**1.将要升级的pro钱包发交易流程应该变成这样(红色部分为此次应该增加的内容)：**

* 用户提交含to、amount、remark参数的请求后。
* 钱包发起请求：xdag\_getTransactionNonce。

(阻塞形，等待拿到nonce，获得nonce则不用继续等待，但设置至多等待10s)

* 拿到nonce(时间到，nonce仍未空则提示重试，此次交易报异常退出)。
* 构造交易块。
* 调用xdag\_sendRawTransaction发送交易。
* 弹窗显示交易详情(即Pending)或者提示从节点返回的错误信息。

**2.确认流程后，流程变动所涉及的需要修改的部分，以及需要增加新内容的部分。**

**2.1**获取用户提交的交易参数后，原逻辑应该是会调” lib/page/detail/send\_page.dart”该文件内的send(String res, String toAddress, String fromAddress)方法来完成组块以及其他钱包和线程相关的业务，这里需要修改的地方是：在组块之前，先查询账户nonce，然后再把nonce连同用户传递参数传入getTransaction这个组块方法中，从而完成合法组块。

原逻辑是109-123行，其中if，else分别是子线程完成组块与接收到组好的块去调rpc把该交易块发送出去，因此，可以在子线程这边调用组块方法之前先完成nonce查询逻辑，再连同nonce一起组块：（以下代码为gpt生成，可能逻辑正确，但细节处可能需要看看是否仍需修改）

if (data is SendPort) {

var subSendPort = data;

// 🆕 1. 获取 nonce

String? nonce;

try {

Response nonceResponse = await dio.post(

rpcURL,

cancelToken: cancelToken,

data: {

"jsonrpc": "2.0",

"method": "xdag\_getTransactionNonce",

"params": [fromAddress],

"id": 1

},

).timeout(const Duration(seconds: 10));

nonce = nonceResponse.data['result'] as String?;

} catch (e) {

setState(() {

error = "获取 nonce 失败，请检查网络";

isLoad = false;

});

return;

}

// 🆗 如果 nonce 合法，再继续发给子线程构造交易

if (nonce == null || nonce.isEmpty) {

setState(() {

error = "获取 nonce 返回空值";

isLoad = false;

});

return;

}

// ✅ 2. 发数据给子线程（多传一个 nonce）

subSendPort.send([res, toAddress, amount, fromAddress, remark, nonce]);

}

**2.2**子线程逻辑处（81行）需要多加一个参数，就是刚刚调用rpc查询到的nonce：

String nonce = data[5] as String;

然后子线程在此处调用的组块方法getTransaction需要再多传递一个这个nonce参数，因此getTransaction该方法需要修改。

**2.3**getTransaction方法大致需要修改的点：

* 在整体上由于会多一个nonce字段，因此，原先根据有无remark，签名字段为4个或者5个，签名时，需要填充12或者11个32字节的0，再签名；现在多了一个nonce字段，因此只需填充11或者10个32字节的0。
* 同理，签名后，组块时所需要的填充的0，也需要相应的减少一个32字节的。
* 具体到组块的各个字段，需要改两部分：①头字段中的第二部分的type、②第二个字段改为放nonce，原先的字段往后顺延一个字段(32B)

1. 头字段中的type部分需要被修改，以下分别给出四种修改后的type：  
   奇公钥+无remark：  
   e1dc560500000000

奇公钥+有remark：

e1dc695500000000

偶公钥+无remark：

e1dc570500000000

偶公钥+有remark：

e1dc795500000000

以下是一个奇公钥+有remark的完整的header字段样例：

0000000000000000e1dc6955000000009239ab5d9c01000000e1f50500000000（标红地方为type）

1. 第二个位置，也就是第二个字段需要放nonce，一下为一个nonce=10的样例：

0000000000000000000000000000000000000000000000000a00000000000000

由于rpc查询出来的nonce（rpc查出来的到的结果是String类型），会放在该32字节的后八个字段，然后前面24个字节的零，这后八个字节存放nonce的方式是小端序存放。

3.以上为新增nonce字段后，组块大体需要改变的地方，然后鉴于安全方面的考虑，觉得pro钱包还是需要在完全升级成0.8.0版本之前，也就是适应现在要更新的主网版本钱包之前，觉得有必要更新一版主网仍然发交易组块逻辑和现在0.7.2未更新时一样，然后测试网发交易组块逻辑为0.8.0版本的钱包，因为虽然我们已经公测了0.8.0版本的代码，但是由于大量用户都是使用的pro钱包，而pro钱包是还没有更新的，所以也就是说，其实大部分用户是没参与到公测中来的，go钱包主要是节点使用，使用go钱包测试转账的用户还是少数，所以，看是就这样先做一版主网测试网发交易逻辑不一样，分别兼容老版方式以及新版发交易方式的钱包，还是说需要继续商议，我们可以语音交流。