第一财经研究院 RESEARCH
Committed to Improving Economic Policy.

Research Note

2017.6.12 (Y-Research RN17-140)

作者：杨燕青 林纯洁/第一财经研究院研究员
linchunjie@yicai.com

www.cbnri.org

研究简报 市场与监管

为什么我们需要监管数字货币

技术进步推动的犯罪、洗钱和恐怖主义从行为上越来越难以被侦测与阻止，全球应对机制的缺失更加剧了这种局面。

只要犯罪存在利益动机，其行为就可以通过货币的方式进行追踪，保证货币的可追踪可能是我们面对不断兴起的运用科技手段在全球搭建非法和犯罪网络的最后堡垒。如果我们放任基于加密技术的数字化货币游离于监管系统之外，所有的努力都将功亏一篑。

全球决策者需要联手启动对数字货币的监管，也应该从中吸取教训，正是公众对当前信用货币体系的担忧才造就了数字货币滋生的土壤。数字货币像一面镜子，能反射出问题，然而却绝非解决之道。

正如苹果公司 CEO 库克最近在 MIT 的演讲所忠告的那样：人类需要担心的不是机器越来越像人类，而是人类越来越像机器。人性、人类和经济社会的秩序需要公平和有远见的规则和监管的守护，尽管这些规则本身很难完美。

技术进步推动的犯罪、洗钱和恐怖主义从行为上越来越难以被侦测与阻止，全球应对机制的缺失更加剧了这种局面。

只要犯罪存在利益动机，其行为就可以通过货币的方式进行追踪，保证货币的可追踪可能是我们面对不断兴起的运用科技手段在全球搭建非法和犯罪网络的最后堡垒。如果我们放任基于加密技术的数字化货币游离于监管系统之外，所有的努力都将功亏一篑。

全球决策者需要联手启动对数字货币的监管，也应该从中吸取教训，正是公众对当前信用货币体系的担忧才造就了数字货币滋生的土壤。数字货币像一面镜子，能反

射出问题，然而却绝非解决之道。

正如苹果公司 CEO 库克最近在 MIT 的演讲所忠告的那样：人类需要担心的不是机器越来越像人类，而是人类越来越像机器。人性、人类和经济社会的秩序需要公平和有远见的规则和监管的守护，尽管这些规则本身很难完美。

1.被打开的潘多拉魔盒

科技的进步使大部分人感受到再无隐私可言，个人信息、喜好、去向、消费无一不暴露在数据中心面前。人们在享用因此带来的便捷和无所不在的服务同时，也开始感到不安，却又无可奈何。

2017 年 5 月全球爆发的大规模 WannaCry（又称 Wanna Decryptor）勒索病毒向我们展示了硬币的这一面带来的可怕未来冰山的一角。

WannaCry 让人们以新的视角关注网络犯罪和基于分布式网络的数字货币比特币，也第一次让很多人听到了暗网（darknet）的存在。

这件事情可以简单归纳如下：

一种政府开发的“网络武器”被匿名的黑客窃取，被窃取的网络武器流入到暗网从而再难被追踪；一个（或者几个）人以匿名的方式从暗网取得（或者购买了）该网络武器去攻击全球的电脑，并且勒索一定量的加密且难以被查清去向的数字货币；在一定程度上这种攻击失去了控制，以至于大量的公共设施成为了被袭击的目标，而在普遍的认识里，只有国与国之间的网络战才会涉及这些目标，聪明的犯罪者会尽量避开这些目标从而避免被激怒的政府猛烈的反击。

2.暗沉水下的网络世界：表层网络、深网和暗网

勒索病毒让暗网成为了一个新的流行名词，那么这究竟是什么？

我们将现实世界的网络分为表层网络（Surface Web）和深网（Deep Web），而暗网则是深网中的一部分。

深网与表层网络相对应，后者是大部分人接触到的互联网。如果将互联网世界比喻为一个海洋，那么那些可以用搜索引擎（谷歌、百度或者是必应）搜索到的有索引的网络是表层网络。在此之下，就是深网，深网资源没有被索引，也无法使用常规的搜索引擎搜索。

理论上深网有多庞大不得而知，但业内普遍估计深网的规模要远大于表层网络。

深网网站数量可能是表层网络的 400 到 500 倍，最大的 60 个深网网站存储的数据几乎相当于整个表层网络数据的 40 倍（Daniel Sui，2015）。正规机构也会在深网中建立自己的网站，比如美国国会图书馆、美国人口普查局和经济数据网站 Freelunch.com 等，另外即时通讯服务器也存在于深网之中。

图 1 你看到的是哪里的网络？

来源：http://www.brandpowder.com

暗网（Darknet）是深网的一部分，也是增长最快的部分。一般而言，暗网指的是深网中以匿名的方式通过分布式网络交换数据的部分，与浅层网络与大部分的深网不同，大部分的暗网都只能以匿名方式进入。

暗网依托于加密技术，而技术并无善恶之分。很多暗网用户的行为不一定非法，比如记者通过暗网来交流信息，那些担心被政府迫害的反对者也通过暗网来传播信息。

洋葱路由（Tor）是目前以匿名方式登录暗网的主要手段之一，每一个连接洋葱路由器的电脑都可以设立一个网站。人们可以连接这个网站，但却不知道其身在何处。美国海军研究实验室是洋葱路由器的发明者和传播者。美国政府仍然在继续发展匿名领域的科技并且对其进行推广。2010 年，洋葱服务器还获得了自由软件基金会（the Free Software Foundation）的 2010 年年度社会福利自由软件奖。

另外，大蒜路由“I2P”（匿名的网络项目，属于动态分布式网络）也越来越普及。其设计理念是不信任网络中的任何一方，所有数据都加密。

3.失控的黑暗世界：犯罪、毒品、洗钱和恐怖交易

网络技术的进步正将世界裂变为两种形态：在网络的一面，人们觉得自己一直被一双看不见的眼睛盯着；而在另一面，我们可以比过去任何时间都要隐藏的更深。

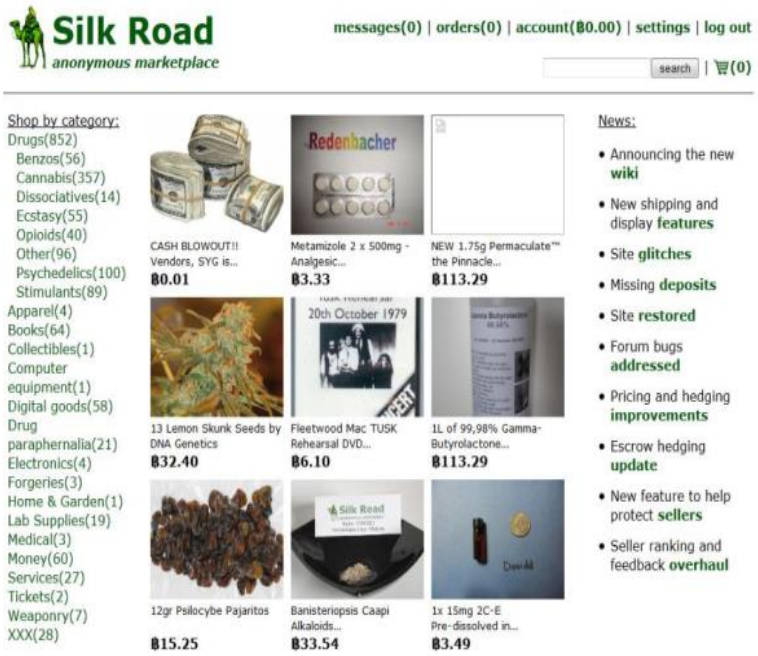
暗网让每个人都躲在面具背后，在这里我们可以看到失去约束之后世界的样子。

2013 年 10 月 1 日丝绸之路被关闭是很多人对暗网了解的启蒙。

外号“恐惧海盗罗伯特”的乌布利希（Ross Willian Ulbricht）在 2011 年创办丝绸之路网站时的目标是建立一个可以不被政府查获的线上犯罪市场。在之后的一段时间内丝绸之路网站声名鹊起，被誉为毒品界的亚马逊（Amazon）和易趣（Ebay）。

与其他网络购物平台一样，在丝绸之路上，商家同样会收到买家的评论，包括商品质量、物流时间等等。但不同的是，通过匿名服务器顾客从未真正接入商家的真正地址（IP 地址），反之亦然。

图 2 丝绸之路网页截图



来源：Global Drug Policy Observatory，Swansea University

美国联邦调查局（FBI）花了相当长的时间才搞清楚了这家众所周知的网站的实际控制人。在丝绸之路网站最终被关闭后，FBI 判断，丝绸之路在 2013 年 6 月前总成交量超过 12 亿美元（以当时价格的比特币计算），有超过 15 万的匿名用户以及大概 4000 个左右的供应商。

基于暗网的犯罪行为不仅仅限于毒品，也并没有在丝绸之路关闭后收敛，这些犯罪行为还包括买凶杀人、付费观看人类屠戮、

性交易、幼儿色情图片、非法证件交易等等。

2016 年部分暗网中售卖服务的名单和价格：

一个小时的 DDOS 袭击 5 美元；

1%的费用出具银行资产证明；

90 美元 30 万公里的航空积分；

30 美元一张美国运通卡；

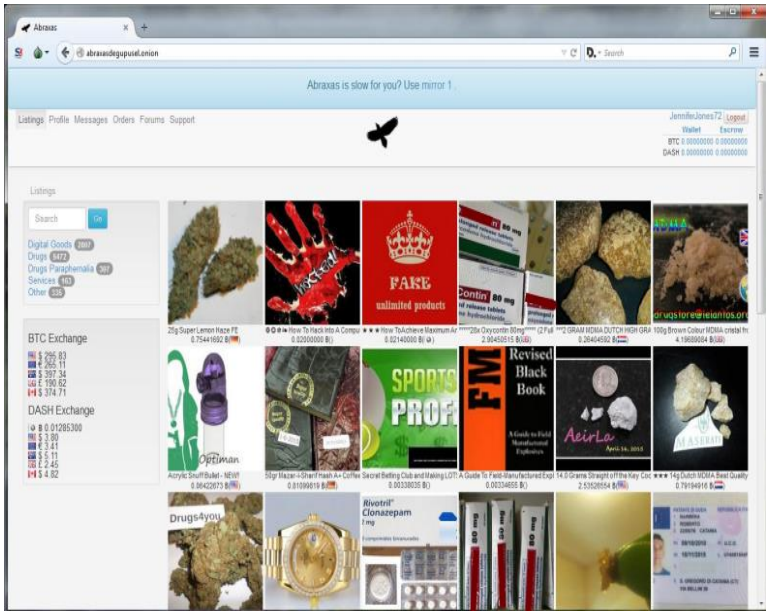
238 美元一张法国驾照，如果你需要的是德国或者美国的驾照，只需要 173 美元；

400 美元学习如何侵入 ATM 提款机；

20 美元的在线教程就可以教会你使用 DDOS 攻击，附赠破解 WIFI 的技能。

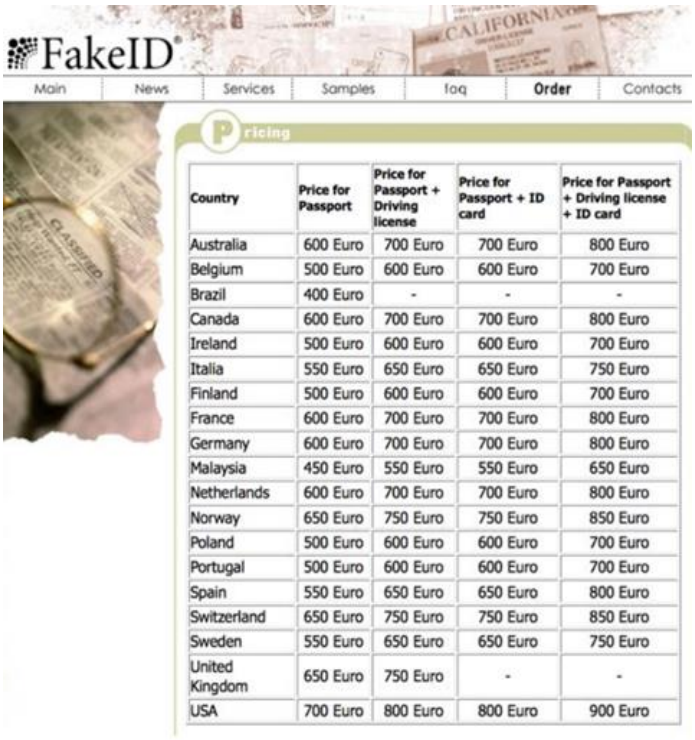
来源：2016 underground hacker marketplace report

图 3　典型的基于洋葱服务器的网络黑市网站



来源：Balduzzi M.,Ciancaglini V (2015)

图 4 明码标价的假证件


FakeID

Main | News | Services | Samples | faq | Order | Contacts

Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

来源：Balduzzi M.,Ciancaglini V (2015)

传奇黑客——Bat Blue 首席执行官帕斯达尔（Babak Pasdar）曾提到其研究中的一个意外发现，那些极具天分的人如何以一种游戏的心态去看待犯罪，比如说谋杀。帕斯达尔举了一个例子：一些网站通过众筹给出奖金，想要得到这笔钱的人需要上传证据证明自己执行了一次谋杀。

暗网并不仅仅为犯罪行为服务，同样也在推动犯罪。从人口占比而言，澳大利亚是全球毒品使用率最高的国家。该国 10%受访的毒品使用者在过去的一年中利用过暗网购买毒品，其中很大一部分是 25 岁以下的男性。那些从暗网购买毒品的人平均使用毒品的剂量更大。

洗钱、恐怖主义分子通过暗网获得武器，也让这些行为以以往难以想象的便利得以扩张。

4．全球化的网络犯罪与瞻前顾后的监管

黑客论坛 darkode 的覆灭可能是各国协查暗网非法网站中最知名的案例之一，超过 20 个国家参与行动。该论坛是黑客组织 lizard squad 专属交流场所，同时是一个从事网络犯罪交易的地方，黑客工具、僵尸网络工具、0day 漏洞、恶意软件程序、偷来的信用卡、垃圾邮件服务应有尽有。

但这些政府的介入仅仅是个案而已。

截至目前，政府和民众的主流倾向对暗网的调查十分谨慎，认为这会触及个人隐私或者商业秘密的底线，事实上他们很大程度上认可这种技术的存在。加之各国在这个领域展开合作也都心存顾忌，这使得对抗基于暗网犯罪的行为存在着天然的难度。

“监管者最初对暗网睁一只眼闭一只眼，事实上他们在很大程度上提供了暗网所需要的基础武器。”黑客“幽灵大象”（Ghost Elephant）说，“现在他们的态度也难说有根本转变。即使他们转变了，也难以扭转这种趋势。技术以野草般蔓延，政府并不拥有优势。”

“幽灵大象”致力于追逐那些存在于暗网的犯罪行为，他通过“污染”的文件侵入出售儿童色情图片的网站，然后反过来追踪到那些恋童癖的所在。但他坦言，“在最初，政府具有优势，而现在犯罪行为带来的利润已经筑起了高耸的防火墙，他们拥有最棒的天才，可以说，我们失去了最好的时机。”

2015 年，欧洲逮捕了使用著名网银木马 zeus 的犯罪团伙的五名成员，但仅在一个月之后该僵尸网络携带更加险恶的功能卷土重来。

在洋葱路由器开始向美国政府多次妥协后，更“安全”的大蒜路由成为了更多暗网网站的选择。

暗网市场正日益发展为传统的有组织犯罪的模样。澳大利亚国家药品和酒精研究中心(NDARC)的研究员巴斯柯克（Joe Van Buskirk）说，由于洋葱网络系统的匿名特性，人们不需要顾忌法律，任何东西都可以被出售。“当我第一次进入这个市场，我震惊了，这些网站看起了非常正规，就像是 eBay 一样，我想任何人都可以很轻松去使用。”

5.如何应对技术暴力？

暗网正滋生犯罪，但这并不是技术在犯罪领域的全部。

如果说过去制止犯罪的重要一环是在监控犯罪执行的过程，并为可能的犯罪工具打上标签，那么基于加密的技术会让这些努力付之东流。

控制枪支买卖可以限制犯罪发生和恐怖主义的泛滥。传统的方法是限制枪支的生产与流通，并通过弹道寻找枪支来源来震慑犯罪。很快，普通 3D 打印机使用普通耗材就能打印出枪支，犯罪后销毁，就像是它从来没有出现过一样，那么又将如何制止这些行为？

又如新型毒品。目前廉价的合成毒品正在大行其道，联合国毒品和犯罪问题办公室(UNODC)发现，每年向其报告的新合成的精神药物（Psychoactive substances）从 2009 年的 26 种飞速增加到 2015 年的超过 500 种，其背后的驱动力是巨大的利益。若未来的新型毒品可以通过家用打印机打印出来，交易的只是“用后即焚”的程序，我们又将如何应对？

技术的发展正将人类从“实力暴力”的时代推向“技术暴力”的时代。

在“实力暴力”时代，拥有最强实力的机构拥有控制权，即便是那些已经非常庞大的有组织犯罪团伙，其实力也难以和由民众

支持、掌握国家机器的政府相比。但现在情况却已经不同，掌握最好最新技术的人已经拥有了为所欲为的可能，而其他人只能任其宰割。优势并不总是在民众一边。

澳大利亚国家药品和酒精研究中心在一份报告中表示，该机构的“毒品趋势项目”从2013年开始就追踪暗网市场的毒品交易，他们发现在暗网市场上，经常会出现不同势力之间互相攻击服务器的行为。其中包括技术天才对那些政府也难以撼动的网络毒品交易网站进行勒索。

6.货币是最后的堡垒

即便是所有的犯罪行为都掩藏在暗处，终有一头会露出水面，只要他们的行为是利益驱动的，而大部分的行为确实如此。

在大多数情况下，犯罪行为要带来现实的财富，其行为才有意义，而货币是唯一的媒介。货币是一般等价物，是一种所有者与市场关于交换权的契约，货币要有价值，需要被越来越多的人认可。

金银时代之后的法定货币以降，发行广泛认可的货币（纸币）一直是政府的特权。这些货币可被追踪，从技术上讲，政府发行的货币可以判定因何而来，为何而去。所以在很长的时间内，如何让非法活动带来的货币变成合法收入一直并越来越是让犯罪者头疼的问题。

但数字货币正在改变这一切。

很多人可能认为政府肆无忌惮使用铸币权才导致了数字货币的兴起，这有道理，但并不能成为拒绝监管数字货币的理由。

注重隐私成为了文明社会的标志，但秩序才是维持文明社会运转的基础，而秩序的依托则是透明、可追踪和犯罪的代价，不管是对个人、企业还是政府都是如此。

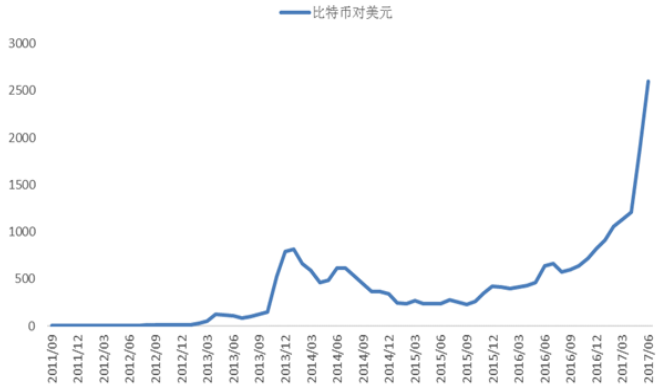
公布执政信息约束了政府的行为；企业依法纳税除了心怀家国，也包括担心偷税漏税后面临的惩罚；个人实施犯罪行为时最大的担忧是行为可能会被发现并最终被惩罚；个人和组织获得非法收入后由于全球反洗钱网络的存在无法“变现”；恐怖主义不仅难以获得资金和武器，并时时担心被歼灭。然而，想象一下：一个做错事和犯罪行为难以被追踪的世界会是什么样子？

潜于黑暗之中的暗网和基于加密的数字货币正成为即将到来的“技术暴力”时代的庞大市场和催化剂，即使对于普通的犯罪也是一种推动。

在“丝绸之路”关闭后的一个月，“丝绸之路 2.0”启动运营，在被捣毁后，使用I2P 匿名网络的“重生丝绸之路”（Silk Road Reloaded）网站诞生。唯一没有被动摇的是其支付手段，事实上更是被扩大了。“重生丝绸之路”不仅仅接受比特币进行支付，还支持其他 8 种不同的加密数字货币。

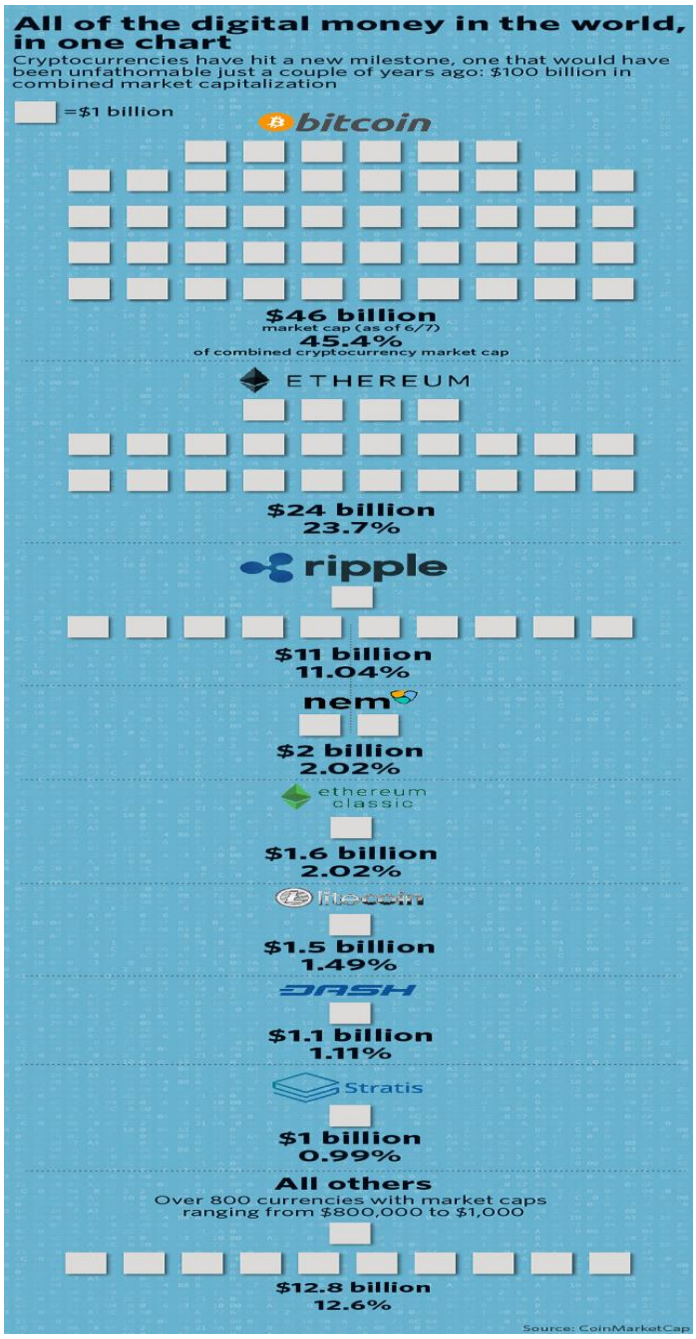
数字货币的总市值在过去几年出现了惊人的增长，截至 2017 年 6 月 7 日，全球数字货币总市值超过了 1000 亿美元，仅仅在 2017 年不到半年的时间内，比特币就上涨了超过两倍。中国的投资者为比特币等数字货币的价格疯涨作出了巨大贡献，2016 年中国比特币交易量占据全球交易量的 93%。

图 5 大幅飙升的比特币价格



来源：第一财经研究院综合

图 6 全球数字货币总市值超过 1000 亿美元

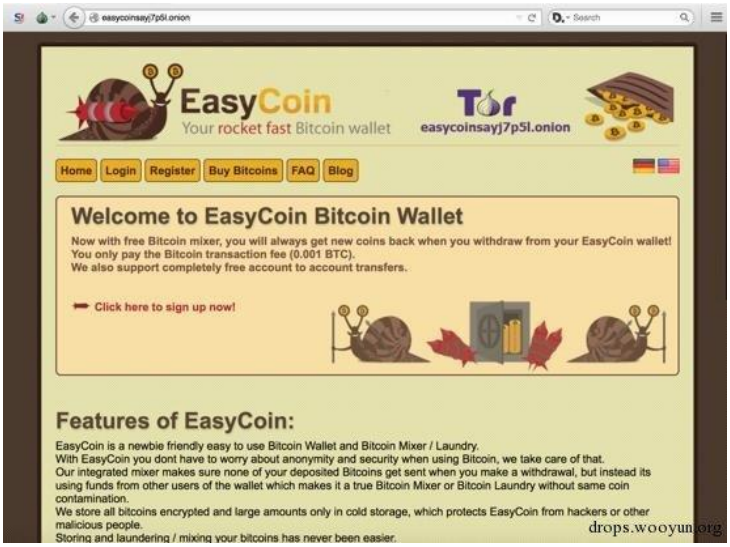


来源：CoinMarketCap

数字货币的加密功能并不是因为他们的交易过程是保密的，事实上由于分布式网络的特性，他们的交易比任何一种货币都要公开。这种保密是基于匿名（只要你不把个人信息与数字钱包联系起来）存在的，这意味着追踪数字货币的流通虽然很难，但仍然是可行的。

一些服务正致力于弥补这个“漏洞”，比如 Easycoin 的服务内容就是把比特币通过大量的微交易后再返回到你手里，从而使追查其流通状况变得更难。

图 7 致力于增强数字货币交易加密的 Easycoin



来源：Balduzzi M.,Ciancaglini V (2015)

数字货币正给这个世界带来改变，其中很多是正面的，在一定程度上它们对政府构成了牵制，给了民众另一个选择，但这并不意味着它们不需要被监管。

其中一个核心的理由是：匿名、不可追踪、不被监管的数字货币会让技术犯罪形成一个闭环，洗钱和恐怖主义大行其道，并消失于无法解开的比特字节中，而其影响却在伤害着这个世界上的每一个人。

如果勒索的每一分钱都会被追踪，发起 WannaCry 勒索病毒的人是否还有足够的动力和勇气对全世界展开攻击？

7、数字货币是货币？资产？还是别

的？

在我们真正开始行动之前，有一个问题要解决。

那就是比特币们究竟是什么？

货币？金融资产？别的？或者什么都不是。这个问题的答案将会决定我们采取怎样的行动。

货币是一种所有者与市场关于交换权的契约。通俗一点货币需要具备四种功能：交易媒介、记账单位、存储价值和延期支付标准。

比特币等数字货币目前已经起到了部分交易媒介的作用；在记账单位方面做得并不好，在其交易场景中他们更多只是用来支付而非定价，即使在大多数非法交易中也是如此；存储价值方面，并不能以数字货币对其他货币一段时间的涨跌做出结论，暴涨之后的另一种可能是暴跌，尤其是在存在价格操纵的情况下；最后一个功能就是延期支付，从目前来看还没有主要的债务合约以数字货币作为偿还方式，或者以数字货币为基准的债务被发行，另一个更简单的判断方式就是我们在谈论数字货币时没有提到过通胀，提到的只是该数字货币对于其他货币的涨跌。

所以数字货币还不是货币，至少目前还不是，甚至连接近货币都算不上。若要大胆畅想，以目前构架的数字货币作为全球货币体系的基础，它只会通向一个灾难性的结局：全球通缩和大萧条。

那么数字货币是金融资产吗？答案也是模糊的。金融资产是一种无形资产，其价值是通过合约的方式来确定的。比如股票是以合约确定公司所有权凭证，该所有权确保股权所有者能分享公司未来的收益；债券则是你有权利到期收回本息。

数字货币看起来也不是金融资产，但人们已经开始将其 ICO(Initial coin offering),类似 IPO。

那么数字货币到底是什么？它可能是一个“新物种”，但其影响已经大到我们无法忽视和不采取行动。

8.监管者应该做什么？

对于监管，这是一个非常难的局面，因为监管者无法对其套用既定的监管原则，但这并非不能解决，人类也不是第一次面对这样的局面。

首先，监管者应根据数字货币的特性制定监管原则。由于数字货币已经跨越国界，全球协作是必须的，G20 应对此有所作为。

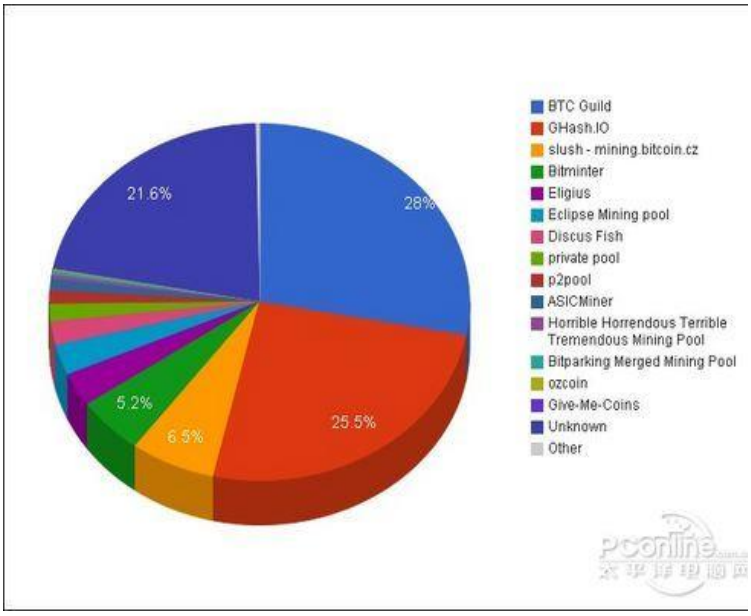
第二，可追踪和增强透明度是监管的方向。但这并不意味着数字货币需要放弃既有的主要特点，比如他们的基础挖掘方式等。

第三，因为数字货币已经被作为交易媒介使用，即使还不是真正意义上的货币，由于黑暗网络、犯罪和恐怖主义藉之的猖獗趋势，反洗钱规则须将数字货币纳入其中。

第四，如果我们假设数字货币是金融资产，那么适用于金融资产的那些基本监管规则例如信息披露、投资者保护等等都应是 ICO 等行为的基本要求。

第五，具体就中国的数字货币交易平台而言，绕过外汇管制、洗钱风险和恐怖主义威胁挥之不去，加之破坏平衡性的“矿机”使得掌握先进矿机和大量比特币的庄家已经形成市场操纵的能力，交易平台只剩下一个通往黑暗的洞口，已经失去了存在的合理性。

图 8. 比特币集中在几个“矿池”



枉过正。数字货币兴起的原因一定程度上与公众对于各国滥发货币现象的担忧相关。央行和政府应该正视这个问题并采取举措恢复公众信心，但在这个过程中不能矫枉过正。数字货币有自身的特点，但从目前来看，并无替代法定货币的基础，数字货币像是真实货币的镜子，它折射出根本性的问题，却带来了更多的问题，然而终究不是解决方案。

(作者分别是本报副总编辑和第一财经研究院副院长)

最后，政府应从中汲取教训，但不能矫