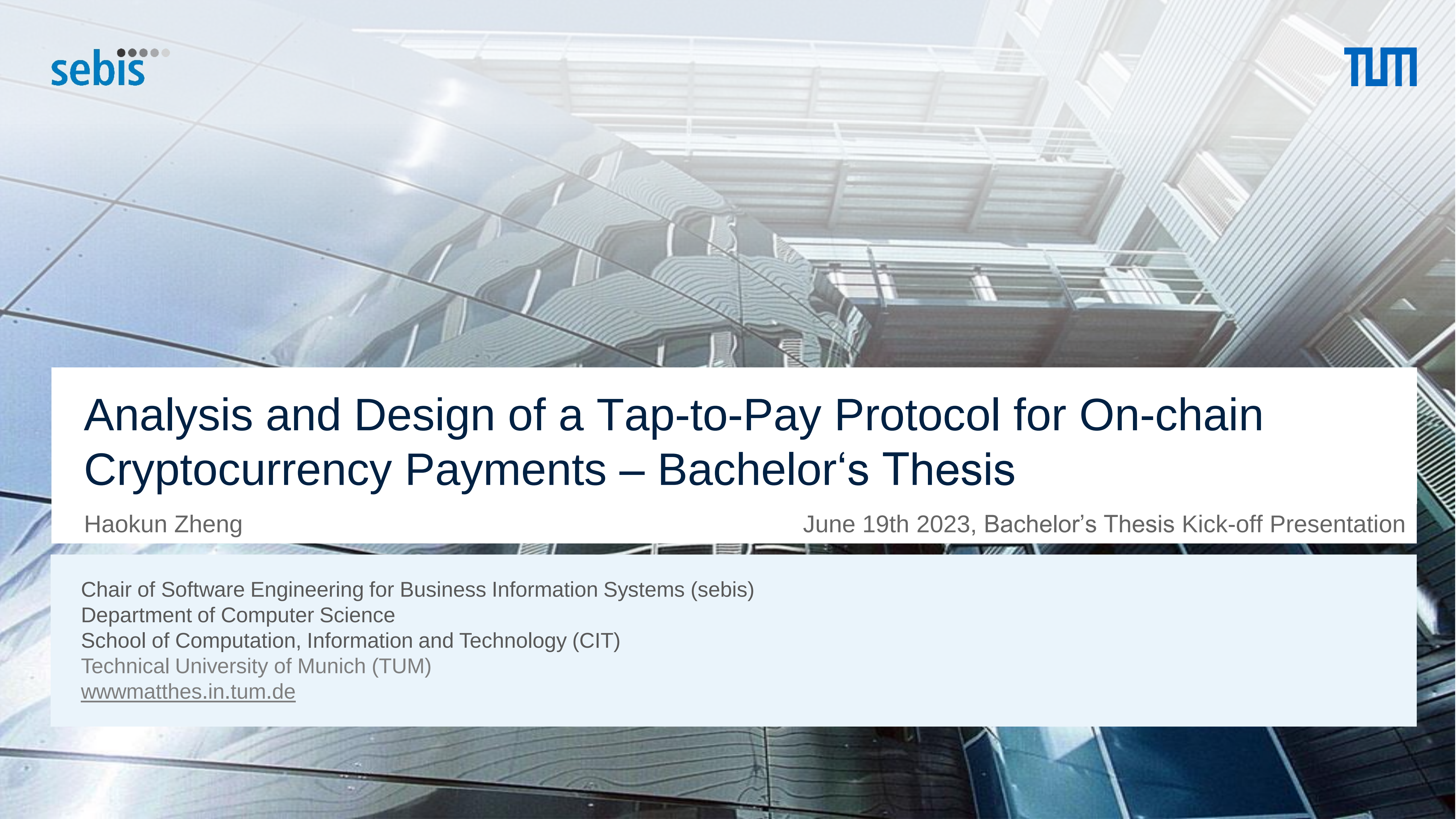


Analysis and Design of a Tap-to-Pay Protocol for On-chain Cryptocurrency Payments – Bachelor‘s Thesis

Haokun Zheng

June 19th 2023, Bachelor’s Thesis Kick-off Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

Motivation & State of the Art

Problem Statement

- Potential approach

Research Questions

Methodology

Timeline

Motivation

On paper…

Modern public blockchain infrastructure supports high enough capacity for mainstream payment volume…

… with potentially orders of magnitude lower transaction fees than Visa & Mastercard

+ Decentralization & Self-custody of funds

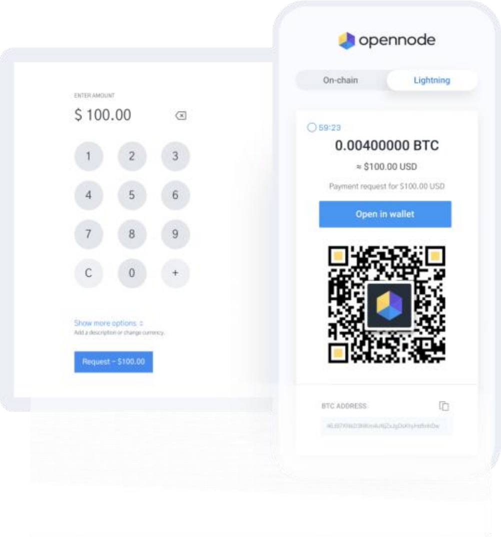
+ Higher degree of transparency

+ Improved security through immutability

+ Greater financial inclusion

State of the Art consumer payment solutions for blockchain tx

opennode



opennode

ENTER AMOUNT

$ 100.00

59:23

0.00400000 BTC

≈ $100.00 USD

Payment request for $100.00 USD

BTC ADDRESS

bitpay

Pay

Relevant Standards:

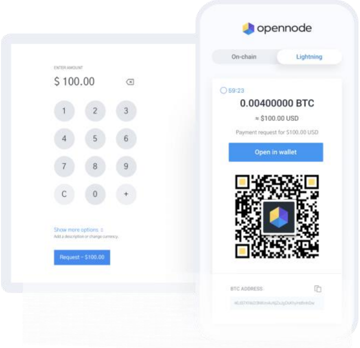
BIP 21

Ethereum ERC-681

Solana Pay

State of the Art consumer payment solutions for blockchain tx

opennode



ENTER AMOUNT

$ 100.00

Show more options

Add a description or change currency.

Request - $100.00

opennode

On-chain | Lightning

59:23

0.00400000 BTC

≈ $100.00 USD

Payment request for $100.00 USD

Open in wallet

BTC ADDRESS

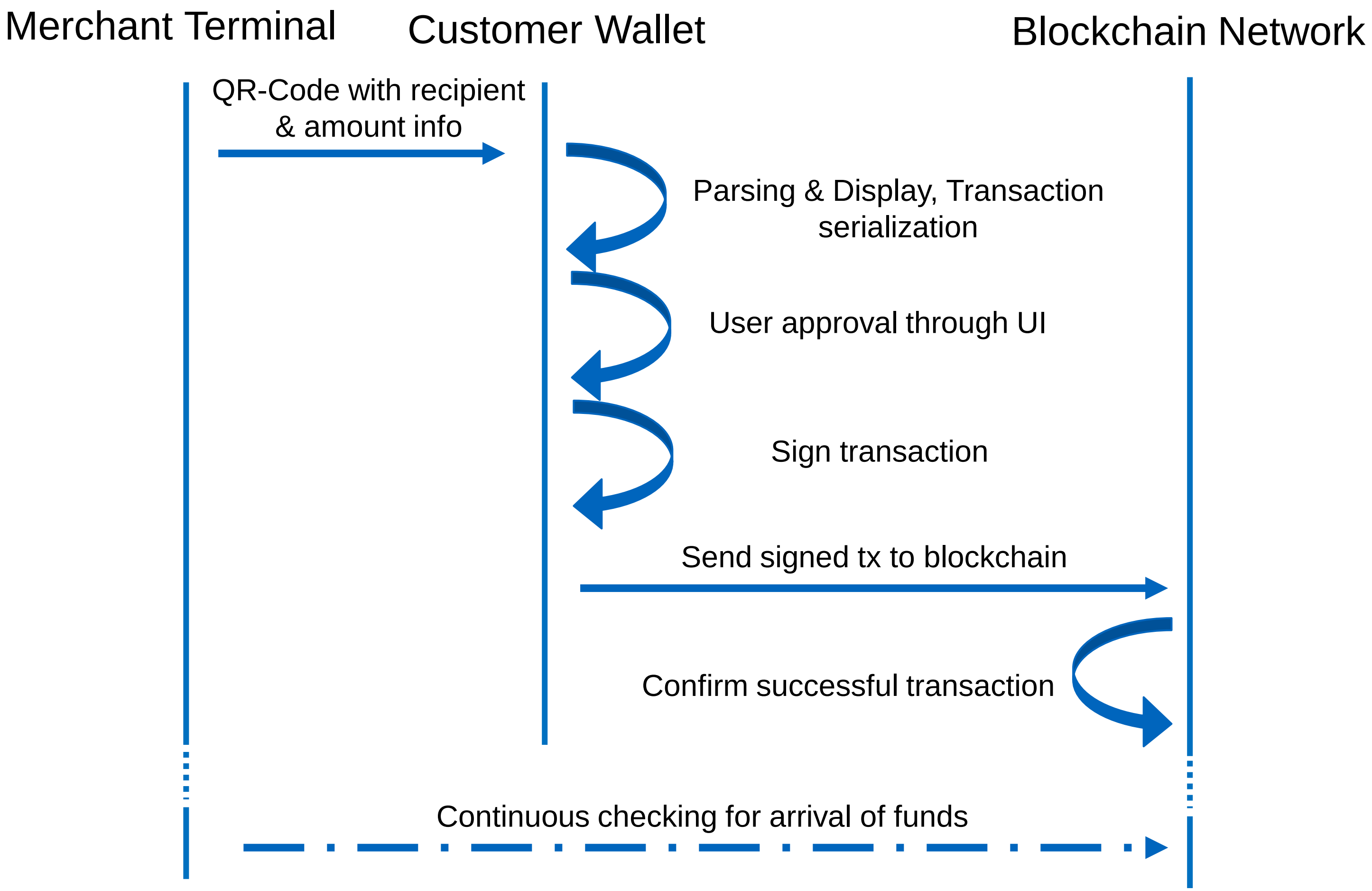
bitpay

Pay

Relevant Standards:

BIP 21
Ethereum ERC-681
Solana Pay

Current interaction flow:



Merchant Terminal

Customer Wallet

Blockchain Network

QR-Code with recipient & amount info

Parsing & Display, Transaction serialization

User approval through UI

Sign transaction

Send signed tx to blockchain

Confirm successful transaction

Continuous checking for arrival of funds

Motivation & Problem

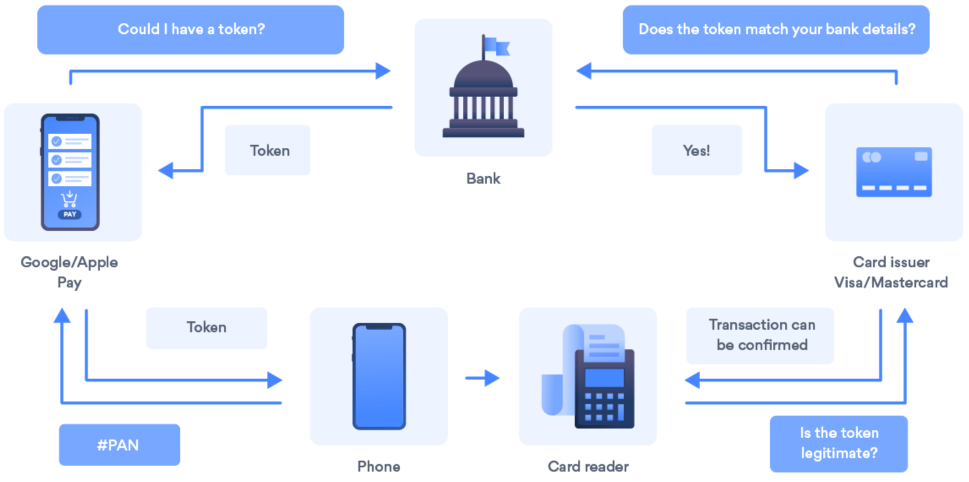
Modern public blockchain infrastructure supports high enough capacity for mainstream payment volume…

… with potentially orders of magnitude lower transaction fees than Visa & Mastercard

Current crypto wallets are complex to set up and funds only accessible on a previously configured device

Slow QR code-based payments & incompatible with current POS hardware
Users must have battery & service

Problem Statement: Analysis & development of a tap to pay protocol



How contacless mobile payments work

Feasibility analysis & development

Fiat mobile and card-based contactless payments widely adopted

Tap to pay protocol for signing and sending on-chain transactions for payment scenarios

Potential approach: Divide classical wallet into two independent components:

1. Universal Wallet Software

Generic wallet software compatible with any device

Stateless & account-less transaction staging & sending

- Prepares to be signed transactions
- Sends off signed transactions
- Functions as general-purpose access point for blockchain networks

2. Physical NFC token/card or digital Apple Pay/Google Pay card – Cold wallet

- Pin-encrypted public & private keys
- “Personalizes” & signs transactions from universal wallet terminal
- Signing happening on card/device -> private key never leaves the cold wallet

Research questions

RQ1: How do current fiat tap to pay payment methods work?

Pay G Pay VISA mastercard

RQ2: What are the current state of the art crypto payment methods?

opennode bitpay Pay

RQ3: What are general functional requirements & critical security properties of any tap to pay payment protocol?

Research questions

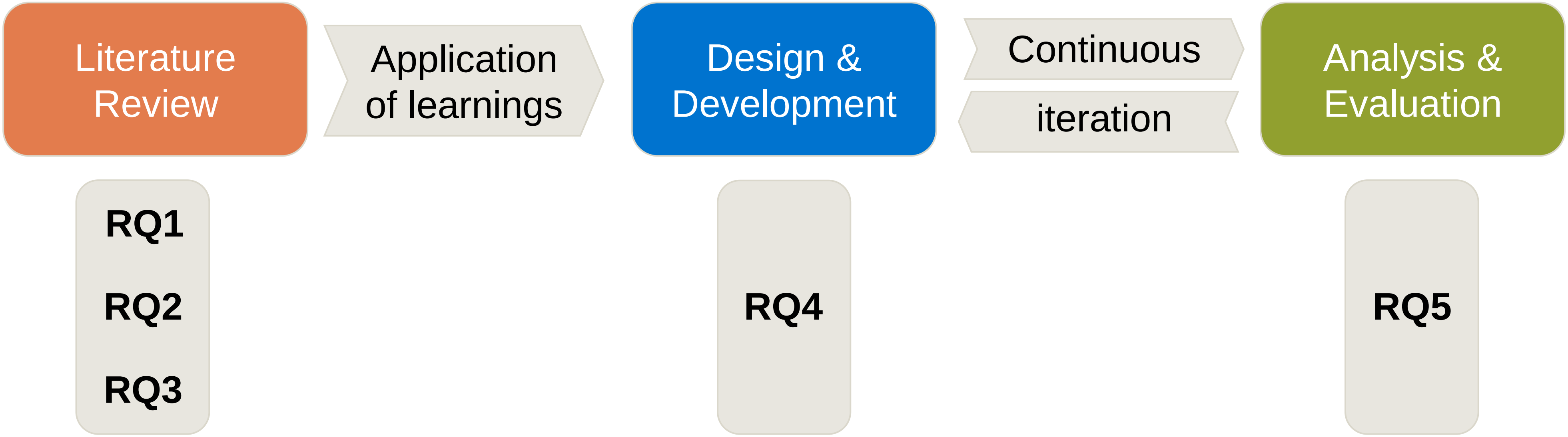
RQ4: How could a usable and secure tap to pay payment system be implemented for on-chain crypto transactions?

- Potential platforms
- Hardware/software/security limitations
- Impact of chosen blockchain platform with regards to block-time/tx finality & consensus type

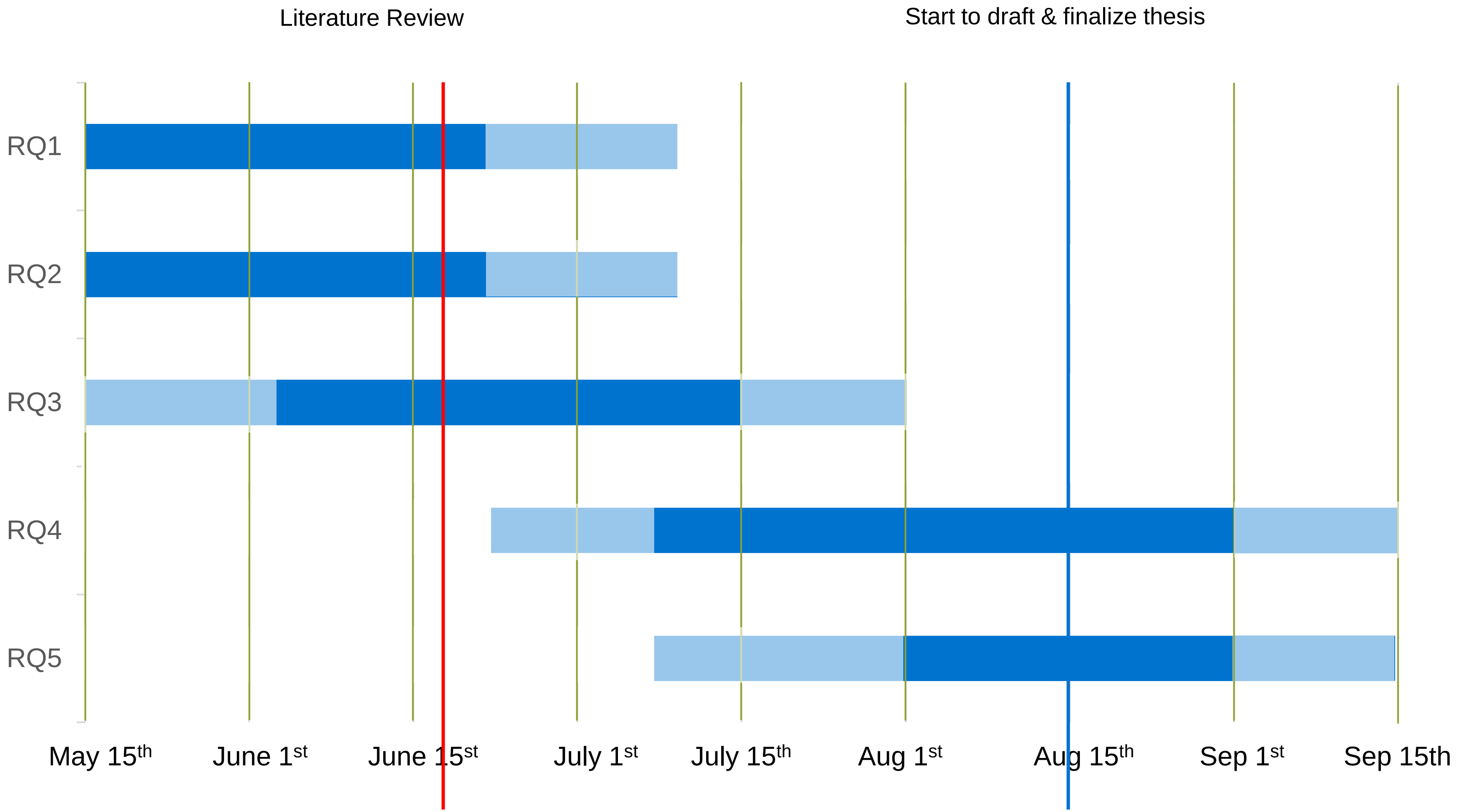
RQ5: How does the proposed tap to pay system compare to existing fiat tap to pay solutions and cryptocurrency payment methods in terms of performance, security, and usability?

- Implementable functional feature set
- Speed & usability comparison
- Resistance against known tap to pay & cryptocurrency specific attack vectors

Methodology



Rough Timeline



Haokun Zheng
haokun.zheng@tum.de

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business
Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

+49.89.289.17132
matthes@in.tum.de
wwwmatthes.in.tum.de

References

- [1] Solana Labs. A decentralized, permissionless, and open-source payments protocol | Solana Pay. Retrieved February 28, 2023. https://solanapay.com/
- [2] Bitcoin.org. Payment processing – Bitcoin Documentation. Retrieved February 28, 2023. https://developer.bitcoin.org/devguide/payment_processing.html
- [3] OpenNode. Bitcoin payment processor. Retrieved February 28, 2023. https://www.opennode.com/
- [4] Bitpay. Bitcoin point of sale terminal - accept crypto in-store with BitPay. Retrieved February 28, 2023. https://bitpay.com/retail
- [5] URL Format for Transaction Requests, Ethereum ERC-681. 2017. https://eips.ethereum.org/EIPS/eip-681
- [6] Michael Froehlich, Jose Adrian Vega Vermehren, Florian Alt, and Albrecht Schmidt. 2022. Implementation and Evaluation of a Point-Of-Sale Payment System Using Bitcoin Lightning. In Nordic Human-Computer Interaction Conference (NordiCHI '22). Association for Computing Machinery, New York, NY, USA, Article 16, 1–12. https://doi.org/10.1145/3546155.3546700
- [7] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. 2021. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 642, 1–14. https://doi.org/10.1145/3411764.3445407
- [8] Dongcheng Li, W. Eric Wong, Matthew Chau, Sean Pan, Liang Seng Koh. 2020. A Survey of NFC Mobile Payment: Challenges and Solutions using Blockchain and Cryptocurrencies. 7th International Conference on Dependable Systems and Their Applications (DSA), Xi'an, China, 2020, pp. 69-77. https://doi.org/10.1109/DSA51864.2020.00018

References

- [9] Abdul Ghaffar Khan, Amjad Hussain Zahid, Muzammil Hussain, Usama Riaz. 2019. Security Of Cryptocurrency Using Hardware Wallet And QR Code. International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 2019, pp. 1-10. https://doi.org/10.1109/ICIC48496.2019.8966739
- [10] Eskandari, Shayan, Jeremy Clark, and Abdelwahab Hamou-Lhadj. 2016. Buy Your Coffee with Bitcoin: Real-World Deployment of a Bitcoin Point of Sale Terminal. Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), Toulouse, France, 2016, pp. 382- 389. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0073
- [11] Shirsha Ghosh, Joyeeta Goswami, Abhishek Kumar, Alak Majumder. 2015. Issues in NFC as a form of contactless communication: A comprehensive survey. International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Avadi, India, 2015, pp. 245-252. https://doi.org/10.1109/ICSTM.2015.7225422
- [12] Tabet, Nour Elhouda, and Media Anugerah Ayu. Analysing the security of NFC based payment systems. International Conference on Informatics and Computing (ICIC), Mataram, Indonesia, 2016, pp. 169-174. https://doi.org/10.1109/IAC.2016.7905710
- [13] Kungpisdan, Supakorn, Bala Srinivasan, and Phu Dung Le. 2004. A secure account-based mobile payment protocol. International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004., Las Vegas, NV, USA, 2004, pp. 35-39 Vol.1, https://doi.org/10.1109/ITCC.2004.1286422
- [14] Mihir Bellare et al. 200. Design, implementation, and deployment of the iKP secure electronic payment system. IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 611-627, April 2000. https://doi.org/10.1109/49.83993