**技术先进性**

**1、区块链用了哪些技术：**

**（1）、安全散列算法（SHA256）**

安全散列算法SHA（Secure Hash Algorithm）是美国国家安全局 （NSA） 设计，美国国家标准与技术研究院（NIST） 发布的一系列密码散列函数，包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 等变体。主要适用于数字签名标准（DigitalSignature Standard DSS）里面定义的数字签名算法（Digital Signature Algorithm DSA）。

在比特币区块链中，每一个区块都指向上一个区块，这些通过SHA256计算的区块哈希链就是比特币账本不可篡改的基础。

在一个区块中，比特币系统用交易（Transaction）来表示一笔比特币交易。一个区块包含至少一笔交易。这些Transaction的Hash通过Merkle Tree计算出所有交易的Merkle Hash，并被包含至区块Hash中，从而实现交易的不可修改。

**（2）、智能合约**

智能合约能够使用一种透明的方式来转移和交换资金或财产，而不需要通过中间人。与传统的合同一样，智能合约也定义了此协议中的所有义务和潜在惩罚，但是智能合约平台能够自动强制执行所有的这些义务与惩罚。这些智能合约平台允许这些去中心化的应用在它的网络上运行。

智能合约的基本理念是，许多合约条款能够嵌入到硬件和软件中。

**（3）、加密算法（ECC）**

密码技术是网络安全的基础，也是核心。现在对隐私保护、敏感信息尤其重视，所以不论是系统开发还是App开发，只要有网络通信，很多信息都需要进行加密，以防止被截取篡改。

椭圆加密算法（ECC）是一种公钥加密体制，最初由Koblitz和Miller两人于1985年提出，其数学基础是利用椭圆曲线上的有理点构成Abel加法群上椭圆离散对数的计算困难性。

椭圆曲线密码体制是目前已知的公钥体制中，对每比特所提供加密强度最高的一种体制。椭圆密码体制有以下优点：

1)安全性高:有研究表示160位的椭圆密钥与1024位的RSA密钥安全性相同。

2)处理速度快:在私钥的加密解密速度上，ecc算法比RSA、DSA速度更快。

3)存储空间占用小。

4)带宽要求低.

**（4）、P2P网络**

对等网络，即对等计算机网络，是一种在对等者（Peer）之间分配任务和工作负载的分布式应用架构[1] ，是对等计算模型在应用层形成的一种组网或网络形式

对等网络是一种网络结构的思想。它与目前网络中占据主导地位的客户端/服务器（Client/Server）结构（也就是WWW所采用的结构方式）的一个本质区别是，整个网络结构中不存在中心节点（或中心服务器）。在P2P结构中，每一个节点（peer）大都同时具有信息消费者、信息提供者和信息通讯等三方面的功能。从计算模式上来说，P2P打破了传统的Client/Server (C/S)模式，在网络中的每个节点的地位都是对等的。每个节点既充当服务器，为其他节点提供服务，同时也享用其他节点提供的服务。

**（5）、数据库（leveldb、Berkeley DB）**

1）、leveldb简介

leveldb是google实现的单机版k-v存储系统，可按照字符串键值顺序映射进行存储，具有以下几个特点：

首先，LevelDb是一个持久化存储的KV系统，和Redis这种内存型的KV系统不同，LevelDb不会像Redis一样狂吃内存，而是将大部分数据存储到磁盘上。

其次，LevleDb在存储数据时，是根据记录的key值有序存储的，就是说相邻的key值在存储文件中是依次顺序存储的，而应用可以自定义key大小比较函数，LevleDb会按照用户定义的比较函数依序存储这些记录。

再次，像大多数KV系统一样，LevelDb的操作接口很简单，基本操作包括写记录，读记录以及删除记录。也支持针对多条操作的原子批量操作。

另外，LevelDb支持数据快照（snapshot）功能，使得读取操作不受写操作影响，可以在读操作过程中始终看到一致的数据。

除此外，LevelDb还支持数据压缩等操作，这对于减小存储空间以及增快IO效率都有直接的帮助。

2）、Berkeley DB（BDB）是一个高性能的嵌入式数据库编程库（引擎），它可以用来保存任意类型的键／值对 (Key/Value Pair)，而且可以为一个键保存多个数据。Berkeley DB可以支持数千的并发线程同时操作数据库，支持最大256TB的数据。

BDB提供诸如C语言，C++，Java，Perl，Python，Tcl等多种编程语言的API，并且广泛支持大多数类Unix操作系统和Windows操作系统以及实时操作系统（如 VxWorks）。

**2、末来技术发展的方向：**

**（1）、隔离验证**

隔离验证其实就是把原来的比特币交易中签名的部分单独拿出来放到另一个叫 witness 的结构中。

交易是交易，签名是签名，对于交易来说，只关心 TxIn 和 TxOut 就好了，我们都清楚一个比特币交易其实就是花一笔之前收到的钱，也就是说要用之前收到的 TxOut 作为这一笔交易的 TxIn 然后发给后续的 TxOut，隔离之后的交易结构使得当您决定好花哪一笔钱、要花给谁的时候，交易的内容就已经是确定了的，交易的数据就不会再发生改变了，最终的 tx\_id 也就是不变的了。想要验证签名？那就去 witness 里找到对应的签名数据验证一下合法性即可，又简单、有没有交易延展性的问题。

隔离验证对于所有的基于比特币区块链的扩展应用（甚至包括交易所和钱包等）都有好处，精确的 tx\_id 当然会让很多基于 tx\_id 所扩展出来的应用都容易的多，也可靠的多。

隔离验证其实是对之前不太合理的比特币交易结构的一次优化，开发者们试图用一种影响尽可能小的、尽可能向下兼容的、“软分叉”的方式来实现，这种改进本身（就像是“压缩格式的公钥”一样）是非常合理的，与块大小之争没什么直接的关系。

**（2）、闪电网络**

在2015年年初，约瑟夫•朴恩（Joseph Poon)和萨帝厄斯•追亚（Thaddeus Dryja）发布了闪电网络白皮书，标志闪电网络的诞生。闪电网络（Lightning Network）是一个去中心化的系统。闪电网络的卓越之处在于，无需信任对方以及第三方即可实现实时的、海量的交易网络。闪电网络的创建者预计这种网络最终将能够每秒处理数十亿笔交易。

隔离验证解决的是比特币交易延展性问题，解决的是比特币长期存在的一些技术问题，闪电网络才是core开发组解决扩容问题核心，把主链上的交易转移到闪电网络上进行处理，从而解决比特币交易拥堵的问题，比特币区块链只是作为一种备用的处理系统，当有人作恶时才能起到作用。

**（3）、高频交易处理（石墨烯技术）**

可参考ETH和EOS的对比：

目前以太坊网络受限于CPU的单线程性能。早期的测试网络达到每秒25次交易(还是在优化了的情况下)，经过优化，可以增加到50次 或 100 次交易/秒。然而，在实际应用中，以太坊网络的交易差不多是10次交易/秒，甚至更少。之前，网络甚至被淹没堵塞，使得只有那些交易费最高的交易能够执行，其他的都被拒绝。这一点在最近的ICO中尤为明显，比如Status 的ICO，在这次ICO中，以太网络完全被堵塞，eth出现了大面积崩溃。

EOS相对与以太坊有两个显著优势，一旦实现，EOS将成为能处理真正商业级去中心应用的唯一平台。第一，EOS将依赖于石墨烯技术，在压力测试中，石墨烯技术已能达到每秒10,000-100,000笔交易。第二，EOS将使用并行技术来拓展网络，处理能力将到达每秒百万笔交易。

**（4）、零知识证明（ZCash）**

零知识证明 （被称为“zk-SNARK”）是实现Zcash的匿名特性的核心技术。“零知识证明”的定义是：证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

Zcash 使用一个被称为 zk-SNARK 的零知识证明架构，该架构是由我们的经验丰富的密码学家团队 开发的。这个框架允许网络在不公开交易参与方或者交易数额的情况下维护一个安全的账户余额账本。Zcash 交易的元数据是加密的，而不是公开地展示交易参与方和交易数额，zk-SNARK 被用来证明没有人进行欺骗或者偷窃。