OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

NFT Markets - Security

Thomas Bocek

04.12.2021

Designing a Market NFT – Lecture 8 - Security Alert

- Store offers
  - `mapping(address => mapping(uint256 => mapping(address => uint256))) private _offers;`
  - Key: nft contract, nft Id, offerer address, value: ethers that were offered
- “Lehnt er die Offerte ab, bekommt der Ersteller der Offerte die Ethers wieder zurück.” → Does not work well with smart contracts
  - The one who wants something has to pay the gas (NFT holder cannot decline 100 offers)

- Alternative: withdraw Offer
  - `makeOffer(address nftContract, uint256 nftId)`
  - `withdrawOffer(address nftContract, uint256 nftId)`
- Use events
  - Offer, Withdraw, Accepted
- Make data visible
  - `offers(address nftContract, uint256 nftId, address offerer)`

Security Alert

Losing Funds

- Reported by Simon and Zvonimir
- Problem: 2 x offer
  - 1st offer nftId 1, 2 ETH, 2nd offer nftId 1, 1 ETH
  - Withdraw: 3 ETH? No, only 1 ETH, 2 ETH is lost

```
function makeOffer(address nftContract, uint256 nftId) payable external {
  _offers[nftContract][nftId][msg.sender] = msg.value;
  emit Offer(nftContract, nftId, msg.sender, msg.value);
}

function withdrawOffer(address nftContract, uint256 nftId) payable external {
  uint256 val =  _offers[nftContract][nftId][msg.sender];
  delete(_offers[nftContract][nftId][msg.sender]);
  payable(msg.sender).transfer(val);
  emit Withdraw(nftContract, nftId, msg.sender, val);
}
```

Fixing and Improving the Market

- Fixing
  - `require(_offerMap[nftContract][msg.sender] == 0, "already made an offer");`
- Improving – make it enumerable
  - `Old: mapping(address => mapping(uint256 => mapping(address => uint256))) private _offers;`
  - `New: mapping(address => mapping(uint256 => mapping(uint256 => uint256))) private _offers;`
  - `New: mapping(address => mapping(uint256 => mapping(address => uint256))) private _offerMap;`
  - `New: mapping(address => mapping(uint256 => uint256)) private _totalOfferCount;`

Fixing and Improving the Market

- New Functions

```
function totalOffers(address nftContract, uint256 nftId) view public returns (uint256){
  return _totalOfferCount[nftContract][nftId];
}

function offerIndex(address nftContract, uint256 nftId, address offerer) public view returns
(uint256) {
  return _offerMap[nftContract][nftId][offerer];
}

function removeAndShift(address nftContract, uint256 nftId, uint256 index) internal {
  delete(_offers[nftContract][nftId][index]);
  uint256 currentTotalOffers = totalOffers(nftContract, nftId);
  _offers[nftContract][nftId][index] = _offers[nftContract][nftId][currentTotalOffers];
  delete(_offers[nftContract][nftId][currentTotalOffers]);
  _totalOfferCount[nftContract][nftId] = currentTotalOffers - 1;
}
```