顶级 VC 豪掷 5000 万美金押注 Web3 新赛道

撰文：Biteye 核心贡献者 Viee编辑：Biteye 核心贡献者 Crush

你是否愿意将十年的个人对话数据交给 OpenAI、谷歌或脸书？

想象一下，未来的 AI 助手能够完美复制你的思维方式，处理日常事务时如同你本人。令人振奋的同时，这也意味着 AI 需要获取大量的数据——包括你过去发送的每条消息，以及构成你独特个性的所有信息，这便引发了文章一开始提出的问题。据调查，59% 的消费者对使用个性化 AI 感到不安，主要原因就是对数据隐私的担忧。

Nillion 作为一个创新的去中心化网络，通过利用多方计算（MPC）和其他隐私增强技术（PET），为这一问题提供了切实可行的解决方案。Biteye 将在本文为大家介绍 Web3 的新概念盲计算，及其如何保障你我的数据隐私。



## 01 数据隐私安全的现状

数据被视为数字化时代的新型「石油」，隐私和安全问题变得愈发重要。传统的数据处理方式通常需要在计算之前解密数据，这使得敏感信息在处理过程中暴露于潜在的安全威胁中。例如，在医疗行业，患者的数据必须经过严格的隐私保护措施，但在进行分析时仍然可能面临泄露风险。这不仅影响了用户对服务的信任，也限制了数据共享和合作研究的可能性。

尽管个性化 AI 展现出巨大的潜力，但在实现这一愿景之前，必须认真对待数据隐私问题，个性化 AI 才能真正迎来「下一个互联网」的时代。

## 02 盲计算是什么？

Nillion 提出了一种新的方法来解决上述问题，那就是「盲计算」（Blind Computing）。它通过去中心化的网络架构和先进的隐私增强技术，使得高价值数据能够安全存储并进行计算，而无需解密。

盲计算（Blind Computing）允许用户在不直接访问原始数据的情况下进行计算。这意味着即使数据存储在不可信的环境中，用户也可以安全地进行操作。

主要包括几个流程：

数据被屏蔽并分成几部分

这些碎片被发送到不同的节点

节点在看不到数据的情况下处理数据

收集和组合结果

只有授权方才能看到最终输出

也就是说，盲计算的核心在于将数据加密后进行处理。具体展开，用户将数据加密，将加密后的数据发送到云服务器或其他计算平台。在这些平台上，进行的所有计算都是针对加密数据的，最终结果同样是加密的。用户在接收到结果后，可以通过解密过程获得最终答案，而无需知道中间过程中的任何信息。就像一个「隐形的计算助手」，「盲计算」因此得名。



盲计算结合了多种先进的技术，确保敏感信息在处理过程中始终保持安全：

1、多方计算（MPC）

多方计算（Multi-Party Computation）是一种允许多个参与方共同计算一个函数的技术，而不需要透露各自的输入数据。每个参与者仅知道自己的输入和最终结果，而无法访问其他参与者的输入。

MPC 的工作原理可以用经典的百万富翁故事来理解。该问题由 Andrew Yao 于 1982 年首次提出。如果两个百万富翁想知道谁更富有，但又不想透露自己的财富。他们可以使用 MPC，通过一系列加密操作共同计算出谁更富有，而无需披露各自的具体财富。这一过程确保了参与方之间的信息安全，同时实现了合作。

这是通过一系列加密操作来实现的，这些操作允许各方将其净值输入到共享计算中。计算的结构方式是仅输出比较结果（即哪个百万富翁更富有），而不会泄露有关他们各自净资产的任何细节。这个问题展示了 MPC 的强大功能——它可以在实现协作计算的同时保护隐私。

应用：在盲计算中，MPC 确保即使在云服务器或其他不可信环境中进行计算，参与节点也无法看到原始数据。这种方式非常适合处理敏感信息，如金融交易或医疗记录。

2、同态加密（Homomorphic Encryption）

同态加密是一种特殊的加密形式，允许对加密数据进行直接计算，而无需解密。用户可以在加密状态下进行各种运算（如加法和乘法），最终得到的结果仍然是加密的。用户可以使用自己的密钥解密得到正确答案。

应用：同态加密在盲计算中扮演着重要角色，使得服务器能够对加密数据进行运算而不需要了解数据本身。这种技术使得数据在云环境中处理时更加安全。

3、隐私增强技术（PET）

隐私增强技术是一系列旨在提高个人隐私保护水平的方法，包括匿名化、伪匿名化和数据脱敏等。

应用：在盲计算中，这些技术可以与 MPC 和同态加密结合使用，以进一步确保数据在处理过程中的安全性和隐私性。例如，通过对输入数据进行匿名化处理，可以防止任何参与者识别出数据来源。

4、量子盲计算

量子盲计算是一种利用量子计算原理实现盲计算的方法。它允许用户在量子计算机上执行加密计算，保护输入和输出数据的隐私。

应用：量子盲计算目前还处于研究阶段，一旦实现预计能够处理更复杂的问题，并可能扩展用户在云环境中的计算能力。

## 03 Nillion 的双网络架构

为了综合以上技术实现盲计算，Nillion 采用双网络架构，由协调层（NilChain）和编排层（Petnet）组成。这一设计确保了高效的数据存储和处理，同时维护了系统的安全性与隐私性。

1、协调层（NilChain）

协调层负责管理网络中的支付操作，包括存储和盲计算。它确保所有交易都能顺利进行，并且能够有效地分配资源。

2、编排层（Petnet）

编排层利用 MPC 等隐私增强技术来保护静态数据，并实现对这些数据进行盲计算。Petnet 确保即使是在多个节点之间共享数据时，也能保持高度的安全性与隐私性。这一层次为开发者提供了灵活的平台，使他们能够构建各种应用程序，以满足不同需求。

## 04 Nillion 目前进展

10 月 30 日，Nillion 刚刚宣布完成 2500 万美元融资，由 Hack VC 领投，并获得了 Arbitrum、Worldcoin 和 Sei 的支持。截止目前，Nillion 总融资金额已经达到 5000 万美元。

自推出以来，Nillion 已取得了一些表现亮眼的数据：

验证者数量：247,660

保护的总数据：711 GB

受到挑战的秘密总数：120,254,931

验证者有助于维护数据的安全性和完整性，该数量的增长意味着 Nillion Network 变得更强大、更安全。

目前 Nillion 的合作伙伴包括区块链网络 NEAR、Aptos、Arbitrum、Mantle、IO.net、Ritual 等。涉及多个领域，比如 Ritual、Nesa，用于私有模型 AI 模型训练和推理；Rainfall、Dwinity、Nuklai，用于存储、共享 AI 训练数据并从中获利；MIZU，用于创建合成数据并保护个人数据。Virtuals Protocol、Capx AI 、Crush AI ，在 Nillion 的帮助下创建个性化的私人代理。PINDORA，用于 DePIN 网络的机密和安全支持。Nillion 试图吸引那些位于区块链和 AI 交汇处的项目，这些项目需要安全地共享和存储大量数据。

在未来，我们可以预见到 Nillion 将在医疗、金融、教育等多个领域得到广泛应用，为构建一个更加安全、透明的数据生态系统贡献力量。

## 05 总结

Nillion 通过创新性的技术架构和强大的隐私保护能力，为解决当前数字世界中的数据隐私问题提供了一条可行之路，使用户能够在享受数字服务带来的便利时，无需担心个人信息被泄露或滥用。

站在现在，我们无法想象人工智能的未来，个性化数字副本的崛起与数据隐私的忧虑就像是跷跷板的两端。如果没有有效的数据隐私保护措施，个性化 AI 将难以获得广泛的市场接受度。因此，如何在推动技术进步与保护用户隐私之间找到平衡，将是行业亟待解决的重要课题。随着 Nillion 网络的发展，期待看到更多基于这一平台的新应用，为 AI 时代的人类社会带来积极影响。