Project Initiation Document

Benjamin Moore

December 11, 2018

1 Introduction

Throughout the past few years blockchain has moved from relative obscurity to a dominant technology that is being adopted for various uses throughout many industries but it's first application, Bitcoin is still currently the most used application of the technology. My project aims to create a Bitcoin wallet application for the Android smartphone creating a mobile interface for the Bitcoin blockchain that users can carry around in their pockets although there are other applications that also provide Bitcoin wallet, most notably Coinbase's mobile application the market for android wallet applications is still relatively small and some are even choosing to forgo decentralisation to create a simpler seeming application. My project will aim to create an interface for the android operating system which is not tied to any single company and can still give users the ease of use of other wallet applications while still providing transparency and not forgoing the core tenant of decentralisation that Bitcoin was initially designed to uphold.

2 Background and Motivation

As someone with an avid interest in crypto currency I have found there are not many android Bitcoin applications available and although there are some good options and the current most popular application is tied too Coinbase, the current largest cryptocurrency exchange. My wallet application will attempt to create something which can provide an interface to both technical and non-technical users while also remaining not tied to any company or exchange allowing the system to remain decentralised. While my wallet will not be tied to any company or person in the blockchain space my application will aim to provide a simple interface for the Bitcoin blockchain while

allowing users to keep their funds on their own device as opposed to keeping them on an external server owned by a third party company.

3 Project Objectives

1. To analyse potential android development methodologies
2. To build an understand of how an application interfaces with a blockchain
3. To implement a system that communicates with the Bitcoin blockchain effectively
4. To implement a system that allows users of non-technical backgrounds to also utilise the Bitcoin blockchain

4 Initial Scope

4.1 Core Deliverables

The proposed application will aim to have the following features

1. Setting up a new wallet for a user
2. Allowing for sending and receiving of Bitcoin transactions
3. Providing the ability to recover a wallet using a private key

4.2 Desired features

1. Allowing the user to view the current price of Bitcoin in GBP or USD before sending their transaction
2. Allowing an interface with other blockchain assets such as Ethereum
3. Providing an extra layer of security for users such as using biometrics built into the mobile device

5 Resources and Dependencies

There are no external resources required for the completion of this project

6 Method of Approach

When approaching this project I will be utilising an agile development methodology while using a kanban board for listing issues and features that require completion, starting with the features in this order.

1. A user can create a wallet with a bitcoin address
2. A user can send Bitcoin transactions
3. A user can receive Bitcoin transactions
4. A user can recover their funds in the event of losing their device

Further increments may be added to develop desirable functionality dependant on time. After researching various development technologies for this project I have decided that I will be using the Kotlin programming language which Google is supporting as the new primary language for the development of android applications. As the focus of this project is an Android application it would be desirable to utilise the most modern technologies for building apps for the platform. Kotlin also provides interpolation with java libraries allowing for the use of older Android libraries if needed. Kotlin also allows for the use of features like anonymous and higher-order functions allowing for programming in a functional style. This will be useful when dealing with a financial application as it will allow me to utilise asynchronous functions while not having to worry about bugs which are related to race-conditions, through trying to achieve function purity in as many core functions as possible, I will attempt to achieve better security through good programming practices.

The technologies utilised in this project will be as follows

1. The Kotlin Programming language with the Android SDK Developing the Android application
2. The Android Operating System
3. Android Studio as a development tool for the application
4. Bitcoind to profide a JSON-RPC interface for the Bitcoin Blockchain
5. Git and Github for development source control and hosting

7 Project Plan

Stage	Expected Start Date	Expected Completion Date	Products/deliverables/outcomes
1. Initiation		14/12/18	PID Final Draft
2. Initial High level design and requirements analysis	28/01/19	03/02/19	Design architecture and HCI
3. Phase One	04/02/19	10/02/19	Develop wallet creation functionality
3. Phase One	11/02/19	17/02/19	Develop address viewing functionality
4. Phase Two	18/02/19	24/02/19	Develop ability to receive Bitcoin
5. Phase Three	25/02/19	03/03/19	Develop ability to view wallet balance
6. Phase Four	04/03/19	10/03/19	Develop ability to send Bitcoin
7. Phase Five	11/03/19	17/03/19	Develop recovery functionality using private key
Easter Holiday (Using this time to develop desirable features)	08/04/19	28/04/19	
8. User Testing	29/04/19	05/05/19	User testing and codebase refactoring
9. Writing Report	06/05/19	12/05/19	Draft Report
10. Assemble code and complete report final draft	13/05/19	19/05/19	Final report and code submission

8 Control Plan

Throughout the completion of the project the following control techniques will be utilised

1. Highlight reports to be submitted as described by the PRCO304 project brief

2. Weekly meetings reviewing my progress with my project supervisor (Dr. Ismini Vasileiou) as described by the PRCO304 project brief allowing for periodical reviewing of my progress

3. Utilisation of my risk management plan, project plan and, other contingency plans.

9 Initial Risk List

Risk	Management Strategy
Technology failure, loss of data	In the event that I have a technology failure I will be using Git as my version control system while also using Github as a repository hosting solution
Schedule Overrun	Schedule Overrun has been considered as part of this project, I have left time free during my Easter break (08/04/19 to 28/04/19) to be used to catch up with any overrun if it is needed
Difficultly learning how to use the development technologies	As I have not developed a blockchain application or developed with Kotlin before, but as I feel I am a competent developer I should be able to utilise the extensive documentation online to overcome this issue. I have also planned for overrun in my project plan which will allow me to catch up if needed
Illness, family emergency	In the event of illness or family emergency, I will contact my project supervisor. If necessary I will apply for extenuating circumstances.

10 Initial Quality Plan

Quality Check	Strategy
Requirements	Requirements will be checked reviewed to check they are correct and adhere to the project objectives as well as being correct, complete and, achievable as these requirements will indicate the criteria of the resulting product. Prototypes will be built and assessed by other stakeholders (friends, users and colleagues)
Design Validation	Throughout the project I will constantly evaluate the project on the delivery of every significant subsystem. If there are any failures in these systems, they will be handled as part of their development stage, or over the Easter break.
End of Stage Verification	To be conducted at the end of each stage.
System and User Acceptance	To be concluded at the end of my user testing stage (Stage 8)

11 Legal, Social, Ethical and Professional Issues

The main ethical issue with my project is the storage of users private keys which means their funds. To mitigate the issues with this I will be utilising the encryption libraries available on Android alongside making sure that the private key never leaves the device. Alongside these issues there may be potentially other issues with losing funds, for example if the user cannot send funds, said funds may become stuck on the device. The main social issues here are that users addresses may be released without them wanting to, therefore allowing people to see the transactions they have made on the blockchain. In order to mitigate this issue, I will make sure the addresses are only shared when the user copies and pastes them themselves.