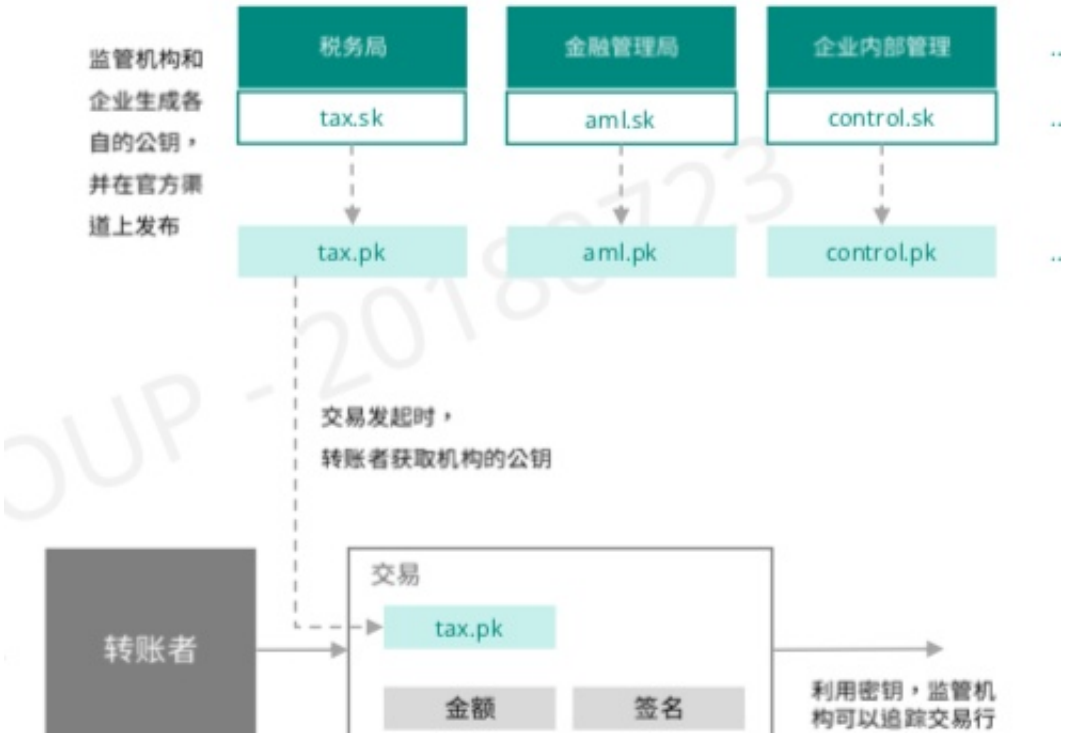

不过，Duncan Wong 表示，监管机构在解密之后也只能看到一个数值，并不能验证加密后的数值是不是加密前的数值，即 A 可能作假，发给 B 只有 5 个 ABE，但是却用 10 个 ABE 进行加密。

那么如何避免作假呢？这就可以通过可验证加密技术来实现。Duncan Wong 表示，相比于零知识证明，可验证加密技术的好处是能提升整个效率。

可验证加密技术至少有 15 年的历史，之前经常用到“群签名”中，“群签名”与加密货币中用到的“环签名”有些像， 最大的不同在于“群签名“有一个中心，这个中心知道真正的签名者是谁，而大众不知道。

ABE 将可验证加密技术引入到 ABE 的可问责隐私中，其中的这个“中心”角色，就由 ABE 网络中的监管机构/企业来担任。

对于具体的使用场景，Duncan Wong 举例称，在物业场景中，如果选用门罗币，那么任何人都不知道你的交易金额、地址，包括物业公司；如果选用比特币，那么任何人都能看到你的交易记录；如果选用 ABE，那么，只有物业公司可以看到你交易记录，从而达到平衡隐私与监管的效果。

抗量子攻击——格密码

ABE 在隐私方面是如何实现抗量子攻击的呢？

针对实现抗量子攻击的必要性，Duncan Wong 表示，目前大多数加密货币将 1980
年代发明的椭圆曲线密码技术作为其签名系统的基础，但是量子计算出现后，NSA 在 2015 年 8 月公开提醒这项技术存在安全隐患。Duncan Wong
认为，量子计算机有可能在 5—10 年内破解椭圆曲线密码技术。

目前，主流的后量子密码技术有四类：Hash-based cryptography（基于Hash函数的后量子密码）；Multivariate-quadratic-equations
cryptography（基于多变量二次方程的后量子密码）；Code-based
cryptography（基于编码理论的后量子密码）；Lattice-based
cryptography（基于格理论的后量子密码）。

ABE 将其中的格密码（lattice-based
cryptography）
技术引入加密数字货币中，基于格密码的数学难题，目前还没有有效的算法能够将其破解。

格密码技术与椭圆曲线加密算法（ECC）技术相比，Duncan Wong 表示，其优势在于矩阵算法，效率会更高，不足在于基于格的公钥、签名、证明等的尺寸太大，导致效率低。所以格密码的优劣相抵后，其效率与 ECC
的效率相差无几，但是却可抗量子攻击。

针对尺寸太大的基于格的公钥、签名、证明等，ABE
的策略主要是增加区块尺寸、缩短出块时间以及将 IPFS
作为数据的存储层和检索层（通过哈希指针）。