IOSG｜科技巨头与人工智能代理创新者的挑战与困境

## 1.集中式人工智能代理的前景

人工智能代理有潜力彻底改变我们与网络互动和在线执行任务的方式。虽然围绕利用加密货币支付轨道的人工智能代理有很多讨论，但重要的是要认识到，已建立的Web 2.0公司也有很好的条件提供全面的agent (人工智能代理) 产品套件。

Web2公司的agent大多以助手形态，或者是垂直工具的形态出现，只具备很弱的执行能力。这里面既有基础模型还不够成熟的原因，也有监管不确定等原因。现在的agent仍处于第一阶段，他们在特定领域里能做的不错，但基本没有泛化能力。例如阿里国际有一个agent是专门帮商家回复信用卡纠纷的邮件。很简单的一个agent，调用了发货记录等数据，按模板生成发送，就有很高的成功率能够让信用卡公司不扣钱。

像苹果、谷歌这样的科技巨头，以及像OpenAI或Anthropic这样的人工智能专家公司，似乎特别适合探索开发agent系统的协同效应。苹果的优势在于其消费者设备生态系统，可以作为人工智能模型的宿主和用户交互的门户。该公司的Apple Pay系统可以使代理能够促进安全的在线支付。谷歌凭借其庞大的网络数据索引和提供实时嵌入的能力，可以为代理提供前所未有的信息访问。与此同时，像OpenAI和Anthropic这样的人工智能强者可以专注于开发能够处理复杂任务和管理金融交易的专门模型。除了Web2大厂，在美国也有大量的创业公司做这样的agent，比如帮助牙医做预约管理，或者辅助生成诊疗后报告这些非常细的场景。

然而，这些Web 2.0巨头面临着经典的创新者困境（Innovator's dilemma）。尽管他们拥有技术实力和市场主导地位，但他们必须在破坏性创新的危险水域中航行。开发真正自主的agent代表着与他们既定商业模式的重大偏离。此外，人工智能的不可预测性，加上金融交易和用户信任的高风险，带来了重大挑战。



## 2. 创新者的困境：集中式提供商面临的挑战

创新者的困境描述了一个悖论，即成功的公司往往难以采用新技术或商业模式，即使这些创新对长期发展至关重要。问题的核心在于现有公司不愿意引入初期用户体验可能不如其现有精细产品的新产品或技术。这些公司担心采用这样的创新可能会疏远其当前的客户群，因为这些客户已经习惯了某种程度的精致和可靠性。这种迟疑源于可能破坏用户长期培养起来的期望的风险。

2.1代理的不可预测性与用户信任

像谷歌、苹果和微软这样的大型科技公司已经在经过验证的技术和商业模式上建立了他们的帝国。引入完全自主的agent代表着与这些既定规范的重大偏离。这些agent，尤其是在早期阶段，不可避免地会有不完善和不可预测的地方。人工智能模型的非确定性本质意味着即使经过广泛测试，也总是存在意外行为的风险。

对这些公司来说，风险非常高。一个失误不仅可能损害他们的声誉，还可能使他们面临重大的法律和财务风险。这创造了一个使他们谨慎行事的强烈动机，可能从而错过agent领域的先发优势。

对于考虑部署agent的集中式提供商来说，客户抗议的风险非常大。与可以快速转向且没有太多损失的初创公司不同，已建立的科技巨头拥有数百万期望一致、可靠服务的用户。agent的任何重大失误都可能导致公关噩梦。

考虑一个场景，其中agent代表用户做出了一系列糟糕的财务决策。由此引发的强烈抗议可能会侵蚀多年精心建立的信任。用户可能不仅会质疑agent，还会质疑公司基于人工智能的所有服务。

2.2模糊的评估标准和监管挑战

此外，如何评估何为“正确的”代理回应进一步使问题复杂化。在许多情况下，我们不清楚代理的回答是否真的有误，还仅仅是意外。这个灰色地带可能会导致争议，进一步损害客户关系。

也许集中式agent提供商面临的最艰巨障碍是不断发展且复杂的监管环境。随着这些agent变得更加自主并处理越来越敏感的任务，它们进入了可能带来重大挑战的监管灰色地带。

金融法规特别棘手。如果agent代表用户做出金融决策或执行交易，它可能会受到金融监管机构的监管。此外，合规的要求可能会很广泛，并在不同司法管辖区有显著差异。

还有责任问题。如果agent做出的决定导致用户财务损失或其他伤害，谁应该负责？用户？公司？人工智能本身？这些都是监管机构和立法者刚刚开始处理的问题。

2.3模型偏见可能成为争议的来源

此外，随着agent变得更加复杂，它们可能会触犯反垄断法规。如果一家公司的agent始终倾向于该公司自己的产品或服务，这可能被视为反竞争行为。这对已经因市场主导地位而受到审查的科技巨头尤其重要。

人工智能模型的不可预测性为这些监管挑战增加了另一层复杂性。当Web2无法完全预测或控制人工智能的行为时，其很难保证遵守法规。这种不可预测性可能导致Web2 agent的创新变慢，因为公司需要应对这些复杂问题，这反倒可能会给更灵活的Web3解决方案带来优势。



## 3.Web3的机遇

随着LLM底层模型能力的提升，agent有机会进入下一形态，具备相对较高自主性的agent。目前看大公司是不太可能敢碰这个方面的，可能帮用户定个pizza就是极限了。创业公司可能会大胆一下，但会面临很多技术障碍，比如agent自身不具备身份，任何操作都需要借用agent使用者的身份和账号。即使借了身份，传统体系也不是那么容易支持agent去自如的进行操作。Web3技术为人工智能代理开发提供了独特的机会，可能解决集中式提供商面临的一些挑战。Web3体系下，agent可以通过掌握钱包实现多个DID，无论是通过加密进行支付，还是使用各类无许可的协议都对agent非常友好。而当agent开始进行复杂的经济行为的时候，agent和agent大概率会有高强度的交互。这时候agent之间的相互猜疑如果没有办法得到解决，agent经济体系就不是一个完整的经济体系。这也是可以利用加密技术来解决的一个方面。

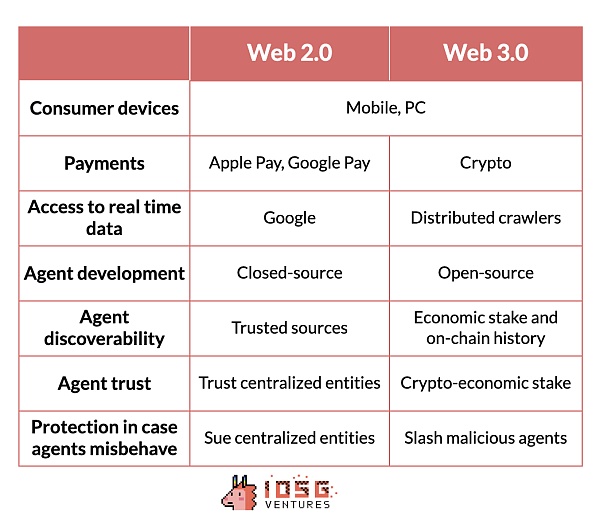
另外，Crypto-economic激励可以促进代理发现，并提供一个如果代理行为不当可以被削减质押或罚没的惩罚。这创造了一个自我调节的系统，其中好的行为得到奖励，坏的行为受到惩罚，因此可能减少集中监督的需求，并为那些早期采用将金融交易委托给完全自主代理的人提供一定程度的安心感。

Crypto-economic质押具有双重作用，在行为不当时需要削减，同时也作为发现agent过程中的关键市场信号。无论是对其他代理还是寻找特定服务的人来说，直觉很简单，质押越多，市场对特定代理性能的信任就越高，用户的心态就越平静。这可能会创造一个更加动态和响应迅速的agent生态系统，其中最有效和最值得信赖的代理会自然而然地脱颖而出。

Web3还能够创建开放的agent市场。与信任集中式提供商相比，这些市场允许更大程度的实验和创新。初创公司和独立开发者可以为生态系统做出贡献，可能导致agent的进步地更快和专业化。

此外，像Grass和OpenLayer这样的分布式网络可以为agent提供访问开放互联网数据和需要身份验证的封闭信息的机会。这种对多样化数据源的广泛访问可能使Web3 agent能够做出更明智的决策并提供更全面的服务。

Web 2.0与Web 3.0对比





## 4.Web3人工智能代理的局限性和挑战

4.1 加密支付的有限采用

如果我们不反思Web 3.0代理将面临的一些采用挑战，这篇文章就不完整。房间里的大象是加密货币作为链下经济支付解决方案的采用仍然有限。目前，只有少数在线平台接受加密支付，这限制了基于加密的agent在实体经济中的实际用例。如果没有加密支付解决方案与更广泛经济的深度整合，Web 3.0代理的影响将继续受到限制。

4.2交易规模

另一个挑战是典型在线消费交易的规模。这些交易中有许多涉及相对小额的钱，这可能不足以证明大多数用户需要无信任系统。如果存在中心化的替代方案，普通消费者可能看不到使用去中心化agent进行小额、日常购买的价值。



## 5.结束语

由于非确定性模型的不可预测性导致科技公司不愿提供完全自主的AI agent，这为加密初创公司创造了机会。这些加密初创公司可以利用开放市场和crypto-economic安全来弥补代理潜力与实际实施之间的距离。

通过利用区块链技术和智能合约，加密人工智能代理可能提供中心化系统难以匹敌的透明度和安全性水平。这对于需要高度信任或涉及敏感信息的用例可能特别有吸引力。

总之，虽然Web2和Web3技术都为人工智能代理开发提供了途径，但每种方法都有其独特的优势和挑战。人工智能代理的未来可能取决于如何有效地结合和完善这些技术，以创造可靠、值得信赖和有用的数字助手。随着该领域的发展，我们可能会看到Web2和Web3方法的融合，利用各自的优势来创造更强大和多功能的人工智能代理。