Saline: Universal Platform for Atomic Multichain Transaction Flows

Rising Sea Labs Ltd

March 2024

Abstract

This paper describes the design and implementation of the Saline Network, a new decentralised blockchain and supporting wallet infrastructure based around a wide and universal notion of Intent. In this new framework, users can govern their digital assets using a unified, composable vocabulary to describe properties that interactions with their wallets have to satisfy. The supporting smart-contract free blockchain and wallet software enforce the atomicity of complex transaction flows involving assets from all networks as part of the Proof-of-Stake validation process, while offloading a lot of logic and computations to off-chain code.

1 Introduction

The release of the Bitcoin whitepaper in 2008 marked the birth of trustless digital currencies, a few of which would go on to become successful and recognised worldwide with widespread adoption: the pseudonymous Satoshi Nakamoto launched the "crypto era" and showed that it was possible to transfer value peer-to-peer without involving intermediaries in the process. The introduction of Ethereum and the Ethereum Virtual Machine was the evolution that showed crypto was not limited to making discrete, single-shot payments in a virtual and decentralized way, but was able to support an entire ecosystem of decentralized applications ("DApps"). This is where the crypto ecosystem started to flourish, differentiate and expand drastically: everyone could create their own currency, their own set of applications and their own blockchains, and dreams of the "Web3 era" proliferated. It is now possible to create a tailored blockchain ecosystem to one's specific use case. However, the laterality and diversity of blockchains had an unexpected negative side-effect: extreme fragmentation. While it was made easy to create blockchains, tokens and "ecosystems" (there are around 120 Layer-1 chains at this time), they remain, for the most part, isolated from each other. Another limiting factor to wider adoption is the difficulty of building anything moderately complex: Smart Contract languages are reserved for a niche of developers with experience and these programs lack the ability to reason about anything outside the chain they are living in.

This litepaper presents Saline, the first Smart Contract-less Intentional Platform, that is able to reason about any blockchain in a native way and is centered around the user experience (for developers, projects and individual users alike).

2 Adoption Is Not What It Should Be

Blockchain adoption, though massive, is not at the level it should be. It is currently reserved to either early-adopters and risk-takers that want to profit from high and regular price fluctuations, or the niche of software developers that craft ever-more complex Smart Contracts and DApps. But the general feeling among the broader population is one of restraint: the complexity and the number of different (and often incompatible!) ecosystems slow down adoption.

The lack of compatibility between the myriad of ecosystems and the sheer difficulty required to implement a behavior (or intent) that can be expressed in a single sentence are the two weaknesses on which Rising Sea Labs focuses and which Saline solves.

2.1 Fragmentation

The sheer number of isolated, incompatible and isolated ecosystems is an obvious concern within the industry: some part of the problem has been the subject of much ink, time and investment, with more and more solutions attempting to bridge across chains. Whether it is the ability to interact with DApps from another chain, swap tokens across two different chains or exchange native assets for wrapped one, they all aim at increasing the cross-compatibility of the systems.

We believe that these solutions are generally limited to point-to-point systems, targeting proprietary Smart Contracts endpoints, and lack the more general-purpose ability that is required for truly merging systems together. Saline solves this by not making the cross-chain ability a separate feature, but rather by baking in the ability to reason about wallets and assets in other chains natively. Foreign events such as the change of a wallet's balance, an incoming, or an outgoing transaction, can be used either as a trigger, a constraint or as part of more complex, compound transactions in the Saline system.

2.2 Complexity

Smart Contracts were among the pillars that enabled the Web3 revolution. The idea of treating a blockchain as a global computer gave it its ability to run programs in a decentralized way; in theory bringing in an entire new realm of possibilities when compared with simple one-to-one payment transactions. In reality, however, if complex programs and logic can be (and have been) implemented, they remain exclusive to developers that are familiar with the general-purpose programming languages used to write Smart Contracts. An everyday person who wishes to issue simple logic such as *"keep my Ethereum wallet X above a certain balance B, possibly provision it with funds from my Solana wallet Y"*, or *"in my Wallet W, make sure that none of the currency make up more than X % of the total value"* are hard-pressed to do it without registering to a (potentially expensive and inevitably trust-based) central service or coding themselves the Smart Contract that do it.

At RSL we think that not everything should be a (D)App, and not everything should be complicated and require knowledge and experience of general-purpose programming language. TradFi traders have been using increasingly sophisticated instruments with Excel as their sole tool for years! We believe the crypto ecosystem would greatly benefit from an "Excel for crypto" and that is what we will build. By placing Intents at the core of the chain and the platform, we give users back the power and flexibility to do what they want instead of focusing on how to do it.

3 The Saline Network

Permeating our thoughts and dictating what our solutions must look like is the notion of simplicity. It's 2024 and we believe Crypto Should Be Simple. Facts say it is not the case yet: there were 300+ rug pulls in 2023 alone and there seems to be around 200k Solidity developers worldwide. This is a clear sign that the technology is immature, still under-resourced, and is prone to bugs.

The first thing we have been working on is *getting rid of Smart Contracts*. While they certainly allowed the blockchain ecosystem to flourish, creating never-be-seen-before (D)Apps, the entry barrier is clearly too high for the kind of adoption to which we aspire.

3.1 Intents at the Core

To understand how and why Intents are so powerful, we need to take a brief look at the inner workings of a blockchain. At its core, a blockchain is a list of transactions (grouped into blocks) which changes a global, shared state. The state is duplicated among all participants (almost a million in Ethereum's case) and the only way to update it is for a sufficiently large number of those participants to agree on the way it should be updated. The basis for agreement is a set of protocol rules that transactions are matched against. In a traditional blockchain, transaction validation looks something like this:

- check that the transaction was signed by the owner of the account (prevents other people spending one's assets)
- check that the currency exists and is supported by both wallets
- check that the balance of the issuing wallet allows the transaction (you can't spend more than you've got)
- other checks related to the protocol, versioning, governance, etc.

One of the most important aspects (and its most limiting) is that a transaction must be signed by the private key owning the wallet. This basic check ensures that no other party can spend your fund: it is a means of identification. The immediate downside is that the wallet's owner must manually sign every single transaction pertaining to his wallet, as a means of validating them. This is where Intents come into play.

Intent are rules that the owner of a wallet broadcasts to the chain, which, if respected, allow a transaction to be considered valid.

Depending on how the Intent is expressed, the transaction can be made valid without the need for even a signature (this is called signature-less transaction), or on the contrary can require multiple signatures (in an MPC-like manner). More complex transactions can involve trigger events or constraints on amount, date, time, N-of-M number of signatures, etc.

3.1.1 Example

As a basic example, let's consider the use-case of someone who pays rent in cryptocurrencies. Every month, on the 3rd, they pay $2,000 in ETH to their landlord. It is a pre-arranged contract and we know that there is going to be a transaction issued, every month, without fail, for $2,000 equivalent in ETH to their landlord's wallet address. And yet every month, that person must connect to his wallet, create a new transaction, sign it and submit it to the mempool, manually. The alternatives to automate such a process would today either involve a third-party custody solution (thus involving trust, relinquishing ownership of the account's private key) or writing a complicated and error-prone Smart Contract.

Intents make it possible to broadcast the following rule to the blockchain: *"every month on the 3rd, a transaction in ETH can be made once, from my wallet XXX to wallet YYY for an equivalent $2,000"*. This expresses the user's goal, intention. Once expressed like this, in its formal form, there is no need for additional verification, and this is where Intents are game-changers. Once this Intent has been published to the chain's nodes, it becomes part of the verification engine: a transaction can now be submitted (by anyone) regarding this wallet. If the transaction looks anything else than $\{from : \text{XXX}, to : \text{YYY}, amount : \$2{,}000\text{-in-ETH}\}$, or if it's not the 3rd day of the month, then it will get rejected and won't happen; otherwise and only in this specific case will it be accepted.

The beauty of this is that the user in this case never has to connect to his wallet, create a Transaction (potentially mistyping the amount or making a conversion error) or sign the transaction ever again.

3.1.2 Baked in

Some other actors in the crypto-sphere are talking about supporting some form of passive-validation scheme which they also call "Intents", but they generally are a very restricted set of rules, most-often running alongside their "normal" mode of operation and generally reserved for simple operations like the one we described: signature-less, N-of-M, etc.

At RSL we don't just support Intents, they are *baked into* our platform design. "Everything is Intent" could adequately describe the way our Saline Network works. We have replaced the outdated, traditional way transactions are verified, as described previously by our Intent Verification Engine (IVE).

Similarly, the traditional (and limited) wallets, whose sole goal is to hold assets in other chains, have been replaced by our Intentional Wallets: all wallets in the Saline Network can have

any number of arbitrarily-complex Intents attached to them, describing *what the user wants* (and not how to do it).

This is the first time that Custody and Utility are being fully merged as they should always have been.

At the protocol level, this means that when a transaction hits the mempool, a Saline Network validator node will run the transaction against the wallets' set of Intents and see if they match any. Only if one Intent is found to validate the transaction will it be included in a block on the chain.

Intents can be installed or uninstalled on a wallet with a special kind of transaction. Of course the traditional "normal transaction" can be expressed trivially with an Intent that reads $\{from$: my-wallet-addr$, to : *, amount : *, signature$: my-signature$\}$. This will be any wallet's default, fallback Intent.

3.1.3 More Examples

This new Intent paradigm brings such an immense sea of new possibilities that this paper would be hard-pressed in trying to list a meaningful fraction of them. We can, however, list a few possibilities that suddenly become not only possible, but almost trivial to express on anyone's Intentional Wallets with Saline:

- Recurring transactions like the ones for paying rents, or a subscription to a service
- Managing a shared account between several persons (friends, corporate account, family account, etc.) and giving spending rights :
  - Per-person spending limits and authorization (*"Alice can spend up to XX per week"*)
  - Per-amount custom authorization (*"At least 2 people are required to sign to spend more than XX"*)
- Managing liquidity among several wallets :
  - Keep balance above a certain value (*"Transfer XXX from* main-account *if* secondary-account *is under YYY"*)
  - Balance Sweeps (*"If* secondary-account *balance is over YYY, allow transaction up to XXX from it to* main-account *"*)
- Any Intentional Wallet can now become part of a distributed liquidity pool:
  - Allow people to exchange currency against your wallet : *"Allow any transaction taking up to 100 ETH from my wallet and sending me back BTC or SOL at exchange rate XXX"*

Those examples are merely scratching the surface of what can be done with Intents in the Saline Network: they are the trivial and basic examples, and yet any of these would require hundreds of lines of Solidity code to implement in a traditional Smart Contract. The Saline Intentional Platform brings back an entire realm of possibilities to everyone, not just expert developers.

3.2 Cross-Chain and Off-Chain

The Intent system we are developing for the Saline platform will, on its own, drastically change the dynamics of blockchain interactions. But we need not accept even the perimeter of "blockchains" as a border that isolates Saline from a wider universe of potential applications and limits its potential to a crypto-centric world.

The real power of the Saline Intentional Platform is revealed when its Intent system is paired with the Off-Chain capabilities that we are baking into the protocol. Other protocols focus on supporting cross-chain capabilities; that is, linking events happening on two different blockchains. Most of the time, the cross-chain capability is used to implement a bridge where a token is locked at one end and another token (either native or wrapped) is minted or released at the other end. This does reduce the isolation of those systems, but it remains extremely limited.

What Saline offers goes beyond simply bridging funds between blockchains: it brings the ability to reason about what is happening, not only on other chains (cross-chain), but as well as outside the chain (off-chain).

As described earlier, at the core of the Saline Network is the Intention Verification Engine, which all nodes use to validate submitted transactions and see if they match Intents installed on Intentional Wallets. We have described a few simple examples so far, but inside Saline, Intents have the ability to reason about events that happened either in other chains or even outside any chain.

3.2.1 Native Support for Remote Chains

Concretely the ability to reason about remote chains is made possible by two technological choices:

- Intentional Wallets on the Saline Network can be a sort of proxy for a wallet on another chain.
- The usual 1:1 Bridge has been replaced by a Distributed Bridge implementation, in a 1:many form

There are two kinds of Intentional Wallet on the Saline Network: $local : \langle addr \rangle$ and $\langle remote \rangle : \langle addr \rangle$. The local wallets ($local : \langle addr \rangle$) are the wallets that are native to the Chain, on which Intents can be installed, they hold assets in the Saline Network itself and are more or less what one would expect a wallet to be in a blockchain (though with the Intent system baked in).

Remote wallets ($\langle remote \rangle : \langle addr \rangle$) are representations (handles) of wallets on other chains. For instance, $eth : xxx$ is the handle for a wallet on the Ethereum chain, whose address is xxx. It allows us to reason about this (Ethereum) wallet, as a *native* object inside the Saline Network: it becomes possible to ask for its balance, make transactions with it, etc. Underneath, it means this wallet is part of the distributed bridge: funds are onboarded and redeemed (at the owner's convenience) between this Intentional Wallet on the Saline Network and the Smart Contract endpoint on the origin (remote) chain.

Remote wallets being a native object inside the Saline Network means they can be part of installed Intents: they can be used as targets, triggers, constraints, "from" and "to" addresses, etc. For someone who has onboarded wallets from several chains, it becomes possible to create Intents that automatically move assets between them, etc.

3.2.2 Native Support for Off-Chain

Besides being able to reason about wallets in other chains, Saline offers the ability to reason about practically anything happening off-chain, that is, outside even the crypto sphere, unlocking yet another dimension. The core concept for such operations is the notion of Provable Observability. It all comes down to being able to prove that something was observed happening.

This means that the Intent Verification Engine doesn't only reason about objects in the Saline Network, but is able to accept proofs about some other events. We are making the Intent Verification Engine flexible and modular enough so that several solutions can be used as proofs.

We will be releasing the Saline Platform first with a Trusted Watcher, which means that Watcher will post signed proofs of events on the Saline Network. The Provable Observability will, in this case, result from the trust put into this Watcher. This is an initial solution which allows the Platform to be released early, while we focus on the second Watcher based on Zero-Knowledge Proofs. The Saline Intent Verification Engine will be equipped with a ZK-Verifier which will allow it to take Zero Knowledge Proofs as a source of truth, thereby removing the need for trust.

This ability to observe events happening outside the Chain is what gives Saline the ability to treat remote wallets as native objects, but it also enables so much more: it becomes possible to include any kind of external data, actions and triggers as part of the transaction validation process. Complex programs that would be prohibitively expensive to run on-chain with traditional Smart Contracts can now be run off-chain, a Zero-Knowledge Proof of its run can be generated and posted on the Saline Network, which can then be cheaply verified by the Intent Verification Engine and thus unlock or triggers transactions.

4 Token

Virtually every cryptocurrency company emits some form of token from an early stage, allocating a large share to early investors, contributors and co-founders. At RSL we believe tokens need to have a utility if they want to be successful in a sustained way. We are not looking for a temporary, flash price bump but rather a sustained alignment of incentives which reflects its economic advantage in the system. We will not be issuing a token initially, and our economic sustainability is not based on it.

At RSL we are truly in the business of Making Things Simple (through the powerful yet intuitive Intent system) and Unifying All Blockchains to stop the fragmentation and isolation that plague the cryptosphere. Our economy is based on fees for providing services, validator rewards for running (part of) the Saline Network and Intent Matcher Rewards.

In a second, later phase, when adoption is confirmed and activity is increasing, we will consider introducing a token where that has clear utility with respect to a specific product - which could be utilized for paying the aforementioned transaction fees, granting a discount and enabling exclusive privilege to token holders. This token would then be backed by utility and will not be mandatory for using the Platform.