为什么需要匿名币?从匿名举报到匿名做好事，从匿名约会到匿名投票，社会是无法避开匿名的合理需求的。人性的基本特点决定了我们对隐私的注重，加密货币的发展迎合了人类社会的发展。从现实来看，权威机构对数字货币监管的增强，使匿名似乎成了不得已的出路。因此匿名是我们的一道防线，匿名币的发展也成为数字货币的一个主流方向。匿名币就是在交易过程中隐藏交易金额、隐藏发送方与接收方的一种特殊的区块链代币。与之相对应的，是比特币、以太坊这些“显币”。 稍微了解一点区块链知识的朋友都知道，比特币的区块链是一个公开的分布式账本，每一笔交易都是可追踪的。也就是说钱包以及交易都是公开的，比特币的匿名性只是钱包地址和个人身份是无法对应的。通过区块链，你可以轻松的知道钱包地址A向钱包地址B转账了一定数量的比特币，但是无法知道究竟是谁发送了这一笔比特币。但是，一旦你知道某个地址属于某一个人，那么你可以轻松知道他这个地址的所有交易。2020年匿名币中哪个最有前景？市面上已经有一些匿名币使用不同技术来解决上面提到的隐私问题，如 Dash, Monera, Zcash，其他还有 PIVX,Grin, Verge, NavCoin。此外，传统通证，如 LTC，正考虑添加匿名属性，使 LTC 作为交易和支付的媒介获得更多的优势。下面将分别介绍每种匿名币。达世币(DASH)

DASH 币创建于2014年的一次 BTC
分叉之后，它在密码学上并非严格保密。DASH 通过使用一种基于 CoinJoin(一种最初用来为BTC增加匿名属性的策略)的技术进行混币以保证匿名性。Dash采用了工作量证明(PoW)的架构，其系统中有两种信息收发角色：主节点和矿工，其中主节点有瞬间发送交易和匿名发送交易的功能。CoinJoin 是 Gregory Maxwell 提出的一种匿名化交易的技术。CoinJoin 提升了用户的隐私安全，因为它将多笔交易合并，使人难以分辨哪笔输入对应哪笔输出,
从而难以追踪某个地址的资金的来源或去向。Monero门罗币(XMR)

Monero 被认为是数字资产领域中最好的匿名币之一，是由 Bytecoin 2014的一次硬分支产生的。Monero 使用编码交易来隐藏地址和传输数量，其中还包含了错误编码，以混淆视听，保护真实的交易信息。该编码使用 Ring CT(环保密交易)来保障交易和钱包的匿名性。Monero 还集成了 Tail(一种通过 TOR 网络传输交易的操作系统)，以进一步保护隐私。此外，Monero 还利用隐形地址来隐藏用户的钱包地址。隐形地址是为每个交易创建的一次性地址，Monero 的用户也有一个发布在区块链上的公开地址，但是他们的大部分交易都是通过一次性的隐形地址进行。基本上，Dash 是将小的交易汇集起来，而 Monero 则是分解成小的交易。因此，Monero 主要依赖于网络资源，而它与 BTC 的不同之处在于，普通的个人电脑就可以运营 Monero 的节点。Zcash(ZEC)

Zcash 是另一个 BTC 分叉诞生的匿名币，它使用 zk-SNARKs(零知识证明算法)，允许矿工在不知道谁发送/接收币的情况下验证交易。该协议开发团队积极与其他团队合作，将隐私属性添加到他们的项目/平台中，被称作“企业版以太坊”的 JP

Morgan 的 Quorum 链也使用了 zk-SNARKs 技术。ZCash运用了“零知识证明”这一密码学原理，在区块链记录中隐藏了交易者的所有信息，包括交易双方的地址和交易的全部。因此即使获取到了某钱包地址所对应的IP,也无法追溯整个交易链。PIVX(PIVX)

PIVX 是一种新型暗网币，代表即时验证的保密交易。PIVX 是 Dash 的一个分支，它应用了 BTC 改进协议(BIP)，并利用权益证明(PoS)来保护网络。PIVX 的用户至少需有10.000个币才能运行主节点 (而 Dash 只需要1.000个 DASH)。GRIN古灵币(GRN)

Mimblewimble 是一个基于 BTC、主打匿名的新项目。2016年7月19日，“TomElvis Jedusor”将项目白皮书丢进一个 BTC 研究平台后就消失了。后来，“Ignotus Peverell”基于这份白皮书启动了一个名为 Grin 的 Github 项目。Mimblewimble是《哈利波特》中让人舌头打结的咒语;Tom Elvis Jedusor是伏地魔的法文名字;Ignotus Peverell 是隐形衣的原始主人。Mimblewimble/Grin改进了BTC的保密交易和CoinJoin，其主要特性包括没有公开地址、绝对的保密性和简洁的区块链。由于Grin币和BTC一样，只能通过PoW 共识机制来出块，因此近来Grin挖矿成为了热点。Grin使用Cuckoo Cycle PoW算法，该算法最初设计是为了对抗ASIC，但现在则被认为是对ASIC友好的。Grin 的主要特点:绝对的保密性交易可扩展性可靠的、经过测试的密码学原理用户间交易简便社区驱动——;以分布式发展和挖矿为目标其他比较有趣的、还处于早期的匿名币包括 MobileCoin 和 BEAM。Verge(XVG)2014年，Verge 币以全球最流行的 meme 数字资产 DogeCoin 的暗黑版 DogeCoinDark 横空出世。2016年，重新命名为 Verge，并在技术和投资界备受瞩目。Verge 是可挖的。相比 BTC 挖矿昂贵且方法有限，Verge 有三种挖矿方法可供选择。Verge 可以用作支付。BTC 支付不具备匿名性，Verge 交易使用 TOR 和 i2P 技术，实现了交易的绝对保密性。Verge 是去中心化的货币。Verge 正在添加智能合约功能，以使其比BTC更能满足用户需求。Verge 有几个重要的合作伙伴，包括色情行业巨头 MindGeek，其子公司包括 Pornhub 和Brazzers。Litecoin(LTC)莱特币已经不甘心屈居于 BTC。多年来，莱特币一直处于 BTC 的阴影下，如今，莱特币的核心开发者们对像 Monero (XMR)和Zcash (ZEC)这样的匿名币越来越感兴趣。Charlie Lee 就可替换性展开了讨论，并暗示在2019年的“全节点应用的未来版本”中将增加保密交易，这将使 LTC 作为交易和支付的媒介获得更多的优势。NavCoin(NAV)NavCoin 是一种由 BTC 分叉产生的去中心化数字资产，它的目标是解决区块链平台中常见的2个问题:数据在区块链上公开，容易受到非法用户的恶意攻击。大多数区块链使

用“回滚”作为数据漏洞的解决方案。它们在数据泄漏后将区块链重置回备份点，这意味着在回滚之前生成的交易将被删除。NavTech 系统是将传统的 BTC 区块链和 NAV 子链结合使用，这使用户可以以完全匿名的方式进行交易。CloakCoinCloak 是一种老牌匿名币，虽然它已经在匿名领域活跃了大约4年，但发展缓慢。其区块链使用权益证明 PoS 共识协议，它具有相对较短的区块时间和快速处理交易的特点。该平台提供了两种方法使交易无法跟踪。第一种是洋葱路由(onion-routing)隐私协议，使用多个 layer (类似于洋葱)来加密消息。第二种是 Enigma 程序，为交易提供额外的隐私保护。当用户申请保密交易时，Enigma 就会开启。Enigma(ENG)Enigma 项目完全独立于 CloakCoin 交易中使用的 Enigma 程序。Enigma 既不是数字资产，也不是区块链，而是一种可以部署在区块链和分布式应用程序上的隐私协议。因此，它的通证 ENG 非常与众不同。Enigma 网络中的节点无法看到它们计算的数据，Enigma 以此来保证隐私性。尽管这些节点不清楚它们正在处理什么，但是它们仍然能够验证计算是否正确。Enigma 想要推广这种新型智能合约——“秘密合约”——在这种合约中，智能合约中处理的底层数据始终保持加密。主要特点:使用Tor隐藏地点，使追踪更加困难隐形地址隐藏接收者环形签名隐藏发送者匿名币的主要用途?说到匿名交易，很多人首先想到的是非法交易与犯罪。但事实上，我们生活中充满着这类交易方式。比如，一笔生意成交后，交易双方一般都不希望将此交易公开，尤其是真实的交易金额。或者，在用智能合约处理招投标、竞拍业务时，在竞拍和招标结束前，交易双方也都不希望把标的金额在区块链上公布，让任何人都可以查到。这些信息的隐秘性在很多商业场合非常重要。当然，这个匿名的特点也被一些犯罪分子利用，成为洗钱、贩毒等活动的资金流通工具。对于匿名币，笔者有一个观点，即：可以采取分层匿名。第一层是交易双方的身份匿名，第二层是交易金额的匿名。如果要防止成为犯罪的工具，可以在第二层上进行匿名，而让交易双方的地址仍旧可查。这就是ZCash的方式，当然，门罗币采取了更为激进的全匿名方式。