**隐私方案调查**

1. **同态加密**
2. **什么是同态加密**

如果我们有一个加密函数fe , 把明文A变成密文A’, 把明文B变成密文B’，也就是说 f(A) = A’ ，f(B) = B’ 。另外我们还有一个解密函数fd能够将fe加密后的密文解密成加密前的明文。

对于一般的加密函数，如果我们将A’和B’相加得到C’。我们用fd对C’进行解密得到的结果一般是毫无意义的乱码。

但是，如果fe是个可以进行同态加密的加密函数，我们对C’使用fd进行解密得到结果C，这时候的C = A + B。这样的算法称之为同态加密算法。

如果满足f(A)+f(B)=f(A+B) ,我们将这种加密函数叫做加法同态

如果满足f(A)\*f(B)=f(A\*B) ,我们将这种加密函数叫做乘法同态。

如果一个加密函数f只满足加法同态，就只能进行加减法运算；

如果一个加密函数f只满足乘法同态，就只能进行乘除法运算;

如果一个加密函数同时满足加法同态和乘法同态，称为全同态加密。那么这个使用这个加密函数完成各种加密后的运算(加减乘除、多项式求值、指数、对数、三角函数)。

1. **同态加密的应用场景**

现在同态加密有些使用在云端数据处理的场景，但是在区块链行业中暂时没有项目使用到，因为全同态加密算法的实现十分困难，现在还处在探索阶段。

1. **CryptoNote协议**

CryptoNote技术致力于开发注重隐私的虚拟货币。因为设计上的原因，比特币代码无法应用CryptoNote技术所开发的匿名功能。Bytecoin (BCN) 是第一个使用CryptoNote的虚拟货币，而XMR（门罗币）则是基于BCN 的代码。

CryptoNote有两个主要特征：分别是环签名（通过混合隐瞒发送人的身份认证）和无链接交易（通过为每笔交易创设一次性的钥匙来实现）。这两个特征可以实现高度的匿名性。

与比特币不同，你们的资金不是存在于你们公布于众的接受地址中。相反，每次你收到一笔资金，这笔资金会存到一个由无序数字生成的无链接地址。当你要花费存在于此一次性地址中的资金时，资金数目将会分解，且每一部分都与区块链中的身份认证输出无法区分。

网址： <https://cryptonote.org/>

1. **零知识证明**
2. **ZCash**

交易过程完全匿名是数字货币ZCash最大的亮点，正是这一点使得ZCash自提出以来便备受关注。其主要使用的就是zk-SNARK这一零知识证明的库，验证过程很高效，生成证明的效率太低。

1. **Fabric**

在fabric1.1的版本中提出了零知识证明的概念，在1.2和1.3版本中将其完善，具体可以参考idemix目录，通过 Identity Mixer 实现匿名客户端身份认证，以及通过零知识资产转移 (ZKAT) 实现保护隐私的资产交换

2.1 **使用 Identity Mixer 实现匿名客户端身份验证**

Hyperledger Fabric 1.1 技术预览版中提供了 Identity Mixer，这将成为 Hyperledger Fabric 1.2 中的一项发布功能。它利用 ZKP 为其交易中的客户端提供匿名身份认证。ZKP 协议发生在 Fabric 客户端（其秘密是其实际身份以及与其关联的任何属性）与其他网络实体（例如其对等节点）之间。这些实体希望确认交易创建者是特定组织的成员（称为“成员资格证明”），或拥有一组特定的属性（称为“属性选择性披露”）。

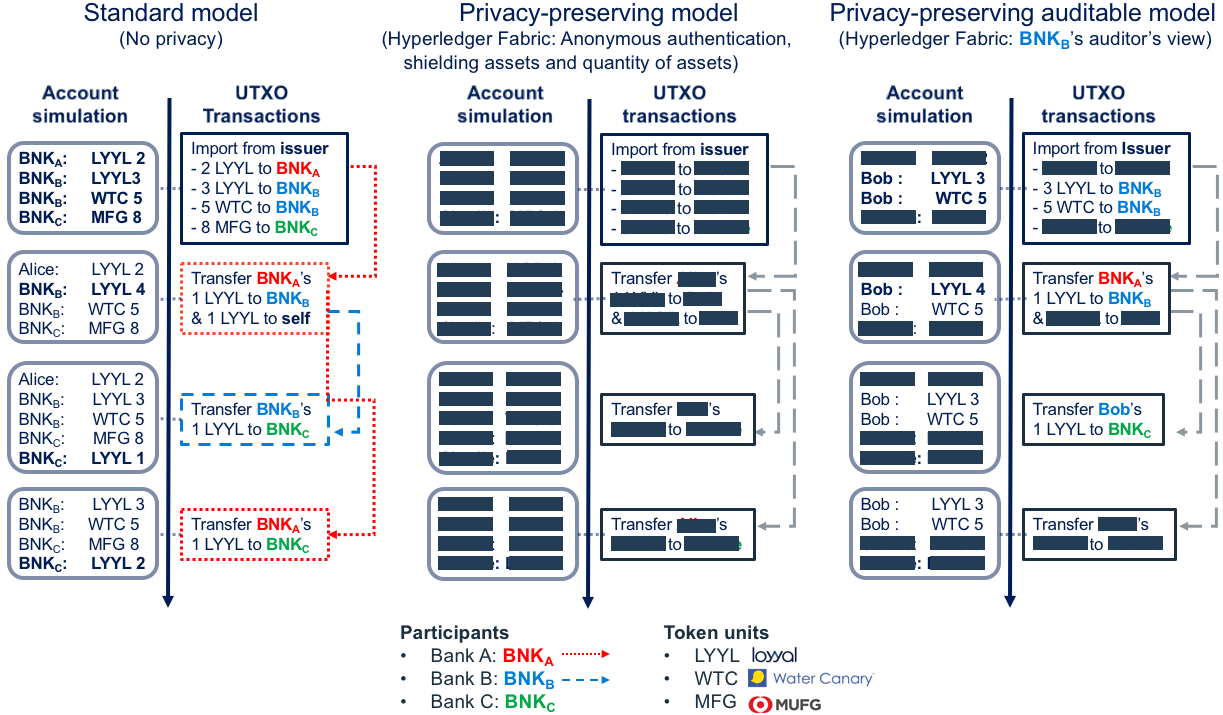
在这两种情况下，协议均保证，除了表明相应表述是否属实之外，不会透露有关客户端身份的一切信息。

**2.2 通过零知识资产转移 (ZKAT) 实现保护隐私的资产交换**

Hyperledger Fabric 将 ZKP 集成到面向资产管理的一系列更广泛的应用中。通过审计支持（也称为零知识资产转移或 ZKAT）来适应隐私保护资产管理。它允许交易者发布资产并请求转移资产，除了表明转移行为符合资产管理规则以外，不会向公共账本透露交易资产的任何信息（即每个资产均按其所有者的要求进行转移，不会通过转移创造新的价值）。ZKAT 建立在 Identity Mixer 提供的匿名身份认证机制之上。

与区块链的其他隐私保护资产管理系统不同，ZKAT 为企业网络的需求量身定制。尤其值得注意的是，隐私保护交易的可审计性是明显不同于其他可用方案的一个关键特征。每个用户都被分配了一个特定的审计员，此人有权无限制地访问该用户的所有交易。审计员是被动的；他们可能会在事后提取审计用户参与的所有交易的机密信息，但他们无法访问任何其他方的数据。

现有的区块链系统目前采用了三种隐私资产管理模型（仅基于未花费的交易输出模型）。下图中对此进行了解释，其中三家银行（A 银行、B 银行和 C 银行）在区块链上交易三种资产（涉及 Loyyal、Water Canary 和 MUFG）。



在该图中，左侧的模型无隐私机制。中间的模型支持完全隐私性，隐藏交易参与者的身份和交易资产细节。右边的模型展示了 ZKAT 的安全审计能力，分配给特定银行的审计员可以无限制访问该银行涉及的所有交易。

支持审计的隐私性在金融用例中尤为有用。银行通过高于他们所获得的资金成本的利率贷款来赚钱。因此，如果一家银行使用的区块链网络应用了这种先进的 ZKP 功能，那么他们可能想要在不泄露交易事实的同时，与交易人交换资产（金钱），并在共享账本中记录相应的交易，或交易中交换的资产数目。如果不这样做，显然会危及他们的保密规定，并暴露他们的业务模式。

凭借零知识证明，可在账本上显示交易，并包含表明资产（金钱）已经交换的可供核实的证据，而不会泄露贷款利率或银行交易的数量以及交易方，这样银行就能够在任何特定时间了解其现金的流动性。Hyperledger Fabric 的额外优势是现在可以基于 ZKAT 对其进行审计。

1. **Ethereum**

2017年底以太坊创始人Vitalik Buter在一次演讲中介绍说，零知识证明(Zero knowledge proofs)是“最为强大”的解决方案，尽管技术实现难度最高，但在保护在以太坊网络的隐私性和安全性上，其效果最佳。

Vitalik Buterin还认为，零知识证明能够被应用于以太坊区块链上几乎所有的场景。他透露，在2018年的升级优化中，以太坊零知识证明的生成证明效率将得到大幅改善，削减到七秒。

但是在最新的以太坊源码中并未找到有关零知识证明的代码。

1. **CoinJoin（混币技术）**
2. **达世币——即之前的暗黑币（DarkCoin）**

达世币有三种转账方式，一是像比特币一样的普通转账；二是即时交易。不需要矿工打包确认，就可以确认交易，几乎可以实现秒到；三是匿名交易。从区块链上看不到是谁和谁进行了转账。

达世币如何进行匿名交易呢？达世币中除了普通节点之外，还有一种节点叫“主节点”。主节点可以提供一系列服务，如：匿名交易和即时支付。想进行匿名交易的交易者发起匿名申请，由主节点进行混币，一般是3笔交易一起进行混币。举个例子，一桌人把自己的钱都放在桌上，混在一起，然后再分别拿回相应面值的钱，这样就不知道你手里的钱到底是谁的了，这就是混币。混币后，网络就不知道究竟谁转账给了谁。

Darksend 是 CoinJoin（提供匿名技术的软件）的改进和扩展版本。除了拥有CoinJoin的核心理念，还进行一系列的改进，例如去中心化、使用链接实现强匿名、相同面值和被动先进的混币技术。（摘自于达世币白皮书）