**全面解析多种区块链隐私保护解决方案**

随着对区块链潜力的探索，银行很快就会推测出这种技术并不像它当初设想的那样能够提供强大的隐私保护。

当中本聪于2009年发明比特币时，他（也许是她或他们）就提供了一种方式供无条件信赖彼此的参与者们协作维护规范且防篡改的交易和电子信息纪录。但这种设计要求所有活动要展现在所有人面前。

一种叫做Zcash的新型匿名数字货币的创始人之一Zooko Wilcox说，“他不得不牺牲机密性。尽管他为了保留它告诉你可以有多个不同的付款地址，但并不能很好地保护机密性。”

这对于金融机构来说有些遗憾，因为它们虽然想从共享账本削减组织成本的优势中获益，但受法律及自身竞争本质的限制必须保证大量业务活动的机密性。

德意志银行全球交易银行首席数字官Edward Budd表示：“对区块链的隐私要求和当前对其他金融市场所采用的技术的规定没有任何不同。因此，任何分布式账本技术的潜在应用都要确保达到金融服务规定的行业安全高标准。”

在过去一年间，软件开发者和加密工程师们投入了大量的时间和资源制定计划来保护基于区块链进行交易的用户的隐私。

去年11月，探索区块链金融应用的银行联盟R3的研究部门向其成员公布了一项研究报告，介绍了最有前景的解决方案。这项研究之前没有公开，它提供了每种方法的隐私级别的细分，同时审查不可避免地参与其中的交易。

经许可方式

银行已经将精力投入到了构建许可账本中去（依靠自己或作为类似R3的联盟的成员），这种策略将区块链的参与者限制在了已知实体的范围内。这在一定程度上是由于银行不愿意依靠匿名操作者确认交易引起的，更不用说反洗钱和了解客户的规定了，这些规定要求银行广泛审查其交易方。但是限制参与者的另一个好处是它限制了谁可以阅读账本并查看交易。

R3研究报告的作者们将限制阅读权限称为保护隐私的“低技术”选项。许可账本通过摆脱挖矿可以加速处理进程，比特币和以太坊中需要用它来确定交易顺序，但会花费大量的时间和精力。

然而，仅凭许可账本还不足以保护参与者不受反垄断和内幕交易法律的限制，这些法律规定即使是同一金融机构的不同部门之间也需要保密。

“如果我在高盛，然后打电话告诉你我们和摩根大通在做很多笔交易，那我八成要陷入法律纠纷了。而这正是你在这些许可网络里会得到的信息，即便你根本还没搞清状况。”纽约梅隆银行新兴业务与技术部门副总裁Jared Harwayne-Gidansky如此说道，“无论从法律监管还是从竞争因素来看，这都是个问题。”

去链方式

侧链、状态渠道和去链消息传递都是进一步隔离主区块链数据的方法。 它们在区块链作为确定记录被保留的程度上有所不同。在摩根大通Quorum这样的系统中，私人消息被去链中继，而它们的加密指纹或哈希被包含在区块链中，作为事件发生的证明。

哈希是单向加扰函数; 如果你只有哈希算法和一串随机的数字字符，那么找出原始数据所耗时间是无法想象的，但该数据每次都会立即产生相同的哈希。 即使对数据进行最小的修改也将完全更改哈希，如下表所示：

侧链和状态渠道允许各方在平行的、私人控制且显示资产的链上进行交易，进而在可调和的更开放的公共链上进行交易。

在解决许多隐私问题的同时，这些去链方法放弃了开放式区块链技术的一个主要特性，这是面对多台计算机拥有重复相同数据的现象做出的调整。

“由于区块链是分布式技术，这就意味着你不会失败。”R3研究报告的主要作者兼Zcash另一位创始人Jack Gavigan说， “例如，如果Facebook出了问题，你就无法访问它了。 但是如果单个区块链节点出了问题，这并不代表你不能访问区块链。它只是意味着你会连接到另一个节点上。”

当交易发生在普遍共享的主要区块链之外时，他们就无法从这个关键特点中受益了。

挖矿

比特币区块链存储每枚币的完整交易纪录，包括它被谁拥有（即它被分配到哪个地址）及何时被消费。将来自多个用户的货币混在一起，进行洗牌，将它们分成较小的量，然后将钱重新分配给预期的接收者，以便将交易历史随机化。

早期的混币服务由第三方运营，用户不得不暂时将钱委托给他们。现在有了其他的去中心化方法，如CoinJoin，允许多人联合签署单个交易给多个收款人。其结果比依靠第三方（他们可能会保留预定的预混交易记录或挪用资金）更安全。一位匿名作者在去年夏天在一篇文章中概述了 MimbleWimble计划，它甚至可以将所有交易混合到所创建的每个新区块中。

理想的混币服务会合并许多随机交易，并在延迟之后分配资金，这意味着它很缓慢并需要协调。

此外，混币业务不太可能为金融业监管者所接受。

Gavigan表示，“如果你对监管者说， ‘没错，我们通过将客户的交易与一大堆其他交易混合为他们实现实现隐私保护和保密，’ 那么监管者可能不太会认可。但是如果资产的来源并不重要，那么它就可能是完全有效的。”

环签名

环签名最初被描述为CryptoNote协议的一部分——该协议在数字货币Monero中执行，用来隐藏交易的发送地址。使用环形签名可以使交易拥有多个发送者，而其中只有一个是真的。仅仅通过查看环签名不可能辨别是哪个地址发起并最终签署了交易。

但其他观察可能增加攻击者的猜测机会。例如，查看来自每个地址的先前交易可能透露交易在一天中最容易发生的时间或交易图分析中使用的其他数据。

和Gavigan一起撰写研究报告的Wilcox称之为“匿于人群中”的策略，并认为它的成功取决于人群的规模和人口随机性。 （需要注意的是Monero与他的项目Zcash存在激烈竞争。）

Monero使用被称为三角分布的方法选择迷惑性地址，该方法倾向于选择在最近交易中频繁使用货币的地址，因此看起来比货币闲置的地址更真实。

Monero源代码的主要维护者Riccardo Spagni表示，“每个环签名至少包含一个最近的输出，要么是因为用户想要消费最近的输出，要么因为虽然他们没有，但我们总想在其中设置最近的输出。这是没有办法知道的，也意味着分析回到了假设环中的每个输出是候选者的论点上来。”

Pederson承诺

Pedersen承诺是比特币核心开发商Greg Maxwell保密交易的关键要素，是Monero的附加条款。

该技术允许发送方通过在区块链上将其作为哈希进行传播来承诺交易量且不用向一般公众泄露。然后，用户可以通过再现存储在区块链上的哈希作为证明来向接收者或可能需要了解该信息的任何其他人（如监管者）揭示金额。

Pederson承诺也是可转让的，使得接收它的人可以在其他地方再次消费，且不会暴露金额。 这是因为选择的哈希是同态的，意味着你可以对它们做简单的算术函数运算，如减法和加法，而不需要解密数据。 此功能使矿工和验证节点检查交易的输入和输出是否彼此抵消，没有人会使用自己没有的货币。

零知识证明

零知识证明是Zcash的关键特点。它的显着特征是，你不必揭示数据的内容就可以使用它来证明关于一组数据的陈述。以Zcash为例，零知识证明用于对加密的交易数据执行加密验证，使发送者和交易额被证明是合法的（尽管它们仍是私有的）。

R3委托的研究报告的作者中，有两位创立了公司并了解到Zcash的发展，他们提到零知识证明的缺点之一是速度缓慢。该计算需要大约48秒完成。除非提高性能，否则零知识证明可能不适合诸如高吞吐量交易的应用，因为它们需要尽快得到结果。

零知识证明还有一个更大的问题。为了在像Zcash这样的电子货币中执行它，开发人员必须酝酿一些其他加密元素，即参数，并将它们加入系统中。该过程衍生出了一种危险的副产品——私钥，可以用于制造假币。任何使用Zcash的人都必须相信参数已经创建且私钥已被彻底销毁 ——这对于彻底的分散主义者来很是煞风景，尽管已经采取了详细的措施来缓解这个问题。

Zcash团队采用了一种去中心参数生成过程，旨在确保私钥的完整副本不会出现。为此，他们创造了六个独立的关键碎片，分散在世界各地的站点中。然后参与者使用他们的分片在协作进行一系列的计算，从而生成一组完整的参数，但不需要在团体内共享自己的分片。最后，每个站店都要毁掉它自己的密钥部分。 如果要破坏这个过程，攻击者必须得到这六个关键碎片并将其拼凑起来。

隐形地址

根据最初的设计，比特币需要想要接收货币的人向发送者提供地址。隐形地址使这个流程颠倒过来。发送者可以创建地址并填上交易。即使地址是新的，发送者也确定接收者拥有将其打开的相应钥匙。

隐藏地址为交易的双方提供了一种无需向系统中其他人传播信息就能确定目的地址的方法，并且不需要共享可能受接收方控制的其他地址。

这些技术每一种解决了一部分的谜题，但我们现在开始寻求如何将它们拼凑起来以构建更全面的隐私保护。

Gavigan说，“许多执行策略都采用了多种不同的技术，并将它们组合在一起以实现相加的结果。 很可能不同技术的结合会产生更好的解决方案。”

同时，他表示，没有办法概括基于区块链技术的公司的需求，因为每家公司想要实现的东西都各不相同。

“从某些方面来看，区块链技术有点像盲人摸象，”Gavigan说， “一个人摸到腿觉得是树干。 另一个人摸到身体觉得是堵墙。而第三个人摸到鼻子觉得是条蛇。”

# 如何保护区块链中的隐私性？已探索出4种方案

目前来看，隐私性的问题确实存在。如果我们仅仅是为了保护区块链交易的安全性，而对隐私性的问题视而不见，或者通过削减节点的方式来使两者得到兼顾，那么我不认为这是妥善有益的解决方法。

由此，该如何在保证安全性的前提下，让隐私性得到保护？发展至今，我们探索出了几种解决方案。

其中有一些是尚存在于理论上的技术解决方案，还有一些是使用上高科技手段的“黑科技”解决方案。下面我开始介绍四种主要的解决方案。

编译：吴阳煜

在2017年12月3日举办的亚太以太坊技术交流会上，以太坊创始人Vitalik Buter压轴出场，发表了主题为“以太坊区块链中的隐私保护”演讲。

在演讲中，Vitalik Buterin为在场听众介绍了四种适用于以太坊区块链的兼顾隐私性和安全性的解决方案：通道（Channels）、混合器（Mixers）、环签名（Ring Signature）及零知识证明(Zero knowledge proofs)。

在其中，他特别提到，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，在明年的升级优化中，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。

他对这些引入应用了以太坊最为前沿技术的解决方案充满信心。

在日前台北BeyondBlock的技术交流会上，Vitalik表示，以太坊隐私性的问题已经被解决了四分之三了，但还有四分之一没有解决，“而在未来这些解决方案必定能随着以太坊的发展，得到更普遍地运用。”

以下为Vitalik Buterin演讲全文（略有删减）：

安全性与隐私性的两难困境



作为一项新兴技术，区块链无疑显露出了更为安全的特性。区块链为什么安全？安全性体现在哪里呢？

因为区块链通过节点，来验证每一个区块上发起的交易。

目前在以太坊的区块链上，全球范围内有25000个节点，其中包括了用户们为推行网络间项目而运行的节点，也包括了交易所管理运行的节点，还包括了矿工们运行的节点。

所以每一笔在以太坊区块链上发起的交易，它的过程都会被全网广播让所有人知道。

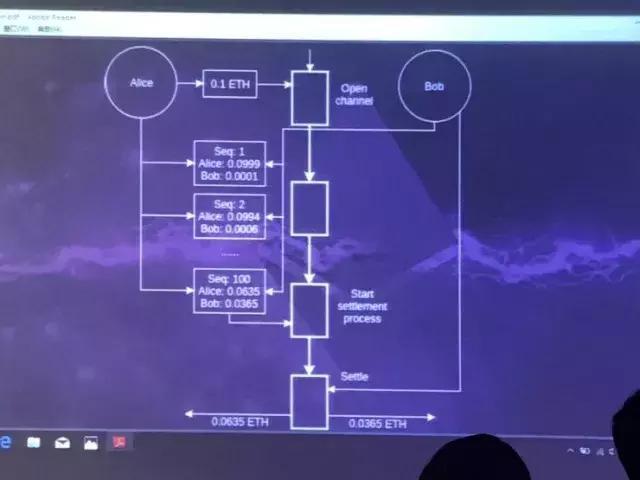
这样是好是坏？从一方面来讲，它保证了每笔交易的安全性。但在另一方面，它确确实实对以太坊网络的用户造成了很大的隐私性问题。

目前来看，每个人都能从这25000个节点中查询到每一单笔交易，交易的具体价格都能被其他所有人看到，每个人发起的交易都成为了链上的公共项目，那么用户的隐私该从从何谈起？

故从目前来看，隐私性的问题确实存在。如果我们仅仅是为了保护区块链交易的安全性，而对隐私性的问题视而不见，或者通过削减节点的方式来使两者得到兼顾，那么我不认为这是妥善有益的解决方法。由此，该如何在保证安全性的前提下，让隐私性得到保护？

发展至今，我们探索出了几种解决方案。其中有一些是尚存在于理论上的技术解决方案，还有一些是使用上高科技手段的“黑科技”解决方案。下面我开始介绍四种主要的解决方案。

解决方案之一：通道(Channels)



第一个我想要介绍的主要解决方案是通道解决方案。支付手段的革新，推动了通道技术的发展。从交易的两方来分别观察这样一个支付通道,其实就是将其开启以后，其中一方便通过它，向另一方发起执行包含交易的智能合约的请求的这样一个过程。

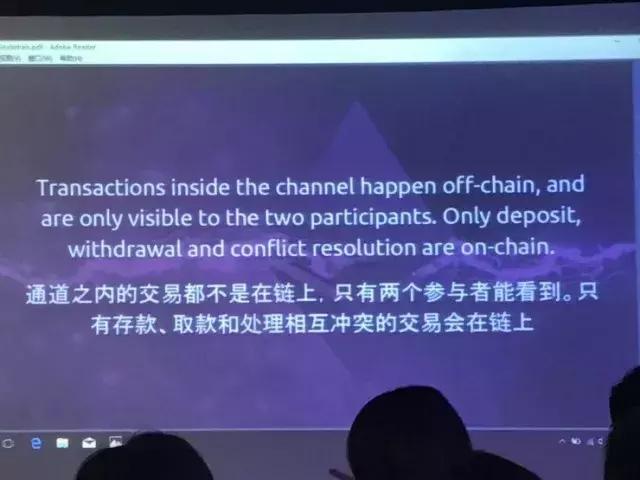
交易双方的隐私性如何得到保护？在我们的网络中，假设有交易两方分别名为Alice和Bob，Alice向Bob发送了双方的交易总额为0.1以太币的智能合约，这个智能合约就代表了支付通道。在发起以后，交易都是在链下进行，支付操作也发生在线下。

作为交易的两方，只有Alice和Bob才能掌握到交易其中的详细信息，通过这一通道发起的交易，和票据交易类似，只有其中任何一方才能进行彼此验证、查看和签名。每一笔交易，都需要Alice签名发出，经由通道被Bob得到，再签名验证。

如图所示，即使是交易额很小的一笔交易，也需要另一方的签名来确认完成。在序列号为1的交易中，我们看到“Alice:0.0999 Bob:0.0001”的字样，这代表着什么？代表着：“我 ，Alice，持有着0.0999的以太币，经过签名确认，向持有0.0001的Bob发起交易”。接着，序列号为2的“票据”亦是同理。

那么，如果还想发起一笔交易，就还需要签名。签名次数越高，说明交易发生的越晚，通过这种方式可以知道交易发起的次序，一直到序列号100的那笔交易，Alice持有0.0635的以太币，而Bob持有0.0365的以太币，从而能够最终确认，在他们总共包含0.1以太币的智能合约交易中，Alice持有0.0635，Bob持有剩余的0.0365。所以，一笔交易的序列号越大，意味着这笔交易越能体现交易双方的近况。

如果，任何一方想起将交易进行溯源查看，只要凭着收到的序列号更高的票据，以此为准，就能根据最近的这一票据进行交易核实。



通道之内的交易都发生在链下，只有参与交易的双方才能看到。并且，只有那些在存款、取款和解决途径出现冲突的交易才会被放到链上。

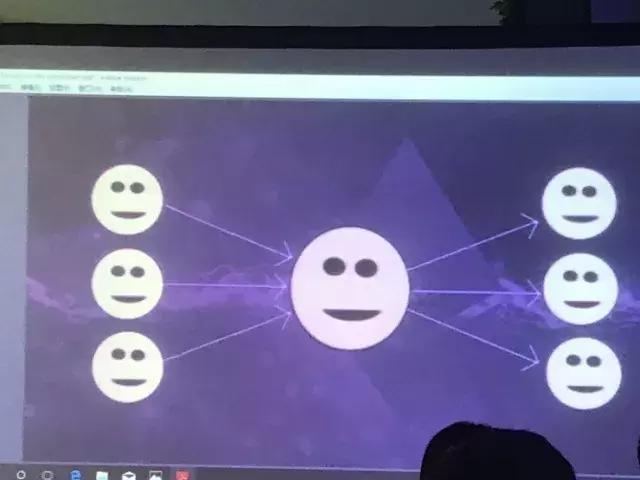
什么是出现冲突的解决途径？继续以Alice和Bob的例子来说明，假如发起交易的Alice一方无法辨认或者不承认Bob的签名，那么智能合约就会认为这笔交易不被交易双方所接受而将其提交至链上待双方追溯处理。

所以，用“通道”这样的方式来发起交易，安全性与在区块链上发起的交易基本一致，但同时保障了交易方的隐私性。

通道解决方案，是完全建立在更高的可拓展性前提之上而得到发明的。你可以在通道中发起交易，而不会使这些交易都暴露在区块链上，原因就在于，每个没有上链的票据，都不会被参与方之外的人看到。

而且同时，任何引入该项解决方案的应用，也能够得到更大的扩展性。

解决方案之二：混合器（Mixers）



接下来是第二种也相对比较“简单”的解决方案，混合器。什么是混合器？

一般来说，在区块链上发起一笔交易，交易双方都需要知道彼此的地址，而在混合器解决方案中，设置好一个与所有交易方都相连的中心平台，左侧的交易方A1把需要交易的货币和A2的地址发予该平台后，B1、C1亦进行同样的操作，对于右侧的A2、B2、C2也是一样。

这样，交易方需要把账户上的货币，发到另一个相连的中心平台，保证彼此打乱联系后，再重新发送到事先指定好的地址里。

在链上参与方以外的人看来，他们只知道A1、B1、C1这些用户，和A2、B2、C2这些用户发生了交易，却不知道它们相互之间具体的对应关系。

但是这也意味着，在混合器解决方案中，需要一个中心化的服务器的存在。左右两侧的交易方都将货币发送到中心处理器，告诉中心处理器（混合器）应该发到哪里。

这个方式很简单，但不仅保护了隐私性，这个地址不会上链，别人不会看到，但需要充分信任中心处理器，这是基于纯粹第三方的信任。



所以，我们进一步发明了Coin Join改良版本，通过引入智能合约的特性来削弱这种中心化的趋势，同时在一定程度上兼顾其安全性和隐私性。 总的来说，分为三个步骤来完成整个流程：

第一步，在明确了有哪些人涉及到交易之后，将Coin Join智能合约发送给这些参与方；

第二步，在智能合约中，每个人都需明确交易对象和具体指定一个交易地址，来发送货币；

而第三步，即在执行环节，需要得到所有的参与者的同意后才会执行。

只有有一个人不同意，这个进程就会被终止。如果顺利，智能合约会最终被发往到在第一步中各参与方的地址中。

在Coin Join混合器解决方案中，通过这三个步骤来执行交易虽然复杂了一点，还会对交易的效率产生一定的影响，但能最大程度保护交易各方的隐私性，他们的代币和那些使用了该技术的应用的安全性也能得到保障。



说到在其他应用上的扩展性，不仅限于虚拟加密货币的交易应用，只要出于加密处理过的隐私保护需求考虑，都能采用混合器解决方案来解决问题。

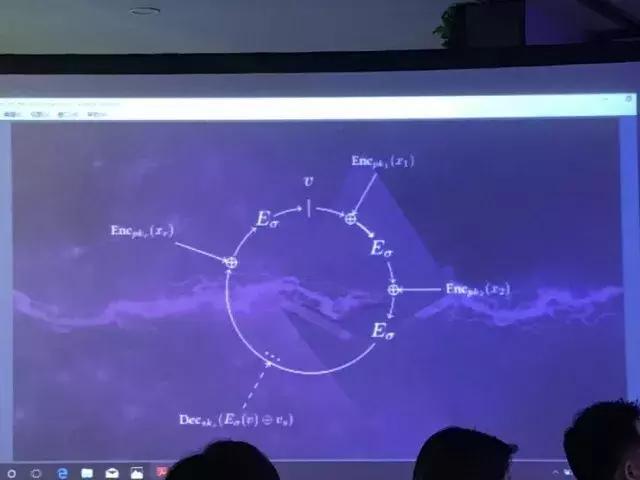
在抵抗Sybil攻击上，采用了混合器解决方案之后，还能防止一个用户创造过多的账户来达到攻击的目的，原理即为用这种算法来提供隐私性的保护，使得在混合器解决方案中，用户和账户之间的一致性和有限性得到了保证。

同理，由于这种特质，混合器解决方案还能被应用在隐私性受保护的匿名投票中。



解决方案之三：环签名（Ring Signature）

除了上述两种解决方案，我们还发明了其他不同的高科技的解决方案。这些“黑科技”解决方案，包括了零知识证明，一种在最近十年或二十年才萌生的密码学领域的新型协议，也包括了环签名，它们都采用了密码学中的技术。



所谓的环签名，是一种特殊的群签名组成的协议。在其中，你需要证明的是，你拥有着这组群签名中的任意一个签名的签署权。

在这种情况下，你可以告诉别人，这里有五个签名，其中有一个是你自己的签名。这样，我传送了一段信息给别人，就能够通过这组环签名中专属于我的签名来证实我就是我，不可能是别人。

但是，你仅能证明你的签名存在于这组环签名之中，不能证明确切哪个是你的的签名。

通过这些可读的环签名，你可以具体指定一个账户地址进行加密货币的交易，别人无法得知发送的这些信息源头在哪里，而只知道你是这五个签名中的一个，但是，如果在同一笔交易中出现了两次你的签名，那环签名的匿名性就被破解了。

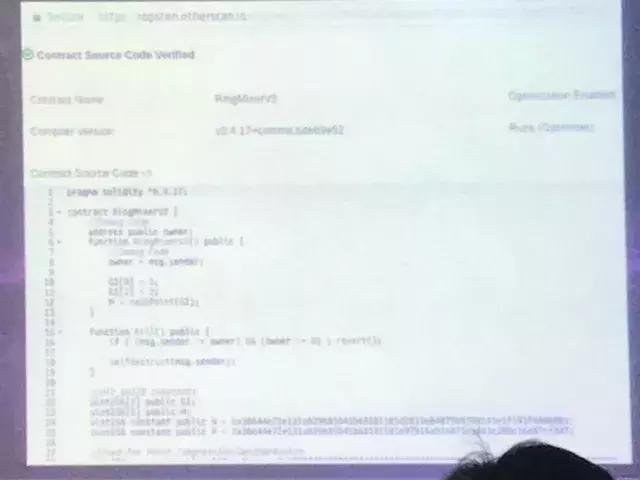
所以，你可以故意“泄露”一个你的签名，来证明你是这组环签名的所有者之一，但别人只知道你是成员之一 ，却不知道这组环签名代表的资产具体的持有者是谁。



并且，这五个签名之间相互连接，同时可以任意拎一个出来，而对于别人，只会看到里面有五个签名，得以证明资产是五个人签名的所有者之一。

还有，如果用环形签名来进行加密处理，组合运用在混合器解决方案中，只要给出了一次环形签名，隐私性和安全性就能得到保护，效果比其他的解决方案更好。

在混合器中执行交易时，你只要确定一次交易约定，就得到这组交易签名的签署权，但不能签两个名。所以，这使得用户能够在确保去中心化的原则下，和现有的单一环签名技术相比，能更为兼容地保护隐私性和安全性。



在上个月以太坊社区，有关于隐私性保护解决方案的动态更新，使得通过环签名的方式来验证智能合约成为了可能，并在测试网络中表现良好。

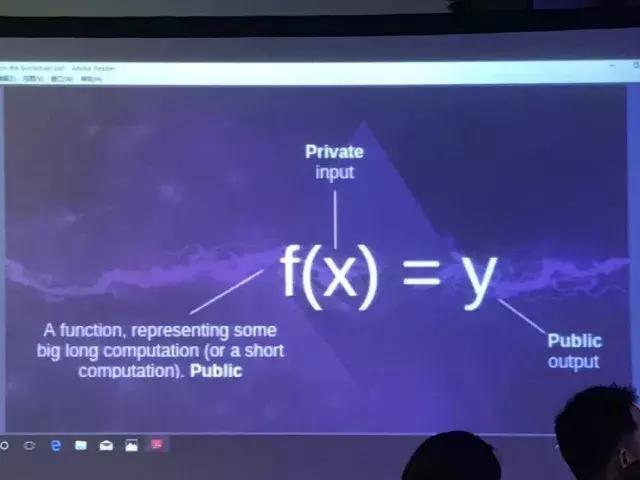
所以，无论你是否曾试用过这项技术，现在在这里，可以作为这项技术真正开始落地应用的起点。

解决方案之四：零知识证明（Zero knowledge proofs）

接下来介绍的解决方案，所应用技术更为“高科技”，我们称之为零知识证明。在保护隐私性上，它也许是使用的技术最为前沿的解决方案，同时也是最强大的。

一般来说，我们该怎么去描述零知识证明？我们可以讲，上述的环签名技术为一种弱化的零知识证明，但接下来我们探讨的是，一般意义上的零知识证明。

我们可以这样来理解，你拥有着一些数字，同时也存在着一个有空缺的等式，你需要证明的是你无需借助任何其他知识，知道填入这个等式的数字是什么，从而使这个等式成立。



这个等式用的数字无论经过加密与否，所有人都能看到，如果它能够让等式成立，这就是零知识证明。不需要经过其他底层数据的辅助即可直接通过验证。

难度最高，保护程度最好

在以往，我们为了证明某些事情，需要引入或借助另外的知识或数据来达到目的，但在零知识证明中，我们无需其他任何底层数据来完成这个证明过程。在区块链公有链的交易中，运用零知识证明使得不需要添加或向外界透露更多的信息即可完成整个交易流程。

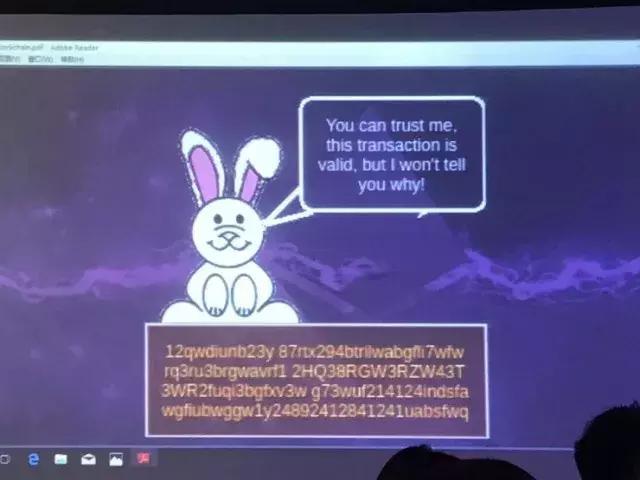
实际上，它支持所有基于公有链的服务。在我们全球的25000个节点的交易中，交易过程可能被加密，但我们不需要对其进行解密。

如果都应用上零知证明，每个区块中将只会有哈希数据的存在，它们已经足够支持整个公有链上的交易运行。

通过零知识证明，我们依然可以在不知道关于每一笔交易更多信息的前提，追溯每一笔交易，可以明白一笔交易是接在哪一项交易之后，也依然能知道每笔交易发起的时间。所以，这真的是一项非常强大的保护隐私性的技术。

我认为，在全球范围内的公有链上的每一笔交易都需要引入零知识证明，用户能够在并不需要知道其他更多的交易信息的情况下即可进行验证。事实上，在过去一年多的时间中，Zcash已经在其代币交易中使用该技术，表现良好。

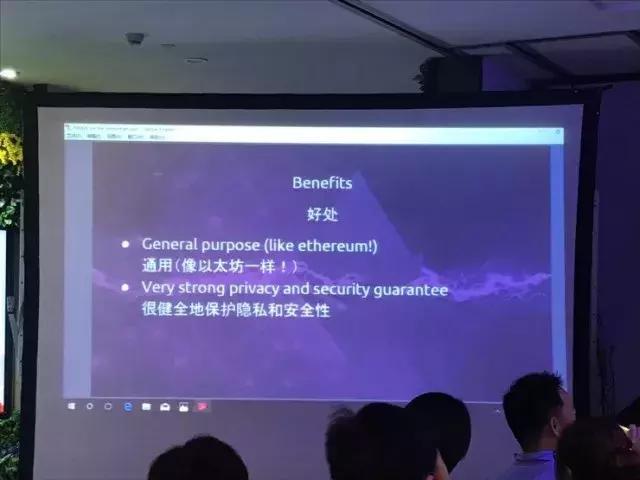
在除去虚拟货币交易以外的其他领域，同样存在着应用零知识证明的巨大潜力空间。在区块链上数以千计的应用，都能够通过调整让零知识证明得以应用。



而我们遇到的问题是，如何将零知识证明作为通用的方案，在广泛范围内应用起来？在以往，困难在于经过加密的数字几乎不可能被写入智能合约中，来进行零知识证明。

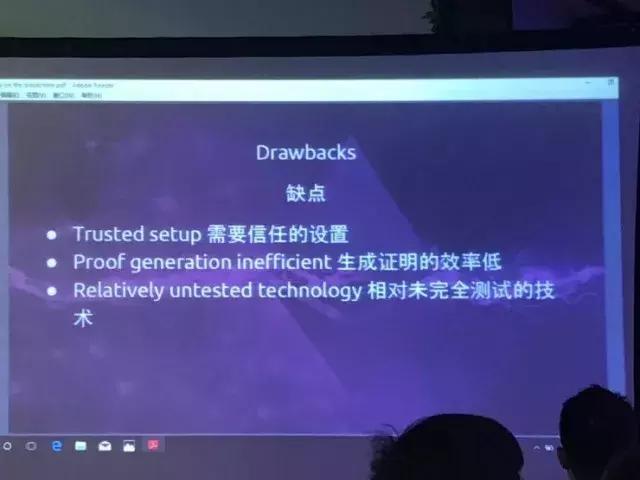
但是，只要你提供的这个答案能够被填入这个等式成立，便能证明你对这个等式有唯一的正确解。

在对这个等式提供了解决答案后，将其放入一个集群中进行优先编译，在其中，它提供所有可能需要的工具来对其进行编译，从而说明零知识证明能够用于所有的场景，最大程度上保证去中心化的原则，并最大程度上对交易的隐私性和安全性进行保护。



零知识证明的优点与不足

总而言之，和其他解决方案相比，零知识具有哪些优点呢？它非常强大，从密码学的角度来看，基于其数学保障性，除了唯一解的数字以外，其他任何数字都无法进行解码，隐私保护性非常高，同时具有非常高的安全性保证。



但与此同时，它还并不是一项完美的技术。其一，它需要建立信任的设置，如果涉及的用户彼此争吵，只要有一个人表示不同意，在这些用户所在的群里没有建立起信任设置，就无法建立零知识证明。

其二，生成证明效率低。但在明年的升级中，我们能够将生成证明的效率从四十秒削减到七秒。

最后，这项新兴的技术仍有待时间的验证。像哈希算法，历经30年才从被提出到真正落地应用，而零知识证明，相对来说，才被投入运用一年多，还是一项没有经过测试的技术。

可是我依然相信，这是一项非常强大的技术，对其充满信心，在未来它能够和以太坊一样，在更普遍的范围内得到应用。