第 14 章

直接投资加密资产：挖矿、交易所和钱包

现在，投资者可通过多种方式购买比特币和其它加密资产。虽然购买选项仍将不断增加，然而基本上包含两大考量：如何获取加密资产以及如何存储它们。加密资产作为数字无记名转让票据（digital bearer instrument），不同于中心化看管人持有的许多其它投资资产。例如，无论投资者通过何种平台购买证券，均有一名中心化看管人“储存”资产，且记录投资者的结余[1]。至于加密资产，创新型投资者可以选择一种相似的情境，或者完全自由地控制加密资产的存储。至于选择何种方式，则取决于创新性投资者最重视些什么；如同对待生命一般，必须权衡取舍。

挖矿(Mining)

为了帮助创新型投资者更好地了解比特币和其它加密资产的当前状况，有必要简述“挖矿”的进化史。此后，我们才会更加轻松地判断此等获取方式是否适当。即便某些投资者对挖矿本身不感兴趣，深入了解它也显得意义非凡，因为挖矿是获取许多新加密资产的一种手段，是一种支持相关交易的安全系统。

2009 年 1 月份比特币网络上线时，挖矿是获取比特币的唯一手段，而中本聪(Satoshi Nakamoto)和哈儿·芬尼(Hal Finney)则是两位主要的挖矿人[2]。如前所述，通过在比特币网络中验证和确认交易，进而制造新的比特币，而其基础则是中本聪创建的一大部分软件。借此可确保以去中心化手段创造出货币，且数量可控，这一切皆发生于比特币尚未布局全球之前。

挖掘比特币的流程，即处理（hash together）几个数据的持续循环以获取满足既定难易度的一个输出信息，主要是输出信息开头的数字 0。我们将此输出信息称之为“黄金哈希（golden hash）”。请想一下，一个哈希函数收集数据（例如：一个句子中的文字），将其转变为固定长度的字母数字串。尽管一个哈希函数的输出具有固定长度，然而它里面的字符却不可预测，因此改变输入信息中一个数据，将大幅改变输出信息。它之所以称之为“黄金哈希”，原因在于它给予了这样一个特权：挖矿人的交易区块附加于比特币区块链上。作为奖励，该挖矿者在一次 Coinbase(一家比特币公司)交易中获得报酬，这是区块内第一场交易。当前，此次交易向这名幸运的挖矿者交付了 12.5 枚比特币。

比特币挖矿作业中采用的计算机采集四个数据：适用于该区块的交易哈希，前区块的哈希（标识符），时间以及随机数 nonce。网络中不同的计算机采用这四个变量，然后增加随机数，也许从 0 这个随机数开始，然后采用 1，再采用 2，期望通过改变这一变量，哈希输出将满足起始 0 这一数字的必要要求。挖矿者可以检测的随机数越多，他们越有希望寻找到满足要求的黄金哈希。测试新随机数的速度，称之为哈希率，即一台计算机通过一个哈希函数，每秒钟运行这四个变量并且得出一个新哈希的次数。

任何人如果拥有一台电脑，均可以连接至比特币网络，下载过去的区块，记录新

的交易，处理必要数据，以寻求黄金哈希。此等开放体系结构，是比特币的最大优势之一。虽然貌似人人可以轻而易举地赚取比特币，然而如今却非常困难。自从比特币上市以后，不仅挖矿的计算机数量增加，采用的计算机类型也发生了极大变化。

最初，联网计算机利用它们的中央处理器（CPU）处理哈希值，而中央处理器是负责计算机正常运转的主要芯片。通过此种方法挖矿，大量占用计算机资源。尽管中央处理器可同时处理多项任务，然而它并非反复完成相同任务的最有效芯片，而这却是搜寻黄金哈希必不可少的过程之一。

理论上，图形处理器（GPU）这一芯片更加适合挖矿。顾名思义，图形处理器一般用于生成那些在屏幕上出现的图形，然而它们如今却被广泛地应用于机器学习应用。图形处理器是高度并行的处理单元，这意味着它们可以同时运行相似运算，因为它们拥有几百个甚至于几千个微型处理器，这与中央处理器正相反——中央处理器只拥有少量处理器[4]。

尽管图形处理器内部的小单元无法完成中央处理器可以处理的一系列抽象应用，然而它们却足以哈希数据。由于图形处理器拥有数千甚至于更多的核心，因此整体而言，一个图形处理器芯片每秒钟搜索黄金哈希的次数远远高于中央处理器芯片。

然而，在使用图形处理器时，必须创造一种新版本的比特币软件，用于指导图形处理器如何完成相应程序，而写这一代码需要时间。最终这一程序在 2010 年夏季上线——这多亏了杰夫·贾兹科（Jeff Garzik）向发行者提供 10,000 个比特币作为奖励，这一挖矿作业称之为 puddinpop，用于开放软件的源代码，方便所有人使用[5]。显然杰夫可能未曾预想比特币的价格在未来几年间增幅如此之大，他的捐赠价值如今已经超过 1,000 万美元。

虽然图形处理器相对于中央处理器而言已经大幅提升，然而另外两个技术更新迭代却生产出一种更加高效的芯片，可以更快速地猜测黄金哈希。第一个即现场可编程门阵列（FPGA），这是其爷爷辈芯片（即：特定用途集成电路（ASIC））出现之前的一种临时芯片。顾名思义，特定用途集成电路用于特定用途，这意味着必须根据具体用途，设计和制造物理硬件。一般而言，我们可以购买中央处理器、图形处理器和现场可编程门阵列，购买后，通过适当设计改造，应用于具体用途。另一方面，特定用途集成电路的物理布局，需要在半导体制造工厂凿刻于芯片上。

设计和制造此等特殊芯片，需要大量的前期投资，因此只有当比特币网络足够大且比特币足够昂贵时，一家公司方可完全利用此等机遇。配备特定用途集成电路芯片且专门用于挖矿作业的首台计算机（或：挖矿设备），于 2013 年 1 月份上线[6]。当前，顶级特定用途集成电路的哈希率是 14TH/秒，这意味着，这些设备每秒钟可以处理数据且输出一个哈希合计 14 万亿次[7]。

整体而言，与比特币网络连接的计算机越多，其中一台计算机发现黄金哈希的比率也更大。条件不变的情况下，计算机数量的增加，将提高新比特币的供应量，

导致失控的供给膨胀。为此，中本聪在比特币软件中植入了这样一条规则：当网络中加入更多计算机时，网络将增加启动哈希时零的数量，进而增大找到黄金哈希的难度。每隔 2,018 个区块或每隔两周做出一次此等调整，目的在于让挖矿者每隔 10 分钟才能找到一个黄金哈希，进而控制铸造新比特币的速度。结果，越来越多的挖矿工在激烈的竞争角逐中寻找越来越小的奖励，这虽然对于专业旷工而言利益颇丰，对于比特币业余爱好者而言却可望不可求。在这一层面而言，比特币网络的全部运算能力，比全世界前 500 台超级计算机的运力之和高出 100,000 倍[8]。

比特币之外的挖矿作业

虽然比特币挖矿网络的能力无与伦比，大多数其它加密货币却并非如此令人心惊胆战。狂热且专注的业余爱好者仍旧可以在以太坊、Zcash 和其它网络内挖矿，而且迄今为止 ASCI 尚未控制这些网络[9]。事实上，您可能会记得，后续资产频频做出的一项调整即面向区块哈希算法，以对抗挖矿者的中心化。为此，ether 和 zcash 以及许多其它加密资产大多数由图形处理器铸造。尽管随着这些资产数值的增加，其挖矿网络内部的竞争也越来越激烈，这是由于以本土资产（native asset）获得报酬的潜在利润越来越诱人。概念上讲，挖矿网络是一个完美的竞争体制，因此随着利润的增加，新的参与者将源源不断地涌入，直至再一次达到经济平衡。因此，资产价值越大，矿工的盈利将越多，这吸引着新的矿工加入此生态系统，进而提高了网络的安全性。这一良性循环确保了：一项加密资产的网络价值越大，其获得的安全性也将越高。

无论是比特币，以太坊还是 Zcash,许多矿工加入矿池，这意味着他们联系到其他矿工，此矿池加强了他们的哈希力，进而找到更多黄金哈希。然后这个矿池共享其利润，而分割利润的模式各有不同[10]。一名矿工每个月可能只能找到一个区块，情况甚至更差。然而加入矿池后，矿工将得到一个更加容易预测的收益流。

挖矿时有这样几大成本：设备、机器占据的必要物理空间、电力和劳力。对于比特币而言，矿工可以购买专业的挖矿设备，例如从蚂蚁矿机（Antminer）和阿瓦隆（Avalon）购买，而有待于寻找的一个关键度量标准即机器的效率。换言之，瓦特/千兆哈希（W/GH）这一比率，表示一定量电力可生成的哈希数量。为了更好地了解这些成本计算，请参考挖矿盈利性计算网站，例如 CoinWarz[11]。

基于云的挖矿（或云挖矿服务）

创意型投资者可能考虑一种云挖矿服务。在此，假如一名投资者买入一个已有的矿池，并且分享此矿池的挖矿作业带来的奖励。此时无需拥有或维护专门的硬件，正如同基于云的软件（例如:软件营销团队（Salesforce））无需维护所有的后端硬件。投资者只需购买由远程数据中心的挖矿作业提供的一部分处理能力即可。

在买入云挖矿服务之前，需要实施彻底的尽职调查和研究，因为以前发生过很多欺诈和诈骗案件。美国南方卫理公会大学的 Marie Vasek 和 Tyler Moore 教授研究了与比特币相关的诈骗案件，他们发现：多起云挖矿作业属于庞氏骗局，唆使投资者付款却从不交付产品。他们在研究中甚至指明了具体的挖矿骗局。“在 Active Mining 和 Ice Drill 作业中，他们筹资，有意制作 ASIC 并且分享利润，

却从未交付产品。AsicMiningEquipment.com 和 Dragon-Miner.com 都属于骗人的电子商务挖矿网站”[12]。

在投资云矿池之前，请务必研究调查潜在的投资项目。假如某个项目好到令人难以置信，恐怕它难以为真。请证实此种作业拥有实体位置以及一系列相关设备，同时追踪其过往项目。Genesis Mining 是全球最大的比特币云挖矿服务之一[13]。自从 2013 年上线以来，对外提供了比特币、莱特币、Zcash 和以太的挖矿服务[14]。其官网展示了自己数据中心的照片和视频；它的许多数据中心位于冰岛，这是因为地热能降低了它们在冰岛的电力成本。

权益证明（Proof of State）

除了工作量证明（proof of work）之外，也存在其它共识机制（consensus mechanism），例如权益证明（proof of state,或 PoS）。权益证明也可以作为挖矿作业的一种替代形式，它无需许多硬件和电力，然而却需要一些人敢于将自己的名声和资产置于险地，以帮忙确认交易的合法性。在逻辑层面，权益证明需要交易验证人在加密资产的结余上“下赌注”，在区块上证实交易的合法性。假如此等验证人撒谎或通过其它方式欺骗网络，他们将丧失自己“已下注的”资产。顾名思义，“为了证明自己有东西可下注”，在物质刺激和鼓励下，验证人将公正诚实地做事。

有时，这些系统将向那些敢于将自己的资产下注以验证交易合法性的验证者提供一定利率，例如 5%。虽然存在多种工作量证明、权益证明挖矿生态系统和其它变种，然而工作量证明确是久经验证、最可靠的共识机制，大多数加密资产都使用它。然而，以太坊在 2018 年初期有可能会转换到权益证明，因为它更加节能，因此许多人认为它的可拓展性更佳。当以太坊从工作量证明转换至权益证明时，对于此等共识机制的可行性而言，必将是一个重大的证明点，证明它可以保证大规模加密资产网络的安全。

加密资产交易所(Cryptoasset Exchanges)和场外交易市场办公室(OTC Desks)

当比特币和其它加密资产铸造完成后，矿工可以将它们换作其它加密货币或者他们选择的法定货币。为此，矿工必须将加密货币出售给其他人，要么通过场外交易市场（OTC），要么通过交易所。

许多矿工和实力颇丰的投资者选择场外交易市场服务，例如“坎伯兰郡挖矿（Cumberland Mining）”、“创世纪贸易（Genesis Trading）”或“itBit”提供的服务。场外交易市场并非一个实实在在的交易所，因为买卖订单并非完全公开。相反，如同上述服务一般的实体，将大型购买物同大型出售物匹配，进而无需在交易所内移动订货记录簿即可完成大型交易。对于那些希望使用大量资本且经过认可的创新型投资者而言，场外交易市场不失为一条可行的道路。

然而大多数投资者必须通过交易所获取加密资产。根据交易所的要求，他们可以连接自己的银行账户、信用卡或存储的比特币。在交易更新奇的加密资产时，往往要求投资者手中已经持有比特币，因为提供这些加密资产的交易所有时候并不

拥有法定货币入口。

在乱哄哄的比特币开端之年，当时比特币还是当时唯一的加密货币，许多交易所相继开张，又纷纷倒闭，而背后的原因并不美好：财政困难、黑客入侵、犯罪活动、各级管理机构的干预以及其它种种[15]。我们有必要在此指出：在比特币出现的早期，并不存在交易所基础设施，当时由于比特币尚处于初期阶段，有意于提供交易所服务的人群往往缺乏必要的设备和基础设施。

记录在案的一家交易所曾经一次性转让 5,050 个比特币，费用只有$5.02。事实上，由于利息问题，它曾经关门数月[16]。Mt.Gox 是全球第一家主流交易所，然而消费者结清账户却需要两周时间，最初必须将法定货币汇至日本。然而，随着资产和底层技术日益成熟，买卖资产的手段也不断发展。鉴于此，如今，投资者可以通过众多高质量的交易所获取和交易当前存在的 800 多种加密资产[17]。

当前最受欢迎的西方交易所包括：Bitstamp,Bittres,全球数字资产交易所（GDAX），Gemini, itBit，Kraken 和 Poloniex。虽然比特币中国,币行和火币网三者控制着中国市场，同时也在其它地理位置提供相关服务。另外也存在针对具体国家的交易所，例如墨西哥的 Bitso，印度的 Unocoin 以及波兰的 BitBay 等等[18]。

在决定使用哪一家交易所时，必须在“安全性和接入性”之间逐渐做出权衡取舍。安全性无需进一步解释。至于接入性，我们是指待售加密资产的多样性。管理规定最严格的交易所，例如 Bitstamp、GDAX 和 Gemini 出售的加密资产最少，因为将某一资产加入它们的平台之前，它们必须确保该资产已经达到了一定程度的成熟度。其它交易所，例如 Poloniex 或 Bittrex,在资产的较早阶段便已经添加到自己的平台上，因此更加冒进或更加敢于冒险的商人倾向于使用这些平台。同样的消费者保护机制不仅没有在这些交易所就位，而且它们提供的资产更加容易受到剧烈价格波动的影响。诸如 Bitfinex 和 Kraken 等交易所，提供安全、管理一致性和使用权等一揽子服务。我们在此并非告诫消费者不要使用任意此等交易所。这完全取决于创意型消费者正在寻求的安全平衡和使用权(access)等。

为了更好地了解与交易所安全和可靠性等相关的一些偏执想法，我们必须知道：随着时间的流逝，交易所已经变成了一个弱项，因为它们是加密资产的中心存放处，因为容易成为黑客的攻击目标。不同于银行抢劫案中需要动用暴力同时盗贼的生命安全也处于危险之中，这些盗贼们在盗取交易所的加密资产时，手脚相对干净，而且可以在全球任意地点操作。除了从远方盗取资产之外，加密资产交易时“不可撤销”的性质，增加了它们对黑客的吸引力。假如某人盗取了一张信用卡或侵入了银行账户，相关机构可以撤销交易。而对于加密资产而言，没有任意一家中心化中间结构可以提供救援。

退单(chargebacks)的隐藏成本

当一名消费者对于信用卡的收费项目存在异议时，此收费项目可以被撤销，这就是所谓的退单。通常情况下，当收费项目被退单时，商家承担损失。处理和调查这些退单事件，信用卡公司将承担相应费用，因此这些费用往往会转嫁给

商家。由于这些额外成本，商家可能需要调整价格以保护自己免于遭受合法和非法的争议收费项目。

而加密资产无法撤销。因此无法退单。虽然无法撤销的交易听起来有些吓人，实际上这有助于提高整体系统的效率。至于信用卡退单，所有相关方都要承担一定成本，而对于加密资产而言，只有粗心大意的相关方才会承担此等成本。

许多人声称，交易所入侵案件足以证明加密资产不安全，然而这表示了人们对于软件构架的根本性误解。请回忆我们在第 2 章节中讨论过任意区块链都具有四个层次：去中心化硬件、加密资产软件、应用和用户。大多数黑客入侵事件皆对准了第三层，即应用层。因此，交易所作为一个依靠各种加密资产软件而运作的应用，容易遭受黑客攻击。底层区块链可以完美地完成其职能，其安全性不会受到破坏。我们可以打个比方，即在苹果操作系统上运作的应用软件。如果其中一个软件被黑客入侵，这并不意味着苹果的基础性操作系统或硬件也不再安全。

由于那些使用和交易加密资产的应用和交易所最容易遭到黑客攻击，因此创意型投资者在决定使用哪一家交易所时必须谨慎，这一点非常重要。消费者最好考虑以下内容。

交易所的声誉如何？

辨别一家交易所声誉如何的最佳办法，即调查其管理层、风险资本投资者以及监管批准情况。搜索声誉良好的在线网站，了解其他用户如何评论一家交易所。消费者是否经常投诉？尤其是，查看一家交易所过去是否曾经遭到黑客入侵，是否存在商业问题。这非常简单，您只需在谷歌搜索页输入交易所的名称和“黑客入侵”这一单词即可。例如“Bitfinex 入侵”。虽然过去的黑客入侵事件也是一件较大的安全隐患，然而，请务必查看安全漏洞出现以后，此交易所做出了哪些改变。了解交易所总部位置也可以帮助我们的用户。假如无法查到此等信息，您最好不要使用此交易所。

哪些加密资产可用于交易？

如果投资者寻找具体的某些资产，请确保交易所提供目标加密资产的交易服务。请务必明白：可提供大量加密资产交易服务的交易所，其面临的潜在风险更大。它们对于这些资产的尽职调查往往松散、不严格，这将把风险和责任转嫁给投资者。

是否拥有其它职能，例如金融衍生工具(Derivatives)或保证金交易(Margin Trading)？

正如同加密资产的种类多样，交易所的职能也不同。某些交易所提供金融衍生工具，例如期货交易合同(futures contracts)，而其它交易所则精于精品金融衍生工具(boutique derivatives)的操作。例如，在 2017 年 3 月份，当我们尚不清楚美国证券交易委员会是否会批准 Winklevoss ETF 时，BitMEX 提供的精品金融衍生工具是一个不错的选项。同样道理，用户还需调查另一个职能——保证金交易，并非所有保证金交易都是公平的。某些交易所提供极高水平的保证金交易，例如 30：1，而其它交易所则更加保守，例如 3：1。在杠杆效率方面，30：1 的

保证金交易意味着一名投资者的$1,000 可换得$30,000。虽然收益及其可观，损失也是如此。同样道理也适用于金融衍生工具。某些交易所面对出错的杠杆率，选择将“损失社会化（socialize losses)”，因为这些交易所无法通过任意其它方法提供产品[19]。“损失社会化”是指，交易所的所有投资者为少数投资者的愚蠢行为买单。

开立账户时可选择哪些筹资机制？

投资机制，将指明创意型投资者在最初时是否可以使用相关服务。已经持有比特币的投资者拥有更多选择，因为交易所允许直接转让比特币，因此可以立即交易平台上提供的加密资产。通过法定货币为账户筹资时，通常需要链接至银行账户或信用卡。它们将需要一个更加全面的账户开立过程，该过程可能持续数天，且受到地方法规的限制。在向交易所提供银行账户信息时，请务必调查此单位以确保安全,这一点十分重要。请不要轻易地在线向任意金融实体提供银行账户信息。

服务是否受区域限制？

许多交易所受地理位置的限制，因此需要一个地址以实现它们服务的某些方面。这与纽约州的居民尤其相关，因为在纽约州,比特币执照让加密资产创业公司的运作尤其困难。比特币执照是实施于 2015 年的一项法规，要求那些从事加密资产的公司完成一段漫长且昂贵的监管程序，之后才可在纽约经营，这导致大多数加密资产创业公司停止在该州的经营。

KYC（了解你的客户）和 AML（反洗钱）的要求有哪些？

“了解你的客户（KYC)”和“反洗钱（AML）法规”对于美国加密资产交易所的强制性逐渐增强，它们旨在避免非法和/或诈骗活动。开立账户时，请考虑所需个人信息的数量。诸多交易所（例如：Bitstamp, GDAX 和 Gemini 等）一直以来积极地参与立法，以便那些登记开立账户的消费者提供更多详细信息。此等信息可能延迟账户的开立过程，通常延迟数天。有些人认为隐私性是加密资产的一大优势且超越国界限制，他们可能避开那些要求提供此等等级文件信息的交易所。整体而言，较高等级的法规可能有利于投资者的消费者保护，确保交易所的稳定性[20]。

交易所是否提供保险？

随着比特币和加密资产交易所的使用率不断增加,交易所的保险计划也不断增长。其中一个保险公司是三井住友保险公司(Mitsui Sumitomo Insurance)，向为数众多的交易所提供损失保护[21]。其它保险公司也正计划进入此领域，有助于创新型投资者调查他们选择的交易所是否具备此保险计划。Coinbase 是首批向其客户的比特币持有权提供保险服务的公司之一，包括 GDAX（即：Coinbase 经营的交易所）的比特币[22]。在某种程度上，Coinbase 能够给自己客户的比特币投保，因为它在线持有客户资金的比率小于 2%；其它资金则在线下以高度安全的方法储存。

钱包和冷存储（cold storage）之间的对比情况

现在让我们回到热钱包（hot wallet）和冷存储之间的差异，以及了解这二者为何如此重要。加密资产的获取和储存是两个独立的考量。虽然在默认情况下交易

所将储存它们交易的资产，然而这并非长期存储资产的最安全之地。

加密资产存储于热钱包或冷存储之中。热钱包的“热”是指它与互联网连接。当通过互联网可以直接访问钱包，或者通过已经接入互联网的机器设备访问钱包时，此钱包可称之为“热”。假如创意型投资者通过一个互联网游览器或者通过联网设备上的桌面或移动应用，可直接使用他或她的加密资产，这就是热钱包。

冷存储，是指以未联网方式存储加密资产的设备。此时，一名黑客必须亲自盗取此设备，方可获取加密资产。许多方法则要求存储加密资产的设备必须从未联网。一次也未联网。虽然这听起来有些极端，这却是公司存储大量加密资产的最佳方式。对于大多数（尽管并非所有）安全意识较强的投资者而言，这一手段十分必要。

这对于加密资产的存储而言有何意义？这意味着存储个人密匙，进而允许持有者将加密资产发送给个人密匙的另一名持有者。个人密匙只是能够打开数字保险箱的一串数字。通过个人密匙，其持有者可以通过数学方法向网络证明：持有者是加密资产的所有者，随时可以处理自己的加密资产。数字钥匙可以存放于热钱包或冷存储中，而众多服务商可提供此等存储方式。

对于冷热存储两种方式而言，创意型投资者可以选择两种方式控制个人密匙，总计四个选项，投资者可以任选其一。例如，大多数交易所帮助消费者保管他们的个人密匙，因此所有消费者只需要通过任意常用网址，登录交易所即可。这些交易所相当于热钱包，而第三方控制个人密匙。Coinbase 等服务商提供冷存储服务，第三方仍旧控制着个人密匙。当第三方控制个人密匙时，服务商往往并未拥有每一位消费者资产的个人密匙。相反，服务商一般拥有可掌控大量消费者资产的少数几把个人密匙，且这些钥匙非常小心翼翼地保管着。

· 热钱包 · 投资者控制着个人密匙	· 热钱包 · 第三方控制着个人密匙
· 冷存储 · 投资者控制着个人密匙	· 冷存储 · 第三方控制着个人密匙

图 14.1： 保护加密资产的四种方式

假如创意型投资者不愿相信第三方，他们还有另外一种选择，即自己直接掌控个人密匙。虽然这同样存在风险（例如：丢失个人密匙等），假如投资者采取了谨慎措施，那么可确保独立自主性，同时将安全的钥匙直接放到所有者手上。

通过交易所保管

默认情况下，交易所必须存储消费者的加密资产，常见方法即运用个人密匙。我

们在此再次重复一遍：许多交易所甚至没有不同消费者的独立个人密匙。交易所配有自己在区块链上负责的加密资产的个人密匙，且保存内部账簿以记录消费者的结余情况。根据交易所类型的不同，安全性等级不同，且通过冷存储或热存储方式保管的交易所资产比率也各不相同。随着时间的推移，经证明这些安全性差异十分重要。为了方便读者更加清晰地了解，我们将披露几个严重的黑客入侵事件，它们都发生于通过热钱包方式全部储存各自比特币的交易所。

首先讲讲臭名昭著的 Mt.Gox。尽管此交易所努力在全球范围内扩张比特币的使用率和识别度，却仍旧在 2014 年早期走上了绝路[25]，当价值 4.5 亿美元[26]以上的客户比特币丢失后，该公司宣布破产。虽然此公司倡导向投资者和兴趣爱好者提供更加简单的比特币获取方式，然而它在资产种类方面的管理能力较差，因为这仍旧处于发展早期阶段。它从来都不是一个优秀的组合。

杰德·麦凯莱布(Jed McCaleb)是 Mt.Gox 公司的最初所有者。创业初期，他意识到匹配比特币买卖方法的难度超出了自己的意料，因为当时成千上万的美元源源不断的汇入。麦凯莱布将网址和其日益增长的经营活动卖给了马克·卡佩勒斯(Mark Karpeles)，他在当时以“魔力塔克（MagicalTux）”这个网名而广为人知，并且喜欢在网上发布猫咪视频。值得称赞的是，卡佩勒斯重写了网址，以满足日益增长的兴趣和活动。在其它比特币交易所快速失败的前期时段，他却活了下来[27]。

虽然卡佩勒斯展现了一定水准的编码能力，然而在商业方面却发现自己捉襟见肘，难以支撑。他未寄希望于自己公司的增长，不久之后自己的编码能力也出现了严重不足。一家经验丰富的科技公司，此时本应该为自己的编码创建了一个测试环境和版本控制软件，这正是 Mt.Gox 经营的支柱。然而卡佩勒斯并未这样做，他直接发送所有编码变化，因此当编码需要快速变动时，此种做法导致了众多瓶颈的出现。

虽然卡佩勒斯可能忽略了 Mt.Gox 商业运作的诸多方面，他却知道比特币冷热存储方式之间的差别。他亲自负责该交易所储存的比特币的所有个人密匙。在 2011 年黑客入侵事件发生以后，卡佩勒斯决定将大多数比特币转入线下，采用冷存储方式，这就要求他写下个人密匙，然后将密匙放到东京（公司所在地）市内的保险箱内。这要求大量的文书工作和会计工作，而它们显然并非卡佩勒斯的强项[28]。虽然个人密匙以冷存储方式存放，卡佩勒斯却宣称：一名黑客通过核心比特币软件中的交易可塑性漏洞操控了他[29]。虽然在比特币社区内许多人怀疑卡佩勒斯的言乱，毫无疑问，此次黑客入侵事件的主因即安全卫生条件较差，公司为了移动比特币而采取的运作流程薄弱。此等疏忽导致投资者损失了价值 4.5 亿美元的比特币。

最近，一名黑客从 Bitfinex 盗取了价值 7.2 亿美元的比特币[30]，这是由于该公司将其所有的客户资产存放于热钱包之中。至于该公司如何这样做，争议不断，难有定论。有可能是处于流动性目的——因为 Bitfinex 是流动性最好、最活跃的交易所之一，或者由于已实施的管理规定之故。在黑客入侵之前，Bitfinex 以 75,000 美元与美国商品期货交易委员会达成初步和解，因为其比特币冷存储的

方式违反了该委员会的相关法规。许多人认为该公司之所以将所有客户资产放到热钱包之中，正是由于此次罚款和美国商品期货交易委员会的相关法规[31]。无论如何，此次黑客入侵事件证明：无论采取了何种安全措施，热钱包的安全性往往低于正确实施的冷存储，因为任何人通过互联网连接均可以在远方访问热钱包。而盗贼只有亲自破门而入才有可能盗取冷存储之中的资产。

在 Mt.Gox 遭遇黑客入侵时，比特币及其底层技术，如同任意其它新科技一般，正处于初期阶段，其忍受的痛楚日增。著名的风险资本家弗雷德·威尔逊(Fred Wilson)在事件发生后不久写道：“我们正在见证一个行业的成熟，而其过程不可避免地出现失败、崩溃和其它麻烦。我亲眼所见，凡是大规模应用的每一项技术，都会经历此等成长的苦恼[32]”。任意一项新技术的创新者和早期采用者都会承担风险，然而随着时间的推移，交易所变得越来越专业。不幸的是，Mt.Gox 并不在此列。Bitfinex 完成了自身的重组，一路上嗡嗡前行。这些黑客入侵事件，不仅给新旧加密资产交易所上了一课，同时也教训了客户。

遭遇客户入侵风险最大的交易所，即在热钱包中存储大量资产的交易所。冷存储方式可能会影响交易所和客户快速获得资产的能力，然而您却用“可及性”的损失，换得了更高的安全性。

加密资产钱包的世界

将加密资产存储于一家交易所，有时候并非最安全的选项。已投保、将大多数资产存放于冷存储之中且采用其它最高等安全措施（例如：渗透测试和常规审计）的交易所，其风险相对较低。而对于其它交易所而言，如果创新型投资者不断地交易且利用交易所的职能（例如：提供更新的加密货币等），那么其风险尚可接受。如果未时常交易，那么投资者可能需要考虑以下钱包选项以安全地存储他们的资产。

广义上讲，共有五种钱包：网络(云)(web(cloud))、桌面(desktop)、移动(mobile)、硬件(hardware)和纸(paper)。为了简洁之故，我们将通过比特币分别介绍它们，因为比特币提供了必要的脚手架，可以帮助我们调查适用于其它加密资产的类似选项。

如果您需要详细了解不同种类的比特币钱包，请前往 bitcoin.org。在此书籍的“资源”部分，我们涵盖了额外的信息来源。请注意：随着人们对加密资产的兴趣持续增加以及越来越多的人使用加密资产，安全存储这些资产的钱包种类也将不断增加。

网络钱包

大多数网络钱包与交易所并无太大差异。投资者无法掌控个人密匙，它们由中心化第三方保管。假如第三方未应用适当的安全技术，加密资产将处于风险之中。如同交易所，从世界上任意地点均可以访问网络钱包，这是其主要优势之一。流行的网络钱包包括 Blockchain.info 和 Coinbase。许多网络钱包也允许投资者自己掌控个人密匙，这使得它们类似于可通过远程访问的轻量型桌面钱包（请参考下文）。

网络钱包的一个特性广受欢迎，即“保险库服务(vaulting)”。保险库(vault)可延缓任意加密资产的提取过程，因此持有者有时间撤销任意非法的提取操作。这种策略主要用于防止黑客盗取用户密码然后将加密资产转移至其它地点。Coinbase 网络钱包的“保险库”服务最知名。

加密资产保险库

Coinbase 的一个优势特征即，它允许消费者轻松地获取比特币结余，以及流动性更好、高度安全的存储方式，称之为“保险库”。尽管将比特币结余放置于保险库之中增加了安全性，然而在提取之前，却要求两因素认证，且存在时间延迟。这意味着，从保险库提取资金需要 48 小时。Coinbase 的双重功能类似于在银行开设一个活期储蓄账户。投资者需要快速提取的比特币，可放置于常规 Coinbase 账户中（活期账户），而需要额外安全性的比特币，则存放于保险库账户（即：储蓄账户）。

桌面钱包

至于桌面钱包，个人密匙直接存储于一台已下载软件的计算机中。用户拥有完全掌控权，任何其他人无法丢失、花费或发送他的比特币。当前共有两种桌面比特币：完全客户型和轻量客户型。此处的“客户”是指在计算机上运行的软件应用的功能性。完全客户型是一个更加全面的软件应用，而轻量客户型则是存储比特币的一种更简便方式。

在 Bitcoin 的前期发展阶段，只存在与中本聪软件相关联的钱包，如今称之为“比特币核心钱包”。它属于完全客户型，意味着它需要完全下载比特币的区块链，因此需要大宽带和存储空间。当一台计算机运行此软件时，它在比特币网络上被视为一个“完全节点（full node）”，这意味着它将记录每一笔比特币交易。完全节点非常有益于安全性和自主性，是传送和验证比特币交易的主干力量，然而只有最铁杆的爱好者才能够满足其硬件需求[34]。

轻量客户型，也被称之为“瘦客户型”，无需下载比特币的全部区块链，也无需传播或验证在网络上传递的新交易。然而，它们依赖于完整节点以获取关于比特币区块链的完整信息，且主要侧重于提供仅与用户的比特币有关的交易信息。对于那些无法运行完整客户型钱包的普通用户而言，轻量型钱包显然更加实际。对于这些钱包而言，个人密匙存储于那些已下载了软件的计算机上。当前广泛使用的轻量型钱包包括：Coinomi,Electrum 和 Jaxx。

移动钱包

在技术层面，移动钱包将个人密匙存储于设备上而非第三方的服务器上。移动钱包也无需下载比特币区块链（因为这样可能损坏智能手机），在这一方面类似于轻量型钱包。如果四处奔波的创新型投资者需要将比特币转让给自己的朋友，用于在那些同意使用比特币支付啤酒钱的当地酒吧结账时，他们可以使用移动钱包。

多种钱包，以移动应用的形式出现于手机软件商店，然而它们在技术层面并非真正的移动钱包。它们属于网络钱包，只是通过移动应用便可以访问。二者之间的

区别在于何人存储个人密匙。假如由第三方存储个人密匙并且钱包通过互联网即可获取此等信息，那么它便是网络钱包，即便以移动应用的形式出现[35]。假如个人密匙存储于智能手机上，那么该移动应用便是移动钱包。移动钱包包括 Airbitz 和 Breadwallet。

硬件钱包

随着比特币越来越受欢迎且应用率不断增加，一些公司不断出现，制作专门存储个人密匙的硬件，因此这些硬件可以存储比特币或加密资产，然后将它们发送给其他人。多种硬件钱包提供了五花八门的功能。一些硬件钱包提供密匙生成、存储和发送等功能为一体的完整套餐。有些硬件钱包则仅仅用于确认交易安全性的额外一层。有些硬件钱包在运作时，需要接入计算机。一些广受欢迎的硬件钱包包括[36]：

- Trezor：它在存储比特币时更加安全，因为由它生成的个人密匙绝不会离开此设备。由于它的存在，那么影响其它设备或在线存储的病毒和恶意软件不会盗取其数据。
- Ledger Nano S.此设备需插入一个 USB 接口，可用于存储比特币、以太和其它替代币。它上面安装了一个简洁的 OLED 显示屏，外形如同一个闪存盘，当设备上发生交易时，可提供验证服务。
- KeepKey.此种 USB 设备不仅可以安全地存储比特币，而且其 OLED 显示器上显示交易信息和确认信息。

虽然用户可能将硬件钱包放错地方，然而这并非一定意味着加密资产的损失。在设置硬件钱包的初始化阶段，将生成一个“种子”，如同备份密码。用户必须将此种子存放于极其安全的地方，因为假如硬件钱包丢失，那么种子将重新生成原本存放于硬件钱包上的个人密匙，进而允许用户再次获取比特币。

由于硬件钱包要求具体的硬件工程和相关的软件工程，因此它们往往无法支持各种类型的加密资产。大多数硬件钱包均支持比特币。Ledger Nano S 支持比特币之外的某些加密资产。KeepKey 如今与 ShapeShift 融合，不仅支持比特币，还支持另外的加密资产[37]。随着更多的硬件钱包不断提高其能力以支持多种加密资产，在未来几年间，我们必将见证此领域的不断扩展。

纸钱包

如果方法得当，那么存储个人密匙的一个最简单方法也最安全。欢迎您了解纸钱包，即将长字母数字串（即公私钥匙对）写在一张纸上。纸钱包等同于一种冷存储。它可以安全地锁在保险箱里长达数十年，只要世界上尚且存在某类资产的区块链，那么用户仍旧可以通过个人密匙获取加密资产。纸钱包支持所有类型的加密资产，因为它只需要一张纸和一支笔。许多客户将此等纸钱包存放于安全位置的防火保险箱中。

多种选择，同一种纪律

至于所有这些可行选项，投资者根据自己需求选择钱包和交易所时，必须小心谨慎，这一点十分重要。基本过程包括“如何获取”和“如何存储”加密资产。虽然同一服务商可提供这两种功能，然而消费者在做出决定之前，仍需考虑哪些最重要。正如同投资者需慢慢地思考应该雇佣哪一名财务顾问，创新型投资者必须仔细调查应该采用哪一家加密资产“获取方和存储方”。

我们承认加密资产领域需要新的习惯模式，这个过程往往令人不安，尤其是当钱（任意形式的钱，包括电子货币或纸币）处于风险之中时。随着加密资产的关注度和市场不断扩张，无需新习惯模式的选项将逐渐成型，因为它们将把加密资产融入投资者熟悉的投资系统和投资工具之中。我们正见证货币经理人、投资公司和其它资本市场选手不断地加入此领域，调查和开发一些符合资本市场资产且可存放于经纪账户(甚至于美国 401（K）计划)的投资工具。

在下一章节，我们将探究一些数量不断增加且可供投资者使用的资本市场投资选项。这包括尽职调查、纪律和研究，但是也包括消除个人密匙存储中令人惧怕的部分以及在创业公司开设新账户等。