11.1 安全准则

比特币的核心准则是去中心化，这一点对安全性具有重要意义。在中心化的模式下，例如传统的银行或支付网络，需要依赖于访问控制和审查制度将不良行为者拒之门外。相比之下，比特币这样的去中心化系统则将责任和控制权都移交给了用户。由于网络的安全性是基于工作量证明而非访问控制，比特币网络可以对所有人开放，也无需对比特币传输进行加密。

在一个传统的支付网络中，例如信用卡系统，支付是终端开放式的，因为它包含了用户的个人标识（信用卡号）。在初次支付后，任何能获得该标识的人都可以从所有者那里反复“提取”资金。因此，该支付网络必须采取端对端加密的方式，以确保没有窃听者或中间人可以在资金流通或存储过程中将交易数据截获。如果坏人获得该系统的控制权，他将能 破获当前的的交易和支付令牌，他还可以随意动用这笔资金。更糟的是，当客户数据被泄露时，顾客的个人身份信息将被盗窃者们一览无余。客户这时必须立即采取措施，以防失窃帐户被盗窃者用于欺诈。

比特币则截然不同，一笔比特币交易只授权向指定接收方发送一个指定数额，并且不能被修改或伪造。它不会透露任何 个人信息，例如当事人的身份，也不能用于权限外的支付。因此，比特币的支付网络并不需要加密或防窃听保护。事实 上，你可以在任何公开的网络上广播比特币交易的数据，例如在不安全的WIFI或蓝牙网络上公开传播比特币交易的数 据，这对安全性没有任何影响。

比特币的去中心化安全模型很大程度上将权力移交到用户手上，随之而来的是用户们保管好密钥的责任。这对于大多数 用户来说并非一件易事，特别是在像智能手机或笔记本电脑这种能能时刻联网的通用设备上。虽然比特币的去中心化模 型避免了常见的信用卡盗用等情况，但很多用户由于无法保管好密钥从而被黑客攻击。

11.1.1 比特币系统安全开发

对于比特币开发者而言最重要的是去中心化原则。大多数开发者对中心化的安全模型很熟悉，并可能试图将中心化的模 型运用到借鉴比特币的应用中去去，这将给比特币带来灭顶之灾。

比特币的安全性依赖于密钥的分散性控制，并且需要矿工们各自独立地进行交易验证。如果你想利用好比特币的安全 性，你需要确保自己处于比特币的安全模型里。简而言之，不要将用户的密钥控制权拿走，不要接受非区块链交易信息。

例如，许多早期的比特币交易所将所有用户的资金集中在一个包含着私钥的“热钱包”里，并存放在服务器上。这样的设计夺取了用户的掌控权，并将密钥集中到单个系统里。很多这样的系统都被黑客攻破了，并给客户带来灾难性后果。 另一个常见的错误是接受区块链离线交易，妄图减少交易费或加速交易处理速度。一个“区块链离线交易”系统将交易数据记录在一个内部的中心化账本上，然后偶尔将它们同步到比特币区块链中。这种做法，再一次，用专制和集中的方式取 代比特币的去中心化安全模型。当数据处于离线的区块链上的时候，保护不当的中心化账本里的资金可能会不知不觉被伪造、被挪用、被消耗。

除非你是准备大力投资运营安全，叠加多层访问控制，或（像传统的银行那样）加强审计，否则在将资金从比特币的去中心化安全场景中抽离出来之前，你应该慎重考虑一番。即使你有足够的资金和纪律去实现一个可靠的安全模型，这样的设计也仅仅是复制了一个脆弱不堪，深受账户盗窃威胁、贪污和挪用公款困扰的传统金融网络而已。要想充分利用比特币特有的去中心化安全模型，你必须避免中心化架构的常见诱惑，因它最终将摧毁比特币的安全性。

11.1.2 信任根

传统的安全体系基于一个称为信任根（ROOT OF TRUST）的概念，它指的总体系统或应用程序中一个可信赖的安全核心。安全体系像一圈同心圆一样围绕着信任根源来进行开发，像层层包裹的洋葱一样，信任从内至外依次延伸。每一层都构建于更可信的内层之上，通过访问控制，数字签名，加密和其他安全方式确保可信。随着软件系统变得越来越复杂，它们更可能出现问题，安全更容易受到威胁。其结果是，软件系统变得越复杂，就越难维护安全性。信任根的概念确保绝大多数的信任被置于一个不是过于复杂系统的一部分，因此该系统的这部分也相对坚固，而更复杂的软件则在它之上构建。这样的安全体系随着规模扩大而不断重复出现，首先信任根建立于单个系统的硬件内，然后将该信任根通过操作系统扩展到更高级别的系统服务，最后逐次扩散到圈内多台服务器上。

比特币的安全体系与这不同。在比特币里，共识系统创建了一个可信的完全去中心化的公开账本，一个正确验证过的区块使用创世区块 作为信任根，建立一条至当前区块的可信任链。比特币系统可以使用区块链作为它们的信任根。在设计一个多系统服务机制的比特币应用时，你应该仔细确认安全体系，以确保对它的信任能有据可依。最终， 唯一可确信无疑的是一条完全有效的区块链。如果你的应用程序或明或暗地信赖于区块链以外的东西，就该引起重视， 因为它可能会引入漏洞。一个不错的方法评估你应用程序的安全体系：单独考量每个组件，设想该组件被完全攻破并被坏人掌控的场景。依次取出应用程序的每个组件，并评估它被攻破时对整体安全的影响。如果你的应用程序的安全性在该组件沦陷后大打折扣，那就说明你已经对这些组件过度信任了。一个没有漏洞的比特币应用程序应该只受限于比特币的共识机制，这意味着其安全体系的信任源于比特币最底层的部分。

无数个黑客攻击比特币交易所的例子都是因为轻视了这一点，他们的安全体系和设计甚至无法通过基本的审查。这种中心化的实现方式将信任置于比特币区块链之外的诸多组件之上，例如热钱包，中心化的账本数据库，简易加密的密钥，以及许多类似的方案。

11.2 用户最佳安全实践

人类使用物理的安全控制已经有数千年之久。相比之下，我们的数字化安全经验的年纪还不满50岁。现代通用的操作系统并不是十分安全，亦不特别适合用来存储数字货币。我们的电脑通过一直连接的互联网长时间暴露在外，它们运行着成千上万第三方软件组件，这些软件往往可以不受约束地访问用户的文件。你电脑上安装的众多软件只要有一个恶意软件，就会威胁到你的文件，可窃取你钱包里的所有比特币。想要杜绝病毒和木马对电脑的威胁，用户要达到一定的计算机维护水平，只有小部分人能做到。

尽管信息安全经过了数十年的研究和发展，数字资产在绵延不绝的攻势下还是十分脆弱。纵使是像金融服务公司，情报机构或国防承包商这样拥有高度防护和限制的系统，也经常会被攻破。比特币创造了具有内在价值的数字资产，它可以 被窃取，并立即转移给他人而无法撤回。这让黑客有了强烈的作案动机。至今为止，黑客都不得不在套现后更换身份信 息或帐户口令，例如信用卡或银行账户。尽管掩饰和洗白这部分财务信息的难度不小，但越来越多的窃贼从于此道。而 比特币使这个问题加剧了，因为它不需要掩饰或洗白，它本身就是具有内在价值的数字资产。

幸运的是，比特币也有着激励机制，以提高计算机的安全性。如前所述，计算机受威胁的风险是模糊的，间接的，而比 特币让这些风险变得明确清晰。在电脑上保存比特币让用户时刻注意他们需要提高计算机的安全性，结果便是这使得比 特币和其它数字货币得以传播和扩散，我们已经看到在黑客技术和安全解决方案双方的提升。简单来说，黑客现在有着一个非常诱人的目标，而用户也有明确的激励性去保卫自己。 在过去的三年里，随着比特币不断被接纳，一个直接的结果是，我们已经看到信息安全领域取得了巨大创新，例如硬件 加密，密钥存储和硬件钱包，多重签名技术和数字托管。在下面的章节中，我们将研究各种实际用户安全中的实践经验。

11.2.1 比特币物理存储

相比数字信息的安全，大多数用户对物理安全更加熟悉，一个非常有效保护比特币的方法是，将它们转换为物理形式。 比特币密钥不过是串长数字而已。这意味着它们可以以物理形式存储起来，如印在纸上或蚀刻成金属硬币上。这样保护密钥就变成了简单地保护印着比特币密钥的物理实体。一组打印在纸上的比特币密钥被称为“纸钱包”，有许多可以用来创建它们的免费工具。我个人将大部分（99%以上）的比特币存储在纸钱包上，并用BIP0038加密，复制了多份并锁在保险箱里。将比特币离线保存的方法被称为冷存储，它是最有效的安全技术之一。冷存储系统是在一个离线系统（一个从来没有连接过互联网的系统）上生成密钥，并离线存储到纸上或者U盘等电子媒介上。

11.2.2 硬件钱包

从长远来看，比特币安全将越来越多地以硬件防篡改钱包的形式出现。与智能手机或台式电脑不同，一个比特币硬件钱包只有一个目的，安全地存储比特币。不像容易受害的常用软件那样，硬件钱包只提供了有限的接口，从而可以给非专业用户提供近乎万无一失的安全等级。我预期将看到硬件钱包成为比特币储存的主要方式。要想看硬件钱包的实例，请 查阅TREZOR。

11.2.3 平衡风险

虽然大多数用户都非常关注比特币防盗，其实还有一个更大的风险存在。数据文件丢失的情况时有发生。如果比特币的数据也在其中，损失将会让人痛苦不堪。为了保护好比特币钱包，用户必须非常注意不要剑走偏锋，这样不至于会搞丢比特币。在2011年7月，一个著名的比特币认知教育项目损失了近7,000枚比特币。为了防止被盗窃，其主人曾之前采取了一系列复杂的操作去加密备份。结果他们不慎丢失了加密的密钥，使得备份变得毫无价值，白白失去了一大笔财富。如果你保护比特币的方式太过了，这好比于把钱藏在沙漠里，你可能不能再把它找回来了。

11.2.4 分散风险

你会将你的全部家当换成现金放在钱包里随身携带么？大多数人会认为这非常不明智，但比特币用户经常会将所有的比特币放在一个钱包里。用户应该将风险分散到不同类型的比特币钱包。审慎的用户应该只留一小部分（或许低于5%） 的比特币在一个在线的或手机钱包，就像零用钱一样，其余的部分应该采用不同存储机制分散开来，诸如电脑钱包和离线（冷存储）钱包。

11.2.5 多重签名管理

当一个公司或个人持有大量比特币时，他们应该考虑采用多重签名的比特币地址。多重签名比特币地址需要多个签名才能支付，从而保证资金的安全。多重签名的密钥应存储在多个不同的地方，并由不同的人掌控。打个比方，在企业环境中，密钥应该分别生成并由若干公司管理人员持有，以确保没有任何一个人可以独自占有资金。多重签名的地址也可以提供冗余，例如一个人持有多个密钥，并将它们分别存储在不同的地方。

11.2.6 存活能力

一个非常重要却又常常被忽视的安全性考虑是可用性，尤其是在密钥持有者丧失工作能力或死亡的情况下。比特币的用户被告知应该使用复杂的密码，并保证他们的密钥安全且不为他人所知。不幸的是，这种做法使得在用户无法解锁时， 用户的家人几乎无法将该财产恢复。事实上，比特币用户的家人可能完全不知道这笔比特币资金的存在。如果你有很多的比特币，你应该考虑与一个值得信赖的亲属或律师分享解密的细节。可以搞一个更复杂的比特币恢复 计划，可以通过设置多重签名，做好遗产规划，并通过专门的“数字资产执行者”律师处理后事。

11.3 总结

比特币是一项全新的，前所未有的，复杂的技术。随着时间的推移，我们将开发出更好的安全工具，而且更容易被非专业人士使用/的做法/去掉。而现在，比特币用户可以使用许多这里所讨论的技巧，享受安全而无困扰的比特币生活。