

北京大学肖臻老师《区块链技术与应用》公开课笔记

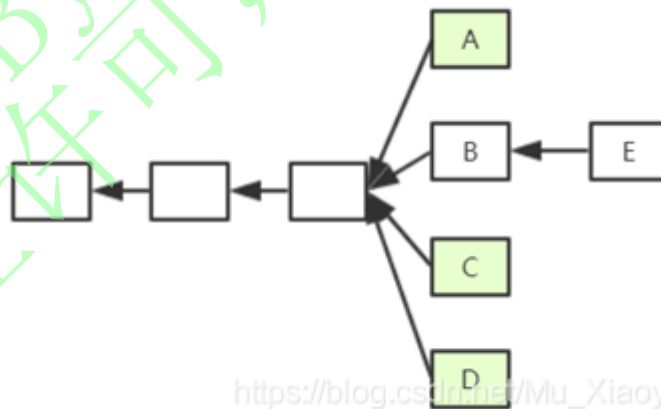
以太坊GHOST协议，对应肖老师视频：[click here](#) 全系列笔记请见：[click here](#) About Me:[点击进入我的Personal Page](#)

BTC系统中出块时间为10min，而以太坊中出块时间被降低到15s左右，虽然有效提高了系统反应时间和吞吐率，却也导致系统临时性分叉变成常态，且分叉数目更多。这对于共识协议来说，就存在很大挑战。在BTC系统中，不在最长合法链上的节点最后都是作废的，但如果在以太坊系统中，如果这样处理，由于系统中经常性会出现分叉，则矿工挖到矿很大可能会被废弃，这会大大降低矿工挖矿积极性。而对于个人矿工来说，和大型矿池相比更是存在天然劣势。对此，以太坊设计了新的公式协议——GHOST协议(该协议并非原创，而是对原本就有的Ghost协议进行了改进)。

GHOST协议

GHOST协议最初版本

如图，假定以太坊系统存在以下情况，A、B、C、D在四个分支上，最后，随着时间推移B所在链成为最长合法链，因此A、C、D区块都作废，但为了补偿这些区块所属矿工所作的工作，给这些区块一些“补偿”，并称其为"Uncle Block"（叔父区块）。规定E区块在发布时可以将A、C、D叔父区块包含进来，A、C、D叔父区块可以得到出块奖励的7/8，而为了激励E包含叔父区块，规定E每包含一个叔父区块可以额外得到1/32的出块奖励。为了防止E大量包含叔父区块，规定一个区块只能最多包含两个叔父区块，因此E在A、C、D中最多只能包含两个区块作为自己的出块奖励



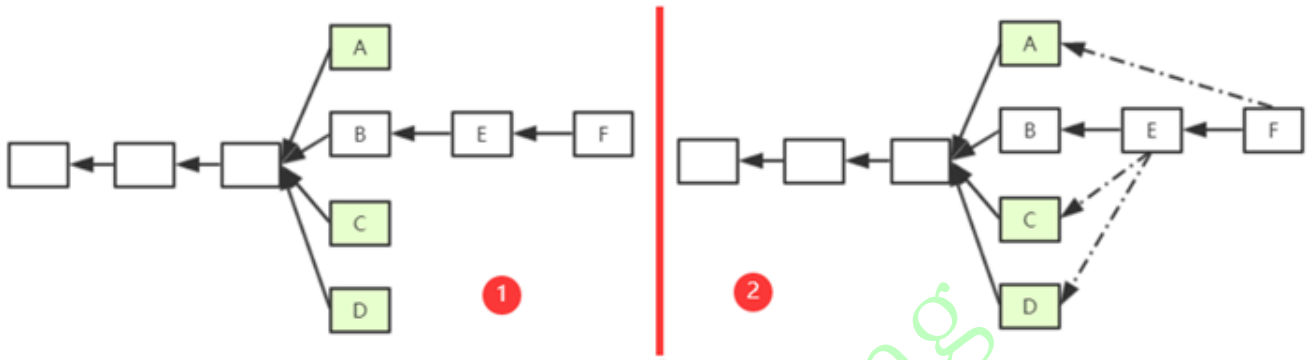
假定一个矿工挖出了B，此时他沿着其所在链继续挖，而他知道A是和自己“同辈”，则可以将A包含进区块挖矿，若挖矿过程中又听到C也是“同辈”，则可以停止挖矿，将C包含进来重新组织成一个新区块重新挖矿，实际中，由于挖矿过程的无记忆性，这样并不会降低成功挖到矿的概率。

最初版本缺陷：

1. 因为叔父区块最多只能包含两个，如图出现3个怎么办？
2. 矿工自私，故意不包含叔父区块，导致叔父区块7/8出块奖励没了，而自己仅仅损失1/32。如果甲、乙两个大型矿池存在竞争关系，那么他们可以采用故意不包含对方的叔父区块，因为这样对自己损失小而对方损失大。

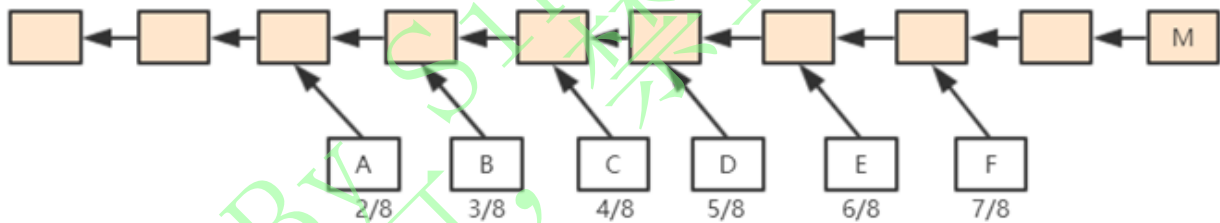
Ghost协议新的版本

如下图中1为对上面例子的补充，F为E后面一个新的区块。因为规定E最多只能包含两个叔父区块，所以假定E包含了C和D。此时，F也可以将A认为自己的叔父区块(实际上并非叔父辈的，而是爷爷辈的)。如果继续往下挖，F后的新区块仍然可以包含B同辈的区块(假定E、F未包含完)。这样，就有效地解决了上面提到的最初Ghost协议版本存在的缺陷。



但这样仍然存在一定的问题。

我们将“叔父”这个概念进行扩展，但问题在于，“叔父”这一定义隔多少代才好呢？如下图所示，M为该区块链上一个区块，F为其严格意义上的叔父，E为其严格意义上的“爷爷辈”。以太坊中规定，如果M包含F辈区块，则F获得7/8出块奖励；如果M包含E辈区块，则F获得6/8出块奖励，以此类推向前。直到包含A辈区块，A获得2/8出块奖励，再往前的“叔父区块”，对于M来说就不再认可其为M的“叔父”了。对于M来说，无论包含哪个辈分的“叔父”，得到的出块奖励都是1/32出块奖励。也就是说，叔父区块的定义是和当前区块在七代之内有共同祖先才可（合法的叔父只有6辈）。



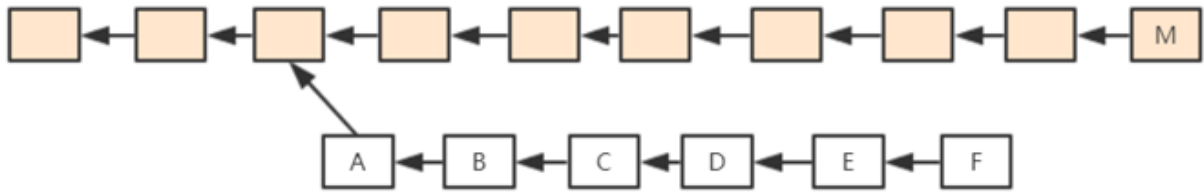
这样，就方便了全节点进行记录，此外，也从协议上鼓励一旦出现分叉马上进行合并。

以太坊中的奖励：

BTC：静态奖励(出块奖励)+动态奖励(交易费，占据比例很小) ETH：静态奖励(出块奖励+包含叔父区块的奖励)+动态奖励(汽油费，占据比例很小，叔父区块没有) BTC中为了人为制造稀缺性，比特币每隔一段时间出块奖励会降低，最终当出块奖励趋于0后会主要依赖于交易费运作。而以太坊中并没有人为规定每隔一段时间降低出块奖励。

以太坊中包含了叔父区块，要不要包含叔父区块中的交易？不应该，叔父区块和同辈的主链上区块有可能包含有冲突的交易。而且我们前文也提到，叔父区块是没有动态奖励的。因此，一个节点在收到一个叔父区块的时候，只检查区块合法性而不检查其中交易的合法性。

当然，对于分叉后的堂哥区块怎么办？例如下图所示，A->F该链并非一个最长合法链，所以B->F这些区块怎么办？该给挖矿补偿吗？如果规定将下面整条链作为一个整体，给予出块奖励，这一定程度上鼓励了分叉攻击(降低了分叉攻击的成本，因为即使攻击失败也有奖励获得)。因此，ETH系统中规定，只认可A区块为叔父区块，给予其补偿，而后的区块全部作废。



以太坊真实数据

[Etherscan网站](#), 该网站可以实时观看以太坊的数据。以下截图为我为于2020/2/28截的图, 和肖老师视频中截图存在一定差异。但具体内容基本一致。

未经许可, 禁止商用。
By Sinocifeng

Sponsored: AMFEIX - INVEST WITH AMFEIX (45%+ Estimated APR). Check it out on AMFEIX.com.

Ethereum Blockchain Explorer

与你同在，加油！

All Filters Search by Address / Txn Hash / Block / Token / Ens

Search

ETHER PRICE \$230.21 @ 0.026 BTC (+5.21%)

LATEST BLOCK 9569855 (13.3s)

TRANSACTIONS 647.39 M (8.9 TPS)



MARKET CAP \$25,295,976,794.269

DIFFICULTY 2,328.38 TH

HASH RATE 180,959.84 GH/s

Sponsored



INVEST WITH AMFEIX (45%+ Estimated APR) To invest with AMFEIX you first need blocks which you can buy from us or others. VISIT OUR WEBSITE FOR FURTHER DETAILS. CHECK IT OUT ON AMFEIX.COM

AMFEIX.COM



最新被挖出的区块

最新执行的交易

Latest Blocks

Bk	9569855	Miner Ethermine	2.06899 Eth
	25 secs ago	198 txns in 7 secs	
Bk	9569854	Miner Mining Express	2.07017 Eth
	32 secs ago	165 txns in 11 secs	
Bk	9569853	Miner Spark Pool	2.20978 Eth
	43 secs ago	105 txns in 19 secs	
Bk	9569852	Miner 0x652d38d814...	2.10997 Eth
	1 min 2 secs ago	150 txns in 6 secs	
Bk	9569851	Miner Spark Pool	2.08422 Eth
	1 min 8 secs ago	95 txns in 34 secs	

View all blocks

Latest Transactions

Tx	0x3b9848b...	From 0x121671cc368...	0.06 Eth
	25 secs ago	To 0xfa4b1bbfd3fb...	
Tx	0x0b02117...	From 0x780f94e09fa...	0.31775 Eth
	25 secs ago	To 0x7f8e61f6660...	
Tx	0xaf6590...	From 0xe91ef3d2494...	0.13045 Eth
	25 secs ago	To 0xf52fe31b843...	
Tx	0x897ecd5...	From 0x272c1feaae0...	0.005 Eth
	25 secs ago	To 0x37435da073c...	
Tx	0x22215ab...	From 0x8e6a6bf6b6d...	8.47818 Eth
	25 secs ago	To 0x885fed5c5a7...	

View all transactions

Chrome浏览器中文翻译后页面:

主办单位: AMFEIX - INVEST WITH AMFEIX (45%+估计APR)。在AMFEIX.com上进行检查。

以太坊区块链资源管理器

与你同在，加油！

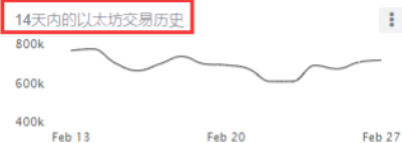
所有筛选 按地址搜索/ Txn哈希/块/令牌/ Ens

搜索

乙醚价格 \$230.21 @ 0.026 BTC (+5.21%)

最新块 9569860 (13.3秒)

交易次数 647.39 M (8.9 TPS)



市值 \$25,295,976,794.269

困难 2,328.38泰铁

哈希率 180,959.84 GH/秒

赞助商



INVEST WITH AMFEIX (45%+ Estimated APR) To invest with AMFEIX you first need blocks which you can buy from us or others. VISIT OUR WEBSITE FOR FURTHER DETAILS. CHECK IT OUT ON AMFEIX.COM

AMFEIX.COM



最新块

最新交易

k	9569860 58秒前	30秒内 Miner Nanopool 76 txns	2.0591 Eth	Tx	0x6261299... 58秒前	从0x477b8d5ef7c... 到0xdac17f958d2...	0 Eth
k	9569859 1分27秒前	矿工BTC.com池 161 txns 在2秒内	2.07219 Eth	Tx	0x352437b... 58秒前	从0xe484233af7c... 到0x435d4183ae...	0 Eth
k	9569858 1分29秒前	矿工Ethermine 130 txns 在22秒内	2.10876以太	Tx	0x0f9ee08... 58秒前	从0x6f5b5668159... 到0xdac17f958d2...	0 Eth
k	9569857 1分51秒	Miner Zhizhu.35 秒内	2.045 Eth	Tx	0x974c736... 58秒前	从0x98a70481d6... 到0x2d625b7bcae...	0 Eth
				Tx	0x379b25a... 58秒前	从0xc71e874e1b0... 到0x661f3361afb...	0 Eth

查看所有方块 [查看所有交易](#) https://blog.csdn.net/MU_Xiaoye

在视频中，肖老师还根据该网站上区块信息分析了GHOST协议中叔父区块奖励等信息，这里不再赘述。

未经许可，禁止商用。
By Sinoclife