Web3 基础设施系列 | 打破验证中间人陷阱

每一份工作申请、公寓租赁和专业执照申请都需要你再次证明你之前已经向颁发机构证明过的资格。

例如，大学在你毕业时会确认你的学位，但雇主仍然需要支付 15 到 20 美元，通过像美国国家学生信息交换中心 (National Student Clearinghouse) 这样的第三方服务机构再次验证，而且通常还会捆绑背景调查费用，导致成本更高。专业委员会在颁发执照时会确认你的执照，但客户需要支付验证费来确认你持有该执照。

此外，还有一些背景调查公司会收取 30 美元来验证你之前的雇主已经在系统中记录的工作经历。

事实上，这种模式在你的职业生涯中会重复数千次，因为每个新的雇主、房东、认证机构或客户都会要求你重新验证那些自最初颁发机构颁发以来从未更改过的资格证书。 2015年获得的学士学位，在2018年换工作时需要重新验证，2020年申请研究生院时需要再次验证，2022年租房时需要再次验证，2024年申请专业资格认证时需要再次验证，尽管证书本身在每次验证中都完全相同。

传统的学历认证通过集中式中介机构运作，每次有人需要证明自己已获得的资格时，这些机构都会收取费用，从而形成了一个基于重复验证的数十亿美元产业。同样的学位、执照或工作记录，即使在颁发数十年后，仍然能够持续产生收入。美国国家学生信息交换中心（National Student Clearinghouse）每年在其约3600家机构的网络中处理数百万次学历认证，作为一家非营利机构，其每年仅从这些认证服务中获得的收入就超过1亿美元。

这些服务之所以联系在一起，是因为它们都基于一种机构间脱节的商业模式：大学、雇主和执照颁发机构拒绝颁发其系统已验证的可移植证书，迫使证书持有者反复购买验证服务，而不是提供他们真正能够掌控的选项。大学在你毕业时确认你的学位已存在于他们的数据库中，但他们没有提供任何机制让你在不付费给中间人的情况下向第三方证明这一点，而这些中间人查询的数据库正是你的毕业证书所引用的数据库。

Web3 基础设施彻底瓦解了这种信息提取方式。机构只需颁发一次可验证的证书，证书上的加密证明便永久有效，验证过程通过数学上的确定性而非数据库查询来实现。此外，隐私保护型证明允许选择性地披露信息，而不会将底层数据暴露给那些利用你的个人信息牟利的验证服务机构。

大学拥有一套名为注册系统的系统，用于追踪每个学位的授予情况，并将毕业记录存储在数据库中。当学位持有者需要验证学历以用于就业、继续深造或申请专业执照时，大学会查阅这些数据库。这些记录在初始数据录入后几乎无需大学维护，它们作为永久性数字文件存在，学位授予后便不再更改。

问题在于，大学没有为毕业生提供独立验证学历的机制，而是要求验证请求者直接联系注册办公室或使用指定的第三方服务，例如全国学生信息交换中心（National Student Clearinghouse）。毕业生在求职时会向潜在雇主提供学位信息，但雇主无法轻易相信毕业生的说法，因此他们不得不付费请验证服务机构查询大学数据库，以确认学位是否如毕业生所述真实存在。

这就形成了一种持续的收入来源：同一个学位会在毕业生的整个职业生涯中产生数十次验证费用，因为每个新的雇主、研究生项目或专业认证机构都需要独立的验证信息。 2020 年的学士学位在未来十年内可能需要被五家雇主验证、三个不同的专业认证项目验证、两次研究生申请验证，以及各种公寓租赁或安全许可的背景调查验证，总共会产生超过 500 美元的验证费用，而大学在颁发学位证书时只确认过一次。

美国国家学生信息交换中心 (NSC) 在学历认证领域几乎处于垄断地位，为超过 3600 所院校处理学历认证，覆盖了高达 97% 的美国学生。大学将认证工作外包给 NSC 是为了避免接听雇主电话带来的行政压力，但 NSC 对每次验

证查询都收取费用，从基本的入学确认 4.95 美元到学位验证 14.95 至 19.95 美元不等，从大学免费提供给 NSC 的数据中榨取利润。

这种经济模式造成了一种反常的激励机制：大学没有动力颁发可携带的学历证书，因为验证过程不会产生任何成本。雇主支付验证费用，毕业生忍受等待确认的漫长过程，而国家安全委员会（NSC）则通过介入院校和验证请求者之间来获取收入。

大学将行政工作外包，并且没有压力去改变那些在他们看来运行良好的系统。

这种验证流程违反了基本的数据所有权原则：毕业生通过多年的学术努力和学费支付获得了学历证书，但却没有任何独立的成就证明可以在不经过院校或其指定验证机构的情况下出示。事实上，文凭除了纸面上的内容之外，没有任何实际意义，因为任何人都可以花100美元在网上购买假文凭，如果没有数据库验证，这张纸质文凭就毫无价值，而数据库验证只能由大学或其授权机构提供。

Uptick 的 DID 基础设施通过符合 W3C 标准的去中心化标识符解决了这个问题，使院校能够颁发可验证的证书，这些证书以加密签名数字证书的形式存在，毕业生可以将其存储在个人钱包中。

当大学授予学位时，他们可以颁发一份使用院校私钥进行加密签名的可验证证书，其中包含学位详情的结构化数据，毕业生可以将这些数据存储在自主身份钱包中，而无需依赖院校数据库或纸质文凭。目前，机构已经可以通过 Vouch 等平台实现这种证书颁发模式的部分功能。在 Vouch 等平台上，任何人都可以使用持有者的 DID 直接颁发证书，或者生成毕业生访问的声明链接，以便获取其可验证的学位。这表明，加密证书的颁发无需大学开发定制的 Web3 基础设施即可实现。

当毕业生需要向雇主证明其学历时，他们只需从钱包中出示可验证证书，雇主即可通过数学方法验证大学的加密签名，而无需联系大学或支付验证服务费用。签名证明证书来自大学，颁发给出示证书的特定毕业生，并且自颁发以来未被篡改，从而提供绝对的数学确定性，无需数据库查询或第三方验证服务。

其工作原理基于公钥加密技术。大学维护公钥，并通过可验证的链上注册表发布，将机构身份映射到加密地址，允许任何人引用和验证签名，但只有大学持有签署证书所需的私钥。伪造的证书会立即无法通过签名验证，因为造假者无法在没有大学私钥的情况下生成有效签名，这使得伪造在计算上不可行，而不仅仅是难以通过人工验证流程检测。

Uptick 的可编程 NFT 协议旨在将这些证书作为不可转让的代币，绑定到具有灵魂绑定特征的特定 DID，从而防止证书欺诈，即个人购买或

租用他们未获得的证书。该证书以 NFT 的形式存在，并通过智能合约与毕业生的 DID 绑定。智能合约可防止证书转移到其他账户，因为尝试转移证书会失败，接收账户无法提供加密证明，证明其与证书所代表的学位相关。

背景调查公司通过核实前雇主已记录在其内部系统中的工作经历来赚取巨额收入。Checkr、HireRight 和 Sterling 主导着全球价值约 120 亿美元的背景调查行业，它们对每位候选人收取 30 至 100 美元的费用，以核实雇主人力资源数据库中已有的工作日期、职位和薪资信息。

核实流程是通过背景调查服务直接联系候选人的前雇主，要求确认候选人是否在所声称的日期和职位上工作过。这需要大量的人工，因为人力资源部门需要处理核实请求、交叉核对内部记录，并向背景调查服务提供书面确认，而背景调查服务再将结果转发给潜在雇主。

每次工作变动都会触发这一核实循环，即使基本事实没有改变，相同的工作记录也需要重新核实。这意味着，某人在2018年至2022年间曾在A公司工作，但当他2022年加入B公司时，其在A公司的工作经历需要再次验证；2024年加入C公司时，需要再次验证；2025年申请专业认证时，又需要再次验证。即便其在A公司的工作经历始终是一个不变的历史事实，且已被多次确认。

前雇主承担了处理验证请求的行政成本，但他们没有动力签发可转移的就业证明，因为验证过程中的摩擦对他们来说并非负担。背景调查公司通过介入需要确认的雇主和持有记录的前雇主之间来收取验证费用，而潜在雇主则承担了这些成本，因为如果雇佣未经验证的候选人，一旦就业声明被证实为欺诈，他们将承担法律责任。

最终，我们陷入了这样一种境地：员工无法独立证明自己的工作经历，除非联系前雇主或付费请背景调查公司联系他们。W-2税表可以证明收入，但无法证明职位或职责；录用通知书可以证明初始工作，但无法证明工作时长；工资单可以证明特定时期的工作，但无法证明完整的就业历史。

目前尚无任何便携式证据表明，员工可以控制展示其完整的职业发展轨迹，而无需前雇主对数据库查询作出回应。

Uptick 的可验证凭证框架旨在帮助雇主在员工离职时颁发加密签名的雇佣凭证，记录员工的

雇佣日期、职位、职责和绩效指标等结构化数据，这些数据由员工存储在他们控制的 DID 钱包中。

当员工申请新职位时，他们可以提供之前雇主的雇佣凭证，潜在雇主无需联系前雇主或支付背景调查费用，即可通过数学方式验证签名。

该框架采用与学术证书相同的公钥加密技术：前雇主使用私钥对雇佣记录进行签名，员工将签名凭证存储在钱包中，潜在雇主使用公钥验证签名，从而证明凭证来自所声称的雇主，而无需直接联系或查询数据库。加密签名提供了雇佣记录真实且自颁发以来未被篡改的数学证明，从而无需电话、电子邮件确认或背景调查服务。

通过零知识证明，员工无需透露完整的雇佣记录即可证明特定的雇佣关系，从而实现保护隐私的验证。员工无需透露具体日期、薪资信息或离职原因，即可证明其在特定公司担任特定职位超过两年，从而满足验证要求并保护个人信息免遭不必要的泄露。

这种选择性披露机制已在生产环境中应用。凭证持有者提交多属性凭证，但可以选择验证者可以访问哪些特定属性，例如仅披露“高级经理，2020-2024”，而将绩效评估和薪酬详情保密。加密签名用于确认所披露属性的真实性，而无需暴露完整的雇佣记录。

Uptick 的 DID 基础设施通过零知识证明协议实现这一功能。在该协议中，员工生成加密证明，证明其雇佣凭证符合特定标准，而无需泄露底层数据；验证者则通过数学方法确认这些证明，而无需访问完整的凭证。例如，要求求职者提供五年管理经验证明的潜在雇主，无需了解候选人的具体工作时间、薪资增长情况或曾就职的具体公司，即可验证其工作经历是否符合要求，只需确认其总体经验即可。

专业执照在职业生涯的多个阶段都需要验证，例如医生、律师、会计师、工程师和技术工人需要向雇主、客户、保险公司和监管机构证明其资质。各州执照委员会维护着追踪每位持证专业人士的数据库，存储着确认个人已完成所需教育、通过考试并通过继续教育保持有效执照状态的记录。

然而，执照委员会并不提供专业人士可以独立出示的便携式证明，而是要求验证请求者直接查询州数据库或使用专门的验证服务。医疗执照验证服务每次向医院收取 50 至 150 美元的费用，以确认医生在特定州持有有效执照；法律名录向律师事务所收取订阅费，以提供律师资质验证服务；工程委员会则要求对每位需要验证资质的专业人士进行人工验证。

这造成了验证方面的繁琐流程，持证专业人士每次加入新机构、接纳新客户、申请医疗事故保险或跨州工作时，都需要进行资质验证。一位在三个州获得执业资格的医生，由于获得医院执业资格、加入医疗集团、与保险网络签约

以及出差从事临时执业等原因，其执业资格每年可能需要验证五次，即使其执业资格全年保持有效且未发生变化，验证费用累计也可能超过 500 美元。

对于持有多个认证的专业人士而言，验证问题会更加复杂，因为除了基本执业资格之外，其他专业资格也需要单独验证。例如，一位拥有三个专科认证的医生，除了持有州级执业资格外，还持有来自不同委员会的专科认证，这使得验证过程更加复杂。医院在核查资质时，必须查询州级数据库以确认其执业资格，并联系专科委员会确认其专科认证状态，从而增加了行政管理和验证成本。

专业执业资格委员会往往不愿颁发可携带的执业资格证书，因为验证收入是委员会运营的资金来源，这些收入包括数据库访问费、打印验证信函费和在线验证服务费。特别是医疗委员会，由于医院、保险公司和资格认证机构需要支付定期费用来确认医生的执业资格，而这些费用实际上在颁发和续签执业资格时，委员会已经验证过这些资格，因此医疗委员会从验证服务中获得了可观的收入。

Uptick 的基础设施使执照颁发机构能够颁发可验证的证书，这些证书以加密签名的形式存储在 DID 钱包中。智能合约会自动更新证书状态，反映续期、继续教育完成情况或纪律处分等信息，而无需专业人员获取新的证书。

当医生续签行医执照时，执照颁发机构会通过执行智能合约更新链上证书的状态。任何验证证书的人都能看到反映最新续期的当前状态，而无需联系机构或支付验证费用。医疗委员会可以选择实施此方案：在医生通过考试后颁发初始执照作为可验证的证书，然后在满足继续教育要求后通过智能合约更新元数据。医院可以通过医生提供的二维码验证证书，而无需等待数天时间等待验证服务查询州数据库并返回确认信息。

该方案通过可编程证书实现：初始颁发会创建一个与专业人员 DID 绑定的基础证书，后续的机构操作会更新链上元数据，供验证者在检查证书时参考。医院在验证医生执照时，首先通过数学方法确认执照证书上委员会的签名，然后查询链上数据，根据委员会最新的续期信息确认当前的有效状态，从而无需直接查询数据库或通过验证服务机构进行验证。

选择性披露使专业人士能够在不公开完整监管记录的情况下证明其执照状态。除非出于验证目的需要，否则纪律处分、投诉或之前的状态变更等信息均保持私密。简而言之，这意味着医生可以在不披露过去曾被调查但最终未采取纪律处分的投诉的情况下，证明其持有有效的、不受限制的行医执照，从而满足验证要求并保护未导致限制的监管事项的隐私。

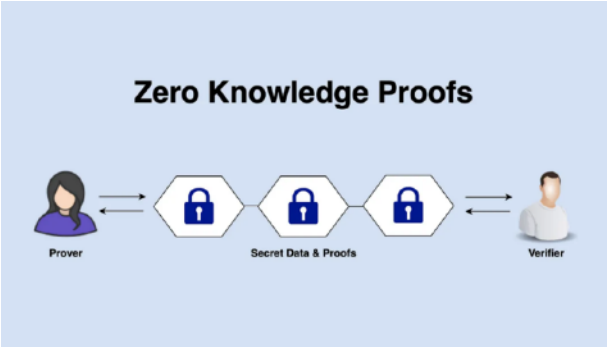
当前的验证流程意味着，持证人需要披露超出验证要求所需的个人信息，从而造成隐私泄露，而验证服务机构则通过数据聚合从中牟利。

当雇主要求进行背景调查时，员工授权验证服务机构访问完整的就业历史、成绩单、全面的犯罪记录和详细的信用报告，尽管雇主可能只需要确认特定信息，例如学位完成情况或无犯罪记录。

一份工作申请可能只需要确认是否拥有学士学位，但学历验证服务机构却被授权访问完整的成绩单，包括成绩、所修课程、学业警告记录和所获荣誉。就业验证也类似地提供了完整的就业历史，包括离职原因、是否符合再次聘用条件以及主管评价，而雇主可能只需要确认工作日期和职位。

这种过度披露的现象源于验证流程采用二元授权模式：员工要么授予完全访问权限，要么完全阻止验证，缺乏选择性披露机制，无法在不泄露底层数据的情况下证明特定信息。候选人若不公开GPA就无法证明自己已毕业，若不披露薪资历史就无法核实工作经历，若不披露完整的监管记录（包括从未导致纪律处分的投诉）就无法确认执照状态。

零知识证明协议通过加密技术解决了这些问题，使证书持有者能够在不泄露底层数据的情况下证明其证书的特定声明。这意味着，员工无需透露具体院校、毕业日期、专业或GPA，即可证明自己拥有认可大学的学士学位，既满足了基本的学位要求，又避免了详细的学术记录被不必要地泄露。



Uptick 的基础设施通过零知识证明（ZK-proofs）实现这一功能，该证明生成加密证明，确保凭证满足特定标准，同时不泄露凭证内容。当验证者需要确认候选人是否持有相关学位时，候选人的钱包会生成一个零知识证明，证明其可验证的凭证满足要求。验证者无需访问包含毕业日期、具体院校、课程或成绩的实际凭证，即可通过数学方式验证该证明。

这使得各种细致的验证场景成为可能：例如，可以通过范围证明来确认薪资要求，证明候选人之前的薪酬已超过阈值，而无需透露具体数字；可以在不泄露获得日期或续期记录的情况下验证专业认证；可以在不披露安全许可级别或颁发机构的情况下确认安全许可状态。

每次验证仅披露满足验证目的所需的最低信息，从而保护隐私并确保被验证声明的数学确定性。

验证中间人陷阱依然存在，因为当前的基础设施将凭证所有权分散在持有者无法独立访问的机构数据库中，人为地造成了对查询这些数据库并将结果打包提供给验证请求者的服务的依赖。

大学维护学位记录，雇主维护雇佣记录，执照颁发机构维护证书状态，但这些机构都无法提供持有者可控制且无需中介即可提供的可移植证明。

改变这种现状需要一种基础设施，其中凭证以加密签名数字证书的形式存在，持有者将其存储在自主身份钱包中；验证通过数学签名确认而非数据库查询进行；选择性披露能够提供保护隐私的证明，仅披露验证所需的信息。

机构已经通过这种基础设施颁发凭证，而无需具备 Web3 专业知识。他们通过接口设计凭证，自动处理加密签名，并通过无需始终在线系统或专用硬件即可在物理空间中运行的方法实现验证。每个组件都通过消除集中式依赖关系来解决当前系统中的特定缺陷，从而避免信息提取。

Uptick 的 DID 基础设施提供身份层，使凭证能够通过去中心化标识符绑定到特定个人，这些标识符可在各个机构间通用，无需中央注册机构或凭证颁发机构之间的协调。

员工来自多所大学、雇主和执照颁发机构的专业凭证均可引用同一个 DID，从而创建一个统一的身份，将来自不同来源的凭证聚合到一个由员工通过加密密钥而非机构权限控制的钱包中。

通过 W3C 标准颁发的可验证凭证提供数据层，使机构能够对凭证进行加密签名，员工能够将凭证存储在他们控制的钱包中，验证者能够通过签名验证来确认凭证的真实性，而无需联系颁发机构。凭证以结构化的 JSON 文档形式存在，其中包含声明数据和证明颁发机构创建声明的加密签名，二者结合可提供凭证真实性的数学确定性。

智能合约提供逻辑层，支持动态更新证书状态。证书的续期、撤销或修改均通过链上交易完成，无需重新颁发证书。因此，作为可验证证书颁发的医疗执照在续期后不会失效，而是由许可机构更新链上状态以反映续期情况。验证者通过智能合约查询自动检查证书的当前状态。

零知识证明协议提供隐私层，支持选择性披露。工作者无需披露底层数据即可证明证书的特定声明，验证请求者只需了解所需信息。工作者在保护详细信息免遭不必要的披露的同时，仍能提供数学证明，证明其证书满足验证要求。

通过 Uptick 的跨链桥 (UCB) 和 IBC 协议实现的跨链互操作性，使得在不同 Web3 基础设施上颁发的证书能够无缝协作，避免了因大学使用基于以太坊的系统而颁发的证书与雇主使用基于 Cosmos 的基础设施而颁发的证书无法互操作的情况。这种可移植性使得工作者可以从任何发行方（无论选择何种区块链）获取凭证，并向验证者提供统一的凭证集，而无需考虑底层技术架构。

验证中间人陷阱之所以持续存在，是因为制造这一问题的机构无需承担任何成本。大学、雇主和执照颁发机构维持着数据库垄断，它们之所以能从中获取验证收入，正是因为它们从不颁发可移植的证书。而任何有能力改变这种现状的人都面临着足够的压力。劳动者承担验证费用，雇主承担背景调查成本，而验证中介机构则从交易双方收取费用。如果证书颁发机构在颁发证书时直接对记录进行加密签名，那么这笔交易原本无需中介。

可验证证书改变的是验证交易背后的经济结构。因此，当大学在毕业生毕业时颁发加密签名的证书后，未来所有验证该证书的雇主都可以通过数学方式进行验证，而无需中间机构查询证书所引用的同一数据库来获取收入。2015年获得的学士学位在2018年、2020年、2022年和2024年将不再产生验证费用，因为毕业生持有可移植的证书，无需访问数据库即可确认。

然而，机构采纳问题才是真正的障碍。像Vouch这样的平台已经表明，颁发加密证书并不需要大学构建定制的Web3基础设施或发展深厚的技术专长，但经济利益仍然阻碍着那些从验证过程中获利的机构采用加密证书。医疗委员会通过证书查询获得收入，国家安全委员会（NSC）从雇主验证中收取费用，背景调查公司从就业确认中攫取数十亿美元，所有这些收入来源一旦证书持有者拥有可进行数学验证的便携式证明，就会消失。

Uptick的基础设施通过去中心化身份、可验证的证书标准、可编程智能合约逻辑和零知识隐私，为这种转变提供了技术基础，从而创造了证书颁发机构停止通过数据库访问盈利，转而开始颁发其记录本身就支持的便携式证明的条件。当竞争压力、监管变化或证书持有者要求使用便携式证明时，这种转变就会发生，因为这些因素会改变目前从基于自身管理便利而非证书所代表的人员利益而建立的系统中获利的机构的考量。

Uptick Network

hello@uptickproject.com

@Uptickproject

@Uptickproject

Uptick Network

Uptick Network