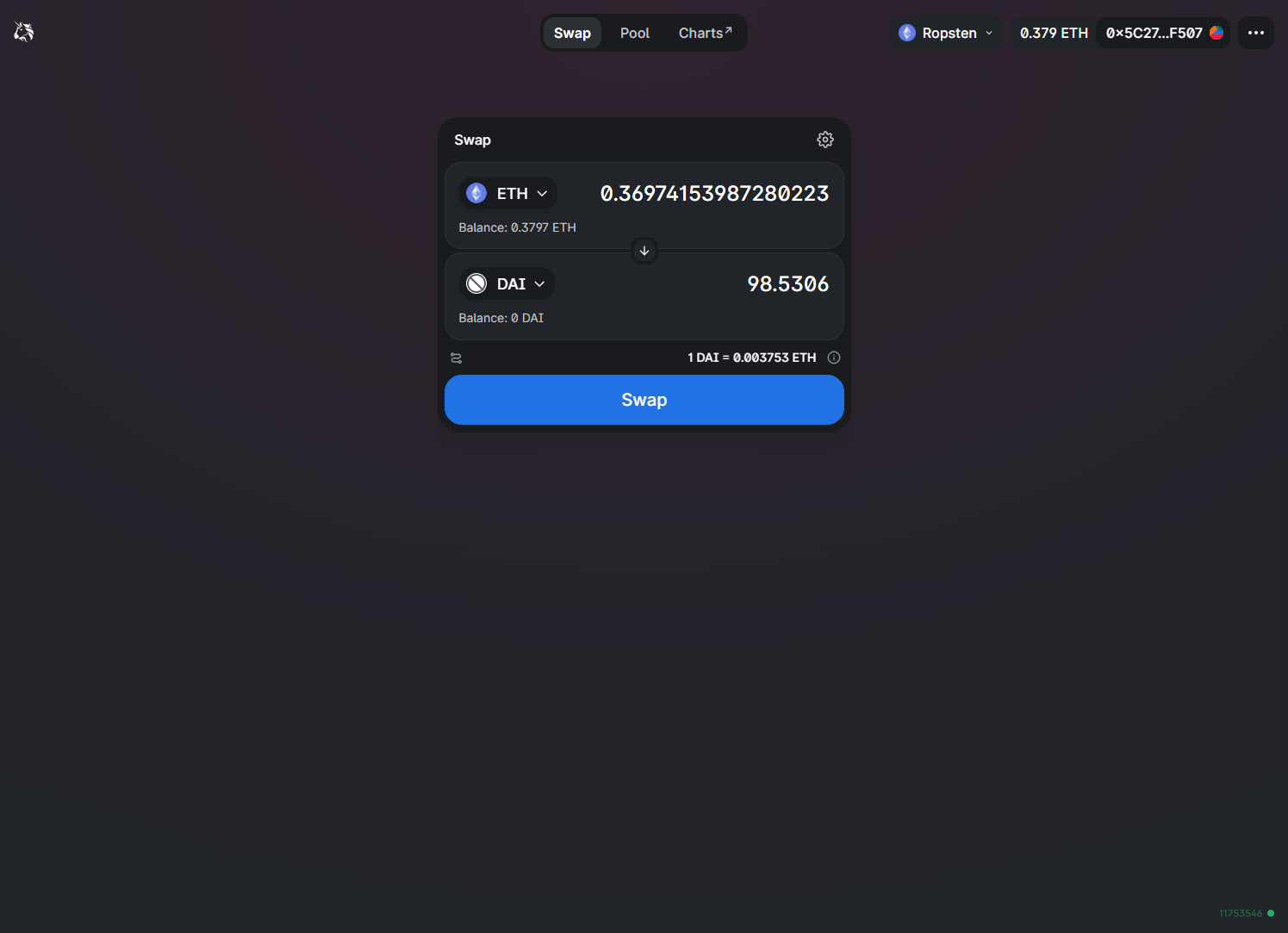


Figure : Uniswap web user interface.

### **dYdX**

*dYdX* is a decentralized exchange protocol for lending and borrowing and margin trading. It currently supports 3 assets - ETH, USDC and DAI. By combining an off-chain order book with on-chain settlement, the dYdX protocol seeks to create efficient, fair, and trustless financial markets that are not governed by any central authority.



dYdX runs on audited smart contracts on Ethereum, which eliminates the need to trust a central exchange while trading. The exchange combines the security and transparency of a decentralized exchange, with the speed and usability of a centralized exchange.

At first glance, dYdX has some similarities to Compound - users can deposit assets (lend) to receive interest and borrow assets (borrow) after posting collateral. However, dYdX goes one step further by introducing margin trading. dYdX allows you to trade ETH up to 5x leverage using DAI or USDC.

## Aggregators

A DeFi aggregator brings together trades across various decentralized finance platforms into a single location, saving users time and increasing efficiency for cryptocurrency trades. As the name suggests, DeFi is spread out across different blockchains such as Ethereum and Binance Smart Chain. Within each blockchain is an ecosystem of isolated financial protocols.

DeFi aggregators siphon the very best prices from DEXs, lending services and liquidity pools into one place so that users can optimize their trades. Without an aggregator, users need to go to each platform on an individual basis to compare prices that will generate the best deal for them. Then, the user must manually execute each transaction using smart contracts. While this strategy may be fine for casual crypto trading, it severely limits those looking to implement advanced trading strategies.

Aggregators *put UX/UI at the forefront*, offering a far superior experience to the traditional way of manually interacting with liquidity layers. As a result, this helps users who are not as crypto savvy as trading experts navigate the world of DeFi with ease.

## Web3

Web2 is the version of the Internet that most of us know today. An internet dominated by companies that provide services in exchange for your personal information. Web3 in the context of Ethereum refers to decentralized applications running on the blockchain. These are applications that allow anyone to participate without monetizing their personal data.

Status of Web3 Implementation in 2019:

Since Bitcoin launched the world's first blockchain in 2009, blockchain technology has improved in several key areas. As of mid-2019, Ethereum has performed the best of any blockchain ecosystem in existence today. Despite this success, adoption of Web3 applications still lags well behind Web2. Web3's goal of becoming the de facto global standard for the Internet remains an elusive goal for Ethereum as well as other blockchain communities.

Many Web3 developers have chosen to build decentralized applications due to Ethereum's inherent decentralization:

* Anyone who is online has permission to use the service - or, in other words, no permission is required.
* No one can block you or deny you access to the service.
* Payments are made through its own token, ether (ETH).
* Ethereum is Turing complete, which means you can program just about anything.

Web3 currently has some limitations:

* Scalability - transactions in web3 are slower because they are decentralized. State changes, like payment, must be processed by the miner and propagated across the network.
* UX - Interacting with web3 applications can require additional steps, software, and training. This can be a barrier to adoption.
* Accessibility - The lack of integration into modern web browsers makes web3 less accessible for most users.
* Cost - Most successful decentralized applications put very small chunks of their code on the blockchain because it is expensive.

## React

React (also known as React.js or ReactJS) is a free and open-source front-end JavaScript library for building user interfaces based on UI components. It is maintained by Meta (formerly Facebook) and a community of individual developers and companies. React can be used as a base in the development of single-page or mobile applications. However, React is only concerned with state management and rendering that state to the DOM, so creating React applications usually requires the use of additional libraries for routing, as well as certain client-side functionality.

### **Semantic UI**

Semantic is a development framework that helps create beautiful, responsive layouts using human-friendly HTML.

Semantic allows developers to build beautiful websites fast, with concise HTML, intuitive JavaScript, and simplified debugging, helping make front-end development a delightful experience. Semantic is responsively designed allowing your website to scale on multiple devices.

# Expected Achievements

Our product, Alpha, aims to provide a fast, stable, simple and responsive user experience for basic and advanced users alike.

## Product Infrastructure and Flow

We plan on using the Google Chrome extension API, backed by the React frontend framework, which we will develop locally using Node.js.

Launching the extensions the user will be prompted by either a login process or the content of the extension which will include: a convenient dashboard with relative user information, frontend services based on DeFi APIs, and a settings panel in which the user will be able to modify his experience using the extension.

## Success Criteria

1. Implementation of multiple initial decentralized finance services (*Uniswap, Compound*)
2. Self-explanatory user interface
3. Smooth and responsive user experience
4. Positive (>75%) user feedback

## Unique Features

1. User experience above all
2. Module-based and extensible – advanced users can implement their own services given an API
3. Non-profit, open-source extension
4. No internal fees

# Engineering Process

This section elaborates the challenges we had faced and are expecting to encounter, as well techniques we had employed during the engineering process of the product.

## Process

The research and development process began by inquiring about the Blockchain field in general, the Ethereum Blockchain, cryptocurrency diversity, DeFi services, and more. This is a new and evolving type of technology which contains many new concepts that required us to study many related ideas and approaches, out of which many are new to us.

Alongside formulating the idea and the use-cases of our project we had also started developing a prototype which helped us to come up with new ideas and discard less successful ones.

During the said process, we also had to learn about web development, mainly Node.js, Web3.js and React, in order to build the prototype. We also got to learn about basic financial concepts as well, which helped to shape our project.

### **Methodology**

As for our process methodology we chose to implement fundamental parts of our project as a simple prototype extension, in order to quickly iterate over ideas and to obtain hands-on experience with the technologies we had learned about.

### **Research**

To maintain chronology for all the studies that have been carried out, you can see in the graphs below, in addition, the technical aspects and technologies are listed as following:

* The Blockchain network and the Ethereum realm
* MetaMask wallet
* Hierarchical Deterministic (HD) wallets
* Web3.js
* Node.js
* Cryptography and Cryptographic Signatures
* React
* Semantic UI
* Infura
* Compound
* Uniswap

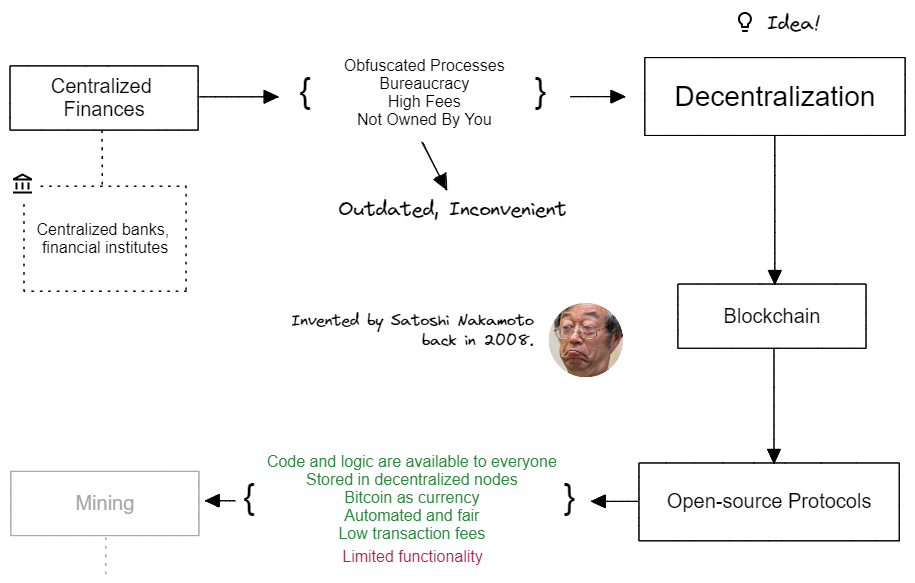


Figure : From centralized finances to creating new blocks of information on the Blockchain.

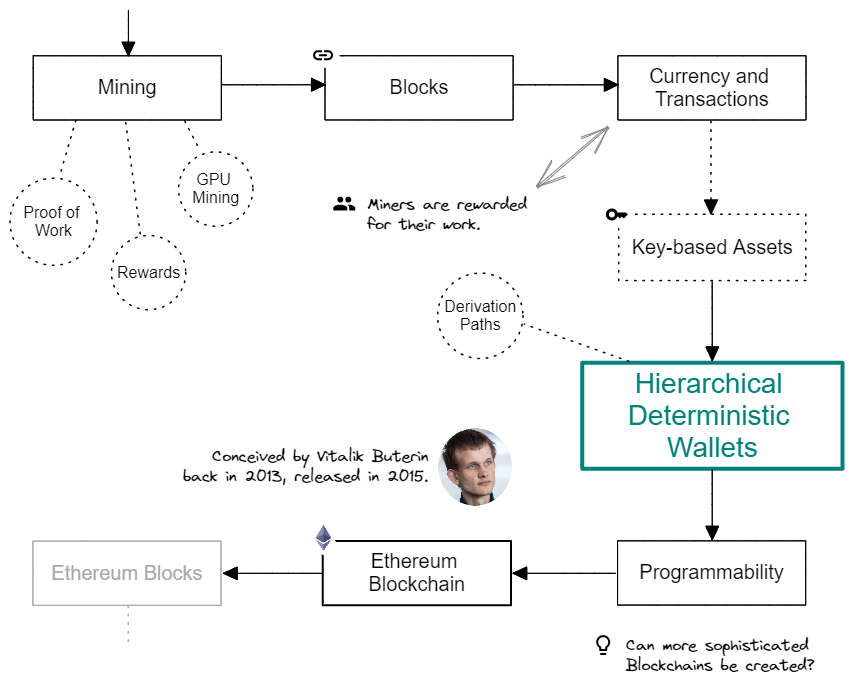


Figure :From transactions using cryptographic keys to developing DeFi services on the Ethereum Blockchain.

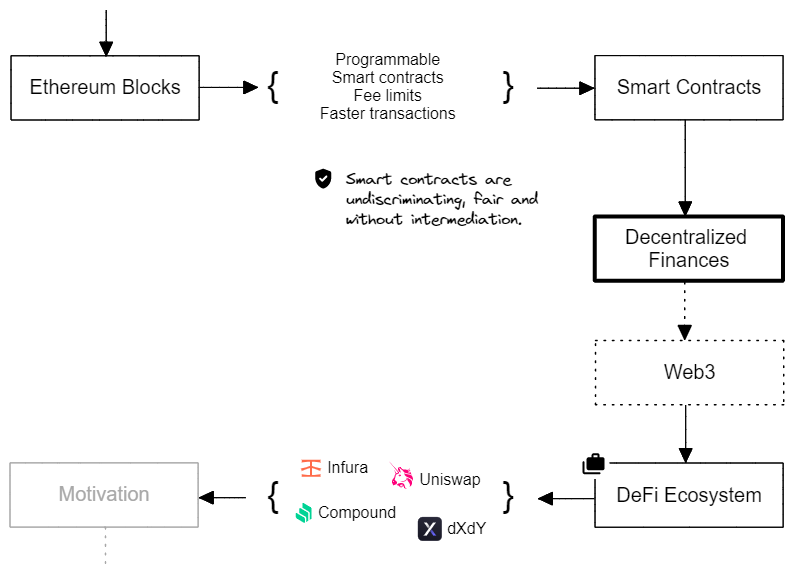


Figure : From the benefits of programmable blocks to the motivation behind our project.

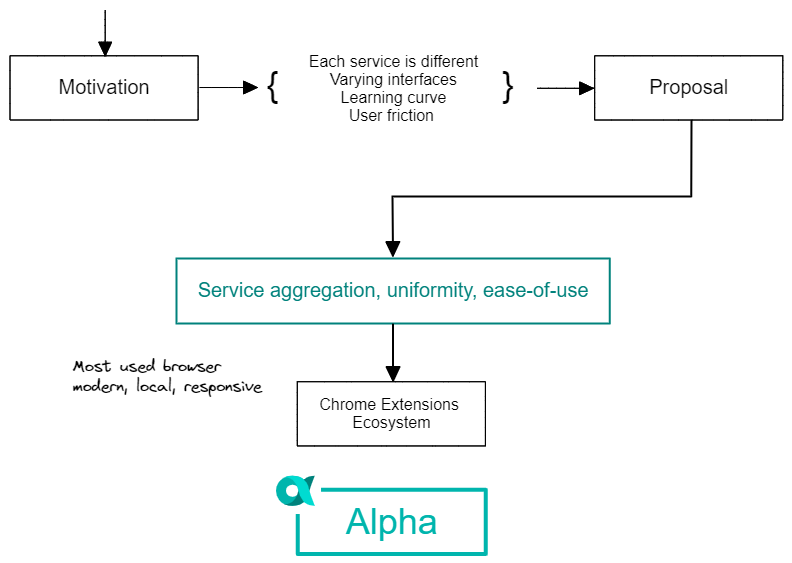


Figure : The motivation and framework of our project.

### **Challenges**

As we started researching the Blockchain realm, we quickly realized we entered a very alien and vast world unbeknown to us that which have to delve deep to understand the underlying concepts, which usually implement traditional concepts in the virtual Blockchain technology.

Alongside the Blockchain technology we also had to learn about fundamental web technologies, the difference between the Web2 and Web3 approaches to the modern internet, the Blockchain-based decentralized financial services (namely Infura, Compound and Uniswap).

We also expect to encounter various hurdles during Phase 2 of the project, where we might run into different implementation problems such as using React, different outdated API documentations, and testing our product using the Ethereum testing networks.

## Product

Originally, our product is a browser extension. However, by the nature of Chrome-based extensions, it can function as a local or hosted standalone website where users can create or import a cryptocurrency wallet.

Once a user creates or import a cryptocurrency wallet into  Alpha, the user can take actions as if they own a small private bank of their own.

Among the aforementioned actions we can expect operations such as: checking account balance, perform transactions between different wallets, borrow and lend money and coin and token conversions.

All the actions available to the users will use external APIs of various services such as Infura, Compound and Uniswap, albeit can be extended by advanced users as mentioned before.

Providing these APIs to the user means that our extension implements these API endpoints in our extension as frontend graphical user interfaces using HTML, CSS, JavaScript and high-level frameworks such as React and Semantic UI.

It is also important to note that using Blockchain technologies and external APIs we do not need a backend server and the extension client can run completely independently from traditional web services that rely on the typical HTTP request-response paradigm.

### **Requirements**

**Functional:**

* The system is based on the Ethereum blockchain.
* The system supports cryptocurrencies.
* The system supports the Infura API.
* The system supports the Compound API.
* The system supports the Uniswap API.
* The system can create new wallet.
* The system can import exist wallet (by a 12-words seed phrase or a private key).
* The system can transfer money to different addresses.
* The system supports borrowing and lending money.
* The system supports ERC-20 token conversion.
* The system supports adjusting various extension settings.

**Non-functional:**

* A secure system for using cryptocurrencies.
* User friendly interface.
* The system is always readily available.
* The system can be used anywhere with Internet access using Google Chrome.
* All services are condensed and utilized in a single extension.

### **Architecture**

A picture containing diagram

Description automatically generated

Figure : An overview of the previously mentioned architecture as a flowchart.

### **API**

A prominent feature of our extension would be extensibility. Advanced users and programmers should be able to easily modify and add new service modules to the extension using methods and classes we would provide, which we will also be using to implement the basic services (Infura, Compound, Uniswap).

Adding a module might be as simple as modifying a JSON list of objects, specifying metadata and available operations:

|  |
| --- |
|  |

Followed by implementing a class which inherits from a base Module class and a React component with its inner logic, hooking the module to the extension in an elegant manner:

|  |
| --- |
|  |

|  |
| --- |
|  |

Resulting in the interface updating accordingly:

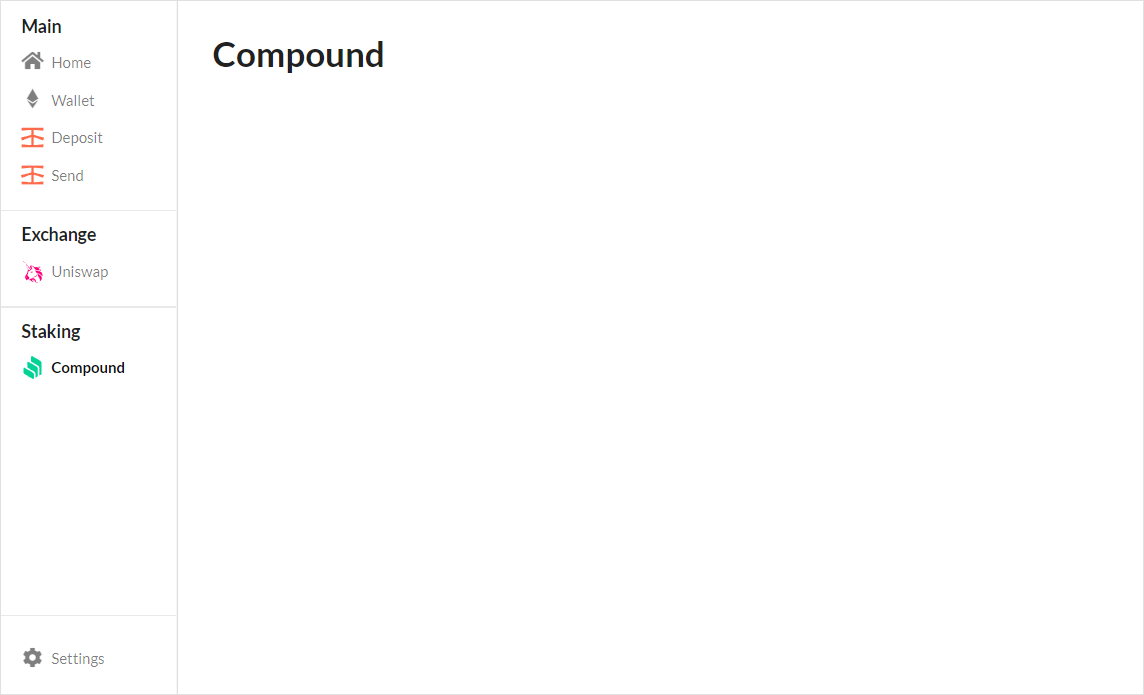


Figure : A first look at the Alpha prototype, showcasing the dynamic menu.

### **Flowcharts and Interface**

This section elaborates on user scenarios one might encounter using.

1. Post-Installation

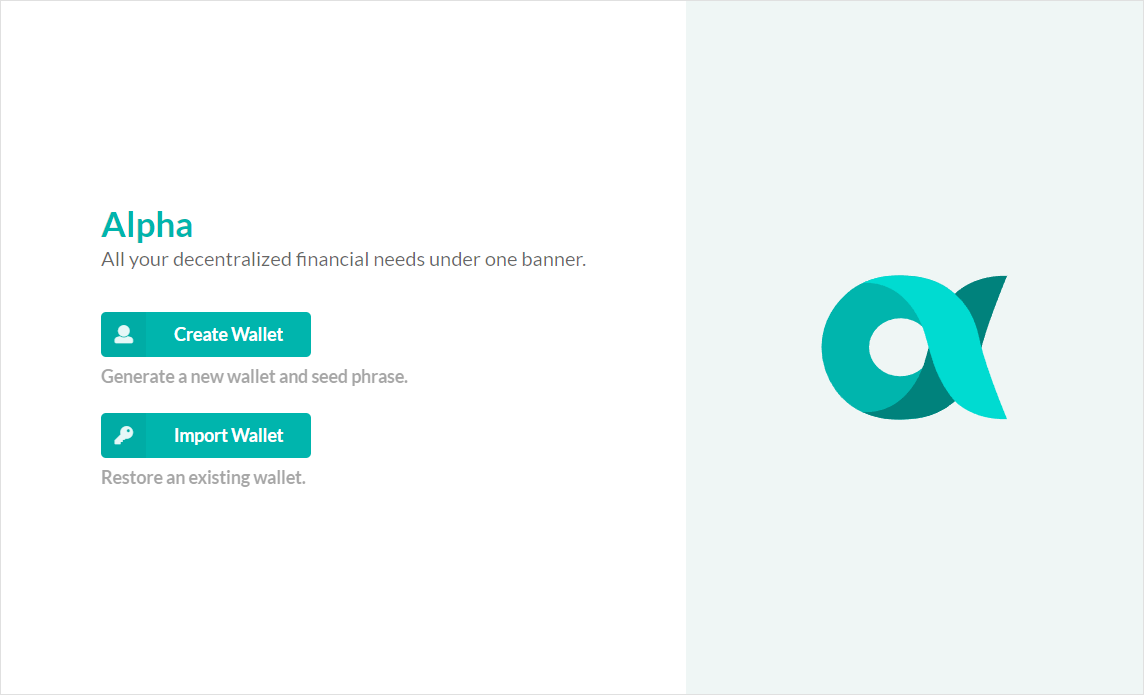
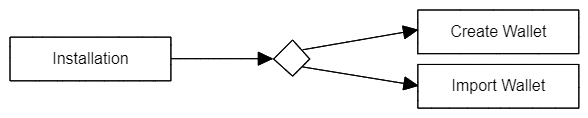


Figure 16: The main menu presented to a new user.



1. **Wallet Creation**

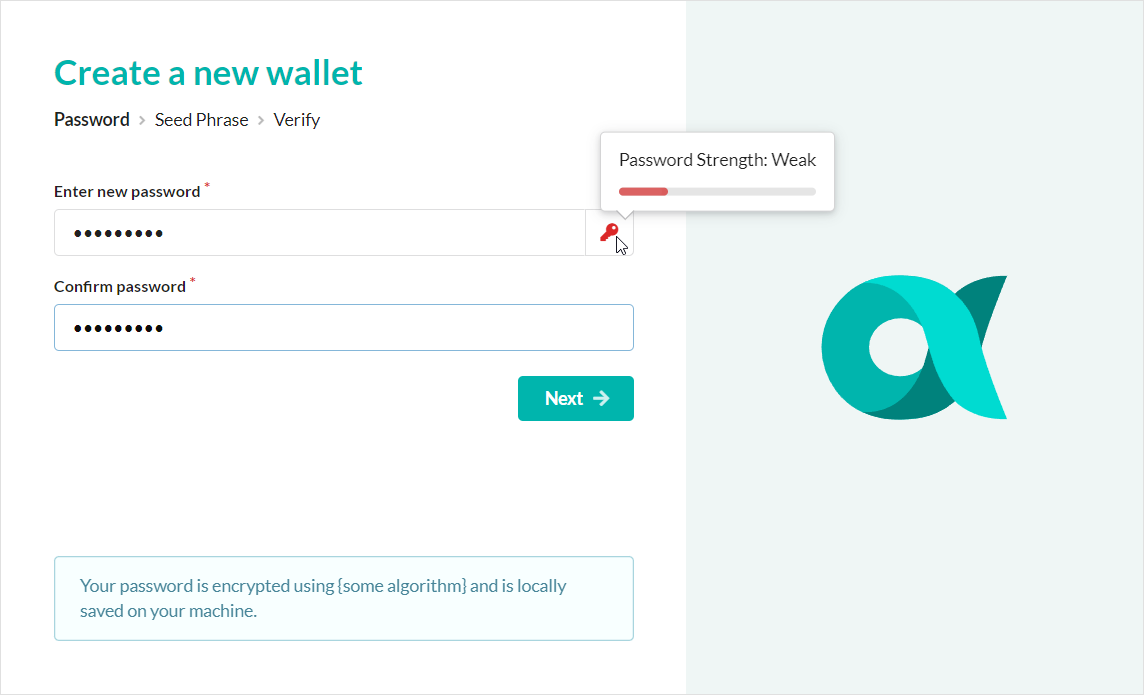


Figure 17: The user is prompted to choose a password of his liking.

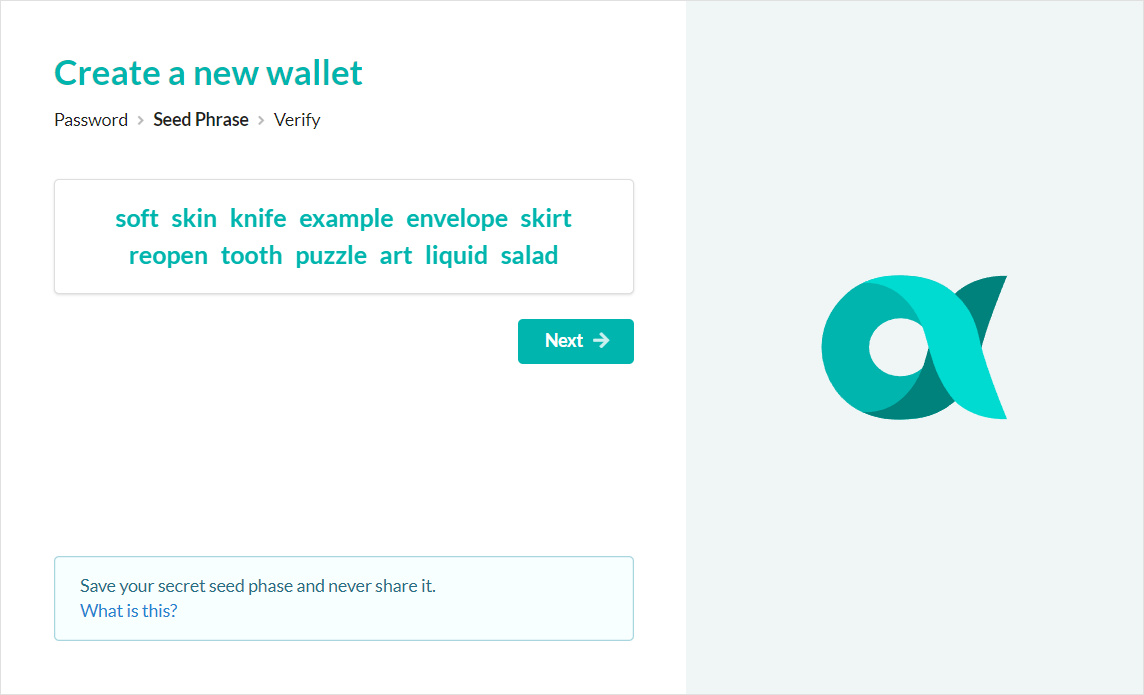
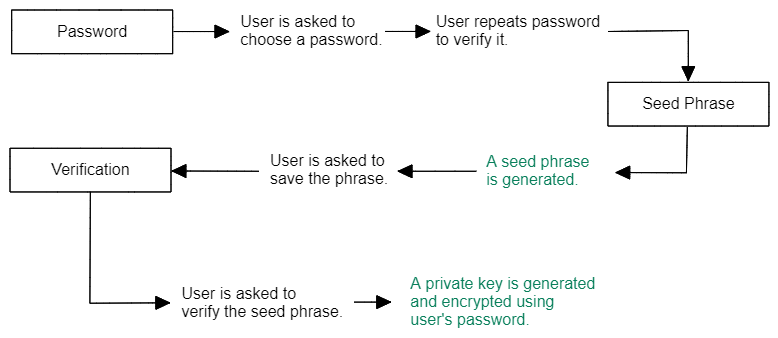
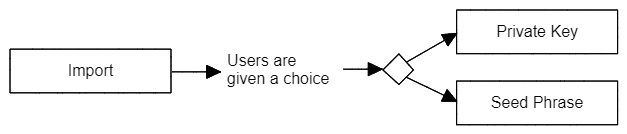


Figure 18: The user is presented with an automatically generated seed phrase.



1. **Wallet Import**



1. **Home (Dashboard) Interaction**

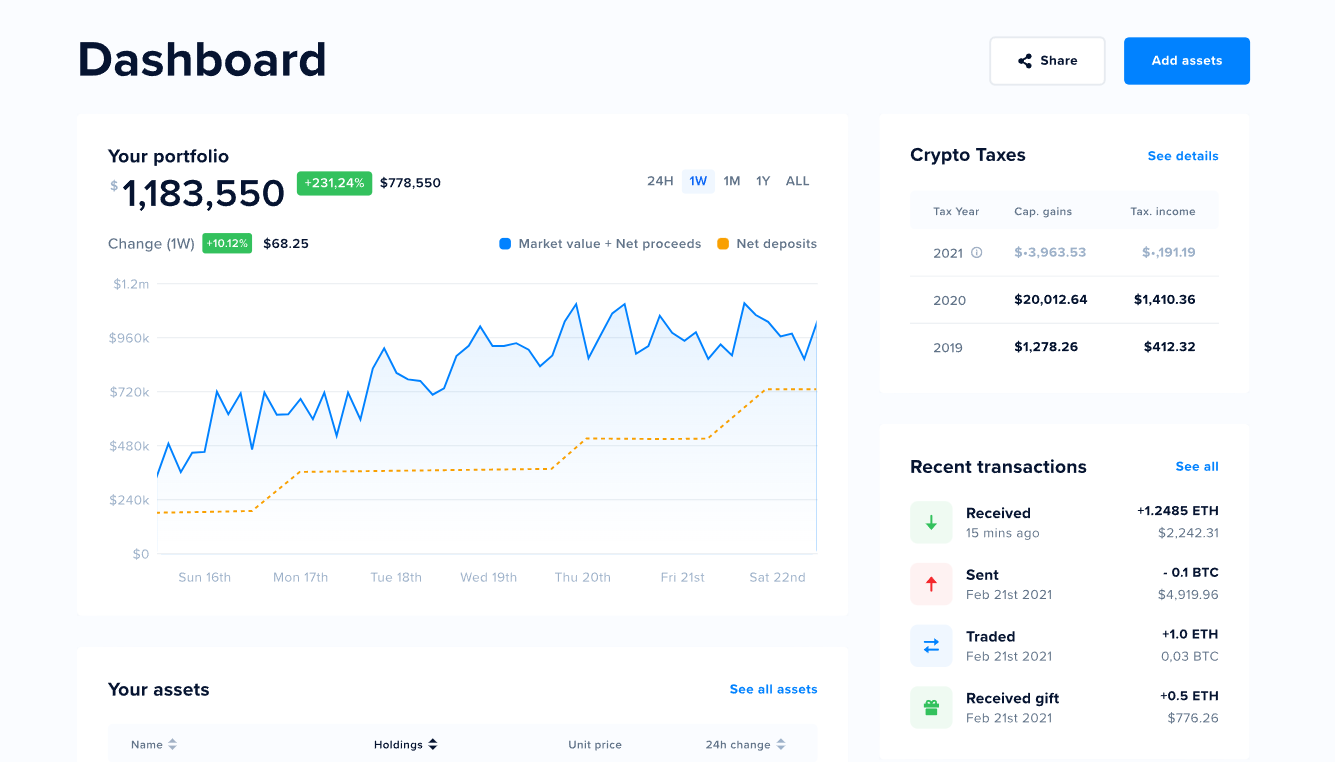


Figure 19: A potential user dashboard mockup.



1. **Infura**

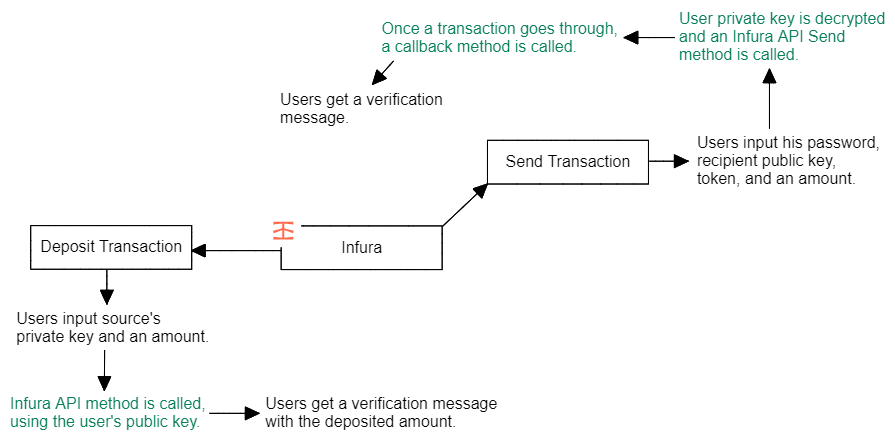


Figure 20: Different interactions based on the Infura API.

1. **Compound**

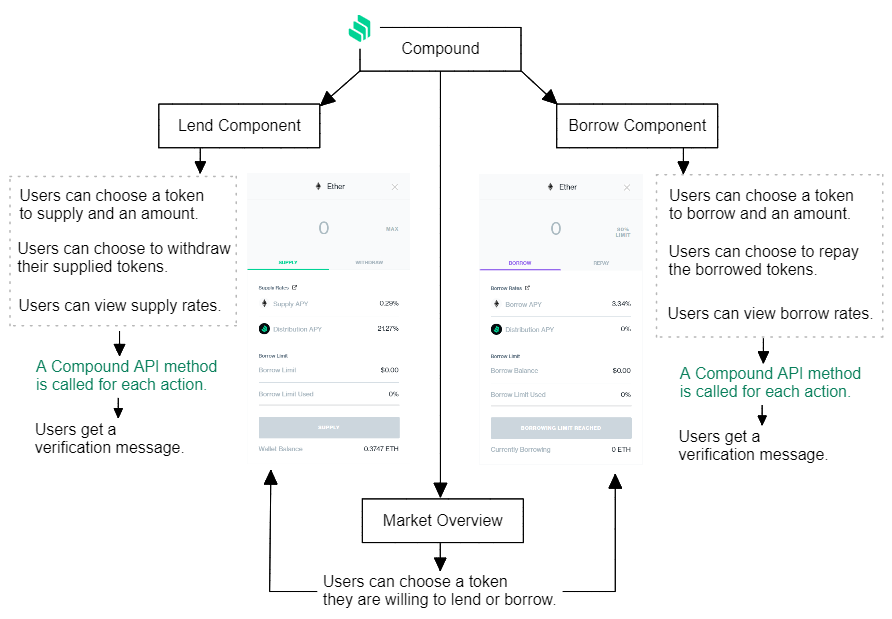


Figure 21: Shows all available actions Compound provides.

1. **Uniswap**

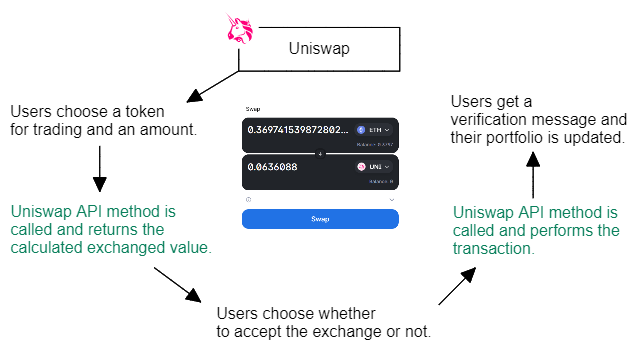


Figure 22: A simplistic sequence of actions within the Uniswap component.

1. **Settings**

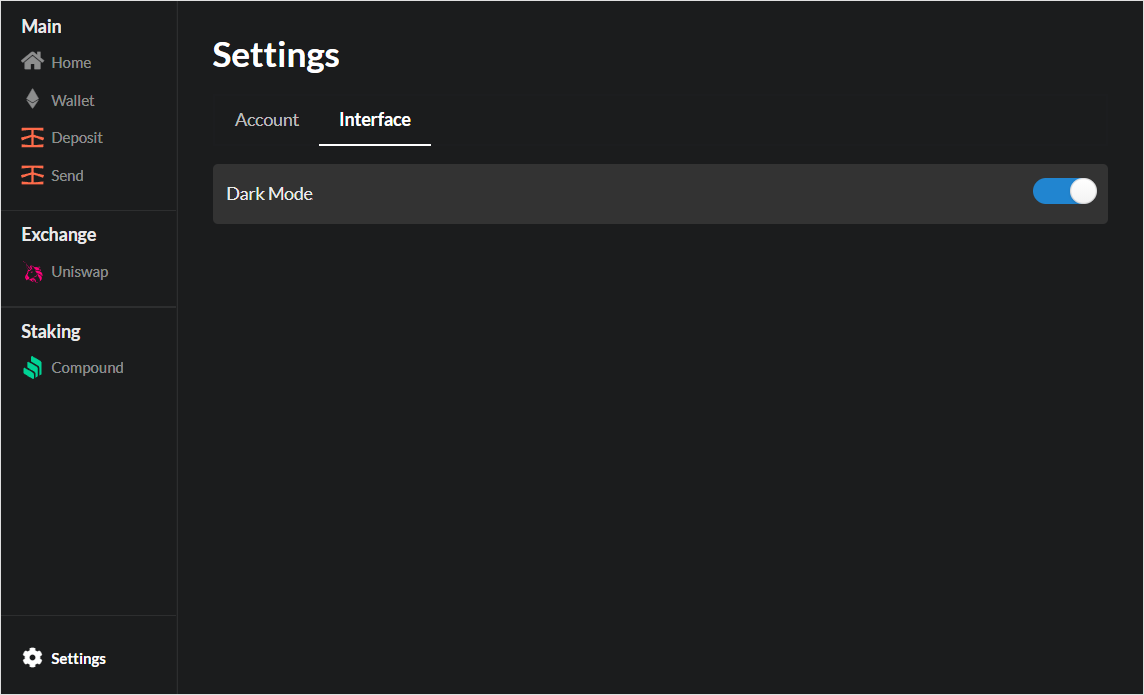


Figure 23: The settings component showing a dark theme mode capability.

### **Deployment**

Acquiring the extension can be done via either cloning the git repository or using the Chrome Web Store.

For deployment developers should:

1. Build the repository using Node Package Manager by running
2. Enable Developer Mode in the Chrome Extensions settings panel
3. Load the unpacked directory directly

# Evaluation and Verification Plan

## Testing

Testing will be conducted on two separate levels:

1. Extension level
2. Blockchain level

For frontend (extension level) testing, we plan on writing unit tests, using multiple JavaScript-based testing frameworks, such as JestJS or Cypress.

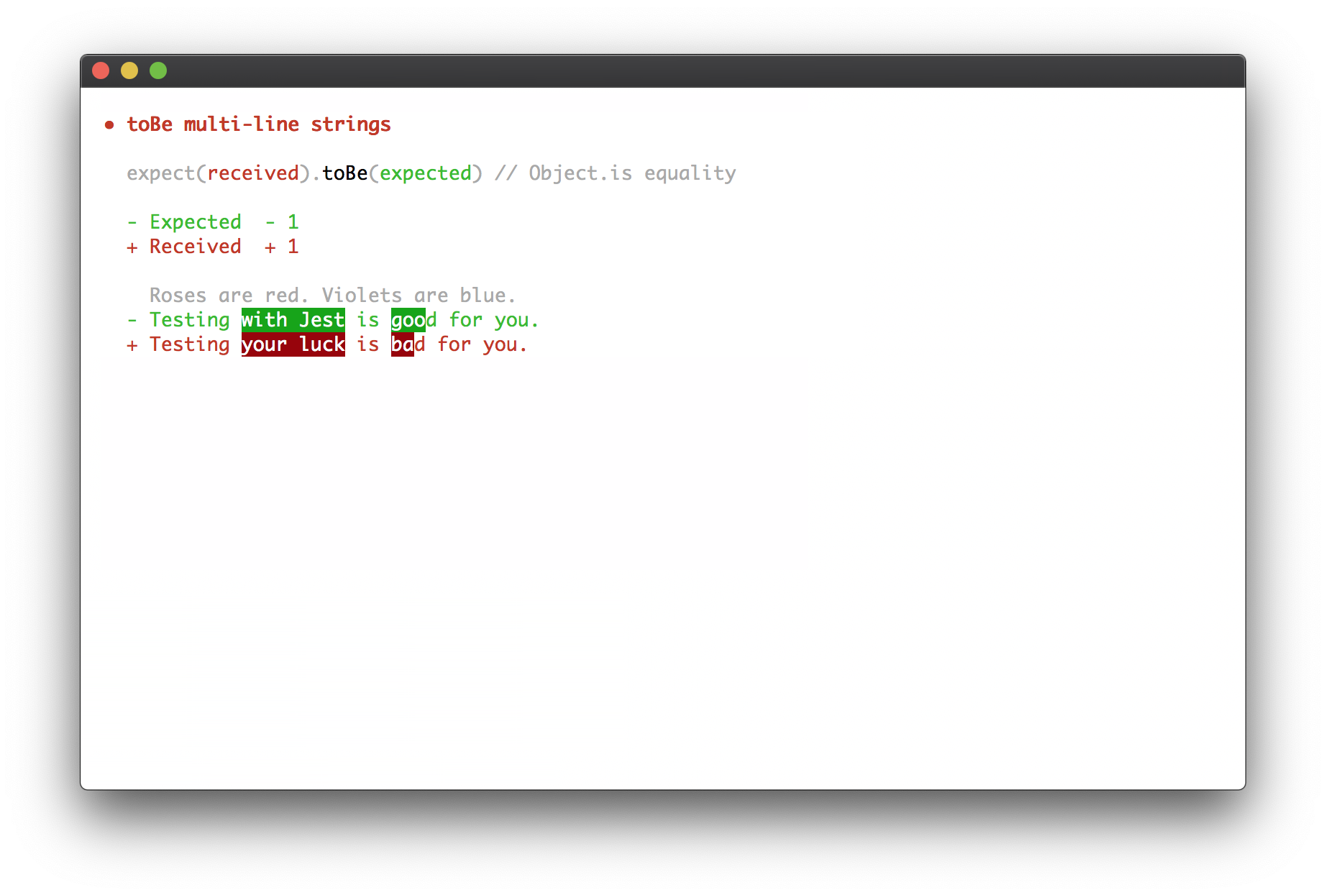


Figure 24:Example of the JestJS CLI tool.

We would also like to test our extension on real human testing group and ask for feedback about the intuitiveness of our system.

For backend (Blockchain level) testing, all of our API logic will run locally using the Ganache Testing Suite as well as a real decentralized testing network such as Ropsten TESTNET.

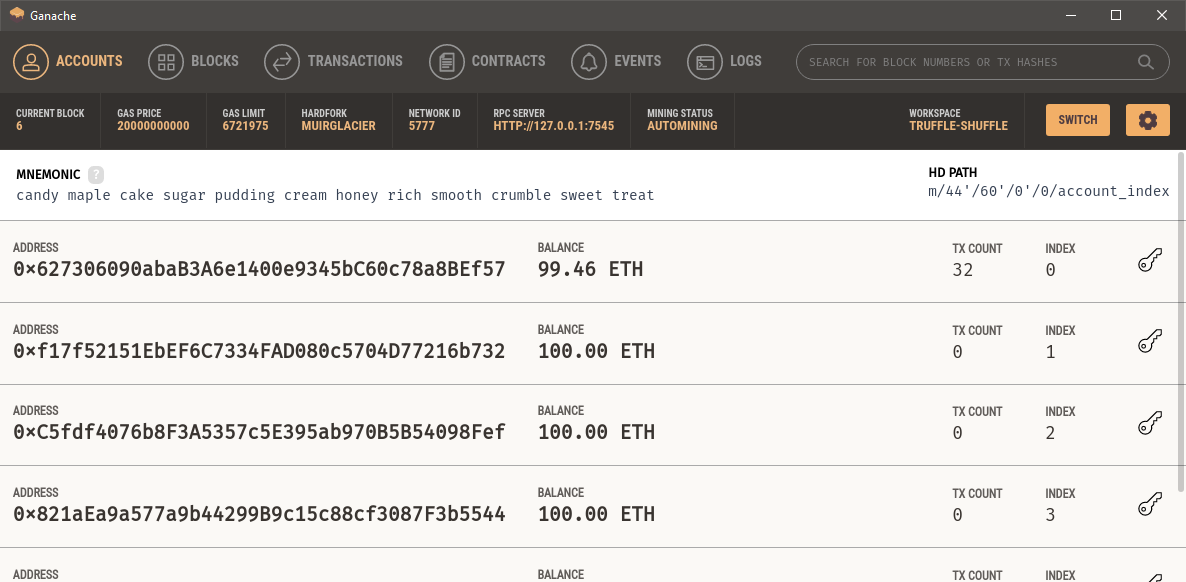


Figure : Example of Ganache GUI.

## Evaluation

Users may be tasked with filling periodic surveys about various parts of the extension and provide any additional textual feedback regarding their user experience or any missing or faulty features within the Alpha extension.

# References

|  |  |
| --- | --- |
| [1] | The Bitcoin Standard, The Decentralized Alternative to Central Banking, 2018,  S. Ammous. |
| [2] | How to DeFi, 2020, D. Lau, D. Lau, T. S. Jin, K. Kho, E. Azmi, T. Lee and B. Ong. |
| [3]  [4]  [5]  [6]  [7]  [8]  [9]  [10]  [11]  [12]  [13]  [14]  [15] | "Alexandria," CoinMarketCap OpCo, LLC, [Online]. Available: https://coinmarketcap.com/alexandria/glossary.  https://freemanlaw.com/  https://blockgeeks.com/  https://ethereum.org/  https://www.cmcmarkets.com/en/learn-cryptocurrencies  https://www.investopedia.com/terms/s/smart-contracts.asp  https://compound.finance/  https://uniswap.org/  https://dydx.exchange/  https://medium.com/the-green-light/https-medium-com-the-green-light-moving-from-web2-to-web3-cf3cd4ac1a62  https://river.com/learn/terms/  https://infura.io/dashboard  https://ethereum.org/en/developers/docs/intro-to-ethereum/ |