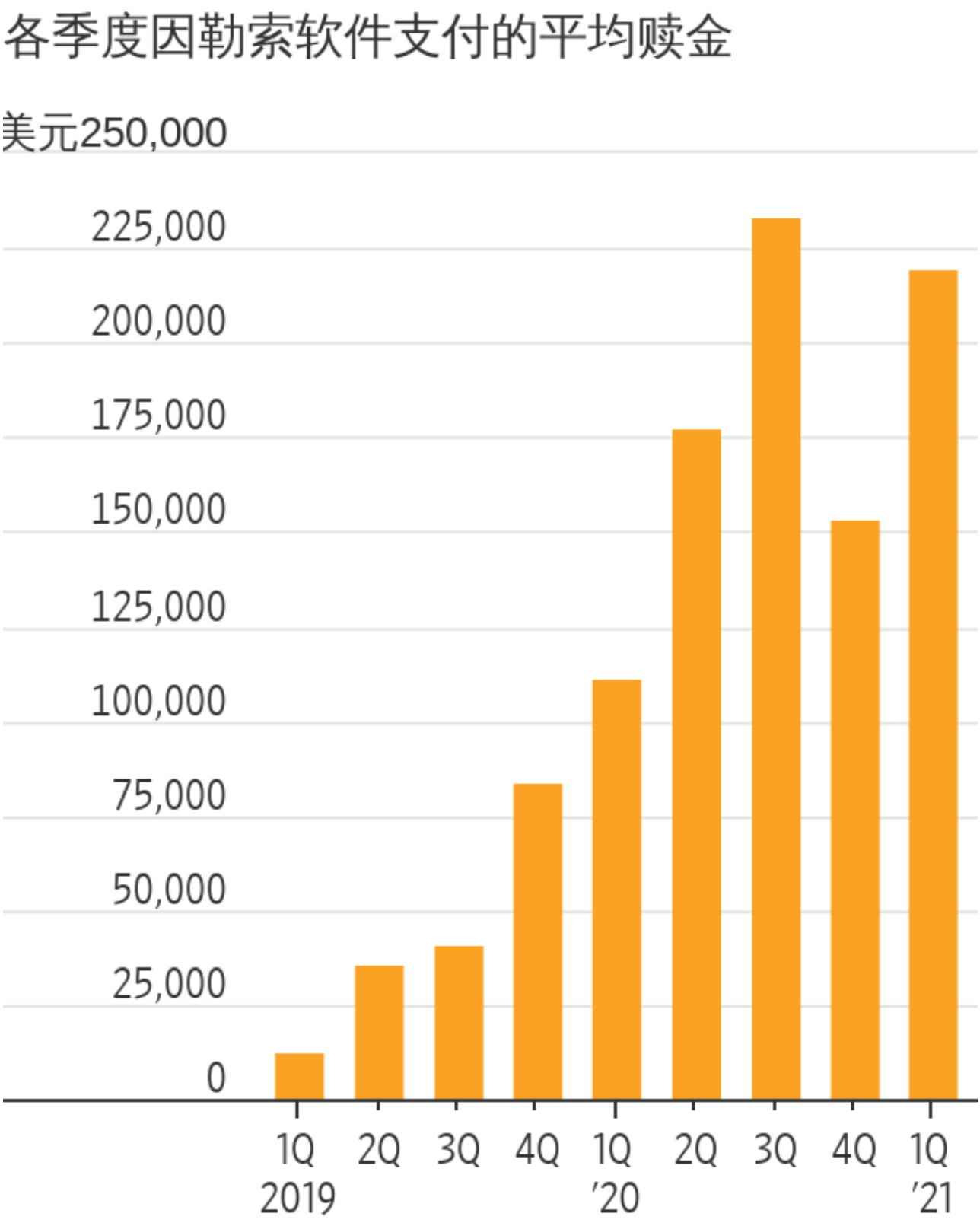
各季度因勒索软件支付的平均赎金
美元250,000
225,000
200,000
175,000
150,000
125,000
100,000
75,000
50,000
25,000
0
1Q 2019
2Q
3Q
4Q
1Q '20
2Q
3Q
4Q
1Q '21
数据来源：Coveware

此后，投机性交易的比重不断上升，但最近发生的一系列勒索软件攻击事件将数字货币犯罪问题的威胁推升至了更高程度。在这些攻击事件中，网络犯罪分子对受害者网络的文件进行了加密，并要求受害者支付赎金才能解锁这些文件，而其中最常见的付款形式是比特币。上个月Colonial Pipeline Co.遭到攻击，导致美国东海岸一条重要的汽油管道关闭；本月早些时候，另一起针对JBS SA的网络攻击导致美国的部分大型肉类工厂运营中断。

面临风险的不只是金钱。如果医院等机构受到攻击，生命可能受到威胁。在最近接受《华尔街日报》(The Wall Street Journal)采访时，美国联邦调查局(Federal Bureau of Investigation, 简称FBI)局长克里斯托弗·雷(Christopher Wray)将近期勒索软件导致的困境与2001年9月11日恐怖袭击造成的挑战相提并论。

执法部门面临的一个问题是，即使可以确认网络犯罪背后的犯罪分子，但与以前需用成袋现金或成箱黄金进行交换不同，现在的赎金交换完全可以在与美国没有引渡条约的国家进行。虽说FBI有能力扣押Colonial Pipeline支付给勒索软件团伙DarkSide的部分加密货币，但据信该团伙在俄罗斯运作，FBI对于其成员可能鞭长莫及。

另一个问题是，使数字安全强化到能把黑客关在数据大门之外绝非易事；我们所依赖的信息保护系统十分复杂，而且漏洞很多，黑客总有可乘之机。

加大网络罪犯接受加密货币支付的难度，从而减少勒索软件攻击的经济诱因，这可能会有所帮助。在这一点上，Wray拿来做对比的9/11事件很能说明问题。袭击发生后，2001年的《爱国者法案》(Patriot Act)在1970年的《银行保密法》(Bank Secrecy Act)基础上，引入了一系列更严格的条款，以破坏恐怖主义网络的融资。

要想解决这个问题，一个直截了当的办法就是广泛禁止加密货币的支付或交易，正如中国有关部门一直试图做到的那样。但考虑到加密货币现在牵动巨大的金融利益，很难想象美国会有这样做的政治意愿。至少不会一出手就走这步棋。根据coinmarketcap.com的数据，加密货币的总值为1.6万亿美元。

但美国还可以采取其他措施，这些措施可能也会削弱加密货币在商业中使用的可行性，或者至少提高加密货币的使用成本。

办法之一是加大被盗加密货币的使用或转账难度，就好比虽然可以用行李箱来装100万美元现金，但要花掉这些现金就很难不引起注意。参照企业现金支付超过1万美元须向美国国税局报告的规定，拜登政府正提议对所有企业持有的加密货币实施同样的规定。

政府也可能加强监督职责。已经有一些措施正在考虑之中。美国财政部去年以“国

家安全需要”等为由，提议对加密货币转账到所谓的“非托管钱包”进行额外核查；这类钱包不与银行或其他受监管的金融中介机构关联。作为全球打击洗钱行为的标准制定者，反洗钱金融行动特别工作组(Financial Action Task Force)最近提出了新指南，大幅扩大安全要求覆盖范围，纳入更多加密货币实体。

这些措施可能会略微削弱一部分比特币等加密货币交易的匿名和去中心化属性，而这是许多加密货币的倡导者不愿意看到的。加强监管还可能让合法交易程序更加繁琐，降低加密货币的吸引力。

但是，加密货币面临的最大风险可能是，这种监管努力无法有效地抑制利用加密货币实现的潜在危险行为。

在这种情况下，犯罪行为可能只会变得更加有恃无恐，同时对使用加密货币进行严格限制在政治上也更容易被接受。