



University of
Zurich^{UZH}

Design, Implementation and Usability Evaluation of the AfriBit Bitcoin Lightning wallet

Marco Leder
Zurich, Switzerland
Student ID: 19-747-773

Supervisor: Bruno Rodrigues, Jan von der Assen, Prof. Dr.
Burkhard Stiller

Date of Submission: December 30, 2023

Abstract

For many Western countries, access to a functioning banking system is taken for granted. However, many people in developing countries are still excluded from having a bank account for savings and worldwide money transfers. In the region of Kenya, MPesa has established itself as a mobile financial money service. This service provides a possible solution to mitigate some of the issues of financial exclusion and offers the possibility of accessing mobile banking services. However, given that financial exclusion is a multi-faceted problem, certain shortcomings of MPesa demand a novel solution, accessible to everyone. This thesis investigates using and adopting blockchain technology for financial inclusion in Kibera, a Kenyan slum, to serve as a feasible alternative to MPesa. Thereby, the requirements of a new solution are gathered collectively with local residents of Kibera, ensuring that both common and area-specific issues are mitigated. The focus lies in offering an improved user interface (UI) for both inexperienced and illiterate users, a major issue of the aforementioned service MPesa. The goal of this thesis is to design and implement a solution that not only reduces financial exclusion but also improves the user experience (UX) of existing solutions. Thereby, Framer is used to improve the design of *Blink*, an existing Bitcoin Lightning wallet developed by Galoy and deployed in El Salvador. Blink was chosen to leverage existing security-audited code, ensuring the safety of the user's funds once the new solution, *AfriBit*, is deployed. As far as the author is concerned, no other Bitcoin Lightning wallet has been improved in its design with a special focus on applying principles from the field of people-oriented computing (POC) and human-computer interaction (HCI) to make the interface more accessible to the region of Kibera. The design process is followed by the implementation of the new UI in React-Native with Typescript, resulting in a functional prototype. This prototype is then used to conduct a 20-person user study, with a group from Kibera and a group from Switzerland. The study involves real-world scenarios to gather qualitative and quantitative data on the new design changes. Thereby, this thesis leverages the Usability Experience Questionnaire (UEQ) to assess the quality of the introduced changes. Furthermore, quantitative time measurements serve as the basis for statistically analyzing the effectiveness of the new UI and its impact on the UX. From the results of the user study, it can be concluded that no participant group exhibits a statistically significant learning effect. This means that in areas where the interface remained the same, no difference in the time for executing real-world scenario tasks has been observed. In areas underlying the changes of the new interface design, it has been shown with a statistically significant p-value of 0.01562, that the Blink UI takes participants longer to complete the given tasks. The inclusion of parts of our changes in the production build of Blink marks the confirmation that the proposed UI changes are not only beneficial to the users of Kenya but also to all Blink users.

Fuer viele westliche Laender ist der Zugang zu einem funktionierenden Bankensystem eine Selbstverstaendlichkeit. Einige Menschen in Entwicklungslaendern sind jedoch immer noch von einem Sparkonto und weltweiten Geldueberweisungen ausgeschlossen. In Kenia hat sich MPesa als mobiler Finanzdienst etabliert. Dieser Dienst stellt eine moegliche Loesung dar, um einige Probleme der finanziellen Ausgrenzung zu bekaempfen, und bietet die Moeglichkeit, auf mobile Bankdienstleistungen zuzugreifen. Da die finanzielle Abschottung jedoch ein vielschichtiges Problem ist, erfordern bestimmte Probleme von MPesa eine neuartige, fuer alle zugaengliche Loesung. In dieser Arbeit wird untersucht, wie die Blockchain-Technologie zur finanziellen Eingliederung in Kibera, einem kenianischen Slum, eingesetzt werden kann, um eine praktikable Alternative zu MPesa zu bieten. Dabei werden die Anforderungen an eine neue Loesung gemeinsam mit den Bewohnern von Kibera erhoben, um sicherzustellen, dass sowohl allgemeine als auch gebietsspezifische Probleme gemildert werden. Der Schwerpunkt liegt auf einer verbesserten Benutzeroberflaeche (UI) fuer unerfahrene und ungebildete Nutzer, ein Hauptproblem des oben genannten Dienstes MPesa. Das Ziel dieser Arbeit ist es, eine Loesung zu entwerfen und zu implementieren, die nicht nur die finanzielle Ausgrenzung verringert, sondern auch die Benutzerfreundlichkeit (UX) der bestehenden Loesungen verbessert. Dabei wird Framer verwendet, um das Design von *Blink* zu verbessern, eine bestehende Bitcoin Lightning Wallet, die von Galoy entwickelt und in El Salvador eingesetzt wird. *Blink* wurde ausgewaehlt, um den bestehenden sicherheitsgeprueften Code zu nutzen und die Sicherheit der Gelder der Nutzer zu gewaehrleisten, sobald die neue Loesung, *AfriBit*, eingesetzt wird. Soweit der Autor Bescheid weiss, wurde keine andere Bitcoin Lightning Wallet in ihrem Design verbessert, wobei ein besonderer Schwerpunkt auf die Anwendung von Prinzipien aus den Bereichen Mensch-und-Computer (POC) und Mensch-Computer-Interaktion (HCI) gelegt wird, um das Design fuer die Region Kibera besser zugaenglich zu machen. Nach dem Designprozess folgt die Implementierung der neuen Benutzeroberflaeche in React-Native mit Typescript, was zu einem funktionalen Prototyp fuehrt. Anhand dieses Prototyps wird dann eine Nutzerstudie mit 20 Personen durchgefuehrt, wobei eine Gruppe aus Kibera und eine Gruppe aus der Schweiz teilnimmt. Die Studie umfasst reale Szenarien, um qualitative und quantitative Daten ueber die neuen Designaenderungen zu sammeln. Dabei nutzt diese Arbeit den Usability Experience Questionnaire (UEQ), um die Qualitaet der eingefuehrten Aenderungen zu bewerten. Darueber hinaus dienen quantitative Zeitmessungen als Grundlage fuer die statistische Analyse der Effektivitaet der neuen UI und ihrer Auswirkungen auf die UX. Aus den Ergebnissen der Nutzerstudie laesst sich schliessen, dass keine Teilnehmergruppe einen statistisch signifikanten Lerneffekt aufweist. Das bedeutet, dass in den Bereichen, in denen die Oberflaeche gleich geblieben ist, kein Unterschied in der Zeit fuer die Ausfuehrung von Aufgaben des realen Szenarios festgestellt wurde. In den Bereichen, die den Aenderungen des neuen Schnittstellendesigns unterliegen, hat sich mit einem statistisch signifikanten p-Wert von 0,01562 ergeben, dass die Teilnehmer mit der *Blink*-Benutzeroberflaeche laenger brauchen, um die vorgegebenen Aufgaben zu erledigen. Die Aufnahme von Teilen unserer Aenderungen in das bestehende Produkt *Blink* ist die Bestaetigung, dass die vorgeschlagenen UI-Aenderungen nicht nur fuer die Nutzer von Kenia, sondern auch fuer alle Nutzer von *Blink*.

Acknowledgments

First and foremost I would like to express my gratitude towards my supervisor Bruno Bastos Rodrigues for his guidance and support throughout the whole thesis. Secondly, I am grateful for the openness with which Prof. Dr. Burkhard Stiller approached my suggested topic and the freedom I was given to explore this field. I would also like to mention my co-supervisor Jan von der Assen and the whole Communication Systems Group, who have always had an open ear.

Concerning that this thesis has been developed in close collaboration with the Galoy team, the Canadian company Securities Industry Data Exchange (SIDE) and the support of the the Ronnie Mdawida Fund, special thanks are also devoted to these teams and individuals, including the participants from the user study.

Last but not least, I would like to thank my family and friends for their support and encouragement, not only in regards to this thesis, but also throughout my entire studies.

Inhaltsverzeichnis

Abstract	i
Acknowledgments	iii
1 Introduction	1
1.1 Motivation	1
1.1.1 MPesa and financial inclusion	1
1.1.2 MPesa and illiteracy	5
1.1.3 MPesa vs Blockchain	5
1.2 Thesis Goals	6
1.3 Methodology	7
1.4 Thesis Outline	9
2 Fundamentals	11
2.1 Background	11
2.1.1 Architecture	11
2.1.2 Ledger	12
2.1.3 Key management	14
2.1.4 Wallets	15
2.1.5 Bitcoin	17
2.1.6 Lightning Network	18
2.2 Related Work	19
2.2.1 General issues	20

2.2.2	Specific issues	21
2.2.3	Recommendations to mitigate issues	21
2.2.4	Illiteracy	22
2.2.5	Cryptocurrency context	23
2.2.6	Recommendations to improve UX	25
3	Design	27
3.1	User requirements	27
3.2	Architecture	29
3.2.1	Infrastructure and backend services	29
3.2.2	Mobile wallet/frontend	30
3.3	Overhauled user interface	31
3.3.1	Universal changes	32
3.3.2	Home screen changes	35
3.3.3	Receive changes	37
3.3.4	Send changes	39
3.3.5	Confirm screen changes	41
4	Implementation	43
4.1	Galoy mobile repository	43
4.1.1	Stack	43
4.1.2	Apollo client	44
4.1.3	Language	44
4.1.4	Icons and color scheme	44
4.1.5	Structure	45
4.1.6	Changes to home screen	46
4.1.7	Changes to receive screen	48
4.1.8	Changes to send screen	50
4.1.9	Changes to confirm screen	52
4.1.10	hitSlop	53

<i>INHALTSVERZEICHNIS</i>	vii
5 Evaluation	55
5.1 Methodology	55
5.1.1 User Testing Session	55
5.1.2 Video Analysis	59
5.1.3 Quantitative measurements	60
5.1.4 Qualitative Analysis	61
5.2 Results	62
5.2.1 Qualitative observations	62
5.2.2 Quantitative UEQ results	67
5.2.3 Quantitative time measurement results	68
5.2.4 UEQ Feedback	70
6 Final Considerations	73
6.1 Summary	73
6.2 Conclusions	75
6.3 Future Work	77
Bibliography	77
Abbreviations	83
List of Figures	84
List of Tables	86
List of Listings	87
A Contents of the CD	91
B Blink STD, QQ-plots, Shapiro-Wilk tests	93
C AfriBit STD, QQ-plots, Shapiro-Wilk tests	99

D	SetAmount Wilcoxon rank sum test	105
E	HomeScreen Wilcoxon rank sum test	109
F	Blink Usability Form	113
G	AfriBit Usability Form	127
H	Usability form data	141
I	UEQ calculations	145

Kapitel 1

Introduction

1.1 Motivation

1.1.1 MPesa and financial inclusion

The definition of the term **financial inclusion using digital technology** entails the *"[...] deployment of cost-saving digital means to reach populations that are currently financially excluded or underserved with a variety of formal financial services that are suited to their needs and delivered responsibly at a cost that is affordable to customers and sustainable for providers."*, Mhlanga, D.[51], page 5. In other words, financial inclusion provides access to financial services to the unbanked population while delivering these services at a low cost, keeping the balance of profitability for the operator and availability for the customer.

Financial inclusion manifests itself in two different areas: It leads to governmental income growth and benefits general economic stability[51]. It has, therefore, become one of the recent strategies of financial institutions that teach poorly educated societal groups without access to financial products. It is furthermore to be noted that leaving all of the wealth in cash exposes the people to inflation[51]. Consequently, blockchain technology has emerged next to traditional finance and is often seen as its counterpart in the fight to mitigate financial exclusion and inflationary pressure. Over the last few years, the mobile money service *MPesa*, operated by Kenya's largest cellular phone provider Safaricom, has been a major success in Kenya and many African countries[47]. Traditionally, money has been transferred between parties using non-licensed companies such as shared taxis (matatu) or buses and official money-transfer services such as PostaPay[47]. The former transfer method buried tremendous risks of theft and loss of money, while the latter suffered from being inefficient and experiencing frequent cash shortages [47].

Mhlanga, D.[51] mentions that the World Bank estimates that around 31% of the world's adults are unbanked, corresponding to roughly 1.7 billion people. Considering certain emerging nations, the percentage is said to be even higher and interestingly skewed between genders, with up to 61% of adults being unbanked and women accounting for 55% of the unbanked population[51]. According to Medhi et al.,[49], there are fewer people with a bank account than a mobile phone.

Even though the technology is available, many people can not be guaranteed access to reliable payment and banking options. Given this situation, MPesa directly leverages access to mobile phones by providing their mobile money service over Short Message Service (SMS), a functionality almost all mobile phones possess. This approach boosts simplicity and benefits usability, as it allows for easy finding of the application without requiring the user to download any additional software[46]. The evidence gathered by Mbiti et al.[47] suggests that MPesa is utilized as an *additional* tool to the formal banking system rather than completely replacing it. This can be partially attributed to the fact that the monetary supply of MPeas works differently and highly depends on the circulation of the digital e-money[47]. Namely, the money only circulates inside the system after being initially deposited. Hence, the total supply is determined by the extent of these deposits[47]. This digital money can then be transferred between the users, whereas the lifecycle ends with the final withdrawal of the amount[47]. Thus, the system can be seen as an evolving alternative to currency”with ”having aspects of banking”[47].

MPesa offers three basic functionalities, whereas the Subscriber Identity Module (SIM) card provides the security keys for encrypting the function messages end-to-end, as in Mas et al.[46]. The three functions are *deposit*, *transfer*, and *withdrawal*, which are described in detail below.

1.1.1.1 Deposit (cash-in)

By exchanging physical cash for so-called *e-float* at an MPesa outlet, the user can effectively top-up his account[47]. Thereby, the user is only allowed to deposit after being verified using the government identification document (ID), hence, the system underlies the concept of KYC (know your customer), with all deposits being logged by the agent and forwarded to Safaricom[47]. After the customer has handed over the cash to the MPesa agent and the latter has broadcasted the transaction to the network, both parties wait for a confirmation SMS[47]. It is important to note that once the money has arrived in the customer’s MPesa account, it does not pay any interest[47]. Even though all the MPesa e-float is fully backed by commercial banks in Kenya where Safaricom has its accounts, all of the interests paid out on the accounts in these local banks are being donated to charity[47]. The reason for this donation is that it allows Safaricom to offer the MPesa service without falling under the regulations of regular banks since no interest payments are conducted[47]. Furthermore, Safaricom can control how much the service is used as a savings product and with the addition of binding agents exclusively to their company, they gather an even stronger control over the provided services[46].

1.1.1.2 Transfer

Once the e-money has arrived in the account, users can transfer the money to other individual users, businesses who accept MPesa, or even institutions[47]. Since MPesa leverages the phone number as the corresponding account number, transferring is as easy as entering the other party’s phone number, just like writing an SMS[47]. Finally, once the transaction has been broadcasted to the network, both parties receive a confirmation SMS and a new statement of their current balance[47].

1.1.1.3 Withdraw (cash-out)

The money circulation ends with exchanging the digital MPesa money for cash at a corresponding MPesa outlet[47]. To withdraw money from the account, again, customer identification is necessary[46, 47]. This time, the customer has to provide the agent with the phone number and the amount he wants to withdraw, whereas the agent waits for the confirmation message and only then hands over the cash[46, 47].

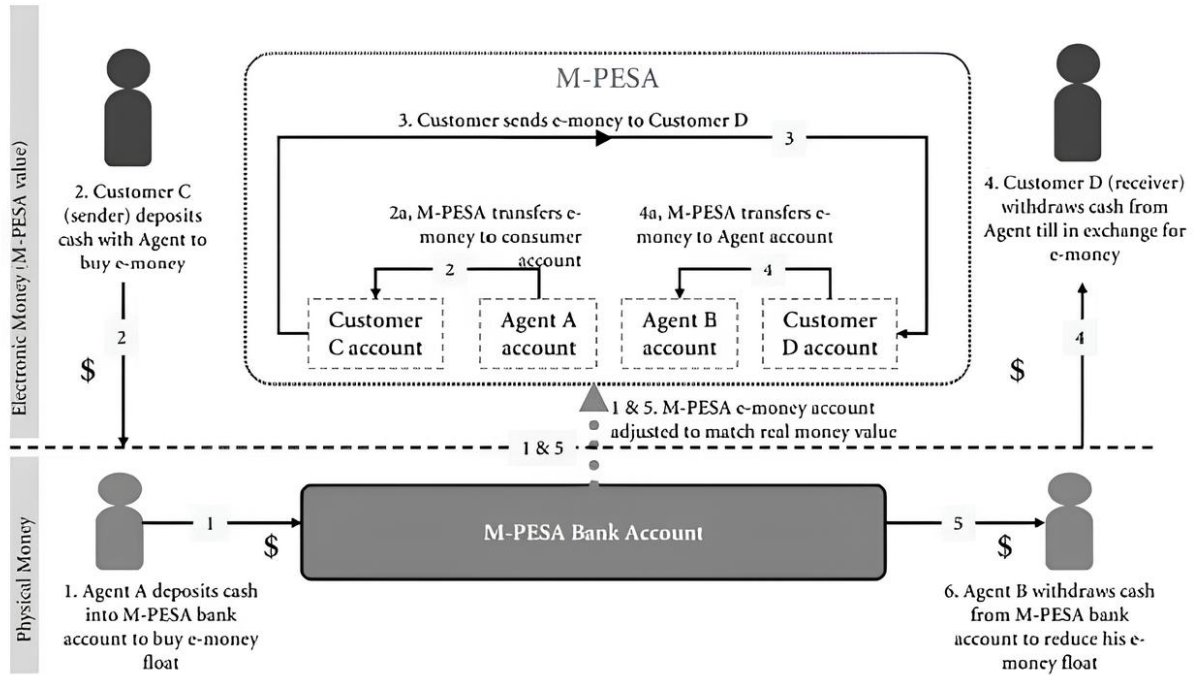


Abbildung 1.1: How M-Pesa works in Kenya, from Prince Muraguri[54]

Figure 1.1 graphically shows the flow of money regarding the above-mentioned functionalities. Given these economic aspects of the services provided by MPesa, it should become evident, MPesa is only rarely used for storing value and evolves more along the lines of serving as a payment system rather than a traditional bank[47]. Not only can this be attributed to the fact that no interest is paid out, but also to the condition that the Central Bank of Kenya does not regulate MPesa, as in Mbiti et al.[46]. However, Mbiti et al.[47] have found in their survey that approximately 26% of the userbase have used or currently use MPesa as a value store. Even though a significant fraction of people use the service to save money, the amount of value stored and the period the money resides in the account are relatively small and almost neglectable[47].

The success of MPesa is not only due to its simplicity and usability but also due to three further aspects summarized below and detailed in their respective subsections:

- **Low-cost:** Users are only charged for transfers and withdrawals; deposits are free
- **Partnerships:** A wide network of Automated Teller Machines (ATMs) ensures smooth operation anywhere in the city
- **Economy:** Local money transfers between family members is a demanded use case

1.1.1.4 MPesa's low cost

Direct deposits are free, given that the amount is at least 100 Kenyan Shillings (KSh) and that the account belongs to the depositor, which is checked by the customer's national ID[46]. No minimum balance is required and no monthly fees are charged, however, transfers, withdrawals, or prepaid airtime top-ups underlie a dynamic pricing strategy, with the fee dependent on the transaction amount[46, 76]. MPesa allows users to send money to registered and unregistered recipients on any mobile network to encourage onboarding and drive adoption. Thereby, unregistered users obtain a code to convert back to cash at any MPesa retail agent[46]. However, some Kenyan residents are still cautious about using MPesa due to previous bad experiences with pyramid schemes or fear of fake MPesa agents[46]. Even though the low-cost solution MPesa has led to competitors such as Western Union and MoneyGram having to lower their fees to remain competitive, the competitors could not compete with MPesa's convenience and simplicity[55].

1.1.1.5 Safaricom's Partnerships

Safaricom partnered with a large and independent network of ATMs, namely Pesa-Point[47]. This has allowed wide access to cash withdrawal without needing big infrastructure investments. Additionally, MPesa has been able to leverage the existing customer network of Safaricom; Mbiti et al.[47] raised data, which constitutes that around 40% of Kenyans (30% of which registered with Safaricom) have signed up for the service.

1.1.1.6 The unbalanced Kenyan economy

The rural-urban divide in Kenya, which is still very prominent to this day, can be attributed to the increased job opportunities in the city, which have led many young male workers to leave their families behind and send money back home to support them[49]. Consequently, local money transfer services between distant family members have gained popularity to overcome this geographical split, especially MPesa[49]. On top of the workers sending money home, people started using MPesa to send money to relatives or even their children in remote colleges[49].

To summarize, the factors above significantly contributed to the shift to MPesa, especially the low costs, which were twice as cheap as other formal money transfer services such as postal money[49]. Mhlanga, D.[51] states that lowering costs boosts the perceived usefulness and ease of use of digital banking alternatives and positively influences financial inclusion. Even though the low costs could not beat informal money transfer alternatives such as family and friends from a cost perspective, the pace of uptake has been significantly higher compared to other solutions[49]. Primarily this came thanks to the gained trustworthiness of service, which was mainly established by employing clear marketing and leveraging the "*[...] strong pre-existing ties with the local prepaid talk-time agents [...]*", as in Medhi et al.[49]. As an outlook for future mitigations of financial exclusion, Mhlanga, D.[51] puts forward that Schuetz and Venkatesh[70] established four pillars of dealing with financial exclusion: *geographic access, high cost, inadequate banking products, and financial illiteracy*, as stated by Mhlanga, D.[51].

1.1.2 MPesa and illiteracy

Touching upon illiteracy, even though MPesa has been a great success in Kenya, some usability problems remain evident. Medhi et al.[49] have conducted qualitative observations and interviews across multiple countries, including South Africa and Kenya. In their ethnographic exploration, they primarily focused on how existing mobile banking services are being used by low-literate and low-income personas[49].

One of the shortcomings of existing mobile banking services has been their extensive use of hierarchical menus. Out of the 90 individuals in the study by Medhi et al., 56 subjects were unable to grasp and comprehend the hierarchical navigation structure of the applications[49]. Given that 40 out of these 56 participants have never used a mobile phone before, it seems like, especially for new users, hierarchically nested information and interaction is hard to make sense of[49]. This can be mainly attributed to the fact that the users lacked an abstract hierarchical mental model, thus not being able to grasp the structure of the menu[49]. Adding to the problem are menus nested deeply or where the categorization was done on uncorrelated functions, making it harder for the users to predict but also find certain functions[49].

One benefit of MPesa is that the interface is not only in English but also offers Kiswahili as a language option, allowing subjects with limited knowledge of the English language to use the system[49]. Nevertheless, participants in the study by Medhi et al.[49] who could not understand the system's language showed great understanding of the use of numbers[49]. Usability problems arose not because the people did not understand what the numbers stood for, but instead, because they struggled with the specific terms used in banking systems, especially if they were unbanked[49]. Concepts such as "Send transaction", "Change Personal Identification Number (PIN)" and so on were foreign and lacked a detailed explanation[49].

1.1.3 MPesa vs Blockchain

To this day, MPesa remains largely centralized, initially funded by Vodafone and operated by Safaricom[47]. On one hand, this benefits the consumer, who can access the SMS-based service without installing any additional software[46]. On the other hand, this leads to exclusion, as users must have a valid Safaricom SIM card to use MPesa, the reason being that the phone number serves as the account number and the SIM card's security keys are needed for the service[46]. Combined with the need for a government-issued identification card (ID / Passport), the above-stated restriction clearly shows the exclusion of certain people from the service.

Mhlanga D.[51] states that Danho and Habte[13] see blockchain as helpful for mobile financial services. Thereby, Danho and Habte[13] have examined the increased access to financial services in Africa thanks to blockchain technology[51]. Since most blockchains are not bound to a specific provider, such as MPesa is bound to Safaricom, they are more accessible to the general public. Furthermore, blockchain technology rarely requires users to identify themselves via an ID or passport, lowering the onboarding barrier.

To conclude, the problem of financial exclusion is multi-faceted and originates from various factors. The service MPesa provides a solution to mitigate some financial exclusion and offers the possibility of accessing mobile banking services. However, all of the above-mentioned shortcomings of the MPesa service demand a novel solution accessible to everyone and promoting financial inclusion. Thereby, the fundamental concepts and functions existent in MPesa shall be preserved, namely the deposit, transfer, and withdrawal of money. If and only if the new service can provide greater or equal functionality whilst offering an improved user experience (UX) than the one of MPesa, it can be deemed a viable alternative. MPesa has established itself to a point where customers will not switch to a new service with less functionality or worse UX.

1.2 Thesis Goals

Given the considerations of MPesa, this thesis investigates using and adopting blockchain technology for financial inclusion in Kibera, a region in Kenya, to serve as a feasible alternative to MPesa. Thereby, the approach taken shall align with the principles and practices of POC and HCI. The Ronnie Fund[48], a local Kibera project, offers programs based on community initiatives, one of which is the initiative by Yogi Golle, the Information and Communications Technology (ICT) academy[19], which aims to educate people in the field of technology. To aid the thesis in reaching its goals, Ronnie's social network shall be leveraged with the ultimate goal of establishing a circular economy where suppliers, retailers, and customers utilize Bitcoin as a method of savings and transactions within the neighborhood. The goals of the thesis are as follows:

1. **Adapting the design** *of an existing mobile user interface (UI) to the Kibera region*
It was decided to target mobile phones because their use and needed infrastructure are widely spread in Kenya
2. **Implementation of the design** *in a functional mobile application prototype*
The design shall promote an accessible, user-friendly interaction, promoting financial literacy and inclusion
3. **Quantitative and qualitative evaluation** *of the prototype and its design*
The changes must be evaluated regarding their effectiveness and if they fulfill the requirements
4. **Development of a point-of-sale (PoS)** *system for merchants and businesses*
A PoS interface would allow merchants and businesses to receive payments easily and keep track of their revenue stream

Due to the extensive time required to implement, onboard merchants, and evaluate another interface, the goal of implementing a PoS was later deemed out of the thesis's scope and dropped. Overall, even without the PoS interface, the thesis can significantly add to the discussion of blockchain technology's potential for financial inclusion, particularly in African populations that are already well familiar with MPesa or other digital money transfer services.

1.3 Methodology

For many Western countries, it is seen as usual to have access to a functioning banking system and a bank account for savings and worldwide money transfers. Cryptocurrencies could reduce the need for physical banks by providing a digital currency that fulfills the properties above, irrespective of Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations. Additionally, certain types of currencies, such as the synthetic US-dollar *Stablesats* provided by Galoy[32], can sometimes serve as a protection against inflation. The inclusion of such a currency dramatically drives daily adoption, allowing users to transact in a stable, US-dollar (USD) denominated currency. However, the principles behind cryptocurrencies can also pose significant barriers to populations with limited technological understanding and should not be underestimated in their complexity.

Literature review: The first step to achieve the goals of this thesis is to gather an overview of the basics of financial inclusion challenges and opportunities, particularly in regions such as Kibera and concerning cryptocurrencies. A solid understanding of the conceptual components of creating an intuitive UI for cryptocurrency-based financial services is vital to the interface's usability. This insight establishes a baseline with the traditional financial systems, outlining a cryptocurrency-based approach's unique advantages and challenges in providing financial inclusion. Financial inclusion thereby refers to the ability of every individual, irrespective of their societal status, to access suitable, affordable, equitable, and secure financial products and services from mainstream providers[79]. Since this thesis aims to design and develop an iPhone Operating System (IOS) and Android app to interact with the Bitcoin Lightning Network, the app shall mitigate the four key factors that have hindered financial products in the specific region of Kibera:

- **Geographic access:** Many of the slums across Africa do not have access to a bank account since there is no local bank nearby
- **Illiteracy:** A certain percentage of the Kibera population is unable to read or write the alphabet, posing a significant barrier to adopting digital financial services, including the many existing Bitcoin wallet apps
- **Government identification:** For opening a bank account, possessing a government identification document is required, which many may not have
- **Inflation:** The region of Kibera is experiencing severe inflation, discouraging residents from saving money since the purchasing power reduces over time

While most Bitcoin wallets target developed economies or literate people, the novel aspect of this thesis is the implementation of an area-specific Bitcoin wallet, that is tailored to the requirements and provides a possibility to mitigate the above-mentioned problems, especially among people who may be illiterate. Ultimately, the application shall increase the range of people engaging in the digital economy. As a point of reference, the application's functionality should be similar to the well-known Twint application in Switzerland[3], allowing both to send and receive money effortlessly.

Applied research: As a second step, the wallet’s UI must be designed with respect to the inclusion parameters mentioned above. This includes defining the features, changes, and reasoning before designing the application’s interface. After these requirements are gathered, Framer[8], a tool to facilitate rapid and straightforward interactive interface design, will be used for the prototyping phase. The newly created designs will be shared with the target audience and the development team, whose feedback will be incorporated as best as possible into the design process.

The third step is to develop the wallet, whereas Galoy, a Bitcoin-native banking infrastructure that offers various security features, will be used as the basis. Furthermore, the application should be based on an existing solution proven to work in El Zonte, El Salvador. By doing so, it is assured that the customer funds are treated with adequate security measures and that this thesis does not underlie severe coding mistakes regarding key management. Hence, this thesis will fork the frontend by Galoy[30], which uses React and Typescript. This was done to reduce the implementation overhead and focus on improving the UI to match the requirements and capabilities of Kibera’s target users. The mobile application in question is the Blink wallet, formerly known as the Bitcoin Beach Wallet (BBW)[28], an open-source project from which vital insights can be harvested and from which existing security-audited code can be leveraged. The new wallet will be called *AfriBit wallet* which depicts a combination of the words *Africa* and *Bitcoin*, matching the target group. The goal is to improve the existing Bitcoin Lightning Wallet’s UI design, allowing unfamiliar users to experience banking services seamlessly. Thereby, React[24], a well-known JavaScript toolkit for creating user interfaces, and TypeScript[52], a typed superset of JavaScript, will be used to implement the front end of the digital wallet. The Galoy[31] stack, a banking infrastructure built from the ground up for Bitcoin, will handle transactions and control security measures. This combination produces an application architecture that is reliable, effective, and secure such that the thesis can put more weight on the application’s design.

Once the prototype is developed and functional, it can be tested for its effectiveness in mitigating the challenges. Therefore, a user study where participants interact with the application will be conducted and quantitatively evaluated. Thereby, the users will walk through the application and perform a series of tasks using the prototype. At the end of the user study, participants should complete a usability form to collect feedback on a semantic differential scale[64]. The later analysis of this questionnaire should allow for clear insights into the usability and UX of the application. Furthermore, time measurements serve as a basis for the statistical analysis of evaluating the prototype’s implementation in real-world scenarios. These timestamps will be crucial in determining if the new UI slows the participants down or demonstrates an actual usability increase. Additionally, the user study explores qualitative feedback and observations from the hands-on sessions, highlighting challenges users might encounter when utilizing the system. The application’s design will need to be refined and improved over time, and these insights will be essential. Therefore, the design will be provided to the Kibera target group before the codebase’s actual development to gather initial feedback in an agile fashion. By gathering user feedback, survey responses, and usability metrics to assess the system’s usability, it is ensured that potential user challenges are identified and that the developed interface is easy to use, even for individuals with limited technological knowledge or shortcomings in reading and writing.

1.4 Thesis Outline

Chapter 1 has delved into the insights of the reason why the work presented in this thesis is necessary. It evolved around the gathering of the context and elicitation of the problems at hand. The highlighted problems and the provided context show that an alternative solution to MPesa could benefit previously excluded groups of people. In **chapter 2**, the background information needed to understand the benefits and drawbacks of a novel solution will be elicited. Thereby, technical aspects are introduced in detail and clarified in their meaning, serving as the theoretical foundation of this work. Secondly, previous research and work done in this field will be shed light upon, mainly highlighting the challenges of new solutions. Thus, the chapter focuses on collecting the technical and theoretical background knowledge and concepts to understand the work presented in this thesis. **Chapter 3**, the insights from the fundamentals will be used to build upon the conclusions and lessons learned. Using these concepts and findings from other studies, this chapter comes up with a design that mitigates common and area-specific issues and gives insight into the process of the choices made. Following, **chapter 4** presents the implementation of the design in functional prototypes and contrasts the output with the region-specific requirements. It elicits the thought process and considerations in the technical implementation of the design into a functional state and highlights deviations between the design and the implementation itself. **Chapter 5** will evaluate the progress made, both quantitatively and qualitatively, serving as feedback if the introduced changes of the prototype are beneficial or not. The last **chapter 6** will conclude this thesis with a retrospective view of what was achieved and where major issues revealed themselves. The closing thoughts take into consideration all of the work conducted, including the reflection on insights from the user study.

Kapitel 2

Fundamentals

2.1 Background

2.1.1 Architecture

2.1.1.1 Distributed System

Distributed systems consist of two or more computers (so-called nodes) that communicate with each other over a network[9]. The nodes coordinate their work and processes to achieve a shared goal[9] collectively. Thereby, a so-called master node takes care of the coordination in the system and acts as a central authority; therefore, the system underlies the concept of hierarchy[73]. In blockchain technology, the nodes pass around messages and replicate the data. However, to the end user, the system appears as a whole, coherent structure[9]. In other contexts unrelated to the blockchain, the nodes can also have shared memory instead of passing around messages[9]. Message-passing systems replicate the data, whereas the nodes underlie two significant challenges: Coordination and fault tolerance[9]. The underlying technology used in this thesis heavily depends on the concept of distributed systems. Hence, this architectural structure is of essence to the thesis.

2.1.1.2 Decentralized System

Like a distributed system, a decentralized system consists of two or more nodes[9]. However, in a decentralized system, no central authority controls the system, unlike in distributed systems[9]. Instead of having single master nodes, all nodes are treated equally, and the control is spread amongst many nodes[9]. This results in a network without hierarchy where all nodes propagate transactions (Tx) and blocks and validate their state[5]. Since blockchain technology is built upon the design principles and foundation of distributed systems, the latter plays a vital role in this thesis.

2.1.2 Ledger

2.1.2.1 Blockchain

Blockchain technology is built upon a combination of distributed and decentralized systems, boasting properties of both paradigms and representing a structure where the system's state is defined by the majority of the involved parties[9]. This control is achieved by having each participant hold a copy of the shared data, explained in section 2.1.2.2, and vote on changes to this data[9]. The word blockchain can be broken down into two parts: block and chain. Thereby, the blocks contain data, in the case of Bitcoin, one or more transactions, the first being the coinbase transaction, whereas each block is identified by a secure hash algorithm (SHA) hash[5]. Thanks to this identifier, the blocks can be chronologically ordered by having each block contain the hash of the previous block[5]. This results in the chain of blocks, the blockchain, where each block is linked to the previous one, and the order can not be altered in any way, thus each block and the contained transactions being immutable and the system operating in an append-only manner[5, 9]. In the geographical context of this thesis, the underlying blockchain technology is vital for the financial inclusion of people in developing countries, exhibiting constant availability, irrespective of the geographical location of the identification of the user. Combined with the possibility of providing a USD-denominated synthetic dollar, it allows for a system in which the main problematic aspects of Kenya, concerning banking, can be mitigated. The study by Schuetz and Venkatesh[70] has shown that in developing countries, blockchain technology can be used to foster financial inclusion, in this case, India.

2.1.2.2 Distributed Ledger

The ledger is a data structure that contains all transactions that have ever been made on the network and, ultimately, in the context of blockchains, is cryptographically secure[9]. A ledger in terms of blockchain is often considered a distributed ledger, allowing data origin authentication, data integrity, and non-repudiation[9]. In this ledger, all balances and transactions are recorded and stored in chronological order[4]. This means that each network participant holds an identical copy of this ledger where, in the Bitcoin scenario, it is updated roughly every 10 minutes[4, 9]. Since all participants of the network hold a copy of the ledger, such an update only happens if the majority of the network has verified that the transactions are valid, no double-spending has occurred, and the balances are correct[4]. This is especially important concerning finality, which refers to the fact that a transaction is irreversible once it has been confirmed by the network[9]. The longer the transaction dates back in the Bitcoin blockchain, the less likely it is to be reverted or rolled back[9]. This allows for a system that is based on verification instead of trust, where the validity is determined by the individual nodes, not a single authority, and the ledger is temper resistant[4, 9]. For large payments, this is of vital interest; for smaller payments, updating the ledger is cumbersome since it has to be updated by using a consensus mechanism, which is both time and energy-intensive, especially in the case of Bitcoin[9]. Therefore, these smaller transactions will likely not be conducted using the distributed ledger but through second layers[4].

2.1.2.3 Layers

Layer 1 (L1) is called the base layer chain and is responsible for consensus. For example, Bitcoin and Ethereum are considered L1 blockchains[5]. Recent research and advancements in the scalability of blockchains have pushed the adoption and expansion of Layer 2 (L2) solutions and architectures[9]. Scalability thereby refers to the capability of adapting to increases in utilization and demand[9]. L2 solutions are built on top, complementing L1 chains without the need to change them in any way. However, L2 handles transactions off-chain and only refers to Layer 1 for settlement and consensus[9].

2.1.2.4 Consensus

One of the most fundamental innovations in terms of decentralized systems is the decentralized consensus, introduced by Satoshi Nakamoto in 2008, a way to determine which node gets to append the following block to the chain[4, 9]. It proposes a possible solution to the Byzantine Generals' Problem (BGP) by using Proof-of-Work (PoW) to establish a consensus between parties that do not need to trust each other[5]. The PoW mechanism is considered a Sybil attack defense mechanism instead of a consensus algorithm, according to Bashir, I.[9]. A Sybil attack is also known as a 51% attack, which refers to the situation where a single entity controls more than 50% of the network's hash rate and, therefore, of the nodes involved in achieving consensus[9].

It is essential to know that there are several types of consensus mechanisms, each with advantages and disadvantages. The main difference between the consensus mechanisms is the underlying trust premise, whereas with the introduction of the PoW consensus mechanism, Satoshi Nakamoto has solved the double-spending problem while ensuring that no third party must be trusted[5, 9]. Therefore, the PoW consensus mechanism is an excellent solution to the BGP, primarily since its trust premise is based on the assumption that the majority of the network is honest[9]. The consensus is said to be emergent, which means that there is no fixed point in time when it is reached, and there is no election of a leader; it is a probabilistic and not deterministic solution[5, 9]. This is due to its nature that the PoW consensus has to be conducted in a brute force approach, where the nodes have to guess a random number (the nonce) until the hash of the block is below a certain threshold[9]. This threshold is referred to as the difficulty, which is the amount of leading zeros the hash has to start with[9]. Instead, nodes interact with each other and race to find the solution to a mathematical problem, where the first one to find it is the only one being rewarded[5]. It is one of the most fundamental concepts for solving a significant mathematical problem, a system in which no third party or intermediary must be trusted[9]. Understanding the consensus mechanism is needed to comprehend the current drawbacks of existing and currently used blockchain systems. Throughout the thesis, these shortcomings of employed systems will be highlighted, analyzed, and explained.

2.1.3 Key management

2.1.3.1 Private key

The private key in itself is nothing different than a large number[5]. Ideally, it is randomly generated in a way that can not be reproduced and is kept secret by the persona to prevent unauthorized access[5]. For each private key, there exists a unique public key, elicited in section 2.1.3.2, whereas both of them are referred to as a key pair, generated by Public Key Cryptography (PKC)[5]. This key is the most important since it is in complete control of the funds and since other keys are generated based on it[5]. Thanks to its use for digital signatures, which a decentralized network can validate, the private key serves as a way of authorization over the funds of a specific holder[5]. Digital signatures are therefore used to associate data origin with an entity, in this case, the private key holder who created the signature[5].

2.1.3.2 Public key

The public key is derived by applying elliptic curve cryptography to the private key. Consequently, the public key can be freely distributed without risking that the associated private key of the key pair can be derived[5]. This is because the function is designed to be one-way, meaning it is easy to derive the public key from the private key, but not the other way around[5]. However, in a publicly available and open system such as Bitcoin, sharing public keys risks being linked to the holder's identity, thereby sacrificing privacy[5]. This thesis will leverage the basis of the whole key management process of public keys to allow for the reception of funds in connection with the user survey and experience testing sessions. It is vital to know that a public key is derived from a private key. This highlights that only the person in control of the private key can spend the funds associated with a given public key.

2.1.3.3 Address

The address serves the purpose of being a human-readable representation of the public key and allowing for the identification of senders and recipients of funds[9]. In the case of Bitcoin, these addresses begin with the digits 1 or 3 and are usually between 26 and 35 characters long, based on Base58 encoding[9]. To get to the address from the public key, again, a cryptographic one-way hash function is applied[5]. When looking up an address on a blockchain explorer, all funds and transactions associated with this address are visible to the public. A blockchain explorer is a tool to search, explore, and see relationships between addresses, transactions, and blocks on a blockchain, similar to a search engine like Google[5]. Addresses play a crucial role in receiving funds in a human-readable format. Therefore, they were used in the user testing.

2.1.4 Wallets

For example, a Bitcoin wallet is an abstraction of a digital collection of key pairs, whereas each pair consists of a private and public key[5]. These keys are used to interact with the blockchain, such as to receive, send, or sign. Since cryptographically, these keys determine ownership, it is vital to safeguard them. For this purpose of safeguarding, multiple types of wallets exist. Even though different vendors and platforms operate multiple types of wallets, the vital aspect is that they all allow the user to interact with the same underlying system, the blockchain. Therefore, almost all wallets that allow the receiving and sending of Bitcoin are compatible and interoperable. Exceptions are wallets operating on a different network or blockchain, such as the Lightning Network.

2.1.4.1 Desktop wallet

Desktop wallets date back to the early days of Bitcoin, where the most prominent desktop wallet for Bitcoin was and remains Bitcoin core[11]. Desktop wallets are desktop applications meant to run on popular operating systems such as Windows, MacOS, and Linux[5]. Desktop wallets are generally not considered the most secure type of wallet, mainly because of the security disadvantages of the underlying operating system[5].

2.1.4.2 Mobile wallet

In the current state of the world, mobile wallets are the most widely used form of the Bitcoin wallet since they are installed on mobile devices[5, 9]. Especially for new users, the easy access, fast onboarding, and mobility of mobile wallets are a great advantage[5]. Important to note is that there exist two types of wallets with different levels of custody:

- **Custodial wallets** refer to a form of wallet where the user’s private key is stored on a server, often owned by a third party. This inherently means that the user does not have complete control over his funds, as the third party manages them. However, this tradeoff benefits the user by allowing them to avoid dealing with key management, effectively enlightening the user experience.
- **Non-custodial wallets** allow users to manage their private keys themselves. Thereby, the user has more control and, in return, more responsibility.

Mobile wallets and their underlying security aspects are essential in this thesis since the target group of the application is people with little to no experience with financial products and services. Furthermore, the target group has limited access to desktop computers; however, mobile phones and their infrastructure use are widespread. Therefore, a custodial mobile wallet was chosen to be improved in terms of usability and UX, especially since custodial wallets are better suited for beginners. Additionally, one notable improvement of mobile wallets compared to other wallet types is the ability to use the internal camera of the mobile device, which allows for scanning a Quick Response Code (QR code) to execute a payment[9].

2.1.4.3 Web wallet

Like custodial mobile wallets, web wallets refer to wallets where a third party manages the private key[5]. Web wallets, as the name suggests, can be accessed over a browser interface[5]. This is analogous to webmail, where the user can access his emails stored on another server over a web browser[5]. Some web wallets function like non-custodial wallets, where client-side code running in the browser handles key management and, therefore, allows the user to be in control of their keys[5].

2.1.4.4 Hardware wallet

Hardware wallets offer to store the private key on purpose-built hardware, such as a Ledger or Trezor hardware wallet[5]. Since all Bitcoin-related operations, such as signing, are done directly on the device's hardware, the private key does not have to leave the hardware[5]. Therefore, these devices are believed to be very secure[5].

2.1.4.5 Backup and recovery

Each of the wallets mentioned in 2.1.4.1 to 2.1.4.4 offers different levels of recovery and backup for the wallet and its associated funds. Backing up a wallet refers to the process of saving the private key or a way to construct the private key to be able to restore the associated funds at a later point in time. Backup and recovery is a vital process in the whole blockchain sector and has to be assured to be taken seriously. Therefore, it also plays an essential role in this thesis since people need access to their funds to ensure recoverability. Since it was decided to use a custodial wallet, the recovery process of the funds is possible through a mobile phone number and via email. This dramatically reduces the burden on people who may be illiterate or have little experience with financial products and services like Bitcoin.

2.1.4.6 Wallet invoice

In order to receive funds, the sending party of the transaction needs to know which address to send the funds to. Instead of exchanging only the address, a wallet invoice can be used to facilitate the process of sending funds[5]. Thereby, the wallet creates a payment request in a standardized format, which can then be shared with the sender[5]. This standardized format, in this case, a Uniform Resource Locator (URL) with parameters, can be encoded into a QR code which the sender can then scan. When scanning the QR, the wallet will automatically pre-fill the amount and address fields[5]. This thesis will also leverage this concept of wallet invoices to facilitate the process of sending funds when dealing with user testing.

2.1.5 Bitcoin

With the introduction of digital cash, Satoshi Nakamoto provided the first functioning digital good that can not be copied and is scarce by design[4]. Thanks to the underlying cryptography, once Bitcoin is transferred, the sender holds no ownership over the funds anymore[4]. Given the ability to send amounts over geographical borders in a matter of minutes and at a low cost, Bitcoin allows people to send and receive money without the permission of anyone else[4]. Thereby, Bitcoin lowers financial exclusion by providing access to international money transfers to people without a bank account or people who experience restrictions in their banking sector[4]. Combining the interconnectedness and global scale of the network with the scarcity of Bitcoin, this asset also makes for a great store of value, sometimes allowing to escape the local inflation in certain countries[4]. This is especially evident thanks to Bitcoin's fixed supply of 21 million coins, which can not be changed by anyone and represents a predictable issuance[4]. The underlying technology of Bitcoin is of essence to this thesis since it allows for the transfer of funds in a fast and low-cost manner[9]. Furthermore, the underlying infrastructure, technology, and terms of Bitcoin are used in the user experience testing sessions, making it essential for the context of this thesis.

2.1.5.1 Transaction

Generally, in blockchain technology, a transaction refers to transferring a digital unit from one address to another[5]. The sender's private key signs the transaction, proving the funds' ownership. The advantage of these transactions is that they are final and fast, allowing for the settlement of vast sums of money in a matter of minutes, irrespective of the geographical location of the sender and receiver[4]. To verify a transaction, three conditions have to be fulfilled, each of which is checked by the nodes in the network:

- The transaction outputs are previously unspent (prevent double-spending)
- The sender's sum of transaction outputs is smaller or equal to the sum of the inputs (prevent spending more than available)
- The digital signature is valid (proof of ownership)

Thereby, an unspent transaction output (UTXO) refers to a positive balance, an output of a previous transaction that has not yet been spent. Before the nodes can verify a transaction, the transaction must be constructed in the wallet of choice[9]. To construct, sign, and then broadcast the transaction, the wallet needs the Bitcoin address of the beneficiary, the amount, and the fee to be set[5]. Once the transaction is successfully broadcasted to the network, the miners[12] will verify and confirm it by including it in a block[9]. When the block, including the transaction, is appended to the blockchain, the fee is paid to the miner who mined the block[9]. A transaction is viewed as final as soon as six confirmations have passed, or in other words, six blocks have been mined on top of the block containing the transaction[9].

2.1.6 Lightning Network

The Lightning Network aims to solve the scalability issues of Bitcoin without compromising the security principles of Bitcoin, achieved by delaying the settlement of a Bitcoin transaction[60]. Two parties commit funds to an address, of which they can update the balance as often as they want[60]. Only two states are needed: The current correct distribution of the balance between the parties and the old deprecated balances[60]. At any point in time, either party can broadcast the latest balance to the blockchain, thereby settling the transaction[60]. The above-described scenario represents a bidirectional, end-to-end encrypted payment channel between two parties[5]. Instead of creating a payment channel with every participant, all channels form an interconnected network through which transactions can be routed[5, 60]. Therefore, the sender does not have to have a direct channel with the receiver and can rest assured that no intermediary node knows source or destination[5]. Combined with only broadcasting the minimum required information to the Bitcoin blockchain, this layer allows for almost instant settlement and has shown to be highly scalable while keeping transaction fees low[26, 60].

2.1.6.1 Payment channel

For a node to send money to another node, a payment channel has to be established between the two parties[5]. This connection is only known to the two parties, and the participants only see the payments in their respective channels[5]. An advantage of these payment channels in comparison with regular on-chain Bitcoin transactions is that they offer the possibility to send amounts as small as the smallest discrete indivisible unit of value, known as a single Satoshi (SAT)[5].

2.1.6.2 Routing

If a node wants to send money to another node and no direct payment channel exists between the two parties, the payment is routed through the network[5]. A path with sufficient capacity needs to be found, and the payment propagated through the network[5]. This is achieved using nested and encrypted instructions, allowing the nodes to connect adjacent payment channels, resulting in a route from the sender to the receiver[5]. Since these instructions are encrypted, the nodes do not know the source or destination of the payment; they only see the adjacent nodes[5].

2.1.6.3 Payment infrastructure

The result of routing the payment channels is a network that offers excellent privacy and a trustless operation between the peer nodes[5]. Furthermore, the payments conducted through the network are not public, unlike the payments on the Bitcoin blockchain[5]. Since the transactions are not committed to a block, the payments are fast, scalable, and cheap[5]. The capacity is, therefore, only limited by the speed and the number of payments a node can be routed through[5].

2.2 Related Work

The landscape of already conducted work in the UI improvements of a Bitcoin wallet is rather sparse and lacks documentation. There are some wallets for low-cost mobile phones, such as the SMS wallet presented by Dlamini et al.[14]. Still, the papers generally focus on the usability of Bitcoin wallets but rarely touch upon the specific UI elements and workings. The focus of existing papers lies more in *eliciting* usability issues, challenges, and recommendations rather than implementing and evaluating the proposed changes[17]. Additionally, Froehlich et al. observed that no study evaluated the usability over an extended period[17].

An overview of the essence of the available literature is provided by Froehlich et al.[17], who have systematically analyzed blockchain and cryptocurrency in human-computer interaction (HCI). Relevant findings include that the data sourcing is primarily done through interview studies and questionnaires, whereas quantitative studies have been the primary indicator for exploring the demographic distribution of cryptocurrency users[17]. Thereby, Froehlich et al. had 34 inexperienced users trying out custodial wallets and noted their findings.

The participants in their user study were advised to gather experience with three different wallets, whereas Froehlich et al.[18] proposed grouping the conceived challenges into the following three categories:

- **User interface challenges**

These challenges and issues arose due to the design choices of the UI[18]

- **Finance challenges**

Financial challenges represent issues related to the offered financial services and products of the application[18]

- **Cryptocurrency challenges**

This category refers to issues related to the underlying technology and concepts of cryptocurrencies[18]

Froehlich et al.[17] extend these categories by proposing a grouping of risk categories in the context of cryptocurrencies:

- **Risk of human error**

Human errors include all sorts of problems that can be attributed to the user's behavior, such as typos, mismanagement, and forgotten passwords[17]

- **Risk of betrayal**

Betrayal refers to the risk of misplacing trust in a third party, such as a wallet provider or exchange[17]

- **Risk of malicious attacks**

This category subsumes issues related to malicious actors, such as theft, fraud, and scams[17]

Having conducted a broad literature review of cryptocurrency and blockchain in the field of HCI has enabled Froehlich et al.[17] to summarize frequent misconceptions from the other studies from Froehlich et al.[16, 18]:

- **Key management**
While some users prefer complete control over their funds, others, especially beginners, do not understand how vital their backup phrase is and struggle with its recovery mechanism[17].
- **Addresses**
New users often associate addresses with the concept of email addresses; however, their length and randomness make them hard to handle or even memorize[17].
- **Transactions and fees (and how they relate)**
For many it is unclear how transaction fees influence the speed of a transaction and how they are calculated[17].
- **Security**
Beginners struggle with securing their funds and that transactions are irreversible[17].

Froehlich et al.[16] note that people with low knowledge and low motivation tend to prefer custodial wallets since their perceived user error is higher. Furthermore, custodial wallets present an excellent opportunity for novice users as they allow for more convenient use[16].

2.2.1 General issues

Generally, issues related to the UI in the field of HCI are mainly attributed to the poor layout and structure of the interface[18, 78]. Furthermore, a general lack of guidance, inaccurate information, or even ambiguous system status add to the perceived complexity and increased issues[18, 78]. Making matters worse, technical jargon hinders usability[53] but, at the same time, is (to some extent) necessary to convey the underlying concepts. Dealing with the topic from a people-oriented computing (POC) perspective, issues such as typos[78], misaligned color schemes[78] and generally confusing icons and naming[18, 78] also contribute to the usability aspect of mobile banking applications. To add to the overall problem, ill-designed error messages also pose a frequent problem that is even further enhanced since the user can not contact a bank or similar to resolve the issue or get support[18]. Voskoboynikov et al. acknowledge the issues related to error messages and thereby put great emphasis on the recoverability of errors[78]. In the same paper, Voskoboynikov et al. also advise constructing cryptocurrency wallets similar to already existing online banking and payment systems[78]. It has been shown that users tend to be more cautious when dealing with new systems. Therefore, it is vital to make the users feel familiar[78]. This correlation between already-known financial systems and new cryptocurrency wallets is also drawn upon by Froehlich et al.[18]. The nature of Bitcoin has brought many new challenges, whereas the high price volatility is reported to be one of the most hindering factors[18]. Both for daily transactions and due to the constant need to update the exchange rates, this volatility has greatly negatively impacted its adoption[78].

2.2.2 Specific issues

Current applications suffer from leaving users confused about the current state of a transaction[18]. Hence, it is vital to immediately display transactions, regardless of whether they have been confirmed or not[18]. Other studies suggest that the status of *pending* transactions is often misunderstood, because the user is unaware of the underlying concepts, such as that an already broadcasted transaction can not be cancelled[78]. In POC, such an issue can mainly be attributed to an inaccurate mental model of the users who expect transactions to be reversible[78]. On the topic of transactions, it has been observed that most applications lack the ability to re-submit a transaction[80], This effectively results in stuck transactions submitted with a too-low transaction fee[78]. This is where a major differentiation between non-custodial and custodial wallets is made. Whereas custodial wallets boost usability by abstracting technical underlying concepts, non-custodial wallets largely expose these technicalities[16]. For users who are confident with dealing with key management, non-custodial wallets are vital in offering this option, rather than having the key pairs generated in the background without explicit mention or the ability to export and import[16]. This can be done through simple backup reminders that ask the users to export their seed phrase and verify that they have stored it correctly to ensure they still have access to the funds in question[78]. Generally, not having the key pairs visible or in control of the user is seen as a restriction for the more advanced users[16]. On the other hand, key management is seen as a burden by the less experienced users, which leads to poor usability for them[16].

2.2.3 Recommendations to mitigate issues

Proposed recommendations are to promote the benefits of cryptocurrencies[38] while also ensuring a transparent system with enough control in the user's hands. Furthermore, the user shall be supported in his learning journey by incorporating some form of gamification[18]. Froehlich et al.[17] also suggest that sensitivity to time acts as a fundamental temporal orientation for meaningful user experiences when designing interactions with blockchains. Most importantly, they note the vital criteria of *allowing* the users to manage their keys by themselves to fully reap the benefits of blockchain technology[17]. Even though this imposes a barrier for novice users, previous research by Froehlich et al.[16, 18] shows that experienced users deem key-export a vital feature. This shows that the userbase of such mobile cryptocurrency wallets is a diverse group with different needs and behaviors[78]. Therefore, it is vital to tailor the application to the needs of the users of a specific group[16, 18, 78] and their different use cases, providing a smooth learning curve for novice users[16]. As suggested by Froehlich et al., the users shall be guided toward a safe transition from custodial to non-custodial wallets[17, 78]. An example of a more advanced scenario of complex transactions could be the replace-by-fee functionality[78]. This feature has been a hurdle for multiple users in the app store review conducted by Voskoboynikov et al.[78] and was also pointed out by Froehlich et al.[17]. Thereby, Voskoboynikov et al.[78] have analyzed 6859 reviews relating to UX issues. The replace-by-fee functionality allows the user to re-submit a transaction with a higher transaction fee to speed up the confirmation process[78].

The main issue is that this transaction is complex, as it has to be resubmitted but with a higher transaction fee[78]. This process of overwriting the transaction should, in a best-case scenario, be automated, such that the user does not have to deal with the technicalities but can press a button[78]. Voskoboynikov et al. emphasize that in such an automated case, the user must be informed that the transaction fee must be paid for both transactions[78]. The user interface is designed dynamically to avoid stuck transactions or interceptions[17]. Therefore, Voskoboynikov et al. recommend that transaction fees shall be customizable by the user whilst offering recommendations of average fees of recently processed transactions[78]. Due to the extensive knowledge needed in this scenario, it is not the main focus of this thesis, which aims to provide usability enhancements for users with little to no knowledge or experience with financial products and services.

2.2.4 Illiteracy

Touching upon the topic of illiteracy and shifting the focus from a more technical perspective to a more human-centered perspective, the illiteracy of certain users remains a challenge. Mesfin et al.[50] have conducted a study in Ethiopia, where they have observed that illiterate users have a hard time using mobile banking applications. The key takeaways from the fieldwork by Mesfin et al.[50] not only include the fact that illiterate users have a hard time using mobile banking applications, but also shed light on more profound issues. Thereby, Kazerani et al.[38] have found that understanding the conceptual models (or the abundance thereof) of the users can be explored best utilizing an ethnographic approach. This highlights the symbolic barriers in naming and language and shows what prevented the correct understanding of Bitcoin and its use of applications[38]. For example, employing an interface that leverages verbal instruction in its design has not improved the usability for illiterate people but rather highlighted the difficulty of translation from verbal instruction to manual action[50]. Verbal communication of the placement of items such as *Left* and *Bottom* have shown to be easily misunderstood by illiterate users[50]. This issue, according to Mesfin et al.[50], can be diminished by the use of photos. This is because illiterate users can easily understand imagery, thanks to the lack of possible abstraction, like with symbols or buttons[50]. On the note of abstraction, Mesfin et al.[50] also note that using icons is not always beneficial for illiterate users. This can be brought down to the fact that visual-illiterate people do not make these abstractions with diagrams and signs[50]. Furthermore, it has been shown that illiterate users have difficulty understanding something they have not seen before[50]. This also applies to menu-based interfaces, which are highly confusing for novice users[50]. However, when looking at the interface of MPesa, it becomes evident that it is a menu-based system, where selections have to be made from a hierarchical display of options[50]. The same goes for the menu-based interface M-birr, which is widely used in Ethiopia, the place of the study conducted by Mesfin et al.[50]. In both systems, the user has to navigate between the different options in the menu hierarchically, going up and down and back and forth between the options, such as conducting a transaction or checking the balance[50]. Given the insights mentioned above, it can only be imagined how complicated and confusing such an interface may be to illiterate people[50]. Both the textual element of M-Pesa and the menu-based interaction make this interface more cumbersome for its users who can not even read or write their name[50].

In this context, the group of Mesfin proposes to leverage the use of photos, even going as far as depicting pictures of the local currency notes[50]. This idea originated from illiterate individuals from the study population who have identified the currency notes based on their size and color, rather than their nominated inscribed value[50]. Even though audio-based interfaces can cause troubles, Mesfin et al. still recommend their use[50].

2.2.5 Cryptocurrency context

In the context of Cryptocurrency, Voskobochnikov et al.[78] have conducted an empirical study in which they have observed that the users have a hard time understanding the concept of a wallet. They identified and thematically analyzed over 6800 app-store reviews related to the UX of mobile cryptocurrency wallet apps[78]. It is to be noted that many of their found issues are also evident in general finance apps[78]. Such general issues include freezes or app crashes, performance issues, unclear color coding or lack of guidance[78]. However, many cryptocurrency mobile wallets still lag in terms of user experience. Thereby, Voskobochnikov et al. distinguish between domain-specific issues to blockchain wallets and general UX issues.

2.2.5.1 General UX

When dealing with the general issues of mobile wallet design, inconsistent use of icons and mixed color schemes add to the inconvenience but do not pose major issues[78]. However, overlays, hierarchical misplacement of items, and the lack of error prevention have led to a loss in functionality and usability issues[78]. To add to the confusion, Kazerani et al. have found that consistency in language and denomination is crucial, common issues in their study included replacing BTC with XBT, a new shortcode for Bitcoin, and general symbols to represent the identical currency[38]. When using the wallet for the first time, especially if the users were novices in the field of cryptocurrency, many reviews have reported that the lack of guidance during setup has posed an entry barrier for them and that they could not create a wallet in the first place[78]. Voskobochnikov et al. have also found that users consider biometrics the preferred authentication method in contrast to using PIN codes[78]. Especially, authentication (if used at all) shall only be in place for sending money since a PIN for accepting/receiving a transaction can be seen as a physical risk: When a user has to enter a PIN for receiving money, if he gets money in person, this PIN can be easily seen by a shoulder surfer who then grabs the phone and now has access to the funds[78]. Instead of leaving away the PIN, there could be a mechanism at hand that allows the user to set different PINs for receiving and sending, effectively mitigating the risk of shoulder surfing. In the home screen, security-conscious users have reported that having the balance displayed in the wallet is risky[78]. Therefore, allowing users to toggle the balance display on and off is vital, effectively giving them control of hiding the transaction and account balances completely. When sending transactions, users reported limitations regarding transaction fee selection and a lack of transparency of the fee structure of the wallet provider[78]. The lack of guidance, not only when sending transactions but generally, has negatively impacted reviews about the UX of a wallet[78].

2.2.5.2 Domain specific UX

Regarding the issues related to blockchain technology and its underlying quirks, Voskobojnikov et al.[78] conclude that inadequate mental models of applied cryptography in these wallets and poor security practices of its users are the main drivers for errors and monetary losses. The underlying cryptography already starts to impose challenges in the setup of the wallet, namely by requiring the seed phrase and wallet setup, which was already seen as tedious by some reviewers[78]. But also, during use, the specific implementation of blockchain technology has been causing trouble for some users[78]:

- Sending unsupported cryptocurrency to the wallet (for example, sending Matic to an Ethereum address)
- Cancelling a transaction that was sent to the wrong address is not possible (unlike in traditional banking)
- Limited access to the wallet due to an unsynced state, leading to incorrect wallet balances and unclear transaction statuses
- Inability to recover assets without the mobile application, even though the option for private key export is available
- Pending transactions that were sent with a too-low fee and therefore not allowing any further transaction submitting
- Lack of guidance in creating their first blockchain transaction or test transaction

On the other hand, some users have reported beneficial aspects of the wallets in question[78]:

- Customizable transaction fees allow the users to choose the processing speed of the transaction
- Additional authentication such as biometrics, PINs and Two Factor Authentication (2FA) are seen as a welcomed addition
- Replace-by-fee on pending transactions greatly contributed towards good UX
- Self-locking after a timeout period increased perceived security
- Open source software boosted trust, and reviewers valued the ability to verify the code source and changes
- Ability to import/export private keys allows for seamless access to funds

2.2.6 Recommendations to improve UX

In the points mentioned above, Voskoboynikov et al.[78] have elicited both positive and negative aspects of the analyzed cryptocurrency wallets. First, following usability guidelines and heuristics is vital for reducing or eliminating the general issues faced by the users of cryptocurrency wallets[78]. Thereby, customizable transaction fees and the ability to speed up stuck transactions are considered advanced, nevertheless, they play a massive role in the UX evaluation of the wallet and significantly add to its overall usability[78]. This customizability helps not only to minimize errors but also to diminish financial losses[78]. To not confuse novice users, Voskoboynikov et al. also put forward the idea of presenting different interfaces to advanced users and novice users[78]. Generally, personalized interfaces have been shown to improve overall UX; therefore, it is believed that distinguishable profiles for users could have the same effect on cryptocurrency wallets[78]. To sum up, providing adequate guidance, especially for novice users, can address most of the issues encountered, and therefore, giving technology support is vital[78].

Voskoboynikov et al.[78] also suggest that the research outcome of an empirical study of user experience with mobile cryptocurrency wallets could entail a set of design heuristics and domain-specific guidelines. To accurately represent the application's usability, these heuristics and improvements must be validated and tested with real users. Given the above recommendation, assessing the UX of the newly designed and developed wallet, which was adapted to a specific target group, is one of the major goals of this thesis. The extension of including domain-specific guidelines and design heuristics would be a welcome contribution.

Kapitel 3

Design

3.1 User requirements

Before starting the design process, it was vital to collect the requirements of the target group. Since this thesis strives to improve the user interface of an already existing wallet, Blink, formerly known as Bitcoin Beach Wallet (BBW)[28], the user requirements are based on missing or unclear functionality of the existing wallet. These initial requirements were gathered by letting the users in Kenya, Kibera, evaluate the existing wallet based on screenshots and provide feedback and feature requests. As this thesis was conducted in cooperation with the company sideXchange[58] in Toronto, Canada, who had a member of the Ronnie Mdawida fund[48] on site, this process was largely facilitated by them. The requests were gathered bilaterally by Ronnie Mdwadmida himself, a resident of Kibera. Thereby, the following user requests were collected:

1. Mpesa integration to load money
2. Add map/merchant locations for Kenya
3. Contacts feature to enable you to send crypto to people
4. Add Swahili as a language option
5. Add tasks, like inviting friends and getting paid for doing so (gamification)

The first request, namely the Mpesa integration, was not included in the scope of this thesis. It would have been a great addition because, as mentioned in the section motivation 1, MPesa is widely spread and has a large existing customer base. However, such integration is considered to be a fiat on-ramp[10] and would have required special implementation and regulation. Such regulation would have directly conflicted with one of the thesis's goals: Providing a wallet without needing KYC. The second requirement, adding local merchants to the map section, would have been more feasible to implement. However, each merchant would have to be onboarded and instructed on how to use the wallet. It is, therefore, left to be implemented after the end of this thesis.

The third point, the ability to send Bitcoin or Stablesats to people in the contact list, was already possible in the existing wallet. Even though this functionality existed, it was buried deep down in the people section, where only experienced users would have found it. Therefore, this requirement was reformulated and included in the thesis to make the contact list more accessible and easier to find. The fourth wish of the target group was support of their local language, Swahili. At first, this might seem unnecessary in the context of this thesis, as it mainly involves translation work and is not directly correlated to UI improvements. However, upon further consideration, we came across a great idea of how to include this feature request to align with this thesis's goals. By showing the interface in Swahili during the user testing sessions, we can mimic illiteracy for the Swiss participants, as explained in section 5.1.1. This allows us to evaluate the usability of the application for illiterate people, which is one of the main goals of this thesis.

Last but not least, the fifth idea of adding gamification to the application was postponed to a later stage. Incentivization is a great way to drive adoption. However, the key focus of this thesis was to improve the usability and user experience of the application. Therefore, this feature request was not included. Other feature requests emerged from bilateral communication with other residents and in meetings with Ronnie and me. These included the following points:

- Person-to-person interactions such as a chat or a social feature to communicate
- 2FA confirmation PIN to execute transactions or make account changes
- Import of contacts from the phone contacts to send money to phone numbers

Upon further consideration, these additional emergent feature requests were not included due to various reasons. The chat/social feature could have been problematic since it would have opened the possibility that malicious people could exploit this way of communication to scam people. Especially when dealing with money, facilitating direct, unmonitored interaction between the users could have been problematic.

Regarding the 2FA confirmation PIN, this would have been a great feature to have, however, it would have required a lot of additional work and would have been out of scope for this thesis. Furthermore, the Blink wallet already offers a PIN code to unlock the application; therefore, the additional 2FA confirmation PIN was considered superfluous. Lastly, touching the deeply nested security practices of the existing Blink application could have introduced serious bugs, and subsequently could have been a cause for loss of customer funds. Since this thesis targets a group with limited access to existing banking services, the security of funds is of utmost importance. Taking this risk could not have been justified.

It was estimated that integrating the phone numbers into the contacts feature could be time-consuming and would have required changes in the backend services. Even though the users have to sign up with their phone number, the established way of sending money to each other is via usernames or wallet addresses. Given that this issue is not UI-related to the existing Blink wallet, it was not included in the scope of this thesis.

3.2 Architecture

This thesis focuses on improving the usability and UX of a particular mobile Bitcoin wallet. Thereby, existing backend services and infrastructure will be leveraged to reduce the implementation overhead. Furthermore, this allows adjusting the extent of this project to the scope of a bachelor thesis. The mobile application Blink[28] presented itself as a viable option, together with its Application Programming Interface (API). Its interface will be improved and the user experience of the existing and the new interface will be evaluated with users and the results thereof juxtaposed.

3.2.1 Infrastructure and backend services

In the context of this thesis, the Galoy managed node was chosen as the backend service. Not only was this choice made due to the below-mentioned advantages, but also because many considerations were made towards dealing with customer funds. Essentially, leveraging an already existing system proven to work and be reliable was chosen over the approach of building a new system from scratch. By doing so, it is ensured that the funds of the customers are being treated with the utmost care, follow existing security practices and allow the customers to use the new system daily without worrying about any serious security implications. Additionally, this also allows wallet interoperability with the existing system, since the user accounts created in the AfriBit wallet (new system) also work on the Blink wallet (current system) and vice versa, ultimately ensuring that customers have access to their funds, irrespective of the actions of this thesis.

3.2.1.1 Galoy managed node

Galoy's native wallet, the Blink wallet[28], offers both on-chain and off-chain payments routed over the Lightning Network. Therefore, a service to interact with the Lightning Network and the Bitcoin blockchain is needed to support these use cases. Especially for the Lightning Network, a well-connected node is needed to route payments, and the payment channels, as well as their liquidity need to be managed. Since this is rather complex, time-consuming, and requires liquidity to provide to the channel, Galoy offers the developers a service known as *managed nodes*.

The Galoy-managed node handles both the on-chain settlement and off-chain transactions from the Lightning Network. The main benefit is that it is fully featured and offers active liquidity management of the payment channels without the user needing to worry about it[26]. Furthermore, the Galoy team constantly monitors the node and assures a high uptime, making it an ideal option for a project to get up and running fast and reliably[26]. All of this while being regulated in El Salvador under BBW, S.A. de C.V.[26].

3.2.1.2 BBW API

Galoy also offers the option to use their API instead of a managed node. Essentially, the API services are used by a managed node, and therefore, the API is a subset of the functionality of the managed node. The API allows for more fine-grained control over the executed instructions when settling to the blockchain; however, this comes at the expense of management and implementation overhead. Even though the API allows for quick integration, does not include any upfront cost (cost is per API call), and is open source[26], it did not suffice as a feasible solution for this thesis. The setup, funding, and management of the Lightning payment channel would have been out of the scope of this thesis; hence, the Galoy-managed node was chosen to be used instead.

3.2.2 Mobile wallet/frontend

3.2.2.1 Galoy mobile wallet

At the heart of the Galoy project and this thesis is the mobile wallet, Blink. It is open source and allows users to create accounts, manage their funds, and execute transactions without knowing much of the technicalities involved. For those wanting to know more and learn about Bitcoin, the wallet also offers an educational overview section of the underlying principles of Bitcoin[26]. The wallet is available for Android, iOS, and Huawei AppGallery, and is available in the respective app stores and allows for a quick setup with only using the phone number[26]. A vital purpose of this wallet, apart from the ability to both transact in native on-chain Bitcoin transactions and Bitcoin Lightning off-chain transactions, is the ability to convert BTC to synthetic USD (Stablesats) without undergoing extensive know-your-customer (KYC) regulations beforehand. In the following sections of the thesis, the terms *stablesat* and *USD* are used interchangeably. The conversion between the two effectively allows its users to save their funds in the dollar-denominated currency *Stablesats*, mitigating the higher inflation that may be present in their local currency. Not only are the users able to put aside money in Stablesats for saving, but they also can conduct transactions in Stablesats, solving the issue of short-term exchange rate volatility[32]. These transactions are supported both Onchain and via Lightning, ultimately making them a very suitable alternative to the volatile Bitcoin currency. This is possible since Stablesats function by leveraging the concept of derivatives. In short, this means that the Bitcoin bank (here Galoy and the managed node) instead of actually exchanging the Bitcoin Satoshis (sats) for USD, opens a short position on the Bitcoin price, and the sats are kept in possession of the bank[32]. Thereby, the short position serves as a hedge against future changes in the BTC to USD exchange rates, where, ideally, in both cases, the Bitcoin bank does not incur any monetary losses or gains.

1. If the Bitcoin price rises, the bank has a loss on the short position, but the value of the sats increases, offsetting the loss.
2. If the Bitcoin price decreases, the bank has a profit on the short position, but the value of the sats decreases, offsetting the profit.

This allows the system to offer the clients the benefits of having a stable USD-denominated currency without the need for the customer to have existing banking access[32]. Combining this with the ability for the customer to have the application in many languages, export a transaction history, and have a Lightning address similar to an email, this product is an excellent basis for people new to Bitcoin who want an extensive feature set without the technical overhead. However, it should be noted that the wallet itself is a custodial solution and that it is impossible to export the private key or back up the wallet using a seed phrase or mnemonics. The abundance thereof is perfectly in line with the target group of the wallet, new and inexperienced users who may have been previously excluded from banking, therefore not posing any problems or conflicts of interest.

3.2.2.2 PoS interface

Initially, it was also planned to improve the UI from the PoS interface to allow for a more seamless experience for the merchants when paying with Bitcoin. Due to the time constraints of this thesis, this was not possible, and therefore, the POS interface remains unchanged. It has been entirely excluded from the scope of this thesis regarding the user testing sessions. The improved usability and user experience version of Blink, the AfriBit wallet, is compatible with the existing POS interface and can be used to pay for goods and services at the merchants. Ensuring that the existing infrastructure was compatible with the new wallet was vital.

3.3 Overhauled user interface

Before tackling the usability problems and suggesting user interface improvements, the existing UI had to be modeled in software, allowing for easy prototyping and further design alteration. To do so, the design tool Framer[8] was used to create the existing UI of the Blink wallet. Framer is a design tool that allows users to create interactive prototypes in a wireframe-like fashion. These prototypes can then be used to test the usability of the user interface. Another reason why Framer was used is that it is free and offers greater flexibility than other prototyping tools, making it the most suitable tool for this thesis. The Galoy team supported this approach and provided the necessary assets to recreate the user interface, including screenshots, Scalable Vector Graphics (SVG) icons, existing Figma designs[27], and color schemes. The recreated UI was constructed as true-to-life as possible; however, it exhibited minor imperfections such as spacing and scaling, which, for this thesis, can be neglected.

After designing the existing user interface in Framer, the new UI was designed, whereas the main focus lied on the usability and UX of the application. Therefore, the replicated UI served as the basis for these improvements and the reference point to which the new user interface was compared. The new UI was also designed in Framer, allowing for a direct comparison between the two versions.

3.3.1 Universal changes

Throughout the whole application, there were certain aspects or design choices that were not consistent. Therefore, the first step was to change these characteristics to provide the user with coherent interactions, terms, and icons. This consistency is viewed as a UI design principle and therefore contributes towards improving the overall user experience[45].

3.3.1.1 Icons

Galoy, the creators of the Blink wallet, designed many icons, allowing them to use custom styling throughout the application. Generally speaking, these icons are well-designed and used consistently throughout the application; however, they are not always canonically defined and sometimes deviate from standard iconography. Canonically defined in this context means that the symbols are universally understood, across different cultures and languages, and are not ambiguous in their meaning - however, such icons are rare[20]. Therefore, the icons were replaced with the standard icons from the Bitcoin icon library[37]. By incorporating well-known icons, we ensure consistency, even across different applications, and allow for a more intuitive understanding of them. This greatly benefits the user experience, as the user does not have to learn new icons but can rely on existing knowledge (if any) from previous systems. Furthermore, the icons were also recolored appropriately to match the application's color scheme, which is discussed in the next section.

3.3.1.2 Color Schemes

Throughout the original Blink wallet, the primary color is identical to the color of the Bitcoin logo, namely orange. Whilst this offers a spotless look when dealing with the Bitcoin currency, it is not ideal when dealing with the synthetic dollar, Stablesats, identified by the color green. It confuses users that the button and UI highlights are orange when confirming a USD transaction. This again can be attributed to the fact that consistency is key in UI design, and therefore, the color scheme should be consistent with the currency it denotes across the whole application[45]. Therefore, three fundamental changes were made to the color scheme of the application:

- All UI elements related to Bitcoin are represented in orange
- All UI elements related to Stablesats are represented in green
- Buttons and UI highlights not related to Bitcoin or Stablesats are represented in white or black, depending on whether the dark-mode is enabled or not

This ensures that the user can form an accurate mental model and draw the correct associations between the colors and the underlying currencies. When dealing with Bitcoin, UI elements and icons are highlighted in orange. Thereby, the person immediately notices if the currency changes, as the color scheme changes accordingly. This level of distinction further separates the two currencies, lowering the chances for errors to occur. These visual cues of which currency is being used are vital for the user experience, not only for the ones new to Bitcoin but also for the more experienced users. The direct impact of this change can be seen and will be discussed later in the user testing sessions, where the users were able to distinguish between the two currencies to a greater extent when having them separated by colors.

3.3.1.3 Use of typography and terms

Since the Blink wallet is available in many languages, it is essential to use universally understood terms. Blink does a great job of providing a wide selection of different languages all across the globe; however, some terms used are somewhat confusing and lead to user error. This can also be seen in the user testing sessions, where the users were confused by the terms *sat* and *stablesat*. The former refers to a smaller fractional unit of a Bitcoin, while the latter stands for the synthetic dollar, Stablesats. Addressing this problem, an ideal approach would have been replacing the term *stablesat* with *USD*. However, this was not feasible due to several reasons:

- The term *Stablesats* is used throughout the whole ecosystem, including the point of sale, admin console, and so on. This change would not only have to be propagated across multiple services and applications but also would have been a tremendous change for the users
- The term *Stablesats* is a registered trademark of Galoy and a product/service they offer, making it hard to justify the change
- The disappearance of the term *Stablesats* would be confusing to the existing user base
- From a technical point of view, the term *Stablesats* is more accurate, as USD usually refers to the fiat currency, which is not the case here as the sats are still in possession of the bank and never exchanged for fiat

Due to the above-mentioned reasons, the term *stablesat* was kept in place. Instead of completely replacing the term *stablesat* with *USD*, the term *USD* was used in addition to the term *stablesat*. Wherever possible, the term *USD* was used instead of *stablesat* and connected to the green color scheme. On a concluding note, we explicitly state our favor of the term *USD* over *stablesat* in terms of usability.

3.3.1.4 Navigation

A bottom navigation bar served the purpose of switching between different screens in the original application design. This navigation bar per se is not bad; however, it adds additional complexity and hierarchical navigation to the application. Section 2.2 highlighted that illiterate people often struggle with hierarchical menus and navigation. Hence, to reduce the application's complexity and make it more accessible to illiterate people, the bottom navigation bar was removed. The original navigation bar consisted of the following navigation items:

- **Home:** navigates to the home screen where the user can see his balance and recent transactions
- **People:** navigates to the circles and contacts screen, where the user can see his contacts and recent interactions with people
- **Map:** navigates to the map screen, where the user can see the merchants and their locations and pay a business by tapping on it
- **Earn:** navigates to the earn screen, where the user can learn about Bitcoin and get rewarded in sats for completing quizzes

When removing the navigation bar it had to be ensured that the functionality of the items therein were not lost, as they represent crucial roles in the application. To guarantee this, the removal was done by relocating the functionality in the respective interaction flow of the corresponding screen. Less critical features were abandoned by removing the functionality of the item altogether. The home screen was kept in place as the application's main screen, the first screen the user sees when opening the application. The people screen previously offered two subitems to see the *contacts* and what the Blink developers call *circles*. Circles allow users to track how many people they have welcomed to the app and how they contribute to Bitcoin adoption with Blink. Blink thereby distinguishes between two circles: The inner circle, which represents people whom the user welcomed, and the outer circle, which represents people who were welcomed by the inner circle. As this aspect of onboarding users is not the central aspect of the application and is not required for the app to function, it was removed entirely. Furthermore, the circles were removed to reduce complexity, ambiguity, and the amount of text, especially for illiterate users.

However, the contacts section inside the people screen is vital to the application. It gives the user an overview of who uses the application and to whom they can send money. Furthermore, contacts are added based on recent transactions, so users also gain insight into whom they have recently sent or received money from. Instead of keeping it as a subitem of the people screen, the contact list was relocated to the screen shown when sending a transaction. The same goes for the map screen. This will be further discussed in the respective section 3.3.4. Lastly, the earn screen was also removed, as it does not serve a vital purpose in the application in the context of this thesis. There are multiple other online resources better suited to studying Bitcoin. Furthermore, illiterate users would not have incurred any benefit from this text-heavy screen.

3.3.2 Home screen changes

Users can see their accounts, respective balances and recent transactions on the home screen. Any changes introduced had to ensure that this functionality remained and was as accessible as possible. This also applies to the actions that can be executed from the home screen, namely converting, receiving, and sending money. The most profound change introduced to the home screen was the removal of the bottom navigation bar, discussed in the previous section 3.3.1.4. Removing the navigation bar allowed for more screen real estate, which is beneficial for using the smartphone application with smaller screens. Furthermore, the removal reduced the data-ink ratio of the screen, thereby effectively conveying the information to the user in a more efficient manner[75]. The data-ink ratio is a concept introduced by Edward Tufte, which describes the ratio of elements in a visual representation to the total elements used[75].

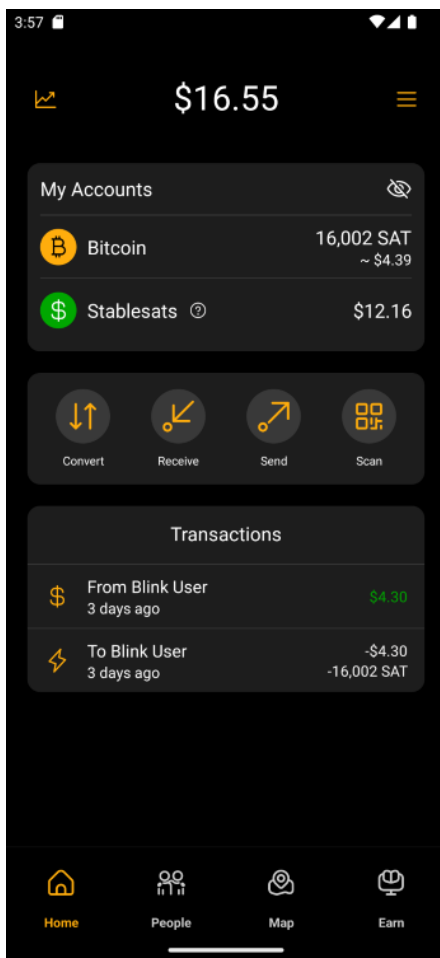


Abbildung 3.1: Blink home screen

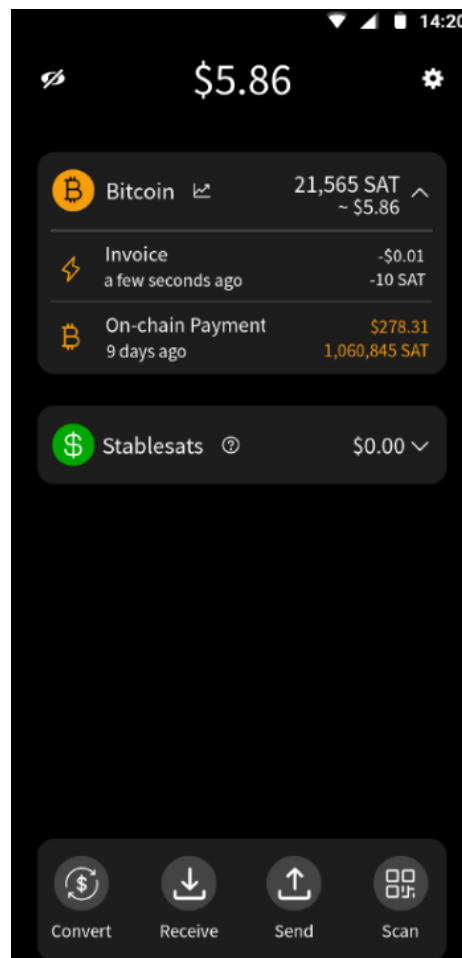


Abbildung 3.2: AfriBit home screen

Figure 3.1 on the left shows the home screen of the existing Blink wallet, whereas figure 3.2 on the right shows the home screen of the new AfriBit wallet. The second prominent change is the new placement of the wallet's actions: convert, receive, send, and scan. In the existing wallet, these actions were placed in the middle of the screen, making them

harder to find and buried between the accounts and recent transactions.

Moving the actions to the bottom of the screen, at the previous location where the navigation bar was, makes them more accessible and easier to find. Furthermore, this also brings the transactions and accounts closer together, ensuring appropriate proximity between the related elements. This aligns with the UI design principle of proximity from the Gestalt laws, which states that related elements should be grouped close together[39]. Additionally, the new icons that follow the standard iconography[37] help the user better transition from existing wallets to the AfriBit wallet. New icons were also introduced for the settings and hiding balance actions, again following the standard iconography[37].

The improved coupling of the accounts and transactions section further amplifies the effect of having the accounts and transactions close to each other. Instead of having a separate container for the transactions, the transactions are now directly shown below the accounts. Furthermore, the transactions are now separated according to their corresponding settlement currency. This means that the Bitcoin transactions are shown below the Bitcoin account, and the USD transactions are below the Stablesats account. To further decrease the number of default shown elements on the screen, the transactions are now collapsed, allowing for less clutter on smaller screens. A caret icon was added to the right of the account's balance to give the user a visual signifier that the transactions can be expanded. The separation of all transactions into two mutually excluding transaction histories and their placement below the corresponding account follows the UI design principle of proximity from Gestalt laws, allowing users to better relate past transactions to the corresponding account.

Minor changes on the home screen include the color scheme change, where now everything related to Bitcoin is represented in orange, and everything associated with Stablesats is represented in green. This can be seen in figure 3.2 on the right, where the received Bitcoin payment of \$278.31 is highlighted in orange, indicating a received amount in Bitcoin. Previously, receiving amounts were highlighted in green, irrespective of the currency. Lastly, the icon placement of the price chart and the balance visibility were changed, namely, moving the price chart icon to the Bitcoin account and the hiding balance icon to the top left corner. This was done because the price chart only applies to the Bitcoin price and because the hiding balance icon is a global setting, hiding the balances of all accounts and their transactions.

In conclusion, the changes introduced to the home screen increased the data-ink ratio, coupling of related elements, and recognizability of icons while simultaneously reducing the overall possible hierarchical navigation of the application and the required screen size to see all elements at once. This was especially vital concerning the target group of this thesis, illiterate and novice users, who are said to have more difficulties with hierarchical navigation in applications. Furthermore, given the geographical location of the target group, namely Kibera, the app also needs to be visible as a whole on smartphones with smaller screens.

3.3.3 Receive changes

This screen allows users to receive money in either Bitcoin or Stablesats via the Lightning Network or Onchain. Receiving via Paycode additionally is available for Bitcoin but not for Stablesats because Paycode uses the Lightning Network Uniform Resource Locator (LNURL) protocol[33]. With the topmost button group, each button consisting of the currency name and icon, the user can select the receiving currency. Beneath, the concept of a wallet invoice, as discussed in chapter 2, is used and encoded in a QR code. The button group below is used to choose the method (Lightning, Onchain, or Paycode) for receiving funds, set the transaction amount, and add a description. Unlike the optional note field, the transaction amount must be set for all methods, except for the Paycode option, where the sender will be prompted to enter the amount when scanning the Paycode.



Abbildung 3.3: Blink receive Stablesats via Onchain



Abbildung 3.4: AfriBit receive Stablesats via Onchain

It should be noted that the title in figure 3.3 remains *Receive Bitcoin* in the Blink interface, even if Stablesats is selected. The overhauled design in figure 3.4 boasts a consistent color scheme, where text and corresponding icons have the new color applied. This is due to the changes that were made globally, namely coloring everything related to Bitcoin in orange and everything related to Stablesats in green.

By doing so, the user's mental model can be better guided and support the visual distinction between the two currencies to reduce confusion and human error. Additional changes to the Onchain receive method include the improved scaling of the displayed on-chain receive address below the QR code.

By adjusting the opacity of the *add notes* element in figure 3.5, it is visible that notes can not be added when using the Paycode as the receive method. Since there is no use in showing an option that is not available, this button was removed entirely from the AfriBit Framer design to free up visual space. The Paycode variant is the only option not requiring the user to set an amount. When using the Paycode option, the only difference to a Lightning payment is that the sender can adjust the amount.



Abbildung 3.5: Blink receive Bitcoin via Paycode

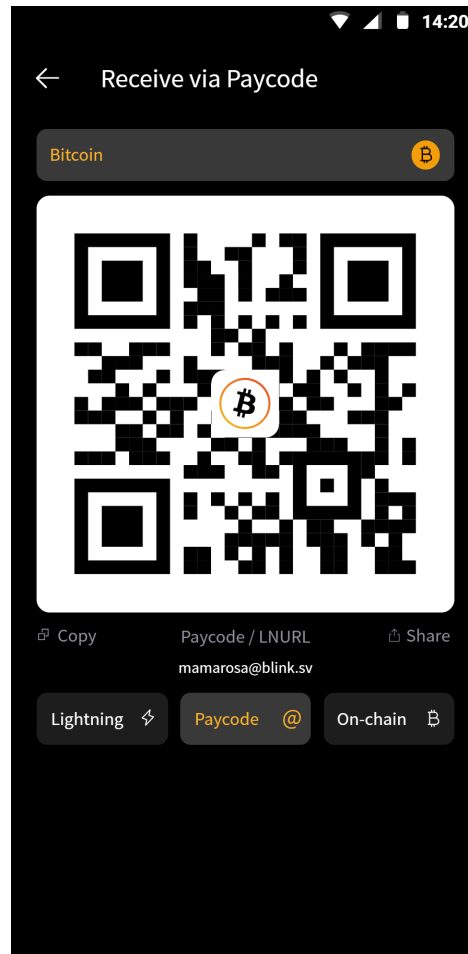


Abbildung 3.6: AfriBit receive Bitcoin via Paycode

However, this is only possible if the receiver has *not* entered an amount. If the receiver has entered an amount, the sender cannot adjust the amount anymore as it is fixed. Hence, when the receiver sets the amount, the Paycode option behaves like a Lightning payment, at least from a UX perspective. Therefore, the set amount option was removed from the receive screen when the Paycode was selected as the receive method. Finally, also in this example, the title of the AfriBit wallet reflects the current chosen method to receive funds instead of displaying the currency, illustrated in figure 3.6.

3.3.4 Send changes

For a user to send money to someone, the recipient's receiving details must be known. In the screen that facilitates executing transactions to other people, the destination has to be typed into an input field. Thereby, either a Lightning or Bitcoin invoice or address can be inserted or a username (Blink ID). Furthermore, the user can scan a QR code to retrieve the receiving details by clicking on the scan icon next to the paste icon on the right, figure 3.7. Any introduced changes should not affect the screen's functionality, as it is a vital part of the application and offers multiple ways to send money. Therefore, the input field was kept in place like in the original application. The only changes introduced were additions to the existing screen, leveraging the screen real estate more efficiently.

3.3.4.1 Send to contact



Abbildung 3.7: Blink send destination screen

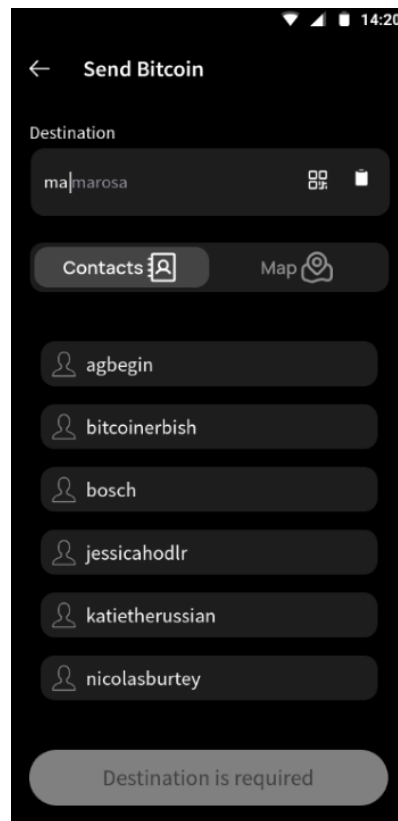


Abbildung 3.8: AfriBit send contacts screen

The first addition to the screen was a contact list, visible in figure 3.8, allowing the user to pick a contact to send money to. From the beginning when opening the screen, the alphabetically ordered list shows all contacts and recent interactions, composed of an icon and the respective name. The design idea is that if the user starts typing, the text field suggests autofill options based on the contacts matching the search. This saves time and reduces possible user errors.

3.3.4.2 Send from map

Noteworthy is the new incorporation of the map screen into the send screen. Figure 3.9 shows how previously the map was a separate screen, accessible via the bottom navigation bar. It allowed to see merchants, their locations, and directly send money by tapping on the business. As paying was the only extraneous action possible on the map screen, incorporating the map into the send screen allowed to further reduce navigation hierarchy and enrich the send screen with already existing, previously separated functionality. Supporting this seamless experience is a toggle below the input field to switch between the map and the contact list, depicted in figure 3.10. This horizontal segmented picker is inspired by the Apple iOS design and is commonly used to pick from different options[6].

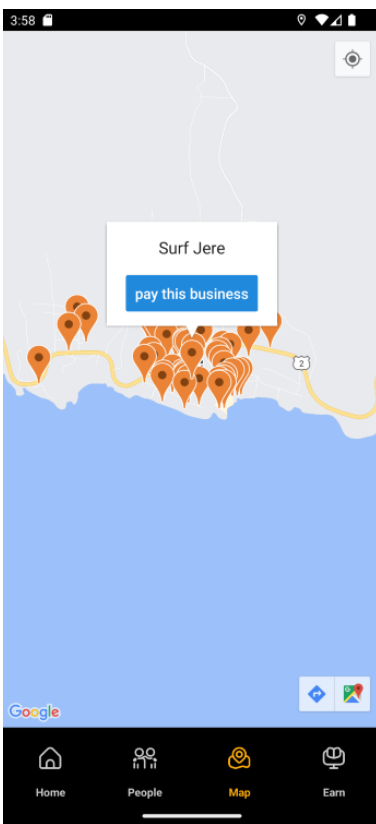


Abbildung 3.9: Blink business map screen

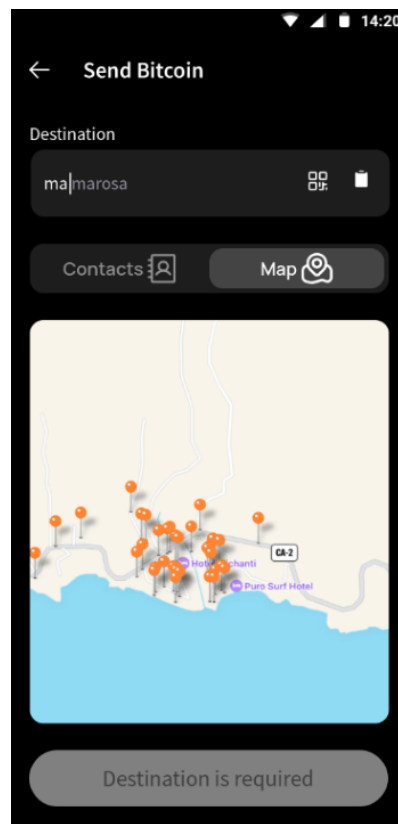


Abbildung 3.10: AfriBit send map screen

Depending on the user's need, switching between the map and the contact list is possible. Ideally, tapping on a business would also fill the receiving details into the input field. Additionally, it would be beneficial if typing in the destination field would filter the businesses on the map, only showing the ones that match the search. To summarize, the changes to the send screen promote more efficient use of previously unused screen real estate and easier access to existing functionality, namely, sending money to existing contacts or businesses on the map, all while ensuring that the existing functionality is not affected. The overall hierarchical complexity was also reduced, and all send-related functionality now appears on the same screen.

3.3.5 Confirm screen changes

After choosing the destination to which funds shall be sent, the user has to choose which account to use, either Bitcoin or Stablesats. The money will then be deducted from the selected account in the respective currency. In cases where no wallet invoice was scanned, the amount has to be set.

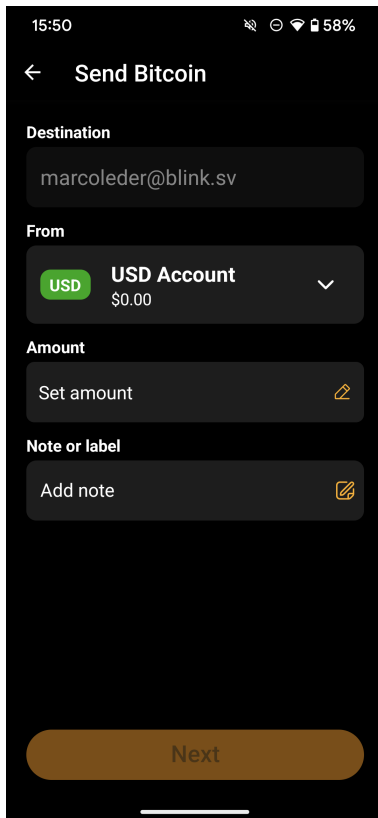


Abbildung 3.11: Blink confirm screen

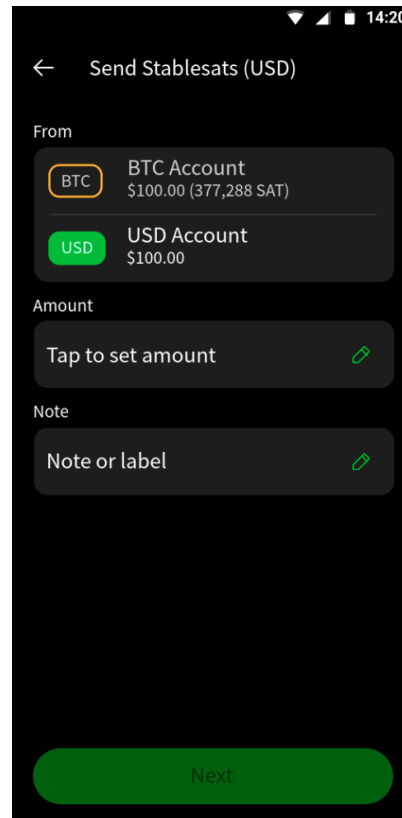


Abbildung 3.12: AfriBit confirm screen

Figure 3.11 on the left shows the confirm screen from the Blink wallet, whereas figure 3.12 on the right shows the AfriBit wallet. Fundamental changes include the new structuring of the account selection as well as the adaption of the color scheme. Instead of having to select the account from a drop-down menu, where only the currently selected option is visible, the user can now see both accounts at once and can select the desired account by tapping on it. This signifies to the user that both accounts are available for selection whilst also informing about the balance of each account. The filled currency bubble on the left of the account name and the increased opacity of the whole account element indicates the currently selected account. Additionally, the title shall represent which account is currently selected, and the button at the very bottom of the page shall also reflect the account with the use of colors. These changes should allow the user to better distinguish between the two accounts and ensure that the correct account is debited when sending money.

Kapitel 4

Implementation

4.1 Galoy mobile repository

The existing repository of the Blink application[30] was forked and renamed to AfriBit wallet[41]. Thanks to the open-source nature and the Massachusetts Institute of Technology (MIT) license of the repository, this was possible without any problems. The repository uses Yarn[21] as a package manager and has explicit instructions on how to set up the development environment, how to structure the code, and how contributions should be handled. Unluckily, some aspects of the repository were not documented well and had to be figured out by trial and error. For example, one of the changes needed to make the *yarn install* command work was to create an external *postinstall.sh* script instead of directly chaining the command in the *package.json* file.

4.1.1 Stack

The code is mainly written in Typescript[52] and leverages the React Native framework[24]. Therefore, to run the code, the React Native Command Line Interface (CLI)[25] is required. As development was done on Linux, the application could only be built for Android, as the IOS build requires a Mac. Hence, Android Studio was required to run the application on an Android emulator[34] and had to be installed. API requests were handled over GraphQL[23], which allows the fetching of only certain fields or parts of data. This drastically reduces the traffic and allows getting many different pieces of information with a single query. Furthermore, GraphQL is very extensible and facilitates easy modifications of the request, making it suitable for adjusting the UI and the needed query.

4.1.2 Apollo client

A remote backend service was used to ease the development process, allowing the application on the mobile phone to function properly, without the need of having a local backend running on the phone or a computer in the same network. Galoy provides such a staging environment[29], an identical copy of the production environment. Therefore, this staging environment was used as a backend, both for development and the prototype builds for user testing.

4.1.3 Language

For translation and languages, the *i18n-react* library[44] is used. As mentioned in the design chapter 3, some titles and terms had to be altered to guide the users better. This demanded changes to the English source file as well as its index. Additionally, to complete the Swahili language, the translation file for the language code *sw* also had to be modified. Not only completion of all translation keys was necessary, but also making sure they conveyed the intended meaning and are not just a word-by-word translation. To do so, the terms were translated using the generative AI model *gpt-4-0613* by openAI[57]. The correctness of the meaning of the translated terms was ensured by Ronnie Mdawida, who is a Swahili native speaker.

4.1.4 Icons and color scheme

Adjustments were made in the *assets* and *components* folders to adjust the icons and smaller visual changes. More often than not, the color scheme changes had to be done individually in the code of the respective component. An example of introducing the necessary logic for differentiating between Bitcoin and Stablesats is given in listing 4.1. Thereby, the styling of the elements is determined based on the value of the variable *color*, which is the result of the GraphQL field *request.receivingWalletDescriptor.currency*.

```

1      <TouchableWithoutFeedback onPress={onPress}>
2          <View style={styles.button}>
3              <Text
4                  {...testProps(text)}
5                  style={color === "BTC" ? styles.textBtc :
6                      styles.textUsd}
7              >
8                  {text}
9              </Text>
10             {typeof icon === "string" ? (
11                 <Icon style={color === "BTC" ? styles.
12                     textBtc : styles.textUsd} name={icon} />
13             ) : selected ? (icon.selected) : (icon.normal)}
14         </View>
15     </TouchableWithoutFeedback >

```

Listing 4.1: button-group.tsx

4.1.5 Structure

The repository is organized similarly to many react-native frontend repositories. There are several configuration files, license, package.json in the root folder, whereas two subfolders, *android* and *ios*, are used as output folders for the builds and store the bundled debug applications. Other folders include docs, *e2e* for testing, *ci*, *.storybook*, with *.app* being the main application folder in which the source code resides. The not exhaustive, heavily truncated structure of the app folder and its essential files that were modified in the AfriBit wallet is visually depicted in figure 4.1:

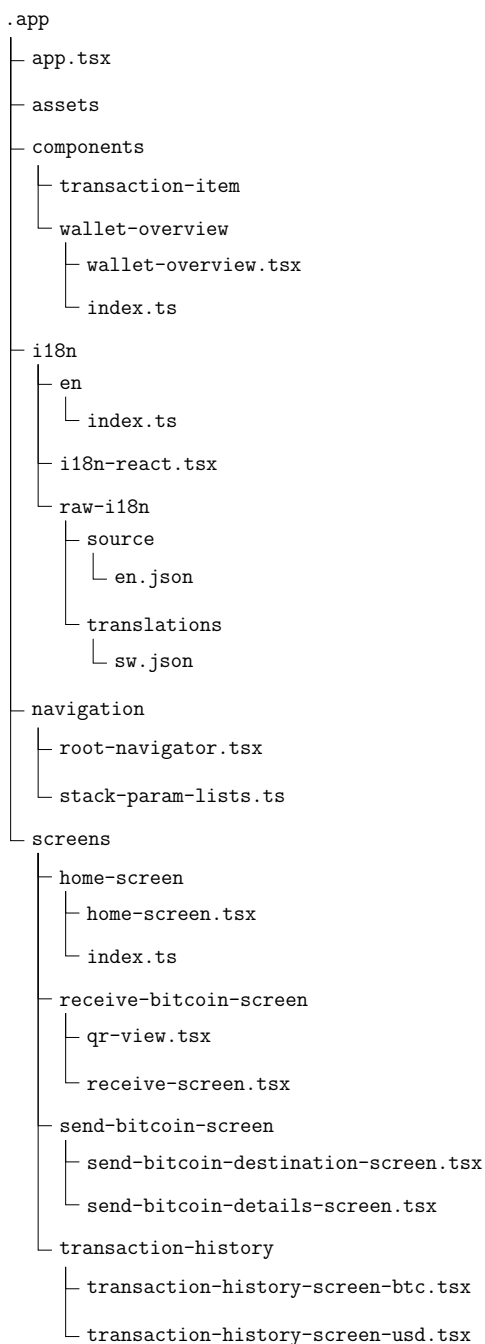


Abbildung 4.1: Application source structure

4.1.6 Changes to home screen

Since the home screen is the application's main view, it has undergone multiple changes. The main file `app/screens/home-screen/home-screen.tsx` was modified to allow all balances to be hidden. Previously, the eye icon only hid the account balances in the Blink wallet. Now, in the AfriBit wallet, this action hides not only the accounts' balances but also the transactions' balances. This functionality was facilitated by modifying `app/components/transaction-item/transaction-item.tsx` to include a hideable area. Since privacy-adverse users who hide their balance might also want to hide the amounts of previous transactions, this feature seemed necessary to include on the screen. Another change to the `home-screen.tsx` file included removing the recent transactions section, which was then incorporated into `app/components/wallet-overview/wallet-overview.tsx`.

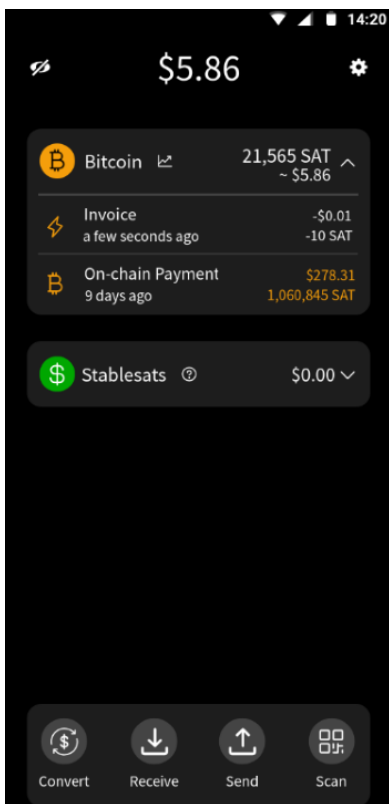


Abbildung 4.2: Home screen design, partially expanded

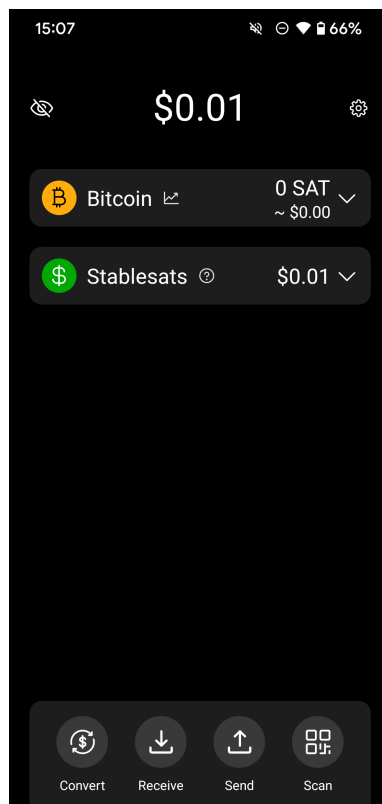


Abbildung 4.3: Home screen implementation, collapsed

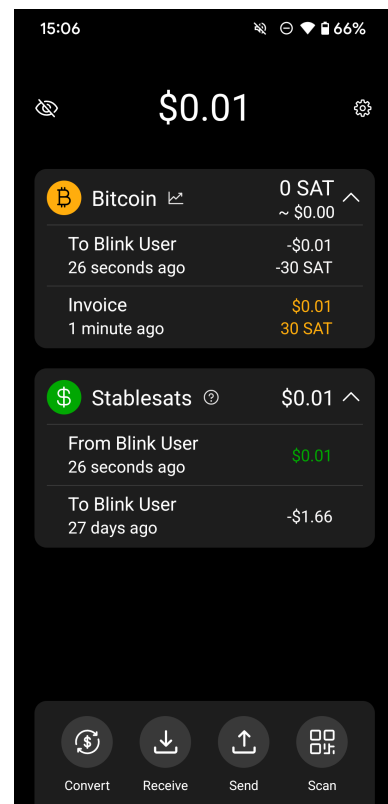


Abbildung 4.4: Home screen implementation, expanded

Thereby, the `wallet-overview.tsx` was adapted such that below each account, the corresponding history of transactions is shown, as depicted in the figures 4.2 to 4.4. The number of shown transactions ranges from one to four, depending on the screen size. This also demanded the creation of `transaction-history-screen-usd.tsx` and `transaction-history-screen-btc.tsx` in the `app/screens/transaction-history` folder, to filter the transactions accordingly and only show the transactions of the corresponding account. Additionally, minor changes to the color scheme had to be made, whereas receiving amounts are now also color-coded

in the respective account color. As mentioned in 4.1.4, these changes had to be made directly in the code of the component, in this case *transaction-item.tsx*.

By actively adapting the number of shown transactions to the screen size and removing the bottom navigation bar, the whole application state can be seen at once, irrespective of the device screen size. This is visible in figure 4.5 and figure 4.6, which shows the expanded version of the home screen on a smaller phone with limited screen real estate. Furthermore, the addition that the elements are collapsible contributes to this concept.

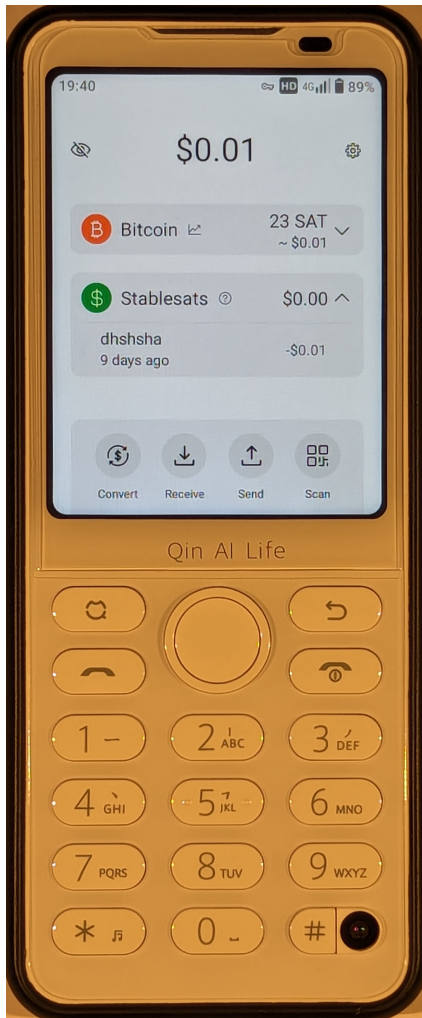


Abbildung 4.5: Home screen small phone, Stablesats

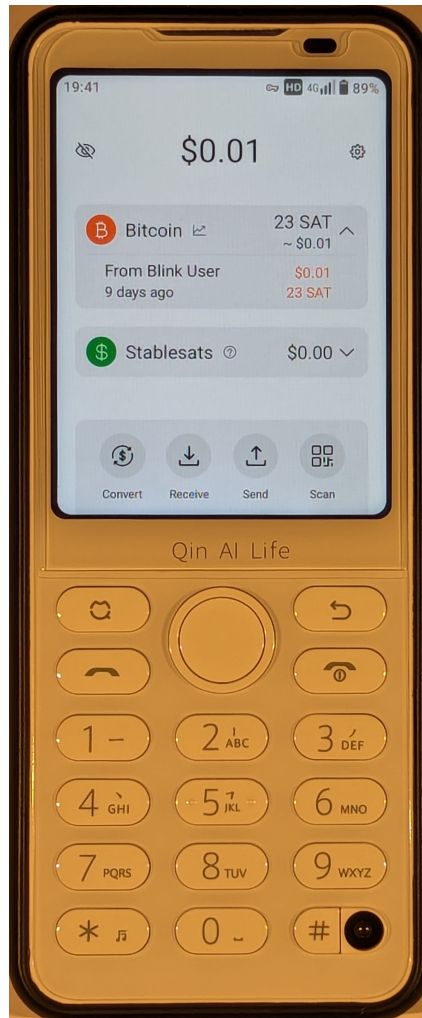


Abbildung 4.6: Home screen small phone, Bitcoin

Last but not least, by modifying *app/navigation/root-navigator.tsx*, the removal of the bottom navigation bar simultaneously supported this approach. Overall, the home screen followed the proposed Framer design closely, the only noticeable deviation is the extra right-padding of past transaction values and the minor differences regarding certain icons. The reason for adding this extra space to the right of the items was to align them with the overall account balance. Thereby, the padding corresponds to the width of the caret-icon, which is used as a signifier to indicate the expandability of the account element.

4.1.7 Changes to receive screen

The only changes in `app/screens/receive-bitcoin-screen/receive-screen.tsx` were swapping the position of Onchain and Paycode and truncating the Onchain address. Thanks to this truncation, the address and the copy and share buttons are now on the same horizontal line, leaving the first and last few characters so that the user can still verify the address's validity. Other changes to this screen mostly focused on the correct color association, as in 4.1, and the visual separation of the two currencies.



Abbildung 4.7: Receive Stable-sats via Onchain design

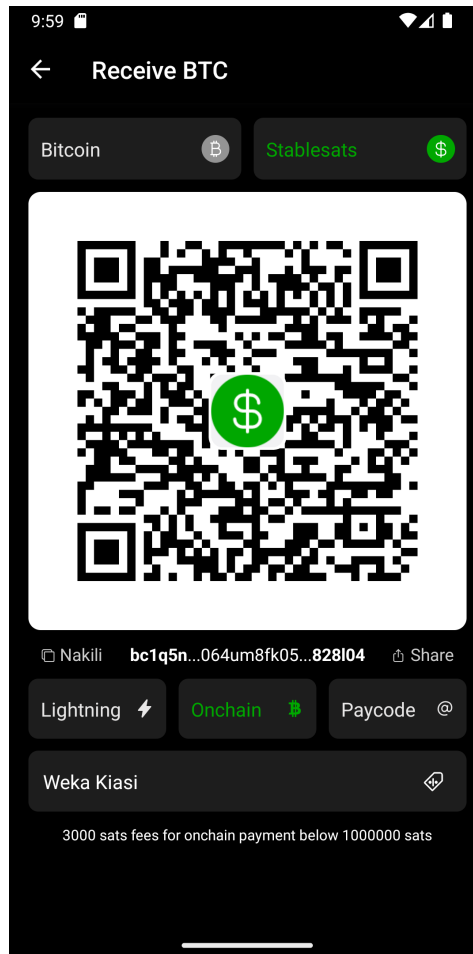


Abbildung 4.8: Receive Stable-sats via Onchain implementation

The design in Framer, visible in figure 4.7, colored the items of the actions *tap to set amount* and *add note* in the color of the selected currency. Given that these actions do not differentiate between the two currencies, the implementation dropped this proposal. Even though not planned in the design, the QR logo was changed to reflect the currently selected account, as visible in figure 4.8, and the Stablesats logo in the topmost button group was changed from a black to a white dollar sign accordingly. Therefore, `app/screens/receive-bitcoin-screen/qr-view.tsx` had to be modified and its logo replaced. Removing the *add*

note element is an unclear and unexplored tradeoff between gaining vertical space and merchants needing to label transactions for bookkeeping.

Figure 4.9 lacks the option to set an amount, a choice which was made due to the reasons mentioned in section 3.3.3. The given reasons were sound and made a valid point, however, novice users might lack insight to why the option was left away. Upon further consideration, aiming for consistency was deemed more vital to the user experience, especially with illiterate users in mind. By taking a look at the other two possible methods to receive funds, Lightning and Onchain, it becomes clear that both of them allow the user to set an amount.



Abbildung 4.9: Receive Bitcoin via Paycode design

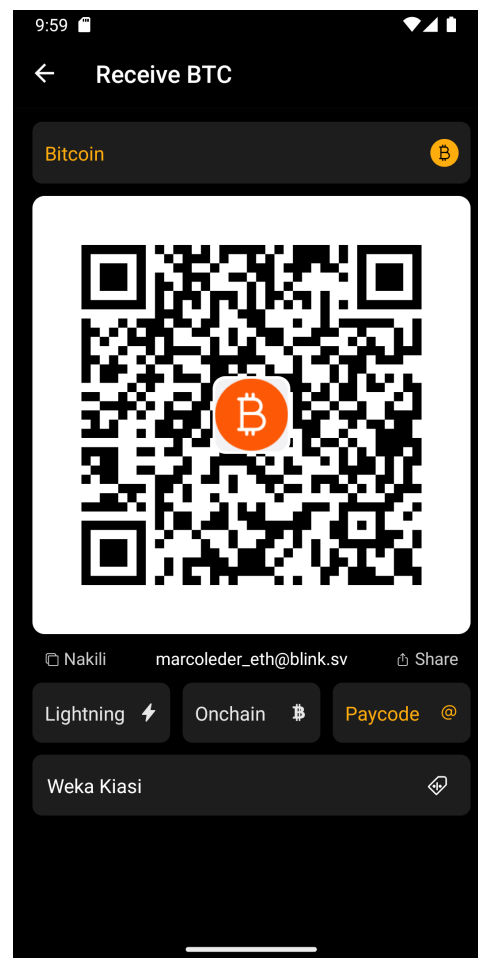


Abbildung 4.10: Receive Bitcoin via Paycode implementation

Thus, allowing the user to also set an amount in the Paycode variant contributes to the overall consistency of the wallet without introducing any issues or confusion. With the Paycode being similar to an email address, it could even be argued that the Paycode variant could serve as the main receiving method for inexperienced users. In comparison to the Lightning payment method, the address format is human-readable, allowing for easier verification of the address's validity. Hence the Paycode option could be used in the

same manner as the Lightning invoice, making the ability to set an amount vital. Since the Paycode option is only available for Bitcoin, as mentioned in section 3.3.3, tapping on it automatically switches the currency to Bitcoin. In fact, the topmost button group drops the ability to select Stablesats as soon as Paycode is selected, visible in figure 4.10.

4.1.8 Changes to send screen

Previously, the ability to send to a contact was deeply nested within the hierarchical structure of the application. Now, thanks to the from the ground up newly redesigned UX and interaction flow when sending to a contact, the scrollable contacts list is directly visible below the input field and allows the user to send money with only a few taps.

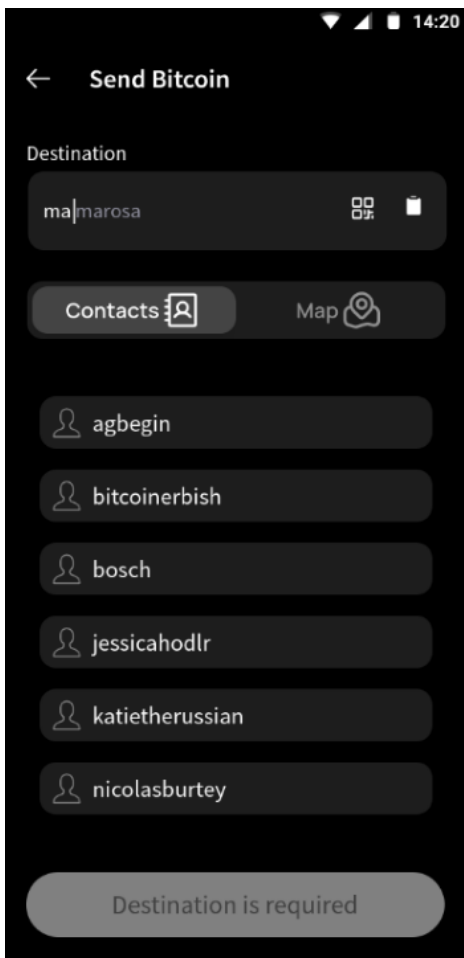


Abbildung 4.11: Send contacts screen design

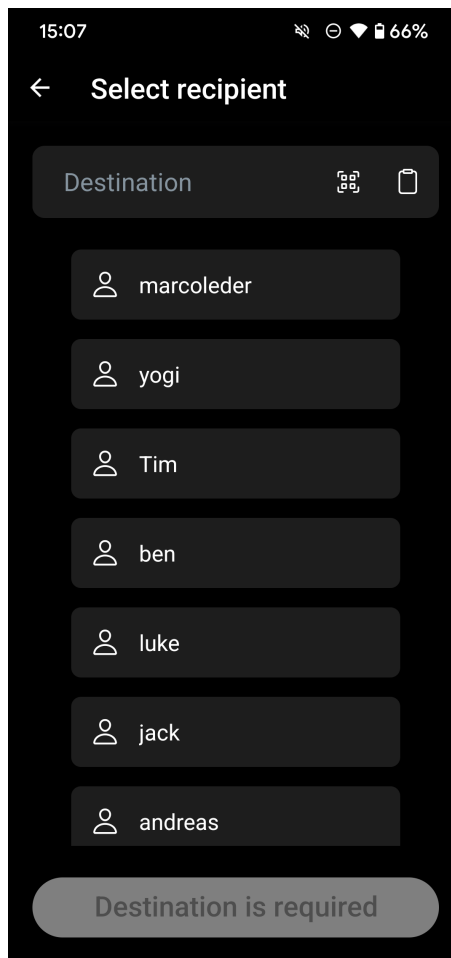


Abbildung 4.12: Send contacts screen implementation

Like in the original application, entering the name of the destination automatically starts to filter the scroll list of all contacts, matching both the pretty name and the username. Looking at the two designs, it becomes evident that the designed variant in figure 4.11 exhibits the IOS style segmented picker, but the implemented screen in figure 4.12 lacks this functionality. Consequently, the map feature is not present on this screen; in fact, it

has been removed entirely from the implementation, leaving the question of why. The map screen only would have made sense if merchants in Kibera were actively onboarded and added to the map. Given the time constraints of this thesis, onboarding and instruction of local merchants would have been out of scope, and the map was left away. Both the onboarding of merchants as well as the implementation of the map screen and the toggle in the wallet can be considered possible future work, highlighted in section 6.3.

When selecting a contact from the list, the search bar automatically fills the contact's name, allowing changes to the name if necessary. Combined with filtering the list upon text entry, the resulting interaction principles are similar to a system with autofill functionality, where completion is facilitated by pressing on a list item from the filtered list. In `app/screens/send-bitcoin-screen/send-bitcoin-destination-screen.tsx` the input field was altered from a `TextInput` from `react-native` to a `SearchBar` from `rneui/base`, introducing an `x`-icon to the left of the scan icon for clearing the input instead of using backspace. Since the list and the input bar share the same state, pressing the `x`-icon, visible in figure 4.13, clears both the text in the search bar and the selected item in the contacts list.

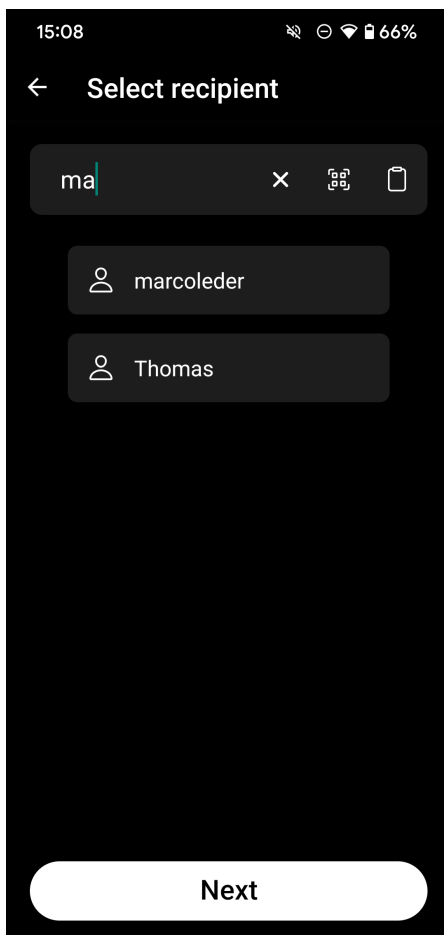


Abbildung 4.13: Send screen autofill implementation

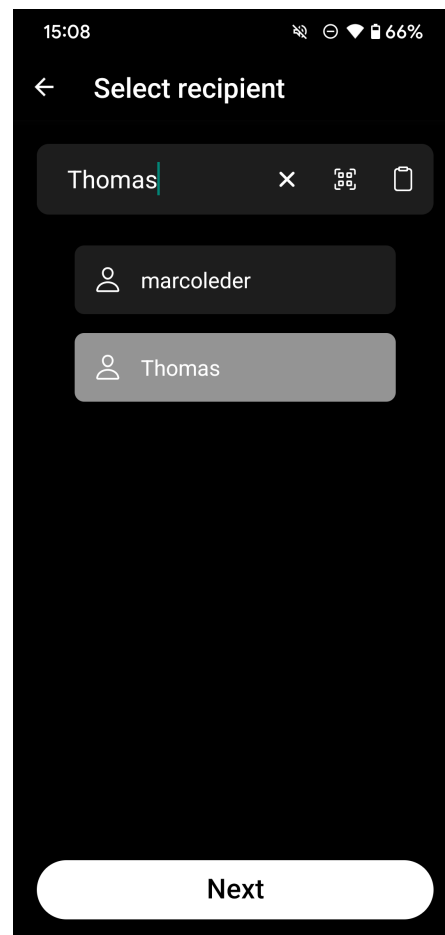


Abbildung 4.14: Send screen selection implementation

For selecting a new item from the list, the search bar content does not need to be cleared beforehand but instead is overwritten by the new selection. Another benefit of this new

contact list is that the user can, without typing anything, directly tap on a contact from the list to send money to. When pressing on a contact list item, the element is visually highlighted to signify to the user which item is currently selected as visible in figure 4.14. The length of the scroll list is dynamic, expanding as much as possible to fill the screen, ensuring that both small and larger screens benefit from the newly introduced functionality. The contact list is empty if the user enters a destination not in his contacts or never sent money to.

Thereby, the AfriBit wallet displays a text warning in the user's language that this address has never been sent money to. This was done by modifying `app/screens/send-bitcoin-screen/destination-information.tsx` to ensure that the user is informed about the state of his entered destination. Minor deviations from the proposed design constitute iconography and screen titles representing one of the current steps in the process of sending funds, *select recipient*, *select account*, or *confirm payment*.

4.1.9 Changes to confirm screen

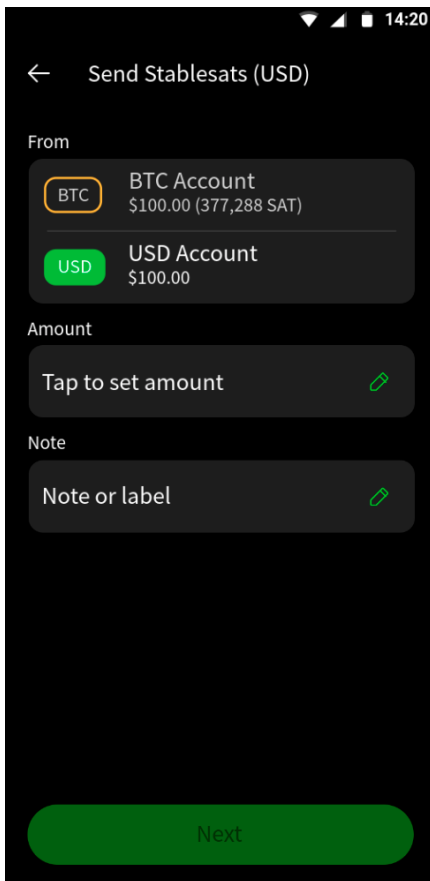


Abbildung 4.15: Send details design

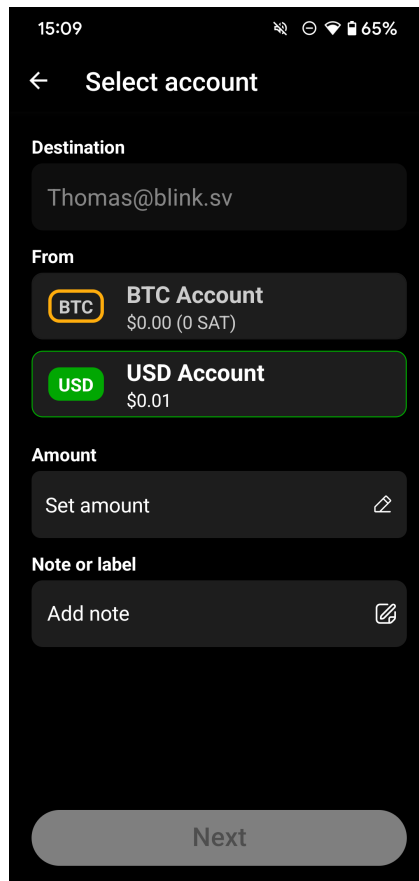


Abbildung 4.16: Send details implementation

The wallet-modal in `app/screens/send-bitcoin-screen/send-bitcoin-details-screen.tsx` was replaced with a `TouchableWithoutFeedback` from `react-native` to facilitate the selection of which account to debit. Thereby, the line divider in the designed screen in figure 4.15

was removed, and the accounts split into two individual elements, allowing for a border around the account as a further signifier of the current selection, as depicted in figure 4.16. Similar to section 4.1.7, the implementation waives the according coloring of the *set amount* and *add note* icons. Furthermore, the title *select account* reflects the current stage of the transaction interaction flow. The inclusion of the destination on the top of the screen was the last deviation from the implementation compared to the design.

4.1.10 hitSlop

The hitSlop property of react-native touchables[1] allows expanding the area of possible interaction around elements without changing the visual appearance of the elements[59]. In the context of the implementation, this property was used to increase the touchable area of certain elements to ease the interaction for certain users. This effectively allows the application to work as expected, even if less accurate touch input occurs, which might be the case for elderly or handicapped people.

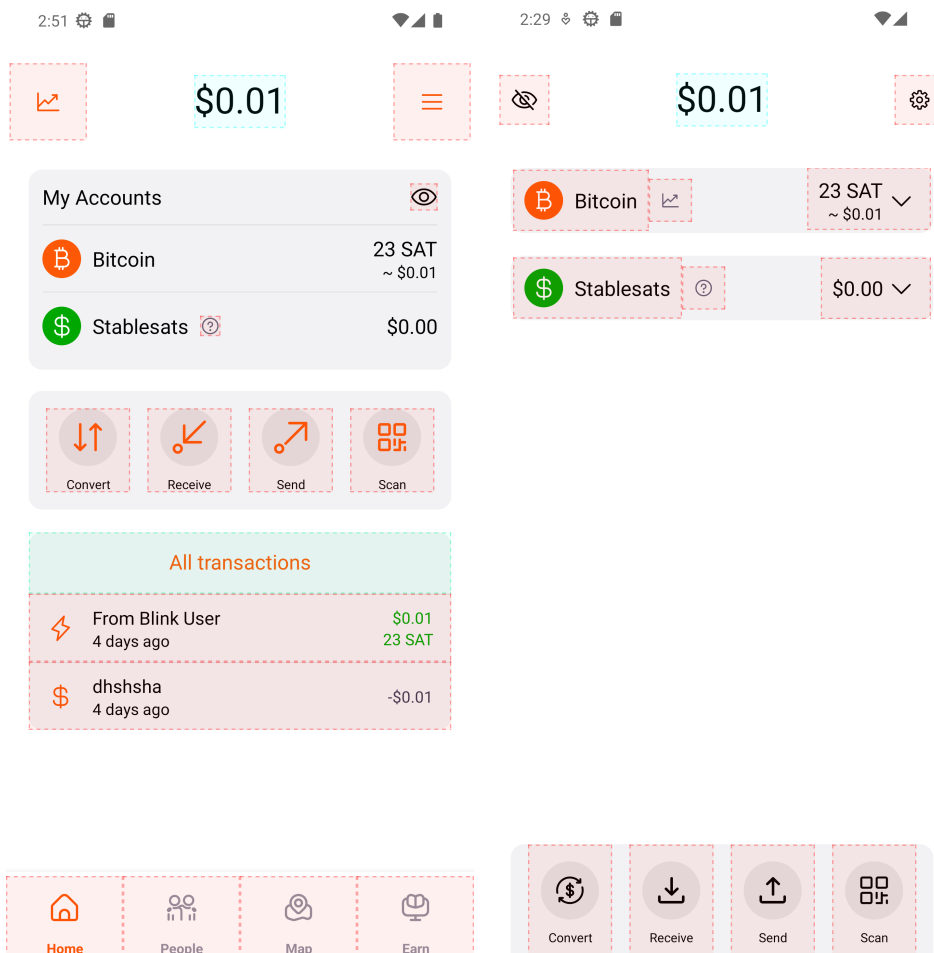


Abbildung 4.17: Blink home screen pressables

Abbildung 4.18: AfriBit implemented home screen pressables

Figure 4.17 shows the application interface of Blink in the light mode to better depict

the touch area of the items visually. Thereby, it becomes evident that the Bitcoin and Stablesats account logo and title do not offer any touch-based interaction. In contrast, figure 4.18 demonstrates that the Bitcoin and Stablesats account titles and logos support touch-based interaction to open the whole transaction history of the respective account but lack any signifiers. The knowledge required for the user to press on the logo and title group in the new version therefore is referred to as *knowledge in the head*[71], since the information is not visually conveyed and needs to be learned by the user through exploration and repetition.

Kapitel 5

Evaluation

5.1 Methodology

5.1.1 User Testing Session

Participants were gathered to test both the Blink and AfriBit wallets in the user testing sessions. Thereby, two participant groups spanning ten people each, one comprising residents from Kenya and the other students from Switzerland, were included in the study. This allowed for direct feedback from the target group while ensuring more samples by recruiting Swiss students. Each of the 20 participants examined both the Blink and AfriBit wallet, always starting with the Blink app first. Starting with the Blink app allowed the users to get familiar with the fundamental concepts of a wallet and to have a point of reference when testing the AfriBit wallet. It is important to note that in this approach, the learning curve plays a crucial role, as participants encountering the AfriBit wallet already have a certain level of knowledge. Therefore, certain aspects of the AfriBit wallet can not be attributed to the UI improvements but underlie the learning effect. To measure the extent of this learning curve, elements that were not altered in the AfriBit wallet were explicitly included in the metrics of the quantitative analysis. This allows us to compare how users performed in consistent UI areas across both wallets, indicating how much of an impact the learning curve plays.

The changes introduced to the AfriBit wallet closely focused on improving the logical connections between elements and minimizing hierarchical nesting. We recall that this was done to make the wallet suitable for users with low reading and writing expertise. Therefore, the changes not primarily targeted the underlying functionality of the application but rather the UI. Given that some people from the target group were illiterate, a question that arose prior to conducting the user study was how to find participants in Switzerland who were illiterate. In Switzerland, the illiteracy rate is relatively low, therefore, a method to mimic the illiteracy for Swiss participants had to be found. This was achieved by presenting the participants the application in a language they were not familiar with, namely Swahili. Even though the Swiss study group members knew how to read and write, they could not understand the Swahili language, therefore serving as a proxy for illiteracy.

5.1.1.1 Goals

The goals of the user testing sessions were multi-faceted. Evaluating whether the AfriBit wallet UI was beneficial and led to a better UX marked the first goal. Beneficial in this sense means that the UI changes should allow the user to complete the tasks faster and reduce the error rate. To measure this, the interactions were screen recorded as explained in section 5.1.2 and later analyzed in section 5.2.1. Additionally, observations and patterns were gathered from the video material and direct feedback from the participants was collected through a survey.

The second goal was to quantitatively measure the UI changes' impact on certain aspects of the application, both in terms of UI and UX. This means a general sentiment of the application's usability or certain aspects should be considered. To achieve this goal, a usability questionnaire was handed out to the participants after completing the tasks for each wallet. As elicited in section 5.1.3, this is shown to be a standard procedure and one of the most common methods for evaluating the usability of an application[40].

Last but not least, the third goal was to be able to distinguish if a particular change negatively impacted usability. The formulation of this goal might seem counterintuitive at first, but due to the learning effect, it had to be formulated as such. Thereby, a quantitative analysis was conducted to measure the time participants took on specific sections or screens. These timings were then compared across both wallets and served as an indicator of the change in usability. Important to note here is the definition of usability as to whether the participants could execute these functions at the same speed or faster.

5.1.1.2 Tasks

In total, there were three tasks backed by the following reasoning of considerations, constraints, and requirements:

1. Receive a payment of 10'000 sats via the Lightning Network
 2. Convert 5'000 sats to Stablesats
 3. Send 1 USD in Stablesats to the user marcoleder
- The tasks should be as close to real-world scenarios as possible
 - Participants should incur as little fees and spend as little time as possible
 - To test the effectiveness of the UI changes, the tasks must span areas of the application that were altered
 - To evaluate the changes in the visually distinctive coloring of the two currencies, the tasks should include both currencies

These tasks were identical for both wallets and had to be completed in the same order, ensuring that participants used the same functionality in both wallets while minimizing as many extraneous factors as possible to allow for a direct comparison. Because receiving and sending money are common daily tasks, they were chosen to satisfy the first requirement. Functions like paying a business were discarded as they required external services or were not feasible in the AfriBit wallet. Secondly, receiving and sending via the Lightning Network seemed to be the most suitable way to send money for this study, as it is fast and cheap. Since both the receiving and sending screens have been altered, the third consideration of testing revised sections was also satisfied. The receiving task was formulated in sats, whereas the sending task was formulated in Stablesats, ensuring that the participants interacted with both currencies, satisfying the fourth constraint. An intermediary step was also necessary to give the user access to a positive balance for both currencies. Therefore, the conversion task was added, allowing us to test further whether the two wallets' terms were understandable. An additional benefit was that receiving real money incentivized the participants to participate in the study.

After conducting the study, it became apparent that task 1 contained an imprecise formulation that led to missing data points in the quantitative evaluation. Instead of stating that the participants should *receive* a payment, the participants should have been asked to *request* a payment of 10'000 sats via the Lightning Network. This is a silver-lining formulation mistake, which led the participants not to act in setting the amount but instead wait for the sender to send the exact amount. However, this was only present in the Kiberan group, where in-person observation could not be conducted. With all participants from the Swiss group having set the amount and inherently, therefore *requested* a payment, this stark contrast could also be attributed to the language barrier. As we had to instruct Ronnie Mdawida to conduct the user testing sessions, the inevitable loss of information due to misunderstandings might have interfered with the role of Ronnie Mdawida as a supervisor. Both the inadequate choice of words and the language barrier therefore led to all Kenyan users not setting the amount in task 1.

5.1.1.3 Think aloud evaluation

In order to get more insight into the thought process of the participants, a think-aloud evaluation was conducted. A think-aloud evaluation is often employed in the context of usability and interaction testing, where the participants are encouraged to speak as they progress through the interface[63]. By doing so, users express their thoughts while completing a task, eliciting their motives and actions behind the interaction. This is especially crucial if a participant descends into a different hierarchical path than intended because by speaking out loud, the reasoning behind why this path was taken and what the expected outcome was become evident. Additionally, the think-aloud evaluation shows the participants' mental model of the application, which indicates how the UI changes influenced the participant's understanding of the product. Section 5.1.2 refers to the video recordings of the sessions, which allowed for revisiting the participant's interactions and thoughts. All participants explicitly agreed to the video recording in the distributed usability form and had the possibility to opt-out at any stage. These insights into the mental model shaped the analysis and further outlook on improving the application.

5.1.1.4 Usability Questionnaire

After completing the tasks for both wallets, the participants were asked to fill out a usability questionnaire. Each wallet had its separate questionnaire, whereas the questions, screenshots, and overall content remained the same. The questionnaire established a common ground between the participants by showing screenshots with highlighted areas with boxes. The usability form of Blink can be found in appendix F and AfriBit in appendix G, respectively, whereas the Google Forms had to be adjusted to show the full labels of the scale. Each participant filled out the corresponding survey after the walkthrough of the respective wallet while their experience was fresh in their heads. Thereby, the people had to give themselves the same pseudonym, allowing for the matching of the results of the two questionnaires. For creating the questionnaire, the Usability Experience Questionnaire (UEQ) from Laugwitz et al.[40], an established standard, served as inspiration and guidance.

Another considered contestant was the System Usability Scale (SUS)[61], which is also a well-established standard. However, the SUS only consists of ten predefined questions, thus not suitable for the scope of this thesis. Estimating the overall usability would have been possible with the SUS, however, specific details and changed items needed to be analyzed too, demanding a solution tailored to the application. In usability tests, as stated by Schrepp et al.[68], page 40, *the number of observed problems and the time participants need to solve tasks are quantitative indicators for the UX quality of a product*". Therefore, the UEQ was used as it allowed to quantitatively measure the usability of an interface by the use of a well-established scale, with half of the selected adjectives appearing in the short version of the UEQ (UEQ-S)[69]. Two of the adjectives that appear in UEQ-S cover *perspicuity*, while the other two cover *efficiency* and *dependability*. *Perspicuity*, how hard it is to get to know the product; *efficiency*, how effortless and fast tasks can be completed; and *dependability*, how the feedback and control are balanced between the product and the user, are considered to be pragmatic quality indicators, known as goal-directed[68]. Pragmatic thereby refers to an application's ease of use and usability, whereas hedonic quality covers a product's experience and emotional aspects, which is not goal-directed[68]. Ultimately, they all influence the product's valence dimension *attractiveness*, identified by adjectives such as annoying, bad, or enjoyable[68].

The UEQ utilizes a semantic differential scale[64], meaning that terms with opposite meanings are used on each side of the spectrum. This choice was made to eliminate the central tendency bias by presenting an odd number of options to choose from, namely seven, and to ensure a standardized format[40]. Consequently, the answers take values from +3 for fully agreeing with the positive term on the right to -3 for fully agreeing with the negative term on the left[68]. The UEQ consists of six sections, three of which were mentioned in the paragraph above: *perspicuity*, *efficiency*, and *dependability*[40]. The two hedonic quality indicators, *stimulation* and *novelty*, complement the three pragmatic quality sections[40]. Stimulation refers to the motivation to use the product, whereas novelty refers to the innovative aspects of the application[68]. Given that examining the usability of the application is vital to this thesis, the novelty aspect was completely excluded from the questionnaire, and the stimulation aspect was minimized with only one related question. Therefore, the final adjectives used in the UEQ were chosen based on a specifically chosen combination of the papers by Schrepp et al.[67–69].

5.1.2 Video Analysis

Each session was screen recorded which allowed to capture the interaction of the participants with the application. Wherever possible, the screen recordings were conducted in a quiet environment and captured both the microphone and the taps on the screen. These taps, combined with the think-aloud evaluation captured by the microphone, allowed for greater insight into the interaction. The video analysis served as a basis for both the qualitative and quantitative analysis.

5.1.2.1 Benefits

Videotaping the sessions allowed for a second analysis of specific problematic interactions and more profound insight. This additional revisiting of past interactions greatly extended the notes from the hands-on sessions. Furthermore, the video material laid the basis for measuring participants' time on various application sections, the quantitative measurements 5.1.3. Due to the variations highlighted in the section 5.1.2.2, the idea of automated time measurements in the code was abandoned. The manual extraction of the times was chosen as the more suitable method for collecting these timestamps and using the video material gathered.

5.1.2.2 Limitations

Even though the video material captured microphone and touch-based interactions wherever possible, in certain cases, the recording was not as high in quality as desired. The lower quality of the recordings refers to the lack of any audio stream, cut-off video files, slow internet, or the lack of touch-based interactions. Additionally, not all participants performed the think-aloud evaluation to the same extent. These issues could not be addressed in real-time without physical presence at the user testing sessions in Kibera. Since the video material and questionnaire were the only sources of information regarding the group from Kenya, these limiting factors had to be considered in the analysis. Given this situation, a manual analysis and time measurement of the video material was conducted, which is explained in section 5.1.3. An automatic analysis, such as recording the timestamps in the application log, was deemed unfeasible because the video material was susceptible to two crucial variations in the data:

1. Participants made misclicks or used an explorative approach before arriving at the correct functionality, thereby leading to unpredictable durations
2. Participants executed a think-aloud evaluation, meaning that the speed of speaking would have had a notable influence on the total duration of the task

5.1.3 Quantitative measurements

The second goal of this thesis was to quantitatively measure the impact of the changes in the AfriBit wallet in terms of UI and UX. As highlighted in section 5.1.1.4, the UEQ addressed this measurement and was handed out to the participants after completing each wallet's tasks. Since the UEQ gathered data through a numbered scale, the data is quantitative and can be evaluated using statistical methods.

The third and last goal of the user study was to ensure that changes in the AfriBit application did not introduce new problems or worsen its usability and interaction. To evaluate this quantitatively, participants first interacted with the Blink wallet, where they had to execute specific functions to achieve their tasks. Then, they transitioned to the AfriBit wallet, where they had to execute the same functions; however, these functions' placement, look, and feel might have changed. Inherently, functions that remain the same across both wallets should underlie a learning curve, meaning that the participants should be able to execute these functions at the same speed or faster in the AfriBit wallet. **If** the participant exhibits a learning effect in the non-altered functions **but** simultaneously experiences a decline in the speed of finding and executing overhauled functions, this change can be attributed to bad UI changes. Meaning that even though the participants are familiar with the functionality, the UI changes slowed them down in the AfriBit wallet compared to the *initial* contact with the Blink application. Utilizing this approach allows us to conclude if the interaction or usability had declined in the AfriBit wallet compared to the original Blink application. However, we can not state whether the usability has improved, as shorter execution times could also be attributed to the learning curve effect.

Due to the mentioned limitations of the video recordings in section 5.1.2.2, the time measurements of specific application sections were taken and did not span the whole task. We chose to take two measurements per task, leaving us with six measurements per participant. In each task, one of the time measurements refers to the time the participant spent on a section of the application that remained consistent across both wallets. The chosen section was the screen where the participant had to set the amount of money to receive, convert, or send. The other time measurement refers to the time the participant spent finding the respective function for the task on the home screen, whereas the home screen differs between the two wallets.

Since the consistent section is identical across both wallets, the total data points would span 120 measurements. However, we recall from section 5.1.1.2 that the usability form exhibited a wrong wording, which accounted for the non-existence of quantitative data for the setting of the amount of task 1, accounting for the loss of 20 data points. An additional four measurements had to be marked with NA (not applicable) as elicited in section 5.1.3.1; therefore, the number of data points comprises 96 time-readings in total. We can draw conclusions about the learning curve by taking 96 measurements of a section that remained consistent through all user experience sessions. Furthermore, with the use of quantiles-quantiles plots (QQ-plots)[15] we have analyzed in section 5.2.3 if the data follows the normal distribution[43]. Therefore, the statistical results can be framed in their context and put into perspective.

To measure the time, the video material was imported into the video editing Kdenlive[77]. The frame rate was set to 30 frames per second, which is important to note since the time measurements were taken by counting the seconds and remaining frames. Cuts were made each time the interface was loaded entirely, meaning that all numbers and elements were rendered and that animations had finished. This mitigates the differences in hardware, internet speed, and video quality of the participant's devices. The time it took participants was then noted into a spreadsheet in the following format: $SS:FF$ where SS refers to the seconds and FF to the remaining frames of the next second. Since no measurement except for one surpassed the 60-second mark, the minutes were not noted. Since all videos were converted to 30 frames per second, the frames could be converted to milliseconds using the following formula: $SS + FF/30$. This results in the measurements being in the floating point format of seconds.

5.1.3.1 Limitations

A problem that arose specifically in the Blink wallet context was that the iPhone IOS application did not offer the ability to convert between Stablesats and Bitcoin directly. Therefore, participants who downloaded the Blink application onto an iPhone could not complete task 2, and the time measurements were missing, marked with *IOS*. Having seen that this was a problem in the group from Kenya, the Swiss students who had an iPhone were given access to an Android device (Google Pixel 6 Pro) for the user testing session. The AfriBit wallet did not suffer from this issue since the application was for Android as an Android Package Kit (APK) file. Hence, this issue could be mostly, with one exception, condemned to the Kenyan group testing the Blink wallet and thereby is an explanation of the missing values for two out of the ten Kibera residents. Upon consultation with the Galoy team, they confirmed that this is due to the AppStore policy from Apple. First of all, transactions to unlock features or functionality within the app must be processed through Apple's in-app purchase system, whereas the feature of receiving Stablesats most likely falls under this category[35]. Secondly, the app can only utilize approved exchanges with proper licensing and permissions, which might not be the case and therefore violate section 3.1.5 of Apple's App Store Review Guidelines[36]. Therefore, the Bitcoin to Stablesats conversion functionality is only covered by the Android application, which is the primary reason why the user testing of the AfriBit wallet was conducted primarily on Android devices. A second reason was that onboarding each iPhone user to Apple TestFlight[7], as well as having to rent a MacOS-capable device to build the IOS application, would have presented too much overhead.

5.1.4 Qualitative Analysis

The methodology of how the qualitative analysis was conducted is based on observation and categorization. The gathered video material was reviewed, and common patterns were identified. The categorization of these items played a vital role in establishing trends of both problematic and beneficial aspects of the application. Furthermore, the qualitative analysis was influenced by the notes, comments during the think-aloud evaluation, and observations originating from the in-person sessions.

5.2 Results

5.2.1 Qualitative observations

The first goal of the user study was to qualitatively assess if the AfriBit wallet UI was beneficial and led to a better user experience, as mentioned in the goals of section 5.1.1.1. The following categories were established for classifying the observations:

- **UI:** *Observations related to how the UI was organized and structured*
For the first task, receiving sats via the Lightning Network, some users started to search for Lightning already on the home screen and did not find it. Only when they navigated to the receive screen did they find the Lightning option. However, a positive observation was that users immediately knew that Lightning was selected when opening the receive screen. This indicates that the UI successfully conveyed the state to the user. In contrast, the screen to convert from Bitcoin to Stablesats was not as intuitive, with users assuming that the section with the top two accounts is used for conducting the swap. They tried tapping on the convert logo between them to start the conversion, however, this icon indicates the direction of the conversion. This observation leads to the conclusion that the UI of the conversion screen needs to more explicitly highlight the direction of the swap and where user input is needed. The general process and required actions were not clear to the users. After converting, the past transactions allowed the users to intuitively check if everything worked, and almost all participants had no issues with the process of verifying.
- **Icons:** *Patterns related to the design, placement, and understanding of the Icons*
Generally, the icons designed by the Galoy team were perceived well and could be identified quickly by the people. This is especially true for the icons related to the functions of the wallet, such as convert, receive, and send. However, the new icons in the AfriBit application were not always well perceived. Participants stated that they show similarities with icons they associate with *download* or *email inbox*, which was not the goal of using the certified Bitcoin icons[37]. This applies to all the wallet functions except the convert icon, which was stated to be superior and more intuitive. Regardless of this observation, all participants were able to identify the function of each icon and were able to execute the tasks accordingly. Nevertheless, overall, the choice of icons was perceived as a downgrade compared to the original Blink application. Thus, it follows that the icons should favorably be changed back in future versions of the AfriBit application. Additionally, the new icon for the *set amount* button was said to be confusing, rather resembling a price tag or discount than setting the amount.
- **Usability / Interaction:** *Discoveries of how the users interacted and used functions*
A problem that arose in the receive screen was the interaction with the scrollable area. When users wanted to scroll down to set the amount or see all options, they scrolled on the scrollable area where the QR code was embedded. However, tapping the QR code copies the invoice, unintentionally copying it while scrolling. To add to this, this often arose before having set the amount, making the copied information worthless most of the time.

Finally, copying the invoice via the QR shows a toast notification, which obfuscates the option to set the amount, making the user wait for the toast to disappear. However, users who already had experience and knew the behavior scrolled not on the QR code but rather on the button group for selecting the network, such as Lightning. Thereby, the QR code was not tapped, and no information was copied. Still on the receive screen, one of the participants tried to set the amount to receive by pressing on the Bitcoin identifier in the topmost button group. Another user thought that the Bitcoin icon next to the Onchain button, which is for choosing the network, is to set the amount. This participant was also the only one to have selected the wrong network for receiving the funds. This shows that the Bitcoin icon is associated with setting the amount for two subjects in the field study. Future exploration of this thought could be to dynamically switch the icon between the Bitcoin and Stablesats logo, indicating of which currency the amount shall be set.

Regarding the screen for converting between the two currencies, most of the participants had issues understanding the topmost section, which shows the two accounts. For most, the direction of the swap was not clear because the icon has both an arrow pointing up and an arrow pointing down. However, most of them resorted to reading this section top-down, meaning that the top account is the account to send *from* and the bottom one to *receive* to. The users could not anticipate the general interaction sequence; most were unaware that they had to set the amount in the same way when receiving funds. On the note of setting the amount, most people did not grasp the concept that the unit of input can be set and started converting the amounts in their heads. This indicates that even though the other unit was shown below, people interpreted it only as a way to see the amount expressed in another format but not being able to switch between the formats. Lastly, many participants lacked any indication that the amount could already be input and first tried to tap on the input field in the hope of getting any visual feedback, such as a cursor, that the application was ready for input. This issue will be further discussed later on.

Overall, the new method of having the account highlighted when selecting in the sending process brings all the stressed benefits from section 3.3.5. Users immediately noticed that they could select which account to debit and, at a glance, saw the balances of both accounts. This resulted in a 50% reduction in sending the wrong currency, with only four people having sent from the wrong account in the AfriBit wallet compared to eight people in the Blink wallet. Furthermore, the new design received positive comments, as the border around the account allowed the users to see which currently is selected. Another insight into the changed AfriBit wallet was that each and every participant was able to select the recipient in task 3 directly from the new contacts list. This is a strong indicator that the usability is good and interaction principles are well known, leaving no user with the need to type the destination address. Last but not least, a general remark that applied to both wallets was that the green tick animation after executing an action helps interpret the feedback that the action has succeeded. Many participants took the green tick animation already as a sign of success and did not check for the balance change or transaction history anymore.

Another interesting observation regarding confirming if a transaction was successful was that most of the Swiss students checked this via the balance rather than the history. This could be an indicator of the cultural differences between the two groups, as the Kenyan participants were more likely to check the history or rely on the green tick animation.

- **Accessibility:** *Learnings about which parts fostered inclusion and great usability*
Having the application displayed in a language that the user does not know has allowed us to mimic the illiteracy of the target group. Thereby, many users stated that they were unaware of what *ada* means, which is Swahili for *fee*, in the screen where they had to confirm the sending of funds. This could imply that the method of conveying the information about the fee as text is not a suitable medium, and other methods, such as a graphical representation, should be explored.

In the conversion screen, most users explicitly stated that the percentage buttons were unclear to them. Largely, this concerned novice users, unfamiliar with previous online banking or cryptocurrency wallets. Some of them showed risk-averse behavior, not touching the percentage buttons at all, in anxiety that they might break something or even lose money. Other users tested the functionality of the buttons in an explorative approach, again suggesting that the percentage buttons were not clear only by looking at them. Only one user stated from the beginning of seeing the screen that he knew what the buttons do and proceeded with swapping 50% of his funds. Another accessibility issue that arose was that people did not feel confident enough that they were on the right screen of the application when solving the tasks. Many of them switched through the whole application only to realize that they had been in the correct section of the app from the beginning. This indicates that the application should provide more guidance to the user, for example, a progress bar in a longer process, such as sending funds or a more explicit indication of the current section.

- **Comprehension:** *Insights of the understanding of terms, tasks, and the current state*
As mentioned in 5.1.1.2, task 1 was formulated misleading, stating that users shall receive a payment instead of requesting it. This was a discovery not only in the quantitative analysis but also in the qualitative analysis, with some participants assuming that the money was already in the wallet. Another discovery was that the participants did not understand the modal to choose the default account. The effects of choosing one or the other account were unclear, and users often just dismissed the modal again. A discovery regarding the modal was that it only appears after the user has received at least one transaction, so on the second payment to receive. Throughout both applications, the ability to set a note via the note field was recognized very well and used by a few participants, even though not stated in the tasks. From this, it can be concluded that the note field properly conveys its functionality and that even first-time users tend to estimate it as trivial.

A prominent issue regarding comprehension was the interpretation and meaning of terms. The terms sometimes made users unable to distinguish between the two currencies, a major problem. Firstly, the term *Lightning* is unclear, with participants searching for it all over the home screen, hoping to find this functionality there.

Secondly, participants had a variety of different interpretations of the "You have never sent money to this address" warning modal. Most of the participants were hesitant, and the interpretation spanned from thinking that this was the final confirmation of sending funds, over to a warning that the address is unsafe, to having to 100% trust the application or be aware of the possibility of losing funds. The wide variety of interpretations highlights the issue of illiteracy and the extensive use of text in this modal, which led to confusion. Lastly, the differentiation between the two currencies and the terms *sats* and *Stablesats*. It has to be noted that participants were given the information that one Bitcoin consists of one hundred million sats, indicating that sats refers to a fraction of a Bitcoin. Even though they had this information, the term *Stablesats* seems to be too similar to *sats*, leading to the assumption that *Stablesats* are the same as *sats*. This inaccurate mental model may have been promoted due to the appearance of the word fragment *sats* in *Stablesats*. The information that one Bitcoin consists of one hundred million sats, which is accurate and correctly reflects the working state of the Bitcoin currency, combined with the naming of *Stablesats* might have led to the assumption that *Stablesats* are a fraction of a Bitcoin, which showed itself in task 1, where participants received the wrong currency, namely *Stablesats*, even though the exercise was to receive sats. Furthermore, participants struggled with associating USD with *Stablesats*, leading to situations where they sent the amount of one USD equivalence of Bitcoin in task 3 instead of sending one *Stablesats*-dollar since the interface in the account selection only differentiated between USD and BTC, not mentioning *Stablesats*. The problematic aspect is that USD and *Stablesats* are both used throughout the system, unclear whether the terms are used interchangeably or have different meanings.

– **Miscellaneous:** *Other findings such as technical issues, bugs, or comments*

A small number of participants were automatically logged out after receiving their first funds without receiving an error message of any kind. Affected were smartphones from the brand Huawei[22]. It was observed that participants get prompted to rate the application, which could be the reason why phones lacking Google Play Services crash. When setting the amount and *Stablesats* being the selected currency, the screen only takes input in the unit USD and lacks the display of the equivalent amount in sats. Only then did participants realize that the wrong account had been selected. Except for a few people who thought manual conversion in the head was necessary, all participants concluded that they had to switch to Bitcoin in order to input sats. Last but not least, participants who received *Stablesats* instead of Bitcoin got stuck in task 2, converting from sats to *Stablesats*, since their balance of sats was zero. The mitigation for this issue was to receive additional funds in the correct currency or to swap in the opposite direction, from *Stablesats* to sats. Other participants tried to swap too large amounts, a problem observed throughout both applications and all tasks, elicited in the next paragraph.

The issues above highlight that the most crucial part is laying an adequate foundation of the used terms. The category *comprehension* spans multiple issues with problematic aspects that have led to serious usability problems. A further observation is participants' difficulties with the screen to set the desired amount. With this issue being present in both wallets and vital to all wallet functions, it will be elaborated in more detail.

Figure 5.1 shows the respective screen where the user is requested to enter the amount for sending or receiving. The first problem encountered was that participants struggled with identifying that the number buttons were indeed pressable. This can be attributed to the fact that the number buttons look grayed out and do not indicate that they can be pressed. Furthermore, they lack any form of visual signifier, such as an outline or button shape, indicating that they are pressable. Since the input field lacks any indication, such as a cursor, some participants thought they were first required to select the input field to write in it by tapping on it. However, the input field is always selected and the buttons are always pressable, what is missing are the signifiers[56] that inform the user that these actions are possible.

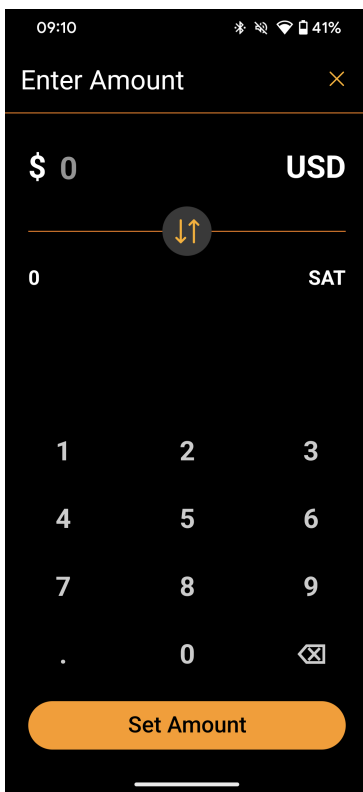


Abbildung 5.1: Enter amount

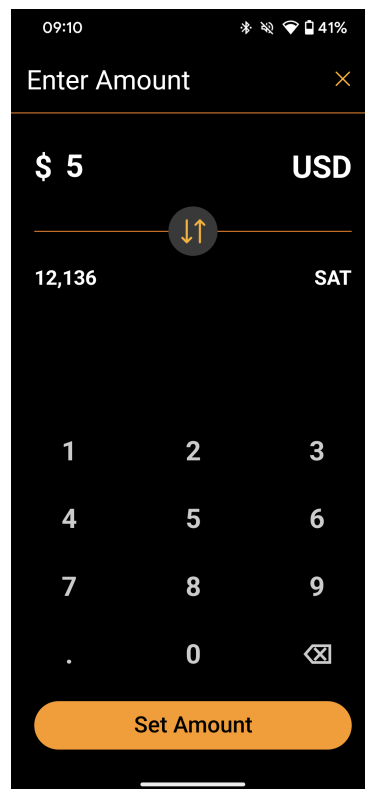


Abbildung 5.2: Enter USD

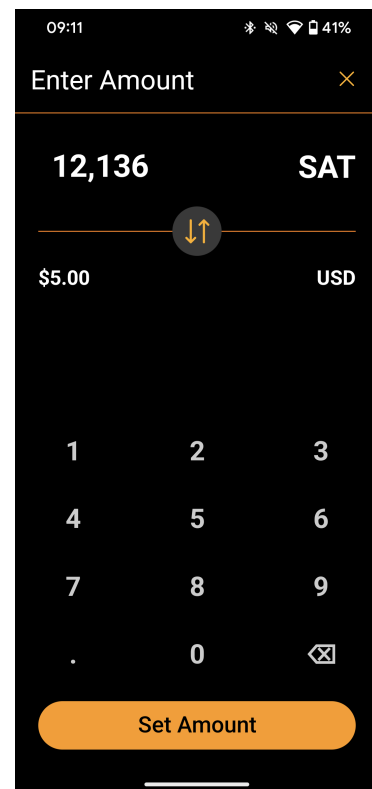


Abbildung 5.3: Enter SAT

Figure 5.2 shows the screen's state after inputting a certain amount. This representation is adequate, as the respective amount in the other currency (in this example, SAT) is displayed below. The button in the middle between the two currencies, separated by a line, allows the user to switch between the two currencies. Exactly there lies the problem that has led many participants to input the wrong amount: When switching currency, the amount stays fixed with respect to the currency, as visible in figure 5.3. In some scenarios this makes sense, however, in the sessions, it became apparent that this behavior leads to confusion, especially for new users. Since the screen defaults to entering the amount in USD, many people entered 5000 USD instead of 5000 SAT during the testing. When wanting to switch the currency, they expected that only the amount would change, but their input of 5000 remains. As this was not the case, many participants had to delete a 7-digit number and re-enter it in the other currency.

5.2.2 Quantitative UEQ results

Analysis and interpretation of the results from the UEQ survey are facilitated by the provided Excel data analysis tool file[2]. Appendix H shows the raw data from the survey, whereas appendix I shows the transformed data used for the calculations and the two sample T-Tests. The mean, standard deviation, and confidence level of each wallet are depicted in table 5.1, and the graphical representation thereof in figure 5.4, with the addition of showing the whole confidence interval for interpretation.

Tabelle 5.1: UEQ Survey result statistics

Scale	N	<i>Blink</i>			<i>AfriBit</i>		
		Mean	STD	CL	Mean	STD	CL
Attractiveness	20	1.85	1.06	0.46	2.20	0.83	0.37
Perspicuity	20	1.50	1.16	0.51	2.24	0.52	0.23
Efficiency	20	2.16	0.75	0.33	2.64	0.43	0.19
Dependability	20	1.88	0.85	0.37	2.46	0.45	0.20
Stimulation	20	2.20	0.95	0.42	2.70	0.57	0.25

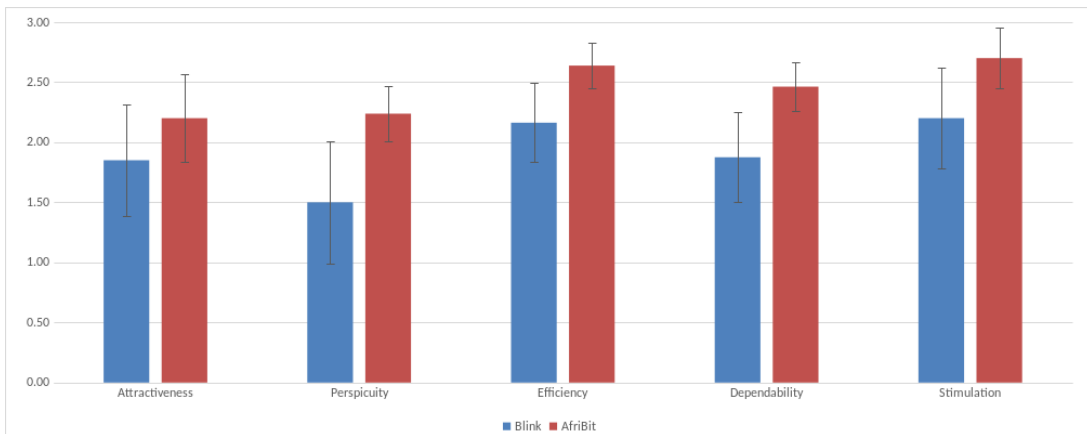


Abbildung 5.4: UEQ Survey results graphic

It can be visually confirmed that the mean of the AfriBit wallet in each scale, for example, *stimulation*, scores higher while exhibiting a smaller confidence interval across the board. Schrepp et al.[67] provide a guideline on how to interpret the results, stating that given two error bars of a scale do not overlap, the difference between the applications is significant regarding this category. Thus, factoring in the exact confidence intervals of appendix I, it becomes apparent that both *perspicuity* and *dependability* exhibit statistically significant differences. Furthermore, Schrepp et al.[67] stress that even though two error bars may overlap, the underlying difference can still be significant, requiring significance tests to be performed. The two sample T-Tests assuming unequal variances in appendix I yield that the scale *efficiency* also exhibits a significant difference. Thus, it can, with statistical significance, be concluded that the AfriBit wallet excels in its pragmatic quality, making it easier to understand the application (*perspicuity*), solve tasks with less effort (*efficiency*) and better predict the behavior and states of the system (*dependability*).

5.2.3 Quantitative time measurement results

Section 5.2.1 provided an overview of the qualitative observations from the conducted user study. This chapter will quantitatively support the aforementioned findings and statistically contrast the two wallets' time measurements from section 5.1.3. After the conversion of the time measurements in the format *SS:FF* to a standardized format in seconds and milliseconds *SS.MS*, the standard deviations were calculated. In addition to the calculation of the standard deviation of the whole scenario, the individual task standard deviations, as well as the standard deviations per group, were calculated, the calculations of which can be found in appendix B for the Blink wallet and appendix C for the AfriBit wallet, respectively. The raw data in seconds and milliseconds and the corresponding standard deviations for the Blink wallet are presented in table 5.2:

Tabelle 5.2: Blink time measurements

<i>Time in seconds [s]</i>	Home screen time			Set amount time		
	Task	1	2	3	1	2
Kibera group	2.37	5.00	3.03	N/A	15.50	14.03
	4.37	IOS	6.67	N/A	IOS	6.10
	1.37	10.40	3.03	N/A	7.13	3.33
	9.23	1.27	5.33	N/A	22.77	3.50
	4.03	3.07	3.03	N/A	error	5.03
	4.00	6.00	15.00	N/A	34.07	11.10
	5.07	IOS	13.03	N/A	IOS	11.13
	2.10	3.20	4.00	N/A	12.10	3.03
	3.97	13.43	4.73	N/A	4.23	4.67
	4.70	4.10	5.87	N/A	7.47	4.33
	Task Standard deviation	2.16	4.10	4.24	N/A	10.54
Group Standard deviation	3.60			8.21		
Swiss group	65.17	39.23	31.00	23.30	8.30	4.20
	16.27	IOS	27.27	13.23	IOS	5.20
	28.30	17.17	23.00	35.17	11.13	2.30
	17.13	1.20	23.10	45.23	7.27	2.10
	70.03	14.10	19.23	21.20	34.23	5.00
	41.43	8.30	3.33	20.27	9.43	1.20
	21.43	9.13	14.23	16.03	11.47	2.03
	24.37	20.13	4.47	11.03	7.07	1.47
	16.37	16.20	16.40	19.17	9.17	8.33
	14.47	19.47	14.33	8.30	3.27	2.37
	Task Standard deviation	20.65	10.60	9.03	11.26	8.95
Group Standard deviation	15.67			11.07		
Scenario Standard deviation	14.09			10.06		

Tabelle 5.3: AfriBit time measurements

<i>Time in seconds [s]</i>	Home screen time			Set amount time		
	Task	1	2	3	1	2
Kibera group	14.17	3.17	12.23	N/A	7.67	4.17
	9.23	22.77	3.17	N/A	6.30	4.50
	4.17	3.70	2.77	N/A	5.03	4.33
	4.87	4.60	3.67	N/A	9.63	2.67
	2.23	4.03	3.17	N/A	6.40	3.13
	8.37	4.07	3.07	N/A	18.17	19.13
	4.13	5.37	2.13	N/A	16.20	6.23
	12.10	4.43	2.33	N/A	6.30	13.17
	5.10	6.10	3.17	N/A	12.13	13.37
	3.20	3.17	1.57	N/A	21.33	4.47
Task Standard deviation	4.02	5.91	3.05	N/A	5.78	5.63
Group Standard deviation	4.53			5.82		
Swiss group	14.17	31.00	13.07	8.23	11.07	2.10
	8.10	9.03	9.13	6.03	7.00	3.17
	36.07	7.13	6.03	9.23	7.17	4.03
	17.07	10.17	4.00	12.37	8.33	7.20
	10.10	8.07	1.00	7.13	6.23	3.20
	6.30	4.27	2.07	10.40	11.17	1.40
	27.10	14.37	16.07	21.40	10.37	3.13
	18.03	4.20	2.10	7.13	18.30	2.20
	10.27	6.07	13.17	10.10	7.13	4.10
	12.17	12.10	4.07	15.10	15.20	4.10
Task Standard deviation	9.27	7.85	5.42	4.63	3.95	1.60
Group Standard deviation	8.29			4.85		
Scenario Standard deviation	7.21			5.23		

Table 5.3 represents the raw data in seconds and milliseconds and the corresponding standard deviations for the AfriBit wallet, respectively. The measurement data from the tables served as the basis for further statistical analysis. Thereby, the data points were imported and evaluated in R[74], whereas it is vital to recall that in both the Blink as well as the AfriBit wallet, the data of task 1 in *set amount time* for the Kibera group is missing, as elicited in section 5.1.1.2. Before conducting statistical hypothesis tests, both the data from the Blink measurements as well as from AfriBit were checked for being normally distributed using QQ-plots[15]. For each scenario, appendix B shows the QQ-plots for the individual groups and the overall scenario for the Blink wallet. Appendix C respectively shows the plots in the same arrangement for the AfriBit wallet. Thereby, the first column refers to the home screen time, whereas the second column shows the set amount time. The QQ-plots visually indicate that the data is not normally distributed since the data points do not closely follow the line which represents the normal distribution.

To confirm this observation not only graphically but also numerically, Shapiro-Wilk tests[65] were conducted to test for normality. A Shapiro-Wilk test's null hypothesis states that the data is normally distributed, which is the hypothesis to be tested against[65]. Thereby, six Shapiro-Wilk tests were conducted per wallet, four of which spanned each group in the respective screen scenario and two constituting the overall scenarios. All of the Shapiro-Wilk tests resulted in a p-value of less than 0.05, meaning that the null hypothesis can be rejected. Hence, the data does not follow a normal distribution, which can be attributed both to the relatively small sample size as well as the outliers, prominently occurring at the upper end of the spectrum, as visible in the QQ-plots. The exact values of the tests of the Blink wallet can be found in appendix B, vice-versa, the Shapiro-Wilk test results for the AfriBit wallet find themselves in appendix C.

Initially, it was planned to conduct a one-way analysis of variance (ANOVA) test, which would have allowed comparison of the means of more than two groups[66]. However, given that the data is not normally distributed, the population mean of the data does not reflect the underlying data well enough. Thus, conducting an ANOVA or a simple two-tailed t-test[62] would not have yielded valuable insights, as both of these methods rely on the average of the data. Therefore, the statistical method to be chosen had to take a more robust value for comparison than the mean into consideration. The median, the middle value of the ascendingly sorted data, presented itself as a suitable alternative, being more robust to outliers and suitable for not normally distributed data[72].

Thus, the Wilcoxon rank sum test with continuity correction, also known as *Mann-Whitney-U* test, was chosen as the statistical method[81]. This test allows statistically verifying the differences of the *median* between two groups, whereas two versions of the test were conducted: For the *set amount scenario*, three two-sided tests, one for each group and one for the total scenario, were conducted with the alternative hypothesis being that the median of the Blink wallet is different from the median of the AfriBit wallet. This was done to verify if a learning effect was present and if participants got faster over time in an area that remained consistent throughout both wallets. All three tests, the results of which are attached in appendix D, exhibited p-values greater than 0.05, meaning that no learning effect is present. For the *home screen scenario*, the three tests were conducted differently, testing if the median of the Blink wallet is greater than the median of the AfriBit wallet, to verify if the AfriBit wallet UI was beneficial and allowed users to complete their tasks faster. Vice versa, the results of the Wilcoxon rank sum test with continuity correction for the *home screen scenario* are attached in appendix E.

5.2.4 UEQ Feedback

At the end of each questionnaire, the participants were asked if they had any additional feedback. This allowed the participants to elicit thoughts and inquiries not covered by the UEQ. The distribution of the feedback between the Blink and AfriBit wallet is somewhat skewed, with every second participant leaving feedback for the AfriBit wallet but only every fifth participant for the Blink wallet. A possible explanation could be that the participants knew that the AfriBit wallet is the newer modified application, hence providing feedback for the next iteration.

5.2.4.1 Blink

Participants expressed the need for features and UI improvements regarding the Blink wallet. The missing feature was the conversion button for IOS users, which would allow exchanging BTC to Stablesats. However, such a button cannot be provided due to the reasons mentioned in section 5.1.3.1. Nevertheless, the Galoy team informed us that a workaround would have existed, where sending money to one-self, respectively the own receiving address, opens the same conversion screen on IOS as available to the Android application. Regarding the UI, one of the users wished for the send and scan interactions to be combined, in the sense that on the home screen, there should not be two separate buttons for each action. The participant reasoned that the scan feature is only used to send money and, hence, shall be placed accordingly under the send screen in the UI. Additionally, the participant wished for icons to be added to the text fields and neglected the need to show a summary before sending the money, as displaying the summary was unclear whether additional information was required.

5.2.4.2 AfriBit wallet

As for the AfriBit wallet, the suggestions were more diverse and ranged from thoughtful insights to minor adjustments or positive feedback. A critical point raised by one participant was that he could not find the drop-down of the transactions, whereas Blink directly showed him this information without the need for input. However, this user seems to be the only one facing this issue, as the number of verified transactions via the history was 34 in Blink and 35 in AfriBit, suggesting that the change in the user interface did not affect the number of verified transactions. Interestingly, most Kibera participants wished for the app to be more colorful. Some Kenyan users described the use of color as inadequate or even as sad. Additionally, one of the Swiss participants noted that the colored action button at the bottom of the screen was more appealing than the black/white button in the Blink wallet.

A deep insight was given by one participant, who noted that the app should be more informative and explain the terms used. This feedback aligns perfectly with the findings from the quantitative analysis, where the participants were asked to rate the terms' clarity. We can, therefore, conclude that in order to use the application successfully, the user needs to be familiar with the terms and that they need to be explained beforehand. Feedback from a participant from Kibera highlighted that being familiar with the terms helped, and therefore, the application was easy to use. Again, this emphasizes the importance of the terms and their impact on the application's usability. Since many participants misunderstood the terms, which resulted in user error, clarifying the used terms is crucial.

Apart from the excellent feedback such as *simple but efficient UI*, *nice contact selection* or *I really liked the real-time feedback I got once my request had been confirmed*, there were also improvement suggestions regarding the introduced changes: *Total chronological order of transactions (independent of currency) would be nice*. Participants also brought up general points not related to new features or UI changes to improve. These included that the percentage buttons when sending were confusing and that it would be beneficial to have visual feedback (such as a cursor) when inputting the amount.

Kapitel 6

Final Considerations

6.1 Summary

The work presented in this thesis is a first step towards a more inclusive financial system in Kibera. Thereby, the challenges were highlighted, and possible solutions to the multi-faceted problem of financial exclusion in Kibera were elicited. By first framing the context, analyzing the shortcomings of existing solutions, and being in direct contact with the residents, the overall picture and setting of this thesis were given. With this deep understanding and valuable insights into the current state of the financial system in Kibera and its daily use, the requirements of a new solution were gathered, and the challenges it must overcome were underlined. Accordingly, an explorative design process was conducted based on an existing solution, the Blink mobile Bitcoin Lightning wallet, that has been shown to be successful in other areas. The resulting designs can be found throughout chapter 3, where the most important changes and their impact on the UX were highlighted. Thereby, the implementation of the changes, elicited in chapter 4, was constructed in a way that allows for future extensions, modifications, and improvements. Thanks to the open-source nature of the Blink wallet and the Galoy stack, the implemented design changes could be made public and are available to everyone.

Regarding the initial objectives of the thesis, one of the goals was to investigate using and adopting blockchain technology for financial inclusion in Kibera to serve as a feasible alternative to MPesa. The introduction in chapter 1 has shown that the currently used solution in the Kenyan area underlies certain drawbacks and limitations. MPesa has helped lay the foundation for a digital monetary system and contributed significantly to Kenya's overall adoption and familiarity with electronic money services. Based on this foundation it is now crucial to further mitigate issues that the help of digital currency can mitigate. We would like to highlight that cryptocurrency is one of many possible solutions to the problem and should not be considered to be the only one. The importance lies in a system that effectively mitigates the issues found, be that through the use of cryptocurrency or other means. In this work, Bitcoin presented itself as the most feasible solution, which, in combination with the synthetic USD solution Stablesats, should provide a reliable alternative to the current system.

The use of the latter enables the residents to allocate savings in a more stable currency than the Ksh, effectively reducing the impact of inflation. Secondly, the use of Bitcoin does not require KYC or any customer identification, hence allowing for a more inclusive system, especially for people without access to a government ID. Therefore, by leveraging the blockchain infrastructure, the AfriBit wallet provides a practical solution to the problem of financial exclusion in Kibera. As a third outcome, the redesign of the Blink wallet incorporated various techniques to improve the user experience for illiterate users and provide a better accessible system for everyone. By the use of colors and a more minimalist and simplified user interface, these changes effectively lower the entry barrier for illiterate users while ensuring a functioning state of the application. The reduction of the hierarchical navigation and elimination of nested menus plays a huge importance in this regard. Thus, not only the use of blockchain technology but also the design of the user interface can contribute to a more inclusive system. Last but not least, by allowing the application to run on mobile devices, the geographical co-location of user and their bank, a predominant issue in rural Kenya, is no longer a problem. This route was only possible thanks to the digital money revolution MPesa has started, which made the target group already well familiar with the concept of digital money, and the widespread adoption of mobile phones in Kenya. Overall, the goal of investigating if blockchain technology can be seen as a viable alternative to the existing monetary system in Kibera, Kenya, is only partially accomplished. The improved AfriBit wallet marks the first milestone in mitigating and reducing the above-mentioned issues and demonstrates a plausible alternative to the current system. However, the long-term effects on financial inclusion and service adoption are yet to be seen, leaving this goal to be fully reached. To accomplish this goal, the practices and suggestions elicited in section 6.3 must be considered.

Another objective was the implementation of a Bitcoin wallet specific to the Kibera area, that is tailored to the requirements and mitigates the resident's problems whilst explicitly offering an improved UI for illiterate users. Chapter 3 highlighted the process of designing such a wallet by first analyzing the existing solution and then proposing changes to the user interface. Thereby, considerations and thoughts behind the changes, as well as their estimated impact on the UX, were elicited and undermined with arguments from both the field of HCI and POC. The resulting design changes were then implemented in chapter 4, eliciting the files and components altered. Furthermore, the implementation of the changes was juxtaposed with the proposed design, and deviations between the two were highlighted and discussed. Given that the newly designed AfriBit wallet is in a functional state and allows the seamless execution of the three fundamental operations of MPesa, namely depositing, sending, and receiving money, the basis for achieving the second objective of this thesis has been laid. Following the laid foundation, the statistical analysis of the implemented changes in section 5.2.2 and 5.2.3 showed the quantitative improvement of the user experience and the speed at which users can execute the required tasks. Ultimately, to constitute the overall achievement of this objective, 6.2 interprets, discusses, and raises considerations regarding these quantitative outcomes. The additional evaluation and user study contribute to the overall understanding of the problem and the proposed solution. Based on these evaluations of the goals, we can conclude that the thesis overall has been successful.

6.2 Conclusions

Noteworthy is that our proposed design changes to the screen where the user can choose the destination to send money have caught the Blink wallet developers' attention. In close contact with the Galoy team, we investigated the usability of the proposed changes and were able to submit a Blink improvement proposal (BLIP) to the development team. The pull request for the aforementioned *BLIP 16 - display recently used contacts for quick send*[42] has been successfully merged into the main branch of the Blink wallet on the 23rd of December, 2023. This goes to show that the work presented in this thesis is not only theoretical but also has a practical impact and is deemed of high enough quality to be included in the production build of the Blink application. Combined with the incorporated open-source approach, we have laid the basis for future improvements to be made to the wallet, allowing for an extensible, inclusive and accessible financial system in Kibera.

Touching upon the analysis of the implemented design choices and their alignment with the user's requirements, quantitative indicators in both the applications UEQ and the time measurement results have been calculated in section 5.2.2 and section 5.2.3, respectively. Having this data from the conducted user study spanning two weeks and twenty participants, valuable insights regarding usability and user experience were granted. The pure numerical results of the study are presented in the above-mentioned sections, whereas this section focuses on the conclusions drawn from these outcomes. To check whether the participants exhibited a learning effect, the time it took to set the amount in the Blink application was compared to the AfriBit wallet and statistically analyzed.

Thereby, the two-sided Wilcoxon rank sum tests with continuity correction showed no difference between the two wallets, with none of the groups exhibiting a statistically significant difference. This result is surprising, as we expected users in the AfriBit wallet to be faster when completing the tasks for a second time. Thus, with all p-values yielding that the completion of the set amount tasks in both wallets does not differ significantly, it can be concluded that for no group a learning effect is present. The p-value of the Kibera group, which can be found in appendix D, was especially high with 0.8669, which could be due to two reasons: First of all, it has to be recalled that one-third of the values were missing in the Kibera group set amount time compared to the Swiss group, which could have influenced the results. Secondly, the survey responses in appendix F and G showed that the Kibera group was twice as experienced with the Blink wallet than the Swiss group. This could have led to the Kibera group exhibiting even less difference between the walkthroughs. The important conclusion of the user study of the set amount time is that no participant group exhibited a statistically significant learning effect.

For analyzing if the AfriBit wallet allowed for faster completion of the tasks, the time measurements from the Blink home screen were juxtaposed with the ones from the AfriBit wallet and statistically evaluated. Thereby, a one-sided test was chosen in order to know in which direction the difference is present, instead of choosing a two-sided test, which would have only indicated the presence of a difference. The one-sided Wilcoxon rank sum tests with continuity correction tested if the time it took to complete the tasks in the Blink wallet was greater than in the AfriBit wallet, whereas the results showed that this statement can be disproved for the Kibera group with a p-value of 0.3926, but not for the Swiss group. Again, the considerations regarding the experience with the Blink wallet apply here as well, indicating that the UI changes in the AfriBit wallet did not lead to a difference in time for experienced users. However, the Swiss group with a p-value of 0.0001329 showed that the time it took to complete the tasks using the Blink wallet was significantly greater than using the AfriBit wallet. This could be attributed to the fact that most of the Swiss users participating in the study had little to no experience with the Blink wallet or any other Bitcoin mobile wallet. As mentioned before, the difference in time needed to complete the tasks can not be accredited to the learning effect, as no statistical difference in time could be determined for screens that has stayed consistent throughout both applications. Therefore, a consideration could be that the AfriBit wallet improved UI is especially appealing to new, inexperienced users. It has to be noted that taking both groups of the home screen scenario together and comparing them across the two wallets, the p-value of 0.01562 is statistically significant, providing evidence that the Blink UI takes participants longer to complete the given tasks' home screen time. All of the above-mentioned statistical results align with the findings from the UEQ analysis, where the AfriBit wallet scored better in all categories. In the three categories *perspicuity*, *efficiency* and *dependability*, the AfriBit wallet exhibited significantly greater means compared to the Blink wallet, thus significantly improving the perceived UX of the application.

Both related works and previous research have contributed with their theoretical importance, considerations, and recommendations to the work presented in this thesis. However, one of the major shortcomings of these works was the lack of actually implementing the suggested changes in a prototype or similar. Some of the works presented, such as Mesfin et al.[50], did design or even implement their proposed changes but lacked the evaluation thereof, leaving the current research in an unknown state of the effect of the changes. Therefore, the evaluation of our newly proposed design was of utter importance and marked our contribution to the research in this field. We deem this goal as accomplished, as the design and implementation results were explicitly tested in a user study and statistically analyzed using renowned methods and careful considerations. The above-mentioned statistical interpretation and conclusion can, therefore, provide the necessary insight for future work. The additional inclusion of the area-specific requirements and the improved user interface for illiterate users further contribute to accomplishing this goal. Hence, we can conclude that the goal of this thesis has been accomplished.

6.3 Future Work

Most of the work presented laid the basis for understanding the problem at hand and proposed a possible but not exhaustive approach to mitigating the issues. An obvious further development would be the implementation of the findings from the usability questionnaire and the hands-on user testing sessions. The gathered feedback greatly outlines the areas that need improvement, and the quantitative data provides a good basis for prioritizing them. Section 5.2.1 serves as a point of reference for the mentioned issues and observed patterns. One of the areas that demand immediate improvement both in terms of accessibility and usability is the set amount modal, one of the most profound observed issues. Currently, the modal is inaccessible for smaller screens, does not allow the user to send money, and is too complex for both educated and illiterate users. The latter insight is based on the statistical calculations showing that the set account modal does not underlie any learning effect and participants struggle with the screen, as elaborated in section 6.2. Already having delved into the problems of this modal in section 5.2.1, the collection thereof shall provide a starting point for future work on an extension of version 2.0 of the AfriBit wallet. Another possible extension would be the implementation of the proposed map feature, incorporated in the send screen.

A less obvious but equally important aspect is the active monitoring and evaluation of the system. So far, the user study is the only point of reference and included only a small number of residents in perspective to the Kenyan population. More extensive fieldwork, testing sessions, or even the public roll-out of the AfriBit wallet in the Apple App Store and Google Play Store would need to be considered. The system can only be evaluated entirely by gathering long-term insights into adoption, transaction volume, and further feedback and analysis. These long-term insights may lead to the conclusion that the concept of Bitcoin and Stablesats is not as suitable for Kenya as initially thought. In this case, exploring other solutions further and evaluating alternative possibilities that mitigate the aforementioned issues is essential. The improvement of a PoS interface would have been a nice addition to the thesis's contributions. However, due to time constraints, this thesis did not tackle this initial objective and did not touch upon a PoS system. Nevertheless, what has been shown is an exemplary approach to improving an existing wallet and adapting its user interface to make it more accessible to the target audience. Thereby, the provided insights, learnings and consideration can be applied to other wallets and systems as well, such as a PoS interface. If the AfriBit wallet strives to be adopted as the main financial system in Kibera, it is crucial to provide a PoS system that follows the accessibility principles for illiterate users and draws upon this thesis's findings and the AfriBit wallet's design.

Last but not least, user onboarding and education play an essential role in the adoption and ability to use the wallet in the long term. Here, classes for locals should be held using the Ronnie Fund's developed social network, where potential users could learn about the digital wallet, transactions, and the advantages and drawbacks of participating in this alternative financial system. This step is crucial for responsible adoption and ensures users can confidently navigate the technology. Members of the Ronnie fund will actively teach and promote the digital wallet as a possible alternative, thereby effectively reducing financial exclusion and ensuring that the works of this thesis are put to good use.

Literatur

- [1] URL: <https://www.javatpoint.com/react-native-touchables>.
- [2] URL: <https://www.ueq-online.org/#:~:text=Download-,Data%20Analysis%20Tools,-Two%20Excel%2DSheets>.
- [3] Twint AG. *Switzerland's payment app - pay, send money & much more*. <https://www.twint.ch/>. 2023.
- [4] Saifedean Ammous. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. 2018.
- [5] Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. 2nd. 2017.
- [6] Inc Apple. *A control for selecting from a set of mutually exclusive values*. 2023. URL: <https://developer.apple.com/documentation/swiftui/picker#:~:text=example%20applies%20the-,segmented%20style,-to%20two%20pickers>.
- [7] Inc Apple. *Beta Testing made simple with TestFlight*. 2023. URL: <https://developer.apple.com/testflight/>.
- [8] Framer B.V. *Use powerful yet familiar tools to create your ultimate website design*. URL: <https://www.framer.com/>.
- [9] Imran Bashir. *Mastering Blockchain - Fourth edition*. März 2023.
- [10] CoinMarketCap. *Fiat on-ramp definition: CoinMarketCap*. Aug. 2023. URL: <https://coinmarketcap.com/academy/glossary/fiat-on-ramp>.
- [11] Bitcoin Core. *Helping you keep Bitcoin decentralized*. 2023. URL: <https://bitcoin.org/en/bitcoin-core/>.
- [12] Bitcoin Core. *Helping you keep Bitcoin decentralized*. 2023. URL: <https://bitcoin.org/en/vocabulary#mining>.
- [13] Sargon Danho und Yonathan Habte. *Blockchain for financial inclusion and mobile financial services: A study in sub-saharan Africa*. 2019.
- [14] Nelisiwe Dlamini, Mfundo Scott und Kishor Nair. "Development of an SMS System Used to Access Bitcoin Wallets". In: Mai 2017, S. 1–10.
- [15] Ludwig Fahrmeir u. a. *Statistik - Der Weg zur Datenanalyse*. 2016, S. 295.
- [16] Michael Froehlich, Felix Gutjahr und Florian Alt. "Don't lose your coin! Investigating Security Practices of Cryptocurrency Users". In: Juli 2020, S. 1751–1763.
- [17] Michael Froehlich u. a. "Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda". Apr. 2022.
- [18] Michael Froehlich u. a. "Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users". In: Juni 2021, S. 138–148.
- [19] Yogi Golle. *Yogi Golle I.C.T Academy*. 2023. URL: <https://ronniefund.org/the-yogi-yolle-ict-initiative/>.

- [20] Aurora Harley. *Interface icons for Bitcoin applications, free to use*. Juli 2014. URL: <https://www.nngroup.com/articles/icon-usability/>.
- [21] *Home Page*. URL: <https://yarnpkg.com/>.
- [22] *HUAWEI Phones - HUAWEI Global*. URL: <https://consumer.huawei.com/en/phones/>.
- [23] Facebook Inc. *A query language for your API*. 2023. URL: <https://graphql.org/>.
- [24] Facebook Inc. *React native - learn once, write anywhere*. 2023. URL: <https://reactnative.dev/>.
- [25] Facebook Inc. *Setting up the development environment*. 2023. URL: <https://reactnative.dev/docs/environment-setup?os=linux&platform=android>.
- [26] Galoy Inc. *Bitcoin banking on an open source standard*. Juni 2022. URL: <https://docsend.com/view/msjqxb8xxh74ifep>.
- [27] Galoy Inc. *Blink (BBW) Mobile App Design*. 2023. URL: <https://www.figma.com/file/rH7A7NquSsXEh7v8eGuYM7/BBW-Wallet-Redesign?node-id=1322%3A35438>.
- [28] Galoy Inc. *Blink (Bitcoin Beach Wallet) App*. Nov. 2023. URL: <https://play.google.com/store/apps/details?id=com.galoyapp>.
- [29] Galoy Inc. *Galoy staging API*. 2023. URL: <https://api.staging.galoy.io/graphql>.
- [30] Galoy Inc. *GaloyMobile*. 2023. URL: <https://github.com/GaloyMoney/galoy-mobile>.
- [31] Galoy Inc. *GaloyMobile*. 2023. URL: <https://github.com/orgs/GaloyMoney/repositories>.
- [32] Galoy Inc. *Transact USD over Lightning without stablecoins or fiat integration*. Jan. 2023. URL: <https://stablesats.com/>.
- [33] Galoy Inc. *What is a Paycode and how can I use it?* Mai 2023. URL: <https://faq.blink.sv/blink-payment-methods/lightning-address/what-is-a-paycode-and-how-can-i-use-it>.
- [34] Google Inc. *Android Studio*. 2023. URL: <https://reactnative.dev/docs/environment-setup?os=linux&platform=android>.
- [35] Apple Inc. *App Store Review Guidelines*. 2023. URL: <https://developer.apple.com/app-store/review/guidelines/#in-app-purchase>.
- [36] Apple Inc. *App Store Review Guidelines*. 2023. URL: <https://developer.apple.com/app-store/review/guidelines/#cryptocurrencies>.
- [37] *Interface icons for Bitcoin applications, free to use*. URL: <https://bitcoinicons.com/>.
- [38] Ali Kazerani, Domenic Rosati und Brian Lesser. “Determining the usability of bitcoin for beginners using change tip and coinbase”. In: Aug. 2017, S. 1–5.
- [39] K. Koffka. *Principles of Gestalt Psychology*. Cognitive psychology. 1999.
- [40] Bettina Laugwitz, Theo Held und Martin Schrepp. “Construction and Evaluation of a User Experience Questionnaire”. In: Bd. 5298. Nov. 2008, S. 63–76.
- [41] Marco Leder. *AfriBit wallet*. 2023. URL: <https://github.com/marcoleder/AfriBit-wallet>.
- [42] Marco Leder. *feat(blip-16): display recently used contacts for quick send*. 2023. URL: <https://github.com/GaloyMoney/galoy-mobile/pull/2949>.
- [43] Aidan Lyon. “Why are Normal Distributions Normal?” In: *The British Journal for the Philosophy of Science* 65 (Aug. 2013), S. 621–649.

- [44] Jan MÅ¼hlemann. *react-i18next documentation*. Dez. 2023. URL: <https://react.i18next.com/>.
- [45] Theo Mandel. "User/System Interface Design". In: *Encyclopedia of Information Systems*. Hrsg. von Hossein Bidgoli. 2003, S. 535–549.
- [46] Ignacio Mas und Olga Morawczynski. "Designing mobile money services: Lessons from M-PESA". In: *Innovations: Technology, Governance, Globalization* 4 (Apr. 2009), S. 77–91.
- [47] Isaac Mbiti und David Weil. "Mobile Banking: The Impact of M-Pesa in Kenya". In: (Juni 2011).
- [48] Ronnie Mdawidag. *The Ronnie Mdawida fund*. 2023. URL: <https://www.theronniefund.org>.
- [49] Indrani Medhi, Aishwarya Ratan und Kentaro Toyama. "Mobile-Banking Adoption and Usage by Low-Literate, Low-Income Users in the Developing World". In: Bd. 5623. Juli 2009, S. 485–494.
- [50] Woldmariam Mesfin u. a. "Mobile Money System Design for Illiterate Users in Rural Ethiopia". In: Juni 2014, S. 482–491.
- [51] David Mhlanga. "Block chain technology for digital financial inclusion in the industry 4.0, towards sustainable development?" In: *Frontiers in Blockchain* 6 (Feb. 2023).
- [52] Microsoft. *TypeScript is JavaScript with syntax for types*. <https://www.typescriptlang.org/>. 2023.
- [53] Md Moniruzzaman, Farida Chowdhury und Md. Sadek Ferdous. "Examining Usability Issues in Blockchain-Based Cryptocurrency Wallets". In: Juli 2020, S. 631–643.
- [54] Prince Muraguri. *How M-Pesa works in Kenya*. 2023. URL: https://www.researchgate.net/figure/How-M-Pesa-works-in-Kenya_fig2_336738552.
- [55] Kabui Mwangi u. a. *Mobile money transfers edge out rival operators*. Sep. 2009. URL: <https://www.businessdailyafrica.com/bd/markets/mobile-money-transfers-edge-out-rival-operators--1946732>.
- [56] Donald A Norman. *The design of everyday things*. The MIT Press. Dez. 2013.
- [57] *OpenAI platform*. URL: <https://platform.openai.com/docs/models/gpt-4-and-gpt-4-turbo>.
- [58] SIDE Org. *Bridging traditional and modern finance*. 2023. URL: <https://sidexchange.com>.
- [59] Rushi Patel. *Increase Touchable Area of Button in React Native*. URL: <https://dev.to/ruship001/increase-touchable-area-of-button-in-react-native-3hek>.
- [60] J. Poon und T. Dryja. *Lightning network whitepaper*. Mai 2017. URL: <https://github.com/lightningnetwork/paper>.
- [61] Assistant Secretary for Public Affairs. *System usability scale (SUS)*. Sep. 2013. URL: <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>.
- [62] Dieter Rasch, Klaus Kubinger und Karl Moder. "The two-sample t test: Pre-testing its assumptions does not pay off". In: *Stat. Pap.* 52 (Feb. 2011), S. 219–231.
- [63] World Leaders in Research-Based User Experience. *Thinking aloud: The Nr.1 usability tool*. URL: <https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/>.

- [64] Benjamin Rosenberg und Mario Navarro. “SEMANTIC DIFFERENTIAL SCALING”. In: Jan. 2017.
- [65] J. P. Royston. “An Extension of Shapiro and Wilk’s W Test for Normality to Large Samples”. In: *Journal of the Royal Statistical Society. Series C (Applied Statistics)* 31.2 (1982), S. 115–124.
- [66] Steven Sawyer. “Analysis of Variance: The Fundamental Concepts”. In: *Journal of Manual & Manipulative Therapy* 17 (Apr. 2009), 27E–38E.
- [67] Martin Schrepp, Andreas Hinderks und Joerg Thomaschewski. “Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios”. In: Juni 2014, S. 383–392.
- [68] Martin Schrepp, Andreas Hinderks und Joerg Thomaschewski. “Construction of a Benchmark for the User Experience Questionnaire (UEQ)”. In: *International Journal of Interactive Multimedia and Artificial Intelligence* 4 (Juni 2017), S. 40–44.
- [69] Martin Schrepp, Andreas Hinderks und Joerg Thomaschewski. “Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S)”. In: *International Journal of Interactive Multimedia and Artificial Intelligence* 4 (Jan. 2017), S. 103.
- [70] Sebastian Schuetz und Viswanath Venkatesh. “Blockchain, adoption, and financial inclusion in India: Research opportunities”. In: *International Journal of Information Management* 52 (Jan. 2020), S. 101936.
- [71] Deepak Singh. *Knowledge in the head + knowledge in the world = performance*. URL: <https://uxdesign.cc/knowledge-in-the-head-knowledge-in-the-world-performance-a-basic-idea-for-an-intuitive-38e4c148b55f>.
- [72] Juthaphorn Sinsomboonthong u. a. “Performance of Robust Confidence Intervals for Estimating Population Mean Under Both Non-Normality and in Presence of Outliers”. In: *Advances in Science, Technology and Engineering Systems Journal* 5 (Juni 2020), S. 442–449.
- [73] Maarten van Steen und Andrew S. Tanenbaum. “A brief introduction to distributed systems”. In: *Computing* 98.10 (Okt. 2016), S. 967–1009.
- [74] *The R Project for Statistical Computing*. URL: <https://www.r-project.org/>.
- [75] Edward R Tufte. *The visual display of quantitative information*. 1982.
- [76] Super User. *MPESA Charges Guide 2023: Sending & Withdrawal Costs — safaricom.co.ke*. <https://www.safaricom.co.ke/personal/m-pesa/mpesa-charges.2023>.
- [77] *Video Editing Freedom*. URL: <https://kdenlive.org/en/>.
- [78] Artemij Voskobochnikov u. a. “The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets”. In: Mai 2021, S. 1–14.
- [79] John P. Wentzel, Krishna Sundar Diatha und Venkata Seshachal Sarma Yadavalli. “An investigation into factors impacting financial exclusion at the bottom of the pyramid in South Africa”. In: *Development Southern Africa* 33.2 (2016), S. 203–214.
- [80] Bitcoin Wiki. *Transaction replacement - Bitcoin Wiki*. https://en.bitcoin.it/wiki/Transaction_replacement. 2023.
- [81] *Wilcoxon Rank Sum and Signed Rank Tests*. URL: <https://stat.ethz.ch/R-manual/R-devel/library/stats/html/wilcox.test.html>.

Abbreviations

2FA	Two Factor Authentication
AML	Anti Money Laundering
ANOVA	Analysis of variance
API	Application Programming Interface
APK	Android Package Kit
App	Application
ATMs	Automated Teller Machine
BBW	Bitcoin Beach Wallet
BE	Blockchain Explorer
BGP	Byzantine Generals' Problem
BTC	Bitcoin (Cryptocurrency)
CL	Confidence Level
CLI	Command Line Interface
HCI	Human-Computer Interaction
ICT	Information and communications technology
ID	Identification Document
IOS	iPhone Operating System
KSh	Kenyan Shilling
KYC	Know Your Customer
L1	Layer 1
L2	Layer 2
LNURL	Lightning Network Uniform Resource Locator
MIT	Massachusetts Institute of Technology
PIN	Personal Identification Number
PKC	Public Key Cryptography
POC	People-Oriented Computing
PoS	Point-of-Sale
PoW	Proof-of-Work
QQ-plots	Quantile-Quantile plot
QR code	Quick Response code
SAT	Satoshi
sats	Satoshis
SUS	System Usability Scale
SVG	Scalable Vector Graphics
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module

SMS	Short Message Service
Tx	Transaction
UI	User Interface
UEQ	User Experience Questionnaire
UEQ-S	Short version of the User Experience Questionnaire
URL	Uniform Resource Locator
USD	US-Dollar
UTXO	Unspent Transaction Output
UX	User Experience

Abbildungsverzeichnis

1.1	How M-Pesa works in Kenya, from Prince Muraguri[54]	3
3.1	Blink home screen	35
3.2	AfriBit home screen	35
3.3	Blink receive Stablesats via Onchain	37
3.4	AfriBit receive Stablesats via Onchain	37
3.5	Blink receive Bitcoin via Paycode	38
3.6	AfriBit receive Bitcoin via Paycode	38
3.7	Blink send destination screen	39
3.8	AfriBit send contacts screen	39
3.9	Blink business map screen	40
3.10	AfriBit send map screen	40
3.11	Blink confirm screen	41
3.12	AfriBit confirm screen	41
4.1	Application source structure	45
4.2	Home screen design, partially expanded	46
4.3	Home screen implementation, collapsed	46
4.4	Home screen implementation, expanded	46
4.5	Home screen small phone, Stablesats	47
4.6	Home screen small phone, Bitcoin	47
4.7	Receive Stablesats via Onchain design	48

4.8	Receive Stablesats via Onchain implementation	48
4.9	Receive Bitcoin via Paycode design	49
4.10	Receive Bitcoin via Paycode implementation	49
4.11	Send contacts screen design	50
4.12	Send contacts screen implementation	50
4.13	Send screen autofill implementation	51
4.14	Send screen selection implementation	51
4.15	Send details design	52
4.16	Send details implementation	52
4.17	Blink home screen pressables	53
4.18	AfriBit implemented home screen pressables	53
5.1	Enter amount	66
5.2	Enter USD	66
5.3	Enter SAT	66
5.4	UEQ Survey results graphic	67

Tabellenverzeichnis

5.1	UEQ Survey result statistics	67
5.2	Blink time measurements	68
5.3	AfriBit time measurements	69

Listings

4.1	button-group.tsx	44
-----	----------------------------	----

Anhang A

Contents of the CD

The enclosed CD contains the following content:

Code

Documentation

Literature

Presentation

Anhang B

Blink STD, QQ-plots, Shapiro-Wilk tests

Quantiles-Quantiles for Blink wallet

```

Kibera_home_screen_T1 <- c(2.37, 4.37, 1.37, 9.23, 4.03, 4.00, 5.07,
                          2.10, 3.97, 4.70)
Kibera_home_screen_T2 <- c(5.00, 10.40, 1.27, 3.07, 6.00, 3.20, 13.43, 4.10)
Kibera_home_screen_T3 <- c(3.03, 6.67, 3.03, 5.33, 3.03, 15.00, 13.03,
                          4.00, 4.73, 5.87)
Kibera_home_screen_total <- c(Kibera_home_screen_T1,
                              Kibera_home_screen_T2,
                              Kibera_home_screen_T3)
cat(paste("Standard deviations Kibera home screen",
          "\nTask 1:", sd(Kibera_home_screen_T1),
          "\nTask 2:", sd(Kibera_home_screen_T2),
          "\nTask 3:", sd(Kibera_home_screen_T3),
          "\nTotal:", sd(Kibera_home_screen_total)))

```

```

## Standard deviations Kibera home screen
## Task 1: 2.16445759179215
## Task 2: 4.10017573665185
## Task 3: 4.24299893942952
## Total: 3.59533015755145

```

```

Swiss_home_screen_T1 <- c(65.17, 16.27, 28.30, 17.13, 70.03, 41.43, 21.43,
                        24.37, 16.37, 14.47)
Swiss_home_screen_T2 <- c(39.23, 17.17, 1.20, 14.10, 8.30, 9.13, 20.13,
                        16.20, 19.47)
Swiss_home_screen_T3 <- c(31.00, 27.27, 23.00, 23.10, 19.23, 3.33, 14.23,
                        4.47, 16.40, 14.33)
Swiss_home_screen_total <- c(Swiss_home_screen_T1,
                              Swiss_home_screen_T2,
                              Swiss_home_screen_T3)
cat(paste("Standard deviations Swiss home screen",
          "\nTask 1:", sd(Swiss_home_screen_T1),
          "\nTask 2:", sd(Swiss_home_screen_T2),
          "\nTask 3:", sd(Swiss_home_screen_T3),
          "\nTotal:", sd(Swiss_home_screen_total)))

```

```

## Standard deviations Swiss home screen
## Task 1: 20.6470444750709
## Task 2: 10.6017710784567
## Task 3: 9.03476274053601
## Total: 15.6704152556885

```

```

Kibera_set_amount_T1 <- c()
Kibera_set_amount_T2 <- c(15.50, 7.13, 22.77, 34.07, 12.10, 4.23, 7.47)
Kibera_set_amount_T3 <- c(14.03, 6.10, 3.33, 3.50, 5.03, 11.10, 11.13, 3.03,
                        4.67, 4.33)
Kibera_set_amount_total <- c(Kibera_set_amount_T1,
                              Kibera_set_amount_T2,
                              Kibera_set_amount_T3)
cat(paste("Standard deviations Kibera set amount",
          "\nTask 1:", sd(Kibera_set_amount_T1),
          "\nTask 2:", sd(Kibera_set_amount_T2),
          "\nTask 3:", sd(Kibera_set_amount_T3),
          "\nTotal:", sd(Kibera_set_amount_total)))

```



```
## Standard deviations Kibera set amount
## Task 1: NA
## Task 2: 10.5427774871168
## Task 3: 3.95263695384346
## Total: 8.21405520684981
```

```
Swiss_set_amount_T1 <- c(23.30, 13.23, 35.17, 45.23, 21.20, 20.27, 16.03,
  11.03, 19.17, 8.30)
Swiss_set_amount_T2 <- c(8.30, 11.13, 7.27, 34.23, 9.43, 11.47, 7.07,
  9.17, 3.27)
Swiss_set_amount_T3 <- c(4.20, 5.20, 2.30, 2.10, 5.00, 1.20, 2.03, 1.47,
  8.33, 2.37)
Swiss_set_amount_total <- c(Swiss_set_amount_T1,
  Swiss_set_amount_T2,
  Swiss_set_amount_T3)
cat(paste("Standard deviations Swiss set amount",
  "\nTask 1:", sd(Swiss_set_amount_T1),
  "\nTask 2:", sd(Swiss_set_amount_T2),
  "\nTask 3:", sd(Swiss_set_amount_T3),
  "\nTotal:", sd(Swiss_set_amount_total)))
```

```
## Standard deviations Swiss set amount
## Task 1: 11.2644958954131
## Task 2: 8.95458541753888
## Task 3: 2.2396329064281
## Total: 11.0733003899964
```

```
home_screen_total <- c(Kibera_home_screen_total, Swiss_home_screen_total)
set_amount_total <- c(Kibera_set_amount_total, Swiss_set_amount_total)
cat(paste("Standard deviations per scenario",
  "\nHome Screen Total:", sd(home_screen_total),
  "\nSet Amount Total:", sd(set_amount_total)))
```

```
## Standard deviations per scenario
## Home Screen Total: 14.0906354969985
## Set Amount Total: 10.0638303735427
```

```
par(mfrow=c(3,2))

qqnorm(Kibera_home_screen_total, main = "Kibera group home screen time")
qqline(Kibera_home_screen_total, col = "steelblue")

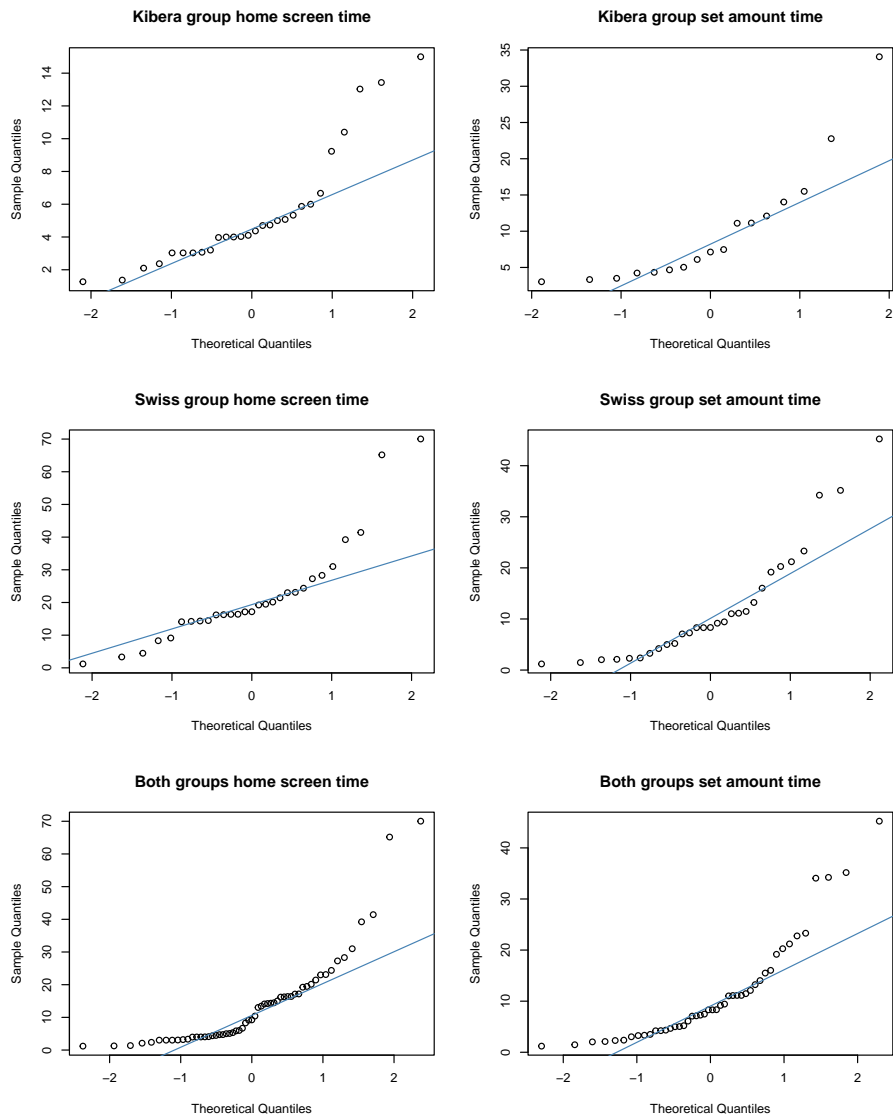
qqnorm(Kibera_set_amount_total, main = "Kibera group set amount time")
qqline(Kibera_set_amount_total, col = "steelblue")

qqnorm(Swiss_home_screen_total, main = "Swiss group home screen time")
qqline(Swiss_home_screen_total, col = "steelblue")

qqnorm(Swiss_set_amount_total, main = "Swiss group set amount time")
qqline(Swiss_set_amount_total, col = "steelblue")

qqnorm(home_screen_total, main = "Both groups home screen time")
qqline(home_screen_total, col = "steelblue")

qqnorm(set_amount_total, main = "Both groups set amount time")
qqline(set_amount_total, col = "steelblue")
```



```
shapiro.test(Kibera_home_screen_total)
```

```
##
## Shapiro-Wilk normality test
##
## data: Kibera_home_screen_total
## W = 0.81855, p-value = 0.0002308
```

```
shapiro.test(Kibera_set_amount_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: Kibera_set_amount_total  
## W = 0.78825, p-value = 0.001406
```

```
shapiro.test(Swiss_home_screen_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: Swiss_home_screen_total  
## W = 0.82315, p-value = 0.0002237
```

```
shapiro.test(Swiss_set_amount_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: Swiss_set_amount_total  
## W = 0.83042, p-value = 0.0003087
```

```
shapiro.test(home_screen_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: home_screen_total  
## W = 0.76023, p-value = 2.823e-08
```

```
shapiro.test(set_amount_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: set_amount_total  
## W = 0.81685, p-value = 4.693e-06
```


Anhang C

AfriBit STD, QQ-plots, Shapiro-Wilk tests

Quantiles-Quantiles for AfriBit wallet

```

Kibera_home_screen_T1 <- c(14.17, 9.23, 4.17, 4.87, 2.23, 8.37, 4.13, 12.10,
5.10, 3.20)
Kibera_home_screen_T2 <- c(3.17, 22.77, 3.70, 4.60, 4.03, 4.07, 5.37, 4.43,
6.10, 3.17)
Kibera_home_screen_T3 <- c(12.23, 3.17, 2.77, 3.67, 3.17, 3.07, 2.13, 2.33,
3.17, 1.57)
Kibera_home_screen_total <- c(Kibera_home_screen_T1,
Kibera_home_screen_T2,
Kibera_home_screen_T3)
cat(paste("Standard deviations Kibera home screen",
"\nTask 1:", sd(Kibera_home_screen_T1),
"\nTask 2:", sd(Kibera_home_screen_T2),
"\nTask 3:", sd(Kibera_home_screen_T3),
"\nTotal:", sd(Kibera_home_screen_total)))

```

```

## Standard deviations Kibera home screen
## Task 1: 4.0175145716392
## Task 2: 5.91400869874985
## Task 3: 3.05026701927698
## Total: 4.52973577671994

```

```

Swiss_home_screen_T1 <- c(14.17, 8.10, 36.07, 17.07, 10.10, 6.30, 27.10, 18.03,
10.27, 12.17)
Swiss_home_screen_T2 <- c(31.00, 9.03, 7.13, 10.17, 8.07, 4.27, 14.37, 4.20,
6.07, 12.10)
Swiss_home_screen_T3 <- c(13.07, 9.13, 6.03, 4.00, 1.00, 2.07, 16.07, 2.10,
13.17, 4.07)
Swiss_home_screen_total <- c(Swiss_home_screen_T1,
Swiss_home_screen_T2,
Swiss_home_screen_T3)
cat(paste("Standard deviations Swiss home screen",
"\nTask 1:", sd(Swiss_home_screen_T1),
"\nTask 2:", sd(Swiss_home_screen_T2),
"\nTask 3:", sd(Swiss_home_screen_T3),
"\nTotal:", sd(Swiss_home_screen_total)))

```

```

## Standard deviations Swiss home screen
## Task 1: 9.27004111221856
## Task 2: 7.85456335868236
## Task 3: 5.42121234903535
## Total: 8.28635285744947

```

```

Kibera_set_amount_T1 <- c()
Kibera_set_amount_T2 <- c(7.67, 6.30, 5.03, 9.63, 6.40, 18.17, 16.20, 6.30,
12.13, 21.33)
Kibera_set_amount_T3 <- c(4.17, 4.50, 4.33, 2.67, 3.13, 19.13, 6.23, 13.17,
13.37, 4.47)
Kibera_set_amount_total <- c(Kibera_set_amount_T1,
Kibera_set_amount_T2,
Kibera_set_amount_T3)
cat(paste("Standard deviations Kibera set amount",
"\nTask 1:", sd(Kibera_set_amount_T1),
"\nTask 2:", sd(Kibera_set_amount_T2),
"\nTask 3:", sd(Kibera_set_amount_T3),
"\nTotal:", sd(Kibera_set_amount_total)))

```

```
## Standard deviations Kibera set amount
## Task 1: NA
## Task 2: 5.77649297680791
## Task 3: 5.62945833194554
## Total: 5.81872682312078
```

```
Swiss_set_amount_T1 <- c(8.23, 6.03, 9.23, 12.37, 7.13, 10.40, 21.40, 7.13,
                        10.10, 15.10)
Swiss_set_amount_T2 <- c(11.07, 7.00, 7.17, 8.33, 6.23, 11.17, 10.37, 18.30,
                        7.13, 15.20)
Swiss_set_amount_T3 <- c(2.10, 3.17, 4.03, 7.20, 3.20, 1.40, 3.13, 2.20,
                        4.10, 4.10)
Swiss_set_amount_total <- c(Swiss_set_amount_T1,
                            Swiss_set_amount_T2,
                            Swiss_set_amount_T3)
cat(paste("Standard deviations Swiss set amount",
          "\nTask 1:", sd(Swiss_set_amount_T1),
          "\nTask 2:", sd(Swiss_set_amount_T2),
          "\nTask 3:", sd(Swiss_set_amount_T3),
          "\nTotal:", sd(Swiss_set_amount_total)))
```

```
## Standard deviations Swiss set amount
## Task 1: 4.62658933652954
## Task 2: 3.95024907794151
## Task 3: 1.60114577030881
## Total: 4.85429465027867
```

```
home_screen_total <- c(Kibera_home_screen_total, Swiss_home_screen_total)
set_amount_total <- c(Kibera_set_amount_total, Swiss_set_amount_total)
cat(paste("Standard deviations per scenario",
          "\nHome Screen Total:", sd(home_screen_total),
          "\nSet Amount Total:", sd(set_amount_total)))
```

```
## Standard deviations per scenario
## Home Screen Total: 7.21264188337762
## Set Amount Total: 5.23133777326213
```

```
par(mfrow=c(3,2))

qqnorm(Kibera_home_screen_total, main = "Kibera group home screen time")
qqline(Kibera_home_screen_total, col = "steelblue")

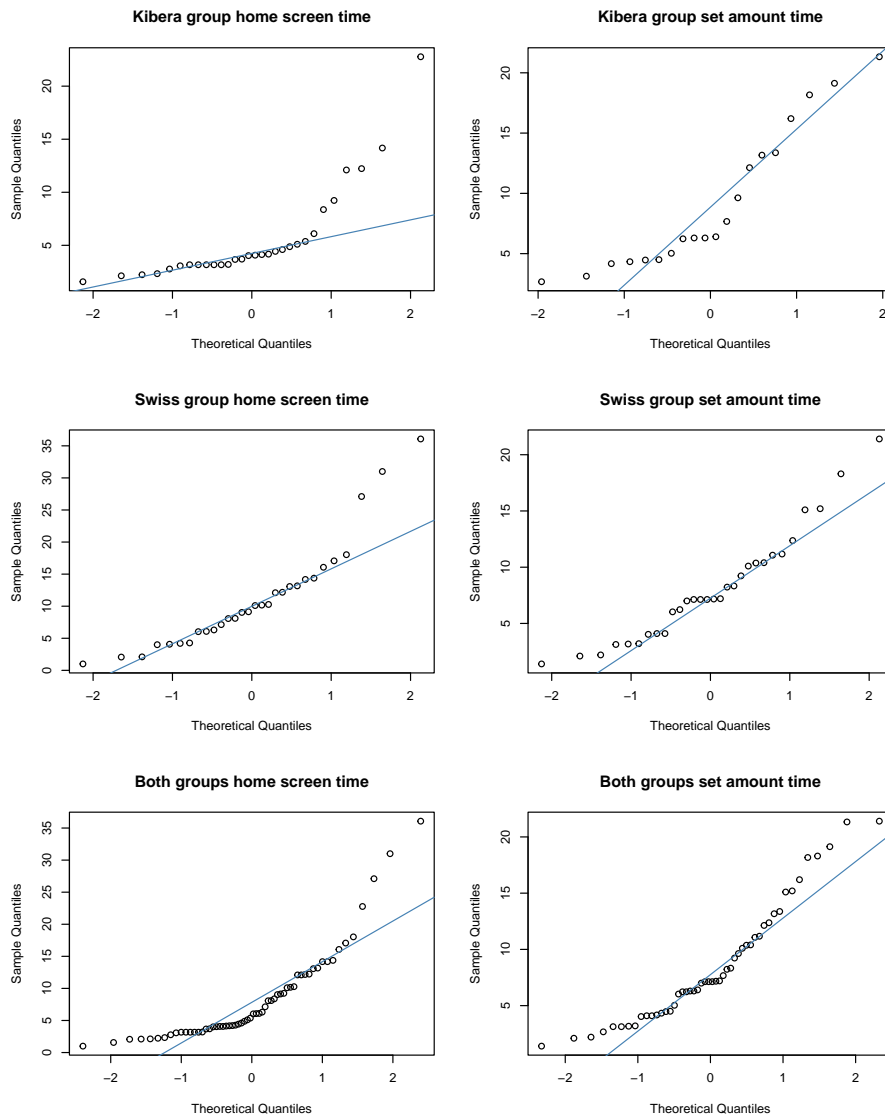
qqnorm(Kibera_set_amount_total, main = "Kibera group set amount time")
qqline(Kibera_set_amount_total, col = "steelblue")

qqnorm(Swiss_home_screen_total, main = "Swiss group home screen time")
qqline(Swiss_home_screen_total, col = "steelblue")

qqnorm(Swiss_set_amount_total, main = "Swiss group set amount time")
qqline(Swiss_set_amount_total, col = "steelblue")

qqnorm(home_screen_total, main = "Both groups home screen time")
qqline(home_screen_total, col = "steelblue")

qqnorm(set_amount_total, main = "Both groups set amount time")
qqline(set_amount_total, col = "steelblue")
```



```
shapiro.test(Kibera_home_screen_total)
```

```
##
## Shapiro-Wilk normality test
##
## data: Kibera_home_screen_total
## W = 0.69902, p-value = 1.51e-06
```



```
shapiro.test(Kibera_set_amount_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: Kibera_set_amount_total  
## W = 0.87418, p-value = 0.01393
```

```
shapiro.test(Swiss_home_screen_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: Swiss_home_screen_total  
## W = 0.86363, p-value = 0.001213
```

```
shapiro.test(Swiss_set_amount_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: Swiss_set_amount_total  
## W = 0.92997, p-value = 0.04902
```

```
shapiro.test(home_screen_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: home_screen_total  
## W = 0.79441, p-value = 9.824e-08
```

```
shapiro.test(set_amount_total)
```

```
##  
## Shapiro-Wilk normality test  
##  
## data: set_amount_total  
## W = 0.9138, p-value = 0.001417
```


Anhang D

SetAmount Wilcoxon rank sum test

Wilcox test of SetAmount

```

Kibera_set_amount_T1_blink <- c()
Kibera_set_amount_T2_blink <- c(15.50, 7.13, 22.77, 34.07, 12.10, 4.23, 7.47)
Kibera_set_amount_T3_blink <- c(14.03, 6.10, 3.33, 3.50, 5.03, 11.10, 11.13, 3.03, 4.67, 4.33)
Kibera_set_amount_total_blink <- c(Kibera_set_amount_T1_blink,
                                   Kibera_set_amount_T2_blink,
                                   Kibera_set_amount_T3_blink)

Kibera_set_amount_T1_afribit <- c()
Kibera_set_amount_T2_afribit <- c(7.67, 6.30, 5.03, 9.63, 6.40, 18.17, 16.20, 6.30, 12.13, 21.33)
Kibera_set_amount_T3_afribit <- c(4.17, 4.50, 4.33, 2.67, 3.13, 19.13, 6.23, 13.17, 13.37, 4.47)
Kibera_set_amount_total_afribit <- c(Kibera_set_amount_T1_afribit,
                                     Kibera_set_amount_T2_afribit,
                                     Kibera_set_amount_T3_afribit)

# kibera group comparison
kibera_group_comparison <- wilcox.test(Kibera_set_amount_total_blink,
                                       Kibera_set_amount_total_afribit,
                                       alternative = "two.sided")
cat(paste("kibera_group_comparison wilcox:", kibera_group_comparison))

## kibera_group_comparison wilcox: c(W = 164) kibera_group_comparison wilcox: NULL kibera_group_comp

kibera_group_comparison

##
## Wilcoxon rank sum test with continuity correction
##
## data: Kibera_set_amount_total_blink and Kibera_set_amount_total_afribit
## W = 164, p-value = 0.8669
## alternative hypothesis: true location shift is not equal to 0

kibera_group_comparison$p.value

## [1] 0.8668599

Swiss_set_amount_T1_blink <- c(23.30, 13.23, 35.17, 45.23, 21.20, 20.27, 16.03, 11.03, 19.17, 8.30)
Swiss_set_amount_T2_blink <- c(8.30, 11.13, 7.27, 34.23, 9.43, 11.47, 7.07, 9.17, 3.27)
Swiss_set_amount_T3_blink <- c(4.20, 5.20, 2.30, 2.10, 5.00, 1.20, 2.03, 1.47, 8.33, 2.37)
Swiss_set_amount_total_blink <- c(Swiss_set_amount_T1_blink,
                                   Swiss_set_amount_T2_blink,
                                   Swiss_set_amount_T3_blink)

Swiss_set_amount_T1_afribit <- c(8.23, 6.03, 9.23, 12.37, 7.13, 10.40, 21.40, 7.13, 10.10, 15.10)
Swiss_set_amount_T2_afribit <- c(11.07, 7.00, 7.17, 8.33, 6.23, 11.17, 10.37, 18.30, 7.13, 15.20)
Swiss_set_amount_T3_afribit <- c(2.10, 3.17, 4.03, 7.20, 3.20, 1.40, 3.13, 2.20, 4.10, 4.10)
Swiss_set_amount_total_afribit <- c(Swiss_set_amount_T1_afribit,
                                     Swiss_set_amount_T2_afribit,
                                     Swiss_set_amount_T3_afribit)

# swiss group comparison
swiss_group_comparison <- wilcox.test(Swiss_set_amount_total_blink,
                                       Swiss_set_amount_total_afribit,
                                       alternative = "two.sided")
cat(paste("swiss_group_comparison wilcox:", swiss_group_comparison))

```

```
## swiss_group_comparison wilcox: c(W = 498) swiss_group_comparison wilcox: NULL swiss_group_compari
```

```
swiss_group_comparison
```

```
##
## Wilcoxon rank sum test with continuity correction
##
## data: Swiss_set_amount_total_blink and Swiss_set_amount_total_afribit
## W = 498, p-value = 0.3433
## alternative hypothesis: true location shift is not equal to 0
```

```
swiss_group_comparison$p.value
```

```
## [1] 0.3432652
```

```
#both groups together
set_amount_blink <- c(Kibera_set_amount_total_blink,
                      Swiss_set_amount_total_blink)
set_amount_afribit <- c(Kibera_set_amount_total_afribit,
                       Swiss_set_amount_total_afribit)
both_groups <- wilcox.test(set_amount_blink,
                          set_amount_afribit,
                          alternative = "two.sided")
cat(paste("both_groups wilcox:", both_groups))
```

```
## both_groups wilcox: c(W = 1247.5) both_groups wilcox: NULL both_groups wilcox: 0.476807813125366
```

```
both_groups
```

```
##
## Wilcoxon rank sum test with continuity correction
##
## data: set_amount_blink and set_amount_afribit
## W = 1247.5, p-value = 0.4768
## alternative hypothesis: true location shift is not equal to 0
```

```
both_groups$p.value
```

```
## [1] 0.4768078
```


Anhang E

HomeScreen Wilcoxon rank sum test

Wilcox test of HomeScreen

```

Kibera_home_screen_T1_blink <- c(2.37, 4.37, 1.37, 9.23, 4.03, 4.00, 5.07,
2.10, 3.97, 4.70)
Kibera_home_screen_T2_blink <- c(5.00, 10.40, 1.27, 3.07, 6.00, 3.20,
13.43, 4.10)
Kibera_home_screen_T3_blink <- c(3.03, 6.67, 3.03, 5.33, 3.03, 15.00, 13.03,
4.00, 4.73, 5.87)
Kibera_home_screen_total_blink <- c(Kibera_home_screen_T1_blink,
Kibera_home_screen_T2_blink,
Kibera_home_screen_T3_blink)

Kibera_home_screen_T1_afribit <- c(14.17, 9.23, 4.17, 4.87, 2.23, 8.37, 4.13,
12.10, 5.10, 3.20)
Kibera_home_screen_T2_afribit <- c(3.17, 22.77, 3.70, 4.60, 4.03, 4.07, 5.37,
4.43, 6.10, 3.17)
Kibera_home_screen_T3_afribit <- c(12.23, 3.17, 2.77, 3.67, 3.17, 3.07, 2.13,
2.33, 3.17, 1.57)
Kibera_home_screen_total_afribit <- c(Kibera_home_screen_T1_afribit,
Kibera_home_screen_T2_afribit,
Kibera_home_screen_T3_afribit)

# kibera group comparison
kibera_group_comparison <- wilcox.test(Kibera_home_screen_total_blink,
Kibera_home_screen_total_afribit,
alternative = "greater")
cat(paste("kibera_group_comparison wilcox:", kibera_group_comparison))

## kibera_group_comparison wilcox: c(W = 438) kibera_group_comparison wilcox: NULL kibera_group_comp

kibera_group_comparison

##
## Wilcoxon rank sum test with continuity correction
##
## data: Kibera_home_screen_total_blink and Kibera_home_screen_total_afribit
## W = 438, p-value = 0.3926
## alternative hypothesis: true location shift is greater than 0

kibera_group_comparison$p.value

## [1] 0.3926452

Swiss_home_screen_T1_blink <- c(65.17, 16.27, 28.30, 17.13, 70.03, 41.43, 21.43,
24.37, 16.37, 14.47)
Swiss_home_screen_T2_blink <- c(39.23, 17.17, 1.20, 14.10, 8.30, 9.13, 20.13,
16.20, 19.47)
Swiss_home_screen_T3_blink <- c(31.00, 27.27, 23.00, 23.10, 19.23, 3.33, 14.23,
4.47, 16.40, 14.33)
Swiss_home_screen_total_blink <- c(Swiss_home_screen_T1_blink,
Swiss_home_screen_T2_blink,
Swiss_home_screen_T3_blink)

Swiss_home_screen_T1_afribit <- c(14.17, 8.10, 36.07, 17.07, 10.10, 6.30, 27.10,
18.03, 10.27, 12.17)

```



```

Swiss_home_screen_T2_afribit <- c(31.00, 9.03, 7.13, 10.17, 8.07, 4.27, 14.37,
                                4.20, 6.07, 12.10)
Swiss_home_screen_T3_afribit <- c(13.07, 9.13, 6.03, 4.00, 1.00, 2.07, 16.07,
                                2.10, 13.17, 4.07)
Swiss_home_screen_total_afribit <- c(Swiss_home_screen_T1_afribit,
                                     Swiss_home_screen_T2_afribit,
                                     Swiss_home_screen_T3_afribit)

# swiss group comparison
swiss_group_comparison <- wilcox.test(Swiss_home_screen_total_blink,
                                     Swiss_home_screen_total_afribit,
                                     alternative = "greater")
cat(paste("swiss_group_comparison wilcox:", swiss_group_comparison))

## swiss_group_comparison wilcox: c(W = 676) swiss_group_comparison wilcox: NULL swiss_group_compari

swiss_group_comparison

##
## Wilcoxon rank sum test with continuity correction
##
## data: Swiss_home_screen_total_blink and Swiss_home_screen_total_afribit
## W = 676, p-value = 0.0001329
## alternative hypothesis: true location shift is greater than 0

swiss_group_comparison$p.value

## [1] 0.0001328882

#both groups together
home_screen_blink <- c(Kibera_home_screen_total_blink,
                      Swiss_home_screen_total_blink)
home_screen_afribit <- c(Kibera_home_screen_total_afribit,
                        Swiss_home_screen_total_afribit)
both_groups <- wilcox.test(home_screen_blink,
                           home_screen_afribit,
                           alternative = "greater")
cat(paste("both_groups wilcox:", both_groups))

## both_groups wilcox: c(W = 2105.5) both_groups wilcox: NULL both_groups wilcox: 0.0156164145511009

both_groups

##
## Wilcoxon rank sum test with continuity correction
##
## data: home_screen_blink and home_screen_afribit
## W = 2105.5, p-value = 0.01562
## alternative hypothesis: true location shift is greater than 0

both_groups$p.value

## [1] 0.01561641

```


Anhang F

Blink Usability Form

20. How was the use of color in the system? *

Mark only one oval.

	1	2	3	4	5	6	7	
unattractive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	attractive

21. If you have comments or remarks, place them here

Anhang G

AfriBit Usability Form

20. How was the use of color in the system? *

Mark only one oval.

1 2 3 4 5 6 7

unattractive **attractive**

21. If you have comments or remarks, place them here

Anhang H

Usability form data

Please enter the data for the second evaluation here!

Use the item numbers in the printed questionnaire and the categories 1 (if the alternative on the extreme left is marked) to 7 (if the alternative on the extreme right is marked).

Leave the cell empty if the person has not answered the item. Please do not enter a special character in such cases, since this would cause errors in the calculations.

You can enter data for a **maximum of 1000** participants. If you need more, you have to adjust the formulas in the Excel.

In the field below you can enter a description for the data set entered in Data2. It will appear in the Scale Means Work-Sheet and helps to identify the results.

Description of data set 2:		AfriBit														
		Items														
1	2	4	5	8	9	11	12	13	17	19	20	21	22	23	24	
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	3
5	5	7	7	7	7	7	7	6	6	7	7	7	7	7	7	
7	5	6	7	7	7	7	7	6	6	6	7	6	7	7	7	
7	5	6	7	7	7	6	7	7	6	6	7	7	6	6	5	
7	5	7	7	7	7	7	7	7	7	7	7	7	7	7	7	
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	
4	2	7	7	7	7	5	5	7	5	4	7	5	7	5	2	
7	7	7	6	7	7	7	7	7	7	7	7	7	7	7	7	
6	7	7	6	5	6	7	7	7	6	6	7	7	6	6	6	
5	6	7	7	7	7	7	6	7	7	7	7	7	7	7	7	
6	4	7	5	7	7	6	6	6	6	7	6	6	6	6	6	
5	5	6	6	7	7	6	6	7	6	7	7	7	6	7	7	
6	5	7	7	7	7	7	7	7	6	6	7	7	6	7	7	
6	4	7	6	7	7	7	7	6	6	6	7	7	6	6	7	
6	4	6	6	6	6	6	6	6	5	6	5	6	4	6	3	
6	4	7	7	5	7	7	7	7	7	5	7	7	7	7	6	
7	2	6	7	6	7	6	7	7	6	7	7	7	6	7	7	
5	6	7	7	6	7	6	5	6	6	6	5	6	7	6	6	
6	4	7	7	7	7	6	7	6	7	6	5	7	7	6	7	
6	5	7	7	7	7	6	6	7	7	7	7	6	7	7	5	

Anhang I

UEQ calculations

Transformed Data (for Blink)

The order of the positive and negative term for an item is randomized in the questionnaire. Per dimension half of the items start with the positive and half with the negative term. Here you can find the transformed values per item. You can use these values for example for own statistical calculations. The +3 represent the most positive and the -3 the most negative value.

Items																									
1	2	4	5	8	9	11	12	13	17	19	20	21	22	23	24	3	6	7	10	14	15	16	18	25	26
0	-3	3	3	3	3	0	1	1	1	3	2	1	3	3	-1	3	3	3	3	3	3	3	3	3	3
3	2	3	3	3	3	3	3	-1	3	3	2	3	3	1	3	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	0	3	2	3	2	2	2	2	1	0	1	1	1	1	3	2	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	0	3	3	1	2	2	3	3	3	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3
2	3	3	2	2	3	3	3	3	3	2	1	3	3	2	3	3	3	3	3	3	3	3	3	3	3
1	2	3	3	2	2	2	2	3	2	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3
1	-1	-1	3	3	2	3	3	0	-1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
-1	-2	1	1	2	1	0	1	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
2	-1	3	2	1	3	0	2	1	0	0	2	-1	0	1	1	1	1	1	1	1	1	1	1	1	1
0	-2	-1	0	1	1	1	0	1	-1	-1	1	-2	-1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	3	1	3	2	1	2	3	2	1	3	-1	1	3	2	2	2	2	2	2	2	2	2	2	2
1	-2	2	2	2	2	1	1	2	1	1	2	1	2	1	2	2	2	2	2	2	2	2	2	2	2
1	-3	3	1	1	3	2	1	3	3	3	3	3	2	-3	1	2	3	3	3	3	3	3	3	3	3
3	0	2	3	1	2	1	3	3	1	3	3	1	2	3	2	3	3	3	3	3	3	3	3	3	3
1	-1	1	1	2	0	2	2	1	1	2	3	1	2	3	1	2	2	2	2	2	2	2	2	2	2
2	1	3	2	3	3	3	3	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	3	3	3	3	3	1	3	3	1	2	2	0	3	2	3	3	3	3	3	3	3	3	3	3	3

Skale means per person (first evaluation)				
Attractiveness	Perspicuity	Efficiency	Dependability	Stimulation
0.00	0.50	2.75	1.75	3.00
3.00	1.75	2.25	3.00	3.00
3.00	3.00	3.00	2.75	3.00
2.00	1.50	1.75	1.50	2.00
3.00	3.00	3.00	2.75	3.00
2.33	2.25	2.25	2.25	3.00
2.67	3.00	2.25	2.50	2.00
2.00	2.50	2.50	2.00	3.00
2.33	0.25	2.75	2.00	3.00
3.00	3.00	3.00	3.00	3.00
0.00	0.00	0.75	0.75	1.00
1.67	0.50	1.50	0.25	2.00
0.33	-1.00	0.50	0.00	0.00
2.00	1.25	2.25	1.75	1.00
0.00	0.75	2.00	1.25	2.00
1.33	1.25	1.00	2.25	1.00
2.67	1.50	2.50	1.50	3.00
1.00	0.50	1.75	1.75	1.00
2.33	2.25	3.00	2.75	2.00
2.33	2.25	2.50	1.75	3.00

Transformed Data (for AfriBit)
 The order of the positive and negative term for an item is randomized in the questionnaire. Per dimension half of the items start with the positive and half with the negative term.
 Here you can find the transformed values per item. You can use these values for example for own statistical calculations. The +3 represent the most positive and the -3 the most negative value.

Items																							
1	2	4	5	8	9	11	12	13	17	19	20	21	22	23	24								
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	-1							
1	1	3	3	3	3	3	3	2	2	3	3	3	3	3	3								
3	1	2	3	3	3	3	3	2	2	2	3	2	3	3	3								
3	1	2	3	3	3	2	3	3	2	2	3	3	2	2	1								
3	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3								
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3								
0	-2	3	3	3	3	1	1	3	1	0	3	1	3	1	-2								
3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3								
2	3	3	2	1	2	3	3	3	2	2	3	3	2	2	2								
1	2	3	3	3	3	3	3	2	3	3	3	3	3	3	3								
2	0	3	1	3	3	2	2	2	2	3	2	2	2	3	2								
1	1	2	2	3	3	2	2	3	2	3	3	3	2	3	3								
2	1	3	3	3	3	3	3	3	2	2	3	3	2	3	3								
2	0	3	2	3	3	3	3	2	2	2	3	3	2	2	3								
2	0	2	2	2	2	2	2	2	1	2	1	2	0	2	-1								
2	0	3	3	1	3	3	3	3	3	3	1	3	3	3	2								
3	-2	2	3	2	3	2	3	3	2	3	3	3	2	3	3								
1	2	3	3	2	3	2	1	2	2	2	1	2	3	2	2								
2	0	3	3	3	3	2	3	2	3	2	1	3	3	2	3								
2	1	3	3	3	3	2	2	3	3	3	3	2	3	3	1								

Skale means per person (second evaluation)				
Attractiveness	Perspiciuity	Efficiency	Dependability	Stimulation
1.67	3.00	3.00	3.00	3.00
2.33	2.25	3.00	2.75	3.00
3.00	1.75	3.00	2.50	3.00
2.33	2.25	2.50	2.25	3.00
3.00	2.50	3.00	3.00	3.00
3.00	3.00	3.00	3.00	3.00
-0.33	1.25	2.50	1.25	3.00
3.00	3.00	3.00	2.75	3.00
2.33	3.00	2.25	2.00	2.00
2.33	2.50	3.00	3.00	3.00
2.00	1.75	2.50	2.50	1.00
2.00	2.25	2.75	2.50	2.00
2.67	2.50	2.75	2.50	3.00
2.67	2.00	2.50	2.50	2.00
1.00	1.50	1.25	1.75	2.00
2.33	2.25	2.50	2.50	3.00
3.00	1.50	2.75	2.25	3.00
1.33	2.25	2.25	2.00	3.00
2.67	2.00	2.25	2.50	3.00
1.67	2.25	3.00	2.75	3.00

Comparison of Scale Means

Shows the scale means and the corresponding 5% confidence intervals.

Scale				Blink						AfriBit		
	Mean	STD	N	Confidence	Confidence Interval		Mean	STD	N	Confidence	Confidence Interval	
Attractiveness	1.85	1.06	20	0.46	1.39	2.31	2.20	0.83	20	0.37	1.83	2.57
Perspicuity	1.50	1.16	20	0.51	0.99	2.01	2.24	0.52	20	0.23	2.01	2.47
Efficiency	2.16	0.75	20	0.33	1.83	2.49	2.64	0.43	20	0.19	2.45	2.83
Dependability	1.88	0.85	20	0.37	1.50	2.25	2.46	0.45	20	0.20	2.26	2.66
Stimulation	2.20	0.95	20	0.42	1.78	2.62	2.70	0.57	20	0.25	2.45	2.95

Two sample T-Test assuming unequal variances

This sheet shows a simple T-Test to check if the scale means of two measured products differ significantly. As default the Alpha-Level 0.05 is used, but you can simply change this value in this sheet if you want to use a different level.

Alpha level: 0.05

Attractiveness	0.2525	No Significant Difference
Perspicuity	0.0152	Significant Difference
Efficiency	0.0205	Significant Difference
Dependability	0.0106	Significant Difference
Stimulation	0.0526	No Significant Difference