MYKEY 自主身份系统
白皮书 1.0

概述

MYKEY（mykey.org）是基于多条公有区块链的自主身份系统，该系统基于 Key ID 自主身份协议。本白皮书详细阐述了 MYKEY 在资产维度上的功能设计，并简要描绘了未来 MYKEY 在另两个维度上的应用，即社会关系维度和数据维度。从资产维度看，MYKEY 是一款多链钱包，它让用户完全掌控自己的财产，且在丢失私钥时可以冻结和恢复账户。另外，MYKEY 是信任网络（Web of Trust）的组成部分。同时，MYKEY 在 web3.0 的背景下将数据主权归还给用户，从根基上保护用户隐私。

1. 介绍

MYKEY 是基于多条公有区块链的自主身份系统，是基于 Key ID 自主身份协议的首个应用实例。用户通过 iOS 和安卓 App 使用该自主身份系统，App 代码开源。Key ID 自主身份协议中的使用权授予通证 KEY，例如，支付 KEY 购买身份名称等。Key ID 协议由 MYKEY Lab 负责建设和部署，作为回报，MYKEY Lab 获得 Bihu Key Foundation 的一次性捐赠 100 亿 KEY。MYKEY Lab 是一家盈利性的公司。MYKEY App 由 MYKEY Lab 负责运营。

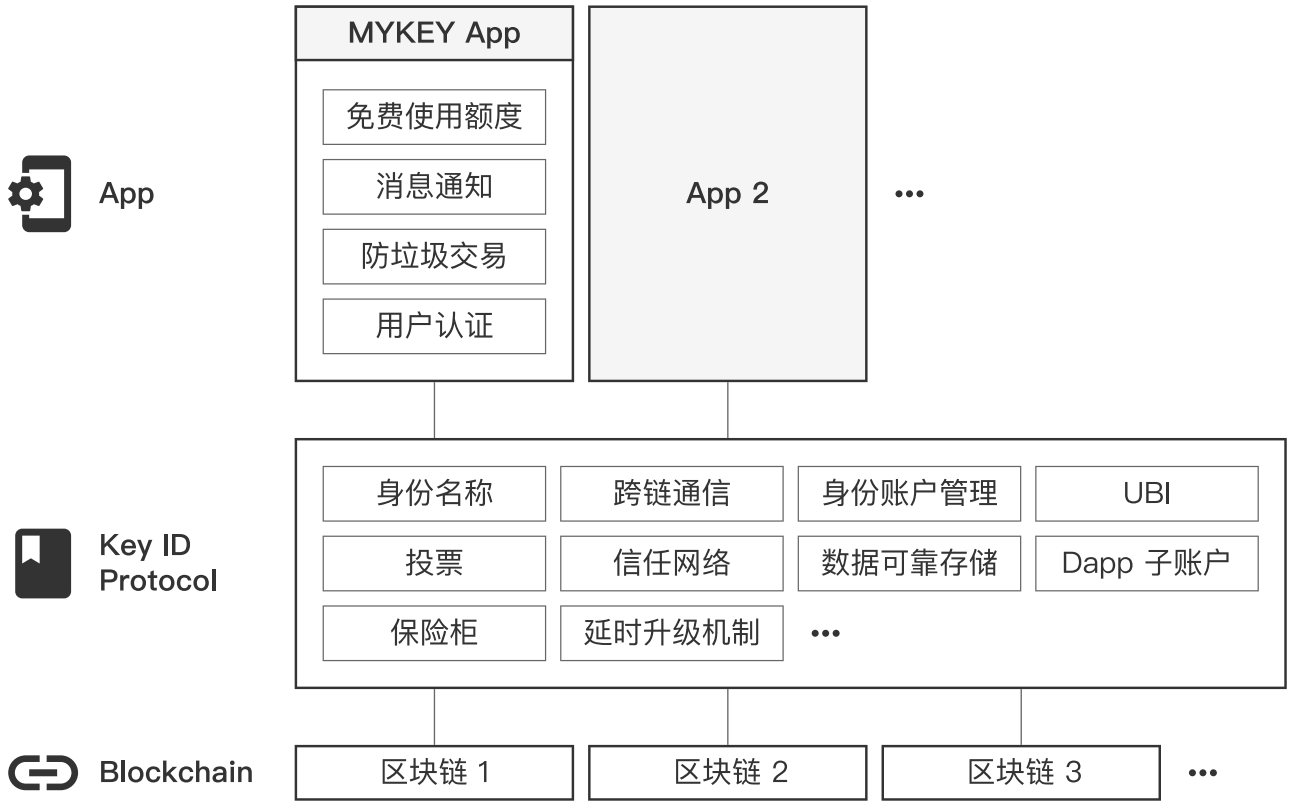

图 1，MYKEY App 与 Key ID 协议功能结构。

MYKEY 作为一款 App 产品，从用户视角看主要有 3 项功能：多链钱包，信任网络，数据的可靠存储。多链钱包，顾名思义，是服务于多条公有区块链的钱包，具有以下特性：

1. 统一的身份名称，
2. 免费使用额度，
3. 互相制衡的权限设计以保障账户安全，
4. 私钥丢失后的身份账户找回机制，
5. 账户的可升级性，
6. 防垃圾交易。

在信任网络中，每个账户由 3 部分组件构成：

1. 全网唯一的、享有永久所有权和使用权的身份名称，
2. 身份账户文件，
3. 由账户合约控制的去中心化存储安全区。

信任网络的基本组成单元为可验证声明（Verifiable Claim），在信任网络中，每个身份账户将会收到若干个来自其他身份账户的可验证声明，每个身份账户也可以对其他身份账户发表任意数量的可验证声明，通过这些可验证声明，身份账户与身份账户之间互相印证，最终环环相扣形成统一的信任网络。每条可验证声明都可以附带证明文件，这些文件存放在基于去中心化存储的安全区里，在身份账户的主人授权下可以代理给其他账户访问。

数据的可靠存储。存放于去中心化存储安全区的资料并不必须与某个可验证声明关联，而是可以独立存储，经账户主人授权可以供其他账户访问。账户主人也可以设定某些文件为公开文件，供所有人访问。如同一对双胞胎，数据的可靠存储服务与信任网络基于相同的去中心存储的基础设施以及类似的授权机制，在 MYKEY 中呈现不同的使用场景。

信任网络的构建，以及数据的可靠存储，均依赖于基于区块链的去中心化存储技术的成熟，因此这两项功能的实现在规划上将晚于多链钱包功能。

2. 身份

什么是身份？身份是一个“壳”，壳里装的是“我”。

身份的 3 种属性：社会属性，财产属性，数据属性。

社会属性是指身份在社会、社交、社区背景下的含义。这个身份是谁？是父亲的儿子，是妻子的丈夫，是下属的上司，是俱乐部的积极分子。社会关系定义了“我是谁”，如果一个身份没有任何社会关系，那么该身份的存在与否，其实也无关紧要。

财产属性是指身份的名下财产，例如，房产登记在某人的名下；这张银行卡的主人是谁；这台租赁电脑的使用权人是谁。这些都是身份的财产属性。

数据属性是指与身份关联的数据，例如，该身份在某月某日买了一张去某地的机票；该身份

拥有 1000 张照片；该身份在某电商网站购物的历史数据；该身份在某社交网站上所有的行为历史数据；可穿戴设备记录的一切数据。

区块链技术结合去中心化存储技术有望通过信任网络重塑身份的全部维度，把原本散布在线上线下的身份共识聚合到信任网络中，在信任网络中记录与该身份相关的一切信息，构建一个完整的“壳”，来定义一个全面的“我”。这些信息完全由自己掌控，根据自己的意愿授权分享。信任网络中的身份是物理世界中的自己在虚拟空间的映射，“我”可以在百年后从世上消失，但如果预付足够多的存储资源，“壳”可以保存千年。

3. 钱包功能

3.1 多链钱包

MYKEY 作为多链钱包，支持多种智能合约平台。由于 MYKEY 账户在每一条区块链上均以智能合约的方式存在，因此 MYKEY 的钱包功能暂时不支持非智能合约平台。

如何实现跨链的通证转移？简单的答案是：不能，在跨链技术成熟之前。KEY 是在以太坊上的 ERC20 通证，如何将一部分的 KEY 转移到其他公有区块链，以实现 KEY 在各条链上的使用权，是 MYKEY 必须立即回答的问题。最简单但也许也是最有效的方式：
MYKEY Lab 将自身拥有的一部分 KEY 在以太坊区块链上公示，并在其他区块链上生成同等总量的映射通证，并提供方便的转换服务，使得映射通证与 KEY 之间可以 1：1 互换（除去网络手续费）。在跨链技术成熟之后，逐步回归到无需信任的方式实现跨链交易。

3.2 身份名称

Key ID 自主身份协议在其部署的所有区块链上使用统一且唯一的身份名称，身份账户对身份名称拥有永久所有权和使用权。在跨链技术成熟之前，需要选择一条公有区块链作为身份名称的确权链，第一条部署 Key ID 身份协议的区块链将作为确权链，而其他区块链上的身份名称体系映射对应确权链上的身份名称所有权关系。

如何映射？在跨链技术成熟之前，可以使用“抵押声明 + 挑战期”的方式实现。同一个用户在不同区块链上的账户在被创建的时候都会被标记同一个 uuid（universally unique identifier），用以表征不同区块链上的系列账户属于同一个用户。同一个用户在不同区块链

上的账户使用同一个身份名称。注意，uuid 在表征不同区块链上的账户是否属于同一个用户方面，并不具有权威性，因为任何人都可以标记任何 uuid 到新账户上。只有当确权链上某个身份名称与账户绑定后，才表示一个身份的真正建立。

在非确权链上首次建立账户与身份名称的映射关系时，首先须确保在确权链上相同 uuid 的账户与该身份名称之间已经建立了绑定关系；之后，发起人须抵押一定数量的 KEY 作为保证金，来发起非确权链上的映射关系的声明；随后，是一定时长的挑战期，在这期间，任何人都可以通过抵押等量的 KEY 保证金来发起针对该对应关系的挑战。如果挑战期内无人挑战，则账户与身份名称在非确权链上的绑定关系确立。如果挑战期内有人发起挑战，则挑战者须抵押等量的 KEY 保证金，仲裁者须检查两份信息：（1）在确权链上的 uuid 与身份名称之间的对应关系是否与该非确权链上的一致；（2）在非确权链上账户的基本公钥以及账户逻辑是否与确权链上的完全一致，此处基本公钥是指账户创建之初就设定的权限类别所对应的公钥。仲裁者根据这两份信息作出裁决，失败一方将失去全部抵押物，由挑战获胜方、仲裁者、MYKEY Lab 分享，比例待定。MYKEY Lab 负责建设基础设施以方便挑战开展。

谁来担任裁决者？如果该非确权区块链上有成熟的预言机（Oracle）机制，则挑战的仲裁者事先指定该预言机；如果没有，则需要事先从 MYKEY 社区中建立可靠的预言机组织。

对于非确权链上已经建立的账户与身份名称的绑定关系，仍然可以通过“抵押声明 + 挑战期”的方式来推翻，以纠正建立绑定关系时可能造成的错误。推翻的门槛比建立要高得多，所需抵押的 KEY 数量远远大于建立绑定关系时所需的 KEY 数量，挑战期持续的时间也相应更长。尝试推翻的挑战次数没有上限。

身份名称命名规则如下：

1. 身份名称可包含 1–63 个字符。
2. 字符的范围包含：a–z 的 26 个小写英文字母，A–Z 的 26 个大写英文字母，数字 0–9，以及连字符“–”。
3. 身份名称不区分大小写英文字母。
4. 身份名称不允许以连字符“–”开头或结尾。

虽然一个 MYKEY 账户可以持有多个身份名称，但是当身份名称一旦与 MYKEY 账户绑定后，该绑定关系永久有效，且不可撤销。一个 MYKEY 账户只能绑定一个身份名称。未绑定的身份名称可以转让。

为预防身份名称被大量抢注，所有的身份名称都以拍卖的形式逐渐释放。身份名称是一个开放的体系，并非只有 MYKEY 账户才能参与竞拍，事实上，所有确权链上的其他账户均可以

平等地参与拍卖。拍卖所得由 MYKEY Lab 获得。拍卖规则如下：

1. 按时间释放的数量限制：
   - 单字符：每 120 天释放 1 个名称
   - 2 字符：每 7 天释放 1 个名称
   - 3 字符：每天释放 5 个名称
   - 4 字符：每天释放 125 个名称
   - 5 字符：每天释放 3000 个名称
   - 6 字符：每天释放 85000 个名称
   - 7 字符及以上：无单日上限
2. 每个身份名称至少支付 0.1 KEY。
3. 对于同一个身份名称的拍卖，每次叫价必须至少是前一次价格的 110%。
4. 当对同一个身份名称 24 小时内无更高叫价时，该身份名称可以被成交。
5. 对于每类身份名称，在可成交的身份名称列表中每天按出价由高到低成交。当达到每日成交数量上限时，未成交的身份名称递延至下一日。被递延的身份名称在第二日不享有优先权。
6. 任何未成交的身份名称均可以被叫价。

3.3 免费使用额度

本小节关于“免费使用”的特性并非 Key ID 自主身份协议的组成部分，而是该协议的首个实现——MYKEY App 的特性。

互联网培养了用户免费使用的心智模式，而公有区块链的使用却必然是收费的，这是为了抵御垃圾交易的攻击。有些看似免费使用的公有区块链，实际上是通过通证的时间价值来支付，本质上仍然是收费的。

收费造成了门槛和摩擦。MYKEY 在多条公有链上均提供一定数量的免费使用额度，用户在注册 MYKEY 账户的时候可以选择向 MYKEY Lab 进行真实身份校验，以获得免费账户和一定数量的免费使用额度。MYKEY Lab 在完成用户身份校验后不保存用户的具体身份信息，只保存相关哈希值，即 Hash(姓名 + 证件类型 + 证件号码 + 随机数)，这么做既确保了单个用户不能无限制地申请 MYKEY 账户，又保护了用户隐私，这是因为负责身份校验的 MYKEY Lab 都不知道任何 MYKEY 账户的真实身份。

免费使用额度以 KeyPoint 的形式（以下简称 KP）来计量，KP 是使用权，不能转让。

1KP = 1 美元，每一个通过真实身份校验的早期用户将获得若干数量的 KP，并每日增加一定数额的 KP，直至上限。

对于未完成真实身份校验的用户，需自行承担公有链使用的一切成本，包括初次建立账户和后续使用。用户可通过购买 KP 获得使用权。

3.4 账户安全

MYKEY 账户的安全性来自多方面。首先，MYKEY App 代码开源，可以调动整个区块链开源社区的力量来全面地审查代码，例如通过开展赏金猎人活动寻找潜在的代码漏洞。

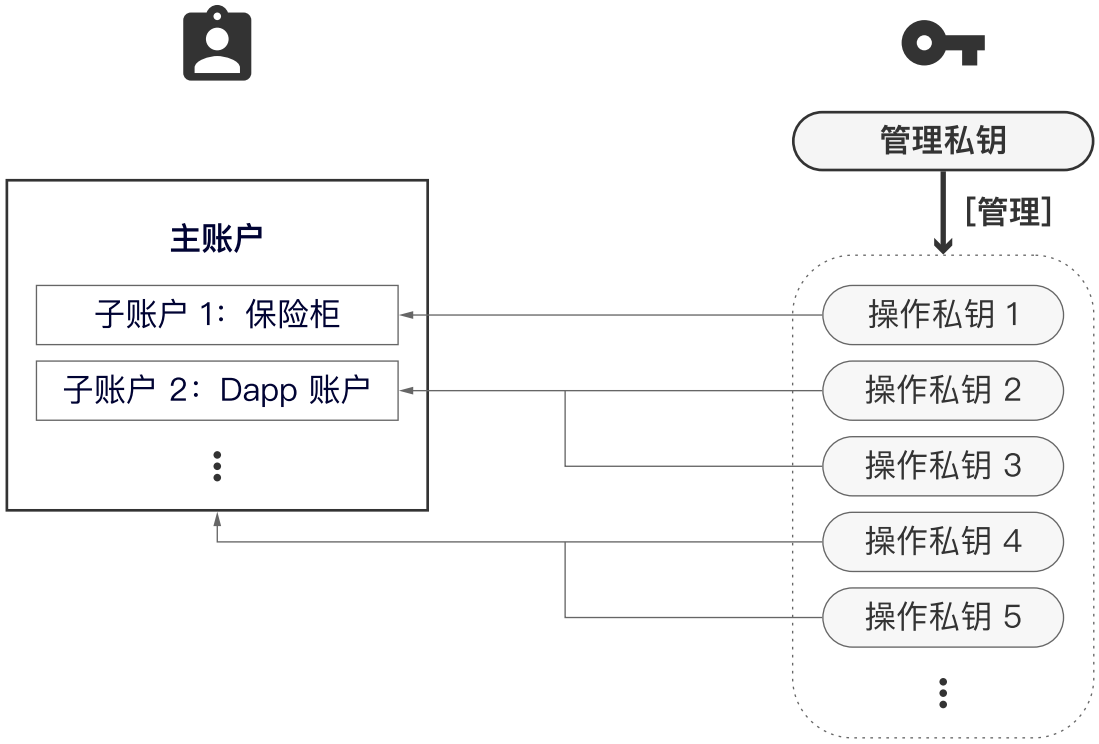

图 2，MYKEY 账户体系和私钥权限结构。

其次，如图 2 所示，MYKEY 的账户体系在设计上设置了多种互相制约的权限，配合权限生效的时间延时，使得账户在整体上不存在单点故障的风险。个人账户的权限由“管理私钥”和“操作私钥”联合掌管，设置如下：

1. 管理私钥。管理私钥掌握账户的最高权限，必须**仅由用户本人**持有，且任何时候不与任何人分享。管理私钥不保存在 App 所在的智能设备里，在 MYKEY App 中以 12 个英文单词恢

复码的形式体现，由用户以纸质形式线下保存；管理私钥在后期可以以硬件钱包的方式保存。管理私钥可以冻结和修改其他的操作私钥以及更换管理私钥本身，但是它不能直接操作账户，例如管理私钥无法动用账户内的任何资产。管理私钥的权限如下：

A. 管理私钥单方面冻结账户的操作私钥，立即生效。
B. 管理私钥单方面解冻账户的操作私钥，延时 7 天生效；管理私钥联合紧急联络人解冻操作私钥，立即生效。
C. 管理私钥单方面变更操作私钥，延时 7 天生效；管理私钥联合紧急联络人变更操作私钥，立即生效。
D. 管理私钥单方面更换管理私钥，延时 21 天生效；管理私钥联合紧急联络人更换管理私钥，立即生效。
E. 管理私钥单方面撤销正在等待生效的管理私钥变更操作、正在等待生效的操作私钥变更操作、正在等待生效的操作私钥解冻操作，立即生效。
F. 管理私钥单方面添加 / 移除紧急联络人，延时 21 天生效。
G. 管理私钥添加操作私钥的类别，立即生效。

2. 操作私钥。操作私钥针对 MYKEY 账户的具体功能，每一项功能都分别对应不同的操作私钥，互不干扰。

2–1. 紧急协助任务的响应私钥。每一个 MYKEY 账户均可以成为其他 MYKEY 账户的紧急联络人，因此每个用户可自行设置信任的个人或机构作为紧急联络人，MYKEY 账户在设立时默认指定 MYKEY Lab 作为紧急联络人，用户可添加或更改紧急联络人，最多可设置 6 名紧急联络人，最少设置 1 名。Key ID 协议本身不规定紧急联络人的数量限制，以上的数量限制来自 MYKEY App。紧急联络人作为一个整体参与账户主人的紧急协助任务，当 60% 及以上的紧急联络人投票通过后，紧急协助任务被执行。紧急协助任务的响应私钥权限如下：

A. 配合被协助人的管理私钥解冻操作私钥，立即生效。
B. 配合被协助人的管理私钥更换管理私钥，立即生效。
C. 配合被协助人的管理私钥变更操作私钥，立即生效。
D. 紧急联络人单方面更换被协助人的管理私钥，30 天生效。

2–2. 资产管理私钥。资产管理私钥用来对 MYKEY 主账户下的资产进行操作，例如转账、抵押等。该私钥对于 MYKEY 主账户下为特殊目的设立的子账户内的资产不具备操作权限。

2–3. 特殊目的子账户的操作私钥，例如储蓄账户、外部应用专用子账户等。

2–4. 登录私钥。以 MYKEY 账户的身份授权登录各种外部应用。

2–5. 投票私钥。以 MYKEY 账户的身份对某些议案进行投票操作。

2–6. 可验证声明的操作私钥。MYKEY 账户是 Key ID 的一种实现，而 Key ID 作为自主身份协议的基本单元，可以对其他 Key ID 发表可验证声明。

通过以上的权限设置，在紧急联络人保持可信的情况下，在以下场景下账户均可被恢复正常:

1. 忘记 MYKEY App 密码。
2. 遗失设备，例如手机。
3. 操作私钥泄露。
4. 管理私钥遗失。
5. 管理私钥泄露。
6. 遗失设备且同时遗失管理私钥。
7. 用户发生重大意外，例如长期失踪或死亡。

用户只有在一种场景下无法恢复账户的正常使用：管理私钥泄露并且同时遗失。在这种情况下，系统实际上无法区分当前掌握了管理私钥的人与理论账户主的区别。此时，这个人掌握管理私钥，且没有其他任何人掌握管理私钥，这正是系统认定账户主人的最终依据。因此，App 在用户设置恢复码（即管理私钥）时会特别提醒用户将恢复码至少抄写 2 份，并分别存放于仅自己知晓的不同地点，那么，如果有人意外发现其中一份恢复码并将其取走，用户还拥有其他备份，不至于彻底遗失恢复码。

后期，MYKEY 将考虑推出针对机构的服务，机构账户的权限设置将更加细化。

3.5 协议可升级

可升级性对于一种协议的长期发展具有重要意义，Key ID 自主身份协议将随着去中心化存储技术、跨链技术等底层技术的成熟而不断更新，以适应新环境，更好地满足用户的需求。

协议的可升级性与无需信任性（trustlessness）有着天然的矛盾，解决这一矛盾的核心是在升级协议前形成社区的广泛共识，并保护用户可退出的权利。因此，Key ID 协议在升级前必须提前经过社区的广泛讨论，新代码经过足够长时间的社区审计以及代码漏洞的赏金猎人计划，并且在升级协议的智能合约逻辑里设置等待期，即等待期无法被跳过。等待期用以保护用户可退出的权利，在协议发展早期等待期设为 4 天，随着协议的发展完备，等待期时间逐渐延长。

协议升级由 MYKEY Lab 控制的多签账户发起。在本白皮书第 6 小节描述的 MYKEY Lab 的通证化改造有助于形成关于协议升级的社区共识。

3.6 防垃圾交易

防垃圾交易功能是 MYKEY App 的功能，不属于协议层。MYKEY App 将通过动态机制来屏蔽干扰用户的垃圾交易信息，以提升用户体验。

4. 信任网络

信任网络的详细阐述将在今后的白皮书中更新，本版白皮书只做方向性描述。

信任网络由两部分组成：身份账户和可验证声明。身份账户是指符合 Key ID 自主身份协议的账户，这些账户统称为 Key ID，MYKEY 账户是其中一种 Key ID；可验证声明是指声明主体（一个身份账户）关于声明对象（另一个身份账户）的描述，例如，身份账户 A 发表关于身份账户 B 的声明：B 的年龄大于等于 21 岁；“可验证”属性则来自于去中心化账本技术，使得声明发表的主体、对象、时间、内容完全明确且不可篡改。

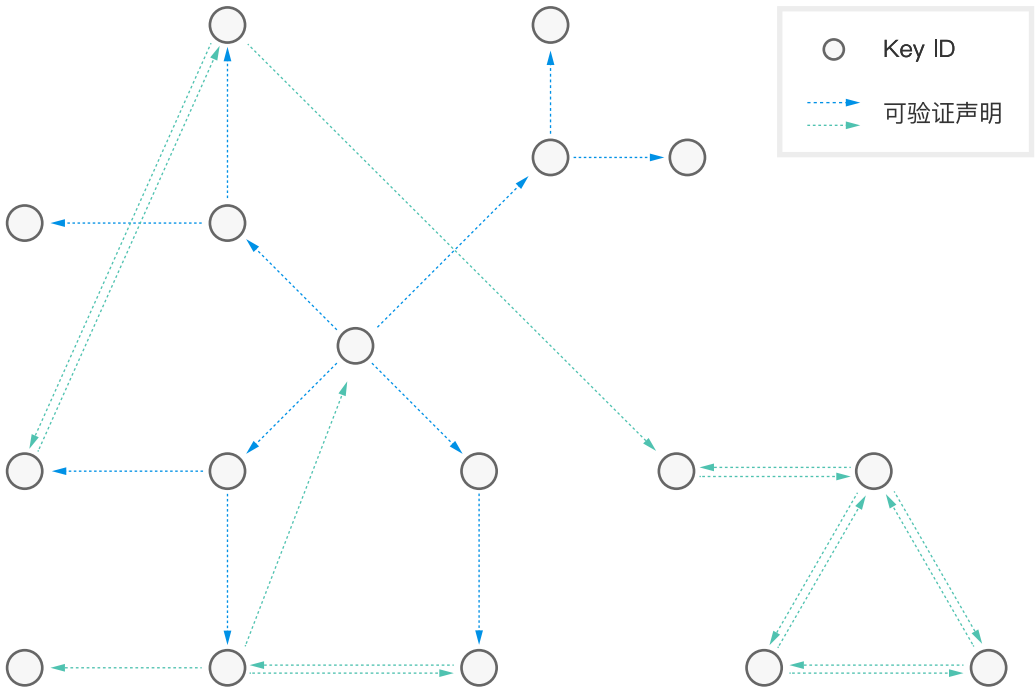

图 3，信任网络示意图。

身份账户是信任网络的组成节点（node），而可验证声明则是节点之间的链接（link），使得原本独立的身份节点互相印证，形成一张巨大的信任网络（web of trust）。信任网络的结构使得证明身份以及证实过往历史变得高效和可靠，使得伪造身份和提供虚假证明变得无所遁形，因为信任网络中的局部造假很容易通过造假部分与其余网络的链接状况来识别。信任的传递结构可以是层级式的（图 3 中蓝色链接），也可以是自由式的（图 3 中绿色链接）。

从技术架构看，身份账户由 3 部分组成：（A）身份名称，（B）身份文件，（C）身份合约控制的、基于去中心化存储的数据安全区。身份名称在 3.2 小节中已详细阐述。身份文件是该身份账户的属性描述，具体请参见此链接。数据安全区是指由身份账户的智能合约控制的去中心化数据存储区域，其访问权限完全由身份账户控制，用于存储身份账户相关的公开数据和隐私数据。数据安全区的开发和技术架构受制于去中心化存储技术的发展和成熟，在去中心化存储技术成熟前需寻找折中方案。

信任网络的重要意义包括但不限于以下几点：

1. 对抗图像和语音合成技术（例如：deepfake）造成的假信息、假新闻、欺诈等问题；
2. 更全面、更高效的个人信用体系，减少协作中因缺乏信任而造成的摩擦（例如：证明我妈是我妈）；
3. 形成基于信任网络发展而来的新型协作模式的组织结构。

5. 数据的可靠存储

数据的可靠存储的详细阐述将在今后的白皮书中更新，本版白皮书只做方向性描述。

在上一小节中已经提及了数据安全区，数据安全区不但是信任网络的基本组成构件，而且在其他身份领域中也起着关键性的作用，因此有必要单独介绍。

5.1 信任网络中的隐私

由于公有区块链上存储的所有信息都是公开的，因此无法存放隐私数据。可验证声明的具体内容不适合直接存放在区块链上，而是应该存放于身份账户控制的数据安全区中，再将某种基于密码学的摘要存储在区块链上，以实现“可证明”属性。摘要的方式可以是哈希树头。

5.2 个人数据的全记录

由于数据安全区基于去中心化存储技术，并且完全由账户身份的智能合约控制，这意味着安全区中的数据完全由身份账户的主人控制，没有其他任何人能够在没有得到主人授权的情况下访问，因此，用户可以将自身极其隐秘和重要的数据存放于此，例如：

1. 个人的健康数据；
2. 线上活动的全记录；
3. 遗嘱；
4. 可穿戴设备记录的数据。

这些数据在主人授权的情况下可以定向分享给其他身份账户，当然也可以设置成完全公开。由于智能合约的可编程属性，这些存放于数据安全区的信息可以事先确定分享的方式，例如遗嘱可以在该身份账户连续若干天无活动记录后分享给某些特定账户访问。再例如，整个安全区内的数据可以在身份账户宣布死亡 50 年后公开所有数据，并有望将数据保留上千年，因为去中心化存储技术带来的可靠性和稳定性。

5.3 去中心化应用

去中心化应用（Dapp）的部分或全部数据会存放在去中心化存储上，那么对于这些数据的访问需要以身份账户的方式来授权，某些与 Dapp 的交互信息也可以存放在身份账户下自己的数据安全区。去中心化应用和身份账户分别有自己的数据安全区，这种双数据存储的结构将为 Dapp 的开发提供灵活性，例如选举 Dapp，在 Dapp 中可以以某种零知识证明的方式隐藏单个用户的投票结果以保护隐私，另一方面，在用户自己的身份账户下记录完整的投票细节。

6. MYKEY Lab 的通证化改造

本小节描述的内容，不作为实质行为发生的任何承诺。MYKEY Lab 是否进行通证化改造，何时进行通证化改造，以何种方式进行通证化改造，均完全取决于 MYKEY Lab 股东和管理层的意愿和决定。

不可否认，中心化相较于去中心化有效率上的优势。一个项目的早期高速发展，通常需要一个中心的强力推动。虽然 MYKEY App 的早期运营以中心化的方式开始，该系统的最终目标

是被 MYKEY 社区接管，为全社区成员所共同拥有和共同治理。

MYKEY Lab 在通证化改造后将变为一个名义实体，对于 MYKEY App 以及 Key ID 协议的决定权将全部赋予一种通证，暂且称之为 Governance Token（以下简称 GT）。通证化改造后，MYKEY Lab 赚取的绝大部分利润将以 GT 的形式保存，该部分 GT 的处置将由全体 GT 持有人每 4 年通过投票决定。

GT 的分配。GT 的总量为 1000 亿，40% 分配给用户，20% 作为运营推广池，25% 给予 MYKEY Lab 的原股东，15% 给予通证化改造后新成立的 Key ID Foundation，其中 25% 和 15% 的部分为 4 年线性释放，从通证化改造完成后开始计算时间，并写入智能合约。

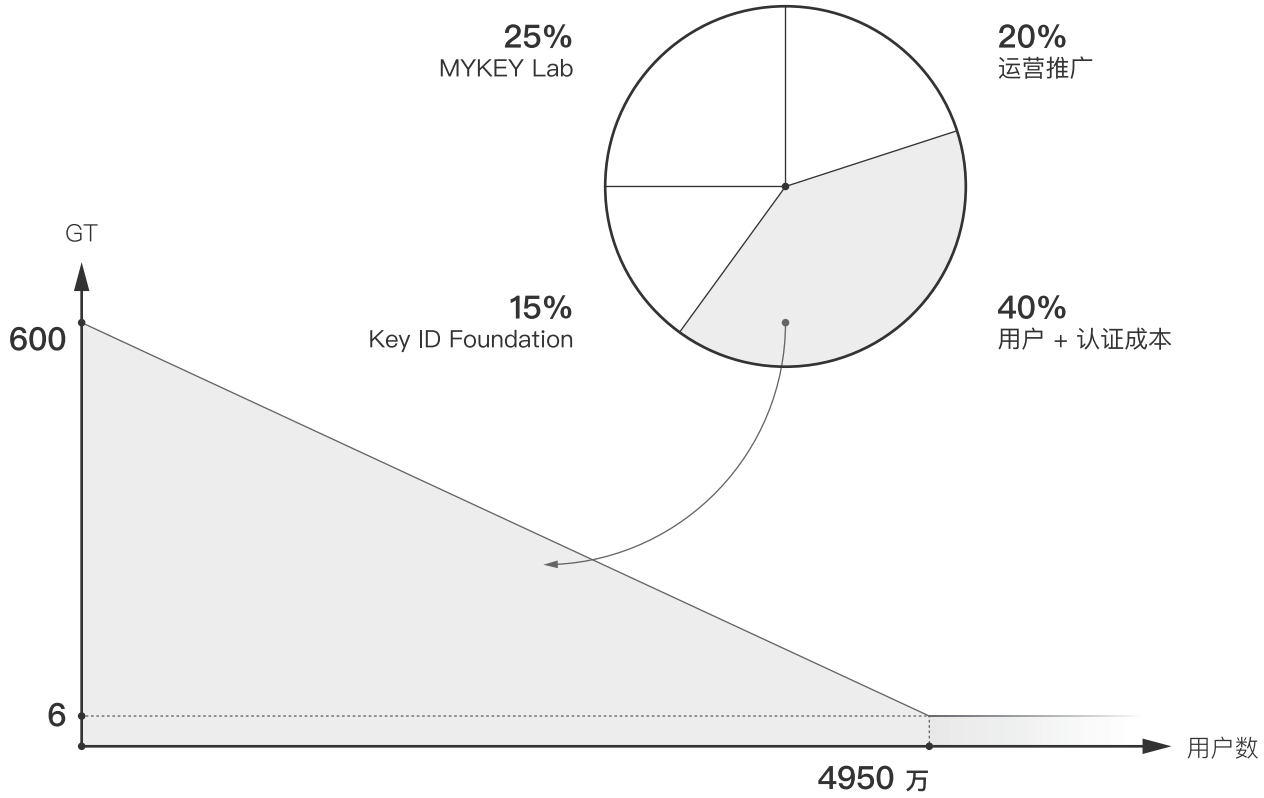

图 4，GT 的分配。

用户池的 400 亿 GT 分配计划如下：

1. 第 1–10000 名通过真实身份校验的用户，每人获得 600 GT；
2. 第 10001–20000 名通过真实身份校验的用户，每人获得 (600–1*0.12) GT；
3. 第 20001–30000 名通过真实身份校验的用户，每人获得 (600–2*0.12) GT；
4. 以此类推，线性递减至 6 GT，之后每名通过真实身份校验的用户均获得 6 GT，直至用户池完全耗尽；

5. 以上为 GT 分配至每位用户的平均数量，具体执行可灵活操作，例如可设置 20% 推荐奖励等；
6. MYKEY Lab 为用户进行的真实身份校验所付的成本，全部由用户池支付。

通证化改造后的 MYKEY 社区将主要以间接民主的方式实现治理，配合必要的直接民主和流动民主。具体来讲， MYKEY Lab 以及届时新成立的 Key ID Foundation，均由一个委员会来管理，委员会由全体 GT 持有人选举产生，每届任期四年；首届临时委员会由 MYKEY Lab 指定产生，任期两年。临时委员会负责制定《MYKEY 社区共识公约》，该公约将成为 MYKEY 社区治理的长期纲领，《MYKEY 社区共识公约》将明确委员会的权利、责任、利益的边界，以及社区规则更改的流程。原则上，只要流通 GT 投票参与率超过一定比例，并且 2/3 以上得分通过（注：得分不一定等于投票数，可与身份结合），则可修改所有基础规则，以使社区治理保持灵活，不断进化。参与投票的 GT 须处于锁定状态方视为有效。