Sia Foundation Preliminary Estimate Report

Table Of Contents

komodo

Adaptor Signature Atomic Swap

Roadmap

- Develop a Rust FFI library written in Go for transaction signing within mm2.
- Interface mm2 with Sia's public RPC servers for lite client functionality.
- Implement ed25519 key generation and handling from your HD wallets.
- Design and develop a more generalized swap protocol mechanism.
- Implement the proposed protocol based on the provided Rust PoC.

Obstacles

- Complex and Novel Cryptography - Advanced developers and cryptographer needed to ensure proper implementation
- Compatibility with existing pairs in mm2 - Adaptor signature atomic swap scheme compatibility would need to be made with existing coins, adding additional work to develop a practical implementation
-

Adaptor Signature Atomic Swap

Preliminary Cost Estimate

Estimated Personnel

- 4 FT Sr. Developers
- 2 FT Jr. Developers
- Cryptographer
- Assorted Support Personnel (Testers, Designers, etc. as needed)

- Estimated Cost: $1-2 Million USD

  * Scope of Work phase needed to give more accurate estimate on cost and personnel needed to complete

Preliminary Time Estimate

- Estimated Time Needed: ~ 2 years
- ~1-1.5 years for protocol implementation
- ~ 6months - 1 year for full Komodo Defi Framework integration post protocol implementation

  * Scope of Work phase needed to give more accurate estimate of time needed to complete

Note: Estimations will cover SoW, Dev & QA

Custom Signature Scheme Soft Fork

Roadmap

- Collaborate with the Sia team to implement a new "UnlockConditions" scheme to emulate HLTCs.
- Develop a Rust FFI library written in Go for transaction signing within mm2.
- Interface mm2 with Sia's public RPC servers for lite client functionality.
- Implement ed25519 key generation and handling from your HD wallets.
- Research and identify any missing RPC methods required for mm2 and implement them in the Sia RPC server.
- Develop a new implementation of the MmCoin and MarketCoinOps traits.

Obstacles

- UnlockConditions will eventually be replaced with SpendPolicy
- Possible coordination issues with Soft Fork

Custom Signature Scheme Soft Fork

Preliminary Cost Estimate

- Preliminary cost estimate: ~ $100-150k
- Estimated Personnel Needed:
- 2 Sr. Developers
- Assorted Support Personnel (Testers, Designers, etc. as needed)

* Scope of Work phase needed to give more accurate estimate of cost and personnel needed to complete

Preliminary Time Estimate

- Estimated Time to Complete: ~ 6-12 months

* Scope of Work phase needed to give more accurate estimate of time needed to complete

- Note: Estimations will cover SoW, Dev & QA

Introducing Spend Policies to Emulate HLTC Behavior

Roadmap

- Collaborate with the Sia team on the "Spend Policy" update.
- Develop a Rust FFI library written in Go for transaction signing within mm2.
- Interface mm2 with Sia's public RPC servers for lite client functionality.
- Implement ed25519 key generation and handling from your HD wallets.
- Research and identify any missing RPC methods required for mm2 and implement them in the Sia RPC server.
- Develop a new implementation of the MmCoin and MarketCoinOps traits.

Obstacles

- Unknown when “SpendPolicy” will be officially live
- Unknown what stage of development or of testing environments for “SpendPolicy”

Introducing Spend Policies to Emulate HLTC Behavior

Preliminary Cost Estimate

- .Preliminary cost estimate: ~ $75-100k
- Estimated Personnel Needed:
- 2 Sr. Developers
- Assorted Support Personnel (Testers, Designers, etc. as needed)
- * Scope of Work phase needed to give more accurate estimate of cost and personnel needed to complete

Preliminary Time Estimate

- Estimated Time to Complete: ~ 6-12 months
- * Scope of Work phase needed to give more accurate estimate of time needed to complete
- Note: Estimations will cover SoW, Dev & QA

Sia Atomic Swaps in Komodo Wallet

All the following options include integration into Komodo Platform's flagship application, Komodo Wallet and its built-in decentralized exchange, 'Atomicdex'.

Integration into the Komodo Wallet, provides Sia users with a secure way of self-custody of Sia and many other cryptocurrency, on desktop, mobile, web and browser extension (soon).

Thank you for the opportunity to investigate how best to incorporate atomic swap technology into Sia. We hope to connect Sia with the rest of the crypto ecosystem soon!