Smartphone Cryptocurrency Wallet Scorecard

Justin Smith
Zcon0 2018, Montreal

This scorecard can be used to help perform a holistic review of the security, privacy, and usability of smartphone cryptocurrency wallets. In the ”Remarks and Score” column, apply a binary score (1 or 0) to each item, where ”1” means the item meets your expectations and ”0” means it does not.

Application Name:

Item	Description	Remarks and Score
Remote node	Can you connect to your own remote node to ensure you are on the correct chain, validate incoming transfers and broadcast signed transactions?	
Open source	Is the software MIT or GPL licensed open source and is the repository public?	
Ready to build	Following developer instructions, can you build the software yourself from the provided source code?	
Known developers	Do you know who the developers are, and can you verify their PGP keys?	
Documentation	Is there a formal specification? Is the documentation clear and up to date?	
Professional audit	Has a professional third party auditor inspected the code?	
Active project	How quickly are issues addressed, how many unique contributors are involved in the project, and how many commits are made each month?	
Key generation	Are keypairs generated on the hardware with the cryptocurrency’s native libraries?	
Access control	Is the PIN you use to access the application hashed and stored securely using keychain or a similar feature?	
Recovery	Is the seed mnemonic compatible with the reference client wallet?	
Multifactor access	Can you require the use two or more authentication factors to initiate outgoing transfers?	
Limited attack surface	Are there any third party integrations, such as exchange or brokerage features?	
System intrusion	Does the app request access to sensitive data, such as your contact list?	
Limiting user error through design	Is the user interface easy to understand, logical, and easy to use?	
Code quality and platform expertise	In what programming language is the wallet written?	
Special privacy features	Does the app offer any additional privacy features?	
Financing	How is software development financed; where does the money come from?	
Cumulative Score		