White-paper of Identity Chain

Identity Chain 项目组

2018 年 5 月 2 日

新加坡

White-paper of Identity Chain

一、区块链与身份标识

1、身份标识

对于人类而言，当你出生时，DNA、指纹、面部特征成为最基本的省份标识；后来你有了身份证、护照、驾驶证；当成为公司的职员时，你有了员工号；当你注册了各种互联网平台时，你有了各种账号密码等等。个体从诞生到消亡的各种阶段，会出现各种不一样的身份标识来证明“你就是你”“你妈妈是你妈妈”。

对于物品而言，整个供应链系统，从原材料到生产制造商、物流商、经销商、零售商再到消费者手中，每个环节都有不同的身份标识来对应每个流程。

因此广义上，我们认为宇宙中所有发生的事情都来源于物质的流动，每一个物质都有它独特的身份标识，这个标识可以为物理上的分子结构、个体特征、行为轨迹等，也可以为基于信息化网络的比如人类的身份证号、互联网账号信息、物品的特征条形码等。这些所有的标识的集合构成了物体的身份标识集合体,这个集合体,记录着个体从诞生到消亡的所有信息。

2、身份标识的痛点

随着信息技术的发展,数字身份已经深深融入社会发展的每一处,深刻改变着传统的社会运转、经济运行模式以及人类的生活形态。当我们使用一些联网设备进行更加方便快捷的操作时，如网络社交、网购、直播、网上支付、在线游戏、视频监控等,都需要经过各种网络身份的注册、登录、

认证和传输等过程。这些信息可能包含自己的银行账户、联系方式、家庭住址、身份证号码等敏感内容，基本所有的信息都涉及到个人隐私和财产安全。无论是人、物或者商品的流通，都伴随着身份标识的流动。如今数字身份已在各个场景得到应用，如个人信用贷款、网络支付交易、公共服务授权或者物流快递跟踪、商品代码溯源等。而由于这些信息碎片化、分散化的特点以及对有效性、真实性、唯一性的合法验证，为其应用和管理带来挑战，目前暂时没有任何一家中心化机构或者组织能完全采集这一集合体。

2.1 数据的碎片化与分散化

在现有的体系下 ,身份标识数据被不同的寡头包括政府机构和其他组织所掌控 ,每个数据互不相通 ,证明材料获取、验证等环节 ,流程长、成本高、数据信息泄露风险大。

2.2 数据的真实性无法判断

基于单一信息管理体系认证难以对个体形成全面的综合的评价，大量低质量的甚至是虚假误导信息的广泛传播，难以准确获知“你是谁”“你从哪里来”“你要到哪里去”。

2.3 数据溯源流程复杂繁琐

在没有主导的流程协作中，不同的数据源之间难以建立信任，参与者越多，流程越复杂，信任关系越难建立，使得溯源面临重重障碍。

2.4 数据源或个人无力掌控数据的流通

基于现有的中心化数据交换体系 ,中心化服务器的数据沉淀往往会对数据源产生利益伤害 ,使得数据源或者个人对数据的使用授权方面没

有足够的话语权。

3、区块链

区块链是一种分布式记账(存储)技术 ,通过多个网络节点共同记账，基于密码学原理，将账目（数据区块）按照时间顺序进行存储形成一条链式结构。

区块链具有以下特征：

高可容错性 :分布式网络、去中心化信息、容错 1/3 左右节点的异常状态。

不可篡改性 :一致提交后的数据会一直存在 ,不可被销毁、修改或者伪造。

隐私保护性：密码学保证了未经授权者虽能访问到数据，但无法解析。

因此，区块链构成的网络，无需额外的第三方担保机构，即可构成多方信任基础。

4、当身份标识遇到区块链

ISC 致力于通过区块链技术建立一套去中心化的新一代分布式融合数据身份标识体系，基于分布式节点网络对个体从诞生开始所有的碎片化身份信息行为轨迹个体特征采集后进行加密整合，纳入多维化信息统计协议及身份标识的唯一性认证，实现跨行业、跨系统、跨链的智能身份认证和溯源体系。

区块链确保了真实完整，每个数据都在大家的监督下被真实、完整的记录在各个节点，证据充分、有迹可循，可以完美解决总理痛斥的“证明你妈是你妈”事件；

区块链获得了全民共识，所有参与者对全网记录的事件顺序和当前状态建立共识，大家共同信任区块链机制；

区块链实现了共享开放，系统对所有参与者开放，所有参与者都享有知情权，人人平等的享有这些区块链信息，且是开源的，有很好的延展性；

最后，区块链保障了安全可靠，所有数据经过非对称密码学技术加密及复杂的校验机制，保证了数据的不可篡改、不可伪造及完整性、连续性、一致性。

二、Identity Chain

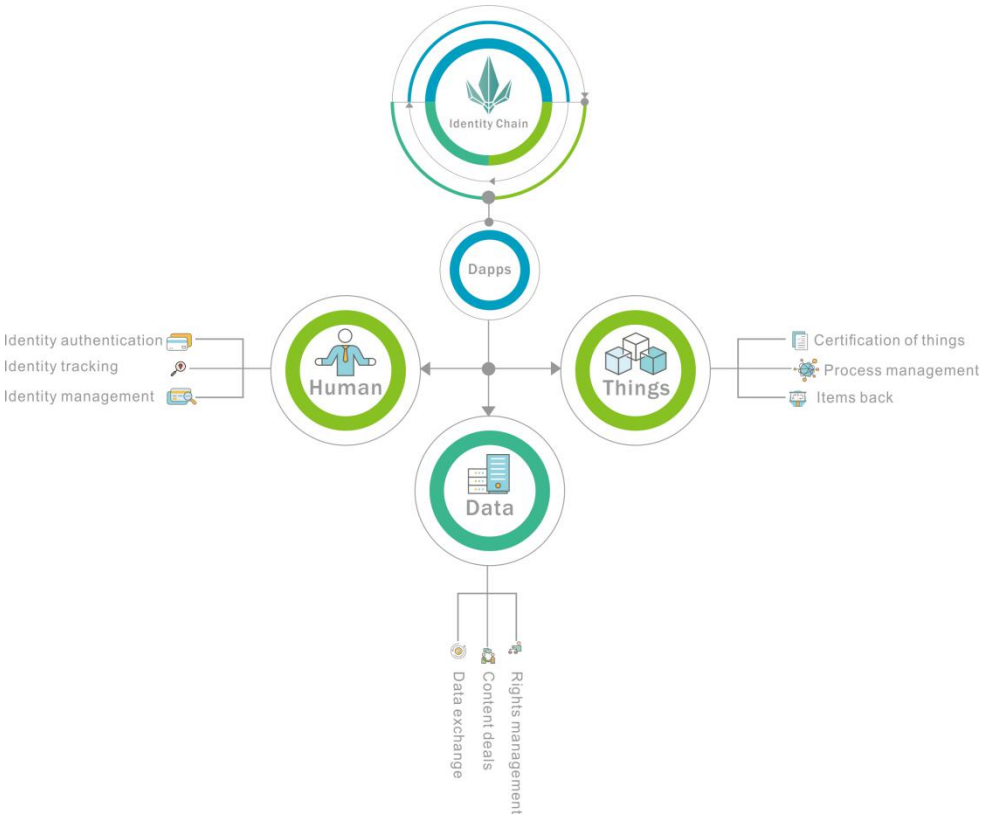
Identity Chain 生态搭建了一个去中心化的分布式融合的数字身份标识认证和溯源体系，基于分布式节点网络对个体从诞生开始所有的碎片化身份信息行为轨迹个体特征采集后进行加密整合，将数据源的多样化在一体化的智能合约中进行协同，纳入多维化信息统计协议及身份标识的唯一性认证，并提供多种应用场景下的开放基础模块，实现跨行业、跨系统、跨链的智能身份认证和溯源。

同时， Identity Chain 在分布式身份标识识别的基础上，扩展了更深的生态和应用。将身份标识的应用扩展到了更多的维度，从基础的身份认证到特定身份标识的追踪，从数据的互换到分布式数据交易，从分布式流程到分布式生态，结合底层的分布式账本体系，联合各类行业的合作伙伴，在不同领域提供多样化的服务，建立新一代分布式融合数据身份标识生态。

三、Identity Chain 生态体系

1、Identity Chain 生态体系

Identity Chain 的本质是一个一致的分布式数据账簿，Identity Chain 将始终跟进区块链技术的发展，契合不同领域的应用，结合 P2P 技术和共识机制，提供分布式账本、智能合约、分布式身份标识认证协议等，为各种应用提供底层协议支持。



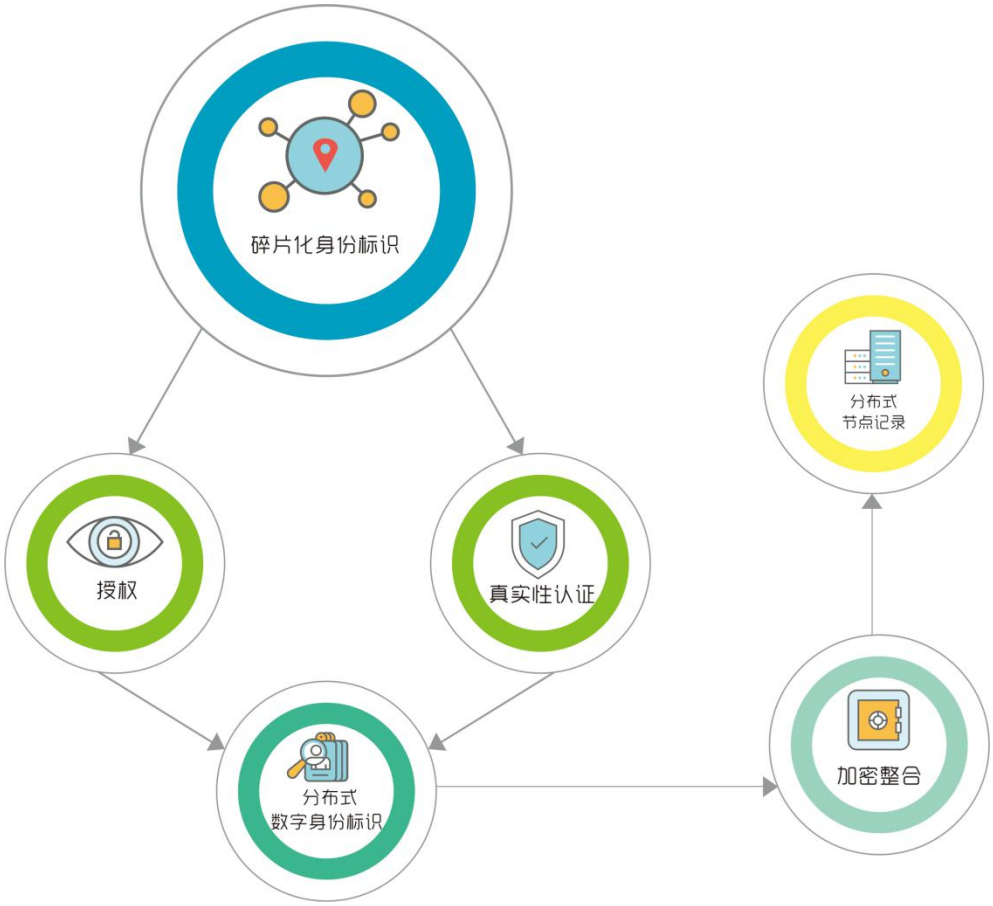
2、分布式数字身份标识加密整合体系

一个融合多源性、分布式，并且能对数据进行加密整合保证隐私安全的标识认证体系是 Identity Chain 的核心协议之一，它能够支持 Identity Chain 生态中任何实体包括人、各类机构组织和物体的分布式和多样性的识别和认证。

3.1 分布式身份标识整合与加密

每一个个体（人、物）都有一系列分布式的身份标识数据源，Identity Chain 通过特定的一体化智能合约和共识体系对这些分布式数据进行加密整合，这个集合体以分布式加密数据的方式仍保存在数据源的提供方，未经授权任何第三方不能获取这些信息，Identity Chain 网络仅对数据源的

提供方进行上链标记，而不会存储任何数据源的信息。



同时，每一个个体在 Identity Chain 网络中也会存在多种不同的身份标识，在经过个体和数据源的授权后，基于 Identity Chain 网络可以对个体建立一套完整的分布式数据身份标识集合体，这个集合体记记录着个体在分布式数据源中的所有信息，只有获得个体授权后，获得授权的组织或者个人，可以通过某一个网络中的身份标识访问其他网络中的使用的身份标识或者寻找个体在其他网络中身份标识的分布情况，整个过程都将基于 Identity Chain 网络中分布式整合和加密合约进行执行，Identity Chain 网络本身不进行任何数据存储。未经授权，任何第三方无法通过某一项身份标识获取其他网络的身份标识。

3.2 分布式账本技术

分布式账本技术的去中心化、不可篡改、共同记账等特点是 Identity Chain 网络分布式融合数字身份标识认证和溯源得以实现的关键，是 Identity Chain 网络底层存储的重要基础设施。

个体身份标识的登记与识别是 Identity Chain 网络中重要基础模块，通过分布式账本技术，Identity Chain 网络设计了多维度多层次的针对参与者和身份标识数据源的授权、认证和登记体系。

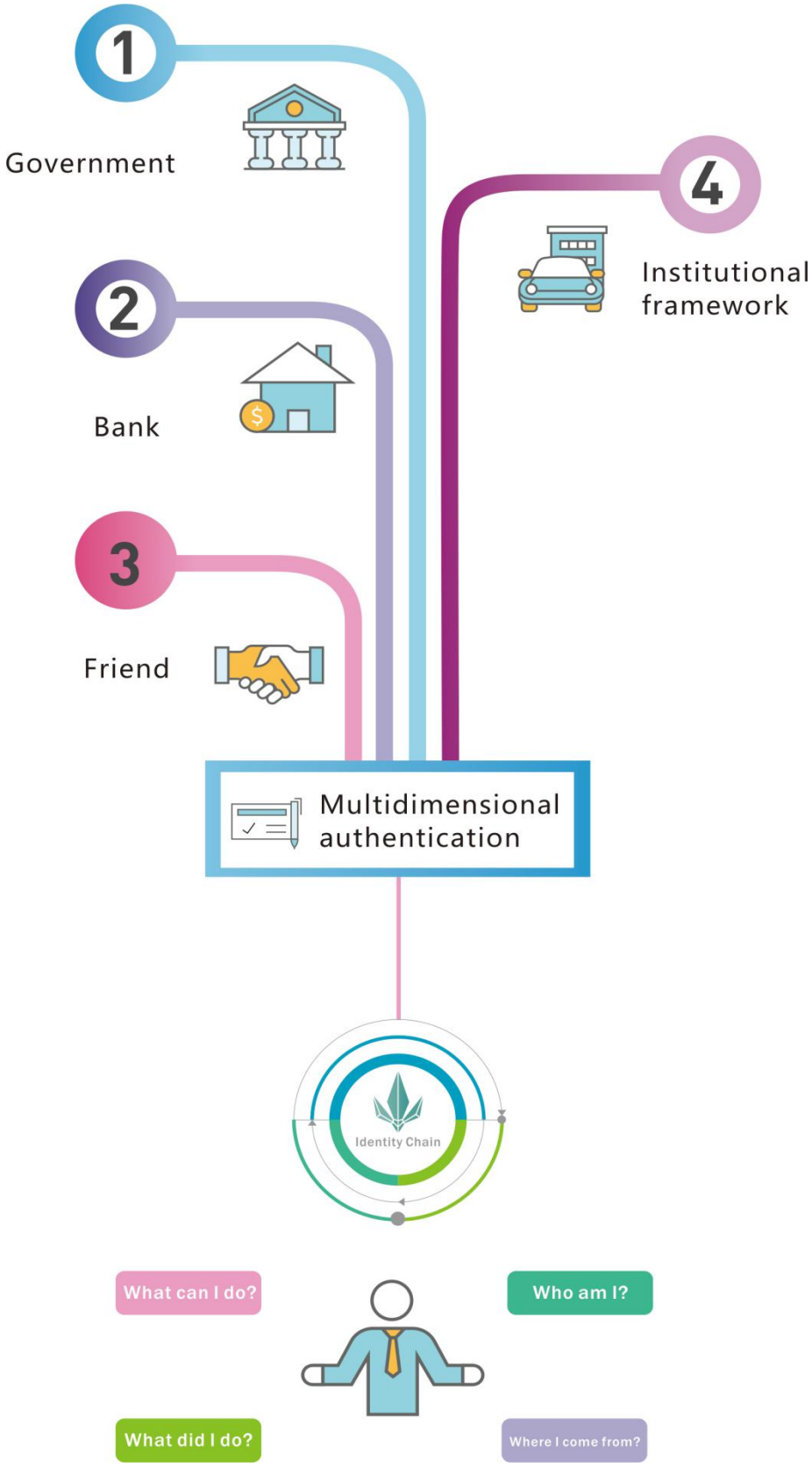
数据分类：通过分布式账本技术，对不同数据源的数据信息进行分类汇总，通过对数据和数据源进行双向唯一性匹配，可以快速定位需求数据所在的数据源地址，并对每一次的数据匹配进行多维度真实性验证，验证结果保留在 Identity Chain 网络，假如被多次记录数据不匹配，对应的数据源会被记录为不可信。

数据交互：通过分布式账本技术，通过特定的跨链协议，实现个体数据在不同系统不同链之间的数据交互。当同一个流程的不同步骤分散在多个系统或者多个链中执行时，保证流程协作的一致性，并保障个体在不同区块链和系统中的隐私。同时实现以个体为基本的数据交换，帮助个体对分布式数据进行掌控，当个体创造的价值被再利用时，为数据的原创者谋求最基本的权益。

行为记录：通过分布式账本技术，将对每一次数据请求、数据匹配、数据调用记录进行记录，保证数据的安全可靠和不被泄露。

3、多维认证与识别体系

4.1 人类的多维认证与识别

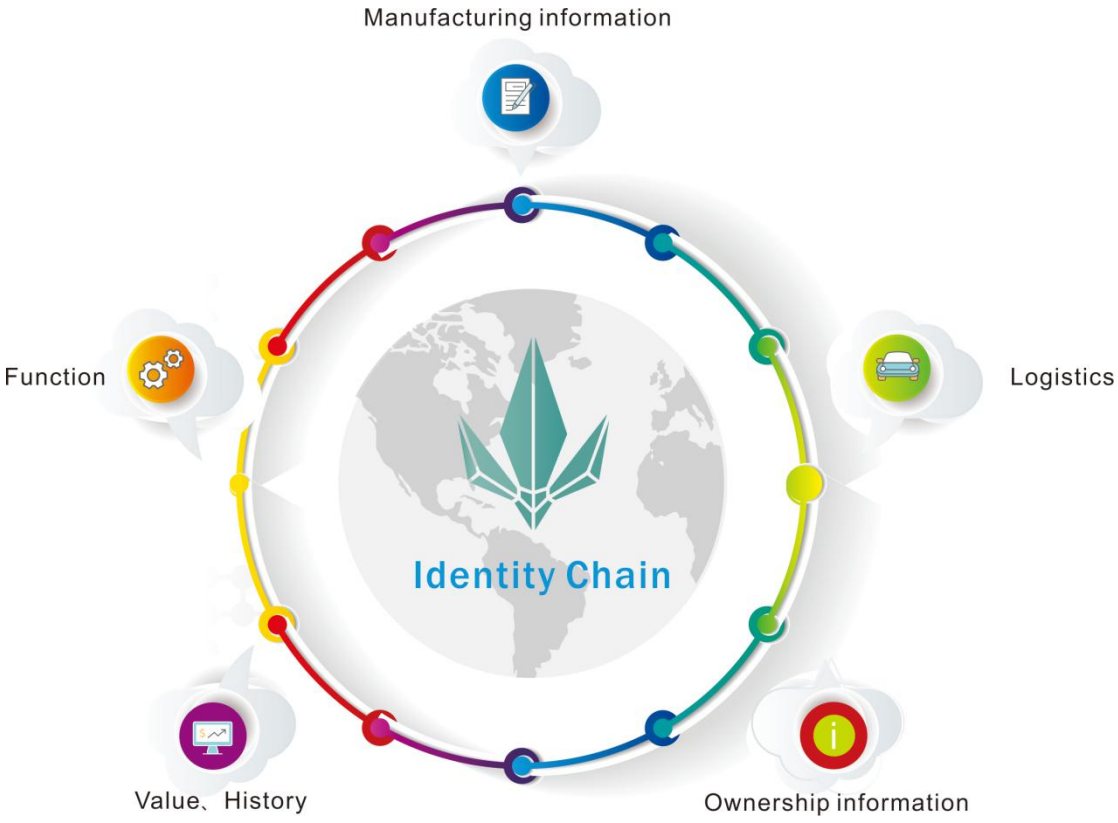


生活中，每个人都有多层社会关系，任何与个人有关的组织或者个人都有掌握这个人的一部分身份信息。通过 Identity Chain 生态系统，个人

可以掌握和授权各种与自己相关联的数据，包括政府机构、信贷机构、银行等，实现一体化的灵活应用，不再为如何证明“我就是我”而烦恼。

同时根据不同数据源的认证，经个体授权，Identity Chain 网络可以建立一套完整的个体画像，这个画像可以体现所有与个体相关的各个维度的情况，包括个体从诞生的身份标识传递轨迹以及创造的价值等。同时基于分布式账本技术，各方的数据都经过数据源方提供的真实性签名，具备不可更改、不可伪造的特性，因此个体的特定身份标识经过用户授权后，可进行可逆性的溯源。

4.2 物体的多维认证与识别



从诞生或被生成出来，物体同样会经历不同阶段，每个阶段都伴随特定的身份标识：

生成制造信息：原材料、生成日期、生成流程等

物流运输信息：承运方、运输过程等

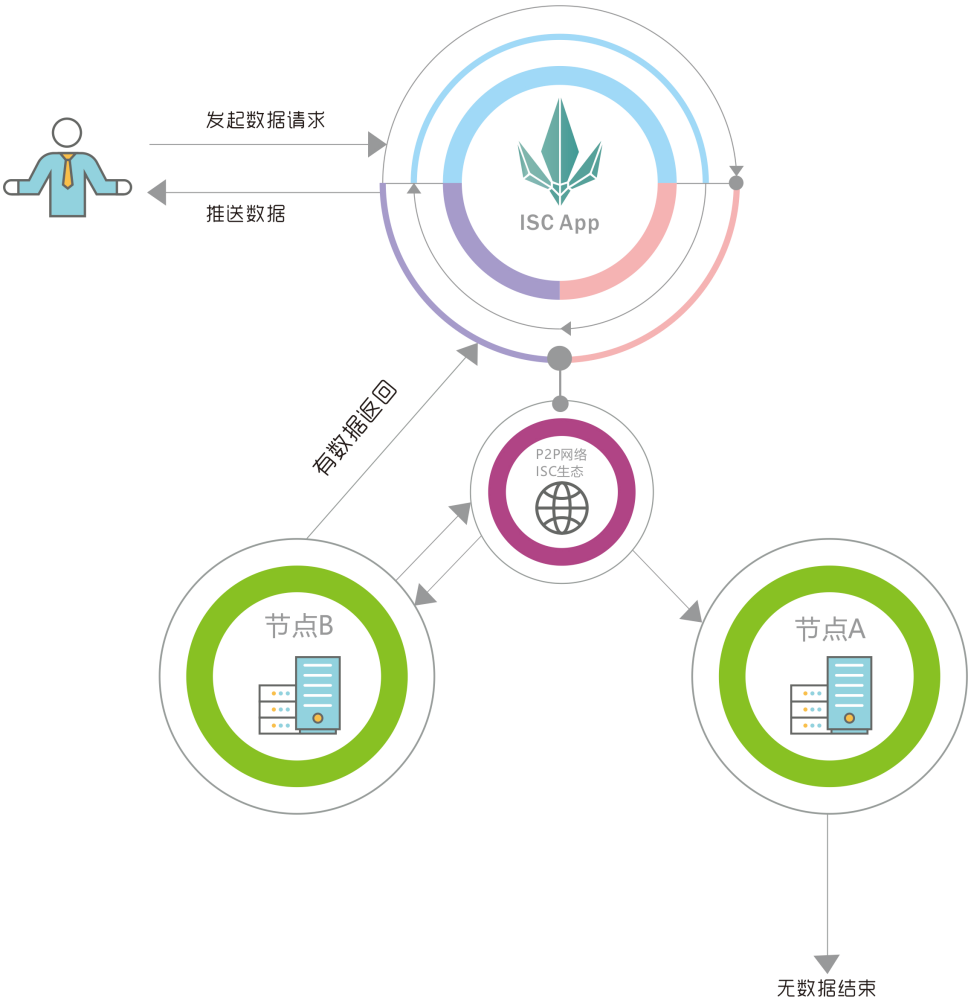
物体属性信息：功能作用、大小形状等

物体价值信息：价格、所有权等

基于 Identity Chain 网络的加密整合体系，这些来自不同数据源的身份标识信息经过多维化认证后都可存储于区块链，从而建立一套完整的数字身份标识集合体。

4、去中心化数据交换体系

Identity Chain 网络提供一种去中心化的数据交换体系，当用户发起数据使用请求时，通过提交智能合约到 Identity Chain 网络，Identity Chain 网络首先判定该数据请求是否包含个体隐私数据，如果涉及隐私数据则触发个体隐私使用授权机制，得到授权后，将此智能合约向全网节点进行广播，如果数据源没有数据则流程结束；如果有则将数据通过非对称加密数据点对点传输给数据请求方。



5、特定标识定位与溯源

特定标识的定位与溯源体系，同去中心化数据交易机制类似。当用户发起针对特定标识的定位或溯源需求时，通过提交智能合约到 Identity Chain 网络，Identity Chain 网络首先判定该数据请求是否包含个体隐私数据，如果涉及隐私数据则触发个体隐私使用授权机制，得到授权后，将此智能合约向全网节点进行广播，如果数据源没有数据则流程结束；如果有则将数据通过非对称加密数据点对点传输给数据请求方。

6、其他底层协议及应用组件

四、Identity Chain 应用场景

1、人类的信息认证

1.1 互联网信息登录

未来理想状况下，ISC 生态 ID 将成为每个人独有的唯一的身份标识，通过跨链数据共享，将可以访问其他的互联网平台，不再为每个平台都要注册一个账号而烦恼。

1.2 实体身份验证

生活中，每个人都有多层社会关系，任何与个人有关的组织或者个人都有掌握这个人的一部分身份信息。通过 ISC 生态系统，个人可以掌握和授权各种与自己相关联的数据，包括政府机构、信贷机构、银行等，实现一体化的灵活应用，不再为如何证明“我就是我”而烦恼。

2、人类的身份标识识别与追踪

通过发布指定人（如犯罪嫌疑人或者失踪人口）的特征身份标识，将相应信息进行全网节点广播，任何一个节点发现类似的身份标识，都可通过 DAPP 回传，经过进一步的匹配后对指定人群进行识别与追踪。

3、去中心化数据交易所

4、物联网智能组件的开发

5、基于 Identity chain 的百科全书

6、食品安全溯源

7、贵重商品防伪与打假

五、ISC 代币

ISC 是 Identity Chain 生态系统代币，共计发行 1 亿枚，永不增发。ISC 在基于 Identity Chain 开发的各种 DAPPS 中均可流通。

类别	数量	占比	用途
发行	5500 万	55%	项目发展、人才招聘
宣传推广	1000 万	10%	前期推广
社区激励	1500 万	15%	ISC 生态的持续运营
创始团队	2000 万	20%	创始团队激励

发行计划：

类别	数量	兑换比例	时间
天使轮	1000 万枚	1ETH=20000ISC	2018.5.14-5.21
私募	2000 万枚	1ETH=10000ISC	2018.5.21-5.31
公募	2500 万枚	1ETH=7000ISC	2018.6.1-6.30

六、Identity Chain 发展展望

七、风险告知

八、免责声明