除了区块奖励减半之外，您是否想了解一下2020年比特币其他发展情况呢?是的，看到这篇文章，就说明您来对地方了，区块链是目前 LinkedIn 上排名第一的工作技能，所以你绝对应该了解更多有关这一领域技术发展的信息，或许能让你未来求职道路走的更轻松一些。

在过去的一年时间里，比特币技术已经获得不错的发展，那种这种趋势会在 2020 年继续延续下去吗?MAST、Taproot、Schnorr 签名、以及其他出色的技术是否能进一步改善比特币安全性、并推动其价格升值吗?

2020年的比特币

最近几年，在比特币核心协议上工作的高质量开发人员和具有创新意识的开发人员数量越来越少，这也引发了部分社区的指责。

但是，如果你真切关注下“引擎盖下发生的情况”，会发现其实许多有趣的功能正在浮出水面。尤其在过去的几年时间里，比特币区块链已经添加了不少令人兴奋的新功能，而且已经计划在 2020 年推出更多新功能了。举个例子，区块链技术公司 Blockstream 在 2019 年发布了 Miniscript，这是一个针对比特币的全新脚本编译器，旨在确保安全性的前提下提升比特币区块链的可编程性。

其他最新的比特币技术提案还包括：

1、Schnorr(一种全新的签名方案);

2、MAST(一种全新的 Merkle 树数据结构);

3、Taproot(一种允许全体参与者就结果达成一致并签署和解交易的方法)。

仅这三个方面的发展，就能大大改善比特币的可替代性和隐私保护功能。因此在本文中，我们就探讨一下这三个主要技术的工作原理，以及在比特币上实施部署之后会给社区带来哪些期望。

1、MAST

MAST，即默克尔抽象语法树(Merkelised Abstract Syntax Trees)，提供了使用所有链接到同一默克尔树(Merkle tree)不同脚本的P2SH来锁定比特币的功能，该技术由Blockstream开发人员 Russell O'Connor、Peter Wuille 和 Peter Todd 开发。

星球君(微信：o-daily)在此首先介绍一下默克尔树，它是一种二叉树，包含了一组节点，含有基础信息的树根拥有大量的叶子节点，一组中间节点，每一个节点都是它的 2 个子节点的哈希。然后，终根节点由 2 个子节点的哈希形成，代表着这树的“顶端”。默克尔树的目的是允许在一个区块中的数据能够被零散的传递:
一个节点只能从一个源来下载一个区块的头信息，树的一小部分关联着另一个源 ，并且仍然可以保证所有数据都是正确的。之所以这样做行得通，是因为哈希值都是向上传导的: 如果一个恶意用户试图在默克尔树的底部替换一个假交易, 这个更改将导致上面的所有节点发生变化，上面节点的变化又会导致上上面的节点发生变化，最终改变数根节点，因此也就改变了该区块的哈希，导致区块链协议将其注册成一个完全不同的区块，这样恶意用户所做的，基本可以肯定是一个无效工作量证明了。简单来说，默克尔树就是设计比特币数据结构技术的一种方式，它是一种数学结构，可将不同数据集散列到单个哈希中。

P2SH 是“Pay to Script Hash”的首字母缩写，是一种支持比特币支付的高级脚本，只需列出创建包含脚本的地址路径，用户就能锁定在在脚本(输出)中的比特币，而这些比特币能够沟通正确密钥(哈希)解锁。脚本无非是每笔交易中记录的一系列指令，这些指令将描述交易方(peer)如何解锁这些比特币。

本质上，MAST是结合了默克尔树技术的P2SH。使用MAST，可以将同一组比特币(一个输入)链接到许多包含不同条件的脚本，以解锁这些比特币。MAST
扩展了比特币智能合约灵活性，提高了可扩展性，并增加了隐私。

2、Taproot

Taproot
创建签名输出，其中包含有关满足条件时会发生的情况说明。本质上，Taproot 技术赋予了比特币网络中添加类似智能合约的功能，用户可以通过输出为简单付款交易的脚本，在交易里添加逻辑。

Taproot 最好与 P2SH 功能配合使用，因为它假定您要将脚本拆分为分离的语句集合，因此它仅显示要使用的脚本部分。Taproot 允许签收者仅显示分支的日志范围数，由于不需要额外存储要求，因此为用户提供了更多隐私并增加了可扩展性。

Taproot技术的另一个作用是使比特币交易在任何区块链浏览器上看起来都完全相同，从而无法分辨交易之间的区别，因此大大提高了比特币的隐私性。可以想象，Taproot通过将多个签名聚合为单个签名，这样就能使Schnorr签名效率更高。事实上，正如 Taproot 背后的开发人员 Greg Maxwell 所解释的那样，Taproot 就是 Schnorr 签名与 MAST 之间的完美连结。

这里提到的 Schnorr
签名，其实就是我们下一章节中即将介绍的一个令人兴奋的全新签名聚合方案。

3、Schnorr 签名

Schnorr 是一种全新的签名聚合方案，由德国密码学家 Claus-Peter Schnorr 于 20 世纪 80 年代发明，之后这个签名技术被发现非常适合应用在比特币上。在该签名聚合解决方案的支持下，所有交易输入签名将会被合并成为一个，我们不再需要多重签名，而是只要一个聚合签名即可。

那么，多重签名和聚合签名之间有什么区别呢?实际上，两者的区别仅在于在聚集签名方案中，每个签名者都有自己的消息，而不是所有人共享的一个消息。验证人查看签名密钥时，Schnorr 签名不会释放有关输入的任何信息，因此所有外部查看者的交易输出看起来像是常规地址，但能够解锁地址中脚本的唯一人员将是相应私钥的所有者。

借助 Schnorr 签名和签名聚合技术，可以创建智能合约功能，并将包含“如果这样/那么那样”的逻辑整合到签名支付条件中。

最后，与传统 ECDSA 签名相比，Schnorr 签名更易于验证，也能提供更高程度的鲁棒性、正确性和灵活性。(星球君注：鲁棒是Robust的音译，即健壮和强壮的意思，通常指在异常和危险情况下系统生存的能力。所谓“鲁棒性”，是指控制系统在一定(结构，大小)的参数摄动下，维持其它某些性能的特性。)这些功能会在 2020年或 2021年通过软分叉添加到比特币吗?