未来互联网新技术作业 1

班级：2018211503　姓名：马瑞遥　学号：2018211915

一、　以太坊

1.1 以太坊简介

以太坊（Ethereum）是一个开源的有智能合约功能的公共区块链平台，通过其专用加密货币以太币（Ether，简称“ETH”）提供去中心化的以太虚拟机（Ethereum Virtual Machine）来处理点对点合约。以太币是市值第二高的加密货币，仅次于比特币。

以太坊是一个平台，它上面提供各种模块让用户来搭建应用。以太坊是一个图灵完备的区块链一站式开发平台，采用多种编程语言实现协议，采用 Go 语言写的客户端作为默认客户端（即与以太坊网络交互的方法，支持其他多种语言的客户端）。基于以太坊平台之上的应用是智能合约，这是以太坊的核心。以太坊的设计原则包括：简介原则、通用原则、模块化原则和无歧视原则。

1.2 以太坊的优点

1) 以太坊允许用户在区块链上使用完整的编程语言，在网络上执行更复杂的智能合约，而不需要依靠任何第三方服务。
2) 以太坊可为其他产品和服务平台提供强大的生态系统。
3) 以太坊拥有一个强大的发展路线图，定位明确。以太坊早期定位为世界计算机，而随着发展，明确了自己的定位是世界去中心化的金融底层账本，目前所有的开发、发展、应用都围绕着这个定位，战略清晰。
4) 有很多公司参与改善以太坊以外的基础。在以太坊企业联盟（EEA）和 Hyperledger 团队批准其第一个以太坊项目之间，有数十家企业组织致力于以太坊的改善生态系统。除了比特币之外，其他区块链还没有得到如此多商业社区的大力支持。
5) 以太坊是一个开放系统，外部的每个人都可以参加此项目。这也使得开

发和改善这个生态系统成为可能。与其他区块链项目不同，以太坊交易费用较低。使用这种加密货币投资最初的硬币发行项目确实非常有益。

1.3 以太坊的不足

1) 以太坊正在试图成为一个分类账/超级计算机/智能合约产生器/等等，为更多的用户提供服务。这种复杂性使其具有了灵活性，但是对于以上任何一种用例而言，都没有进行过深度优化。
2) 以太坊计划实现将 POW 机制改为 POW/POS 混合共识机制。但这个涉及到技术开发和矿工双方能否达到利益共识的问题了。如果协议发生了变化，社区意见不合时，就会导致分叉。
3) 以太坊只有一条链，没有侧链，它把所有的程序对等的跑在全球所有节点的矿机上，导致区块快速膨胀，速度较慢，扩展性不足。
4) 缺乏帮助开发人员的教程或文档是成为以太坊开发人员的严重障碍。用户所搜索到的大多数教程都是过时的，或者只是教授对技术的概念性理解，或者只是一个基本的“hello world”教程，没有任何实质性内容。
5) 以太坊智能合约费用过高。在以太坊协议中规定，交易手续费 = Gas 数量 x Gas 价格，其中 Gas 数量由智能合约的复杂程度决定，而 Gas 价格则由合约发起人决定。这意味着虽然读取本地区块链是免费的，但写入和运算是花钱的，储存更是尤其昂贵，因为任何写入的信息都会被永久的储存着

二、 IBM HyperLedger Fabric

2.1 HyperLedger Fabric 简介

Hyperledger Fabric 是开源的企业级许可制分布式账本技术(Distributed Ledger Technology, DLT)平台，是一个分布式的智能合约平台。Hyperledger Fabric 提供一个模块化的构架，把架构中的节点、智能合约的执行(Fabric 项目中称为"chaincode") 以及可配置的共识和成员服务。 一个 Fabric 网络包含同

伴节点（"Peer nodes"）执行 chaincode 合约，访问账本数据，背书交易并称为应用程序的接口。命令者节点（"Orderer nodes"）负责确保此区块链的一致性并传达被背书的交易给网络中的同伴们。

2.2 HyperLedger Fabric 的优点

1) Hyperledger Fabric 平台是一种由 The Linux Foundation 托管的开源区块链框架。它拥有一个活跃而且还在不断发展的开发人员社区。
2) Hyperledger Fabric 网络采用许可制，也就是说，所有参与成员的身份都是已知的，而且经过验证。这项优点在包括医疗、供应链、银行和保险等数据无法对未知实体开放的行业里尤其实用。例如，Hyperledger Fabric 区块链网络上的一家保险公司可以与经过许可的各方分享客户的索赔数据，还能继续保护客户的隐私。
3) Hyperledger Fabric 网络由多条通道组成，它们是两个或两个以上具体网络成员之间通信的私人“子集”，网络上的成员可以在私下以机密方式处理事务。区块链网络上的每项事务在某通道上执行，每一方必须经过身份验证与授权才能在该通道上处理事务。这可以提供额外的访问控制层，而且当成员想要限制数据曝光（如竞争对手在同一个网络中）时特别有用。Fabric 还提供 Private Data Collection 功能集，它可将访问通道上特定事务的权限限制于某个参与者子集。
4) Hyperledger Fabric 专为支持企业级用例而设计，而且可以通过其一致性机制为快速事务吞吐量提供支持。由于 Fabric 是许可区块链框架，它不需要解决在网络上验证事务时可能导致性能变慢的 Byzantine Fault Tolerance 问题。

2.3 HyperLedger Fabric 的不足

1) HyperLedger Fabric 框架较新，缺乏经过验证的用例，除了官方文档以外难以找到其他资料可供参考。
2) Hyperledger Fabric 因为架构的完全不兼容而与公有区块链切割开来，其智能合约语言无法在公有区块链和私有区块链中无缝切换。

HyperLedger Fabric 是要获得允许的，因此不是公有区块链，不允许完全透明。

3) 基于 Hyperledger Fabric 的实验将面临区块链复杂且不安全的问题，同时区块链的可拓展性可能也不能满足业务快速增长带来的需求。HyperLedger Fabric 中的共识算法不像工作量证明机制一样安全，没有工作量证明机制，就不会有真正的不变性。

4) 如果没有加密通证，节点将无法像矿工在比特币网络中那样保持网络的安全。

5) HyperLedger Fabric 没有特别完善的数据管理方案。

三、 Lisk

3.1 Lisk 简介

Lisk 是一个基于 node、js 与 JavaScript，建立于区块链技术之上的区块链应用平台，开发者可以通过官方提供的 sdk，使用 JavaScript 语言在 Lisk 平台内开发自己的 blockchain app。Lisk 提供一种简单，易行的方式，让开发者可以很快速的在区块链上建立自己的应用。Lisk 是一个区块链应用平台，可以让开发者从头开始构建应用程序。分散平台将允许侧链的部署和分发到可以独立于主链的 Lisk 区块链上。Lisk 旨在促进这一趋势，允许项目在封锁网络上开展 ICO。

3.2 Lisk 的优点

1) 基于 Java 语言开发,对开发者友好,Lisk 是第一个完全写在 Javascript 里的去中心化的应用解决方案。

2) 技术团队强大，GitHub 上代码更新频繁。

3) 采用侧链技术，应用 DAPP 都基于侧链开发，保障主网的安全性和承载力。Lisk 的侧链模式给在处理高交易量下如何解决网络拥堵的问题提供了一种方法，用户只有用到相关的应用时才需要下载对应的侧链，大大

减小了无效的同步数据，保持了整个 Lisk 网络的高效运行。

4) Lisk 平台针对寻求创建区块链应用程序或实验区块链技术的常见开发人员。Lisk 使开发人员能够部署自己的侧链，从而增强安全性并实现可扩展性，并在 Lisk 网络上提供自定义令牌，从而实现创造力。

3.3 Lisk 的不足

1) 侧链技术进展缓慢，导致其生态推进的不好。基于侧链技术的项目目前也层出不穷，都是属于早期探索阶段，花落谁家还未得知。
2) 社区运营不理想，国外在某些地区还可以，国内运行的较差。
3) Lisk 目前的沙箱机制不足以限制侧链代码的权限，也就是说无法运行不受信任的代码，那些代码可能会盗取服务器的关键信息，或者直接对服务器进行破坏 。
4) Lisk 的侧链代码是运行在一个拥有全部能力的 JavaScript 环境，这里面有些可以导致不确定因素的函数，比如 Math.random 等。

四、 Cardano

4.1 Cardano 简介

Cardano 是一个智能合约平台，但 Cardano 通过分层架构提供可扩展性和安全性。Cardano 的方法在空间本身是独一无二的，因为它建立在科学哲学和同行评审的学术研究之上。Cardano 是第三代区块链，专注于为区块链空间带来可扩展性和互操作性。有三个组织全职工作来开发和照顾 Cardano：Cardano 基金会、IOHK 和 Emurgo，这三个组织协同工作，以确保 Cardano 的发展进展顺利。

4.2 Cardano 的优点

1) 纵观所有的公链，Cardano 项目拥有史上最多学术机构的理论技术支撑，进行先提交文案再进行同行评审保证理论先进性和可行性，为项目注入了强大的生命力。由于 Cardano 项目开发具有科学性的色彩，某种意义

上说 Cardano 项目团队在试图实现行业规范的协议系统，为将来的 DAPPS 开发人员树立商业可行性的标准。

2) 大多数其他智能合约平台都是通过命令式编程语言编码的。Cardano 使用 Haskell 开发源代码，这是一种函数式编程语言，有助于提高可伸缩性，使程序更加精确。
3) Cardano 使用名为 Ouroboros 的新的股权证明算法，该算法确定各个节点如何就网络达成共识。Ouroboros 是第一个在数学上被证明具有可证明的安全性的股权协议证明，并且是通过同行评审的第一个证明。
4) Cardano 团队通过观察区块链代币项目与政府之间的微妙关系，实行去中心化技术的同时留有监管的余地缓和了相关方面的压力，通过追求多方平衡为项目赢得与社会最大化的接触。

4.3 Cardano 的不足

1) Cardano 目标过于庞大、理想，实施难度不小，难以实现落地应用的项目。
2) 目前 ADA 持币者 95%以上是日本人，分布过于集中，不利于实现国际化。
3) Cardano 偏理论化，周期漫长。路径依赖是人类发展过程中的基本规律，比特币，以太币虽然有很多不足，但在不断的进化，不断的改进，Cardano 很难靠 roadmap 来与已经成熟的项目竞争。