Ronin Whitepaper:
An Antifragile Network Built for Billions of Gamers

June 13, 2024

Abstract

Contents

1 Introduction **1**

2 Ronin Infrastructure **3**
2.1 Ronin Consensus . . . 3
2.1.1 Delegated Proof of Stake . . . 3
2.1.2 Block production . . . 3
2.1.3 Finality Voting . . . 5
2.1.4 Rewards . . . 5
2.1.5 Slashing . . . 6
2.2 Ronin ZKEVM . . . 7
2.3 Ronin bridge . . . 8
2.3.1 Ronin-Ethereum Bridge . . . 8
2.3.2 Bridges between Ronin and ZKEVMs . . . 8
2.4 Governance . . . 8
2.5 Security Consideration . . . 9
2.5.1 Ronin Consensus . . . 9
2.5.2 Ronin ZKEVM . . . 9
2.5.3 Ronin bridge . . . 10

3 Tokenomics **10**
3.1 Utility . . . 10
3.2 Ronin Treasury . . . 11
3.3 Economic consideration . . . 11

4 Ecosystem discussion **12**

5 Conclusion **13**

1 Introduction

Blockchain history began with the introduction of Bitcoin in 2008, created by the pseudonymous Satoshi Nakamoto. Bitcoin's blockchain technology enables decentralized, transparent, and secure digital currency transactions without the need for intermediaries. Following Bitcoin's success, blockchain technology evolved beyond cryptocurrencies, inspiring the development of platforms like Ethereum in 2015, which introduced smart contracts—self-executing contracts with terms directly written into code. This innovation opened up numerous applications across industries, from finance to supply chain management. The growth of blockchain has been marked by increasing adoption, regulatory developments, and continuous technological advancements, positioning it as a transformative force in the digital economy.

Blockchain - a path to economic freedom. Blockchain can potentially increase economic freedom by offering an open, global network that allows borderless transactions, ensuring property rights through secure wealth storage and smart contracts, providing unbiased access to financial services regardless of personal attributes, and enabling mobility by facilitating easy transfer of wealth across borders. This decentralized and inclusive system empowers individuals to participate in the global economy without dependence on traditional financial institutions or government control.

However, despite its potential, blockchain has yet to fulfill its promise as a vessel for economic freedom, often serving instead as a playground for speculators and institutional investors. Many projects have been funded without fully considering distribution strategies and competitive advantages, resulting in a lack of practical applicability and widespread adoption.

Ronin's strategy. Ronin takes a fundamentally different approach, we focus our innovation on web3 mechanics, leveraging tokens for user acquisition, and fostering robust community building. We prioritize creating a vibrant, engaged user base from the outset. Initially, Ronin was developed to meet the needs of a single game and its community. This focused approach allowed us to refine our platform and prove its viability before expanding outward.

This strategy mirrors the paths of successful companies like Amazon, which began by selling books before diversifying its offerings, and Apple, which started with personal computers and gradually broadened its product line to include a wide array of consumer electronics. Similarly, Nintendo's initial go-to-market (GTM) strategy for their hardware revolved around the iconic Mario franchise, ensuring a strong foundation before expanding into other ventures.

Permissionless blockchains effectively function as a global app store. Those that can scale their social layer and foster lasting user relationships with high-retention products and services become the largest aggregators of demand. Consequently, developers will naturally be drawn to launch their products and services on these platforms. Axie Infinity, utilizing the Ronin blockchain, became the first GTM strategy for a gaming blockchain, demonstrating the potential for a well-integrated and community-focused approach. Many other gaming blockchains struggle with adoption and lack a dedicated community, exposing them to the common risks faced by most blockchains, advanced technology without a solid user base.

Ronin is designed to bridge this gap between cutting-edge technology and user engagement, with the mission to *onboard billions of users*. By serving as the GTM for the Ethereum Virtual Machine (EVM), Ronin provides a scalable and user-friendly platform that not only supports gaming applications but also fosters a thriving ecosystem of users and developers. Our commitment to community building and strategic user acquisition ensures that Ronin is not just another blockchain, but a dynamic and evolving foundation for the future of web3 applications.

Ronin has established itself as a leading force in the web3 gaming ecosystem, boasting impressive metrics that highlight its widespread adoption and robust community. Dominating the market, Ronin holds an 80% market share among web3 gamers, cementing its position as the go-to blockchain for gaming applications. With 1.3 million daily active users (DAU) and 3.3 million monthly active users (MAU), the platform demonstrates consistent and significant user engagement. The 17 million Ronin wallet downloads further underscore its popularity and ease of use among gamers and crypto enthusiasts alike. Additionally, the network's security is bolstered by 120,000 stakers, reflecting strong community trust and participation.

With this vision, our strategy to create a network effect and leverage initial distribution power to kickstart the flywheel is as follows:

- *State-of-the-art technologies.* We diligently adopt state-of-the-art technologies to construct a decentralized, secure, and scalable infrastructure capable of accommodating billions of web3 users.

- *Economics and incentive driven.* We envision directly connecting the economic activity happening at the application layer with the Protocol. This starts by building a synergistic relationship between the Protocol and dApps where where leading dApps contribute a percentage of their fees towards the growth and maintenance of the entire ecosystem and receive strong goodwill and support from the Ronin community as a result.

- *Vibrant and innovative ecosystem.* In our ecosystem, we prioritize a seamless user experience with innovations such as MPC wallets, social logins, and gas sponsoring. Additionally, we understand

the significance of establishing community building standards, and we actively advise games and dApps on Ronin to enhance community participation and trust.

2 Ronin Infrastructure

2.1 Ronin Consensus

Security and decentralization are two important factors in blockchain. Decentralization in blockchain refers to the distribution of power, authority, and control across multiple participants in a network rather than being concentrated in a single central authority. This fortifies Ronin's security by eliminating vulnerabilities associated with a singular point of failure or control.

However, increasing the level of decentralization often necessitates trade-offs, such as slower response times, decentralized decision-making, and governance processes – all of which may delay the development process. We are operating within the web3 gaming sector, one of the most dynamic industries in the world. Thus, during our early stages, decentralization manifests as a spectrum across different aspects of Ronin. Nevertheless, we are committed to progressively enhancing the decentralization of the Ronin chain as the network matures.

In May of 2021, Ronin began using the Proof of Authority (PoA) consensus mechanism. In Ronin's PoA consensus mechanism, Sky Mavis and its community hand-selected reliable validators to maintain the network and verify transactions. However, the PoA consensus mechanism required an enormous amount of trust in the chosen group of validators. As the next step toward decentralization, in April of 2023, Ronin upgraded to Delegated Proof of Stake (DPoS), allowing everyone to become validators.

2.1.1 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, vote for finality, 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 and voting for finality 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 and vote for finality. A summary of Ronin's consensus is given as follows:

- **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 reputable Governing Validators chosen by the community is meant to help prevent such attacks. Besides Governing Validators, any token holders can register to become Validator Candidates.
- **Block production.** For every epoch (or about every 10 minutes), a set of block procedures are randomly selected to produce blocks. Of which 12 are reserved for Governing Validators. The remaining 10 slots are chosen among the Validator Candidates based on their staked amount.
- **Finality Voting.** All validators can participate in finality voting. The voting weight of a validator is proportional to their staked amount.
- **Delegation.** 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.

2.1.2 Block production

At the DPoS launch in April 2023, 22 validators, including 12 Governing Validators and 10 Standard Validators, are selected daily to produce blocks. The 10 Standard Validators are chosen from the Validator Candidates with the highest staked amounts. However, this design does not incentivize token holders to become Validator Candidates if they cannot make it into the top 10 to become Standard Validators. Additionally, the current requirements for validators are exceptionally high.

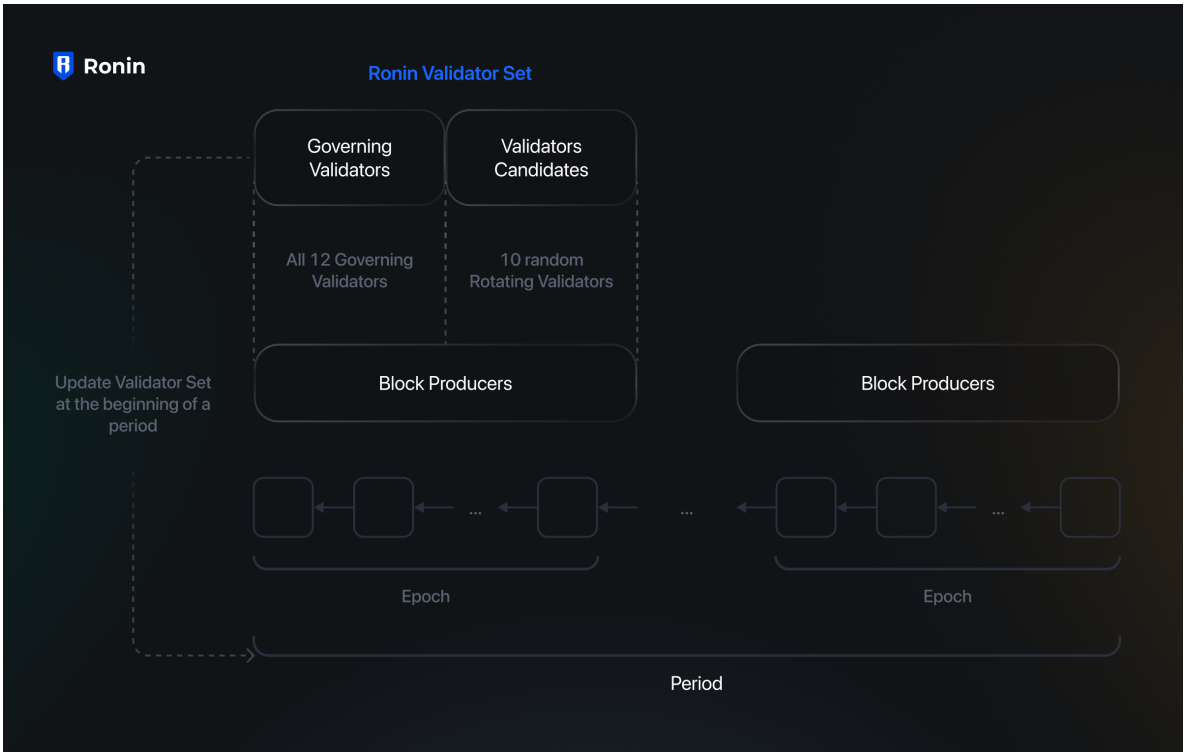

Figure 1: Ronin consensus.

We launch an upgrade to introduce Rotating Validators. With this new design, the validator set responsible for producing blocks will be updated every epoch (approximately every 10 minutes). This upgrade will ensure that all validators have an opportunity to produce blocks and receive rewards, thereby providing greater incentives for token holders to participate as Validator Candidates.

Below is the overview of how block producers are selected in every epoch.

- For each period (1 day), the validators jointly compute a random beacon.
- The random beacon in period $i-1$ will be used to select the validators in period i.
  - In each epoch, 12 Governing Validators and 10 Rotating Validators are selected.
  - Rotating Validators are randomly selected based on the random beacon.
- For each epoch of period i, a set of validators is selected based on the random beacon in period $i-1$ and the epoch number.

Compute random beacon. A verifiable random function (VRF) is a public-key pseudorandom function that provides proofs of its output's correct calculation. The owner of the secret key can compute the function value and an associated proof for any input value. Everyone else, using the proof and the associated public key, can check that this value was indeed calculated correctly. However, this information cannot be used to find the secret key.

The process of computing the random beacon for period i, executed in period $i-1$ consists of 4 steps.

- Step 1: At the beginning of period $i-2$, the Ronin Validator Contract sends the set of Governing Validators to the Random Beacon Contract. At the same time, the Random Beacon Contract sends the random beacon R_{i-1} to the Ronin Validator Contract (this is Step 4 in the previous period).
- Step 2: Each Governing Validator j queries its VRF worker using the random beacon R_{i-1} and obtains the output σ_j and the proof π_j.

- Step 3: Each Governing Validator j submits the output σ_j and the proof π_j to the Random Beacon Contract (via a system transaction).
- Step 4: At the last epoch of period $i-1$, the Random Beacon Contract computes the random beacon R_i and sends it to the Ronin Validator Contract. R_i is computed as the hash value of all outputs of governing validators. The random seed is the output of VRF with the input as the concatenate of the random beacon of the previous period and the current period number.

2.1.3 Finality Voting

All validators have the ability to vote for finality. The weight of their votes based on the staked amount:

- If the staked amount of a validator is smaller than or equal to 1/22 of total stake, the weight is directly proportional to the staked amount.
- If the staked amount of a validator is bigger than 1/22 of total stake, the weight equals 1/22 of total stake.

Validators confirm a block's validity by providing their signatures on the block's hash. If a block receives enough votes, the validators can create a quorum certificate (QC) to attest to the block's validity. The block's QC is included in its direct descendant block.

Validators vote according to the following rules:

- Rule 1: A validator must not publish two distinct votes for the same height.
- Rule 2: A validator always votes for the latest block of its best chain.
- Rule 3: A validator only votes for the block with a bigger block height than its previous vote.

Once the validators vote for a block, the next block producer collects those votes and creates a Quorum Certificate (QC) if the weight of the voted validators is more than 2/3 of the total weight. If the validators cannot collect enough votes before the next block is generated, the QC will not be generated.

The QC will be verified by other nodes in the network. A block containing an invalid QC will be considered invalid. To optimize the size and verification time of QCs, we use the BLS signature scheme. The BLS signature allows us to aggregate the signatures of validators on a block into a single signature. Compared to unaggregated signatures, the aggregated signature can save up to n times the space. Additionally, we can verify the QC of validators with a single signature verification operation.

Finalizing a block involves two steps: justification and finalization.

- A block is considered justified if its QC is included in the header of its direct descendant block.
- A block is considered finalized if it is justified and its direct descendant (in the same epoch) is also justified. If a block is finalized, all of its ancestor blocks are finalized.

In Ronin, validators use the sum of the difficulty field to compare and confirm which chain is the best ancestor to pick. This finality mechanism requires the chain to grow under a new fork choice rule.

- The chain that includes the highest justified block is considered the best chain, even if there are other chains with a higher total difficulty.
- If multiple chains include the highest justified block, the chain with the highest total difficulty is selected as the best chain.

2.1.4 Rewards

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 rewards are divided as follows: 15% for block production and 85% for finality voting.
- 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.

2.1.5 Slashing

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

Double-sign It's a serious error when a validator signs more than one block with the same height. 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 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 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 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.

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.

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 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 cannot bail out.

Double-vote A validator must not publish two distinct votes for the same height. Anyone can submit a slash request with the double-sign evidence, which should contain the two signatures of finality voting of two blocks at the same height. 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.

2.2 Ronin ZKEVM

With a rapidly growing ecosystem, Ronin must be able to support scalability. Out strategy is scaling Ronin with Zero-knowledge (ZK) rollups. ZK rollups use advanced cryptographic techniques known as ZK proofs to validate transactions. The idea is straightforward although the implementation is complex: a rollup verifies a transaction's validity without making any information public. That means transactions can be verified in shorter periods of time, and settled on the mainnet sooner.

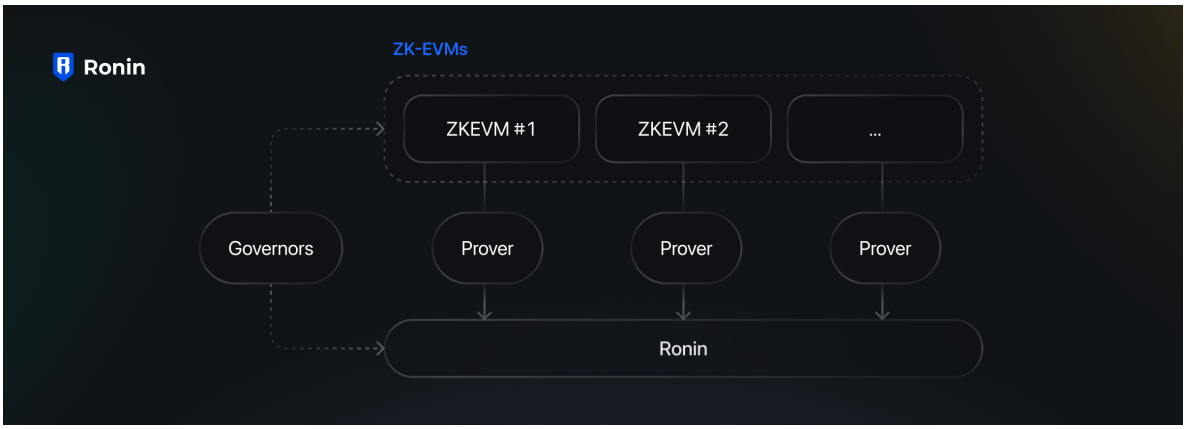

Figure 2: Ronin ZKEVM.

We've seamlessly integrated a ZK prover into Ronin, empowering validators to establish their own ZK-EVMs. Validators can initiate a ZK-EVM by submitting a transaction containing the necessary information for the new ZK-EVM chain. Once initiated, validators must maintain their status and cannot opt out of the validator set.

The upgrade of the ZK-prover version can be facilitated through an on-chain proposal, eliminating the need for validators to upgrade the Ronin version. This feature streamlines the process of upgrading the prover without causing any disruption to the Ronin mainnet. Furthermore, ZK-EVMs have the flexibility in gas token selection. ZK-EVMs on Ronin now offer the freedom to utilize any ERC-20 token available within the network. This presents opportunities for web3 games and dApps, enabling them to customize their ZK-EVM chains according to their specific preferences and requirements, thus enhancing the ecosystem's versatility and accessibility.

In addition, transaction fees on layer-2 are distributed to delegators, aligning incentives for game studios to operate validators and ZK-EVMs. Increased activity on the ZK-EVM results in higher rewards for delegators. This incentivizes more delegators to join the validator, ultimately leading to higher rewards for the validator.

The ZK-EVMs are operated and governed as follows.

- **Sequencer:** Sequencers are tasked with the crucial responsibility of generating blocks. Their role ensures the efficient execution of transactions. To serve as a Sequencer, individuals must hold validator status on the Ronin, demonstrating their commitment to upholding network security and reliability.
- **Prover:** Provers play a pivotal role in the validation process of transactions within the ZK-EVM environment. By generating and submitting Zero-Knowledge proofs to Ronin, they contribute

to verifying transaction integrity. Unlike Sequencers, anyone can assume the role of a Prover, promoting inclusivity and decentralization within the network.

- **Governor:** The Governor, comprised of 12 Governing Validators, serves as the governing body overseeing the ZK-EVM ecosystem on Ronin. Their responsibilities include managing governance processes and decision-making regarding upgrades or modifications. Any proposed changes must undergo an on-chain proposal process, requiring approval from at least 75% of the Governing Validators.

2.3 Ronin bridge

2.3.1 Ronin-Ethereum Bridge

Currently, the bridge between Ronin and Ethereum is managed by 22 bridge operators, ensuring secure and reliable cross-chain transactions. For each transaction, every bridge operator is responsible for verifying its validity and casting a vote to approve or reject it. To ensure a high level of security and consensus, a transaction can only be executed if at least 70% of the bridge operators approve it. This mechanism ensures that transactions are thoroughly vetted and agreed upon by a majority of the operators, reducing the risk of fraudulent or erroneous transfers and maintaining the integrity of the Ronin-Ethereum bridge. This robust system is designed to provide users with confidence in the security and reliability of their cross-chain transactions.

In the future, we aim to further strengthen security by implementing a bridge with a multi-proof system. Specifically, we will retain the current design as one layer of proof and introduce a Zero-Knowledge proof as an additional layer of verification. This enhanced approach will provide multiple layers of security, ensuring that cross-chain transactions are not only verified by the consensus of bridge operators but also validated through advanced cryptographic techniques. By incorporating Zero-Knowledge proofs, we can enhance the privacy and integrity of transactions, making the Ronin-Ethereum bridge more robust and secure for all users.

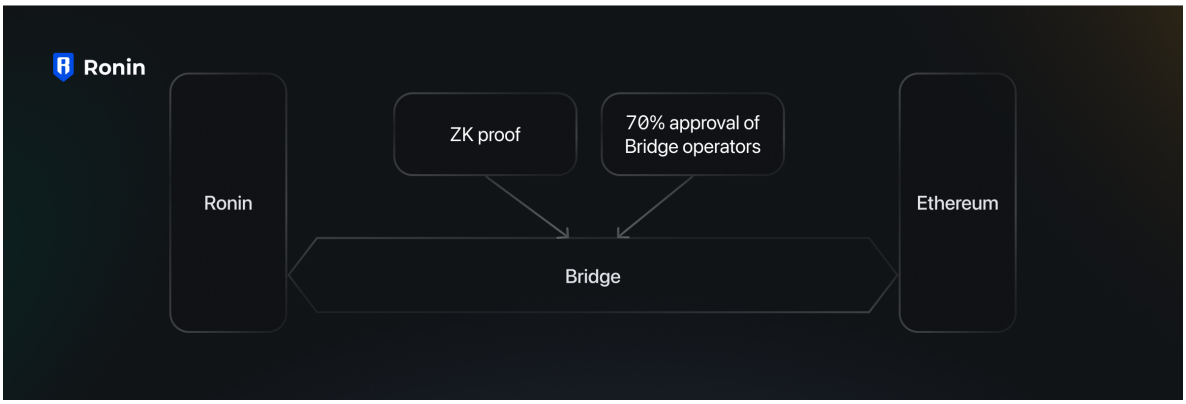

Figure 3: Multi-proof system bridge.

2.3.2 Bridges between Ronin and ZKEVMs

We design a bridge to enable users to execute cross-chain transaction between any chains in the Ronin ecosystem. Similar to Ronin-Ethereum bridge, we use a multi-proof system bridge in the Ronin ecosystem. Executing a cross-chain transaction requires two layers of verification.

- A ZK proof to verify the transaction is valid.
- 70% of the bridge operators to approve the transactions.

2.4 Governance

The Ronin chain operates under the governance of 12 governing validators who manage protocol upgrades and alterations. These enhancements may encompass advancements in the network's security,

scalability, and overall functionality. Within the Ronin ecosystem, any upgrades must undergo an on-chain proposal, necessitating the approval of at least 75% of the governing validators. Decentralized governance ensures that the Ronin ecosystem remains adaptable and responsive to the evolving needs and preferences of its users. By allowing stakeholders to participate in decision-making processes, Ronin promotes transparency, inclusivity, and consensus-driven development.

2.5 Security Consideration

In this section, we analyze the security for Ronin consensus, ZKEVM, and bridge.

2.5.1 Ronin Consensus

A secure consensus protocol must satisfy two properties: safety and liveness. In addition, we will analyze a new property called fast finality.

- Safety. If a block is finalized, it cannot be reverted, i.e., two blocks in different forks cannot be finalized.
- Liveness. New blocks will be added to the chain after some certain time.
- Fast finality. A block will be finalized after 2 blocks.

Safety. If the weight of honest validators is at least 2/3 of the total weight, then two blocks in different forks cannot both be finalized.

Let m be the total weight of all validators and k be the weight of honest validators. First, we show that two blocks a_i and b_i (which are in different forks and at the same block height) cannot both be justified. Assume toward contradiction that a_i and b_i are both justified. In this scenario, the voted weight on a_i and b_i are more than $2m/3$. Since the weight of malicious validators is $m - k$, the weight of honest validators who voted on a_i and b_i are at least $k - m/3$. Therefore, the total number of votes from honest validators for a_i and b_i is at least $2k - 2m/3 > k$. However, since honest validators can only vote for at most one block at a given block height, this case cannot occur.

Next, we show that blocks a_i (at block height i) and b_j (at block height j), which are in different forks, cannot be finalized. Assume, for the sake of contradiction, that two blocks a_i and b_j are in different forks and are both finalized. Without loss of generality, assume $i < j$. Let a_{i+1} be the direct descendant block of a_i. As a_i is finalized, a_{i+1} is justified. Since two blocks at the same block height cannot be both justified, we have $i + 1 < j$.

As a_{i+1} is justified, the weight of honest validators who vote for a_{i+1} is $k - m/3$ (as a justified block needs at least $2m/3$ votes). In the views of those validators, the highest justified block will be a_i. Those validators have not voted for block b_j (based on Rule 2). Plus, based on Rule 3, they will not vote for any blocks that are not descendants of block a_i, which includes b_j. Therefore, there are at most $4m/3 - k < 2m/3$ validators who vote for b_j. Hence, block b_j cannot be justified, leading to a contradiction.

Liveness. If at least $\lfloor n/2 \rfloor + 1$ (= 12, when $n = 22$) validators are honest and online, they are able to continue producing blocks. As the Governing Validators are always selected to produce blocks, this is guaranteed.

Fast finality. When the weight of honest validators is at least 2/3 of the total weight, and all votes from the honest validators are received within 3 seconds (the block time) by the next validator, then every block will be justified after 1 block. Consequently, every block will be finalized after 2 blocks.

2.5.2 Ronin ZKEVM

As the Prover continuously submits Zero-Knowledge (ZK) proofs of transaction execution from the ZKEVM to Ronin, the ZKEVM effectively inherits the robust security measures of the Ronin network. This ongoing submission process ensures that each transaction executed within the ZKEVM is verified and validated through Ronin's established security protocols. Consequently, users and developers can trust that the ZKEVM maintains the same high level of security as the Ronin mainnet, providing a secure environment for decentralized applications and transactions.

2.5.3 Ronin bridge

Each cross-chain transaction on the Ronin network undergoes a stringent two-step verification process to ensure its security and integrity. The first layer involves generating a Zero-Knowledge (ZK) proof to confirm that the transaction is valid. This cryptographic proof ensures that all transaction details are correct. The second layer requires approval from 70% of the bridge operators, who are trusted entities such as Google, Animoca Brands, Nansen, and others.

To compromise the Ronin bridge, an attacker would face significant hurdles. Firstly, they would need to gain control of at least 70% of the bridge operators, which is a formidable task given the reputable and diverse nature of these operators. Secondly, the attacker would either need to compromise the Ethereum network itself, which is highly secure and decentralized, or identify a critical vulnerability within the ZK proof system. These combined requirements make the Ronin bridge highly resilient against attacks, ensuring the security and reliability of cross-chain transactions.

3 Tokenomics

RON is the native utility token of the Ronin blockchain. RON was launched in JAN '22, with no private sales conducted. 10% of the total token supply was distributed over 90 days to community members who contributed liquidity on the Katana Decentralized Exchange[1].

3.1 Utility

RON has multiple utilities as follows.

- **Gas fees:** RON is used to pay for transactions on Ronin.
- **Staking:** Users can stake RON in the Delegated Proof of Stake consensus
  - RON is staked by validators to run a validator node and validate blocks for rewards.
  - RON is delegated to validators by users to further increase the economic security and earn a share of rewards.
- **Governance:** Holders may participate in network governance decisions in the future and influence usage of the Ronin Treasury which receives fees from decentralized applications like DEXes and NFT marketplaces.

Other than the base utilities built into the protocol, RON is positioned as the central token within the broader ecosystem of decentralized applications built on Ronin.

- **Medium of Exchange:**
  - RON has the deepest onchain liquidity and widest distribution of holders
  - RON is paired with every new token for liquidity provision on decentralized exchanges.
  - RON is the transaction currency on NFT Marketplaces
- **Gaming Revenue & Payment Token:** Games built on Ronin commonly use RON as payment currency for key revenue sources such as game item purchases, NFT mints and Token sales.
- **Exclusive Opportunities:** Stakers and Holders of RON have received airdrops, whitelist opportunities and launchpad allocations for token launches by projects building on Ronin.

[1] https://blog.axieinfinity.com/p/katana

3.2 Ronin Treasury

Ronin's mission to acquire billions of users will require the continuous and long term support of a deep war chest. We envision directly connecting the economic activity happening at the Application layer with the Protocol. This starts by building a synergistic relationship between the Protocol and dApps where leading dApps contribute a percentage of their fees towards the benefit of the entire ecosystem and receive strong goodwill and support from the Ronin community as a result.

Ronin encourages this incentive structure via social consensus and also via technical features towards the Treasury. The first flagship Decentralized Applications like Katana DEX and Mavis Market have set the standard for dApps to contribute a percentage of fees to the Treasury. The Protocol can start to activate Treasury assets towards the key goals of the protocol and its users and developers.

The characteristics of a well functioning Treasury and Treasury management function on Ronin include but are not limited to:

- **Self-sustaining funding mechanism:** Contributions to the Treasury must outweigh spending.
- **Clear goals for Treasury spending:** Direct benefit to a significant amount of users, dApps and achieve long term protocol goals.
  - Public goods funding such as oracles for pricing, and maintenance of multisig wallet infrastructure.
  - Gas sponsoring for onboarding new users.
  - Buyback & burn or buyback & make models.
- **Optimized for decentralized decision making:** Which means less operationally heavy workloads and governance decisions.
  - *Simplicity.* Choose to make decisions that are easily understood to scale social consensus - simple rules that the majority should be able to support.
  - *Accountability.* It should be easy for any community member to publicly track progress and see if objectives and key results are being met.

3.3 Economic consideration

The intention of this section is to provide commentary on significant protocol features that have economic impacts on the RON Token. The Ronin Protocol aims to follow best practices from other blockchain ecosystems, design and support innovative solutions that create more demand for the RON token and encourage economic activity on Ronin.

EIP-1559 for Ronin. EIP-1559 gets rid of the first-price auction as the main gas fee calculation. In first-price auctions, people bid a set amount of money to pay for their transaction to be processed, and the highest bidder wins. With EIP-1559, there will be a discrete base fee for transactions to be included in the next block. For users or applications that want to prioritize their transactions, they can add a "tip", which is called a "priority fee" to pay a miner for faster inclusion. In Ethereum's case, the protocol has chosen to burn all base gas fees. Since ETH has an infinite supply, introducing a burning mechanism helps make ETH scarcer, thereby benefiting holders and aligning with the ethos of being credibly neutral. For RON, which has a capped supply, we plan to direct the base gas fees to the Ronin treasury.

ZKEVM Sequencers stake RON. Sequencers for ZKEVMs are required to be Validators on the Ronin base layer and will need to stake a significant amount of RON. This alignment between Ronin validators and zkEVM sequencers is significant as Maximal Extractable Value (MEV) captured on the L2s is distributed to L1 Validators and Delegators. Ronin zkEVMs thus, have skin in the game to make decisions with the Ronin base layer in mind. As more chains are created on top of Ronin, demand for RON increases proportionally.

Treasury Buyback. Fees accumulated in the Treasury can be used to buy back RON from the market. This connects the value generated by the ecosystem to the wider market of token holders, forming a long term alignment between dApps, protocol, and users.

4 Ecosystem discussion

Ronin's goal is only achievable through a vibrant and innovative ecosystem of infrastructure, products and socially enforced standards.

Frictionless onboarding experience. Our approach to onboarding new users balances convenience, security, and choice. For example, the Ronin Wallet allows anyone to access and manage their blockchain address on Ronin using seedphrases, MPC/keyless technology, and social account logins. These options reduce barriers of entry while ensuring users' ability to self-custody their private keys. Users can also sponsor each other's gas fees, which further eases the burden of onboarding to a new ecosystem.

Standards for community building. We encourage projects on Ronin to build sustainable communities. For example, we advise teams to ensure they've fulfilled any promises made during mints before expanding offerings. We also recommend the implementation of reward designs that incentivize loyalty and dApps that contribute to the Ronin Treasury. Together, these strategies build trust over a long time horizon, which promotes economic stability throughout the Ronin ecosystem.

Ecosystem security. The security of Ronin's ecosystem involves a combination of hard guardrails and adaptable guidance. For example, we ensure all Ronin smart contracts undergo rigorous testing and auditing before deployment. We also maintain a robust bridge to Ethereum and are integrating zero-knowledge proofs to scale the network. At the same time, our trusted domain system alerts users of potential risks, while our collaboration with other game developers produces an ever-evolving understanding of industry best practices. Security is a spectrum. We adjust our comprehensive perspective to create the most secure and trustworthy ecosystem possible.

Ecosystem loyalty and reputation-based rewards systems. We are interested in building an ecosystem that rewards users for their contributions. This encourages sustainable engagement among existing users while incentivizing the accrual of new users. Reputation must therefore be earned – it cannot be feigned. It also serves as a buffer against botting, which is why we must strike a careful balance between decentralized identity standards and proof of humanity. The second-order effects of these considerations will lead to higher-quality incentive designs that benefit users with the strongest reputations in our ecosystem.

Data Ownership powers Web3 Performance Marketing. We encourage user ownership of data while supporting privacy preservation. Users who own their data can choose to monetize it by sharing with advertising platforms. The eventual establishment of wallet personas can help connect advertisers with their intended audience. This increases their spending efficiency while enabling targeted reward strategies benefitting users.

Interoperable ecosystem between Ronin and Ronin ZKEVM. While Enshrined zkEVMs support scalability, they introduce potential for fragmented ecosystems. For example, users might need to use an overwhelming number of chains if every game or dApp launched its own rollup. This may be more than an inconvenience: it can spread liquidity too thin and result in high slippage fees during token swaps. As a result, we've introduced the Cross-Chain Relayer Service to address this challenge.

The Cross-Chain Relayer Service facilitates cross-chain transactions including token and NFT transfers and swaps across various rollups. The Ronin Bridge's design ensures that the Cross-Chain Relayer Service only executes transactions as intended by the user. In a single transaction, users would be able to interact with smart contracts across zkEVM chains.

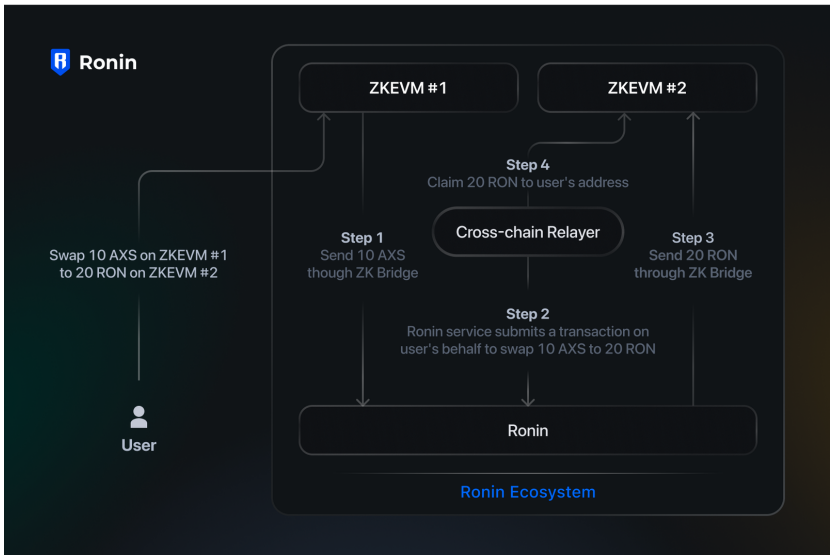

Figure 4: Swapping 10 AXS on zkEVM Chain #1 for 20 RON on zkEVM Chain #2.

We've also upgraded Ronin dApps like the Katana DEX and Mavis Market to support cross-rollup bridging. Here are a few example of cross-chain activities that users would be able to do in a single transaction:

- Transfer tokens to any chain in the Ronin ecosystem from their Ronin Wallet.
- Swap tokens between any chain in the Ronin ecosystem on the Katana DEX.
- Buy and sell NFTs across any chain in the Ronin ecosystem through Mavis Market.

For example, imagine a user wants to swap 10 AXS on zkEVM Chain #1 for 20 RON on zkEVM Chain #2. They could initiate a single transaction and the Cross-Chain Relayer Service will facilitate the rest of the process seamlessly.

5 Conclusion

In conclusion, the journey of blockchain technology towards fulfilling its promise of economic freedom has been fraught with challenges, often overshadowed by speculation and institutional interests. However, Ronin stands apart with its commitment to a fundamentally different approach. By prioritizing web3 mechanics, leveraging tokens for user acquisition, and fostering robust community building, Ronin diverges from the conventional tech-first mentality.

Ronin adopts a focused strategy that emphasizes refining its platform and proving its viability before expanding outward. This approach has culminated in Ronin becoming the go-to blockchain for gaming applications, boasting impressive metrics that underscore its widespread adoption and robust community. With security, scalability, and ecosystem support at the forefront of its goals, Ronin is poised to continue its trajectory as a leading force in the web3 gaming ecosystem, ensuring a dynamic and evolving foundation for the future of decentralized applications.

Disclaimer: The visions outlined in this whitepaper are proposed by the authors and may not necessarily be implemented on the Ronin. Any development or changes to the Ronin blockchain protocol must receive approval from the validators.