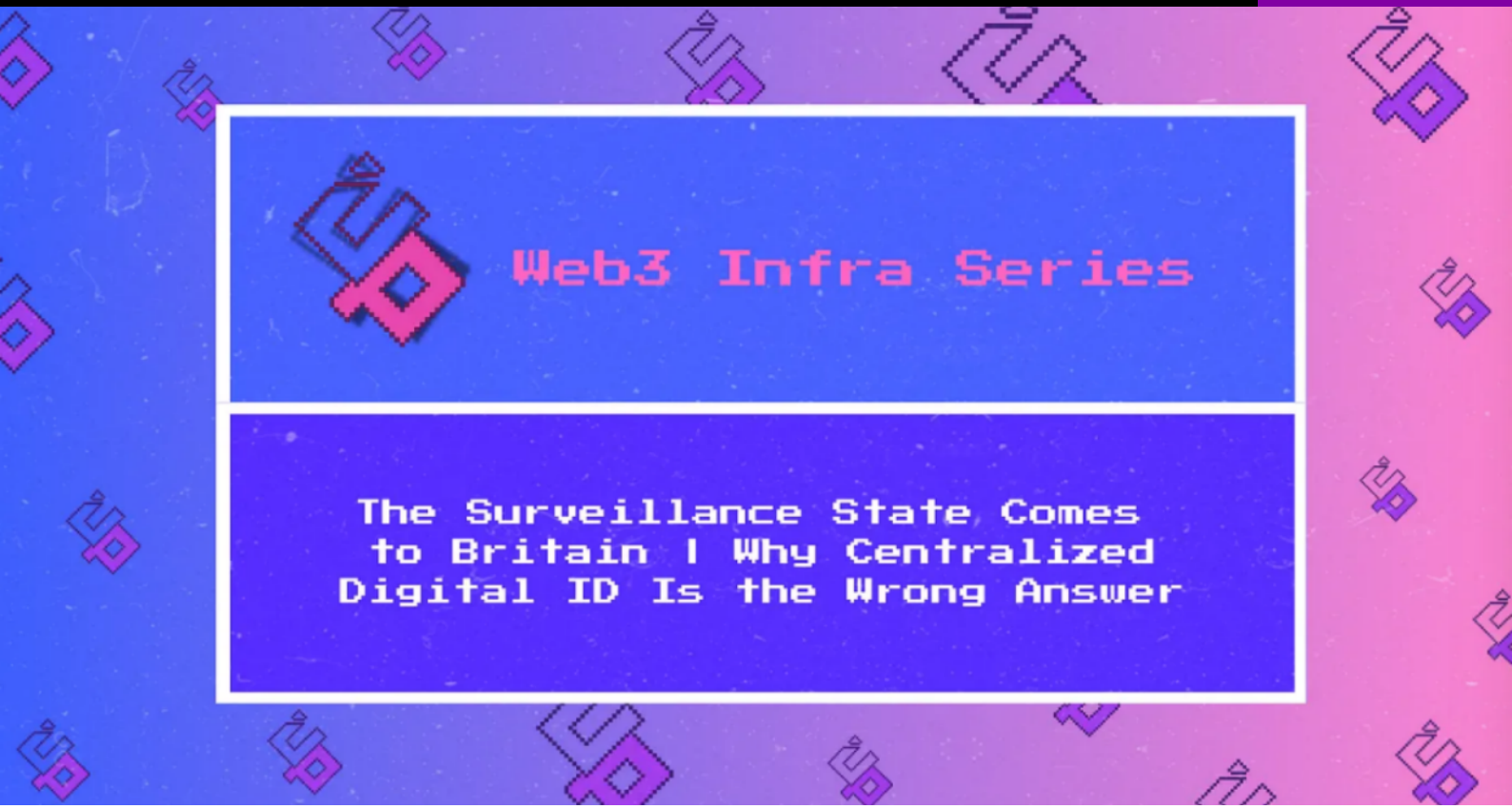
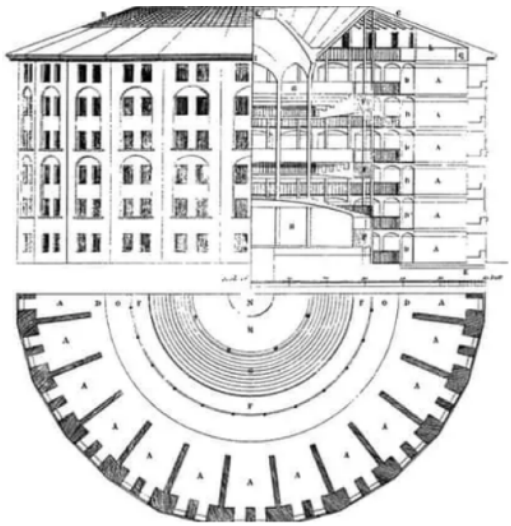


Web3 基础设施系列 | 监控国家降临英国 | 为什么中心化数字身份是错误的答案

1785年，英国哲学家杰里米·边沁设计了一种完美的监狱，他称之为“全景监狱”。其特点是中央设有瞭望塔，四周环绕着排列成圆形的牢房，一名狱警可以观察每个囚犯，而囚犯却浑然不知。这种设计对心理的影响非常深远，囚犯会不断调整自己的行为，即使没有监视，也会假设自己受到了监视，从而形成一种持续的自我监控状态，仅仅通过观察就能实现控制。

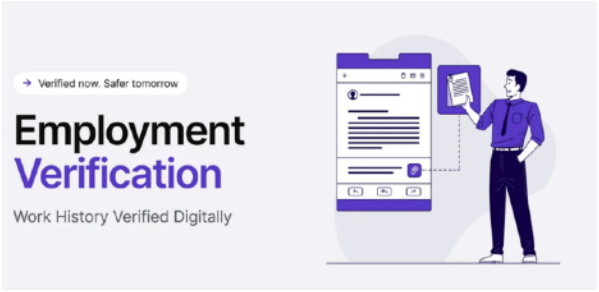


240年后的今天，英国首相基尔·斯塔默宣布强制推行数字身份证，在全国范围内构建了边沁的圆形监狱。这标志着公民与政府关系的根本性转变，他们用来之不易的隐私权换取了虚假的便利承诺。时机的选择暴露了伪装成进步的政治投机主义的本质：世界各国政府抓住危机时刻，将全面的人口监控常态化，而民粹主义在移民问题上的压力，为监控基础设施提供了便利的掩护，而这些基础设施的用途远远超出了其既定的用途。

英国的这项计划计划于2029年实施，要求所有公民和合法居民持有基于智能手机的数字身份证件，用于就业验证。尽管官员承诺这些身份证件无需每日携带，但正在建设的基础设施却为比移民管控更具侵略性的措施奠定了基础。历史告诉我们，监控系统一旦建立，其范围永远不会受到限制，而是会演变成全面的社会控制工具，其最初的支持者会对此感到震惊。

政府的宣传套路与专制政权的惯用伎俩如出一辙，承诺效率、安全和现代化，使数字身份证看起来像是必然的进步，而非潜在的越权行为。回想一下东德，斯塔西（Stasi）将公民身份识别变成了一种无处不在的监控机制，以行政必要为幌子追踪日常生活并控制行动。如今，爱沙尼亚、丹麦和澳大利亚等国家被视为数字身份系统带来实际效益的成功案例，它们构建了一种技术进步的叙事，掩盖了人们对权力和控制的更深层次的担忧。

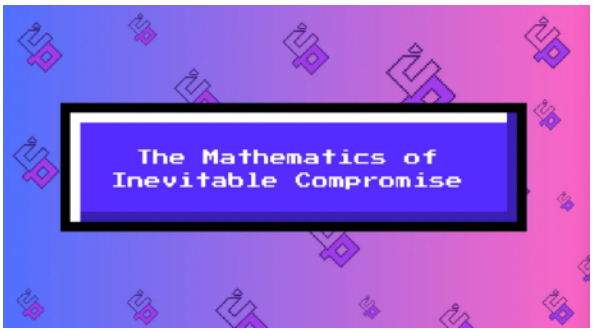
这种说法将监控基础设施描绘成纯粹的行政便利，掩盖了政府监管力度空前的现实。



如果我们揭开行政效率的面纱，就会发现一幅更加令人不安的景象：这些系统正以惊人的速度从用途有限的工具演变成全面险恶的监控基础设施，今天的就业验证将成为未来医疗、银行、交通乃至公民生活方方面面的访问控制。其技术架构揭示了真正的野心：中心化的数字身份系统创建了全面的档案，实时追踪用户的移动、交易、关系和行为，因为每个验证请求都将成为庞大政府数据库中的数据点，构建公民活动的详细地图。

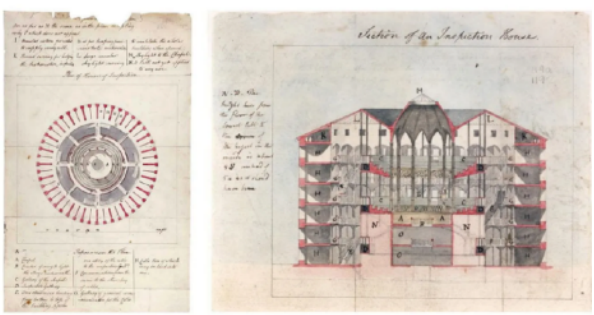
国际特赦组织英国分部的隐私倡导者警告称，此类系统“存在巨大的身份盗窃风险，并为黑客和网络犯罪分子提供诱饵”，但与政府积累大量

人口数据档案所带来的政治风险相比，网络安全风险绝对微不足道。一旦这些基础设施建成，扩大监控权力的诱惑就变得无法抗拒，将最初的行政便利转变为社会和政治控制的工具，从根本上改变了个人自主权与国家权力之间的关系。

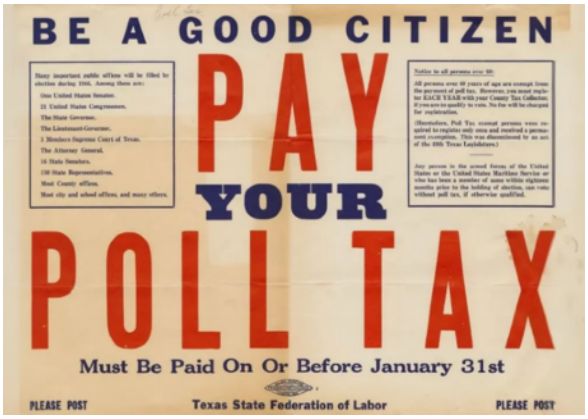


边沁的圆形监狱在他有生之年从未真正建成，但其心理学原理自此便萦绕在监狱设计中，其天才之处在于行为矫正而非建筑创新。19世纪英国维多利亚时代的济贫院也采用了类似的监视机制，以机构照护为幌子，通过严格的观察和行动控制来监管穷人。当人们认为自己可能受到监视时，他们会自我监督，从而构建了一个通过监视的简单可能性而非持续存在来运作的控制系统。

现代英国正在构建一个技术化的圆形监狱，公民们知道他们的每一次数字互动都可能被监控和记录，这从根本上改变了个人自主权与国家权力的关系，其方式甚至会让自由民主的缔造者感到震惊。



排斥效应加剧了这些监控担忧，正如大赦国际指出的那样，“许多老年人没有智能手机或无法正确登记”，“有些人可能难以获得服务”，从而造成系统性歧视，使技术合规成为获得完全公民权的先决条件。历史上，类似的官僚障碍，例如吉姆·克劳时代的人头税和南非的通行证法，都利用证件要求剥夺社区的权利并进行隔离，这表明身份强制执行可以成为社会排斥的工具。



这实际上将社会划分为能够驾驭政府强制系统的人和无法驾驭系统的人，从而形成了一种双重公民身份，基本权利取决于技术素养和智能手机拥有权，而非法律地位或民主参与。

想象一下，当就业等基本权利取决于维持有效的数字凭证时，会发生什么？政府获得了前所未有的权力来控制个人行为，而那些反对政策、参与抗议或从事政治反对活动的公民可能会发现他们的数字身份特权受到限制或被彻底剥夺。经济流放的基础设施变得像更新数据库条目一样简单，从而创建了一个系统，在这个系统中，政治上的一致性成为经济生存的必要条件，而异议最终将面临被社会数字排斥的惩罚。

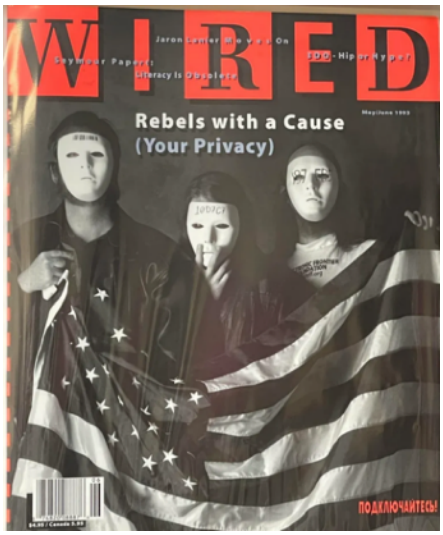
1970年，计算机科学家詹姆斯·马丁（James Martin）撰文探讨了集中式数据系统的“鱼缸效应”。他指出，数据存储库越大、价值越高，对攻击者的吸引力就越大，因为他们可以专注于高价值目标，而不是分散的小型数据库。集中式数字身份系统是这一原则的终极体现，它构建了包含数百万人数字身份的存储库，为黑客创造了难以抗拒的目标，他们可以用最小的努力造成最大的破坏。

当这些系统被攻破时——数学上的确定性告诉我们它们会被攻破——损害会同时波及整个人群，相比之下，个人身份盗窃显得微不足道，因为攻击者获得的是完整的个人资料，而不是孤立的信息片段。政府数据囤积造成了宪法学者所说的“道德风险”，权力的积累不可避免地导致滥用，因为全面的监控基础设施变成了政治控制而非行政效率的工具。

每个数据库都面临着来自老练对手的持续攻击，包括政府支持的、寻求情报的黑客、追求利益的犯罪组织，以及利用特权访问的不法内部人员。因此，问题不再是这些系统是否会被入侵，而是何时以及损害将蔓延到多大程度。

一旦攻击者获得政府精心汇总成便捷软件包的个人信息集中存储库的访问权限，入侵将影响到整个人口，而非个人账户，从而造成连锁故障，同时危及所有人的安全。

20 世纪 90 年代，一群密码学家和计算机科学家开始探索关于数字隐私和个人主权的激进理念，他们设想未来由数学而非法律或信托来保护个人隐私，使其免受政府过度干预和企业监控。这些“密码朋克”为现代区块链技术奠定了基础，并为我们当前的危机奠定了关键基础，即去中心化身份系统，将控制权交还给个人，而不是将其集中在政府数据库中。



其根本洞见依然有力，因为中心化数字身份的缺陷源于中心化控制而非数字验证本身。这表明，基于区块链基础设施构建的自主主权身份系统可以提供一种截然不同的方法，既能保留验证优势，又能消除监控风险。这些系统并非将控制权集中在政府数据库中，以免成为黑客攻击的目标和政治压迫的工具，而是允许用户维护自己的加密安全凭证，并决定在何种情况下与谁共享哪些信息。

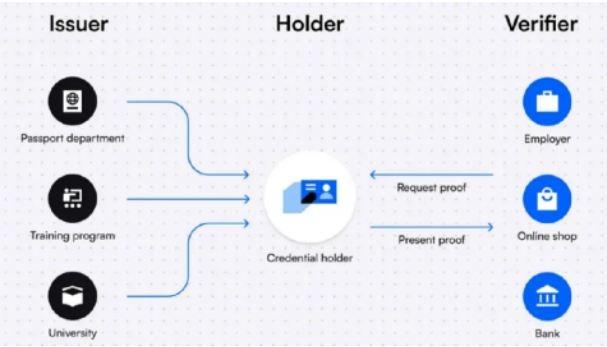
因此，个人数据将分布在整个网络中，用户对其信息保持精细控制，从而创建无需数据收集和监控即可进行验证的系统，而中心化系统的设计初衷正是如此。其技术基础依赖于成熟的加密技术，这些技术能够实现无需披露即可进行验证，使人们无需透露移民身份、国籍或地址即可证明其工作权利，无需向政府监控数据库公开其完整的个人历史记录即可证明其服务资格。

零知识证明通过数学突破实现了这一点，它允许在不泄露底层数据的情况下验证特定声明，因此人们可以在不透露确切出生日期的情况下证明自己已年满 18 岁，或者在不透露签证状态或国籍的情况下证明工作许可。这些并非理论构想，而是经过验证的数学工具，能够提供比中心化系统更强大的安全保障，并保护个人隐私和自主权，通过数学确定性而非机构信任，实现无需监控的验证。

密码朋克愿景需要的不仅仅是密码学理论，还需要能够满足现实世界对安全性、可扩展性和用户体验需求的实用基础设施，因为它弥合了理论可能性与实际应用之间的差距。像英国数字身份方案这样的中心化系统中的每一个缺陷都指向了去中心化替代方案必须解决的特定技术要求，从防止政府监控到消除单点故障，再到维护用户对个人数据的自主权。

在去中心化身份实现中，Uptick DID 展示了如何将这些原则转化为实用的基础设施，通过成熟的技术架构来解决中心化系统的每个故障。

英国方案的根本弱点在于中心化，它创建了蜜罐，攻击者只需一次入侵就能危及数百万个身份。Uptick DID 基于 Cosmos-SDK 构建的分布式架构，旨在让用户通过私钥对自己的凭证进行加密控制，从而减少身份数据在中心数据库中的集中度。



政府锁定是另一个重大失败，因为受困于英国体系的公民，当他们的数字身份特权因政治原因或官僚错误而受到限制时，别无选择。Uptick DID 通过 Uptick 跨链桥和 IBC 协议在多个区块链环境中运行，旨在跨以太坊、Cosmos、币安智能链和 Polygon 等不同生态系统提供一致的身份管理，因此，即使政府颁发的凭证受到限制的用户，仍然可以通过超越

政治界限且无法单方面撤销的去中心化网络验证身份并访问服务。

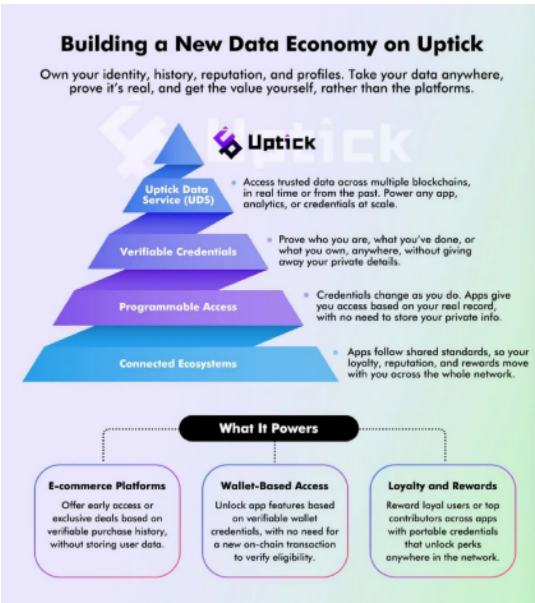
嵌入在中心化数字身份系统中的监控架构会追踪每一项验证请求，构建公民行为的全面档案，从而实现政治控制。Uptick DID 通过可验证凭证解决了这一问题，这些凭证通过零知识证明来证明身份，使用户无需透露国籍、签证状态、工作经历或任何超出特定凭证范围的信息即可证明其拥有工作授权。该架构旨在实现点对点验证，通过加密签名确认真实性，从而减少对监控中介机构的依赖。

数据持久性在中心化系统中会带来额外的风险，因为如今收集的信息会无限期地保存在政府数据库中，并被用于公民从未授权或想象过的用途。Uptick 的基础设施通过 IPFS 集成了 Uptick Storage，用于去中心化凭证存储，创建了防篡改的记录，无需依赖中心化服务器即可访问。用户可以控制自己持有的凭证、哪些验证者可以访问这些凭证以及何时撤销访问权限，从而提供对数字身份的精细控制，而中心化系统在设计上是拒绝的。

英国将缺乏智能手机或技术素养的公民排除在外，揭示了中心化数字身份系统如何造成双重公民身份。Uptick 通过用户友好的设计解决了这个问题，使去中心化身份无需太多技术专业知识即可访问，并通过加密安全的密钥对系统和零知识证明将直观的界面与全面的加密保护相结合，从而在无需机构监控的情况下提供机构级安全性。

Vouch 平台和 Upward Wallet 通过简化的凭证管理实现了这种便捷的方法。持有者通过“发行者-持有者-验证者”模型完全控制其凭证，发行者负责处理凭证创建的复杂性，验证者可以快速确认其真实性。

或许最重要的是，当政府滥用权力、任意限制访问权限或将监控范围扩大到超出既定目的时，中心化数字身份系统无法承担责任。Uptick 的去中心化数据服务旨在提供透明的追踪，其中加密签名保持真实性，并通过可审计的流程以不可篡改的方式记录在链上，用数学证明取代机构承诺，使每个操作都完全可追溯，并防止了中心化监控系统特有的隐形滥用。



这种问题解决架构向我们展示了，通过 Uptick DID 实现的去中心化身份并非简单地在区块链基础设施上复制中心化系统，而是从根本上重新构想了数字身份的运作方式，使其服务于用户而非监视用户。每项技术选择都针对中心化方法中的特定缺陷，创造出无需监视的验证、无需排斥的自主性以及无需集中权力（后者必然会导致腐败）的安全性。

去中心化身份的经济效益远不止于成本节约，但考虑到不同数字身份管理方法的全生命周期成本和经济效益，这些优势就显得尤为重要。英国的数字身份系统需要政府在基础设施、持续维护成本以及行政和支持方面投入巨额资金，这些成本将给纳税人带来负担，无论他们是否选择使用该系统，因为这会为扩大监控范围创造经济诱因。

像 Uptick 这样的去中心化系统确实将成本分摊到整个生态系统，并消除了大部分行政管理成本，允许通过智能合约进行点对点验证，从而降低管理成本，并通过数学而非制度保障来提高安全性和隐私性。尽管去中心化系统需要在用户教育和基础设施建设方面进行初始投资，但消除持续的行政管理成本和中心化维护成本将带来长期的经济优势，这种优势会随着网络效应降低每用户成本而不断累积。

Uptick 将去中心化身份与智能合约自动化相结合，可以简化凭证验证等用例。可验证凭证使用户无需依赖中心化服务即可证明其身份、资格或属性，从而带来效率提升，其效果不仅限于直接的成本节约，还涵盖减少经济交易中的摩擦。

这些经济优势形成了积极的反馈循环，鼓励创新和应用。随着越来越多的组织和个人加入 Uptick 的去中心化身份生态系统，并通过提升效率和自动化程度持续降低成本，网络效应将为所有参与者创造价值。最终形成了一个良性循环：更优的技术创造更优的经济效益，进而推动更广泛的应用和进一步的技术改进。与中心化替代方案相比，去中心化系统更具吸引力。中心化替代方案会给用户带来他们从未选择承担的监控成本，而其收益将集中在政府机构及其承包商手中。

去中心化身份系统最根本的方面或许在于其治理模式，它用数学确定性和社区共识取代了政治控制，从而消除了中心化系统中常见的腐败和偏见。Uptick 的实施涵盖了 DAO 功能，通过其社交 DAO 基础设施，允许社区建立和维护治理标准和社区决策流程，从而提供能够适应不同社区需求的治理，并通过透明、可审计

且不可篡改的链上流程，确保安全性和可靠性。

DAO 治理提供了政府系统通常缺乏的透明度和问责制，所有治理决策均记录在链上，任何社区成员均可审计，从而确保身份验证标准的一致和公平应用，避免了中心化系统中可能存在的政治操纵或歧视性待遇。尽管 DAO 治理面临着去中心化决策固有的协调挑战，但链上流程的透明度和不可篡改性提供了中心化政治系统无法比拟的问责保障，从而对权力形成了数学而非制度上的约束。

去中心化治理模式允许在身份验证方法上进行创新和试验，让不同的社区能够测试各种方法，因为成功的创新是通过自愿采用而非政治当局自上而下的强制要求传播的。这创造了一个治理模式的市场，在大多数情况下，最佳方法的成功取决于自身能力而非政治权力，从而避免了中心化系统特有的监管俘获和官僚僵化，因为它允许社区共同拥有和管理其身份验证系统。

这种所有权促成了利益相关者的协调，鼓励长期可持续性，而不是驱动政府政策的政治短视主义，从而形成服务于社区需求而非政治野心的治理体系。

英国的数字身份计划是全球趋势的一部分，即通过数字身份系统加强政府监控和控制。类似的项目正在世界各地实施，因为它们被人们熟知的安全、效率和防欺诈等论调所掩盖，掩盖了其作为人口监控基础设施的真正目的。这一刻将定义数字社会的演变，决定我们是接受监控作为便利的代价，还是通过技术创新而非政治妥协，构建既能维护安全又能维护自由的替代方案。

通过 Uptick DID 等解决方案实现的去中心化身份识别，为抵制这种数字威权主义趋势提供了一条途径，因为它保留了数字身份识别所能提供的合法优势，向世界展示了安全高效的身份验证是可能的，而无需将控制权交给必然会滥用权力的中央集权机构。区块链的全球性意味着去中心化身份识别系统可以通过 Uptick 的跨链协议跨越国界运行，即使在本国政府实施限制性数字身份识别方案的情况下，也能为个人提供身份验证功能，因为它创造了超越政治控制的国际互操作性。

随着越来越多的个人和组织采用 Uptick 的去中心化身份基础设施，他们给政府带来了压力，迫使政府放弃专制的数字身份方案，转而采用尊重隐私的替代方案。去中心化系统的经济和效率优势，为企业和机构提供了令人信服的理

由，即使面临政府的阻力，他们也要支持采用去中心化身份。尽管政府可能会通过支持中心化系统的法规或强制要求来抵制，但经济和安全优势创造了能够克服政治阻力的激励机制，因为企业和公民认识到被排除在跨辖区运营的去中心化生态系统之外的代价。

从本质上讲，网络效应为采用创造了强大的激励机制，可以克服政治阻力，因为参与的收益会随着网络规模的扩大而增加，而被排除在 Uptick 等去中心化身份生态系统之外的代价对组织和个人来说都越来越明显。

英国正处于杰里米·边沁时代英格兰的境地，正处于一种伪装成进步的新型社会控制的门槛上。政府的数字身份方案构建了全面的监控基础设施，将前所未有的权力集中在中央集权机构手中，同时也为公民的隐私和自主权带来了巨大的漏洞。另一种选择是走向像 Uptick DID 这样的去中心化系统，它提供身份验证的优势，但又不带有专制色彩，使用数学保证而非政治承诺来保护个人自由，同时保留了数字身份验证的合法优势。

如今，构建比中心化替代方案更安全、更私密、更高效的去中心化身份系统的技术已经存在。Uptick 的 DID 基础设施证明，这些系统能够满足现实世界的需求，因为它们通过实际操作而非理论可能性来维护个人主权和民主价值观。数字自由的基础设施之所以存在，是因为经济激励机制倾向于选择尊重隐私的解决方案而非监控系统，在政府数字身份方案根深蒂固、无法逆转之前，只剩下选择去中心化身份而非中心化控制的政治意愿。

剩下的就是认识到，英国的经验警示我们，当公民接受安全和便利的承诺，而不去审视潜在的权力结构，也不去考虑那些既能保障安全又能保障自由的替代方案时，民主社会会多么迅速地接受专制技术。数字身份的未来取决于今天的选择，这决定了我们是接受英国政府关于强制实施数字身份方案的愿景，将权力集中在中央集权机构手中，还是通过像Uptick Network这样的平台构建去中心化的替代方案，通过技术创新而非政治屈服来维护个人自主权和隐私。

问题不在于我们是否拥有实现去中心化身份的技术，而在于我们是否有智慧和勇气在数字全景监狱变得像边沁的实体版本所设想的那样不可避免之前做出选择。

在边沁的时代，全景监狱仍然只是一个从未完全实现的理论构想，但今天的数字全景监狱没有这样的限制，这使得我们的选择比以往任何一代人在自由与控制的斗争中所面临的选择都更加紧迫，也更加重要。

hello@uptickproject.com

@Uptickproject

@Uptickproject

Uptick Network

Uptick Network