

## Hardhat Smart Contract Lottery

```
1 // SPDX-License-Identifier: MIT
2
3 pragma solidity ^0.8.7;
4
5 import "@chainlink/contracts/src/v0.8/interfaces/VRFCoordinatorV2Interface.sol";
6 import "@chainlink/contracts/src/v0.8/VRFConsumerBaseV2.sol";
7 import "@chainlink/contracts/src/v0.8/interfaces/KeeperCompatibleInterface.sol";
8 import "hardhat/console.sol";
9
10 error Raffle_UpgradeNotNeeded(uint256 currentBalance, uint256 numPlayers, uint256 raffleState);
11 error Raffle_TransferFailed();
12 error Raffle_SendMoreToEnterRaffle();
13 error Raffle_RaffleNotOpen();
14
15 /**@title A sample Raffle Contract
16  * @author Patrick Collins
17  * @notice This contract is for creating a sample raffle contract
18  * @dev This implements the Chainlink VRF Version 2
19  */
20 contract Raffle is VRFConsumerBaseV2, KeeperCompatibleInterface {
21     /* Type declarations */
22     enum RaffleState {
23         OPEN,
24         CALCULATING
25     }
26     /* State variables */
27     // Chainlink VRF Variables
28     VRFCoordinatorV2Interface private immutable i_vrfCoordinator;
29     uint64 private immutable i_subscriptionId;
30     bytes32 private immutable i_gasLane;
31     uint32 private immutable i_callbackGasLimit;
32     uint16 private constant REQUEST_CONFIRMATIONS = 3;
33     uint32 private constant NUM_WORDS = 1;
34
35     // Lottery Variables
```

```
35     // Lottery Variables
36     uint256 private immutable i_interval;
37     uint256 private s_lastTimeStamp;
38     address private s_recentWinner;
39     uint256 private i_entranceFee;
40     address payable[] private s_players;
41     RaffleState private s_raffleState;
42
43     /* Events */
44     event RequestedRaffleWinner(uint256 indexed requestId);
45     event RaffleEnter(address indexed player);
46     event WinnerPicked(address indexed player);
47
48     /* Functions */
49     constructor(
50         address vrfCoordinatorV2,
51         uint64 subscriptionId,
52         bytes32 gasLane, // keyHash
53         uint256 interval,
54         uint256 entranceFee,
55         uint32 callbackGasLimit
56     ) VRFConsumerBaseV2(vrfCoordinatorV2) {
57         i_vrfCoordinator = VRFCoordinatorV2Interface(vrfCoordinatorV2);
58         i_gasLane = gasLane;
59         i_interval = interval;
60         i_subscriptionId = subscriptionId;
61         i_entranceFee = entranceFee;
62         s_raffleState = RaffleState.OPEN;
63         s_lastTimeStamp = block.timestamp;
64         i_callbackGasLimit = callbackGasLimit;
65     }
66
67     function enterRaffle() public payable {
68         // require(msg.value >= i_entranceFee, "Not enough value sent");
69         // require(s_raffleState == RaffleState.OPEN, "Raffle is not open");
```

```

70     if (msg.value < i_entranceFee) {
71         revert Raffle__SendMoreToEnterRaffle();
72     }
73     if (s_raffleState != RaffleState.OPEN) {
74         revert Raffle__RaffleNotOpen();
75     }
76     s_players.push(payable(msg.sender));
77     // Emit an event when we update a dynamic array or mapping
78     // Named events with the function name reversed
79     emit RaffleEnter(msg.sender);
80 }
81
82 /**
83  * @dev This is the function that the Chainlink Keeper nodes call
84  * they look for `upkeepNeeded` to return True.
85  * the following should be true for this to return true:
86  * 1. The time interval has passed between raffle runs.
87  * 2. The lottery is open.
88  * 3. The contract has ETH.
89  * 4. Implicity, your subscription is funded with LINK.
90  */
91 function checkUpkeep(
92     bytes memory /* checkData */
93 )
94     public
95     view
96     override
97     returns (
98         bool upkeepNeeded,
99         bytes memory /* performData */
100     )
101 {
102     bool isOpen = RaffleState.OPEN == s_raffleState;
103     bool timePassed = ((block.timestamp - s_lastTimestamp) > i_interval);
104     bool hasPlayers = s_players.length > 0;

```

```

105     bool hasBalance = address(this).balance > 0;
106     upkeepNeeded = (timePassed && isOpen && hasBalance && hasPlayers);
107     return (upkeepNeeded, "0x0"); // can we comment this out?
108 }
109
110 /**
111  * @dev Once `checkUpkeep` is returning `true`, this function is called
112  * and it kicks off a Chainlink VRF call to get a random winner.
113  */
114 function performUpkeep(
115     bytes calldata /* performData */
116 ) external override {
117     (bool upkeepNeeded, ) = checkUpkeep("");
118     // require(upkeepNeeded, "Upkeep not needed");
119     if (!upkeepNeeded) {
120         revert Raffle__UpkeepNotNeeded(
121             address(this).balance,
122             s_players.length,
123             uint256(s_raffleState)
124         );
125     }
126     s_raffleState = RaffleState.CALCULATING;
127     uint256 requestId = i_vrfCoordinator.requestRandomWords(
128         i_gasLane,
129         i_subscriptionId,
130         REQUEST_CONFIRMATIONS,
131         i_callbackGasLimit,
132         NUM_WORDS
133     );
134     // Quiz... is this redundant?
135     emit RequestedRaffleWinner(requestId);
136 }
137
138 /**
139  * @dev This is the function that Chainlink VRF node
140  * calls to send the money to the random winner

```

```

140     * calls to send the money to the random winner.
141     */
142     function fulfillRandomWords(
143         uint256, /* requestId */
144         uint256[] memory randomWords
145     ) internal override {
146         // s_players size 10
147         // randomNumber 202
148         // 202 % 10 ? what's doesn't divide evenly into 202?
149         // 20 * 10 = 200
150         // 2
151         // 202 % 10 = 2
152         uint256 indexOfWinner = randomWords[0] % s_players.length;
153         address payable recentWinner = s_players[indexOfWinner];
154         s_recentWinner = recentWinner;
155         s_players = new address payable[](0);
156         s_raffleState = RaffleState.OPEN;
157         s_lastTimeStamp = block.timestamp;
158         (bool success, ) = recentWinner.call{value: address(this).balance}("");
159         // require(success, "Transfer failed");
160         if (!success) {
161             revert Raffle__TransferFailed();
162         }
163         emit WinnerPicked(recentWinner);
164     }
165
166     /** Getter Functions */
167
168     function getRaffleState() public view returns (RaffleState) {
169         return s_raffleState;
170     }
171
172     function getNumWords() public pure returns (uint256) {
173         return NUM_WORDS;
174     }

```

```

169         return s_raffleState;
170     }
171
172     function getNumWords() public pure returns (uint256) {
173         return NUM_WORDS;
174     }
175
176     function getRequestConfirmations() public pure returns (uint256) {
177         return REQUEST_CONFIRMATIONS;
178     }
179
180     function getRecentWinner() public view returns (address) {
181         return s_recentWinner;
182     }
183
184     function getPlayer(uint256 index) public view returns (address) {
185         return s_players[index];
186     }
187
188     function getLastTimeStamp() public view returns (uint256) {
189         return s_lastTimeStamp;
190     }
191
192     function getInterval() public view returns (uint256) {
193         return i_interval;
194     }
195
196     function getEntranceFee() public view returns (uint256) {
197         return i_entranceFee;
198     }
199
200     function getNumberOfPlayers() public view returns (uint256) {
201         return s_players.length;
202     }
203 }

```