区块链基础知识与关键技术

前言

最近对在上 HKU 的 <COMP7408 Distributed Ledger and Blockchain Technology> 课程，对区块链的基础概念有了更系统的认知，结合之前上过的北京大学肖臻老师《区块链技术与应用》公开课，深知区块链知识体系之庞大，打算更新系列文章对区块链、比特币、以太坊等进行系统的知识梳理，如有错漏，欢迎交流指正。

区块链中的密码学原理

区块链和密码学紧密相关，如比特币采用的核心的公私钥加密技术、数字签名、哈希等，包括很多共识算法也是基于复杂的密码学概念，因此，在开始学习区块链之前，要先了解几个核心的密

码学概念，从而能够更深入理解其在区块链体系中的应用。

哈希函数

哈希函数是把一个任意长度的源数据经过一系列算法变成一个固定长度输出值的方法，概念很简单，但其具备的几个特性使它被各个领域广泛应用。

可以访问这个 Demo 体验一下哈希函数的工作原理（以 SHA256 为例）！

第一个特性是单向不可逆性。将一个输入 x 进行哈希运算得到值 H(x)，这一过程很容易，但是如果给定一个值 H(x)，几乎不可能逆推得到 x 的取值，这一特性很好地保护了源数据。

第二个特性是抗碰撞性。给定一个值 x 和另一个值 y，如果 x 不等于 y，那 H(x) 几乎不可能等于 H(y)，并非完全不可能，但是几率非常低，因此，一个数据的 Hash 值几乎是唯一的，这可以很好地用于身份验证等场景。

第三个特性是哈希计算不可预测。很难根据现有条件推导出哈希值，但是很容易检验是否正确，这一机制主要应用于 PoW 挖矿机制中。

加密/解密

加密机制主要分为对称加密和非对称加密两类。

对称加密机制是两方用同一个密钥来进行信息的加密和解密，很方便，效率也很高，但是密钥的分发存在很大的风险，如果通过网络等方式进行分发，很容易会出现密钥泄漏，从而导致信息泄漏。

非对称加密机制主要指的是公私钥加密机制，每个人通过算法生成一对密钥，称为公钥和私钥，如果 A 想发送一个信息给 B，可以用 B 的公钥对文件进行加密，将加密后的信息发给 B，这个过程中，即使信息被截获或出现泄漏，也不会暴露源文件，所以可以用任何方式进行传播，当 B 收到加密文件后，用自己的私钥进行解密，从而获取文件内容。B 的私钥没有经过任何渠道进行传播，仅自己知道，所以具备极高的安全性。

在现实应用中，对很大的文件进行非对称加密效率较低，所以一般采用一种组合机制：假设 A 想发送一个大文件 D 给 B，则先将文件 D 用一个密钥 K 进行对称加密，再用 B 的公钥对密钥 K 进行非对称加密。A 将加密后的密钥 K 和文件 D 发送给 B，期间即使被截获或泄漏，因为没有 B 的私钥，所以无法得到密钥 K，也就无法访问文件 D。B 收到加密后的文件和密钥后，则先用自己的私钥解密得到密钥 K，再用密钥 K 对文件 D 进行解密，从而获取文件内容。

数字签名

数字签名是非对称加密机制的另一种用法，上文讲到每个人拥有一对生成的公钥和私钥，在加密/解密应用中，是用公钥进行加密，用私钥进行解密，而数字签名机制刚好相反，假设一个文件持有者用自己的私钥对文件进行加密，其他人可以用他的公钥进行解密，如果得到结果则可以证明文件的归属权。

数字签名机制最典型的应用就是比特币区块链网络中，用私钥证明自己对比特币的归属权，对交易进行签名，其他人则可以用公钥来验证交易是否合法，整个过程无需暴露自己的私钥，保障了资产的安全。

区块链基本概念

随着历史的发展，人们的记账方式从单式记账，发展到复式记账、数字记账，最后到分布式记账，因为传统的中心化数字记账则往往依赖于某个或某些组织的可信度，存在一些信任风险，而区块链技术本质上就是一种分布式账本技术，一群人共同维护着一个去中心化的数据库，通过共识机制来共同记账。区块链很容易追溯历史记录，而因为去中心化信任机制的存在，也几乎不可篡改（或者是篡改的成本远远大于收益）。

相比于传统的数据库，区块链只有增加和查询两种操作，所有的操作历史记录都会准确地保存在账本中且不可变，具备很高的透明度和安全性，当然，代价就是所有节点必须通过一些机制达成共识（因此效率较低，不适合实时性的操作），而且因为每个节点都要永久保存历史记录，会占据很大的存储空间。

应用场景

> 那怎么判断一个公司/业务是否适合采用区块链作为解决方案呢?

1. 是否需要数据库?
2. 是否需要共享写入
3. 是否需要多方达成信任?
4. 是否能够脱离第三方机构运作?
5. 是否能够脱离权限机制运作?

区块链作为一个分布式数据库，主要做的还是信息存储的工作，只是通过其各类机制，在不需要第三方机构介入的前提下让有共同需求但并不互相信任的实体之间也能以相对较低的代价达成一致，从而满足需求，除此之外，系统还有加密认证、高透明度等特性，能够满足一些业务需求。而如果所涉及到的数据不能公开/数据量非常大/需要外部服务来存储数据，或者是业务规则经常发生变化，那区块链就并不适合作为其解决方案。

> 因此，在以上的标准下，有如下一些需求很适合区块链作为其解决方案：

1. 需要建立一个共享的数据库，且有多方参与
2. 参与业务的各方没有建立信任
3. 现有业务信任一个或者多个信任机构
4. 现有业务有加密认证的业务需求
5. 数据需要集成到不同的数据库且业务数字化和一致性的需求迫切
6. 对于系统参与者有统一的规则
7. 多方决策是透明的

8. 需要客观的、不可改变的记录
9. 非实时性处理业务

但其实在很多应用场景里，企业需要在去中心化和效率之间做一些权衡，且有时候很多复杂的业务对透明度、规则都有不同的需求，因此，基于复杂的商业化需求，也有“联盟链”这样的解决方案，能够更好地与现有的系统结合，以满足业务需求。

区块链类型

区块链也有不同的类型，主要有私有链、公有链、联盟链三种。

私有链主要是应用于某一个特定领域或者只是在某一个企业运行的区块链，主要是用于解决信任问题，如跨部门协作等场景，一般不需要外部机构来访问数据。

公有链则是公开的交易，往往用于一些需要交易/数据公开的业务，如认证、溯源、金融等场景，比如比特币、以太坊和 EOS 等。

联盟链最大的特征是节点需要验证权限才能参与到区块链网络中，而认证一般都是与其现实角色所关联的，因此，联盟链也具有中心化的属性，但效率、拓展性和交易隐私则大大提升了，满足了企业级应用的需求，其中最广泛使用的就是 `Hyperledger Fabric` 了。值得一提的是，联盟链往往不需要代币来作为激励，而是将参与的各个节点作为记账节点，通过区块链机制实现跨部门之间的业务协同所带来的经济效益作为内部激励，是一种更健康、更符合企业应用的方式。

长期来看的话，公有链和联盟链在技术上也会逐渐趋于融合，即使是同一个业务，可以将需要信任的数据放在共有链上，而一些行业数据和私有的数据则可以放在联盟链上，通过权限管理来保障交易隐私。

区块链基本框架

> 那一个区块链究竟由哪些部分组成呢?

1. 区块
2. 区块链
3. P2P 网络
4. 共识机制
5. …

区块

区块链就是由一个个区块组成的生态系统，每一个区块中包含了前一个区块链的哈希值、时间戳、 `Merkle Root` 、 `Nonce` 以及区块数据几个部分，比特币的区块大小为 1 MB。可以访问这个 Demo 来体验一下一个区块的生成过程。

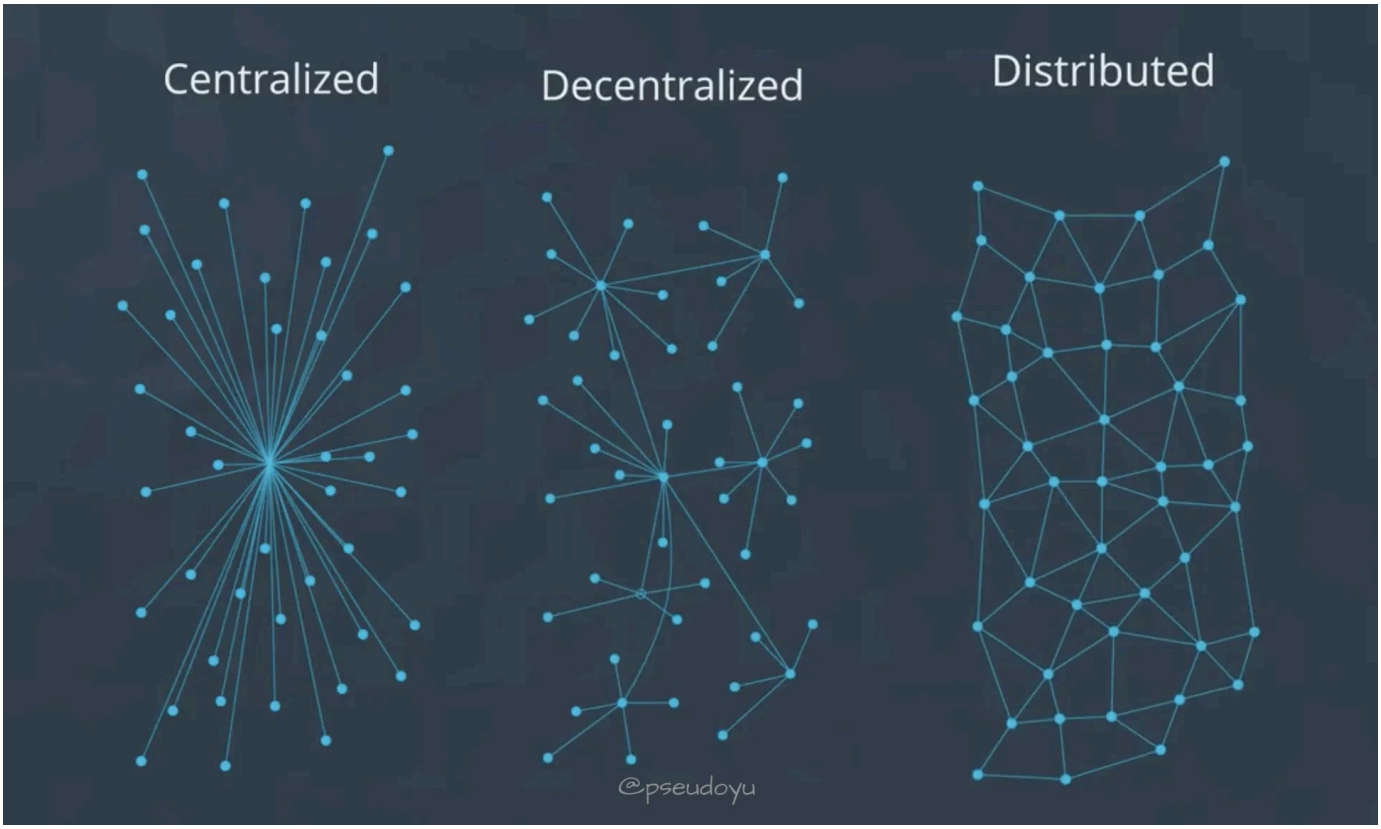
因为每个区块都包含前一个区块的哈希值，根据前文所述的哈希性质，哪怕是极其微小的改变哈希值也会截然不同，因此很容易检测某个区块是否被篡改；Nonce 值则主要是用于调整挖矿难度，可以把时间控制在 10 分钟左右，以保障安全性。

区块链

所有的区块串联起来就形成了区块链，是一个存储着网络中所有交易历史记录的账本，因为每一个区块都包含着上一个区块的哈希信息（比如比特币系统是将上一个区块的块头取两次哈希），因此如果有交易发生变化则会造成区块链断裂，有一个小 Demo 很好地演示了这一过程，大家可以体验一下！

P2P 网络

P2P 网络是用于不同用户之间共享信息和资源的一种分布式网络，是一种分布式网络，网络中的每个人都能够得到一份信息备份，而且都有访问权限；而中心化网络是所有人都连接至一个（或一组）中心化网络；去中心化网络是有多个这样的中心网络，但没有一个单点网络可以拥有所有的信息。下图很好地解释了它们之间的区别：



共识机制

区块链网络是由多个网络节点组成的，其中每个节点都存有一份信息备份，那它们是如何对交易达成一致的呢？也就是说，它们作为独立的节点，需要有一种机制来保障互相信任，这就是共识机制。

常用的共识机制有 `PoW(Proof of Work)` 工作量证明， `PoS(Proof of Stake)` 权益证明， `DPoS(Delegated Proof of Stake` 委任权益证明， `DBFT(Delegated Byzantine Fault`

Tolerance) 等。

比特币/以太坊主要采用的是工作量证明机制，通过算力比拼来增加恶意节点的作恶成本。通过动态调整挖矿的难度来让一笔交易时间控制在 10 分钟左右（6 个确认），但随着比特币挖矿越来越火热，消耗资源越来越多，对环境造成破坏；有些矿池拥有大量资源，也会造成一些中心化的风险。

权益证明机制则是通过权益（一般是代币）持有者进行投票来达成共识。这种机制不需要像工作量证明一样进行大量的算力比拼，但是也有一些风险，称为 Nothing at Stake 问题，很多权益持有者会在所有区块都投注并从中获利。为了解决这个问题，系统设置了一些规则，如对同时在多个链创建区块的用户/在错误链上创建区块的用户设置一些惩罚机制。目前以太坊正在向这种共识机制转变。

EOS 则采用了委任权益证明，选出一些代表性的节点来进行投票，这种方式目的是优化社区投票的效率和结果，但带来了一些中心化的风险。

DBFT 共识机制则是通过对节点分配不同的角色来达成共识，这样可以很大程度降低开销和避免分叉，但是也有核心角色作恶的风险。

区块链安全与隐私

安全

区块链作为一个较新的技术，也存在很多安全隐患，如对数字货币交易所的攻击、智能合约漏洞、对共识协议的攻击、对网络流量（互联网 ISP）的攻击以及上传恶意数据等。比较著名的案例有 Mt.Gox 事件、以太坊 DAO 事件等，因此，对区块链的安全风险也是区块链的重要研究方向。

可以从协议、加密方案、应用、程序开发和系统等角度进行风险分析，提高区块链应用的安全性。例如在以太坊区块链中，可以对 Solidity 编程语言、 EVM 和区块链本身进行一些分析。

如智能合约中的一种叫低成本攻击的方式，就是通过识别以太坊网络中较低 Gas 费用的操作，重复执行以破坏整个网络。

对于安全问题，构建一个通用的代码检测器来检查恶意代码将会是一个更通用的解决方案。

隐私

在讲区块链概念的时候，提到了它很重要的一个特征，隐私性。也就是说，所有人都能看到链上的交易细节和历史记录，这一特性主要应用在食品、药物等供应链环节，但是对于一些金融场景，如个人账户余额、交易信息，则容易造成一些隐私风险。

> 那有哪些技术能够应用于这些存在高价值、敏感信息的隐私保护呢?

硬件层面，可以采用可信的执行环境，采用一些安全硬件，如 Intel SGX，很大程度保障了隐私；网络可以采用多路径转发以避免从节点的 ip 地址推算出真实身份。

在技术层面，混币技术可以把很多交易进行一些混合，这样不容易找出对应的交易发送方和接收方；盲签技术可以保障第三方机构不能将参与交易的双方联系起来；环签用于保障交易签名的匿名性；零知识证明则可以应用于一方（证明者）向另一方（验证者）证明一个陈述是正确的，而无需透露除该陈述是正确的以外的人和信息；同态加密可以保护原数据，给定 E(x)和 E(y)，可以很容易计算出某些关于 x, y 的加密函数值（同态运算）；基于属性的加密（Attribute-based Encryption，ABE）则为各个节点添加一些属性/角色，实现权限控制，从而保护隐私。

值得注意的是，即使一笔交易生成多个 inputs 和 outputs，这些 inputs 和 outputs 的地址也可能被人关联；除此之外，地址账户和现实世界中的真实身份也可能产生关联。

总结

以上就是对区块链基础知识的一些梳理，主要从概念和原理层面进行了一些学习，后续还会更新对比特币、以太坊、Hyperledger Fabric 等典型应用的分析与思考，并对 IPFS、跨链、NFT 等热门技术进行一些探究，敬请期待！

参考资料

1. COMP7408 Distributed Ledger and Blockchain Technology, *Professor S.M. Yiu, HKU*
2. Udacity Blockchain Developer Nanodegree, *Udacity*
3. 区块链技术与应用，*肖臻，北京大学*
4. 区块链技术进阶与实战，*蔡亮 李启雷 梁秀波，浙江大学 | 趣链科技*