



Hub

人类信任协议 - **Human Trust Protocol**
“信任，是新经济的货币”- **Rachel Botsman [1]**



作者: **Eric Ly, Rich Miller, Miko Matsumura**
翻译: **Henry Yan**



概述

互联网应用为全球数十亿用户提供了前所未有的机遇，通讯(messaging systems)，在线社区和社群（online communities），社交网络（social networks），和点对点电商 / 共享经济（peer-to-peer marketplaces)等为无数的应用场景赋能，比如内容分发（content），相互连接（connect），和电子商务 [Commerce]等。虽然这些应用软件可以让人们可以在虚拟世界与更多的用户产生互动，但是，因为陌生人之间缺乏一种虚拟化的信任 (Virtual Trust), 互联网有非常大一部分的经济价值仍无法实现。

区块链和加密货币技术的发明，创造了“价值互联网” (Internet of Value)这一机会[2] - 这个基于智能协议的系统不仅能传输信息，还能传递代表经济价值的单位 (units of economic value)。这些技术让去中心化的网络(Decentralized networks) 保持共识状态，同时通过交易代币 (token)来激励所有用户一起共同增加此网络价值。区块链技术通过保护网络免受恶意攻击, 和激励有价值的贡献，产生了经济网络效应，从而实现快速扩张。

Hub人类信任协议是人类历史上首个通过区块链技术实现, 针对虚拟化信任（virtual trust）的解决方案。这是一个无处不在的信任覆盖层，覆盖在不同的网络应用上, 帮助用户评估可信任度。Hub制定了人类信任协议（Human Trust Protocol），并提供了可验证的, 便携式的信任机制，使人们可以在互联网应用中用到这一信任，为用户在与陌生人互动时提供“远程信任”（trust-at-a-distance）。



1.Hub代币可以激励用户, 通过完成任务的表现和结果产生声誉数据 (reputation data), 从而激励他们做出更多有利于增强互联网信任的行动。

2.用户在交互，执行任务时可以拿出Hub代币作为“信任股份”，任务执行的结果好坏会影响这些“信任股份”的重新分配。

3. 用户的所有声誉数据将会以不可篡改的方式保存在公链上（public blockchain），这上面的声誉数据，信任档案可以在别的应用场景安全地使用。



4. 成立一个任务的应用商店（Task “app store”），来激励社区的开发者来开发新种类的任务，从而支持多样化的交互体验。在这些交互中，信任尤其重要。

1	市场现存痛点	5
1.1.	Dunbar常数和远程信任	5
1.2.	劣质的信息，和信息超载	6
1.3.	交易风险	6
1.4.	数据拥有权中心化，数据的不完整性，缺乏可携带性能	7
1.5.	从LinkedIn复盘的经验	7
2.	信任的原则	7
2.1.	声誉	7
2.2.	身份	8
2.3.	信任	9
3.	人类信任协议的愿景	9
3.1.	远程信任的价值	9
3.2.	信任度必须可被验证	10
3.3.	信任应是便携，可移植	10
3.4.	声誉数据的用户控制	10
4.	人类信任协议的定义	11
4.1.	协议架构	11
4.2.	任务	12
4.3.	信誉档案	13
4.4.	任务商城	13
4.5.	钱包	13
5.	数字货币经济学	13
5.1.	信任股权	14
5.1.1.	信任股权实例	14
5.1.2.	信任股权的经济学基础	16
5.1.3.	信任股权要求	17
5.2.	仲裁员，法官和争议	17
5.3.	任务和信任股权的标准化	17
5.4.	激励信任	17
6.	Hub数字货币	18
6.1.	用户使用场景	19
6.2.	全节点的使用场景	19
6.3.	任务开发人员的使用场景	19
7.	股权奖励	19
8.	任务分类示例	20
9.	攻击和防御	23



9.1.	共谋	23
9.2.	不诚实评估者，和可变用户	24
9.3.	不诚实的代币挖掘行为	24
10.	信任评估人员	24
11.	Hub 应用软件	25
11.1.	社群	25
11.2.	通讯产品	25
11.3.	交易	26
11.4.	安全和隐私	26
11.5.	人类信任协议与Hub应用软件的结合	27
12.	分布式信任网络的定义	27
12.1.	数据结构	27
13.	任务模版定义	28
13.1.	数据结构	28
13.2.	协议	29
13.2.1.	实例化	29
14.	任务定义	29
14.1.	合约	29
14.1.1.	结算	29
15.	信用档案定义	30
15.1.	数据结构	30
15.2.	合约	30
15.2.1.	映射	34
15.2.2.	验证	34
16.	任务商城定义	34
16.1.	数据结构	35
16.1.1.	添加更新	35
16.1.2.	搜索	35
17.	任务模版示例：发讯息	36
17.1.	数据结构	36
17.2.	合约	36
17.2.1.	举出实例	36
17.2.2.	接受	37
17.2.3.	解决	37
18.	任务模板示例：发布工作	38
18.1.	数据结构	38
18.2.	合约	38
18.2.1.	实例创造	38
18.2.2.	添加推荐人	39



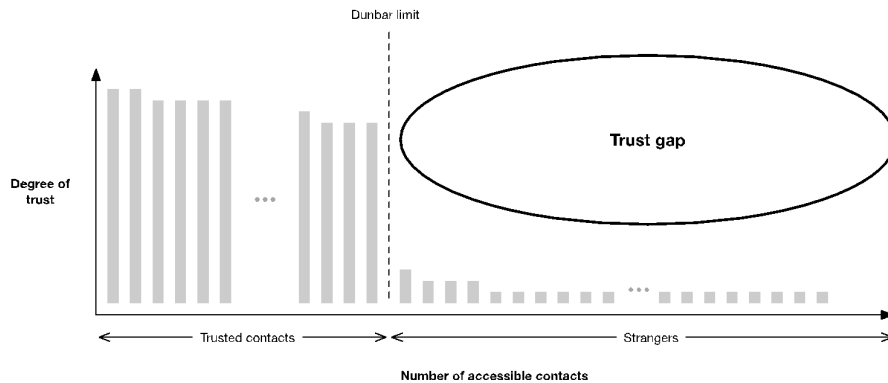
18.2.3. 结算	39
18.3. 争议	40
19. 未来的工作	40
19.1. 构建有效信任评估的任务分类法	40
19.2. 信任风险值默认值的计算	40
20. 结论	41
21. 致谢	41
22. 参考文献	41

1. 市场现存痛点

社交网络，点对点电子商务的快速、大规模的中心化导致了一系列有关陌生人之间进行互动，物品 / 服务交易的信任问题。每天有数以千亿计的陌生人在发生互动。至于交易，有报道估计在2020年之前，每天在互联网上产生的交易会达到四千五百亿。[3] 在这些场景中，如果没有信任的存在和共识，将会导致大量价值（互动，交易）流失，不良后果的可能性增加，成本和过程阻力增加。随着越来越多的人使用及依靠互联网，因没有信任而产生的各种挑战会变得越来越严重。

1.1 Dunbar常数，和远程信任

有一种方法可以让我们直观的理解这个问题-Dunbar常数提出了关于稳定人际关系的认知上限。人类学家Robin Dunbar[5]的理论认为，一个普通人最多可以保持150个社交关系，这个理论被成为Dunbar常数。一个用户最信任的社交网络圈子将会是此用户最宝贵的（一些情况下，最有经济价值）的互动圈。虽然互联网的来到让我们可以接触到的人增加到数以十亿计，但是互联网目前为止没有很好的解决陌生人之间的信任问题。这样导致了用户在和陌生人产生互动，网络交易时面临着很大风险。



智能合约的发明者，Nick Szabo，将比特币的价值定义为“一种可以超越距离传递的价值”[6]。但是，在一个去中心化的价值网络中，有一个很大的问题 - “远程信任”。是否能够成功的超越距离传递价值，在本质上取决于能否很好的解决“远程信任”这一问题。这里提到的远程并不是地理上的距离概念，而是信任程度。为了完善去中心化的这一愿景，远程传递价值的能力不可或缺。

1.2 劣质的信息，和信息超载

许多网络世界的互动，由用户分享信息开始。信息帮助人们决策，但是劣质的信息和不可信任的信息源会导致不良的决策。一个例子便是最近社交网络对于最近政治选举的影响。社交网络上有很多心术不正的投机者，比如垃圾信息发送者，他们以欺诈，假新闻和假广告的形式提供低质量信息。电子邮件是最大的消息平台，拥有37亿用户[7]，每天消息量为2260亿[8]，但它也是最缺乏用户之间信任的消息平台。因此，如今一半的电子邮件流量都是垃圾邮件[9] - 由于消息创建和传输的成本非常低，大量不必要的垃圾信息，让低质量信息的出现成为可能。垃圾邮件这一问题为邮件过滤软件和邮箱自动化创造了机会。检测安全威胁所花费的时间，精力和成本是一个巨大的市场，包括保护专有信息的泄露，并防止有害信息的渗透。这些本身就是一个巨大的行业，可以考虑为是一种用互联网工具的“税收”，而此带来的正面边际价值不断减少。

1.3 交易风险

有关交易的决策受信息影响，对信任的需求也更大。随着在线交易的需求增加，越来越多的系统，特别是成功但比较旧的系统，最有可能对依赖于它们的用户造成损害。当今用户的交互和交易更多是“线下” (off-platform)和“链下” (off-chain)的- 用户越来越多地使用电话会议，和见面会议来交易并希望他们的假设某种程度上会得到满足：相关的风险和高成本得以减轻风险某种程度上会得到满足。



1.4. 数据拥有权中心化，数据的不完整性，缺乏可携带性能

即使有些现存的软件（比如一些P2P电商）存在信誉系统，这些信誉数据只是被这些程序公司所拥有，不能实现对外的价值，或者网络效应的价值。用户在不同软件上的评论和数据，比如Yelp，Quora，Reddit，StackOverflow等，都不能被其他平台所利用。略有反讽意味的是，一些越是成功的共享经济应用，向外界共享他们平台数据的可能性越小[10]。随着这些共享经济应用在过去十年中的普及，这些平台所有者已成为用户声誉数据的实际管理者。因此，数据的所有权和使用权已经远远地从个人转移到中心化机构。用户在多个应用程序中的声誉数据的不完整化，碎片化则是另一个结果。通常，要获得对陌生人声誉信用数据的全面了解，需要进行繁琐的尽职调查，这涉及到对分散在不同互联网应用上信用数据的组装和比较，这些拼图往往不完全可靠。此外，即使用户已经投入了大量努力来培养在一个社区中的信用，现在也没有任何机制能将该信用转移到另一个社区。加入新社区，意味着信用数据只可重新开始。

1.5 从LinkedIn复盘的经验

我们自从创立LinkedIn以来（领英LinkedIn，全球最成功的，拥有超过5亿用户的职业社交网络）[11]，获得大量的第一手经验。尽管这一社交网络已有较高连接性，缺乏信任仍然会阻止大量有意义的互动有效地发生。例如，职业档案造假，职称造假，就业时间造假，学位造假等[12] [13] [14]。此外，有用户会用垃圾邮件，和社群中的自我推销帖子滥用用户社区。回想起来，现在仍然很难设计出能解决这些恶意用户活动，和失信行为的方案。这些缺陷不但减少了用户之间的信任，也会对商业产品本身产生危害，因为限制了广告定位的有效性，和工作机会的相关性。这些问题也以不同形式存在于其他社交平台上。

2.信任的原则

我们在协议的框架下，讨论信任和其相关术语，声誉和身份。在讨论信任之前，我们首先将信誉和身份作为基础，因为这两个领域都有很多研究，以往有系统试图解决这些问题。

2.1 声誉

声誉是由社区通过一个人过往行为的历史而决定[15]。声誉数据能将这种知识以数字形式来表示，并且是一种可以让用户预测别人未来行为的一种数据资源。[16]提供了迄今为止对市场上信誉系统的较好总结，他们创建在一些最成功的点对点交易系统上。在许多情



况下，这些程序通过映射计算并将大量数据计算成一个信誉评分，让用户更直观解读信用评分。信用评分例如FICO [17]和芝麻信用[18]则是众所周知的例子。

在协议的框架中，声誉（reputation）是多方面的，很大程度上据情景而定。因此，定义一个普遍所有场景的“信誉评分”并不可行，也不可能只有一个单一的定义。例如，一名运动员在足球比赛中赢得很多分可能被认为是成功的，可以普遍推测他是一名出色的运动员并具备良好的团队合作能力，但他们在打网球时也许并不出色。因此，这个协议将用户的信誉数据（reputation data）定义为记录用户实际行为的，不可篡改的历史记录。声誉通过执行任务产生。

执行任务的结果（outcome）是构成用户声誉数据的重要组成部分。用户单独执行的项目并不会成为声誉数据；但是，完成受其他人赞赏的项目则会创造声誉数据。结果由参与者仲裁，或是仲裁员和法官，或是通过算法手段来判断。结果取决于任务种类，可以由接受（acceptance），拒绝（rejection），评级（rating）或评论（review）的形式表达。根据具体的任务，结果会被相应形式表达。

Hub人类信任协议的目标是获取丰富和原始的信誉数据，通过这些数据，客户端应用程序可以让用户更好地懂得可信任程度（trustworthiness）。

2.2 身份

信任是根据个人身份进行评估的，是Hub协议的必要基础。随着分布式账本技术，和提供电子身份服务中性化系统的出现，关于去中心化，更安全，自主控制身份（self-sovereign identities）[19]的工作正进行展开。身份系统方面的工作仍然是一个竞争激烈和不断发展的空间，新标准将会出现。（例如，请参阅[20]。）如今，身份系统还支持多个角色和匿名使用场景。然而，即使是更强大的身份系统也不能完全实现远程信任（trust-at-a-distance）。不幸的是，即使怀有恶意的不良行为者能被系统识别出来，他们总是会存在的。身份不是Hub协议的原生数据，我们会通过将身份与声誉数据产生关联来实现远程信任。每个帐户将使用开放式数字身份标准（如[21]，[22]和[23]）来引用身份。我们将特别考虑由uPort [24]和Sovrin [25]等组织提供的自治主权身份标准。SSI与远程信任有高相关，因为SSI提供了一个可验证身份证明的体系，这些身份是由教育机构（如学位）和政府机构（如驾驶员许可证）等可信赖机构发布。此外，中心化系统提供的身份可以附加在SSI上。（例如，用户可以将他们的SSI与经过认证的LinkedIn帐户相关联，可被赋予一定数量的声誉数据。）这些身份声明与声誉一起打造了可评估，可征信的基础，并且系统会加入可以分析身份声明和信任声誉的方法。



2.3 信任

信任是一种对未来行为的预测。为了帮助预测，并实现“远程信任”，人类信任协议提供了评估用户能力和意图的方法。能力可通过用户的声誉数据来评估，即他们是否已经成功完成了他们将被要求做的任务。意图是执行未来任务的动机。即使用户拥有能力，但缺乏意图，他们也不能被托付来做未来的任务。

我们用上述概念来激励我们的解决方案，在该方案中，我们构建了一个由Hub协议打造的去中心化的，分布式信任网络。此网络本身可以被认为是对于人类未来行为的一个去中心化预测市场。类似于Augur作者表达，去中心化的价值所在，在人类行为这一背景下，改变了人们接受和验证他人可信任程度的方式[26]。

3.人类信任协议（Human Trust Protocol）的愿景

设想一个世界，互联网上陌生人之间的互动和交易由人类信任协议启动的新信任交互层支持。用户拥有声誉数据的自主权。只要有适当的许可，任何人都可以评估即将与他们产生互动的人的相关可信度，并且用户可以将他们的声誉数据和信任度从一个社区，转移到其他任何社区。总之，这是一个可以重新改善社交网络和共享经济服务的机遇，改善其基本激励机制，来创建更加值得信任，可靠的互动。我们将概述此协议的主要原则。

3.1 远程信任的价值

大规模创建远程信任（trust-at-a-distance）可为互联网带来更真实的内容，更可靠的交互和可靠的交易。信任会在现实社区中创造更多的经济机会，这在数字和虚拟化交互中也是如此。随着互联网上数十亿日常交易的进行，拥有更高信任度和声誉的人和企业将获得超越竞争对手的显著优势[27]，从而：

- 获得更多的机会
- 提高他们的产品和服务的市场价格
- 获得更多合作机会

简而言之，更大范围上产生超越距离的人际信任，可以让机会更加民主化，使真正的人才能够跻身到顶端。对于企业，远程信任能够赋能他们的所有商业互动，交易，并帮助他们与其大量的客户和合作伙伴的建立信任。



信任，声誉系统和共享经济领域的领先专家Rachel Botsman，在2012年的TED演讲中描绘了一个愿景：“在不久的将来，我们完全能够对一个人进行类似Facebook或Google的搜索，并看到随着时间的推移，不同情况下对某人行为的描述。我设想一个能够实时看到的信息流，可以看到谁信任过你，何时，何地，为什么信任你，你在TaskRabbit上的可靠性，作为客人在Airbnb上的租房整洁程度，以及你在Quora平台上展示的知识。他们都会一起保存在一个地方，这将存在于某种声誉和信任度的仪表盘上，绘制一张关于你声誉和信任度的蓝图。”[28]

3.2 信任度必须可被验证

可验证性意味着信任的规模提升，因为用户能根据可靠的信息源验证信任度。信任应该通过两种方式进行验证：（1）若获得披露的许可，构成信任度的互动记录可供其他用户查看；（2）交互的结果已经由过往活动的参与者验证（拥有数字签名），并且不可篡改。这些数据不会被用户单方面声称（或修改）。

3.3 信任度应是便携，可移植

用户的信任必须有便捷性，和可移植 / 跨界性，可从一个应用程序移植到另一个程序。能代表信任度的交互可以跨界多个应用程序使用。如果用户在一个应用程序建立了可信任度，他们应该能够在其他应用程序上也使用此信任度。这种可跨界性使用户能够利用他们建造的信任度扩展到新的应用程序。如此可以提供互联网上最广泛的用户应用。可移植性还可以激励更多的应用程序来加入，使用Hub人类信任协议，因为他们可以访问到更准确的用户数据和画像。新建立应用程序和社区也可以迅速从已加入Hub人类信任协议的用户群中获得可靠的用户，帮助他们利用每个应用程序各自的优势。

3.4 声誉数据的用户控制

在声誉数据的自主控制权原则下，用户拥有隐私和访问数据的控制权。当新的应用程序和社区索要用户声誉数据时，用户可以有选择地披露他们声誉数据的相关部分。当用户想在新的社区和平台上建造信任度时，他们将有动力去分享他们的声誉历史数据。通过披露他们的声誉历史数据，他们会很快成为新社区和平台中值得信赖的参与者。

例如，在职业人士的就业市场中，用户可以披露有关其过去工作项目的声誉数据，但他们过去租房的数据就相对无关。他们还可以控制被披露信誉数据的数量。在某些情况下，他们也许会决定不透露相关的声誉数据，并被视作信任度低的全新用户。虽然用户自主控



制功能很强大，但社区和应用程序指定用户进行“完整”和适当的声誉数据披露也同样重要。否则，用户拒绝披露其声誉信息本身这一行为，就是一个关于用户可信度的重要信号。

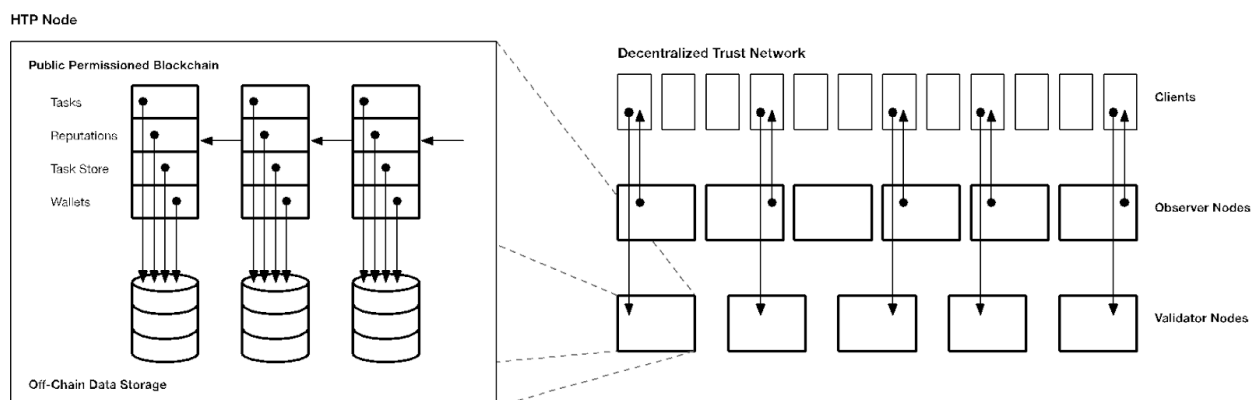
4.人类信任协议的定义

人类信任协议（Human Trust Protocol, HTP）为互联网建造了一个新的信任层（trust layer）。用户被定义为任何包括人和企业，和任何需要运用到远程信任（trust-at-a-distance）的实体。人类信任协议的功能有：

- 1.赋能用户与其他参与者进行更有价值的互动
- 2.激励用户为了产生良好结果的互动意图
- 3.激励用户通过完成互动和任务，产生成信誉数据
- 4.使用户能够评估其他用户的可信度，以便未来的互动和任务

4.1 协议架构

人类信任协议由一个去中心化的，分散的网络节点运行在公链上。这是一条公链（public blockchain），因为任何实体都可以访问该区块链，只要该实体获得用户的许可。下图显示了不同组成部分的交互方式。



节点协调由智能合约实施的交互，并成为可验证，可携带性的信誉数据存储库，通过交互模板（interaction template）可以生成新的信誉数据。每个节点都将不可篡改的记录



引用（immutable references）存到区块链上，并将全部数据加密，存储在本地数据库副本中。

HTP节点协调由智能合约实施的交互，并成为一个可验证，可携带性的信誉数据存储库，通过交互“模板”（interaction template）可以生成新的信誉数据。每个节点都将不可篡改的记录引用（immutable references）存到区块链上，并将全部数据加密，存储在本地数据库副本中。

网络将通过多层节点方法（multi-layer node approach）实现可扩展性。基础层的验证节点（validator nodes）接受交易记录的记录，并使用拜占庭容错（Byzantine Fault Tolerant）共识进行同步。他们还将验证用户，以防Sybil攻击者（Sybil attackers）。

（验证将在后面的章节中介绍。）在第二层上，会有更多的观察者节点（Observer Nodes）向应用客户端提供只读请求（read-only requests），并且将信誉数据提供给客户端。

最后，客户端（Clients）通过人类信用协议来访问此网络的软件应用。客户端代表用户执行两项基本的功能。第一个是帮助用户在特定情景，或社区的背景下预测其他用户的可信度。这些客户端可能包含信任评估程序（Trust Evaluators），客户端库包含能分析用户可信度的算法。（信任度评估算法将在后面的章节中进行描述。）第二个功能是帮助用户执行交互，从而产生更多的信任度数据。

人类信任协议涉及以下主要实体：任务，声誉信息档案，任务商城，和钱包。

4.2 任务

我们将用户间交互和交易的行为，作为任务实体（Task）进行封装，任务的执行结果会影响参与者的声誉档案。例如，考虑在聊天软件（messaging applications）上发起单方面联系的用户，无论目的是营销，销售机会还是专业技能请求，都应该被激励去产生真正有价值的互动。在产生内容分发和交互的在线社区中，用户的行为，例如发布内容，点赞，评论或提问题，都可以被其他用户判断是否有价值，并纳入可信度和声誉档案中。随着市场上卖家和买家进行点对点交易，例如销售产品或服务，或发布招聘信息，这些交互的结果也可以为用户的可信任度提供重要的信号。任务（及其扩展应用）有助于用户之间的交互，并记录结果。

任务模板（task template）是一个任务的抽象原型，可以被参与者实例化和执行。它被实现为一个参数化的智能合约（parameterized smart contract），尽管它本身不被执行。人类信任协议定义了一组核心的任务模板，以支持常用情景。新任务模板可由开发者社区中的开发人员创建，以协调新的交互方式并记录相关结果。现有的模板可以通过被修改或



扩展，只要它们符合基本任务模板就是有效的。创建新模板的能力需要一种任务分类的定义（Task taxonomy）。在稍后章节中，任务分类法会展示范例模板。

4.3 信誉档案

网络上的节点存储着用户的信誉档案。每个声誉文档为一个用户所定义。这将包含用户所有参与过的历史任务记录。由于信誉档案记录了用户的实际表现和任务成果，信誉档案提供了可验证的信誉。因信誉档案存在于网络上，所以它是可移植，便捷性的，它可以被用户使用的任何客户端访问。虽然信誉档案也是不可篡改的，但用户有自主控制权，该协议允许信誉档案向受到许可的外部实体有选择性地分享（selective disclosure）。

4.4 任务商城

即将发布的人类信任协议将引入任务商城（Task Store）。与苹果应用商店（App Store）类似，任务商城维护着任务模板库，提供可让用户使用的一系列任务模板。任务商城激励社区中的开发人员创建可扩展的任务，从而提升整个人类信任协议的总体价值。

任务商城的记录将储存在区块链上，在分布式账本上保留任务模板的修订历史记录和更新。任务模板本身存储在链下节点中。任务模板本身也具有相关的信誉数据，允许用户查看和提供有关此任务模板效果的反馈。

任务存储中的任务模板将公开，允许任何客户或用户使用。只要符合基本模板，协议也将支持私有的任务模板（private Task Templates）。

4.5 钱包

为了使用户能够从多个客户端与人类信用协议进行交互，包含Hub代币（Hub Token）的钱包将存储在网络，并保护在协议的区块链上。每个钱包将与用户帐户关联，并且与钱包关联的私钥（private key）将由用户保存。

5. 数字货币经济学

本节介绍Hub代币，和与其相关的代币经济学。

人类信任协议的主要目标之一是激励互联网上产生更多可信度高的互动。虽然提供适当的激励非常重要，但消除信任度和信誉值被造假的可能性也很重要。因为信任度和信誉数据



只可能通过与信誉相关联的互动产生，该协议保持其公平可靠性。为实现这一目标，我们引入了信任股权（Trust Stake）的概念。

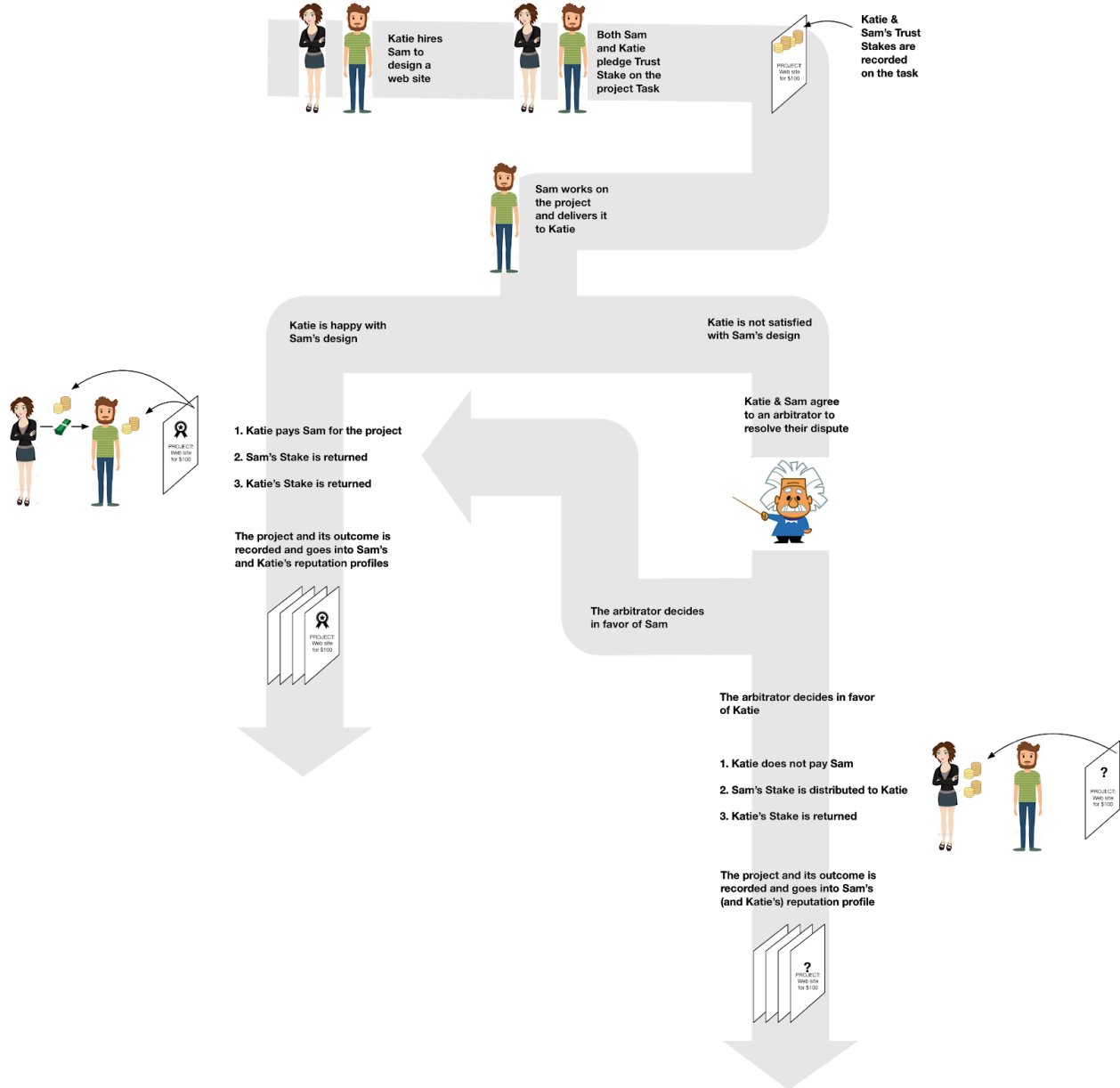
5.1 信任股权

信任股权（“Stake”）：任务参与者会投入代币，当任务的结果没有按计划进行时，这些代币会成为风险抵押。

5.1 信任股权实例

为了更好地理解信任股权（Trust Stake）在人类信任协议中的运行方式，研究一个例子。想象名为Katie的用户正在寻找一位有网站项目经验的设计师。另一位用户，Sam，有兴趣与Katie一起合作。通过成功执行该项目，Sam不仅能够获得报酬，还有机会增加他作为一名网站设计师的声誉数据和可信任度。

开始此项目时，Katie和Sam为此项目的成功投入信任股权。Sam为了担保他能取得项目成功而承诺信任股权。同样重要而可能不是很明显的是，Katie也将承诺一部分信任股权，表明她成功后会履行付款诺言。双方还同意为该项目支付一笔款项，这与双方承诺的信任股份分开。





若项目进展顺利，Katie对Sam的设计成果满意，Sam会获得报酬，并且双方的信用股权都会随着系统奖励（rewards）一起返还。（奖励制度的细节将由后面章节介绍。）如果结果有争议，并且双方无法解决分歧，Katie和Sam则需支付仲裁员（arbitrator），在本例中，仲裁员将决定支持Sam或者Katie。如果仲裁员决定Sam正确，则仍是一起成功案例，信任股权会返还给双方（及奖励）。如果仲裁确定Katie正确，那么Sam的信任股权也会交给Katie。取决于仲裁员的裁决，Sam可能不会被支付。

任何情况下，项目本身，项目类型以及项目产生的信任度结果都被添加到Sam和Katie的项目历史中，这样未来的评估者可以看到他们之前任务的历史数据。在Sam的档案中，该项目反映了他作为设计服务提供商的声誉数据。在Katie的档案中，该项目反映了她作为客户的声誉数据，以及她与供应商做生意的声誉数据。

此例可推广到更简单，或更复杂的情景，说明几点：（1）参与者在互动协作时承诺有价值的信任股权；（2）取决于任务结果，有重新分配信托股权的明确规则；（3）任务的描述数据和结果保存在声誉档案中，以便将来对于用户可信任度的评估；（4）信任股权与实际任务付款不同。任务（task）总会涉及到信任股权（trust stakes），但任务并非一定包含交易付款。

5.1.2 信任股权的经济学基础

信任股权的概念以经济学实践和理论为基础。这与履约保证金[29]类似，如果另一方未能成功履行某些义务，则需支付毁约金。经济学家Alex Tabarrok阐述的优势策略保证合同（Dominant Assurance Contracts）则是更严格的基础。在这个博弈论体系中，只要足够数量的参与者愿意贡献，“企业家”就会激励“参与者”为“公众利益”贡献力量。

如果玩家数量不足，则无法生产此公众利益，但参与的玩家仍可通过企业家承诺的回报获利。如果有足够的玩家承诺贡献，那么公众利益就会产生，使得包括企业家在内的每个人都受益。这种情况下参与者更倾向于贡献给公共利益，因为他们意识到无论合同成功与否，参与贡献都是符合他们的最大利益。Tabarrok表明此机制下，所有参与者的“主导”或最佳策略（dominant strategy）都是参与和贡献。人类信任协议的信任股权相当于用户为鼓励他人参与“公益”而作出的承诺，即取得成功的结果。

优势策略保证合同的原始形式（不解决 free-rider 搭便车问题[31]），保证合同，为 Groupon 和 Kickstarter [32] 的成功提供了基础。Tabarrok 认为，在去中心化和智能合约时代，现代保证合同的形式将比以往更加相关[33] [34]。

5.1.3. 信任股权要求

对大多数任务来说，所有参与者都应该承诺信任股权，来承诺履行和可信任度。这些任务是所有参与方承诺股权（fully-staked）的。此要求解决了 nothing-at-stake 问题[35]：由于无任何损失，参与者可能会采取恶意，不良行动。有些任务不需要所有参与者的参与承



诺股权，这些情景应仔细评估。他们被称为部分参与方承诺股权的（partially-staked）任务。至少有一名参与者下注信任股权。（一个例子是给陌生人发送消息请求。）

5.2 仲裁员，法官和争议

如果一项任务未按原计划进行并发生争议，参与者可决定招募一名仲裁员，该仲裁员担任该任务的法官，并可对该任务结果作出判断。

仲裁过程本身也是任务，代表正常任务之外的一系列链式任务。（链式任务在本文后面部分介绍。）仲裁过程本身也会有所不同。一些仲裁程序可能只需一名仲裁员，而其他程序可能涉及一组具有特定投票方案的仲裁员判决。因此，可根据任务场景设计不同的任务模板来处理纠纷。

仲裁员的服务将得到奖励。奖励条款由仲裁任务定义，即可以来自原始任务的信任股权，也可以来自单独付款项。一旦仲裁人对一方或多方做出判决，原任务就可得到解决。仲裁员的可信度也可以根据他们在HTP协议中的声誉档案来评估。

并非全部任务都需要仲裁员，因为该流程增加复杂性和成本。对于简单的任务，参与者在作出判断时可充当自己的仲裁员。

5.3 任务和信任股权的标准化

在正式的术语中，任务范围内的信任股权如下定义：

1. 每个参与者所需承诺的信任股权由具体任务决定，并由参与者共同商定并同意。
2. 每个参与者必须由足够量Hub代币保证他们的信任股权参与。
3. 参与者参与实际任务的执行。
4. 任务完成时就会发生结算（settle ment），此时参与者之间的信任股份重新分配。
5. 若任务的结果被认为成功，则参与者的信任股权通常将回返给他们，减去网络节点执行任务的费用。
6. 否则，裁决（无论是由参与人还是仲裁人）将发生来解决争议。
7. 如果判定任务未成功完成，则将被判决失信的那一方的信任股权转移给另一方，减去执行任务的费用。

5.4 激励信任

考虑以下情景：通过多次成功完成任务，持续承诺信任股份，用户将“增加”他们自己的远程信任度。未能成功履行任务的用户将会“减少”他们信任度，不仅会留下未能成功履行任务的历史记录，而且失去他们所承诺的信任股份代币。



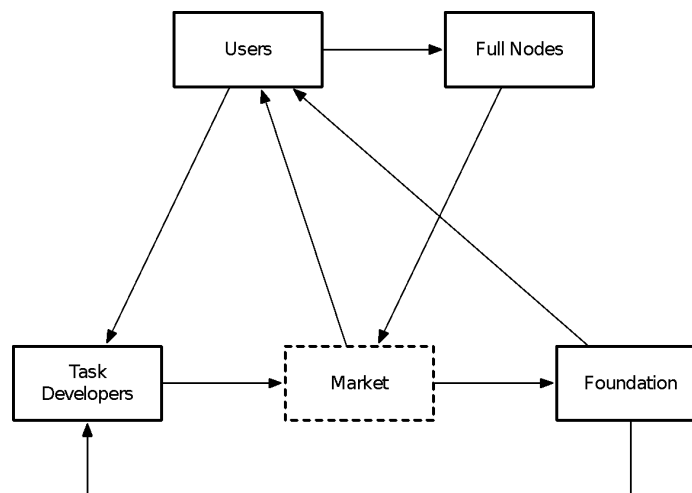
信任股权的数额取决于任务本身。信任股权的下注行为体现了参与者完成任务的动机。买方可指定一个最小股权下注额，以便排除没有足够股权参与竞标的卖家。卖家可通过优化股权下注额，赢得正在评估多个竞标的买家。一般而言，重要性更大的任务将获得较高的信任股权下注，而意义较小的任务将获得较低的下注。这些设计在人类信任协议定义之外，旨在作为任务层上的设计决策。为让下注更容易执行，应用程序还可根据用户的偏好或动态推荐算法，代表用户作出信任股份下注。后者是需要进一步探讨的话题。

互联网对信任度的更大需求将增加对代币的需求。对各种实际任务的信任度的增需也将导致对代币的增需。用户拥有的Hub数字货币越多，参加更多任务和参与更高重要性的任务机会便会越多。这些机会让他们有机会增加他们的信誉数据和可信度，并获得在现实世界中的利益。

6. Hub数字货币

Hub数字货币为人类信任协议提供了激励机制，促进用户之间的信任值验证，并促进信誉数据生成。通过完成网络社区中活动获得Hub代币的用户可认为是矿工（miners），他们通过创建声誉数据来帮助验证信任值。

下图总结了Hub代币在主要生态系统间产生流动的形式：



上图中，市场代表用户可以交易Hub代币的各种方法，包括市场交易（或通过atomic swaps）。



为达到以下目标，将创建一只基金。首先，它负责在任务完成后向用户提供信任股权奖励。（下文介绍了奖励机制细节）。其次，它会激励生态系统的发展，包括激励开发人员创建新任务。该基金会也可能在正确时机向市场购买Hub代币，以激励生态系统。

6.1 用户使用场景

用户使用Hub代币为任务压价信任股权。也会向相应任务开发人员和允许节点支付代币，以使用或托管他们的任务。他们在任务成功完成时收到代币回报（类似挖矿）并可能从其他参与者处收集代币（当任务结果完成不好的情况下）。信任股权的奖励激励了用户通过信任与其他人进行交互，并通过创建额外的信誉数据来推动协议。

此外，还可使用Hub代币作为任务付款方式。随着对Hub代币需求的增加，用户可从市场上增购代币。

6.2 全节点的使用场景

节点运行者通过帮助运行进行代币挖矿。随着代币的积累，他们也可以在市场上销售。

6.3 任务开发人员的使用场景

任务模板的开发人员将从使用他们所开发任务中获取代币。开始的时候，该基金将激励新任务模板的开发。随着开发者累积代币，他们也可在交易市场上出售。

7. 股权奖励

人类信任协议包括激励制度，以增加用户量。股权奖励制度将激励用户以可靠，高信任度的方式进行互动，通过完成任务产生声誉数据。奖励制度的概念支持以下情况：（1）创建帐户时奖励用户代币，以激励用户开始参与任务；（2）任务参与者在成功完成任务后获得股权奖金回报。

激励机制所用代币来自于一个用于激励生态系统发展的资金池，随着时间的推移，奖励将逐渐减少，随着网络成熟逐渐消失；从长远来看，由于人类信任协议存在巨大内在价值，奖励制度不是必须的。

在以下两种情况下，为防止Sybil攻击，用户必须满足以下先决条件才有资格获得奖励：

- a.** 帐户已经与一个或多个“强”用户身份相关联，例如Civic[37]，SSIs，LinkedIn等。
- b.** 用户未曾被识别为恶意
- c.** 对于新帐户而言，与帐户关联的身份之前未曾收到相同奖励。

对于情况（1），因为前提条件规定帐户必须与至少一个来自强身份系统身份关联，该系统减轻Sybil攻击的影响。



对于情况（2），该功能激励承诺股权并成功完成任务;该系统还解决了没有后果的问题，因为若参与者在任务中没有下注信任股权，他们将不会收到奖励。

以下公式表示了随着用户数量的增加而衰减的数学因子 ϵ ：

$$\epsilon = \max(1 - \frac{\log(N)}{\log(T)}, 0)$$

此处：

ϵ ：衰减因子

N：网络上用户数量

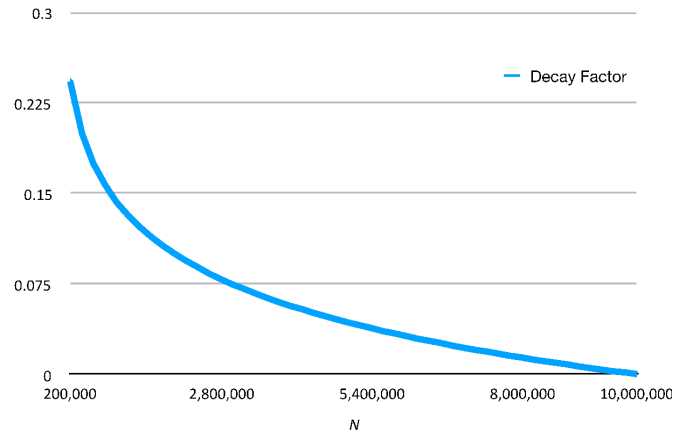
T：用户数量超过此上限，系统停止激励

激励机制方程式定义如下：

1. 建立账号	2. 任务结算
$b \lceil \epsilon \rceil$ 元素： b：建立档案的奖励机制 ϵ：衰减因子	$s \cdot \epsilon(an + bn')$ 元素： s：返还用户的信任股权 ϵ：衰减因子 a：新用户系数 $a \in [0, 1]$ n：（对于新用户）满足任务条件，且为新联系人的任务参与者 b：existing user coefficient, $b \in [0, 1]$, where b:现存用户系数, $b \in [0, 1]$, $b \ll a$ n'：（对于已存用户）满足任务条件，且为新联系人的任务参与者

因为人类信任协议系统激励用户与新的用户互动，网络效益（network effects）将得到优化。

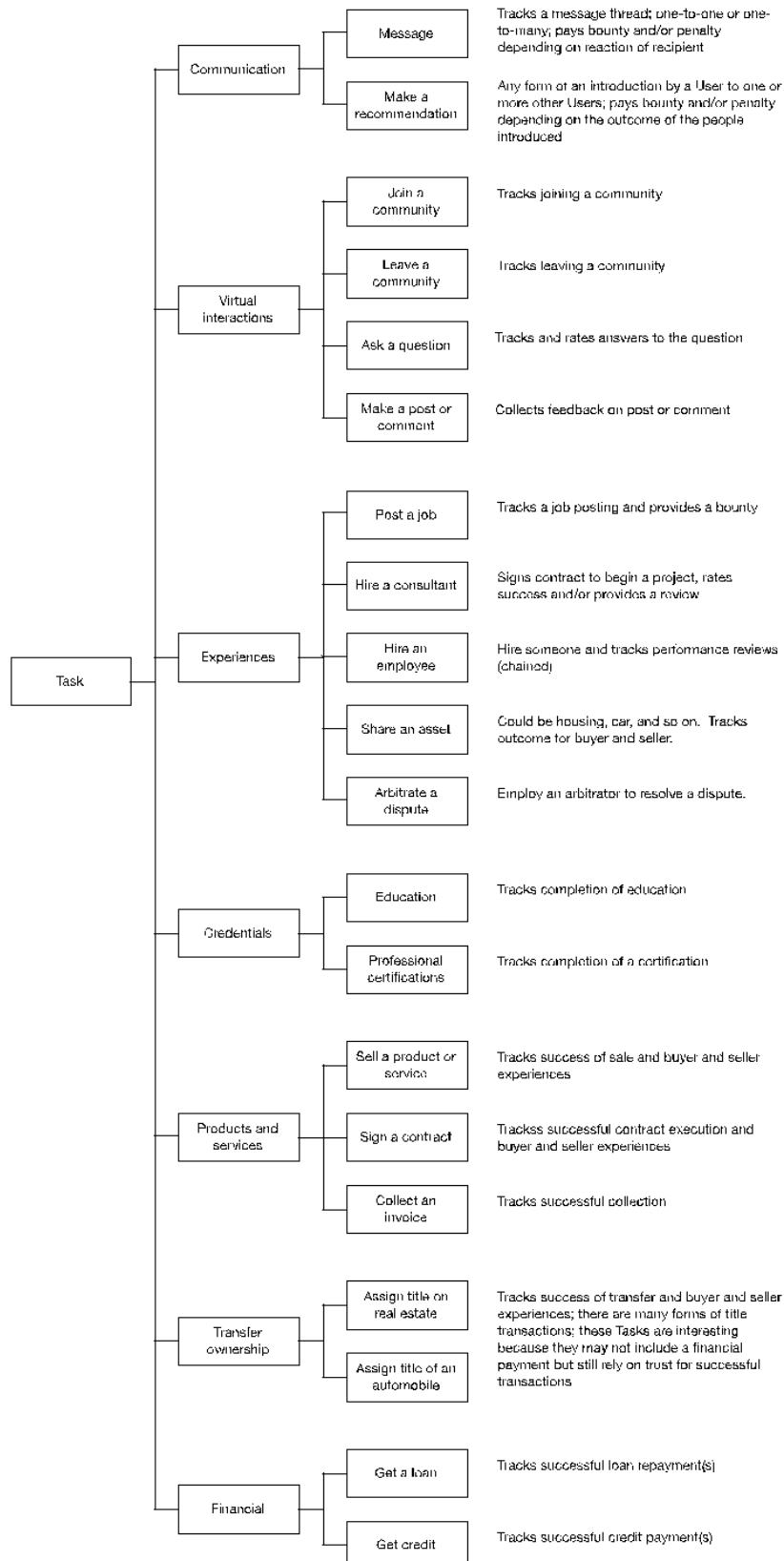
下图显示了当T被设置为一千万用户时，两个奖励案例中的的 ϵ （衰减因子）。



8.任务分类示例

人类信任协议的价值（以及Hub代币的价值）将随着任务存储库中（task store）任务的效用和多样性的增加而增加，因此激励一个开发者社区创建任务非常重要。

下图显示了人类信任协议设想到可以建立在任务商店中的一些任务。由于远程信任的重要性，和应用场景的广度，任务种类是开放式，下图只阐述一部分。我们计划提供一些核心任务，并鼓励社区创建新类任务，以增加人类信任协议的价值。





9. 攻击和防御

与许多分布式系统一样，由于用户之间的交互模式创建了社交网络图[1]，系统面临Sybil攻击的风险。本节概述相关的攻击场景并概述相应防御措施：

9.1 共谋

攻击：共谋攻击者创建多个身份并执行任务，以此提高其表面上的信任度，或合谋损害别人的利益（此类中包括一般类的Sybil攻击）。目前针对Sybil攻击的解决方案通常分三类[1]：（1）中央权威认证；（2）资源测试；（3）利用到信任网络。虽然在集中式系统有效，但（1）不完全适用分布式的系统。资源测试是一种去中心化的方法，比特币的工作证明（proof-of-work）众所周知，但随使用量增加会出现可扩展性问题（scalability issues）。

9.2 防御

人类信任协议将采用信任网络方法进行用户验证，以防御Sybil攻击。

SybilShield [41]概述了一种近期较成功的方法。与其他基于信任图谱算法类似，SybilShield假设社交网络图谱由多个诚实的Sybil社区用户，通过“尖端”相连。它通过随机漫步（random walk）策略与“代理”方法结合来识别Sybil社区，以减少误报。Sybil社区在网络将被标记，其可信度受负面影响，以免他们进一步造成负面影响。在真实数据实验中，SybilShield相比类似算法已取得极其优异的结果，特别是降低了误报 / 假阳性率，也能有效识别Sybil节点。

人类信任协议将采用去中心化的分散式信任网络法来验证用户，具体如下：

1. 验证全节点（full nodes）将通过信任网络Sybil攻击算法和SybilShield定期验证数据库。执行验证时，用户及关联信誉数据将被标记为诚实，Sybil或可疑（执行分析时的过渡态）。
2. 为确保验证的真实，只有至少2/3验证者达成共识，用户才会被标记为Sybil。
3. 标记为Sybil或可疑的帐户会被标记。直到他们的状态重新返回正常状态前，他们将不参与激励制度，并无权从其他特权中获益。

随着算法改进，人类信任协议将采取新的分析方式。但新的分析仪必须建立在社交网络正快速融合[42]的前提下。



9.2 不诚实评估者，和动态可变用户

攻击：社交网络存在不同类型的攻击者。一个不诚实用户把一个好的任务错误地评定为不良，反之亦然。动态的个性的定义是用户一开始是诚实的，后来变为不诚实的用户。

防御：在人类信任协议中，仲裁员可帮助解决这两类不良行为者的影响。结果有争议时，参与者可以使用仲裁员来解决争议。仲裁员的可信任度也可以由协议进行评估。

9.3 不诚实的代币挖掘行为

攻击：受到网络的不良影响，攻击者可能会窃取本应留给诚实用户的奖励。

防御：为了最大程度减少不诚实挖掘行为，股权奖励系统通过向创造任务这一行为收费而减少共谋者。随着更多的任务运行，消费的代币越多，运行任务成本也越高，长期以来共谋者会耗尽Hub代币。信任股权奖励制度的设计同样可减少共谋者出现的可能性。

10. 信任评估人员

信任评估者（trust evaluators）为系统中最后一部分。将帮助用户（委托人）评估其他用户（受托人）的信任度。信任评估程序内置于客户端应用程序中，通过算法访问人类信任协议生成分析，访问受托人的信誉档案的相关部分信息。评估员计算信任分数以提供快速总结。也会在特定情况下输出受托人的历史。

项目将提供可被集成到客户端应用中信任评估程序的开源客户端。这些评估人员将实施信任评分的最佳实践，以便所有客户端应用从中受益，分析以下方面：

1. 受托人加入的时间
2. 他们任务离现在的远近（“褪色”比较旧的任务历史来处理动态人格问题）
3. 通过任务受益的数字货币数量
4. 参与受托人任务的参与者的多样性
5. 受托人是否被标记为Sybil攻击者

信任评估者可通过评估相似任务的信任股权，来分析受托人对新任务的意图与诚意。

我们强调，信任评估者不是一成不变的，因为声誉是有情景性。信任评估者是为特定的应用而设计。提供的标准库作为基础，以定制适合客户端应用程序的任务。



由于新任务模板是由社区开发的，评估人员仍是重点调查对象。评估人员应该被不断改进，从而可以使用新的形式进行交互。

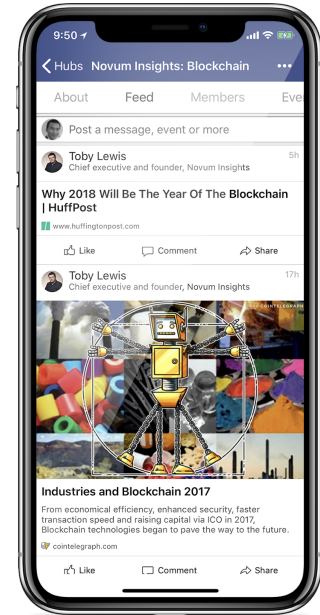
11. Hub 应用软件

我们认为人类信任协议将证明其价值，成为互联网不可或缺的信任层，但它的价值在得到更广泛采用前需再做进一步验证。为促进人类信任协议的发展，我们计划打造Hub应用程序。Hub应用程序是基于Messenger体验的下一代职业社交网络。更广泛的职业用户将可使用Hub应用程序发现其针对的行业领域和社区内的机遇，并在应用程序中进行沟通和商业交易。

虽然消费者领域的通讯产品（messenger）竞争激烈，专业人士和商业用户的使用案例仍有大部分未被开发，这是巨大的潜在市场机会。职业社交网络是人类信任协议的最佳应用，因为专业人士和商业用户通常会接触“陌生人”-包括客户，供应商和合作伙伴，他们必须评估可信度并确保商业交易信任度。时至今日，今天的商业用户经常因他们的身份信息，内容和在线交互会被全部透露给别的商务人士，而感到不合适。

Hub应用程序将作为“参照应用”来使用和推进协议是我们目前正在开发中的项目。尽管大量工作将投入Hub应用程序开发中，我们仍希望成功创建人类信任协议和创造应用程序的生态系统，从而为互联网用户带来更广阔的信任空间。

以下将介绍Hub应用程序的主要功能。

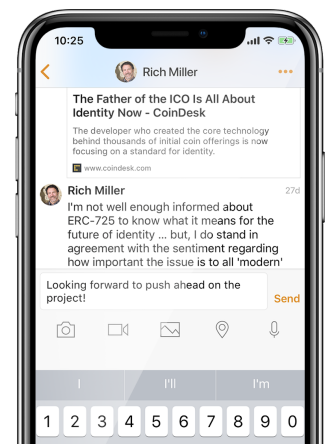


11.1 社群

Hub应用程序的核心是社群，围绕不同行业，商业社区，兴趣，网络，协会和集合体的组织。每个社群有供会员共享内容的信息流（Feed），并有社交媒体功能（如喜欢，评论和分享）与其他成员进行交流，在会员界面可发现同社区其他成员。Hubs对活动(events)具有本地支持，以便社区创建和管理活动。Hubs具有高扩展性，可允许文档存储库，人物模版和电商功能等新服务。Hubs将提供高灵活的治理机制，可定义私人 and 公共访问，和用户的访问权限。一个重要的目标是为社区的自治（self-governance）提供适当的工具。

11.2. 通讯产品

Hub社群为会员直接提供了发现和交流的机会，因此Hub应用将提供内置的通讯功能(messaging)，以实现快速，安全的一对一和群组通讯。用户可以发起通信，协作和未经请求的交互，如营销（





marketing)。与当代的消息应用程序一样，Hub应用程序将支持多媒体消息，文档附件，语音，视频聊天以及聊天机器人等。

11.3. 交易

随着用户互动，他们会对交易（transactions）产生兴趣。Hub应用程序将为付款交易提供支持。交易将在Hub应用的社区级别，和点对点级别上得到支持。下表总结了不同种类的交易，并提供范例：

层次	Examples
社群	● 会员 ● 付费内容 ● 活动 ● 交易市场
点对点交易 & 通讯	● 产品和服务合同 ● 发票收据 ● 所有权转手 - 不请自来的要求 ● 营销信息 ● 专业技能询问

11.4 安全和隐私

由于安全和隐私在职业社交网络上的重要性，Hub将会为通讯软件和社群内容提供端对端的加密（end-to-end encryption），并将其作为默认设置。目前比较适合的是Signal Protocol。我们也会尝试把软件的后端（back—end）进行分布式去中心化。这个科技现在仍处于早期阶段，但也在显著进化中。团队会继续研究这些创新科技，并在合适的时机嵌入新科技到Hub应用软件中。

Hub应用软件的功能会频繁更新，这会相对独立于与人类信任协议的更新。



11.5. 人类信任协议与Hub应用软件的结合

Hub应用软件将会同时作为人类信任协议（HTP）的消费端产品和贡献者，帮助用户在社群中建立起信任。很多活动可以被表现成HTP类型任务，我们会逐步增加更多的任务，同时增加协议的可扩容性（scalability）。

阶段	描述
1. 信任评估者	应用软件上的所有用户都有信誉数据。信任评估的基础最初会植入应用，并从最初数据如SSI申明和其他外界数据接入。
2. 社群互动	第一个大规模进行实施的任务将是由Hub数字货币支持的（而非支付）任务。这些行为可包括例如申请加入一个社群，或发布一则公告。
3.社区层面的支付相关互动	社区层面的互动，如会员，或发布工作等有关支付的行为将得到支持。在这个阶段，Hub数字货币作为一种支付手段也会受到支持。
4.点对点(P2P)交互与交易	随着协议规模扩大以处理更多交易，用于点对点交互和交易的任务将被支持。例子包括联系行业专家，和收据发票。
5. 任务商城结合	在任务商场发布后，Hub应用程序将提供一个通用容器，供用户使用新开发的任
	务。

12. 分布式信任网络的定义

在后续章节中，我们会正式定义人类信任协议的数据结构和协议。我们将从基本定义开始，并会细述两个实际应用场景：发讯息，和陈列招聘信息。

首先是分布式信任网络（decentralized trust network），这是一个节点的集合体，执行人类信任协议并且储存声誉相关的数据。节点结构如下。

12.1 数据结构



每个full node完全的节点可以接触到任务商城，过往任务的历史数据，和用户的声誉档案。随着协议的用户人数增加，将使用不同的科技创新来确保节点储存功能的可行性。

$$N := \{TS, \{t_1, \dots, t_n\}, \{r_1, \dots, r_n\}\}$$

- N , node
- TS , Task Store
- $\{t_1, \dots, t_n\}$, Task ledger
- $\{r_1, \dots, r_n\}$, Reputation Profiles

13. 任务模版定义

任务模版是对于其他任务的抽象概念。任务的实例形式会具体化信任股权额度，和不同情况下股权分配的逻辑。所有任务都需要有一定的原数据（meta-data），由以下表明。

13.1 数据结构

$$T := \langle id, desc, source, cost, (u_1, \dots, u_n), \{u_1 \rightarrow s_1, \dots, u_n \rightarrow s_n\}, start, completed, outcome, ou$$

- T , Task Template
- id , globally addressable unique Task Template ID
- $desc$, short description of Template
- $source$, Client from which Task instantiation was requested
- $cost$, amount in Hub tokens to be paid to Task developer to instantiate a Task
- $(u_1, \dots, u_n)$, users; for User identity IDs
- $\{u_1 \rightarrow s_1, \dots, u_n \rightarrow s_n\}$, required stakes s_i from User u_i in Hub tokens
- $start$, timestamp of Task execution start
- $completed$, timestamp of Task execution completion
- $outcome$, enumerated outcome result
- $outcome\ data$, variable outcome data



13.2. 协议

13.2.1 实例化

从任务模板中创建任务实例

Creates a Task instance from the Task Template.

$t := \text{Instantiate}(\text{client source}, (u_1, \dots, u_n), \{u_1 \rightarrow s_1, \dots, u_n \rightarrow s_n\})$
Inputs: • client source, Task Client • $(u_1, \dots, u_n)$, participating Users; u_0 is the Task initiator • $\{u_1 \rightarrow s_1, \dots, u_n \rightarrow s_n\}$, stakes s_i of participant u_i Outputs: • t, instantiated Task 1. Set source := client source 2. Validate at least one User has stake in the Task 3. Validate all Users have required stakes according to template requirements 4. For each User u_i, add Task t to u_i's Reputation Profile 5. Stakes are pledged to t before it begins 6. Transfer tokens in amount of cost to Task developer

14. 任务定义

一项任务就是一个任务模板实例。一项任务的数据是加密密封的，其数据只有其参与者有权访问。

14.1 合约

14.1.1 结算

结算协议是在一项任务完成时被激活的，根据结果激活信用股权，并重新分配给参与者。它不是在基本任务模板中专门实现的，而是在其扩展情景中实现的。

Settle(outcome[, outcome data])
Inputs: • outcome, Task outcome • outcome data, additional data related to <i>outcome</i> Outputs:



- t , Task
1. Trust Stakes are redistributed to participants according to the Task outcome, implemented by template's smart contract

15. 信用档案定义

信用档案是用户的任务历史记录。其记录用户参与的任务类型及其相关结果。每个信用档案都具有自主性。该合约定义了核心操作，提供了对配置文件的许可，以及对档案的选择性披露。

15.1 数据结构

$R := \langle u, \text{invalidated}, (t_1, \dots, t_n) \rangle$

- R , Reputation Profile
- u , User identity ID
- invalidated , 0 if the User is considered honest by validation; 1 otherwise
- $(t_1, \dots, t_n)$, task history of Tasks in which u is a participant

15.2 合约

15.2.1 映射

映射协议提供了一套方案，此方案可根据用户的许可向另一方提供访问和评估用户信誉档案。客户可以使用映射“评估”一个特定用户的信誉，例如，计算信任评分或可视化用户的信誉数据。无论任何情况下，访问都必须获得由作为智能合约实施的配置档案所有者的许可。搜索规范参数可以作为扫描任务历史记录的过滤标准，以及作为要返回的结果属性。档案所有者必须认同搜索规范和结果属性的可见性。

Map(u , search spec, result attributes)

Inputs:

- u , requesting User
- search spec , the search criteria for the Reputation Profile; a query tree of mappings of attributes and attribute criteria



- *result attributes*, the permissioned attributes of Tasks that may be returned and made visible to the requester

Outputs:

- $(t_1, \dots, t_n)$, list of Tasks matching *search spec* with only the attributes of *result attributes* available
1. Confirm permission from owning User that User u is allowed *search spec* and *result attributes*. If not, fail.
 2. Otherwise, compute $O :=$ for each Task t_i in the Reputation Profile, collect for output t_i with only the attributes in *result attributes* if t_i matches *search spec*
 3. Output O

15.2.2 验证

在拥有用户许可的情况下，在用户信誉档案中为请求的证明实施零知识证明。根据需要的证明查询，通过zk-SNARKs^[1]实施的零知识证明(zero-knowledge proof)需要可配置的“可信赖的设置”。这将是该项目的一个调查领域。

Attest(u , criteria)
Inputs: • u, requesting User • <i>criteria</i>, a specification of reputation to be attested to; a mapping of Task attributes to their expected values Outputs: • <i>true</i> if the attestation succeeds. Otherwise, <i>false</i>. 1. Confirm permission from owning User that User u is allowed to attest <i>criteria</i>. If not, fail. 2. Set $R := \text{false}$ 3. Otherwise, for each Task t_i in the Reputation Profile, set $R := \text{true}$ if t_i matches <i>criteria</i> 4. Output R

16. 任务商城定义

¹ <https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/>



任务商城将在未来版本的协议中得到支持，并将存储可用于实例化的公共任务模板。

16.1 数据结构

$TS := \{\langle T_1, r_1 \rangle, \dots, \langle T_n, r_n \rangle\}$ • TS, Task Store • $\langle T_i, r_i \rangle$, tuple of Task Template and associated Reputation Profile

16.1.1. 添加更新

添加新的任务模板或将更新应用到现有模板。

AddUpdate(T)
Inputs: • T, Task Template Outputs: None 1. Search for existing template T_0 using $T.id$ 2. Check that requesting User can add or update template. If not, fail 3. Otherwise, if T_0 exists, replace it with T 4. Otherwise, add T

16.1.2 搜索

根据给定的搜索条件查找任务模板。

Search(criteria)
Inputs: • $criteria$, mapping of attributes to desired values Outputs: • $(T_1, \dots, T_n)$, Task Templates matching criteria 1. Set $O := \{\}$



2. For each T_i in the Task Store, if T_i matches criteria, then append $\langle T_i, R_i \rangle$ to O
3. Output O

17. 任务模版示例：发讯息

在以下各节中，我们提供了各种有用的任务模版的示例。我们将这些模板称为“任务”，即使它们实际上是“任务模板”。

讯息是互联网上许多社交应用程序的基础。它可以用于协作，并且在营销信息和其他各种交互中起到很大的作用。收款人可以选择指定一个付款人作为接收联系人，例如，收款人可以是行业专家并收取咨询费用。讯息任务表示的是发件人和收件人之间的一条信息或一则消息。在这个公式中，讯息任务是部分股权任务的一个例子，因为它只需要来自发件人而不是收件人的放样。讯息任务可以扩展到包含两个以上的用户，并成为群聊以及用户点赞多的基础。

客户根据用户（发件人）的兴趣创建消息任务以联系其他用户（收件人）。发件人保证发送该邮件的利益。付款（如果收件人要求付款）也会提交，并在发送邮件时从发件人传送给收件人。只要任务未解决，收件人和发件人就可以继续交换消息，并且该任务保持被激活状态。如果收件人最终将该任务链标记为垃圾邮件，则邮件任务标记为已解决，并且收件人收到发件人已承诺的股份。然后该任务就结束了。

消息任务使用适合于此任务的属性扩展了的基本任务模板。（我们注意到并非所有形式的消息都需要被描述为任务，而只是那些应该影响信任的消息。）

17.1 数据结构

$M := T + \langle \text{message id}, \text{payment} \rangle$

- M , message
- T , base Task Template
- message id, reference to off-chain message thread data
- payment, optional payment to recipient upon replying or accepting contact; also specifies currency type, which can be in Hub tokens

17.2 合约

17.2.1 举出实例

扩展基本任务模板的实例化协议。



$m = \text{Instantiate}((s, r), \{s \rightarrow s_s\}, \text{message id } [, \text{payment}])$
--

Inputs:

- s , sender User id
- r , recipient User id
- s_s , sender's stake
- message id, message thread reference
- payment, recipient's payment

Outputs:

- m , Message Task

1. Set participants to be (s, r)
2. Set stakes to be $\{s \rightarrow s_s\}$
3. Set Task's id := "message"
4. Message referenced by message id is sent from s to r

17.2.2 接受

Accept()

Inputs:

None

Outputs:

None

1. If payment is specified, it is transferred from s to r

17.2.3 解决

扩展基本任务模板的解决协议，有效地关闭信息链并阻止用户之间的进一步交换信息。

Settle(outcome)



Inputs:

- outcome, one of sent|read|accepted|replied|spam

Outputs:

- m, message Task

2. If outcome is spam, then r mines s_s from s

3. Otherwise, s_s is returned to s

18. 任务模板示例：发布工作

在“发布工作任务”中，工作发布者承诺发放信任股份并发布一份工作，这可能代表在某个社区中发布的适当性。此外，招聘工作的发布者还提供一个推荐计划，包括成功推荐的奖励。推荐人还承诺赌注，表示他们已经做出适当的推荐。

在线招聘和网上招聘平台是一个产业金额高达数十亿的行业，但目前的招聘流程仍然费时费力。从可信推荐的激励、简历的真实性到参考检查，所有内容都为远程信任模式提供了多种机会。任务模板通过在所有参与者中组织招聘流程并采取适当的激励措施，可以为此流程带来更高的可靠性，提升其速度，并降低其成本。

发布工作任务模板使用户可以发布工作列表并提供推荐计划。此任务显示任务模板是如何从一个任务模板扩展到另一个模板，并将其他任务链连接在一起，以完成此任务。在这种情况下，工作模板既扩展了消息模板，又延长了消息任务链，从而来实时更新和推荐人信息。

客户代表工作发布者开启工作模板，并提供工作发布所需的参数。在发布成功后，向收款人付款，收款人可以是工作委员会或社区。在任何情况下，另一个用户可将候选人引荐到工作招聘板中，并且客户端调用AddReferral协议将邮件形式的引荐链接到工作任务。一旦发布的职位被关闭，无论职位是否成功填补，客户都会在任务中激活结算协议。如果工作成功完成并且工作发布者决定其中一个推荐人应该收到奖金，则奖励将被支付给成功的推荐人。如果进行了不良的互动，相应的赌注将被重新分配给其他参与者（下面有更多关于这方面的内容）。否则，抵押股权将返还给原始参与者。

18.1 数据结构



$J := M + \langle \{r_1, \dots, r_n\}, \text{job title[, salary, ...]} \rangle$

- J , job
- M , Message Task Template
- $\{r_1, \dots, r_n\}$, set of Message Tasks representing referrals
- job title[, salary, ...], attributes relevant to the job posting as needed

18.2 合约

18.2.1 实例创造

$j := \text{Instantiate}(p, p \rightarrow s_p, \text{job title, job description, bounty[, salary, ...]})$

Inputs:

- p , User id of job poster
- $p \rightarrow s_p$, poster's stake
- job title, job's title
- job description, stored off-chain and referred in Message's message id
- bounty, kept in Message's payment

Outputs:

- j , job Task
1. Set p to be Task's participant
 2. Set s_p as p 's stake
 3. Set message id := job description
 4. Set payment := bounty



18.2.2 添加推荐人

以消息任务的形式向工作任务添加推荐人。

AddReferral(m)
Inputs: • m, message Outputs: None 1. Confirm that m's receiver is the job Task's creator 2. Confirm that m is not already part of the job Task 3. Add m to job Task

18.2.3 结算

在职位发布结束后调用，并评估是否应将奖金支付给推荐人。

Settle(outcome[, outcome data])
Inputs: • outcome, one of not placed placed • outcome data, if outcome is placed, then outcome data is the User identity ID r of the referral who should get the bounty Outputs: None 1. If <i>outcome</i> is placed and successful referrer r exists, then transfer bounty to r.

18.3 争议

在招聘过程中可能会出现一些争议情景，我们来总结一下如何解决争议更。更重要的是，如何重新分配信用股权以确保适当的激励措施。

假设有这样的情况，即招聘者收到推荐的人并将其标记为不合适人选，即使被推荐的人没有任何问题，推荐人的股份也会有风险。与此相似，招聘人可能最终招聘了其中一个被推荐人，但却忘记了向推荐人支付奖金。



我们认为，在这两种情况下，争议都可以通过使用仲裁员来解决，仲裁员在这种情况下可以是发布工作的社区的经理。仲裁员可以查看情况的细节。如果他们决定支持推荐人，那么发布招聘信息的人会失去他们的权益，并且奖励股份会平均重新分配给所有推荐人。反之，若招聘广告是正确的，发布招聘信息的人将收到来自未推荐成功的推荐人的股权（所有其他推荐人收回他们的股份）。

19. 未来的工作

19.1 构建有效信任评估的任务分类法

随着任务模板数量的增加，对信任评估进行分类的动机也随之增加。传统上，组织分类法是在中央权力下进行的。我们寻求一个分散的计划，是我们可以创建任务模板，并最终将其有效地分类。

19.2 信任风险值默认值的计算

通过适当确定各种任务的信任关系值，可以使信任市场的激励更加有效。对经济模型及其应用的适当研究不仅将帮助用户确定恰当的任务量，而且可以促进协议书的整体成功。

20. 结论

最初，互联网是被设计成一个开放的、基于协议的星球网络来给使用者共享信息。社交和消息系统已是互联网中最成功和持久的服务。不幸的是，随着这个网络的发展，由于用户无法与陌生人建立远程信任，从而产生的各种限制会阻碍用户实现未来在互联网上的经济机会。

不可变账本和分散式信息架构的概念可创建一个全新的，高诚信信任层，可为那些在互联网上与其他人互动的用户提供更大的经济价值。

21. 致谢

作者要感谢下列人士提供了宝贵的反馈意见，改进此论文：Ken Fromm, Ken Keller, Fred Krueger, Nikolai Oreshkin, Alex Poon, Mike Prince and Kyle Wang.



22. 参考文献

- [1][https://www.ted.com/talks/rachel botsman the currency of the new economy is trust](https://www.ted.com/talks/rachel_botsman_the_currency_of_the_new_economy_is_trust)
- [2] [http://www3.weforum.org/docs/WEF Realizing Potential Blockchain.pdf](http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf)
- [3] <http://blogs.teradata.com/international/how-much-data-we-create-daily/>
- [4] [https://en.wikipedia.org/wiki/Dunbar%27s number](https://en.wikipedia.org/wiki/Dunbar%27s_number)
- [5] [https://en.wikipedia.org/wiki/Robin Dunbar](https://en.wikipedia.org/wiki/Robin_Dunbar)
- [6] <https://twitter.com/NickSzabo4/status/917474578640732160>
- [7] <https://www.lifewire.com/how-many-email-users-are-there-1171213>
- [8]<http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf>
- [9] <https://www.lifewire.com/how-many-emails-are-sent-every-day-1171210>
- [10] <https://www.wired.com/2014/05/sharing-economy-fico/> - see Monroe Labouisse of Airbnb's quote
- [11] <https://www.linkedin.com/>
- [12]<https://www.csoonline.com/article/3036072/social-networking/the-rise-of-linkedin-fraud.html>
- [13] <https://www.linkedin.com/pulse/why-so-many-fake-data-scientist-bernard-marr>
- [14] <https://3qdigital.com/socialmedia/linkedin-fake-profile-heaven#.WinVjVQ-fUI>
- [15] <https://books.google.de/books?id=myAAyj0hmq8C>, p. 95
- [16] <https://web.stanford.edu/~leinav/pubs/AR2016.pdf>
- [17] <http://www.fico.com/en/products/fico-score>
- [18] [https://en.wikipedia.org/wiki/Sesame Credit](https://en.wikipedia.org/wiki/Sesame_Credit)
- [19]<https://medium.com/learning-machine-blog/the-time-for-self-sovereign-identity-is-now-222aab97041b>
- [20] <http://oneworldidentity.com/identity-industry-landscape/>
- [21] <https://oauth.net/2/>
- [22] <http://openid.net/>
- [23] <http://identity.foundation/>
- [24] <https://www.uport.me/>
- [25] <https://sovrin.org/>
- [26]<https://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf>
- [27]<http://presnick.people.si.umich.edu/papers/postcards/PostcardsFinalPrePub.pdf>
- [28][https://www.ted.com/talks/rachel botsman the currency of the new economy is trust](https://www.ted.com/talks/rachel_botsman_the_currency_of_the_new_economy_is_trust)
- [29] [https://en.wikipedia.org/wiki/Performance bond](https://en.wikipedia.org/wiki/Performance_bond)
- [30] <http://mason.gmu.edu/~atabarro/PrivateProvision.pdf>
- [31] [https://en.wikipedia.org/wiki/Free-rider problem](https://en.wikipedia.org/wiki/Free-rider_problem)
- [32]<http://marginalrevolution.com/marginalrevolution/2013/08/a-test-of-dominant-assurance-contracts.html>



- [33] <https://www.cato-unbound.org/2017/06/07/alex-tabarrok/making-markets-work-better-dominant-assurance-contracts-some-other-helpful>
- [34] https://en.wikipedia.org/wiki/Assurance_contract
- [35] <https://ethereum.stackexchange.com/questions/2402/what-exactly-is-the-nothing-at-stake-problem>
- [36] <https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/>
- [37] <https://www.civic.com/>
- [38] https://en.wikipedia.org/wiki/Sybil_attack
- [39] <https://www.cs.ucsb.edu/~ravenben/publications/pdf/reputation-ecrj10>, p. 246
- [40] <https://nymity.ch/sybilhunting/pdf/Levine2006a.pdf>
- [41] <http://ualr.edu/computerscience/files/2014/01/Paper-6.pdf>
- [42] <https://pdfs.semanticscholar.org/d877/826ef2db3e7b3d955ca4b7265123be62154f.pdf>, p. 2
- [43] <https://www.cs.ucsb.edu/~ravenben/publications/pdf/reputation-ecrj10.pdf>, p. 246
- [44] https://en.wikipedia.org/wiki/Signal_Protocol
- [45] <https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/>
- [46] <https://eprint.iacr.org/2018/046>



LEGAL DISCLAIMER

THIS WHITEPAPER DOES NOT GIVE PERSONAL, LEGAL OR FINANCIAL ADVICE. YOU ARE STRONGLY ENCOURAGED TO SEEK YOUR OWN PROFESSIONAL, LEGAL AND FINANCIAL ADVICE.

As of the date of publication of this whitepaper, Hub Tokens have no known potential uses outside of the Hub platform ecosystem and are not permitted to be sold or otherwise traded on third-party exchanges. This whitepaper does not constitute advice nor a recommendation by Hub, its officers, directors, managers, employees, agents, advisors or consultants, or any other person to any recipient of this document on the merits of the participation in the Hub Token Sale. Participation in the Hub Token Sale carries substantial risk and may involve special risks that could lead to a loss of all or a substantial portion of amounts used to purchase Hub Tokens. The purchaser of Hub Tokens undertakes that such purchaser understands and has significant experience in cryptocurrencies, blockchain systems and services, and that such purchaser fully understands the risks associated with tokens as well as the mechanism related to the use of cryptocurrencies (including storage of tokens). Do not participate in the Hub Token Sale unless you are prepared to lose the entire amount you allocated to purchasing Hub Tokens. Hub Tokens should not be acquired for speculative or investment purposes with the expectation of making a profit or immediate resale. Hub shall not be responsible for any loss of Hub Tokens, or situations making it impossible to access Hub Tokens, which may result from any actions or omissions of the user, or any person undertaking the acquisition of Hub Tokens, as well as in case of hacker attacks.

No promises of future performance or value are or will be made with respect to Hub Tokens, including no promise of inherent value, no promise of continuing payments, and no guarantee that Hub Tokens will hold any particular value. Unless prospective participants fully understand and accept the nature of Hub and the potential risks inherent in Hub Tokens, they should not participate in the Hub Token Sale. Hub Tokens are not participation in Hub and Hub Tokens hold no rights in Hub. Hub Tokens are sold as a functional good and all proceeds received by Hub may be spent freely by Hub, absent any conditions set out in this whitepaper. This whitepaper is not a prospectus or disclosure document. This whitepaper is for information only. Written authorization is required for distribution of any or all parts contained herein.

Hub's business is subject to various laws and regulations in the countries where it operates or intends to operate. No regulatory authority has examined or approved of any of the information provided in this whitepaper. No such action has been or will be taken under the laws, regulatory requirements, or rules of any jurisdiction. The regulatory status of tokens and distributed ledger technology is unclear or unsettled in many jurisdictions. It is difficult to predict how or whether regulatory agencies may apply existing regulation with respect to such technology and its applications, including the Hub platform and Hub Tokens. It is likewise difficult to predict how or whether legislatures or regulatory agencies may implement changes to laws and regulations affecting distributed ledger technology and its applications, including the Hub platform and Hub Tokens. Regulatory actions could negatively affect the Hub platform and Hub Tokens in various ways, including, for purposes of illustration only, through a determination that the purchase, sale and delivery of Hub Tokens constitutes unlawful activity or that Hub Tokens are a regulated instrument that requires registration or the licensing of some or all of the parties involved in the purchase, sale and delivery thereof. There is a risk that certain activities of Hub may be deemed in violation of laws or regulations. Penalties for any such potential violation would be unknown. Additionally, changes in applicable laws or regulations or evolving interpretations of existing law could, in certain circumstances, result in increased compliance costs or capital expenditures, which could impede Hub's ability to carry on the business model and the Hub Tokens model proposed in this whitepaper. The Hub platform may cease operations in a jurisdiction in the event that regulatory actions, or changes to laws or regulations, make it illegal to operate in such jurisdiction or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

This whitepaper is for information purposes only and is subject to change. Hub cannot guarantee the accuracy of the statements made or conclusions reached in this document. You agree that you purchase, receive and hold the Hub Tokens at your own risk and that the Hub Tokens are provided on an "as is" basis without warranties of any kind,



either express or implied. Hub does not make and expressly disclaims all representations and warranties (whether express or implied by statute or otherwise) whatsoever, including but not limited to:

- any representations or warranties relating to merchantability, fitness for a particular purpose, suitability, wage, title or non-infringement;
- that the contents of this document are accurate and free from any errors; and
- that such contents do not infringe any third party rights.

Hub shall have no liability for damages of any kind arising out of the use, reference to or reliance on the contents of this document, even if advised of the possibility of such damages.

It is your responsibility to determine if you are legally allowed to purchase the Hub Tokens in your jurisdiction and whether you can then resell the Hub Tokens to another purchaser in any given jurisdiction. You bear the sole responsibility for determining or assessing the tax implications of purchasing, receiving and holding the Hub Tokens in all respects and in any relevant jurisdiction.

This whitepaper includes references to third party data and industry publications. Hub believes that this industry data is accurate and that its estimates and assumptions are reasonable; however, there are no assurances as to the accuracy or completeness of this data. Third party sources generally state the information contained therein has been obtained from sources believed to be reliable; however, there are no assurances as to the accuracy or completeness of included information. Although the data are believed to be reliable, Hub has not independently verified any of the data from third party sources referred to in this whitepaper or ascertained the underlying assumptions relied upon by such sources.

Please note that Hub may decide to amend the intended functionality of its Hub Tokens in order to ensure compliance with any legal or regulatory requirements to which we are subject. In the event that Hub decides to amend the intended functionality of its Hub Tokens, Hub will update the relevant contents of this whitepaper and upload the latest version of this to its website.

This whitepaper does not constitute an agreement that binds Hub. Hub, its directors, officers, employees, and associates do not warrant or assume any legal liability arising out of or related to the accuracy, reliability, or completeness of any material contained in this whitepaper. To the fullest extent permitted by any applicable law in any jurisdiction, Hub shall not be liable for any indirect, special, incidental, consequential or other losses arising out of, or in connection with, this whitepaper, including, but not limited to, loss of revenue, loss of income or profits, and loss of data.

Persons who intend to purchase Hub Tokens should seek the advice of independent experts before committing to any action set out in this whitepaper.

In addition, this whitepaper may be updated or altered, with the latest version of the whitepaper prevailing over previous versions, and we are not obliged to give you any notice of the fact or content of any changes. The latest version of the whitepaper in English is available at the website <http://bit.ly/HubWhitepaperEnglish>.

Any Hub Tokens could be impacted by regulatory action, including potential restrictions on the ownership, use or possession of such tokens. Regulators or other circumstances may demand that the mechanics of the Hub Tokens be altered, all or in part. Hub may revise mechanics to comply with regulatory requirements or other governmental or business obligations.

This whitepaper and the related documents may be translated into languages other than English. Should a conflict or an inconsistency arise between the English-language version and a foreign-language version, the English-language version of this whitepaper shall govern and prevail.

CAUTION REGARDING FORWARD-LOOKING STATEMENTS



This whitepaper contains forward-looking statements or information (collectively “forward-looking statements”) that relate to Hub’s current expectations and views of future events. In some cases, these forward-looking statements can be identified by words or phrases such as “may”, “will”, “expect”, “anticipate”, “aim”, “estimate”, “intend”, “plan”, “seek”, “believe”, “potential”, “continue”, “is/are likely to” or the negative of these terms, or other similar expressions intended to identify forward-looking statements. Hub has based these forward-looking statements on its current expectations and projections about future events and financial trends that it believes may affect its financial condition, results of operations, business strategy, financial needs, or the results of the Hub Token Sale or the value or price stability of the Hub Tokens.

All information here that is forward-looking is speculative in nature and may change in response to numerous outside forces, including technological innovations, regulatory factors, and/or currency fluctuations, including but not limited to the market value of cryptocurrencies.

In addition to statements relating to the matters set out here, this whitepaper contains forward-looking statements related to Hub’s proposed operating model. The model speaks to its objectives only, and is not a forecast, projection or prediction of future results of operations.

Forward-looking statements are based on certain assumptions and analysis made by Hub in light of its experience and perception of historical trends, current conditions and expected future developments and other factors it believes are appropriate, and are subject to risks and uncertainties. Although the forward-looking statements contained in this whitepaper are based upon what Hub believes are reasonable assumptions, these risks, uncertainties, assumptions and other factors could cause Hub’s actual results, performance, achievements and experience to differ materially from its expectations expressed, implied or perceived in forward-looking statements. Given such risks, prospective participants in a Token Sale should not place undue reliance on these forward-looking statements. [Risks and uncertainties include, but are not limited to, those identified in the Token Sale terms and conditions.] These are not a definitive list of all factors associated with purchasing Hub Tokens.

Hub undertakes no obligation to update any forward-looking statement to reflect events or circumstances after the date of this whitepaper.