The Dispute Protocol (TON Realization) v0.1

Ilya Mikheev

28/05/2024

Executive Summary

It's said, that majority of people are exited at participating in polls. The aim of this protocol is to create an opportunity to make decentralized polls where you are not relying on the third party. Anyone could create a pool and choose referee that is trusted by all of participators and bet without a fear to lose their money because of bans on third party platforms. Your bets are protected by the smart contract and that is the future of betting in particular and, of course, for polls and disputes in general.

Revision History

Revision	Date	Author(s)	Description
v0.1	21.03.2024	Mikheev Ilya	First draft

Contents

1 General overview

The Dispute Protocol (TDP) is an opportunity to create decentralized polls where anyone could set conditions of the dispute and pick judges by his own choice. After creating this poll is free to access for anyone who agree with the terms of creator (and want to bet some money). In this section we will review the interface of our polls. We'll go through an average user's story (from creating a poll to claiming rewards).

1.1 Creation

To create a poll you should fill this fields and deploy the contract:

ID Here you should pass a random number in order to be sure that your contract code is unique.

Name Name of your poll. Something brief and clear.

Description Some clarification if needed.

BetUntil Time when betting is closed. Passed in unix time in seconds

Referees List of referee's wallets. They would be judges in this poll.

Outcomes List of outcomes. Now amount is limited due to UI and commissions reasons

Duration The duration of this poll. If there would be no consensus after this time all players could take their bets back

After deployment all players could participate in this poll by sending messages to the contract.

1.2 Betting

There is an opportunity for all players to participate in polls. You should pass the message with outcomeID (PlayerBetInit type) to the contract you want to interact with. The value of this message is value of your bet. For example: if you send 7 toncoins with outcomeID 0 that means that you make a bet of 7 TON to the first outcome (numeration of outcomes starts from zero). In reply of your message you would see betID - unique identifier of your bet. Save it to claim your prizes. Remember, that you should place your bet before time of BetUntil variable comes.

1.3 Voting

Referees were chosen by dispute creator to vote for the right result (according to their opinion). To vote they should pass message with their refereeID and outcomeID that won by their opinion. Type of the message 'Vote', fields: refereeID and outcomeID.

1.4 Claiming

If you have won and you see that vote has ended you could claim your prize (exact amount of the prize you would get at the end of the voting due to our distribution system). To claim it you should send the message with type 'Claim' and field 'betID' (you have received earlier). After that your prize would be automatically sent to your account.

2 Rewards distribution overview

In this section the crucial part of our technology would be presented. The main reason for everyone to participate in polls and disputes is of course to get a reward. Let's discuss our current approach and another opportunities.

2.1 Distribute bank between the winners

To come to our current distribution system let's look at the real life's dispute. It usually work pretty simple: all of participant place their bets (usually they are equal) and after the end of the event winners split the pot. So our main difference with this variant of dispute betting is that we allow bets with different amounts and there would be some important details that would make other feel uncomfortable. For example large bet attack: let's imagine that some group of friends has decided to make a poll and one of them would be a judge (it was their choice and they trust him). So someone find that poll in the blockchain and place a large bet (more than all of them combined) on the winning option. In that case if that random man wins no one from this group would gain fair prize. However there is an opportunity for them, they could ask a judge (and point that in the poll description) that some random guy has made an unfair bet and judge could make this guy lose and after distribution of this big bet between the group (they are friends) they would just reopen their poll. That case is the main reason why it is not profitable to just come to random guys and try to steal their bets. You should always check the referee before voting. Another problem that this distribution system couldn't guarantee anyone the exact amount of their prize until the betting time would be over. It could be unusual for average betting platform user but this is not a problem for everyone who had participated in a real life's polls.

2.2 Future approaches

In order to solve the problems of previous approach we consider "frozen betting" as one of opportunities. It is the system where bank is divided to 2 parts: frozen and hot. Hot part is making coefficient at the moment of bet and frozen part is responsible for previous bets. It could resolve the situation with floating coefficient due to the fact that frozen part of the bank is not affected by hot part. However, this approach is not only hard to build but it is hard to make it fair enough, that's why it is only the concept

by now. Another approach is always to make a bet against the player (it could be a good option in 2-variants polls where the chance of winning for both is about 50%). For example that would be a great part of price prediction polls.

3 Referee and voting system

3.1 Why one judge could be an option?

The only way to find the winner is to make "the judge" to choose. "The judge" here could be all of the concepts you could imagine: the council of delegated judges, all of players by their direct vote, oracle or special person that is chosen by players (or that is accepted by them) to select a winner. It is obvious that the majority of polls where people could bet on something are ruled by one judge (the company, that provide an interface to bet). In our approach we only provide an interface of the contract but referees choice is up to the poll creator. After the creation of decentralized poll list of referees is public and every person could do their own research to decide should they bet in this poll or not. We suppose that TON DNS could help us to determine referees more easily and it would be more clear for players.

3.2 Voting system with ≥ 1 judge

It is obvious that if we have only 1 judge his vote will determine which variant is right. Situation with more than one judge is more complex and has several ways solve this. In our version of protocol, the winner is determined by choosing the option with the most votes if all judges voted and by the absolute majority method if not all voted. If the voting time has ended, but there is no absolute majority in the voting, or if everyone voted, but there was a draw, then the funds would be returned to players.

We would be careful with the feedback of this decision and would definitely implement the version where only absolute majority would define the winning variant.

3.3 Random judges

One of our key milestones is to create the Random Judge System that would help to make truly decentralized polls. We will reward users who vote correctly (according to the majority) and fine those who try to cheat. In our opinion this would be more fair in perspective for the community because you don't have to find the judge for your poll and this will lead to our dao token launch. However, this is very hard for implement at this time and we will deal with it later.