# Witness Chain Watchtowers: The First Line of Defense for Rollups

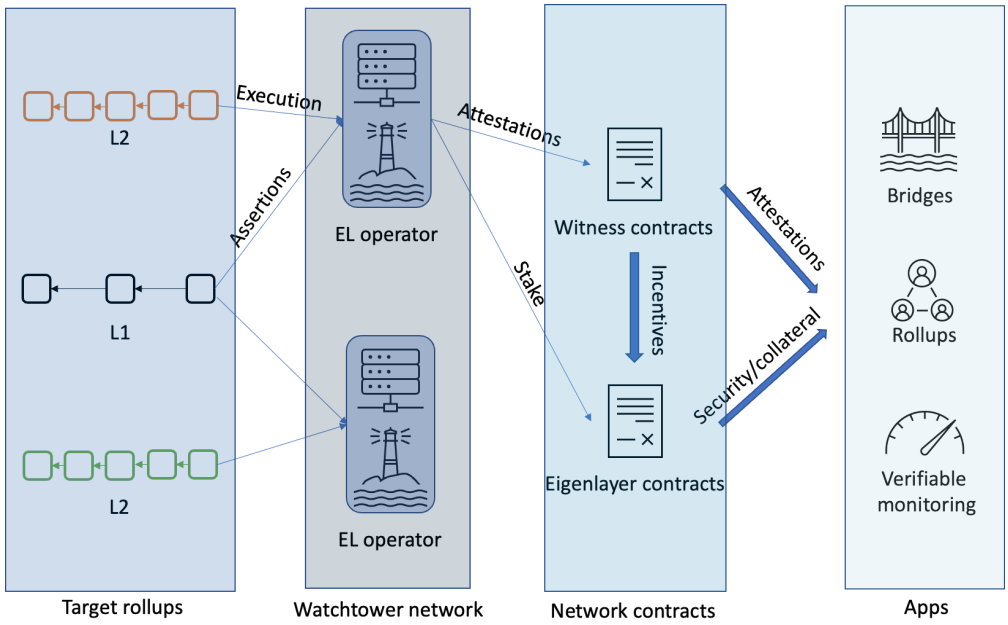
Security for optimistic rollups (ORs) is derived from dispute resolution at L1 for suspicious transactions. The first line of defense is offered by parties who first *identify* suspicious transactions. Currently deployed ORs rely on relatively centralized (and trusted) entities who offer this line of defense; e.g., Arbitrum's state assertion can only be disputed by a set of 12 whitelisted defensive validator nodes.

The surge in demand for app-specific rollups and platforms to support them (e.g., Base and Eigenlayer) results from increasing value and diversity of transactions relying on L2s. In turn, there is a need for decentralized and trust-free validators who *diligently* raise the alarm when they detect a suspicious transaction.

Witness Chain Watchtowers provide the first line of defense for rollups, which is:

1. Trustfree and Incentive Compatible: provides Proof of Diligence of watchtowers with Ethereum trust (through EigenLayer)
2. Decentralized: provides a Proof of Location for verifying the geolocation of watchtowers and enforcing desired physical decentralization.
3. Programmable: provides SLA smart contracts to scale the number/stake of watchtowers and their decentralization properties with the value of vulnerable transactions.

Witness Chain upgrades the OP stack through an in-built Proof of diligence. Such an upgraded OP stack bound by a Witness Chain SLA can be immediately deployed over EigenLayer with full Ethereum security.




# Features of Watchtower Network

## Trust-free and incentive-compatible

Watchtower's main task is to verify state assertions posted on L1; to do so, they need to execute transactions on the Optimistic rollup. If a watchtower is not *diligent* and blindly accepts all transactions, it will be caught by other nodes in the network. However, such adversarial path events are rare for the protocol, and we need to make sure that the watchtowers are incentivized to perform L2 execution even in the happy path. Witness chain's watchtower network deploys an incentive mechanism on a Proof of Diligence that ensures incentive compatibility of execution by enforcing the properties below:

1. *Predictable payout for execution*: The incentive payout for watchtower does not depend on state assertion frauds; hence, watchtowers are incentivized even in the happy/normal path.
2. *Sybil resistance*: Setting up a watchtower pool can help decrease the computing and staking costs for watchtowers. In particular, watchtowers will be validating independently and will get rewards in proportion to their stake. An incentive payout is specific to a watchtower; hence, if one watchtower finds a bounty, they cannot inform other watchers of that exact incentive payout.

Proof of Diligence works through an incentive process reminiscent of Bitcoin mining - watchers get rewarded only if they mine execution bounties, and the only way to mine execution bounties is to execute the transactions themselves.

### Decentralized network

Watchtower network's robustness is enhanced by utilizing Witness chain's Proof of Location mechanism that can be used to provably verify a watcher's location claim. A geographically decentralized network not only ensures robustness from localized attacks but also ensures that the computation happens on different hardware, ensuring independent execution. A watchtower that enrolls in the service can claim a location on the globe, and the Witness chain's decentralized challenger network will verify that claim within a radial accuracy. This is done using network delay measurements between the challenger and the prover, followed by a robust reconciliation algorithm applied to these measurements. The claimed location and accuracy will be fed directly onto a geographical diversity incentivization policy that rewards watchers in less dense locations.

### Programmable security

Optimistic rollups can order a watchtower network in any configuration they desire based on their security needs and value to be secured by signing up for their custom SLAs. Rollups can use their token emissions to pay for the watchtower service; the constraints in the SLA ensure that the payment covers the cost of execution of these watchtowers. The SLA enables the following configuration parameters:

- Watchtower network size - Market dependent/custom
- Watchtower network rotation - Enabled/disabled
- Geographical decentralization config
- The payment amount and insurance bucket size
- SLA term length

Any rollup can enroll in this service by signing the SLA; we will upgrade the watchtower stack to add support for that rollup.

## Integration with Eigenlayer

The watchtower network will utilize Eigenlayer's restaking mechanism to stake the watchtowers and slash them if they deviate from their expected behavior. Watchtower network enables stakers to participate in the L2 economy by providing computational trust and crypto-economic security to L2 transactions. Our staking paradigm allows for a low minimum stake unit and small lock-in periods with an option to provide insurance for high-value transactions. Watchtower network attestations backed by Eigenlayer stake can be used by applications on L2, such as bridges and oracles, to enable secure interoperability across L2s and L1s. Operators participating in the watchtower network will execute transactions on a single rollup. They will get rewarded for their computation by any application utilizing watchtower attestations for their security.