1. 以太坊的共识机制将经过怎样的发展转变过程?转变完成后，将对以太坊挖矿产生怎样的影响?

Casper是将Ethereum主网共识算法从Proof of Work(POW)顺利转向Proof of Stake(POS)的实施方案。Casper由两个项目组成：Casper CBC和Casper FFG。FFG以保守的方式，在PoW 基础上实施了权益证明。FFG、依然通过PoW 算法增加区块，但是每50个块有一个PoS “检查点”，通过网络验证人来评估区块的最终有效性。FFG解决的是短期内将主链迁移到PoS上，实现混合的PoS模式，只是过渡方案。而CBC是最终方案，以太坊共识机制将全面转为权益证明，从形式化的设计和形式化建设方面都是正确的算法。

5月，FFG阶段第一个代码版本已正式发布，旨在将以太坊工作量证明转变为权益证明。在Casper FFG阶段，以太坊每50个区块中，会有1个由权益证明产生。在未来Casper CBC中，以太坊共识机制将全面转为权益证明，Casper CBC 与传统协议设计的不同之处在于协议在开始时仅约定了一部分并且协议的其余部分需要采用实证方式获。CBC做两方面升级：加入保证金制度，上线分片技术。

保证金制度是为增强安全性而设立的。Casper规定，节点需提交以太坊币作为保证金，一旦其想作弊，比如在为全部“块”进行投票，或者试图对网络发起攻击，则他们的保证金将全部被没收。而分片技术，是为了进一步提升系统处理交易的速度。分片技术指的是，先将节点分组，再将完整的交易数据分片，随机放到不同组内验证，最终结果打包成“块”，组成“链”。

对挖坑的影响：

PoS 的设计对矿工产生了负面影响。随着拜占庭升级的实施，挖矿难度将会大大降低。这就意味着以太坊交易时间会大大缩短，而矿工挖矿所获回报也将大大减少。在以太坊上，矿工也运行着以太坊客户端，因此也需要相应地为拜占庭升级进行更新，而这也将引起重大变化。

这种更新会使区块挖矿速度得到提升，而为了抵消这一点影响，在拜占庭升级实施之后，矿工区块奖励就会减少2 ETH。

具有分片的Casper将块创建时间从当前的15秒减少到2秒。在15秒的当前去看时间内，每分钟向矿工支付12个ETH。在Casper POS下，它将是每分钟15块x .82奖励=每分钟12.3 ETH矿工奖励。如果分片的效果比预期的要好，虽然采矿奖励减少了80%，支付给矿

工总 ETH 可能会增加。

转变完成之后，以太坊将具有以下优点：

去中心化（PoS）：在 POS 权益证明的情况下，一美元就是一美元。这样的好处是，你不能通过汇集在一起，使得一美元值得更多。您也不能开发或购买专用集成电路（ASIC），从而在技术上占有优势。所以，PoS 不同于 PoW 挖矿收入的累计分配方式，采用了比例分配。（成熟的去中心化的声誉/身份管理服务为按比例分配收益成为可能）。

能效（PoS）：PoW 工作量证明机制通过浪费资源来保障网络，在 PoS 中，共识成本较低（无电力和硬件成本），从而允许低发行量。随着网络的成熟，甚至可能会出现负发行（网络交易燃烧的，以及罚款和销毁的），并形成稳定的价格。

明确的经济安全（PoS）：PoS 具有更好的恢复属性。在 PoW 中，存在一个可以使块链不可用的 “51%算力攻击问题。在 PoS 中，网络可以处罚没收攻击者的股权，防止重放攻击。

以太坊的扩展性：在 PoW 链中，最终共识是隐性的（如 “游戏中的皮肤” 特效是通过花费电力进行渲染）。当您检查交易在真实用例中的最终确定时，PoW 链中的最终性的隐性是显而易见的。根据付款的金额大小和重要性，您可以等待额外的块确认（最长链中出现交易以来的区块个数）。例如，对于买咖啡，您可以使用较少的确认，但是为了购买汽车，您可能使用比平均确认数量更多的区块个数来确认交易。相反，Casper 提供了一个明确最终共识的概念。例如，Casper FFG 开始将最终性依赖于在 PoW 链上。因此，基础链依然有一种隐性的方式来确定交易的最终结果。然而，Casper FFG 在大约 2.5 个 epoch 时间窗口之后提供了明确的最终性（每个 epoch 是一个 50 个 PoW 区块，一个检查点是一个 epoch 的最后一个块，区块首先被合理的提出，然后被验证人确定，在上面链接的文章中或以后的文章中可以看到更多的细节。）在这一点上，使用某些拜占庭容错假设，我们可以确定我们的假设是否被违反，或是检查点是最终的。既然我们也意识到验证人设定了先验（也可以是动态的），则不良行为者将通过分析故障归因而受到惩罚。

2. 什么是以太坊分片技术?简 述其概念、工作原理和主要作用。

什么是“分片”技术：

分片技术就是讲以太网络分成多个平行并发的网络，扩展网络，缓解网络拥堵。以太坊目前采用的是二次方分片，通过网络双层设计增加交易量。

具体过程：

将区块链网络中的每个区块变为一个子区块链，子区块链中可以容纳若干（目前为 100 个）打包了交易数据的 Collation，这些 Collation 最终组成一个在主链上区块；因为这些 Collation 是整体作为区块存在的，所以其数据必定是全部由某个特定的矿工所打包生成，本质上和现有协议中的区块没有区别，所以不再需要增加额外的网络确认。这样，每个区块的交易容量就大概扩大了 100 倍。

也就是说，将以太坊网络上的节点分成 100 片，主链上发布的校验器管理合约（VMC）进行分片系统维护。每个分片是独立的账户，当有交易产生时，需要选择一个分片处理，即同一个交易只由一个分片处理，如果网络内有 M 件事务待处理，现在每个节点只需要处理 M/100 件即可，之后这些打包的子区块的数据组成一个主链上的区块，相当于主链区块容量扩大了 100 倍。

作用：

分片的目的实际就是扩容，提高处理事务的效率。以太坊网络可延展性不足，每秒执行事务的数量（TPS）大概 30，远不能满足其网络的处理量。

分片（shard）技术就是为了要很多比计算同步进行，提高整体的性能，每个分片中，都会有它自己独特的转账收据。而这些收据都会存储在分布式的分片记忆储存中，这些收据可以被其他分片看到，但是却不能更改。