**现在的隐私保护困境：**

1、获取用户的个人数据涉及到大小公司的核心利益，FaceBook如此，BAT也一样；

2、现在用户的明示同意等，只是尽到了告知等责任，更多的是为了合规或者规避风险(现在许多公司连这一步都懒得搞)，用户的个人数据依然被获取，并未真正保护用户隐私；

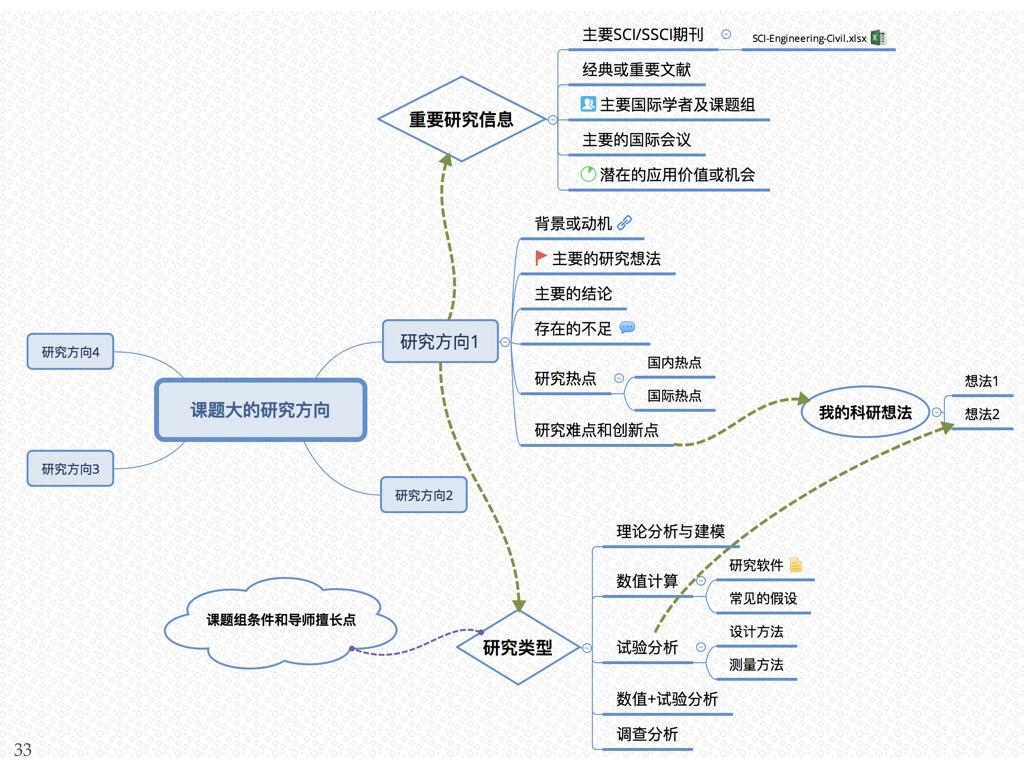
3、从另一方面考虑，即使是从用户角度看，有些个人数据也确实需要提供，譬如提升用户体验等等；

4、如何平衡各方的利益，除了法规要求外，还可以借助各种隐私保护技术；5、隐私保护当在当前有些研究热点，但是从实际应用来看，除了苹果的差分隐私，其它鲜有公开的，大规模的应用；

6、随着GDPR实施日期即将来临，更严格的法律要求，更大额的罚款，将推动企业更有动力关注隐私保护。说不定，隐私保护会成为某些企业的核心竞争力，希望这种企业在国内首先出现。

总结一下就是，隐私保护技术的核心价值就是从用户角度出发，真正保护用户隐私的同时，实现服务提供商的商业价值。

*作者：上学记  
链接：https://www.zhihu.com/question/37545236/answer/379130793  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。*



**区块链保护还是泄漏隐私？**

理论上区块链能解决一切信任问题。但隐私问题一直是区块链应用落地时最受关注的问题之一：我们要在区块链上保护版权、签合同、匿名交易、投票、溯源，甚至追星？那么在实现这些事的过程中，区块链是保护了我们的隐私、为隐私数据确权，还是最终会因其记录不可磨灭等特点，以侵犯、倒卖我们的隐私告终？

**正方：**

匿名是隐私保护的一种手段，区块链无疑可以保护隐私

随着互联网的飞速发展，整个社会被强行拉入“大数据”时代，个人数据的网络化和透明化已经成为不可阻挡的大趋势。不管我们是否愿意，我们的个人数据正在不经意间被动地被互联网产品搜集并使用。这些用户数据对互联网公司来说是珍贵的资源，因为他们可以通过数据挖掘和机器学习从中获得大量有价值的信息。与此同时，用户数据亦是危险的“潘多拉魔盒”，数据一旦泄漏，大量用户的隐私将会受到侵犯。近期，Facebook就因为曾经无意间泄露了超过5000w用户的隐私数据备受责难，而社会也因为这些数据的泄露受到了重大影响。

首先要区分两个概念，就是匿名和隐私。隐私是一种与公共利益、群体利益无关，当事人不愿他人知道或他人不便知道的个人信息。匿名是一种不具名或使用化名的行为，目的是不想表露自己身份，或者因为多种原因身份/特征不明。从概念上讲，匿名是隐私保护的其中一种手段。

我们都知道比特币的白皮书名字叫做一种点对点的电子现金系统，其中“现金”这个词的使用是值得关注的，之所以叫现金，意味着一定程度的匿名性，比特币的核心设计理念就包含了一定程度的匿名性。事实上，比特币本身不是匿名的，而是假名制的。比特币的假名制在日常生活中是非常脆弱的。连接交易会降低隐私水平，日常的使用都会在互联网上留下痕迹。因此我们也看到了诞生了匿名性更强的门罗和Zcash等。

对于更广义的使用场景来说，区块链主要利用零知识证明和同态加密等手段，在数据为个人所有的情况下，可以不暴露隐私对个人的数据进行有效的使用和交换。

作为一种分布式记账技术，区块链在诞生之初就需要考虑公共数据的管理问题，没有一定程度的隐私保护，区块链技术是无法获得广泛认可的。因此，区块链技术确定无疑是可以保护隐私的。

**反方：**

区块链典型应用比特币匿名弱点太多，保护隐私远远不够

要谈论区块链的是否保护隐私，我是先从区块链的典型应用btc的开始分析。比特币匿名性体现在：

（1）比特币地址不能对应到真实身份，比特币地址生成在本地进行，用户可以用不同的地址来接收一笔收入

（2）比特币交易中包含了时间、输入、输出、金额、签名等要素，但没有包含任何个人真实身份信息

（3）新交易通过比特币网络辐射式传播，其他节点无法确定新交易的来源 IP，保护了发送者的 IP 地址不泄露。

比特币匿名性弱点体现在：

（1）比特币服务商实名认证，记录了用户身份信息如邮箱、手机、家庭电话、信用卡、居住地址等，通过这些信息可以对应到提款地址和充值地址

（2）在互联网上如论坛、微博、微信、Facebook、TWITTER、QQ 群等留下的比特币地址，能对应到用户帐号。

（3）交易链透明可查。只需知道一个比特币地址就可以找到一系列相关联的地址，与交易所实名或其他比特币服务商的实名相结合，可以找到用户的转币途径与一系列地址。这是核心问题所在，匿名需要的是交易无关联性（unlinkability），而这个交易链数据的透明可查，将暴露我们所有的交易数据。

（4）交易的汇总输入特性，使得交易汇总了大部分地址中的币发送出去，会暴露用户的其他地址。

（5）用户向外发币时有多余金额，比特币就随机生成一个新地址，即找零地址，来接收多余的金额，交易的找零地址可以归类到发送者头上。

针对反匿名技术，主要着重于两类方法：第一类交易链分析，即通过比特币公开的区块链数据和交易链数据，以比特币匿名性几个弱点来聚类比特币地址，并且对应到真实身份或虚拟身份。第二类是比特币协议和网络分析，利用比特币协议和比特币网络的特性来推断新交易的来源 IP 地址，攻击方法有比特币协议监控、女巫攻击、入口节点判定法和伪比特币节点等。

**正方**

比特币设计上对隐私保护确实不足，并且这也不是比特币设计的主要目的。作为后来者的门罗和Zcash，是否在区块链隐私保护上做了更多的增强？

**反方**

门罗主要是采用环签名技术，但是环签名也有一个缺点，就是环签名中依旧需要与其他用户的公钥进行混合，因此可能会遭遇恶意用户从而暴露隐私。

ZCash的零知识证明没有太深入研究，确实没有发现漏洞但是据说存在上帝之钥。

如何防范区块链上隐私数据被授权访问后的二次转卖？

**正方**

这其实是区块链保护隐私的第二部分，利用零知识证明或者同态加密做到数据使用权和所有权的分离。隐私数据的授权访问是为了下一步对数据的使用，而在未来的区块链世界里，我们不再需要对隐私数据做授权访问，对于隐私数据的使用，也就是计算，都在用户这边进行，数据永远不暴露出来，对方只拿到计算结果，和对这个计算结果的一个密码学证明，保证结果可信，这样子再也不会发生隐私数据的泄露。

**反方：**

我们认为，相比现有技术，区块链比中心化的、完全某个机构控制的系统，在保护隐私方面确实有进步，但是远远不够。所以我们才需要进行改进。一种是对抗第一类交易链分析，提高窃取隐私成本。第二种是则是对抗第二类比特币协议和网络分析。包括Tor网络和远程交易释放(TRR)。从目前市场情况来看，那种更有竞争力？

**正方：**

对抗交易链分析的方法，其实就是链上做加密，这种方法比较有前景，但是目前面临很多技术上的局限，比如速度太慢，支持的计算类型太小，现在还很难大规模使用。从一个更长远的角度来看，技术的局限是可以突破的。而洋葱网络这种类型的匿名网络，本质上只是对连接进行了多次转发，从网络更底层来看没有什么大的区别，只是追踪的成本上升了。丝绸之路的网站，最终还是被干掉了。

**反方：**

目前来说，区块链隐私保护可能最容易在数字货币领域。现在技术之下，我们还是可以做到匿名支付，我们的safe币通过使用双层网络，就实现了即时支付和隐私支付。

在区块链泄露隐私的例子上，更多的属于交易所泄露事件——韩国Bithumb客户数据泄露去年就闹得比较大；还有维基解密的btc捐献地址——所有人都看得清清楚楚。

最后一个问题，区块链数据不可篡改磨灭的性质是在隐私保护上有什么缺点？如果密钥丢失咋办？

**正方：**

不可篡改造成的问题就是一旦密钥丢失，就代表着数字身份丢失了，这确实是目前区块链系统面临的问题，用户都习惯了用户名和密码，丢失了可以找回，但区块链的密钥丢失了谁也没有办法。

目前有一些解决方法在尝试，比如简单的做分级权限控制，对不同安全级别的密钥做不同强度的安全保管，或者密码学正在研究的一些基于人体特征的属性密码。

**正方：区块链的隐私保护机制会越来越成熟**

区块链技术发展到今天，仍然还处于一个相对早期的阶段，无论是技术还是使用场景都还不够成熟，我们可以从中找出非常多的问题来。但是作为从一种分布式记账技术，区块链从设计之初就考虑了大量和隐私相关的设计，这些特性未来会随着区块链的普及落地在各个应用场景中，并给社会带来更好的隐私保护机制。

另一方面，区块链技术是以开源和分布式为基础的，隐私安全也是区块链共识的重要组成部分，区块链社区有非常强的保护隐私的动机，底层的共识会保证区块链相关应用会比中心化的应用更加重视对参与者的隐私保护。这些是中心化的互联网产品所不具备的。

最后，由于区块链上的数据一旦记录就无法被篡改，因此也给我们所有的使用者带来更高的自我要求，哪些数据应该放在公共存储设施，哪些数据应该放在私有的存储设施，是信息社会中生存的必备技能。

**反方：用户便利与数据安全是永恒的矛盾**

区块链的数据永远存在就如同达摩克利斯之剑，永远悬在隐私保护的头上，今天能保护的数据，明天新的技术出现，破解的可能性就大幅度增加。凡事皆有代价，用户便利和数据安全是永恒的矛盾，保护隐私还是选择便利，选择权就交给用户吧。

道高一尺魔高一丈，数据的保护和泄露，是永恒的话题，也只有这样才能相互促进，共同发展。