www.hive.id

hive

基于区块链技术和代币的去中心化身份管理生态系统

执行摘要

最近更新日期
2018年7月9日

版
1.2

背景与愿景

互联网建立伊始，并没有标准的方法来识别个人和组织。自万维网面世以来，网站通过密码和用户名的用户验证解决了这一难题。从那时起，解决方案并没有发生太大变化，而万维网却发生了翻天覆地的变化 。

一个普通的互联网用户每天都会访问几十种服务。现如今，基于应用平台的方法（用户必须在与之交互的每个网站进行身份验证）已经彻底过时 。这种可用性灾难为黑客提供了盗取个人数据的温室。在这种情况下，身份盗窃行为对整个互联网服务生态系统的完整性构成了持续性威胁。

> **“互联网建立伊始，无法得知您与谁或什么建立了联系。这就限制了我们对它的使用，且使我们暴露在更多的危险中。如果我们什么都不做，我们将面临迅速增多的盗窃和欺骗事件，这将渐渐侵蚀公众对互联网的信任。”**
>
> *《身份法则》Kim Cameron*
> *微软身份总设计师*

自我主权身份为解决这一问题提供了三个要素：个人控制、安全性和完全可移植性。个人和组织仍然是他们数字身份的唯一所有者和管理者。因此，这些个人充当他们自己的身份提供者。没有第三方能够向他们“提供”另一个身份，因为身份本质上就是他们自己 。自我主权身份的数字化存在与任何组织无关。

自己全权控制的数字记录就是自我主权身份的最大表现。自己可以完善更多的数据，或者请他人代为执行。

只有您能决定您想透露的内容以及具体透露的时间。您可以记录您同意与他人共享数据，并促进共享。这一操作具有持久性，且不涉及任何第三方。在身份交易中对您的声明可由您自行证明或由第三方证明。

为了建立互联网身份层，还需一种新的可信基础设施。要求此设施允许身份所有者共享他们的数字化身份和已验证属性，以及管理许可并记录同意。

问题与挑战

数字存储和共享信息功能存在很多好处，因此已经成为一种日益增长的趋势。然而，除了成本和便利性的优点之外，一系列新的问题也浮出了水面。

数据所有权

绝大多数互联网身份通过中心化方式进行管理。这意味着所有此等身份由单一实体（如电子商务网站或社交网络）拥有和控制。

安全性

组织存储、管理和保护大量用户数据的成本随着负债的增加而增加。然而，安全性无法永远保证，用户不断成为数据泄露的受害者。

信任

数字商业的真正货币是信任。消费者自身的几十或上百个信息碎片分散在不同组织中，自身却无法对其进行控制、更新或保护。

用户体验

用户在使用另一个网站或应用程序时，经常要求输入与想使用的其他50个服务输入的相同信息。此外，他们还需记住所有的用户名和密码。

我们发现目前身份管理存在以下4个问题：

- **数据所有权**
- **安全性**
- **信任**
- **用户体验**

&

2017年，共有1670万名身份欺诈受害者，继前年的最高纪录之后再创新高。去年被盗金额达到168亿美元，同比增加12%。

2017年的账户侵权事件是2016年的三倍，亏损总额达到51亿美元。

2017年的大部分数据泄露对商业部门造成了影响，商业泄露事件达到了泄露总数的55%，其次是医疗/保健泄露，占23.7%，再者为银行/信贷/金融部门泄露，占8.5%。商业部门的泄露事件数量连续三年占据第一。

53%的客户放弃了交易：因为1）缺乏可见的安全性，2）帐户设置需要过多的信息和3）一次性购买需强制创建帐户。

HIVE解决方案

Hive是一个完整的自我主权身份管理解决方案，建立了企业和消费者之间的关系系统。

它的目的是创造，管理和保护消费者的独特主权数字身份，同时满足企业的需要：能够承受的KYC/AML合规性、综合客户尽职调查机制、欺诈预防、账户侵权预防、帐户和促销泛滥等。

通过集成一种创新机制来存储标识符、密钥、指针和证明，而不依赖于中心化的大机构，从而使得个人和组织能够处理一系列事务以可靠地证明他们的身份。

消费者利好

- 全权控制身份
- 许可准入的最少披露
- 使用假名与安全性
- 代币化忠诚计划
- 内在解决方案

企业利好

- 提高转化率
- 全球网络信任
- 捕捉所有欺诈和滥用踪迹
- 最小的监管暴露
- 不变性、透明化

主要优势和特殊功能

身份验证

通过Hive用户可以构建多个级别的数字身份。首先，在初始注册期间，他们创建他们的在线法律身份并通过 Hive供应商验证索赔(即PII，包括护照，驾驶执照，出生证明等)。根据不同司法管辖区的业务要求，将需 要不同类型的身份验证。例如，在远程开立银行账户时，德国需要与申请人进行视频采访，作为其身份验证 过程的一部分。

同时，虽然网络上的许多索赔只能通过供应商进行验证，但一些 索赔可能会进行自我验证。例如，电子邮件 和电话号码。自我认证的要求是识别的主要层面。它们用于在向Hive生态系统中的企业进行注册的同时更快 地注册，获得KYC合规性和CDD协议。使用法定身份，客户可以在与企业互动时管理其个人身份信息访问的 权限，并在互联网上安全地自我识别身份。

教育验证

这个概念随着新型供应商的增加而发展，这些供应商能够验证用户的教育证书和学术成就。因此，用户可以 获得安全存储更高级类型个人信息的更复杂的保险库。借助Hive，在线和离线教育机构可以成为供应商，以 验证其学生的现有凭证，并 供数字证书，文凭等，并通过Hive区块链验证。我们相信，获得证书便携和不 可变的技术将影响世界各地教育系统的发展。此外，拥有不变的凭证作为其数字身份的一部分将有助于在需 要可靠的专业技能检查(如求职，学术和高等教育应用等)的情况下分享这些凭证的过程。借助Hive，用户 的数字身份保险库有望彻底改变面试应用程序的执行方式。与通过电子邮件发送文件相比，申请人只需简单 地让企业访问由教育机构直接捐助形成的专业档案，由供应商验证并存储在不变的分类帐上。

就业筛选

要完成他们的数字身份，用户将能够验证他们的工作经验，存储就业参考资料，并要求供应商 供就业筛查 服务(包括背景检查，驾驶记录，药物和健康检查等)，以向其个人资料添加相应的证明。这将使他们能够 在工作申请过程中轻松地为任何企业供所有必要文件的访问权限。此外，Hive还将推出一项功能，允许拥 有经过验证的凭证的用户相互认可。与流行的专业社交网络形成鲜明对比的是，该服务消除了操纵配置文件 伪造背书的风险。如果用户希望将Hive用作所有个人，专业和教育证明的安全保险库，以保持100%负责所共 享的数据，那么用户将被激励为其配置文件添加尽可能多的验证声明。此外，Hive用户每获得企业的批准请 求，就可以获得IDCoins的先前已核实的索赔。

主要优势和特殊功能

身份保护

为保护已建立的数字身份，Hive市场上将 供身份保护服务。当涉及到身份盗用保护时，对用户造成的后果 可能非常有害。通常情况下，冻结信用是不够的，因为小偷仍然可以在黑暗网站上出售你的信息，用于开设 新帐户，并且更多地消耗它们。
有四分之一的人遇到数据泄露。
受害者包括老人，工作的成年人甚至孩子。
Hive Identity Protection将 供以下服务(视某些国家/地区的可用性而定):

- 地址更改验证 – 监控USPS中与用户身份相关的地址更改请求。
- 黑暗网络监控 – 监控服务，以通知用户数据是否 供销售。
- 信用监控 – 监控信用档案中的关键变化，并 醒用户检测欺诈行为。
- 数据泄露通知 – 监控各行业的大规模违规行为，以通知用户并帮助他们保护他们的身份。
- 年度信用报告和分数 – 从Hive Vault中访问用户的年度信用报告和信用评分。
- 保险保障套餐 – 涵盖身份盗用的保险政策。
- 全天候客户支持

Hive防欺诈和机器学习

Hive正在为企业解决的核心难题之一是客户尽职调查流程，该流程引入了内部评分系统来对网络上的帐户进行评级。我们将此功能视为一种实施工具，以创建共享的知识库，帮助企业节省大量的欺诈活动资金。
欺诈是互联网上可扩展的可编程操作，我们相信只有在互联网的身份层得到改善的情况下才可 以控制欺诈。Hive网络上的所有业务都能够标记滥用其协议的用户。由于Hive用户只能在网络上创建一个帐 户。因此他们只有一个信誉栏。这种方法有助于防止欺诈活动的扩展。
此外，企业还可以与Hive Fraud Prevention共享用户生成的事件，例如创建内容(评论，列表，消息，帖子， 个人资料，评论)，Chargeback，登录，注销等，以便进一步进行机器学习分析，以识别不寻常的行为模式 并通知企业有关潜在威胁。Hive是针对不同类型欺诈的单一智能解决方案。

帐户接管和滥用

促销滥用

声望和评分方

技术：如何将身份和区块链有机结合?

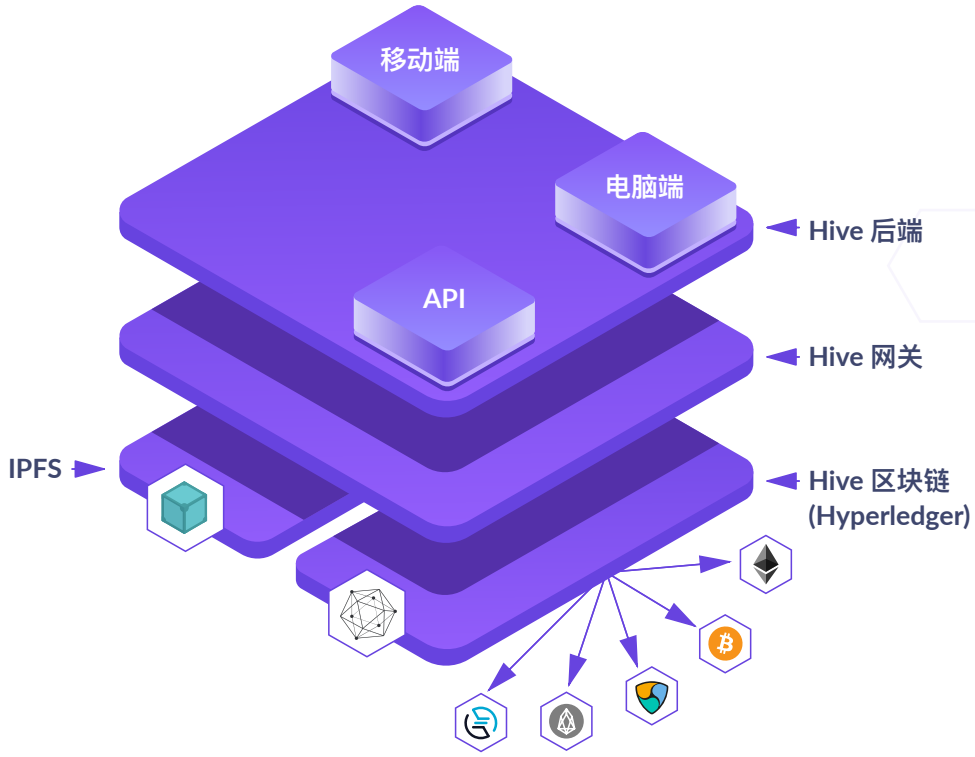
Hive提供了一个数字身份管理生态系统，个人可以通过下载Hive应用程序，在自己的设备上建立他们的数字身份，并验证身份信息成为Hive用户，从而实现访问。一旦完全验证，对该数据的证明将被Hive写入区块链，数据接收方可以来验证其真实性和所有权。

Hive Vault使用由用户自己生成、提供和控制的分层确定性密钥，使用高级加密，安全地存储设备上的所有用户的个人识别信息（PII）。Hive不会以任何方式处理PII的存储，数据只存储在用户自己的设备上。

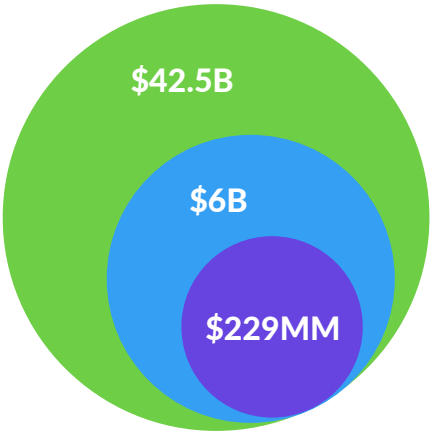
Hive业务伙伴可以用Hive Vault扫描定制的二维码来请求获取用户信息。用户可以扫描二维码，准确地查看对方请求哪些信息，并选择批准或拒绝这一请求。然后使用非对称密钥加密以及预期接收者的公钥在用户和请求方之间执行交换，这样一来，只有它们可以进行解密。

Hive使用混合区块链模型 – “私人许可”账本（定期锚定在公共账本上）建成，这样便可提供两全方案：公共访问和可信治理。第一个区块链存储已经验证的声明并控制对身份记录的访问，此区块链使用超账本Fabric构建。第二个区块链可以是任何公共区块链，可对其进行已经验证的声明的定期锚定，以确保数据完整性（以太坊、比特币、EOS、NEM等）。一般来说，解决方案是以区块链平台无关性为基础建立，为未来的不断发展和新兴的区块链技术创新提供依据。

代币化是使用以太坊网络上的ERC20代币标准完成的。



市场与策略



- **TAM – $42.5B (2023 – $88B)**
  - **身份管理 – $20B** (2023 – $30B, CAGR – 8.45%)
  - **身份验证 – $13B** (2023 – $40B, CAGR – 25%)
  - **身份保护 – $6B** (2023 – $12B, CAGR – 15%)
  - **使用筛选 – $3.5B** (2023 – $6B, CAGR – 11.45%)
- **SAM – $6B**
- **SOM – $229MM（3年内），$603MM（5年内）**
  - **第1 年**- $29MM　**第 2 年**- $111MM　**第3年** - $229MM
  - **第 4 年**- $402MM　**第 5 年**- $603MM

TAM – Total Available Market 产品的潜在市场范围

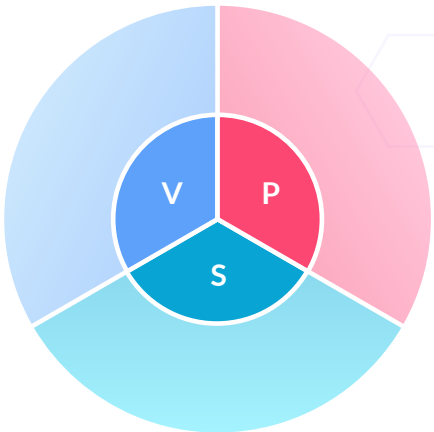
SAM – Serviceable Available Market 可服务市场范围，指在我们地理覆盖范围内对我们产品可服务的市场范围

SOM – Serviceable Obtainable Market 可获得市场范围，指在我们可以服务的范围内我们实际可以获取的市场

关键价值定位

进入市场策略

- 利用现有的和发展新的战略伙伴关系来启动和发展身份验证业务
- 给予奖励，为用户和服务提供商创造强大的激励机制，以使其加入并继续使用这一平台
- 向现有用户增销身份保护和使用筛选产品
- 不断扩大身份验证和发展新的战略伙伴关系，以扩大身份保护和使用筛选业务



交易额
3年-$229MM
5年-$603MM

代币量
固定-$25MM

代币生成事件

名称

Hive ID (HID)

总供应

700 000 000 (永远不会产生新的代币)

代币价值

1 HID = 0.10 美元

软顶

5 000 000 美元

硬顶

25 000 000 美元

未售出代币

所有未售出的代币都将被销毁

主要交易所上币

2018年第4季度

大户奖励

承诺在代币销售期间以等于或大于500,000 HID的金额购买代币的购买者将有资格获得奖金。所有此类奖金都将与每名潜在购买者单独讨论商定。

资金使用

- **15%** 研发
- **5%** 管理与运营
- **10%** 储备
- **7.5%** 法律与合规
- **45%** 销售和营销
- **10%** 国际扩张
- **7.5%** 收购与伙伴关系

代币分配

- **10%** 团队
- **5%** 顾问与赏金
- **20%** 储备
- **65%** 销售和奖励

发展蓝图

2017年第3季度

【过程】观点启动与市场分析

2017年第4季度

【过程】区块链可扩展性问题研究

【过程】平台启动核心的开发

2018年第1季度

【过程】原型发布

【过程】美国特拉华注册公司

【过程】种子轮：筹集350 000美元

2018年第2季度

【过程】Alpha版本发布

【过程】区块链技术定型与集成

2018年第3季度

【过程】 Beta版本发布

【过程】公共应用程序发布（IOS、Android）

【过程】其他国家的专利申请

【产业】流行平台和框架的身份验证插件（Shopify、Wordpress、Passport.js）

2018年第4季度

【过程】多国语言支持

【过程】使用确认与甄别

【过程】教育与专业技能认证

【产业】使用软件集成（Lever、Greenhouse、TriNet、ZipRecruiter）

2019年第1季度

【地理】扩张到加拿大

【过程】开发者社区建立

【产业】自动售货机及专业自动柜员机

2019年第2季度

【地理】扩张到亚洲

【过程】第三方开发者SDK发布

【产业】第三方身份验证解决方案集成（Auth0、Okta、Duo Security）

2019年第3季度

【地理】扩张到向欧洲

【产业】企业市场解决方案（MFA、SSO、AD）

【产业】专用金融科技解决方案

2019年第4季度

【过程】第三方应用程序市场推出

【产业】机器对机器身份验证集成（物联网设备）

团队与合作伙伴

Kostiantyn Shterental
联合创始人兼首席执行官

Yuriy Znatokov
联合创始人兼首席技术官

Kyrylo Sopot
业务发展副总裁
（拉丁美洲）

Yevgen Yurash
业务发展副总裁
（亚太地区）

Alena Yudina
业务发展副总裁
（欧洲、中东和非洲区）

Ivan Arabadzhy
高级用户界面/用户体验设计师

Sergei Poznanski
领先后台架构师

Artem Mirchenko
领先前端与软件开发工程师

Sergey Zenkov
高级区块链开发人员

Alexander Ivanov
首席研发官

顾问

Gary Baiton
增长黑客

Ismail Malik
区块链研发、战略家

Colin Breeze
高级法律顾问

Andrey Verbitsky
代币建筑师

战略合作伙伴

JUMIO　GoodHire.　HYPERLEDGER　THE LINUX FOUNDATION　ENQ ENECUUM

Intercoin　POPCHEST

代币生成事件伙伴

SOLUTIONS　CRYPTO LAWYERS CORPORATION　modern token　ICO bazaar crypto market insight