Towards Usable Blockchain Interfaces –

Understanding Seed Phrase Storage in Practice

Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Problem Statement

An increasingly popular method to generate private/ public key pairs for cryptocurrency wallets is Hierarchical Deterministic Key Generation based on a series of random words. These words (mnemonics) can be stored and subsequently used to (re-)generate the original private key file, in case it is lost.

The goal of this thesis is to analyze how users actually store these phrases in practice, to look at the benefits and drawback of different strategies and ultimately develop a new concept for improved handling of mnemonics.

Tasks

- Review of related literature
- Analyze key phrase/ mnemonics storage strategies in practice
    - Online Research
    - User Interviews
- Design a user study to systematically compare the different strategies
- Develop and evaluate a concept to improve upon existing strategies

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://github.com/bitcoin/bips
https://ieeexplore.ieee.org/abstract/document/7966967
https://link.springer.com/chapter/10.1007/978-3-662-47854-7_31

https://www.reddit.com/r/Bitcoin/comments/58zst0/how_do_you_store_a_digital_backup_of_your_bip39/
https://bitcointalk.org/index.php?topic=3327310.80
https://blockchainjournal.news/how-to-store-a-mnemonic-seed-phrase-from-a-cryptocurrency-wallet/