针对您的研究主题，以下是一些建议的英文关键词：

1. Blockchain and privacy protection
2. Decentralized identity management
3. Blockchain-based data security
4. Personal data on blockchain
5. Zero-knowledge proofs in blockchain
6. Blockchain and GDPR (General Data Protection Regulation)
7. Homomorphic encryption in blockchain
8. Privacy-preserving smart contracts
9. Blockchain data obfuscation
10. Self-sovereign identity on blockchain

我要设计一个用区块链技术保护用户的个人隐私信息的系统，当用户访问网站或执行关键操作时，网站要求验证用户的身份，或者要采集用户的个人信息。这时所有对用户个人信息的访问操作必须记录到区块链上。区块链上并不存储用户的个人信息，而是存储加密的用于访问用户信息的API的地址。访问者通过API访问用户信息，API提供加密的用户信息。而访问者需要多方解密才能获得最终信息。这个过程中如何保证以下规则：1. 如果一个攻击者要得到最终的解密信息，只有他是区块链上的申请者。2. 区块链的申请者如何泄露信息给别人，则会被发现和举证（用隐写术）。3. 整个环节中不会泄露信息，除非攻击者获得了多方解密过程中所有参与方的私钥。4. 参与方都得不到完整的信息，信息的分布较为均匀。5. 解密后的信息被转换的难度较大，不容易被直接提取和泄露。

您的系统设计目标十分具有前瞻性，并且涉及到多个技术难题。以下是一些建议的设计方案，以满足您提出的规则：

1. \*\*多方计算 (MPC, Multi-Party Computation)\*\*:

- 通过多方计算，用户的信息被分割成多个部分，并分发给多个参与方。只有当所有的参与方合作时，才能对数据进行完整的解密。

- 这确保了即使攻击者获得了其中一个参与方的私钥，他们也无法获得完整的信息。

2. \*\*零知识证明\*\*:

- 这可以保证申请者是区块链上的申请者，而不必揭示他们的身份或他们所请求的确切信息。

- 同时，使用零知识证明的另一个好处是，信息提供者只能知道他们正在提供信息，但不知道这些信息的确切内容。

3. \*\*隐写术\*\*:

- 为满足规则2，可以在返回的加密信息中嵌入特定的水印或隐写术。

- 如果申请者非法地将信息泄露给他人，这个水印或隐写术可以用作证据。

4. \*\*加密和分片\*\*:

- 为了确保信息在整个环节中不被泄露，用户的信息首先被加密，然后被分割成多个片段或分片。

- 每个片段都由不同的参与方进行管理和存储。

5. \*\*混淆技术\*\*:

- 一旦信息被解密，可以进一步使用混淆技术，使得解密后的信息结构混乱，难以被直接提取和泄露。

- 只有具有特定密钥或算法的实体才能从混淆的数据中提取有意义的信息。

通过结合上述技术和方法，您可以设计出一个健壮、安全且隐私友好的系统，以满足您提出的所有规则。但请注意，实施这样的系统可能需要大量的研发工作，并可能需要与区块链和加密技术的专家合作。