1. 去中心化

区块链从功能上来说就是实现分布式账本，账本可以反映多个不同地理位置的节点或者多个机构组成的网络里进行共享的数据。在分布式账本的模式下，没有中心服务器也不需要中心服务器存储账本，原因是每一个节点都能够存储一个真实账本的副本，具体的实现是：在分布式网络中存在一种机制，在这种机制下首先会生成一个网络中唯一的真实账本，在生成真实账本的同时所有的节点都会生成一个与其完全相同的副本账本。在真实账本中的任何数据的改动都会在所有的副本中被反应并同步，同步所需的时间会在几分、甚至几秒之内。

通过由区块链实现的分布式账本可以完全取代传统的由中心服务器处理并存储所有节点数据的工作模式，实现了一种去中心化的新的工作模式。网络中的任意两个节点之间都是平等的，它们有着相同的整个网络中所有的数据，任意两个节点之间的通信也不再需要借助于第三者的参与，最后在通信结束后两个节点数据的更新会被网络中其它的所有节点更新到自己的账本中。同时整个网络中任一个节点停止工作都不会影响系统整体的运作，这使得整个系统具有极好的稳定性。

1. 多层级

区块链是多层级的,它的基础架构可以分为四层，包括数据层、网络层、区块链层和应用层。每一层分别完成不同核心的功能，各层之间互相配合，从而实现了一个去中心化的信任机制。

数据层我们可以理解成数据库，对于区块链来讲，这个数据库是不可篡改的、分布式的数据库，也就是上述的“分布式账本”，主要可实现两大功能：数据存储、账户和交易的安全。数据层主要描述区块链的物理形式，是区块链上从创世区块起始的链式结构，包含了区块链的区块数据、链式结构以及区块上的随机数、时间戳、公钥、私钥数据等，是整个区块链技术中最底层的数据结构。

网络层来实现区块链节点之间的信息交流。主要通过P2P技术实现分布式网络的机制，网络层包括 P2P 组网机制、数据传播机制和数据验证机制，因此区块链本质上是一个P2P（点对点）网络，具备自动组网的机制，节点之间通过维护一个共同的区块链结构来保持通信。每一个节点既接收信息，也产生信息。

区块链层中，包含了共识机制、激励机制、智能合约这三种重要技术，其中共识机制是该层的核心。在区块链中的共识，即是要求整个网络要依据所有节点一致同意的更新数据的规则，来维护更新区块链系统中的真实账本。共识算法以及共识机制，能让高度分散的节点在去中心化的区块链网络中高效地针对区块数据的有效性达成共识; 激励机制主要包括经济激励的发行制度和分配制度，其功能是提供一定的激励措施，鼓励节点参与区块链中安全验证工作，并将经济因素纳入到区块链技术体系中，激励遵守规则参与记账的节点，并惩罚不遵守规则的节点；智能合约体现为存储在区块链上的一段代码，能在达到某个确定的约束条件的情况下，无需经由第三方就能够自动执行

智能合约主要是用于代替人去仲裁区块链中的各种交易，从而避开第三者使得网络中的两个节点能够直接进行交易，为我们节省巨额的信任成本。

1. 去信任

在网络环境中，任意两个互不相识的设备要进行数据的交易是具有极高风险的。必须通过双方都信任的第三方的信任中介的担保，才有可能建立起有限程度的信任，而且这种信任，将随着双方对第三方信任程度的变化而变化，因为不能保证信任中介总是能够对交易做出正确合理的判决。

区块链系统中，所有运行在系统中的节点通过数字签名进行验证，无需第三方认证也可交易，从而实现了业务交往中点到点信任关系的建立。这种有区块链系统建立的点到点信任一般可以分为两个方面：交易的安全性和交易的隐私性。

安全性建立在利用技术手段实现的链上数据的真实性有效性和数据不可篡改不可伪造的特点之上。

区块链通过非对称密码，实现了每个个体在区块链系统中（可以是匿名）的身份认证，由于其他人难以伪造他人的数字签名，因此也就难以伪造相关的数据内容。

区块内数据记录完成之后，负责者会对当前区块内容打包，计算出当前区块内所有数据的哈希值，并将这个哈希值记录在下一个区块的头部。哈希函数的性质保证了记录到区块上的数据的完整性，一旦数据被篡改，接受者只要重新验算一遍哈希函数，并对验算之后的哈希值做比较，就可以发现数据被改动的事实。同时由于区块链上的数据不仅仅保存在一台计算机上，而是所有的数据会在全网范围内的所有节点上都做一个完整的备份。因此即使个别人可以改变一两台计算机上的数据，但也没有办法对全网所有节点上的数据进行同步改变。如果某一节点的数据得不到网络中多数节点的认可，那么就会被认为对数据进行了恶意篡改，其他节点会拒绝接受这些被篡改的数据。由于在区块链化之后，每一节点都必须对上链的信息和数据资料负责。因此我们可以对那些进行数据篡改的节点进行溯源和定位。

隐私性借助于区块链的非实名上链与密码学实现。在互联网时代下，用户的个人隐私泄露成为了一个严重问题，用户通过网络传递的各种个人信息、邮件等，都随时处于可能被监听的状态。这种个人隐私泄露本质是由于用户在网络中的实名性造成的。

在区块链的分布式网络中，每个节点在网络中进行通信时具有非实名性，使用者无需使用真名，而是采用公钥哈希值作为交易标识，而公钥哈希值就可以代表使用者的身份，与真名无关。尽管通过溯源性可以追查到通信和交易记录，但是对于交易者是谁是不可知的。这些信息只有持有私钥哈希值的节点本人才能查询。

1. 可扩展性

随着区块链技术的普及，主流公链如BTC、ETH的交易数量不断增加，以及ETH链上部分现象级DApp的火爆，区块链网络拥堵现象逐渐显现。公有区块链出于非中心化与保证网络安全的考虑，形成了一定的共识机制，同时对区块间隔时间和区块体积大小有所限制，从而能够处理的交易数量不足以支撑高并发的应用。

为了能将区块链大规模应用于实际场景就必须对区块链进行扩容。区块链领域的扩容即围绕如何在“更短的时间实现更多的交易”，增强区块链的可扩展性。而可扩展性是指系统、网络或进程处理越来越多的工作的能力，或者适应增长而扩展的潜力。

目前已经提出的扩容方案包括三类，分别针对区块链逻辑架构的不同层级进行改进。三类扩容方案分别为第0层扩容、链上扩容和链下扩容。

链上扩容通过改变基本协议提升区块链效率。链上扩容方案又包括数据层改进方案、共识层改进方案和网络层改进方案，基本思路是增加区块大小（直接以及变相）或减少区块验证传播时间和形成共识时间。

链下扩容不改变基本协议，在应用层进行改变提升扩展性。链下扩容方案主要有状态通道、侧链、跨链和链下计算四种方式，思路均为将部分链上交易转移到链下执行，减轻链上处理压力，提升整体效率。

第0层扩容通过改变区块链底层数据传输协议提升区块链可扩展性。

每一种方案都对改善区块链的可扩展性提供了解决方案，针对不同的应用场景与需求，选择适合的区块链扩容技术或是解决目前区块链网络拥堵问题的主要途径。