Block Chain

DDS

vs

Block Chain

区块链

- 狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。
- 广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式

区块链技术创新

- 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
- 分布式账本
- 非对称加密和授权技术
- 共识机制
- 智能合约

分布式账本

- 交易记账由分布在不同地方的多个节点共同完成，而且每一个节点都记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。
- 跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。
- 没有任何一个节点可以单独记录账本数据，从而避免了单一记账人被控制或者被贿赂而记假账的可能性。也由于记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

非对称加密和授权技术

- 存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。

共识机制

- 所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。
- 区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。
- 以比特币为例，采用的是工作量证明，只有在控制了全网超过51%的记账节点的情况下，才有可能伪造出一条不存在的记录。当加入区块链的节点足够多的时候，这基本上不可能，从而杜绝了造假的可能。

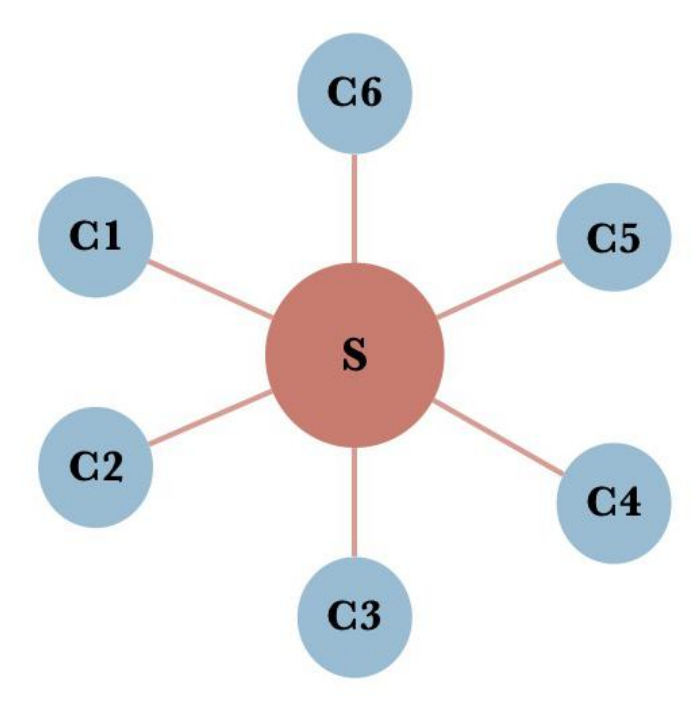
智能合约

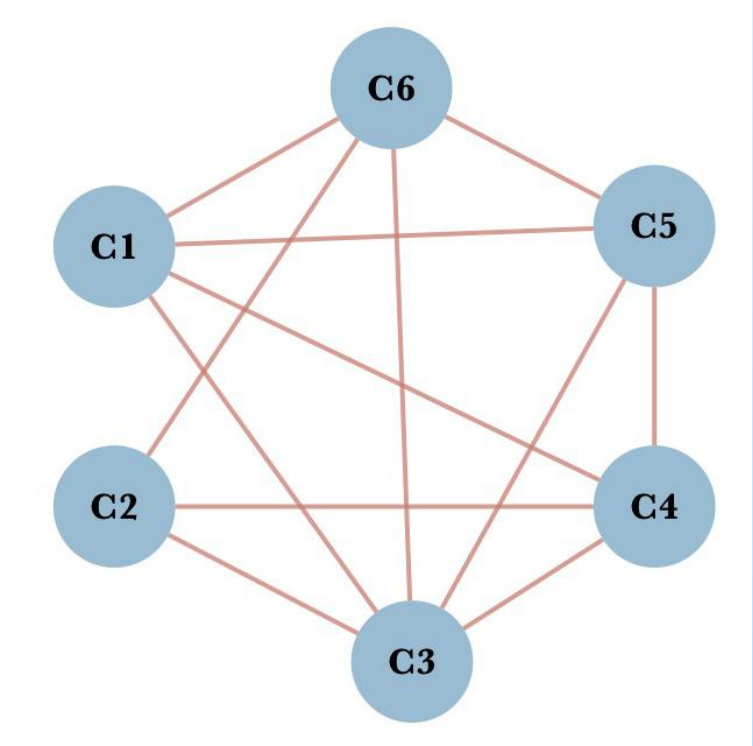
- 基于这些可信的不可篡改的数据，可以自动化的执行一些预先定义好的规则和条款。以保险为例，如果说每个人的信息（包括医疗信息和风险发生的信息）都是真实可信的，那就很容易的在一些标准化的保险产品中，去进行自动化的理赔。
- 在保险公司的日常业务中，虽然交易不像银行和证券行业那样频繁，但是对可信数据的依赖是有增无减。因此，笔者认为利用区块链技术，从数据管理的角度切入，能够有效地帮助保险公司提高风险管理能力。具体来讲主要分投保人风险管理和保险公司的风险监督。

区块链特征

- 1.去中介化。由于使用分布式核算和存储，体系不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。
- 2.开放性。系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。
- 3.自治性。区块链采用基于协商一致的规范和协议（比如一套公开透明的算法）使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。
- 4.信息不可篡改。一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。
- 5.匿名性。由于节点之间的交换遵循固定的算法，其数据交互是无需信任的（区块链中的程序规则会自行判断活动是否有效），因此交易对手无须通过公开身份的方式让对方对自己产生信任，对信用的累积非常有帮助。

网络结构





六大核心算法

- 拜占庭协定
- 非对称加密技术
- 容错问题
- Paxos 算法（一致性算法）
- 共识机制
- 分布式存储

典型应用

- 比特币
- 超级账本
  - 华为Hyperledger
- 金融
  - 支付宝App---蚂蚁区块链
- 物流
- 公共服务

Checkpoint

- 一个节点只要承认了Checkpoint的区块为合法的区块，那就可以避免这个高度以之前的所有的区块被其他力量重组，特别是可以避免被51%优势算力攻击重组区块。
- Checkpoint在一定程度上改变了最长链为有效链的原则，改成了只有包含了Checkpoint的最长链才是有效链。
- Checkpoint可以用来部署协议分叉，所有节点都统一运行带有Checkpoint的完整节点软件，然后一旦heckpoint的区块被挖出，那此后所有的协议就可以被统一更改。

区块链时代

- 区块链1.0
  - 挖矿卖矿囤矿，物以稀为贵的数字货币乌托邦时代！
- 区块链2.0
  - 智能合约
  - 发币买币炒币，玩概念、投项目、炒市值的泡沫时代！
- 区块链3.0
  - 开发落地服务，应用开发完成、项目落地完成，为人民提供服务的价值时代！