R3 报告

身份深度

伊恩格里格

内容

R3 Research 旨在为决策者和 DLT 爱好者提供有关商务语言 DLT 的简明报告。这些报告由该领域的专家撰写，并植根于该技术的实际经验。

如需更多研究，请访问 R3 的 Wiki。

身份深入

Ian Grigg

2017 年 3 月

3 日

1 身份是边缘协议

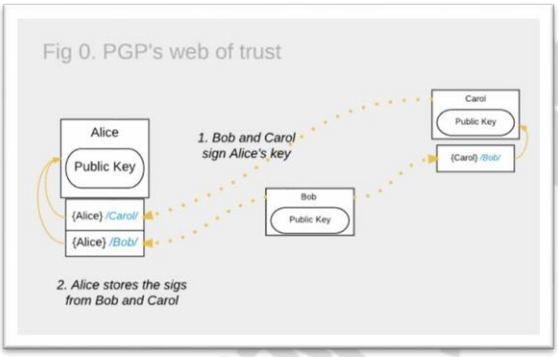
有两条推文让我可以制定一个愿景，即为什么我们将来会朝着略微不同的方向前进。首先是这一个：

为了在技术层面上理解这一点，我们必须回过头来看一个名为“信任网”的失败的小发明，该发明于 20 世纪 90 年代初由原始电子邮件安全程序 PGP 发明。在这个概念中，我们希望其他人向我们发送加密电子邮件，但其他人不知道我们的密钥。

所以我们都签署了我们遇到的任何人的钥匙，从而创建了一个相互关系的图表，或者他们称之为信任网络，我们可以用它来从一个密钥导航到另一个密钥。网络运作，但信任没有，部分是因为没有人说信任意味着什么，所以人们强加了他们自己的真相的各种但不相容的版本。

在 20 世纪 90 年代中期，一个名为 Thwarte 的认证机构（CA）将 PGP 概念融合到 CA 概念中，使用名为 Notaries 的社区成员进行“聚会”并以更精细的方式报告 - 以一个松散地说“我是看到鲍勃的护照“。但是，从长远来看，这个过程也没有起作用，部分原因是 CA 被买断（并且不再对社区有兴趣），实际上因为它们的机制不可审计。

然而！在 CAcert 中发现了相同的机制是可审计的 - 另一个社区 CA 在那里我作为审计员工作了一段时间。再次感到愤怒，因为在我们观察的过程中，成为“可接受的”CA 的障碍逐渐增加，但我们在此过程中建立了一个可自我验证的可审计社区。

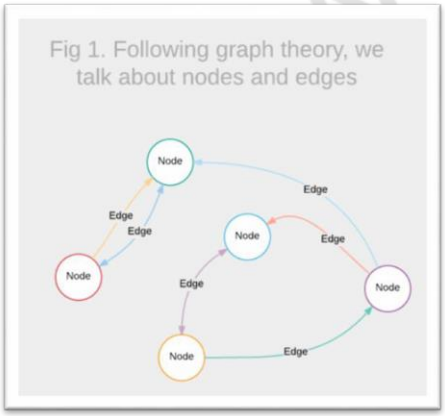


强烈地，通过许多弱关系。这样做的结果是我们现在知道如何建立信任网络。

在这个过程中，观察到中心（在这种情况下是 CAcert）对这个人几乎一无所知。但它对人们对人们所说的内容了如指掌。事实上，它的全部有价值的数据集并不是它对我和你的了解，而是你对我的评价，你和我对别人所说的，以及爱丽丝对鲍勃所说的话。通过捕获足够的这些关系，我们得到了一个坚不可摧的图表。

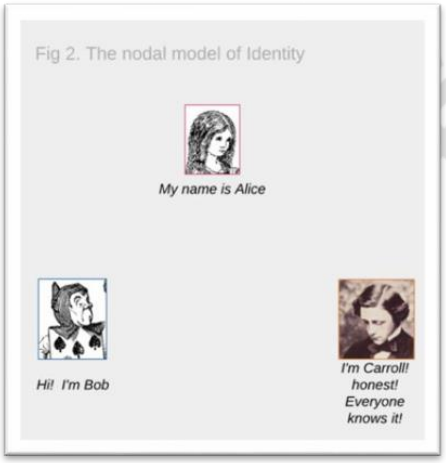
因此，当 AA 高于所述身份是一个边缘协议时，这在我的脑海中形成了一种描述新身份的技术方式。这给我们带来了推文#2：

好吧，所以非技术人员显然不会出现这些图片。因此，让我看看我是否可以在三张图片中描述它。首先，“边缘”一词仅表示关系图中节点或顶点之间的线。



然后，让我们回到经典或 IT 方法来思考身份。我们认识爱丽丝，我们认识鲍勃。我们有一个人力资源部门说这个。我们有 CA 出售用途

证书说爱丽丝是爱丽丝。我们有各州发放身份证，这也是这样说的，企业 IT 部门就是建立在这个意义上的 – 让我们在称为 Alice 的节点上，让我们为称为 Bob 的节点添加权限，让我们弄清楚这个节点是否被称为 Carol 可以与称为 Bob 的节点进行交易。



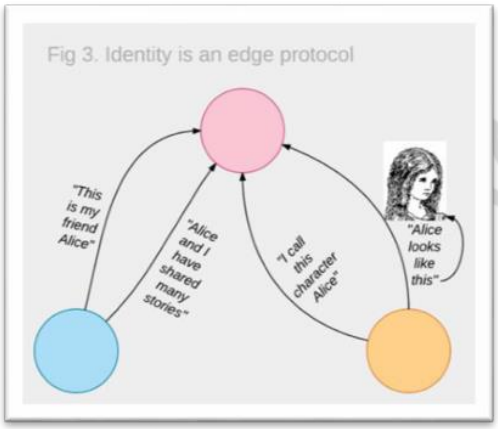
然而，这不是人们的想法。它也没有规模 – 有时在入职部门工作并计算损失率和成本率。布莱什！世界各地的账户和活动正在缩减。那么结晶的是我们 – 整个 IT，信息安全和合规领域 – 让它倒退了。

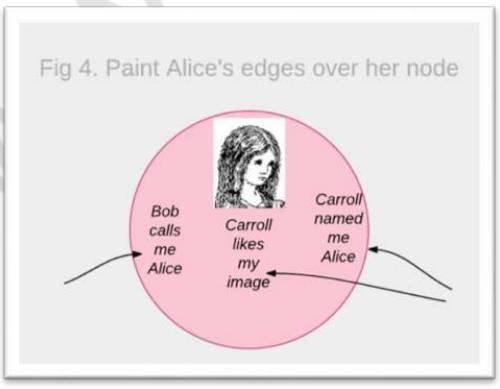
身份是边缘协议，而不是节点协议。有价值的不是节点，而是我们可以在任何两个给定节点之间检查和记录的关系。它有助于将节点 – 人 – 视为一个空白圆圈，然后想象在你的脑海中追踪圆圈之间的关系。

当我们走得那么远时，为了分析起见，我们可能需要回到节点思考。但这很容易 – 想象一下这些关系的一部分并暂时将它们画在一块空白的画布上。

最终得到的信息与旧的节点方法非常相似。但这一次它是可扩展的。我们并没有真正限制我们收集和分析的关系，只要我们收集它们并将它们分析为独立的动态，薄弱环节，然后在绘制在一起时为我们创造一个愿景。但是，如果我们尝试将所有信息推送到节点中，并将其作为静态数据进行管理，那么我们肯定会遇到复杂性限制。

这就是问题所在 – 我们过于关注身份是一个人的事实，而实际上，身份是我们每个人内部共享的社会背景。Ergo：身份是一种边缘协议。

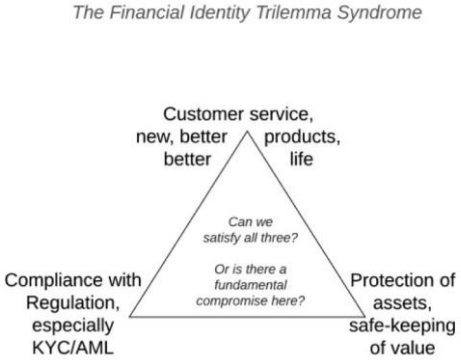




2 对身份的探索

2.1 身份的三个动力

似乎商业概念概念有三个一般动机：合规性，安全性和客户服务。了解哪个人是合规问题。知道某人授权使用自己的资金是一个安全问题。知道一个人能够轻松地移动她的钱而不受阻碍是一个客户服务问题。有时这三个激励因素是兼容的，有时它们会发生冲突。



2.2 FITS - 金融身份三元论综合症

如果您患有 FITS，可能是因为合规。正如“身份白皮书”中详细讨论的那样，麦肯锡已经将合规成本称为同比增长 20%。同时，合规性问题已经陷入困境并降低了安全性，并降低了客户服务的质量。这不仅仅是对顾客的不愉快，这是一个危险的迹象 - 如果顾客因服务质量不好而离开，或银行减少罚款风险，银行缩水，在当前微妙的资产负债表环境中，合规成本上升，经济衰退，银行客户群减少是一个危及生命的问题。

如果我们能够纠正这种平衡 - 将客户服务重新列入清单 - 而不会损害其他两个，那么不仅可能值得客户投资新系统，它实际上可能会节省一些银行。

我们怎么可能这样做？从我们目前对身份认识的角度来看，很明显今天的系统和解决方案一样是问题所在。然后，有必要从头开始重新审视这个过程。

让我们从一张干净的纸张开始，问一下 - 我们如何做出决定？

2.3 语境意味着一切

我们人类可以从背景中快速评估，无意识的评估。

例如，如果我们与一群人的所有通信都在一个封闭的朋友或已知同事的网络中，我们可以假设我们可以与该群体分享什么，我们不会为公共论坛做出这些假设。或者，在外面工作，如果我们发现自己在当地的酒吧，我们可能会认为酒吧里的所有人都可能像我们城市的普通人一样诚实可靠 - 在一个城市我们可能会留下我们的电话和钥匙在参观便利设施时，桌子不在另一个地方。

在上面的例子中，当决定是否相信我不偷你的手机时，你根本不需要知道我的身份。你需要知道的是，我在哪里？我订阅了哪些规范？

考虑到银行和交易的背景等等，知道我是那个着名的权力经纪人经纪人 A 的交易者可能就足够了。这可能就是你所需要的。好吧，这不是全部，你也想知道我在哪个办公桌，我的限制是什么，以及我有权交易什么。但你不需要知道的是我的名字。

当我们将自己局限于公司银行业务 - 背景 - 那么我们对这两个身份感兴趣
- 交易者和公司，但我们真正感兴趣的不是身份本身，而是身份之间的关系和相互作用。让我们把它看作一个边缘协议（参见前面关于 Edge Protocols 的图 3）并将其应用于交易：每个人都说经纪人 A 是一个很好的经纪人，经纪人 A 说我是那里的交易员，那应该是足够。

如果我们与经纪人 A 做生意，我们基本上都依赖于该公司的信任级别，而且不应该担心我们正在与之交谈的公司中的哪些人 - 他们都应该是好的，否则为什么要与那家公司打交道？

如果它只是边缘，那么我们可以收集它们，分析它们，我们就是液体。将边缘 Hoover 连接到关系 AI，我们就完成了。实用，外包，利润，我们来了！

但是这个过程存在一些障碍。让我们看看三个，即风险，可靠性和责任。

2.4 别人的事实

理想情况下，我们希望将一家银行的决定权交给一个人，并将其与数据一样复制到其他银行。但风险分析排除了 - 一家银行的风险与另一家银行的风险不同。因此，我们需要避免外包决策，在当今世界，我们仅限于外包事实 - 关系或边缘。

2.5 追捕事实

让我们把注意力放在事实上。一个典型的事实是鲍勃在这句话上签字：“爱丽丝持有的护照上有她

的名字和她的好照片”-Bob

这是有价值的证据，即爱丽丝是爱丽丝，如果依赖派卡罗尔需要证据，她可能会很高兴能够依赖鲍勃的陈述。

或者她可能不会。这可能在很多方面都会出错，但是假设我们已经过滤掉了无用的事实，我们剩下的就是交易的金块。我们仍然留下：

名词。..

无论如何，护照是什么？

什么名字？任何其他的玫瑰。..什么是好照片？

凶悍，漂亮还是平淡无奇？

谁是鲍勃？

他为什么关心？

他有什么动力来说实话？他有什么动力来做好工

作？

事实是否可靠？

它是否可靠，现在是否可靠，明天是否可靠？

我们担心的主要问题是收集的边缘可能不可靠。即，如果我的名字不是爱丽丝会怎么样？或者我在经纪人 A 隔壁工作，只是潜入一天晚上使用他们的终端？或者，千种场景中的任何一种 - 这里的结论是，虽然事实可能仍然是事实，但鲍勃说这些话，它可能不是现实世界的准确或可靠的表示。如果发生这种情况，那么上面的黄金分析就会变成傻瓜的黄金。

2.5.1 我们不可靠的根源

任何特定事实可能不可靠的原因都是军团 – 我曾写过其中的 99 个。我们可以尽职尽责地保证会更加小心，但这在过去并不顺利。我们需要更好的营销和空洞的竞选承诺，使这项工作。幸运的是，我们已经更清楚地说明为什么事实不可靠以及如何解决它。四种技术将为事实奠定基础：

1. 游戏中的皮肤 – 每个代理人不仅需要积极地激励在这种关系建设中工作，而且还要在出现问题时积极纠正。需要有工程师称之为负反馈回路 – 纠正能力之一。
2. 质量控制 – 如果上述纠正是戏剧性的，我们需要一种方法来证明代理人做得很好。陈述是用语言表达的，它们可以是广泛的标记和误解。为了解决这个问题，我们可以制定明确适用于事实制造者和事实用户或“依赖方”的最低质量标准，并努力运作。
3. 源代码中的冗余 – 获得一个完整准确的事实是非常昂贵的，但是要获得许多小事实收敛于相同的近似大事实是便宜的。
4. 来源中的当局 – 某些事实是由某些方“拥有”的，如果我们能够在安全的环境中获得它们，那么我们就可以提高质量，至少在事实上如此。

这些应该是熟悉的，并将创建可靠性的基础，但我们需要更多。

2.6 提供者的责任确定了事实的质量

为了对卡罗尔有用，我们需要事实不仅可靠，而且可出口。也就是说，适合其他人依靠自己风险评估的事实。我们可以通过上面列出的前两种基本方式完成此操作：

> 首先，通过为不良工作设定负债，尤其是不遵循第二条标准。
>
> 其次，通过建立前沿和操作至最低质量标准，该标准明确且适用于事实的制造者和事实的“依赖方”。

对于糟糕的工作负有责任需要谨慎处理，因为有两种普遍的可能性

- 在创造事实时所做的工作和关心，它具有一个价值，和
- 依赖事实可能造成的损害，哪种损害具有另一个价值。这两个值有时会大不相同。

一般而言，很难评估可能导致预付损害的责任，因为预测事实的用途是不可信的。这就是密码学家所说的奶奶家的问题：如果我签名马洛里是一个好人，奶奶依赖我的陈述，结果是奶奶失去了她的房子，谁应该受到责备？有一所学校认为她相当依赖我，所以我得给她一个房子。另一所学校认为，因为我只审查了马洛里的护照，这是一个过程或行政方面的影响而已，不再需要，并回到护照复习学校。

这是什么？

为了减少戈尔迪结，我们通常会在解决纠纷之前提出这样的问题，这个人可以决定哪种解释适用。这接受我们完全不确定一个特定的争议将如何发展，我和奶奶，但我们知道它会以这种或那种方式解决。因此，这种不确定性是争论的关键所在，我可能会做得更好而不是因为我的责任可能会高涨，而且奶奶也不会把她的房子放到一个索赔的赌博中，因为她的资产可能会去摇滚到底！

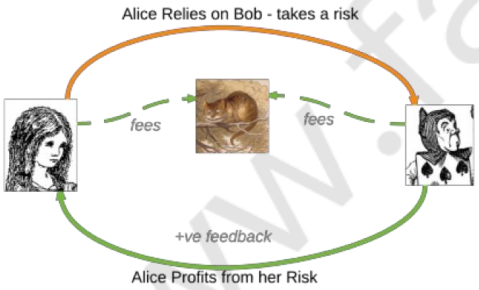
但是，如果我的责任可能会高涨，我为什么要介入？正是出于这个原因，我需要受到标准方法的保护 – 经过深思熟虑，同意，记录和审计的方法。特别是，最后一步是说服仲裁员我完成了我被要求做的工作。

因此，良好的负债框架最初仅限于事实的正确性。然而，为了依靠这些事实获得任何牵引力，我们至少需要提高事实的质量，使其可靠 – 它们满足最低标准，允许其他人依赖它们。

因此，尽管责任解决方案最初是必要的，以解决当一个人依赖另一个人产生的事实时产生的负债，但它还有另一个副作用 – 它通过鼓励事实的提供者预先采取特殊照顾来提高质量，好像他们对尚未确定尚未确定风险的另一个人负有责任。出于这个原因，我们需要用一个标准来保护事实的提供者，这样他们就不会因为简单的流程操作而承受不可能的高负债。

2.7 替代路线缺乏问责制

在典型的替代方法中，事实提供者声称零责任，因为这是不可预测责任的唯一商业解决方案。但是，这就是我们所说的正反馈循环，其中提供者同样获得好的和坏的结果。在正反馈循环中，活动会增长并增长，直到机器自行销毁。由于当机器脱轨时没有纠正，缺乏责任也意味着缺乏问责制，在这种情况下，有一个不幸的后果：数据的质量缩小为零。实际上，零责任解决方案导致竞争到底，并且提供者打印不可靠的语句而没有限制。



我们需要解决责任问题不仅是因为直接责任本身，而且因为系统需要适当的质量水平，并且为了实现这一目标，事实提供者需要适当的激励来达到这种质量水平。

简而言之，我们需要一种反馈机制，使提供者相信，与广告治疗相比，值得采取真正的谨慎态度。

可以在证书颁发机构（CA）业务中看到不良责任后果的示例。事实的提供者，CA，通常说两件关于公司的事情，例如 R3

- 保存标识所标识的公钥的私钥，并且，
- 是域名的持有者，例如 r3.com。

这两个事实在证书中被记录（如果没有解释）。

但事实的提供者，CA，并不承担任何责任。因此，由于该免责声明，如果银行要进行依靠证书的 Corda 交易（假设示例）下载最新的 Corda 版本，并且银行遭到 Closet Internet 攻击的中间人无政府主义者注入零日，然后通过菲律宾向孟加拉国风格的银行汇款。...

然后。..谁站起来？谁承担责任？

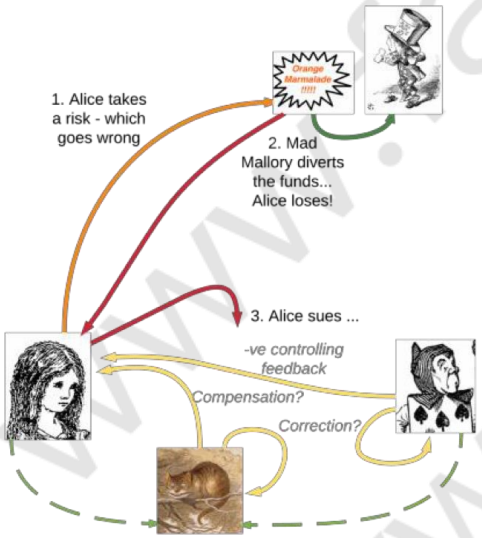
不是 CA--它的合同（深埋）说“零责任”，这意味着它 - 由于各种原因，我们无法将 CA 告上法庭。无论出现什么问题，CA 都完全被覆盖。因此，最终，不可避免地，所有治理和经济学的法律和历史以及侵蚀和演变以及所有这些科学概念，CA 都会采取低级别的谨慎措施来检查证据中的数据。CA 已进入竞争底线，我们不是这场比赛的赢家。

如果存在反馈循环，CA 可以具有适当的质量水平，该反馈循环用于根据客户的更广泛用途向上或向下移动质量。如果责任以某种方式愚蠢 - 如果某些参与者不受其行为的影响 - 那么质量会随着时间的推移而下降，整个系统就变得毫无用处。这最终会导致诸如欺诈或黑客攻击或网络钓鱼之类的灾难，然后引发官僚主义的过载以增加越来越多无意义的良好规则或监管回扣。或两者。

2.7.1 关闭循环

它不是关于银行，爱丽丝，监管机构，或 CA 或自然，欲望或人性。这是关于系统的。我们需要一个控制信息质量的反馈回路，工程师称之为负反馈回路。

这些信息/这些数据的性质是灾难是不可预测的 - 没有办法在事前添加拨号，允许将责任设置到某种程度。我们都承担一些风险，我们每个人，无论是个人还是整个社会，我们需要的是一种在风险爆发时控制风险的机制。因此，我们需要一个可以在事后检查灾难的争议解决机制，在标准的背景下承担更广泛的责任问题，并在数据失败时返回人的答案。



我们需要爱丽丝和鲍勃不要陷入道德风险的陷阱 - 希望一些神秘的其他人涵盖所有可能性。我们需要他们两个都要小心，并准备好在护理不充分时站起来。我们还需要将其包装成一个有效的包，以便激励他们参与。

如果爱丽丝和鲍勃以及其他所有人都已就参与达成共识，那么边缘将会增长并流动。通过足够的边缘流动性，节点上的决策任务变得易于处理，甚至跨越全球，跨语言，跨越管辖区。

然后我们可以回到创造有利可图的共享贸易的业务。由人际关系边缘构建的身份结构支持的交易。

R3 是一家使用分布式总账技术构建下一代金融服务基础架构的企业软件公司。

R3 的成员基地包括六大洲的 80 多家全球金融机构和监管机构。它是金融市场上同类最大的合作财团。联盟成员可以获得项目，研究，监管外展和专业服务的见解。

我们的团队由金融行业资深人士，技术专家和新技术企业家组成，汇集了电子金融市场，密码学和数字货币的专业知识。

Corda