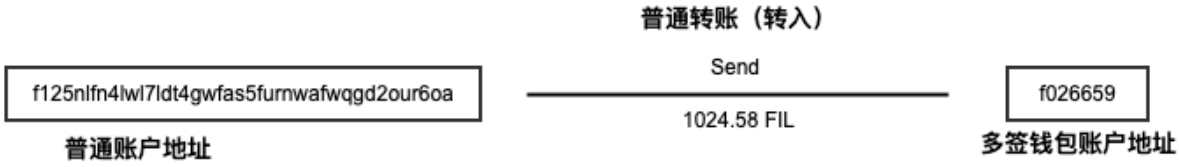
Filecoin多签钱包指南

概览

和普通账户的区别

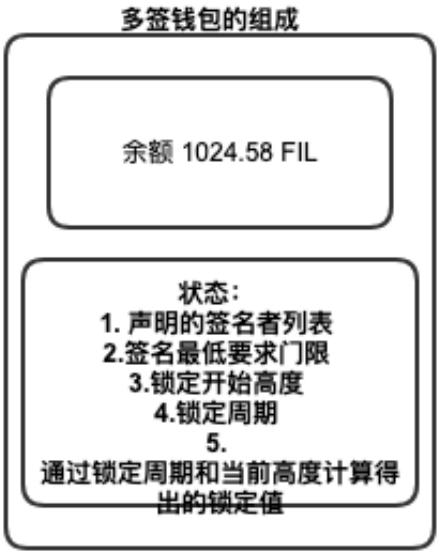
多签钱包是一个合约账户，它像普通账户一样，拥有一个标示账户唯一性的ID和账户地址。同样，多签钱包也拥有账户余额，可以向它以普通转账方式向它充值。



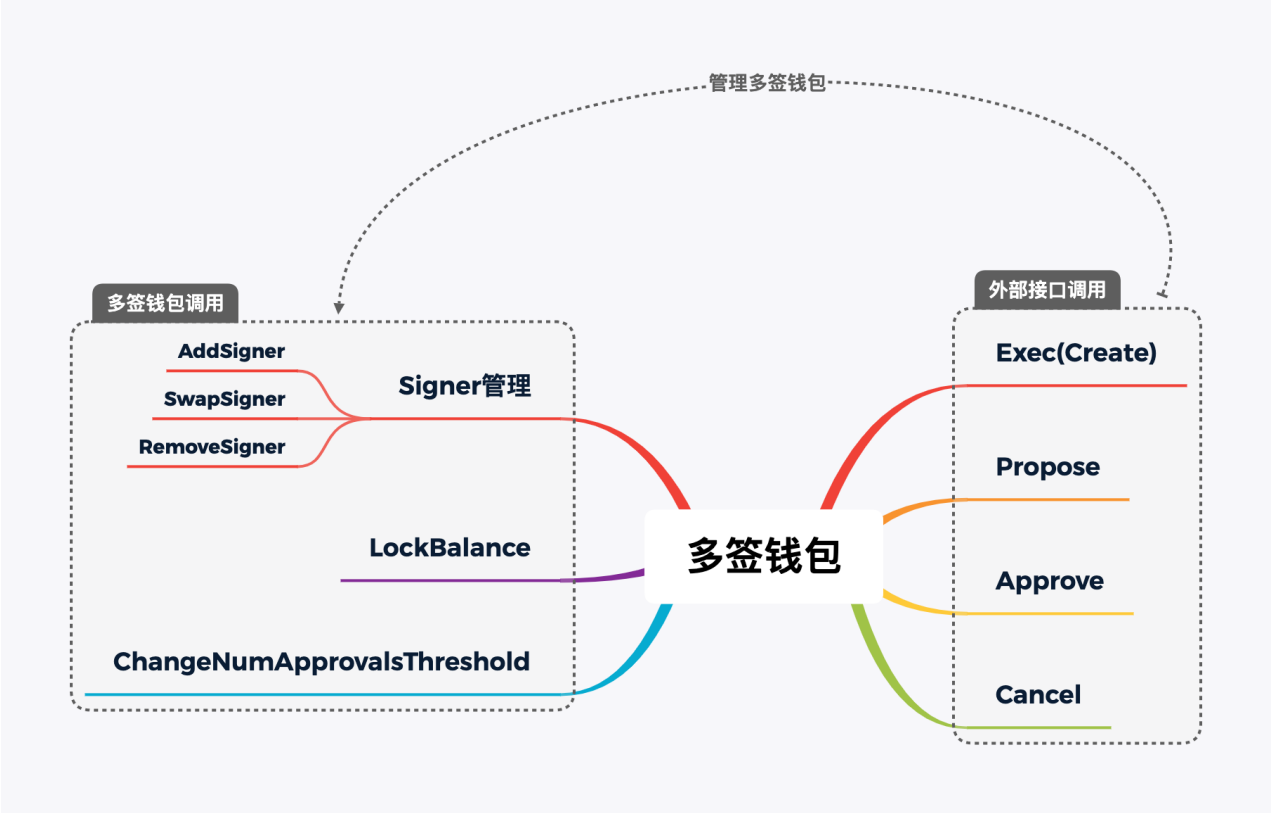
通过操作多签钱包的方法，来控制和设定多签钱包的签名者（或称共同管理人）、最低多人签名人数要求、锁定金额和锁定期。在从多签钱包转出金额的时候，就会由设定好范围内的签名者（共同管理人）按照最低签名数投票决定是否批准转出该笔交易。

多签钱包的组成

多签钱包包含余额和状态两部分。添加修改删除签名者、设置最低多人签名人数、以及更改锁定值都是修改多签钱包的状态。



它支持以下几个管理多签钱包签名者、最低签名门限值和锁定金额的方法：



它的锁定金额是指，从指定起始高度开始`StartEpoch`，经过一定周期`UnlockDuration`，按照每个高度线性释放一部分数额，当申请转出的数额超出多签钱包规定的可用部分时，转账会失败。

锁定部分的计算公式为：

$$locked = ceil(InitialBalance * remainingLockDuration / UnlockDuration) \quad (1)$$

`InitialBalance`是初始设定的锁定值。如果多签钱包账户余额小于该值，且仍在锁定期内，该钱包是无法转出金额的。

同时，多签钱包的锁定，是一锤子买卖，当过了锁定期`UnlockDuration`，这个钱包的锁定功能将失效，所有的锁定都变成0，即所有的余额都可用。想要启用锁定功能，就需要重新创建一个全新的多签钱包。

使用方式

多签钱包对外开放1中创建方式和3中调用方式。操作多签钱包都需要发送消息。对外开放的调用方法有:`Exec` / `Propose` / `Approve` / `Cancel`。其中`Exec`调用了链系统Actor（f01）合约，来创建一个新多签钱包合约，并为之分配唯一ID和内置地址。多签钱包的转出、阈值管理、签名者管理统统开始于调用`Propose方法`，结束于`Approve`方法或`Cancel`方法。其中`Cancel`方法只能由`Propose`发起者调用，一旦取消立即生效。

钱包的创建

多签钱包的创建和创建矿工号相似。通过发消息（交易）给系统内置Actor创建一个新Actor（合约）。这个Actor就是多签钱包。其消息构成规则如下：

```
{
  "From": "多签钱包创建人",
  "To": "f01",
  "Value": "多签钱包初始金额",
  "Method": 2,
  "Params": {
    "CodeCID": "",
    "ConstructorParams": enc
  }
}
```

`Params`使用**cbor**进行序列化，将序列化后的结果填入发送的消息`Params`字段中。以下是`ConstructorParams`参数内容，也需要使用cbor进行序列化后填入`ConstructorParams`参数。

```
{
    "Signers": ["签名者1", "签名者2"],
    "NumApprovalsThreshold": 0,
    "UnlockDuration": 0,
    "StartEpoch": 0
}
```

`From`是创建钱包的发起人，需要填入到`Params`的`Signers`参数内。如果不填，系统不会自动填入，那么钱包发起人想要操作钱包就需要后续采用管理钱包的方式添加进多签钱包了。

`To`是固定账号，`f01`表示系统内置Actor。

`Value`填入多签钱包初始金额。可以是0。

`Method`填2，表示执行`f01`的`Exec`方法。2是`Exec`的方法ID。

`Params`参数是创建多签钱包必填项，其参数有3-4个。其中`StartEpoch`是当前版本新加字段。

`Signers`，表示钱包共同管理者，最多人数不能超过8192个，最少人数不能少于“最低共同签名数量”。

`NumApprovalsThreshold`，最低共同签名数量，最低共同签名数量为0时，需要全部签名账户签名。

`UnlockDuration` 可以是0

`StartEpoch`

钱包转账

发起交易

Propose 是发起转账交易、管理多签钱包的起点。多签钱包的目的就是多人共管同一个钱包，根据钱包

构建消息

发起提案是向链上发送一条普通消息，只有多签钱包签名者账户列表中的账户才能发起交易提案。消息中需要涵盖多签钱包账户地址，要转入的账户地址，要转入的数额这三个必要条件。以下是构建消息的伪代码，`消息中的Value`不需要填数额，填0即可，`Method`方法ID填2，表示调用多签钱包合约的`Propose`方法。

`Params`中`To`填要转入的账户地址，`Value`填待转入目标账户地址的数额。`Method`填0（表示Send），表示该提案通过后调用`Send`向目标地址转账。`Params`为null。

`Params`使用**cbor**进行序列化，将序列化后的结果填入发送的消息`Params`字段中。

```
{
  "From": "提案发起者",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 2,
  "Params": {
    To:     "要转入的账户地址",
    Value:  "待转入目标账户地址的数额",
    Method: 0,
    Params: null,
  }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

获取TxnID，需要给到其他签名者。

确认交易

构建消息

批准交易是向链上发送一条普通消息，只有多签钱包签名者账户列表中的账户才能发起批准。

`Params`使用**cbor**进行序列化，将序列化后的结果填入发送的消息`Params`字段中。

```
{
  "From": "批准人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 3,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

如果不提供ProposalHash是可以执行确认提案操作的。也可以增强交易确认。增强交易确认是需要提案发起人账户地址、要转入的账户地址、待转入目标账户地址的数额、方法ID和方法参数的。如下。

```
{
  "Requester": "Proposal发起人",
  "To": "要转入的账户地址",
  "Value": "待转入目标账户地址的数额",
  "Method": 0,
  "Params": null
}
```

`ProposalHash`使用**cbor**进行序列化，而后使用`blake2b.Sum256`进行哈希。

哈希的结果放入消息的`Params`->`ProposalHash`字段中。

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

取消交易

只有提案发起人才可以取消交易。其消息内容与批准交易相似。只是消息的`Method`为4（方法ID）。

```
{
  "From": "Proposal发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 4,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

`ProposalHash`的内容：

```
{
  "Requester": "Proposal发起人",
  "To": "要转入的账户地址",
  "Value": "待转入目标账户地址的数额",
  "Method": 0,
  "Params": null
}
```

无返回值。执行通过后该交易被直接取消。

阈值管理

发起提案

要更改最低签名确认数，也需要发起`Propose`方法调用，由多数人`Approve`表决通过后生效。其消息内容构造如下：

```
{
  "From": "提案发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 2,
  "Params": {
    To:     "多签钱包账户地址",
    Value:  0,
    Method: 8,
    Params: {
      "NewThreshold": 5
    },
  }
}
```

`Params`使用**cbor**进行序列化，将序列化后的结果填入发送的消息`Params`字段中。

`Method` 8 表示调用`ChangeNumApprovalsThreshold`方法。

`NewThreshold`不能超过`Signers`总数。可以为0，0表示全部`Signers`都需要签名确认。

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

拿到`TxnID`给到其他人。

批准阈值更改

等同于发送交易

```
{
  "From": "批准人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 3,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

`ProposalHash`的内容：

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 8,
  "Params": {
    "NewThreshold": 5
  }
}
```

`ProposalHash`的内容可以缺省，但拥有则更加安全。

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

当`Applied`为true，阈值更新成功。

多签钱包资金管理

发起锁定提案

发起锁定提案的前提条件：

1. `UnlockDuration`必须大于0
2. `Amount`必须大于0
3. 在创建钱包时，设定的`UnlockDuration`为0。如果创建钱包时`UnlockDuration`非0，则不允许该提案。

```
{
```

```
  "From": "提案发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 2,
  "Params": {
    To:     "多签钱包账户地址",
    Value:  0,
    Method: 9,
    Params: {
      "StartEpoch": 148888,
      "UnlockDuration": 900,
      "Amount": 100
    },
  }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

批准锁定余额

```
{
  "From": "批准人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 3,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 9,
  "Params": {
      "StartEpoch": 148888,
      "UnlockDuration": 900,
      "Amount": 100
    }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

取消余额锁定

```
{
  "From": "Proposal发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 4,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 9,
  "Params": {
      "StartEpoch": 148888,
      "UnlockDuration": 900,
      "Amount": 100
    }
}
```

查询锁定额度

查询多签钱包两个高度之间的锁定部分差值。

Signer管理

添加签名人

发起提案

```
{
  "From": "提案发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 2,
  "Params": {
    "To": "多签钱包账户地址",
    "Value": 0,
    "Method": 5,
    "Params": {
      "Signer": "要添加的签名人",
      "Increase": false
    }
  }
}
```

`Params`参数`Method`为5 表示 `AddSigner`，如果`Increase`为true，则添加签名人成功后，`NumApprovalsThreshold`会增加1。

`Params`使用**cbor**进行序列化，将序列化后的结果填入发送的消息`Params`字段中。

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

拿到`TxnID`给到其他人。

批准添加

官方提供的多签钱包范例代码中是**必须**要提供要添加的签名人和是否增加`NumApprovalsThreshold`的。也就是说`ProposalHash`不应该被省略。

```
{
  "From": "批准人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 3,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

`Params`使用**cbor**进行序列化，将序列化后的结果填入发送的消息`Params`字段中。

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 5,
  "Params": {
      "Signer": "要添加的签名人",
      "Increase": false
    }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

取消添加签名人

取消只能够是提案发起人取消，执行取消方法会立即取消。

```
{
  "From": "Proposal发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 4,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

取消需要提供签名人和是否增加`NumApprovalsThreshold`信息。

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 5,
  "Params": {
      "Signer": "要添加的签名人",
      "Increase": false
    }
}
```

成功与否无返回结果。

交换签名人

发起提案

```
{
  "From": "提案发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 2,
  "Params": {
    "To": "多签钱包账户地址",
    "Value": 0,
    "Method": 7,
    "Params": {
      "From": "旧签名地址",
      "To": "新签名地址"
    }
  }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

批准交换

```
{
  "From": "批准人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 3,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

`ProposalHash`内容：

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 7,
  "Params": {
      "From": "旧签名地址",
      "To": "新签名地址"
    }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

取消交换签名人

取消只能够是提案发起人取消，执行取消方法会立即取消。

```
{
  "From": "Proposal发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 4,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

```
{
  "Requester": "Proposal发起人",
  "To": "多签钱包地址",
  "Value": 0,
  "Method": 7,
  "Params": {
      "From": "旧签名地址",
      "To": "新签名地址"
    }
}
```

移除签名人

发起提案

```
{
  "From": "提案发起人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 2,
  "Params": {
    "To": "多签钱包账户地址",
    "Value": 0,
    "Method": 6,
    "Params": {
      "Signer": "要添加的签名人",
      "Decrease": false
    }
  }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

批准移除

```
{
  "From": "批准人",
  "To": "多签钱包账户地址",
  "Value": 0,
  "Method": 3,
  "Params": {
    "ID": TxnID,
    "ProposalHash": null
  }
}
```

返回结果

```
{"Ret": null, "Code": 0, "TxnID": 0, "Applied": false}
```

附录

方法ID编号对照表

方法名称	方法ID	To
创建钱包（Exec）	2	f01
发起交易（Send）	0	
发起提案（Propose）	2	多签钱包账户地址
批准提案（Approve）	3	多签钱包账户地址
取消提案（Cancel）	4	多签钱包账户地址
更改阈值（ChangeNumApprovalsThreshold）	8	多签钱包账户地址
添加Signer（AddSigner）	5	多签钱包账户地址
交换Signer（SwapSigner）	7	多签钱包账户地址
移除Signer（RemoveSigner）	6	多签钱包账户地址
锁定余额（LockBalance）	9	多签钱包账户地址