

# THEKEY

基于国家大数据和区块链技术的身份识别工具

## 项目介绍

**2017 年 10 月**

# 目 录

<b>摘要</b>	<b>4</b>
<b>项目背景</b>	<b>6</b>
<b>THEKEY 项目</b>	<b>8</b>
内涵和外延	8
技术实现方法	9
项目组已有的解决方案	14
<b>THEKEY 生态圈</b>	<b>17</b>
THEKEY 生态圈	17
THEKEY 生态圈的运营	19
<b>THEKEY 的未来</b>	<b>21</b>
<b>THEKEY 的发展路线图</b>	<b>23</b>
<b>项目执行团队与合作伙伴</b>	<b>24</b>
项目团队	24
早期投资人	30
顾问团队	29
团队的区块链项目经验	31
项目合作伙伴	32
管理委员会的设置	32
<b>结论</b>	<b>33</b>

## 摘要

“不可抵赖”和“不可篡改”是区块链技术的核心和精髓，因此与之相对应的身份识别技术也必须具有“不可抵赖”和“不可篡改”的特性。否则，就不可能在互联网世界中建立起相互信任的关系。目前网络实名制（VEID）、手机实名制以及各种生物学认证技术均未能解决互联网身份识别的上述痛点问题。在这一背景之下 THEKEY 项目团队行将开发和研制 BDMI 技术，其目的是在互联网上提供具备“不可抵赖”和“不可篡改”特性的身份识别服务、彻底解决网络身份虚拟化问题。

BDMI (Blockchain Based Dynamic Multi-dimension Identification) 是基于区块链的动态多维身份识别技术，顾名思义，是由两大部分技术组成：动态多维身份识别技术(DMI)+区块链技术。DMI 身份识别技术将用户实时身份数据、行为数据以及场景数据交叉验证，确保身份验证结果的“不可抵赖”性质。而区块链技术保证身份验证结果的“不可篡改”。目前，THEKEY 项目组已经在动态身份识别技术方面取得了突破性进展，因此为项目的成功奠定了坚实的基础：

- 获得 23 项著作权,另有 15 项相关发明专利已经获得受理并进入实质审查阶段。
- 动态多维身份识别技术作为移动医疗保险支付解决方案中的关键技术已经在两个试点城市得到了实际应用。通过移动医疗保险支付，用户可以获得基本医疗保险的报销。目前 THEKEY 项目组正在 41 个城市部署移动医疗保险支付，覆盖人口 1.3 亿。
- 目前 THEKEY 项目组已经实时联通了 66 个城市、2.1 亿人口的相关政府的身份识别数据，为其身份识别产品的开发和升级换代奠定了坚实的基础。
- 已经和诸多世界著名企业签署了商业合同，THEKEY 项目组对商业模式的设想得到了充分验证。
- 已经发起并主持了由政府、银行、商业保险公司以及大学相关学科的六个国家级实验室。

为了推广 BDMI 技术的应用，THEKEY 项目组将建立一个由参与者（个人用户、服务提供商、身份识别验证方），智能合约和 TKY 积分三元素组成的去中心化的生态系统。建立和营造 THEKEY 生态圈的目的有两个：第一，维护良好的数据

治理环境，确保个人数据的合理充分使用以及数据安全。第二，使身份识别验证方获得及时、足额的报酬以支持身份识别服务的快速、健康和可持续的发展。在 THEKEY 生态圈内，以一个北京常住居民在新加坡购买当地医疗保险，当地医疗保险公司触发身份识别请求，同时需要获取用户健康档案为例，THEKEY 用户身份识别包括以下 8 个步骤：

- 新加坡保险公司作为服务提供商发起身份识别请求。
- 用户通过手机 THEKEY 的 APP 或者通过保险公司端设备提交自己的指纹或者其他生物学特征如人脸、虹膜等，并与 THEKEY 以及保险公司签署相关的智能合约。
- THEKEY 作为身份识别验证方将保险公司请求与行业要求进行比对从而检查保险公司请求的合理性。
- THEKEY 将用户上传的生物学识别信息与政府数据库中该用户经政府认证过的生物学识别信息进行一致性检查确认用户身份。与此同时，THEKEY 还将其生物学识别数据与来自其他数据源的同一用户行为数据和场景数据进行交叉校验以确保结论的可靠性，这一切都是通过加密安全的接口自动完成的。
- 用户身份得到确认之后，THEKEY 将依照智能合约的要求采集用户健康档案并发布上链。
- 身份认证服务完成之后，智能合约将依照合约的规定分配 TKY 积分。
- 与此同时 THEKEY 将所有计算结果存证以供日后数据审计。
- THEKEY 将定期进行数据审计并对用户信用做出评价。

整个身份识别验证的结果高效、准确、可信，并且能够根据保险公司的业务需求，在遵守行业标准以及相关法律法规的前提下，对身份识别要求进行定制化解决方案，降低保险公司成本，进而降低保费，从而实现多方共赢。

与身份识别领域内同样采用区块链技术的产品相比较，THEKEY 具备以下 3 大优势：

- 结论更可靠：由于在身份识别过程中采用了实时、全面、准确和可靠的数据，特别是公权机构认证的身份识别数据，BDMI 所产生的身份识别结论将更加可靠。

- 成本更低廉：由于全部采用了现有数据进行身份识别，避免了数据采集、处理、分析、加工和认证等重复投入的巨大成本。
- 用户更友好：采用 BDMI 技术用户可不用安装、注册任何产品和上传任何信息，而在进行身份认证的过程中也可不用携带任何设备、甚至手机！

我们特此邀请您参与 THEKEY 项目，创造历史、改变世界。

## 项目背景

2015 年 4 月 8 日，中国的人民日报发表评论《怎么证明我妈是我妈》，提到北京市民陈先生出境旅游填自己母亲为紧急联络人，却被要求证明他和他母亲是母子关系的案例。2015 年 5 月 6 日的中国国务院常务会议，讨论确定进一步简政放权、取消非行政许可审批类别时，中国总理李克强痛斥证明“我妈是我妈”是天大的笑话，一时为世人所熟知。

但在现实生活中我们不但要证明“我妈是我妈”，还时时刻刻要证明“我是我”。从清晨出门上班，我有权锁自己家的门、我有权开自己的车、我有权进入自己的办公室、我有权搭乘火车、飞机和入住酒店。甚至去幼儿园接自己的孩子回家，我也必须证明“我真的是我”。凡此种种，不一而足。由此可见，“我妈是我妈”和“我是我”不仅仅是一个深刻的哲学问题、社会问题，更是一个摆在我们每个人面前的现实问题。

随着越来越多的社会活动和经济活动从线下向线上的转移，身份识别问题日益突出，已经成为互联网技术发展的瓶颈问题。由于互联网技术虚拟化的特性，人们非常容易在网上隐藏其真实身份，从而在带来便利的同时带来了巨大隐患。一个明显的例证就是信用卡使用造假。使用信用卡的不一定是信用卡持有者本人。当然，现在银行采取了一些诸如向用户手机发送验证码等重复校验的措施。但这些措施并非一定有效和可靠，如果手机与信用卡同时被盗、手机和信用卡同时在另一个人手中又该如何呢？更为重要的是，身份识别在大多数情况下还要承载着经济、技术、政治、道德和法律的责任，因此必须具备“不可抵赖”和“不可篡改”的特性。

由此可见，互联网上进行有效身份认证必须包括以下要素：

- 身份识别必须使用公权机构认证过的相关数据，以确保结论的可靠性。采

用用户自己上传数据作为身份识别依据的做法容易造成数据源污染并给欺诈等犯罪行为留有空间。

- 须采用同一用户不同数据源数据进行交叉验证的方法以确保身份识别的可靠性。
- 必须采用动态数据进行身份识别以避免身份识别结果的错误。
- 必须尽可能多地获取同一个人的身份识别数据以满足不同服务提供商的身份识别需求。
- 必须完成身份识别数据在通讯协议、文件格式以及术语上的标准化工作以保证数据应用和分析。此外，
- 必须要根据法律的规定形成良好的数据治理环境。良好的数据治理环境不仅仅包括个人隐私的保护，同时还包括社会稳定和国家安全的维护。

如果无法满足上述条件，就无法在互联网上形成有效的身份识别，有可能形成以下后果：

- 财产损失，例如信用卡和社会保障卡的冒用和盗用。
- 法律和名誉损失，例如冒用他人姓名在网络上散布不当言论。
- 技术失误的责任转移。冒用他人名义进行技术操作导致不良后果。
- 个人隐私的盗取或者泄露。
- 国家机密信息的泄露。数据安全不仅仅事关个人隐私，同时还事关社会的稳定和国家安全。因此不同的国家对此都有相关的法律规定。对数据的错误理解、算法的错误和分析结论的错误均有可能导致社会动荡和损失。此外，在一些情况之下接触个人数据，比如与武器实验相关的个人数据在各国均需得到政府事先授权。

尽管现有互联网身份识别产品可以满足部分需求，并且也有不少实际应用的例证，但迄今为止，由于上述种种原因尚未见有真正意义上的突破性进展。目前世界上所有基于互联网的身份识别技术所产生的结果都不具备“不可抵赖”和“不可篡改”的两个特性，因此也无法支撑区块链技术建立一个互相信任的互联网世界。

## THEKEY 项目

### 内涵和外延

在上述背景之下,THEKEY 项目组将采用区块链以及智能合约等技术开发第二代互联网身份识别技术,以期解决目前在互联网身份识别解决方案中所存在的全部问题。

THEKEY 将采用 NEOContract 作为智能合约体系,使用 DNA 框架开发,与 NEO 同构,共同构建数字资产+数字身份+智能合约的智能经济。而 THEKEY 将更加专注于身份识别这一专业领域,成为整个体系身份认证坚实的基础,充分利用 NEO 对多编程语言的兼容性以及 NEOVM 虚拟机的通用轻量化、高并发、高扩展等特性,快速实现各领域的身份识别智能合约开发和普及。

THEKEY 项目组的身份识别解决方案叫做 BDMI 技术。BDMI (Blockchain Based Dynamic Multi-dimension Identification) 是基于区块链的动态多维身份识别技术。BDMI 为互联网开发了一个强大而高效的身份识别工具,其根本目的是通过 BDMI 形成一个“不可抵赖”和“不可篡改”的身份识别结论,进而建立一个可以互信的互联网世界。

为实现以上目的,BDMI 在解决身份识别问题时,需同时具备以下 6 个要素:

- 以用户生物学识别特征为基础。
- 以政府认证的身份识别数据为依据。
- 采用同一用户身份识别数据与其行为数据和场景数据进行多维度数据交叉验证以确保身份识别的可靠性。
- 采用实时更新的数据进行身份识别,以确保身份识别的有效性。
- 采用尽可能全面的身份信息满足不同服务提供商个性化的身份识别需求。
- 为求万全,身份识别信息一经使用,需存证以供日后数据审计,从而为个人信誉评价建立基础。



## 技术实现方法

如前所述，BDMI 包括了两个部分的技术，即动态多维身份识别技术以及区块链技术。

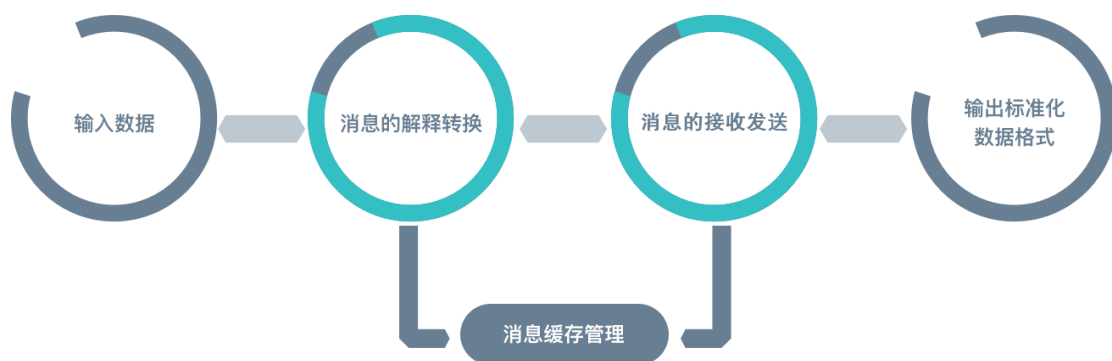
### 动态多维身份识别技术 (DMI)

与传统的做法不同，THEKEY 项目组没有建立中央化的个人隐私数据采集、加工、存储和应用中心。在其现有的解决方案中 THEKEY 项目组依托在省级或者地市级政府的信息中心中建立自己的动态多维身份识别系统。这样做带来的最大好处是避免了数据采集、加工处理、存储和认证系统重复建设费用、在提高身份识别可靠性的同时极大地降低了身份识别的成本。

THEKEY 项目组的动态多位身份识别系统由数据采集、数据标准化、用户主索引建立、数据存储以及身份识别引擎等 5 个主要模块构成，一如下述：

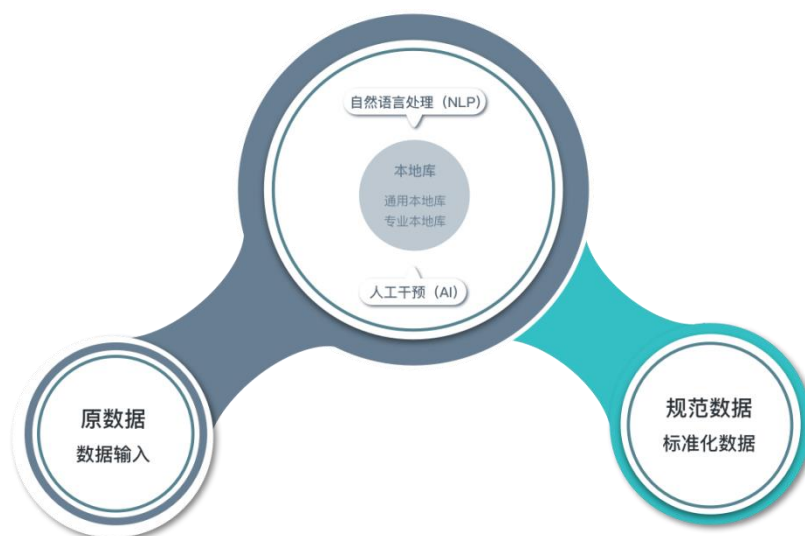
- 中心化数据采集模块。中心化数据采集主要依托于 ETL 技术（即从数据源端抽取（extract）、转换（transform）、加载（load）至中心端的技术）实现。数据采集模块的功能是将来源广、类型多、格式多样化的数据，在每个业务点上抽取和格式的统一并传输到中心端进行集成。数据抽取采集的方式，一般有全量抽取和增量抽取两种。数据采集模块集成了数据清洗的功能，目的是将不一致、输入错误、不完整的数据进行清洗转化。数据抽取、转换和加载功能都是可插拔，可以任意组装的。各组件之间通过数据总线共享数据，以提高数据采集的性能，由于全部采用了现有数据进行身份识别，避免了数据采集、处理、分析、加工和认证等重复投入的巨大成本。
- 数据标准化模块。数据采集完成之后要进行数据标准化。数据标准化是指不同数据源之间要进行通讯协议、文件格式以及术语的标准化。数据只有标准化之后才能进行数据分析和数据应用。数据标准化的难点是通讯协议标准化和术语标准化两个部分，如下所示：
  - 1) 通信协议标准化模块。THEKEY 项目组在国际通用的行业信息交换标准基础上建立标准化的信息传输协议。以健康数据为例，THEKEY 项目组在医疗信息交换标准（Health Level 7）基础上，建立了一套普遍适用于通用领域的标准化的信息传输协议。它的主要作用是能够在不同的异

构数据系统之间，进行数据交互传输。通信协议标准化模块是一组支持通讯过程中传输、调用的中间件。模块本身并不干扰系统自身各部分正常工作，不会参与内部信息交换过程，也就不会对内部信息处理增加负担。只有当系统与系统之间发生信息交换时，模块才会按照通信协议标准化的约定，完成信息的访问和交换。模块包括消息的解释转换功能、发送接收功能以及消息的存储管理功能。其中消息的解释转换模块为技术核心。



通讯协议标准化引擎工作原理

- 2) 术语标准化模块的逻辑设计是基于知识本体 ( Ontology )、自然语言处理引擎 ( NLP )、人工干预 ( AI ) 三大支柱。其中本体涵盖通用本体库和专业本体库 ,可满足在不同应用场景下对数据的需求。流程如下图所示：



术语标准化原理图示

- 用户个人主索引模块。用户个人主索引是指个人基本信息检索目录。其主要用途是在一个复杂的数据体系内，通过唯一的用户个人信息将多个信息有效地关联在一起，以实现信息之间的互联互通。从用户个人数据模型可以看出，用户个人信息主要分为两类，一类为“能唯一标识用户的个人信息”，一类为“不能唯一标识用户的个人信息”。用户个人主索引的建立主要通过以下工作流程：
  - 1) 提取用户个人静态信息；
  - 2) 匹配静态数据；
  - 3) 判断是否符合；
  - 4) 匹配成功分配主索引号，建立交叉关联索引；
  - 5) 未能匹配成功，匹配动态数据，写出日志数据。
- 数据存储模块。目前，大数据的存储是一大挑战，大量数据高效、安全的长期保存，快速、简单的管理维护，是当下大数据管理人员需要关注的主要问题。与此同时，数据存储模块中还镶嵌了数据库修改、统计、检索、打印等功能。
- 身份识别引擎（IDV 引擎）。身份识别引擎的主要功能是在上述四个模块所组成的数据交换平台之上，根据不同场景下的需求完成身份认证。当接收到一个身份识别请求时，身份识别引擎首先将收到的用户生物学特征数据与政府数据库经过认证的该用户生物学特征数据进行一致性检查。与此同时，还会将此次身份识别数据与不同渠道、不同时间的同一用户行为和场景数据进行交叉验证。通过这些验证之后，身份识别引擎还将依照需求采集其他相关数据，并以身份认证的方式提供。身份认证提供之后将把所有服务中所采集的数据和计算结果全部存档以供后期数据审计。在数据审计过程之中将综合历次身份识别认证的结果对个人征信情况作出评估。

综上所述，采用动态多维身份识别技术可以非常便捷的对不同系统之间的多源异构数据实现中央化的采集、加工整理、存储并进行身份识别。此后，数据将通过哈希加密算法上链，并进行去中心化的应用。数据的确权、授权、定价和交易也将在区块链上完成。

## **区块链技术**

区块链是一种分布式数据库模式，数据存储于不同的节点，他们共同维护着数据和交易活动，并采用非对称加密算法保障数据传输与使用的安全，具有不可伪造和实时更新的特性。同时通过可编程的脚本实现所需的智能合约，提高了区块链的实用性。正是区块链技术的这些特性，将身份识别技术应用的难题很好的化解，下面的逻辑架构图很好的展示了身份识别技术运用区块链进行数据采集、清洗、加密、确权、交易等过程。

THEKEY 项目组致力于通过区块链技术达到以下功能 -

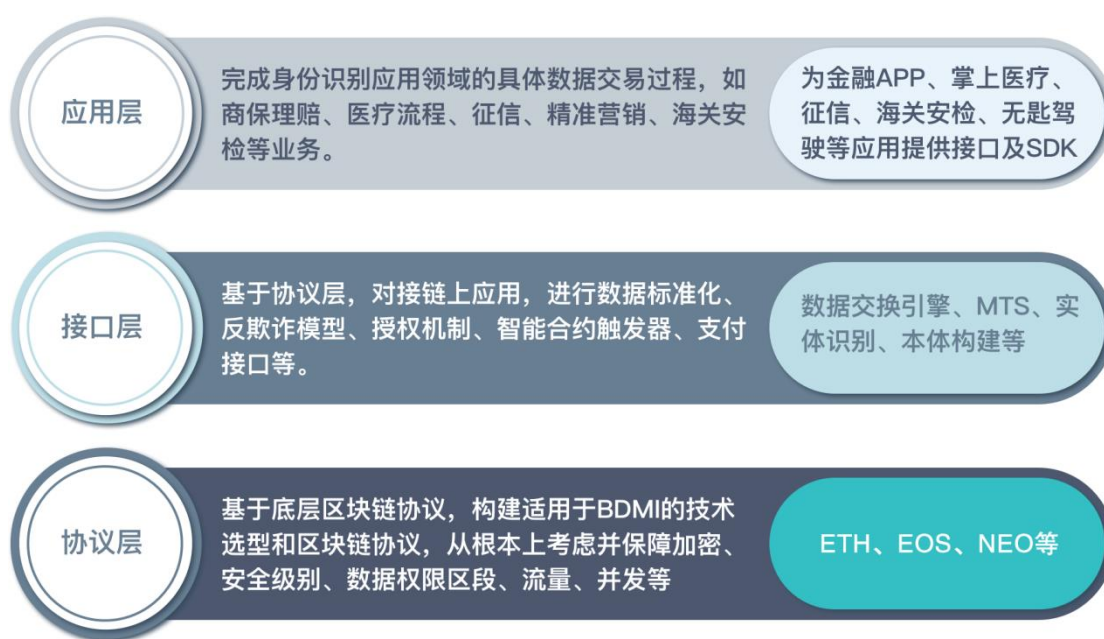
- 通过签订智能合约的方式使个人用户掌握个人身份验证数据的调取，并且保障身份验证符合个人隐私、数据安全、行业标准等方面的法律、法规，防止滥用个人信息；
- 所有身份数据的调取、使用和验证，都记录在区块链上，以备审计并进一步防止滥用；
- 目前重要数据都存储在各个机构的中心化服务器。这样不能有效防止数据被篡改以及灾难性的节点故障。未来所有重要数据全部与身份数据区块建立索引——对应，并采用分布式存储的解决方案保障数据高可用，确保所有关键数据的安全、准确、不可篡改。
- 由于区块链现阶段存储量有限，所以可考虑把身份数据加密保存在 THEKEY 生态中身份识别验证方的 ETL 数据库以及个人移动设备中，仅把数据对应的哈希值存储在区块链上。



BDMI 逻辑架构图

### BDMI 技术

就 BDMI 技术框架本身而言，可划分为三个层次，即协议层、接口层及应用层，如下图。协议层基于原生区块链技术构建适用于 BDMI 的技术选型，如 ETH、EOS、NEO，这一层制定了安全级别、数据权限、并发和流量处理等规则；接口层为协议层对接具体应用，提供身份数据的建模，实现数据标准化、反欺诈模型、智能合约触发器等一系列工作过程；应用层则负责实现具体的身份识别应用场景，为每一种身份识别所需的数据交换提供接口及 SDK（软件开发工具包）。



BDMI 协议层次图

## 项目组已有的解决方案

在我们谈及第二代产品之前我们先回顾一下我们现有的解决方案。THEKEY 项目组已有的解决方案是动态多维身份识别技术。这一技术在 THEKEY 项目组医疗保险 123 的手机 APP 上得到了应用。在两个试点城市中人们在就医时可以通过医疗保险 123 直接支付医疗保险的费用。一般用于购物等目的移动支付使用的是用户个人自己的钱，而移动医保支付使用的则是医保基金。因此，在医保管理部门确定支付之前需要满足更多的条件。而参保人员身份识别和资格审核是其中最为基础、最为重要的前提条件。我们现有的动态多维身份识别就在移动医保支付中起到了关键作用，实现流程包括以下几个步骤：

- 用户使用生物学特征信息比如指纹进行 APP 的注册。随即指纹将与医保管理机构中经过认证的指纹信息进行比对，并同时与电信、银行等机构分别存储的身份信息进行交叉比对，以确保原始身份识别的可靠性。
- 注册成功之后用户就医时就可使用手机进行医保支付了。用户通过所注册的 APP 发送指纹等生物学识别信息向医院发出付款申请，从而触发身份识别请求。
- 医院收到用户的付款申请之后即通过 APP 向医疗保险管理机构发送医疗保



险结算单。

- THEKEY 随后就该用户所发送的生物学特征信息与医疗保险管理机构认证过的同类信息进行一致性检查。
- 生物学信息一致性检查获得通过后，THEKEY 将该用户信息与公安、电信、互联网公司的同一用户的信息进行交叉校验。进行交叉校验的目的包括两个方面，1) 确定用户是否依然存活；2) 确定用户是否依然依法享受医疗保险待遇。
- THEKEY 将按照医疗保险管理机构的要求进一步采集相关数据并次第对本次医院付款请求进行真实性、合法性、合规性以及合理性检查。如果审核通过，医疗保险管理机构将会批准付款请求。
- 与此同时，THEKEY 将每一步计算的结果存证并根据医疗保险管理机构反欺诈、滥用和浪费的政策进行定期数据审计。审计结果计入用户或者医院的征信档案中。目前，THEKEY 还以社会保险、银行以及电信对的标准对个人征信进行评估尝试。

在我们现有的解决方案中有两个令人瞩目的特征：

- THEKEY 没有使用用户自传生物学特征信息作为身份识别的依据。相反，用户上传的生物学信息与医疗保险管理机构所存同类信息的一致性检验是身份识别的基础。这一设计的最大优点是避免了数据源头的污染，从而保证了身份识别的可靠性。如果从用户获取数据并以用户自身提供的数据为依据进行身份识别势必造成伪造、欺诈的空间。
- APP 不存储大量个人隐私信息，APP 只是用户生物学特征信息和存储在公权以及其他机构信息之间的桥梁。采用这种方法不但避免了个人身份重复存储的成本，同时也降低了个人隐私数据的泄露风险。

THEKEY 项目组已经在动态多维身份识别技术方面取得了突破性进展，因此为项目的成功奠定了坚实的基础。THEKEY 项目组业已取得的成就包括：

- 获得 23 项著作权,另有 15 项相关发明专利已经获得受理并进入实质审查阶段。
- 上述移动医疗保险支付方案已经在两个试点城市得到了实际应用。通过移动医疗保险支付，用户可以获得基本医疗保险的报销。目前 THEKEY 项目组正

在 41 个城市部署移动医疗保险支付，覆盖人口 1.3 亿。

- 目前 THEKEY 项目组已经实时联通了 66 个城市，2.1 亿人口的相关政府身份识别数据，为其身份识别产品的开发奠定了坚实的基础。
- 已经和诸多世界著名企业签署了商业合同，THEKEY 项目组对商业模式的设想得到了充分验证。
- 已经发起并主持了由政府、银行、商业保险公司以及大学相关学科的六个国家级实验室。

THEKEY 项目组截至目前所取得的成就已经证实了本项目在技术上的可行性和商业上的巨大价值。

尽管我们在身份识别领域里获取了重大进展，但是我们现有的解决方案只能在一个中心化的社区中应用。因此，我们身份识别技术的社会价值和商业价值受到了极大的限制。而区块链技术则给身份识别技术、给互联网和人类文明的进步带来了巨大的机会。首先，区块链技术可以在一个去中心化的自治社区里一方面确保数据安全、一方面确保数据的合理充分使用。其次，区块链技术、智能合约以及积分机制可以帮助我们建立起一个生态环境。在这个生态环境之中，所有为身份识别做出贡献的机构和个人都能够“按劳取酬”，从而能够使身份识别技术走上快速、健康和可持续发展之路。据此，我们计划在我们现有的 DMI 技术基础上引入区块链技术，进而形成革命性的互联网身份识别技术 BDMI。通过采用区块链技术，我们期望我们的产品能够更好的服务于用户。今后人们将不再需要在开设银行账户、申请贷款、入住酒店、搭乘飞机、领取养老金和医保报销时使用身份证、社保卡、护照、信用卡、钥匙、甚至手机去证实自己的身份。

与身份识别领域内同样采用区块链技术的产品相比较，THEKEY 具备以下 3 大优势：

- 结论更可靠：由于在身份识别过程中采用了实时、全面、准确和可靠的数据，特别是公权机构认证的身份识别数据，BDMI 所产生的身份识别结论将更加可靠。
- 成本更低廉：由于全部采用了现有数据进行身份识别，避免了数据采集、处理、分析、加工和认证重复投入的巨大成本。



- 用户更友好：采用 BDMI 技术用户可不用安装、注册任何产品和上传任何信息，而在进行身份认证的过程中也可不用携带任何设备、甚至手机！

## THEKEY 生态圈

随着第二代互联网身份识别技术的开发和 TKY 积分的销售，THEKEY 项目组将建立和营造一个 THEKEY 生态圈。THEKEY 生态圈是一个去中心化的自治社区，由三个部分组成：生态圈参与者（个人用户、服务提供商和身份识别验证方），智能合约以及 TKY 积分。建立和营造 THEKEY 生态圈的目的有两个：第一，维护良好的数据治理环境，确保个人数据的合理充分使用以及数据安全。第二，使身份识别验证方获得及时足额的报酬以支持身份识别服务的快速、健康和可持续的发展。

## THEKEY 生态圈

### 生态圈参与者

整个生态系统的参与方有个人用户、服务提供商和身份识别验证方三方组成。其中身份识别验证方是整个生态圈的支柱，身份识别验证方包括 THEKEY 项目组、政府相关部门、银行、电信以及其他相关部门。由于 THEKEY 能够从政府相关部门、银行、电信以及医疗机构获取身份识别相关的数据，甚至个人医疗健康档案，因此它无疑是去中心化自治社区中的一个重要节点，但它既不是唯一的节点也不是唯一的身份识别验证方。THEKEY 的身份识别服务往往由多个身份识别验证方共同完成。在 THEKEY 生态圈中，身份识别的发起方，例如酒店、机场、银行等被称为“服务提供商”，而身份识别的对象则被称为“用户”。当身份识别验证方从服务提供商收到一个对用户的身份识别请求，以及该用户同意其服务提供商所发起的身份识别请求的智能合约时，身份识别验证方将依照合约规定将用户的相关身份识别信息上链，是为“身份认证”。“身份认证”一方面保证了用户的数据安全，同时也满足了服务提供商对身份识别的需求。

### 智能合约

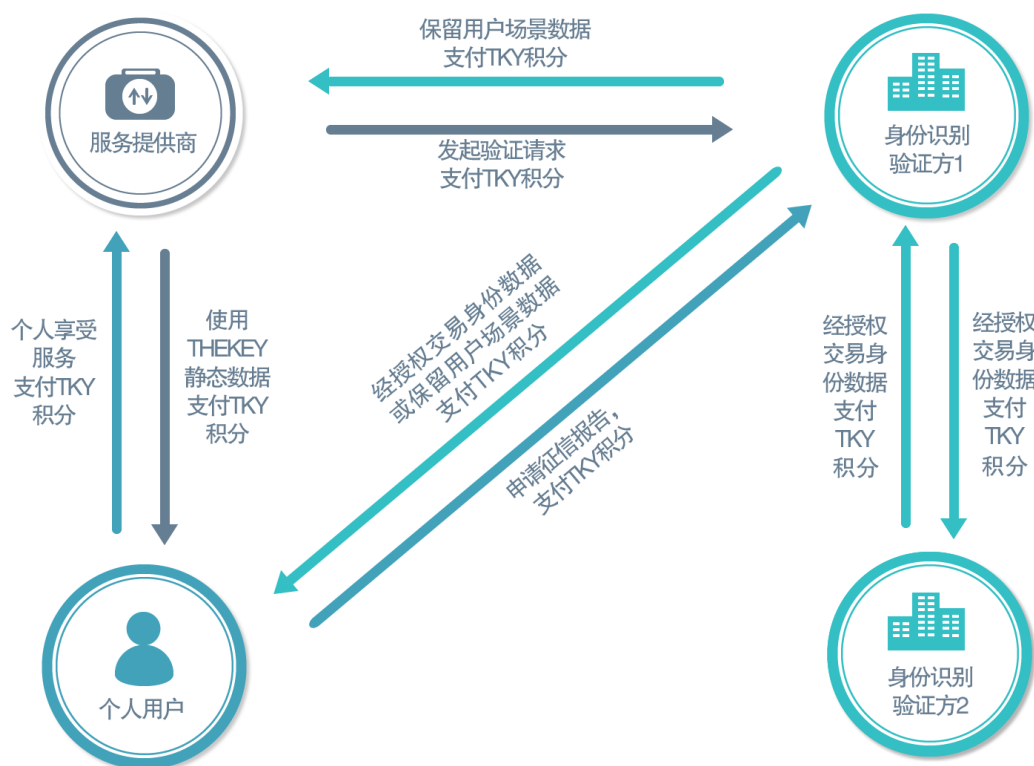
智能合约在 THEKEY 的生态圈中起到了关键作用。在提供身份认证之前，所有相关方，包括用户、服务提供商以及身份识别验证方，都将签署智能合约以明确

各方的责任和权利。智能合约将内嵌政府相关法律和法规，以及不同领域中服务所需的用户信息，即 KYC ( Know Your Customer )。采用内嵌式做法的好处不但营造了一个良好的数据治理环境、确保用户隐私和数据安全，同时也自动帮助用户时时处处确认所披露信息的范围边界。

此外，智能合约还可以让身份识别验证方在用户授权的前提条件下，向服务提供商收取身份认证的 TKY。服务提供商将根据各自的政策和法律法规的要求选择来自不同数据源的用户识别信息。身份识别验证方可以随时调整和公布其身份认证的价格。

### TKY 积分

TKY 积分是 THEKEY 生态圈中另外一个重要组成部分，是结算智能合约的唯一方式。除了购买 TKY 积分外，各参与方还可通过在生态圈上进行有价值的行为赚取 TKY 积分。例如 TKY 积分可以根据所需信息来源及价值，在各种身份识别验证方和个人用户之间进行分配。另外，目前使用 THEKEY 第一代身份识别产品的用户可以在使用产品时获得 TKY 积分。TKY 在 THEKEY 生态圈内会被高频次地使用，所有 THEKEY 生态圈的参与者都有机会获取和使用 TKY 积分。例如，首先用户会使用 TKY 积分向身份识别验证方兑换身份识别相关服务，例如个人背景调查、个人征信查询等。其次，服务提供商在发起身份请求之后需要按照智能合约向身份识别验证方支付 TKY 积分。第三，如前所述，有鉴于身份识别是区块链技术的底层应用，我们预计将会有许多 DAPP 应用的开发者加入 THEKEY 社区并向 THEKEY 采购身份识别服务。最后，THEKEY 项目组本身也需要 TKY 积分用于兑换其他身份识别验证方，如电信、银行等的服务。TKY 积分兑换不受空间的限制，更是结算 KEY 生态圈智能合约的唯一途径。



TKY 积分的发行总量固定不变。TKY 积分会在账本上记录，具有其他数字加密货币的特点，TKY 积分也是可以流通的。账本记录机制为 TKY 积分持有者与 THEKEY 生态圈参与者之间提供了交易基础。随着越来越多的参与者活跃在 THEKEY 生态系统中使用身份识别以及相关服务，TKY 积分的核心价值体现在促进身份识别技术的发展和推动 THEKEY 生态圈的扩张。

## THEKEY 生态圈的运营

THEKEY 生态圈里进行的身份识别过程具有以下几个特点：

- 个人用户永远控制自己的个人信息。任何身份识别程序的启动必须经过个人用户的授权，例如通过服务提供商的软件进行指纹或者人脸识别。
- 除了个人用户授权外，身份识别验证方还将按照服务提供商所在行业的 KYC 标准审核身份识别请求中的个人信息字段是否合理。例如，一个酒店发送过来对客人进行身份识别的请求中包含客人的健康档案，这个请求就会被视为超出行业所需要的身份识别范围，不予进行。相反，如果一个医疗保险公司提出同样的请求，这个请求就会被接受。

- 个人用户无须上传他们的个人信息。身份识别验证方会在上述两点前提条件满足后自行收集个人信息。
- THEKEY 利用 BDMI 技术对个人实时的身份数据、行为数据和场景数据进行多维交叉验证。身份识别数据来自于政府不同的机构，行为数据来自于银行、运营商、保险公司等机构，而场景数据一般来自于寻求身份认证的服务提供商。比如一个人早上 9 点在香港酒店进行了身份识别验证，过了 1 小时美国一家酒店对同一个人进行身份识别验证的结果可能会被拒绝。因为场景信息有冲突。将这些数据集中在一个中心极其困难，而在一个中心化的社区中提供如此庞大、复杂、精准的身份认证也同样不具备可操作性。区块链技术的出现使得身份识别技术的进步成为可能。在 THEKEY 生态圈中每一个数据源都会作为身份识别验证方，从而成为一个去中心化自治社区中的一个节点。通过分布式公共账本人人都明白“谁拥有什么数据”。

在 THEKEY 生态系统内，以一个北京常住居民在新加坡购买当地医疗保险为例，医疗保险公司触发身份识别请求，同时需要获取用户健康档案为例，THEKEY 用户身份识别包括以下 8 个步骤：

- 新加坡保险公司作为服务提供商发起身份识别请求。
- 用户通过手机 THEKEY 的 APP 或者通过保险公司端设备提交自己的指纹或者其他生物学特征如人脸、虹膜等，并与 THEKEY 以及保险公司签署相关的智能合约。
- THEKEY 作为身份识别验证方将保险公司请求与行业要求进行比对从而检查保险公司请求的合理性。
- THEKEY 将用户上传的生物学识别信息与政府数据库中该用户经政府认证过的生物学识别信息进行一致性检查确认用户身份。与此同时，THEKEY 还将其生物学识别数据与来自其他数据源的同一用户行为数据和场景数据进行交叉校验以确保结论的可靠性，这一切都是通过加密安全的接口自动完成的。
- 用户身份得到确认之后，THEKEY 将依照智能合约的要求采集用户健康档案并发布上链。
- 身份认证服务完成之后，智能合约将依照合约的规定分配 TKY 积分。

- 与此同时 THEKEY 将所有计算结果存证以供日后数据审计。
- THEKEY 将定期进行数据审计并对用户信用做出评价。

这个身份认证程序大大降低了保险公司对用户进行核保的成本,保险费率将会降低,同时保证了认证的真实性和准确性。

## THEKEY 的未来

随着社会经济活动逐渐从线下向线上的转移,互联网身份识别将快速增长。以 BDMI 技术为核心,采用分布式多方认证以及 TKY 积分为驱动的 THEKEY 生态圈必将成为一个出色的身份识别平台。这个平台将成为链上链下、线上线下众多生态圈的底层技术。用户将不必携带信用卡、身份证、护照、驾驶执照、钥匙甚至手机来证明“我是我”。只要用自己的指纹、指静脉、虹膜或者人脸直接接入 THEKEY 生态圈即可完成动态多维身份识别,满足不同的身份认证需求。由于用户数量的巨大和需求的快速增长,我们确信 THEKEY 生态圈将有极其光明的前途和无限的可能。

## 便捷的日常生活

开门可以通过摄像头的人脸识别和门把手上的指纹/指静脉扫描,确定个人身份,跟链上的上次行为比对,确定时间、地点的合理性。开车时除了做身份识别,还要实时验证其驾驶执照的有效性,验证和学习个人驾驶习惯,当发现激烈驾驶行为时给予驾驶人提醒和给予车辆所有者预警。宾馆入住时,通过前台摄像头的人脸识别来确认个人身份,根据其以往住宿记录和信用情况办理入住,并给予免住宿押金/赠送早餐/更换枕头等服务。海关出入境是比较复杂的场景,需要通过人脸识别和指纹识别确定个人身份,后台验证近期出入境记录、公安黑名单、签证记录、机票和酒店信息,最终实现快速通关。

## 疾病的自动诊疗

当你感觉有些发烧,你身上的智能设备将检测到你身体的详细数据。你还可以告

诉它哪里不舒服，MTS<sup>1</sup>技术会诊断出你的疾病，并结合你的病史通过智能设备推送给你最合适的药品和诊疗方案，或是推荐给你最近最好的医生。区块链物联网技术会帮助你最快拿到最便宜的药，并且药品是可溯源的。突然休克怎么办？智能设备会发出求救，最近的医院会派出救护车，在救护车上医生便可以通过BDMI确定你的身份、调取历史诊疗数据，并制定抢救方案。到达医院进行检查，仪器输出的数据会通过MTS技术综合分析得出精确的诊断结果，并列出生世界上关于该病首选的解决方案，你的病会得到更快、更精准的救治。当你出院结算时新的电子身份证再次更新。

## 精准推送

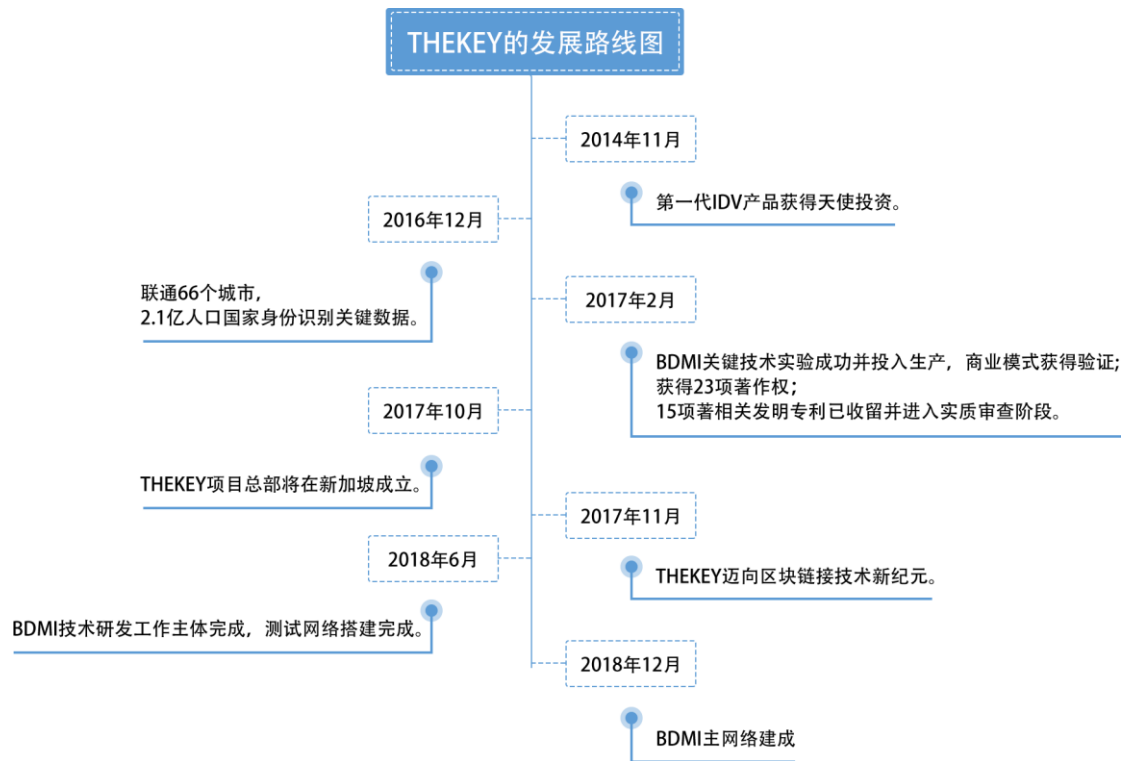
智能设备会检测到你是否缺水、是否需要休息，甚至在附近是否想吃什么，因为它知道你的一切偏好。或许你想买份保险，你可以选择加入互助保险组织，也可以选择一家大型保险公司。你开放一定身份查阅权限给保险公司，他们会根据你的情况制定合适的保险，投保、核保、理赔全部基于你的电子身份由智能合约完成。

我们可以看到乘车、打卡、安检、开车、开门、就医、购物等等全场景生活无一不需要动态多维身份识别，THEKEY的存在将使互联网和现实身份融为一体，方便每个人生活的方方面面。

---

<sup>1</sup> MTS 技术：Medical Term Standardization，即医学术语标准化。

## THEKEY 的发展路线图





## 项目执行团队与合作伙伴

THEKEY 项目强大的执行团队和合作伙伴是项目取得成功的可靠保障。

### 项目团队



**李雪莉 (Catherine) (董事长兼首席执行官) Bch. Med., M. Sc.,**

首次提出区块链应用到动态多维身份识别领域,对区块链的行业应用有深刻理解。加拿大国际研究委员会 5 年工作经验,期间主管欧美著名大学的大型合作项目。艾美仕(IMS Health)10 年的管理与销售经历。大数据与计算机科学跨界人才,丰富的大数据领域、医学信息学和跨国公司从业和管理经验。加拿大 McGill 大学计算机科学硕士,加拿大国家级与魁北克省级奖学金同时获得者。

李雪莉负责项目战略制定和战略执行,其主要相关成就如下:

- 动态多维身份识别技术的发明人。世界上首次在互联网上提供动态多维身份识别服务并得到政府、银行、保险公司、第三方支付公司、医院、药店的广泛认可和赞誉。
- 团队负责人,成功地制定并实施了动态多维身份识别项目的数据采集方案、实时联通了 66 个城市、2.1 亿人口政府相关部门、银行、电信等部门的身分识别数据,为动态多维身份识别技术的成功奠定了基础。
- 团队负责人,和政府、银行、保险公司、以及大专院校一道发起并主持了相关领域的 6 个国家级实验室。
- 团队负责人,中国社会保险数据应用大赛冠军和最佳创意奖,2017 年,中国人力资源与社会保障部。
- 中国最杰出女企业家,2017 年,中华全国妇女联合会。





### 黄连金（总裁，身份识别与区块链技术，2017 年 12 月 21 日起）

- 著名 ICT 公司首席区块链专家和首席身份管理系统架构师。
- 中国电子学会区块链专家委员 CISSP (ISC 注册信息系统安全专家)。
- 曾经就职与美国 CGI 公司 18 余年，曾任 CGI 区块链实验室负责人，CGI 安全技术总监，CGI 云安全主管和首席安全架构师等职务。创建了 CGI 联邦身份管理和网络安全能力中心。在 CGI 工作时，曾经为美国联邦政府、金融机构和公用事业公司提供金融，区块链，安全等方面的专家咨询。



### 王剑（CBO）B.Sc

15 年研发管理经验。担任江苏地税大数据、央行冠字号溯源、南京市区块链电子证照、南京互联网+政务+金融等项目的总架构师。历任江苏润和政企事业部部长，江苏荣泽 CTO。Hyperledger 第一代开发者，参与过数十个区块链行业应用的架构设计和代码评审。南京区块链电子证照项目是国务院“互联网+政务服务”的全国示范项目。毕业于南京航空航天大学。

王剑是区块链技术团队负责人，针对身份识别业务进行底层选型与构建，带领团队与 DMI 研发团队搭建了 BDMI 的原型验证系统。其主要相关成就为：

- 团队负责人，打造中国第一个区块链政务项目，是国内最早开始区块链行业应用研究的团队之一。
- 团队负责人，带领团队取得 1 件软件发明专利，4 个软件产品，21 件软件著作权。



### 徐国春 (CTO) B. Sc.

拥有 17 年计算机软件行业工作经验，曾就职于中国联通信息化部，任职技术专家 10 年，8 年以上技术管理工作经历，擅长大数据处理、自然语言处理等技术，在大数据应用区块链技术方面有所建树。黑龙江工程学院计算机科学与技术专业。

徐国春是产品设计、开发、实施和运维的负责人。他的主要相关成就是：

- 团队负责人，成功的完成了动态多维身份识别产品的设计、开发、测试、66 个城市的部署和运行维护。
- 团队负责人，带领团队成功的获取了 8 项著作权并申请了 7 项发明专利（含区块链技术）。
- 团队负责人，带领团队成功的通过了 ISO27001 和 CMMIII 的认证。



### 张贺宁 (CPO) B.Sc., M.Sc.

曾任苏州涑哲区块链产品总监，摩森特（大数据）总经理，瀚海产品总监（BPM），天极产品总监（DSP）。设计过 RBC 联盟链底层技术产品，以及南京区块链普惠金融平台、上海区块链能源微网平台等行业应用。合作、服务过 IBM、微软、思科、农总行、中国银行总行等多家 500 强企业的业务和市场咨询。张贺宁是产品团队负责人，负责动态多维身份识别产品的原型框架设计并对多领域身份识别场景 KYC 建模。他的主要相关成就是：

- 团队负责人，针对满足大规模用户数量的应用场景，设计可提供高并发交易的区块链产品，同时很好地保护用户隐私与数据安全。

**黄玉丽 (CDO) Bch. Med., M. Sc.,**

曾在好医生和中国知网等企业担任数据专家，在大数据实体及其关系识别、术语标准化、电子病历结构化、诊断智能辅助等领域具有丰富经验。中南大学湘雅医学院硕士。

黄玉丽负责数据交换平台的设计、开发和运行维护，其主要成就为：

- 团队负责人，负责设计、开发、测试、部署了数据交换平台为多维动态身份识别奠定了成功的基础。
- 团队负责人，获取了 15 项著作权并申请了 8 项相关发明专利。

**陈騄 (CMO) B. Sc., M. Sc. Ph. D.**

曾在中国药学会、海虹、华渊多家公司任职，从事医药数据、服务及软件的市场营销工作，在原始数据的产品化、市场定位和新业务拓展方面有丰富经验。中国海洋大学海洋药物与食品研究所博士。

陈騄博士负责政府和企业合作事务，其主要相关成就为：

- 团队负责人，成功地向 20 余个世界著名企业推销并签署了身份识别相关的商业合同。
- 团队负责人，具体执行了动态多维身份识别项目的数据采集方案、实时联通了 66 个城市、2.1 亿人口政府相关部门、银行、电信等部门的相关身份识别数据，为动态多维身份识别技术的成功奠定了基础。

**左霖 (COO)**

丰富的超大型信息系统集成项目运作与管理经验，区块链行业应用推动者，垂直搜索技术领域架构设计专家，曾负责清华大学国家级人工智能实验室多模态搜索引擎及其他前沿技术的运营推广。曾主导安邦保险 IT 部核心技术系统建设，在紫光软件系统有限公司任项目总监。北京航空航天大学软件工程与管理专业硕士。

左霖负责产品推广，他的主要相关成就为：

- 团队负责人，负责动态多维身份识别服务的全国推广，获取用户 230 万人。
- 团队负责人，负责动态多维身份识别技术商业合同的执行。

**丁艺明 (R&D Manager) B. Sc., M. Sc**

15 年研发与架构经验。历任摩托罗拉、趋势科技、万达金融等五百强企业的研发中心架构师。专长在大数据挖掘，并且在 IDC 设计、数据库设计、非关系型数据库存储方案、主流 Web 开发框架、多开发语言应用服务等领域都有深入的研究和实施经验。东南大学研究生，曾出版技术教程。

丁艺明是区块链技术团队研发经理，与团队共同搭建了 BDMI 的原型验证系统，完成多个身份识别应用场景下的智能合约 DEMO 研发。其主要相关成就为：

- 项目负责人，主持开发的南京区块链普惠金融平台，已经打通了南京市信息中心、南京市房产交易中心等部门和中、农、工、建、交等 9 家银行的按揭贷款业务。

**丁大伟 ( Implementation Manager ) B. Sc.**

10 年开发和实施经验。历任江苏润和政企事业部项目经理，江苏荣泽区块链事业部实施组长。在南京政务区块链项目中，完成了对 1600 项市级办件事项的标准制定和接口设计。毕业于山东工商大学。

丁大伟负责项目实施部署，他的主要相关成就为：

- 团队负责人，负责江苏电信号码百事通、江苏电信 E 卡通、必胜客宅急送、贵州茅台电商、皇家加勒比中国官网、常州人民银行冠字号、南京区块链政务等项目中的 WebService、SNS、前端、搜索、支付等关键技术环节的実施和成本及质控管理。

**顾问团队****Roger Lim ( 区块链和数字货币投资顾问 )**

Roger 是区块链和数字货币领域的著名投资人并参与了多个相关项目。他将在 THEKEY 项目的代币发行过程作为投资顾问提供行业经验和建議。

- Webvisions 联合创始人和前 CEO，Webvisions 是亚洲最大的管理托管服务供应商之一；
- Innosight Ventures 合伙人，Innosight Ventures 是新加坡著名风险公司

机构。



**陈青越**

臻之科技创始合伙人，特许金融分析师，风险投资人，区块链金融体系设计资深专家。

## 投资人和战略合作伙伴



**何长龙**

启沃资本 CEO



## 团队的区块链项目经验

团队成员均在传统软件行业取得过卓越成绩，分别在政务、金融、医疗、互联网等领域领导过行业知名项目，并较早向区块链转型，是国内第一代专业的区块链开发者团队。

从 2015 年开始与 Hyperledger 合作开展联盟链的行业解决方案设计和各种 POC。已经取得以下成果：

- 基于 Fabric 超级账本，优化了近半代码，封装了自主底层技术产品。解决了隐私、安全、控制、管理以及交易效率等关键问题。并采用智能组网技术、椭圆曲线加密算法、拜占庭共识算法打造，具备快速构建上层应用业务的能力，满足大规模用户数量的应用场景，可提供每秒 3000 次交易的高性能服务，并很好地保护用户隐私与数据安全。该产品体系取得多项技术突破和创新，1 个软件发明专利，4 个软件产品，21 件软件著作权。
- 拥有全国第一个区块链电子证照的先发技术和标准优势，去中心化组网、分布式账簿和公私钥机制打通将政务部门之间数据打通，解决安全与隐私的矛盾。并创新的将电子证照的目录体系重新建立标准和接口，把证照数据的粒度和使用形式重新定义，解决证照数据的灵活使用。该区块链电子证照平台已经在南京落地实施，打通了数十个市级部门，1600 个办件事项的公民与法人数据，已经有数十个事项开始运行。南京市民和企业在南京“互联网+政务”服务的主入口“我的南京”已经可以一键办理购房资格证明等政务事项。
- 将自主封装的联盟链底层技术产品在各行业进行应用测试。区块链+信用生态，解决了信用机构联盟的数据安全共享；区块链+共享经济解决了物权/使用权的分离和可信确权；区块链+版权防伪解决了版权的可溯可信和高效交易；区块链+智慧医疗发挥了电子病历和基因大数据的价值。



## 项目合作伙伴



## 管理委员会的设置

THEKEY 项目组还将组织成立管理委员会（以下简称“管委会”）作为本项目的组织管理机构。管委会是一个去中心化的组织，致力于全球范围内身份验证体系的标准化，并推动该体系的普及。具体来说，它将负责对项目涉及的各种资源进行合理的利用与管理，包括运营管理、市场推广、底层技术与服务体系的搭建等，制定计划，支持与推动项目所需技术的发展，从顶层设计上促进整个良好生态的形成。

管委会由投资者代表、创始团队、合作伙伴代表等组成，肩负着决策、监督等方面的职能。另外，管委会的架构可以通过成员投票被改变，从而使其按照人们希望的方式去运作。



## 结论

THEKEY 项目组成立于 2015 年。自项目组成立以来一直致力于向公众提供先进同时又有良好用户体验的身份识别服务。我们基于动态多维身份识别技术的第一代互联网身份识别产品的巨大胜利,充分展示了团队完全具备获取第二代产品设计、开发、测试和工业化规模部署成功的能力。THEKEY 项目组期望通过现有 DMI 与区块链技术相互结合能够产生一个去中心化的新型身份识别产品,改善民众生活、推动社会经济的发展。

此外,THEKEY 项目的身份识别技术不仅仅能够为人工智能提供底层服务,而且是所有网络法律关系(包括著作权和数据交换)的必不可少的先决条件。因此,必将成为区块链技术走向成熟的不可或缺的底层技术。

如需了解更多信息,请联系 [info@thekey.vip](mailto:info@thekey.vip), 或者访问 [www.thekey.vip](http://www.thekey.vip)