区块链线下活动第1期 | 与金融量化专家杨叶博士对谈，解析比特币与区块链

A group of people standing in front of a crowd posing for the camera

Description generated with very high confidence

*比特币刚出来的时候一万个比特币买一个披萨饼，现在一个币差不多可以买一辆车*

# 导读

比特币集加密 计算，博弈论，计算机等各种技术于一体，这场伟大的实验已经稳定运行了9年，其价格也是屡创新高。11月4日下午，红点指南在NTU的The Hive，组织了关于“区块链与虚拟货币”的线下分享会，我们邀请了金融量化专家、NTU MFE 讲师杨叶博士为我们介绍以及剖析当下非常火热的区块链技术。

# 嘉宾介绍

杨叶博士是1999届 SM2的学生（第3届）。PhD读的是计量与结构生物（Computational and Structural Biology)。早期是技术黑客，曾是SETI@home 分布式计算项目新加坡的第二名（至2006）。2008年开始做量化金融，接触数学，统计。现在是Cargill的Quantitative Risk Lead, 且是NTU MFE（金融工程）的讲师，教授区块链，数据分析，以及金融量化模型。拥有丰富的科研经历，是金融量化的专家，具备庞大的阅读量，涉猎AI,区块链，量化金融，结构生物，计算机，历史与哲学，且具有丰富的旅行经历以及对人生的思考。

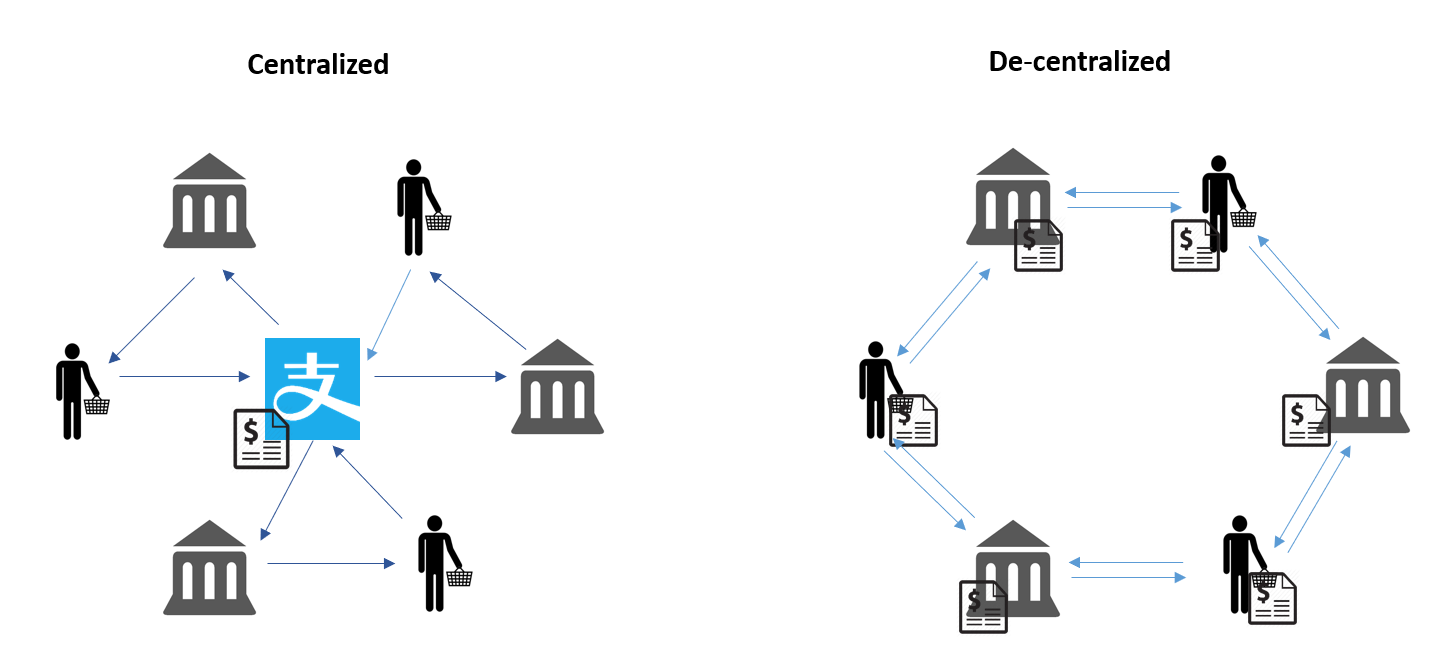
# 开场

90年代末，出现了MP3, 人们可以用电脑储存控制音乐，一首歌从磁带上变成了电脑上的文件。后来，一部电影又变成了电脑上的文件。现在，比特币，钱变也成了电脑上的文件。可见，技术融入到了生活的方方面面。罗马不是一天建成的，比特币集非对称加密，博弈论，分布式储存等各种技术于一体，其出现是人类过去几十年知识的结晶。

比特币自2008年出现，其价值从2016年开始发生质的飞跃。当年，英国退欧，Trump同学在大洋彼岸登基，ISIS大行其道, 南美大宗商品进出口受到严重打击。印度废除500面值钞票；委内瑞拉，津巴布韦通货膨胀严重。阿根廷一年内的通货膨胀达到24%，加上政府贪污腐败，类似于阿根廷这种中等收入国家的人们选择比特币来保值资产，然后用比特币转成美元。比特币价值从去年开始上涨，有其国际政治，经济背景。

随着价格飞速发展，更多的人选择持有比特币。目前，少数人掌握了大量的比特币。Winklevoss Twins (当年控诉扎克伯格偷窃其社交网络idea的俩兄弟)号称拥有1%的比特币； 美国政府通过缴获黑市交易网站丝绸之路（silk road）掌握了大量的比特币；在中国，据说李笑来拥有6位数的比特币；比特币创始人中本聪作为最大拥有者，有98万枚（当然，中本聪目前只花出去50枚）。有人在质疑比特币是庞氏骗局，也有人在欢呼区块链的伟大！

# 去中心化

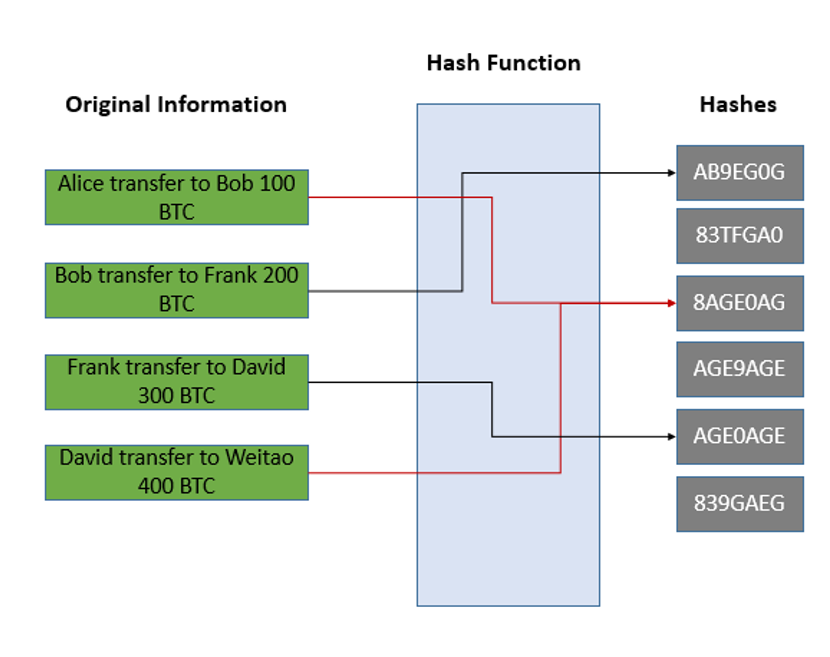


去中心化的理念很早都有了，从P2P资源下载的电驴/Bittorrent/迅雷，去中心化储存的Sync（基于BitTorrent protocol），包括P2P通讯Skype,都体现了去中心化的理念。 而比特币和以往分布式系统的不同在于区块链。区块链最关键的三个特性如下

* 每个地方都一样
* 不可改变
* 没有人拥有它（同时，每个人都拥有一部分）

区块链本质是一种新的数据结构。尽管区块链上能做的事情，都可以通过现在中心化的模式实现，但是由于上面提到的三个特性，区块链提供了智能协议的基础，使得智能交易变成可能。

# Hash

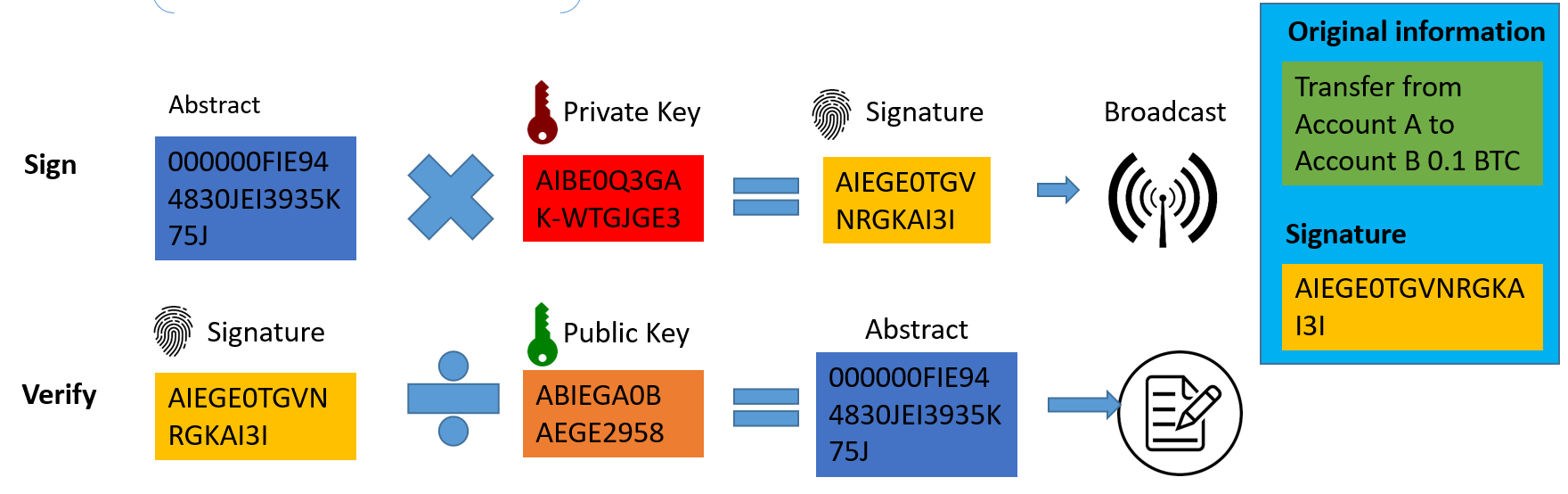


哈希（Hash）函数是可用于将任意大小的数据映射到固定大小的数据的任何函数，通常使用的哈希函数有md5和sha256。哈希函数具有以下特性。

* 同样的输入值任何时候做哈希都会得到相同的哈希值
* 输入值很小的改变会导致哈希值很大的改变
* 不可以通过哈希值倒推出输入值

破解哈希是很困难的，这种困难通常包含两种，CPU hard 和 RAM hard。 例如，破解md5就是CPU hard，需要耗费大量的算力。但它不是RAM hard的问题,也即破解md5可以通过牺牲储存空间来提高速度，例如可以构建彩虹表去核对哈希值来推断其原始信息。而RAM hard指的是无法通过牺牲存储空间来更快破解，例如，SHA256就是RAM hard的算法，比特币使用的正是SHA256。

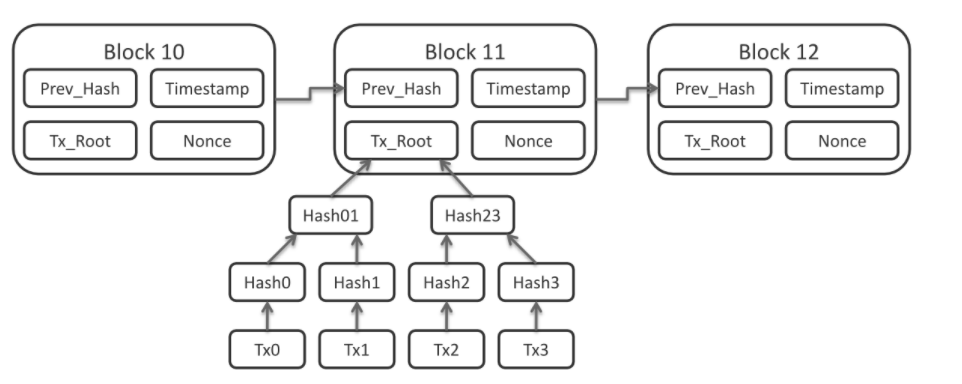
# 非对称加密



比特币采用了非对称式加密技术。使用私钥（Private key）对信息加密，用公钥（Public key）解密信息。如果要质数分解很大的数（2\*\*256量级）, 现有计算机没法快速分解。数学上的描述是，S=p\*q，其中， p和q都是质数。可以通过p和q导出S, 但是S不可以导出p和q。p和q可以理解为私钥，而S可以理解为公钥。在比特币网络中，公钥是公开的，私钥只有自己知道。例如，如果A要发起交易，A需要用私钥和交易信息的哈希值一起创建自己的签名，然后把交易信息和签名一起广播出去，网络中其他的人，比如B, 可以通过与A对应的公钥来验证该签名是否属于A。验证成功就把交易记录到区块链上，否则就视为虚假交易。

# Merkle tree

Merkle Tree 是由计算机科学家 Ralph Merkle 在很多年前提出的，并以他本人的名字来命名。



从图中我们可以看出Merkle树被应用在了交易的存储上。每笔交易都会生成一个hash值，然后不同的hash值向上继续做hash运算，最终生成唯一的Merkle根。并把这个Merkle根放入数据区块的区块头。利用Merkle树的特性，以确保每一笔交易都不可伪造和没有重复交易。这样做的好处，也就是中本聪描述到的“简化支付验证”（Simplified Payment Verification，SPV）的概念:一个“轻客户端”（light client）可以仅下载链的区块头即每个区块中的80 byte的数据块，而不是下载每一笔交易以及每一个区块。如果要验证单个交易是否存在于某个区块，只需要进行log(N)次的验证（N是区块中交易数量）。

# 共识算法和挖矿

挖矿的过程是在网络中随机选一个人,且确保这个人记录的信息传播给所有人。这个人选的产生通常有两种共识机制，PoW( Proof of Work)和PoS(Proof of Stake)。

PoW的前身就是Hashcash算法，Hashcash算法主要用于减少垃圾邮件。发送邮件的人要计算一个Hash值，该Hash值要符合一定条件才行。这就使得发送垃圾邮件的人的成本很高，邮件之间的时间时延很长。（据说，中本聪给了发明Hashcash算法的人50个比特币，这也是中本聪唯一的比特币使用记录）在比特币网络中，矿工需要在1分钟之内猜出一个特定的随机数（nonce）, 成功猜到的人才有权记录交易信息到区块链上。中本聪最原本的设计是one CPU one vote，也即每个CPU具有理论上相同的被选中的概率。但是他没有预料到比特币选用的SHA256算法容易被专门化的GPU, FPGA, ASIC芯片计算，所以可被用来大量挖矿，这也导致了后来矿池算力的集中。莱特币选用了另一种较难被ASIC芯片实现的hash算法scrypt，也是出于这样的考虑，但这并非是最终的解决方法。

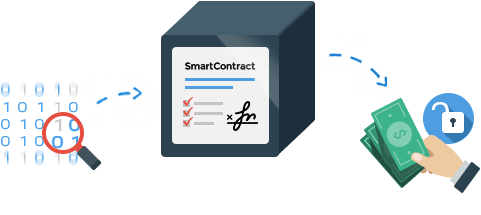
Intel后来提出过one cpu one vote的想法, 也即把挖矿算法内嵌在CPU里面，这样就避免了算力操纵，就是Proof of Elapsed Time。

在PoW中，每个人都可以加入区块链网络，不需要拥有比特币。而PoS在验证你的时候要参考你拥有多少比特币，这样，矿工自己的利益牵扯其中，某种程度上激励参与者保护网络而不去攻击网络。但通俗来讲，PoS就是“富者越富，穷者越穷”；PoW是算力越强的人越富有，算力越弱的人越穷。

# BFT 拜占庭将军问题

首先谈谈Two General’s Problem。这其实是一个思想实验，两支军队，分别由两个将军领导，正在准备攻击一个坚固的城市。两支军队都驻扎在城市旁边的两个不同的山谷里。两军之间隔着第三个山谷，两个将军想要通讯的唯一方法就是穿过第三个山谷传送信件。问题是，第三个山谷被城市的守卫军占据，并且经此传送的信件可能会被守卫军截获。这个思想实验致力于考虑两军怎么做才能达成一致，这个实验被证明是无解的。由这个实验引申出拜占庭将军问题：在一个网络中，如果同时存在错误节点和正确节点，应该如何确保信息的准确流通？1982年，Lamport, Shostak, and Pease 的论文指出，如果网络中存在F个制造假冒消息的节点，那么需要至少3F+1个节点传播正确的消息才可以确保网络正确运行。在比特币网络中，解决拜占庭将军问题的方法叫做The Nakamoto Consensus。（这里不详细介绍）

# Smart Contract - Code is the law



智能合约标志着Blockchain 2.0时代，其概念1994年就提出了，在以前只是概念，无法实行，现在基于区块链可以实行智能合约。第一个在区块链上实现智能合约的是以太坊，以太坊提供了一个图灵完备的World Computer （虚拟机），合约以代码的形式跑在以太坊虚拟机上。智能合约提供了一种不需要中间人的settlement方式。交易双方可以在不需要第三方信任担保的情况下完成合约交易。

## Private Chain & Public Chain

像比特币，以太坊，莱特币等都是基于公共链的货币系统，任何人都可参与其中，这也被称作Permissionless。但也正因如此，公共链的共识机制（无论是PoW还是PoS）都导致了交易速度很慢，比特币每秒交易速度是 4 TPS （Transactions Per Second）,以太坊是20 TPS。而作为中心化的交易方式visa,其交易速度是2000 TPS。基于公共链的货币想要取代现有支付方式的挑战性很高。

与此对应的，私链（Private Chain）指的是特定的人或机构才可参与其中，而且每个参与者都有特定的职责，这也被称作Permissioned。该类项目有Linux Foundation 的Hyperledger，IBM的HyperLedger Fabric，Intel的Sawthoothe （有意思的是这个链提出了新的共识算法叫Proof of Elapsed Time，有兴趣的可去了解）。除了大公司，各国政府也在加入私链的领域，如中国央行有计划发行加密货币，英国，新加坡也有类似打算。

# 提问

Q: 你买过比特币吗？

杨叶: 认识比特币背后的技术是最有意思的事情，并没有买。

Q:投资比特币是在投什么？

杨叶: 比特币相当于股票，去掉那些骗钱的ICO，投的是区块链网络能带来的变革。

Q:这么多的虚拟货币中，为什么比特币会占据主要的市值？

杨叶: 比特币曾经就是虚拟货币的代言人，其交易现在已经降到了币圈的60%左右。现在出现的很多货币的创始人和团队往往拥有了大量的代币，因此有他们自己的经济利益在里面。而中本聪虽然拥有大量比特币，但是没有使用这些币。股票通常是有人做庄的，现在的ICO有很明显做庄的痕迹，而比特币早已经过了割韭菜的阶段，相对而言，比特币更加纯粹。

Q: 挖矿这么耗电力，怎么看?

杨叶: 举个列子，如果去银行取钱，需要用ATM， ATM也要耗电，也需要人维护，还有安全问题，这些都是成本。现金社会的安全运转都需要成本，需要很多人力。而比特币用算力代替了这些人力，物力，未必就是更坏的选择。英国央行曾经指出比特币每年运转所需电量约等于冰岛一年的消耗，以后会达到德国的水平。我个人对能源问题还是比较乐观，石油之后还有其他的能源，只要比特币创造的价值大于其消耗的成本，就是有用的。

Q: 比特币会被政府控制码?

杨叶: 当挖完所有比特币的时候，交易费用是否可以支持比特币网络发展，是一个很大的问号。我不觉得政府有能力控制比特币，但比特币自己是否能长久存在是个疑问。

Q: AI和blockchain哪一个对个人生活影响大？

杨叶: 都大，但在不同层面。Blockchain更加偏向于工程层面，创造了很多编程工作，比如solidity 工程师。AI目前还没有出现first principle, 还是初期发展阶段，前不久Hinton还出了capsule的文章，感兴趣的可以去了解。如果要读 PhD ，最好选AI, 工作的话可以选blockchain。