Lesson 10 - Randomness

Randomness sources

- (Review) Block hash and timestamp
- (Review) Hashing and bytes conversion
- Creating a random number from block.hash and/or block.timestamp
- Mining exploitation
- False randomness

References

https://github.com/wissalHaji/solidity-coding-advices/blob/master/best-practices/timestamp-can-be-manipulated.md

https://fravoll.github.io/solidity-patterns/randomness.html

Generating numbers from pseudorandom sources

- Using a trusted party for randomness
- Signing a message
- Verifying signature
- Sealing a message with signature
- Committing a sealed seed for randomness
- Revealing a seed and processing randomness
- Beware of hash collisions and parameter amplitude

References

https://blockchain-academy.hs-mittweida.de/courses/solidity-coding-beginners-to-intermediate/lessons/solidity-11-coding-patterns/topic/commit-reveal/

https://en.wikipedia.org/wiki/Hash_collision

Theory: Other randomness sources

- Bias in decentralized randomness generation
- Oracles
- Data sources
- Oracle patterns
- On-chain data
- VRF
- RANDAO

References

https://fravoll.github.io/solidity-patterns/oracle.html

https://betterprogramming.pub/how-to-generate-truly-random-numbers-in-solidity-and-blockchain-9ced6472dbdf

https://docs.chain.link/docs/chainlink-vrf/

https://github.com/randao/randao

Lottery contract

- (Review) Design patterns
- Architecture overview
- Lottery structure

Implementation details

- Implement ownable
- Owner start lottery and define betting duration and fee
    - Define a block number target
- Players must buy an ERC20 with ETH
- Players pay ERC20 to bet
    - Only possible before block number met
- Anyone can roll the lottery
    - Only after block number target is met
    - Randomness used from the hash of the block at block number
- Winner receives the pooled ERC20 minus fee
- Owner can withdraw fees and restart lottery
- Players can burn ERC20 tokens and redeem ETH

References

https://coinsbench.com/how-to-create-a-lottery-smart-contract-with-solidity-4515ff6f849a

Homework

- Create Github Issues with your questions about this lesson
- Read the references
- Complete test scenarios for Lottery.sol
- (Optional) Try to implement some contract features
- (Optional) Experiment with the Randomness sources presented