加密货币与《银行保密法》

2008 年年末，一个（或多个）化名为中本聪 (Satoshi Nakamoto) 的人发布了一篇 9 页长的技术文章，声称解决了电子资金转账的双重支付问题；而在此之前，电子资金转账需要金融机构的参与，才能实现在线支付。中本聪声称，利用这种解决方案，“[可以] 把在线付款从一方直接发给另一方，无需通过金融机构。”[1] 他把这种解决方案称为比特币。

中本聪并不是第一个提出加密资金转账方法的人；事实上，类似的支付方法至少可以追溯到 20 世纪 80 年代初。[2] 不过，中本聪这篇论文发表的时间——2008 年金融危机全面爆发之际——可谓恰到好处。人们对金融体系的信心大幅下降，这种与显然日渐失败的体系并无关联的支付方法和价值存储方法很可能正是人们需要的解决办法。另外，被称为区块链的分布式总账就是中本聪为解决双重支付问题而提出的新方法；只有具备不断提升的高水平计算机处理能力和广泛的互联网运用，该方法才可行。

自中本聪的论文发布以来，加密货币就呈爆炸式增长，目前全球有超过 1,500[3] 种加密货币，而且似乎每天都会涌现出更多的加密货币。除了在线交易所以外，加密货币还可以通过自动柜员机 (ATM) 购买，比特币期货可以在芝加哥商品交易所 (CME) 或芝加哥期权交易所 (CBOE) 进行交易，比特币掉期则可通过 LedgerX 交易，但要求缴纳 100% 的保证金。因此，众多金融机构可能会面临加密货币带来的风险，他们以前从未处理过加密货币相关事务，完全不知道如何应对相关风险。更具体地说，对反洗钱 (AML) 专业人员来说，有时候很难理解加密货币与《银行保密法》(BSA) 合规和报告要求之间的关系。在这个方面，金融犯罪执法网络 (FinCEN)

[1] 中本聪，“Bitcoin：A Peer-to Peer Electronic Cash System”（比特币：一种点对点的电子现金系统），Bitcoin，2008 年，第 1 页，https://bitcoin.org/bitcoin.pdf

[2] Victor Dostov 和 Pavel Shust，“Cryptocurrencies：an unconventional challenge to the AML/CFT regulators？”（加密货币：反洗钱 / 反恐融资监管机构面临的非常规挑战？）*Journal of Financial Crime*，2014 年第 21 卷第 3 期，第 250 页。

[3] www.coinmarketcap.com，访问时间：2018 年 2 月 8 日。

发布了指导意见，但其适用对象是加密货币交易所、[4] 矿工、[5] 支付处理商 [6] 和交易平台。[7] 对于未参与这些活动但其客户却有参加的金融机构，该如何是好？这些机构要遵循哪些《银行保密法》规定的报告义务？这些问题需要由监管机构来回答。本文的目的是强调其中的部分问题，并为《银行保密法》专员提出可能的解决之道。

数字现金

为了解加密货币对《银行保密法》报告的适用性，我们首先需要了解加密货币是什么。这并非易事，因为加密货币通常是按其功能来定义的。在有些情况下，它们可能是一种商品，[8] 其他情况下则可能是一种担保物。[9] 出于本文目的需要，我们将采用中本聪的定义，将加密货币视为现金。[10] 传统上，人们将现金理解为由政府法令支撑并被当作交易媒介的纸币和硬币。然而，如果采用一种抽象的理解，就如中本聪那样，把现金理解为任意匿名交易媒介，我们就能更加深入地了解加密货币在一般洗钱循环中的位置，尤其是在《银行保密法》报告中所处的位置。

这里我们需要探讨一下匿名的意义，因为纸币和加密货币通常被认为是匿名的，虽然后者不完全是。在论文（加密货币：反洗钱 / 反恐融资监管机构面临的非常规挑战？）中，Dostov 和 Shust 通过一个类比很好地解释了这一点：

> “我们需要区分真正的匿名与大众对匿名互动的理解，后者又被称为‘不可能性’。例如，不具名（但匿名）账户与其户主有着内在的关联性，如果至少有一笔用该匿名账户实施的交易可以追溯到一个真人，我们就可以把该账户（以及过去和将来通过该账户实施的支付）与其户主关联起来（例如，如果户主经常买可卡因，但犯了一个重大错误，即用同一个账户支付机票或酒店客房费用）。”[11]

对于加密货币，用“私钥”代替以上引文中的“账户”即可。图 1 进一步展示了这一区分。

像纸币一样，加密货币只有在金融体系以外才具有匿名性。由于交易会在总账里留下数字签名，所以，它们的匿名性甚至不如纸币和硬币。Adam Ludwin（上图即来自其文章）解释说：

> “普通用户要知道，[比特币] 的匿名性当然不如现金。与此同时，如果用户愿意竭尽全力、一心匿名，也可以找到办法，以匿名方式获取和使用比特币；但是，交易总账的开放性和其他未知因素导致始终存在一种可能性，即一度被认为绝对安全的身份和活动信息有可能在未来某个时候被揭露出来。”[12]

鉴于这种数字踪迹，更加准确的做法可能是把加密货币比作银行本票，而非纸币。[13]

《银行保密法》试图通过记录保存要求，消除其他现金形式的部分匿名性，比如金融票据日志、现金交易报告 (CTR) 和金融票据或现金的国际流动报告 (CMIR) 等。缓解

像纸币一样，加密货币只有在金融体系以外才具有匿名性

[4] “Application of FinCEN's Regulations to Persons Administering，Exchanging or Using Virtual Currencies”（金融犯罪执法网络监管规定对虚拟货币管理者、交易者和使用者的适用性），金融犯罪执法网络，2013 年 3 月 18 日，https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering

[5] “Application of FinCEN’s Regulations to Virtual Currency Mining Operations”（金融犯罪执法网络监管规定对虚拟货币挖矿企业的适用性），金融犯罪执法网络，2014 年 1 月 30 日，https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf

[6] “Request for Administrative Ruling on the Application of FinCEN’s Regulations to a Virtual Currency Payment System”（就对虚拟货币支付系统实施金融犯罪执法网络监管规定申请行政裁决），金融犯罪执法网络，2014 年 10 月 27 日，https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf

[7] “FIN-2014-R011”，金融犯罪执法网络 (FinCEN)，2014 年 10 月 27 日，https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf

[8] “In the Matter of Coinflip, Inc., d/b/a Derivabit，and Francisco Riordan”美国商品期货交易委员会，2015 年 9 月 17 日，http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf

[9] “Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934：The DAO”（依据《证券交易法》（1934）第 21(a) 节实施的调查的报告：DAO），美国证券交易委员会，2017 年 7 月 25 日，https://www.sec.gov/litigation/investreport/34-81207.pdf

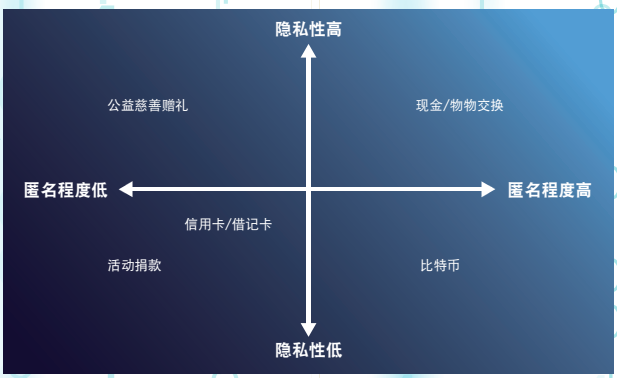
[10] 中本聪论文的副标题就提到了这一点：“一种点对点的电子现金系统”。

[11] Victor Dostov 和 Pavel Shust，“Cryptocurrencies：an unconventional challenge to the AML/CFT regulators？”（加密货币：反洗钱 / 反恐融资监管机构面临的非常规挑战？）*Journal of Financial Crime*，2014 年第 21 卷第 3 期，第 251-252 页。

[12] 同上。

[13] 银行本票的匿名性使其也应被理解为一种现金形式。

图 1



资料来源：Adam Ludwin，“How Anonymous is Bitcoin? A Backgrounder for Policymakers，”*CoinDesk*，2015 年 1 月 25 日，https://www.coindesk.com/ anonymous-bitcoin-backgrounder-policymakers/

图 2

资料来源：CME Group，http://www.cmegroup.com/trading/interest-rates/stir/eurodollar_quotes_globex.html [cmegroup.com]

图 3

资料来源：CME Group，http://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html [cmegroup.com]

加密货币伪匿名性问题的一种办法是要求超过一定金额的电子现金交易提交类似的报告。这种办法符合金融行动特别工作组 (FATF) 在有关虚拟货币的指导意见里提出的建议：“反洗钱 / 反恐融资控制措施应针对可转换虚拟货币 (VC) 节点——即通往受监管金融体系的交点。”[14]

美国已经要求用加密货币换取法定货币的人在金融犯罪执法网络注册，登记为货币服务企业 (MSB)，因而这些人需要遵守某些反洗钱要求。扩大这些要求的适用范围，要求超过指定美元等价金额的交易所交易（如用加密货币换法定货币，或者各种加密货币之间交换）提交报告，可助力执法部门更加深入地了解网络现金动向，使有关加密货币的要求与其他类型现金的要求更好地统一起来。

可疑活动报告

《银行保密法》的核心是向监管机构和执法部门提交可疑活动报告 (SAR)。事实上，《银行保密法》的所有其他要求（客户身份识别制度、了解您的客户、监控、培训等）对可疑活动报告起到了夯实的作用。金融犯罪执法网络就加密货币可疑活动报告提出了一些指导意见，称“各报告机构提交的可疑活动报告有可能提供有价值的账户、所有权和其他身份信息，以及与可疑活动相关的比特币地址。”[15] 虽然这有助于我们了解金融犯罪执法网络希望在报告中看到的信息，但我们仍然不清楚，在什么特殊情况下，加密货币交易会触发调查和报告要求。

首先，购买或使用加密货币的行为本身可疑吗？ 40 多年来，为了更有效地打击犯罪和恐怖主义，世界各地的政府一直在努力消除金融体系里的匿名性，并且取得了长足进步；但中本聪及其拥趸却让一切又回到了原点。在此背景下，我们当然可以问，使用加密货币的行为本身是否应该触发监管要求？事实上，有证据表明，将加密货币作为一种支付形式的人，这样做可能是为了达到不可告人的目的。在文章*《性、毒品与比特币：有多少非法活动的资金是源于加密货币？》*中，Sean Foley、Jonathan Karlsen 和 Tālis J. Putninš 估计，比特币市场有一半涉及非法活动：

> “……约有四分之一的用户 (25%) 和接近一半的比特币交易 (44%) 与非法活动有关。另外，以美元计价的交易总量约有五分之一 (20%)，比特币持仓量约有一半 (51%) 与非法活动有关。”[16]

[14] “Guidance for a Risk-Based Approach to Virtual Currencies”（虚拟货币“风险为本”方法应用指引），金融行动特别工作组，2015 年，http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

[15] “SAR Stats：Technical Bulletin”（可疑活动报告统计：技术公告），金融犯罪执法网络，2014 年 7 月，https://www.fincen.gov/sites/default/files/sar_report/SAR_Stats_proof_2.pdf

[16] Sean Foley、Jonathan R. Karlsen 和 Tālis J. Putninš，“Sex，Drugs and Bitcoin：How much illegal activity is financed through cryptocurrencies？”（性、毒品与比特币：有多少非法活动的资金是源于加密货币？）*SSRN*，2018 年 1 月，第 2 页，https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

然而，出于反洗钱风险考虑，我们需要区分将加密货币作为支付方式的人和投机者。正如 Foley 等人指出，“……非法用户主要用比特币进行支付，合法用户则更多地将比特币视为一种投资资产。”[17] 买入加密货币作为投资的人在风险状况方面与为采购目的而买入加密货币的人不同。由此推断，如果金融机构的客户进行加密货币交易，我们就应该查明，前述交易的目的是交易、转移资金还是投机，因为每种不同的目的意味着不同的风险水平。

可以根据涉及的币种把风险进一步分为不同的子类，因为有些加密货币（如达世币 (Dash)、零币 (Zcoin) 等）是为了避开多数加密货币的伪匿名性，几乎无法追踪其所有权。如果用户使用此类加密货币，金融机构就必须进一步查明使用这些加密货币的具体原因。

加密货币与洗钱

具有讽刺意味的是，加密货币由于被广泛用于上游犯罪，在洗钱方面似乎不太有吸引力。主要原因是，作为支付方式，加密货币尚未普及。Brenig、Accorsi 和 Muller 在其文章*《对以加密货币为支撑的洗钱活动的经济分析》中所指出，*

> “……加密货币目前的接受度有限，这直接影响了洗钱的实施流程，对洗钱犯罪分子使用加密货币的行为起到了抑制作用。即使将来情况会好转，加密货币也不大可能在接受度上超过被广泛用于各个经济部门的传统金融工具和服务。”[18]

美国联邦调查局在一份泄密的非机密情报评估报告中反映出同样的看法；该报告称，联邦调查局“评估结果表明，从用户和供应商当前的接受度来看，不法分子利用比特币洗钱的可能性很低。”[19] 尽管这份评估报告研究的是 2012 年

[17] 同上，第 26 页。

[18] Rafael Accorsi、Christian Brenig 和 Gunter Muller，“Economic Analysis of Cryptocurrency Backed Money Laundering”（对以加密货币为支撑的洗钱活动的经济分析），AIS Electronic Library，2015 年，http://aisel.aisnet.org/ecis2015_cr/20

[19] “(U) Bitcoin Virtual Currency：Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity”（(U) 比特币虚拟货币：情报独有特点为遏制非法活动带来显著挑战），美国联邦调查局网络情报科与刑事情报科，2012 年 4 月 24 日，https://www.wired.com/ images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

加密货币交易具有决定性且不可逆转

的情况，但时至今日，用户和供应商对加密货币的接受度仍然不高，这可能是区块链编程的通病。正如 Dostov 和 Shust 简要指出，

> “但几乎没有证据表明，比特币或任何其他加密货币的任何特点会促进加密货币的广泛使用。人们认为的加密货币匿名性仍是一个主要吸引因素，但其带来的欺诈、欺骗和技术风险巨大，令人难以接受。客户习惯了零责任和买卖双方保护措施，加密货币交易不可逆的特性会使他们望而却步。这种情况会使比特币限于少数鼓吹者的范围内，在 2140 年最后一枚比特币被挖出之前，投机市场早就萎缩了。”[20]

简言之，在信用卡交易和自动清算中心交易中保护消费者，使其免受不良商家影响的规则，在商家不提供服务或者商品时退款的规则，都不再适用；加密货币交易具有决定性且不可逆转。由于这些原因，普通消费者很难会将加密货币作为一种日常支付方式；如果得不到普通消费者的采用，则加密货币对洗钱犯罪分子的吸引力会下降。

另一个不利因素是价格的大幅波动，既不利于普通大众将其作为支付方式，也不利于用加密货币洗钱的人。例如，2017 年 12 月中旬首次亮相芝加哥商品交易所时，比特币期货短暂超过 20,000 美元，但不到一个月后，价格就跌去了将近一半；其后继续大幅波动，其间还多次出现巨额市场缺口，如下方的芝加哥商品交易所图 2 所示。与这种波动性形成鲜明对比的是芝加哥商品交易所欧洲美元期货合约同期的表现（见图 3），欧洲美元期货合约的波幅要小得多。[21]

这些产品在主要交易所上市后，其波动性最终有可能会下降，但当前市场的波幅仍然很大，可能导致比特币持仓价值大幅波动。犯罪分子洗钱是为了在不受执法部门干预的情况下，享用非法所得；如果还没用上，这些非法所得的价值就腰斩了，这种做法显然对他们没有太大的吸引力。

在洗钱循环中，加密货币主要出现在处置阶段。不法分子在暗网上完成非法交易，然后尽快把这些非法交易所得换成法定货币。因此，在与加密货币打交道时，必须把好通往金融体系的大门。如果金融机构有客户经常在各交易所之间来回倒腾资金，就应该把这些账户列为重点监控对象。

要报告什么？

然而，对于使用加密货币的客户，到底要报告什么，还有许多问题没有答案。除了交易、客户行为和一般人口分布特点，区块链本身也有大量的信息，可能需要列入报告范围。区块链中的信息是以加密格式保存的，但只要使用正确的工具，就可以轻松识别出来，而目前市场上有大量的这类工具。金融机构有义务扫描区块链，检查最近发生的交易吗？如果发现有客户最近通过加密货币交易所或者已知暗网发送过虚拟币，那么，金融机构需要向执法部门报告此事吗？如果需要报告，这种可疑事件需要离当前区块多远？如果是其到达金融机构之前的最后一次交易，或者距离 5 个区块，该怎么办？需要回溯多远？金融机构有义务扫描客户钱包，确定其持有哪些虚拟币吗？例如，如果有客户持有旨在更好地保护用户匿名性的基于零知识链的虚拟币，要报告吗？如果他们有链中的客户部分或者私钥，要报告整件事吗？

结语

回答所有这些问题超出了本文的范围。随着监管机构和执法部门越来越熟悉加密货币及其促进条件——区块链——并且随着用户模式日益显现，这些问题自然会得到解答。监管机构只是零星地提出指导意见，在一些具体情形中，他们显然有充分的理由不去妨碍一种很可能改变全球金融体系运作方式的技术。在过渡期，面临这些技术所带来风险的那些机构的银行保密法专员必须独自搏斗。虽然本文希望在区块链等方面提供一些帮助，但可能提出的问题比给出的答案还要多。 A

Chris Phillips，CAMS，峡谷国民银行副总裁兼反洗钱质量保证主管，美国新泽西州韦恩市，cphillips@valleynationalbank.com

[20] Victor Dostov 和 Pavel Shust，“Cryptocurrencies：an unconventional challenge to the AML/CFT regulators？”（加密货币：反洗钱 / 反恐融资监管机构面临的非常规挑战？）*Journal of Financial Crime*，2014 年第 21 卷第 3 期，第 259 页。

[21] 访问日期：2018 年 5 月 2 日，芝加哥商品交易所比特币图表可通过以下网址获取：http://www.cmegroup.com/trading/equity-index/us-index/bitcoin.html