对于区块链技术而言，比特币只是一个开始。

目前市场上已经发行了
500多种数字货币，共占有了27,845.399亿元的市值，其中的40.97%
的市值都归比特币所有，可想而知，比特币作为区块链应用中备受关注的一个，从发行之日起已经成功运行了 8 年。这个结果说明，这项具有革命性的新技术是可信而且稳定的。并且引领了一场包括货币体系、 金融服务、 经济学、 分布式系统、投票系统、 联合监管和合同体系在内的创新浪潮。

自2009年比特币诞生以来，关于区块链底层技术的创新就从未停止。

为了更好的理解这些技术创新，在介绍这些之前，我们先来简单解释一下比特币的关键技术。

区块

一个区块就是若干交易数据的集合。区块头经过哈希运算后会生成一份工作量证明，从而验证区块中的交易。 有效的区块经过全网络的共识后会被追加到主区块链中。比特币系统中平均每个区块至少包含超过500个交易。

共识机制

由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识。

工作量证明

通过有效计算得到的一小块数据。 具体到比特币，矿工必须要在满足全网目标难度的情况下求解SHA256算法。优先完成工作量证明的矿工可以获得比特币奖励。

如上图所示，比特币系统由用户[用户通过密钥控制钱包]

、交易[交易通过节点被广播到整个网络]
和矿工[通过共识机制和工作量证明产生新的区块] 组成。

区块链技术的5项重大创新

在理解比特币的一些基本技术的基础之上，接下来我们主要来了解一下那些在区块链底层技术上的重大的里程碑式的创新。所有的创新都是基于比特币的区块链技术而做出的改进，主要包含：

- 对比特币协议层的创新
- 对货币属性的创新
- 对共识机制的创新
- 对挖矿算力的创新
- 对智能合约的创新

对比特币协议层的创新：彩色币(coloredcoin)

“染色币”或者“染色币”是一种在少量比特币上存储信息的一种元协议。一个彩色币是用于表达另一种资产的比特币。彩色币可以用作替代货币、商品证书、智能财产以及其他金融工具。彩色币本身就是比特币
，存储和转移不需要第三方，可以利用已经存在的比特币的基础。

区块中的第一笔交易是笔特殊交易，称为创世交易或者coinbase交易，只有在这里才有空间可以存储字符信息或者标记。中本聪就在创世区块的Coinbase交易的输入中包含这样一句话“The Times 03/Jan/2009 Chancellor onbrink of second bailout forbanks.” “彩色币”就是在这里被标记成具有其他意义的货币，而被转移到特殊的钱包地址上。

应用举例

可以创建20单位带有元信息“MasterBTC”的染色币，
其中“MasterBTC”代表了可以获取本书免费拷贝的兑换码。
每一单位的这种染色币， 都可以被出售或赠予给任何装有兼容染色币协议钱包的人，拥有这种染色币的人可以继续转手或者用它来兑换本书的免费拷贝。

对货币属性的创新

比特币的总量固定为2,100万枚，新币的生成速度随时间递减，区块生成速度为十分钟，这个频率也控制了整个比特币系统交易的确认速度和新币的生成。所以，比特币是总额固定且不通货膨胀的货币。很多其他种类的货币对总量、区块时间等属性进行调整而产生不同货币政策的货币。

其中的典型代表是：莱特币（Litecoin）、狗狗币
（Dogecoin）和弗雷币
（Freicoin）。它们有着更快的出块速度和更多的货币总量。狗狗币的出块速度达到了60秒，货币总量达到了1000亿。

对共识机制的创新

比特币区块链采用了 Proof of Work（ PoW）工作量证明的机制来实现共识。矿工通过计算来猜测一个数值，保证在一段时间内，系统中只能出现少数合法提案。所以，比特币的新区块产生速度为10分钟，就是在进行工作量证明的数学计算。比特币通过工作量证明机制很好的解决了一致性问题，使得比特币网络中的所有节点对有效的交易达成共识。在2013年，作为工作量证明的一种替代机制，权益证明（PoS）应运而生，成为现代竞争币的基础。

权益证明的典型方式：通过保证金如代币、资产、名声等具备价值属性的物品来对赌一个合法的区块成为新的区块，收益为抵押资本的利息和交易服务费。提供证明的保证金（ 例如通过转账货币记录）
越多，则获得记账权的概率就越大。合法记账者可以获得收益。

权益证明（Proof of Stake）系统中，货币的所有人可以将自己的通货做利息抵押。参与
者可以保有他
们货币的一部分，通过利息
和矿工费的方式获取回报。
权益证明是试图解决在工作量证明中大量算力资源被浪费的缺点。

其中典型的代表是：

Peercoin（点点币）

于2012年8月发布， 是首款工作量证明和权益证明混用的竞争币

出块速度：10分钟

货币总量：没有上限

Myriad（多彩币）

同时使用5种工作量证明算法（ HA256d, Scrypt, Qubit, Skein, or MyriadGroestl），根据参与矿工的情况动态选择。这是为了让整个Myriad系统不受集中化的ASIC矿机的影响，同时也加强了其抵御一致性攻击的能力。

出块速度：平均30秒

货币总量：到2024年达到 20 亿

NXT（未来币）

一种只采用权益证明的竞争币， 它甚至不采用工作量证明的挖矿机制。 NXT是一款完全自己实现的加密货币，并非衍生自比特币或其他竞争币NXT具有很多先进的功能，包括名字注册、去中心化资产交易、集成的去中心化加密信息和权益委托。

出块速度： 1分钟

货币总量： 没有上限

对挖矿算力的创新

一些比特币的批评者认为挖矿这一行为是一种毫无意义的浪费。新一代的加密货币试图解决这个争议， 多目的挖矿算法就是为了解决工作量证明导致的“浪费”问题而出现的。赋予这些原本无意义的工作量证明计算新的需求参数。其中的典型代表是：

Primecoin(XMP) 质数币/素数币

Primecoin是在2013年7月发布的。它它的工作量证明算法可以搜索质数，计算孪生素数表。在用于维护公共交易账簿的同时，还会产生一份公开的科学发现（素数表）。

出块速度：1分钟

货币总量：没有上限

一致性算法：含有素数计算功能的工作量证明算法

Curecoin

它将SHA256工作量证明算法和蛋白质褶皱结构的研究结合了起来。
蛋白质褶皱研究需要对蛋白质进行生化反应的模拟， 用于发现治愈疾病的新药，但这一过程需要大量的计算资源。

一致性算法：含有蛋白质结构研究功能的工作量证明算法

对智能合约的创新：以太坊（Ethereum）

> 以太坊（Ethereum）被誉为区块链2.0，由于其在智能合约上的重要创新，在这里我们不得不提及，以太坊将区块链的应用层面推向了一个新的高度。

根据以太坊官方的宣称，以太坊（Ethereum）目标是打造成一个运行智能合约的去中心化平台 Platform for Smart Contract ，平台上的应用按程序设定运行，不存在停机、审查、欺诈、第三方人为干预的可能。以太坊平台由 Golang、C++、Python 等多种编程语言实现。

以太坊提供了一条公开的区块链，并制定了面向智能合约的一套编程语言。智能合约开发者可以在其上使用官方提供的工具来开发支持以太坊区块链协议的应用，即所谓的DAPP。

应用举例

智能合约如同一纸不可更改的合同，并且一旦合同约定的条件达成，会自动履行这份协议。一个典型的应用举例是有提现限额的储蓄钱包：

假设隔壁老王想确保其资金安全，他担心丢失或者被黑客盗走私钥。于是把以太币放到和老李签订的一个合约里，如下所示：

- 老王单独每天最多可提取1%的资金；
- 老李单独每天最多可提取1%的资金，但老王可以用私钥创建一个交易取消老李的提现权限；
- 老王和老李一起可以任意提取资金；

有了上面这样的智能合约，每天1%对隔壁老王来说已经足够了，如果他想提现更多可以联系老李一起提取。如果老王的私钥被盗，他也可以立即联系老李把资金转移到新的合同。如果老王弄丢了私钥，老李也可以帮他把钱一点点提出，并且如果老李出现了违背合约的意图，老王可以随时关闭老李的提现权限。如此，老王的资金在这样合约下就得到了妥善的保护。

总结

> 对于区块链技术而言，比特币只是一个开始，如同其他一切新兴技术一样，比特币有着许多尚未解决的问题，但稳定运行了8年的比特币网络给了这项技术足够的信心，创新每天都在继续。

这篇文章从技术创新的角度分析了一些数字货币的创新技术，由此可见，我们在看待数字货币的时候，不应该被数字货币的铜臭味和投资者的疯狂而蒙住双眼，去拒绝深度而且认真的审视和研究这项技术。

对于区块链技术，这样的创新仍在继续，或许疯狂的投资市场正是将这项技术推向落地应用的关键因素，虽然它充满了争议，如此才不至于让区块链在学术派的象牙塔中老死，而是真正应用去解决人们的需求和问题。

本文由 @ 区块链老垚 原创发布于人人都是产品经理。未经许可，禁止转载。

题图来自Pixabay，基于CC0协议