上周五，日本东京数字货币交易所Coincheck遭遇了数字货币领域有史以来最大虚拟货币失窃案，损了价值约480亿日元NEM币，折合人民币约33.7亿元。因为涉及金额巨大，再一次引起了人们对于以区块链技术为代表的数字货币安全性的担忧。

其实近年来，随着数字货币的高速发展，以比特币为代表的数字货币始终面临着诸多安全、隐私和监管问题。随着数字货币越来越多被各国人们接受、玩家愈发增多、大规模发行与交易行为频发，它的安全性显得愈发重要。

数字货币的安全指什么？

简单来说，数字货币的安全主要指下面几个维度的安全。

首先是算法安全。当前区块链或者数字货币技术中使用到的哈希算法和数字签字的算法，都是应对的传统攻击模型。目前的底层算法是否安全是算法安全的核心问题。比方说MD5和SHA-1算法，哈希函数算法MD5与美国标准技术局颁布的算法SHA-1，居于国际应用范围最广的重要算法之列，然而目前这两个算法却被证明有重大安全漏洞，之前却一直被认为是安全的哈希函数算法。目前流行的数字货币设计的一些关键密码算法尚未得到足够理论分析和检验。由于这些系统承载了虚拟数字资产，底层算法的潜在问题一旦暴露，会对资产安全构造严重威胁。与此同时，大量的安全算法在量子计算下已经不再安全了。区块链技术采用非对称加密算法保障数据库的可信赖性，使用户在互联网无实名制的背景下防止诈骗，但随着量子计算的不断突破，其计算机能力的大幅跃升将使得许多加密算法变得相当脆弱。

对于算法安全来说，当前很迫切的问题是要随时做好用抗量子密码算法来代替当前的传统算法的准备。

其次是协议安全。安全协议是建立在密码体制基础上的一种交互通信协议，它运用密码算法和协议逻辑来实现认证和密钥分配等目标。协议安全的核心问题就是，现在数字货币所设计的协议能否通过理论的验证。

目前数字货币的安全现状是，当前所有协议都没有详细的形式化证明，安全模型定义与实际应用之间的差别较大。

然后是实现安全。实现安全的问题主要是算法是否存在安全漏洞。国家互联网应急中心在代码层面发现相关开源软件的高危漏洞和安全隐患非常多，这也给当前的数字货币和区块链技术带来了一些挑战。其实，比特币早在2009年就进行了开源项目，一经开放吸引了无数的热情志愿者和核心开发者的参与。目前，在开源平台Github的网站上，我们可以看到如“Chain”等公司的专属区块链和分布式总账的源代码。这些公司希望，通过将加密技术的源代码进行开放，可以让更多的人在其软件

上增加应用或是建立专属网络。但这也意味着，如果这些源代码出现漏洞，相关的应用也会出现安全问题。

最后是使用安全，使用安全的核心问题表现在数字货币资产的私钥安全问题。最明显的例子就是有人早期在低价时买进了一些比特币，在高价想把这些比特币兑现时，发现自己忘记私钥存在哪里了，或是，对私钥进行托管后，如托管、存储在数字平台交易所出现了丢失的情况。

当然，除了以上安全性问题，数字货币常见的还包含隐私问题（比如玩家在实体空间与区块链应用互动、使用私人密钥常常要在相关交易网站上用密码注册，或者是在更加安全的网站上进行多因素身份验证，而这就有可能出现其他人盗取密码或身份标记，然后使用私人密钥进行交易的风险）、监管问题（数字货币当前面临的一个重要问题就是监管的问题，比如比特币最早就是暗网丝绸之路上的交易货币，由于其可以隐藏身份，可使非法交易很难被追溯，当比特币的账户没办法被冻结时，交易也就没办法被制止。今年非常火的勒索病毒，也是采用比特币作为勒索的支付手段）等。

数字货币的安全性到底如何？

首先，我们不能一概去否认数字货币的安全性。以区块链技术为代表的数字货币拥有其独特的安全优势。主要在于以下三个方面：

1.利用高冗余的数据库保障信息的数据完整性

2.利用密码学的相关原理进行数据验证，保证不可篡改

3.在权限管理方面，运用了多私钥规则进行访问权限控制

利用区块链的安全优势，可以进行多重安全应用的开发，如认证和PKI。

但与此同时，数字货币毕竟具有交易属性，是一种可以实时转账到全球任何一个个人账户内的虚拟货币。由于数字货币币是一种P2P形式的货币，点对点的传输意味着一个去中心化的支付系统，因此这一货币的管理大多是基于软件以及约定俗成的网络协定来管控的，任何政府、银行、机构和个人都无法独自对其施加影响。随着全球数字货币交易量迎来了巨大提升，越来越多的国家开始承认数字货币的合法化。数字货币已然被全球黑客盯上，成为黑客盗取和勒索的首选对象，黑客常常以攻击手段攻击网络和计算机，要求支付数字货币作为赎金、或通过技术手段直接在交易平台盗取数字货币。

2014年8月，国内著名的山寨币交易所比特儿遭到攻击，被盗5000万个NXT（未来币）；2016年8月，来自香港的比特币交易平台Bitfinex遭受黑客攻击，该平台约有11.9756万个比特币从账户中被盗，损失价值约7000万美元；2017年7月，韩国最大比特币交易所遭黑客入侵，投资者一夜损失数十亿韩元……数字货币安全问题频发，广大参与者需要格外留意。

我们如何保障数字货币的安全？

在了解如何保障我们的数字货币安全之前，首先需要明确区块链的局限性，主要表现在三个方面：

首先是对共识机制的挑战。

对于区块链技术中的共识算法现在已经提出了多种共识机制，最常见的如PoW、PoS系统。但这些共识机制是否能实现并保障真正的安全，需要更严格的证明和时间的考验。

区块链中采用的非对称加密算法可能会随着数学、密码学和计算技术的发展而变的越来越脆弱。未来技术中对于非对称加密算法可能具有一定的破解性。其次，在比特币的机制下，私钥是存储在用户的本地终端中，如果用户的私钥被偷窃，依旧会对用户的资金造成严重损失。区块链技术上的私钥是否容易窃取的问题仍待进一步的探索与解决。

其次是所谓的“51%攻击”。

在比特币中，如果一个人控制节点中绝大多数的计算资源，他就能掌控整个比特网络并可以按照自己的意愿修改公有账本。这被称为51%攻击，一直是比特币系统中受到诟病的设计之一。

拥有整个网络51%算力的人可以做到以下这些事情：

1.他们可以不经过验证就阻止交易的发生，让交易变得无效，潜在地阻止人们交易货币。

2.他们在掌控网络的这段时间内也可能你想改变交易的双方，并且可能阻止其他的人寻找到新的区块。

在现实情况下，发起51%攻击是具有一定可行性，特别是随着矿池兴起的当下。尽管攻击者的潜在威胁并不大，我们也应该考虑到这种针对区块链系统的安全威胁的

存在并寻找解决策略。

最后是非区块链技术问题，也是我们最常遇到的问题。

以此次日本数字货币交易所被盗为代表，我们发现这些非区块链技术问题大多由以下两个原因导致：

1、黑客入侵官方人员账号，黑掉软件，将付款地址修改成黑客制定的地址；

2、获取用户地址、钱包交易密码，盗走其钱包货币。

随着行业的发展，各个国家及地方组织也加强了对区块链的潜能研究及对ICO的监管。作为ICO开发者，应努力维护好内部网络安全；作为ICO投资者，应加强对钱包的安全意识。

ICO投资者加强自身安全意识主要表现在：

1、记好钱包密码：自己千万别忘记这个密码，别人猜不出的，越有强度越复越好。

2、管理好自己机器上的安全软件：防止把钱包存到“云”上去。如果你的钱包没加密，而且还开着带云功能的杀毒防护软件的话，那你就会面临不断的信息盗取风险。

3、做好钱包的同步更新，经常备份钱包。

4、将短期不会卖的币转回钱包：防止交易平台塌陷，现在交易平台增长数量与山寨币的发数量成正比，如果囤币期不想套现，可以把大部分的币从平台提到钱包里来，自己捂着币，以后哪都能卖，这样也就不用担心交易平台问题了。

日本Coincheck的被盗不是第一次，也不会是最后一次，但这给我们提了个醒：数字货币特别是数字货币交易平台的安全性至关重要。从数字互联的角度出发，数字货币交易平台带来了数字产业的发展，也给比特币和其他数字货币的爱好者提供了一个平台，但这也同时在安全性方面也提出了更高的要求，只有做好数字货币交易平台的安全性，才能保证数字货币持续健康的发展。

本文源自投资界