Philip Glazman

Senior Project

# Atlas – C++ Bitcoin Wallet Implementation

## Introduction

The aim of this project is to create a user-friendly bitcoin wallet implementation that encourages self-ownership of bitcoins and the use of bitcoin’s Script language. This is done by providing the end user the following:

* A bitcoin wallet software that manages the keys and addresses.
* A friendly-to-use graphical interface.
* A dashboard to track analytics about payments and fees.
* A dashboard to configure custom scripts.

## Background

Bitcoin is a digital money developed in 2009 where each node participating in the network can independently validate transactions and propagate them throughout the network using software similar to bittorrent. The protocol relies on public-key cryptography to create public addresses for the end-user. In terms of bitcoin, a wallet software manages the private keys that are associated with each public address. These keys gives users ownership in spending transactions and bitcoin. In bitcoin, the wallet is an abstraction that allows the end-user to send and receive payments.

This project aims to create a new wallet following security standards that can give the end-user an ability to create new transactions using a custom script dashboard as well as track payments using an analytics dashboard.

More on bitcoin: <https://bitcoin.org/en/>

## Specification

The design of the wallet will follow object-oriented principles. It will mostly be written in C++ with the exception of embedded python code used in the analytics dashboard described above. The Qt framework will be used to write a cross-platform GUI. Libbitcoin Library and Boost Library be dependencies. I am including Libbitcoin for its useful math and cryptographic methods. Boost is being included for its useful methods and as a dependency for Libbitcoin.

*Boost:* *http://www.boost.org/*

*Libbitcoin: https://github.com/libbitcoin/libbitcoin/wiki*

*Qt:**https://www.qt.io/*

### Base Wallet

|  |  |
| --- | --- |
| Components | Description |
| Mnemonic Code Words | Following a wallet standard, |
| HD Wallet |  |
| Bloom Filter |  |
| Peer Networking |  |
|  |  |

#### Analytics Dashboard

|  |  |
| --- | --- |
| Components | Description |
|  |  |

#### Script Dashboard

|  |  |
| --- | --- |
| Components | Description |
|  |  |
|  |  |