Mobile Bitcoin Wallet Applications

Chance Cochran
Michael Dorn
Shreyas Prabhakar
Freddie Pope

December 1 2016

TABLE OF CONTENTS

Mobile Bitcoin Wallet Applications

Chance Cochran, Michael Dorn, Shreyas Prabhakar, Freddie Pope

December 1, 2016

Group - 1
Mobile Bitcoin Wallet Applications

Introduction

Bitcoin is a crypto-currency format that was introduced to the world by an unknown programmer, or group of programmers, who went by the name Satoshi Nakamoto in 2009. The system is a peer-to-peer payment system that allows users to make transactions between one another without an intermediary. Transactions are verified by distributed nodes across a network and then recorded in a public ledger (which also happens to be distributed) called a "blockchain". Bitcoins are created to reward users for using their computing power to verify transactions (i.e. act as a node in the distributed system) and store the results into the blockchain. This is known as "mining", and successful miners are rewarded a percentage of the Bitcoins traded in the transaction and potentially any newly created Bitcoins as well. New Bitcoins are created when new blocks of memory are found to be added to the blockchain. Bitcoin is a finite currency in that there is a fixed-limit on the number of bitcoins that can be created. When bitcoin was created it was determined that there would only ever be a maximum of 21 million bitcoins in circulation.

Bitcoin is notable for being the first decentralized digital currency. Being a decentralized currency means that Bitcoin unlike a centralized currency there is no entity that "creates" bitcoins. Once the finite supply of bitcoins has been exhausted there will never be more created. Also, bitcoin is not backed by any bank or government and therefore not insured. Bitcoin is a currency that has taken to the ethos of the free software foundation in power being given back from the users. Instead of having a credit card processing system or a bank bitcoin is processed via a peer-to-peer system using blockchain. The blockchain is one of the main reasons why Bitcoin is very secure. In order for bitcoin currency to be falsified, a malicious user would have to replicate all previous blocks in the blockchain before any new transactions are added. This is computationally not feasible. Also all transactions once, completed are listed publicly on www.blockchain.info so any user can go to check if their transaction is valid.

In summary, Bitcoin is a digital currency focused on security and it was the focus of our usability study. The researchers Chance, Evan, and Shreyas conducted the usability study by transferring funds from their individual Bitcoin wallets to research participants in their respective groups. Time for completion for various actions was logged and participants filled out a pre and post study survey. The goal of this research was to find usability flaws in a current Bitcoin wallet app and suggest improvements to the system.

Group - 1
Mobile Bitcoin Wallet Applications

Executive Summary

The research centred around a usability test of the Bitcoin wallet “Green Address”. Green Address was chosen because it is an open platform anyone with a computing device can access from OS X, Windows, or a mobile OS such as iOS or Android. Also, Green Address focuses on security; it’s log in is based on a mnemonic password scheme followed by a personalized pin. Green Address also has the ability to be used with a public PGP key and a physical NFC strip. Green Address is obviously secure, but the question proposed for the study was “is it useable?”. The Bitcoin Wallet app usability test performed took place at Clemson University as well as the researcher’s hometowns. 10 participants total took part in the study. Each Participants were asked to set up a Green Address bitcoin wallet, then funds amounting to $1USD in Bitcoin was transferred to each participant’s newly created wallet. The entire process time was logged from account creation to finally performing the transaction. However, account creation and making a transaction were recorded as two separate data points.

The test identified the following problems:

- Users didn’t like the default mnemonic login.
- At the start of the study, participants didn’t actually know what Bitcoin is.
- Users had trouble figuring out how to perform a transaction.
- Users had a hard time finding where their bitcoin address is located.
- Users didn’t understand how to spend Bitcoin.

Summary of User Needs:

From our study, the needs of the average user are as follows

- Be able to quickly and easily access funds via wallet app.
- Be able to securely perform transactions at will amongst a wide array of merchants.
- Be able to access their funds as if they were cash.
- Not have government / legal repercussions for solely using Bitcoin for legal purposes.
- Shortened time for performing a transaction with a Bitcoin wallet app.

Bitcoin as a payment method:

From our study, a resoundingly common result was that participants had no prior knowledge of Bitcoin. Once sufficiently educated, the participants felt that Bitcoin offered no benefit over traditional cash or credit card payment methods. They also felt that Bitcoin was extremely limited and difficult to set up and that having to transfer funds to gift cards through 3rd party services outside of the wallet app was

a hassle. For several participants, just the mnemonic based login was enough to make them disinterested. The study shows that Bitcoin has a huge area for improvement in terms of usability. From a user standpoint, the user doesn't care how private / secure it is, if it offers no further utility or ease of use for them. It is extremely difficult for them to set up or understand how to use. Overall, Bitcoin is certainly secure, but it seems to have come at a hefty cost of usability, hurting its chances of reaching the much less security minded general public. Our suggestions in the recommendation section will list our ideas for just a few usability improvements to the Bitcoin system, using Green Address as a mode of improvement.

This report contains the participant feedback to survey questions, data for time of completion of the study, ease or difficulty of completion ratings, and suggestions for improvements including a prototype mock-up. A copy of the survey results, and prototype mock-up are included in the Appendix section.

Methodology

Sessions

Our group decided to run a Usability test with the application Green Address. Each member of the group was given 6.724 mBTC (~$5). From here, we reached out to participants.

Participants were asked to download the application Green Address. They then were asked to fill out a pre survey (Appendix - A).

Next, participants watched an informative video on the basics of Bitcoin. [7]

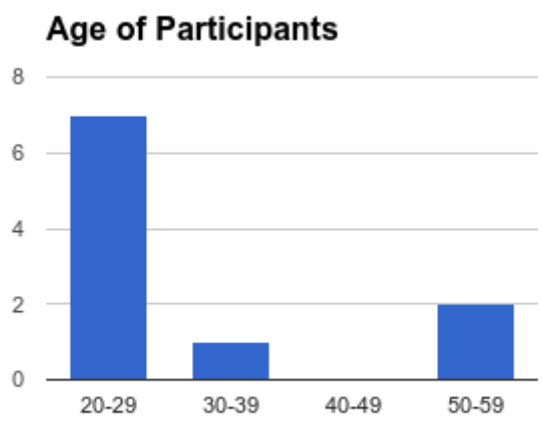
Upon finishing the video, the participant was told to create a wallet using Green Address, and a timer began. The timer was stopped once the participant entered the main menu of the application.

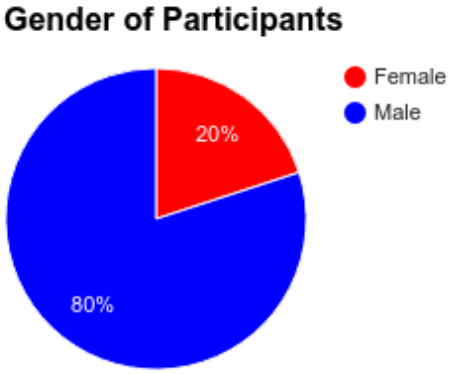
In the second part of the test, participants were timed in making a transaction. After the timer started, participants were asked to find their wallet's address for the proctor to send 1.62717 mBTC (~$1). Upon receiving the Bitcoin, they were asked to send to a given Wallet Address (the proctor's). Once this was verified, the timer was stopped.

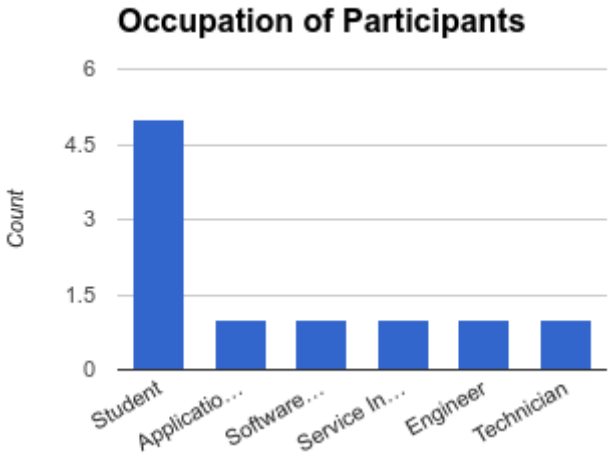
Participants were given an exit survey (Appendix - A) to record their reaction to the process and suggestions for improvement.

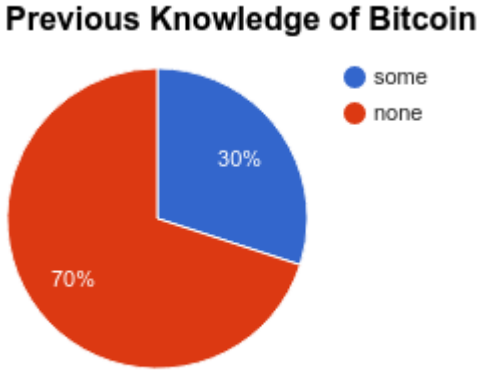
Participants

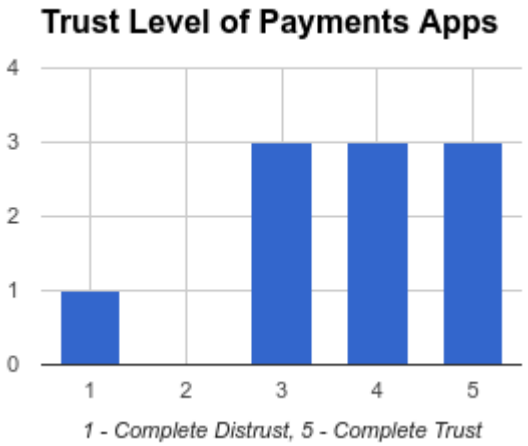
Ten total participants were performed the tasks involved in the study. Three participated on November 23 and the remaining seven on November 25th. The study group chosen was mainly young tech savvy twenty somethings in the age range of 20 to 29. Three outliers were chosen older than 29. A younger and more technically savvy group was chosen with the assumption that they would already know about bitcoin or easily be able to figure out how to use it. Surprisingly, 70% of participants studied had never heard of bitcoin, and 100% had never used it. By an overwhelming majority, the occupation of the most of the participants was student. Of the 10 participants studied, eight were male and two were female. Almost all participants surveyed stated they had decent or about average technical skills, and felt confident in using an online financial application. The level of trust in Green Address and banking apps in general was pretty high with only one participant stating that they don't trust any online banking app.











Evaluation Tasks/Scenarios

Participants were asked to complete the following:

- Download the Green Address from their OS's secure app store.
- Complete the Pre Survey.
- Create an account with Two Factor Authentication.
- Find their Bitcoin Address in order to receive Bitcoin.
- Send the Bitcoin to the Proctor's Bitcoin address.
- Complete the Post Survey.

Results

Task Ratings

After the completion of each task, participants rated the ease or difficulty of completing the task for three factors:

- It was easy to navigate to the required section.
- As I was navigating through the application, I was able to keep track of where I was in the application.
- I was able to do the task without much help.

The 5-point rating scale ranged from 1 (Difficult) to 5 (Easy).

Easy ratings with a mean easy rating of 3.7 and ranging between 3 and 5 considered for the Task-1, the users agree that it was easy to setup a Bitcoin account on Green Address, although they were not completely satisfied with the process.

Easy ratings with a mean easy rating of ~3.1 and only 3 participants rating both the process >4 for the Task-2 and Task-3, the users felt it was very difficult to make a transaction.

Ease of Using the Application

All the participants agreed it was easy to setup a Bitcoin wallet account on Green Address, they were annoyed with the mnemonic passphrase. The way the passphrase was implemented on iOS and Android was a little different. The Android users was more approving of it, compared to the iOS users. Only 30% of the participants were able to make a transaction with ease. Most of them found it hard to find their Bitcoin Address, to perform a Receive transaction. For the Send Transaction, the participants felt it was tedious to get the confirmation code from the email for every single transaction.

Test 1 – Mean Task Ratings & Percent Agree

Task	Ease	Overall Satisfaction
1 – Setting up a Bitcoin Wallet account	3.7(60%)	3.2
2 – Perform a Receive Transaction	3.1(30%)	3.3
3 – Perform a Send Transaction	3.2(30%)	4.0

**Percent Easy (%) = Easy & Very Easy Responses combined*

Time on Task

We recorded the time on task for each participant. Some tasks were inherently more difficult to complete and had a lot of steps that the people had to go through than others and is reflected by the average time on task.

The table below displays Time on task for each participant and the Average Time on Task. Very high time on tasks are bolded.

Time on Task

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Avg TOT
Task 1	7	**10**	5	6	5	**10**	5	4	5	7	6.4
Task 2	10	10	10	**12**	**15**	**20**	9	4	7	10	10.7
Task 3	10	8	18	**27**	2	4	12	15	9	**23**	**12.8**

**Time is in Minutes*

Task 1 required participants to setup their account. However, completion times ranged from approximately 4 minutes to 10 minutes with most times around the 5 minutes' range.

Task 2 required participants to make a Send Transaction. However, completion times ranged from approximately 4 minutes to 20 minutes with most times around the 10 minutes' range. This task took more time as I required participants to log in their e-mail account to get the one-time code for completing the send transaction.

Task 3 required participants to make a Receive Transaction. However, completion times ranged from approximately 2 minutes to 27 minutes with Average Time-On-Task of 12.8 minutes. Most users took most time to complete this task as they struggled to find their Bitcoin Address or the QR Code of their Bitcoin Address. Even after they found their bitcoin address, they struggled to copy it to clipboard and sending it to the Sender.

Summary of Data

The table below displays a summary of the test data. Low ease of completion and satisfaction ratings and high time on tasks are highlighted in red.

Summary of Ease of Completion, Time on Task, Mean Satisfaction

1	3.7	3.2	6.4
2	3.1	3.3	10.7
3	3.2	4.0	12.8

Recommendations

Based on our study, it has been found that Green Address wasn't very usable for most people. There were two problems that faced users. The first being getting the account creation process setup and getting into their account. The second being that users didn't really understand how to use the app and had a hard time navigating through the menus and then figuring out how to send Bitcoin currency or perform a transaction. It is recommended that first, the overall user experience of logging in and creating an account be improved. Mnemonics can work, but that are difficult for some users to understand or just not their preference. It would be an improvement to add the option to choose between mnemonics or a default 2 factor authentication with username and password followed by pin. Second, it is recommended that some friendly way of informing the user how to use the app be added. This could come in the form of a tutorial at the start of the app or, a UI overlay that is displayed on first use. The UI overlay could direct users to locations of key functionality within the app. A third feature that was requested but is potentially outside of the scope of this particular study is adding the ability to purchase Bitcoin / transfer bitcoin to funds and gift cards from within the app. Functionality to have a centralized "hub" within a wallet app would make Bitcoin much more usable to the average everyday user. Currently, Bitcoin is primarily used by the security conscious and highly technical users. A Bitcoin wallet app such as Green Address could benefit greatly in terms of usability from suggestions previously mentioned above.

The recommendations section provides recommended changes and justifications driven by the participant success rate, behaviours, and comments. Each recommendation includes a severity rating. The following recommendations will improve the overall ease of use and address the areas where participants experienced problems or found the interface/information architecture unclear.

Conclusion

In conclusion, although Bitcoin and the Green Address application are very secure, they aren't as usable as they need to be to attract the general public from their current payment methods. Through our study it became clear to us that the complexity of the Green Address app and general confusion surrounding Bitcoin lead to a difficulty for users to interact easily with the app. The average user doesn't understand how to Bitcoin works or how to use the application upon first use. It is the recommendation of the study, based on the recorded data that first, other login options are provided to users. Second, that some form of in app guidance be added. Both a tutorial, or simple directions as a layover on first use directing users in the way they should go about using the app, would help the user understand use of the app so that the user feels less lost on their first attempt to use Bitcoin and the app. In continuation of the study, it would be ideal to explore improving login and in-app functionality through adding the ability to buy Bitcoin, and transfer Bitcoin to store gift cards / cash all within the app. These were requests from several users in the study and would greatly improve the utility and usability of the system.

References

1. Nakamoto Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." (2008): 109-22. https://bitcoin.org/bitcoin.pdf, 31 Oct. 2008. Web.
2. George Hurlburt, Irena Bojanova, " Bitcoin: Benefit or Curse?", IT Professional, pp. 10-15, 2014, ISSN 1520-9202.
3. Bohr Jeremiah, Bashir Masooda, "Who Uses Bitcoin? An exploration of the Bitcoin community", Twelfth Annual Conference on Privacy, Security and Trust (PST), pp. 94-101, 2014
4. "Get Started." Incorporating Bitcoin. https://incorporatingbitcoin.com/get-started/, 12 June 2016.
5. "Bitcoin FAQ - Newcomers Please Read." Reddit. https://www.reddit.com/r/Bitcoin/comments/533fxl/rbitcoin_faq_newcomers_please_read/, Web. 01 Dec. 2016.
6. "99Bitcoins" 99 Bitcoins. https://99bitcoins.com/, 28 Nov. 2016. Web.
7. Weusecoins. "What Is Bitcoin? (v2)." YouTube. YouTube, https://youtu.be/Gc2en3nHxA4, 24 Apr. 2014. Web.
8. Spectrummag. "The Bitcoin Blockchain Explained." YouTube. YouTube, https://youtu.be/M_zCjjy59cg, 06 July 2016. Web.
9. Khoslaventures. "Bitcoin 101 | Balaji Srinivasan." YouTube. YouTube, https://youtu.be/JIxwTx7o_B4, 22 June 2015. Web.

Appendix A –

Pre-Survey

Age:

Male/Female:

Occupation:

What payment methods do you usually use?
(Cash / Debit Cards /
Credit Cards / Online Transactions):

Which Online/Mobile apps for
sending or receiving money that you use:

(Banking apps / 3rd party apps like Venmo, Facebook etc.):

What is your Level of trust?
of these applications: (Don't Trust) 1 2 3 4 5 (Trust):

Have you heard of Bitcoins before? If yes, Where?

Have you used Bitcoins before? If yes, how
frequently do you use? Which wallet? And what are your thoughts on Bitcoins?

How well would you rate your
technical skills? (No Skill) 1 2 3 4 5 (Very Skilled):

Appendix B –

Exit-Survey

How easy was it to set up an account with Green Address?
(Difficult) 1 2 3 4 5 (Easy):

Time to set up Account:

Suggestions on improving the Set-up process:

How easy was it to make a transaction? (Difficult) 1 2 3 4 5 (Easy):

Time until confirmation:
Sending:
Receiving:

Suggestions for
improving the transaction process?

Suggestions for improving the entire experience/app in general:

How likely would you use Bitcoins/other cryptocurrency in the future?

How well do you feel you understand Bitcoins now?

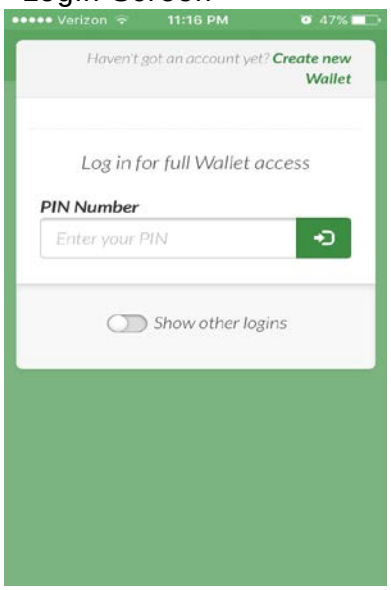
How likely would you suggest Bitcoins to others?

What else would you like to know?

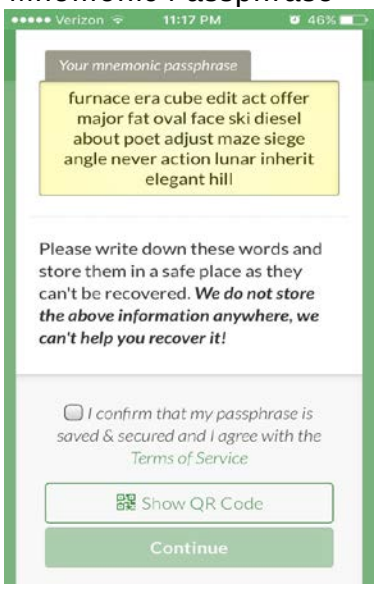
Appendix C –

Original Application Layout

Login Screen

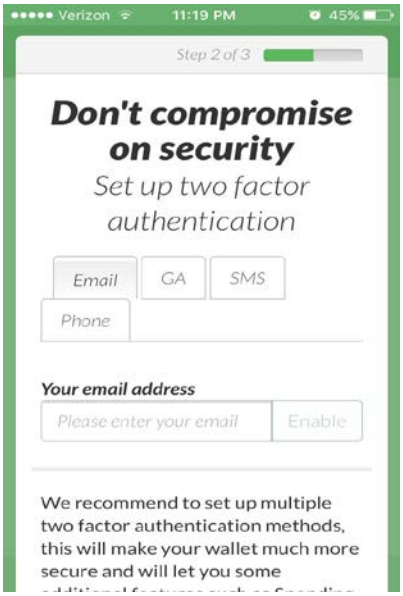


Mnemonic Passphrase

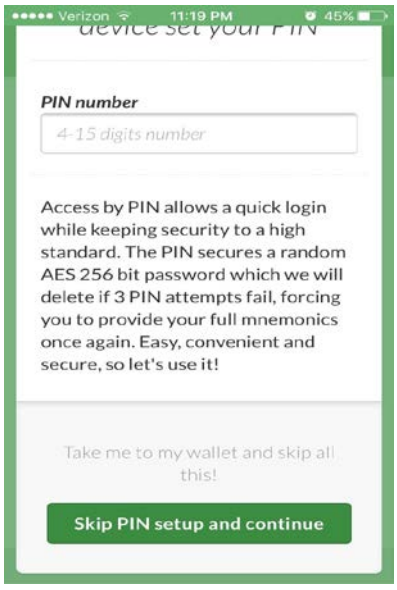


Mnemonic Entry

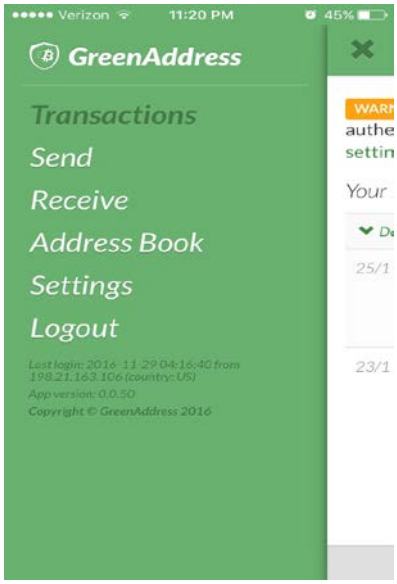
Two Factor Entry



PIN Entry

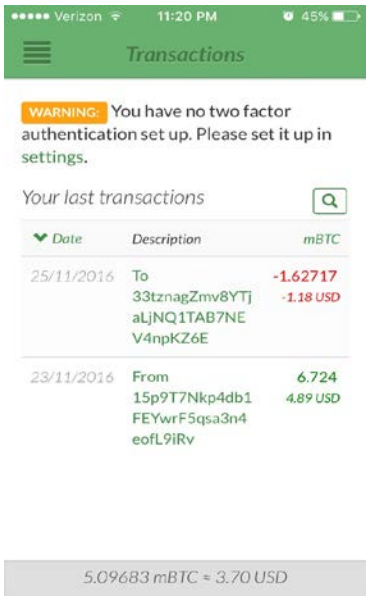


Menu

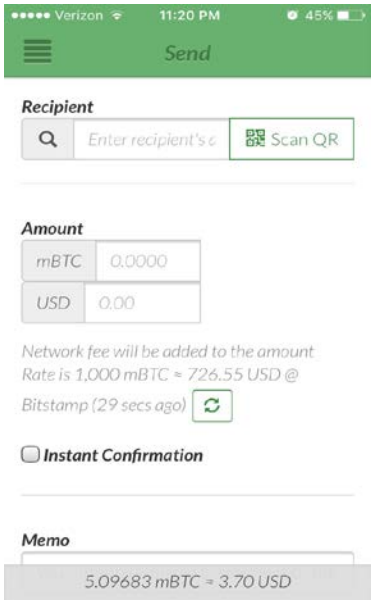


Group - 1
Mobile Bitcoin Wallet Applications

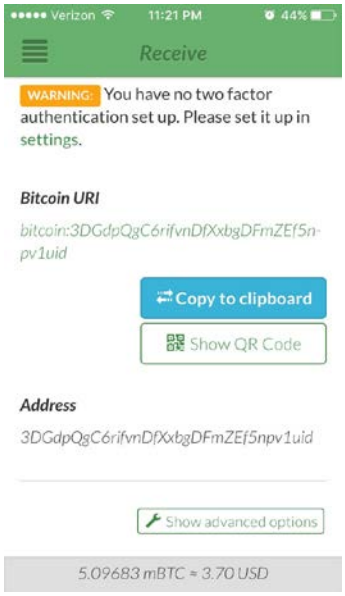
Transaction Tab



Send Tab



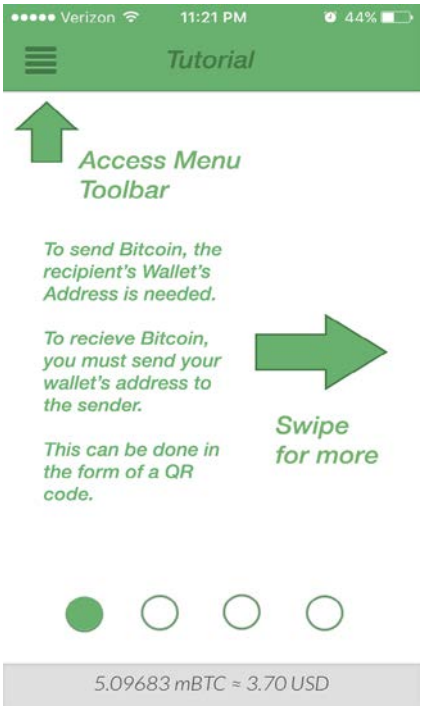
Receive Tab



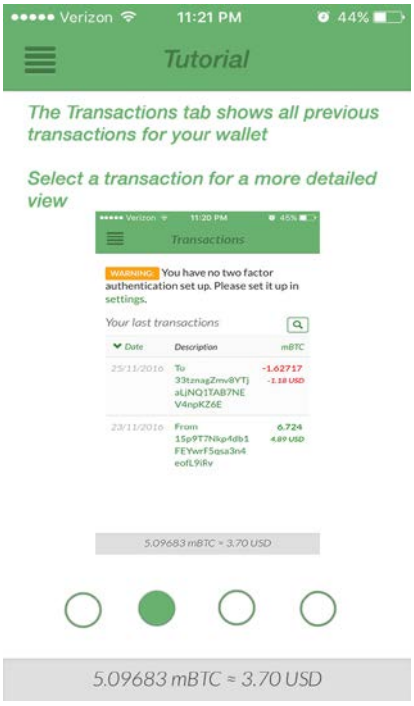
Appendix D –

Prototype Update - 1

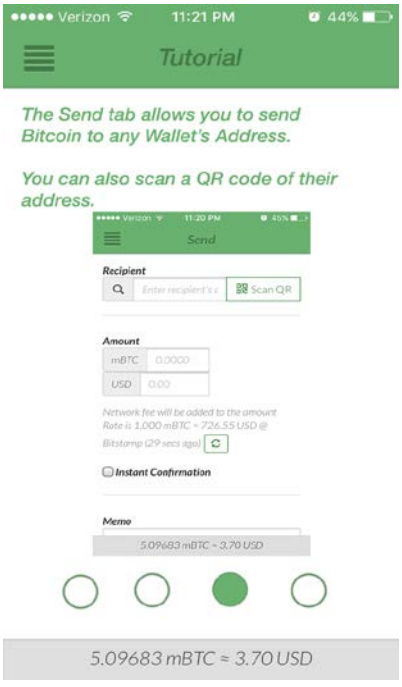
UI Tutorial



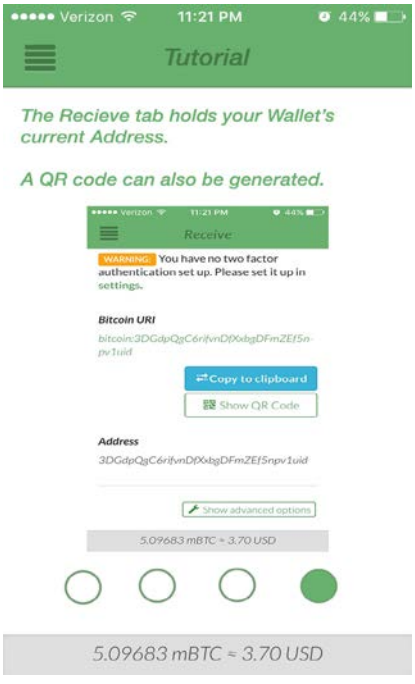
Transaction Tutorial



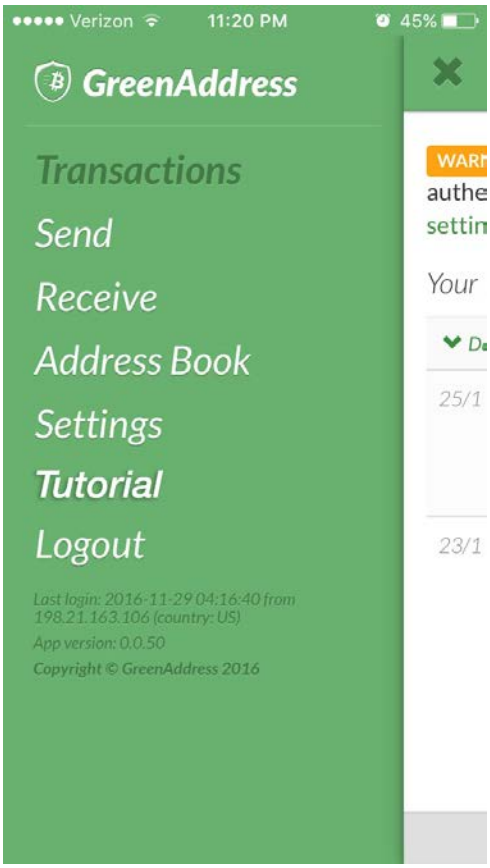
Send Tutorial



Receive Tutorial



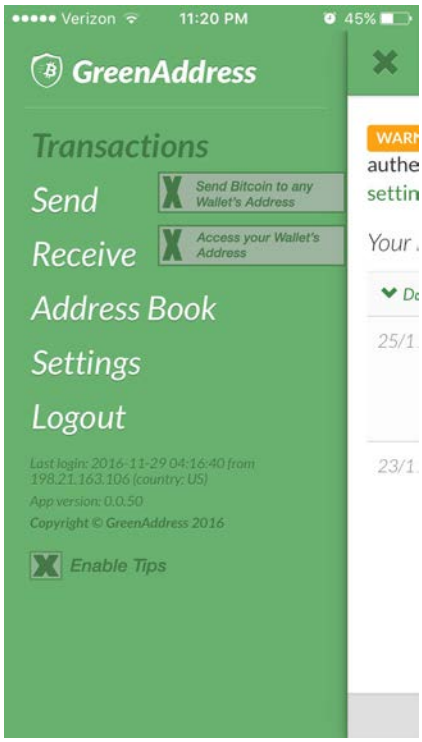
Updated Menu



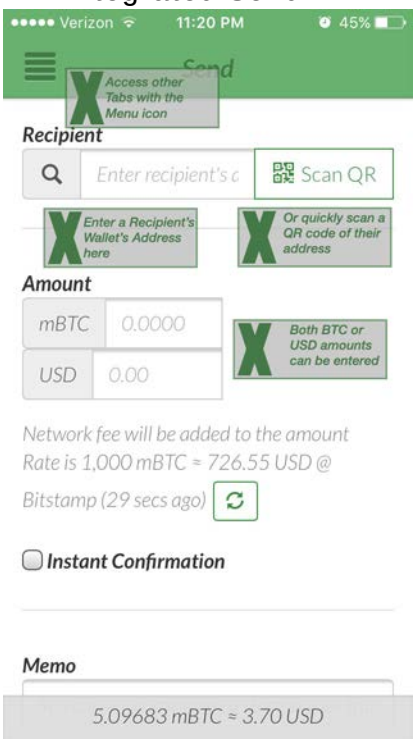
Appendix E –

Prototype Update - 2

Integrated Menu



Integrated Send



Integrated Receive