CryptoPunk等特殊交易市场

CryptoPunks

- CryptoPunks Market：https://etherscan.io/address/0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb#code
- 该合约即是一个token合约，也是一个Market合约
- 合约代码解释：https://www.cnblogs.com/wanghui-garcia/p/9506390.html
- 重要状态变量：

```
//临时账户：买方想要购买NFT、出价时，必须先将ether转到合约中，如果最后购买失败，此处存储用户可取回的出价金额；卖方成功卖出NFT后，货款也会记录在此处。需要用户主动到合约中调用withdraw() 领取
    mapping (address => uint) public pendingWithdrawals;



// 声明想要卖出的token的信息。比如用户A要卖出一个NFT，那么就会构造一个Offer对象
struct Offer {
        bool isForSale;//true即token正在卖出，false表示取消卖出
        uint punkIndex;
        address seller;//卖方（NFT的主人），即上方的用户A
        uint minValue;          // in ether，卖出最低价
        address onlySellTo;     //用于设置卖给谁，不设则卖给谁都可以
    }

    //通过token索引来查看该token的卖出信息，也可能没有
```

```
    mapping (uint => Offer) public punksOfferedForSale;


// 声明想要卖入的NFT信息。比如用户B想要买入一个NFT，那么就会构造一个Bid竞价对象
    struct Bid {
        bool hasBid;//是否正在竞标、还是已取消订单
        uint punkIndex;
        address bidder;// 买方，即用户B
        uint value;
    }
//通过token索引来查看该token的“最高价”竞标信息，也可能没有(当多个用户竞标时，只保留最高价)
    mapping (uint => Bid) public punkBids;
```

买or卖CryptoPunk

- 最常规的流程为 1. --〉2. 或 3. 3. 3. --〉4.

1. 卖方挂一个offer卖单---offerPunkForSale

- 合约方法：function offerPunkForSale(uint punkIndex, uint minSalePriceInWei)
- 参数说明：punkIndex为要卖出的NFT的tokenId，minSalePriceInWei为卖出价格
- 方法作用：将卖出意图组装为一个Offer结构体对象，保存到punksOfferedForSale键值对中；触发一个PunkOffered事件
- function offerPunkForSaleToAddress(uint punkIndex, uint minSalePriceInWei, address toAddress)：与上方方法不同之处为，指定要卖给特定的用户toAddress

2. 买方根据已有的offer单进行购买---buyPunk

- 合约方法：function buyPunk(uint punkIndex) payable
- 参数说明：punkIndex为要购买的NFT的tokenId
- 方法作用：首先根据punkIndex查找Offer对象，判断Offer.isForSale为true、即仍为卖出状态；然后校验出价msg.value大于等于offer中的卖价；校验offer.seller仍为NFT所有者；然后完成NFT的transfer，清空卖出offer信息，记录seller可以收取的货款信息等；如果msg.sender之前针对该NF T有Bid信息，则清空，并将投标钱放入临时账户中

3. 买方挂一个Bid竞标买单（必须比之前的最高出价还要高才能成功）---enterBidForPunk

- 合约方法：function enterBidForPunk(uint punkIndex) payable
- 方法作用：msg.sender对punkIndex指定的NFT进行出价，出价金额为msg.value（**买方需要先将钱转入合约中！！**）。合约中首先会从punkBids中读取之前的最高出价信息，当前出价必须更高、否则revert。当前出价信息覆盖原有的Bid信息。

4. 卖方接收目前最高的Bid，完成交易---acceptBidForPunk

- 合约方法：function acceptBidForPunk(uint punkIndex, uint minPrice)

- 参数说明：minPrice表示卖方接受投标的最小价格（当前最高的Bid必须要大于minPrice才能成交）
- 方法作用：校验各种信息；完成NFT从卖方到买方的transfer；清空Offer对象、Bid对象总的🧍各个字段。卖方赚到的钱记录到临时账户中

5. 买方取消对某个NFT的出价并拿回竞标的钱---withdrawBidForPunk

- 合约方法：function withdrawBidForPunk(uint punkIndex)
- 作用：从punkBids中查出msg.sender对于该punkIndex 的投标信息并清空，然后将投标价退回给用户

Opensea中如何批量购买CryptoPunk

1. 聚合器合约批量调用CryptoPunk合约的buyPunk(uint256 punkIndex)，然后调用CryptoPunk合约的transferPunk(address to, uint256 punkIndex)转给用户

- buyPunk示例：https://etherscan.io/tx/0xff6420cc37f60728967743384427aec3fab22e65b98078717f9d96fda84a4c0b3
- transferPunk示例：transferPunk(address to, uint256 punkIndex)

MoonCat

- 合约及交易市场：https://etherscan.io/address/0x60cd862c9C687A9dE49aecdC3A99b74A4fc54aB6#code

买or卖MoonCat

1. makeAdoptionOfferToAddress(bytes5 catId, uint price, address to)：挂一个卖单，可以指定接单者to
2. acceptAdoptionOffer(bytes5 catId) payable：接单、买入一个MoonCat。msg.value需要大于等于定价offer.price，多余部分会记录下来、允许用户提取差额。
3. cancelAdoptionOffer(bytes5 catId)：cat的owner取消卖单。
4. makeAdoptionRequest(bytes5 catId) payable：挂一个offer单，单价即为msg.sender。对于同一个cat，每次出价都必须大于之前的人
5. acceptAdoptionRequest(bytes5 catId)：接受一个offer单，将cat卖给挂单者
6. cancelAdoptionRequest(bytes5 catId)：取消offer单
7. giveCat(bytes5 catId, address to)：将cat转送给他人
8. withdraw()：提取offer单失效时的退款、以及接卖单时多付的部分