Development and Evaluation of a Blockchain-Based Application for Mobile Social Payments

Lucas Grabmaier
Advisor: Michael Fröhlich
Chair of Decentralized Systems Engineering
https://dse.in.tum.de/

15.04.2022 – 15.12.2022

Outline

1. Motivation
2. Research Gap
3. Solution Overview
4. Implementation
5. Evaluation

Adoption of crypto is comparable with the early Internet [3]

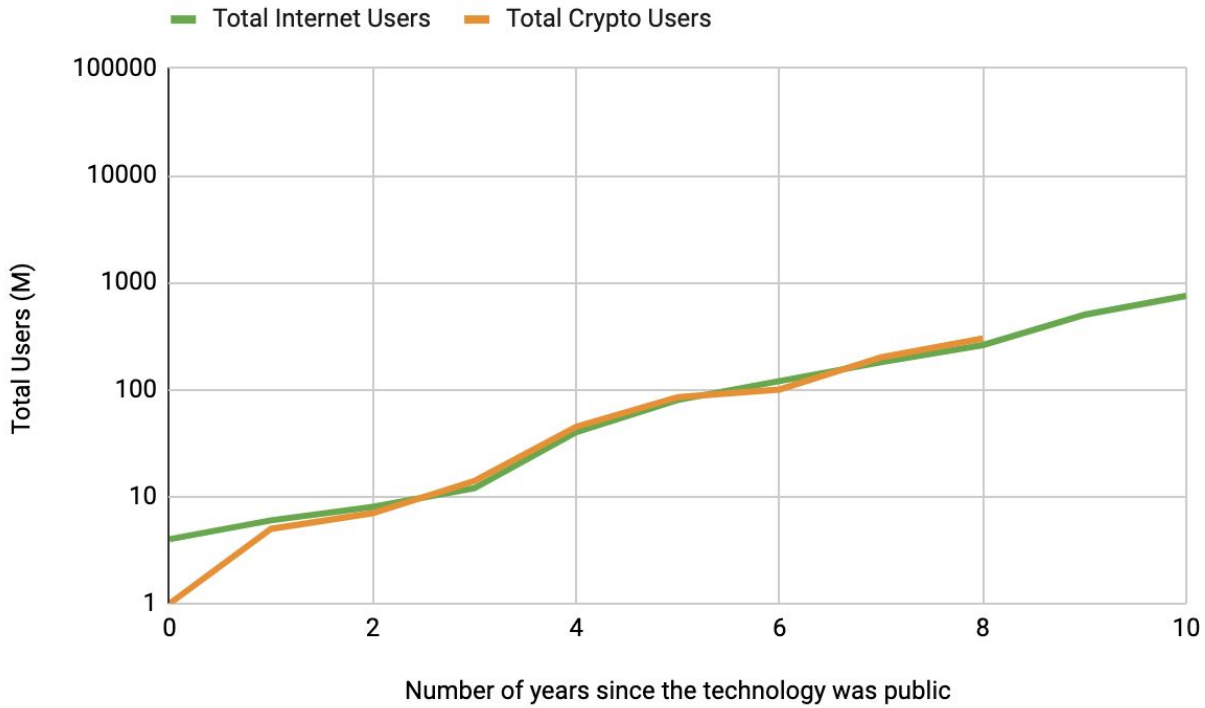


Figure adapted from: “Third Quarter 2021 Shareholder Letter“ (Coinbase, 2021), Sources: World Bank, Crypto.com

Payment apps gained significant adoption in a similar timeframe [5]

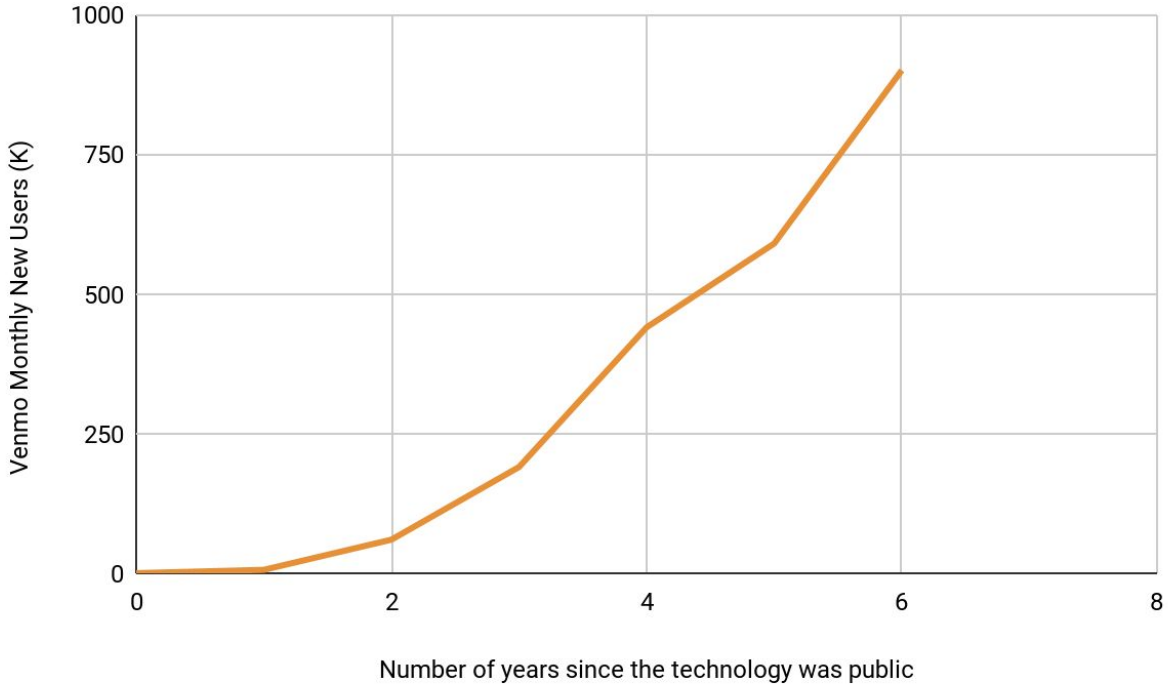


Figure adapted from: “Examining the Evolution of Mobile Social Payments in Venmo.” (C. Unger, D. Murthy, A. Acker, I. Arora, and A. Chang, 2020)

Cryptocurrencies struggle to find adoption as means of payment [4]

- Payment apps are the **default means of payment** for P2P transactions
  - Venmo: $230B total transaction volume in 2021 [6]
  - Social Awareness Streams (SAS) drive usage and engagement by allowing users to follow their friends transactions and establish **payments as social media** [7]
- Cryptocurrencies struggle with **issues rooted in their technological foundations**
  - Slow transaction speed and high transaction fees [8]
  - Poor user experience: Key management, volatility in transferred asset [9]
- Layer 2 protocols promise solution to **overcome those challenges**
  - Transaction settlement at near real-time speeds and low transaction costs [10]
  - No research on validity in practice for P2P use case, only Point of Sale (PoS) [11]

Research Gap

Do Layer 2's advancements enable P2P social payments on crypto?

A system is needed to provide a **reference implementation** of a social payment system built on Layer 2 protocols to evaluate:

1. Is it possible to build a mobile payment app using Layer 2 blockchain technologies as a viable alternative to established applications?

2. How do users interact with such an app when using it as a payment service in their everyday life?

3. Do "social payment features" such as a wallet feed add value to a mobile payment app?

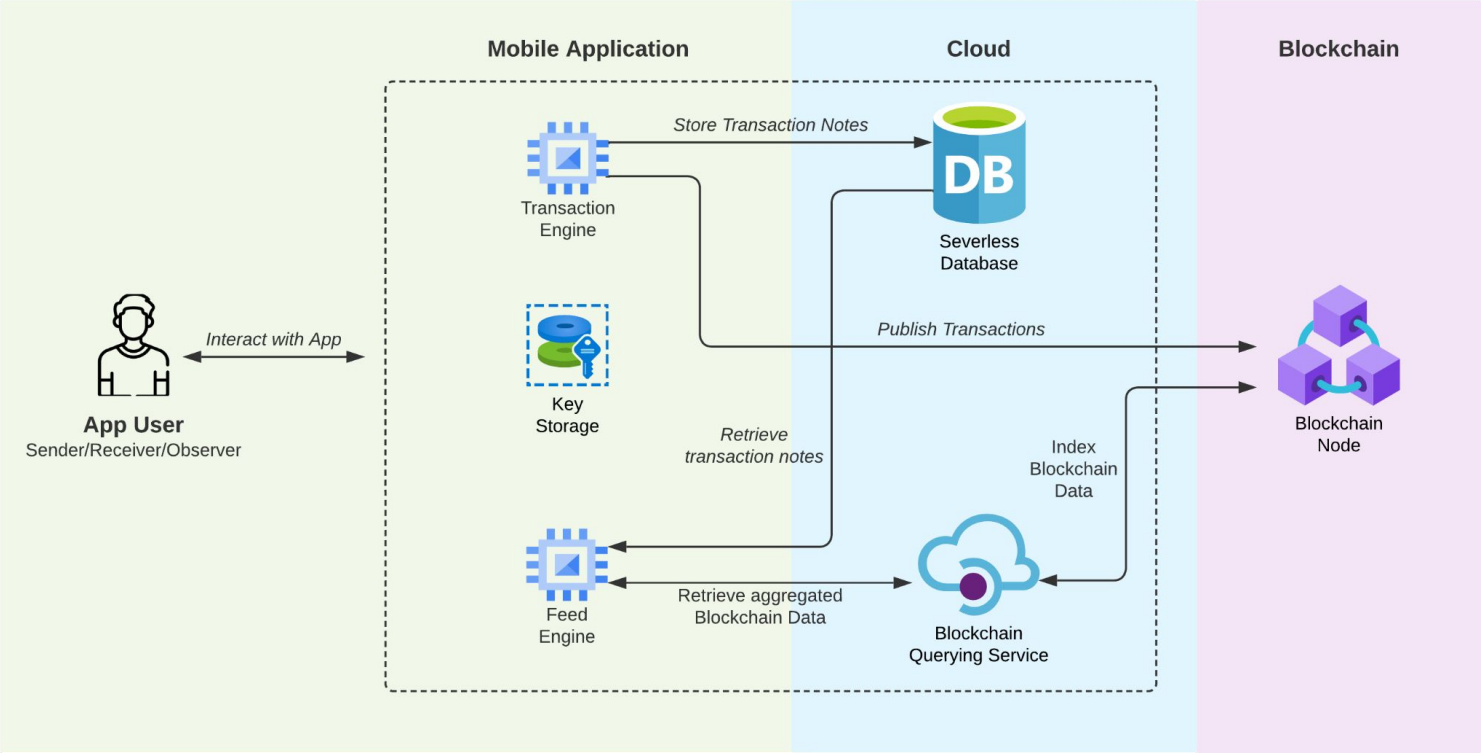
A P2P social payment application built on the Layer 2 Polygon

- Non-custodial wallet
- Multi-platform for iOS and Android
- Supports USDC stablecoin to address volatility

Three Use Cases:

1. Sending a transaction and adding a transaction note
2. Receiving a transaction via address or QR code
3. Following friends' transactions in a social feed

The system is built as a two-tier serverless architecture



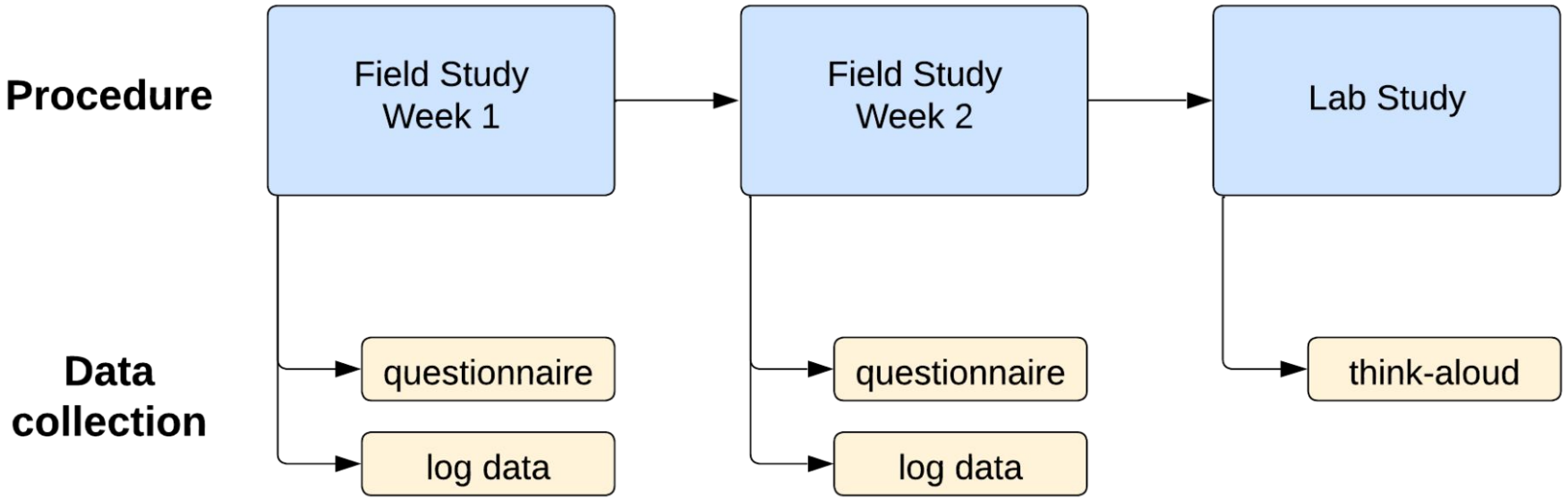
rainbow

Built with Firebase

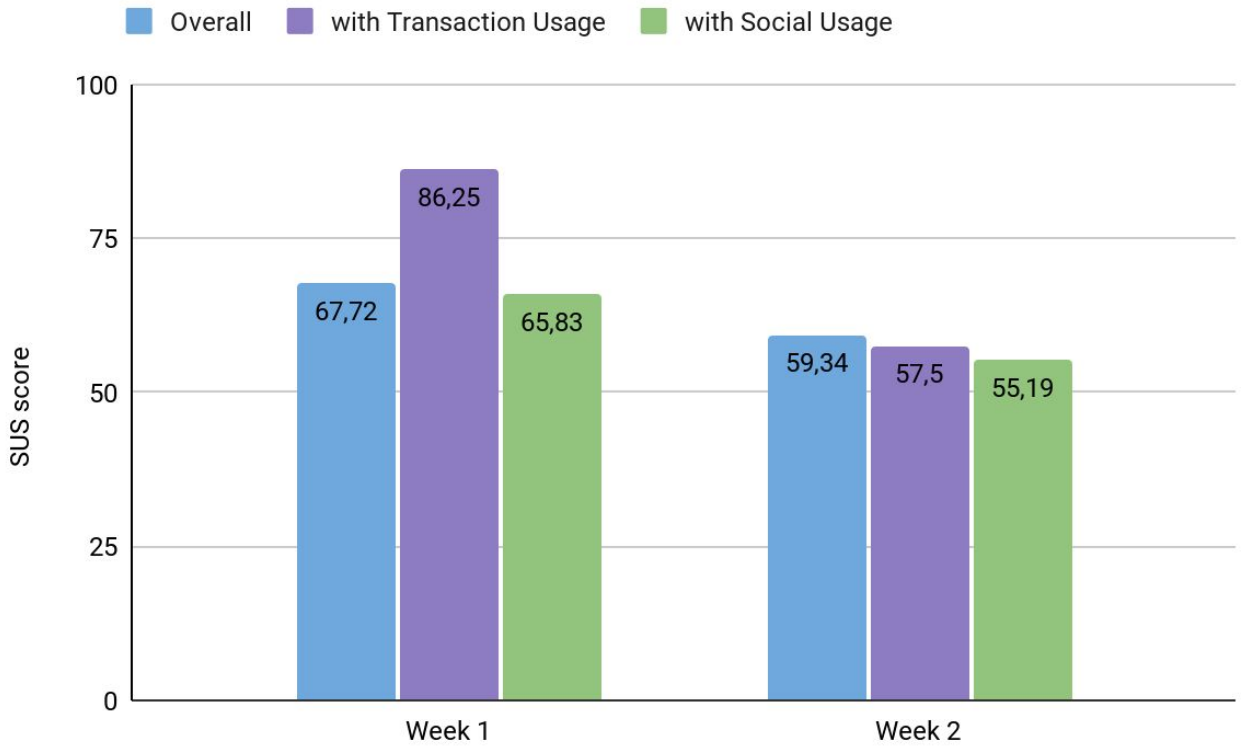
Covalent

polygon

23 participants in the Field Study and 6 interviewees in the Lab Study



The wallet received below average SUS scores [1] [2]



Transaction Usage: Transactions / Week > 2; Social Usage: Contacts added/Notes sent > 0

- Below average scores expected for an early stage prototype
- Social Usage led to a slight score decrease
- WoW differences rooted in longer and more critical use of the system in week 2

Insight 1: Payment applications need to offer a distinct benefit

- Perceived value of system for users is based on:
  - Whether all expected functionality is provided
  - Whether a **distinct benefit** is provided over currently used systems like PayPal

- Network effects strengthen the position of established players like Venmo and PayPal [12]
  - **An existing habit with another system was cited by 43%** of all field study participants
  - These habits are based on who of their friends is using the system

- Users need to be incentivized to switch to a new system
  - Users state interest trying in novel solutions like cryptocurrencies
  - Usability challenges posed by blockchain-based systems **keep users from changing their habits**

Insight 2: Crypto-based usability challenges need to be abstracted

- Various usability challenges **still persist when using Layer 2 protocols**
  - Requirement to check whether recipient can receive a certain token instead of SEPA
  - Mnemonic phrase as backup instead of customer support
- Additional **guidance can be a solution** for technical inclined users
  - Is often ignored by impatient or inexperienced users as they are complicated
- **Abstracting usability challenges** is the better solution for most users
  - Most users do not care about the underlying technical implementation or understanding it
  - They “just want to achieve [their] goal instead of needing to worry whether the other party can receive a transaction” (P6)

Insight 3: Privacy features are key for social payment applications

- Privacy are the main reason for below average SUS score
  - All participants had privacy concerns about sharing transaction history with friends
  - 50% of the participants would not use the application if it features the Wallet Feed

- Main concerns:
  - Getting judged for one's spending
  - Fostering negative emotions such as jealousy in a friend group

- Privacy features allow all parties to use the application
  - Enable providing a social payment experience for interested users
  - Enable providing a standard payment application to all other users

Summary

Established cryptocurrencies like Bitcoin are not designed for P2P payments

- Technical limitations cause low transaction speed and high fees
- Volatility of asset impedes payments of everyday life

Our Wallet based on Layer 2 Polygon:

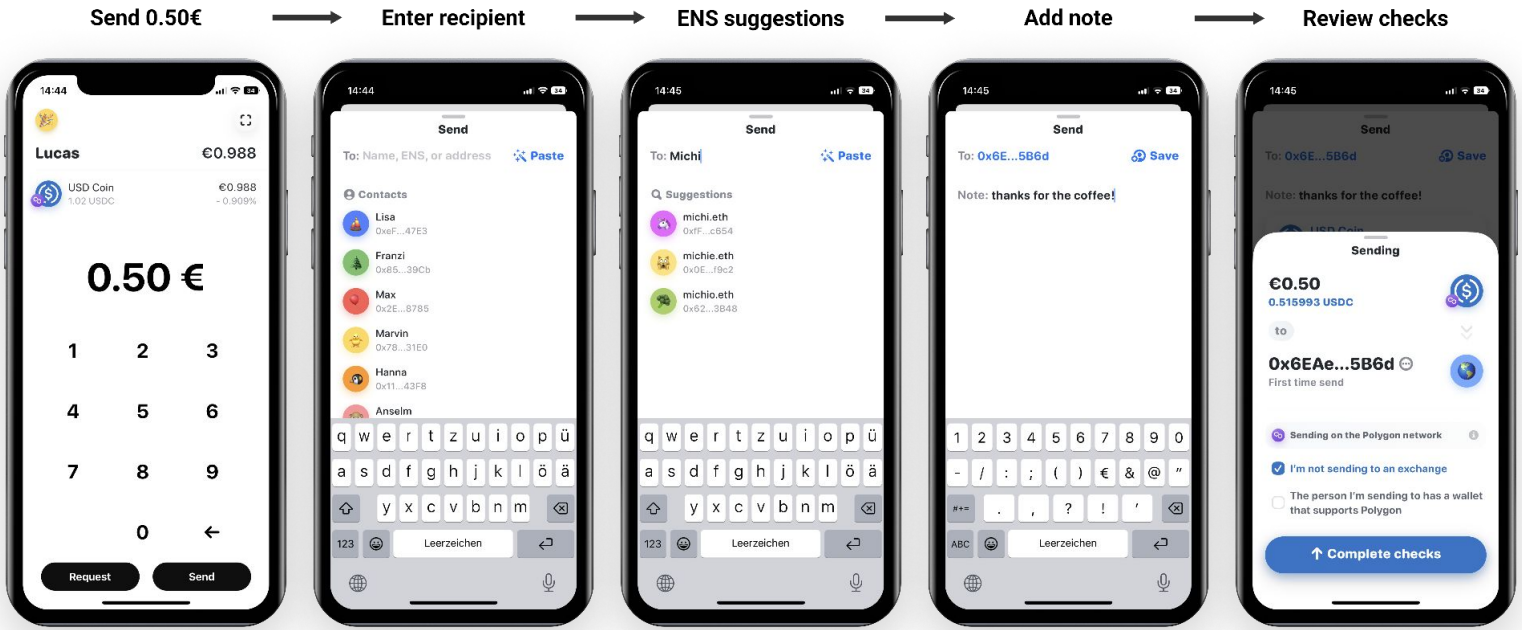
- Provides a reference implementation and demonstrates **viability of building a social payment system** on the Layer 2 protocol Polygon
- Provides near-instant speed, low fees and **no volatility**
- **Usability challenges still exist** for inexperienced users
- Social payment features only add limited value and **involve privacy concerns**

Q&A

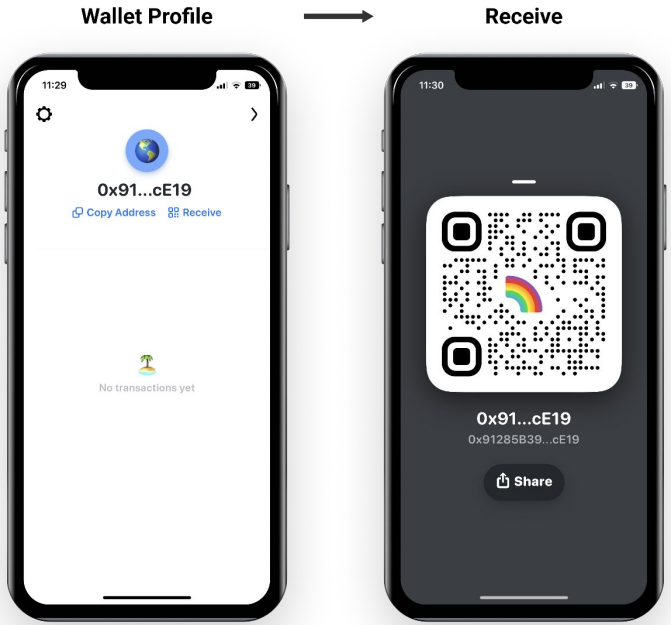
Thank you for your attention!

Backup

Use Case 1: Sending a transaction and adding a note for the recipient

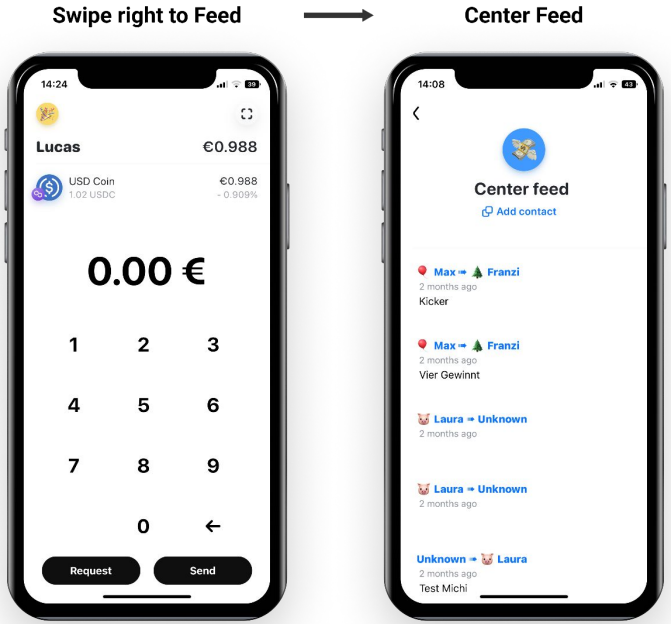


Use Case 2: Receiving a transaction via QR code or address



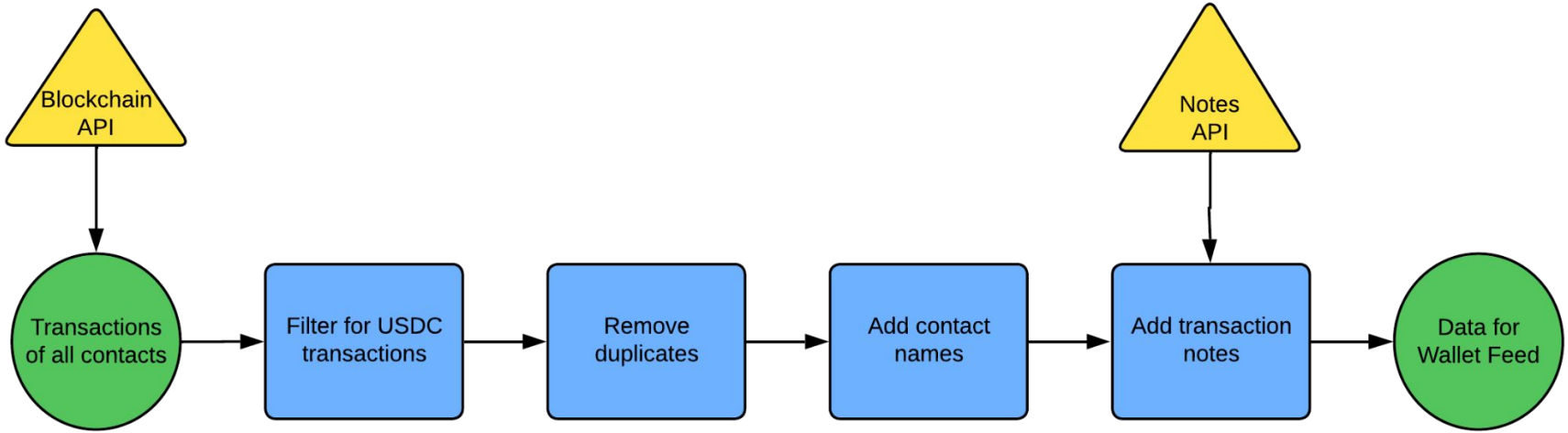
- Wallet Profile displays all transactions of the individual wallet
- Wallet can be customized with name and profile picture
- Funds can be received by either sharing the wallet address or showing a QR code representing the address

Use Case 3: Following friends' transactions via the Wallet Feed



- Wallet Feed displays the transactions of all saved contacts
- Each transaction entry features
  - Sender
  - Recipient
  - Time elapsed since transaction
  - Transaction Note

Feed Engine leverages APIs to generate the Wallet Feed on device



The resulting data is displayed for the user as the Wallet Feed in the UI

Design Decision for Polygon as the Layer 2 protocol

	Polygon	Rollups	Solana
EVM Compatibility	Yes	Yes	No
Transaction Cost	0,002€	0,45€	0,00025€
Transactions per Second	7k	40k	710k
Project Status	Active	In Testing	Active
Developer Resources	Plenty	Developing	Sufficient

The Polygon network does well in all criteria without missing any (like Solana)

Lab Study interview tasks

1. Create a new wallet with the Rainbow App
2. Fund your wallet with $2 USDC Coins and 2 MATIC Coins
3. Send a transaction of 0,5 € to Lucas with the note “Test {your name}”
4. You paid for my lunch and want me to pay you back using the Rainbow App. How can I send you your money?
5. You use the Rainbow App with your friends and have saved them as contacts. Take a look at the transactions of their friends.
6. You want to protect your wallet. Create a backup of your private keys.

The application’s SUS score can be improved in three steps

Achieve Feature Parity 	**Provide Distinct Benefits** 	**Offer Privacy Controls** 
1. Fiat on-ramp 2. Sharable URL 3. Security	1. Engagement features 2. Payment insights	1. Audience controls 2. Friend requests

Sources

[1] J. Brooke. “SUS: A quick and dirty usability scale.” In: *Usability Eval. Ind.* 189 (Dec. 1995).

[2] A. Bangor, P. Kortum, and J. Miller. “Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale.” In: J. Usability Stud. 4 (Dec. 2009), pp. 114–123.

[3] Marc Andreessen. “Why Bitcoin Matters“ (2014) URL: https://archive.nytimes.com/dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/ (last accessed: 12.12.2022)

[4] K. Krombholz, A. Judmayer, M. Gusenbauer, and E. Weippl. “The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy.” In: Dec. 2017, pp. 555–580. isbn: 978-3-662-54969-8.

[5] C. Unger, D. Murthy, A. Acker, I. Arora, and A. Chang. “Examining the Evolution of Mobile Social Payments in Venmo.” In: International Conference on Social Media and Society. SMSociety’20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 101–110. isbn: 9781450376884. doi: 10.1145/3400806. 3400819.

[6] “Value of payments processed of Venmo” (Statista, 2022) URL: https://www.statista.com/statistics/763617/venmo-total-payment-volume/ (last accessed: 12.12.2022)

[7] A. Acker and D. Murthy. “Venmo: Understanding Mobile Payments as Social Media.” In: SMSociety ’18: Proceedings of the 9th International Conference on Social Media and Society. Dec. 2018, pp. 5–12. isbn: 9781450363341. doi: 10.1145/3217804. 3217892.

[8] C. Sas and I. E. Khairuddin. “Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users.” In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. CHI ’17. New York, NY, USA: Association for Computing Machinery, 2017, pp. 6499–6510. isbn: 9781450346559. doi: 10. 1145/3025453.3025886.

Sources

[9] M. Froehlich, M. Wagenhaus, A. Schmidt, and F. Alt. “Don’t Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users.” In: Dec. 2021, pp. 138– 148. doi: 10.1145/3461778.3462071.

[10] K. Grauer, W. Kueshner, E. McMahon, and H. Updegrave. The Chainalysis State of Web3 Report. 2022.

[11] M. Froehlich, J. A. Vega Vermehren, F. Alt, and A. Schmidt. “Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning.” In: Association for Computing Machinery (ACM), Oct. 2022, pp. 1–12. isbn: 9781450396998. doi: 10.1145/3546155.3546700.

[12] A. Milne. “What is in it for us? Network effects and bank payment innovation.” In: Journal of Banking & Finance 30.6 (2006), pp. 1613–1630. issn: 0378-4266. doi: https://doi.org/10.1016/j.jbankfin.2005.09.006.