11比特币安全

Securing bitcoin is challenging because bitcoin is not an abstract reference to value, like a balance in a bank account. Bitcoin is very much like digital cash or gold. You've probably heard the expression, "Possession is nine-tenths of the law." Well, in bitcoin, possession is ten-tenths of the law. Possession of the keys to unlock the bitcoin is equivalent to possession of cash or a chunk of precious metal. You can lose it, misplace it, have it stolen, or accidentally give the wrong amount to someone. In every one of these cases, users have no recourse, just as if they dropped cash on a public sidewalk.
保证比特币的安全是很有挑战性的事，因为比特币不像银行账户余额那样是价值的一个抽象引用。
比特币非常像数字现金或黄金。你可能听过这样的说法：占有是法律的9/10。
在比特币中，占有是法律的9/10。持有解锁比特币的密钥就等于持有现金或贵金属一样。
你可能会将密钥丢失、放错地方、被盗或不小心错支了数额。
无论是哪种情况，用户都没有办法撤回，因为这就像将现金丢在了车水马龙的大街上一样。

However, bitcoin has capabilities that cash, gold, and bank accounts do not. A bitcoin wallet, containing your keys, can be backed up like any file. It can be stored in multiple copies, even printed on paper for hard-copy backup. You can't "back up" cash, gold, or bank accounts. Bitcoin is different enough from anything that has come before that we need to think about bitcoin security in a novel way too.
不过，与现金、黄金或银行账户相比，比特币具有它们没有的能力。
比特币钱包中包含你的密钥，可以像任何文件一样备份。可以保存多个备份，甚至打印在纸上。
你不能备份现金、黄金或银行账号。
比特币与至今为止的其它东西都如此不同，以致于我们也需要以一种新的方式来思考比特币的安全性。

11.1 安全原则

The core principle in bitcoin is decentralization and it has important implications for security. A centralized model, such as a traditional bank or payment network, depends on access control and vetting to keep bad actors out of the system. By comparison, a decentralized system like bitcoin pushes the responsibility and control to the users. Because security of the network is based on Proof-of-Work, not access control, the network can be open and no encryption is required for bitcoin traffic.
比特币的核心原则是**"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，需要依赖访问控制和审查制度将不良行为者拒之门外。
相比之下，去中心化系统则将责任和控制权都交给了用户。
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，也无需对比特币流量进行加密。

On a traditional payment network, such as a credit card system, the payment is open-ended because it contains the user's private identifier (the credit card number). After the initial charge, anyone with access to the identifier can "pull" funds and charge the owner again and again. Thus, the payment network has to be secured end-to-end with encryption and must ensure that no eavesdroppers or intermediaries can compromise the payment traffic, in transit or when it is stored (at rest). If a bad actor gains access to the system, he can compromise current transactions *and* payment tokens that can be used to create new transactions. Worse, when customer data is compromised, the customers are exposed to identity theft and must take action to prevent fraudulent use of the compromised accounts.
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对盗窃者一览无余。
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。

Bitcoin is dramatically different. A bitcoin transaction authorizes only a specific value to a specific recipient and cannot be forged or modified. It does not reveal any private information, such as the identities of the parties, and cannot be used to authorize additional payments. Therefore, a bitcoin payment network does not need to be encrypted or protected from eavesdropping. In fact, you can broadcast bitcoin transactions over an open public channel, such as unsecured WiFi or Bluetooth, with no loss of security.
比特币则截然不同，一个比特币交易只授权向指定收款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。

Bitcoin’s decentralized security model puts a lot of power in the hands of the users. With that power comes responsibility for maintaining the secrecy of the keys. For most users that is not easy to do, especially on general-purpose computing devices such as internet-connected smartphones or laptops. Although bitcoin’s decentralized model prevents the type of mass compromise seen with credit cards, many users are not able to adequately secure their keys and get hacked, one by one.
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 安全地开发比特币系统

The most important principle for bitcoin developers is decentralization. Most developers will be familiar with centralized security models and might be tempted to apply these models to their bitcoin applications, with disastrous results.
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比特币应用中去，这将带来灭顶之灾。

Bitcoin’s security relies on decentralized control over keys and on independent transaction validation by miners. If you want to leverage bitcoin’s security, you need to ensure that you remain within the bitcoin security model. In simple terms: don’t take control of keys away from users and don’t take transactions off the blockchain.
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，不要从用户手中拿走密钥控制权，不要把交易转移到链下。

For example, many early bitcoin exchanges concentrated all user funds in a single "hot" wallet with keys stored on a single server. Such a design removes control from users and centralizes control over keys in a single system. Many such systems have been hacked, with disastrous consequences for their customers.
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。这样的设计拿走了用户的掌控权，并将密钥集中到一个系统里。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。

Another common mistake is to take transactions "off blockchain" in a misguided effort to reduce transaction fees or accelerate transaction processing. An "off blockchain" system will record transactions on an internal, centralized ledger and only occasionally synchronize them to the bitcoin blockchain. This practice, again, substitutes decentralized bitcoin security with a proprietary and centralized approach. When transactions are off blockchain, improperly secured centralized ledgers can be falsified, diverting funds and depleting reserves, unnoticed.
另一个常见的错误是接受区块链离线交易，试图减少交易费或加速交易处理速度。
一个区块链下系统把交易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，用集中方式取代比特币的去中心化安全模型。
当数据处于链下时，保护不当的中心化账本里的资金可能会不知不觉被伪造、挪用、消耗。

Unless you are prepared to invest heavily in operational security, multiple layers of access control, and audits (as the traditional banks do) you should think very carefully before taking funds outside of bitcoin's decentralized security context. Even if you have the funds and discipline to implement a robust security model, such a design merely replicates the fragile model of traditional financial networks, plagued by identity theft, corruption, and embezzlement. To take advantage of bitcoin's unique decentralized security model, you have to avoid the temptation of centralized architectures that might feel familiar but ultimately subvert bitcoin's security.
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，因为它最终将摧毁比特币的安全性。

11.1.2 信任的根

Traditional security architecture is based upon a concept called the *root of trust*, which is a trusted core used as the foundation for the security of the overall system or application. Security architecture is developed around the root of trust as a series of concentric circles, like layers in an onion, extending trust outward from the center. Each layer builds upon the more-trusted inner layer using access controls, digital signatures, encryption, and other security primitives. As software systems become more complex, they are more likely to contain bugs, which make them vulnerable to security compromise. As a result, the more complex a software system becomes, the harder it is to secure.
传统的安全体系是基于一个概念，称为“信任根”（root of turst），它是一个可信任的核心，是整个系统或应用的安全的基础。
安全体系是围绕信任根发展起来的，就像一系列同心圆，把信任从中心扩展到外围。
每一层都构建在更可信的内层之上，方法是使用：访问控制、数字签名、加密、其它安全原语。
随着软件系统变得日益复杂，它们更可能包含bug，这导致它们更容易受到安全威胁。
结果是，软件系统越复杂，就越难保证它的安全。

The root of trust concept ensures that most of the trust is placed within the least complex part of the system, and therefore least vulnerable, parts of the system, while more complex software is layered around it. This security architecture is repeated at different scales, first establishing a root of trust within the hardware of a single system, then extending that root of trust through the operating system to higher-level system services, and finally across many servers layered in concentric circles of diminishing trust.
信任根的概念保证了多数信任放置在系统的更简单部分，因此该系统的这部分也相对坚固，而更复杂的软件放在它之上。
这个安全体系在不同的规模上不断重复，首先在系统的硬件上建立一个信任根，然后把信任根从操作系统扩展到更高级的系统服务，最后，在许多服务器上层同心圆的信任减少。

Bitcoin security architecture is different. In bitcoin, the consensus system creates a trusted public ledger that is completely decentralized. A correctly validated blockchain uses the genesis block as the root of trust, building a chain of trust up to the current block. Bitcoin systems can and should use the blockchain as their root of trust.
比特币的安全体系不是这样。
在比特币中，共识系统创建了一个可信的公共账本，它是完全去中心化的。
一个正确验证过的区块链使用创世区块作为信任根，建立一条到当前区块的信任链。
比特币系统可以并应该使用这个区块链作为它们的信任根。

When designing a complex bitcoin application that consists of services on many different systems, you should carefully examine the security architecture in order to ascertain where trust is being placed. Ultimately, the only thing that should be explicitly trusted is a fully validated blockchain. If your application explicitly or implicitly vests trust in anything but the blockchain, that should be a source of concern because it introduces vulnerability.
在设计一个复杂的比特币应用（它由许多不同系统上的服务构成）时，你应该仔细检查这个安全体系，以确认对信任放在哪里。
最终，唯一可以明确信任的是一条完全有效的区块链。
如果你的应用或明或暗地把信任放在别的地方，而不是放在区块链上，就应该引起重视，因为它可能会引入漏洞。

A good method to evaluate the security architecture of your application is to consider each individual component and evaluate a hypothetical scenario where that component is completely compromised and under the control of a malicious actor. Take each component of your application, in turn, and assess the impacts on the overall security if that component is compromised. If your application is no longer secure when components are compromised, that shows you have misplaced trust in those components. A bitcoin application without vulnerabilities should be vulnerable only to a compromise of the bitcoin consensus mechanism, meaning that its root of trust is based on the strongest part of the bitcoin security architecture.
评价应用的安全体系的好方法是，考虑每个组件，并评价一个假设场景：这个组件被攻破，处于攻击者的控制之下。
依次取出应用中的每个组件，并评估它被攻破时对整体安全的影响。
如果应用的安全性在该组件沦陷后大打折扣，那就说明你对这些组件过度信任了。
一个没有漏洞的比特币应用应该只受限于对比特币共识机制的攻击，这意味着，它的信任根是基于比特币最强健的部分。

The numerous examples of hacked bitcoin exchanges serve to underscore this point because their security architecture and design fails even under the most casual scrutiny. These centralized implementations had invested trust explicitly in numerous components outside the bitcoin blockchain, such as hot wallets, centralized ledger databases, vulnerable encryption keys, and similar schemes.
无数被黑客攻破比特币交易所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。
这些中心化实现将信任置于比特币区块链之外的许多组件上，例如热钱包、中心化的账本数据库、易受攻击的加密密钥，以及类似方案。

11.2用户安全最佳实践

Humans have used physical security controls for thousands of years. By comparison, our experience with digital security is less than 50 years old. Modern general-purpose operating systems are not very secure and not particularly suited to storing digital money. Our computers are constantly exposed to external threats via always-on internet connections. They run thousands of software components from hundreds of authors, often with unconstrained access to the user's files. A single piece of rogue software, among the many thousands installed on your computer, can compromise your keyboard and files, stealing any bitcoin stored in wallet applications. The level of computer maintenance required to keep a computer virus-free and trojan-free is beyond the skill level of all but a tiny minority of computer users.
人类使用物理安全控制已经有数千年的历史。
相比之下，我们在数字安全上的经验不到50。
现代通用操作系统不是十分安全，并不特别适合存储数字货币。
我们的计算机因为总是连接互联网，所以不断暴漏与外部威胁之下。
它们运行成千上万的软件组件，这些组件由成百上千的人编写，这些软件经常不受约束地访问用户文件。
计算机上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计算机的威胁，用户要达到一定的计算机维护水平，但只有很少的人能做到。

Despite decades of research and advancements in information security, digital assets are still woefully vulnerable to a determined adversary. Even the most highly protected and restricted systems, in financial services companies, intelligence agencies, and defense contractors, are frequently breached. Bitcoin creates digital assets that have intrinsic value and can be stolen and diverted to new owners instantly and irrevocably. This creates a massive incentive for hackers. Until now, hackers had to convert identity information or account tokens—such as credit cards and bank accounts—into value after compromising them. Despite the difficulty of fencing and laundering financial information, we have seen ever-escalating thefts. Bitcoin escalates this problem because it doesn't need to be fenced or laundered; it is intrinsic value within a digital asset.
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。
迄今为止，黑客在得手之后，都不得不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。

Fortunately, bitcoin also creates the incentives to improve computer security. Whereas previously the risk of computer compromise was vague and indirect, bitcoin makes these risks clear and obvious. Holding bitcoin on a computer serves to focus the user's mind on the need for improved computer security. As a direct result of the proliferation and increased adoption of bitcoin and other digital currencies, we have seen an escalation in both hacking techniques and security solutions. In simple terms, hackers now have a very juicy target and users have a clear incentive to defend themselves.
幸运的是，比特币也有着激励机制，以提高计算机的安全性。
前面所说的计算机受威胁的风险是模糊和间接的，而比特币让这些风险变得明确清晰。
在计算机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，我们已经看到黑客技术和安全方案双方的提升。
简单来说，黑客现在有一个非常诱人的目标，而用户也有明确的激励去保护自己。

Over the past three years, as a direct result of bitcoin adoption, we have seen tremendous innovation in the realm of information security in the form of hardware encryption, key storage and hardware wallets, multisignature technology, and digital escrow. In the following sections we will examine various best practices for practical user security.

在过去三年里，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、多签名技术和数字托管。
在下面的小节中，我们看看对实际用户安全来说的各种最佳实践。

11.2.1 物理的比特币存储

Because most users are far more comfortable with physical security than information security, a very effective method for protecting bitcoin is to convert them into physical form. Bitcoin keys are nothing more than long numbers. This means that they can be stored in a physical form, such as printed on paper or etched on a metal coin. Securing the keys then becomes as simple as physically securing the printed copy of the bitcoin keys.
相比信息安全，多数用户更熟悉物理安全，保护比特币的一个非常有效的方法是：把它们转换为物理形式。

比特币密钥不过是一长串数字而已。这意味着，它们可以以物理形式存储起来，如印在纸上或金属硬币上。这样，保护密钥就变成了简单地保护物理实体。

A set of bitcoin keys that is printed on paper is called a "paper wallet," and there are many free tools that can be used to create them. I personally keep the vast majority of my bitcoin (99% or more) stored on paper wallets, encrypted with BIP-38, with multiple copies locked in safes. Keeping bitcoin offline is called *cold storage* and it is one of the most effective security techniques. A cold storage system is one where the keys are generated on an offline system (one never connected to the internet) and stored offline either on paper or on digital media, such as a USB memory stick.
打印在纸上的一组比特币密钥被称为“纸钱包”，有许多可以用来创建纸钱包的免费工具。
我个人将大部分的比特币存储在纸钱包上，并用BIP-38加密，复制了多份放在保险箱里。
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（没有连接过互联网）上生成密钥，并离线存储到纸上或U盘等电子媒介上。

11.2.2 硬件钱包

In the long term, bitcoin security increasingly will take the form of hardware tamper-proof wallets. Unlike a smartphone or desktop computer, a bitcoin hardware wallet has just one purpose: to hold bitcoin securely. Without general-purpose software to compromise and with limited interfaces, hardware wallets can deliver an almost foolproof level of security to nonexpert users. I expect to see hardware wallets become the predominant method of bitcoin storage. For an example of such a hardware wallet, see the Trezor.
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。
与手机或计算机不同，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。我预期硬件钱包将成为比特币储存的主要方式。
要想看硬件钱包的实例，可以看看Trezor。

11.2.3 平衡风险

Although most users are rightly concerned about bitcoin theft, there is an even bigger risk. Data files get lost all the time. If they contain bitcoin, the loss is much more painful. In the effort to secure their bitcoin wallets, users must be very careful not to go too far and end up losing the bitcoin.
虽然大多数用户都非常关注比特币防盗，其实还存在一个更大的风险。
数据文件丢失的情况时有发生。如果丢失的文件包含比特币，损失将会让人痛不欲生。

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。

In July 2011, a well-known bitcoin awareness and education project lost almost 7,000 bitcoin. In their effort to prevent theft, the owners had implemented a complex series of encrypted backups. In the end they accidentally lost the encryption keys, making the backups worthless and losing a fortune. Like hiding money by burying it in the desert, if you secure your bitcoin too well you might not be able to find it again.
2011年7月，一个著名的比特币认知教育项目损失了近7000个比特币。
为了防止被盗，主人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，就好比于把钱藏在沙漠里，你可能都找不回来了。

11.2.4 分散风险

Would you carry your entire net worth in cash in your wallet? Most people would consider that reckless, yet bitcoin users often keep all their bitcoin in a single wallet. Instead, users should spread the risk among multiple and diverse bitcoin wallets. Prudent users will keep only a small fraction, perhaps less than 5%, of their bitcoin in an online or mobile wallet as "pocket change." The rest should be split between a few different storage mechanisms, such as a desktop wallet and offline (cold storage).
你会将全部财产放在钱包里随身携带么?
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比特币在一个在线的或手机钱包里，就像零用钱一样，其余的应该采用不同存储机制分散开来，例如计算机钱包和离线（冷存储）钱包。

11.2.5 多签名管理

Whenever a company or individual stores large amounts of bitcoin, they should consider using a multisignature bitcoin address. Multisignature addresses secure funds by requiring more than one signature to make a payment. The signing keys should be stored in a number of different locations and under the control of different people.
当公司或个人持有大量比特币时，他们应该考虑采用多签名的比特币地址。
多签名比特币地址需要多个签名才能花费，从而保证资金的安全。
多签名的密钥应存储在多个不同的地方，并由不同的人掌控。

In a corporate environment, for example, the keys should be generated independently and held by several company executives, to ensure no single person can compromise the funds. Multisignature addresses can also offer redundancy, where a single person holds several keys that are stored in different locations.
例如，在企业中，密钥应该独立生成，由多个公司管理人员持有，以确保没有个人可以独自花费资金。
多签名的地址也可以提供冗余，例如一个人持有多个密钥，并将这些密钥分别存储在不同的地方。

11.2.6 存活能力

One important security consideration that is often overlooked is availability, especially in the context of incapacity or death of the key holder. Bitcoin users are told to use complex passwords and keep their keys secure and private, not sharing them with anyone. Unfortunately, that practice makes it almost impossible for the user’s family to recover any funds if the user is not available to unlock them. In most cases, in fact, the families of bitcoin users might be completely unaware of the existence of the bitcoin funds.

一个非常重要，却又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能力或死亡时。
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，这种做法使得除了用户自己，用户的家人几乎也无法获得财产。
事实上，比特币用户的家人可能完全不知道这些比特币资金的存在。

If you have a lot of bitcoin, you should consider sharing access details with a trusted relative or lawyer. A more complex survivability scheme can be set up with multi-signature access and estate planning through a lawyer specialized as a "digital asset executor."
如果你有很多比特币，你应该考虑向一个值得信赖的亲属或律师提供解密的细节。
可以设置一个更复杂的比特币恢复计划，它使用多签名，并有通过律师（数字资产执行人）的遗产规划。

11.3结论

Bitcoin is a completely new, unprecedented, and complex technology. Over time we will develop better security tools and practices that are easier to use by nonexperts. For now, bitcoin users can use many of the tips discussed here to enjoy a secure and trouble-free bitcoin experience.
比特币是一个全新的、前所未有的、复杂的技术。
随着时间的推移，我们会开发出更好的安全工具和实践，能够更容易被非专业人士使用。
而现在，比特币用户可以使用这里讨论的许多技巧，体验安全无忧的比特币。