Bytom公有链的安全设计

比原链
James

- Bytom是一种多样性比特资产的区块链交互协议，运行在比原链上的不同类型资产可以通过该协议进行交换、对赌和基于智能合约的复杂性交互操作

我们能做什么

- 无需信用背书的C2C的币币交易工具
- 去中心化的ICO众筹的基石
- 保证对赌协议得到公正执行的裁判
- 公司期权分配的管理者

——用区块链来安全管理/投资你的资产，以任何你想要的方式

Bytom链上资产

- 任何人都可以在Bytom上发行资产
- 比原基金会利用ODIN技术为公司/个人提供“区块链CA认证”
- 取得Root认证的公司可为自己旗下的资产发放二级认证

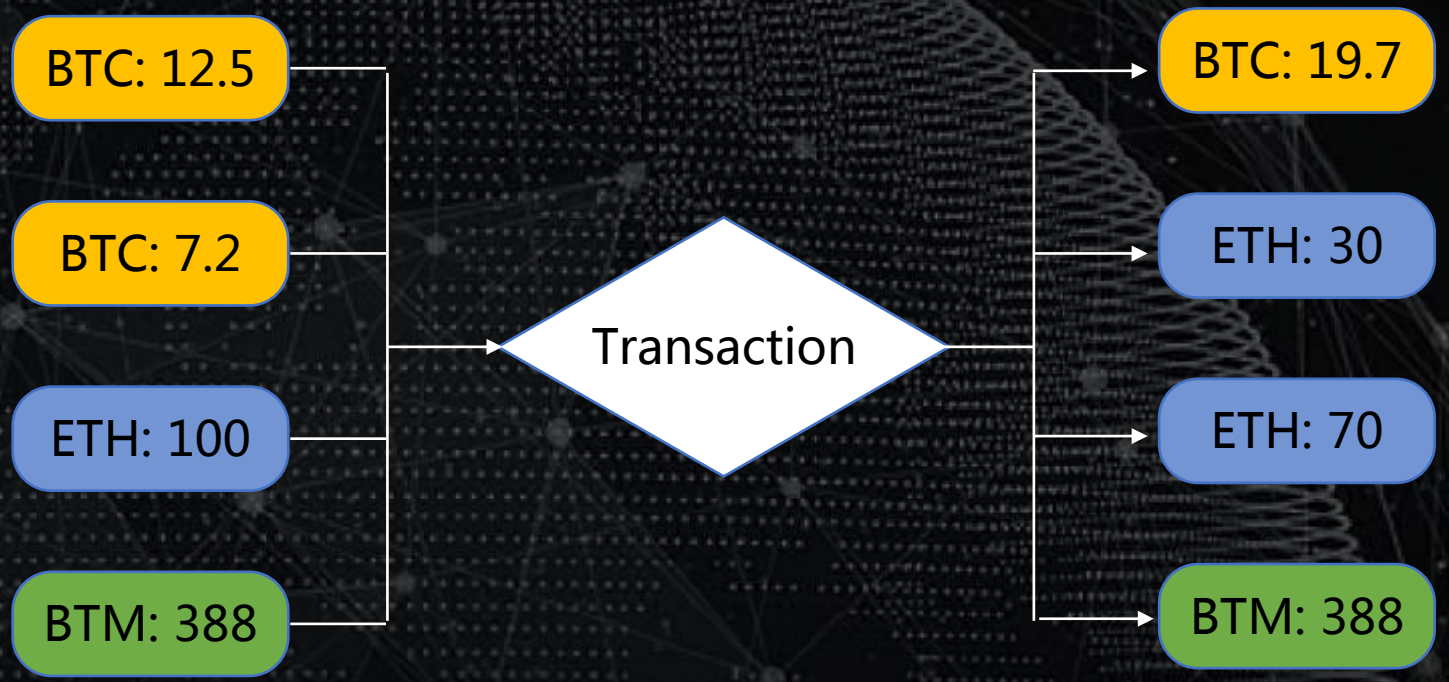
Bytom交易的设计

1. 一笔交易可同时操控多种类型的资产

2. 不同于以太坊的账户模型，Bytom上的资产是基于UTXO

3. 同种资产的多笔UTXO输入可以合并为一笔UTXO输出

4. 一笔资产的UTXO输入可以拆分为多笔UTXO输出



Bytom的智能合约

- 每一笔Bytom的链上资产UTXO都是由图灵完备的智能合约所守护
- 通用的资产转账使用默认的合约模版
- 自定义合约可由Ivy语言写完后编译而来
- 合约执行结果只有成功或失败两种状态，执行成功则解锁资产

```
b.AddOp(vm.OP_DUP).AddOp(vm.O
b.AddOp(vm.OP_SHA3)                                    // st
for _, p := range pubkeys {
    b.AddData(p)
}
b.AddInt64(int64(nrequired))
b.AddInt64(int64(len(pubkeys)))
b.AddOp(vm.OP_CHECKMULTISIG).AddOp(vm.OP_VERIFY)
b.AddOp(vm.OP_FROMALTSTACK)
b.AddInt64(0).AddOp(vm.OP_CHECKPREDICATE)
```

通用模版

```
contract C2CTrade(
            btc: Asset,
            btcAmount: Amount,
            seller: Program,
            cancelKey: PublicKey
          ) locks offered {
  clause trade() requires payment: btcAmount of btc {
    lock payment with seller
    unlock offered
  }
  clause cancel(sellerSig: Signature) {
    verify checkTxSig(cancelKey, sellerSig)
    unlock offered
  }
}
```

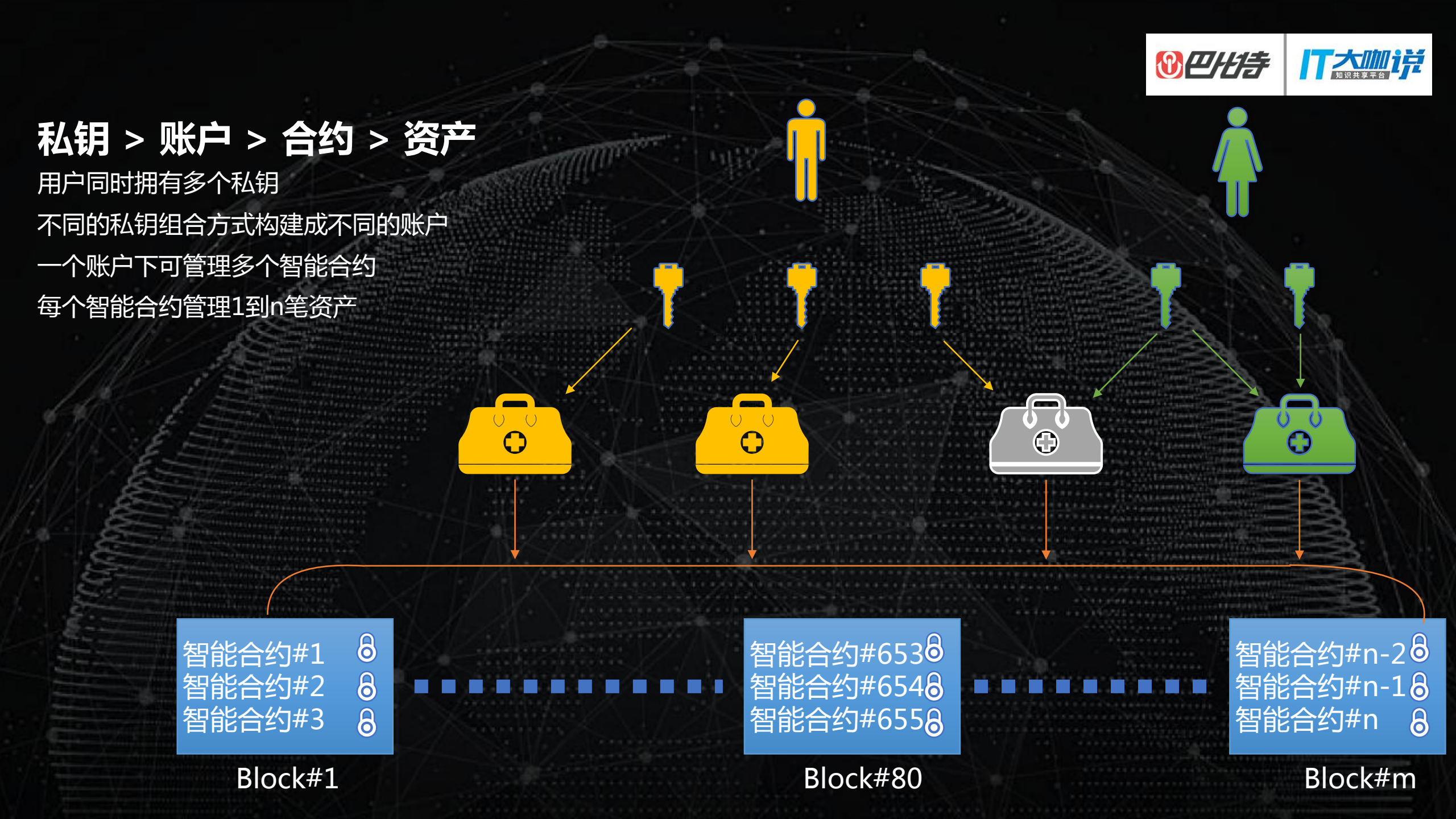
私钥 > 账户 > 合约 > 资产

用户同时拥有多个私钥

不同的私钥组合方式构建成不同的账户

一个账户下可管理多个智能合约

每个智能合约管理1到n笔资产



安全和隐私

- 账户只有本地可见，只有合约会被记录到区块链中
- 账户可推导出合约，但合约不能逆推回账户
- 账户下的每一笔交易都自动生成一个新合约，没有人可以找出交易之间的relation map

隐形合约

生成合约　　哈希合约　　合约哈希锁定链上资产

- 想发起一笔智能合约却不想让第三人知道合约的内容
- 使用智能合约的hash锁定资产
- 解锁资产的时候再将智能合约公开

更安全的合约调用

- 11月07日一个叫做devops199的人发现了以太坊Parity钱包的漏洞，使51.37万个以太冻结至今
- 这次错不在Parity钱包，漏洞出在钱包调用的一个library上
- 以太坊的合约调用是把地址当指针使用

- Bytom的合约调用是创建智能合约的时候就将其作为子合约加入进来
- 保证了合约写好之后不会因为任何外部因素而失效


Thanks, Question?