IAME

区块链身份验证专家系统

Nathaniel Tsang Mang Kin
Suryani Chang

www.iame.io

摘要：

一个去中心化的识别系统，将允许各方进行区块链交易时　在主要层面上验证彼此的身份，而不必向对方披露不必要的个人敏感信息；并在次要层面上说明交易中加密货币的来源。识别过程将由多个独立的第三方验证者进行，每个验证者将验证碎片化的识别数据，而所有碎片化的验证讯息将构成一个完整的验证讯息，确保只有个人敏感信息的原始所有者保留自己的数据。识别过程的结果将被散列到指定的区块链上，并且可以在公共存储库上访问，从而可以查阅与特定区块链地址相关联的加密货币的识别状态和来源，而不是身份验证数据。

内容

1. 导言

目前的身份识别系统依赖于人们必须与交易方分享他们的个人信息和支持文件，以识别他们自己的身份及财富来源。这些交易方共同拥有一套完整的个人数据，因此一个人与这些交易方共享的数据越多，针对此人身份及其财富来源的识别就越清晰。如果一个人与n方进行交易，它会因此形成星形拓扑网络并具有n个节点，每个节点都可能成为数据共享者的漏洞。不管有怎样的安全措施，一个人交出的数据越多，因安全漏洞带来的负面影响就越严重。

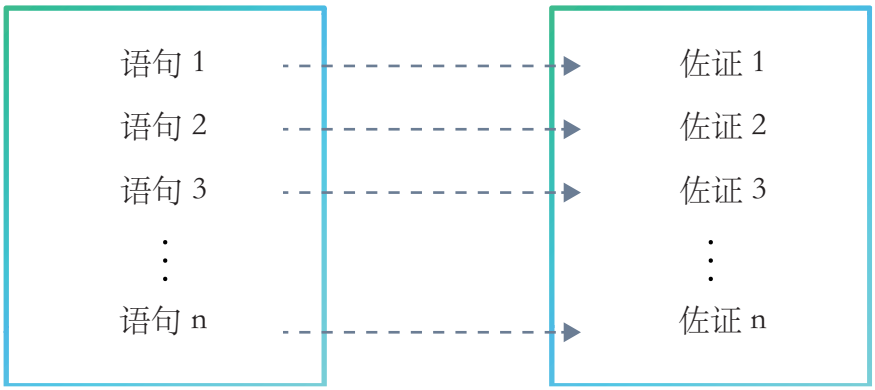
通常情况下，交易方/节点又会与第三方共享部分或全部数据，这又进一步扩展了初始的星型网络，从而增加了前一个网络中漏洞的数量。而目前加密技术的创新主要用于保护网络中两个或更多节点之间的数据传输，但不解决感知数据网络中节点数量增加的问题。随着一个人进行电子交易的次数增加，其个人数据网络中的节点数目亦呈指数增长，因此也增加了可受攻击漏洞的数量。

我们提出的解决方案是改变识别过程的方式，例如将一个人的身份碎片讯息交由交易方之外的多个独立第三方进行验证。这些第三方将被指派验证身份碎片讯息的任务，而这些资料本身无法被恶意利用，但这些被验证的碎片讯息汇总后对于交易方而言却是有效的身份验证讯息，借此绕过了任何交易方必须处理或存储非必要数据的需要。

而上述过程将发生在IAME识别网络上，这是一个专门建立的系统，通过使用我们的IAM加密代币，我们为交易方进行身份碎片讯息验证服务。IAME识别网络的功能将主要为基于区块链的P2P交易提供服务，不过在日后将会把区块链服务拓展到商户交易和金融机构上。

2. 解构身份识别过程

传统的识别过程开始于一方（甲方）收到交易方发出的身份验证请求后作出授权，以便对方对其交易对象的身份有一定的了解。在授权后，甲方将提交一份含有交易方认为需要的数据的语句和相应的佐证。在将数据映射到支持证据之后，就甲方的身份验证是否可被标识达成一个共识。



该验证过程假定：如果甲方是真实的，则所有提供的语句都可以映射到相应的支持文档上。原则上，可以在更多支持文档上映射的数据越多，甲方就越难伪造其身份。

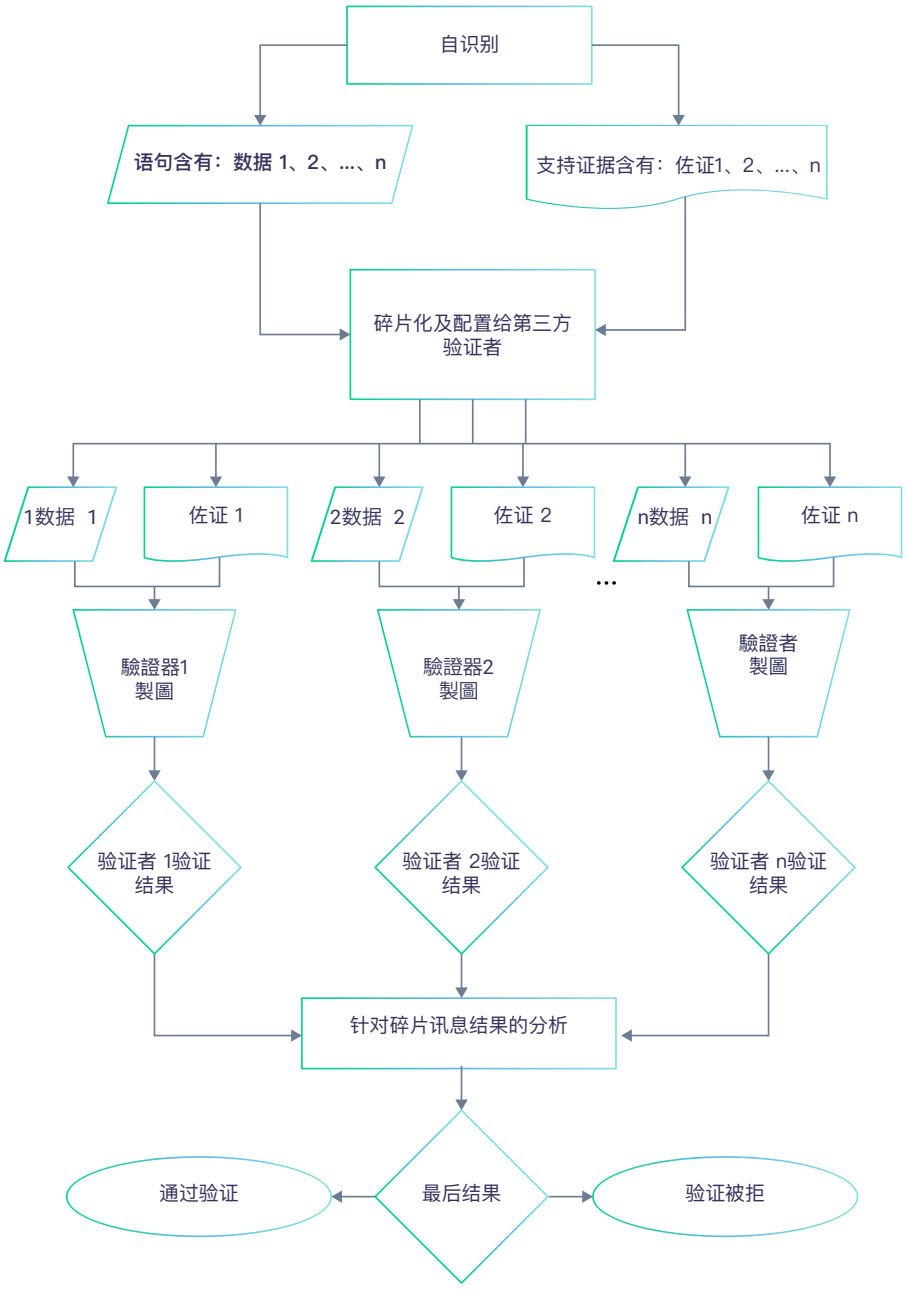
映射过程本身是相当简单的，可以分类如下：

1. 语句与字符串的确认；
2. 语句与非字符串的确认；
3. 语句与公开可用信息的确认；
4. 语句与私人提供的信息确认；和
5. 语句与政府记录的确认。

任何能够最大限度地收集上述映射数据的识别过程对于交易方而言都有助于确保交易的对象是真实存在的，但对于提供讯息的一方而言，一旦因安全漏洞导致身份讯息外泄，却可能带来灾难性的后果。

3. 碎片化识别过程

在前一种身份识别程序的基础上，只要通过委托第三方验证者进行映射，也可以在不向对方公开任何不必要的数据的情况下，实现相同的映射功能。不过语句，支持证据和其功能，首先必须先进行碎片化处理，然后再交由第三方验证者去验证身份碎片数据，而任何单独的身份碎片数据将无法被任何恶意的第三方滥用，只有将全部的身份碎片数据汇总，才能够组成一个完整的身份验证。



举一个简单的例子，交易方需要确认3个字符串类型的语句，并附上一个标识文档作为支持证据：

1. 名字：“John”
2. 姓氏：“Doe”
3. 国家：“毛里求斯”

如上所述，可以通过将3个需要被确认的字符串类型的语句与标识文档字符串的对应部分发送给3个不同的第三方验证者来确定字符串的内容，从而简单的将数据碎片化。因此这些第三方验证者独立验证后的结果汇总将等同于交易方自行验证这3个字符串语句。

与传统的识别过程相比，在分散的识别过程中，数据的可用性随着碎片的增加呈指数级下降。

利用碎片化的标识原则，语句可以进一步分解，以将任何可用的字符串类型语句转换为不可理解的数据：

1)字符串类型语句：John

2）碎片A：“Jo”

3）碎片B：“hn”

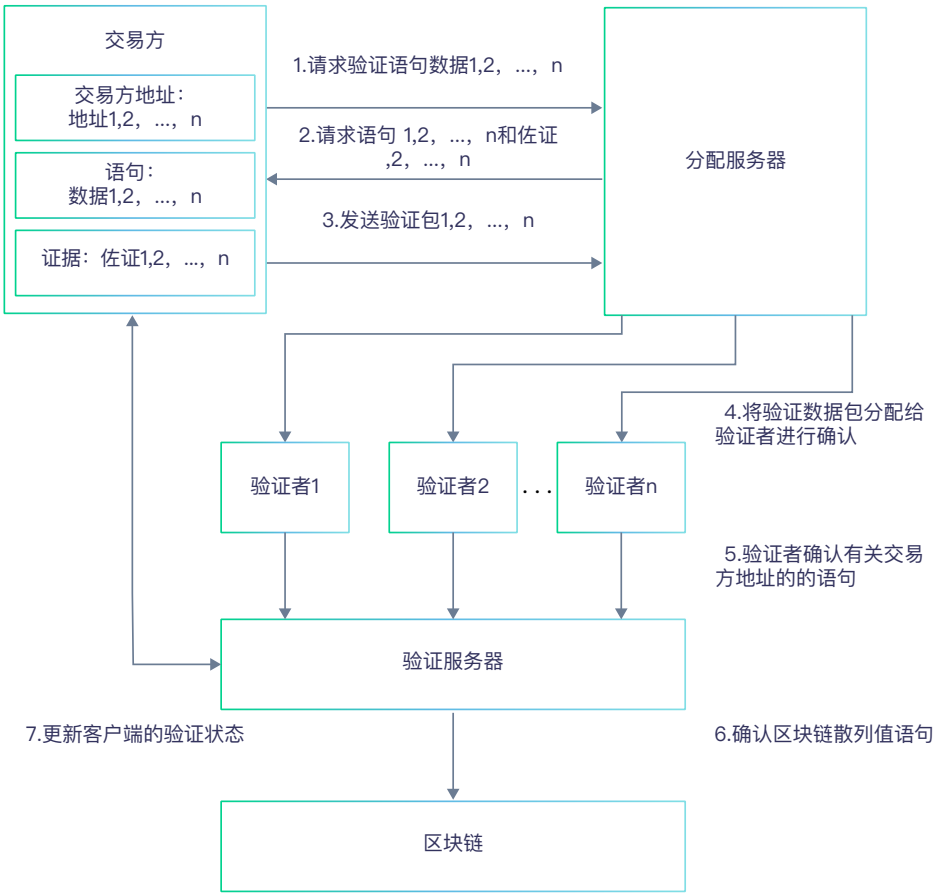
4）碎片C：“oh”

通过上述这样的过程，我们已经让字符串类型语句“John”对任何潜在的恶意第三方验证者都不再有意义。

4.IAME识别网络

我们设计的IAME识别网络将由以下几部分核心构成：客户端，分配服务器，验证服务器，写入区块链和身份服务器。每个组件都将执行特定的功能，并可以通过两个过程进行演示：即验证过程和识别过程。

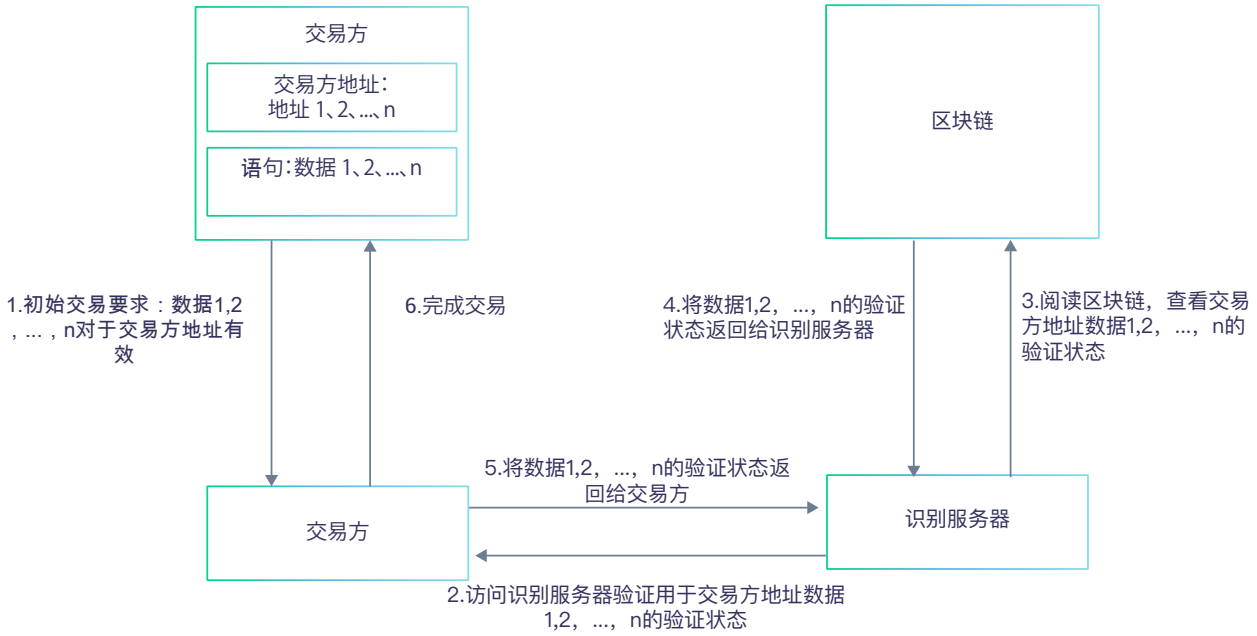
验证过程



验证过程是指客户通过第三方验证者验证其信息的过程：

1. 根据请求，语句及其相应的佐证将在客户端级别进行碎片化处理，之后再加密转变为验证数据包发送到分配服务器
2. 分配服务器将把验证数据包随机分配给第三方验证者，第三方验证者验证后将把结果送返验证服务器。
3. 完成上述操作后，验证服务器将评估来自第三方验证器的验证结果，以及将确认的哈希数值或布尔值在指定的可写区块链上与特定语句进行配对。

识别过程



对于通过客户端与交易方进行的交易，必须经过一个识别过程。这个过程是基于交易方提出的具体要求。

1. 假设交易方需要将数据1、2、... n 与甲方进行的特定交易作出验证，交易方将发送请求到识别服务器以验证数据1、2、...n。
2. 识别服务器将读取区块链以获得关于甲方数据1、2、...n的验证状态，并将已验证的数据送返交易方，以完成与交易方的交易。

根据前面的图表所陈述的情况，一方可以自行识别自己的语句以与交易方进行交易，同时可完整保留个人敏感数据，确保即使有恶意第三方验证者盗取其敏感数据，也将一无所获。

IAME识别网络的主要功用并非让交易双方绕过分享数据这个环节，而是协助将个人敏感讯息进行碎片化处理，然后再进行分散式验证。

5.IAM代币

为了IAME识别网络的正常运作，我们将发布一种名为IAM代币的功能性代币，用于IAME识别网络上的验证数据包发出确认请求。交易的各方将通过IAME识别网络客户端消费代币，并且在扣除区块链哈希成本之后，IAM代币的余额将作为奖励支付给以营利为目的的第三方验证者。

代币的价值并非固定的，其市场价值由对识别过程的需求及供应量来决定。IAM代币的价值实质上取决于两个因素：

1. 验证的成本，与指定区块链上请求的数据数量散列的财务成本成比例，作为代币的价格底线；和
2. 市场需求，即与基于IAME识别网络的区块链识别需求成正比。

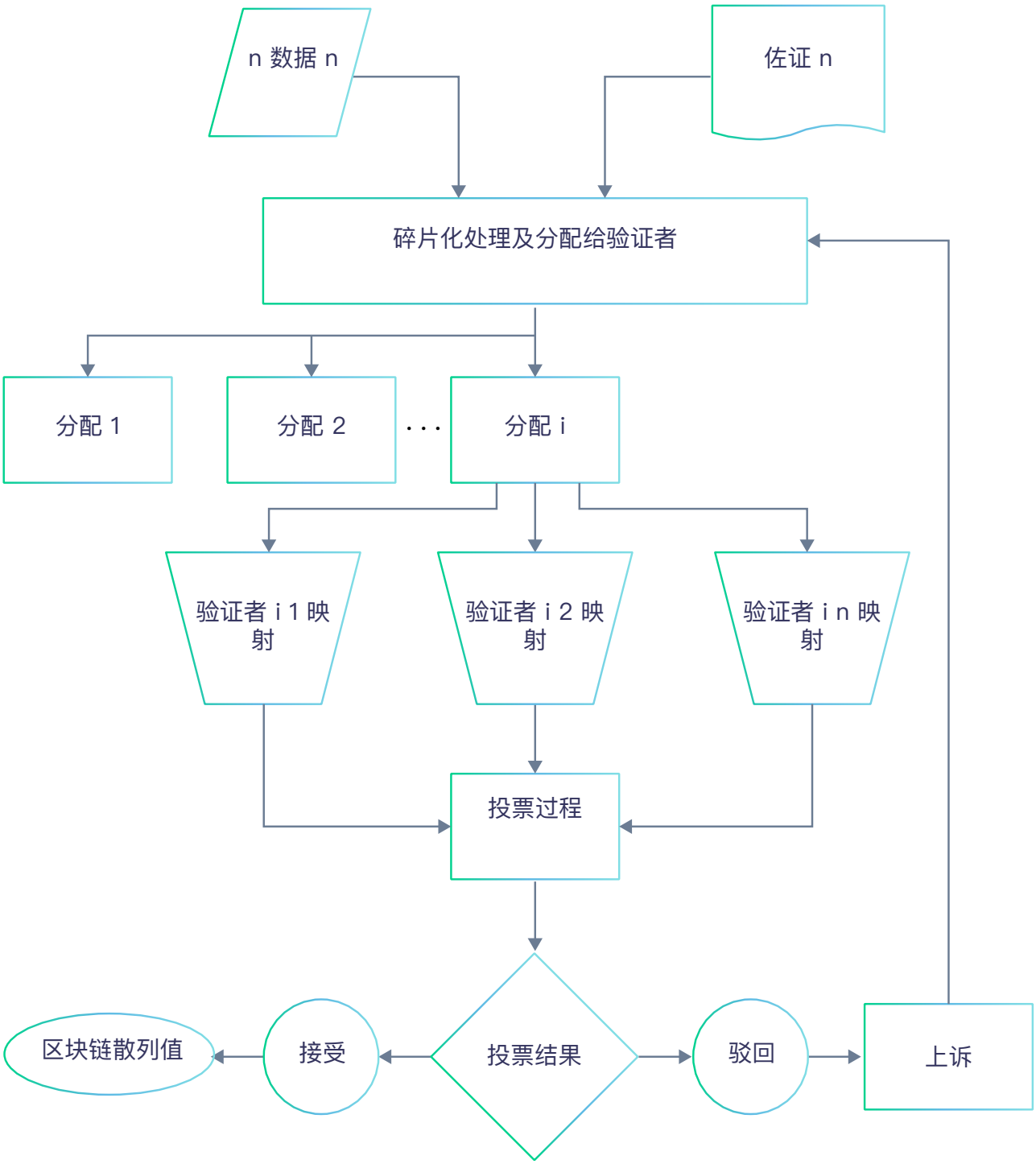
有鉴于识别领域数据验证的短暂性，对代币的市场需求将继续反复，并只会在IAME识别网络获得更广泛的采用而获得提升。

6.第三方验证

根据IAME碎片化身份识别系统的概念，将要求有一个分布式的第三方验证器系统，因为由多个第三方验证者进行的验证将更可靠，且与由单一机构或一方进行的身份验证相比，较不易遭受欺诈风险。然而，作为一个以盈利为目的运行的系统，例如“支付”给第三方以让他们验证讯息，将自然的为参与这个系统的各方创造一个良性增长的环境，这些第三方验证者为了持续收到报酬，将共同参与到这个系统中的验证过程。我们提出的解决方案是一个对称的游戏模型，它将促进与拜占庭容错算法也就是试算法类似的真实验证过程。

试算法的原则

1. 每个语句和其相应的佐证将以碎片（证据）方式被处理
2. 证据不是由单一的第三方验证者校验 （“陪审团”），而是由一组评审团进行（一个“法庭”）；
3. 每个评审团以指定的方法验证证据是否与语句相符；
4. 法庭的验证结果计算出来，并达成了多数人的共识。
5. 如果对证据的验证无法形成多数共识，证据将发往第二法庭（“上诉”）；和
6. 除非上诉陪审团的投票结果对最初法庭的判决达致同样共识，否则最初法庭作出的决定将被驳回。



试算法的目的是为了支持真实验证过程，最重要的是，可支持真正的异议，特别是发生第三方验证者在验证机制中出现大范围出错的时刻。

在我们所提出的技术实施建议中，第三方验证者将随机分配为法庭，上诉庭和控制法庭（“控制法庭”）。控制法庭是指将与证据不匹配的语句分配给第三方验证者，使得第三方验证者得以随机在双盲程序的情况下工作。

7.奖励和排名机制

作为试验算法的持续发展，需要一种奖励和排名机制，以便优秀的第三方验证者得到奖励，而恶劣的第三方验证者受到惩罚。对于这个机制，我们提议执行两种奖励系统：其一为代币奖励系统，另一个则是节点排名系统：

1. 代币奖励系统为第三方验证者分配一个IAM代币池，以类似于挖矿的过程去执行碎片式讯息验证任务；和
2. 排名系统则通过将IAME识别网络内的第三方验证者划入一个排名系统内进行比较，使得排名较高的验证者获得与其等级相符的更高比例的代币。

原则上，任何IAM代币池的分配将是由法庭正常运作的一个结果，而排名系统则是上诉庭和控制法庭正常运作的结果。由于采用双盲程序，第三方验证者在任何时刻都不会知道他们究竟被指派为法庭、上诉庭还是控制法庭，这将进一步降低了系统运作所带来的风险。第三方验证过程将向公众开放，从长远来看，排名不佳的第三方验证者将自然从节点中排除。

8.区块链上的P2P交易识别系统

随着IAME识别网络的正常运作，其主要的应用将是协助在区块链上进行P2P交易，如电商交易。以一个简单的在线购物进行说明，当顾客使用加密货币向一个在线商家购买实体货物时，顾客传送给商家的个人数据可以分为两类：与交易相关的重要讯息，与交易无关的不必要讯息：

1. 重要讯息将包括一个名字和一个地址，缺乏这两者交易将无法进行或货物将无法被送达正确地点；而
2. 非必要信息将包括可验证客户名称的身份证明文件、可验证客户地址的公用事业费账单以及客户的具体出生日期。

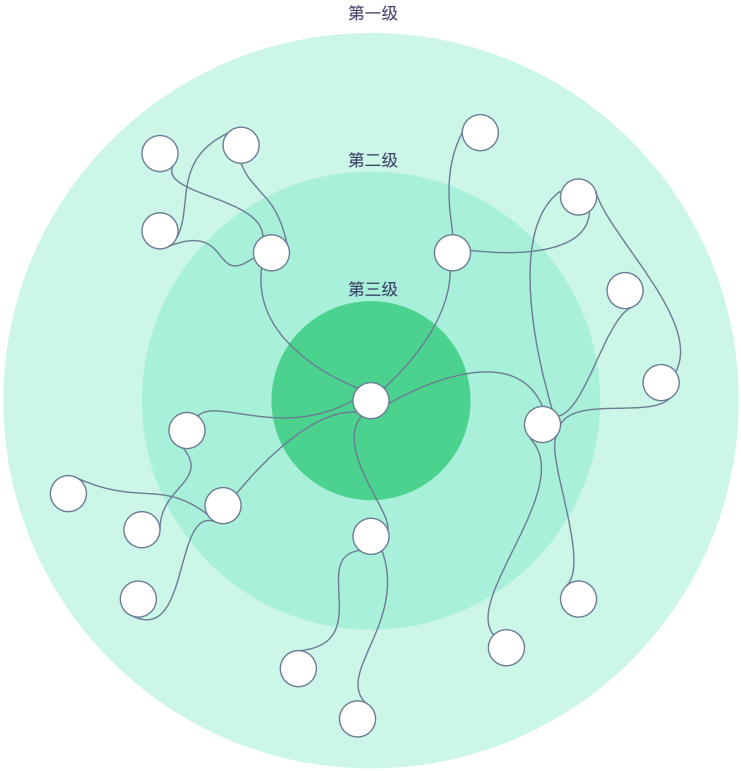
传递非必要信息的一个主要原因是基于监管需要。但是通过采用一个替代的身份识别系统，可以在不传播非必要信息的情况下实现同样的目标，这不但可降低客户的安全风险，也减轻商家因防范安全漏洞而带来的麻烦。

在P2P情景中，商家将咨询IAME识别网络的公共存储库以查阅与客户区块链地址相关联的非必要信息是否已经在识别网络上进行了验证。这么做的原因可能出于监管的要求或是纯粹为了了解交易对手。

9.向金融机构提供一个平台

无论对于加密货币的监管分类被将归类为货币、证券或软件，肯定的是它将需要具有一定的反洗黑钱功能，即针对加密货币的追溯性，可在一定程度上追踪到其来源，以确保它们不是来自犯罪活动的收益。使用公共分类帐目虽然能够建立电子痕迹，并一直追溯到加密货币通过挖矿/产生的过程，但却不能识别加密货币通过的钱包。

作为IAME网络和公共存储库的扩展，识别系统将可为金融机构提供相关的工具，建立一个可进行识别的拓扑空间，协助它们鉴定所处理的加密货币的来源到第n 级。.



部分网状系统的建立将让金融机构处理加密货币时更容易追溯到加密货币的第n级源头，从而成为一个比目前现有的加密货币程序更有效的反洗黑钱工具。

10.结论

在进行身份识别时最大安全风险主要来源于与交易方分享个人数据。加密技术和常规安全措施只有在处理信息的交易方是安全的情况下才能起作用；但是在电子交易急速增长的现代经济中，潜在的安全漏洞也呈指数级增长，从而降低了安全创新带来的任何好处。

通过使用本白皮书中提到的IAME识别网络，我们试图解决在区块链中进行交易的各方在身份识别中所面对的问题，我们提供的解决方案，既保留了一方的匿名性，同时也满足了另一方对于身份验证的需求。

分散式区块链技术的非侵入式识别系统既有实际需要，也有商业需求，我们相信，IAME识别网络将成为将区块链技术与受监管世界联系起来的桥梁。