User governed oracle and forecast protocol built on Polkadot

Adawi, Marsel
marsel@optionroom.finance

Najjar, Nasser
info@optionroom.finance

Version 1.0.0

Abstract

OptionRoom is a user governed oracle and forecast protocol built on Polkadot. OptionRoom has the ability to serve as a OaaS - Oracle as a Service where oracle requests are solved by governance. Oracle requests cost a fee and a solution incentive paid in ROOM, rewarded to request solvers. OptionRoom allows users to create and participate in event derivatives that are pegged to real world outcomes by governance consensus. Introducing a dual token model with a utility token (ROOM) and a governance token (COURT). COURT tokens are obtained by providing liquidity/staking ROOM, while ROOM tokens are rewarded to protocol participants. COURT tokens are staked into governance for voting power determined by authenticity score - amount of time staked. Honest governance participants are rewarded with ROOM tokens while dishonest participants are punished by token slashing and authenticity score reset. Protocol fees power a buyback mechanism.

Contents

1 Our Vision

- OaaS - User governed oracle as a service
- User incentives for protocol and governance participation
- Limitless and user governed forecast markets and polls
- Polkadot/substrate integration once synthetic assets go live
- A self sustainable protocol
- Removing barriers for entry: dAPP UI that is simple and user friendly

2 Protocol mechanics

2.1 OaaS - User governed Oracle as a Service

Anyone can create an oracle request by paying the oracle request fee (in ROOM) and allocating ROOM as rewards to the request solvers. Requests appear in the oracle governance section of the dAPP. Governance participants with staked COURT and voting rights participate in solving these requests.

The oracle request creator sets a confidence threshold in form of minimum number of voting participants, minimum number of votes and a percentage vote threshold.

If the oracle request is solved successfully meaning it fulfils the request creator criteria, the rewards are split across the winning votes based on their voting weight over the total voting weight for that request. Losing votes are taxed a percentage of staked COURT and their authenticity score gets reset. The percentage is to be announced before protocol launch.

In case the oracle request fulfilment criteria aren't met, the oracle request creator gets to choose between withdrawing their ROOM, or to re-submit the request. The request creation fee isn't refunded. Bigger rewards for request solvers mean faster and more accurate request results.

2.2 Forecast market creation

Forecast markets proposals are created by paying the contract deployment cost. The user has to input:

- A string condition, a proposition which takes the answers (yes/no)
- Market expiry date
- Lock timer

2.3 Market validity voting

After a user creates a market it is put to validity voting. The validity voting starts in the current epoch if epoch time remaining is over 50% [5.1]. Market validity voting lasts until epoch current expiry and voting is done in COURT. The address that created the market is not allowed to vote. Voting mechanism is as described in section [6], the acceptance threshold is set at 51%.

Market validity voting has two outcomes:

1. In case a market is found to be invalid, the pool gets discarded.
2. Market is found valid and is taken to the bidding stage.

Voting participants get awarded ROOM tokens for participating in market validity governance in both outcomes. There is no penalty for voters on the losing side. The reward formula is described in [5.3]

2.4 Market participation (bidding stage)

On a successful validity vote the market is added to the pool list on the main page of the dApp.Users can choose to participate in market pools that are currently in the participation stage. Odds are calculated based on ratio of the pool. Deposit fee is set at 0%. To combat spoofing and last minute withdrawals, OptionRoom has a withdrawal fee of 0.5%. This fee goes toward filling the reward buffer pool.

Users receive yes/no participation tokens by participating in the pool in a 1:1 ratio relative to their contribution. Each pool generates a set of 2 tokens a (yes) token and a (no) token. At the settlement of each pool, the winner tokens will be used to claim winnings based on this equation:

$$\text{POOL}_{\text{usdt}} = \text{USDT in market pool after taking fees out}$$

$$\text{Claim Amount} = \frac{UserTokenAmount}{TotalTokenAmount} * POOL_{\text{usdt}}$$

These tokens are transferable, giving the market participants the opportunity to trade their positions after the market pool is locked. Participation token deploy-er will be triggered on market creation. Token minting is done on contribution deposit by the market participant. The participant receives participation tokens proportional to their bid on a successful deposit. To withdraw their contribution they will need to deposit back the participation tokens. The tokens are burned in the same transaction and a withdrawal fee is taken.

2.5 Market locking (bidding stage)

An active pool is locked when the expiry timer set by the pool creator runs out. Pool stage changes to locked. Users can't deposit/withdraw contributions from locked pools till the market settles. If the market is lacking sufficient contributions on lock, it gets canceled and the original contributors can claim their deposited contribution at any time using their participation tokens.

2.5.1 Market position trading

Position trading interface/marketplace functionality/maturity phase in version 2 of the protocol. See road-map [8]

2.6 Market settlement

If no claim proposals are filed before market expiry, the market is put into the governance portal for a settlement vote. A proposal will be automatically made to decide on the outcome of the current market. Users vote if the market expired as a win or a loss. The consensus threshold is set at 66%. Polls not reaching the consensus threshold are re-cast. To understand how OptionRoom is planning to prevent fraudulent votes and manipulation read [7].

2.7 Market settlement claim proposal

Users have the ability to create a market claim proposal if they believe the market condition has been met before expiry. The proposal is put into current epoch voting if epoch remaining time is over 50% and moved into the next epoch if less time is remaining. Voting and governance consensus is described in [4.1] and [6].

2.8 Market settlement dispute proposal

After a market has reached the market settlement voting threshold, there is a 1 epoch window for users to create a dispute proposal. The tokens of the governance participants that voted on the market settlement vote get locked for the time of the dispute. This is in case participants believe the market settlement vote outcome was invalid and market settled differently in the real world. There is a minimum requirement of 0.5% total supply of COURT staked to create a dispute. The dispute creator gets rewarded 50% of the losing side slashed tokens from the disputed pool. If the dispute is found to be invalid, the dispute creator loses 100% of COURT tokens staked. This is to prevent protocol manipulation. The dispute proposal is open for 1 epoch.

2.9 Protocol mechanics summary

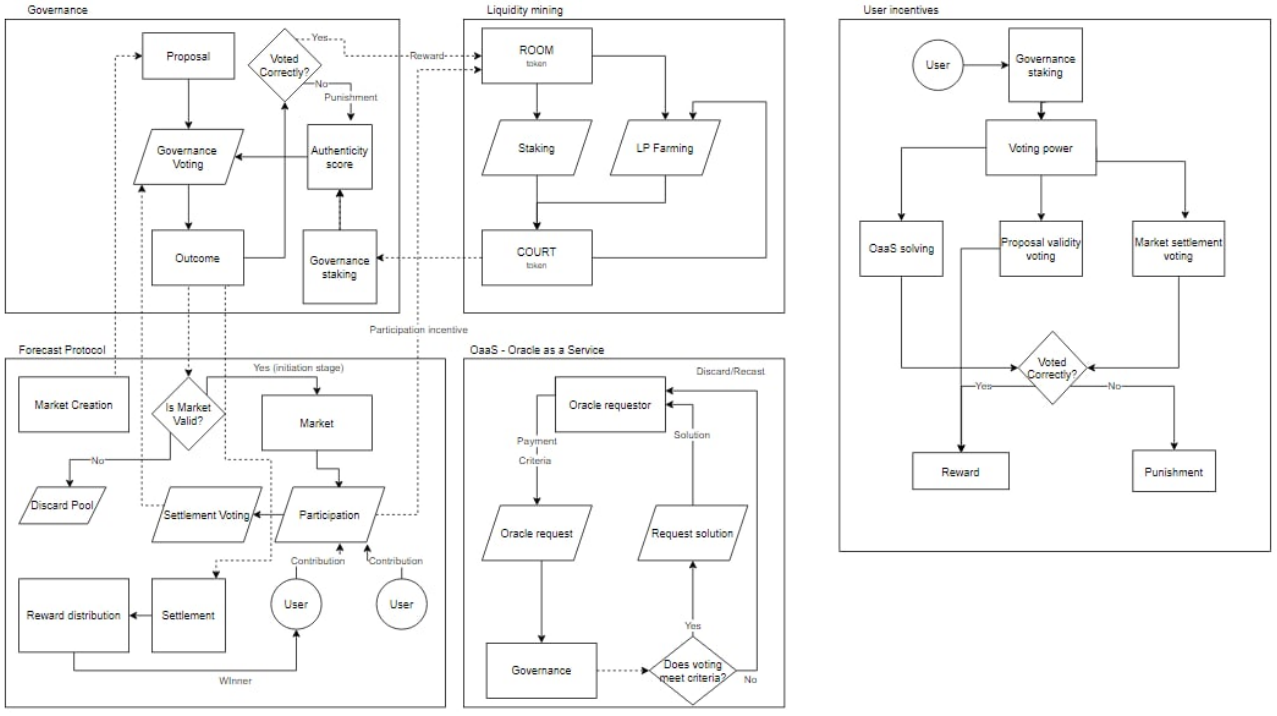

Figure 1: Protocol mechanics summary

3 Token mechanics

We are introducing a dual token system consisting of two tokens:

ROOM & COURT

ROOM is the utility token in the OptionRoom ecosystem. It is given as rewards for participation in the protocol. The daily epoch inflation mechanism is described under token distribution [5.3].

COURT is the governance token for the protocol, users stake their COURT tokens getting the ability to vote on the market validity, market settlement and governance proposals.

3.1 COURT governance voting

COURT is the governance token which is used to participate in protocol governance. By locking COURT in governance users get the ability to vote on oracle requests, market validity, market settlement, and governance proposals.

Each user gets assigned an authenticity score (A). This score ranges from 0-100 based on the number of days staked. The maximum A is 100. A user can reach maximum A after 100 days of staking which is estimated to take around 650,000 blocks.

$$c = COURTstaked$$

$$VoteWeight** = c + c(A/50)$$

1. User locks up COURT for the minimum maturity period of 24 hours
2. User gets assigned a vote weight
3. User can cast votes on multiple proposals simultaneously

Losing side of the vote loses half of their COURT tokens (50%) and their authenticity score (A) gets reset to 0.

3.2 COURT governance rewards

OptionRoom is introducing a 3 pool system:

- **Pool 1:** LP for ROOM:USDT receive COURT
- **Pool 2:** LP for COURT:USDT receive COURT
- **Pool 3:** Stake ROOM receive COURT

Distribution of COURT block rewards is as follows:

- **Pool 1:** 3/7
- **Pool 2:** 3/7
- **Pool 3:** 1/7

4 Protocol reward mechanics

4.1 Epochs

OptionRoom divides physical time into epochs that the protocol runs in. Each epoch runs for around 24h - 6500 blocks.

4.2 Epoch rewards

ROOM rewards are disbursed by the protocol at the end of every epoch as incentives for governance participation. Each epoch has a ROOM reward allocation of 54,794 tokens.

4.3 Governance rewards

ROOM are distributed for participating in governance as follows:

- 54,794 tokens per epoch
- 2/6 Pool validity voting = 18,264 tokens per epoch
- 3/6 Market settlement = 27,397 per epoch
- 1/6 Pool participation rewards = 9,132 per epoch

4.3.1 Pool validity voting rewards

Pool validity voting reward (PVR): 18,264 tokens per epoch. Vote weight [4.1].

Voter Side Ratio (VSR) = 0.6 for the winning side / 0.4 for the losing side
Pool Reward ratio (PRR) = 1 / Number of pools in current epoch

$$\textbf{Voting Reward} = PVR * PRR * \frac{VoteWeightofvoter}{TotalVoteWeight} * VSR$$

4.3.2 Market settlement rewards

Pool Settlement Reward = 27,397 per epoch We use vote weight [4.1].

There are two ways a market can settle:

1. Market pool expires - first person to claim the pool (create the market settlement proposal) gets the pool settlement reward. (Creator pays the proposal creation fees + gas fees)
2. User creates a claim proposal before pool expiry. (Creator pays the proposal creation fees + gas fees)

Market settlement proposal creator gets a percentage of the pool settlement reward dedicated to the pool while the remaining percentage is divided between the voters as to the formula below:

Number of pools settling this epoch = PSn

Pool settlement reward ratio = PSr

$$PS_r = \frac{1}{PS_n}$$

Market settlement Voter Reward $= PS_r * PoolSettlementReward * \frac{VoterWeight}{TotalVoteWeight}$

Losing side loses 50% of their COURT and their authenticity score gets reset to 0.

4.3.3 Pool participation rewards

There are 9,132 ROOM per epoch as pool allocated as participation rewards.

The formula for pool participation rewards is as follows:

$$Pool_{\text{reward}} = \sum_{d=start_{\text{epoch}}}^{end_{\text{epoch}}} \frac{\frac{1}{6} Reward_{\text{d}} * Pool_{\text{volume}}}{LockedUSDT_{\text{d}}}$$

Winning side reward (SR) = 60% of the total reward

Losing side reward (SR) = 40% of the total reward

$$Poolrewardratio(PRr) = \frac{1}{PL_e} \quad Poolweightratio(PWr) = \frac{currentpoolUSDT}{totalUSDTinlockedpools}$$

$$Contributionweight(CW) = \frac{contributedUSDT}{totalUSDTinthecurrentpool}$$

$$\underline{\text{User reward} = SR * PW_r * CW * PR_r * Pool_{\text{reward}}}$$

4.4 Governance rewards buffer pool

In case the settlement fees generated from the pool exceed the rewards allocated for that pool, the rest of the ROOM tokens generated by the buy back will be stored in a buffer pool for future rewards.

Once a settlement on a pool is reached and there's not enough settlement fees to cover the voting rewards, the rest of the rewards will be taken from the buffer pool, this mechanism is used to reduce the daily inflation of ROOM token.

4.5 Buyback mechanism

Each market settlement has a fee of a percentage of the winnings from which a part is used to buyback ROOM tokens from open market. Withdrawal fees and other fees are also included in this buyback mechanism.

4.6 Farming rewards and COURT token

- COURT initial circulating supply: 1 COURT
- COURT max supply 500,000 COURT
- COURT per block in the first 30 days: 1 COURT
- COURT per block thereafter: 0.1 COURT

Pool 1 and 3 provide 1/3 of the total COURT block rewards while Pool 2 has 2/3 of the block rewards.

4.7 Pool odds mechanics

Pool odds are calculated based on this formula:

$$\text{Odds calculation: Odds(x)} = \frac{Contribution(x)}{TotalContribution}$$

When a user adds a certain contribution to a pool, the new odds are calculated in real time based on the following formula:

$$\text{New odds: Voting Odds(x)} = \frac{CurrentContributions(x) + UserContribution(x)}{TotalContributions + UserContribution(x)}$$

5 Governance and voting

Governance is the cornerstone of the OptionRoom protocol, it serves as a means to create a truly decentralised forecast markets platform, by allowing token holders to vote for pool outcomes.

The governance system is designed to discourage voting manipulation in certain cases where the outcome is not speculative.

5.1 Governance system

A proposal needs to be submitted by a user in order for the voting to happen. Once a user has created a proposal, it becomes visible on the governance page for the users to vote on. Users then decide the outcome of the proposal by voting with their locked COURT tokens.

5.2 Voting threshold

There is a minimum ratio of votes that is needed for a proposal to pass. For market validity voting this threshold is set at 51%, for market settlement voting this threshold is set at 66%. For normal proposals not related to markets the threshold is also set at 51%. For market validity voting if the vote threshold isn't met the proposal gets re-cast.

6 Protocol risks & preventing bad actors

6.1 Address blacklisting

If any evil actors are found to be abusing the system, the foundation can decide to blacklist an address. This will always be put to vote by governance first.

6.2 Losing side market settlement voting

Based on section [5.3.2] users who vote wrong on the market settlement voting lose 50% of their stake COURT in addition to getting their authenticity score reset to zero, effectively reducing their voting power. Since market outcome is a clear fact, monetary loss is a valid response to those who try to manipulate the market outcome.

6.3 Audits

OptionRoom takes contract security seriously, therefore the following steps will be taken to ensure the maximum protocol security:

- A bug bounty program, with rewards to hackers who are able to find bugs in the contracts.
- A professional audit will also be conducted before protocol launch.

6.4 Risks

Usage of the OptionRoom protocol carries risks, some of which are listed in the sections below.

6.4.1 Internal risks

Smart contracts may contain bugs. OptionRoom developers will do their best to make sure that smart contracts work as intented but this can't be guaranteed.

OptionRoom is an experiment in beta, do not deposit funds you can't afford to lose.

In terms of consumer side risks, there is always the possibility of a bug or hack of a user's browser or OS which could cause a loss of funds.

6.4.2 Impairment risks

The Ethereum Virtual Machine: If the EVM fails or breaks, OptionRoom will break. This is extremely unlikely as such a bug would break the entire Ethereum ecosystem.

6.4.3 Tax disclaimer

We cannot provide tax or accounting advice. Tax regulations are specific to the jurisdiction where you or your company reside. For any legal or tax matters we recommend consulting your own attorney.

7 Roadmap

ROOM is planned to be unlocked and trade-able in January 2021. OptionRoom is planning to launch COURT mining in March 2021. Protocol launch is scheduled to be in early Q2 2021 on Etherium in addition to smart contract audits and reward reduction phase. OptionRoom is planned to be ported to Polkadot in Q3/Q4 2021 depending on the timeline of synthetic asset solutions in the Polkadot ecosystem.

Q4 2020:

- Concept
- Phase 1 research
- Funding round

Q1 2021:

- Development Phase 1: MVP
- Token Generation Event: ROOM
- Staking Launch v1

Q2 2021:

- Protocol Launch
- Governance Portal Launch
- Bug Bounty/Audits
- Staking Launch v2

Q3 2021:

- Polkadot integration
- Protocol launch v2

8 Team & Advisors

- **Marsel Adawi**: Software Developer with 5 years of experience, 3 years experience in blockchain development. Full time trading/arbitrage bot developer for the past 3 years.

- **Tareq Doufish**: Senior developer and team lead with more than 15 years of experience. Co-founded PinchPoint, a mobile gaming company for four years. Previously: World Bank, Milan innovicy, and Tailormed

- **Nasser Najjar**: Senior team lead with more than 18 years of experience in software development industry, having extensive portfolio of experience, education, and technical abilities. Previously: INTEL, Mellanox, Microsoft

- **Wajed Afaneh**: Senior technical team lead with more than 8 years of experience in System design & Architecture, Previously: Argus, Via, and HighCon

Advisors:

- **Jack Lu**: Managing Director, NGC Ventures. Co-founder of Bounce Finance
- **Chris Tom**: Founding Partner, NetZero Capital