区块链

是什么： 它是一个共享数据库，存储于其中的数据或信息，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。基于这些特征，区块链技术奠定了坚实的“信任“基础，创造了可靠的“合作”机制，具有广阔的运用前景。

1. 一个存储每个人身高的区块链。
2. 一个存储每个人对国家认知的区块链。
3. 一个存储每个人财产信息的区块链。
4. 一个存储每个人的婚姻状态的区块链。

信息链条：(狭义区块链) 确保数据不可篡改性质

哈希算法

简单来说就是一个生成信息指纹的方法。

比如说我有一个通讯录，每个名字可以找到对应的唯一的一串字符，但是从这串字符没有办法往回找到名字。

信息区块 --》 信息区块

每个区块中包含了上个信息区块的信息指纹。

如果偷偷修改了上个信息区块的信息，生成的信息指纹就会变化，就会和现在的信息区块中存储的信息指纹冲突。所以为了圆谎，必须修改现在这个区块的关于信息指纹的信息，者导致现在这个区块的信息指纹被改变了，那么它就会和下一个信息区块相冲突。

牵一发动全身：母信息改变，所有后面的信息都会改变。

所以信息会很难被篡改。

信息加密：确保数据传输安全性

非对称加密算法：RSA算法

概念阐述

我想要你寄给我一个快递，但是我们害怕中途有人拆开快递查看其中到底是什么东西。

假设：存在这样一种带锁的箱子，不能用除了钥匙以外的方式打开，并且不同箱子的钥匙是不同的。

传统solution：你使用箱子将快递锁在里面，然后将快递连带箱子一起寄过来；之后你再通过其他的途径将钥匙寄过来。

问题：如果钥匙被截胡箱子仍然有风险。

非对称solution：你和我联系之后，我将我的带锁箱子寄给你，你将快递锁在箱子之后一起寄给我，我使用自己的钥匙打开。

完全没有截胡钥匙的风险。

应用场景

言论自由

共识算法：使用算法确保群体共识

拜占庭将军问题：

拜占庭帝国的军队正在围攻一座城市。这支军队被分成了多支小分队，驻扎在城市周围的不同方位，每支小分队由一个将军领导。这些将军们彼此之间只能依靠信使传递消息（无法聚在一起开个会）。每个将军在观察自己方位的敌情以后，会给出一个各自的行动建议（比如进攻、撤退或按兵不动），但最终的需要将军们达成一致的作战计划并共同执行，否则就会被敌人各个击破。但是，这些将军中可能有叛徒，他们会尝试阻止其他忠诚的将军达成一致的作战计划。

共识算法的目标：让忠诚的将军们能够排除叛徒的影响，通过信使就能够达成共识，

PBFT算法（拜占庭容错）

我发送建议给所有将军

将军们将“收到我的建议”这个信息传给所有人

将军们计算收到“收到我的建议”的个数，如果大于一定个数就认为我的建议是一种共识

raft算法

http://thesecretlivesofdata.com/raft/

每个人有三种状态：

- leader
- follwer
- candidate

分布计算：

数据结构： 区块链

共识算法：保证共识

谁去提出新的区块添加的请求?

挖矿

如果有人使用机器对区块生成进行了计算，并且最先将自己区块添加的申请变成共识，那么就会得到奖励。所以分布式计算算的是新的区块。

将上述内容整合一下举个例子

分布式农庄