想知道什么是加密货币？它&#039；看完这本就够了！

作为一个虚拟货币初学者，我觉得最重要的是了解什么是虚拟货币和加密货币。今天这篇文章

就是带你了解所有关于虚拟货币的基本概念，让你在参与虚拟货币的交易市场之前打下一个稳定的基础！

虚拟货币是什么？

首先，什么是虚拟货币？

我觉得其实可以从一个很简单的角度来看，就是非实物货币就是虚拟货币，

而我们一般所说的实物货币就是世界上流通的货币，比如各国使用的铜板、纸币，

因此，

，不是这种看得见摸得着的实体货币，实际上可以统称为虚拟货币。

早期的虚拟货币

还有虚拟货币的出现，我觉得跟互联网的兴起有非常大的关系。

它创造了一个不同于我们现实的虚拟世界，

所以，说实话，我们很早就有机会接触到虚拟货币，最常见的虚拟货币就是出现在网络游戏世界里的游戏币，

。

像西蒙小时候流行的网游枫谷的枫币，是一种虚拟货币。通过这个枫叶币，玩家可以购买游戏世界中的任何商品和服务，基本上就像生活在与我们现实世界平行的时空里一样。

加密货币是什么？

如今，虚拟货币常被称为数字货币、电子货币、加密货币等不同的名称，

然而，在虚拟货币的投资市场中，加密货币通常被用作代理。

，会更准确一些，

因为加密货币是一种可以通过密码学来提高安全性的虚拟货币，和不涉及密码学的虚拟货币有很大的区别。

虚拟货币和加密货币

所以，从定义上来说，虚拟货币是一个越来越宽泛的名词；加密货币是一个狭义狭义的货币名称。

以及后面的介绍将主要以加密货币为名！

加密货币的历史

简单来说，你可以先记住两件事因为加密货币会出现：

加密货币系统的创造者：中本聪&#039；第一种加密货币：比特币。

字体首先，谁是中本聪？2008年，有一个自称中本聪的人发表了一篇论文。

，叫做&quot比特币：点对点电子现金系统&quot，

而本文主要解释。金融货币体系的建立不同于传统的，即第一种加密货币(比特币)及其相关算法。

2009年，比特币的相关金融系统正式上线，最早发行的比特币也转移到了中本聪&#039；的账户。

据说中本聪有大约一百万枚比特币。

然而，中本聪的真实身份仍然是一个未解之谜，有人认为他可能不是一个单独的人，而是一个特殊的组织。

比特币（Bitcoin）

什么是比特币？

刚才提到了，比特币是2009年创造的，是最早的加密货币。比特币本身是一种有固定金额的货币，一开始设定的总金额是2100万。

目前市场上，一枚比特币兑换成人民币的价值已经高达30万元，也是现在出现的加密货币中最有价值的加密货币。

加密货币的原理

如果你想详细了解加密货币和比特币的工作原理，这里有一些你必须先了解的术语和特性！

区块链（Blockchain）

区块链其实可以应用在很多领域。

在今天&#039；区块链是加密货币中最常用的领域，也是加密货币中最核心的技术概念。

简单来说，在加密货币中，你可以把区块链看作是一个公共会计的系统数据库。

比如今天小王给小张传了一块钱，小王会亏一块钱，小张会赚一块钱，这个交易记录会记录在其他人&#039；s街区除了小王&#039；s块，

并且每个块将通过密码术相互连接。

确保记录信息的安全性，这是使用区块链的技术理念。

去中心化（Decentralization）

从区块链的技术中，其实可以找到一个特点。

也就是通过这种分布式的记录方式，每个人都可以共享信息，也就是说每个人都可以扮演监督者的角色。这就是分权的概念。

因为在我们目前普遍的传统金融体系下，大家&#039；美元货币交易。，有一个中介作为监管，比如银行或者政府，

所以，只要中间多了一个流程，办理时间自然就多了，效率就降低了，

而且只要有人在，就有人出错。

，或者漏洞出现的地方，因此，安全问题也会受到考验，

而区块链的出现可以帮助你解决这样的问题。

公共帐本（PublicLedger）

就像刚才说的。

在加密货币中，利用区块链技术，每一种货币之间的每一笔交易的信息都会同时记录在所有的账户块中，

而这种开放的记账方式使得加密货币的所有块信息都成为一套人人皆知的公共账本。为了证明所有人的控股地位&#039；的钱在同一时间。

这个其实和你的银行存折差不多，只不过它不需要借用第三方，也就是不需要通过银行帮你记录，而是直接由区块链系统自动记录。

货币数量上限

在加密货币的世界里，每种加密货币的数量都是一个固定值，

因为它们都是由特定的算法生成的，而每种制作加密货币的算法都有一定的规则，无法重写。

所以和我们现在一般的金融体系下发行的货币有很大的区别。与现在的货币不同，加密货币跟随国家政府的步骤，想什么时候印钞票就什么时候印。

所以不会出现货币超发，造成通货膨胀。

，货币贬值的问题。

工作量证明（ProofofWork）

说实话，从简单的角度来看，网上虚拟货币之间的交易，其实就是一些数字在变化。

这时候如果你遇到专门研究程序演算的高材生(黑客？)，很容易出现重复支付的问题，

因此，你可能会有疑问。既然区块链是分散的，那么就没有人来保护我们资金的安全。

关于这一点，有必要说一下区块链中一个非常重要的机制，那就是工作量证明。

简单来说，工作量证明(workloadproof)是一种安全的保护机制，它使用强大的算法来保证区块链中打开的书籍和资料的一致性。

PS:工作量证明更完整的意义与加密货币的开采有关，即通过工作量证明的共识机制，货币的生成可以有一定的规则，也可以保证矿工获得货币奖励的公平性。

公/私钥匙（Publickey/

在加密货币的交易中，主要需要两个密钥，即公钥和私钥，而且基本上公钥和私钥会成对出现，即一个公钥一定会匹配一个私钥，

公钥可以帮你生成支付地址，它不会&#039；公开不公开无所谓，但是私钥一定要保管好，因为它负责决定你对加密货币的使用权！

如果交易消息由一个密钥加密，则必须与另一个密钥匹配才能解密。

简单来说，交易双方使用的密钥是不一样的，这就是所谓的非对称密码技术。

补充说明：

基本上

生成公私钥的过程有点复杂，但是你可以先记住一个核心概念，就是生成的起点是私钥，从私钥生成公钥，公钥会生成支付地址。

加密货币钱包

以及装有加密货币的钱包。

，也就是刚才说的公私钥结合，也就是通常存放公私钥和支付地址的地方，主要用于交易、收款、付款和记录金额。

加密钱的钱包基本上可以分为两种：

。

热钱包冷钱包

热钱包（HotWallet）

什么是热钱包？

简单来说就是一个在线钱包，也就是会连接互联网。

，以及常见的热门钱包类型，主要像网页插件钱包(MetaMask)，手机APP钱包(TrustWallet，BitoEX)等等。

冷钱包（ColdWallet）

冷钱包和热钱包正好相反。平时不联网，只有用的时候才联网。所以也叫离线钱包，主要像硬件钱包(Ledger，Trezor)和纸质钱包(键码打印或写在纸上)。

伪匿名性（Pseudo-anonymity）

加密货币的钱包基本上不包含任何与你真实身份相关的个人资料，

也就是说，无法直接识别每个交易者的真实身份。

，而这也使得加密货币匿名，

但是就像刚才说的，因为加密货币有区块链技术，每一笔交易数据都会被记录在所有的区块里，

所以交易信息是共享的。，即可以通过追踪交易记录获得更多交易者的信息，进而知道交易者的真实身份。

比如有一天，你的钱包不小心被别人知道了，也公布了。那就意味着所有人都会知道你的真实身份，以后你所有的交易记录都会被别人知道，这简直就是赤裸裸的摆在所有人面前。

所以，加密货币的匿名性应该更像伪匿名。

加密货币优缺点分析

优点

货币数量固定：加密货币在产生之初，根据算法的规则会有一定的数量，所以不会像现在发行的货币太多那样受到通货膨胀的影响。

，导致货币贬值。高安全性：加密货币使用密码术来加强其安全性。除非你有私人钥匙，你可以&#039；根本不用账户里的加密货币，比普通货币安全多了。手续费低：因为加密货币的核心概念也就是去中心化，也就是不需要通过中介进行金钱交易，基本没有手续费，可以帮你节省很多交易成本。高透明度：由于加密货币采用区块链技术，每一笔交易信息都可以记录在所有区块中。实现信息共享的概念，因

此，它的消息透明度相当高。跨境转账便捷：如果加密货币能够普及，跨境转账就不需要经过太多的关卡，而此时转账速度会变得更快，也就意味着跨境转账会变得更加便捷。

缺点

交易的不可逆性：由于加密货币的交易是不可逆的，如果你今天已经把加密货币发给了别人，并且交易被确认，那么即使你发送错误，也没有办法更改，除非收件人自己寄回来。。忘记密码可以&#039；t被找回：加密货币只有一个密码，而且由于去中心化，无法通过相关验证获得新的密码，所以如果你忘记了密码，就意味着你的加密货币也会离开你。。(相当多的人忘记了自己的密码.)非法使用：由于加密货币没有监管单位，无法有效追踪交易者身份，很容易被有心人利用，产生洗钱或诈骗等违法行为。分配不公平：说实话，加密货币的分配相当不公平。

比如比特币刚出现的时候，只有少数人知道，所以就像现在的世界一样，主要的财富还是掌握在少数人手中。

加密货币有哪些？

加密货币除了第一枚比特币，

事实上，还有其他不同类型的加密货币。因为加密货币的相关开发信息是公开的，这意味着只要有心，就可以设计出新的加密货币。

现在市面上有5000多种加密货币。其中，著名的加密货币有以太坊(ETH)、瑞波币(XRP)、TEDA币(USDT)等。

图片来源：Coinmarketcap

PS:如果你想了解更多不同的加密货币，

可以参考Coinmarketcap。

加密货币如何来应用？

学了这么多加密货币的知识，你肯定会想知道加密货币是怎么应用的。

常见的方式主要有五种：

挖矿赚币

挖矿加密货币是获取加密货币最重要的方式之一，那么究竟为什么可以通过挖矿来获取加密货币呢？

这个原因来自刚才提到的区块链公共账本，因为要想让交易记录记录在所有区块上，就必须依靠强大的计算能力。

因此，系统会给提供计算的计算机一些额外的奖励，这些奖励就是加密货币。

但是，想要通过挖矿赚取加密货币，其实有相当多的坎需要跨越，比如你是否有强大的硬件设备(矿机)，以及挖矿电费的考虑(挖矿的耗电量惊人……)。

购物交易

利用加密货币买卖东西，进行交易，我觉得这其实是货币最原始的功能之一。

这就像最早的使用加密货币购买实物的案例，发生在2010年5月22日。一个工程师花了一万个比特币买了两个披萨，然后5月22日就被称为比特币披萨日。(今天这两个披萨简直是天价XD)

其他的就像美国知名的在线支付系统Paypal。，还与一家加密货币公司(Paxos)合作。预计到2021年底，将有2800万笔业务串联起来，让美国人民可以使用加密货币进行交易。

但是，目前可以使用加密货币购物的地方，

相对来说，还是很少的。看来还有很长的路要走！

投资交易

按照目前的趋势来看，加密货币的主要应用之一就是经常用于投资交易，

。

这有点类似于股市投资，就是当你在市场中间看到加密货币，并且它处于一个相对较低的价格时，你买入，然后当它攀升到一个较高的价格时，你卖出，从而获取中间的差价利润。

然而

加密货币在交易市场的波动性相当大。虽然利润空间也增加了，但是风险比较大，投资的时候需要特别注意！

贷款交易

加密货币本身也可以用于贷款交易，也就是你用现有的加密货币来借钱，

而在这个前提下，通常是因为你确定手里的加密货币还有增长空间，所以想继续持有，

。

另一方面，因为你的资金有限，你预测某个加密货币的收益率远远超过你所借的利率，所以你想用加密货币借钱进行投资。

但是，这自然就像借钱买股票，开杠杆的概念，所以风险相当高。

小心点。

放贷生息

加密货币可以用来放贷，自然你也可以成为放贷人，也就是把钱借给别人，然后通过放贷赚取利息的概念。现在有很多交易平台提供这种借贷服务。

，如币安和Bitfinex。

而如果你想在熟悉的情况下理解这个概念，其实和把钱存在银行(把钱借给银行)赚利息是一样的，只是利息水平不一样。

加密货币怎么买？

从刚才加密货币的应用可以知道，获取加密货币的途径主要是通过挖矿或者交易。

那么如果你今天想直接买加密货币，怎么买呢？

主要可以分为三个部分：

场外交易（OTC）

OTC在英文中是Over-The-Counter，所以经常被直接称为OTC，

而这种交易方式，

，即不需要依靠中间的大平台，直接和有加密货币的人进行交易。可以选择网上交易，也可以直接面对面交易。

的主要优势是保密性高，交易价格会更优惠，但是相对来说，

缺点是因为通常没有中介介入，容易被骗，交易安全性低。

兑换所

It&#039；这实际上有点像我们去银行把人民币换成外币的原因。

兑换购买的加密货币主要优点是操作方便简单，缺点是可供选择的货币种类较少，买卖价差比较大。

交易所

并且去交易所买卖加密货币。

，就像我们去一个证券账户买卖股票的概念一样，

基本上，要在交易所进行买卖，需要完成相关的信息申请，包括邮箱验证、手机绑定、身份认证等。才能开始交易，

主要优点是可以选择的货币种类比较多，有时候交易所也会举办一些奖励活动，

主要缺点是申请账号的过程比较麻烦。此外，如果所有资金都存放在交易所，

，可能有被黑的风险。(It&#039很容易发现交易所被黑的消息.)[XY002]

加密货币的风险

[XY001]每一笔投资都必然伴随着相应的风险，加密货币也不例外。至于加密货币的风险，

，可以总结为以下四点：

市场波动大

如果你在观察加密货币的价格变化，其实可以发现它的波动性是相当大的，

以比特币为例。

今年4月份飙升至每只近40万元。结果一个月后跌至25万元左右，跌幅超过40%。很夸张，就像坐过山车一样。

所以，在投资加密货币的时候，你要非常注意市场的波动和你的投资策略。

否则你所谓的投资就变成只是投机了！

诈骗夸张多

西蒙觉得这个世界真的很奇妙，时代的科技在不断进步，诈骗集团也在提高诈骗技巧(另类进步...)，

而加密货币除了被普通投资者扣押之外，自然也成为了诈骗分子使用的手段之一。

比如有人在交易加密货币时遇到诈骗，或者一些不法分子利用资金盘子的概念吸引投资者大量资金投入。结果最后钱都烧光了，随便搜一下资料就能找到很多跟诈骗有关的举报。

所以，如果有人告诉你哪里有好的身体，投资一些本金就能赚到高薪，请你勒紧裤腰带，慎重考虑。

他身体好的时候为什么要告诉你？

黑客攻击

除了诈骗，黑客&#039；s攻击也是参与加密货币应该注意的一大风险，因为你可以发现，只要网络参与其中，就一定存在相关的漏洞。

毕竟网络是人为的，会被找弱点攻击。其实也不算太意外。

比如你稍微搜一下，世界上几乎所有顶级的大型加密货币交易所都被黑客攻击过。

所以，如果你想跻身交易所，

投资加密货币时，这是需要特别注意的风险之一！

监管问题

基本上加密货币最初的概念应该是去中心化，而去中心化，相对来说是不受中介机构管理的动作，而是

在目前的情况下，这里似乎也成了相关犯罪分子的有用之地。此外，加密货币也有很多投机问题。

因此，很多国家也开始进行监管行动，比如中国政府就出台了很多相关的法律法规。

，以限制加密货币的交易业务，因此一些交易所已经开始退出中国市场。因此，对于加密货币来说，监管问题将是未来需要克服的一个主要障碍！

结论

跟其他投资一样。

在投资加密货币之前，做足功课和研究，可以帮助你大大降低投资的风险。说实话，加密货币的相关知识真的很广泛，可能要花很多时间去学习。另外，虽然近年来，加密货币的相关机制已经比以前先进。但是，仍然有许多需要改进的地方。希望今天给大家分享的虚拟货币入门概念对你有所帮助。有问题可以在下面留言！