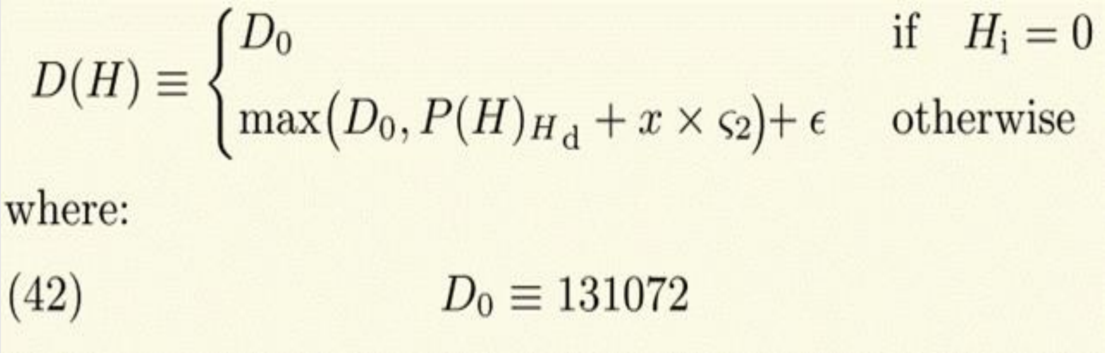
以太坊难度调整算法

现行版本



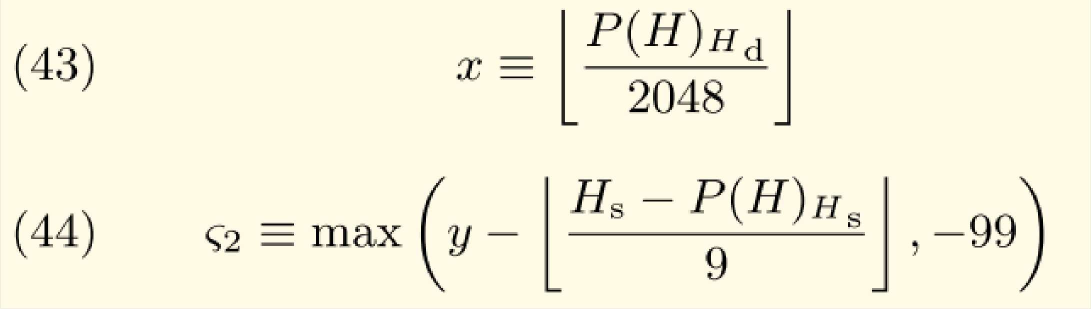
$$D(H) \equiv \begin{cases} D_0 & \text{if} \quad H_{\mathrm{i}} = 0 \\ \max\left(D_0, P(H)_{H_{\mathrm{d}}} + x \times \varsigma_2\right) + \epsilon & \text{otherwise} \end{cases}$$

where:

(42) $$D_0 \equiv 131072$$

- $D(H)$是本区块的难度，由基础部分$P(H)_{Hd} + x \times \varsigma_2$和难度炸弹部分 ϵ 相加得到。
  - $P(H)_{Hd}$为父区块的难度，每个区块的难度都是在父区块难度的基础上进行调整。
  - $x \times \varsigma_2$ 用于自适应调节出块难度，维持稳定的出块速度。
  - ϵ 表示设定的难度炸弹。
- 基础部分有下界，为最小值$D_0 = 131072$。

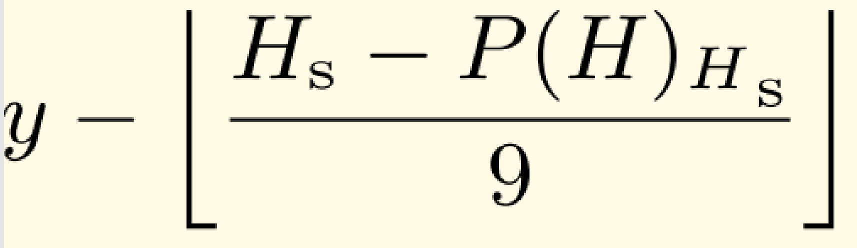
自适应难度调整 $x \times \varsigma_2$



$$x \equiv \left\lfloor \frac{P(H)_{H_{\mathrm{d}}}}{2048} \right\rfloor \tag{43}$$

$$\varsigma_2 \equiv \max\left(y - \left\lfloor \frac{H_{\mathrm{s}} - P(H)_{H_{\mathrm{s}}}}{9} \right\rfloor, -99\right) \tag{44}$$

- x是调整的单位，ς_2为调整的系数。
- y和父区块的uncle数有关。如果父区块中包括了uncle，则y为2，否则为1。
    - 父块包含uncle时难度会大一个单位，因为包含uncle时新发行的货币量大，需要适当提高难度以保持货币发行量稳定。
- 难度降低的上界设置为−99，主要是应对被黑客攻击或其他目前想不到的黑天鹅事件。



$$y - \left\lfloor \frac{H_s - P(H)_{H_s}}{9} \right\rfloor$$

- H_s是本区块的时间戳，$P(H)_{H_s}$是父区块的时间戳，均以秒为单位，并规定$H_s > P(H)_{H_s}$。
  - 该部分是稳定出块速度的最重要部分：出块时间过短则调大难度，出块时间过长则调小难度。
- 以父块不带uncle的情况$(y = 1)$为例：
  - 出块时间在[1,8]之间，出块时间过短，难度调大一个单位。
  - 出块时间在[9,17]之间，出块时间可以接受，难度保持不变。
  - 相差时间在[18,26]之间，出块时间过长，难度调小一个单位。
  - …

难度炸弹ϵ

$$\epsilon \equiv \left\lfloor 2^{\left\lfloor H'_{\mathrm{i}} \div 100000 \right\rfloor - 2} \right\rfloor$$

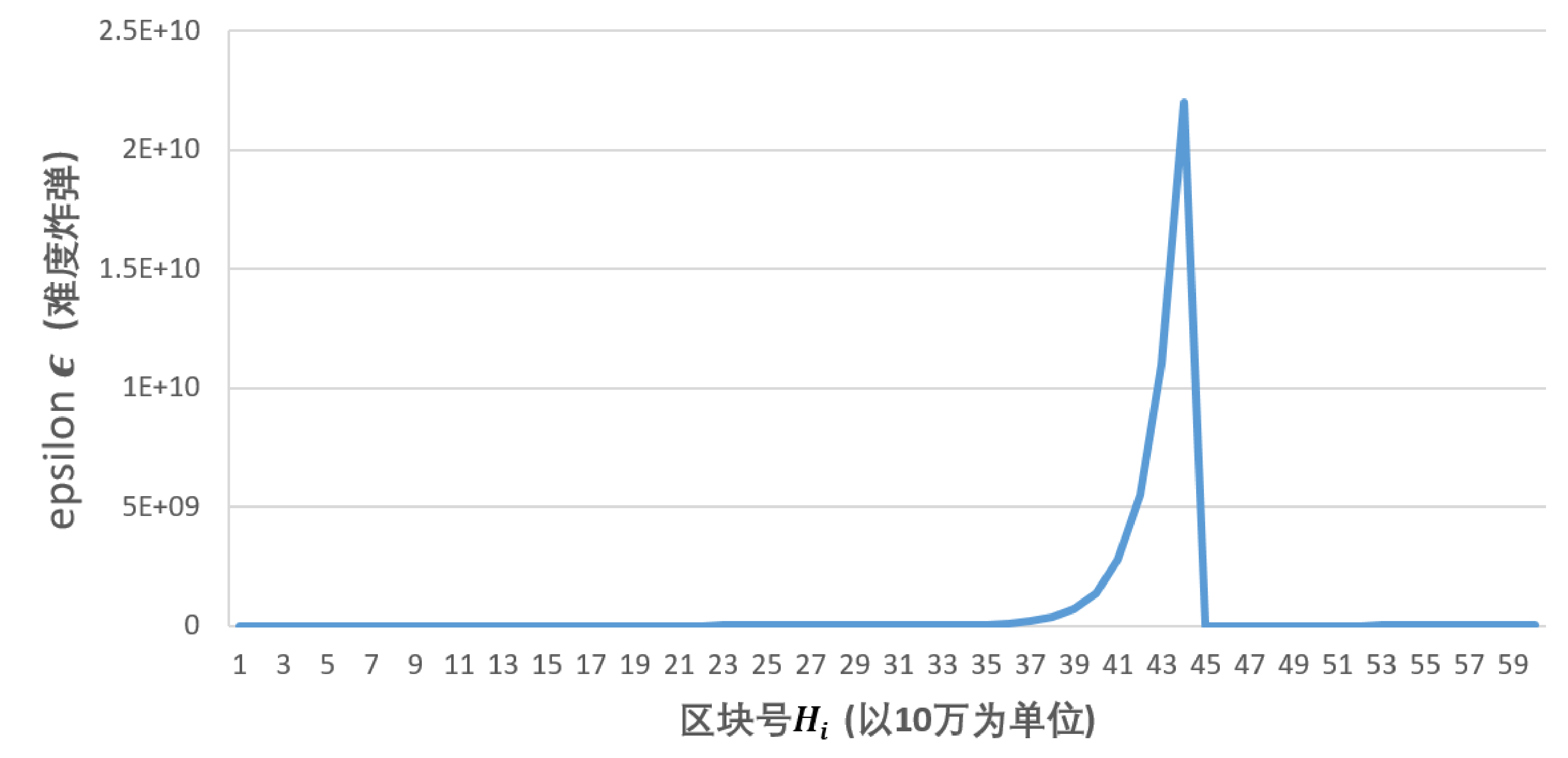
$$H'_{\mathrm{i}} \equiv \max(H_{\mathrm{i}} - 3000000, 0)$$

- ➢ ϵ每十万个块扩大一倍，是2的指数函数，到了后期增长非常快，这就是难度“炸弹”的由来。

- ➢ 设置难度炸弹的原因是要降低迁移到PoS协议时发生fork的风险：到时挖矿难度非常大，所以矿工有意愿迁移到PoS协议。

- ➢ H'_i称为fake block number，由真正的block number H_i减少三百万得到。这样做的原因是低估了PoS协议的开发难度，需要延长大概一年半的时间(EIP100)。

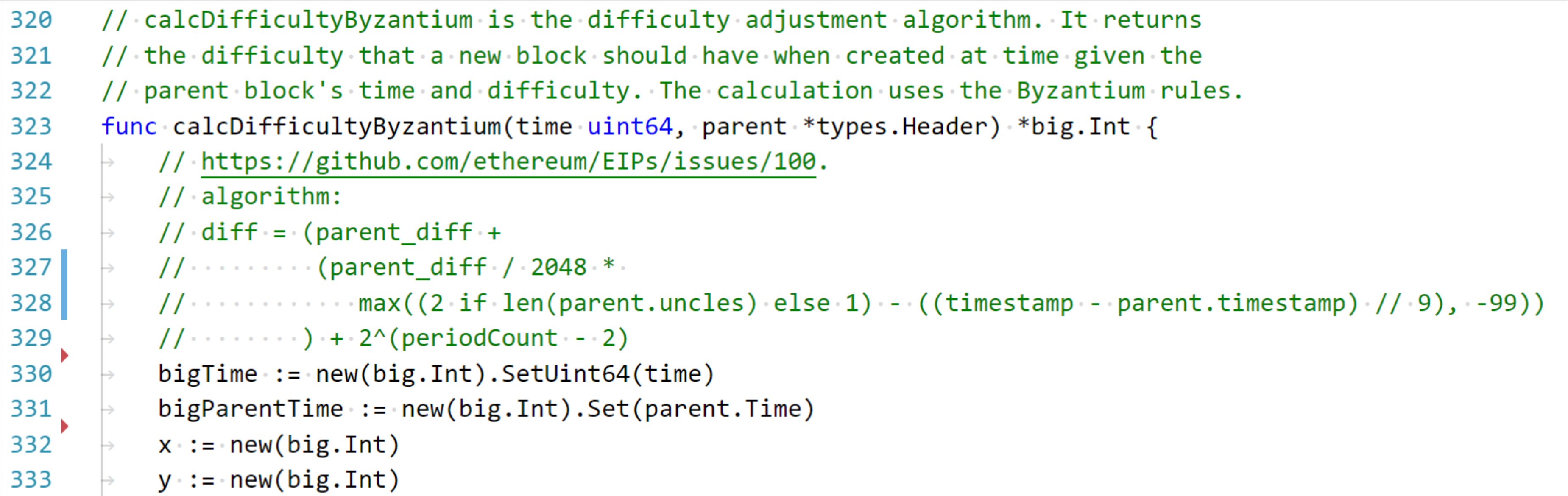
难度炸弹（difficulty bomb）的威力



以太坊发展的四个阶段

- Frontier
- Homestead
- Metropolis
  - 又分为Byzantium和Constantinople两个子阶段
  - 难度炸弹的回调发生在Byzantium这个子阶段，在EIP（Ethereum Improvement Proposal）中决定
  - 同时把block reward从5个ETH降为3个ETH
- Serenity

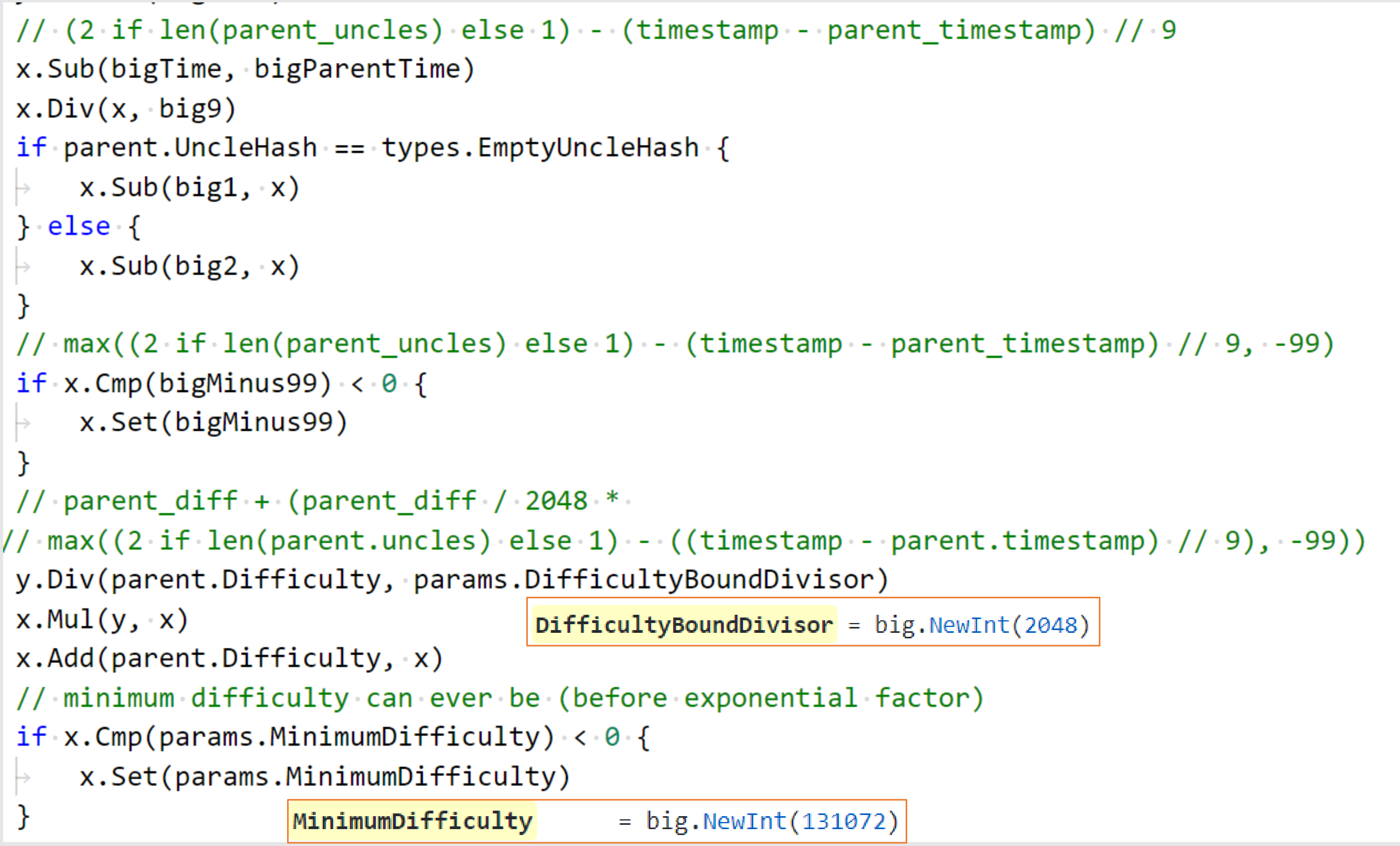
具体代码实现



```go
// calcDifficultyByzantium is the difficulty adjustment algorithm. It returns
// the difficulty that a new block should have when created at time given the
// parent block's time and difficulty. The calculation uses the Byzantium rules.
func calcDifficultyByzantium(time uint64, parent *types.Header) *big.Int {
	// https://github.com/ethereum/EIPs/issues/100.
	// algorithm:
	// diff = (parent_diff +
	//         (parent_diff / 2048 * 
	//            max((2 if len(parent.uncles) else 1) - ((timestamp - parent.timestamp) // 9), -99))
	//        ) + 2^(periodCount - 2)
	bigTime := new(big.Int).SetUint64(time)
	bigParentTime := new(big.Int).Set(parent.Time)
	x := new(big.Int)
	y := new(big.Int)
```

/go-ethereum/consensus/ethash/consensus.go

基础部分的计算

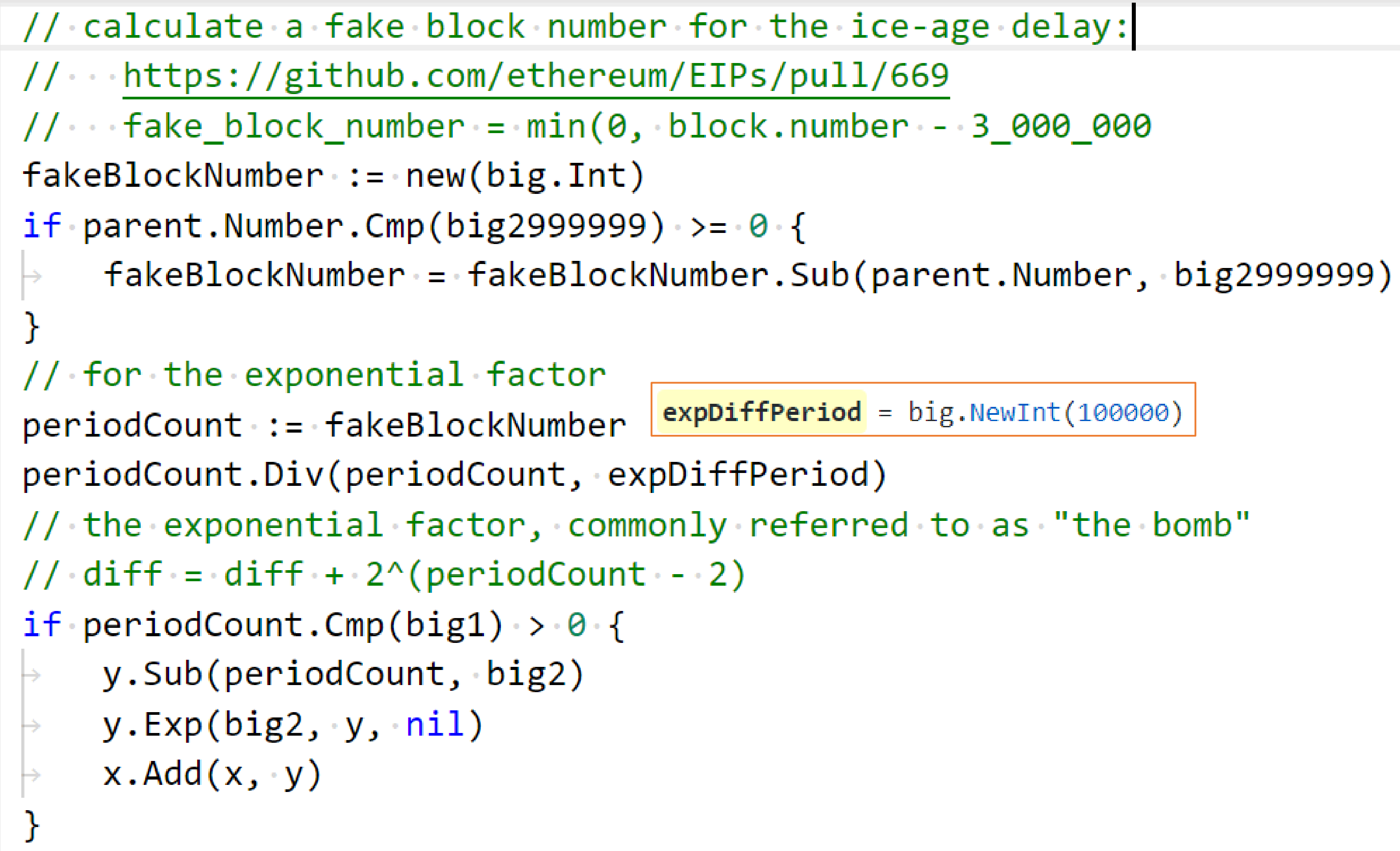


```
// (2 if len(parent_uncles) else 1) - (timestamp - parent_timestamp) // 9
x.Sub(bigTime, bigParentTime)
x.Div(x, big9)
if parent.UncleHash == types.EmptyUncleHash {
    x.Sub(big1, x)
} else {
    x.Sub(big2, x)
}
// max((2 if len(parent_uncles) else 1) - (timestamp - parent_timestamp) // 9, -99)
if x.Cmp(bigMinus99) < 0 {
    x.Set(bigMinus99)
}
// parent_diff + (parent_diff / 2048 *
// max((2 if len(parent.uncles) else 1) - ((timestamp - parent.timestamp) // 9), -99))
y.Div(parent.Difficulty, params.DifficultyBoundDivisor)
x.Mul(y, x)
x.Add(parent.Difficulty, x)
// minimum difficulty can ever be (before exponential factor)
if x.Cmp(params.MinimumDifficulty) < 0 {
    x.Set(params.MinimumDifficulty)
}
```

```
DifficultyBoundDivisor = big.NewInt(2048)
```

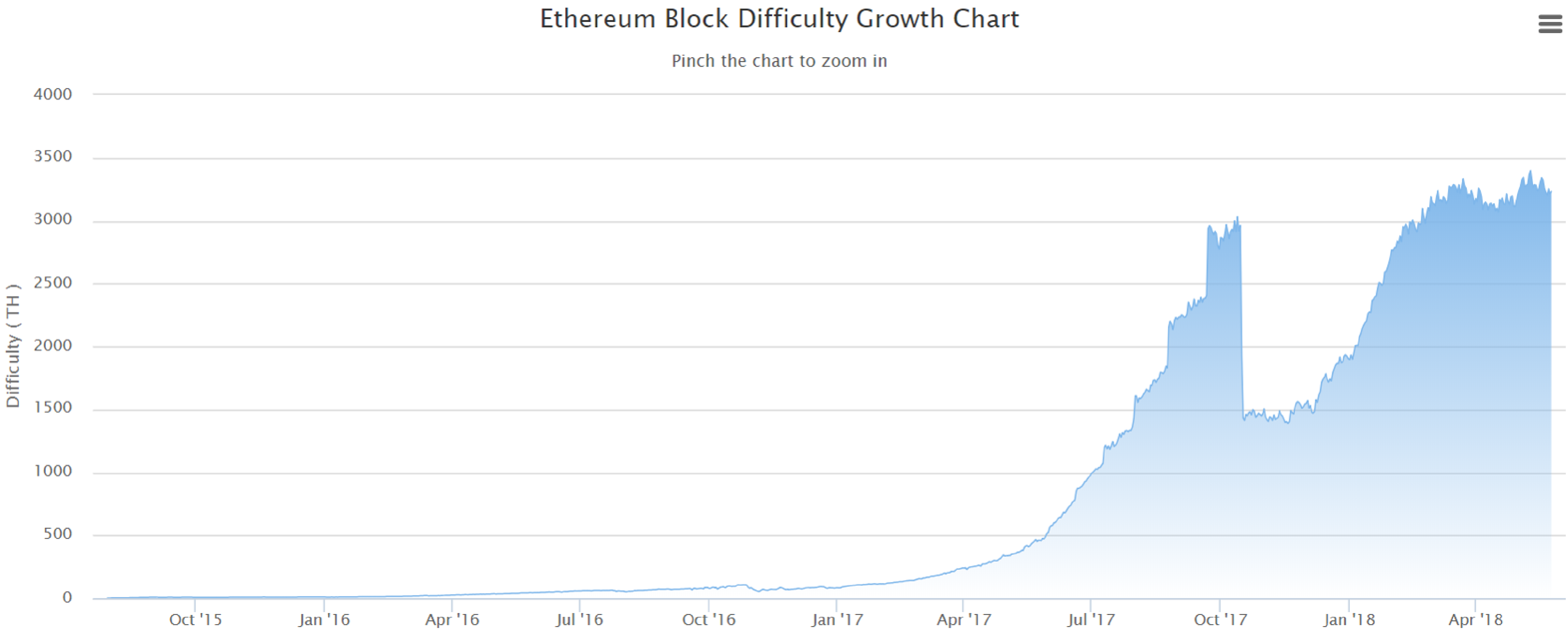
```
MinimumDifficulty      = big.NewInt(131072)
```

难度炸弹的计算

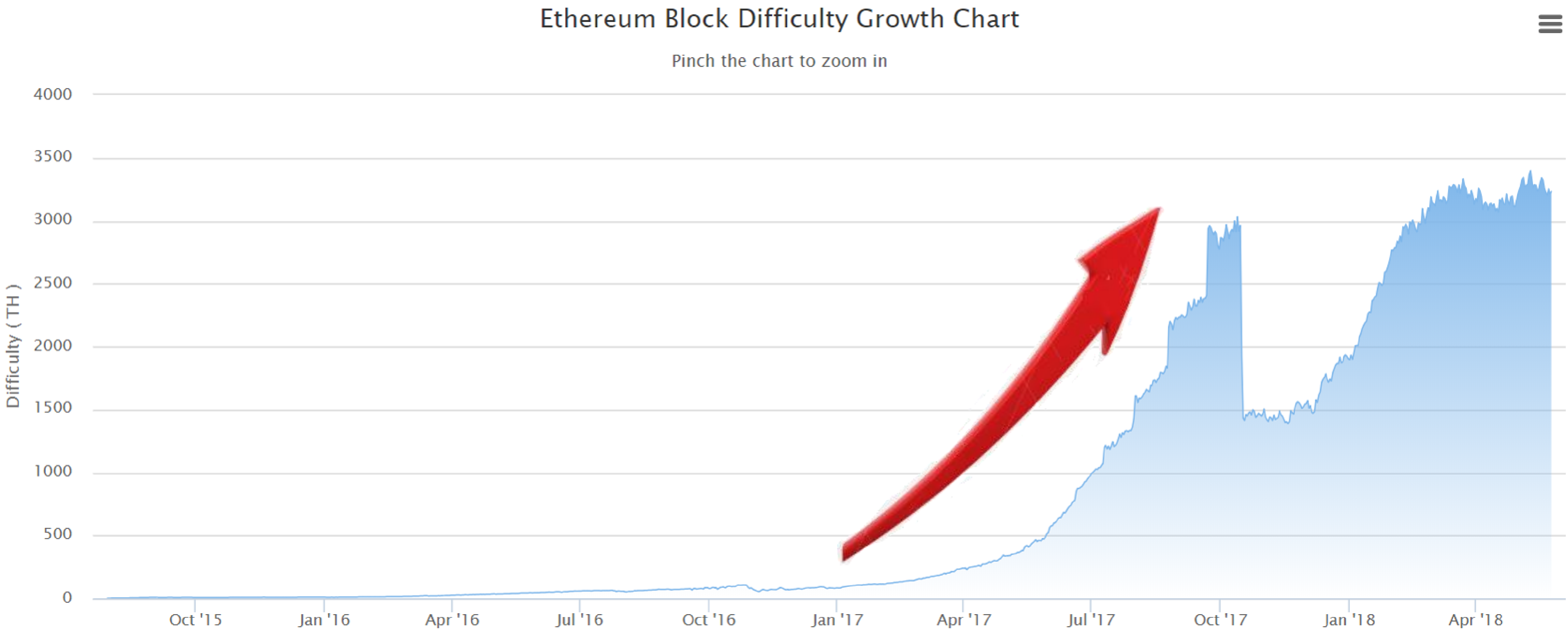


```go
// calculate a fake block number for the ice-age delay:
//   https://github.com/ethereum/EIPs/pull/669
//   fake_block_number = min(0, block.number - 3_000_000
fakeBlockNumber := new(big.Int)
if parent.Number.Cmp(big2999999) >= 0 {
	fakeBlockNumber = fakeBlockNumber.Sub(parent.Number, big2999999)
}
// for the exponential factor
periodCount := fakeBlockNumber
periodCount.Div(periodCount, expDiffPeriod)
// the exponential factor, commonly referred to as "the bomb"
// diff = diff + 2^(periodCount - 2)
if periodCount.Cmp(big1) > 0 {
	y.Sub(periodCount, big2)
	y.Exp(big2, y, nil)
	x.Add(x, y)
}
```

```go
expDiffPeriod = big.NewInt(100000)
```



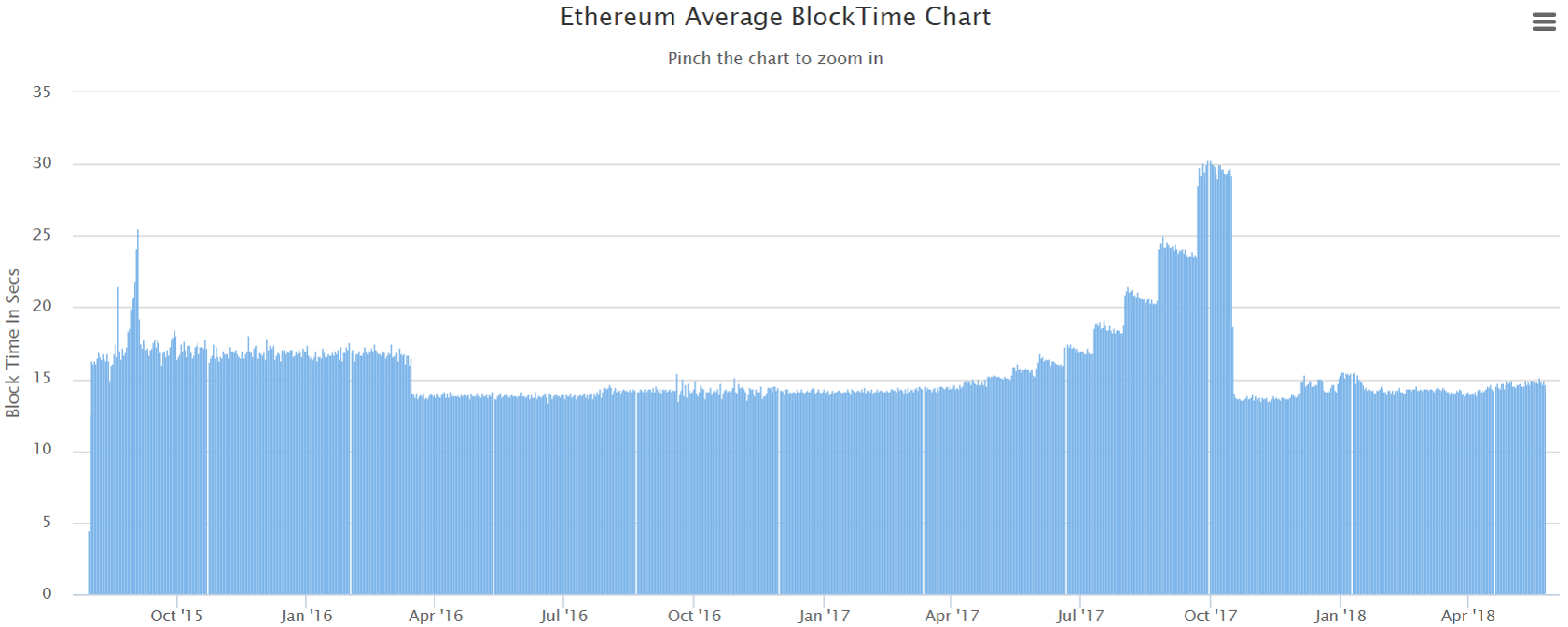
Source:Etherscan.io



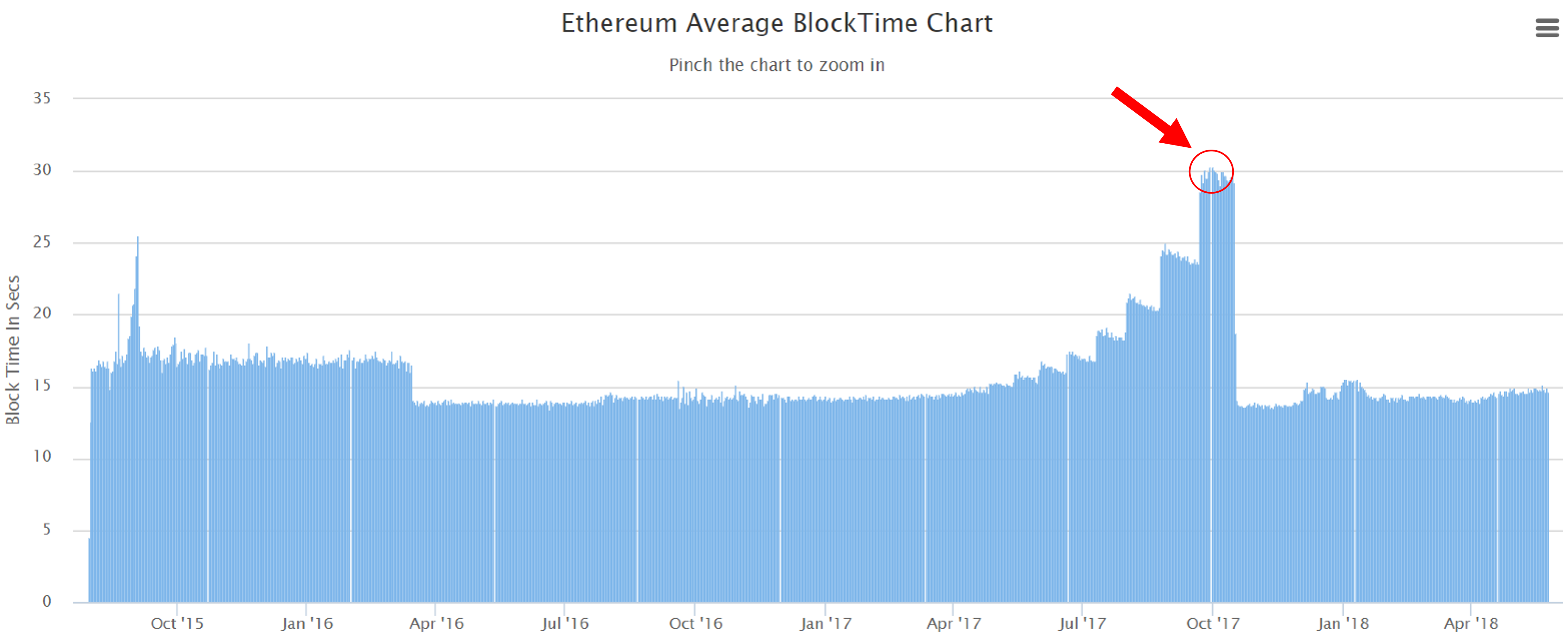
Ethereum Block Difficulty Growth Chart

Pinch the chart to zoom in

Source:Etherscan.io



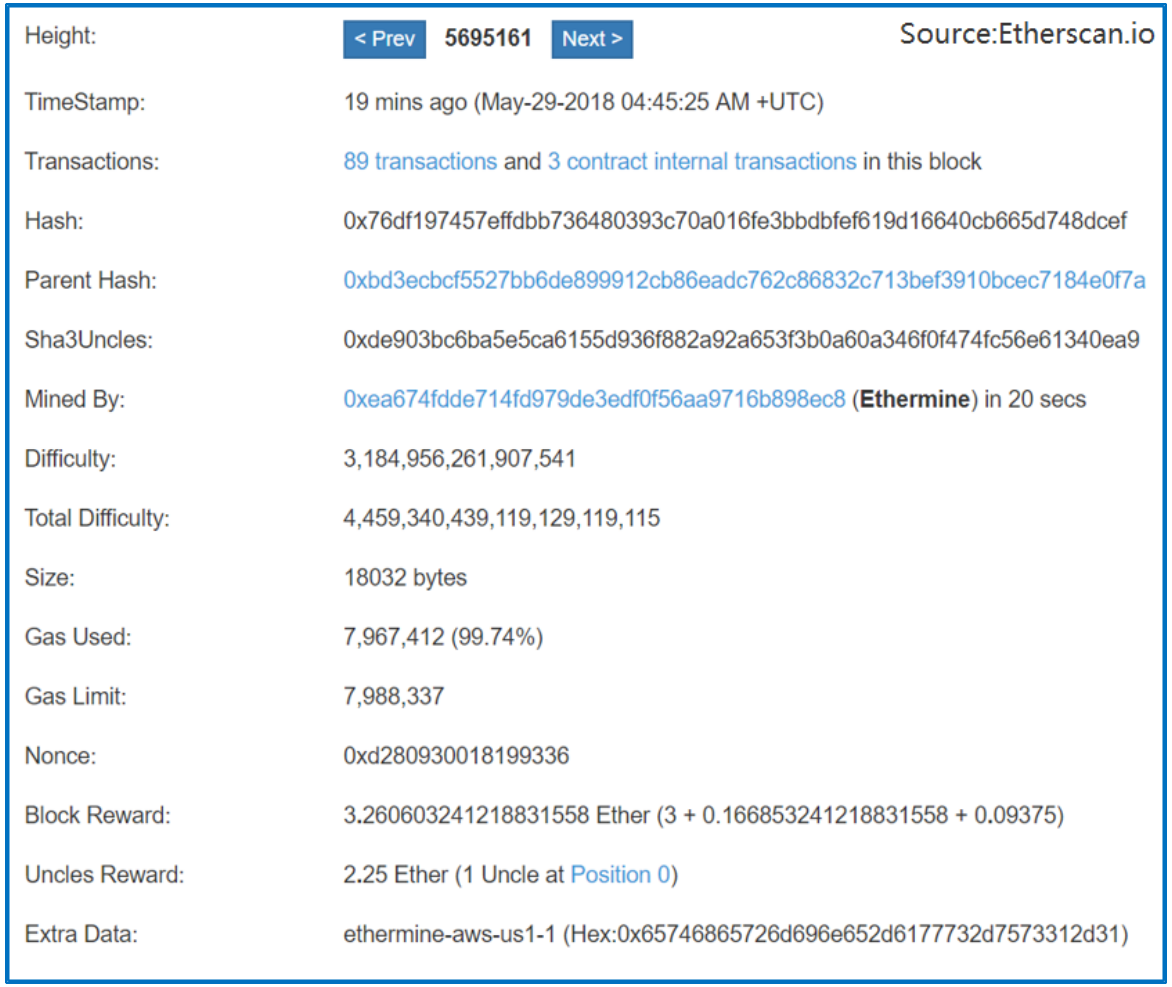
Source:Etherscan.io



Ethereum Average BlockTime Chart

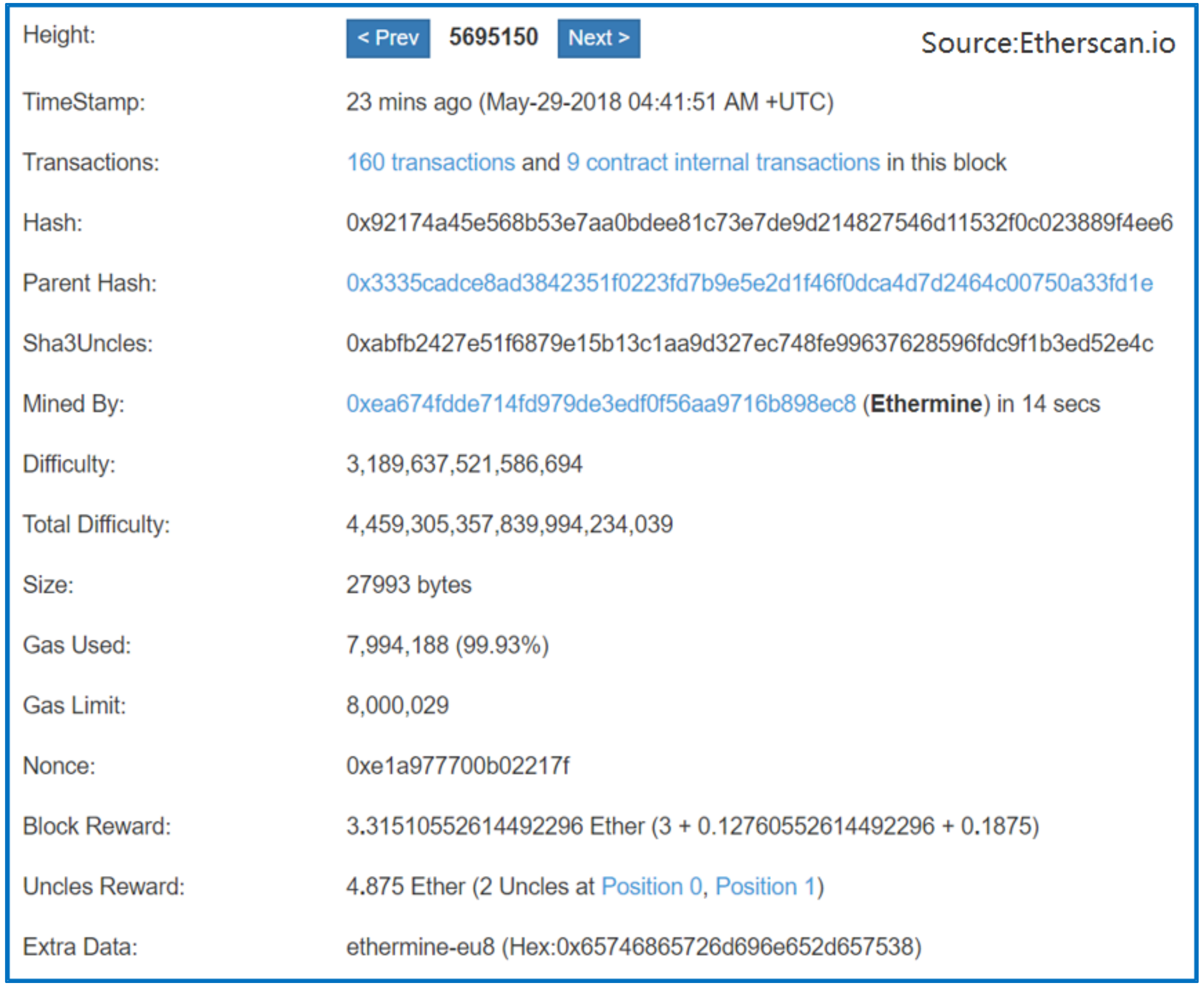
Pinch the chart to zoom in

Source:Etherscan.io



Source:Etherscan.io

Height:	< Prev **5695161** Next >
TimeStamp:	19 mins ago (May-29-2018 04:45:25 AM +UTC)
Transactions:	89 transactions and 3 contract internal transactions in this block
Hash:	0x76df197457effdbb736480393c70a016fe3bbdbfef619d16640cb665d748dcef
Parent Hash:	0xbd3ecbcf5527bb6de899912cb86eadc762c86832c713bef3910bcec7184e0f7a
Sha3Uncles:	0xde903bc6ba5e5ca6155d936f882a92a653f3b0a60a346f0f474fc56e61340ea9
Mined By:	0xea674fdde714fd979de3edf0f56aa9716b898ec8 (**Ethermine**) in 20 secs
Difficulty:	3,184,956,261,907,541
Total Difficulty:	4,459,340,439,119,129,119,115
Size:	18032 bytes
Gas Used:	7,967,412 (99.74%)
Gas Limit:	7,988,337
Nonce:	0xd280930018199336
Block Reward:	3.260603241218831558 Ether (3 + 0.166853241218831558 + 0.09375)
Uncles Reward:	2.25 Ether (1 Uncle at Position 0)
Extra Data:	ethermine-aws-us1-1 (Hex:0x65746865726d696e652d6177732d7573312d31)

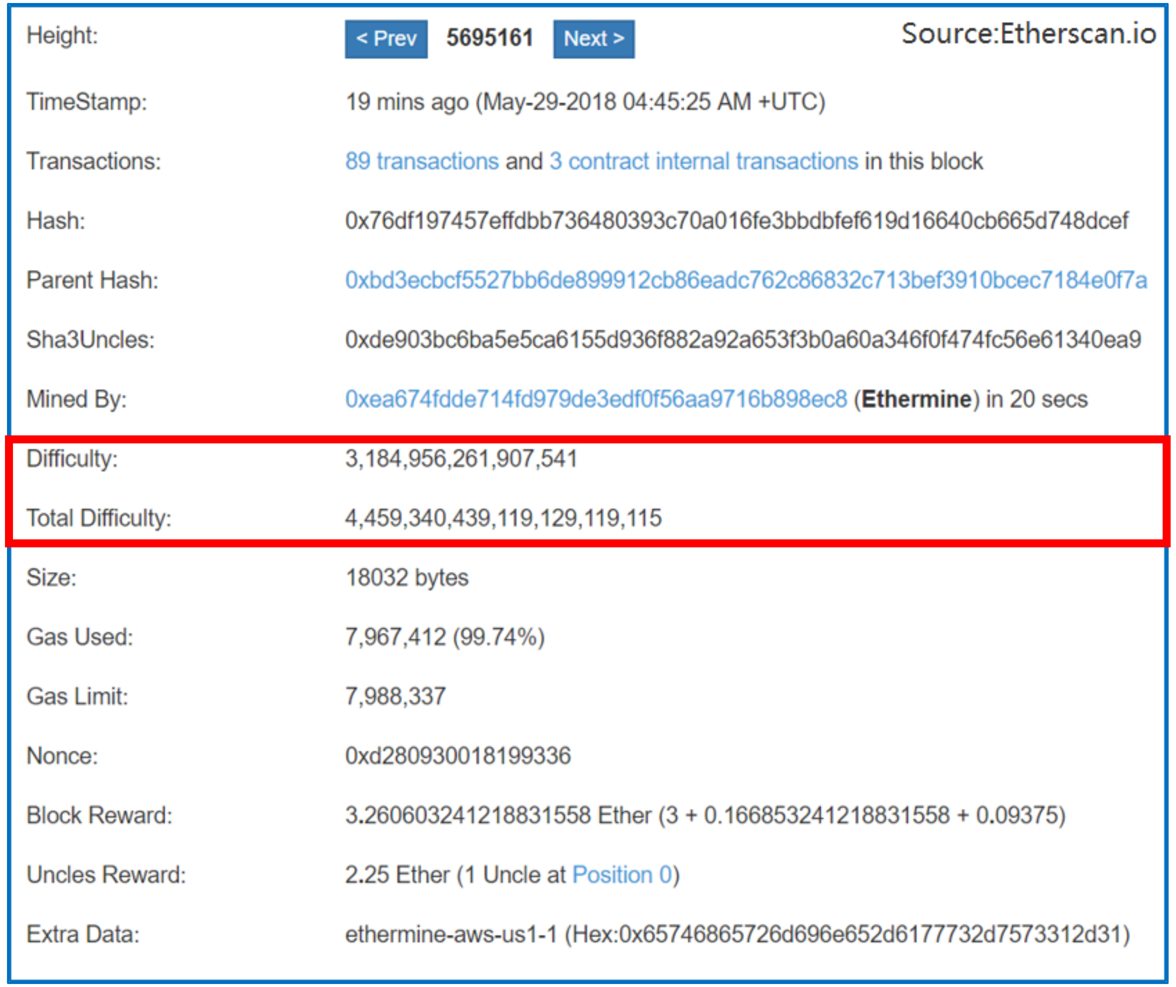


Source:Etherscan.io

Height:	< Prev **5695150** Next >
TimeStamp:	23 mins ago (May-29-2018 04:41:51 AM +UTC)
Transactions:	160 transactions and 9 contract internal transactions in this block
Hash:	0x92174a45e568b53e7aa0bdee81c73e7de9d214827546d11532f0c023889f4ee6
Parent Hash:	0x3335cadce8ad3842351f0223fd7b9e5e2d1f46f0dca4d7d2464c00750a33fd1e
Sha3Uncles:	0xabfb2427e51f6879e15b13c1aa9d327ec748fe99637628596fdc9f1b3ed52e4c
Mined By:	0xea674fdde714fd979de3edf0f56aa9716b898ec8 (**Ethermine**) in 14 secs
Difficulty:	3,189,637,521,586,694
Total Difficulty:	4,459,305,357,839,994,234,039
Size:	27993 bytes
Gas Used:	7,994,188 (99.93%)
Gas Limit:	8,000,029
Nonce:	0xe1a977700b02217f
Block Reward:	3.31510552614492296 Ether (3 + 0.12760552614492296 + 0.1875)
Uncles Reward:	4.875 Ether (2 Uncles at Position 0, Position 1)
Extra Data:	ethermine-eu8 (Hex:0x65746865726d696e652d657538)

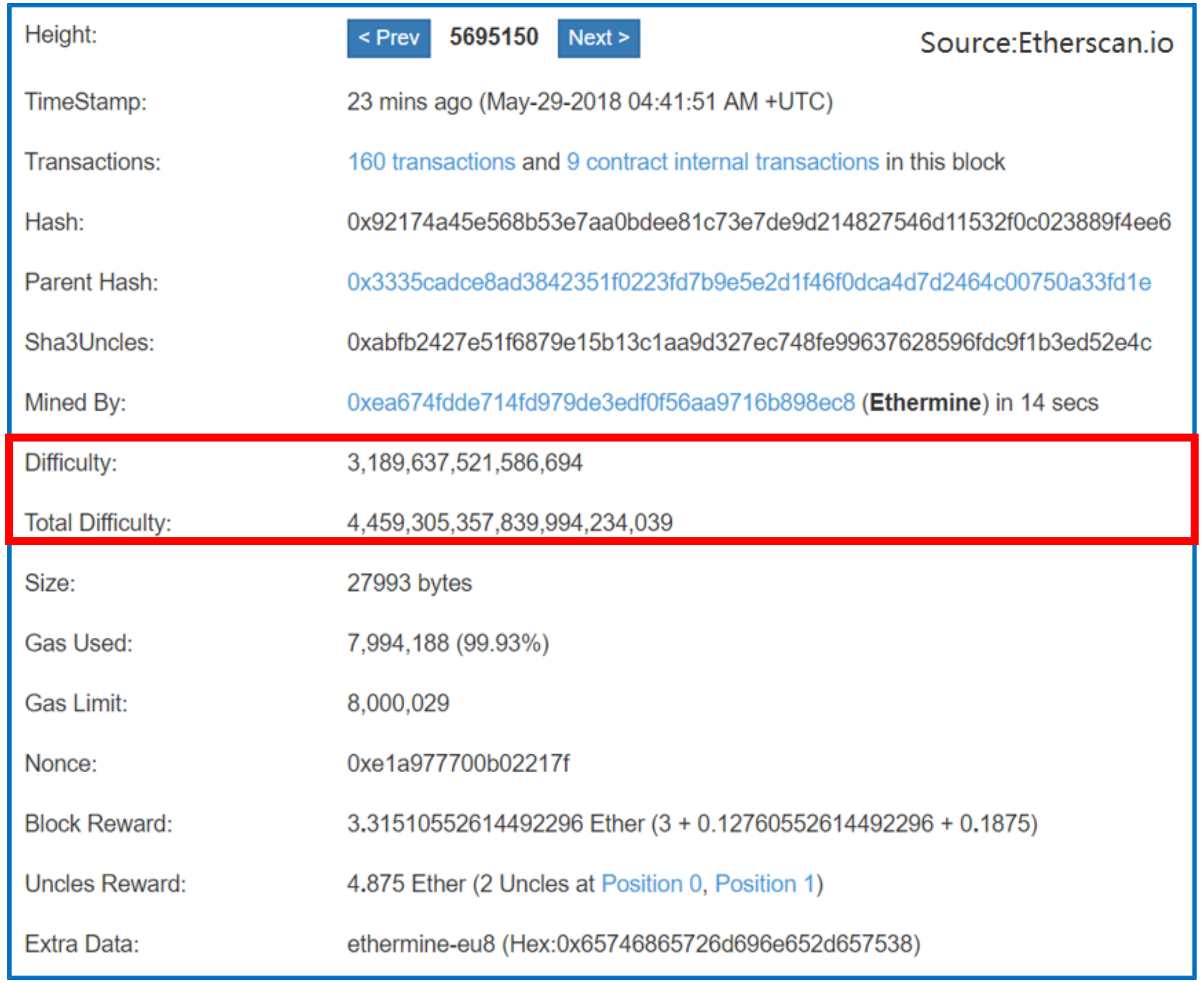
引入1个uncle的reward是$3\times\frac{1}{32}=0.09375$

引入2个uncle的reward是$2\times 3\times\frac{1}{32}=0.1875$



Source:Etherscan.io

Height:	< Prev 5695161 Next >
TimeStamp:	19 mins ago (May-29-2018 04:45:25 AM +UTC)
Transactions:	89 transactions and 3 contract internal transactions in this block
Hash:	0x76df197457effdbb736480393c70a016fe3bbdbfef619d16640cb665d748dcef
Parent Hash:	0xbd3ecbcf5527bb6de899912cb86eadc762c86832c713bef3910bcec7184e0f7a
Sha3Uncles:	0xde903bc6ba5e5ca6155d936f882a92a653f3b0a60a346f0f474fc56e61340ea9
Mined By:	0xea674fdde714fd979de3edf0f56aa9716b898ec8 (**Ethermine**) in 20 secs
Difficulty:	3,184,956,261,907,541
Total Difficulty:	4,459,340,439,119,129,119,115
Size:	18032 bytes
Gas Used:	7,967,412 (99.74%)
Gas Limit:	7,988,337
Nonce:	0xd280930018199336
Block Reward:	3.260603241218831558 Ether (3 + 0.166853241218831558 + 0.09375)
Uncles Reward:	2.25 Ether (1 Uncle at Position 0)
Extra Data:	ethermine-aws-us1-1 (Hex:0x65746865726d696e652d6177732d7573312d31)



Source:Etherscan.io

Height:	< Prev 5695150 Next >
TimeStamp:	23 mins ago (May-29-2018 04:41:51 AM +UTC)
Transactions:	160 transactions and 9 contract internal transactions in this block
Hash:	0x92174a45e568b53e7aa0bdee81c73e7de9d214827546d11532f0c023889f4ee6
Parent Hash:	0x3335cadce8ad3842351f0223fd7b9e5e2d1f46f0dca4d7d2464c00750a33fd1e
Sha3Uncles:	0xabfb2427e51f6879e15b13c1aa9d327ec748fe99637628596fdc9f1b3ed52e4c
Mined By:	0xea674fdde714fd979de3edf0f56aa9716b898ec8 (**Ethermine**) in 14 secs
Difficulty:	3,189,637,521,586,694
Total Difficulty:	4,459,305,357,839,994,234,039
Size:	27993 bytes
Gas Used:	7,994,188 (99.93%)
Gas Limit:	8,000,029
Nonce:	0xe1a977700b02217f
Block Reward:	3.31510552614492296 Ether (3 + 0.12760552614492296 + 0.1875)
Uncles Reward:	4.875 Ether (2 Uncles at Position 0, Position 1)
Extra Data:	ethermine-eu8 (Hex:0x65746865726d696e652d657538)

引入1个uncle的reward是$3 \times \frac{1}{32} = 0.09375$

引入2个uncle的reward是$2 \times 3 \times \frac{1}{32} = 0.1875$