以太坊白皮书

笔记本:	区块链		
创建时间:	2019/10/8 18:27	**更新时间:**	2019/10/14 13:56
作者:	jyyhermance@163.com		

1 历史

比特币账本 = 状态转换系统？比特币所有权状态+状态转换函数
UTXO unspent transaction outputs 未花费的交易输出
挖矿，不断试错以生成新的有效区块，成功即可获得奖励 coinbase （奖励逐渐减少，预计2140年比特币发行完毕）
重复计算区块哈希，不断修改参数，执行SHA256计算，直到与难度目标值匹配
一般攻击交易顺序，利用区块链分叉，算力追赶制造更长的支链
区块哈希：区块头（含时间戳，随机数，上个区块哈希，存储了所有区块交易的默克尔树）的哈希
简化支付确认（SPV）协议： “轻节点”，只下载与交易相关的默克尔树分支
默克尔树
一种二叉树，对树的任何部分进行改变都会导致链上某处不一致
杂凑算法
SHA256 不可预测的为随机函数

比特币脚本语言缺陷:
缺少图灵完备性：不支持循环语句，防止死循环
价值盲 value-blindness：用户取款额度没有精确控制（输出找零）
缺少状态：UTXO只有已花费/未花费状态（初衷是强卖家保护，适合不可退换的商品）
区块链盲 blockchain-blindness：UTXO看不到区块链数据

其他应用:
域名币（namecoin）去中心化的名称注册数据库
彩色币（colored coins）在比特币区块链基础上创建自己的数字货币，为UTXO着色
元币（metacoins）在比特币基础上创建新的协议，状态转换函数'APPLY'不同
共识协议： 建立独立网络（实施困难）/在比特币网络上建立协议（不继承SPV特性）

2 以太坊

以太坊 -> 提供一个带有内置的成熟的图灵完备语言的区块链（以太坊虚拟机 Ethereum Virtual Machine）
开源的，基于区块链技术的，具有智能合约功能的公开分布式计算平台
价值协议 + 价值协议搭建的价值网络 + 网络上运行的分布式应用及生态
智能合约： 根据事先任意制定的规则来自动转移数字资产
智能合约存储在公网上的每一个节点，导致性能损失很大

以太坊的目的是基于脚本、竞争币和链上元协议（on-chain meta-protocol）概念进行整合和提高，使得开发者能够创建任意的基于共识的、可扩展
的、标准化的、特性完备的、易于开发的和协同的应用。以太坊通过建立终极的抽象的基础层-内置有图灵完备编程语言的区块链-使得任何人都能够创
建合约和去中心化应用并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。
共识机制更为高效
图灵完备性
支持智能合约
账户包含:

随机数，确保每笔交易只被处理一次
账户的以太币余额
账户的合约代码
账户的存储
一般而言，以太坊有两种类型的账户：外部所有的账户（由私钥控制的）和合约账户（由合约代码控制）1
外部所有的账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息
每当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，和发送其它消息或者创建合约

以太币 Ether：
在节点间传递/用作参与节点公式计算的助燃剂（gas）-> 交易有成本，需要付出费用，防止无用交易和资源浪费

操作可以访问三种数据类型空间：
堆栈
内存
合约的长期存储
以太坊区块含交易记录，最近的状态，区块序号和难度值
提升确认效率 --> Patricia Tree，允许改变、插入和删除节点，不必存储全部的区块历史

3 应用
金融：子货币，金融衍生品，对冲合约，储蓄钱包，遗嘱，一些雇佣合约
半金融：为解决计算问题而设的自我强制悬赏
非金融：在线投票，去中心化治理

4 杂项
改进版幽灵协议
作废的区块，叔区块，也加入最长链证明。防止算力大的矿池对挖矿过程掌控过大。
以太坊产生新区块的速度远远大于比特币，会带来分叉问题和区块作废问题，甚至区块有可能连续作废，在未被纳入主链的孤区块后持续挖矿
货币和发行
伟，萨博【12】，芬尼【15】，以太【18】
X + 0.099X + 0.099X
图灵完备
循环实现：条件语句/调用合约
最大计算步数STRAT 每步消耗瓦斯 GASPRICE
瓦斯耗尽，则计算停止，被恢复原状，但交易费用已被扣除（防止陷入恶意无限循环问题
抵御挖矿的日益中心化（硬件要求上升，矿池所占算力份额过大
抵御中心化风险（SVP带来的欺诈风险