# OP_GROUP & Colored Coin

姜家志

# 内容简介

- 彩色币
- OP_GROUP
- 通过OP_GROUP实现彩色币
- OP_GROUP与ERC2.0
- BCH上的创新

# 什么是彩色币

- token
- 彩色币就是BCH
- 让UTXO具有不同的标识
- 存储和转移只需要复用BCH系统即可
- 定制化不同的权益证明
- 股权，商品证书，Token……

# OP_GROUP

- BUIP077-Andrew Stone
- 使堆栈的数据做为group identifier
- 关联input和output
- group balance must zero

# 普通交易

**锁定脚本：** `OP_DUP, OP_HASH160, <pubkeyHash>, OP_EQUAL_VERIFY, OP_CHECKSIG`

**解锁脚本：** `<sig>, <pubkey>`

# OP_GROUP

<colored_hash>, OP_GROUP, OP_DUP, OP_HASH160, <pubkeyHash>,OP_EQUALVERIFY, OP_CHECKSIG

# colored_hash

- 160-bit hash

- BCH地址

# 铸币

- <blue>为铸币者的地址
- <blue> =OP_GROUP identifier
- <blue> = hash160地址
- 铸币的input和output之间没有fee
- 如果要使用Fee需要另外使用input
- 使utxo具有不一样的标识

```
{
  "inputs": [
    {
      "outpoint": XXXXXXXXXX,
      "value": 1000000,
      "linkedScript": OP_DUP
OP_HASH160 <blue> OP_EQUALVERIFY
OP_CHECKSIG
    }
  ],
  "outputs": [
    {
      "value": 1000000,
      "script": <blue> OP_GROUP OP_DUP
OP_HASH160 <pubkeyHash> OP_EQUALVERIFY
OP_CHECKSIG
    }
  ]
}
```

# 铸币的描述文档

- OP_RETURN
- URL

```
[{
  "ticker": "string, required",
  "name": "string, optional",
  "summary": "string, optional",
  "description": "string, optional",
  "legal": "string, optional",
  "creator": "string, optional",
  "contact": { "method": "string, optional",
"method2": "string, optional" }
 },
"<signature>"]
```

# 彩色币转帐

- 输入和输出匹配
- 原子交换
- 正常的TX

```
{
  "inputs": [
    {
      "outpoint": XXXXXXXXXX,
      "value": 1000000,
      "linkedScript": <blue> OP_GROUP
OP_DUP OP_HASH160 <pubkeyHash>
OP_EQUALVERIFY OP_CHECKSIG
    }
  ],
  "outputs": [
    {
      "value": 1000000,
      "script": <blue> OP_GROUP OP_DUP
OP_HASH160 <pubkeyHash> OP_EQUALVERIFY
OP_CHECKSIG
    }
  ]
}
```

# 销毁彩色币

- 输入和输出的value匹配
- 满足原子交换
- 使用正常的TX
- 褪色
- 使用op_return作为记录

```
{
    "inputs": [
        {
            "outpoint": XXXXXXXXXX,
            "value": 1000000,
            "linkedScript": <blue>
OP_GROUP OP_DUP OP_HASH160
<pubkeyHash> OP_EQUALVERIFY
OP_CHECKSIG
        }
    ],
    "outputs": [
        {
            "value": 1000000,
            "script": OP_DUP
OP_HASH160 <pubkeyHash> OP_EQUALVERIFY
OP_CHECKSIG
        },
        {
            "value": 0,
            "script": OP_RETURN <blue>
        }
    ]
}
```

# OP_GROUP的安全边界

- OP_GROUP给UTXO一个特殊的标记
- OP_GROUP会标记UTXO，但不会改变
- OP_GROUP在操作码上是出了堆栈操作，但是只是为了平衡input和output
- OP_GROUP会增加一个操作码一个地址的空间

# 实现

- 全节点
- 钱包开发
- OP_GROUP的开发
- JSON-RPC的开发

# OP_GROUP的优点

- 完全复用现在BCH的交易系统
- OP_GROUP和脚本系统兼容，未来BCH上的脚本升级也可以在彩色币上使用
- 使UTXO具有了不同的属性
- 价值转移通过矿工
- SPV轻钱包支持

# 解决增发问题1

- 多重签名

- 监控地址

# 解决增发问题2

```
OP_CHAINHEIGHT <505500> OP_LESSTHAN OP_VERIFY <pubkey> OP_CHECKSIG
```

- 使用P2SH address替代P2PKH
- 类似的脚本保证只能发行一次
- OP_CHAINHEIGHT现在并没有这个操作码

# OP_GROUP和ERC2.0

- ERC2.0更加灵活
- ERC2.0合约内能解决增发的问题
- OP_GROUP的token会内含了BCH的价值
- OP_GROUP需要使用聪做单位
- 灰尘交易的问题（可以通过有op_group的tx不归类为灰尘交易解决）

# UTXO和账户的对比

- UTXO无需维护余额的
- UTXO是独立的数据记录，提升验证交易的速度
- UTXO下无需关心事务问题，只关心锁定脚本和解锁脚本
- 账户余额容易计算
- 账户容易记录
- 账户容易实现图灵完备的智能合约

# 关于OP_GROUP的争论

- 突破了以前脚本的限制
- 运行效果不如ERC2.0
- 何时上线的问题?

# 个人支持OP_GROUP尽快上线

- 在安全风险不会外溢的情况下
- 彩色币仍然存在一个不小的市场
- 无状态的智能合约也有很大的价值
- 代码先行，开发者应该提供更好的测试环境

# BCH上应该支持更多的创新

- 加密货币未来的竞争会更加的激烈
- BCH应该向BTC学习，也要向ETH以及向其它加密货币社区学习
- BCH应该加快进步的步伐

# BCH社区可能需要关注的技术点

- 更多的操作码
- 并行验证
- UTXO证明
- weak block
- 致密区块
- schnorr
- 分片
- 智能合约
- 跨链交易以及双向挂钩
- ……

# 谢谢 Q&A