Solidity Lottery Contract Documentation

Εργασία 1
Μπόγκα Παναγιώτης ics21046

Σχετικά με το συμβόλαιο

Αυτό το έξυπνο συμβολαιο κάνει προσομοίωση μιας λαχειοφόρου αγορά.
Το συμβόλαιο υποστηρίζει μεταβλητό πλήθος παικτών και αντικειμένων. Ο beneficiary μπορεί να προσθέσει όσα items επιθυμεί και μπορούν συμμετέχουν όσοι παίκτες επιθυμούν. Κάθε παίκτης μπορεί να εγγραφεί μόνο μια φορά και να λάβει 5 λαχεία κατα την εγγραφή του. Τα 5 αυτά λαχεία μπορεί να τα ποντάρει σε όποια items επιθυμεί. Για να εγγραφεί ο παίκτης θα πρέπει να έχει τουλάχιστον 0.005ETH τα οποία πληρώνει και στο συμβόλαιο για να ολοκληρώσει την εγγραφή του και να λάβει 5 λαχεία.
Το συμβόλαιο αυτό λειτουργεί με στάδια. Οι εγγραφές παικτών να επιτρέπονται μόνο όταν η stage είναι Reg, οι τοποθετήσεις λαχείων σε κληρωτίδες μόνο όταν η stage είναι Bid και οι κληρώσεις να επιτρέπονται μόνο όταν η stage είναι Done.Το Init είναι το stage που επικρατεί συνήθως όταν γίνεται δημιουργία items στο συμβόλαιο.

Structures and Enums

Struct: Person
Αντιπροσωπεύει πληροφορίες του συμμετέχοντα που έχει εγγραφεί.

- personId: Unique identifier for a person.
- addr: Ethereum address of the participant.
- remainingTokens: Number of tokens remaining for the participant.

Struct: Item
Αντιπροσωπεύει το αντικείμενο στο οποίο μπορούν οι συμμετέχοντες να τοποθετήσουν / ποντάρουν τα λαχεία τους.

- itemId: Unique identifier for an item.
- itemTokens: Array of Ethereum addresses representing tokens bid on the item.
- winner: Ethereum address of the winner for the item.

Enum: Stage
Εδώ ορίζουμε τα διάφορα στάδια / stages του λαχείου. (Init, Reg, Bid, Done). Οι εγγραφές παικτών να επιτρέπονται μόνο όταν η stage
είναι Reg, οι τοποθετήσεις λαχείων σε κληρωτίδες μόνο όταν η stage είναι Bid και οι κληρώσεις να επιτρέπονται μόνο όταν η stage είναι Done.Το Init είναι το stage που επικρατεί συνήθως όταν γίνεται δημιουργία items στο συμβόλαιο

- Init: Initialization stage.
- Reg: Registration stage.
- Bid: Bidding stage.
- Done: Lottery completion stage.

Variables

- **stage**: Current stage of the lottery (Init, Reg, Bid, Done).
- **tokenDetails**: Mapping of participant addresses to their corresponding Person struct.
- **bidders**: Array containing information about all registered participants.
- **items**: Array containing information about all lottery items.
- **winners**: Array containing the Ethereum addresses of the winners.
- **beneficiary**: Ethereum address of the contract owner and beneficiary.
- **bidderCount**: Counter for the number of registered participants.
- **itemCount**: Counter for the number of lottery items.
- **emptyArray**: An empty array of addresses.
- **emptyAddr**: An empty Ethereum address.

Modifiers

- **onlyOwner**: Ensures that a function can only be called by the contract owner (beneficiary).
- **onlyBidders**: Ensures that a function cannot be called by the contract owner.
- **bidderFundsCheck**: Ensures that a bidder has sent at least 0.005 ETH to participate in the lottery.
- **bidderNotRegistered**: Ensures that the participant has not already registered.
- **bidderIsRegistered**: Ensures that the participant has already registered.

- **bidderHasEnoughTokens**: Ensures that the participant has enough tokens to bid.
- **regStage**: Ensures that a function is only callable during the registration stage.
- **bidStage**: Ensures that a function is only callable during the bidding stage.
- **doneStage**: Ensures that a function is only callable during the completion stage.

Constructor

constructor() payable: Initializes the contract, setting the beneficiary and the initial stage to Init.

Functions

addItems()
Visibility: Public (onlyOwner)
Description: Creates new items for the lottery.

register()
Visibility: Public (onlyBidders, bidderFundsCheck, bidderNotRegistered, regStage)
Description: Allows participants to register for the lottery and receive initial tokens.

random()
Visibility: Public
Description: Generates a pseudorandom number based on block information and the number of registered participants.

bid(uint _itemId, uint _count)
Visibility: Public (onlyBidders, bidderHasEnoughTokens, bidderIsRegistered, bidStage)
Parameters:

_itemId: Identifier of the item being bid on.
_count: Number of tokens bid by the participant.
Description: Allows participants to bid on lottery items using tokens.

revealWinners(uint _itemNum)
Visibility: Public (onlyOwner, doneStage)
Parameters:
_itemNum: Identifier of the item for which winners are being revealed.
Description: Randomly selects a winner for the specified item and emits a Winner event.

withdraw()
Visibility: Public (onlyOwner)
Description: Allows the contract owner to withdraw the contract's funds.

reset()
Visibility: Public (onlyOwner)
Description: Clears the items, bidders, and winners arrays.

advanceState()
Visibility: Public (onlyOwner)
Description: Advances the lottery to the next stage.

Events

Winner(address winner, uint itemId)
Parameters:
winner: Ethereum address of the winner.
itemId: Identifier of the item for which the winner is revealed.
Description: Triggered when a winner is revealed for an item.