北京大学肖臻老师《区块链技术与应用》公开课笔记

> 以太坊概述篇，对应肖老师视频：click here 全系列笔记请见：click here **About Me:**点击进入我的Personal Page

BTC和ETH为最主要的两种加密货币，BTC称为区块链1.0，以太坊称为区块链2.0。之前文章中提出了比特币设计中存在某些不足，以太坊便对其进行了改进。例如：出块时间、共识协议、mining puzzle（对内存要求高，反ASIC芯片使用） 未来，以太坊还将会用权益证明(POS)替代工作量证明(POW)

> 2022.10.14补充：以太坊已经完全切换到POS，但后续内容仍然跟着视频走，请理解。 此外，以太坊增加了对**智能合约（smart contract）**的支持。

为什么要开发“智能合约”

BTC本身是一个去中心化的货币，在比特币取得成功之后，很多人就开始思考：除了货币可以去中心化，还有什么可以去中心化？以太坊的一个特性就是增加了对去中心化的合约的支持。 如果说比特币系统本身是一个货币应用，以太坊则由于智能合约，升级成为了一个平台，用户可以依据该平台自行开发业务应用。

关于BTC和ETH

BTC的发明人为中本聪(疑似日本人)，ETH为Vitalik Buterin收到BTC启发发明出来的“”下一代加密货币与去中心化应用平台””。BTC中货币最小单位为“聪”，最少的钱为一聪；ETH中货币最小单位为“Wei”，最少的钱为一Wei。

去中心化的合约

首先，讨论去中心化货币。货币本身由政府发行，政府公信力为其背书，BTC通过技术手段取代了政府的职能。 现实生活中，我们经常提到“契约”或“合约”。合约的有效性也是需要政府进行维护的，如果产生 纠纷需要针对合法性合同进行判决。ETH的设计目的就是，通过技术手段来实现取代政府对于合约的职能。 那么，去中心化的合约有什么好处？ 若合同签署方并非一个国家，没有统一的司法部门（如：众筹）。如果可以编写无法修改的合约，所有人只能按照相关参与方执行，无法违约。

后续内容

后续内容会涉及到以太坊的数据结构、共识机制、挖矿算法(POW和POS)、智能合约。 具体内容，请关注后续文章。