大家好，今天来为大家分享区块链的一些知识点，和数据隐私性是指的问题解析，大家要是都明白，那么可以忽略，如果不太清楚的话可以看看本篇文章，相信很大概率可以解决您的问题，接下来我们就一起来看看吧！

本文目录

谁提出了注重隐私安全的密码

1982年，戴维.乔姆（DavidChaum）提出了注重隐私安全的密码学网络支付系统，该系统具有不可追踪的特性，被认为是比特币区块链在隐私安全方面的雏形

1990年，Paxos算法由莱斯利.兰伯特（LeslieLamport）提出，这是一种基于消息传递的一致性算法，Paxos算法解决了分布式系统如何就某个值（决议）达成一致。

1991年，斯图尔特.哈珀（StuartHaber）与W.斯科特.斯托尔内塔（W.Scott.Stornetta）提出利用时间戳确保数位文件安全的协议，此概念之后被比特币区块链系统采用。

1997年，亚当.巴克（AdamBack）发明的哈希现金是一种PoW演算法，此演算法依赖成本函数的不可逆特性，从而实现容易被验证但很难破解的特性，最早备用应用于阻挡垃圾邮件。哈希现金之后成为比特币区块链采用的关键技术之一。

1998年，戴伟（WeiDai）发表匿名的分散式电子现金系统B-money，引入PoW机制，强调点对点交易和不可篡改特性。同年尼克.萨博发表了去中心化的数位货币系统BitGold，参与者可贡献运算能力接触加密谜题，后来，哈儿.芬妮提出RPoW（可重复使用的工作量证明机制），将B-money和亚当.巴克提出的哈希现金结合起来创造了密码学货币。

2008年11月1日，比特币白皮书发布，有中本聪首先在《比特币：一种点对点的电子现金系统》（Bitcoin：APeer-to-PeerElectronicCashSystem）一文中提到了比特币。

2009年1月4日，中本聪创建了比特币世界的第一个区块。

2009年1月11日，中本聪发布了比特币客户端0.1版本。

比特币就这样诞生了。

区块链和物联网有必然的联系吗？

首先，区块链解决了数据不能被篡改的信任问题。

但这里有个前提，就是数据首先得是正确的。如果虚假数据上了区块链，那么这种虚假数据，也不能被修改，也不能被删除。于是乎，垃圾被固化在区块链里了。这还了得？

怎么办？

唯一的办法，是在数据源头上下功夫。怎么下功夫？拿着枪逼着录入数据的人不要录入虚假数据？所以，这时就要靠物联网设备了。物联网设备是机器，不是人。它不会主观犯错，也不会有意识地上传虚假数据。除非出现故障，否则数据会接近客观真实。

因而，物联网负责线下真实世界的数据源，上传到区块链线上世界。这就是物联网与区块链结合的意义所在。

可以更进一步讲，每一个区块链ORACLE语言机最终都将是物联网设备的ORACLE语言机。

区块链如何保护我们的隐私？

每个人都应该能够控制自己的资料，这是最大的前提，每个人都应该要求有权利决定在何时用什么方式提供自己哪些身份资料，到多么详细的程度给其他人。

尊重一个人的隐私权和尊重他人如何行使隐私权，是不同的两件事，缺一不可。

中本聪的演算法解决我们必须把信赖建立在其他人身上的问题，也免除了我们必须要先知道对方的真实身份才能与之互动的必要性。我跟许多工程师和电脑科学家请教过一次的问题，结果他们告诉我，而且每个人都这么说，当然可以呀，我们当然可以在设定资料格式和设计程序时纳入个人隐私资料，这些技术上一点问题也没有，隐私权是基本人权，也是社会的基础，过去20年，公司部门都会用集中式资料库在网络上收集个人或者组织的各种机密资料。

比如说在对方不知道的情况下，使得世界各地的人都担心大型机构会把它们留在数字世界的资料拆解，从组成所谓的虚拟负责人。美国国家安全局之前在揭穿未获批准的情况下，完全监控网络就是一个明显的例子，这些情况对于个人隐私造成双重侵害，首先是在我们不知情未取得我们许可的情况下收集我们的个人资料再任意使用，随后又在黑客窃取资料时束手无策。

而今天，关键在于我们能否抛弃旧有的认知，二取一的立场，选择站队边输和赢，对我们而言，这些损害生产力的想法都已经如同明日黄花一样过时了，我们应该改变采用能带来正效益的模式，其中一个最基本的就是让你可以拥有隐私权，以及在资料栏留下空白的权利。

中本聪在网络层的设定中并不涉及身份认定这一点，也就是说任何人都可以不用提供姓名电子邮件地址或者其他个人资料，就能够下载使用比特币的软件，比特币区块链也不需要知道参与者是谁。中本聪不需要或许任何人的个人资料推销其他产品，而他开放原始码的选择，已经是最引领操作的这种。

市场营销观念完全符合环球银行卡金融电信协会Swift的做法，只要有人付现钞，Swift不会过问付款人的身份。这是金融机构一定要遵守防洗钱机制，了解客户的原则才能够加入，所以获取协会的服务，另外呢，识别层验证曾两者也会与交易城脱钩，因此，当某个人在区块链公告自己要把比特币从自己的一个地址转移到另一个人的地址是交易过程，并不用提及任何人的身份，只要让网络架构确认。的确，拥有符合数量的比特币，他也同意将这些比特币用于交易，然后就可以把a公告的信息与b的地址建立联系。如果日后要动用这些比特币是网络架构才会再行确认B是否真的拥有这些比特币，相比较之下，信用卡的运作机制就显得非常看重持有人的身份，所以每次只要爆发资料库，被入侵的实践结果就是几百万比以上的住址跟电话被窃取。

由于区块链的参与者，不需要把不相关的详细资料与身份进行连接，也不需要把详细的个人资料留存的集中式的资料库，所以能够自行决定要维持个人资料的匿名信到什么程度，这个改变之大，再怎么强调也不为过。区块链不存在引狼入室的个人资料，区块链协定可以让我们在每一笔交易，或者是在不同的环境下用让自己感到安心的方式保住隐私，帮助我们把个人账号维护的很好，更容易管理自己身份与这个世界的活动过程。

互联网时代下，还有隐私可言吗？

看来提问者已经察觉到互联网信息结构下人们的隐私危机，的确随着互联网的发展人们想要隐藏秘密会变得越来越难。但是从多维空间来看，人们根本就是没有隐私的。

什么是最终极的互联网结构？

就是指你的所作所为，甚至你的思想，其实在这个多维宇宙空间里本就是互联互通的，通过各种渠道都可以探知甚至预测你的所思所想、所作所为，严格来讲一个人本就没有任何隐私。

为什么没有隐私？有几种想象，

在多维的隐形空间里有无数只超级外星人的眼睛（记录仪）在盯着你，所以你的一切都存留在这个宇宙信息场里。

你所有言行举止的信息都是上传到“宇宙云”的，这些信息永久保存，有密码就能读取。

今天如果你能利用一个超光速的设备，穿越时空，那么就可以看到自己之前所有的言行了。

从宗教上讲，人在临终之际会回放此生的经历，从这个角度来看，我们的一切言行举止都会存储在某个信息场里。

所以佛学里说“善有善报恶有恶报，不是不报时候未到”就是指其实你是没有隐私的，你的作为都已经被记录，最后会和相关的人产生后续的果报。

我们觉得互联网只是提示人们，人类科学的发展将更透彻地认识宇宙是一个互联互通的整体，如今的互联网只是开始发现宇宙信息结构的一小步而已。所以人们如果觉得有隐私，自己做的事情没人知道，不过是基于肤浅的物质世界层面而已，对整个宇宙、人生，智慧的人们应该有更深奥的认识。

文章到此结束，如果本次分享的区块链和数据隐私性是指的问题解决了您的问题，那么我们由衷的感到高兴！