Towards Usable Blockchain Interfaces –

Interaction Concepts for Key Management

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Problem Statement

Public key cryptography is a concept frequently used in computer science – however recent increase in popularity of blockchain systems (e.g. Bitcoin, Ethereum) now requires users outside of this domain to deal with private/ public key cryptography.

The goal of this thesis is to look at public key cryptography from an HCI perspective and analyze interaction concepts for key management. How do (end-) users interact with blockchain systems? How do they deal with the challenges of public key cryptography? And which novel interaction concepts – building on existing work – can be developed to reduce complexity of key management?

Tasks

- Review of related literature
- Analyze existing strategies for key management
- Design and conduct user study
- Develop and evaluate an (improved) concept for key management

Preferred Qualifications

- Knowledge in the area of human computer interaction
- Independent thinking and creative problem solving
- Interest in designing and conducting user studies
- Web Development Experience (optional)
- Interest in crypto currencies (optional)

Related Work

https://dl.acm.org/citation.cfm?id=1251435
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7031848
https://www.usenix.org/system/files/conference/soups2018/soups2018-ruoti.pdf
https://arxiv.org/abs/1802.04351
https://www.scitepress.org/Papers/2017/62700/62700.pdf