进入加密货币世界的第一步是要有钱包和收款地址。加密钱包原则上是一个容器，可以生成一个虚拟货币收款地址，管理所有可用的货币。在进行任何交易时，用户也必须通过钱包进行操作。

在现实世界中，我们可以同时将美元、台币、日元等货币放入钱包，但在区块链，钱包生成的支付地址只能接受特殊类型的加密硬币。

一个钱包可以管理多组支付地址。但是比特币收款地址只能收比特币，以太币收款地址只能收以太币，不能在货币间通用。接收者必须给其他人正确类型的支付地址，以便转移加密货币的所有权。

大多数虚拟货币收款地址，是由字母数字字符组成的不合理字符串。为了方便软件阅读和记忆，很多时候付款地址会用二维码呈现。

至于加密货币钱包，款式相当多样化。消费者可以插上电脑、手机、网页甚至浏览器，在极短的时间内通过钱包软件创建相应币种的支付地址。

一般来说，加密货币钱包大致可以分为冷钱包和热钱包，两者都可以用来管理虚拟货币收款地址。。但冷钱包不会持续联网，减少了黑客偷钱的机会，所以安全性比热钱包好。

进一步明确冷钱包和热钱包的区别。首先，我们必须从&quot私钥&quot在区块链货币领域。

比特币核心是比特币的官方原生客户端，属于电脑上的热门钱包。虽然可以接收和转移加密货币，但是消耗大量硬盘容量和内存，不适合新手使用。

加密货币界有句话：&quot不是你的钥匙，不是你的硬币&quot，也就是说不管你选择使用哪个平台或者软件，只有用户手里有私钥才是掌握所有资产的关键。

如果没有私钥，用户可以&#039；不要在支付地址操作钱包或使用加密货币。私钥就像银行账户中ATM卡的密码一样。

据调查，在世界各地被挖出来的比特币中。，至少有20%是因为所有者&#039；的私钥丢失了，它就变成了一种没有人能存取、交易或继续流通的货币，只剩下一行数字能看但不能用。

▲ 没有私钥就掌握不了加密货币比如图中的比特币收款地址虽然有近8万个BTC，但是从来没有转出过，私钥可能早就不见了。

私钥是由计算机随机生成的随机数，包含大约五十个数字和大小写字母。没有固定的逻辑和规则。哪里有私钥，哪里就有公钥。两者是成对产生的，世界上只会有一个唯一的群体，不会重复。在虚拟货币的世界里，公钥会分散在网络上，而私钥只能由自己持有，所以私钥代表资产的所有权。拥有私钥的人有权使用钱包地址。

比特币的公钥既然散落在网络上，会被窃取吗？你不&#039；你不必担心这个。公钥可以&#039；t被推回到私钥。因此，即使公钥暴露，也不会影响私钥的安全性。

比特币地址通过两个哈希函数(上图中的SHA256)转换成公钥哈希，同样是不可逆的，然后对公钥哈希进行编码计算得到地址。地址的作用是接收比特币。一个地址收到比特币后，，只有拥有对应于该地址的私钥的人才能使用它。

正是因为有了私钥，才拥有了对钱包中加密货币的控制权，所以冷钱包的主要功能就是&quot存储私钥&quot。

冷钱包可以有各种各样的外观。有些看起来像u盘，有些是卡，专业级的硬件冷钱包，甚至附加了密码输入、指纹识别等额外的解锁功能，配合专有程序工作。

总之，只要有办法存储私钥，远离联网的东西。，也算是冷钱包了。举个例子，如果你把私钥手写下来，记录在纸条上，那么纸条可以看作是一个冰冷的钱包，因为它远离互联网。

▲ 冷钱包的款式非常多元，但重点还是要有离线存储私钥的能力。比如获得CES创新奖的LedgerNanoX，内部就有特殊的安全芯片。

冰冷的钱包虽然安全性高，但和现金一样，也会丢失损坏。，它不能用于实现快速在线交易。

如果消费者拥有的加密货币量不大，又想体验虚拟货币的操作和消费情况，那么随时联网的热钱包还是一个方便的选择。，这也是本课题研究介绍的主要内容。

热门钱包有多种形式，其中大多数是&quot多币种钱包&quot可以生成各种加密货币的支付地址，而它们的私钥通常只存储在用户&#039；s设备。

选择热门钱包，重点将是用户&#039；对服务商和App开发者的信任，其次是对操作界面、支持币种和备份难度的考虑。每一套热门钱包都有其优点和缺点，取决于消费者需要什么。

虽然网上交易所本身有存放钱的钱包功能，但是由于用户无法完全掌握私钥，所以将大量的虚拟硬币长时间放在交易所里实际上是相当不安全的。

以上就是什么是冷钱包，什么是热钱包？私钥和公钥呢？更多冷钱包、热钱包、私钥信息，请关注dadaqq.coM其他相关文章(www.dadaqq.coM)！

本网提醒，投资有风险，入市需谨慎。此内容不作为投资理财建议。

标签：冷钱包热钱包私钥公钥区块链