一、数字货币初探

目前，数字货币尚没有公认的标准定义。从广义上讲，数字货币泛指一切以电子形式存在的货币。狭义的数字货币一般特指以非对称密码技术为基础的“密码货币”，这也是本文的主要研究对象。
按照数字货币的发行者不同，可以被分为私人发行、不受法律保护的私人数字货币（比特币、以太币等）和中央银行发行并进行监管的法定数字货币（央行数字货币）。

随着计算机和互联网技术的迅猛发展，除了数字货币外，还出现了多种新的“货币”概念，如虚拟货币和电子货币。三者概念既有不同也有重合之处，法定数字货币和电子货币因均由央行发行容易被混淆，私人数字货币和虚拟货币因均由私人机构发行容易被混淆。我们首先对这些概念进行区分，以界定本文所研究的数字货币的范围。

电子货币和法定数字货币。
1）电子货币是指法币的电子化，即纸币在银行或其他相关金融机构将法定货币电子化和网络存储和支付的形式，并没有创造新的货币类型，只是现有货币的电子形式。按照其发行主体的不同又可分为银行卡、储值卡（如公交卡、购物卡）和第三方支付（如支付宝、财付通）等。2）法定数字货币本身是货币（属于M0的范畴），与纸币、硬币共同构成现金，不仅仅是支付工具，如中国央行即将发行的央行数字货币。

虚拟货币和私人数字货币。
1）虚拟货币通常指基于网络的虚拟性，由网络运营商提供发行并应用在网络虚拟空间的类货币，如腾讯公司发行的Q币，各大网游公司发行的游戏币等，一般只在自身生态内流通，政府出于稳定金融体系的目的规定其不可与法币双向流通。2）私人数字货币是指无发行主体或私人机构发行的可以被用于真实的商品和服务交易的“货币”，其不仅仅局限在虚拟空间中，如比特币、以太币等。

二、区块链：多种技术的集大成者

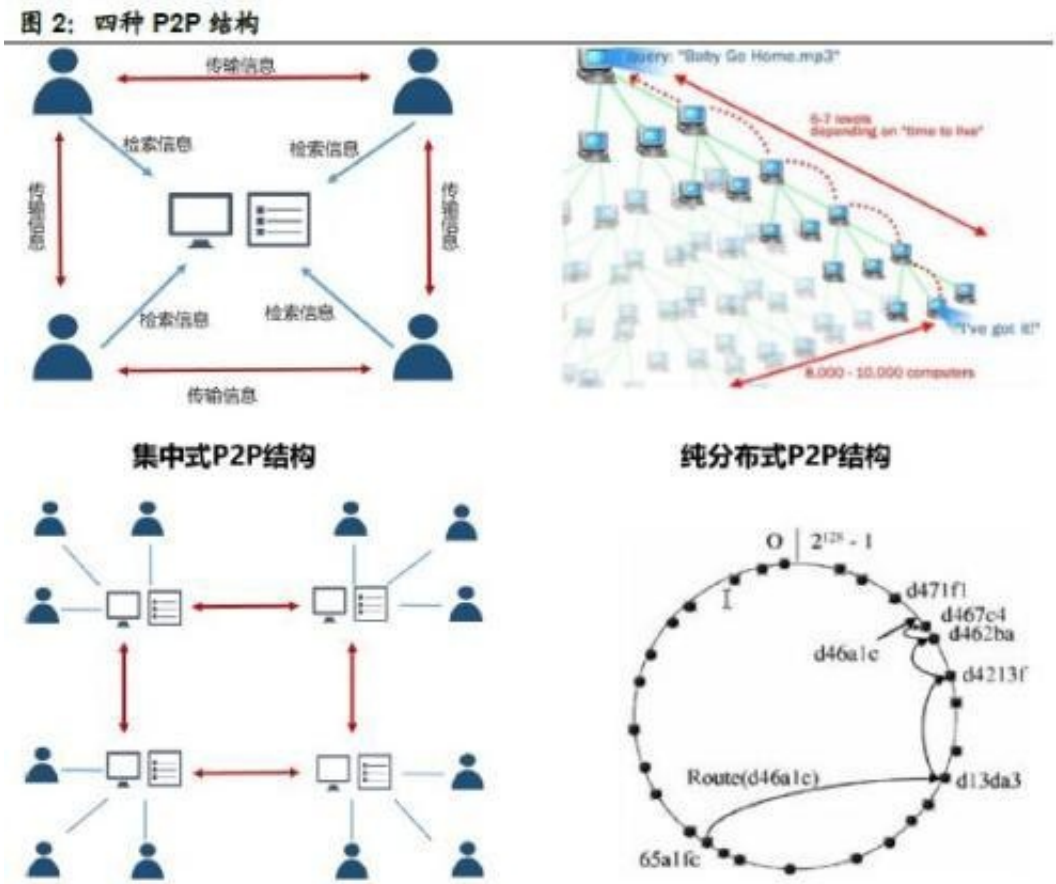
数字货币的产生及应用涉及复杂的底层技术，在梳理其发展历史之前，通俗的理解这些技术是必要的。

与名噪一时的比特币等数字货币一起声名鹊起的，莫过于区块链技术。也正因为区块链经常与比特币一起出现，所以很多人容易将两者混淆，更有甚者认为区块链就是比特币。

事实上，比特币只是区块链技术的一个具体应用，区块链不仅可应用于比特币等数字货币，还可以应用于所有数字化的领域，如数字票据、征信、政务服务、医疗记录等。
数字货币也不一定应用区块链技术，我国央行相关人员也多次指出“法定数字货币未必使用区块链技术，区块链只是央行数字货币备选的底层技术之一”。那么，区块链技术究竟是什么呢？

当前，对于区块链的定义，业界尚未有唯一的明确答案。

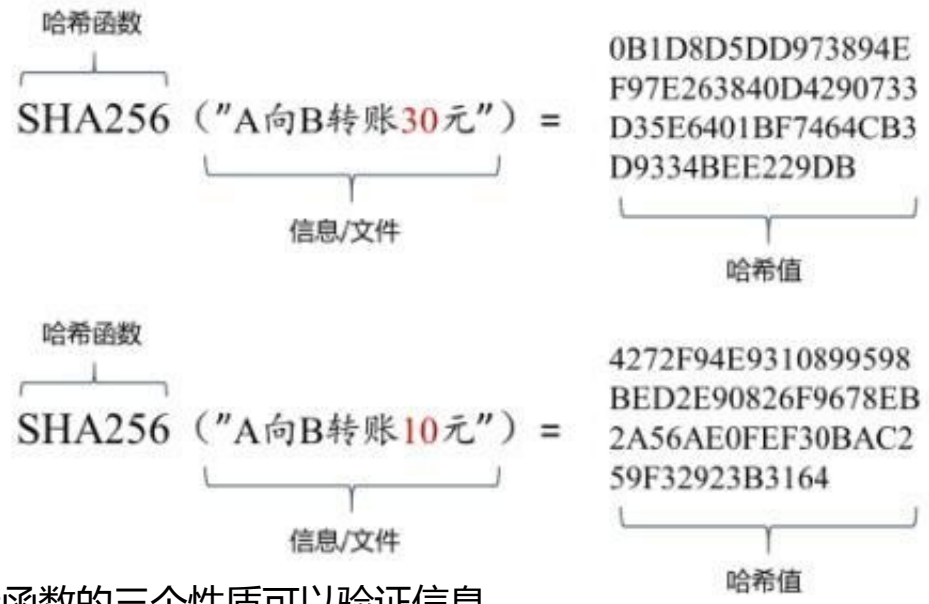
从形式上看，区块链（BlockChain）是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构。
每个区块（Block）主要包含三个部分：1）数据信息，具体的信息类型与区块链协议规定相关。例如，在比特币系统中是转账信息，包括付款人、收款人、比特币数量等。2）哈希值，表明区块内包含的所有信息。3）哈希指针，包含上一个区块的哈希值，表明上一个区块的信息。哈希指针可以将区块一个个连接起来形成“区块链”。




P2P技术解决了点对点之间数据传输问题，而分布式存储解决了去中心化系统中数据储存的问题。
在传统的储存方式中，所有数据都集中储存在一个中心化的节点中，而在P2P网络

中，不存在中心化节点，需要使用分布式存储技术。简单来说，分布式存储就是将数据存储在多个计算机节点中。应用到区块链中，即各节点进行信息传输时，需要将该信息广播在系统中，收到信息的节点均储存该条信息。

图 4：哈希函数转换示意图




哈希函数的三个性质可以验证信息
是否被篡改，
具体流程如下：首先，发送者将信息输入哈希函数，得到一个哈希值，并将哈希值用私钥加密。其次，发送者将原始信息、加密的哈希值以及公钥一起发送给接收者；最后，接收者收到后用公钥将哈希值解密，并将原始信息输入哈希函数，将得到的哈希值与收到的哈希值对比，即可验证原始信息是否在传输过程中遭到篡改。

图 6：区块链工作量证明共识机制流程图


PoW的意义在于增加了各节点广播信息的成本，且该成本远大于发布虚假信息的收益，各节点就不会有做“叛徒”的动机。
因为如果节点对信息有任何的修改，就会完全改变哈希值，哈希函数虽不易逆解但容易验证，当无法通过51%节点的验证时，该节点必须重做工作量证明，既会花费大量成本，又会降低率先完成的概率从而降低获得奖励的概率。其次，由于率先算

出谜题的节点是随机的，所以我们无法得知下一个争得记录权的节点，各节点也无法掌控自己将获得哪个区块的记录权。

以上过程通过PoW机制解决了单个区块内信息储存的共识问题，但不能保证系统（整个区块链）的最终一致性。
因为两个不同节点同时挖出区块（解出谜底）的情况也可能出现（由于网络通信问题，每个节点的区块信息可能不一致），这时区块链会出现分叉，网络各节点需要对哪条区块链上的交易能够得到确认形成共识。

整条区块链的共识遵循最长链原则，只有最长链上的交易能够得到确认，也就是包含的工作量最大的那条区块链。
“分叉链”不可持续，在下一次区块竞争时，每个节点会选择在某条分叉链上进行下一次记账权的竞争，由于存在巨大的工作量证明，同一时间内两个节点同时挖出区块的概率将呈指数级下降，因此，很快就会有“最长链”出现，最长链上的交易将获得确认，同时，较短链上的交易信息也会随之释放，重新标记为“未确认”，打包在下一个区块中。

图 8：比特币能源消耗


（3）权益证明——以太坊区块链的共识机制

权益证明机制（Proofof Stake，简称PoS）是对PoW机制的改进，与节点需要做计算工作证明不同，PoS按照各节点拥有的密码货币的数量和时间竞争记账权，这

这种机制类似于利息制度，PoS算法中有一个名词叫做“币天”，是货币数量与持有天数的乘积（例如若持有100个密码货币10天，则币天为1000），各节点每发现一个区块，拥有的币天就会被清零，每清空365个币天，可获得一定数量的新币奖励（相当于持币利息）。

PoS作为PoW的一种升级共识机制，成功地改进了PoW机制的一些缺陷。1）低延迟：根据每个节点所持有代币的数量和时间，等比例的降低挖矿难度，在一定程度

上缩短了共识达成的时间。2）资源消耗少：不再需要消耗大量能源进行计算。