Design and Evaluation of Secure Multi-Party Computation Approaches for Non-Custodial Crypto Wallets with a Focus on User Experience and Security

Lucas Kissling

27.11.2023, Master's Thesis Kick-Off

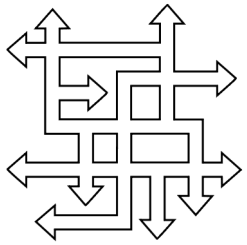
Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

1. Motivation and Introduction
2. Problem Statement and Initial Findings
3. Research Questions & Methodology
4. Timeline & Current Status

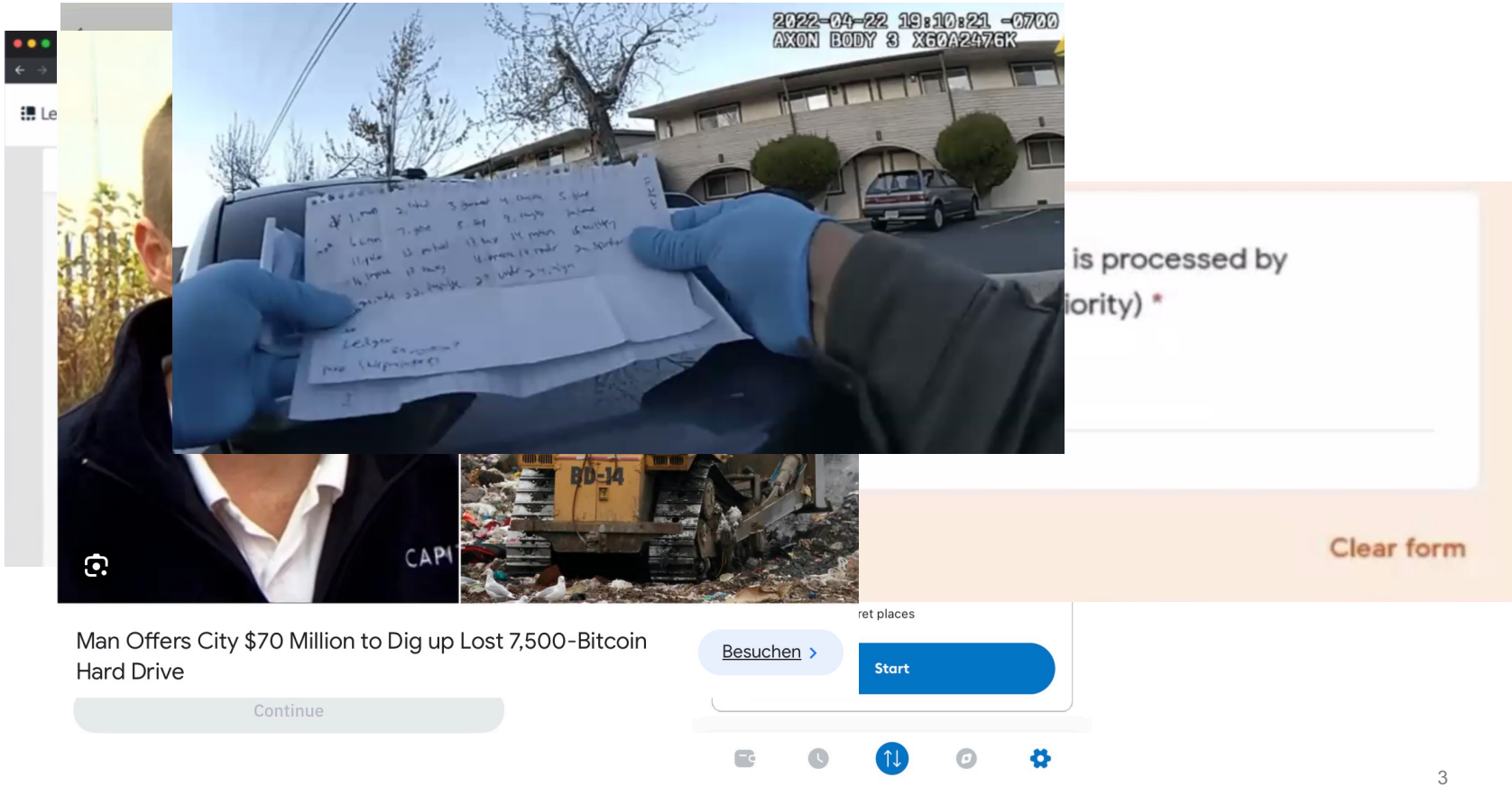
Motivation - Security and usability challenges of crypto asset self-custody

- Digital assets such as cryptocurrencies have revolutionized financial transactions
  → Surge in the development of mobile wallets for these assets
- These crypto assets enable independence from centralized institutions like banks (and should prevent bank runs)



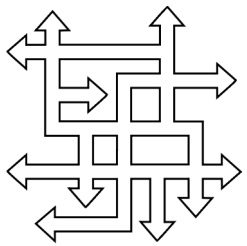
High complexity and many pitfalls of crypto asset self-custody for average user

But …



Motivation - Security and usability challenges of crypto asset self-custody

- Digital assets such as cryptocurrencies have revolutionized financial transactions
  → Surge in the development of mobile wallets for these assets
- These crypto assets enable independence from centralized institutions like banks (and should prevent bank runs)

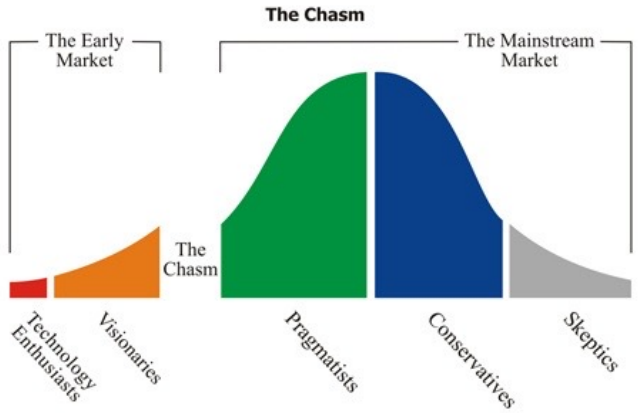


High complexity and many pitfalls of crypto asset self-custody for average user

But …

FTX

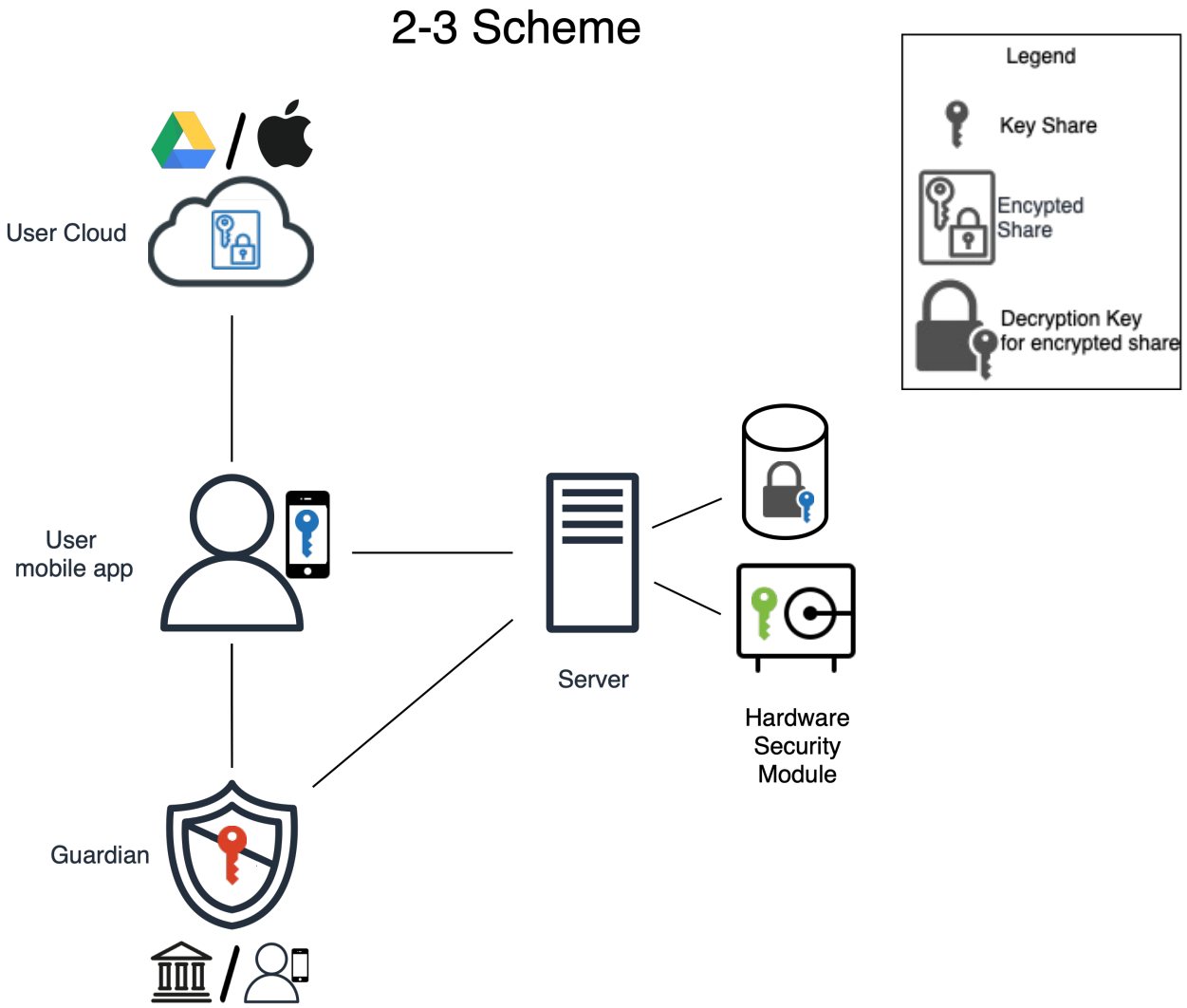
Contrary to the blockchain ethos, users leave assets on centralized exchanges.



Barrier for mass adoption

Signature scheme and recovery architecture – first exemplary artifact version

- Multi Party Computation: Each party generates a share of a private key together with the other parties off-chain
- Account Abstraction: Functions of parties are defined on-chain and co-signing also happens on-chain
- User co-signs transactions with service provider
- In case of censorship/bankruptcy of service provider or switching the mobile platform, the user can regain access to the funds through a guardian
- 2-3 or 2-2 Threshold Signature Scheme



Outline

1. Motivation and Introduction
2. Problem Statement and Initial Findings
3. Research Questions & Methodology
4. Timeline & Current Status

Problem Statement - Goal

- Wallet without need to write down private key mnemonics
- No single point of failure (private key)
- Further bring user experience closer to a custodial solution like on a bank account or an exchange (with functionalities like transaction limits, inheritence, ...)

Goal: Design of a secure and user error-free crypto asset management platform that is truly non-custodial and ensures asset recoverability in any scenario

Problem Statement

- Positive impact of MPC on security has been shown
  - But the impact on user experience and its interplay with security has not yet been explored

- Various possible setups of the signature scheme and recovery architecture with different implications on security and user experience
  - But an optimal one has not jet emerged
  - Room for improvement

Requirements

Functional Requirements (FR):

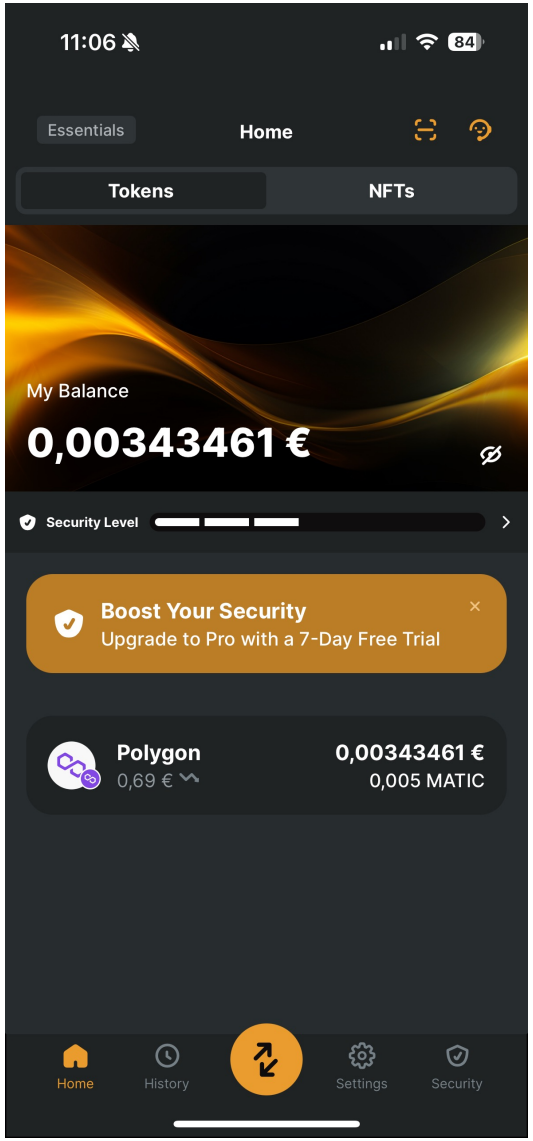
- User can **always recover assets (main focus)**:
  - if phone is lost
  - if switched to another OS
  - if application server not responding because of bankruptcy
  - if application server not responding because of censorship/ sanctions
  - If user wants to leave the platform and export seed phrase
- Plausible deniability (wrench attack): This requirement concerns the system's ability to offer a specific function that aids in user security under specific conditions (like under threat).
- In case of unauthorised access or user error, the damage can be contained through transaction limits
- Assets are not lost, when user passes away —> inheritance

Non-Functional Requirements (NFR):

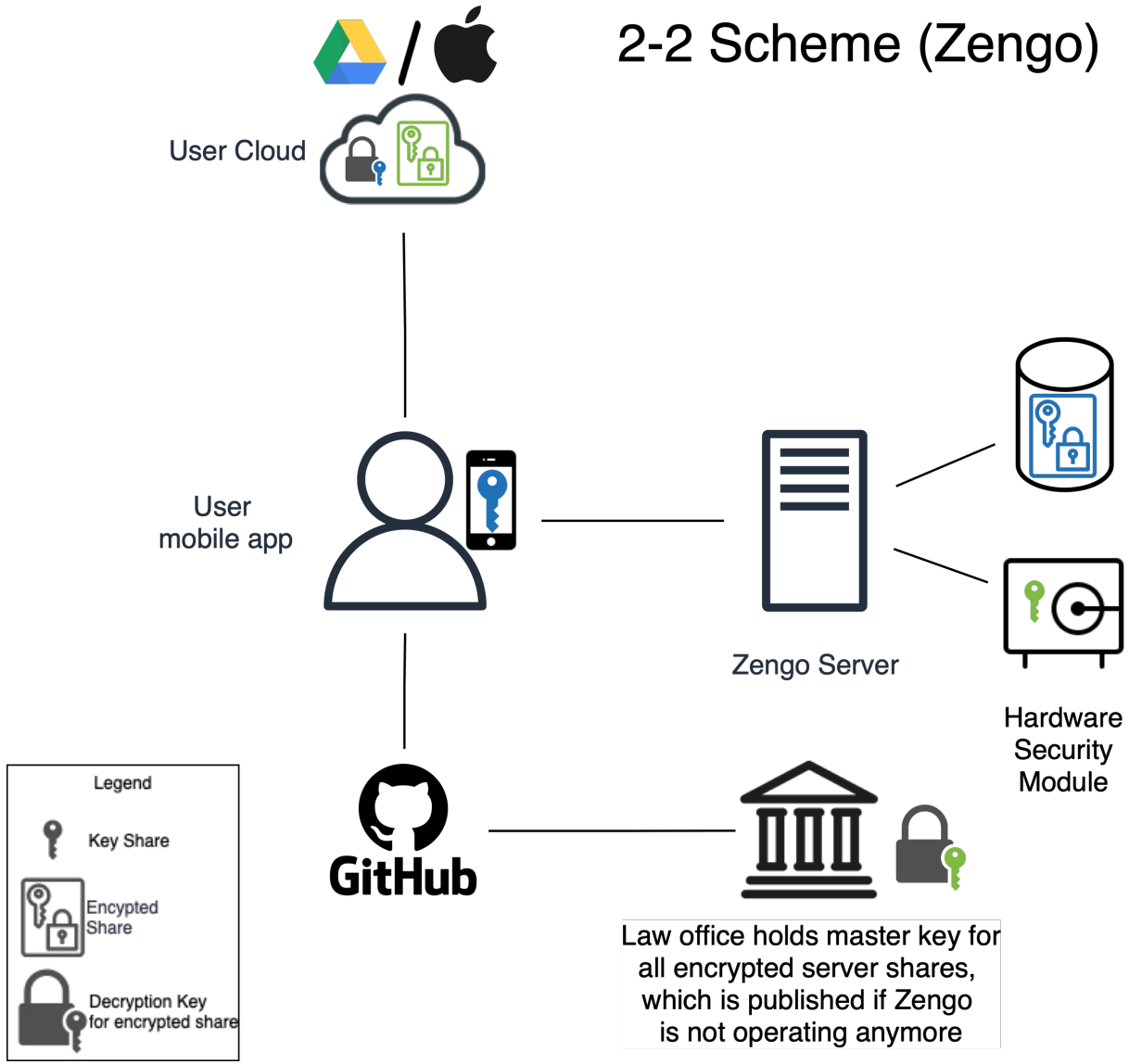
- Intuitive UI (user finds what he wants to do in under 10 seconds, e.g., payment, receive/send funds, recover account)
- Onboarding within 1 minute
- Safety requirements
  - **private key cannot be derived by a single party** as long as the account is active

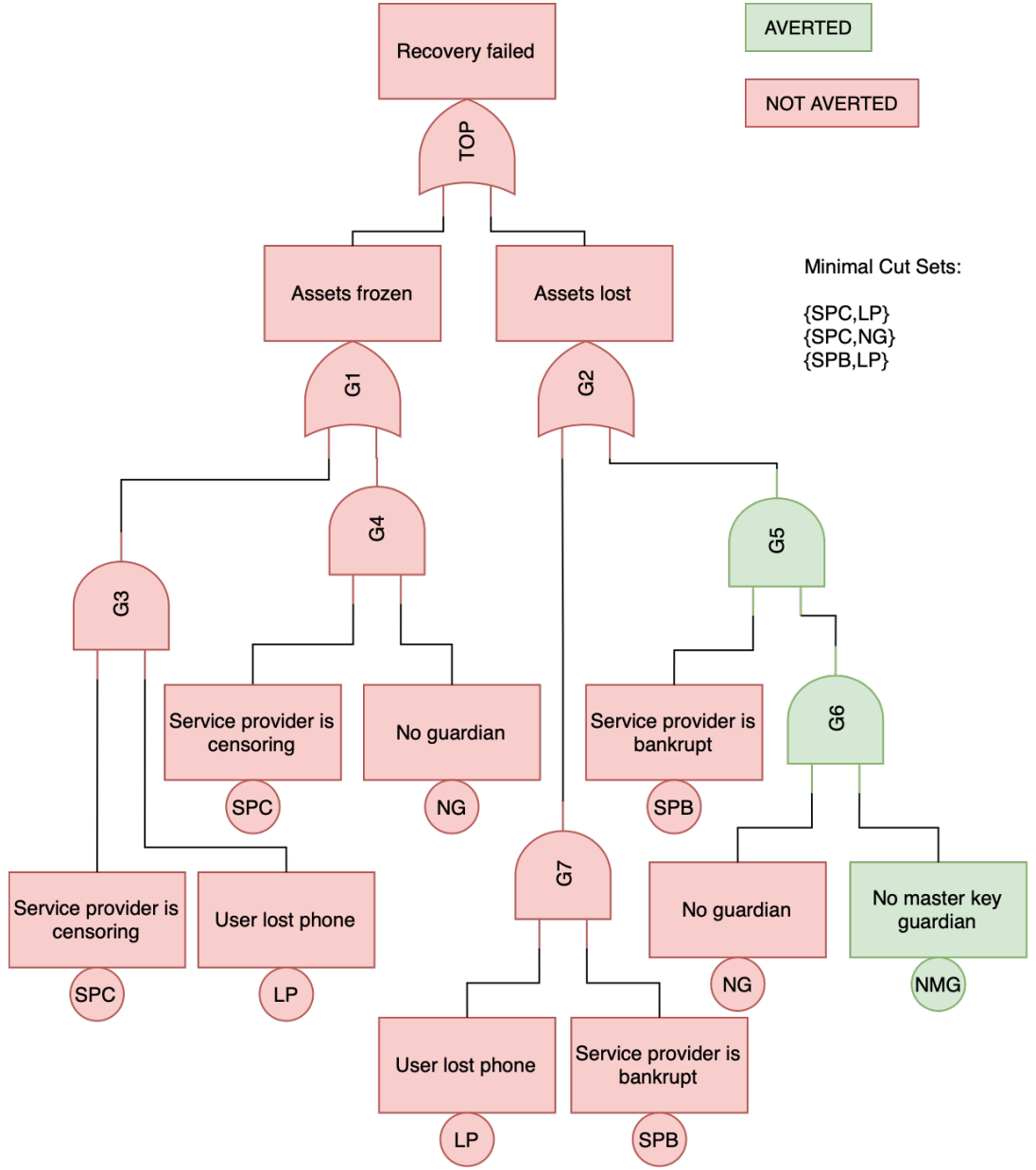
Signature scheme and recovery architecture – Example Zengo

zengo

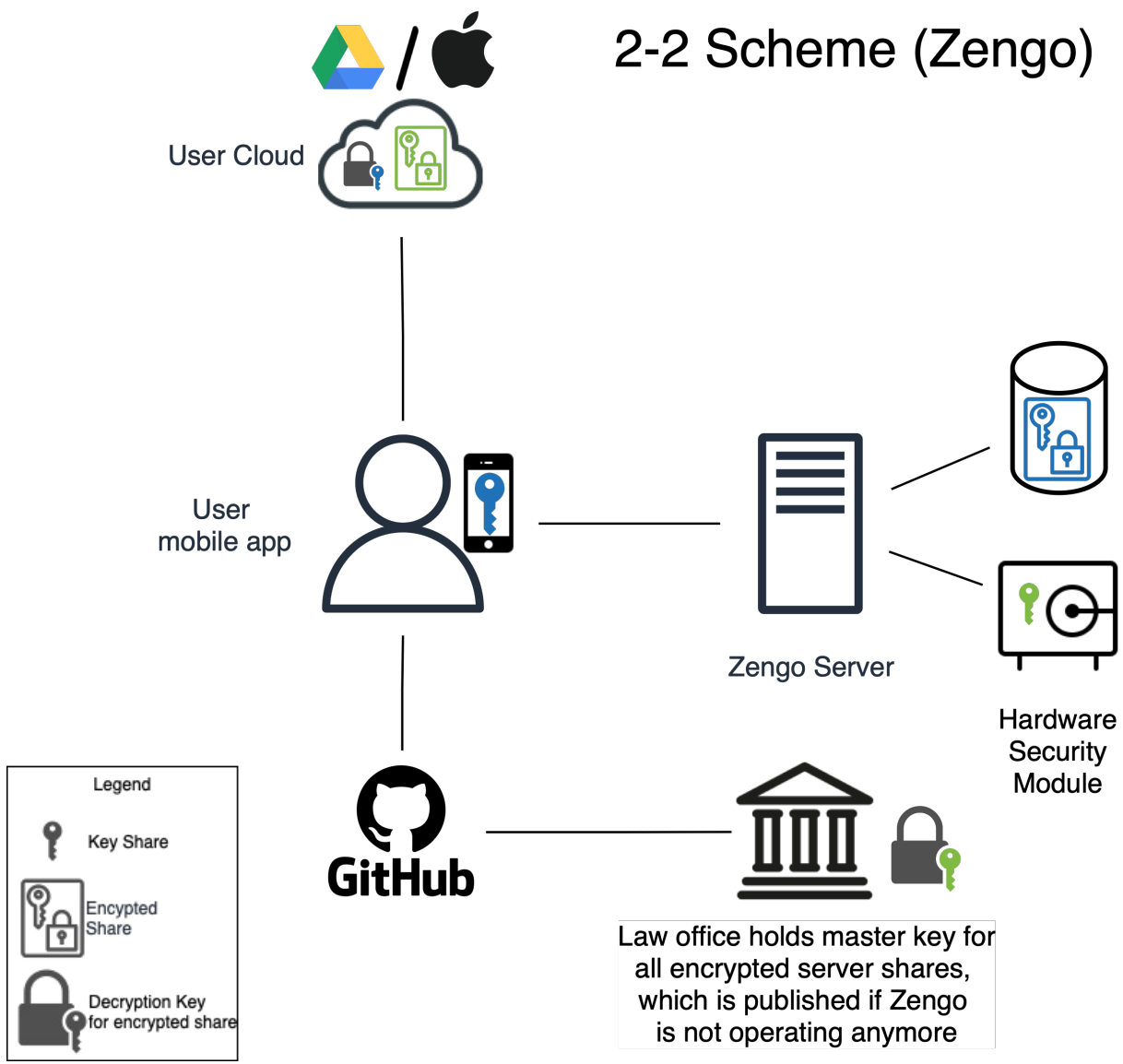


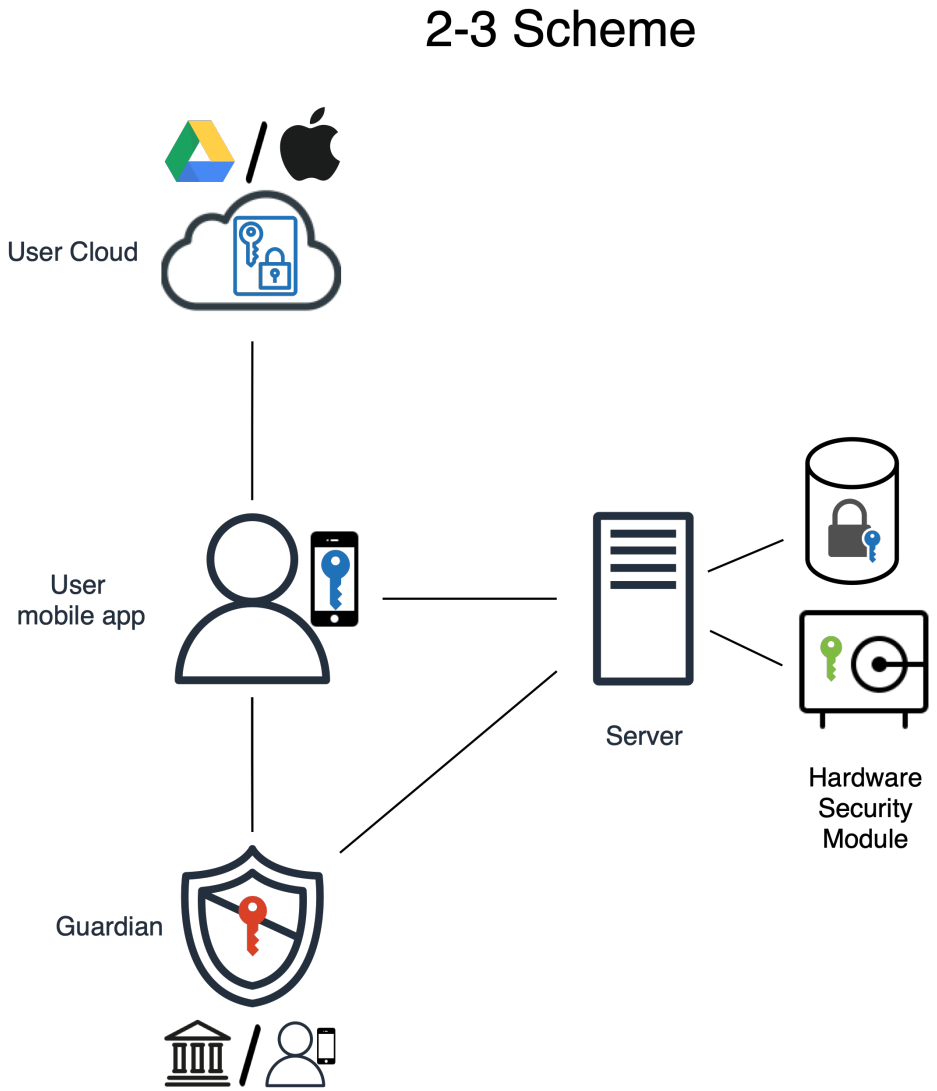
Signature scheme and recovery architecture – Zengo Fault Tree





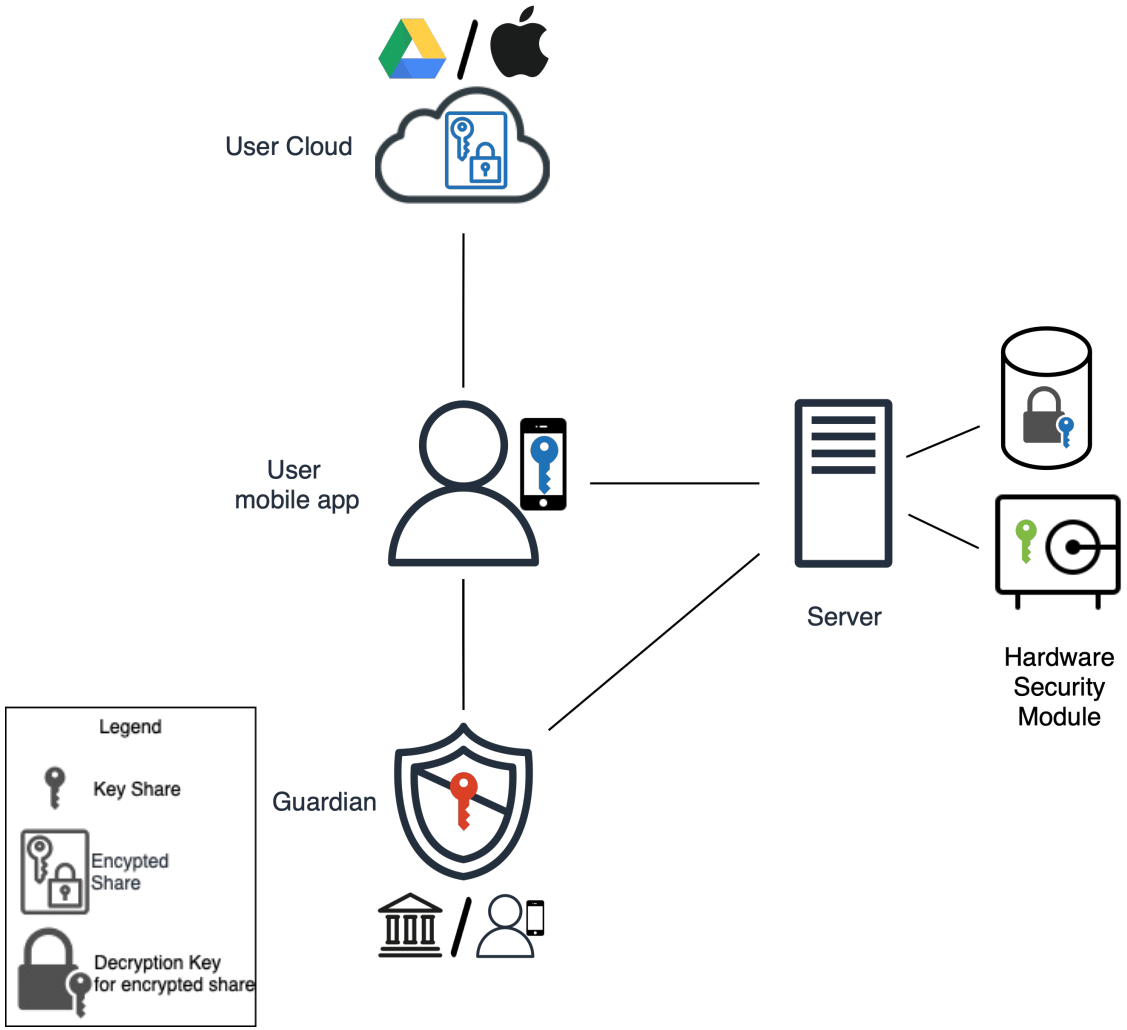
Signature scheme and recovery architecture – Zengo Fault Tree

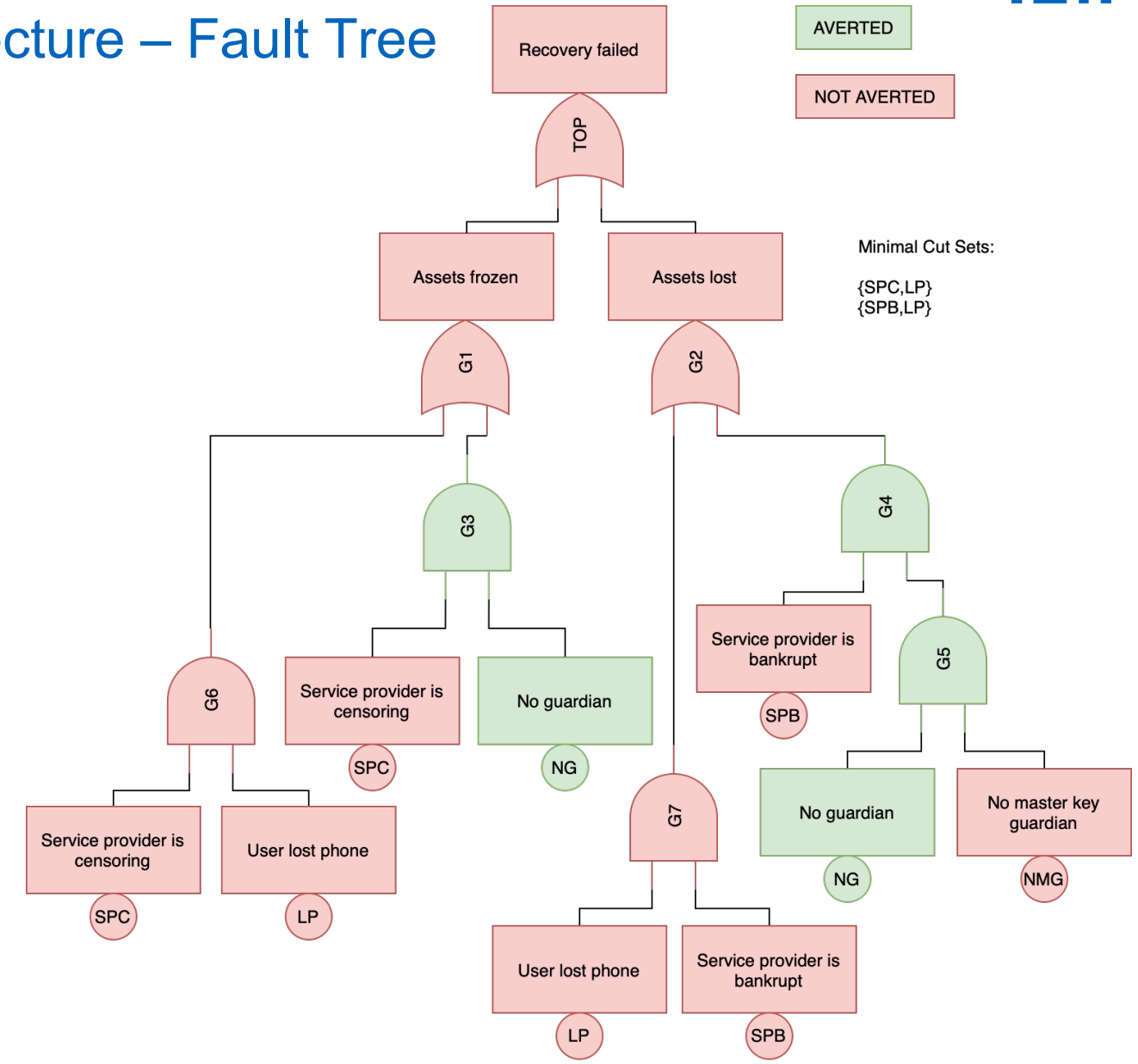




Signature scheme and recovery architecture – Fault Tree

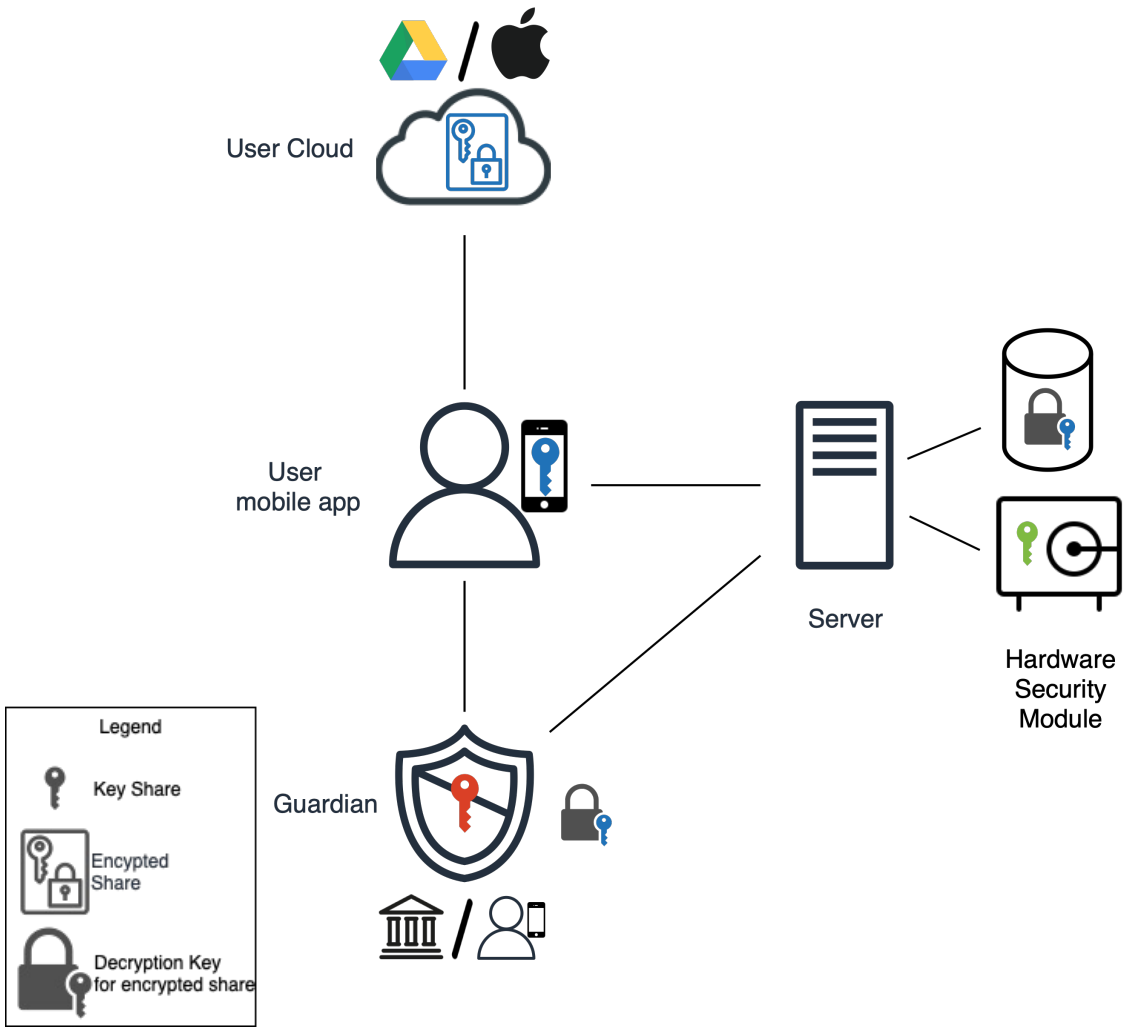
2-3 Scheme

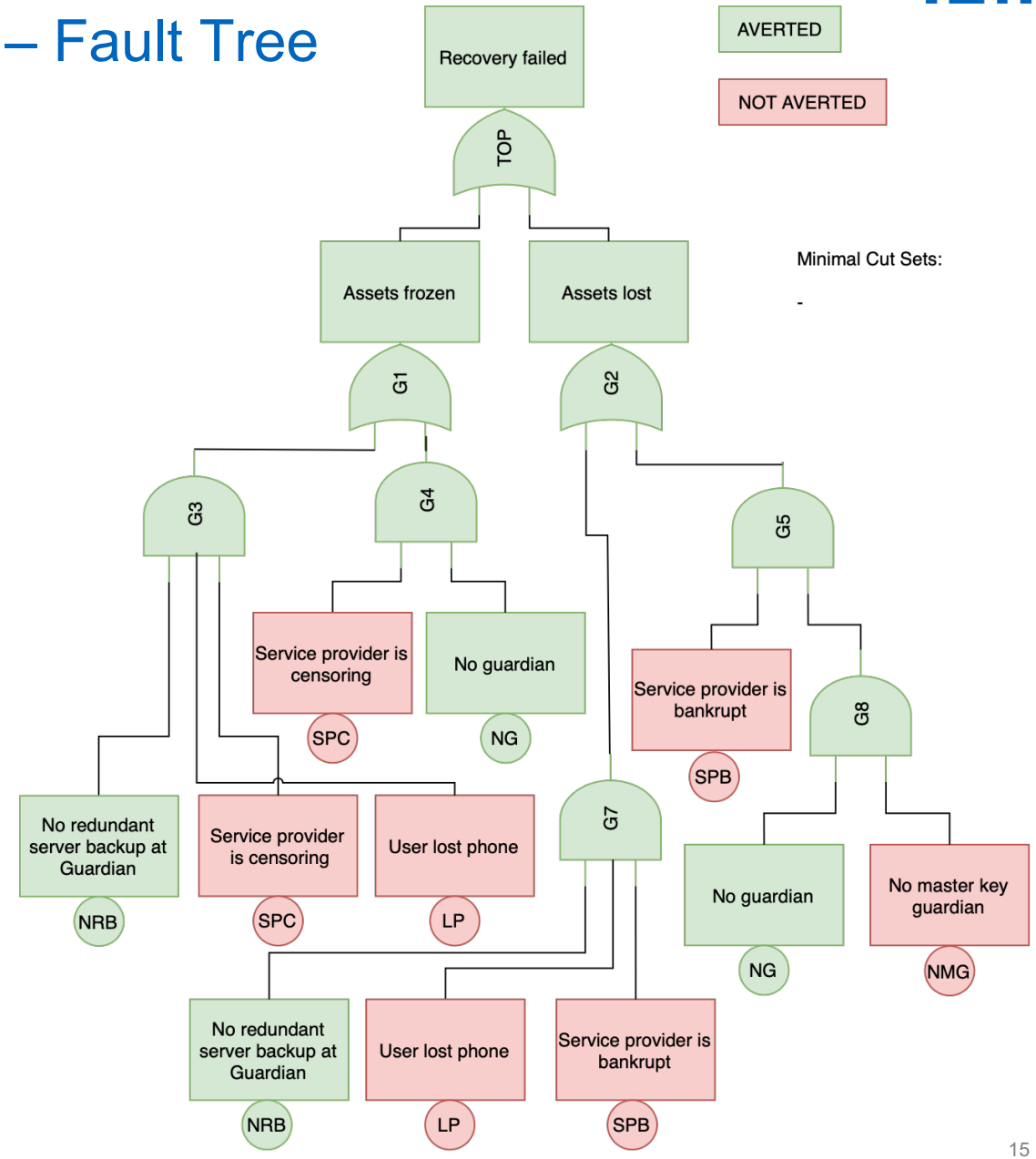




Signature scheme and recovery architecture – Fault Tree

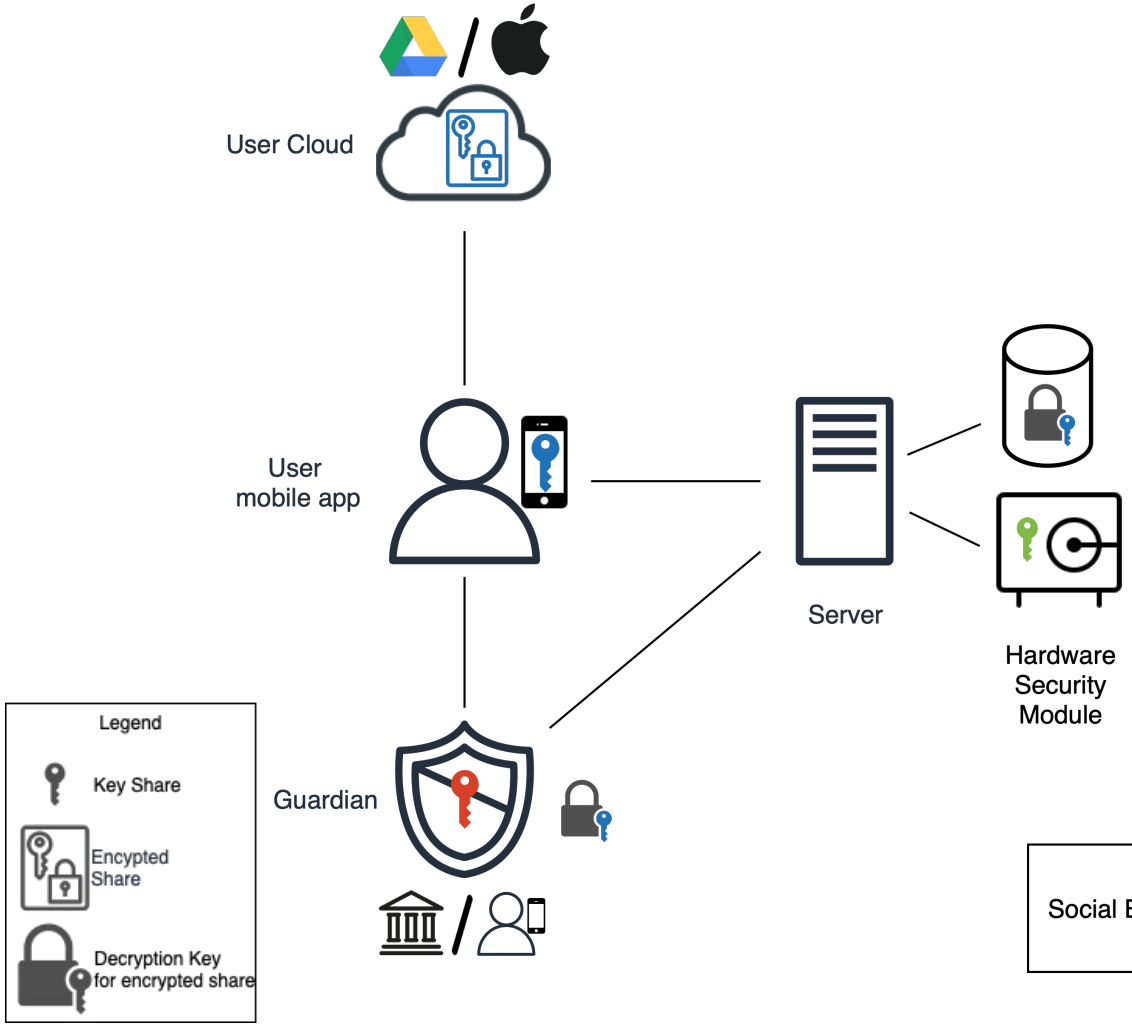
2-3 Scheme

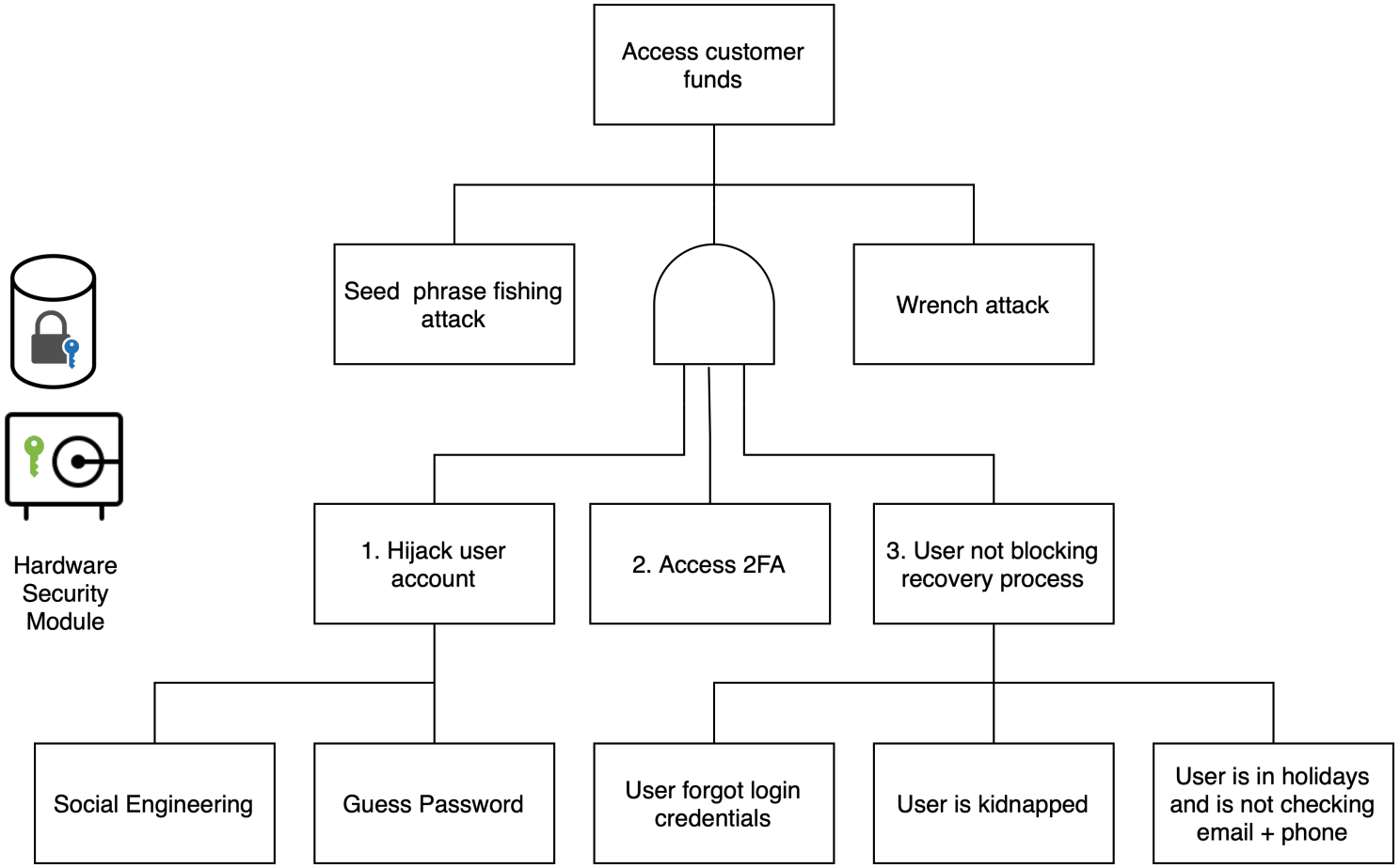




Signature scheme and recovery architecture – Attack Tree

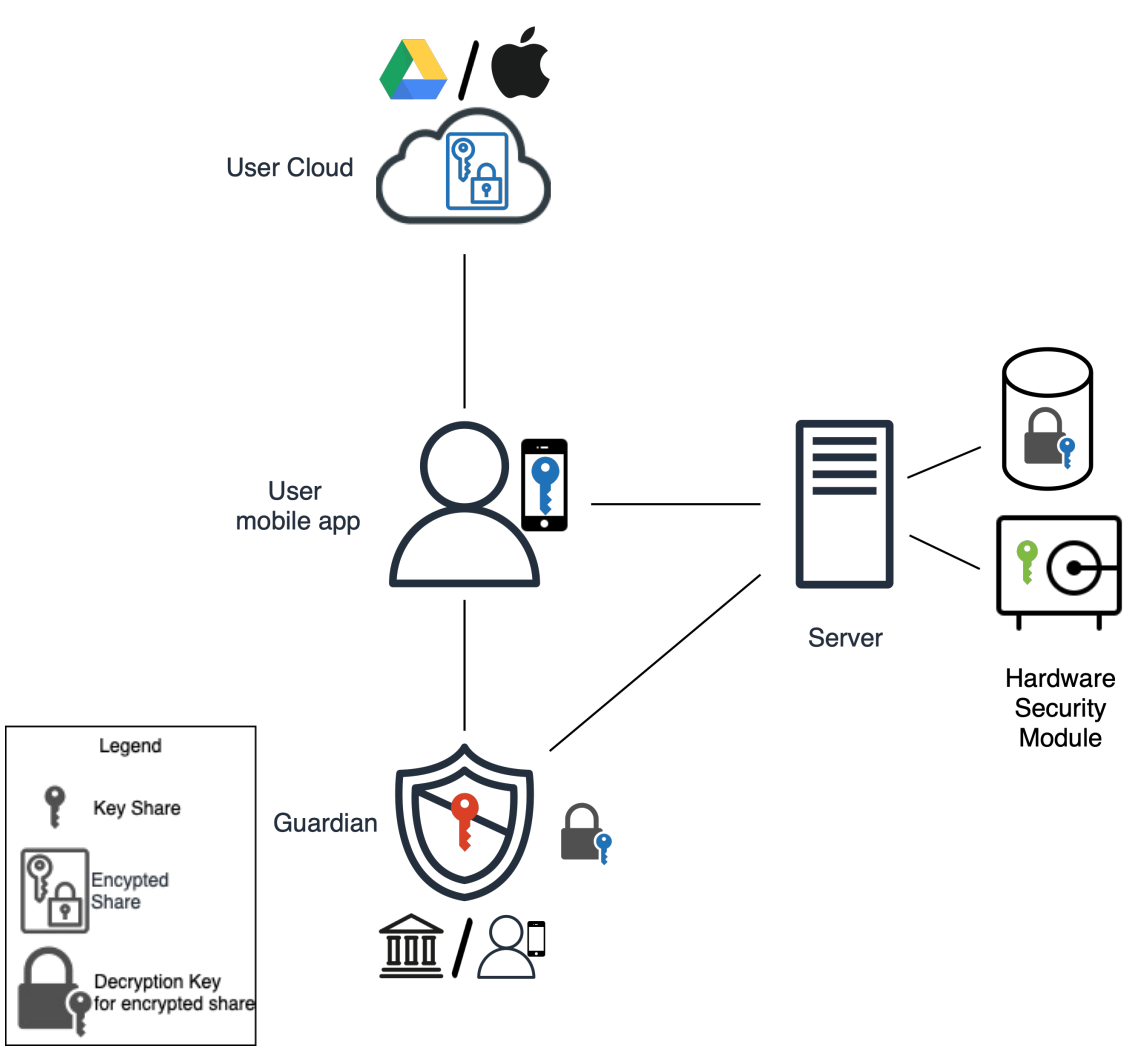
2-3 Scheme

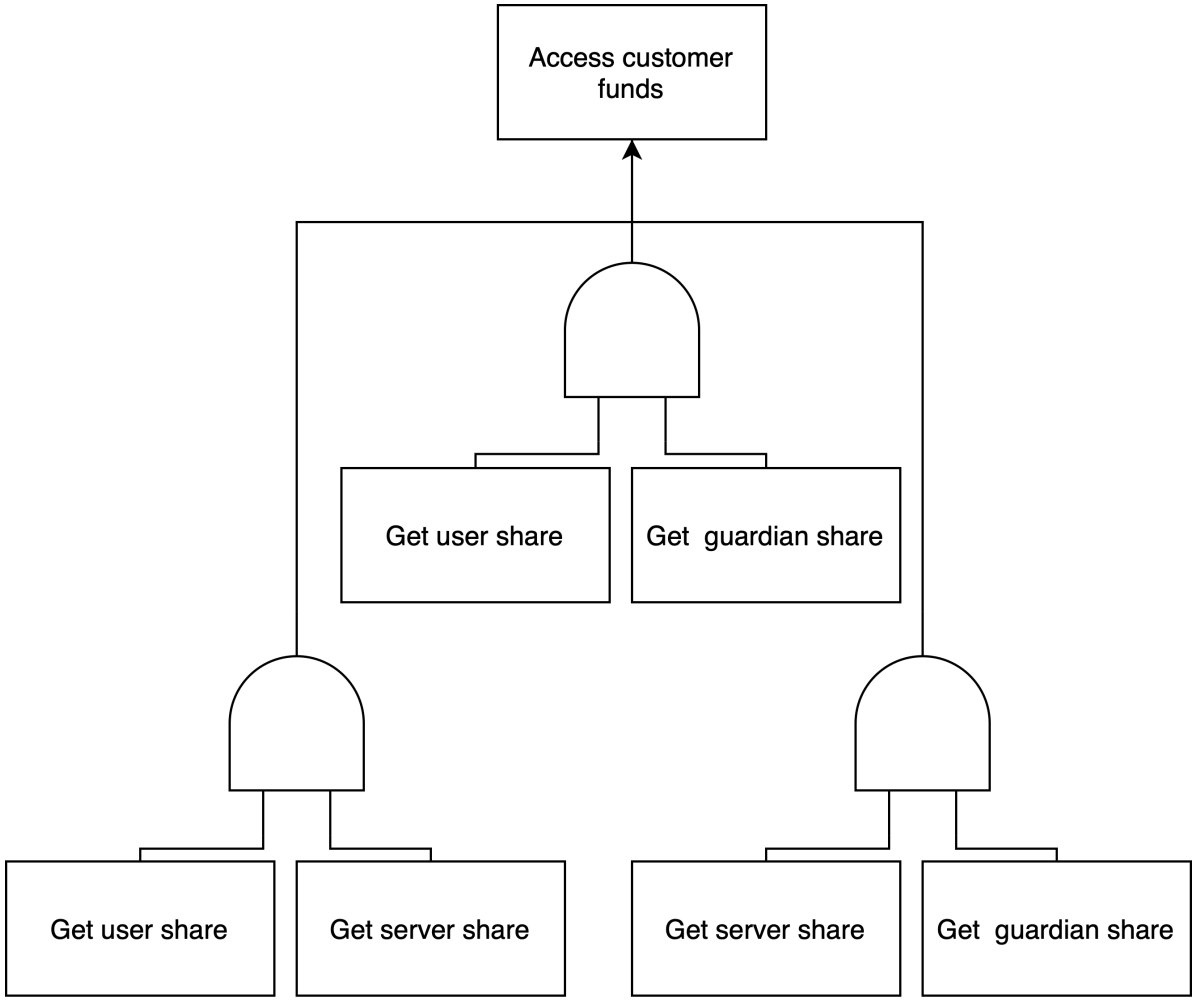




Signature scheme and recovery architecture – Attack Tree

2-3 Scheme





Outline

1. Motivation and Introduction
2. Problem Statement and Initial Findings
3. Research Questions & Methodology
4. Timeline & Current Status

Research Questions

RQ 1

How can inherent security and usability challenges in crypto wallets be technologically addressed and what design requirements, principles and features emerge for enhancing wallet solutions?

a) What challenges in digital asset management and transaction security are addressed by Multi-Party Computation (MPC) and Account Abstraction technologies?

→ Recoverability, Seed phrase vulnerability, MEV, …

b) How can we leverage MPC techniques to implement new features in crypto wallets, such as recoverability, transaction limits or inheritance of assets, while maintaining security and useability?

→ Initial Design Requirements, Principles and Features

Methodology:

a)

- Extensive literature research
- Analysis of non-custodial and custodial, MPC and AA solutions

b)

- Definition of design requirements that serve as meta requirements based on initial user interviews and survey (Walls et al. 1992)
- Development of design principles based on requirements and derivation of adequate design features to instantiate the principles inrecovery architecture and UX design prototypes

Research Questions

RQ 2

How can the application of Multi-Party Computation (MPC) in non-custodial mobile cryptocurrency wallets improve their security and user experience, thus enabling mass adoption of digital assets?

a) How do different recovery mechanisms and their associated threshold signature schemes (2-2 and 2-3) affect the security and user experience?

▶ Recovery mechanism architectures, Fault & Attack Trees, UI/UX designs

b) How is the security and user experience perceived compared to other non-custodial and custodial solutions

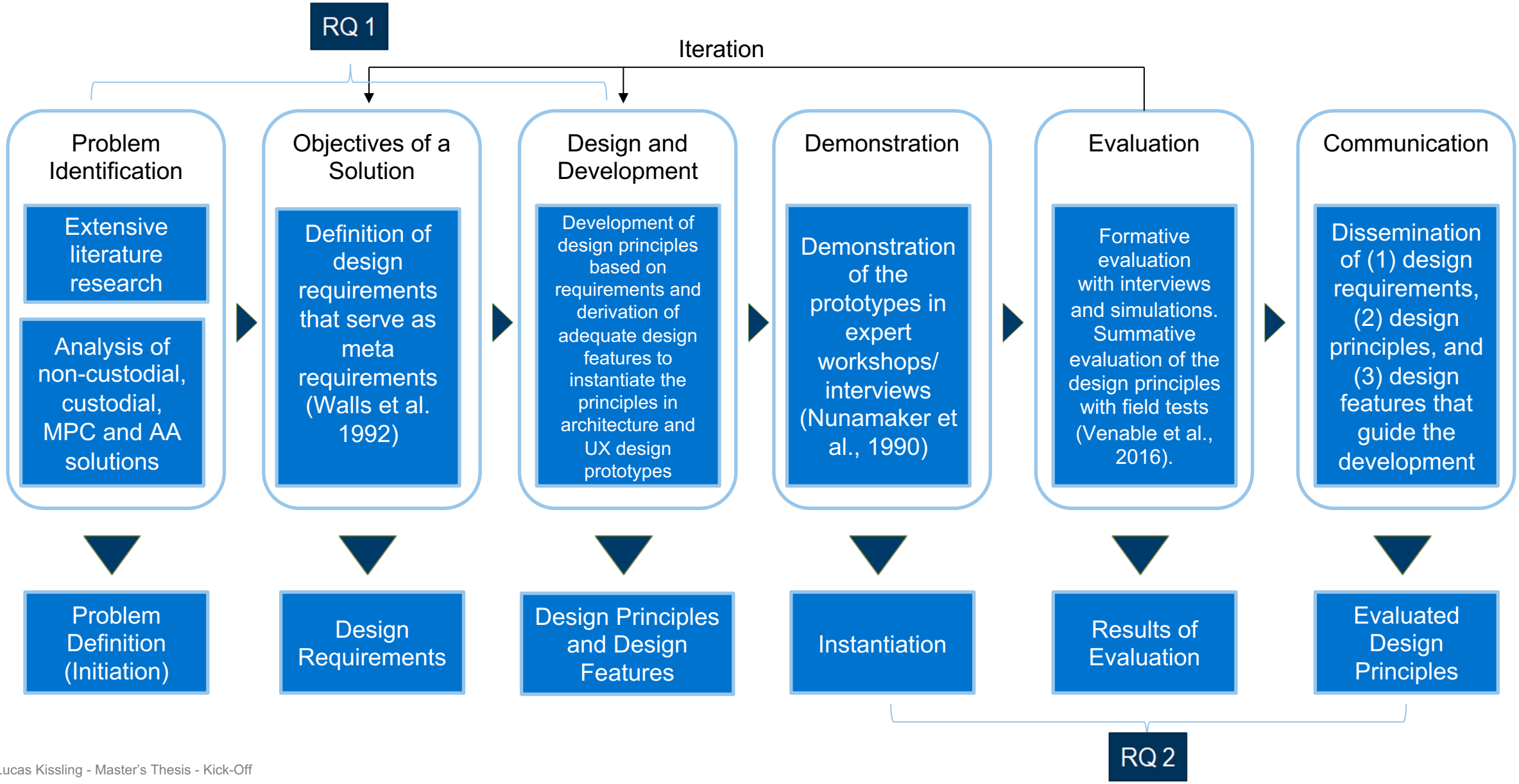
▶ Taxonomy

Methodology:

Demonstration of the prototypes in expert workshops/ interviews (Nunamaker et al., 1990)

Formative evaluation with interviews and simulations. Summative evaluation of the design principles with field tests (Venable et al., 2016).

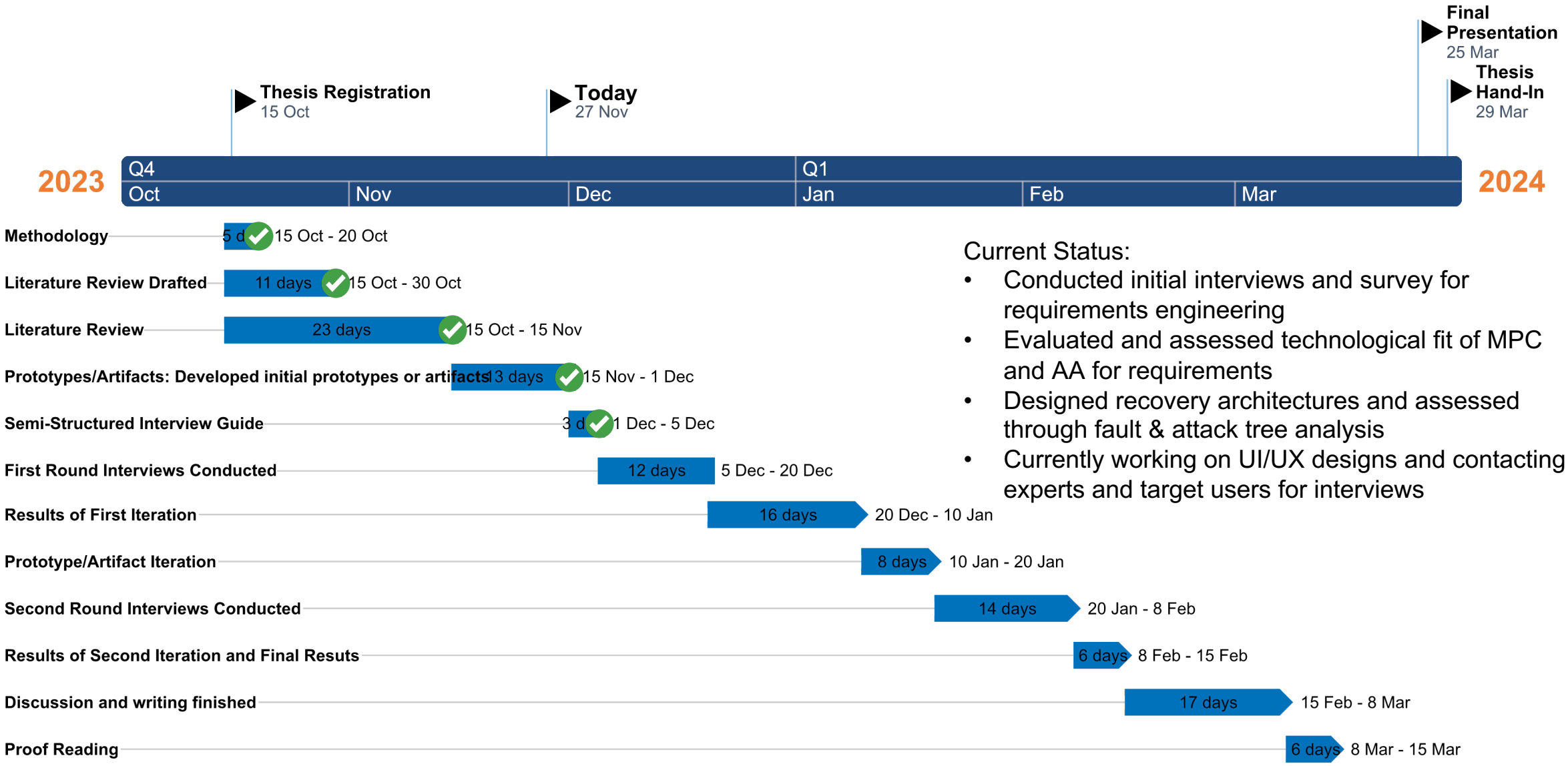
Design Science Research Approach based on Peffers et al.



Outline

1. Motivation and Introduction
2. Problem Statement and Initial Findings
3. Research Questions & Methodology
4. Timeline & Current Status

Timeline



Current Status:

- Conducted initial interviews and survey for requirements engineering
- Evaluated and assessed technological fit of MPC and AA for requirements
- Designed recovery architectures and assessed through fault & attack tree analysis
- Currently working on UI/UX designs and contacting experts and target users for interviews

Lucas Kissling
lucas.kissling@tum.de

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de