

October 9th, 2017



SECURE IDENTITY LEDGER

WHITE PAPER

6329 Arlington Blv Suite N
Falls Church, Virginia 22044

SECURE LEDGE IDENTITY CORPORATION (SILC) IS A NEW COMPANY. SILC IS NOT REGISTERED WITH THE UNITED STATES SECURITIES AND EXCHANGE COMMISSION, OR ANY OTHER REGULATORY AGENCY. SILC IS NOT SUBJECT TO ANY PUBLIC REPORTING OR FILING, AND HAS NO OPERATING HISTORY FOR MY SECURE LEDGER USERS TO REVIEW. SILC IS NOT OFFERING ANY SECURITIES, INVESTMENT CONTRACTS, OR INTERESTS IN THE COMPANY. SILC PLATFORM USERS AND THOSE PARTICIPATING IN THE SILC TOKEN SALE ARE ADVISED TO CAREFULLY REVIEW THIS WHITEPAPER (INCLUDING RISK FACTORS), COMPANY WEBSITE, AND ANY TOKEN PURCHASE AGREEMENT BEFORE PURCHASING SILC TOKENS.

SILC TOKENS ARE NOT OFFERED FOR SALE, AND MAY NOT BE PURCHASED IN NEW YORK, SINGAPORE, SOUTH KOREA, CHINA, OR ANY OTHER JURISDICTION WHERE THE SALE OF SILC TOKENS OR OTHER CRYPTOCURRENCY IS PROHIBITED OR SUBJECT TO PRIOR REGISTRATION OR REGULATION.

SILC TOKENS ARE NOT CURRENTLY LISTED ON ANY CRYPTOCURRENCY EXCHANGE AND NO SECONDARY MARKET FOR THE SILC TOKENS EXISTS AT THIS TIME.

目录

执行摘要	1
我们并非在进行常规令牌销售	2
从互联网时代到区块链时代 SM	4
介绍	4
保护个人身份面临的挑战！	6
SILC 的唯一数字身份 SM （SILC ONE Digital ID SM ）解决方案！	7
“唯一数字身份 SM ”能提供哪些具体的解决方案？	8
SILC SM 的区块链平台	9
我们为何独一无二？	10
为何值得您关注？	11
令牌销售	11
使用从令牌销售获取的收益	Error! Bookmark not defined.
定义及核心概念	12
公司	12
我能看看区块链吗？	13
为何我们要求将您的数据用于验证？	13
唯一身份和钥匙	14
使用唯一身份的优势	14
SILC 积分	14
使用案例	15
案例 1	15
案例 2	15
案例 3	15
案例 4	16

执行摘要

安全身份账本公司（Secure Identity Ledger Corporation，缩写：SILCSM）所推出的分布式账本技术是一种强大的创新科技，在您和用户购买/拥有唯一数字身份的过程中，能够提供颠覆性的消费应用体验，从而使您们顺利过渡到区块链时代SM（Blockchain AgeSM）！这个唯一数字身份SM（One Digital IDSM）是您独一无二拥有的，不被其他任何人掌握。您凭其能够控制个人信息的使用分发方式，其结果是，您可以在全球的数字化社区建立起信用。一如现在，所有的交易都记录在我们的区块链中。

我们的 SILCSM 平台是 SILC 公司两位创始人多年努力的结晶，其中还得到了诸多医学和财务领域专家的帮助，他们对个人数据的价值性和薄弱点有着深刻的理解。我们并非是在建议您，要放弃自己的用户 ID、密码、pin 码和其他您正在使用的安全措施；我们所提供的唯一数字身份能够保障您敏感信息的安全性。事实上，今日的我们已经被数字的汪洋大海所包围，我们置身其内，却无法得到任何足够的保障。我们对密码、pin 码的控制已经失效，从而导致我们自己的身份也遭到了泄露¹。与其他苦苦钻研数字身份领域的公司不同，SILCSM 已经创建了一个独立研发、且行之有效的解决方案，而这正是基于区块链技术！

我们的解决方案对数字身份给予了重新的思考。若要真正实现掌控，首先我们必须拥有我们的身份，只有这样，我们才能决定要分享哪些信息类型，或使用哪种技术。我们的应用在创建数字身份的过程中，融入了区块链，以作为实现所有未来应用和服务的底层技术。威廉·莫加耶

（William Mougayer）以一言蔽之，“基于区块链的身份前景广阔，它能让我们无所顾虑地尽情消费，而无需证明我们身份的真实性……”

我们的解决方案简单易用，您无需一遍遍地使用密码，也不必报出社会安全号，您所有的数据都存储在没人（包括我们）能够看的地方。用户可以上传任何信息到区块链中，它会保证信息安全加密、不可更改，且无法否认。在数字世界里，SILCSM 的区块链是您个人的“证人”。

无论是用于注册、认证、验证，还是个人监控，SILCSM 是唯一能为企业、政府和消费者提供全盘数字身份系统的公司。这一平台将为个人提供唯一的数字令牌，使他们能够向第三方证明自己的身份。与其他基于权益证明（Proof-of-Stake）或工作证明（Proof-of-Work）的区块链解决方案不同，SILCSM 是用存在证明（Proof-of-Existence）实施运作，交易双方借此可以通过 SILC 控制板交换和确认信息，无需将信息进行记录。SILC 的唯一数字身份SM 经过了安全加密，它不可更改且合规合法。

我们构设了美好的愿景：为这个星球上的每个人、每台机器和每家企业都创造一个唯一数字身份SM。我们意欲提供一种令沟通和交易变得更为安全的方式。对于那些曾经饱受身份欺诈的受害者，SILC 的平台和解决方案为其提供一个崭新的开始，从而帮助他们放心驰骋于数字市场。

首次代币发行（ICO）是基于概念性的想法和承诺，我们的做法与之大相径庭。SILCSM 已经开发出了首批产品。此外，多数 ICO 的解决方案是建立在公共区块链的平台上，这限制了他们产品的功能。而 SILCSM 开发了自己的专有复合区块链平台，使我们能够提升区块链能力。我们保证，SILCSM 区块链始终可以使用，能为您提供支持，且即将到来的区块链膨胀不会影响到您的帐户。

¹<https://advizex.com/2016/06/02/3-devices-per-person-not-anymore/>

我们还删除了矿工需求，从而防止了区块链分叉。我们的数字身份产品解决方案行之有效。我们还开发了一个名为“验证存在证明（Proof of Verified Existence）”的自定义共识算法，以对我们专有区块链平台上的交易进行校验。虽然在互联网时代，您可能没有自己的电子邮件，但在区块链时代SM，您在事实上已经拥有了自己的唯一数字身份SM。

SILCSM是一家美国公司，我们在首次令牌发行（Initial Token Sale）中发售的 SILCSM令牌单价为 0.25 美元，最低购买金额 25 美元。我们接受所有形式的付款：维萨卡、万事达卡、运通卡、发现卡和比特币。

我们并非在进行常规令牌销售

我们拥有区块链技术带来的全部潜在利益，且没有加密货币其他方面的缺陷，因此我们与众不同。

以下四个重要因素令我们的令牌销售与之前的有所不同：

- 在完成私有区块链的基础上，我们是唯一的令牌销售公司
- 在完成并提供了有效数字身份解决方案的基础上，我们是唯一的令牌销售公司
- 我们拥有能接受信用卡和比特币的平台
- 能直接将令牌购买记录至我们私有区块链的平台只有一个，它被我们所拥有。

“我真的很喜欢这个想法，因为它把所有权、验证和认证过程从第三方（不管是否可信）转移到我这里。我拥有自己的身份，可以根据需求决定是否允许对我的身份进行访问。”

克里斯·斯金纳 (*Chris Skinner*) (*thefinanser.com* 公司)，2017年9月11日 - “拥有身份证件的自主权势在必行 (*Equifax* 公司数据泄露事件)”

“数据是一种资产！您现在并不拥有的那个虚拟的您，可能比您自身更了解您……隐私是自由社会的基础！”

唐·塔普斯科特 (*Don Tapscott*) (哈佛大学伯克曼克莱恩互联网及社会研究中心副主任)，2016六月 TED 峰会 - “重获我们的身份”

“设计一个坚固的数字身份系统可能是数字时代最大的难题；没有它，您基本上就会被困在文明体系的罗网中！”

康纳·奥希金斯 (*Connor O' Higgins*)，*CryptoInsider* 公司

从互联网时代到区块链时代SM

互联网 1.0 - 1968 年到 1995 年，前互联网时代：这一阶段主要是共享资源以交换信息。多数的交流都是通过简单的文本进行。例子是友思网、新闻组、电子公告板，和简单的电子邮件。

互联网 2.0 - 1995 年到 2008 年：这一阶段见证了电子邮件、网站、电子商务和社交媒体的兴起。交流已经从简单的文本跳跃到超文本，及下载图片/视频。

互联网 3.0 - 2008 迄今：无线接入、移动应用、云计算和无所不在的移动互联网接入，主导了这一阶段的发展。

区块链时代SM：在互联网发展的这一阶段，我们开始看到互联网 2.0 和 3.0 发生了融合，内容和信息已经变得比访问方式更为重要。在此阶段，传感器将提供数据，并通过特定接触点从用户那里收到如何收集或共享数据的反馈。

介绍

您的社会安全号（SSN）在设计之初并非用于身份识别，这与很多人的看法大相径庭。同样，互联网最初的设计目的不是给人们提供一个“身份”。安全身份账本公司（SILCSM）认为，与他人在网络上的互动时，每个人都必须拥有一个数字身份。它将在人与人之间建立信任，这是互联网生态系统²的社会基础，尽管技术很重要，建立信任的方式还是要从自我开始。

区块链能否成为通用数字身份系统的骨干？SILCSM 认为它在未来将起到身份管家的作用。我们的唯一数字身份SM 系统允许您在登录任何网站时，使用数字令牌来验证和保障您的身份。SILCSM 的产品将允许您使用一次性验证证书（以加密形式）创建个人数字身份，而身份将用于任何其他场合，以代替当下使用的登录认证过程。您的数字身份还将保留您对身份拥有的权限，无需将其移交给第三方。

目前，基于密码的在线认证方法不够完善，因为消费者必须要记住各种网站的用户名和密码。SILCSM 的数字身份系统将彻底改变您交流信息的方式。您可以（加密形式）一次性上传个人数据，然后您的身份就可以在任何其他场合使用。

数字身份是指个人或实体在网络或互联网中的真实身份（如商业或政府机构），用于在个人电脑、手机或其他个人设备的连接或交易中进行身份识别。若要相信真实身份和数字身份之间的联系，首先需要可靠地验证这个身份，换句话说，要证明您是您所说的那个人。一旦建立了这个联系，

²《信任：互联网生态系统的社会基础》，作者：Jardine 和 Hampson，2016 年 12 月 5 日。

就可以使用涉及某种类型认证的数字身份，就是当您使用像因特网这样的数字连接时，能够证明您确实是您的那种方法。

SILCSM 力图将自身定位为行业领先的数字身份企业，将我们的唯一数字身份SM 产品普及给每个消费者、每家企业和每台机器。我们借助的这个平台即可以升级扩展，又能允许用户相互操作，同时还兼顾私密和安全，从而帮助消费者和企业进入区块链时代SM，增强自身实力。

我们见证了 SILCSM 区块链平台的崛起，它已经成为了公共区块链的首要替代技术，将帮助企业和消费者从互联网的上下文信息发展阶段迈入到崭新的科技时代³。

人们常常错误地将比特币和区块链混为一谈，但是两者区别很大，不能互换。比特币是一种加密货币。而区块链是一个具有特殊属性的新型数据库，能够将交互和交易永久性地记录下来。发明它的目的是交易比特币，但与之相伴的也会产生各种其他事物。

您拥有的唯一数字身份SM 不会改变，是因为区块链的不可逆性和永恒性构成了区块链时代SM 坚实基础。在 SILCSM，我们正在构建的缺失的互联网身份层将会极大地促成很多发生于今天的交易。

从事商业活动和社会交往的人以他们的身份而被人所知。在前互联网时代，身份是由您的名字、地址、出生日期和社会安全号定义的。但在数字时代，身份是生成您唯一数字身份SM 的一组数据点集合。

正如家用电器和自来水一样，您的唯一数字身份SM 会成为将您周围的一切连接起来的必需品。在区块链时代SM，数据是通过您与多个接触点的交互收集得来的（如恒温器、电灯、汽车、音箱、聊天机器人、机器等等……），然后与您的上下文信息融合。

在 1989 年，当 CompuServe/MCI 邮件首次给我们展示了第一个用户电子邮件地址时，电子邮件主要在 CompuServe 内网用于同朋友和家人进行交流。许多人都对电子邮件能否成为一种可行的数字通信工具持怀疑态度，有些人甚至怀疑互联网本身能否会对我们的个人生活、社会活动和商业行为产生影响。然而不过寥寥数年，网络和电子邮件已经从科研人员使用的边缘技术，华丽转身为普罗大众的主要通信工具。根据研究机构瑞迪卡迪集团的数据，全世界有 37 亿个电子邮件用户，占地球人口的 54%，每个用户平均拥有 1.7 个电子邮件账户。⁴

如今 30 年时间弹指而过，区块链和身份管理成为了新兴的边缘技术。它们构成了共享经济的基础。共享经济是一种“获取、给予或共享商品和服务的对等活动”⁵。共享经济是立足于如区块链的最新技术进步，它兴起的基础在于：（1）大幅降低交易成本；（2）促进安全和分散的方式交

⁴上下文信息：我们所知道的有助于理解文本的有关信息，包括：

- (1) 文本中命名的事物身份：人、地点、书籍等
- (2) 关于文本中命名的事物信息：出生日期、地理位置、出版日期等
- (3) 解释信息：主题、关键词
- (4) 度量标准化：日期等

⁵《共享经济的当下和未来状态》，作者：Niam Yaraghi 和 Shamika Ravi，2017 年 3 月

换价值，无需通过中介。人们总是存在着这样那样的需求，诸如购买小众产品、找到栖居之所、获得现金、吃家常菜、寻找任务助手，或是从 A 点到 B 点等等。而问题就是难以找到一个愿意以合理价格提供所需商品或服务的人。有了区块链，软件应用不再需要部署在一个中心服务器上，它们可以在对等网络中运行，不受任何一方的控制。

作为共享经济的典范，优步™ (Uber™) 仍然中心化十足，他们仍然控制着您所有的数据。今天，当您使用优步™时，仍然需要由人工处理中央计算机提供的信息，以找到从 A 点到 B 点的最快路线。在区块链时代™，它拥有同样的处理和记录数据的权力，但已经没有了人为因素或中心计算机。

在互联网的 2.0 和 3.0 时代，您并不拥有自己的用户名、数据，或与他人分享的数据。在您不知情或未批准的情况下，数据被别人收集、分析、包装和销售。您没有任何的控制权，在这种情况下您唯一的选择是，要么注册帐户，要么离开网站。这被称为“霍布森选择效应”或“选择幻觉”——这是托马斯·霍布森 (Thomas Hobson, 1544–1631) 首先提出的概念。霍布森选择是一种虚假的“选择幻觉”，因为它不是在两个等价选项之间做选择，也不是在两个不受欢迎的选项之间做选择；您只能选择接受或拒绝。

在互联网时代，“选择幻觉”无处不在，因为我们唯一的选择就是信任拥有我们数据的网站。正如我们选择登录雅虎、易趣、索尼、塔吉特、Equifax、哈特兰德支付系统、TJX、摩根大通、Anthem，及 OPM (个人管理办公室) 公司一样，事实上，它们都是数据泄露的受害者。

您在登录时相信，您的数据将得到保护，当您发现数据没有得到足够的保护时，您才意识到没的选择。唯一数字身份™现在给您提供这种选择：哪些数据可以共享、何时共享、共享多久等等。

保护个人身份面临的挑战！

传统身份识别系统的规范是，使用用户的个人信息来访问他们的账户。我们作为消费者习惯性地认为，给电话另一头的客服代表设计的 5 层问题能够保护我们的个人信息。它管用吗？未必！尽管存在着诸多流程——事实上，银行还以 PIN 码和验证码的形式增加一层验证，您的信息在黑客攻击面前仍然不堪一击。最近的黑客网络攻击对象有医疗业（整个英国的国家医疗服务系统/NHS 等）、大型百货公司商业链（家得宝、塔吉特等）、政府机构（国税局、美联储、国土安全部等），甚至攻击了一些我们最喜欢的网站（易趣、雅虎、谷歌等）。无论系统设置了多少层验证，您的信息均遭泄露。只要这些老古董的验证程序还在使用，此类数据泄露事件将继续发生。像指纹和视网膜扫描之类的生物识别技术已经发展了很久，但还是能够起到一部分作用。不过，生物识别技术本身并非 100% 准确，也不能完全抵御黑客攻击！

在讨论我们的解决方案之前，先来扪心自问，我们是否真的拥有自己的个人身份吗？我们认为，自己拥有着社会安全号、驾照、电子邮件，甚至电话号码。这些对我们所有人可能都不是新事物，但实际上我们并没有自己的身份。许多情况下，我们甚至无法控制任何与我们身份关联的信息。我们的个人数据和信息据存放在其他第三方的场地，由他们管理和拥有。这让我们错误地相信，

自身的信息非常安全，因为有数不清的安全功能在保护着这些数据。作为我们的身份管理者而言，这些受到我们信任的机构（银行、政府机关等）是非常失败的！

目前，Equifax 的泄密影响了美国几乎一半的人口，近 1.43 亿人。泄露的信息包括姓名、社会安全号、出生日期、地址，有的甚至包括驾照。如果信息继续以可访问的格式存储，那么此类事件将层出不穷。

据统计，2016 年全球有 34 亿网民，约占世界人口的 46.1%⁶。同年，管理用户身份数据的系统遭到侵入的事件共有 1209 宗。在过去八年中，全球一共曝光了超过 71 亿个身份⁷。2016 年，约有 11 亿的身份遭到暴光⁸。同样在 2016 年，身份欺诈率创下历史新高，给美国带来了 1540 万名受害者，造成超过 160 亿美元的损失⁹。在全球范围内，美国是受身份盗窃影响最大的国家，中国位列第二，巴西名列第三（但差距较大）。

SILC 的唯一数字身份SM（SILC ONE Digital IDSM）解决方案！

人人都在寻找一个能积极主动加强数字身份，并对其给予保护数据公司。人人都在寻找 SILCSM 这样的公司¹⁰。

SILCSM运营着一个专有技术的区块链平台，它允许您建立一个完全不受上述挑战的身份。首先，您在 SILC 拥有您的数字身份！我们的解决方案致力于让您对自己的个人身份获得绝对的拥有权和控制。您将能监督个人数据的状态，能够创建个人数据，同时保持匿名，而且有权力选择如何、何时、何地、与谁共享这些信息。在创建了 SILC 的唯一数字身份SM后，您就可以使用唯一的身份验证证书，从而避免将您身份的各种信息散布在网络的各个角落，还能防止他人未经同意就获取您的个人数据并出售。您将是您个人数据的唯一保管者，可以安全地与其他用户进行交互，并在从事数据交易时无所顾虑。

简而言之，我们相信，能否做出进一步保护，要取决于我们能否重获个人数据的所有权、控制权和使用权。一旦您的信息不在第三方手中，它就不能被其他人利用，不会对您产生不利的影响。采用 SILC 的唯一数字身份SM后，您可以根据交换的背景，对想发给第三方的信息做出有效选择。

例如，在申请一份新工作时，一个潜在的申请人可以选择只发布与他申请流程相关的证书（教育程度、工作经历、工作研究项目等）。雇主不需要知道申请人的政治立场或其他不必要的细节，避免因为雇主可能的偏见对雇佣决策产生负面影响。申请人还可以控制发布哪些“虚拟印记”的

⁶ www.internetlivestats.com

⁷ <http://www.livemint.com/Industry/mCSJfFzrxk8USJ0Rxh8l/11-billion-identities-exposed-in-data-breaches-in-2016-say.html>

⁸ 《互联网安全威胁报告》，赛门铁克公司，2017 年 4 月。

⁹(a) <http://www.lii.org/fact-statistic/identity-theft-and-cybercrime>; (b) <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new> ; (c)

《今日美国报》，2017 年 2 月 6 日。贾夫林战略研究机构报告。

¹⁰ 《数字迷雾带给我们的麻烦》，数字公民联盟，2017 年 6 月。

元素。借助 SILC 的唯一数字身份SM，您可以将您身份的各种元素存储在区块中，之后选择发布哪些信息。通过重获您的个人信息，权力将从根本上回到您的手中！

这个“唯一数字身份SM”用于管理您的个人身份，可与其他用户交换数据。数据本身经过加密存储后，哈希到我们的令牌上。在我们的系统中，您的区块不大可能被黑客入侵，因为它（1）由其他用户验证；（2）记录在区块链中。

我们要确保，您作为一个用户可以（1）从物理身份向数字身份转变；（2）学习和了解使用区块链的好处；（3）安全自信地进行在线交易；（4）能控制他人的个人数据和身份。

“唯一数字身份SM”能提供哪些具体的解决方案？

我们相信，您对自身数据和信息实现完全掌控将为未来几乎所有的创新变革奠下基石。SILCSM的专有平台为您的个人数据解决 3 个主要挑战：

1. 防止网络罪犯侵入公司服务器盗取有价值的个人数据。
2. 保护您个人数据不在网上曝光。
3. 在密码之外（电子邮件、社交媒体、在线购物、银行和其他需要登录的服务）实现了一种全新的认证校验制度

借助我们各种即将面世的应用，您的“唯一数字身份SM”将为您实现：

- 跨越 SILCSM 平台参与多种交换（财务/数据或其他）
- 从我们即将面世的移动交易能力中获益：SILCSM可能会部署一个能提供登陆机制的手机登陆应用，以确保为用户在登录系统时带来更多的安全。这种应用将包含指纹生物识别技术、符号图、二维码，及其他可能的登陆机制。
- 使用我们的云存储集成：所有的加密文件存储于自动生成的无限容量云存储账户内。这为用户存储所有他们提交和访问的文件/数据提供了一席之地。为避免未经授权的访问，我们对云存储账户内的每个文件使用双加密技术，因此它只对授权用户共享。
- 获取信息和通知：SILCSM计划发布一项能让用户互相发送加密信息的信息加密系统，它可通过公钥和私钥进行加密/解密。该信息系统能协助用户接收交换请求和交换完成的通知。除在线信息系统之外，用户还能设置电话和电子邮件通知。
- 提供可选择的增强云存储服务：用户可以选择备份所有的个人数据，包括在我们个人云服务上的区块链文件。这种备份能令用户在恢复数据时获得更多的安全性。所有云上的个人数据都使用用户的私钥加密，所以只有用户可以访问。
- 信任建设最大化：SILCSM还有一个让它声名鹊起的重要特性，即用户在交换令牌后可进行互相反馈。如果用户未能将其在交换中所述的项目交付，就会出现一个负反馈选项，将用户未能交付项目的行为在区块链中进行永久性标记。

SILCSM 的区块链平台

通过建立自身的区块链平台，安全身份账本公司（SILCSM）正在清除诸如矿工支配费和区块分叉等路障。我们保证，SILCSM 区块链将始终可用，可为您提供支持，即将到来的区块链膨胀不会影响在 SILCSM 开设的账户。与其他体量型平台不同，SILCSM 运作的是时间型平台，此种方式能够对每日所有的交易进行处理。这会永久性地避免区块链膨胀。信息和数据上传到区块链之后，会利用井号标签进行加密隐藏，所以您的数据将会彻彻底底的变得安全。区块链对存储的数据一无所知！我们所借助的平台可以升级扩展，易于获取，又能允许用户相互操作，同时还兼顾私密和安全，从而助力消费者和企业进入区块链时代SM，增强自身实力。

就区块链的功能性和特性而言，我们的平台与所有的公共链别无二致，唯一的不同是我们不会出现分叉，我们没有矿工，我们很难发生膨胀。用户（具有数字身份验证的用户）本身就是校验者，连同其他两个交互方进行数据交换的验证。在此方面，我们也实现了去中心化。没有任何一方能够控制我们的区块链；在外行人看来，SILCSM 是系统/平台的“观察者”。

在典型的比特币交易中，矿工使用“工作证明”校验用户 A 和用户 B 之间的交易，并将交易上传至区块。作为对比，SILCSM 平台内用户 A 和用户 B 之间的交易并非由矿工校验，因为我们没有任何的矿工。至少有三方在我们的平台中校验数据，用户 A 、用户 B，及系统内的其他用户。一旦所有各方校验了数据，它会立刻被记录到公共区块链，及用户 A 和用户 B 的私有区块中。

没有了矿工，我们也就不再需要比特币中的“工作证明”，或以太坊的“权益证明”等概念。我们使用了新型的“验证存在算法SM”（Verified Existence AlgorithmSM），您区块链上所有的用户都可以互相校验。就我们区块链的分布方面而言，每个人都对公共区块链做出贡献，因此不存在中央机构。您的数字身份号码能让您参与/浏览/分享所有的信息，并最终扩展至我们区块链上其他的应用。我们系统的内部既没有投票表决，也没有中央机构。只有平台用户才能决定是否进行上传或共享。虽然有些用户可能只拥有数字身份，从未进行过交易，但是该用户将与我们系统内所有用户拥有的相同权限和特权——想想那个您从未用过的电子邮件地址吧。

我们创建了自己的区块链，因为我们希望（1）建立规则；（2）利用区块链架构的核心元素优势；（3）建立信任；（4）为新数据驱动的业务模型设立框架。

1. 建立规则：我们的平台有 4 条规则，它们都与形成身份规则的组件相符。
 - 用户控制：我们的身份系统平台只有在用户许可的情况下才会披露信息。
 - 最小泄露：我们的平台包含最小数量的身份信息。
 - 合法的当事人：平台在设计时，就考虑到只有合法的当事人才可以进入。
 - 简单的用户体验：平台简单易用，用户可以监控到所有与其数据相关的活动
2. 区块链核心元素：在保持数据完整性的同时，区块链核心元素具有让数据共享变得更简单的潜力。我们的区块链是不可改变、确凿无疑的，兼具去中心化，还具有强大的隐私和安全保障能力。
3. 建立信任：我们的区块链平台能促进彼此之间不信任的人们进行合作和交易。

4. 新数据驱动的业务模型：我们的平台将帮您控制数据，将部分数据披露给能带来明确利益回报的公司。Facebook 在 2017 年二季度获得了 90 亿美元的广告收入，是因为它收集了 13.2 亿活跃用户的数据。能带来收益的活跃用户占比有多大？

SILCSM希望确保每个用户能够（1）从物理身份向数字身份顺利过渡；（2）学习、了解区块链，并享有从中获得的利益；（3）以异常轻松的方式进行安全和自信的交易；（4）完全控制自身的个人数据；（5）直接从自身的个人数据货币化中获益。

为了引导常规用户进入区块链时代SM，安全身份账本公司（SILC）将为您创建和注册一个颠覆性的唯一数字身份SM。之后，您的新数字身份会被记录在区块链中。

我们为何独一无二？

我们填补了互联网缺失的身份层。数字身份现有的模型是建立在用户姓名、电子邮件、文本和密码的基础上，这些可能会被人控制利用，这是网络和互联网的根本性缺陷。

安全身份账本公司推出了业界首个能够交付全盘数字身份系统的区块链平台。我们的新型区块链平台将协助您控制自身的在线身份。该平台具备的一些独一无二的功能所列如下：



彼得·斯坦纳 (Peter Steiner) , 《纽约人》杂志, 1993 年 7 月 5 日

我们为您创建的数字身份属于您自己。您可以选择对其使用，也可置之不理，但始终属于您自己。如果您选择使用我们的系统，您可以决定在虚拟令牌上加载何种类型的数据，从而与其他用户安全的交易，同时所有的交易都会被记录到区块链中。

为何值得您关注？

- 目前存在着太多需要您记住的用户名和密码。我们的系统消除了这一需求。
- 身份盗窃和欺诈在互联网上肆无忌惮。我们的系统将提供全新的方式避免身份盗窃和欺诈，因为没有密码可偷。
- 当下，互联网上有很有数据弱不禁风，很容易被篡改。我们的系统采用了区块链技术，它不可更改，能确保任何区块链中的信息用不被篡改和调换。我们还在区块链上创建了一个定制的加密和分布式存储机制。
- 互联网中有很多管控数据的机构系统。如果这些系统被侵入，那么数据也就完全暴露了。我们的系统是分布式的，采用零知识方法工作，即使我们的系统被侵入，也能确保侵入者不会得到用户的数据。
- 许多用户使用假身份，并不是他们自己。我们的定制验证流程使得这种身份造假行为十分困难。

令牌销售

如需购买 SILECSM 令牌，您必须参加 SILECSM 的令牌销售活动。在首期 16 天销售活动中，全部的令牌被称为 SILECSM 令牌。SILECSM 首期令牌的销售将于 2017 年 10 月 9 日开始，10 月 25 日结束。在此期间，参与者可以注册他们的令牌，获得唯一数字身份SM。SILECSM 令牌将在令牌销售结束后发行，您将在此时付款。购买 SILECSM 令牌可使用维萨卡、万事达卡、运通卡、发现卡、贝宝和比特币。没有折扣。

SILECSM 将发行合计 15 亿个令牌，其中 7500 万（5%）将在即将开始的令牌销售中出售。公司将保留 14.25 亿个令牌在未来销售。SILECSM 计划发行更多的令牌，以进一步强化其平台，继续打造各种其他应用，这些令牌计划在未来几个月内发行。未来发行的令牌数量和价格将视具体应用的需求而定。其他批次的令牌销售量在首期令牌销量的基础上平均浮动 20%-30%，而我们的首期令牌销售只限制于 5%。SILECSM 制定了具体的计划，以在未来几个月内开发和推出新产品和新应用，公司对未来的令牌销售或令牌制作活动也制定了计划。

现阶段向公众提供 7500 万个令牌，单价为 0.25 美元。最低参购金额 25 美元，即 100 个令牌。SILECSM 还为大宗购买提供令牌奖励。例如，任何人购买了 10 万美元的 40 万个令牌，将得到 10% 的额外令牌。就是说，在令牌销售完成后，SILECSM 将对其发行合计 44 万个令牌。下表列出了奖励办法。同时，为了贯彻我们以消费者为中心的理念（正如脸谱网和美国在线），SILEC 不选择实施机

构预售（或朋友和家人预售）。我们相信，所有令牌销售的参与者都应受到平等对待，每个人都有平等的购买机会。

令牌数量	购买价（美元）	对应的奖励
100 - 199,999	小于 \$50,000	0%
200,000 - 399,900	\$50,000 - \$99,975	5%
400,000 - 599,900	\$100,000 - \$149,975	10%
600,000 - 799,900	\$150,000 - \$199,975	15%
800,000 及以上	\$200,000 以上	20%

定义及核心概念

数字身份：数字身份是一种在线化身，由个人、组织或电子设备组成，其属性只有拥有人知晓。

令牌化：一种将敏感数据的曝光风险最小化的流程。

身份管理：对他人对您个人信息实施访问的一种长期的管理流程。这涉及为社区所有用户创建唯一的身份，还涉及社区用户的关联和交互，从而建立起“信任”。

区块链/分布式账本：一种分布式的防篡改数据库/平台，确保所有的记录（无论它们身处何地）都被添加于其内。每条记录至少包含一个时间戳和之前记录的安全链接。

信任：社会学家詹姆斯·科尔曼（James Coleman）对其做了如下定义：“信任是在您知道别人如何行动之前投入到合作努力中的意愿。”（Coleman, 1990）。¹¹

公司

¹¹詹姆斯·科尔曼。《社会理论基础》1990。

我们的公司 — 安全身份账本公司 (SILCSM) 在美国特拉华州注册成立。公司总部位于美国维吉尼亚州，地址：6329 Arlington Blvd, Suite N, Falls Church, VA 22044, USA。除了由 5 人组成的执行管理团队，我们还拥有 10 名软件开发人员和 6 名业务拓展精英。

我能看看区块链吗？

为使事情变得简单，我们相信，一定要让用户能够看到他们的交易，并确切知晓交易被记录到公共区块链的具体位置。如果有需要，用户可以检索信息，从而建立一个审计轨迹。

注册、认证和验证

在注册和参与令牌出售时，SILCSM 将创建一个唯一身份。用户可以在 SILCSM 的注册/登录系统中注册一个帐户。之后会随机生成一个临时密码，每登录一次，就会发送临时密码到电子邮件或手机。

临时密码的有效期只有 10 分钟。之后生成另一个密码。

每个在我们系统注册用户，在一开始都是未经验证的。未经验证的用户可以参与令牌销售，但他们无法访问未来的应用和服务，如即将开始的令牌交易和数据存储。

要成为经过验证的用户，您必须提交以下所有文件来支持您的物理身份，从而在平台创建您的数字身份：

- 8 个身份字段：用户显示名、名、姓、街道、城市、州、邮编、国家
- 3 个字段：地址证明（电、天然气、车辆登记等）、政府颁发的照片身份证件、本人照片

验证过程只需一次，不再重复。如需再次验证，请联系我们获取新账户。

为何我们要求将您的数据用于验证？

所有的用户数据都被打乱，然后存储在 SILCSM 数据库，在这一定制的过程中，我们无法查看或访问这些数据。包含了所有嵌入验证数据的用户数据，连同 SILCSM 令牌数据将通过验证。

我们要求验证的数据几乎不可能造假，不会表现出不一致。虽然我们无法看到您的数据，但是其他方，如政府可能要求您提供钥匙解密这些数据。如果数据在这种情况下被解密，因输入假数据导致的不一致之处会表现出来。

每人的区块链是个唯一账本，由每个用户账户独占，其包含了该特定用户的所有令牌交换记录，及区块链交易记录。

注：未验证的用户无法访问我们应用的全部功能。然而，他们可以浏览公共区块链，查看自己的令牌。

唯一身份和钥匙

SILCSM 为每个用户（无论是否经过验证）分配唯一身份，将其用于确定每个账户。这个唯一身份是目前区块链上仅有的身份识别形式。唯一身份没有特定模式，可以是任何长度。

用户经过验证后，SILCSM 系统将为每个用户生成私钥和公钥，然后对其进行分配。

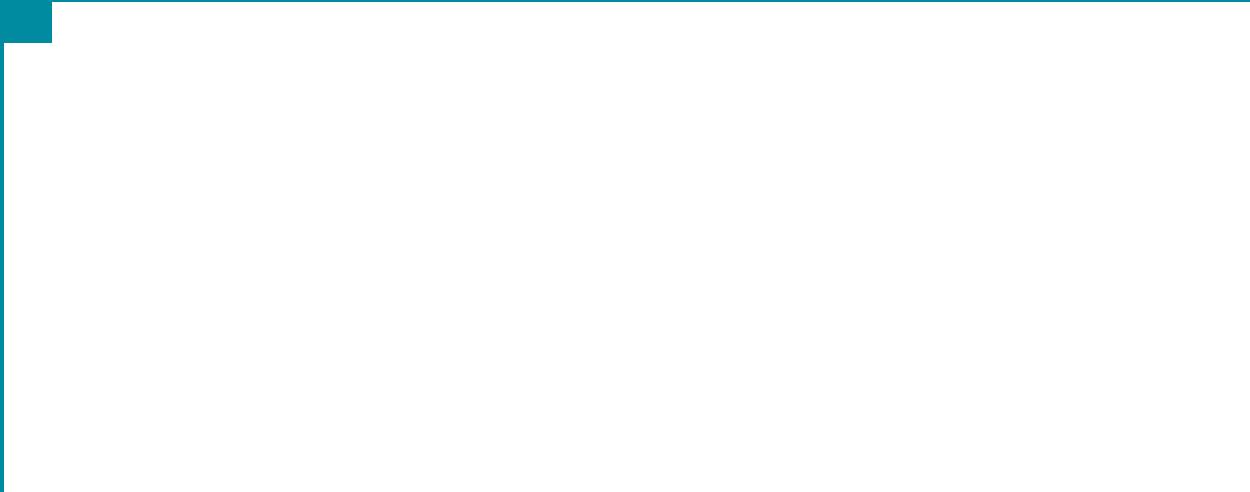
使用唯一身份的优势

唯一数字身份是基于数字创建的区块链身份，能够增加在政治交往、经济往来和社会参与等方面的机会。我们所规划的应用的最大特性是提供一个集用户验证和认证于一身的系统，任何企业都可将其用于线上和线下交易。每一笔交易都记录在我们自定义的区块链上，我们保证：

- 持久性：区块链中的一切事物都是永恒的；当一个区块产生了交易的永久性记录后，不能对相邻区块进行改变或变更。
- 不可变性：在区块链中，事物在创建后无法修改。
- 不可逆性：区块链中的任何事物都无法删除。

这些特性为区块链增添了一层透明的窗户，用户凭之可以相信，他们进行的每个区块交易都将永久性地存于区块链中，不会发生任何改变。

SILC 积分



使用案例

案例 1

亚历克斯想交换联系信息，并发送订单给商家（在线或离线），他要提供（1）他的订单；（2）送货地址；（3）信用卡信息；（4）其他要求。所有这些数据可以加载和加密到一个预先设定了截止日期的区块中。这些信息被发送给一个拥有密钥来解密区块数据的商家。商家将通过订单加密确认回执、或通过电邮确认回执发送给亚历克斯。整个交易已经记录在亚历克斯的区块链中，及商家的区块链中。

注：这些区块仅仅是真实生活中物体/服务的代表。亚历克斯和商家都因付出交易成本而失去了一个积分，这是因为，他们将其中一个空载区块分别转换为“订单”和“回执”的区块。

案例 2

例如，亚历克斯希望用铅笔换鲍伯的苹果。亚历克斯发起与鲍伯的交换，将“铅笔”分配给一个区块，并要求获得一个带有“苹果”价值的区块。亚历克斯这时用掉了一个积分。如果鲍伯接受交换条件，同意将“苹果”作为一个价值分配给他的区块，那么在交换完成时也会失去一个积分。整个交换活动已经记录在区块链上。

注：这些区块仅仅是真实生活中物体/服务的代表。亚历克斯和鲍伯都因付出交易成本而失去了一个积分，这是因为，他们将其中一个空载区块转换为具有“苹果”和“铅笔”价值的“价值”区块。该笔交易被记录在区块链上。

案例 3

比方说，亚历克斯想将文档发送给鲍伯。亚历克斯发起与鲍伯的交换，将“文件”分配给他的区块，并请求鲍伯提供一个“回执”区块。在鲍伯结束交换后，亚历克斯会失去一个积分。在亚历克斯接受“回执”区块时，鲍伯也失去一个积分。交换条件将被正式履行，并记录在区块链中。

注意：这个交换仅仅是真实生活中物体/服务的代表。亚历克斯和鲍伯都因付出交易成本而失去了一个积分，这是因为，他们将其中一个空载区块转换为具有文档价值的“价值”区块。

案例 4

假设亚历克斯想和鲍伯达成一个协议，但亚历克斯想要对方提供 3 个额外的身份，以确认鲍伯就是鲍伯本人。亚历克斯发起与鲍伯的交换，将“身份证明”分配给一个区块，并请求对方发回一个“证据”区块。鲍伯可以加密 3 个额外身份，并加载到只有亚历克斯可以查看的区块中，鲍伯还可以给“证据”区块上的数据添加截止日期。一旦亚历克斯从鲍伯那里收到“证据”，该笔确认活动将记录在区块链中，证据区块随之失效。

注：这些区块仅仅是真实生活中物体/服务的代表。在发送“验证身份证明”和“证据”区块的过程中，亚历克斯和鲍伯都使用了积分。