Segregated Wallet Provider SWP

Inventor
Djerroud Mohamed salah
djerroud.mohamed.salah@gmail.com
https://twitter.com/salah_djerroud

Co-inventor
Bekouche Sirajeddine
ets.sirajedine@gmail.com

Co-inventor
Abdou Hameur Lain
simplyabdou@gmail.com

Abstract. Bitcoin performs all the functions of neutral sound money but struggles with the medium of exchange functionality, an ideal value transfer system would handle any load of transaction per second. We propose a new frictionless centralized solution that we believe would solve the bitcoin scalability problem once and for all. It uses public-key cryptography. A public key provides identity, and a digital signature provides proof of ownership.

1. Introduction

Usually, public-key cryptography is associated with decentralized apps, but they could be used for centralized apps, public-key cryptography comes with built-in information security concepts. identification is ensured by the public key (public key acts as a user id). authentification and authorization and Non-repudiation are ensured by a digital signature, it is up to the centralized app provider to tell the user what needs to be signed, to ensure he owns the private key (a digital signature acts as a password), users don't need to register to the centralized app, and the centralize app provider doesn't have to store digital signatures.

In our case, a single signature bitcoin address act like the user id. Every SWP is identified by one single signature address. A user must sign the SWP deposit address as a message, the result is a signature that acts as a user password.

Example

- SWP deposit address
  bc1qcceqdgq90q5xnsm7pp3wzghnj8wxdy60cwwngl
- User address
  bc1q65ncnh04tva7jqx54j55n44j7qxmgftzsck8lx
- User signature
  H1BIlhXWo2i6CpnfWEw/BuItMJ0VzM/BH7NVfg8H/+KubAIOR9ZuVsqeGifDEUl MUEA/QagkB6e9VPl283vR8Ho=

2. Transactions

2.1. **Deposit transactions** happen on the blockchain, they are the most important transactions and must follow these rules to be interpreted by the SWP as a valid deposit transaction:

- All inputs are from the user same address.
- The first output is the SWP deposit address.
- Optional second output for the change must be the same as the input address therefore the user address.
  Once it hits the confirmation target set by the SWP, the deposited amount will be credited to the user address automatically on SWP servers.

2.2. **Inner transactions** happen on SWP servers. it is a simple database update operation.

2.3. **Withdraw transactions** happen on the blockchain, they will have these rules:

- All inputs are from the SWP deposit address.
- The first output is the user withdrawal address.
- Optional second output for the change must be the same as the input address therefore the SWP deposit address.

3. Conclusion

Wallet providers should start adding signing/verifying, single address, and coin control features. SWP may defer on many aspects. Legal, business, log, and limit structures. For legal structure, the SWP is either public (owned by the state there for no need for an SWP license, might have a state monopoly) or private (need an SWP license from the state). For business structure, the SWP is either nonprofit (feeless rely on donation by sending bitcoin to the SWP deposit address using an inner transaction) or for-profit by imposing a fee structure. For log structure, the SWP is either logless (does not log inner transaction data so the receiver doesn’t know the sending address but his balance would increase, plus the address will be deleted from SWP servers if its balance becomes zero) or logged (SWP might be required by the state to log inner transaction, plus the SWP might link a bitcoin address to a real-world identity). For limit structure, might be limitless or limited. The ideal SWP would be public or private, logless, nonprofit, and limitless.