white-paper

Overview

This is the Ronin chain's white paper. As a living document, it's a work in progress and can be updated in the future without prior notice.

Motivation

Decentralization is a key aspect of blockchain technology and one of the most prominent forces of its innovation. Our goal is to gradually increase the decentralization of Sky Mavis's products.

At launch, Ronin used Proof of Authority (PoA) as its consensus protocol. In PoA systems, transactions and blocks are validated by approved accounts known as validators. The PoA protocol, however, is often criticized for being less decentralized than Proof of Stake (PoS) and Proof of Work (PoW).

As the next step toward decentralization, we integrated the Delegated Proof of Stake (DPoS) features such as delegation and validator selection, while retaining an element of PoA.

Consensus

Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is a consensus mechanism where token holders delegate their stake to select validators. These validators verify transactions, produce new blocks, and earn rewards for their work.

Token holders can vote for themselves or delegate stake to a representative. The more tokens a validator receives, the higher their chance of selection. Rewards for producing blocks are shared between validators and delegators (who delegate stake to validators).

In Ronin, a set of validators is selected using DPoS. Then, validators take turns producing blocks in PoA manner. A summary for Ronin's consensus is given as follows:

- The set of *validators* consists of 22 slots, of which 12 are reserved for Governing Validators who are selected in the PoA manner. The remaining 10 slots are open for anyone who wishes to become a validator and meets the minimum staking requirements. These are referred to as Standard Validators.
- Users who registered to become a validator have the role of a Validator Candidate until they're selected to become a Standard Validator.
- The *delegators* delegate their own stake to any validator of their choosing, increasing the validator's chance to be selected as a Standard Validator and earn block production access.
- Selected validators earn the block reward after verifying the transactions in a block, and those rewards are then shared with their delegators.

Validator selection

Any token holder can register as a Validator Candidate. They can also play the role of delegators by staking their tokens to the Validator Candidates. At the beginning of each day, the system updates the staking of validators and delegators. After that, the system selects a set of 22 validators, which includes 12 Governing Validators, and 10 Standard Validators chosen among the Validator Candidates with the highest votes (staked amount).

During the day, some validators might be temporarily removed from the validator set. For example, due to *jailing*, which is a form of slashing, or because of scheduled maintenance. These changes are updated every epoch, where one epoch consists of 200 blocks or around 10 minutes.

Staking and delegation

Token holders who do not have a large enough RON supply to meet the minimum staking requirements on their own, can earn the staking reward and participate in the network as delegators. To do that, a token holder can contribute their RON stake to any validator (Validator Candidate, Standard Validator, or Governing Validator).

Here's the core logic of staking:

- The staking token is RON.
- Token holders (including Governing Validators) must stake at least 250,000 RON to become Validator Candidates.
- Staking takes effect at the beginning of the next day.
- Standard Validators are selected daily from the top 10 Validator Candidates with the highest staked amount.
- Validators can renounce their role and withdraw their tokens (unstake) after a waiting period of seven days.
- Delegators can unstake at any time as long as three days have passed since they last staked in to this validator.

Governing Validators

While increasing the decentralization of the network, the validator selection process via staking also enables a new vector of attacks. An attacker that controls more than 51% of the tokens can take over the blockchain.

The group of 12 Governing Validators chosen by the community and Sky Mavis is meant to help prevent such attacks. Because the Governing Validators take 12/22 slots in the validator set, the attackers cannot control the majority of the validators and take over the blockchain.

Bridge operators

The role of the bridge operator is to acknowledge deposit and withdrawal events to facilitate asset transfers between Ronin and other EVM-based chains. Bridge operators have their own rewarding and slashing logic.

On Ronin, each validator is required to run a validator node and a bridge operator. A validator who doesn't run a bridge operator is not eligible for the block reward.

Security and finality

The Clone attack paper shows that the PoA-based systems can tolerate less than $N/3$ Byzantine validators. To confirm a transaction, the users are encouraged to wait until receiving at least $2N/3 + 1$ sealed blocks. With $N = 22$ validators and block time being 3 seconds, the users should wait for 45 seconds to confirm transactions in a block.

To perform the Clone attack, the Byzantine validators must create two blocks on the same block height, also known as double-sign. This behavior can be detected by other validators in the system. Thus, we use a slashing mechanism to penalize Byzantine validators. This mechanism exposes malicious validators in a short time and makes the Clone attack non-beneficial.

To perform a non-detectable attack—when the Byzantine validators can only seal at most one block on each block height—the attacker must control the majority of validators. Fortunately, the selection of Governing Validators guarantee the majority of validators are honest, thus ensuring the security of Ronin.

Rewards

Out of the total supply of 1,000,000,000 RON tokens, 25% are allocated to fund the staking reward. According to the RON unlock schedule, the rewards are set to be allocated over 108 months.

Rewards for validators and delegators

Validators have two sources of rewards: transaction fees and 90% of the staking reward. When the validator generates a block, they earn the transaction fees in that block and some fixed amount of the staking reward.

- The reward is not sent to the validator right away, but is distributed and accumulated on a smart contract.
- At the end of each day, the smart contract allocates the reward to the validator and their delegators. The allocation happens only to validators who are eligible to receive the reward (not being slashed).
- The validator and their delegators can claim the allocated reward at the end of the day.

Each validator can set a commission rate that indicates the percentage of the self-allocated reward. The remaining reward is allocated based on the staked amount.

For example, consider validator A with the commission rate of 10%. This validator self-delegates 1000 RON. There are three delegators—B, C, and D, who delegate their tokens to validator A with the amounts of 500 RON, 250 RON, and 250 RON, respectively. The total amount of staked tokens to validator A is therefore $1000 + 500 + 250 + 250 = 2000$ RON. If a reward of 10 tokens is given to validator A and their delegators, here's how this reward is allocated:

- Validator A receives $10 \times 10\% + 10 \times 90\% \times 1000 \div 2000 = 5.5$ tokens.
- Delegator B receives $10 \times 90\% \times 500 \div 2000 = 2.25$ tokens.
- Delegator C receives $10 \times 90\% \times 250 \div 2000 = 1.125$ tokens.
- Delegator D receives $10 \times 90\% \times 250 \div 2000 = 1.125$ tokens.

Rewards for bridge operators

Bridge operators receive 10% of the staking reward, which is distributed at the end of each day based on the number of votes from the bridge operators on that day.

Slashing rules

We use a slashing mechanism to penalize validators and bridge operators for malicious behavior.

> ⓘ NOTE
>
> A "day" in the slashing rules refers to the period from midnight to midnight UTC.

Double-sign validator

It's a serious error when a validator signs more than one block with the same height. As mentioned in Security and finality, validators who engage in double-signing effectively launch a Clone attack to break the security of the blockchain. Because our implementation already has a logic to prevent double-signing, only malicious code can trigger this behavior.

Anyone can submit a slash request with the double-sign evidence, which should contain the two block headers with the same height, sealed by the same validator. Upon verifying the evidence, the offending validator is penalized as follows:

- The validator is jailed for $2^{63} - 1$ blocks and can't be a validator in the future.
- The validator is slashed the minimum staking amount of self-delegated RON.
- The validator doesn't earn commission and the staking reward while in jail.

Unavailability validator

The performance of Ronin relies on the ability of everyone in the validator set to produce blocks on time when it's their turn. If a validator misses their turn, it affects the performance of the entire system. Thus, we implemented a mechanism that penalizes validators who miss too many blocks.

We use a smart contract to record the number of missed blocks for each validator. If the number of missed blocks exceeds a predefined threshold, the validator gets slashed.

Tier 1 validator slashing

If a validator misses more than 100 blocks in a day, they don't earn commission and the staking reward on that day.

Tier 2 validator slashing

If a validator misses more than 500 blocks in a day, the following penalties apply:

- The validator doesn't earn commission and the staking reward on that day.
- The validator is slashed 1,000 of self-delegated RON.
- The validator is jailed for about 2 days (57,600 blocks) and is banned from the validator set while in jail.

> ⓘ CREDIT SCORE AND BAILOUT SYSTEM
>
> While we encourage validators to be online and produce blocks in turn, technical issues can still happen. A validator might be well-performing, but if their machine suddenly crashes, they get slashed and jailed. Ronin's credit score system awards validators with credits that can be used to bail out of jail in the event of tier 2 validator slashing.
>
> Here's how this system works:
>
> - Every day, each validator (who is not in jail) is given 50 credits. The maximum number of credits per validator is 600.
> - A validator loses 1 credit for every missed block.
> - A jailed validator can use 2 credits for each epoch to bail out of jail.
> - After getting bailed out, the validator can claim half of the reward for the remaining time of the day.

Tier 3 validator slashing

After getting bailed out, if the validator misses 100 more blocks on the same day, the following penalties apply:

- The reward after bailout is removed.
- The validator is slashed 1,000 of self-delegated RON.
- The validator is jailed for about 2 days (57,600 blocks).

This time, the validator can't bail out.

> ⓘ TEMPORARY MAINTENANCE MODE
>
> Validators can schedule temporary maintenance, during which they don't get slashed for unavailability.

Unavailability bridge operator

The system slashes bridge operators for not providing enough signatures. This is checked against a smart contract that records the number of the bridge operators' votes.

Tier 1 operator slashing

If a bridge operator misses more than 10% votes in a day, the operator doesn't earn the bridge reward on that day.

Tier 2 operator slashing

If a bridge operator misses more than 30% votes in a day, the operator doesn't earn any rewards (commission, staking reward, bridge reward) on that day.

Relaying slash

In addition to producing blocks, Governing Validators are in charge of the following tasks:

- Updating the system parameters, such as slash thresholds.
- Adding or removing other Governing Validators.
- Syncing the set of bridge operators to the Ethereum chain every day.

We require 9/12 Governing Validators' votes to perform the above tasks.

If a Governing Validator doesn't sync the set of bridge operators to the Ethereum chain for three consecutive days, the following penalties apply:

- The validator is slashed 10,000 of self-delegated RON.
- The validator doesn't earn commission on the day of slashing.