Usable Crypto Wallet Interface

Rohit Raj
19CS10049
rrohit2901@gmail.com

Haasita Pinnepu
19CS30021
pinnepu.haasita@gmail.com

D G Pranathi
19CS10025
gyana1500@gmail.com

Ansari Md Saad
19EE38023
saadshun@gmail.com

K Rakesh Krishna
19CS30024
rakhikrish1319@gmail.com

Parth Tusham
19CS30034
parthtusham@gmail.com

ABSTRACT

In this report, we deal with the analysis of a proposed Usable crypto wallet interface, which would make the transaction of crypto currency hassle-free. This paper describes the current state of crypto wallets on the market, the choices of a better solution for transaction of cryptocurrencies and using crypto wallets and future trends in their development.

KEYWORDS

Usability, Cryptocurrency wallet, Cryptocurrencies, User-interface, User-experience, Transactions

ACM Reference Format:
Rohit Raj, Haasita Pinnepu, D G Pranathi, Ansari Md Saad, K Rakesh Krishna, and Parth Tusham. 2022. Usable Crypto Wallet Interface. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 MOTIVATION

With the inception of Bitcoin in 2008 a new form of digital currency called cryptocurrency has come into existence. The primary goal of such a digital currency is to carry out financial transactions among respective parties without any trusted intermediaries. This is fundamentally different to the existing financial transactions systems which rely on a single or group of trusted organisations for any financial transaction to happen. This strong property of a cryptocurrency is often regarded as a fundamental breakthrough in financial technology domains. The undertone for all digital currencies is to either complement or supplement the flat-currency based traditional monetary systems in different application scenarios. This can only be possible with a wide-scale adoption of these cryptocurrencies. One of the crucial barriers for the wide-scale adoption of any novel technology is the issues in usability. Usability is the degree to which a software is easy to use and a good fit for the audience. A cryptocurrency heavily relies on cryptographic mechanisms which are often diffcult to utilise in an effective manner, even for experienced security programmers.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

A cryptocurrency uses asymmetric cryptography for security through a pair of keys: the private and public. A private key is a secret number that allows a user to use the currency. It must remain secret at all times as revealing it to third parties is equivalent to giving them control over the corresponding currency. As such, these keys are fundamental to manage and transfer the ownership of a cryptocurrency to another user. To facilitate the management of such keys, a software called Wallet is used to create and store the required cryptographic keys and hence, plays a vital role in all use cases of a cryptocurrency.

Managing cryptocurrencies using such wallets, however, has been found to be challenging for the users. Eskandari et al.[3] conducted cognitive walkthroughs with bitcoin wallets and identified shortcomings, such as misunderstood metaphors and abstractions, that could lead to user errors. Voskobojnikov et al.[2] interviewed cryptocurrency users and found that the majority of them found current software tools difficult and unintuitive to use.

Research [1] has also shown that some reviewers had conventional payment systems in mind when using the apps and believed that, similar to online banking, transactions had fixed fees, were reversible, and could be canceled, none of which are the case in reality. Further, reviewers also had limited understanding of the underlying technology and were confused about the fundamental building blocks, including public key cryptography, recovery mechanisms, transactions, and even the role of a wallet. Often, these misconceptions resulted in reviewers blaming the wallet providers even when the latter were not at fault.

Therefore, we propose a wallet that mimics the functionality of traditional payment systems. In this report, we mention the methodology we followed, our study design, the analysis techniques we plan to use and the future scope of this work.

2 RESEARCH QUESTION

As noted in the introduction, the current crypto wallets have several drawbacks and limitations. And people are finding it difficult to adapt to these despite various changes and updates brought about by wallet designers. Meanwhile, people find it familiar and easy to do UPI transactions using QR codes and expect something similar along these lines. So by this study, we want to answer the question 'Can we design a novel usable crypto wallet interface in line with users' usual financial experiences and familiar bank payment interfaces'.

3 STUDY DESIGN

3.1 Recruitment

The participants for the study are recruited through an advertisement flyer designed for this purpose. The study participants are mostly comprised of college students. A preliminary interview to determine whether the applicants are familiar with using general transaction through a mobile phone is done. The participants' knowledge about crypto currency and crypto wallets is asked about, but this is to get a balance in the dataset, as we do need the user-experience review of the interface from both new users and experienced users. After recruitment, the participants are asked to sign a consent form and are briefed about the process they have to go through.

3.2 Experimental setup

We conducted the study with various participants with varying demographics. Participants were given a mobile phone with pre-installed two interfaces. Our experimental setup consists of two interfaces

(1) The baseline interface
(2) Our new implementation using a QR Code

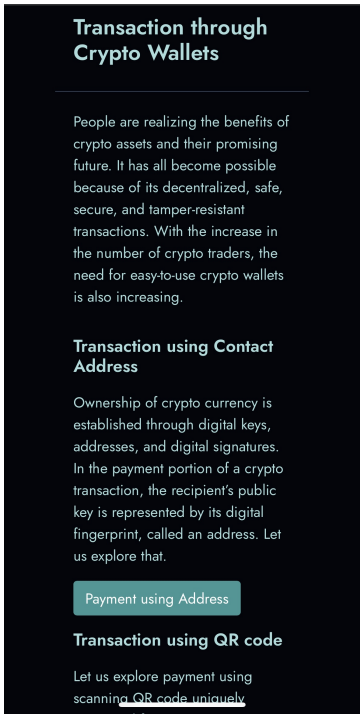

Figure 1: The experiment prototype of the user Landing page of the interface, describing briefly the context and telling the user what to do.

For the first part of the lab test, we asked the research subjects to carry out cryptocurrency transactions using the baseline interface, in which they were provided with five addresses ranging from 27 to 34 alphanumeric characters, with each one beginning with 1, 3, or bc1 (in accordance with the BTC standard address format).
For carrying out a successful transaction in the baseline interface, the user must:

(1) Navigate to the transaction page titled "Transaction 1" from the Landing Page.
(2) Enter the correct cryptocurrency address without any inconsistencies.
(3) Select the target cryptocurrency as provided beforehand.
(4) Enter the amount as given.
(5) Click on the button titled 'Transfer the amount' to finalise the transaction.

There were two possibilities for each transaction: Either the transaction was successfully or unsuccessfully executed. A transaction is considered unsuccessfully executed if:

- The cryptocurrency address entered by the user was not identical to the given address.
- The amount and/or currency entered by the user was not identical to the given data.
- The user was unable to understand the process of the transaction.
- The user had unintentionally canceled the transaction during the process.

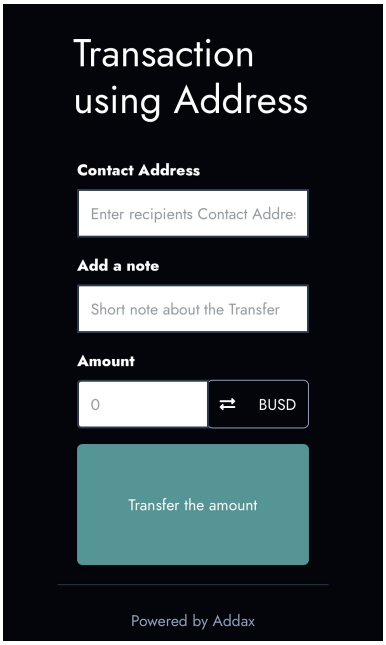

Figure 2: The experiment prototype of the baseline interface for transaction using Address of the recipient, different use cases are to tested here.

After attempting transactions with the baseline interface, participants were then asked to fill out a short survey outlining their experience, as well as their opinions on the usability of the interface. In the survey, a link was provided to the landing page of the

second interface, after which the participants were then exposed to the novel QR-code based transaction interface. For this interface, the participants were given five transactions to complete, this time using QR codes instead of text-based addresses. This time, for a transaction to be classified as successful, the user must:

(1) Navigate to the transaction page titled "Transaction 2" from the Landing Page.
(2) Click on the "Scan QR" button.
(3) Use the camera of the mobile phone to scan the QR code, and automatically enter the address.
(4) Select the target cryptocurrency as provided beforehand.
(5) Enter the amount as given.
(6) Click on the button titled 'Transfer the amount' to finalise the transaction.

For this interface too, there were two possibilities - Either a transaction was successfully, or unsuccessfully executed. A transaction is considered unsuccessfully executed if:

- The user failed to scan the QR code.
- The amount and/or currency entered by the user was not identical to the given data.
- The user was unable to understand the process of the transaction.
- The user had unintentionally canceled the transaction during the process.

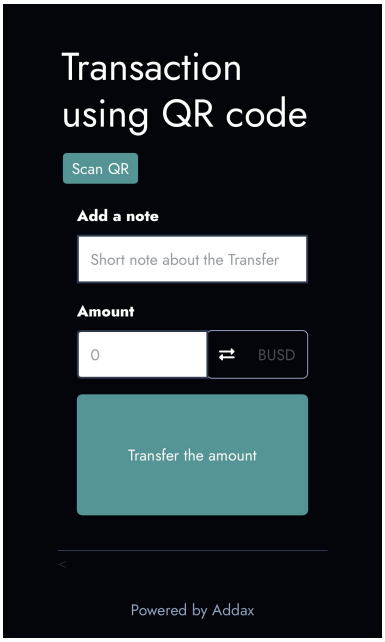

Figure 3: The experiment prototype of the proposed interface for transaction using OR code of the recipient uniquely generated, different use cases are to tested here.

Similar to the first interface, participants were then asked to take a short survey highlighting their experience and their opinions, followed by a short demographic survey for analysis. We chose to provide a demographic survey at the end of the experiments and the surveys to avoid priming the subjects and making them conscious about their choices in line with their identity. All data collected from the surveys was anonymised to preserve subjects' security and privacy. We haven't collected any emails or tracking information during any part of the survey.

During the experiment, we recorded the time taken by each participant, as well as the number of successful and unsuccessful transactions carried out by the participant, in accordance to the definitions given above.

4 ANALYSIS PLAN

We collect data from the participants from both the lab tests and the surveys. From the lab test, we receive data pertaining to each participant, about (i) the time taken by them to complete the transactions, and (ii) the number of transactions successfully completed by the participant during this time. From the survey, we gain insight about participant opinions about the usability of our new interface, and demographic statistics.

Despite the regulatory uncertainty and confusion regarding policies affecting crypto, India's crypto adoption rate has continued to grow rapidly.There are dozens of different factors that govern the sentiment toward crypto-adoption in India. From education around crypto to regulatory constraints, some of these issues continue to affect the sentiment of investors and upcoming ones.

We are finding patterns by separating research subjects according to:

- **Age:** As people of new generation are more adoptive of new technology such as crypto and are willing to learn more
- **Occupation:** Our target audience is small shop owners as we have observed the usage of UPI payments using QR codes are high compared to other sectors
- **Gender:** Usage of crypto-currency overly biased as men tend to use more crypto based applications
- **UPI usage:** to better know the subjects prior knowledge of performing transactions on mobile/web based applications
- **Crypto usage:** to better know the subjects prior knowledge of performing transactions on mobile/web based crypto applications

We have modelled all variables as categorical variables, and our main source of data is the survey, so we will be primarily using the Chi-Square test to find correlations, to break down the data by demographics. We will also find the correlation between our data and the ground-truth UPI usage statistics, broken down by similar demographic parameters. We will especially be focusing on the opinion statistics of regular UPI users with low cryptocurrency exposure, as they are the target demographic for this new interface.

5 DIVISION OF WORK

The following is a brief description of the work done by each member of the group. The work was divided equally among the group members and everyone executed the allotted tasks accordingly.

5.1 Rohit Raj - 19CS10049

Implemented pages for the interface like buy coins page from exchange and design of transaction pages. Implemented small backend

for the interface which can measure time person spends in completing transaction starting from dashboard and number people who go wrong about transactions. Hosted the interface.

5.2 Haasita Pinnepu - 19CS30021

Upon deciding on the research question, I first made the IRB form for our project using the IRB template. In the following weeks, after the division of work, I worked on the website, mainly 2 of its web pages. And finally, I worked on writing this report.

5.3 Ansari Md Saad - 19EE38023

Earlier, I had made the recruitment flyer for the experiment. I was involved in making the survey questions. I have also written some parts of the final report. I formulated the study design as well as the analysis part of the experiment.

5.4 D G Pranathi - 19CS10025

First, I have learned about the various crypto wallets and the transaction processes they undergo. After that, I referred to some research papers on the study of crypto wallets to know the possible research questions. I have also contributed to creating a website design, mainly for 2 webpages where the user tests the interface.

5.5 K Rakesh Krishna - 19CS30024

Firstly, I did some background reading and studied the current usability standards in crypto wallets and identified a few drawbacks and areas where improvements can be made. Prepared the consent form for research participants. Made some suggestions on how to design the survey and test the interface. Coded one of the html pages of the designed interface and worked on few sections of the report.

5.6 Parth Tusham - 19CS30034

I reviewed various crypto-currency applications and websites to understand more about how the transactions are processed and to learn more about what difficulties one might face during executing a transaction. I also partially helped in designing the survey questions and proof read it. I was also involved in making the report.

6 FUTURE WORK PLAN

This study brings out a number of interesting behavioural patterns and mental models of the current crypto-currency users. As explained in the Study Design section we plan to carry out the study by doing a Lab test followed by a survey. We want to test this on people with some familiarity and experience with crypto wallets and find out whether the suggested interface made things easy for them by eliminating the Null hypothesis. We'll try to avoid a convenient sample and be careful about the demographics so that external validity holds. We would provide the subjects with both interfaces and then conduct a survey with the questionnaire mentioned above. Other than that we will implement this novel idea as an android based app either a stand alone app or integrating it as a interface/subroutine of an existing app. We hope that our effort will help someone understand blockchain technology and blockchain security issues. The users who use blockchain to do the transactions will pay more attention to the security of blockchain itself. We also expect that the researchers will benefit from our study for their further research in developing blockchain technology and addressing blockchain security issues.

7 PRESENTATION AND MATERIALS

The Google drive link for the presentation is here.

The Experiment Website link is here.

The survey form for interface-1 is here.

The survey form for interface-2 is here.

REFERENCES

[1] Masoud Mehrabi Koushki Volker Roth Artemij Voskobojnikov, Oliver Wiese and Konstantin (Kosta) Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. *CHI Conference on Human Factors in Computing Systems (CHI '21)* (2021). https://doi.org/10.1145/3411764.3445407

[2] Yue Huang Artemij Voskobojnikov, Borke Obada-Obieh and Konstantin Beznosov. 2020. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non) Users. *International Conference on Financial Cryptography and Data Security* (2020).

[3] David Barrera Shayan Eskandari, Jeremy Clark and Elizabeth Stobert. 2015. A First Look at the Usability of Bitcoin Key Management. *Proceedings 2015 Workshop on Usable Security* (2015).