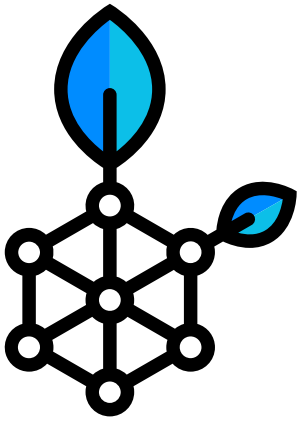


rif

RSK Infrastructure Framework

Architecture

Building the infrastructure for the next generation of distributed applications

V 1.31

Introduction

RIFOS is a set of protocols, rules and interfaces, for accessing decentralized services which we expect most decentralized blockchain applications will require. We call them Root Infrastructure Services, because they form a coherent infrastructure that decentralized applications can rely on. These protocols will initially include: Name Resolution, Data Storage, Secure Certified Communications, Data Feeds (i.e. oracles), and Payment Processing. Third parties can implement any of these protocols by creating a "Service Provider," which is a piece of software that either provides all the service functionality or bridges RIFOS with other external networks that provide such service. Service Providers of RIFOS protocols can be directly accessed by user applications (i.e. a service provider of RIF Storage can serve as a decentralized Dropbox replacement directly accessed from the user desktop) or be consumed by other service providers. (i.e. a wallet may use a RIF storage service provider to store the encrypted user data in remote servers). All protocols that form part of RIFOS share some characteristics:

(i) protocols are prepared to interact, stake or consume RIF tokens;

(ii) anyone can become a service provider of a RIF protocol by advertising the service, and

(iii) all RIF protocols should be designed so that, if a smart contract layer is required for providing the associated services, then the services can be smoothly implemented on top of the RSK Smart Protocol.

RIFOS is designed to promote a fair market for distributed infrastructure services, which can be provided by any third party targeting the RIFOS user base. For instance, the RIF Storage Protocol promotes competition of storage providers by enabling a storage marketplace.

RIFOS facilitates the development and deployment of distributed applications for users without an in-depth understanding of the underlying technology. This is because the RIFOS protocols are designed to hide some technicalities and inner workings of decentralized services. Therefore RIFOS aims to increase the adoption of distributed blockchain technologies by application developers and, through new applications, by end users.

RSK Labs has built the first service implementing one of the RIFOS protocols, the RIF Directory but, by design, RIFOS is an open system. Any third party can contribute a service, provided that the service complies with the requirements of the applicable protocol.

Initially, RIFOS will be built to be compatible with the RSK Smart platform, given that we foresee an enormous synergy among the two projects by leveraging the security of Bitcoin mining combined with the extensibility and functionality of RSK. However, RIFOS protocols should try to be blockchain agnostic whenever possible, and in the future service providers could span any number of blockchains.

RIFOS in the Context of Financial Inclusion

Three billion people are currently excluded from the financial system, limiting the ability of people to sell the result of their labor, save for harder times, or receive microloans for micro-enterprises that create wealth in a local communities. Emerging countries around the world often undergo successive economic crises and periods of hyperinflation, which together with inefficient and incompetent governments, make it impossible for citizens to have an immutable and permissionless secure store of value. Financial inclusion to a secure, decentralized, and censorship-resistant financial system is a once-in-a-millennia opportunity to improve people’s lives on a widespread and global level. Stateful smart contracts, combined with the security and broad network effect of the Bitcoin Network, can truly transform and improve the lives of millions of financially excluded individuals around the world.

The initial set of services provided by RIFOS was selected to simplify applications that tackle financial inclusion problems. However, other RIFOS compatible infrastructure services that prove to be useful and generic, targeting other use cases, may be integrated into the framework and offered to developers. RIFOS is a standard protocol that can be used to deliver solutions for a very wide spectrum of problem sets, while leveraging the same underlying technology and ecosystem.

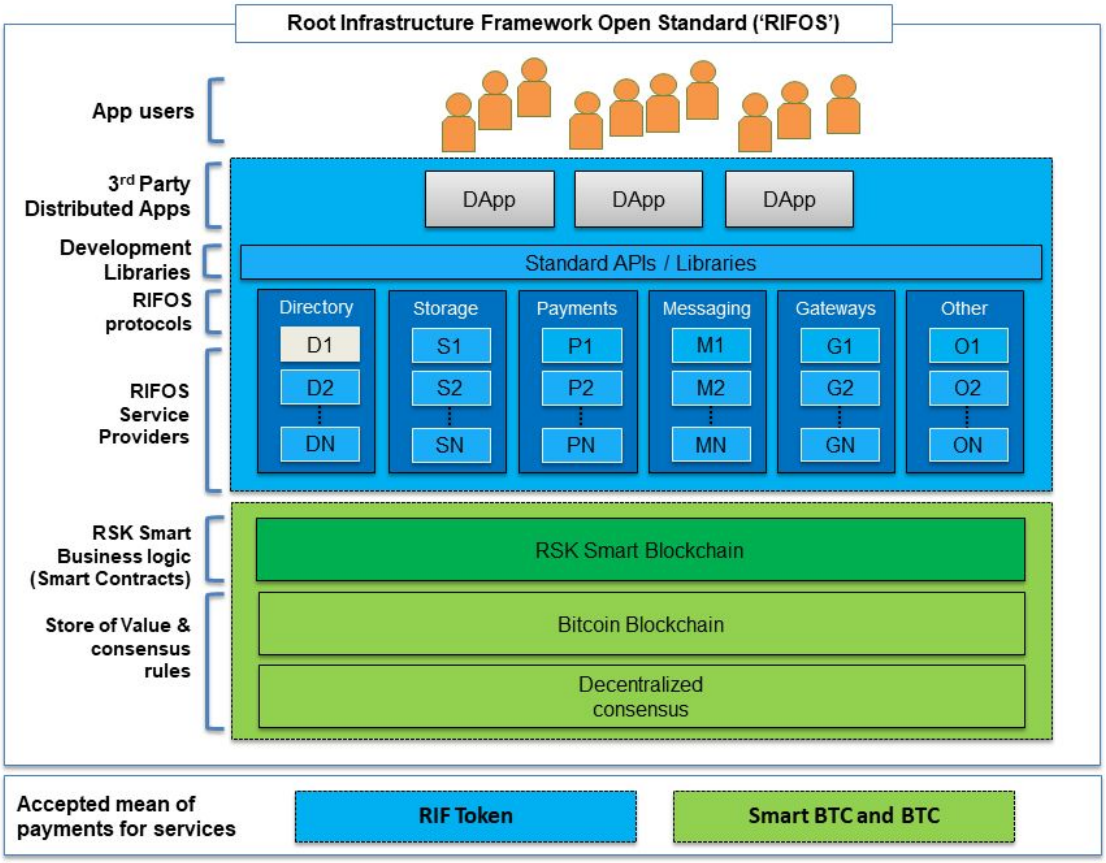
Architecture

RIFOS is a set of protocols that help user applications consume decentralized services. Protocols are implemented by service providers, which can serve user applications and also other service providers. There is no inherent RIFOS protocol hierarchy, but a protocol hierarchy materializes for each specific distributed application. In other words, some protocols can be "support protocols" of other service providers in some applications or provide the main functionality in some other distributed applications. The more protocols RIFOS integrates, the greater the benefit for the developer.

RIFOS is aimed at making the deployment of applications using distributed blockchain technology much easier and faster, without the need to provision any infrastructure services ahead of time. So, for instance, a walletmay grow from being a lightweight, SPV-mode application with very low storage and bandwidth requirements, to a full-blown multi-currency wallet, connecting to or running several full nodes consuming gigabytes of storage and bandwidth, without updating a single line of code. The change in functionality can be accomplished by changing the service providers. RIFOS is envisioned to enable a marketplace that can satisfy growing demands. Developers can integrate their RIF-compatible products and services seamlessly within the RIFOS ecosystem.

RIFOS services may be run by anyone. At the center of RIFOS is a utility token called the RIF Token. The RIF Token is managed by a smart contract running on the RSK Smart

Protocol. Although RIFOS protocols do not obey a hierarchical structure, when considering RIFOS together with RSK and Bitcoin, RIFOS becomes a multi-layered development stack.



D1 refers to the RIF Naming Service that is deployed in the RSK blockchain.

RIFOS Core components

One key feature of the RIFOS design is it accepts third-party service providers for the existing infrastructure protocols. Furthermore, new infrastructure protocols may be added in the future, either by RIF Labs or by any member of the RIFOS community, in order to enhance this open standard framework and offer greater functionality to the RIFOS user base. Any RIFOS component that conforms to the RIFOS design principles should be able

to seamlessly interoperate with other components, draw on resources available within the ecosystem and compete fairly for users and businesses.

RIF Labs will initially deploy the following RIFOS protocols (also called “core components”):

- **RIF Payments**: A protocol to access any off-chain payment network, specially payment-channel based networks. This protocol should enable scalable, cheap and high-speed off-chain payments; RIF Payments enables the use of different off-chain payment networks that can be deployed on top of RSK, supporting both smart bitcoins and standard fungible tokens. The protocol provides methods with clear semantics to enable a uniform interaction between the user, a hypothetical RIF-compatible wallet, and distinct payments networks. The RIF Payments API can help build bridges between different networks. The open-source, open-provider nature of the API enables new networks to advertise their services using the RIF Directory Protocol. Each payment network gets a distinct address namespace so that addresses are always unique. By using the RIF API, services like Point-of-Sale gateways (PoS) can be built, and these PoS services can work across all existing and future RIF-integrated payment networks. The end goal of the RIF Payments protocol is to generate a competitive environment where payment networks can flourish to provide low fees and low latency, and that can scale to match the volume and exceed the performance of legacy credit card networks. RIF Payments also proposes a conceptual framework that is intuitive and relies on legacy concepts such as savings accounts, checking accounts and term deposits.

- **RIF Directory**: An alias system (Naming Services) protocol enabling name actions and 2nd markets. We believe that cryptocurrencies will grow exponentially in the next decade. However, to genuinely enable mass adoption, not only by the tech-savvy community, anyone needs to be able to manage digital wallets and assets. So, one of the principal barriers to adoption is the inherent complexity of the blockchain technology. Ease of use is key for reaching the unbanked and non-technical users. It’s difficult to expect a widespread adoption if users must copy and paste long hexadecimal addresses to

transfer or receive digital assets, for example. In addition, manually typing addresses is an error-prone process, and a simple typo may result in a loss of funds. By adding a name resolution service, also known as “aliases” or “domains,” the probability of errors is greatly reduced, as is the apparent complexity of the system: the easier the technology is to use, the faster the adoption. The RIF Directory goal is to find different types of resources by simple resource names. Example resources are: RSK addresses, personal encryption public keys, social network handles, and so forth. In addition, centralizing the access to multiple resources associated with a human-readable name improves the RSK platform user experience. RIF Directory can also allow non-for-profit organizations to add transparency to their treasury management by publicly disclosing their names in the public addresses. As resource names may change over time, the system needs to be flexible to support frequent changes. Lastly, the system enables users to easily buy, sell and auction names, using the RIF token.

- **RIF Secure Communications**: Peer Discovery protocol for authenticated and encrypted communications. RIF Secure Communications Infrastructure (RSCI) is a protocol to enable parties that need to communicate to register their communication methods, discover other parties and contact them through their preferred communication method by using their public keys as a discovering mechanism. By using the protocol, Alice may publish her pseudonym on the RIF Directory, along with her communication's public key. Whenever she uses her alias to establish a connection, the counterparty can look up her communication's public key, and use it to create a secure connection, enabling pseudonymous communication among participants. RSCI aims to fulfill the need for establishing secure communication links between RIFOS parties or services. These communication links should at least assure confidentiality, integrity, and authenticity. On top of the properties mentioned above, it is possible to build additional features, such as group communications, non-repudiation, and forward secrecy.

- **RIF Storage**: Decentralized redundant data storage access protocol. The RIF Data Storage Layer (RDSL), is a protocol acting as a connectivity layer for third-party storage

providers. This protocol introduces concepts to enable the seamless transfer of data and negotiation of prices between storage providers and clients over the RSK blockchain. The open-source, open-provider nature of the protocol allows for new networks to advertise their services on the RIF Directory. Most people take for granted the ability to store personal data reliably. Distributed storage networks are intended to afford anyone in the world with an internet connection, regardless of location or means, the ability to store their digital identity, resources, and sensitive information, with the confidence that their data is cryptographically secure and private. RIF Data Storage Layer enables different third-party storage networks to coexist and compete, so each storage network registered in the RIF Data Storage Layer gets a distinct address namespace so that addresses will always be unique. Using the RIF API, it will be possible to build compatible services that work across all storage networks. The end goal of the RIF Data Storage Layer is to enable a competitive environment where storage networks can thrive to provide scalable storage solutions with low fees and low latency, while allowing the users to store their critical ID information encrypted in distributed servers around the globe.

- **RIF Data Gateways**: Oracle protocol to access external data feeds. Blockchain protocols with on-chain smart-contracts must communicate with external systems through oracles. The RIF Data Gateways Service provides an implementation-agnostic protocol for external data consumption through Data Service Providers. Some examples of external data that frequently needs to be consumed by smart contracts are price feeds, and the state of foreign blockchains. Securely notifying contracts about the state of foreign transactions makes it possible to transfer tokens by building bridges between blockchains.

- **RIF Explorer**: Explores the services registered for every component of the RIFOS. The RIFOS Platform provides a set of abstractions and APIs to support third-party implementations in the form of RIFOS Service Providers. This decoupling enables the platform to switch to new, potentially more enhanced implementations as the technology of each service evolves, and new solutions emerge. In this context, it is necessary to provide mechanisms to register and discover these implementations allowing developers

and clients to choose which one they want to use for their particular use cases. RIF Explorer is a service of the RIFOS Platform that provides the required functionality to register and discover third-party implementations of the RIFOS Services (aka Service Providers) in the RIFOS Platform. RIF Explorer extends the RIF Naming Service (RNS) capabilities to support the recovery of Service Providers' addresses not only by domain name but also by different criteria, such as service type or optional meta-data.

Creating and Advertising New Protocols

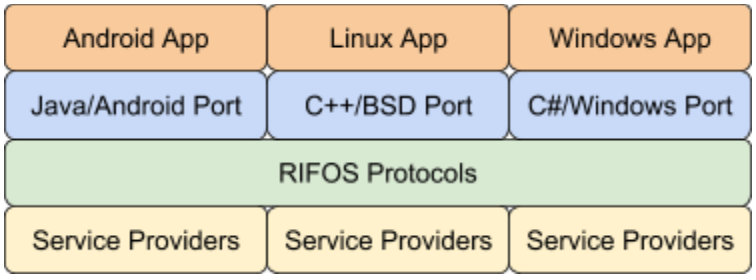
RIF Protocols can be advertised by using the RIF Directory service. Name resolvers are used to expose links to information relevant to each protocol, such as authors, license, URLs, repositories, documentation, prices, and so on. Anyone can register a new name and associate a RIF protocol with it. Also user applications can discover available protocols using the RIF Explorer. RIF Labs will maintain a curated list of advertised protocols that have been tested and serve the vision of financial inclusion, but anyone is free to provide a protocol directory that selects or prioritizes the protocols based on other criteria. Helper applications may be used to automate tasks or import protocol interfaces.

A sample hypothetical RIFOS component that could be added is a protocol to access hardware wallets that can manage tokens, including RIF, and the corresponding implementation of a service provider for such a protocol would be in the form of a software library. Other vendors can plug-in compatible libraries that conform to the protocol.

Another hypothetical example of a useful RIF protocol to be added would be RIF Reputation, which lets users score protocols based on their utility, number of bugs, and response of the development team in event of security vulnerabilities.

RIFOS Ports

Apart from the initial interfaces provided by RIFOS, the RIF protocols interfaces could be implemented on other programming languages and for other target platforms by third parties in the form of "ports." Implementers of these ports should provide the required glue code in the form of software libraries to simplify the discovery and connection of service providers with the actual interfaces, as required by the protocols. Although RIF Labs may work to provide a first port of the protocols, no port should be viewed as "the reference port," and all ports should comply with the RIFOS protocols independently. The following diagram shows three possible ports of RIFOS protocol interfaces, for Android and for Linux.

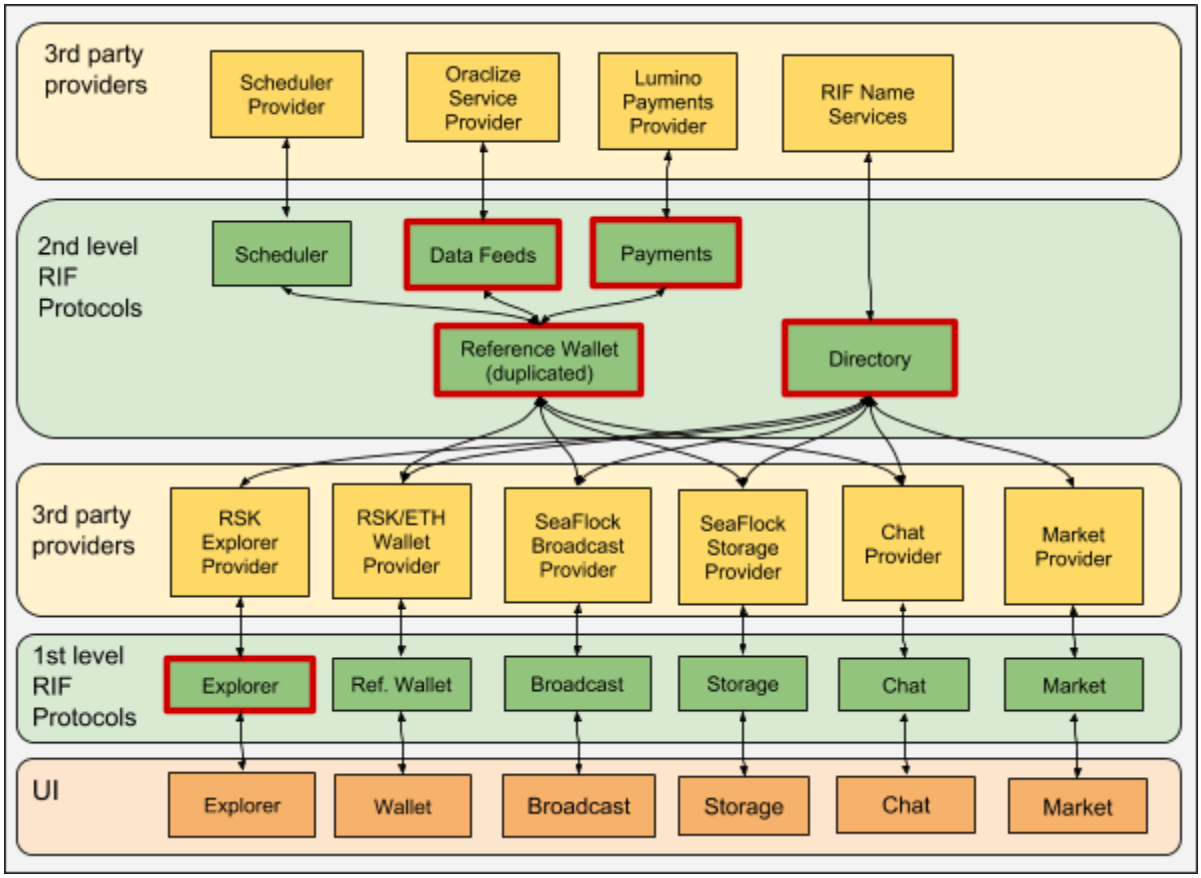


Extensibility

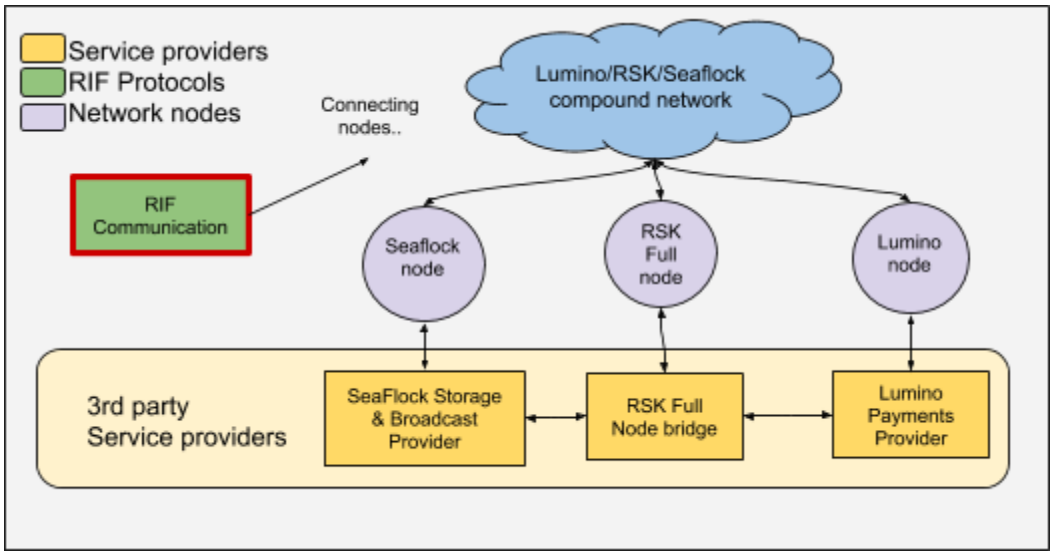
RSK Labs has architectured five core protocols, but there are other possible protocols that are interesting and could enhance decentralized applications. To show how RIFOS could grow, we'll present a series of examples related to an hypothetical decentralized reference wallet ("Reference Wallet"), that interacts with a hypothetical decentralized social network ("Chat"), a decentralized broadcast messaging service ("Publish"), and a decentralized marketplace of RIFOS-enabled applications ("Market"). These examples will let us show

how the different protocols interact, and why some protocols (such as storage) are fundamental for so many use cases. Also, these examples will let us show how RIFOS may be used to address the needs for financial inclusion.

In the following figure we show the architecture of a hypothetical extension that adds new protocols and service provides to integrate a decentralized wallet, a decentralized group messaging network and a decentralized storage network.



The following diagram shows how each service provider interacts with the network nodes.



The green boxes framed in red represent current advertised RIFOS components. All other green boxes represent hypothetical future components to be added. Yellow boxes represent service providers. Orange circles represent network nodes.

A new decentralized network is created merging the functionality of several networks into a single backbone (the "compound" network). Each peer in this network can advertise and provide one or more of the many services offered. Three of these services are Storage (storing third-party information for long periods), Payments (supplying off-chain payments through a multi-hop payment channel path) and Broadcast (providing temporary message storage to support a message broadcast network). This network also provides an alternate incentivized network for propagating RSK blocks and transactions (even for another cryptocurrency).

For each of these fundamental services, we present the corresponding UI, plus a configuration and application market UI. These services will use current RIFOS protocols, in addition to any protocols that may be added to RIFOS. Here we briefly describe each component:

- **RIF Reference Wallet**: RIF tokens can be accessed with several existent third-party wallets (e.g. Jaxx, MyCrypto, Ledger, Trezor). However a Reference Wallet protocol

could be helpful to facilitate the construction of new competitive products by third party developers. We envision a Reference Wallet that enables users to perform monetary transactions on RIF-supported blockchains, and supporting features generally missing, such as:

  - Multi-signature control with configurable thresholds depending on payment amounts;
  - Covenants with address whitelisting and different configurable periods for different payment amounts;
  - Reimbursable deposit-based DoS protection for partial signatures;
  - One-time signatures/revocation codes;
  - Configurable fee limits;
  - Withdrawal limits configurable for different tokens specified in any fiat/crypto coin;
  - Encrypted mnemonic seed backup and secret sharing;
  - Device-to-device payments;
  - On-chain and off-chain transfers;

- **ETH/RSK Wallet Provider** (for the RIF Wallet protocol): Provides a smart-contract-based wallet that is deployed in one or more RSK or ETH compatible blockchains. The interaction with blockchains (either RIF-compatible or UTXO-based, such as Bitcoin) is performed through self-hosted full nodes over RIF secure communication channels. To support UTXO-based wallets, a UTXO Wallet provider is required.

- **RIF Chat**: The Chat protocol enables groups to chat securely and privately. It leverages on the RIF Directory as a public-key repository to find contacts' public keys. It establishes peer-to-peer links using RIF Communication, and it can negotiate multi-party contracts in natural language, from simple token transfers to more complex atomic exchange operations.

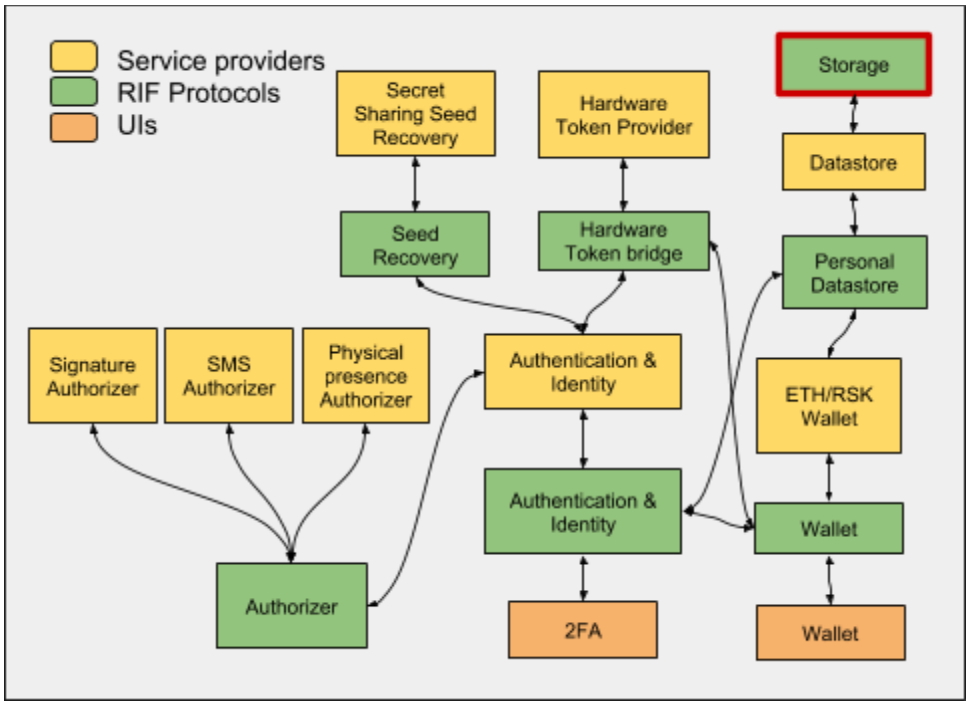
- **RIF Broadcast:** A protocol to spread one-to-many messages over an incentivized decentralized network (as a decentralized-Twitter). Messages have a specified timeout, and nodes store these messages for that amount of time.

- **RSK Full Node Bridge**: This component enables communications with remote-full nodes through its JSON-RPC interface, encapsulated in an authenticated and encrypted secure communication channel.

- **SeaFlock Storage and Broadcast Provider**: This is a single provider for the storage and broadcast services. Peer-to-peer micropayments through payment channels incentivize the network. Nodes should regularly challenge peers to comply with temporary storage requirements (broadcast service) and penalize peers that do not. The storage provider node also verifies other peers storing the same data and competing for the same reward.

- **Lumino/SeaFlock/RSK Compound network**: This is a new compound network where nodes can provide one or more advertised services. Nodes can establish peer-to-peer payment channels to perform micropayments on communication, data and computing requirements.

The following diagram shows how the Wallet interacts with hypothetical RIF protocols for authentication and identity, and how it stores private user information on a decentralized storage network.



The diagram includes the following new components:

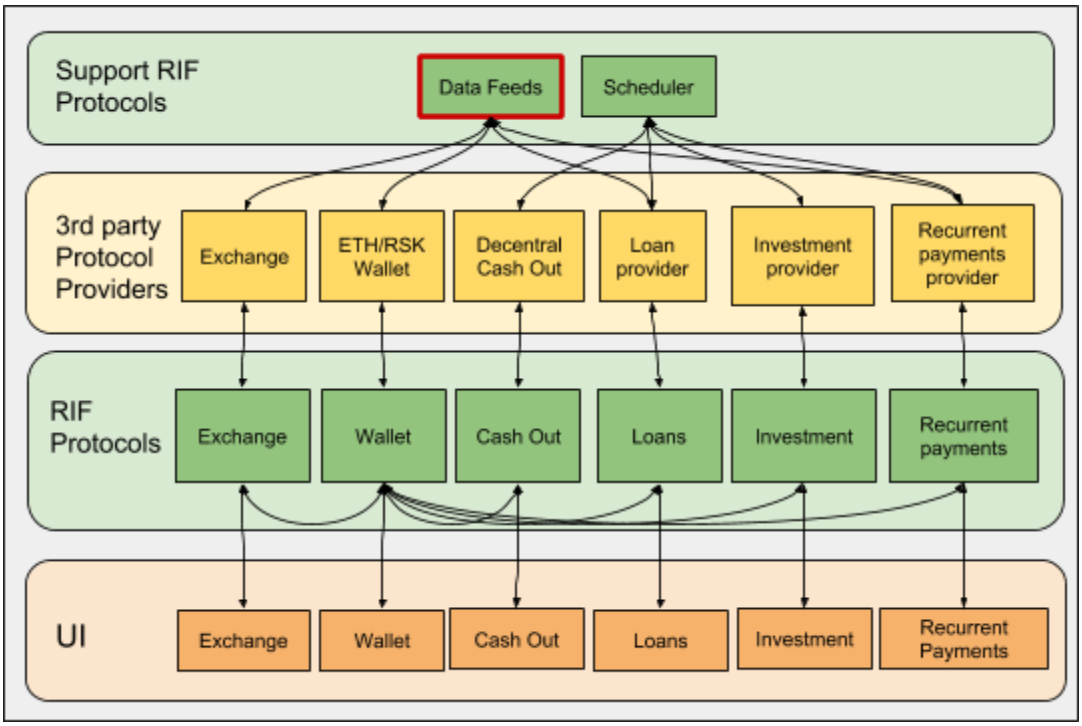
- **RIF Hardware-Wallet Bridge**: A protocol to connect to hardware wallets from different vendors, and provide transaction and general signing services.

- **RIF Authentication & Identity**: a FIDO Universal 2nd Factor (U2F) authentication protocol that uses RIF hardware-wallet bridge to connect to signers implemented in hardware wallets. It also manages a set of access tokens, and privacy-preserving reputation tokens to manage a decentralized identity.

- **RIF Authorizer**: Enables users to select third party authorizations for different secure actions, such as withdrawal of funds, high-amount transfers, or private information disclosure. Providers can offer methods to delegate authorization, such as SMS messaging, third-party signing keys, one-time passwords, or event identity confirmation through physical presence and biometrics.

- **RIF Personal Datastore**: The Personal Datastore manages an encrypted personal memory space, which is automatically replicated in outsourced servers using RIF Storage. The memory space includes a list of identities, and for each identity, it contains a backup of the transaction history, active authentication tokens and handles for third-party systems, passwords, private key/seed, reputation identifiers, and privacy-preserving personal information tokens.

The following diagram expands the RIF Wallet with potential bank-in-a-box protocols:

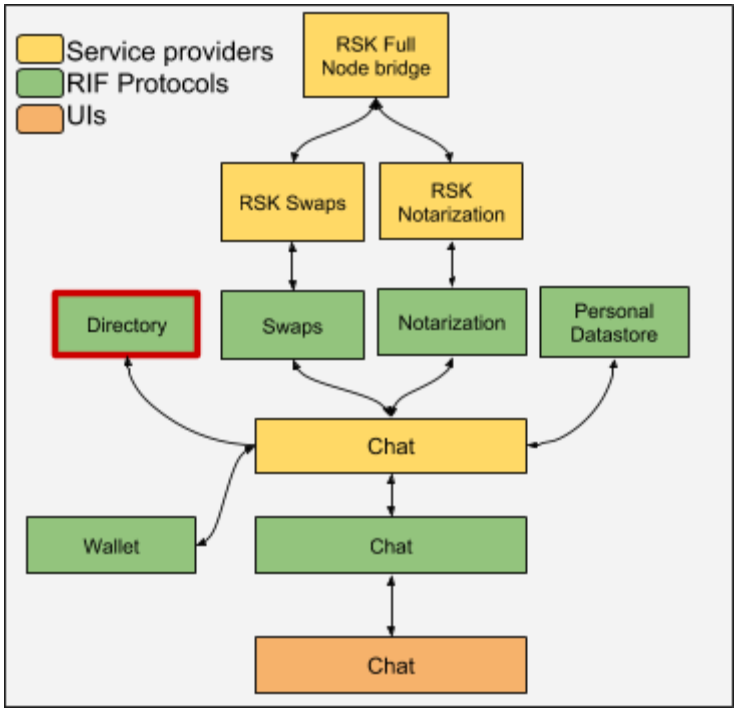


- **RIF Loans**: Enables different loan providers to offer loans to the user. Sample loan providers are decentralized systems or centralized banks. It also enables crowdfunding commercial loans.
- **RIF Investment:** Enables different investment providers to offer loans to the user. Sample investments providers include crowdfunded projects or term deposits.
- **RIF Recurrent Payments:** Enables payments to be scheduled on a periodic basis, both for fixed amounts and for variable amounts (e.g. electricity bill). In the case of variable

amounts, service providers can notify users of rate changes and users can set up automatic variable payments restricted to user-selected limits.

- **RIF Cash Out**: RIF Cash Out enables cashing out funds in fiat physical currency at PoS, ATMs or with the help of other users. Also, it enables third party cash-out for remittances. Providers can be centralized (e.g. Western Union), or decentralized, like the Abra cash-out network.

The following diagram expands the RIF Chat component showing several other hypothetical services that enrich the chat experience:

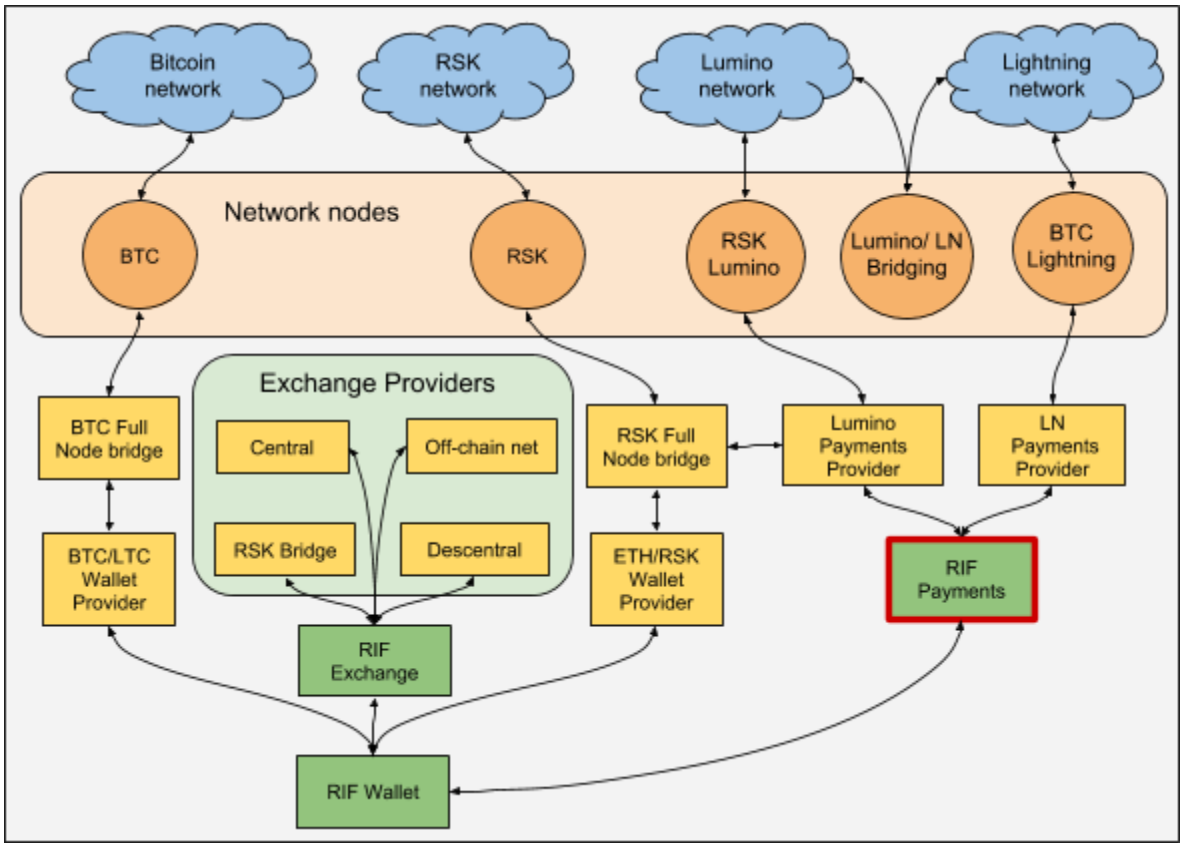


The Chat Protocol enables triggering payments and atomic swaps of digital assets between the users in the group directly from the chat interface. Also, any written text can be time-stamped and notarized (signed by the group of participants or an external entity). The evidence is left in the blockchain in the form of a hash digest of the data and the signatures

(no information is revealed to third parties). A copy of the notarized text is automatically saved by each participant in its Personal Data Store.

- **RIF Notarization**: A protocol that enables information to be notarized through digital signatures and time-stamped in the blockchain using a hash digest.
- **RSK Notarization Provider**: Uses the RSK Ephemeral data to distribute messages to be time stamped and a smart contract for anonymous message aggregators to submit candidate root hashes for Merkelized collections of published messages. An automatic dispute resolution protocol enables parties to punish bad aggregators. By doing so, the cost of notarization is kept low a there is no central party responsible for aggregation.
- **RIF Swaps**: A protocol to create atomic-swaps between fungible tokens, cryptocurrency, and non-fungible tokens.

The following diagram shows how RIFOS components may interact with Bitcoin in the future through hypothetical bridging services provided by third parties.



A hypothetical RIF Exchange Protocol defines the interfaces to provide exchange between currencies and tokens. Four hypothetical providers are shown. The decentralized provider uses a decentralized exchange running over RSK. The off-chain network exchange provider allows bitcoins locked in Lightning Network payment channels to be sent directly to Lumino payment channels using a hypothetical Lumino/LN Bridging node. The RSK bridge exchange provider allows BTC to be exchanged for Smart Bitcoins and vice-versa through the RSK autonomous bridge. Therefore the wallet could manage at least four methods for Bitcoins to be exchanged for smart Bitcoins and vice-versa, enabling higher liquidity and the lowest possible friction.

The wallets shown interact with two hypothetical wallet providers, the RSK wallet provider enables management of RSK-based tokens and smart bitcoins, and the BTC wallet provider enables management of BTC and colored coins. The RIF Payments protocol interacts with

two hypothetical payment providers: A BTC Lighting Network enabler and a Lumino enabler. Therefore, the user can send bitcoins or smart bitcoins cheaply and instantly.

Listing Protocols on RIF Labs's Websites

RIF Labs has established simple criteria for listing RIFOS protocols on its own websites, based on RIF principles. Users are free to create their own RIFOS protocol listings under any other preferred criteria on their own websites. In this regard, our listing is similar to a p2p file tracker index, which provides links to decentralize protocols but does not hold a copy of the protocol itself. RIF Labs's listing intends to prioritize protocols that help financial inclusion, but RSK Labs may change or adapt the criteria at any time. Currently, the criteria consider the following protocol properties:

- The protocol must help the development of decentralized applications.
- The protocol should be open for service providers to register.
- The protocol should support the RIF token, consume the RIF token, or be destined to increase the features and potential of other RIF protocols.

For example, a RIF hardware-wallet bridging protocol will not directly "consume" RIF tokens, but it will increase the security for RIF-compatible wallets, so RIF Labs may select it for its listing.

Summary

RIFOS is a set of protocols, rules and interfaces, for accessing decentralized services. These services can form a coherent infrastructure that decentralized applications can rely on. The initial protocols include: Name Resolution, Data Storage, Secure Certified Communications, Data Feeds (i.e. oracles), and Payment Processing. Third parties can implement any of these

protocols by creating a “Service Provider,”. All protocols and service providers seamlessly interact with the RIF token. RSK Labs has built the first service implementing one of the RIFOS protocols, the RIF Directory, on top of the RSK blockchain, which provides smart-contract capabilities ideal for RIF service provision.