



VerifyUnion

白皮书

---

## 声明

---

本文件及任何其他VerifyUnion文件均不构成任何类型的招股说明书，也不代表任何的投资清偿。UC Coin不代表拥有任何公共或私人公司的所有权或份额，或者任何管辖范围内的其他实体。通过Crowdsale购买的UC Coins不予退还。UC币只能在条款与条件要求下与VerifyUnion联合使用。任何获取和使用UC代币都会带来显著的财务风险，包括使用实验软件。

版本1.17

2017年9月15日

VerifyUnion 团队撰写

[www.verifyunion.io](http://www.verifyunion.io)

# 目录

## 摘要

- VerifyUnion 建立在以太坊区块链上
- 需要一种新的方案
- 社会信任服务（社会评分和验证）

## 代币说明

- “UC Coin” –VerifyUnion的加密货币
- 代币销售分配

## 研究与发展

- VERIFYUNION 是一种解决方案：
  - 数字身份管理
  - 目前的金融服务业
  - 数据采集和共享的成本
  - 安全和隐私

## 公司

- 法律结构
- 网络参与者
- 联系方式

## 总结

## 采用区块链技术

- 在VerifyUnion中集成区块链
- 区块链的安全
- 使用区块链进行身份验证和识别
- 为什么我们需要区块链？
- 目前的制度缺乏效率
- 区块链应用方案
- 提出的方法
- 当前信息共享存在的问题
- 解决问题

## 团队

## 顾问

## 合作伙伴

## 社交媒体

## 参考文献

## 发展中的生态系统

- VERIFYUNION 原型 - PROS解释

## 产品说明

- VerifyUnion的程序流程
- 真正的价值组合
- 锚定方法和机制

## 强化安全验证

- Union智能锁
- Union智能引起
- 防御区块链受到攻击的支出

# 摘要

黑客，身份盗窃，个人数据泄露，密码泄露和文件欺诈只是当前在线安全措施不被信任的几个原因。

我们为用户引入了一个新的系统，该系统可以利用区块链和以太坊网络的优势，并将其应用于在这个隐私和安全受到威胁的世界中帮助我们的用户。

当我们使用数字服务，并上传我们的个人文件和信息时，我们大多数人都没有意识到谁在使用这些详细的识别信息以及具体目的。现行制度的低效率和重大风险在于，一旦文件或个人资料被转移，信息所有者的权力将被切断而不能检查或追踪其流向的细节。

VerifyUnion为所有用户开发了一个独特的组合，它将返回“真值”。真值是一个融合了包括数字身份，社交和公众个人资料以及与用户独特个人资料相关的财务细节的综合值。用户通过提高信任和验证服务的真实性，将获得价值收益。这种方法允许用户提供完成验证所需的基本信息，并且可以通过提供附加的用户和评估资料的数据来增加他们的组合的真值。

区块链可以通过分散证书的所有权来提供去中心化的解决方案，并提供一个通用的协议来验证一个人在不可变的数据链中的记录。这个数据，存储在一个共享的去中心化账本，而不是存储在一个单独的应用程序中。这个共享的分散账本由区块链的每个用户下载，并且包含有史以来所有交易的历史记录。

VerifyUnion在过渡阶段提供了同时具有两种方案优势的混合版本，同时我们完成了完全分散式解决方案的开发。通过使用区块链技术，我们致力于向个人用户授予数字验证过程的完整权利。

VerifyUnion是一个集成平台，通过在这个平台注册，用户可以安全地实现所有安全的数字身份识别需求。个人信息仅保存在用户的个人存储器中，而不是将其发送给一个匿名人员或公司，然后用户可以决定是否共享该信息而无需发送给中央管理机构。个人信息将被发送给请求者，并且用户保持对所传送的信息拥有完全的权限。



# 摘要

VerifyUnion 提出了更广义的信任验证的概念，而不局限于数字身份验证。这有利于用户和请求方交易合作，同时验证包括社交简介，社会影响，兴趣和数字标识。

VerifyUnion 是利用区块链技术的高级功能来识别和验证互联网上的数字身份的平台。VerifyUnion 将为我们的客户（寻求验证其客户或用户的组织）提供卓越的功能，和通过在不同行业应用我们定制的算法对用户进行快速验证。

在区块链技术发展的推动下，通过将身份链接到区块链上来建立防篡改系统，这有助于减少欺诈活动和数字身份诈骗。通过在现有的区块链技术上构建，而不再需要信任服务器管理员，同时，通过我们的平台，可以创建更高的真实性和可验证性。

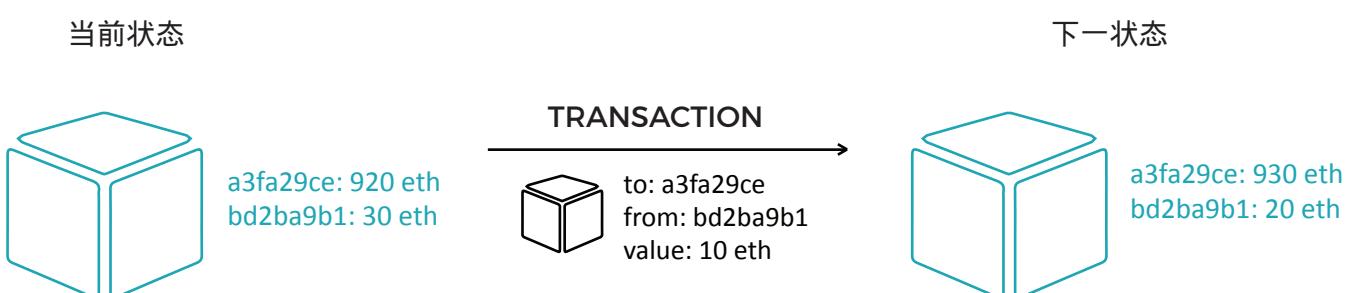
VerifyUnion 还计划当你从平台要求信任验证服务和社会评分信息时，在这个生态系统里用UC币进行交易，即是作为软件即服务（SaaS）的商业模式的平台代币。VerifyUnion 希望这个生态系统能够减少当前集中式平台的缺陷。

## VERIFYUNION 建立在以太坊区块链上

以太坊是一个分散的平台，运行智能合同：应用程序完全按照程序运行，没有任何停机，审查，欺诈或第三方干扰的可能性。

这些应用程序运行在一个定制的区块链，有力地共享全球基础设施，可以转移价值和代表财产的所有权。以太坊区块链的结构与比特币非常类似，因为它是全部交易历史的共同记录。网络上的每个节点都存储此历史记录的副本。以太坊的最大区别在于除了所有以太网交易，它的节点存储每个智能合同的最新状态。对于每个以太坊应用程序，网络需要跟踪“状态”或这些应用程序的当前信息，包括每个用户的余额，所有智能合同的代码以及所有存储的具体位置。

我们正在Ethereum 区块链上构建VerifyUnion，这为我们提供了一个额外的外部安全的优势，由于Ethereum 的分散性，用户可以无忧无虑，因为相对于集中式系统，分散式系统显着降低了黑客成功入侵的可能性。



# 摘要

---

## 需要一种新的方案

随着网上业务交互业务的比例不断攀升，对安全的数字身份的需求空前强烈。

无论是与供应商签订订单的公司，还是从网上商店购物的消费者，亦或是个人开设账户或申请工作或信贷，实现身份的证明，都是每个在线交易至关重要的一步。

**随着知情客户（KYC）和反洗钱（AML）的国际法律以及各国打击欺诈和腐败的具体法律出台，数字验证的需求日益增长。**

在处理公共事务方面，这种需求也在增长。企业和消费者都越来越多地在与政府机构进行各种繁琐的互动沟通时遇到阻力。太多的人在证明自己的身份时遇到了大量的摩擦，导致他们提供的信息比他们应该提供的更多，而不知道如何正确使用它们。

虽然已经有一系列的数字身份识别系统在应用，但仍然需要一个可以由多个组织统一采用的方法。拥有这样的基础设施，将简化互动，同时确保个人身份始终保持安全。另一方面，这个问题似乎很明显。我们都需要一个一致的数字身份（可以认为是虚拟身份证），可以识别和验证我们，不仅为我们所有的设备，而且我们的所有在线服务，商业和银行账户，基本上包含任何我们需要的数字（验证），或甚至在物理上验证我们是谁。

然而要解决这个问题，被证明是非常困难的。首先，任何类型的数字身份解决方案都要求平台和设备是独立的。用指纹识别器扫描手机是很好的，但大多数人拥有的设备不仅仅是一个智能手机，而且在很多情况下，他们在不同的平台上运行不同的软件。

**在英国，2015年身份盗窃的受害人数上升了57%。这些来自英国261家公司的数据表明，欺诈者越来越多地从社交媒体网站获取个人信息。Facebook，Twitter和LinkedIn已经成为身份盗窃者的“狩猎场”，2015年英国有超过14.8万名受害者，而2014年则为94,500名。**

在这种情况下，引入区块链技术，为数字验证问题提供了一种高效率的长期解决方案。区块链是比特币数字货币背后的技术，是一个分散的、没有人或公司拥有或控制的公共分散式账本。相反，每个用户都可以访问整个区块链，并且每个用户从一个帐户到另一个帐户的资金转移都是通过使用从密码学借鉴的数学技术，以安全可验证的形式记录下来的。随着区块链分布在全球各地，可以有效地防篡改。区块链可以在三个方面提高安全性：阻止身份盗用，防止数据篡改，并阻止服务受到攻击。

# 摘要

---

## 社会信任服务（社会评分和验证）

我们正在不断发展一个复杂的社会“信任”系统，该系统使用社交评分系统来确定用户在平台内的验证水平。信任验证是我们开发的二级平台的一个组成部分，是一个重要的独立利润中心，以“信任即服务”的形式提供信任和社交评分模块。这些信息中的大部分将来自于与用户的数字身份并行运行的社交评分算法。用户将收到他/她的社交分数和他/她管理下的所有社交媒体和公共文件以及公众可用或不可用的其他公共数据的更新。用户可以在收到提示时共享此信息或拒绝此类请求。

这些数据可以包括社交媒体评分和历史记录，信用记录，公司

持股和董事职位，枪支许可证，驾驶执照，警方记录和犯罪记录等等。

用户可以通过提供更多关于自己的信息，来提高他们的社交分数，

并将这些信息存储在他们的私人存储中，并根据个人的判断向请

求方分享加密信息。通过使用此平台，用户可以获得VerifyUnion加

密代币（UC Coins）作为奖励，并将其用于将来的验证服务。



当代币的需求增加时，我们也期望从用户那里购买代币以获得更高的价格。

# 研究与发展

以非常简单的方式来说，数字身份是对您真实身份的数字表示。数字身份是在线服务转型的重要组成部分，这是数字交易的“钥匙”。VerifyUnion是一个安全可靠的数字身份管理器，只要客户选择使用，它就会被行业所接受。目前，我们都有多个数字身份，通常是每个服务提供商独特的一个，围绕传统的公司和组织中心的服务交付和商业模式而设计。但是，这种模式随着世界强调数字化，正在发生快速转变，正在向以客户和用户为中心的服务设计时代发展。为了支持这一趋势，出现了一种新的数字身份识别方法。一个用户因此能够控制他们的身份信息。这从用户，提供商和行业角度初步探讨了如何使用单一数字身份访问多种服务。

**缺乏适当的核查制度既有经济成本，也有社会成本。根据截至2017年8月的数据，发展中国家有17.5亿人缺乏合适的身份证件，其中包括2亿多5岁以下的儿童。全球大约有25亿成年人，占全球成年人口的一半以上，不使用正规的金融服务来存款或贷款。22亿无名成人生活在非洲，亚洲，拉丁美洲和中东地区。**

例如：在英国境内，没有单一的权威来源或证书，可用于在线交易中安全地声明身份。英国的3600万成年人（成年人口的75%）每天都在线，其中72%的成年人在网上购买商品或服务。这些统计数据，加上网上交易（例如银行和政府服务）日益敏感，对于需要验证和验证每个客户或公民的身份的组织来说，都是一个挑战。随着我们看到更多的政府服务在网上推动，我们需要考虑访问在线医疗记录，就业福利和税务事务所需的安全性，并且认识到这些类型的交易在涉及身份认定时需要更高级别的安全性。

## VERIFYUNION 是一种解决方案：

### 数字身份管理

随着世界上越来越多人在网上进行互动和交易，这意味着还有额外的要求来创建网上“信任”来降低在线欺诈和其他形式的滥用风险。

通过标准和治理框架创建数字身份，是创建这种信任的一种方法。当组织可以信任使用数字身份的人时，这意味着更多的服务和交易可以迁移到在线，从而节省大量成本。

### 目前的金融服务业

金融服务行业需要完成“了解您的客户”（KYC）检查身份验证是否符合法规。这是一种基于风险的方法，可以在产品和制度的基础上进行解释。由于数字革命，这个行业正在经历一个巨大的转变。提高客户参与度以及更好的用户体验、选择、竞争、透明度以及创新的服务，是受技术革命推动的理想结果。

# 摘要

---



## 数据采集和共享的成本

对于一家银行加入一名客户，他们平均花费15美元至25美元来加载完整的KYC资料。如果用户想申请额外的服务（例如：信用卡，汽车贷款），那么他们需要提供额外的文件，这些文件对于交易可能需要也可能不需要，浪费了提供者和顾客的时间（以及更多的成本）。此外，完成KYC档案所需的总时间也日益增加，越来越严格的规定增加了用户档案的要求。一般来说，为了安全起见，监管机构要求收集尽可能多的信息来确认用户的身份，导致不必要的和敏感的信息被多次传输，如SSN号码，IRD号码等对于KYC是不需要的。



## 安全和隐私

最大的问题是依靠数字渠道销售产品和服务的公司。随着每一个关于重大数据泄露事件的提起，关于共享数据的安全性的怀疑在上升。每天有数十亿人在互联网上分享想法，进行金融交易，并与家人，朋友和同事保持联系。用户通过这个全球网络发送和存储个人医疗数据，业务通信，甚至是亲密的对话。为了互联网的发展和繁荣，用户必须能够相信他们的个人信息是安全的，他们的隐私要受到保护。

移动网络上的数据传输是最不安全的方法，使用数字钱包的交易将受到任何移动交易中固有的风险的影响。您的手机也有丢失或被盗的危险，危及您的个人和财务信息。数字钱包最大的风险之一就是在发生欺诈时的个人责任。大多数使用借记卡或信用卡支付购物的消费者对银行或信用卡公司都有一定的保护。大多数金融机构不会持卡人对其信用卡进行欺诈性购买负责。对于使用数字钱包的消费者而言，这种欺诈保险目前不存在。

根据美国人口普查局收集的数据。对41000多户家庭进行的调查显示，调查前12个月，1900万家庭的互联网使用家庭中有19%受到过网络安全漏洞，身份盗用或类似恶意行为的影响。通过使用区块链技术，它将允许用户对他们同意共享的信息拥有完全的权力，并且只有在用户需要的情况下才能根据需要将其发送给发布请求的权威机构。通过使用生物特征保护和2FA的先进技术，正常情况下区块链安全服务器还有额外的安全层。在很多情况下，公司需要支付高额费用来验证几秒前可能已经为不同供应商验证的个人身份。通过在区块链中加入身份验证，并使用哈希函数来验证区块内容的真实性，可以降低成本并显着缩短时间。

# 采用区块链技术

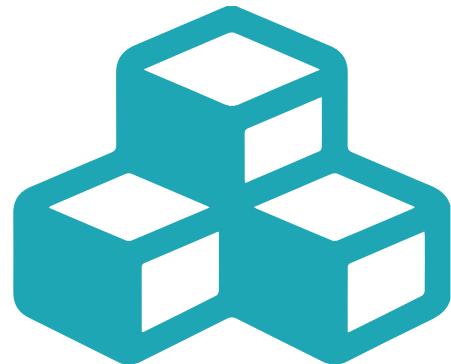
## 在VerifyUnion中集成区块链

VerifyUnion是独特的解决方案，它集成了使用区块链技术的分散式身份验证，并启动了从当前集中验证方法的过渡，解决所有用户信息处于危险之中并且个人不能控制其个人信息的问题。

通过在网络的所有成员之间分配分布式账本，区块链认证消除了人们恶意更改分布式账本的可能性。每次将“交易”或数据块添加到链中时，大部分网络都必须验证其有效性。这保证了分布式账本的完整性。然后可以使用公钥加密（例如非常安全的RSA加密）来安全地发送他们的证书。然后收件人可以对照不可变区块链中的条目进行验证，从而以非常安全可靠的方式处理身份验证。

## 区块链的安全

区块链依靠三大支柱：(1)共识，(2)分布式，(3)无需信任，而安全来源于工作证明问题。这个问题的设计需要大量的计算能力才能完成，因此，对于一个人来说，这可能需要几年的时间。而对于一个电脑网络，可能只需要几分钟。因此，可以连续地添加链，并且在保证数据不被篡改的情况下及时处理事务。这个问题的本质使得在数学意义上不可能有人改变区块链。更改一个块（只能通过创建一个包含相同前驱的新块来完成）需要重新生成所有后继，并重做它们包含的工作。



## 使用区块链进行身份验证和识别

现在，新公司已经开始开发区块链的潜力，并利用该技术开发各种服务。区块链身份验证的中心将是区块链ID。这个ID本质上是一个链上的数据块，可以被任何第三方验证，并可以显示必要的信息，如出生日期。这个验证的秘密是椭圆曲线数字签名算法（ECDSA）。在向区块链添加ID时，身份识别发行服务系统默认绑定公钥，然后将私钥的所有权转让给用户。这允许用户，而且仅仅是该用户，可以签名，对存储在区块链的公钥进行验证。用户的这种识别将作为分散的认证来源。它基本上是一个单点登录门户，可以被任何应用程序访问，而不被任何单个实体所有。受保护的应用程序只需要请求访问用户的数字签名和ID。

然后应用程序可以验证签名是否有效，并且通过用户的ID验证他们是谁。

# 采用区块链技术

---

## 为什么我们需要区块链？

这在很大程度上是由于我们的身份识别系统缺乏安全性。但是，完全切换到这个分散的系统将是一个漫长的过程，同时，用户需要一种方法来保护他们的数据和身份。这是为什么要引进多因素身份验证的原因。服务提供商可以使用区块链实现多因素身份验证，而无需取消当前的身份验证方法。这将有助于为应用程序增加一层额外的安全性，同时慢慢地让人们从区块链技术中获益。像拍照一样简单，整个过程可以自动完成，只需要用户创建一个ID并下载一个应用程序来处理必要的认证确定。区块链的分散性质可能允许用户手动签署请求并将其返回，但是，对于可用性来说，最有可能利用此技术的是一个应用程序。简单地拍摄一个QR码，对验证请求进行编码，应用程序将对请求进行签名，并将其返回给受保护的应用程序。

## 目前的制度缺乏效率

目前有两种选择用于双因素认证。例如，最常用的方法之一是通过SMS发送代码。但短信是臭名昭着的不安全。潜在的攻击者可以嗅探来自任何号码的消息，并且除了伪造消息的发送者之外还读取它们。这是一个很大的问题，因为如果攻击者知道你的名字，并且你的帐号使用短信作为认证的备份方法，他们可以在网上找到你列出的电话号码，然后拦截这些信息，获得他们发送的任何代码。这很容易，无处不在，但不可能在不改变SMS协议本身的情况下进行保护。目前双因素认证的另一个问题是服务的专有性质。Google身份验证器等方法安全且易于使用。但是，Google可以访问您的所有双因素代码。这个选项更加安全，但带回了拥有认证数据的单个实体的问题。攻破Google可能会导致您的所有验证码泄露。区块链提供的分散化方法消除了这个问题，因为该链对公众100%开放，并且没有任何敏感数据存储在区块链上。

# 采用区块链技术

## 区块链应用方案

### 握手和散列

区块链ID是一个可行的解决方案，可以解决验证用户是谁的问题。而且，这个功能可以扩展为代表个人进行各种安全的数据传输。与身份验证密切相关的一项服务是在不披露不必要信息的情况下共享身份信息。除了共享数据之外，用户还可以将数据添加到链中作为交易的证据，而不会泄漏交易的原始数据。任何一方都可以根据这个条目验证一个文档，并证明它实际上是有效的，从而能够对数据进行快速可靠的审计。这种方法将基于消息签名和哈希的原则。许多服务已经使用这项技术来安全地验证数据（例如JSON Web令牌），而不公开原始数据。

### 提出的方法

一个依赖于区块链中心握手的通用的认证流程。已经被企业（如：blockstack）进行了测试和利用。这个“握手”向验证应用程序和用户验证他们正在与谁进行通信。在此示例中，受保护的应用程序是请求身份验证的应用程序，用户是试图访问受保护的应用程序的实体。此流程的第一步与任何登录的步骤相似。但是，用户不会被提示输入密码。相反，用户会在受保护的应用程序上看到一个用户名的表单，然后显示一个QR码进行验证，或者在其记录中查找首选的验证方法。

QR代码示例将更容易设置，并简单地编码来自受保护的应用程序的身份验证请求。这个认证请求是握手的第一步。下一步是验证请求并发送响应。此步骤包含许多确保身份验证的子步骤。首先，用户将验证请求数据是合法的，受保护的网站是他们期望的。这可以通过使用公钥密码来完成。这将允许受保护的应用签署请求，然后通过区块链或证书颁发机构进行公开验证。为了支持简单的转换，从HTTPS的TLS中使用的认证授权系统开始，这是合理的。然而，这可以通过在区块链上创建应用程序ID来转换为完整的区块链认证，然后可以验证该应用程序ID。

验证这个请求后，用户将点击一个按钮来验证登录。然后，这将创建一个响应，签名，然后将其发回到受保护的应用程序上的指定路线。这个请求将在被保护的应用程序上使用公钥加密来验证，用户将被登录。使用区块链的好处是它是完全分散的。如果您不想使用应用程序来促进此流程，则用户可以简单地使用其公钥生成自己的签名，然后以表单提交，然后由网站验证。这显示了分散系统的真正好处。因为任何人都可以访问这些数据，并且用户可以控制他们的私钥，那么作为一个用户，您就不会被迫使用给定的API来为这个请求提供便利。你可以给予你所愿意给予的其他系统尽可能多的信任。

# 采用区块链技术

---

## ① 当前信息共享问题

目前的身份验证问题是，您经常需要提供比请求者真正需要的信息更多的信息。如果您的交易受到损害，而某人可以以某种方式拦截数据，那么他们将拥有大量信息来开始伪造身份。为了解决这个问题，可以扩展先前的认证流程来创建一个解决方案。

首先协议将定义一个“许可”集或请求一组特定的数据。这个“许可”级别将由一个通用的用例来定义。例如，如果系统想要收集信用信息，则可以发送“付款”请求。然后用户可以看到并确定他们是否想要向其供应商披露他们的信用卡信息。如果他们信任它，他们可以签署请求并发送一个包含相关信息的数据包。如果他们的银行支持区块链认证，他们可以简单地发送一个签名的支付包，然后网站可以转发给银行并完成交易，从而防止用户向供应商提供任何个人信息。否则，数据包可能包含相关的财务信息，如信用卡号码等。但是，为了防止欺诈，网站可以验证这个人真的是数据的拥有者，而且他们没有使用被盗的卡。

为此，可以使用加密哈希来验证数据。数据包首先被散列并由用户签名。这将告诉供应商，它确实是一个给定的人发送数据。接下来，该网站将在Blockchain上查看该数据的签名和散列版本。如果散列与签名匹配，供应商将知道数据实际上与该人相关联，并且数据未被篡改，从而合理地保证该卡由认证的个人拥有。

## ③ 解决问题

为了确保 ID 确实是其所声称的人，需要更安全的验证形式，而不是仅仅简单地使用社交媒体帖子等验证。一个可信的权威机构必须分发这些ID或由第三方安全地审核用户的敏感文档，以便更好地验证ID。因此，类似于TLS协议的证书颁发机构的情况，人们必须相信这些机构正确地审查了这些文件。一个基于hash的系统可以用来存储文档的使用记录，所以有人可以验证一个文档是给一个特定的身份，但是，这个文档信息可能是敏感的，因此所有者不希望明文在区块链上可用。这介绍了当前将信任置于第三方的问题。

# 发展中的生态系统

---

在完成第一阶段的部署之后，VerifyUnion将超越常规的数字验证术语并执行以下连续的开发计划：

1. 在Ethereum网络上启动智能合约开发，建立一个系统，让我们的用户可以在预定义的条件下创建合同，在特定的时间执行，并合并到我们现有的所有客户端平台。
2. 为VerifyUnion创建一个名为“UC Coin”的代币并进行初始代币发行，我们将在第二阶段的开发中使用到它，并为我们的令牌奖励计划给身份和评估者的服务付款。,
3. 过渡到一个完全分散的应用程序（DApp），允许更多的权力给用户端，保持对自己的ID共享，以保持对验证过程的控制。

另一个阶段的发展是将VerifyUnion作为SaaS加入到我们最初的客户“Entisy”，这是一个在澳大利亚，亚洲和非洲（迄今为止）六个国家和全球虚拟服务市场上的点对点市场。我们还将使用令牌作为我们开发或共同开发的所有应用程序的加密货币，这将允许我们的用户在多个平台上使用货币，并同时获得验证的好处通过使用入口。

## VERIFYUNION 原型 - PROS解释

通过开发VerifyUnion生态系统的主要好处是：

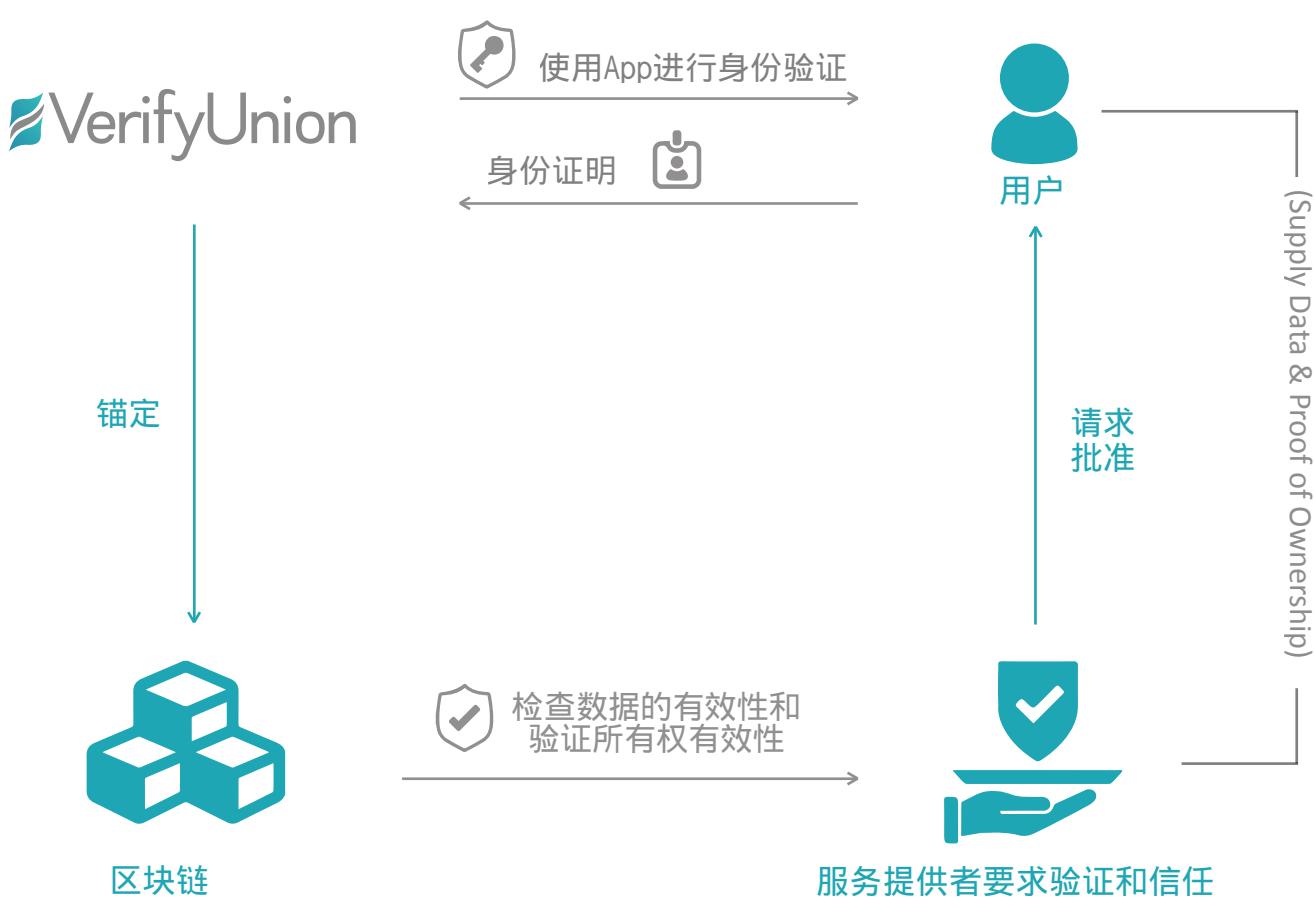
- 用户完全控制验证过程和数据被共享给信任的社会认同的机构。物理数据在最终用户的控制之下，这意味着用户可以控制正在进行的识别，和控制验证的目的。他们可以使用UC Coin代币作为未来的验证过程中的奖励，或者用其在我们生态系统中进行支付。
- 政府部门，金融机构和企业可以使用这个系统，可以以低成本高效益的方式实时地进行用户身份验证和信任。
- 评估人员可以通过评估用户的身份，以及通过获得UC Coin代币奖励而受益，并且可以使用区块链系统实时更改评估和徽章的价格。
- 需要验证的服务提供商可以在一个平台上获得所有需要的记录（在用户验证之后），而不是去多个机构，这大大降低了验证成本。

# 产品说明

## VerifyUnion的程序流程

在第一阶段，VerifyUnion将建立一个集中和分散平台的混合平台，使用政府机构、中央机关和金融机构的评估者来验证用户想要验证的ID和交易激励代币（UC代币），UC代币用于评估者和用户正在进行他们可以使用代币用于未来的验证活动或者销售代币以释放代币值。

通过使用VerifyUnion手机移动应用程序，用户可以设置生物识别安全功能和2FA方法来创建初始安全层。然后，用户保留审查信息请求的能力，并决定是否允许或拒绝该请求，并仅给出验证所需的最少ID信息。这种方法允许用户使用最少的所需文件和安全的数据传输方法进行实时ID验证。

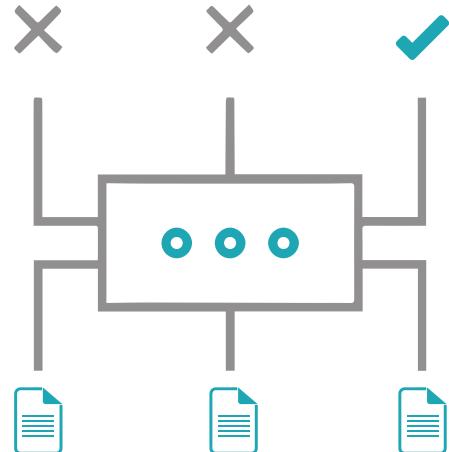


VerifyUnion致力于开发帮助用户获得全面控制权的生态系统。我们使用区块链保护的现代方法来提供最高安全级别的验证和信任服务。通过使用VerifyUnion 的app程序，用户可以使用这些被政府机构、官员和金融机构在内的“评估人员”存储和验证的文件进行验证。

# 产品说明

在验证身份证明之后，会给用户资料一个“徽章”，证明这个身份已经被验证，并被加到我们称为“锚定”的区块链中。

在下一阶段中，银行，金融机构和所谓“服务机构”的所有机构需要进行身份验证的主管部门将可以减轻独立验证过程的负担。他们可以依靠评估者已经完成的工作，评估者已经通过请求用户的授权，并使用哈希函数从区块链中获取细节。通过这种方式，用户将确切地知道哪个授权机构正在访问信息以及该ID被使用的方式。



评估者可以向经用户同意要求进行身份验证的主管部门提供服务，并且VerifyUnion会奖励评估者和使用我们的令牌币进行验证的用户，他们可以将这些币用于未来的身份识别服务以及生态系统内接受我们的硬币的所有其他功能。

VerifyUnion平台通过使用系统内部的智能合约，为验证和信任服务提供实时交易，并为用户提供可扩展性和更多强大功能。生态系统将为用户提供控制权，通过用户同意共享所需数据。评估人员可以使用智能合约将徽章出售给提供商，提供商可以看到用于验证的报价范围，并选择他们更愿意的评估用户身份的报价范围。

评估人员可以实时更新引用以进行验证，这取决于区块链的锚定时间，并将相应地反映在VerifyUnion平台上。

一旦评估者和用户之间通过智能合约进行握手，就进行交易，并将用户同意的数据传送给需要验证的提供者进行验证。交易完成后，按照UC Coin约定的价格付款给评估者，用户可以参与UC Coin，并在我们的生态系统和所有合作伙伴生态系统中使用。 UC代币也可以转换为以太坊和比特币（将在以下阶段的VerifyUnion交易所和钱包中发布）。要求验证的服务提供商将向VerifyUnion支付菲亚特代币或者其他加密货币（如果他们没有持有UC Coin），我们将使用这些钱币购买支持评估者和用户的UC Coin代币，并从那些想要转换的用户那里购买回到菲亚特货币或任何其他加密货币。这将有效地奖励用户更多的钱来验证他们的身份。因此，对代币的需求就越大，这意味着用户可以利用我们的平台使用更多的服务，并获得更多的代币作为使用奖励，从而通过我们的平台赚钱。

用户可以使用VerifyUnion应用程序将他们的数据存储在个人设备上，也可以根据个人喜好备份到基于云或分布式存储平台。 VerifyUnion不会处理这种形式的数据存储，主要是由于在多个司法管辖区负责的重大监管影响个人身份信息。

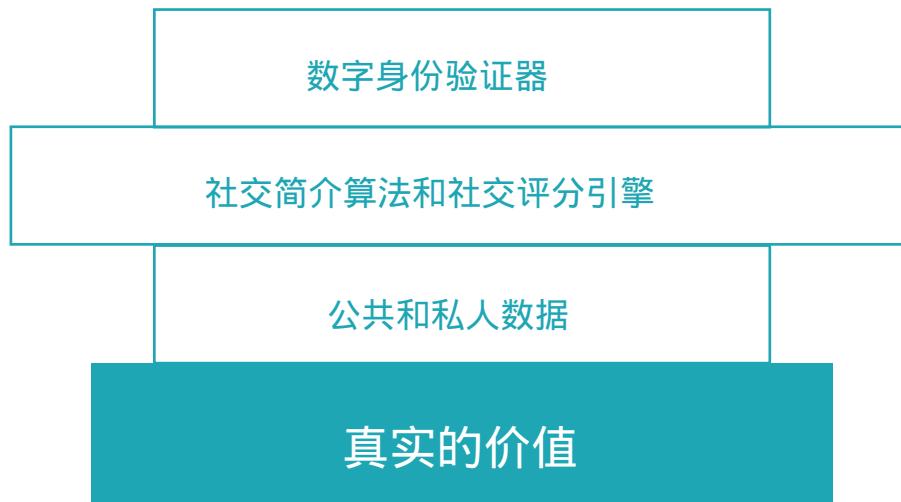
# 产品说明

## 真实价值组合

投资组合将包括不同的模块，并基于用户希望提供给信托和验证服务的信息来计算“真实价值”。该投资组合包括一个社会评分引擎，该引擎将用户配置文件和用户份额与系统的社交数据相关联，并将其添加到正在评估的社交分数中。通过使用更多的验证服务，用户可以创建更高价值的产品组合，以最低的成本和延迟为生态系统中的未来服务所用。

评估人员可以在验证过程中分析完整的用户组合，而不是执行重复的数据搜索，从而使用户和提供商能够在最短的时间内以更高的效率完成交易。这样，用户就可以完全控制交易，并可以通过VerifyUnion应用程序接受或拒绝基于用户请求服务的共享信息的请求。

社交评分引擎将使用户能够相应地使用他们的公共和私人个人资料用于不同的验证服务。他们可以通过使用VerifyUnion应用程序提供引用来轻松完成验证，这些应用程序允许供应商完成并即时访问用户。这将消除常规验证方法遇到的延迟，可能需要几个工作日才能进行小规模的验证，而这些验证不需要复杂的程序和冗长的时间。

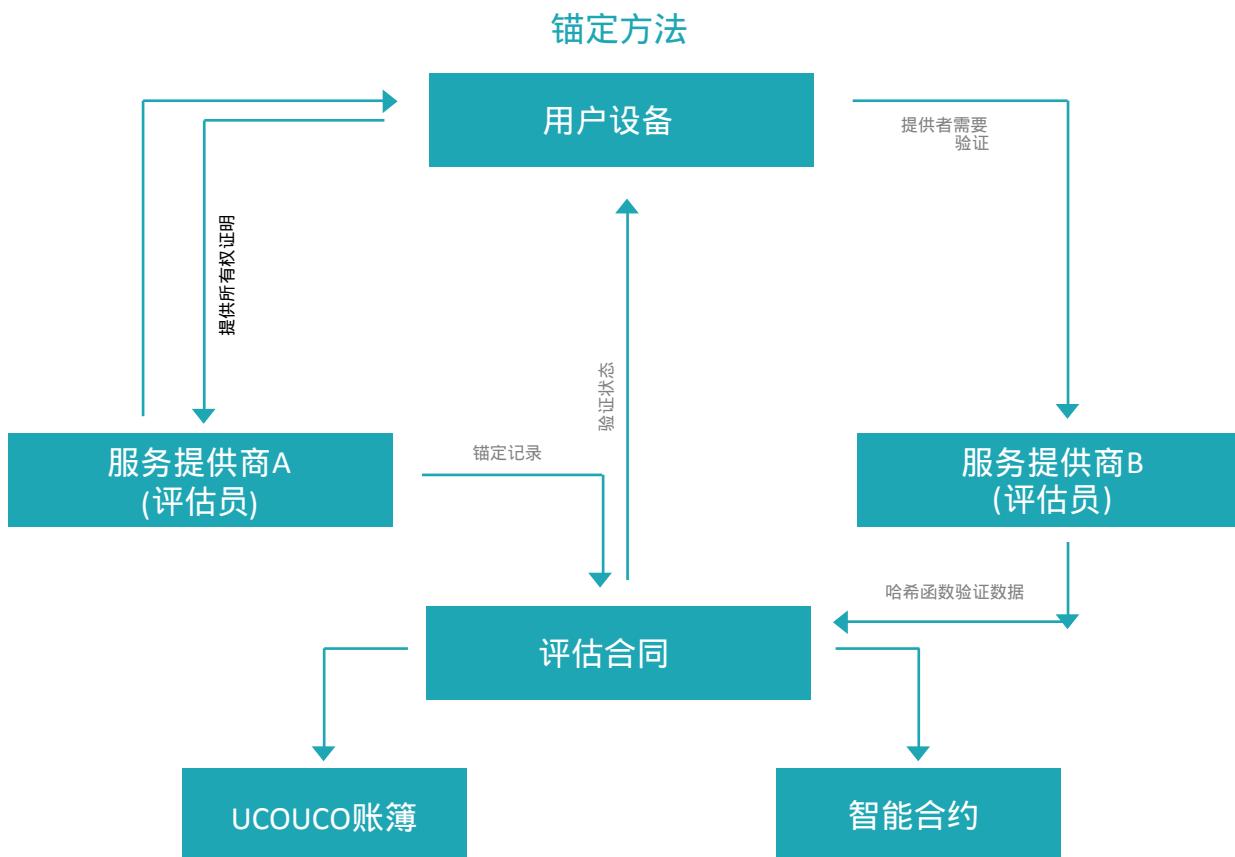


# 产品说明

## 锚定方法和机制

在下面的阐述中可以解释徽章处理和锚定到区块链。

- 当用户想要通过服务提供商A申请新服务时，用户通过VerifyUnion应用程序发起发送所需个人资料信息的请求。.
- 充当评估者的服务提供者A使用现有方法来验证用户的身份和信任，并根据给出的数据为用户创建社交分数。
- 提供商A对数据和“社交分数”进行哈希计算，并将其作为徽章处理的一部分锚定到区块链。然后，提供者A将把区块链交易的参考数值传送给用户。
- 将来，当用户向提供者B申请服务时，提供者B将向用户请求提供相关用于服务的数据。
- 如果用户同意请求，供应商B供应商B和用户将相互同意验证签字过程的评估者，假设它是供应商A.供应商A在供应商B可接受的过程中以UC代币提供价格，以及同意一个智能合约。
- 提供者A将使用提供者B想要在提供者A之前锚定的区块链上验证的哈希键来验证用户授权和交易细节。提供商B将使用哈希函数进行验证，如果它返回相同的值，则提供商B可以验证用户身份并按照智能合约的约定向提供者A以UC币的价格付款。
- 一旦在UC Coin中进行支付，用户就可以通过VerifyUnion的应用程序将所需的数据发布给提供者B.
- 交易完成后，用户可以使用应用程序完成交易，然后使用UC代币支付用户和评估者（即提供者A）所提供的服务，并按照智能合同获得付款。



# 强化安全验证

---

VerifyUnion在区块链上另外增加了两层，以确保用户的隐私，允许用户验证个人信息的共享。

使用的两个协议是：

## UNION智能锁

从历史上看，隐私危机曾经是由肇事者从登录领域和服务提供者的漏洞访问用户输入引起的。 Union Smart Latch图层通过获取登录表单上的最少的用户信息来提供全面的安全性。 当用户在注册期间被要求输入他们的电子邮件地址时，Union Smart Latch会从我们的认证服务器生成一个唯一的令牌，并将其传送给用户的电子邮件。 令牌生成一次，并通过特定的加密算法加密。 如果该令牌被黑客攻击，则由于静态令牌与动态令牌不匹配，入侵者无法访问用户信息，因此访问被禁止。

## UNION 智能引擎

所有客户的验证信息都由UNION智能引擎加密和压缩，存储在区块链网络和我们的专用服务器上。 当客户端从区块链请求信息时，我们的专用服务器将查找并加载该数据并运行可靠的双向验证。 提供的数据是匹配的，然后UNION智能引擎解密数据，并将交付给客户端。 当然，这将增强响应时间，并提供更快的结果和更好的处理时间。

# 强化安全验证

---

## 防御区块链受到攻击的支出

假设攻击者决定追溯修改使用工作证明（例如，比特币区块链）的无权限的加密货币区块链上的锚点。为了做到这一点，攻击者需要覆盖从包含目标锚点的块开始的区块链。根据工作区块链共识规则，攻击者需要产生一个替代链块，其中包含比正式维护者创建的更多累积工作证明。此外，攻击者需要保持他的版本的区块链秘密，直到它变得比网络的真实部分产生的区块链更好。普通的大多数攻击（例如，审查不是由攻击者产生的所有块）不会改变区块链历史，因此它不会完成攻击者的目标。

请注意，攻击会有明显的问题：

- 完整节点将保留攻击后诚实矿工维护的区块链版本。因此，现有的区块链用户（包括锚定区块链的用户）将能够验证攻击发生，大大减少了它在大多数使用情况下的效用（参见在印刷媒体上的锚定，成功的攻击将需要不明显的交换现有的媒体印刷问题）。袭击本身需要大量的准备工作，进一步削弱了暗中完成攻击的机会。
- 由于攻击非常明显，攻击者不太可能通过销售被发现的加密货币获得利润，因为攻击后其汇率可能会大幅下降。因此，目标区块链上的理智维护者不太可能支持这种攻击。

假设攻击从  $t = 0$  时刻开始，攻击锚点对应于  $t = -ta < 0$  (即,  $ta$  为锚定年龄)。当条件  $t < 0$   $h(t) = 0$  时，诚实的哈希率和攻击者的哈希率分别用函数  $g, h : \mathbb{R} \rightarrow [0, +\infty)$  来表示。我们进一步假设  $h$  和  $g$  都是单调递减的： $t h'(t) \geq 0, g'(t) \geq 0$ 。

攻击者链的初始累计难度差是  $\delta = \text{def} - ta \int_0^0 g(t) dt$ 。攻击在  $\tau$  时刻结束，攻击者链的累计难度达到诚实网络链的累计难度，即可用下式表达：

$$\int_0^\tau h(t) dt = \delta + \int_0^\tau g(t) dt. \quad (1)$$

$$J(h, \tau) = R + Ch(\tau) + O \int_0^\tau h(t) dt \rightarrow \min \quad (2)$$

# 强化安全验证

## 攻击成本

攻击成本包括三个因素：

- R，以美元计是运算哈希的设备生产中的弹性资本支出
- C，以美元计/(GH/s)，生产和部署一套运算哈希的设备弹性资本支出
- O，以美元计/GH，是维护一个运算哈希的设备单元运营开支

自然，R，C和O都是正数。

注意到(2)的积分部分可以用(1)简化，导致控制h的单边优化控制问题：

$$\begin{aligned} J = & R + O\delta + Ch(\tau) + O \int_0^\tau g(t) dt \rightarrow \min_{\tau, h} \quad \text{s.t.} \\ & \int_0^\tau h(t) dt = \delta + \int_0^\tau g(t) dt; \\ & h(0) = 0; \quad \forall t \in (0, \tau) \quad \dot{h}(t) \geq 0. \end{aligned} \tag{3}$$

我们不试图在通用情况下（这可以通过数字来实现）来解决这个问题，而是验证一个简单的部分例子。

### 假设 1

$h(t) = h$  在区间 $(0, \tau]$  是恒定的常量(即攻击者在初始设备采购之后开始攻击并且在攻击期间不增加设备的量)。

通过以下观察，可以证明向不变攻击者的哈希率的转变是合理的。

**陈述 1:** 恒定攻击者的哈希率  $h(t) = h^*$  在(3)中对任意给定的  $\tau$  是最优的。

证明：假设 5 种约束，则(1) 可以简化为

$$h^* \tau = \delta + \int_0^\tau g(t) dt,$$

从而导出

$$J(h^*, \tau) = R + O\delta + C\delta/\tau + (O + C/\tau) \int_0^\tau g(t) dt,$$

# 强化安全验证

上式只依赖于  $\tau$  而不依赖于  $h^*$ 。

由于  $h$  的不递减性

$$h(\tau) \equiv \frac{1}{\tau} \int_0^\tau h(t) dt \geq \frac{1}{\tau} \int_0^\tau h(t) dt = \frac{\delta}{\tau} + \frac{1}{\tau} \int_0^\tau g(t) dt. \quad (5)$$

将(3)中的  $h(\cdot)$  替换为(5)产生一个下界估计  $J(h, \tau) = J(h^*, \tau)$ ， $h^*$  被理解为一个常数函数。 $J(h, \tau) \geq J(h^*, \tau)$  持有 iff  $h = h^*$ 。

对于  $\tau$ ，最小化 (4) 中的  $J$ ，我们得到

$$\frac{\partial J}{\partial \tau} = \left( O + \frac{C}{\tau} \right) g(\tau) - \frac{C}{\tau^2} \left( \delta + \int_0^\tau g(t) dt \right) = 0. \quad (6)$$

陈述 2: 如果  $g(t)$  是连续的，则等式 (6) 在区间  $\tau \in (0, +\infty)$  上是唯一的解。

证明:

$$\lim_{\tau \rightarrow +0} \frac{\partial J(\tau)}{\partial \tau} = O g(0) + \lim_{\tau \rightarrow +0} \left( \frac{C g(0)}{\tau} - \frac{C \delta}{\tau^2} \right) = -\infty.$$

由于  $g(t)$  是非递减函数，

$$\frac{\partial J(\tau)}{\partial \tau} \geq \left( O + \frac{C}{\tau} \right) g(\tau) - \frac{C}{\tau^2} \left( \delta + \int_0^\tau g(\tau) dt \right) = O g(\tau) - \frac{C \delta}{\tau^2} > 0 \text{ with } \tau \rightarrow +\infty.$$

因此， $\partial J / \partial \tau$  在探索区间的末端有不同的标志，由于它是一个连续的函数，至少有一个点  $\tau$ ，使得  $\partial J(\tau) / \partial \tau = 0$ 。

接下来，观察 (6) 在  $\tau \in (0, +\infty)$  具有方程相同的解

$$\tau^2 \frac{\partial J}{\partial \tau} \equiv O \tau^2 g(\tau) + C \tau g(\tau) - C \delta - C \int_0^\tau g(t) dt = 0. \quad (7)$$

对方程 (7) 的左边变量  $\tau$  进行偏微分，得到：

$$\frac{\partial}{\partial \tau} \left( \tau^2 \frac{\partial J}{\partial \tau} \right) = (O \tau^2 + C \tau) \frac{\partial g(\tau)}{\partial \tau} + 2 O \tau g(\tau) > 0 \quad \forall \tau \geq 0,$$

# 强化安全验证

因为  $\partial g / \partial \tau \geq 0$ ,  $g(\tau) > 0$ 。因此，(7)的左边部分单调增加意味着(7)和(6)有且只能有一个解。这就完成了证明。

考虑真实哈希率函数  $g(t)$  的最简单实例：对于所有  $t$ , 常数  $g(t) = g_0$ ; 在这种情况下，攻击者的链条的初始障碍  $\delta = g_0 t_a$ 。等式 (6) 简化为：

$$\left(O + \frac{C}{\tau}\right) g_0 - \frac{C(\delta + g_0 \tau)}{\tau^2} = 0,$$

从中获得最佳的攻击持续时间  $\tau^* = \sqrt{C\delta/Og_0}$ , 和最优的开销。

$$J^* = \underbrace{R + O\delta + Cg_0}_{J_0} + \underbrace{2\sqrt{O\delta \cdot Cg_0}}_{J_{const}}.$$

费用的一部分  $J_0$  可以看作是诚实的矿工在时间  $t=0$  花费在锚安全上的费用,  $J_{const}$  是额外的惩罚。一个非常理想的特性是  $J_{const}$  可以和  $J_0$  相对比, 即花费在固定锚上的保护费用显著低于攻击它的费用 (图 1)。

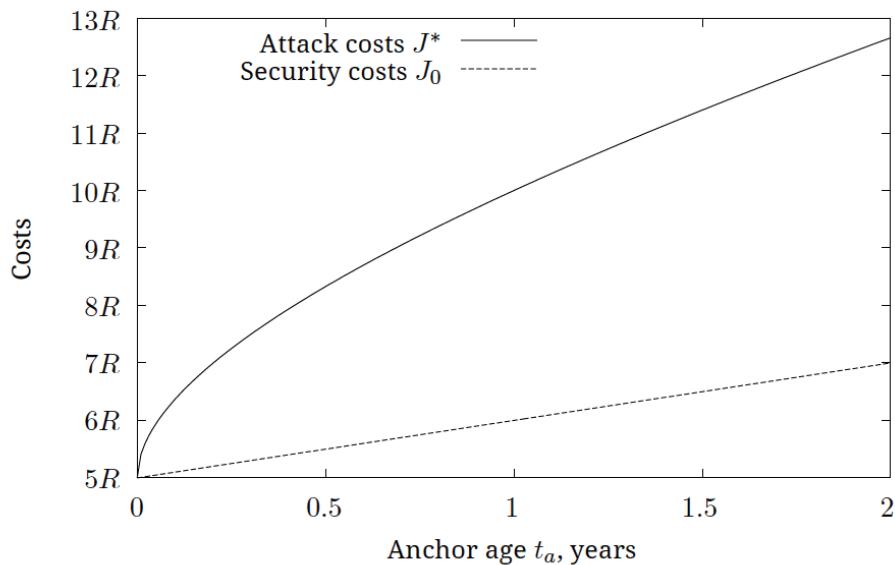


图1：用来攻击锚定一个具有静态诚实哈希率  $g_0$  的区块链的成本取决于锚定年龄  $t_a$ 。假定 (2) 中的成本因素是  $R = O g_0 \cdot 1 \text{ year} = C g_0 / 4$ , 这是由我们的估计接近于比特币区块链的因素的当前分布。

# 代币说明

## “UC Coin” – VerifyUnion的加密货币

VerifyUnion正在部署我们自己的代币，可以在我们的生态系统中应用。 UC Coin作为VerifyUnion平台中的一种付款方式，在奖励计划中用于支付我们的评估人员和用户。 这是由用户和评估者预先确定并同意的智能合同定义的，由“统一认证”参与者处理。

VerifyUnion 参与者。

在下一个发展阶段，VerifyUnion计划扩大其服务范围，并且当令牌需求增加，导致令牌价值更高时，用户可以将令牌卖给我们，从而使用户受益。



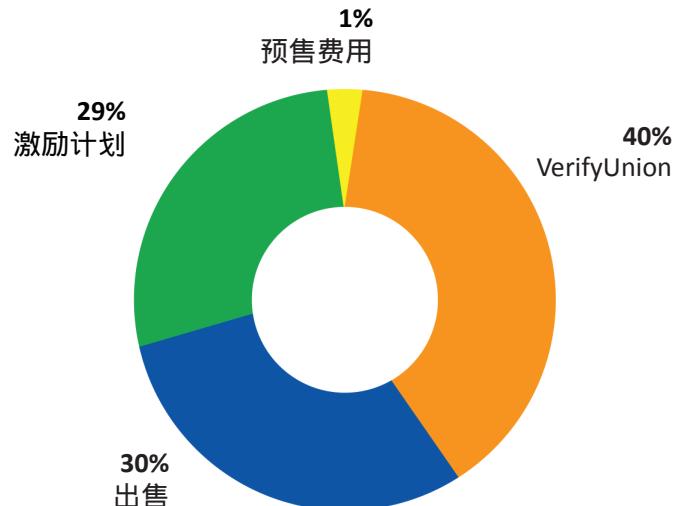
在初始代币发售后期间将创建固定数量的UC Coin，并且使用智能合约和区块链方法在参与者之间记录UC币的每次转账的分布式账本。 在生态系统中的多个平台上使用UC Coin，将使我们能够防止由于在广泛的生态系统中使用代币而导致的令牌价值的恶化。 奖励计划将通过奖励所有参与者，同时增加代币的价值，奖励的价值随着生态系统的增长而增加。

生态系统中还包含一个新的用户推荐计划，在该计划中，现有用户可以推荐给他人获得代币，新用户可以验证他们的个人资料并获得更多的代币。

## 代币销售分配

UCN代币总量:5亿

- 1% 用于预售费用
- 30% 用于出售
- 29% 被分配给激励计划
- 40% 由VerifyUnion团队保留



## 代币资金的存储

ETH will be stored in a multi-sig wallet

**CAP = \$30 MILLION USD**  
正常的代币成本(奖金将降低单价)

**1 UCN = \$0.1948 USD (approx.)**  
(奖金红利根据购买阶段添加在顶部)

**1 ETH = 1540 UCN (approx.)**

# 总结

VerifyUnion致力于通过部署一套经济高效的新系统来为我们的客户和用户消除数字身份欺诈，便于客户和终端用户使用验证和信任数字服务。 VerifyUnion将删除那些不必要的用于欺诈活动的个人用户数据存储，并消除对任何存在重大黑客攻击威胁的集中式系统的依赖。在 VerifyUnion平台上服务提供商可以降低用于验证用户所提供的服务的成本。 通过代币激励终端用户使用门户网站进行所有在线和数字服务的验证，终端用户并可以使用该代币作为投资，以便以后支付或在VerifyUnion的生态系统上使用。

用户可以完全控制他们正在经历的端到端流程，并且可以增强对他们所接受的所有服务的信任。他们会使用我们的社交分数增加他们的信任验证，同时赚取更多的代币。 通过拥有全部用户组合，提供商可以获得更广泛的图像，并授予更多的用户请求的服务，因为有更多的用户信任信息可用。

通过VerifyUnion可以显著降低在线欺诈率，用户哈希函数和所有权验证通过VerifyUnion的验证过程被验证，并且用户可以授权他们想要验证的所有信息来增加信任和社交分数。 当前ID欺骗的问题和各种社会概况使得欺诈行为将会大大减少，因为这很难绕过VerifyUnion系统。



# 公司

---

## 法律结构

**VerifyUnion** 私人有限责任公司 (201726332G) 在新加坡注册登记。

## 网络参与者

代币持有人 (全球性的，遵守当地的法律法规向所有人开放)

VerifyUnion基金会负责整体管理和监督所有代币，贡献以及其他收入流动，以保VerifyUnion网络的健康发展。目前，其董事会成员包括VerifyUnion运营公司的董事。

**VerifyUnion**有限责任公司是由基金会承包建设和部署核心分散应用的经营实体。

## 联系方式

VerifyUnion Pte. Ltd. (201726332G)

Email: info@VerifyUnion.com

101 Cecil Street, #11-04, Tong Eng Building, Singapore 069533

Web: <https://www.VerifyUnion.io>

# 团队

---

## 管理团队



### AJ SMITH- 总经理

AAJ Smith是一名商业战略家，导师，连续创业者，风险投资家，市场专家，金融科技经验丰富，并且在竞争激烈的市场中不断赢得高水平的业务。他毕生创办了20多个成功的企业，为数千人创造了就业机会。他还是新西兰科技公司Imperial Digital和Entisy的联合创始人，同时在全球超过12家初创公司（主要是金融科技公司）投资。他对加密货币，区块链和金融科技充满热情，经常被邀请担任研讨会小组成员。他已经退休了两辈子，总是因为下一次成功创业的热情而退休。



### KERRY FRIEND- 财务总监

Kerry Friend Kerry Friend是一位成就卓越的高级行政人员，具有强大的首席财务官背景，展现出商业智慧和领导才能，最近刚刚在亚洲工作了18年后返回新西兰。他最近的就业角色是他从头开始建立起来，并在新加坡成立了一家在美国上市的娱乐软件公司，在亚洲地区开展了重要的业务。在此之前，他控制了美国一家主要的美国媒体集团在日本的一个10亿美元的多频道电视合资企业的财务。

特许会计师（澳大利亚和新西兰）

董事学会成员（新西兰）

# 团队

---

## 技术团队



**SEUNG HYUN MYUNG**  
技术总监  
区块链工程师



**KWANGKUE AN**  
软件工程师  
区块链工程师



**THILAN PATHIRAGE**  
软件工程师



**SHRUTIKA SHEDHA**  
图形/UI设计师



**TIM ATAMBAY**  
软件工程师



**AISHA HANIF**  
软件工程师



**ZEESHAN NAVEED**  
数字专家

# 团队

## 顾问团队



### LEANNE GRAHAM- ex-Xero Rainmaker / SaaS Expert

新西兰少数IT企业家之一，也是NZX公司的首席执行官。以前的Xero国家经理，推动Xero从一个新的云产品成为全球会计软件标准。董事会职位：Velpic - 主席，认知委员会主席以及这些顾问委员会的角色：Nibo（巴西）- Cloud Accounting，Anfix（西班牙）- Cloud Accounting，Yudoozy（NZ）自由职业平台，Big -（澳大利亚）视频平台。



### NICK FITNESS- 金融分析师

Nick是投资顾问，股票经纪人和投资者。在英国和新西兰拥有超过10年的顶尖投资银行（Forsyth Barr，麦格理和摩根士丹利）的经验。他是一位授权财务顾问（2012年），以及新西兰证券交易所顾问（2013年）。尼克也是新西兰领导人的成员，指导领先的企业和寻求知识，网络和资本发展的初创企业。



### GREG SHARP- IT安全工程师

Greg Sharp 在英国和新西兰的IT行业工作了23年，是CISSP资深IT安全工程师，现在是位于新西兰奥克兰的Base 2公司的总经理。



### ROGIN THADATHIL- ICT业务分析师

Rogin是一位专注于基于区块链金融技术的ICT业务分析师。他拥有梅西大学（2016）的企业融资和战略银行硕士学位。在以软件系统工程师的荣誉毕业后，他将技术融入财务的愿景为他创造新的金融元素和晋升金融工程师的方式铺平了道路。

# 合作伙伴

---



Alpha测试合作伙伴



区块链开发合作伙伴



安全伙伴



# 社交媒体

---

开放和透明的相互沟通对于VerifyUnion Crowdsale的成功以及企业的持续发展至关重要。您的任何问题和建议欢迎在以下社交平台中询问和提议：



# 参考文献

---

- Ethereum White Paper - [http://www.the-blockchain.com/docs/Ethereum\\_white\\_paper-a\\_next-generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next-generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf)
- Ethereum Project – [Ethereum.org/](https://ethereum.org/)
- Mining? What Is Bitcoin. "What Is Proof of Work." Everything You Need to Know about Bitcoin Mining - 18 June 2015 - 09 Dec 2016.
- Blockstack. "Blockchain Auth" GitHub - 04 Dec 2016.
- Application of the Blockchain For Authentication and Verification of Identity Ben Cresitello-Dittmar. November 30, 2016
- The value of digital identity to the financial service sector - Bryn Robinson-Morgan, December 2016
- Investigating challenges in digital identity - report written by Gary Simpson & Emma Lindley south Yorkshire credit union & innovate identity
- The digital identity dilemma - [recode.net/2016/8/10/12413592/digital-identity-virtual-id-card-fido-web-api](http://recode.net/2016/8/10/12413592/digital-identity-virtual-id-card-fido-web-api)
- Establishing digital identity causing problems as users giving away too much - Ian Grayson: Oct 4, 2016
- How Safe Are Blockchains? It Depends. Allison Berke - March 07, 2017
- Are Concerns About Security and Privacy Threatening the Future of Online Commerce? - Mihaela Paun : Jun 02, 2016
- Digital Identity Issue Analysis Report v1.6 - 8th June 2016
- Identity fraud up by 57% as thieves 'hunt' on social media <http://www.bbc.com/news/uk-36701297>