2018年10月12日区块链技术晚报 第29期

一.Tech News

0️⃣今天360区块链实验室推送了一篇关于 Dice2win的区块链博彩游戏的公平性分析的文章

摘要如下：

Mental poker:在没有可信第三方的参与的情况下(可信平台或软件)，两个不诚实的参与方如何在网络上进行一场公平的棋牌游戏。在公平性的定义中，有非常重要的一点：如果任何一方收到了游戏结果，那么所有的诚实方都应该收到结果。

游戏总体工作流程如下：

1. 【庄家承诺】庄家(secretSigner)随机生成某随机数reveal，同时计算commit = keccak256(reveal)对该reveal进行承诺。然后根据目前区块高度，设置一个该承诺使用的最后区块高度commitLastBlock。 对commitLastBlock和commit的组合体进行签名得到sig，同时把(commit, commitLastBlock,sig)发送给玩家。
2. 【玩家下注】玩家获得(commit, commitLastBlock,sig)后选择具体要玩的游戏，猜测一个随机数r，发送下注交易placeBet到智能合约上进行下注。
3. 【矿工打包】下注交易被以太坊矿工打包到区块block1中，并将玩家下注内容存储到合约存储空间中。
4. 【庄家开奖】当庄家在区块block1中看到玩家的下注信息后。则发送settleBet交易公开承诺值reveal到区块链上。合约计算随机数random_number=keccak256(reveal,block1.hash)。如果random_number满足用户下注条件，则用户胜，否则庄家胜。此外游戏还设有大奖机制，即如果某次random_number满足某个特殊值(如88888)，则用户可赢得奖金池中的大奖。

dice2win中的所有游戏都会受到庄家选择性中止攻击，庄家可以选择性公布中将结果从而导致用户无法获胜或赢得彩票

攻击场景

场景1：

用户下注额大，且赔率高的情况下。用户下下注产生block1后，block1.hash实际上就已经固定了。此时庄家已经可以计算出random_number，从而计算出用户的投注结果和盈亏。则庄家可以选择性中止交易。如果用户不中奖，则庄家公布正常开奖结果。如果用户中奖，则庄家可因为“网络用户和技术原因”从而导致用户该笔下注失效。

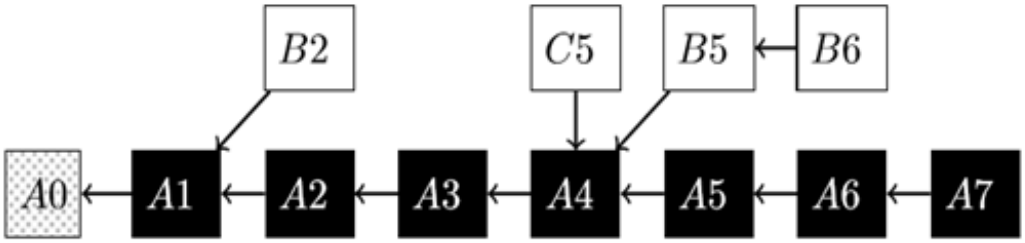
场景2：

用户下注额不大，但是block1产生后庄家发现random_number导致用户中彩票。则庄家可以选择性中止交易，导致用户该笔下注失效。

在这两种攻击场景下，庄家都能够轻松控制交易结果。当然庄家并不会对每笔交易都发起这种攻击，而是可以选择用户获奖特别大的交易进行操控。Dice2win官方实际上已经在智能合约代码得注释中声明了可能会发生“技术问题和以太坊拥堵”原因造成荷官无法开奖(大约1个小时内)，则用户可以提回下注款。

通讯模型问题：

区块链智能合约上玩家交互的通讯模型，与传统的互联网用户点对点通讯模型是有区别的。传统的点对点通讯模型下证明的安全协议，直接套用到智能合约平台上未必能保证其安全性。核心原因在于：传统的点对点通讯模型下，协议的执行是顺序的，不可逆的。而智能合约的通讯模型中，由于POW等共识算法存在分叉的可能性，协议的执行可能是非顺序的可逆的。在下图中，假设黑色区块为网络主链，白色区块是分叉区块。如果一个安全多方计算的协议步骤（某笔交易）在白色执行，那么该交易将不会生效。例如Alice和Bob在区块链上进行某种计算。Alice在区块B5上执行某笔交易，Bob随后在区块B6上公布某个秘密。随后因为网络发生分叉，B5、B6上的交易都失效了。但是Alice却收到了秘密。



查看原文点这里

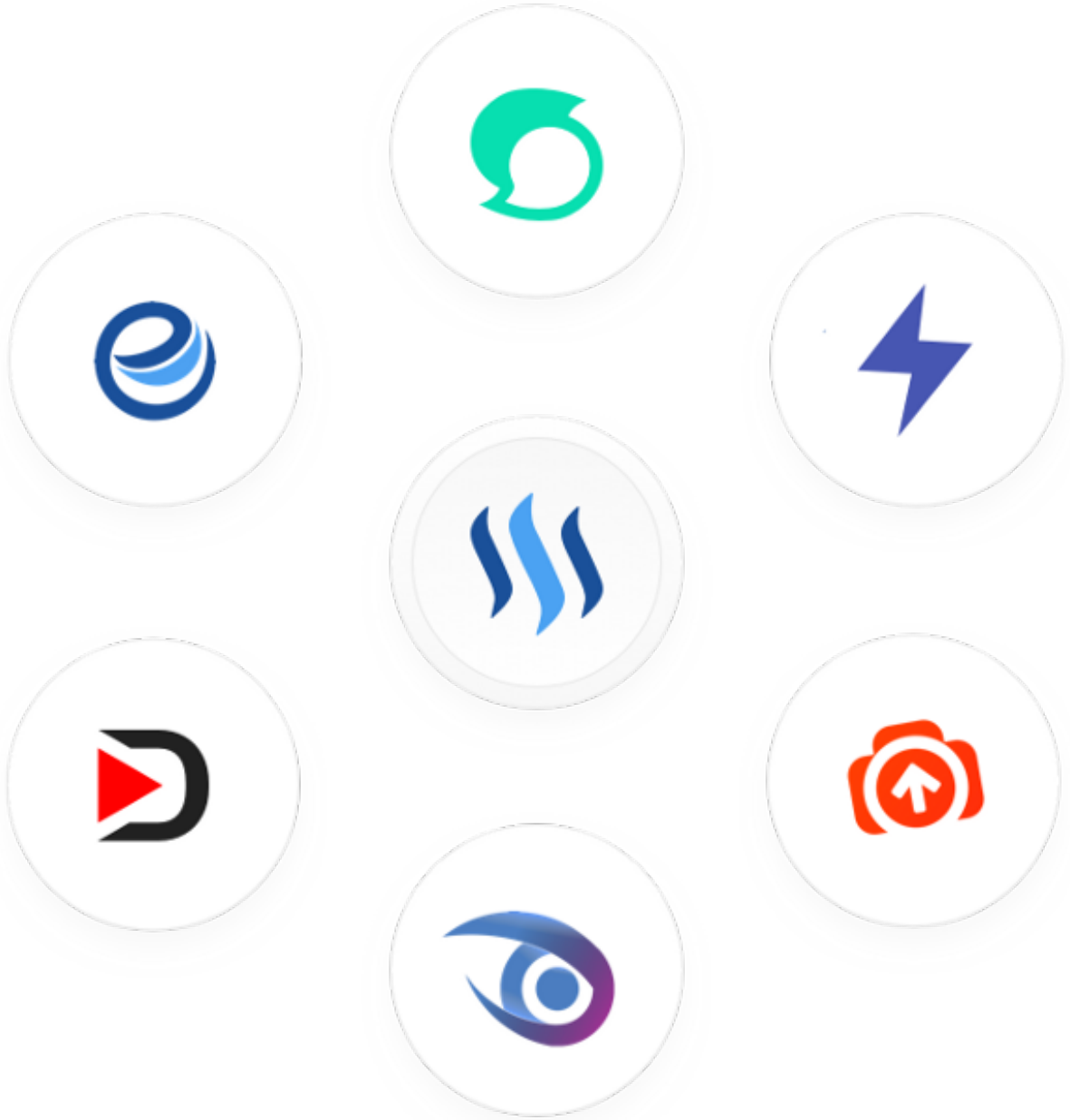
1️⃣一份加密经济学的终极学习指南

需要点经济学知识

原文点这里

2️⃣如果想研究区块链UGC的话，Steemit真的是不二直选

下图是其周边生态！



https://steemit.com,

https://busy.org/,

https://steepshot.io/,

https://join.utopian.io/,

https://d.tube/,

https://esteem.app/

steem Github官网

3️⃣what is Token Ecomomics?

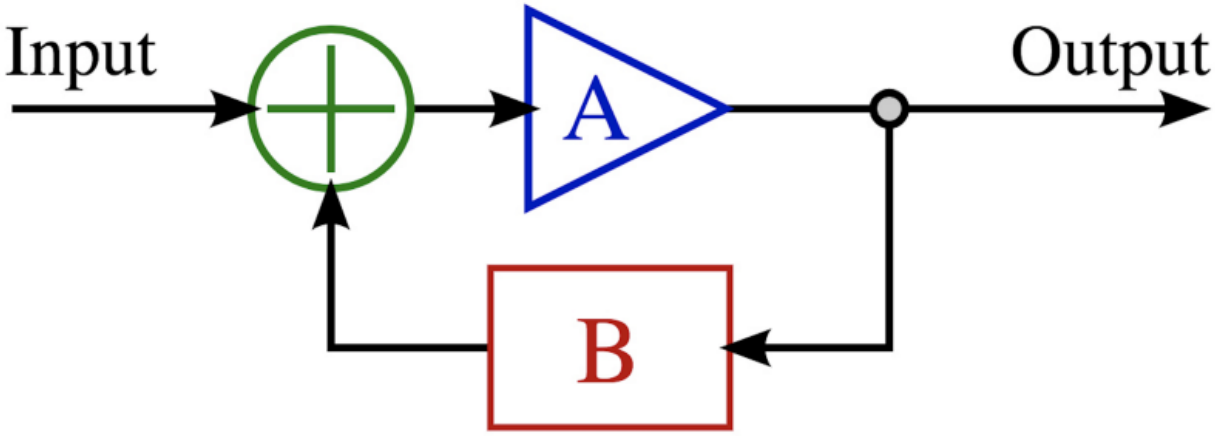
Part1 What is Token Economics?

Part 2 Top Token Economic Models

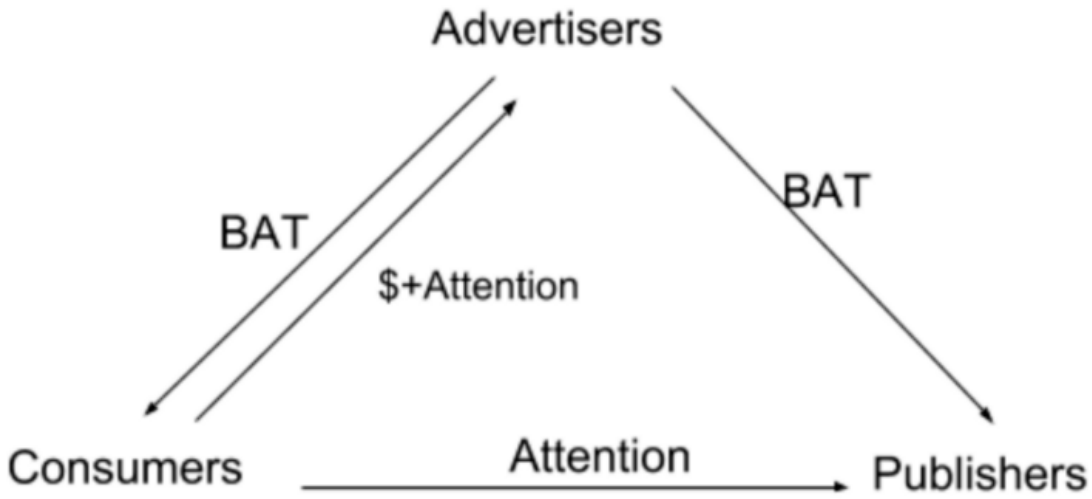
Part 3 Systematic Token Economic Issues

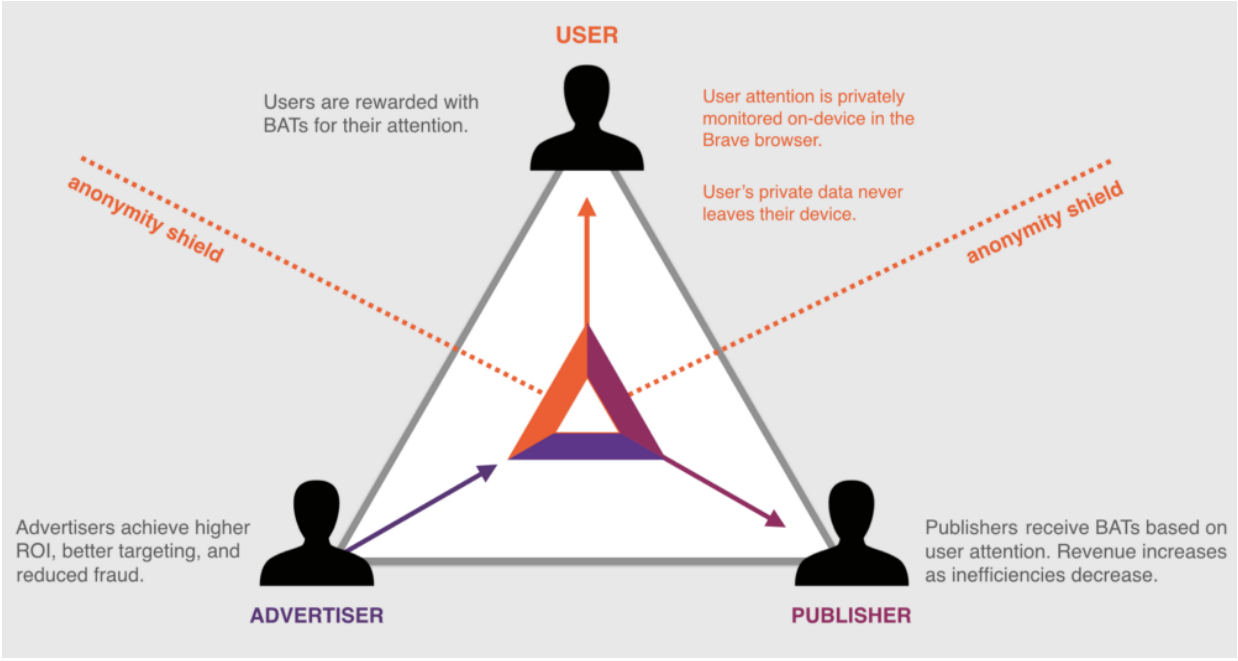
Part 4 A Guide to Creating a Token Incentives

4️⃣激励循环——加密算法如何实际修复现有激励循环

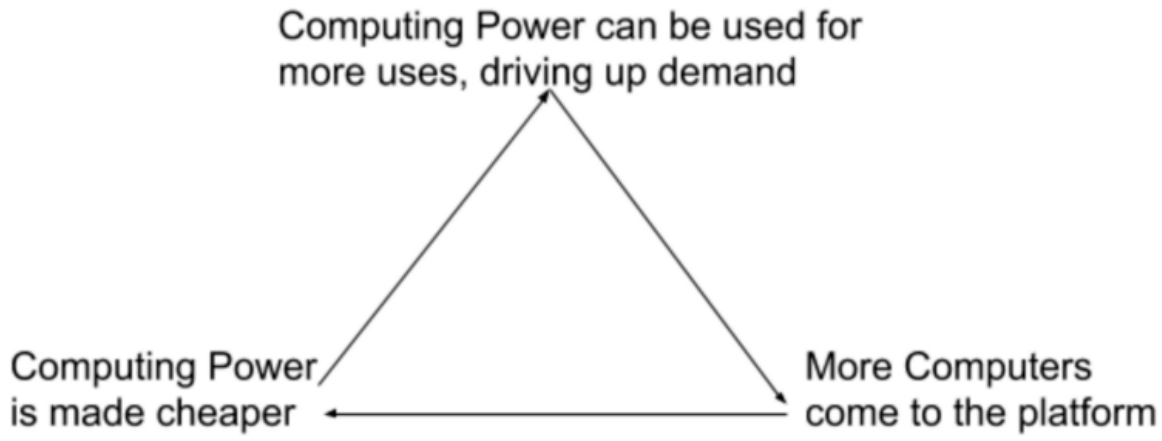


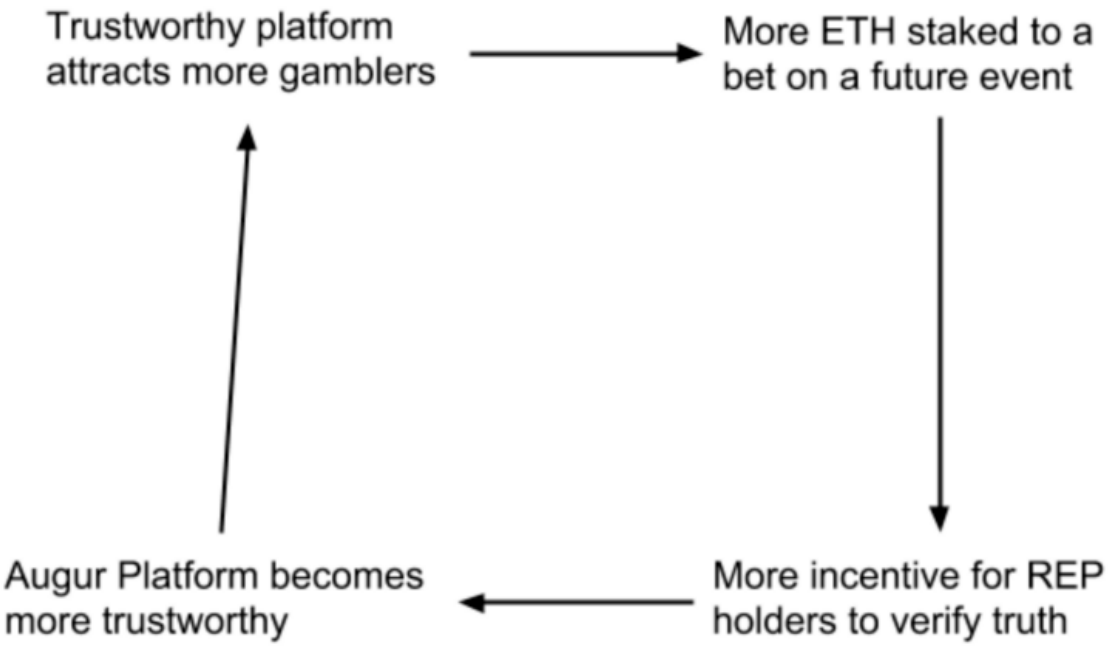
只有向消费者支付 BAT 代币，才能向消费者推送广告。广告商也只能向接受 BAT 代币的出版商发送广告。这种保护壁垒能够修复现在破损的互联网中的许多功能。（BAT 代币中）激励循环如下：





下面是原文中用的几个模型





重点是看翻译者的评论！

[原文点这里]

5️⃣基于以太坊的交易所BANCOR算法实现-转换算法框架

原文点这里，[推荐看看]

6️⃣今日BTC， ETH , EOS

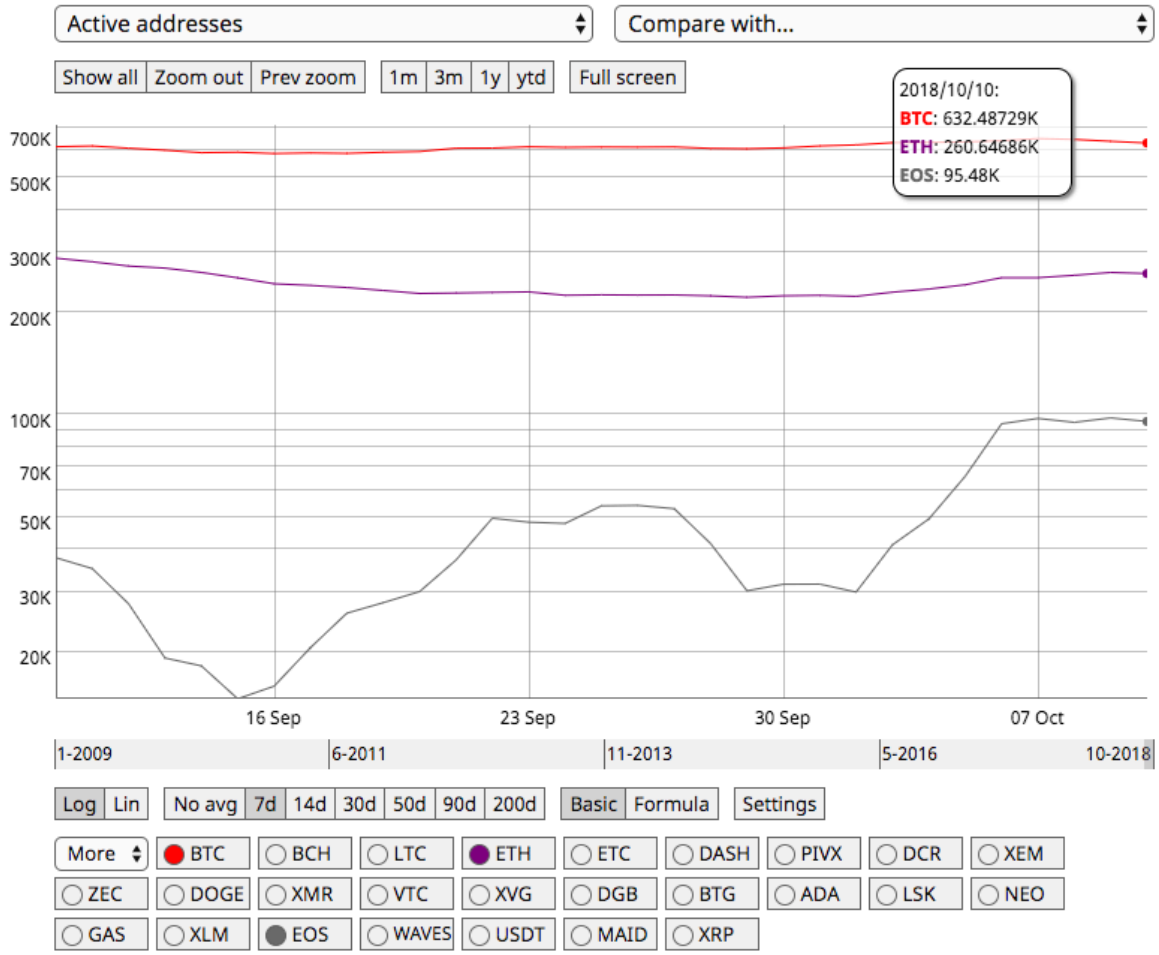
BTC:

date	txVolume(USD)	adjustedTxVolume(USD)	txCount	marketcap(USD)	price(USD)	exchangeVolume(USD)	generatedCoins	fees	activeAddresses	averageDifficulty	paymentCount	medianTxValue(USD)	blockSize	blockCount
2018/10/1	3868196006	1982712570	242662	114509724600.00	6619.85	4000970000	1975	21.82334691	672475	7152633351910.00	360525	194.2998131	135422735	158
2018/10/2	4369755902	2142437458	244635	114062551875.00	6593.24	3979260000	1712.5	25.72269107	678543	7152633351910.00	359131	199.6045389	139101005	137
2018/10/3	3787349114	1962649041	242158	113392236466.00	6553.86	3887310000	1812.5	21.36448501	694010	7152633351910.00	427200	173.7370612	121542722	145
2018/10/4	3847994118	1847601505	243007	112435991226.00	6497.91	3838410000	1875	18.70916379	642395	7364268059360.00	381204	167.7808447	119796008	150
2018/10/5	3511070704	1796495299	244589	113767335788.00	6574.15	3671500000	1625	21.33672301	688115	7454968648260.00	409154	188.890713	125204415	130
2018/10/6	2748743396	1408659700	214718	114614282649.00	6622.45	3259740000	1562.5	17.57876392	588478	7454968648260.00	336658	142.5010182	115262735	125
2018/10/7	2209576383	1036458505	219589	114074648410.00	6590.68	3306630000	1774.999999	13.06671747	598361	7454968648260.00	313022	80.69628592	118128874	142
2018/10/8	3460203706	1922593448	247906	114251052224.00	6600.19	3979460000	1687.5	16.79599849	646076	7454968648260.00	350251	168.0665781	130298970	135
2018/10/9	3559088725	2082698666	235732	115177623331.00	6653.08	3580810000	1625	16.66631934	621386	7454968648260.00	347881	179.63316	125633758	130
2018/10/10	4675374054	2207747475	244801	114967098651.00	6640.29	3787650000	1800	15.6339373	642600	7454968648260.00	364305	170.3765608	129154395	144
2018/10/11	5247183922	2858094847	262308	114051783103.00	6586.74	5181640000	1987.5	18.4172056	686810	7454968648260.00	374053	197.564458	146411276	159

ETH:

date	txVolume(USD)	adjustedTxVolume(USD)	txCount	marketcap(USD)	price(USD)	exchangeVolume(USD)	generatedCoins	fees	activeAddresses	medianTxValue(USD)	averageDifficulty	paymentC	blockSize	blockCount
2018/10/1	327751125.8	327751125.8	476308	23855852479	233.22	1597500000	20302.40625	611.8068788	222642	1.39932	3240652601420000.00	220008	149896751	6095
2018/10/2	280175439.9	280175439.9	490262	23643704719	231.1	1542080000	20514.1875	646.2650811	219856	0.27732	3211925078740000.00	214715	148979852	6180
2018/10/3	402749305.8	402749305.8	559006	23168243633	226.41	1683930000	20293.21875	444.7257819	259693	0	3226085186420000.00	230837	130142896	6075
2018/10/4	385579141.6	385579141.6	559181	22562709805	220.45	1479500000	20371.875	441.2275467	269797	0.042702047	3261753458930000.00	245847	139236168	6146
2018/10/5	377926618	377926618	595361	22753360914	222.27	1547330000	20177.0625	429.8314017	285832	0	3277001275790000.00	251591	127159907	6099
2018/10/6	267972513.4	267972513.4	596865	23299225467	227.55	1505070000	20491.96875	290.7691987	284750	0.00236652	3252608506130000.00	265479	109566965	6222
2018/10/7	240300634.8	240300634.8	497767	23087109194	225.44	1470480000	20521.3125	314.1878292	231585	0.0135264	3275289114570000.00	215643	96121905	6241
2018/10/8	401059846.2	401059846.2	542842	23201746333	226.51	1470740000	20424.9375	431.4967026	251483	0.020122967	3311602077650000.00	236715	105264175	6179
2018/10/9	361058088	361058088	537028	23534297243	229.71	1405130000	20352.9375	387.4958371	255081	0	3289361288760000.00	216626	112188265	6149
2018/10/10	387803952.6	387803952.6	516772	23324309565	227.62	1384040000	20361.75	447.9409647	246000	0.136572	3294910495260000.00	226089	104033046	6168
2018/10/11	771323591.8	771323591.8	570525	23123377668	225.61	2167620000	20485.3125	471.9269088	260509	0.028111006	3219699284380000.00	243204	111592995	6143

date	txVolume(USD)	txCount	marketcap(USD)	price(USD)	exchangeVolume(USD)	medianTxValue(USD)	activeAddresses	paymentCount	blockCount
2018/10/1	63690010.8	1416553	5197660279	5.74	695608000	1.435	36951	372509	172788
2018/10/2	47042344.59	1883906	5202480272	5.74	564671000	0.7175	75943	507607	172793
2018/10/3	57454858.25	1377687	5083643720	5.61	595740000	0.70125	99742	406992	172800
2018/10/4	52165132.03	1472277	5098014680	5.63	613679000	1.4075	72562	384275	172772
2018/10/5	55295052.38	1461405	5247946540	5.79	554553000	0.579	135802	461164	172728
2018/10/6	38995259.92	1668258	5269277407	5.81	486075000	0.581	210680	643966	172798
2018/10/7	33683383	2118245	5193475087	5.73	525930000	0.573	50548	558341	172684
2018/10/8	176306101.3	1876704	5226386210	5.77	627571000	1.4425	19103	506036	172689
2018/10/9	67797114.51	2210207	5368459762	5.92	538883000	0.9472	96145	509187	172784
2018/10/10	120929142.8	2020724	5341903994	5.89	533169000	1.4725	83520	538653	172290
2018/10/11	143145255	1978872	5324615715	5.88	758737000	1.47	52656	536901	172779



7️⃣EOS的.....日常被黑.....

10:30 Friday , October 12th 2018In a response to a blockchain investor and researcher called James Spediacci who listed "13 Reasons Why EOS Is a Disaster," Block.One's CEO Brendan Blumer said that "The constitution is an iterative community process and was not put forth by Block.One. It provides transparency over authority opposed to the lackthereof (ETH DAO reversal by mining pools)." From coinness.com

The 13 reasons, as concluded by James Spediacci, are shown as follows:

1.The constitution was resubmitted based on the problems with ECAF;

2.RAM over-speculation;

3.Fake transaction volume;

4.Centralization;

5.It's not Byzantine Fault Tolerant;

6.It's not permissionless, immutable, or censorship-resistant;

7.Cartels;

8.Transaction fee tradeoff for inflation;

9.Investors lose everything and their tokens get confiscated and redistributed if they don't vote for 3 years;

10.EOS had an uncapped ICO that raised $4B;

11.The EOS ICO raised about $20m/day for a year thanks to an abitrage trading scheme;

12.EOS pushes costs onto developers;

13.EOS doesn't protect investors against inflation.

8️⃣How to Build an EOS FULL NODE SERVER!

肯定有坑，自己拆坑吧!

原文点这里

9️⃣Parity Ethereum 2.1.2-beta: Constantinople coming to Kovan and Ropsten

Parity Ethereum 2.0.7-stable and 2.1.2-beta were released today

两个测试网的区块高度和时间!

- Ropsten: Block #4,230,000 — October 14th, 2018
- Kovan: Block #9,200,000 — October 25th, 2018

原文点这里

Ethereum layer-2 protocols 的进展点这里

项目更新 AirSwap平台更新

新的AirSwap平台现在支持名为Spaces的自定义交易环境，使团队能够发现，交谈和进行分散交易。

POA网络启动BlockScout

BlockScout是一款易于使用且安全的工具，可让用户搜索和浏览以太坊，以太坊经典和POA网络区块链上的交易，地址和余额。

CryptoZombies第2季即将来临

CryptoZombies是由Loom Network创建的免费在线课程，旨在帮助人们学习以太坊的母语Solidity。本周，该团队宣布他们将在不久的将来推出一个全新的课程。

Augur V2详情

Augur的团队概述了在不久的将来V2协议的所有升级，包括：DAI集成，回购和刻录费系统，ERC777支持等等。

DDEX发布移动钱包

DDEX（使用0x协议的exchange）在App Store和Google Play Store上发布了他们的移动钱包。

Meridio推出release

reLease dapp允许任何人租用当天的工作区来在一组创意同伴中工作，没有订阅或锁定。

1.

你要是忍不住打赏我点咖啡钱呐，😆😆

我的BTC地址：38weDdkcor1RNwxYAZoZfaJS9ZaPc1si99

我的ETH地址：0x8C1d4aCfF198AaE62e78944A5E49aed745162A89

微信打赏：

以上内容由平妈整理，感谢阅读！日报汇聚地址为：https://github.com/allinbc/BlockChain_Daily_Report （原先已经删除，待整理后，重新上传）

欢迎大家star&watch!