区块链复习资料

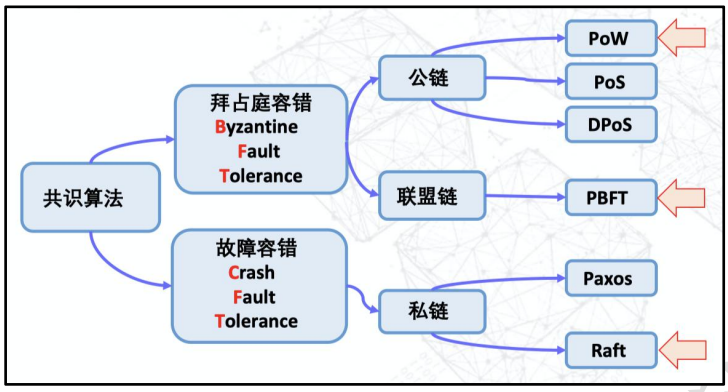
成绩构成：作业 20 分 / 随堂小测 10 分 / 实验 20 分 / 期末考试 50 分。

期末考试题型：选择、判断、简答题。

第 1-3 周：区块链技术[李超]

(区块链技术概述、区块链的密码学原理、区块链共识)

1.分布式共识算法分类：(图很重要，知道怎么分类，代表性的共识算法有哪些)



2.什么是分布式共识？分布式的节点就某个全局状态达成一致。

3.Raft 共识算法：(Raft 不重要，但注意 Raft、PBFT、PoW 的对比图)

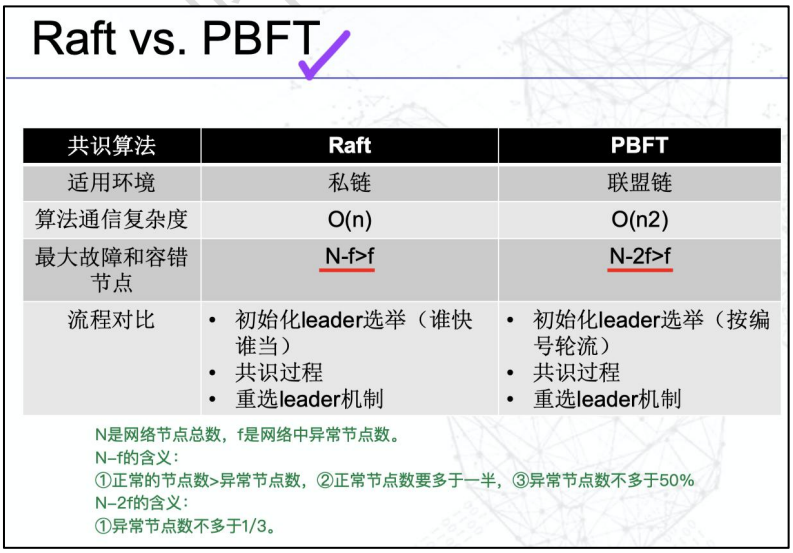
4.PBFT 共识算法：

节点：有一个节点当做主节点，其他节点都是备份节点。

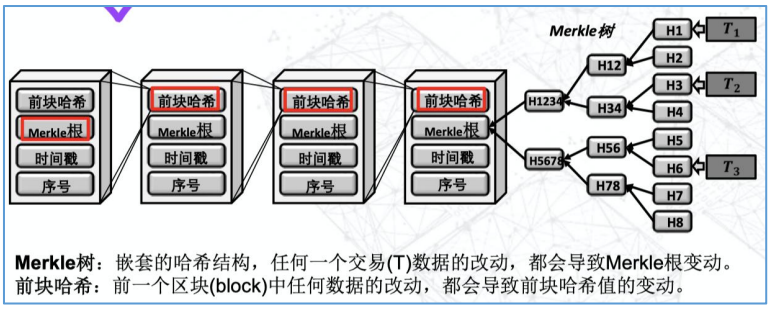
通信：内部所有节点都会相互通信。

目标：少数服从多数的原则达成数据的共识。(如果主节点出现明显的撒谎迹象，其他节点也可以联合起来更换主节点)

5.Raft 和 PBFT 共识算法的对比：



6.PoW （Proof-of-Work）



Merkle树：嵌套的哈希结构，任何一个交易(T)数据的改动，都会导致Merkle根变动。
前块哈希：前一个区块(block)中任何数据的改动，都会导致前块哈希值的变动。

7.PoW 的三个共识：

共识 1：区块链算力竞赛的优胜者有权生成区块。

共识 2：多个优胜者时，以先接收到为暂时优胜者。

共识 3：以最长区块链为准。

问题 1：如果同时出现 2 个优胜者，怎么办？信息的传输有时延，先听到谁的，就认为谁是优胜者。

问题 2：当连续两轮算力竞赛同时出现两个优胜者怎么办？等第三轮。

8.Raft、PBFT、PoW 对比

共识算法	Raft	PBFT	PoW
适用环境	私链	联盟链	公链
算法通信复杂度	O(n)	O(n2)	O(n)
最大故障和容错节点	N-f>f	N-2f>f	51%
流程对比	• 初始化leader选举（谁快谁当） • 共识过程 • 重选leader机制	• 初始化leader选举（按编号轮流） • 共识过程 • 重选leader机制	• 解题 • 如果解开，广播答案，此轮胜出；如未解开，进入下轮。 • 以最长链为合法链。

9.PoS （Proof of Stake）

①PoS 和 PoW 的区别（PoS 的特点）：在 PoS 中，一个账户的余额越多，就越容易发现下一个区块。

②PoS 优点：降低资源浪费、区块生产者与区块链发展的经济利益一致

③PoS 攻击：长程攻击、无利害攻击

10.共识安全问题有哪些？①双花问题、②51%攻击

11.什么是双花问题？同一笔钱重复支付。

12.51%攻击的四个诱因是什么？

①大矿池。(低算力的矿工抱团，不再单打独斗，而组成一种算力，拿抽成)

②算力市场。(矿机所有者可以把矿机租赁给更有经验的矿工，增加了算力市场所有参与者的利润，创造了一个双赢的局面。)

③硬件熊市。(硬件价格突然下跌遭受重大损失)

④受区块链奖励的影响。(每隔 4 年，区块奖励除以 2，长期以往下去奖励会向 0 接近，当后期挖的钱少了，挖的人少了，那么就很容易集中矿力来进行 51%攻击。)

第 7-10 周：以太坊[李超]

（以太坊基础、智能合约基础、去中心化应用开发、以太坊实验）

注：能考的内容集中在前两节课。

1.以太坊与比特币的异同点：

①P2P 网络（一样。都属于 P2P 网络）

②区块（不一样。以太坊区块复杂，有三棵树。）

③交易（不一样。以太坊有三种交易，比特币只有一种。）

④共识（不一样。同属于 PoW 阵营，但以太坊再往 PoS 迁移。）

⑤出块速度（不一样，以太坊出块速度更快，12s vs. 10min）

⑥以太坊支持智能合约。

2.以太坊的特色技术：智能合约、以太坊虚拟机（EVM）。

3.智能合约：以太坊是可编程的区块链，智能合约就是一段程序代码。

4.以太坊虚拟机（EVM）【考理解】：EVM 是图灵完备的虚拟机，智能合约运行在 EVM 上。（EVM 虚拟机可以将区块链全球的网络抽象成一台电脑）

5.智能合约的交易有哪些?

①智能合约的创建交易、②智能合约的调用交易、③普通的转账交易。

6.合约的四部分，Transaction,From,To,Data。

①智能合约的创建交易，To 为 null；智能合约的调用交易，To 为 SimpleStorage。

②智能合约的调用交易步骤：a)创建一个合约调用交易 b)发送到区块链里

7.什么是 DAPP？DApp 是运行在区块链上的应用软件。

8.DAPP 特点是什么：后端运行在区块链上，逻辑由智能合约实现，数据存储在区块链网络节点中。

9.DAPP 和去中心化应用的区别是什么？DAPP 后端使用的是智能合约。

10.以太坊的两种账户：外部账户、合约账户。

注：比特币里没有“账户”这个东西；以太坊的智能合约里有“账户”这个东西。

11.**外部账户**：

①由人创建，由公钥和私钥控制的账户。

②生成私钥->私钥生成公钥(使用加密算法 secp256k1 椭圆曲线)->公钥生成账户地址(SHA3)

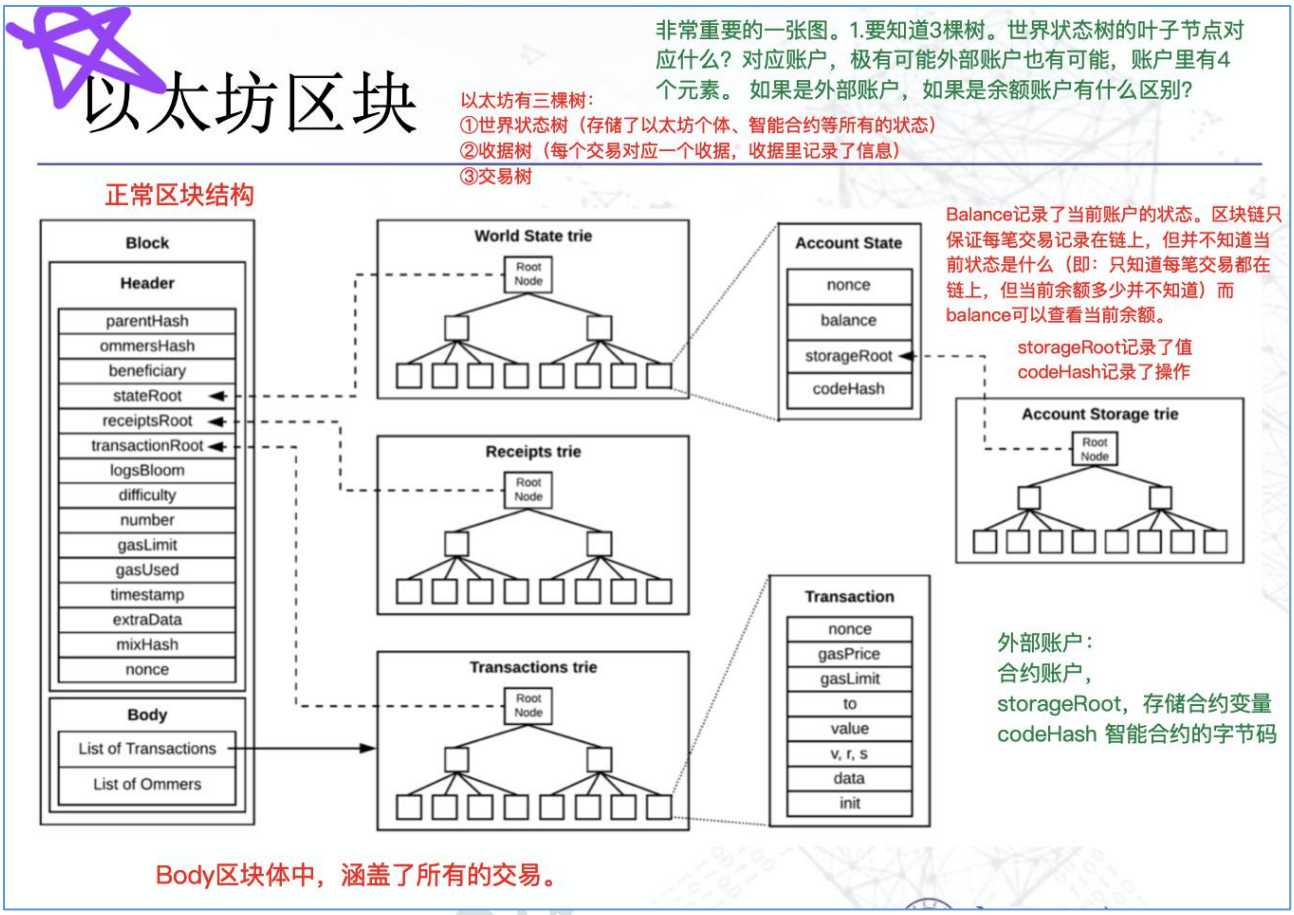
③私钥极其重要！密钥文件通常保存在 keystore 目录中，丢失则账户永久丢失。

录中，丢失则账户永久丢失。

12.**合约账户**:

①由外部账户创建，由合约代码控制。

13.以太坊区块介绍，如下图【很重要】:



14.以太坊的三棵树?

①世界状态树 World State trie（存储了以太坊个体、合约的所有状态）

②收据树 Receipts trie（每个交易对应一个收据，收据里记录了信息）

③交易树 Transactions trie

15.世界状态树的叶子节点对应了什么？对应了账户，可能是外部账户，也可能是合约账户。

16.智能合约常见的安全问题【考判断题，考察发生原因】:

①访问控制（使用 require()等）

②integer-overflow 攻击（整型溢出，加条件限制）

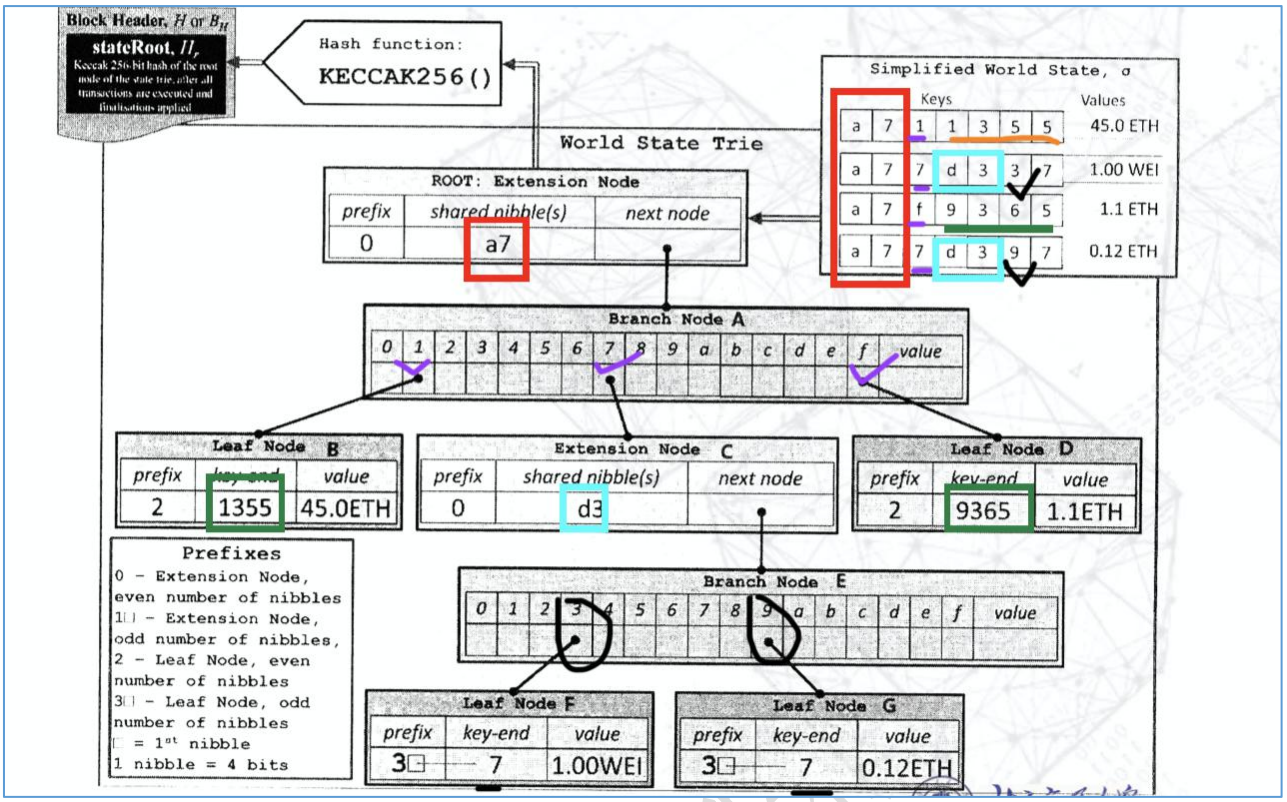
③reentrancy 攻击（转账与状态改变的顺序）

17.三棵树用什么数据组织形式？Merkle Patricia Trie（MPT）

18.Merkle Patricia Trie 有几种节点?

①空节点、②叶节点、③扩展节点、④分支节点

19.数据结构与存储图【填空，挖空要会填】



20.世界状态树的 4 个 value 的作用。

Nonce：是从此地址发送出去的交易数量，可变。

Balance：是此账号所拥有的以太币数量，可变。

codeHash：在 CA 中是此账户存储 EVM 代码的哈希值，在 EOA 中是一串空字符串的哈希值，不可变。

storageRoot：是账户存储树的根节点哈希值，只在 CA 中有，在 EOA 中为空，所有智能合约的数据都以 32 字节映射 的形式保存在账户存储树中。

21.Ethash 共识机制 **（以太坊的 PoW）**：

①特点：挖矿效率与 CPU 无关，而与内存、带宽成正相关。

②对比：比特币耗 CPU 搞共识，以太坊耗内存搞共识。

22.Casper 共识机制 **（以太坊的 PoS）**：

①PoS 算法，带有惩罚机制。

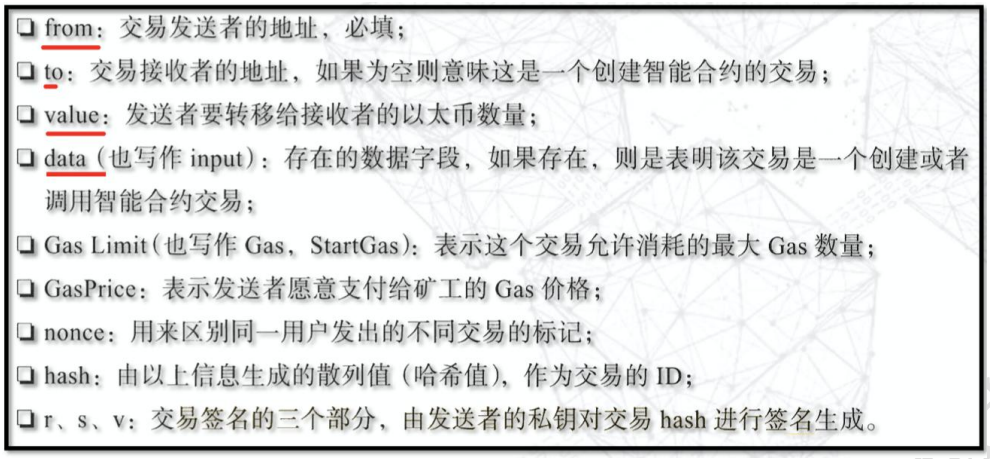
②出块原理：Casper 中有很多抵押了一定数量代币的验证人，验证人投票决定新块有效性，结果由多数人意见确定，投“有效 ”的验证人可收回押金并获得奖励，“作恶”的验证人会被没收押金。（注：少数服从多数的原理）

23.以太坊交易的分类：

①to 是一个地址->普通的转账交易。

②to 是一个智能合约的地址->智能合约的调用交易。

③to 是 null->智能合约的创建交易。



24.智能合约的交易类型：

根据 value-data 是什么，分成了 EOA、CA、0X0 （转账交易、合约调用交易、合约创建交易）

recipient	value	data	result
EOA	√		fund transfer transaction
		√	ignore
	√	√	fund transfer transaction
CA	√		fallback/failure
		√	function invocation transaction
	√	√	function invocation transaction
0x0		√	contract creation transaction

25.转账、合约调用交易的生命周期：

①发送者发起交易请求

②对等节点检验、存储、转发交易

③获得记账权的节点打包交易、执行合约

④生成区块的节点发送区块到网络

⑤所有节点保存交易到本地

26.合约创建交易的生命周期：

①发送者发起交易请求

②获得记账权的节点打包交易、部署合约

27.什么是智能合约？智能合约是区块链上一个包含合约代码（code）和存储空间（storage）的虚拟账户。

28.智能合约的存储方式分为三类：

①账户存储（Storage）：注，账户存储非常昂贵

②内存（Memory）：注，内存是以太坊虚拟机运行代码时临时分配的一种线性空间，会随着合

约调用的结束自动释放。

③栈（Stack）：注，栈是“先进后出”或“后进先出”的结构

29.智能合约的两种调用方式：

①消息调用 call、②代理调用 delegate call

30.什么是消息调用？以太坊允许合约在执行过程中通过创建一条“消息”的方式来调用其他合约，称之为消息调用。

31.call 和 delegate call 的理解：

例子：

智能合约 A 的逻辑是乘法，A 的数值是变量 a 和变量 b 的值，分别是 1 和 2。

智能合约 B 的逻辑是加法，B 的数值是变量 a 和变量 b 的值，都为 0。

注：代理调用就是用 A 的变量值，用 B 的逻辑运算：执行结果为 a+b 等于 1+2=3。

32.智能合约的日志 log：

①开发者可以在合约代码运行过程中记录各种事件产生的日志。

②在智能合约中不能访问日志。

③区块链并不会保存完整的日志文件。

33.solidity 编程语言的结构：

①	状态变量	uint someData; // 状态变量

②	函数	function doNothing(){
		// 函数
		}

③	函数修改器
	【可以理解为面向对象的前置方法】
		function abort() onlyCreater{
		// 调用函数修改器
		}
		
		// 定义函数修改器
		modifier onlyCreater(){
		require(msg.sender == creater);
		_; // 使用下划线指代原函数
		}

④	事件 event	event Deposit(address _from, unit _amount); // 定义一个事件
		
		function donate() payable{
		Deposit(msg.sender, msg.value); // 触发事件
		}

注：要求会写 modifier，会写 require，会写 event，会触发 event。

34.solidity 变量类型分类：

①根据参数传递方式，分为：值类型、引用类型

②根据位置，分为：状态变量、局部变量

35.solidity 变量类型：

①值类型：布尔 bool

②值类型：整型 int/uint，int 默认 int256

③值类型：枚举 enums

④值类型：地址 address，长度 20 字节。

⑤引用类型：数组

⑥引用类型：结构体 struct

⑦引用类型：映射 mapping（key-value 形式的存储结构。为了省钱，映射不存储 key 的数据，仅存储 hash(key)的值，value 存的实际是 value 的值）

36.类型转换：隐式转换、显式转换。

uint32 a = 0X12345678;

uint16 b =uint16(a); //32 位的 a 强制转换成 16 位的 a

37.solidity 的异常处理：

①assert(bool condition)：当条件不为真时，抛出异常，用于处理内部的错误。

②require(bool condition)：当条件不为真时，抛出异常，用于处理输入或外部的错误。

③revert()：中断程序执行并回退状态改变。

例子：判断以太币的数量必须是偶数：

require(msg.value % 2 == 0); // 偶数会继续往下执行，否则抛出异常。

38.solidity 函数 4 个可见性的区分：

①public：可以在合约外部，也可以在合约内部。(类比：public)

②external：只能通过其他合约发送交易的方式调用外部函数。

③internal：只能在当前合约，或继承自当前合约的其他合约中访问。(类比：protected)

④private：只有当前合约内部才可以访问。(类比：private)

39.solidity 特殊函数：

①constant：使用 constant 关键字告诉编译器这个函数进行“只读”操作

②fallback：不能接受任何参数并且不能拥有返回值；当合约匹配函数名不成功时被触发，默认抛出异常，可以通过 fallback(){…}进行重写。

第 13-15 周：热点区域[李超]

(区块链扩充技术、区块链中心化度量技术、区块链跨链技术)

1.当前的区块链系统普遍存在严重的性能可扩展性瓶颈：交易吞吐量不足。

2.区块链技术使得任何用户可以在不需要第三方信任机构的情况下建立信任关系√

3.当前比特币区块链系统理论上支持 7 笔/s 的交易确认；以太坊区块链系统最高支持 15 笔/s 的交易确认。

4.分布式系统中的“CAP 理论”：系统最多只能满足数据一致性、可用性和网络分区容忍 3 个特性中的 2 个。

5.区块链的“三元悖论”：性能扩展、去中心和安全性这 3 个特性不能同时得到满足。

6.区块链扩容的方式：链上扩容（5 种）和链下扩容（3 类）。

7.链上扩容和链下扩容的区别：

①链上扩容是动房子，链下扩容是动房子的前后左右（周边）。

②链上扩容方案是针对区块链自身的基本协议、体系结构进行修改优化，达到扩容效果，提升系统性能。【针对自己】

8.链上扩容有：数据层扩容、网络层扩容、共识层扩容。

9.数据层扩容方案：对数据区块进行修改，增加区块容纳交易的数量。目前有 3 种技术路线：

①扩块（即：扩大区块容量。这是最简单、最直接、易实现的方法，但区块大小不能无节制随意扩大，容易导致 a.算力中心化 b.区块在网络中的传输时延）

②隔离见证（主要思想：将原本存在在区块中的“交易签名”提取出来，放到外部）

③有向无环图（DAG 技术，改变了区块链的块链式线性存储结构。在 DAG 中每一笔新的交易都可以单独作为一个“区块”提交“共识”，DAG 与区块链的区别如下图所示）

- 区块链组成单元是Block（区块），DAG组成单元是TX（交易）。
- 区块链是单线程，DAG是多线程。
- 区块链所有交易记录记在同一个区块中，DAG每笔交易单独记录在每笔交易中。
- 区块链需要矿工，DAG不需要矿工。

10.网络层扩容方案：分片（sharding）

分片：在网络层将区块链网络节点进行分片，每个分片网络各自进行共识，并行处理交易。

根据分片对象的不同，可以分为：网络分片（基础和前提）、交易分片、状态分片。

①网络分片：将区块链网络分成多个子网络。

②交易分片：在网络分片的基础上，将全网交易划分到不同的网络分片中进行分区域共识。

③状态分片：每个网络分片不再存储账本的全部，只存储特定状态的部分账本信息。

11.共识层扩容方案：共识机制改进。共识层的扩容方案主要是修改“共识机制”。提出了 PoS、DPoS、PBFT 等扩容算法，但目前尚未解决三元悖论问题。

12.链下扩容：主要思想是将部分数据转移到链下进行计算处理，将最终的结果返回至链上进行存储记录。（链下计算，链上存储）

13.根据转移方式不同，目前有 3 种技术路线：①状态通道、②侧链、③链下计算

14.状态通道的转移方式主要是链下通道交互、链上清算。

15.状态通道的流程：（注意顺序，可能会考判断题，给个流程看看顺序对不对）

①锁定状态、②开辟通道、③通道内数据交互、④关闭通道、⑤提交更新状态、⑥链上清算

注：先锁定状态再开辟通道；先关闭通道再提交状态，中间核心的是数据交互，最后要进行的是链上清算。

16.侧链：

①目的：是让比特币安全地在比特币主链和其他区块链间互相转移。

②侧链是一个独立的区块链，通过侧链资产的双向锚定进行数据交互。侧链依赖于主链，但是独立于主链处理事物。

③侧链容易成为攻击者的目标。

17.根据目前主、侧链间资产锁定与解锁管理方式的不同，目前有三种技术路线：

①托管模式

②简单支付验证模式 SPV

③驱动链模式

18.链下计算三种方案：

①链下可信执行环境 （Trusted Execution Environment，TEE）计算

②链下安全多方计算

③链下激励驱动

19.区块链扩容技术对比（很全面，值得一看）

扩容层次	扩容方案	原理简述	优势	劣势
链下扩容	状态通道	建立通信双方间的私密双向通道，将计算下放到通道进行	隐私性和实时性好，理论上可无限扩展	技术难度高，安全隐患多
	侧链	锚定主链资产，建立性能更高效的侧链	独立性好，灵活性高	创建侧链成本及维护成本高，易成为攻击目标，技术难度高
	链下计算	将复杂的计算放到链下，将计算结果返回链上验证记录	链下可用传统安全高效方法做复杂计算，间接提升性能	技术难度高，适用范围有限
链上扩容	扩块	通过扩大区块容量，增加数据区块能够打包的交易数量，间接提升系统吞吐量	技术简单易实现，实施周期短，短期效果明显	区块容量增大会增加区块在网络中的传播时延，容易产生分叉
	隔离见证	将数字签名信息移除区块，增加区块容纳交易数量	提升链上交易安全，易实现，降低交易费用	不是针对性能优化提出，扩容效果有限
	DAG 技术	块链式结构改为 DAG 网状并发式结构，实时验证交易	节点越多，交易验证速度越快，理论上无上限	安全性和一致性未得到充分验证，适用范围有限
	分片技术	将网络分片，每个分片独立并发处理全网交易	并行处理事务，节省系统资源	技术难度高，实施周期长
	共识机制改进	PoS、DPoS、PBFT 等改进算法、混合共识算法	降低能耗，提升共识效率	存在技术壁垒，较难实现
第 0 层扩容	覆盖网络	覆盖网络能够快速传播区块，减少区块在网络间传播时延	不影响区块链自身架构	扩容效果有限，适用受限
	QUIC 优化协议	优化 OSI 传输层协议，加快区块传播速度，减少网络时延	不影响区块链自身架构	技术难度高，扩容效果有限，适用受限

课堂测试题（一）

区块链技术课堂测试

院系 计算机与信息技术学院 姓名 [redacted] 学号 [redacted]

一：选择题

1.以下哪个不是区块链特性？（C） 10

A. 不可篡改 B.去中心化 C.升值快 D.可追溯

2.比特币使用的区块链属于（A）

A. 公有链 B.联盟链 C.私有链 D.公有链和私有链

3.对于数字货币拥有者来说，最重要是保护好自己的？（B）

A. 公钥 B.私钥 C.数字签名 D.支付密码

4.51%攻击能做什么？（A）

A.修改自己的交易记录，这可以使他进行双重支付

B.改变每个区块产生的比特币数量

C.凭空产生比特币

D.把不属于他的比特币发送给自己

5.比特币挖矿的本质是争夺一个区块的（D）

A.使用权 B. 拥有权 C.维护权 D. 记账权

6.下面哪种不属于区块链的隐私保护方案？（A）

A.sharding B.环签名 C.同态加密 D.零知识证明

7、加密数字货币如果设置过短的确认时间会更容易导致什么出现？（C）

A.高效率 B.低效率 C.孤块 D.双花

8、比特币在区块链中记录的是？（C）

A.账户信息 B.账户余额 C.交易记录 D.未花费的输出

9.下面哪些属于比特币扩容方案？（ABCD）

A.增加区块容量 B.隔离见证 C.闪电网络 D.侧链

10.下面哪个区块链图中哪个顺序是正确的？（B）C

A. 甲乙丙 B.丙乙甲 C.丙甲乙 D.甲丙乙

课堂测试题（二）

请对你认为正确/错误的表述分别打√/×.

[ ] 1. 以太坊中的每个智能合约对应一个~~外部地址（External Owned Account, EOA）~~。

[ ] 2. 以太坊的每个全节点都包含一个以太坊虚拟机（EVM）以运行智能合约代码。

[ ] 3. 以太坊虚拟机（EVM）~~能够支持~~存在不确定性的操作。

[ ] 4. 智能合约的内容几乎不可能被篡改，合约执行的强制力基本可以保证。

[ ] 5. 以太坊虚拟机是基于栈的虚拟机，栈有~~先进先出~~的性质。

[ ] 6. 以太坊中，使用账户存储相比使用内存~~更廉价~~。

[ ] 7. 以太坊中，内存是~~持久化存储，并不会随着合约执行结束而被释放~~。

[ ] 8. Solidity语言中，布尔类型（bool）可能的取值是常量 true 和 false。

[ ] 9. Solidity语言中，映射是一种键值对映射关系的存储结构。

[ ]10. Solidity语言支持if...else if...else选择结构与for循环，~~不支持while循环。~~

课堂测试题（三）

区块链技术课堂测试

10

院系 计算机 姓名 [redacted] 学号 [redacted]

一：选择题

1. 以下哪项不是区块链目前的分类？（C）

A、公有链 B、私有链 C、唯链 D、联盟链

2. 关于超级账本和比特币的说法，错误的是（C）

A. 超级账本是联盟链

B. 比特币是 UTXO 账户模型

C. 超级账本使用 POW 共识算法

D. 比特币平均每 10 分钟产生一个新的区块

3. 哪些不属于超级账本的节点类型（ D）

A. 背书节点 B. 锚节点

C. 排序节点 D. 超级节点

4.[多选题]对于 ChainCode 的概念，下面描述正确的是 (ACDEF

A. 一个接口的实现代码

B. Fabric 区块链系统中所有变量的值的集合 //这是 word state 的描述

C. 部署在 Fabric 区块链网络结点上

D. 与 Fabric 区块链交互的唯一渠道

E. 生成 Transaction 的唯一来源

F. 智能合约在 Fabric 上的实现方式

5. 在 Fabric 1.0 中，peer 节点可以扮演不同的角色：endorser、orderer 和 committer。其中模拟交易(transaction)执行，用以防止不稳定或非确定的交易通过网络传播出去的节点是(X)A

A. Endorser B. Orderer

B. Committer D.Leader

6.账本的隔离和隐私性用什么技术来保护？(C

A. Endorser/Committer B. 读写集（ReadWriteSet）

C.多通道（Multiple Channels） D. Query System ChainCode（QSCC）

7.Fabric 中的交易数据保存在哪类账本中？(A

A. Block ledger B. State ledger

C. History ledger D. Transation ledger

二．判断题

1. 公有区块链、联盟区块链与私有区块链是依据中心化程度进行区分的。(X)

2. 和公有链一样，联盟链参与方之间互相并不知道彼此在现实世界的身份。(X)

3. 联盟链和公有链一样，也需要额外的代币进行激励。(X)