2009年1月，一种新型的电子货币来面世了：比特币。这具有开创性的技术立刻吸引了技术爱好者，一眨眼就得到了整个世界的关注。比特币是一个方便，可信的去中心化支付网络，但更重要的是，比特币用户的资金的控制权归属于各用户。转让比特币必须拥有一串特殊密码，也称为密钥，使用数字签名验证转款。如果一个未授权的第三方没有密匙，那就无法控制该用户持有的比特币。另外，货币供给的大小和增长取决于比特币网络用户所约定的规则。对于一般货币(美金)来说，因为政府或中央银行为了偿付原本付不起的债务或打工仔的工资，所以他们想要多少的钞票，就会印刷多少的新钞。而这本质上也会使他们的货币贬值，引发通货膨胀。无论是技术上、经济上、人道主义上，还是其它什么理由，比特币的优势都在逐渐被世人所认可。

尽管比特币有其突破性，但它同时也有一个主要缺陷：隐私。由于区块链总帐是公开的，所有地址的交易都是完全暴露的，这必然会让人感觉缺乏安全感。读到这里，你们中有些人或许会说：“这没什么，我没有东西需要隐藏。”或者说：“我不介意别人知道我做了哪些交易。”但是，我会尊敬地表示不同意!就算我们没有做任何错事，我们的交易也与他人无关。假设我让你随便拦下一个陌生路人，然后给他看你最近5年的信用卡账单，或者把你的手机借给你的同事，然后让他浏览你的邮件和信息。你会怎么做?会犹豫吗?会觉得受侵犯吗?你没有东西需要隐藏，但这并不代表别人或者政府可以有理由窥探你。如果你同意，或至少明白我要表达的点，那么就可以接着读下去了。

人们已经注意到比特币有一个严重的隐私问题，因而开始寻找“下一个比特币”。很多尝试都简单地复制比特币，再加入匿名交易功能。嗯，这是一个好的开始，但是还远远不够。最终，人们总能打破系统最薄弱的环节，破坏端到端交易的锁链。就算一个交易本身是隐秘的，那么其它的呢?交易通讯 和购买历史
是否也要隐秘呢?