加密货币市场发展日新月异，本文主要介绍选取的五种加密货币，分别是比特币、以太币、莱特币、瑞波币和狗狗币。

在介绍加密货币之前，先介绍挖矿的过程，挖矿是一种对加密货币十分重要的机制。

一方面通过共识规则验证交易，保证去中心化的安全性，另一面构建区块时，会创造出新的加密货币，类似央行发行新的纸币。

挖矿

每一个计算机的CPU就是一个矿工，加密货币是一个去中心化的系统，它依赖于共识规则来运行。

一个交易只要得到大多数的参与者的认可，那么就是真实可信的，这意味着发生的交易需要向比特币所有节点进行广播，所有节点需要验证这些交易的真实性。

每个节点首先需要构建一个候选区块，然后从交易池选择交易并打包进该区块，这个区块头包含有前一个区块的哈希值，时间戳、随机数和难度目标值等字段。

挖矿就是改变随机数，以寻找符合难度目标的新哈希值，该哈希值是根据一个算法计算，而得到的。

哈希函数的特点，是任意长度的不同的输入，几乎不会产生相同的输出，而且不能逆向求解，在进行哈希计算的时候会产生工作量证明，这需要耗费电力和算力资源，保证了交易的安全性和公平性。

尽管这有可能扩张能源消耗，给环境带来不利冲击，这种方式构建的区块是堆栈起来的，所有的区块都是连在一起的，也就产生了区块链。

由于摩尔定律指出计算机的运算能力。每18个月会增加一倍，这意味着挖矿的难度，是需要进行调整的。

加密货币是没有实物载体的，它的所有权需要通过数字密钥、地址和数字签名来确定，数字密钥可以通过加密货币钱包自动生成的。

并且这个过程与比特币协议相互独立，甚至不需要联网，一个数字密钥包括了一个私钥和一个公钥，公钥和地址均可以由私钥生成，生成的方法是哈希函数。

这意味着对私钥的所有权，就表明对加密货币的所有权，也就表明私钥必须要妥善保管，如果遗失，对应的加密货币也就丢失了，无法找回。

加密货币的交易都需要通过钱包，钱包是连接用户和区块链的中介，这个钱包没有加密货币，只有密钥，因为加密货币保存在区块链中，钱包可以创建交易，追踪余额，管理密钥和地址等。

挖矿的硬件设备也发生了改变，最开始通过普通电脑的CPU计算，是可以获得比特币的。

但是随着节点增多和技术更新，更为强大的ASIC（专用集成电路）设备被大量投入挖矿，它可以产生更高的运算速度，此外，GPU（图形处理器）也是一种较高效的挖矿设备。

由于挖矿的原理和难度调整机制，会出现“空区块”而无法获得收益，因此，截至目前，个人矿工几乎无法获得新的加密货币，导致了一些大型矿池的出现。

因为从人类发展的历史来看，合作是人们进行风险分担，是最常见也最有效的手段，保险就是最好的例子，每个参与者投入自己拥有的矿机，整体组合在一起进行挖矿。

这样能够提供最大算力，也就最有可能率先找到符合目标区块的哈希值，创建新的区块以获得奖励，最终按照贡献的哈希率进行收益分配。

这种情况下，每个参与者贡献的哈希率，只有在获得了奖励之后才有，因为有可能挖出“空块”，得不到奖励。

第二种是按照参与者贡献的哈希率，只要找到部分解就支付一个固定的费用，这种方式就相当于“时薪”，或者是参与者将他们的哈希率出租给矿池。

第三种是云挖矿（Cloud Mining），不同于第二种的出租哈希率，该机制是反向运行的，每一个矿工预付一个固定的费用给矿池，然后就可以获得哈希率并用于自己单独挖矿。

加密货币并不是实实在在的货币，它是虚拟的，没有实物载体，加密货币的价格波动趋势大致是相同的，但是价格整体差距大。

价格对比

对于比特币来说，其价格从开始时，约为139美元一枚，到2021年9月20日，其价格约为42000美元一枚，是初始价格的300多倍；对于以太币来说，初始价格约为0.7美元一枚。

截止2021年9月20日，其价格为2700美元一枚，增加了3800多倍；莱特币的价格，从开始时的约4美元一枚，到2021年9月20日，其价格约为156美元一枚，增加了38倍。

瑞波币和狗狗币的价格，相对较低，瑞波币的价格，从开始的0.005美元一枚，到2021年9月20日，其价格约为0.9美元一枚，是初始价格的180倍。

狗狗币的价格，从开始的0.0002美元一枚，增加到2021年9月20日的0.2美元一枚，增加了近1000倍。

从微观角度看，加密货币的价格变动最为剧烈的时间段，是2017年末到2018和2020到2021年两个阶段。

例如比特币，它的价格从2017年初时的约777美元一枚，增加到2017年末约19000美元一枚，增加了约24倍，随后价格出现回落，但是整体保持在3000美元一枚以上。

而在2020年，比特币从最低时约4900美元一枚，到2020年末增加到了29000美元一枚。

之后更是犹如脱缰的野马，在2021年4月13日，更是达到了约63000美元一枚，相较于2020年最低时增加了近13倍。

而以太币的价格，从2017年年初最低时的约10美元一枚，到2018年年初时，上

涨为约1300美元一枚，增加了130倍，之后价格猛跌，但基本维持在100美元一枚。

之后在2020年到2021年，以太币的价格更是猛增，从最低时约110美元一枚，在2021年5月11日增长为约4100美元一枚，增长了也将近37倍。

莱特币的价格，从2017年最低时的约4美元一枚，上涨为约358美元，增加了88倍，之后价格迅速下降，基本保持在30美元一枚。

而在2021年5月9日，其价格又暴涨到了386美元一枚，瑞波币的价格，也是经历两次较大的大波动，从2017年最低时约0.006美元一枚，增长到了3.3778美元一枚，增长了560多倍。

之后价格迅速回落，但是基本保持在0.14美元一枚，之后在2021年4与14日其价格涨到了约1.8美元一枚，没有超过2018年年初的最高价格。

而狗狗币的价格，在2020年以前波动都是很小的，其价格在2021年5月6日，达到了0.68美元一枚，之后一直保持在0.1美元一枚以上的价格水平。

比特币

比特币（Bitcoin）是最受欢迎的加密货币，截止2021年9月20日，它的市值是8064亿美元。

诞生于2009年1月3日，它是由中本聪创造出来的，它的总量是2100万个单位，但是它的最小单位不是通常货币的“分”，而是“聪（Satoshi）”。

1比特币等于10*8聪，比特币矿工的收益，主要来源于两个方面，其一是通过建立新的区块而得到的奖励，其二是交易费用。

根据中本聪的原始设定，大约每10分钟产生一个新区块，每21万个区块奖励减半，即大约是4年，最开始的奖励是50个比特币一个区块。

到2012年11月28日，减半为25个，2016年7月10日为12.5个，2020年5月11日减半为6.25个，预计2140年比特币将被全部挖出来。

比特币的共识机制是工作量证明，这种机制，既保证了安全，也让所有人认可交易，但是需要消耗大量的能量，看到比特币的能源消耗接近200TWh，大约等于泰国的全年能源消耗。

而ETH的接近100TWh，大约和菲律宾的全年能源消耗相等。

比特币挖矿的核心就是计算机算力，谁拥有了更多的算力，谁就更有可能得到收益，所以导致了大型矿池的出现，目前个人几乎不可能挖到比特币。

根据Statista的数据。我们可以发现排名前5的矿池，占据了超过一半的算力，即算力趋向于中心化、集中化，这与加密货币的核心理念去中心化是相互矛盾。

因为足够的去中心化程度，对于加密货币区块链的安全来说，是十分重要的。

以太币

以太坊，它的原生资产是以太币（ether），它是用来支付使用以太坊，这个超级计算机的花费，是维塔利克布特林在2013年创立。

随后通过ICO（Initial Coin Offering）获得发展，截止2021年9月20日，它的市值是3480亿美元。

以太币是在比特币区块链的基础上发展起来，以太币可以看成是一个开源的、全球的去中心化超级计算机。

这就意味着它的本来目的，不是成为数字货币的支付网络，而是为智能合约的发展提供平台。

智能合约本质是一个计算机自动执行的程序，包括了触发条件和执行结果，它可以在最少依赖第三方中介的条件下，最大限度内减少欺诈、意外损失、仲裁成本和交易成本。

以太币提供一个平台，让每一位开发者能够自主编写智能合约，并上传到以太币区块链上，所有的以太币虚拟机（EVM）都运行相同的初始状态，输出完全相同的最终状态，所有的智能合约只有被交易触发才能被调用。

以太币的挖矿过程与比特币不相同，它的工作量证明叫做Ethash，该方法被设定为减少ASIC的效率，使得普通的设备可以进行挖矿，激励更多人参与，保证去中心化的矿工。

但是目前以太币的挖矿共识机制，正逐步转向了工作量证明，最终过渡到权益证明，以减少能源的浪费。

以太币的面额比较复杂，以太币的最小单位是wei，一个以太币等于10^18个wei，此外还有10^3（kilowei）、10^6（megawei）、10^9（gigawei）等。

在以太坊上进行交易的时候，为了避免拒绝服务和过度消耗资源，需要燃料（gas），燃料使用以太币支付，燃料价格和以太币之间存在一个汇率关系，燃料价格最低为零。

而且是处于变动状态的。以太币在2016年由于一个智能合约漏洞，其中价值约1.5亿美元的以太币被偷走，最终通过社区投票，以太币进行了硬分叉，将偷走的以太币追回来。

但是一部分人认为不应该人为干预，坚持不分叉，这些人没有转入以太币新的区块链，而是留在了原来的以太币区块链，被称为以太币经典。

莱特币

莱特币（Litetcoin）是查理李，在2011年10月基于比特币推出来的，鉴于比特币的挖矿过程会出现集中化和专业化，莱特币在这些方面有所改进，截止2021年9月20日，它的市值是104.4亿美元。

首先他在协议中采用了区块哈希算法，该方法可以让业余爱好者，更加容易轻松地参与挖矿过程，而专用设备无法获得较大优势。

其次，莱特币产生一个区块的时间是2.5分钟，是比特币的1/4，可以更加快速的

进行交易的确认，增强了交易的安全性。

而这意味着莱特币的总量是8400万个单位，相应的每84万个区块奖励减半，莱特币的矿池算力份额，排在前5的矿池大约占了73%的份额，它的算力集中度高于比特币和以太币。

瑞波币

瑞波币（Ripple）是瑞恩福格尔于2004年就创建的一种加密货币——Ripple Pay，但是它并没有吸引到很大的关注度。

直到2012年克里斯拉森和杰德迈克卡勒伯与福格尔建立合作关系，

瑞波币开始发展起来，它的核心是建立一种高效、快速和方便的支付转移系统，不同于其他加密货币为个人提供服务。

瑞波币的目标群体是银行等金融机构，其原生资产是瑞波币（XRP）,截止2021年9月20日，它的市值是427.6亿美元。

它拥有独特的技术，它没有矿工，不需要挖矿，总计1000亿单位的瑞波币是由三个创立者持有200亿，并向瑞波实验室（Ripple Labs）捐赠了800亿。

2017年实验室建立了55个10亿XRP的合约，合约在第0月到第54个月每个月的第一天到期，释放出XRP。

瑞波币的最小单位是“滴”（Drop），1瑞波币等于10^6滴。由于分配瑞波币的方式和瑞波币具有一定的中心化，导致一些加密货币社区

对它的信任度低。其次，它是基于可信子网络的共识算法，即XRP Ledger共识机制，当交易发生之后，每个节点会自我选择一些验证节点对交易和顺序进行投票。

投票权的大小取决于这个节点本身拥有的加密货币数量，数量越多，被选中的概率就越大，当有超过80%的节点验证通过，这个交易就会被确认，添加到区块链上。

它除了使用原生资产XRP以外，还可以使用任意的货币，包括法币、数字货币和其他形式的价值，并且处理交易速度快，只需要3-5秒，而比特币需要500秒，容量大，每秒1500笔，比特币每秒3笔。

狗狗币

狗狗币（Dogecoin）是2013年12月8号出现的，截止2021年9月20日，它的市值是272亿美元，比利马库斯使用莱特币的代码推导出狗狗币，狗狗币的总量是没有上限的。

并且使用的挖矿算法也不同于比特币的算法，狗狗币使用Scrypt算法，这使得狗狗币大约每1分钟就可以产生一个区块，挖矿的难度也很低。

马库斯团队计划每年发行大约50亿个狗狗币，它与莱特币和比特币的通货紧缩，形成巨大反差，狗狗币主要在互联网打赏者中广受欢迎。

由于供应的时间表，每个狗狗币的价值一般是几美分，这非常符合它的预期，它与其它加密货币风格迥异。

狗狗币的使用更加简单快速，例如你可以直接资助你认为好的网络博主，或是直接捐赠一笔钱给慈善机构。

整个过程完全匿名，也没有任何中介机构参与，它为在互联网时代如何争取社区支持提供了宝贵的经验。

例如狗狗币社团依靠狗狗币筹集了资金，在2014年资助牙买加雪橇队参加冬奥会，同年又为肯尼亚筹资金修建水井等。