Hack VC：区块链隐私4大解决方案及相关项目详览

作者：Duncan Nevada，Hack VC合伙人；翻译：本站xiaozou

透明的加密账本从根本上改变了我们如何看待信任系统。正如老话所说：“don't trust, verify（非经验证，勿信）”，而透明性恰恰让我们可以去相信。如果一切都是开放的，任何造假都可以被标记。然而，这种透明性已被证明是可用性的若干制约因素之一。当然，有些事情应该公开，例如结算、储备、声誉（也许还有身份），但我们不希望每一个人的所有财务状况和健康档案连同个人信息一起被公开。

## 1、区块链的隐私需求

隐私是一项基本人权。没有隐私，就没有自由和民主。

正如早期的互联网需要加密（或SSL）来实现安全的电子商务以及保护用户数据一样，区块链需要强大的隐私技术才能充分发挥其潜力。SSL允许网站加密传输中的数据，确保信用卡号等敏感信息不会被恶意行为者截获。同样，区块链需要隐私技术来保护交易细节和交互，同时维持底层系统的完整性和可验证性。

区块链上的隐私保护不仅仅是为了保护个人用户，它对于企业采用、数据保护合规以及解锁新的设计空间来说至关重要。世界上没有哪家公司希望自己的每个员工都能看到其他人的薪水，也没有哪家公司希望竞争对手能够了解排序他们最有价值的客户然后挖走他们。此外，医疗保健和金融等某些行业对数据隐私有严格的监管要求，区块链解决方案要成为一种可行的工具，就必须满足这些要求。

## 2、私隐增强技术（PET）地图

随着区块链生态的发展，出现了几个关键的PET技术，每个PET都有自己的优点和利弊权衡。这些技术——零知识证明（ZK）、多方计算（MPC）、全同态加密（FHE）和可信执行环境（TEE）——跨越六大关键属性。

通用性：解决方案应用于广泛用例和计算的容易程度。

可组合性：该技术与其他技术相结合以减轻劣势或解锁新的设计空间的容易程度。

计算效率：系统执行计算的效率。

网络效率：随着参与者或数据规模的增加，系统的可扩展性如何。

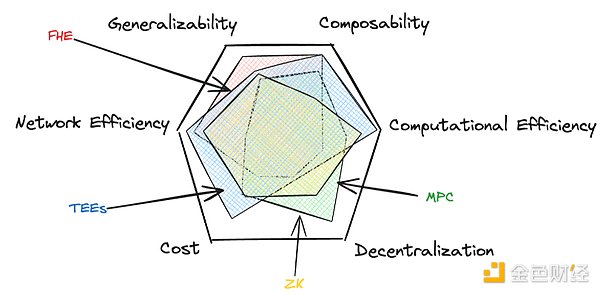
去中心化程度：安全模型的分布式程度。

成本：隐私的实际成本。

就像区块链的可扩展性、安全性和去中心化三难困境一样，同时实现所有六个属性是具有挑战性的。然而，最近的发展进步和混合方法正在突破可能性边界，使我们离负担得起的高性能综合隐私解决方案越来越近。

现在我们手里有了地图，我们来大体看一下全貌，探讨一下这些PET技术的未来前景。

## 3、PET景观图



我想我在这里需要补充一些定义。

### （1）零知识证明

零知识（ZK）是一种技术，它允许验证一个计算确实发生并且实现了一个结果，而不透露输入信息。

通用性：中。电路是高度特定于应用程序的，但却离不开基于硬件的抽象层，如Ulvatana和Irreducible以及通用解释器（如Nil的zkLLVM）。

可组合性：中。它独立于可信prover（证明者）工作，但证明者必须看到网络设置中的所有原始数据。

计算效率：中。随着真正的ZK应用程序（如Leo Wallet）上线，证明正在通过新颖的部署实现指数级增长。随着客户采用的增加，我们期待进一步的发展。

网络效率：高。Folding的最新进展为并行化带来了巨大潜力。Folding本质上是构造迭代证明的一种更有效的方法，所以它的开发建设可以基于已完成的工作进行。Nexus就是其中值得关注的一个项目。

去中心化程度：中。理论上，证明可以在任何硬件上生成，但实际上，GPU更受欢迎。尽管硬件变得越来越统一，但在经济层面上，可以通过AVS（如Aligned Layer）进一步去中心化。输入只有在与其他技术结合使用时才具有隐私性（详见下文）。

成本：中。电路设计和优化的初始部署成本很高。运营成本适中，证明生成成本相对较高，但验证效率也高。造成这一成本结构的一个显著因素是以太坊上的证明存储，但这可以通过其他方法来缓解，例如使用EigenDA或AVS等数据可用性层。

以《沙丘》为例：想象一下，Stilgar需要向Leto公爵证明他知道一个香料田的位置，但不想透露确切的位置。Stilgar把蒙着眼睛的Leto带上了一架扑翼机，在香料田的上空盘旋，直到肉桂的香味弥漫了整个机舱，然后他带着Leto回到Arrakeen。Leto现在知道了Stilgar能找到香料，但他却不知道自己怎么才能到那里。

### （2）多方计算

多方计算（MPC）是指多方可以共同计算结果，而无需向彼此透露各自的输入。

通用性：高。鉴于MPC的特殊性（如秘密共享等）。

可组合性：中。MPC是安全的，但是可组合性随着复杂性的提高而降低，因为复杂性会带来指数级的网络开销。然而，MPC有能力在同一计算中处理来自多个用户的隐私输入，这是一个相当常见的用例。

计算效率：中。

网络效率：低。参与者的数量与必须完成的网络量成平方比。Nillion等项目正在努力解决这个问题。纠删码（Erasure coding）/ 里德-所罗门码（Reed-Solomon codes）——或者更宽松地说，将数据分割成片（shards），然后保存这些shards——也可以用于减少错误，尽管它并非传统的MPC技术。

去中心化程度：高。但参与者也有可能串通一气，危及安全。

成本：高。实施成本中高。因通信开销和计算需求，运营成本较高。

以《沙丘》为例：考虑到Landsraad的大家族们确保他们之间有足够的香料储备，这样他们就可以互相帮助了，但他们并不想透露他们的个人储备的具体信息。第一家可以向第二家发送消息，在他们的实际储备中添加一个大的随机数。然后第二家再加上他们的实际储备数量，以此类推。当第一家收到最终总数时，只需要减去他们之前添加的那个大随机数，就能知道实际的香料储备总量了。

### （3）全同态加密

全同态加密（FHE）允许对加密数据执行计算，而无需事先解密。

通用性：高。

可组合性：单个用户输入的可组合性高。必须与其他多用户隐私输入技术相结合。

计算效率：低。但从数学层到硬件层经历了一致优化，这将是一个巨大的潜力解锁。Zama和Fhenix在这方面做了很多出色的工作。

网络效率：高。

去中心化程度：低。部分原因是因为计算需求和复杂性，但随着技术的进步，FHE的去中心化程度可能会接近ZK的去中心化程度。

成本：非常高。由于复杂的加密和严格的硬件要求，部署成本很高。由于计算量大，运营成本很高。

以《沙丘》为例：设想一个类似于霍尔兹曼护盾的装置，但用于数字。你可以在这个防护盾里输入数字数据，激活它，然后把它交给一个Mentat。该Mentat可以在看不见被屏蔽的数字的情况下进行计算。计算完成后，他们会把防护盾还给你。只有你能还原该护盾，看到计算结果。

### （4）可信执行环境

可信执行环境（TEE）是计算机处理器内的一个secure enclave或区域，与系统的其余部分隔离，可以在其中执行敏感操作。TEE的独特之处在于它们依赖于硅和金属，而不是多项式和曲线。因此，虽然它们在今天可能是一项强大的技术，但理论上来说，因为受到昂贵硬件的限制，其优化速度应该更慢。

通用性：中。

可组合性：高。但由于潜在的旁路攻击（side channel attacks），安全性较低。

计算效率：高。接近服务器端的效率，以至于英伟达最新的H100芯片组系列都配备了TEE。

网络效率：高。

去中心化程度：低。但受限于特定的芯片组，如英特尔的SGX，这意味着容易遭受旁路攻击。

成本：低。如果使用现有TEE硬件，部署成本较低。由于接近原生性能，运营成本较低。

以《沙丘》为例：设想一下宇航公会的Heighliner机舱。即使是公会自己的领航员在使用时也无法看到或干扰内部发生的事情。领航员进入机舱，进行折叠空间所需的复杂计算，并且机舱本身确保在里面进行的一切都是私密和安全的。公会提供并维护这个机舱，保证它的安全，但他们不能看到或干扰领航员在机舱里的工作。

## 4、实际用例

也许我们不需要与香料巨头竞争，而是只需要确保关键香料等特权数据保持特权。在我们的现实世界里，各技术对应的一些实际用例如下。

ZK在我们需要验证某个过程是否生成了正确的结果时非常适合。当与其他技术结合使用时，它是一种出色的隐私技术，但单独使用会牺牲信任，并且更类似于压缩。通常我们用它来验证两种状态是相同的（即“未压缩”的L2状态和发布到L1的区块头，或者证明用户年龄超过18岁，而不泄露用户任何实际个人身份信息）。

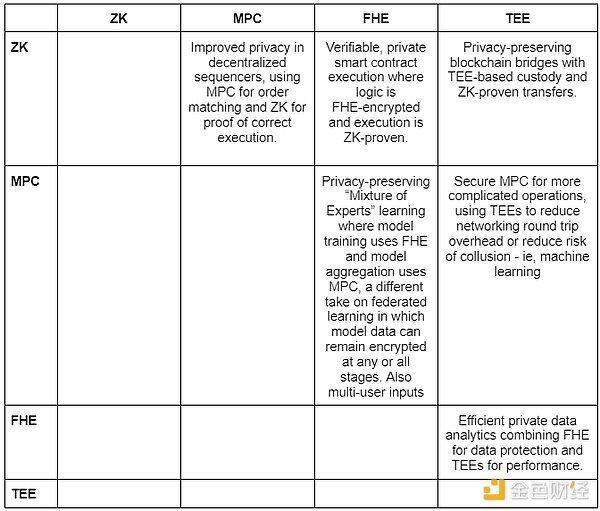
MPC通常用于密钥管理，可以是私钥或与其他技术结合使用的解密密钥，但它也用于分布式随机数生成、（较小的）隐私计算操作和oracle聚合。从本质上讲，任何使用不该相互勾结的多方来进行基于轻量级聚合的计算的方法都非常适合MPC。

当需要在计算机看不到数据的情况下完成简单的通用计算时（例如信用评分、黑手党的智能合约游戏，或在内存池中排序交易而不透露交易内容），FHE是一个不错的选择。

最后，如果你愿意信任硬件，TEE非常适合复杂性更高的操作。例如，这是私募基金会模型（存在于企业或金融/医疗保健/国家安全机构中的LLM）唯一可行的解决方案。相关的利弊权衡在于，由于TEE是唯一基于硬件的解决方案，理论上，改进缺点的速度应该比其他技术更慢，成本也更高。

## 5、其他解决方案

很明显，没有完美的解决方案，而且一项技术也不太可能成长为完美的解决方案。混合式解决方案是令人兴奋的，因为它们可以利用一种方法的优点来缓解另一种方法的缺点。下表显示了通过将不同的方法组合在一起可以解锁一些新的设计空间。实际做法截然不同（例如将ZK和FHE结合起来可能需要找到正确的曲线参数，而将MPC和ZK相结合可能需要找到某一类设置参数来减少最终的网络RTT时间。



简言之，高性能的通用隐私方案可以解锁无数的应用程序，范围涉及游戏、治理、更公平的交易生命周期、身份认证、非金融服务、协作和协调。这在一定程度上可以解释为什么我们发现Nillion、Lit Protocol和Zama让人如此着迷。

## 6、结论

总之，我们看到了巨大的潜力，但我们尚处于可能性探索的早期阶段。个别技术可能在某种程度上来说近乎成熟，但staking技术仍然是一个可供探索的领域。PET将按照该领域量身定制，从行业角度来看，我们还有很多事情要做。