区块链技术是中本聪在2008年发布的比特币系统白皮书《比特币:一种点对点的数字货币系统》中提出的底层核心技术，是一种结合了分布式存储，一致性共识和密码学等多方面知识的应用技术[1]。区块链最大的特点在于实现了摆脱第三方信任机制的交易系统，在该系统中交易的确认由所有节点共同参与完成，数据采用分布式存储方式，存储到区块中。区块与区块相互链接形成区块链。

2.1.1 区块链中的交易

区块链中的交易的生成是由用代币的拥有者基于私钥对该代币的上一次交易以及本次交易的接受方签署数字签名。该数字签名被附加在代币的末尾形成交易单，然后被广播到区块链网络中的其他节点。在网络中的节点收到交易清单后会开始对该交易进行验证，以PoW(Proof of Work)为例，节点进行开始被称为挖矿的复杂hash运算操作，首先完成交易验证工作的节点将所有的交易进行打包并广播给其他节点。当网络中的其他节点收到该区块后验证其时间戳以及交易是否有效，在确认签章有效以及没有重复花费后再将区块上链，此后数据无法更改。综上所述，在区块链网络中，一个交易的完成过程包括交易的发出、数字签名的广播、共识算法验证交易的正确性、打包区块、验证区块链和上链六个步骤。区块的结构如图2.1所示，其中最重要的信息包括前一个区块链的哈希指针和本区块的哈希值、时间戳、完成本区块打包工作的节点(Miner)的账户等信息。图2.2为某区块的实际示例。

2.1.2

以太坊系统是一种无需中央管理和协调机制的分布式系统，该系统可以运行智能合约和小型应用，其创造者的初衷是开发一套可以自治的“世界计算机”。它在比特币的基础上更进一步，不仅可以在全网节点上验证和存储交易数据，还可以在全网所有节点中运行智能合约代码，节点使用EVM(Ethereum Virtual Machine)运行智能合约。以太坊同时具有分布式数据存储和计算的能力。

以太坊的使用是通过以太坊客户端(Ethereum client, Geth)实现，用户通过以太坊客户端连接以太坊网络中的其他节点，并参与区块同步、挖矿、交易验证的工作。以太坊上的所有节点地位相同，同时没有中心协同和管理节点。在成为以太坊节点后可以进行连接以太坊网络、查看以太坊区块链、发布交易和智能合约、运行智能合约以及挖矿等工作。

智能合约是以太坊提供的可以运行在EVM(Ethereum Virtual Machine)中的图灵完备语言。相对于比特币的原始脚本语言，它更高级，同时其图灵完备性意味着它可以被用来实现任何功能或者执行任和计算。通常，智能合约在Dapp(Distributed Application)中被用于定制化代币或交易等操作。