HTLC Upgrade for Sia for use in Atomic Swaps

Scope of Work

Background

The Sia Foundation is funding a grant allowing the Komodo team to integrate the cryptocurrency, SIA, into Komodo Wallet. This integration will enable Sia users to engage in trustless peer-to-peer atomic swaps with the extensive range of cryptocurrencies that are currently supported by the wallet, as well as any that may be supported in the future. Sia users will also have access to a fully functioning web wallet and mobile wallet. The Sia team will be provided all the necessary source code and documentation to enable the team to host their own version of wallet if they so choose.

Document Objective

The purpose of this document is to guide API development efforts while providing a blueprint for GUI developers and UX designers. It offers a detailed breakdown of the problems at hand, proposed solutions, potential complications and affected functionalities. The document is designed to facilitate the parallel workflows of both the Komodo and Sia development teams. The document will also allow the Komodo GUI developers and UX designers to conceptualize how these features will be presented while development is underway.

1. **Problem Identification:** Details the specific issue needing resolution.
2. **Solution Proposal:** Describes the suggested approach to tackle the identified problem.
3. **UX Design Considerations:** Discusses potential user interface and experience design opportunities and challenges relating to the proposed solution.
4. **Potential Complications:** Anticipates potential obstacles or drawbacks that might emerge from the proposed solution.
5. **QA Considerations:** Discuss how the solution will require new scopes of testing (if applicable)
6. **Technical Details:** Provides technical specifics of the proposed solution.
7. **System Impact:** Identifies what existing parts of the system may be impacted by the proposed solution.
8. **Future Vision:** Envisions the optimal solution considering practical constraints.

Stakeholders

This document will have certain portions directed towards the different parties involved, including:

- The Komodo API team
- The Komodo GUI team
- The Komodo UX / Design team
- The Komodo QA team
- The Sia development team (or “Sia team”)

Objectives

1. Integrate SIA wallet functionality into Komodo Wallet API.
2. Integrate peer-to-peer trading based on Sia's new v2 consensus protocols.
3. Publish all relevant source code and documentation.
4. Integrate SIA into Komodo Wallet GUIs including the web app and mobile apps

Scope

In-Scope

- SIA support within Komodo Wallet including wallet functionalities and peer-to-peer trading functionalities.
- Peer-to-peer SIA trading support for at least “BTC-like” coins and “EVM-based” coins and tokens. All reasonable efforts will be made to support as many coin protocols as possible.
- All code and relevant documentation published publicly under a GPLv2 license.
- Support and training for Sia Foundation team members prior to and during the “App Release” phase.

Out-of-Scope

- Intentional support for SiaFunds wallet or trading functionalities.
- Ongoing infrastructure hosting and maintenance of the “Sia lite wallet API”
- Team training and support beyond the “App Release” phase.

SIA support will remain within Komodo Wallet indefinitely assuming the following conditions:

- Any impactful SIA consensus model updates are communicated to the Komodo team with an appropriate amount of lead time.
- An appropriate public API endpoint is provided and well maintained to facilitate “lite wallet” functionality within Komodo Wallet.
- Unforeseen shifts in Komodo's business models or technical strategies. The Komodo team will not make any efforts targeting the particular removal of the SIA coin from Komodo Wallet.

As stated in the grant proposal, the Komodo team has proposed 4 unique phases of this grant process each differentiated by a distinct deliverable milestone.

Breakdown

Phase 1: Scope of Work

The purpose of this phase is to determine the exact work needed to complete each phase of the grant. This document is aimed at providing both the Komodo and the Sia development teams a clear breakdown and delegation of tasks. The document aims to facilitate the parallel workflows of the various stakeholders.

Beyond the writing of this document, this phase will be used to research and evaluate the current state of Sia’s codebase. The Komodo team has identified development tasks required of the Sia team that have potential to stall the Komodo team’s development efforts.

This phase will be concluded with the delivery of this document.

Phase 2: Development Phase

This phase will last 30-32 weeks, and it will include several concurrent tasks required from the API team and Sia team.

The foundational development work will occur during this phase. This will include the creation of the interface between Komodo Wallet API and Sia’s API and the integration of standard wallet functionality.

The API the Komodo team intends to use for fetching user blockchain data is not fully developed. Therefore this phase in particular will require a high degree of interaction and cooperation between the API team and the Sia team.

It must be noted that the timeline set out for this phase assumes no major changes are required to Sia's newly introduced consensus mechanisms and no major changes will be made to the proposed walletd API schema.

A summary of all ongoing and finished development tasks will be published at the conclusion of this phase. A proof of concept demonstration will be provided alongside this report.

Phase 3: QA Testing and Security Hardening

This phase will last 3-4 weeks. This phase can overlap the end of the previous phase at the discretion of the API team. During this phase, the QA team will be responsible for testing the full user interface. The API team will be responsible for finalizing user and developer documentation during this period.

The Sia team and community are encouraged to begin testing and providing feedback during this phase.

Phase 4: Release Candidate

This phase will last for the remaining time of the grant's overall 8-10 month time estimate. This phase will consist of polishing and finalizing all tasks across all relevant teams.

The rollout of SIA's new consensus model may act as a roadblock for the release of SIA support within Komodo Wallet. The Komodo team will proceed on the assumption that the "v2" activation will happen within the 8-10 month timeline of this grant.

Implementation

The following will detail various technical details and tasks.

Development Environment and Testnet

Problem Identification: A test suite will be required by the API team. This will require a mocked version of the proposed walletd API schema. This requires documentation of how to establish a personal testnet or a private testnet to be shared amongst the development teams. This testnet should provide a nearly identical API to that of the eventual mainnet implementation of Sia's walletd.

Solution Proposal: The API team will produce documentation of how to establish a "regtest"-like network. This type of testnet will provide temporary networks(or mocked networks) used

exclusively for manual testing, unit tests and integration tests within the Komodo DeFi Framework API. These networks will be established within temporary Docker containers.

Additionally, a persistent private test network will be established. This network will also be used for manual testing, unit tests and integration tests. This network will be useful for long term test cases and contribute to the ease of use for the UX/UI and design teams. The API team will be responsible for maintaining a functional private testnet to be available for all relevant parties.

UX Design Considerations: N/A

Potential Complications: All parties relying on the persistent testnet must understand that the blockchain itself may be subject to rapid restarts and new genesis blocks as the Sia team continues to develop their blockchain node software and consensus model.

This persistent testnet will eventually be accessible to the public. No confidential or potentially harmful testing should be executed on this network.

QA Considerations: The API team should provide a familiar experience to the QA team in regards to unit and integration tests. The API team can accomplish this by analyzing existing tests throughout the Komodo DeFi Framework codebase and following similar patterns.

Technical Details: The API team will create a fork of Sia's node software making minimal edits to facilitate these testnets. Technical changes must be made to the already existing "Anagami" testnet. The proof of work required to create blocks must be minimal. An API endpoint must be created to allow progressing the blockchain by an arbitrary amount of blocks. The hardfork activation heights for consensus changes must be lowered to activate shortly after the creation of the network.

System Impact: The changes involved here require various placeholders or "stubs" to be created throughout the Komodo DeFi Framework codebase. These stubs will provide a way of activating the test coin within the API while most of the functionality is still in active development.

Future Vision: The persistent testnet can be deprecated when a stable public testnet is provided by the Sia team.

Test Coin Activation

Problem Identification: A test coin utilizing the aforementioned placeholder implementation is required.
Solution Proposal: Using the aforementioned persistent testnet, a test coin implementation will be created by the API team. This coin will act in a similar fashion to the existing test coins such as DOC, MARTY and ZOMBIE. Initially, the test coin will have little or no functionality beyond the ability to activate it.

UX Design Considerations: The UX team must create a name, ticker and placeholder icon for this test coin.
Potential Complications: The process of adding this test coin to the API requires close coordination between the API team and the UX/UI teams. Initially, this coin will serve very little purpose to the QA team as much of the functionality of a typical coin will not exist at its inception.
QA Considerations: This test coin (or similar copies of it) will be the basis for nearly all manual testing performed by the QA team. It is crucially important for the QA team to communicate any additional needs or pain points to the API team while utilizing this test coin.

Technical Details: The initial iteration of this test coin implementation will have extensive use of the unimplemented!() and todo!() macros in rust. These macros act as a way of instructing the compiler to ignore certain code requirements. If a tester or user triggers a code path leading to one of these macros, it will intentionally trigger a panic.

System Impact: End users must not be able to trigger any unimplemented!() or todo!() statements. Any such use of these macros should be conditionally compiled when merged into the Komodo DeFi Framework's development branch.
Future Vision: This test coin implementation acts as the foundation for the real SIA coin implementation. As development progresses, this implementation will make a gradual transition from an initial test framework to the fully finished Sia coin implementation.

Sia Consensus Model Testing

Problem Identification: The Sia team has introduced new mechanisms to their consensus model to facilitate HTLC-like transactions. These HTLC-like features are untested.

Solution Proposal: These newly introduced mechanisms must be fully vetted by the API team. Any potential need for changes to these mechanisms must be immediately identified and communicated to the Sia team. It's important to give this feedback to the Sia team immediately, ensuring there's enough time for necessary adjustments, remediation, and further testing.

UX Design Considerations: N/A

Potential Complications: Close cross-team coordination is required to ensure the overall security and safe implementation of these new mechanisms. It is the shared responsibility of all parties to ensure these on-chain consensus mechanisms cannot result in the loss of user funds.

QA Considerations: The QA team must create a series of tests implementing the standard usage of these new consensus mechanisms.

Technical Details: The newly introduced “Spend Policy” mechanism introduces the ability to emulate a traditional HTLC-like atomic swap. This is accomplished with a series of individual Spend Policies such as “PolicyTypeAfter”, “PolicyTypeAbove”, “PolicyTypePublicKey” and “PolicyTypeThreshold”. Each of these individual policies must be tested to ensure they work as expected and suit the needs of the API team.

These policies must also be tested in conjunction with each other ensuring that they are sufficient to support peer-to-peer HTLC-like atomic swaps.

System Impact: A mistake introduced into either the consensus mechanisms themselves or the implementation of these mechanisms for usage in peer-to-peer atomic swaps could result in reputational damage for both development teams.

Future Vision: The API team will assess whether advanced features such as the “trading protocol upgrade”, “watcher nodes” or block header validation would require any further changes to SIA’s consensus model. The API team will advise the Sia team on potential “future proofing” of their consensus mechanisms.

Informational Wallet Functionality

Problem Identification: Sia’s walletd API stands out within the cryptocurrency industry due to its original development from foundational principles, without deriving from or forking a previous blockchain project such as Bitcoin or Ethereum. The API team must develop an interface between the Komodo DeFi Framework and the SIA blockchain to enable basic wallet functionality such as generating an address, receiving coins to an address, checking the balance of an address and checking the confirmations of transactions. These features do not require any cryptographic functions.

Solution Proposal: An interface between Sia’s walletd software and the Komodo DeFi Framework must be developed. Initially this interface will serve as a way of requesting data from the SIA blockchain. This interface will be further developed to enable interactive functionalities, broadcasting data to the SIA blockchain, in later tasks.

UX Design Considerations: At this point in development, the user experience should appear essentially no different than any other coin or token within the Komodo DeFi Framework. The UX should be familiar to both users and developers.

Potential Complications: Sia’s walletd API is in active development. The API team is currently waiting on the release of walletd’s “index mode” from the Sia team. This may act as a blocking item for the API team. The walletd API is similar to that of other cryptocurrencies APIs currently

implemented within the Komodo DeFi Framework. However, Sia's unique functionality surrounding file hosting contracts must be accounted for in wallet transaction history.

QA Considerations: The QA team can begin to run any relevant tests from their typical suite of manual tests. At this point in the development, the aforementioned testcoin will support features such as balance checking and transaction history.

Technical Details: Sia's walletd API is a REST API enabling all typical functionality of a blockchain node. In the case of a remotely hosted instance, SSL will be required from the server. For locally hosted personal instances, password authentication is enabled. The authentication details for the server must be provided within the equivalent of the enable method typical of other coin implementations.

System Impact: This interface will serve as the foundational interaction between the Komodo and Sia teams and their respective codebases. Any changes to this interface in the midst of the development cycle will have rippling effects throughout all teams.

Future Vision: The interface should be developed in an extensible fashion to enable any potential future cooperative developments between the Komodo and Sia teams. This interface should at least be minimally aware or easily adapted to be aware of Sia's unique consensus functionality regarding file hosting contracts.

Sia Rust Library

Problem Identification: Sia's codebase is written in Go for the backend server and Typescript and Go for the user interfaces. There are no other implementations of the Sia blockchain consensus model. Integrating into the Komodo DeFi Framework necessitates capabilities for creating, signing and validating transactions. Additionally, Sia's seed phrase derivation algorithm must be adapted to work within the Komodo DeFi Framework or the HD wallet functionality of the Komodo DeFi Framework must be adapted to work with Sia addresses.

Solution Proposal: Komodo DeFi Framework is written in the Rust programming language. The API team will create a Rust library to allow creating, signing and validating transactions as well as the handling of SIA's ed25519 private keys.

UX Design Considerations: N/A

Potential Complications: A full port to Rust of the Sia consensus model is not a feasible task within the given timelines. Therefore, the minimum work needed to facilitate atomic swaps should be committed to this Rust library. Careful consideration must be taken while determining what this minimal implementation consists of. It is likely that this Rust library will need to

implement at least some elements of Sia's file hosting contract functionality in order to properly validate transactions.

QA Considerations: The QA team must create a series of tests consisting of valid and invalid Sia transactions and signatures. These test cases will be run against both the Go and Rust implementations of transaction validation. These test cases should include all possible use cases of SIA transactions such as the older "v1" consensus model, all newly introduced features in the "v2" consensus model and all file hosting contract functionality.

Technical Details: Implementing Sia's equivalent of Bitcoin's "sighash" function will be the most critical part of this library. This function serves as the basis for all signatures generation and validation. There is zero room for error while porting this functionality to Rust. The API team may consider using an FFI within this Rust library to directly integrate the relevant Go code into the Komodo DeFi Framework. However, an FFI between Rust and Go is not a well supported feature of either language and requires extremely careful consideration for memory management and type safety.

System Impact: There is potential to introduce critical flaws in the atomic swap protocol while implementing this Rust library. For example, a transaction validated by walletd but failing validation within the Komodo DeFi Framework or vice versa could potentially result in a loss of user funds.

Future Vision: Further cooperation between the Komodo and Sia teams could enable this Rust library to develop into a full implementation of Sia's consensus model and node software.

Interactive Wallet Functionality

Problem Identification: The interface between the Komodo DeFi Framework and Sia's walletd as well as the Sia Rust Library will enable the API team to implement the remaining wallet functionalities such as sending coins, receiving coins and broadcasting transactions.

Solution Proposal: The API team will adapt the existing wallet functionalities within the Komodo DeFi Framework to work with SIA.

UX Design Considerations: The intent from the API team should be to provide a nearly identical UX to that of other coin implementations. If the UX or design teams identify any inconsistencies, these inconsistencies should be clearly communicated to the API team.

Potential Complications: SIA should be easily adapted to the existing set of methods provided by the Komodo DeFi Framework. However, any issues identified here must be identified and remedied with coordination between all teams. If the API team identifies a technical hurdle in

regards to reusing the existing set of methods, discussion must be initiated with the UX and design teams in order to minimize additional work for the UX and design teams.

QA Considerations: The QA team will be able to reuse their typical testing methodology assuming the API team can successfully integrate Sia into the existing set of API methods.

Technical Details: At this point, the following methods or SIA-specific equivalents should be fully functional: enable, disable_coin, get_raw_transaction, my_balance, my_tx_history, send_raw_transaction, show_priv_key, validateaddress and withdraw.

System Impact: All prior tasks lay the foundation to enable the peer-to-peer atomic swap business logic. With the culmination of this task, the Komodo DeFi Framework will be a fully functioning SIA wallet.

Future Vision: Further coordination between the Komodo and Sia teams can explore the possibility of integrating Sia's unique functionalities such as file hosting contracts.

Peer-to-Peer Swap Protocol

Problem Identification: The newly added SIA consensus mechanisms must be adapted to work within the Komodo DeFi Framework to facilitate peer-to-peer atomic swaps with SIA and BTC-like coins and ETH-like coins.

Solution Proposal: The Sia team has provided all the necessary consensus components to facilitate "HTLC-like" atomic swaps. At this point, the Komodo DeFi Framework API will be a functioning wallet capable of sending and receiving SIA coins. Given this foundation, extending this to support atomic swap is a matter of implementing each transaction type in the swap process.

UX Design Considerations: The user experience of SIA within Komodo Wallet should closely or identically mimic that of a typical coin implementation. If the UX or design teams discover any pain points while attempting to create this experience, they must be communicated clearly to the API team.

Potential Complications: Assuming each aforementioned implementation step has been completed, the integration of the swap protocol should have no major complications. This step builds entirely on the successful completion of all other steps combined.

QA Considerations: The QA team will be responsible for running their typical suite of manual tests and responsible for monitoring the CI test suite.

Technical Details: The implementation of the atomic swap protocol involves implementing several already established traits within the Komodo DeFi Framework such as

“MarketCoinOps”, “SwapOps”, “TakerSwapMakerCoin” and “MakerSwapTakerCoin” among others. These traits serve as a mechanism for generalizing the business logic involved in order matching and atomic swap execution across numerous protocols.

System Impact: All possible coin integrations will be made compatible and tradeable with the newly established Sia integration enabling peer-to-peer atomic swaps with the numerous coins and tokens listed in Komodo Wallet.

Future Vision: Further collaboration from the Komodo and Sia teams can produce more intricate and complex DeFi capabilities. There is potential for Sia’s unique feature set surrounding file hosting to be made directly accessible within Komodo Wallet.

Deliverables

Phase 1: Scope of Work

- Research and Evaluation of Sia’s Codebase
    - Delivered in previous grant
- Finalization of Scope Document
    - Deadline: February 9, 2024
    - Deliverable: Completed scope document with clear breakdown and delegation of tasks for both teams.

Phase 2: Development Phase

- Development Environment and Testnet
    - Deadline: February 23, 2024
    - Deliverable: Documentation on establishing a “regtest”-like network and a persistent internal testnet for development and testing.
- Test Coin Activation
    - Deadline: February 23, 2024
    - Deliverable: A test coin activated within the Komodo DeFi Framework for testing purposes, with a clear name, ticker, and placeholder icon.
- Sia Consensus Model Testing
    - Deadline: On-going research and feedback throughout the duration of the grant. Initial report March 22, 2024
    - Deliverable: Document providing a brief description of tests performed on each newly added SpendPolicy as well as a general overview of all “v2” consensus.

- Informational Wallet Functionality
    - Deadline: June 21, 2024
    - Deliverable: Demonstration of SIA coin activation within Komodo Wallet including receive, transaction history, checking balance and checking confirmations

- Sia Rust Library
    - Deadline: August 2, 2024
    - Deliverable: Developer documentation of the library as well as a demonstration of SIA coin activation within Komodo Wallet including signing and sending transactions.
- Interactive Wallet Functionality
    - Deadline: August 23, 2024
    - Deliverable: send, receive, maybe gen addresses
- Peer-to-Peer Swap Protocol
    - Deadline: September 27, 2024
    - Deliverable: Demonstration of peer-to-peer atomic swaps within Komodo Wallet.

Phase 3: QA Testing and Security Hardening

- Comprehensive QA Testing of User Interface
    - Deadline: October 18, 2024
    - Deliverable: QA report outlining identified issues and their resolutions.
- Finalization of User and Developer Documentation
    - Deadline: October 18, 2024
    - Deliverable: Complete documentation ready for publication.

Phase 4: Release Candidate

- Release Candidate of Komodo Wallet with full SIA integration
    - Deadline: October 31, 2024
- Training and support for potential Sia branded white-label of Komodo Wallet
    - On-going support throughout the duration of the grant
    - Deadline: October 31, 2024
    - Deliverable: Training materials and all relevant code ready for white-label deployment of Komodo Wallet

Timeline

- Phase 1: Scope of Work
    - Deadline: February 9, 2024 - Finalization of Scope Document.
- Phase 2: Development Phase
    - Deadline: February 23, 2024 - Development Environment and Testnet; Test Coin Activation.
    - Deadline: March 22, 2024 - Initial Sia Consensus Model Testing Report.
    - Deadline: June 21, 2024 - Informational Wallet Functionality.
    - Deadline: August 2, 2024 - Sia Rust Library.
    - Deadline: August 23, 2024 - Interactive Wallet Functionality.
    - Deadline: September 27, 2024 - Peer-to-Peer Swap Protocol.
- Phase 3: QA Testing and Security Hardening
    - Deadline: October 18, 2024 - Comprehensive QA Testing and Finalization of Documentation.
- Phase 4: Release Candidate
    - Deadline: October 31, 2024 - Release Candidate of Komodo Wallet with full SIA integration and Training Materials for Sia branded white-label of Komodo Wallet.