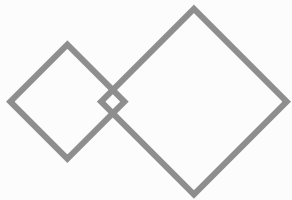


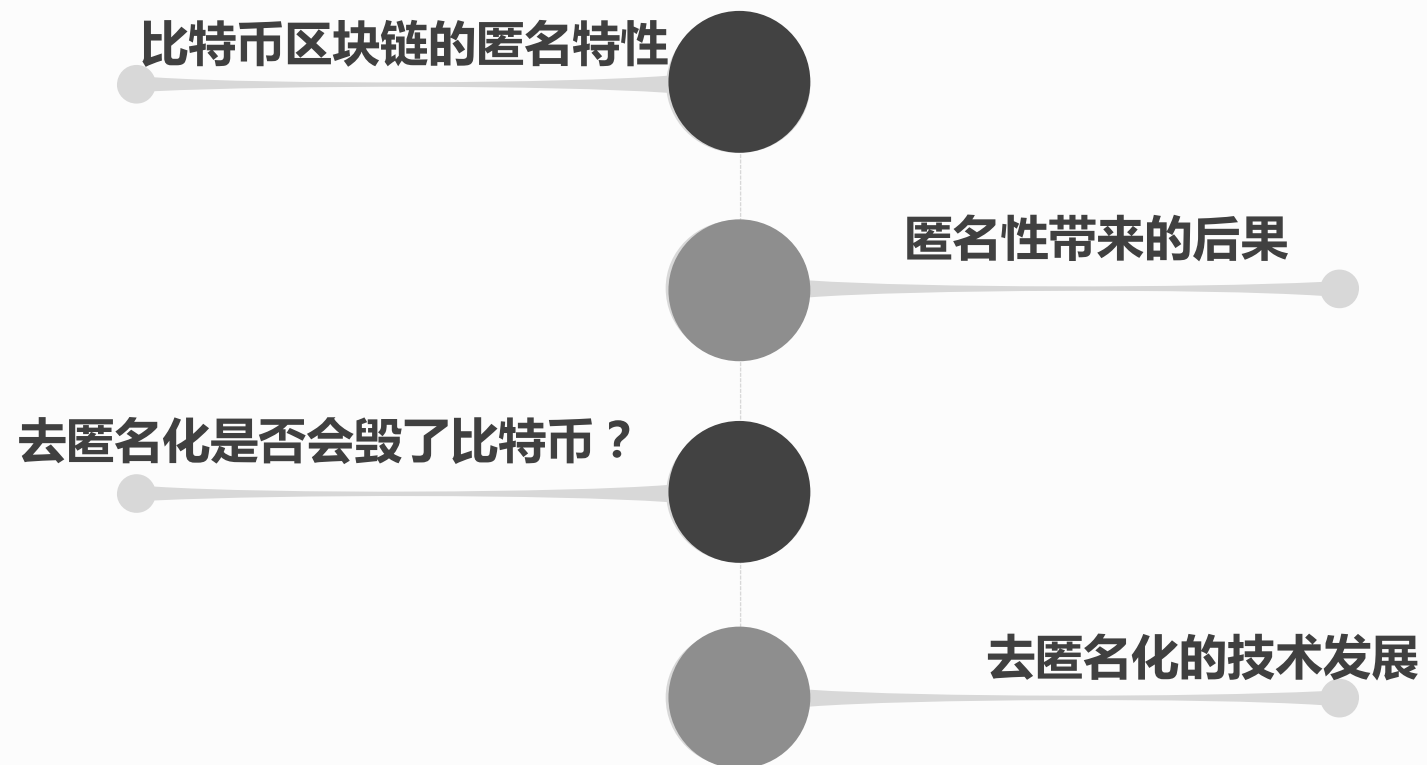


汇报人：罗毅

比特币区块链的去 匿名化



目录



1
PART 01
1

比特币区块链的匿名特性



比特币——去中心化的支付系统

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。

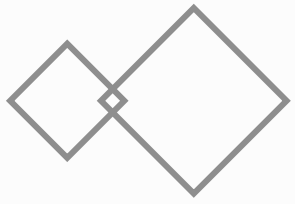


去中心化让比特币具有极高的匿名特性（非实名）

PART 02

匿名性带来的后果





匿名性带来的后果

1. 报告称，加拿大金融监管机构对区块链匿名性感到担忧

最新的报道显示，加拿大的金融情报机构—加拿大金融交易和报告分析中心(FINTRAC)对于区块链技术的匿名性所可能引起的犯罪和警务问题感到担忧。

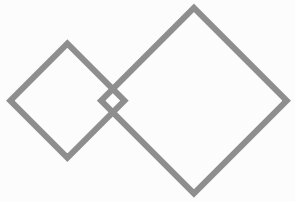
“该项研究会确认是否需要覆盖新的实体或规范新的报告要求，以解决这些未涵盖的交易和实体利用新兴技术洗钱或恐怖主义融资行为对加拿大金融体系造成的威胁。”



3
PART 03

去匿名化是否会毁了比特币？





去匿名化是否会毁了比特币？

1. 区块链交易的匿名性是“必要之恶”

匿名性很重要，信息的保密性和交易的安全性是分布式账本技术（DLT）匿名性环境带来的优势。

2. 可控制性

以《华尔街日报》的一篇有关Facebook和谷歌的潜力的文章，Epstein提出了大型企业都喜欢控制公众舆论的观点。他说那些缺乏匿名性保护的平台用户通常更容易受到其他人的操控。



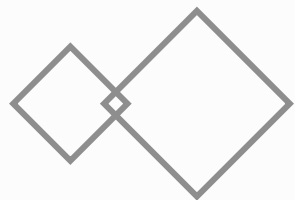


4
PART 04



去匿名化的技术发展

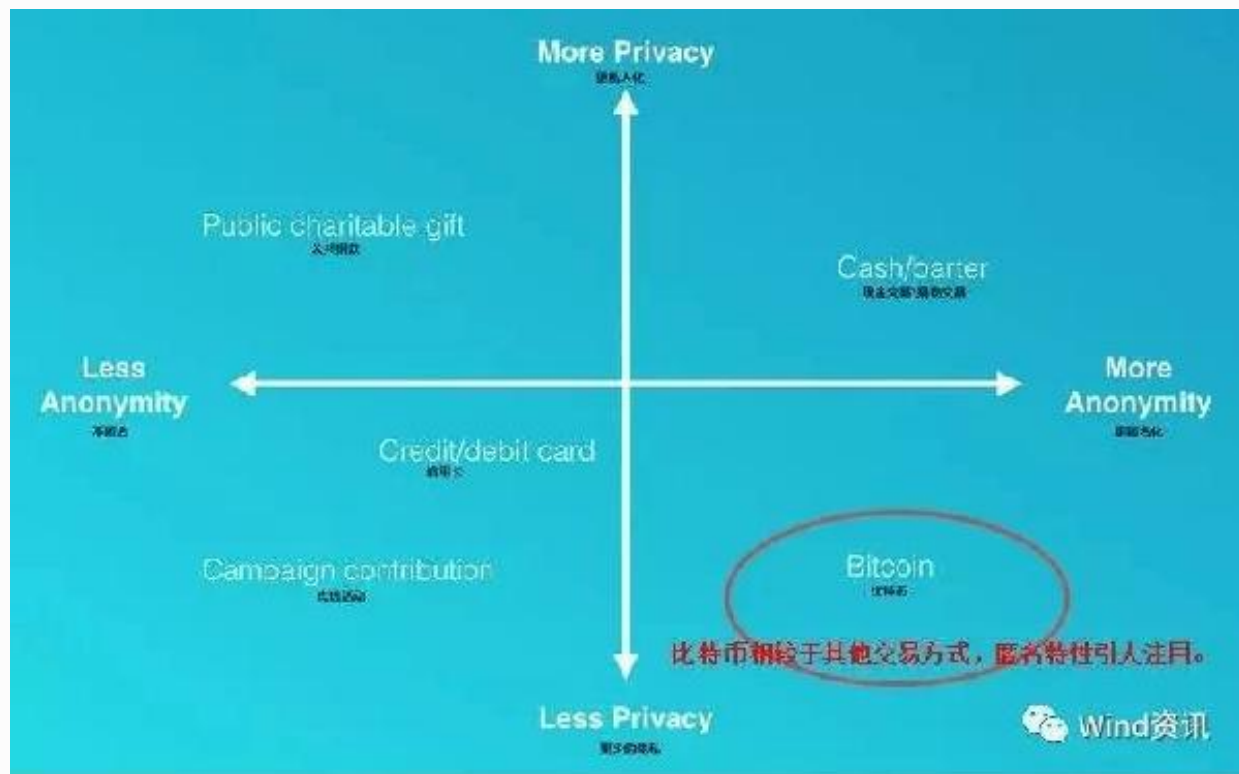




去匿名化的技术发展

比特币的匿名属性一直是金融监管部门面临的巨大挑战，但是这种情况早就发生改变。美国国税局已经开始采用新的区块链技术，追踪比特币的持有者。

数年来，比特币最大的卖点就是它的匿名性，竟然有那么多人信以为真。特别是当斯诺登(Edward Snowden)和维基解密这样的人何组织出现之后，盲目相信数字世界的匿名性显得“很蠢”。联邦调查局已经证实比特别的匿名性有多脆弱，一段时间以来，联邦调查局跟踪比特币交易并逮捕背后的交易者确实发生过。不管比特别交易员如何巧妙的掩饰自己的交易路径，但联邦调查局总有办法追踪到交易者的信息。





感谢您的观看