有没有可能创造一个包含个人敏感数据与处理函数的结构体，这个结构体作为个人敏感数据在线上传播唯一的形式。外部只能通过调用函数来访问其中的敏感数据。所有的敏感数据被加密，整个结构体被所有者签名。为了防止敏感数据的泄露，所有对这个结构体的访问都记载在区块链上。而为了防止信息泄露后多个曾经的访问者相互抵赖，每次访问都会加互斥锁，即只有当下的访问者可以访问结构体，也是唯一可能泄露的人。而这个结构体存放在区块链上因此不可能被篡改。而一般的访问者要想泄露这个结构体中的数据或处理函数，则需要同时获得之前所有访问者的私钥，才可能进行泄露或篡改。请具体谈谈这个想法的难点和可行性。

ChatGPT

这是一个非常深入且具有前瞻性的问题，关于个人敏感数据的保护和权限管理。这个想法涵盖了密码学、并发控制、区块链等多个领域的知识。我会分别从这些领域来分析这个想法的难点和可行性。

1. **密码学**：敏感数据的加密和签名技术已经相当成熟，例如使用对称加密算法（如AES）或非对称加密算法（如RSA、ECC）进行加密，以及使用数字签名技术进行身份验证和完整性保证。这部分应该是完全可行的。
2. **访问控制和互斥锁**：你提到的“每次访问都会加互斥锁，即只有当下的访问者可以访问结构体，也是唯一可能泄露的人”，这是一种典型的并发控制机制，也在操作系统和数据库系统中有广泛的应用。然而，这在分布式环境中，特别是在区块链这样的去中心化网络中实施可能会比较困难，因为需要所有的节点对锁的状态达成一致。这可能需要某种形式的共识机制，而达成共识本身就是分布式系统中的一大难题。
3. **区块链**：你提到的“所有对这个结构体的访问都记载在区块链上”，这是区块链技术的一个重要应用，即通过公开透明的方式记录所有的操作。然而，区块链技术也有其局限性，例如交易吞吐量有限，确认时间可能较长，而且对存储容量有很大的需求。此外，一旦数据被写入区块链，就无法被修改或删除，这可能与数据隐私保护法规中的“被遗忘权”相冲突。
4. **权限管理**：你提到的“一般的访问者要想泄露这个结构体中的数据或处理函数，则需要同时获得之前所有访问者的私钥，才可能进行泄露或篡改”，这是一种多方计算（MPC）的概念，即需要多个参与者共同协作才能完成某个操作。这在理论上是可行的，但在实践中可能会遇到很多问题，例如如何确保所有的参与者都按照规则行事，如果有人失去了私钥怎么办，如果有人拒绝合作怎么办等。

总的来说，你的这个想法在理论上是有一定可行性的，但在实践中可能会遇到很多技术和实施的挑战。其中的一些问题可能可以通过现有的技术解决，但也有一些问题可能需要新的技术和方法才能解决。这是一个非常好的研究方向，值得进一步探讨。



那么这个结构体中的处理函数应当怎样设计才能同时保证安全性，又满足访问者的需求呢

ChatGPT

设计这样一个处理函数，需要满足两个主要的目标：一是保护敏感数据的安全，二是满足访问者的需求。这需要在数据的可用性和安全性之间找到一个平衡。以下是一些可能的设计考虑：

1. **最小权限原则**：处理函数应只提供访问者所需的最小数据权限，而不是全部的数据。例如，如果访问者只需要获取某个用户的年龄，那么处理函数就应只返回这个信息，而不是返回用户的全部个人信息。这可以通过设计具有不同权限的处理函数来实现。
2. **输入验证和错误处理**：处理函数应进行充分的输入验证和错误处理，以防止攻击者通过提供恶意输入来获取未经授权的数据。例如，处理函数应检查输入的参数是否在预期的范围内，是否符合预期的格式，等等。
3. **数据加密**：处理函数应在返回敏感数据之前对其进行加密，以保证数据在传输过程中的安全。访问者需要使用正确的密钥才能解密获取的数据。
4. **安全审计**：处理函数应记录所有的访问请求和响应，以便进行安全审计。这些记录应包括访问者的身份、访问时间、访问的数据和处理函数的结果等信息。
5. **使用安全编程实践**：处理函数的编码应遵循安全编程的最佳实践，例如避免使用已知存在安全漏洞的函数、避免使用不安全的编程模式等。
6. **多方计算**：如果可能，可以考虑使用多方计算（MPC）技术，让数据的处理在多个参与者之间进行，而不是在单一的处理函数中进行。这样可以进一步保护敏感数据的安全。

以上这些方法可以帮助设计一个既能满足访问者需求，又能保护敏感数据安全的处理函数。然而，需要注意的是，设计和实现这样的处理函数是一个复杂的过程，需要深入的安全知识和技能。

有没有这样的可能，所有者将私人信息加密后传给访问者，但是加密方式比较特别，需要多方参与才能解密信息。首先，假设有3个其他方参与解密，那么所有者随机生成一个这3个其他方的解密顺序，并用访问者的公钥加密这个顺序放置在最终加密信息的头部，然后，依次用这三方的公钥加密一段信息，并为每一段信息生成hash，依次放置在最终加密信息的体中。访问者要获取明文信息则需要多方配合解密，而又可以用hash来验证参与方是否提供了真实信息，而参与方只有一部分信息，无法猜测最终的明文。访问者在搜集到所有的解密信息并验证过hash后得到解密的信息，然而这个明文信息中一部分数据被所有者隐去了，比如用X来代替。但是，这时访问者通过比对自己数据库中的信息，已足以确认用户的身份，这个明文的最后还有完整明文信息的hash值，访问者猜测后可以用hash做验证。这个明文是以图片的方式给出的，图片中有用户的私人信息但是其中随机地隐去了一小部分，同时这个明文的图片中有访问者的水印，以防止访问者泄露图片后抵赖。这个想法可信吗，存在什么问题？