

深圳区块链技术工坊第4期



该二维码7天内(12月13日前)有效, 重新进入将更新

以太坊零手续费及其安全防御的实现

钟瑞仙 2018.12.06

钟瑞仙 Rolong

- 早期从事游戏开发，DDoS防御
- 以太坊DAPP开发者
- 以太坊底层实现的研究和应用
- 现任以太零研发团队技术总监

大纲

- 一、以太坊手续费简介
- 二、零手续费的必要性
- 三、零手续费的实现
- 四、零手续费带来的安全问题及其解决方案
- 五、零手续费的副作用

一、以太坊手续费简介

1、认识以太坊手续费

- ① Gas不是手续费，而是资源消耗的衡量单位
- ② 手续费是： 购买Gas的费用
- ③ 手续费 = Gas * GasPrice
- ④ GasPrice常用单位： Gwei
- ⑤ 1 Gwei = 0.000,000,001 Ether

2、作用

- 安全：增加攻击成本，防止恶意交易占用网络资源
- 调控：发挥经济调控的作用，主要体现在GasPrice
- 激励：鼓励矿工记账（手续费也叫矿工费）

3、特点

- Gas先预购，再消耗，剩余的退还，不足则交易失败
- 手续费和网络资源稀缺性相关，越稀缺越贵
- 手续费和转账金额大小无关

二、零手续费的必要性

1、一笔普通转账的费用

20 Gwei = 0.000,000,02 eth

$0.000,000,02 * 21000 = 0.00042 \text{ eth}$

当以太坊价格为1000RMB时
手续费为 $0.00042 * 1000 = 0.42 \text{ 元}$

当以太坊价格为10000RMB时
手续费为 $0.00042 * 10000 = 4.2 \text{ 元}$

Rinkeby Test Net

CONFIRM TRANSACTION

TestNet1
2c0016...2883
18.748 ETH
2022.06 USD

Account 1
046BC7...8389


Amount	1.000 ETH 107.85 USD
Gas Limit	<input type="text" value="21000"/> UNITS
Gas Price	<input type="text" value="20"/> GWEI
Max Transaction Fee	<input type="text" value="0.000420"/> ETH 0.05 USD
Max Total	1.000 ETH 107.90 USD

Data included: 0 bytes

RESET **SUBMIT** **REJECT**

2、一笔代币转账的费用

<https://rinkeby.etherscan.io/tx/0x2ff87de7df31b9ccd1d01c065ba21f10f9b91f5c2ac6b9f493c0c24bf477e912>

TxHash:	0x2ff87de7df31b9ccd1d01c065ba21f10f9b91f5c2ac6b9f493c0c24bf477e912
TxReceipt Status:	Success
Block Height:	3456672 (1 Block Confirmation)
TimeStamp:	35 secs ago (Dec-05-2018 02:59:12 AM +UTC)
From:	0x41623962c5d44565de623d53eb677e0f300467d2
To:	Contract 0x149f1650f0ff097bca88118b83ed58fb1cfc68ef 
Tokens Transferred:	► From 0x41623962c5d445... To 0x149f1650f0ff097b... for 0.01 ERC-20 (ZRX)
Value:	0 Ether (\$0.00)
Gas Limit:	470000
Gas Used By Transaction:	183799 (39.11%)

普通转账消耗2.1万Gas，这笔交易消耗18.38万Gas，增长约9倍

3、合约部署的费用

<https://etherscan.io/tx/0xf63e775e10b0f662574ab49cd4c080ddcda8ca7d0012b5f0fbf0b03ad1c977ac>

交易哈希值:	0xf63e775e10b0f662574ab49cd4c080ddcda8ca7d0012b5f0fbf0b03ad1c977ac
交易回条 状态:	成功
区块高度:	5915466 (914099 区块 确认)
时间戳:	151 天 21 小时前 (Jul-06-2018 11:17:45 AM +UTC)
发送方:	0xf39e044e1ab204460e06e87c6dca2c6319fc69e3
接收方:	[合约 0xa62142888aba8370742be823c1782d17a0389da1 已创立] 
价值:	0 以太币 (\$0.00)
燃料限制:	6500000
交易燃料费用:	6181746 (95.1%)
燃料价格:	0.000000082500000101 以太币 (82.500000101 Gwei)
实际支付的矿工费:	0.50999404562435 以太币 (\$54.38)
随机数 & {位置}:	75 {37}

如果按以太坊单价1万RMB计算，这笔交易的手续费是5000RMB

4、零手续费是DApp普及的前提

【回看历史】

网银早期：每一笔交易都要收费，转账流程复杂

支付宝：免手续费，流程简单

微信红包：免手续费，小额转账，结合社交，进一步普及移动支付

【展望未来】

目前区块链支付和应用还处于“网银早期”阶段

DApp的普及，也必须简化转账流程、免手续费

三、零手续费的实现

- ① 零手续费 \neq 没有Gas
- ② 零手续费网络里仍然要消耗Gas
- ③ Gas不再需要花ETH购买
- ④ 用其他代币 (Power) 购买Gas
- ⑤ 免费的途径获得代币 (Power)

以太坊的零手续费实现（不考虑安全问题）

go-ethereum/core/state_transition.go

```
@@ -160,7 +160,7 @@ func (st *StateTransition) buyGas() error {
    st.gas += st.msg.Gas()

    st.initialGas = st.msg.Gas()
-   st.state.SubBalance(st.msg.From(), mgval)
+   // st.state.SubBalance(st.msg.From(), mgval)
    return nil
}

@@ -222,7 +222,7 @@ func (st *StateTransition) TransitionDb()(ret []byte, usedGas uint64, failed bo
    }
}
st.refundGas()
-   st.state.AddBalance(st.evm.Coinbase, new(big.Int).Mul(new(big.Int).SetUint64(st.gasUsed()), st.gasPrice))
+   // st.state.AddBalance(st.evm.Coinbase, new(big.Int).Mul(new(big.Int).SetUint64(st.gasUsed()), st.gasPrice))

    return ret, st.gasUsed(), vmerr != nil, err
}
```

更多实现细节，在下一章节

四、零手续费带来的安全问题 及其解决方案

带来了哪些安全问题？

以廉价的成本发送大量垃圾交易，导致网络拥堵

如何解决？

- 攻击成本的转移，例如增加时间成本
- 抵押方式分配网络资源的使用权，例如EOS里通过抵押获得CPU和NET的使用权
- 灰度等级共识，通过共识算法识别恶意交易并进行阻止或者冻结

案例：以太零的Power机制

Power为以太零原生代币，PoS机制发行，不可交易，仅用于购买Gas

console下查询自己的可用Power：

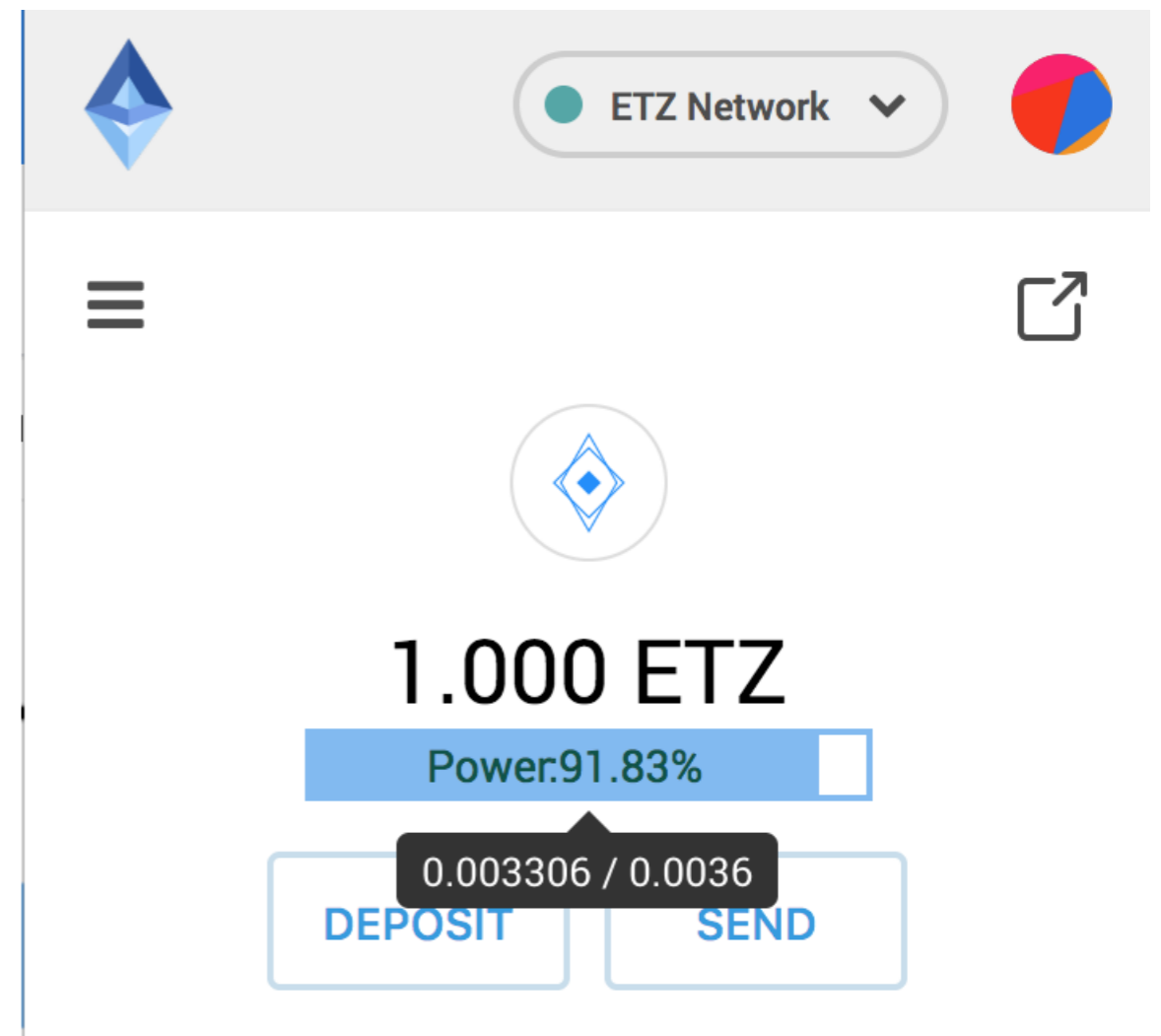
```
eth.getPower("your address")
```

```
Welcome to the Geth JavaScript console!  
  
instance: Geth/v1.8.12-unstable-526ebeac/linux-amd64/go1.10.1  
modules: admin:1.0 debug:1.0 devote:1.0 eth:1.0 masternode:1.0 miner:1.0  
  
> eth.getPower("0xdd5b67E58B3A0ad20757c10Cee9B0e33331eaAfd")  
3600000000000000
```

1、获得Power的两个条件

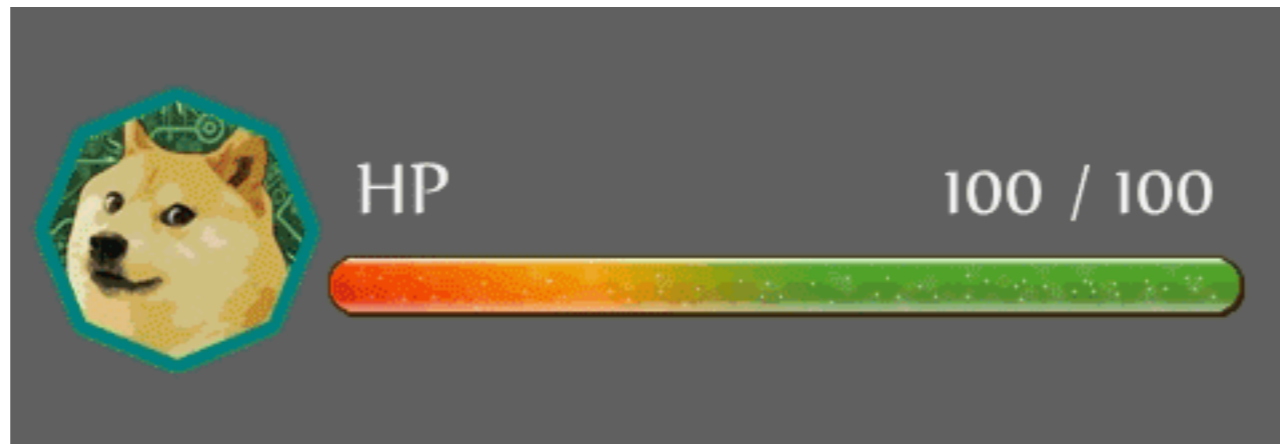
- ① 帐号上有币 (0.01以上, 不消耗币, 不锁定)
- ② 时间

所有余额大于或等于0.01etz的账号, 都会随着区块的增长持续产出Power, 直到达到Power上限。



2、Power的两个属性

- ① 最大值：PowerMax
- ② 每个区块产出Power的速度：PowerSpeed

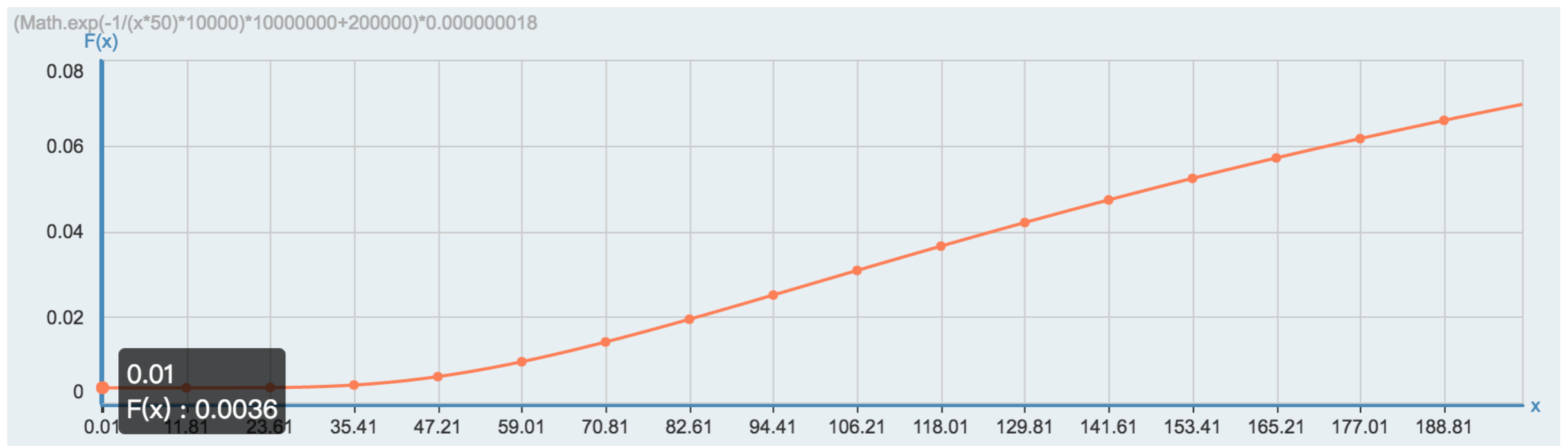


等级越高，装备越好，血就越厚，回血速度也越快

最大值的计算

$$\text{PowerMax} = (\text{Math.exp}(-1/(x*50)*10000)*10000000+200000)*0.000000018$$

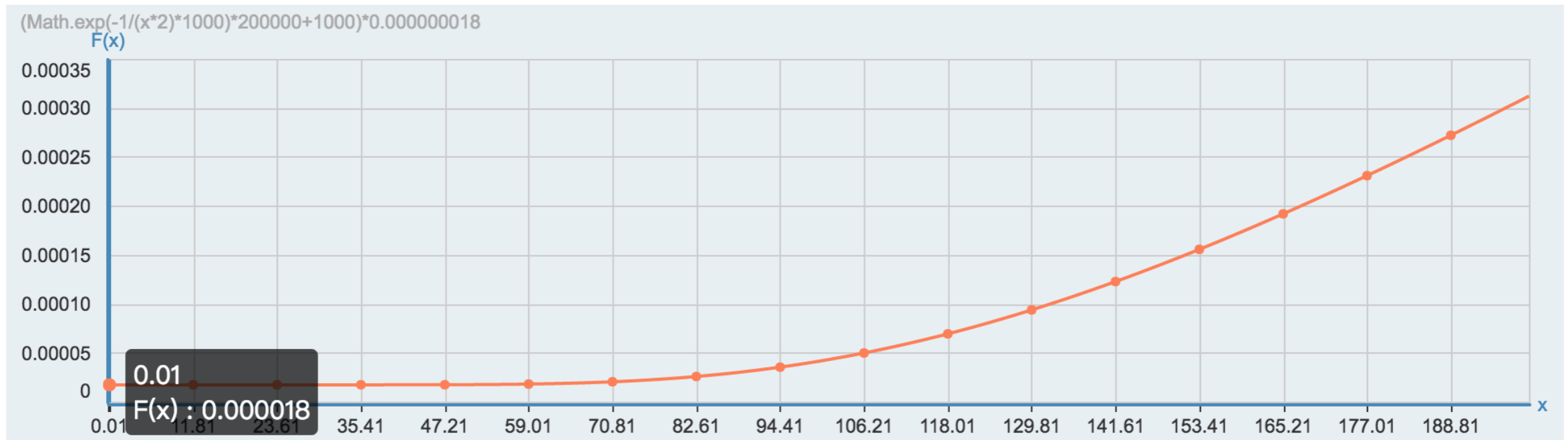
x为余额

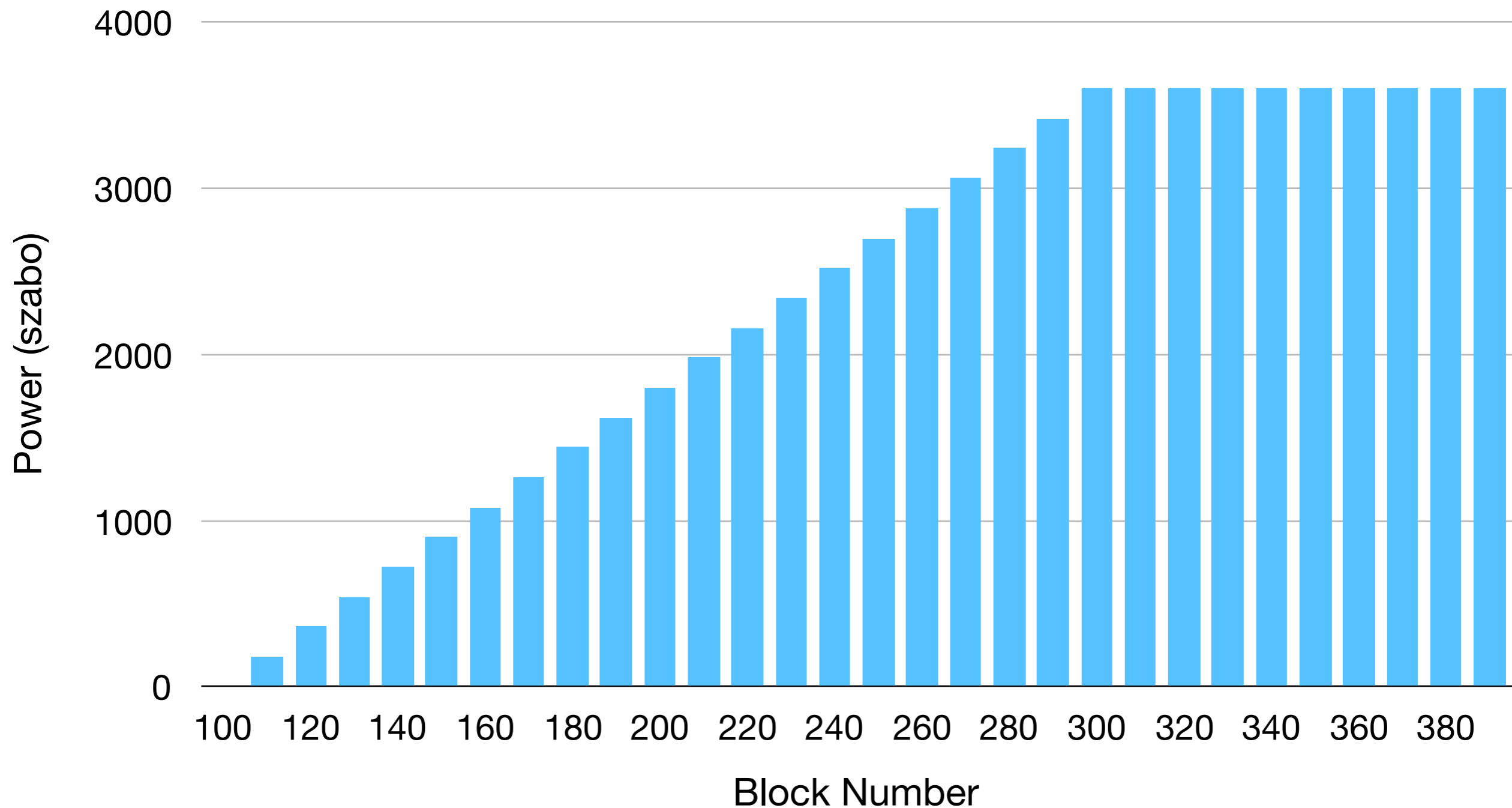


产出速度的计算

$$\text{PowerSpeed} = (\text{Math.exp}(-1/(x^2)*1000)*200000+1000)*0.000000018$$

x为余额





一个余额为0.01etz的账户，在区块高度100时收到了0.01etz，随着区块的增长而获得Power，区块高度300之后，已经达到了上限值0.0036，不会再继续增长。

例如一个有0.01 ether余额的账户， PowerMax为0.0036 ether，

假设GasPrice设置为18Gwei（即0.000000018 ether），

这个0.01 ether余额的账户单笔交易最大可用Gas = $0.0036 / 0.000000018 = 200000$

GasPrice为18Gwei的情况下， 这个账户不能发送gas超过20万的交易

假设GasPrice设置为36Gwei（即0.000000036 ether），

这个0.01 ether余额的账户单笔交易最大可用Gas = $0.0036 / 0.000000036 = 100000$

GasPrice为36Gwei的情况下， 这个账户不能发送gas超过10万的交易

3、计算一个账户的当前Power

$$\text{Power} = \text{Min}(\text{PowerMax}, (\text{Power0} + \text{BlockGap} * \text{PowerSpeed}))$$

Power0 = 上一笔交易之后剩余的Power

BlockGap = 当前区块高度 - 上一笔交易的区块高度

4、消耗Power

PowerSpend = Gas * GasPrice

一笔普通转账的Gas为21000, GasPrice假设为20 Gwei

20 Gwei = 0.000,000,02 ether

一笔普通转账需要power = 21000 * 0.00000002 = 0.00042 ether

Power不足则转账失败

三、零手续费的副作用

- ① 实现逻辑变得更复杂
- ② 用户体验可能会更差（例如EOS）
- ③ 零矿工费，没有了矿工激励

讨论时间

期待大家给予更好的零手续费解决方案!

<https://github.com/etherzero-org>