

[https://www.bilibili.com/video/BV1Ca411n7ta?
p=3&spm_id_from=pageDriver&vd_source=9d36b198f5426d1b8930b3600065dd35](https://www.bilibili.com/video/BV1Ca411n7ta?p=3&spm_id_from=pageDriver&vd_source=9d36b198f5426d1b8930b3600065dd35)

blockchain basic

智能合约的作用

- blockchain oracle 区块链预言机
- hyper smart contract : 混合智能合约
DApp, 去中心化协议, 智能合约应用, 去中心化应用 都是同一个东西

智能合约是什么

contract/agreement = promises 电器, 木材 任何事情都可以看作是一个对另外一个对承诺
broken promises

视频里面说的深入理解 智能合约部署在去中心化区块链 结合去中心化的预言机网络获取真实世界资产和信息 实现不可能更改 找链接 (youtube原版)

细节需要了解

优势：去中心化，去中介化，数据和资产更加安全，很难被攻击，很难被操纵

第一笔交易

Overview State

[This is a Rinkeby Testnet transaction only]

⑦ Transaction Hash:	0x8b8ff2c073b26d8fbe938d32835384d5904284aecdbfc919eeaaee1fb2c5e0e7
⑦ Status:	Success
⑦ Block:	10394763 45 Block Confirmations
⑦ Timestamp:	11 mins ago (Mar-26-2022 04:09:16 PM +UTC)
⑦ From:	0xa7a82dd06901f29ab14af63faf3358ad101724a8
⑦ To:	0x1066618d0973e44efd2fe5114fd18b64c6420abb
⑦ Value:	0.1 Ether (\$0.00)
⑦ Transaction Fee:	0.000052500000483 Ether (\$0.00)
⑦ Gas Price:	0.0000000025000000 Ether (\$0.00)

最上面的这个是交易哈希

Gas

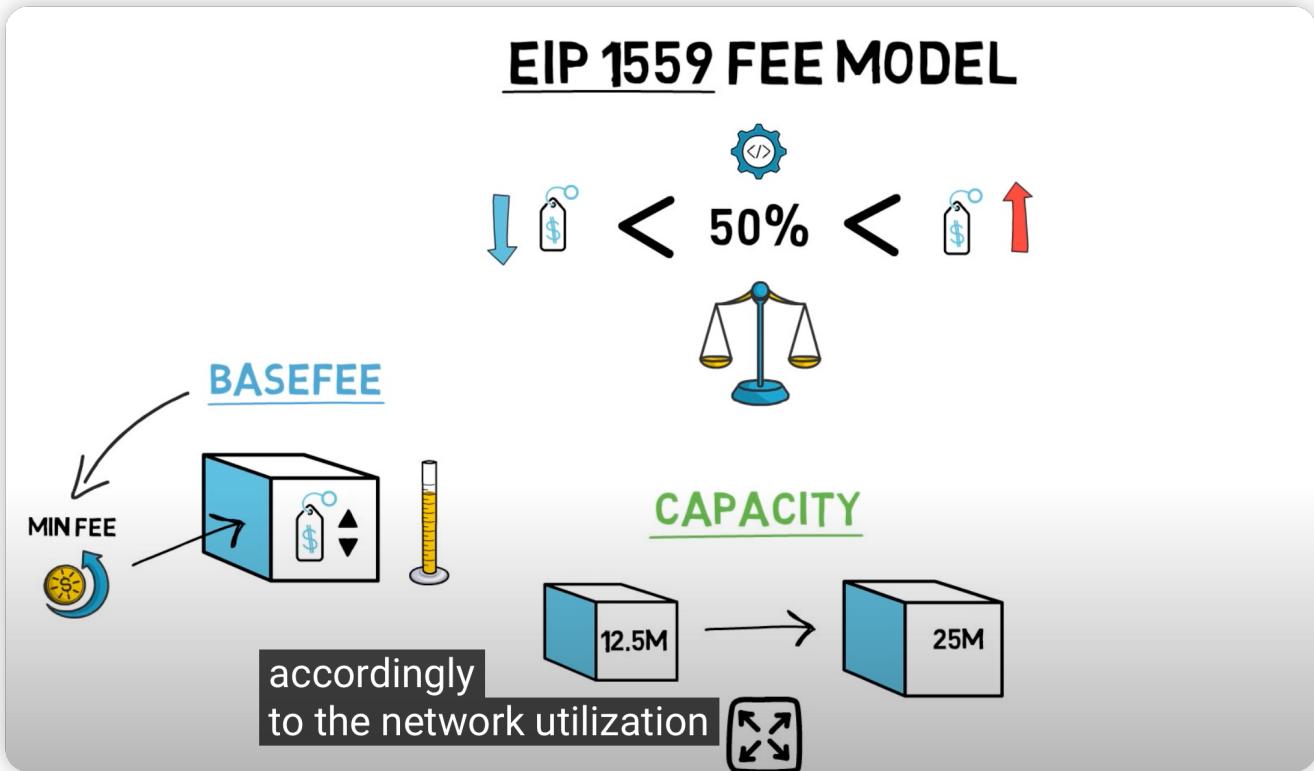
gas fee x gas amount = transaction fee

总费用=(区块基础费+ 最大优先费 per gas) * gas 使用数量

base fee 会被算法调整适配, 调整的目标是期望每个区块被写入50%

EIP 1559

ETHEREUM IMPROVEMENT PROPOSAL



区块链运作机制

sha256 hash: A unique fixed length string, meant to **identify** a piece of data. They are created by placing said data into a "hash function"
<https://andersbrownworth.com/blockchain/block>

ETH: keccak256哈希算法,

Nonce: A "number used once" to find the "solution" to the blockchain problem. It's also used to define the transaction number for an account/address.

区块block：寻找一个nonce符合，哈希条件

区块:	#	1
随机数:	40910	
数据:	fdfasdfewrfwerewrfwe	
哈希:	0000e963dc0550bb4f910fe66a60ab991318798928d6da03c2f87a85d3c8ae62	
<button>挖矿</button>		

区块链：多了一个prev节点 进行计算哈希

前一个节点全是00000.的称为创世块

分布式： 多处运行这些区块

代币Token

签名和验证 私钥和公钥

Signing a transaction: A "one way" process. Someone with a private key signs a transaction by their private key being hashed with their transaction data. Anyone can then verify this new transaction

hash with your public key.

1 Private key |> Public Key > Address

共识机制

中本聪共识

chain selection 链选择

- 最长链 选择 (btc and eth) : 哪条链最长 有最多的区块就用哪条

sybil resistance

Sybil Attack, 中文翻译为“女巫攻击”，2002年由John R. Douceur在《the Sybil Attack》提出，它是p2p网络中的一种攻击形式，攻击者利用单个节点来伪造多个身份，是攻击数据冗余机制的一种有效手段。

- 工作量证明 PoW Proof-of-Work

采用POW工作量证明机制，要证明你是一个节点，就要用计算能力证明，这只是意味着攻击成本极大的增加而已。

在工作量证明的网络中，叫矿工。在权益证明的网络中，叫验证者

- 权益证明 PoS Proof-of-Stake

在权益证明中，节点会被直接选举出来，然后提出一个区块，别的节点会验证这个被提出的区块是否有效

随机数选择==== RanDao

- DPoS 委托权益证明机制

sharding 分片 可扩展性

区块链的分片指的是多个区块链的区块链，有一个主链 协调 其他链

Layer 1: Base layer blockchain implementation

Layer 2: Any application built on top of a layer 2

Rollups: 把它们自己的交易集中起来，然后写入以太坊这样的 layer 1中，rollup 类似于一个分片的链，它继承了以太坊这样的基础链也就是 layer1 的安全性，都会把交易写进 layer1

Optimistic : dispute resolution system

ZK zero knowledge

侧链：安全性来自自身协议 更高的效率