第1章 区块链概述

目录

CONTENTS

第一章 什么是区块链

CONTENTS

章节

CONTENTS

章节

第一章 什么是区块链

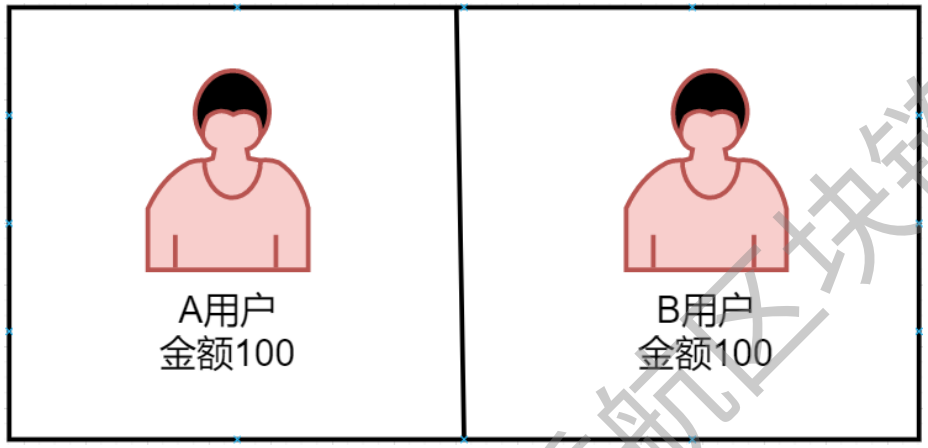
什么是区块链?

- 什么是区块链？
  - 从科技层面来看，区块链涉及数学、密码学、互联网和计算机编程等很多科学技术问题。从应用视角来看，简单来说，区块链是一个分布式的共享账本和数据库，具有去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点。这些特点保证了区块链的“诚实”与“透明”，为区块链创造信任奠定基础。而区块链丰富的应用场景，基本上都基于区块链能够解决信息不对称问题，实现多个主体之间的协作信任与一致行动。

区块链的定义

- 区块链的定义
  - 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链（Blockchain），是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

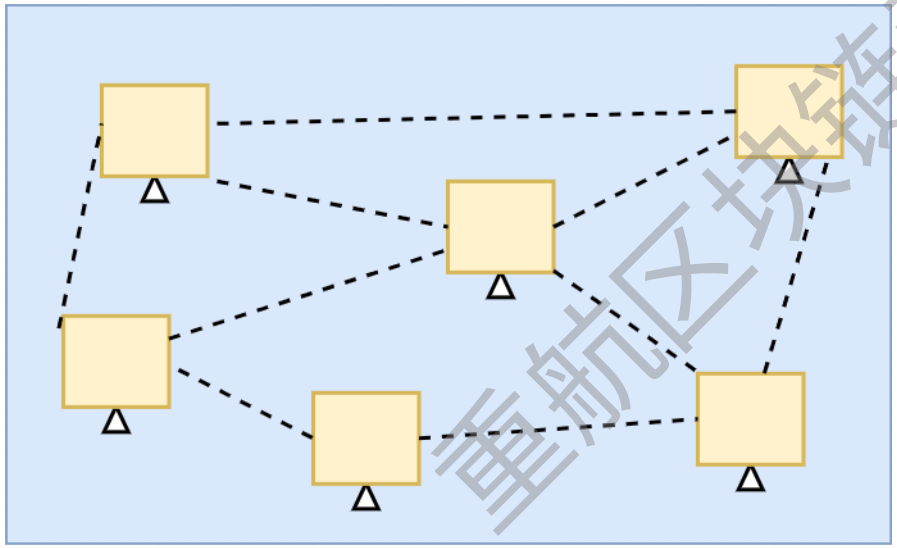
了解区块链



- 在传统情况下，无论大小系统背后都有一个数据库，数据库就像一个大的账本。例如支付宝，当A向B转账1块钱的时候，A的账户会扣除1块钱，相应的B就会增加1块钱。但是用户无法参与具体的记账行为。

- 我们通常认为。谁维护系统谁就天经地义的管理数据库。而其他使用者无权参与。但是区块链可以让系统中每一个用户参与其中，区块链就是一个大的账本，系统中每一个用户都可以参与记账。并且可以随时查阅过去的账单。

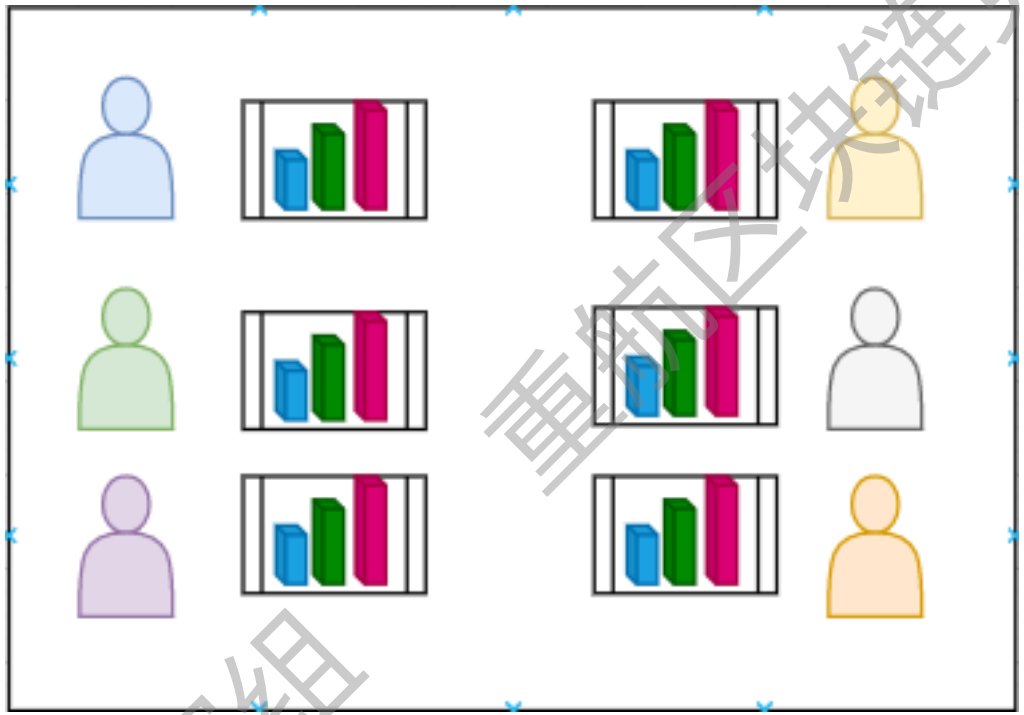
了解区块链



- 在每个时间段内，系统会在竞争者中找出记账最快，最好的用户，该用户把这段时间内的数据变化写到一个区块中，就像写到一张账页上，并把这张账页复制给系统内所有用户进行备份，完成整个动作，在下一个阶段周而复始，于是系统中每个节点，都有着完整账本的副本，由于每个区块数据是通过密码学技术来链接在一起，所以我们程为区块链，或者分布式总账技术。

腾讯云

了解区块链



- 区块链，让全民参与记账
  - 全民记账更稳定：由于全网中并没有特定记账人，系统中任意部分节点失联或者被摧毁，都不会影响系统的运行。
  - 全民记账更高效：由于没有中心化的中介机构存在，完全通过预先设定的程序自动运行，能够极大降低成本和提高效率，并且确保账本记录过程和内容公开透明。

了解区块链

- 全民记账更安全：系统规定相同数量最多的账本是真账本，少部分和其他用户不一致的账本为假账本。这让具有足够多节点的区块链很难被攻击和篡改，这些节点分布在互联网的任意角落，除非控制大部分节点，否则无法篡改，因此，区块链被认为是有史以来最安全的数据管理方式。

腾讯云

什么是共识机制

- 共识机制的由来
  - 我们都知道，区块链可以看作一本记录所有交易的分布式公开帐簿，区块链网络中的每个参与者都把它看作一本所有权的权威记录。
  - 公开账本历史数据不可篡改，只允许往后添加，每个节点都具有相同的权限，那么就带来一个问题：公开账本每个新区块由谁来负责写入？
  - 因为所有节点都一样，如果所有节点同时一起写入账本数据，那么肯定数据会不一致。
  - 因此需要一种机制来保证区块链中的每一区块只能由一个节点来负责写入，如何选出写入账本数据的节点，这就是共识机制。让平等的参与者按照某种秩序达成一致意见。

什么是共识机制

- 共识机制的作用
  - 现在有一个中心数据库，所有客户端都能来查询，每个客户端权限都是一样。
  - 但如果要对数据库进行增删改，不好意思，每次只允许一个客户端来操作，通俗讲，就是让数据库串行修改数据库。
  - 通过一个算法机制来抉择出操作的客户端。这个机制就是共识机制。
  - 所谓的共识就是在人人平等的社会里需要大家共同形成一个共识，产生一个操作者、临时决策者，代表大家来进行中心化的操作，大家按照这个共识来维持去中心化的网络世界。

什么是共识机制

- 常见的共识机制
  - PoW算法，即工作量证明，简单理解就是一份证明，用来确认你做过一定量的工作。监测工作的整个过程通常是极为低效的，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。比如现实生活中的毕业证、驾驶证等等，也是通过检验结果的方式（通过相关的考试）所取得的证明。
  - PoS算法，全称为 Proof of Stake 股权证明。字面意思就是，股份制。谁的股份越多，谁的话事权越大，这和我们生活中的股东的意思差不多。例如 PoS 在虚拟货币的应用中，我们可以把持币量的多少，来看作拥有股权、股份的多少，假设一个以太坊网络，共有3个节点，A 和 B 和 C，其中 A 节点拥有10000 个 ETH 代币，而 B 和 C 分别有 1000 和 2000 个，那么在这个以太坊网络中，A 的区块是最有可能被选中的，话事权是比较大的。

什么是共识机制

- 常见的共识机制
  - DPoS算法类似于民主选举的运行模式，该算法根据数字货币持有的数量对区块事务进行投票管理，并且轮流来选举出块人进行出块。
  - PBFT是著名的拜占庭容错机制，该方案通过多次通信交互来区分恶意节点和诚实节点，接收诚实节点的区块数据，丢弃恶意节点发送的数据和消息。
  - PoST是存储公链的共识算法之一，即统计节点有效存储的数据的大小和时长，将其作为节点的算力，来竞争成为出块节点，算力越大成为出块节点的概率越高，算力越大生成恶意数据的动力就越小，这是通过一种经济手段约束恶意行为的共识算法。

什么是区块链交易

- 区块链交易过程
  - 有人发出交易请求。
  - 交易被发送(广播)到特定区块链网络中所有参与的计算机。
  - 网络中的每台计算机根据特定区块链网络创建者设置的一些验证规则检查事务。
  - 经过验证的事务存储在一个块中，并用锁(哈希)进行密封。
  - 当网络中的其他计算机验证块上的锁是否正确时，这个块就成为区块链的一部分。
  - 现在该交易是区块链的一部分，不能以任何方式更改。

腾讯云

什么是区块链挖矿

- 区块在被增加到区块链之前，并不是所有区块都可以生成区块数据，也不是所有区块数据都能被增加到区块链成为最新的数据，这个过程有一定的门槛。
- 需要筛选出一个值得信任的节点来生成数据，然后由其他节点来验证其生成数据的有效性。
- 这个生产区块的过程会得到数字货币的激励，因此很多节点会加入生产区块的竞争。如果某个节点生产的区块数据得到了其他节点的验证，则其他节点会将最新的区块存储在本地，然后加入下一个数据块的生产竞争，这个过程被称作挖矿，而生成数据的节点被称作矿工。

什么是区块链挖矿

- 以比特币为例，每产生一比交易，并不算完成，只有将交易数据写入数据库，才算成立，对方才能真正收到钱。首先，所有的交易数据都会传送到矿工，矿工负责把这些交易写入区块链。
- 计算哈希的过程叫挖矿，计算哈希的机器就叫矿机，操作矿机的人就叫矿工。根据比特币协议，一个区块的大小最大是1MB，而一笔交易大概是500字节，因此一个区块最多可以包括2000多笔交易。矿工负责把这2000多笔交易打包在一起，组成一个区块，然后计算这个区块的哈希。

什么是区块链挖矿

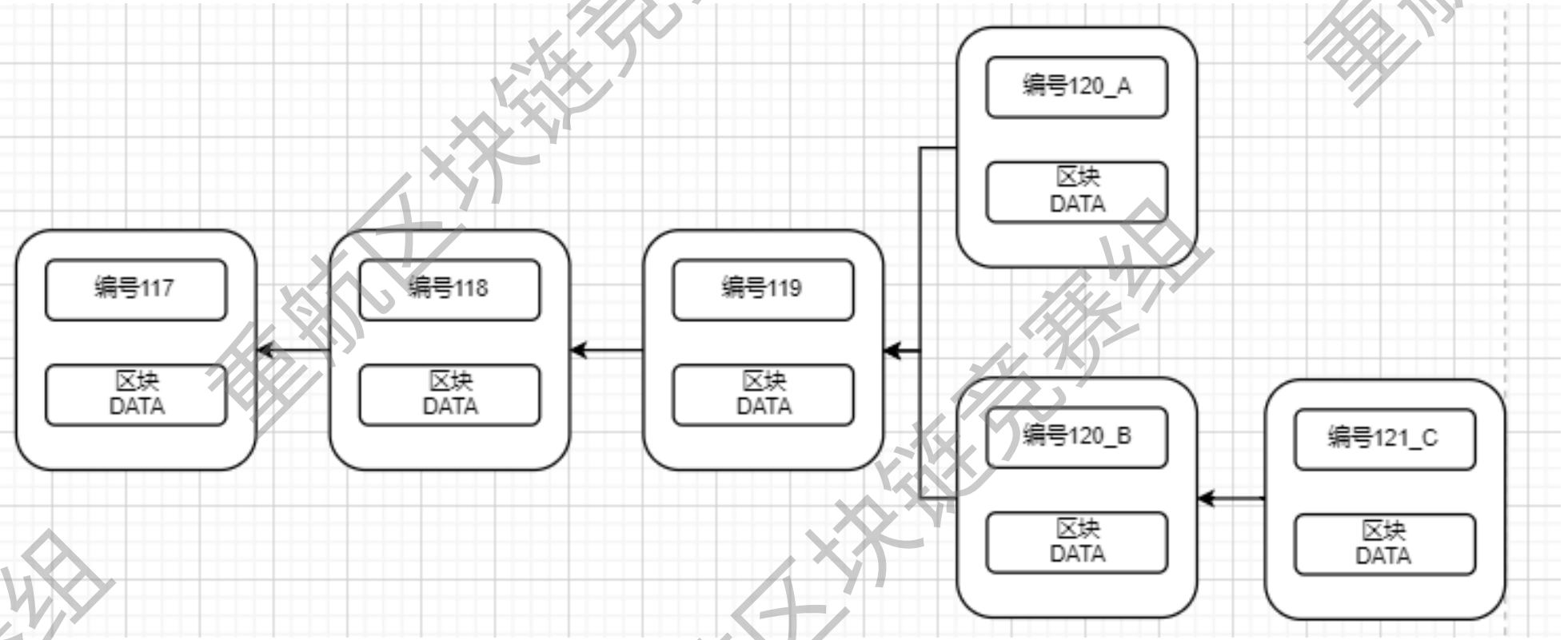
- 成为出块人就可以成功拿到奖励，奖励分为系统的奖励和交易中的交易手续费。
- 在每一笔交易数据中，转账人都可以手动设置手续费，这些手续费用于奖励矿工打包的工作。
- 在转账时设置的手续费越高，转账时间就越短，转账速度就越快，这是因为矿工们会优先选择手续费高的交易进行打包。
- 而如果交易的手续费过低，很有可能会因为没有矿工愿意为其打包而导致转账失败。

腾讯云

分叉

- 什么是分叉
  - 因为整个区块链系统是点对点的对等网络，没有统一的中心机构协调各个节点的行为，所以在生产区块时，各个节点的行为都是相互独立的，很有可能同时由多个矿工在同一区块高度生产出2个以上的区块来。这些区块打包的交易很可能是不一样的，同时满足条件的数字n不是唯一的，多个矿工之间生产的数字n是不一样的，但是同样是满足不等式的。在这种情况下，网络中的其他节点很可能同步到不同的区块数据，并且这些数据在数学上都是合法的、有效的。当不同的节点中的不同的区块作为当前最新区块时，就会存在分叉的情况，即不同的矿机对同一高度的区块生产了内容不一样的新区块，并且这些矿工都找到了满足不等式的数字n。如下图所示。

分叉



分叉

- 分叉的选择
  - 这个分叉非常像我们在微信群里参加某项活动时的报名接龙，由于报名者在看到报名接龙消息后，并不知道其他报名者的报名意愿和状态，很可能出现多个人报同一个序号的情况，在这种情况下，接下来的人会选择其中一个信息次序往下接龙，而未被选中的那一个次序将被抛弃，被抛弃的报名者只能基于最新的接龙信息来重新报名。

CONTENTS

章节

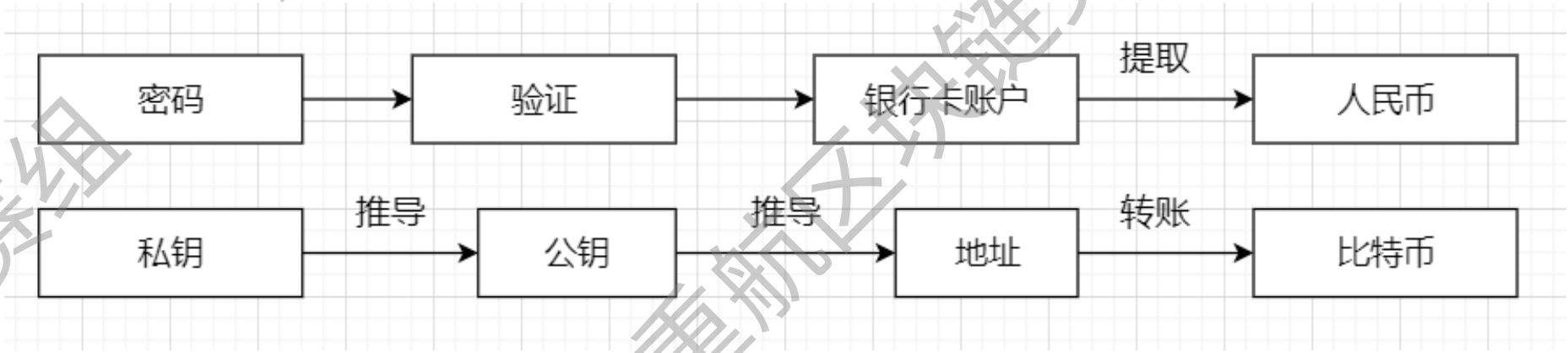
第二章 区块链的几大公链

比特币

- 比特币背景
  - 2008年爆发全球金融危机，同年11月1日，一个自称中本聪的人在P2P foundation网站上发布了比特币白皮书《比特币：一种点对点的电子现金系统》，陈述了他对电子货币的新设想——比特币就此面世。
  - 和法定货币相比，比特币没有一个集中的发行方，而是由网络节点的计算生成，谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。

比特币

- 比特币产生原理
  - 比特币的本质其实就是一堆复杂算法所生成的特解。特解是指方程组所能得到有限个解中的一组。而每一个特解都能解开方程并且是唯一的。以钞票来比喻的话，比特币就是钞票的冠字号码，你知道了某张钞票上的冠字号码，你就拥有了这张钞票。而挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组的特解，这个方程组被设计成了只有 2100 万个特解，所以比特币的上限就是 2100 万个。



比特币

- 比特币特征

比特币的货币特征

去中心化：比特币是没有中央银行。去中心化是比特币安全与自由的保证 。

全世界流通：比特币可以在任意一台接入互联网的电脑上管理。

专属所有权：操控比特币需要私钥，它可以保存在任何存储介质。除了用户自己之外无人可以获取。

腾讯云

以太坊

- 以太坊产生背景
  - 以太坊（英文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（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。
  - 比特币并不完美，其中协议的扩展性是一项不足，例如比特币网络里只有一种符号——比特币，用户无法自定义另外的符号，这些符号可以是代表公司的股票，或者是债务凭证等，这就损失了一些功能。另外，比特币协议里使用了一套基于堆栈的脚本语言，这语言虽然具有一定灵活性，然而却不足以构建更高级的应用，以太坊从设计上就是为了解决比特币扩展性不足的问题。

以太坊

- 以太坊设计原则
  - 简洁原则：以太坊协议将尽可能简单，即便以某些数据存储和时间上的低效为代价。一个普通的程序员也能够完美地去实现完整的开发说明。
  - 通用原则：没有“特性”，取而代之的是，以太坊提供了一个内部的图灵完备的脚本语言以供用户来构建任何可以精确定义的智能合约或交易类型。
  - 模块化原则：以太坊的不同部分应被设计为尽可能模块化的和可分的。开发过程中，应该能够容易地让在协议某处做一个小改动的同时应用层却可以不加改动地继续正常运行。

EOS

- EOS产生背景
  - EOS，可以理解为Enterprise Operation System，即为商用分布式应用设计的一款区块链操作系统。EOS是引入的一种新的区块链架构，旨在实现分布式应用的性能扩展。它并不是像比特币和以太坊那样的货币，而是基于EOS软件项目之上发布的代币，被称为区块链3.0。

EOS

- EOS特点
  - EOS类似于微软的windows平台，通过创建一个对开发者友好的区块链底层平台，支持多个应用同时运行，为开发DAPP提供底层的模板。
  - EOS通过并行链和DPOS的方式解决了延迟和数据吞吐量的难题
  - EOS是没有手续费的，普通受众群体更广泛。
  - 当你拥有了EOS的话，就相当于拥有了计算机资源，随着DAPP的开发，你可以将手里的EOS租赁给别人使用，单从这一点来说EOS也具有广泛的价值

第三章 区块链的应用场景

章节

CONTENTS

数字货币的应用

- 普通货币
  - 普通银行业则往往基于央行的信用，作为中介和担保方，来协助完成多方的金融交易。
  - 发行机构必须能时时刻刻保证交易的可靠性和确定性。为了做到这一点，传统的金融系统设计了复杂的安全流程，采用了极为复杂的软件和硬件方案，其建设和维护成本都十分昂贵。
  - 即便如此，这些系统仍然存在诸多缺陷，每年都会出现安全攻击和金融欺诈事件。此外，交易过程还常常需要经由额外的支付企业进行处理。这些实际上都增大了交易成本。

腾讯云

数字货币的应用

- 数字货币
  - 降低成本：纸币和硬币的印刷、铸造、储藏、运输、防伪等各个环节的成本很高，数字货币将有效降低这些方面的成本。
  - 降低监管难度：纸币存在洗钱风险，监管十分困难，发行数字货币可以有效降低被洗钱的风险，减少监管难度。
  - 推动人民币国际化进程：央行如果率先发行数字货币将有效推动人民币国际化进程，美元霸权地位即将不保。

金融资产交易结算

- 区块链＋跨境支付
  - 当前跨境支付结算，每一笔汇款所需的中间环节不但费时，而且需要支付大量的手续费，其成本和效率成为跨境汇款的瓶颈。通过区块链的平台，不但可以绕过中转银行，减少中转费用，还因为区块链安全、透明、低风险的特性，提高了跨境汇款的安全性，以及加快结算与清算速度，大大提高了资金利用率。
- 区块链＋数字票据
  - 票据业务通过区块链技术可以搭建一个可行的交易环境，避免信息的互相割裂和风险事件。在数据上，有效保证链上数据的真实性、完整性；在操作流程上，不仅反映了票据的完整生命周期，还从发行到兑付的每个环节可视化，确保票据真实性；在风控上，监管机构可以作为独立的节点参与监控数据发行和流通全过程。
  - 目前区块链票据产品可以实现的功能包括供需撮合、信用评级、分布式监管、数据存证和智能交易等。

金融资产交易结算

- 区块链＋资产托管
  - 典型的托管业务流程往往涉及多方，同时由于单笔交易金额大，各方都有自己的信息系统，交易方以往大多依托于电话、传真以及邮件等方式反复进行信用校验，费时费力。采用区块链技术能实现信息的多方实时共享，免去了重复信用校验的过程，将原有业务环节缩短了60%至80%。
- 区块链＋用户身份/账户识别
  - 在用户身份识别领域，不同金融机构间的用户数据难以实现高效的交互，使得重复认证成本较高，也间接带来了用户身份被某些中介机构泄露的风险。区块链技术可实现数字化身份信息的安全、可靠管理，无法追踪，保护客户隐私
- 区块链＋清算、结算
  - 传统的交易模式是双方各自记账，在交易完成后，双方需要花费大量的人力物力对账，真实性难以保证。而区块链上的数据是分布式的，每个节点都能获得所有的交易信息，一旦发现变更可通知全网，防止篡改。

数字政务

- 数字政务的背景
  - 数字中国是一个包括数字经济、数字政府、数字社会“三位一体”的综合体系。其中，数字政府是重中之重，将点燃新一轮改革创新的核心引擎。2018年7月31日出台的《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》提出，要在2022年底前，全面建成全国一体化在线政务服务平台，实现“一网办”。

- 数字政务发展现状及痛点
  - 信息共享是建设数字政务的前提，然而我国的数字政务建设长期存在“各自为政、条块分割、烟囱林立、信息孤岛”等问题。
  - 因此目前，在政务数据共享领域，存在办事入口不统一、平台功能不完善、事项上网不同步、服务信息不准确等诸多痛点。此外，数据的安全可信流通也是数字政务发展面临的另一大考验。

腾讯云

数字政务

- 区块链+数字政务
  - 区块链去中心化、不可篡改、非对称加密、可追溯等特性，正好契合数字政务对于数据流通安全性和可信性的需求，通过共识机制构建一个多方参与的信任网络，进一步实现互联网与政务的深度融合，优化政府业务流程，使得政务公开真正走向阳光、透明、可信。
  - 区块链有助于建立对数据流通的信任机制。分布式的区块链节点能够帮助各部门在不依赖第三方的情况下在数据传输过程中对数据真实性、原始性进行验证，从而确保数据传输的可信关系。

腾讯云

存证防伪的场景应用

- 电子数据存证现状
  - 电子证据主要呈现出四个特点：数量多、增长快、占比高、种类广。
  - 电子证据容易被篡改。
  - 在取证时，电子证据和相关设备如果发生分离，则电子证据的效力会降低。
  - 在出示证据时，需要将电子证据打印出来转化为书证，可能破坏电子数据的内容，同时司法认定成本也较高。
  - 由于其易篡改性的特点，所以会出现双方电子数据内容不一致的情况

存证防伪的场景应用

- 区块链+电子数据存证
  - 区块链可以提供规范的数据存储格式、原数据的保障、安全存储，以及可追溯，提高证据的真实性；
  - 在取证环节，区块链给司法带来的价值在于数据经由参与节点共识，独立存储、互为备份，用来辅助电子证据的真实性认定；
  - 在取证时，电子证据和相关设备如果发生分离，则电子证据的效力会降低。
  - 在示证环节，可采用智能合约，区块链浏览器示证，以提高电子证据的合法性和真实性；
  - 质证环节，区块链可以固化取证和示证这两个环节，全流程可追溯

腾讯云

数据服务的场景应用

- 物流服务
  - 跟随中国“一带一路”政策的开放，中国与周边国家的贸易往来更加的便利和快捷，整个物流市场的运作规模也进一步扩大。
  - 在我们看不到的物流行业背后，从下单、派送到确认收货是物权和资金的转移，涉及到物流供应链中多方的数据共享、合约信任等问题。如果按照传统的物流行业工作模式运转，其流程十分冗长，并且消耗着大量的人力和物力。在任一环节都可能出现问题，监管追溯困难。

腾讯云

数据服务的场景应用

- 区块链+物流
  - 在物流运输行业，用户信息安全与隐秘是一个困扰服务者以及用户双方的问题，而区块链中的数字签名和秘钥则能很好的解决这个问题。
  - 快递员和快递接收者双方掌握秘钥完成交接，同时客户也可以通过区块链系统查询到快递目前的发货程度。因为快递员无法伪造秘钥，所以既保障了快递安全，又使得客户隐私得到保证。
  - 区块链还能提高国际物流效率。跨国运输因为距离问题，涉及到的部门和国家多且杂，为了提高效率，信息的互换非常重要，而区块链恰好能增加信息透明度和传递性，并且保障信息可信度，从来使得各部门协调更方便。

作业

1. 什么是区块链，它有什么特点？
2. 常见的共识机制有哪些？
3. 什么是挖矿？
4. 比特币是如何产生的？
5. 比特币的特征有哪些？
6. 区块链的应用主要有哪些？你还有哪些可以应用区块链的想法？

腾讯云

谢谢