火币大学
HUOBI UNIVERSITY

2018年9月22日 火币区块链技术学习与分享群-今日区块链技术晚报

一.Tech News

0️⃣澳洲交易所BitTrade宣布，由澳币担保的稳定币预计明年问世！

We're partnering with Emparta to build and launch Australia's first Aussie dollar-backed stablecoin!

详细的内容参见其交易所的公告！点我，点我，快点我！我是Link！

1️⃣Ethereum dApp Bancor Moves to EOS to Open up BancorX。前几期已经发了，现在后续来点后续报道吧。

Bancor already operates LiquidEOS, a block producer on the EOS network, and its protocol is already being used on the EOS network to govern the market for RAM. The company has reportedly released open-source codes for smart contracts on the network.

1.Bancor2BancorX

2.其他媒体文章

2️⃣SEC又delay了ETF。美国证券交易委员会在2018年9月20日提交的文件中称，美国证券交易委员会再次推迟了对VanEck和Solid X支持的交易所交易基金的决定，该基金希望收到更多反馈。

1.SEC delay ETF

3️⃣TTC协议与白帽黑客社区Hacken合作，以改善其网络安全.

TTC 在设计中并没有抄袭Stemmit，它的Token激励机制值得学习！

Reward Engine& & Architecture img source : TTC

TTC Reward Engine Configuration

Rewarding pool distribution

Proportion of content reward	50%
Proportion of reputation reward	50%

Content reward distribution

Content value calculation

- [x] Fixed number
- [ ] Proportion in all contents

Weight of interactions

Weight of liking	1
Weight of commenting	1.5
Weight of sharing	1.2
Weight of customized behavior 1 *	0

Distribution between content creator and curators

Proportion of content creator	61.8%
Proportion of content curators	38.2%
Proportion of liking	10%
Proportion of commenting	18.2%
Proportion of sharing	10%
Proportion of customized behavior 1 *	0%

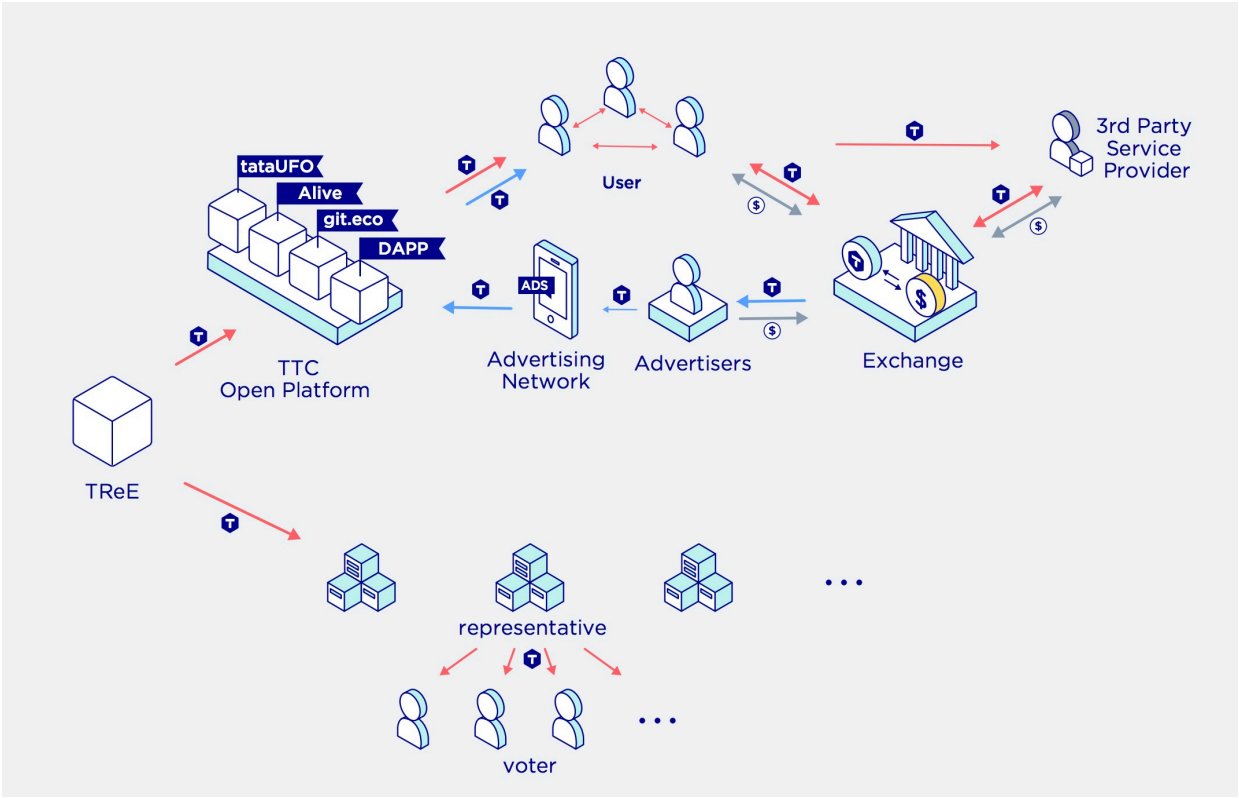
Curators' distribution pattern

- decrease in sequence
- equal division

Reputation reward distribution

Proportion of reputation elements

Proportion of retention value	20%
Proportion of value of content created	30%
Proportion of follower value	30%
Proportion of auditing & reporting value	20%



1.TTC protocol & Hacken

2.TTC en writepaper

4️⃣HitBTC Integrates Gemini Dollar HitBTC开始集成GUSD了！

Gemini was also the first licensed exchange in the world to offer trading and custody services for ether and Zcash.

双子座也是世界上第一家为Ether和Zcash提供交易和托管服务的持牌交易所。

1.HitBTC & GUSD

5️⃣新的BTC挖矿芯片发布，来点详细的内容吧！

Bitfury Group是总部位于美国旧金山的最大的私人比特币区块链基础设施提供商和交易处理公司。最近，该公司推出了一款名为Bitfury Clarke的加密采矿应用专用集成电路（ASIC）芯片。新推出的芯片正在为大规模生产做好准备，部署期望很高。

BitFury进一步将**14nm** Bitfury Clarke ASIC描述为“在性能和效率方面无与伦比”。事实上，该**芯片完全针对SHA256比特币采矿而定制，拥有55千焦耳/千兆赫（mJ / GH）的电源效率和高达120千兆每秒（GH / s）哈希值**。此外，它还提供完全集成的可控时钟生成，集成上电复位电路，并采用无铅6×6 mm FCLGA 35L或FCLGA 4L封装。 Bitfury Clarke的供电电压可低至0.3伏。

此外，数据表显示Bitfury Clarke已针对较小的PCB设计优化了封装尺寸。 ASIC可以轻松地在两个任务缓冲区之间切换 - 一个用于SHA256计算，而另一个可以通过“任务写入”命令填充。

除了销售这些芯片外，BitFury还计划将Bitfury Clarke整合到该公司拥有的其他BTC采矿硬件中，包括其采矿服务器和BlockBoxes。 Bitfury将在加拿大，挪威，冰岛和格鲁吉亚共和国的采矿中心实施新的ASIC。

值得注意的是，Bitfury建立的格鲁吉亚采矿厂本月早些时候进行了升级。正如Coinspeaker报道的那样，该公司为冷却系统配备了位于第比利斯的40兆瓦中心，采用了最强大的两相浸入式冷却（2PIC）技术，因此降低了95%的冷却成本，同时使采矿过程更加环保。

1.Bitfury 新的芯片原文

6️⃣Selfish Mining Prevention：如何防止私自挖矿：

来自Bitcoin-dev 邮件组：

Andrew Karamaoun提出了一个阻止自私挖掘的想法，即允许块奖励由峰值哈希率决定。

例如，如果p是365个周期或1年的峰值哈希率，由144个块组成，h表示最后144个块（1天周期）的哈希值，以及r用于挖掘块的基本补贴或奖励，目前12.5比特币，最大块奖励可以使用公式0.5r（1 + h / p）计算，最低可能块奖励为0.5r。在峰值哈希值时，矿工获得完整的12.5 BTC奖励，否则奖励将根据哈希值确定。

这将阻止矿工以较低的哈希值开采，因为他们只能在前144个区块的低哈希值下获得全部奖励，之后他们将无法获得以相同速率挖掘区块的全部奖励。这可能听起来不对，因为“采矿对于早期矿工来说更加糟糕”，因此可能必须修改难度算法。

费用将是未来矿工的唯一动力。那时，如果没有达到峰值费率，可以扣留部分费用，称为准备费的概念。

这个概念表明，在未来进行交易时，用户可以指定他们希望在“储备”中持有的费用的百分比以及多长时间，例如2016年的阻止。当他们的哈希值增加时，“矿藏费”将支付给矿工。

再次假设当前哈希值为h并且前一年的峰值哈希值为p，则对于每个周期（1天），基于当天的哈希值计算新的哈希值h1。如果h1> h，则在2016年的区块中创建的“准备费”的一部分（h1-h）/ p将提供给矿工，分布在该期间的144个区块中。

在挖掘“合同结束”之前，将基于哈希值发布更多的预留费用，并且拥有预留费用的用户随后可以仅将其用于在网络上支付费用，但不作为未来交易的输入。

这将阻止矿工“赶走”竞争，因为他们获得的“预留费”金额将取决于他们的哈希值。

来自Zawy的一个值得注意的反馈是，这个计算存在一个问题，即“一个放大振荡的正反馈回路。”如果由于价格变化或“随机解决时间变化”，净回报随着h上升或下降，矿工将会当然要获得更高的净奖励，直到达到极限。这是一个积极的反馈循环。

更糟糕的是，矿工选择使用哪种硬币，这是由利润驱动的，是一种“非线性”功能：例如，如果难度下降30%或者采购山寨币的回报增加30%，它可能导致哈希值上升300%。通常，144个过去区块中的72个区块的自私矿只会导致12.5%的损失，如果使用上述功能则会更糟。

或者，应该通过类似的功能而不是奖励来增加难度，因为它对仅对（价格+费用）/难度比感兴趣的矿工没有区别。

1.Selfish Mining Prevention

7️⃣在自己的笔记本上玩过Bitcoin的全节点么？是不是磁盘被.dat数据塞满了！！下面是个解决方案，（我的以太坊节点刚占了我350G的硬盘！WTF！怎么解决呢！）

It is possible to configure your node to to run in pruned mode in order to reduce storage requirements. This can reduce the disk usage from over 145GB to around 5GB.

Running a node in pruned mode is incompatible with `-txindex` and `-rescan`. It also disables the RPC `importwallet`. Two RPCs that are available and potentially helpful, however, are `importprunedfunds` and `removeprunedfunds`.

To enable block pruning set `prune=N` on the command line or in `bitcoin.conf`, where `N` is the number of MiB to allot for raw block and undo data.

A value of `0` disables pruning. The minimal value above `0` is `550`. Your wallet is as secure with high values as it is with low ones. Higher values merely ensure that your node will not shut down upon blockchain reorganizations of more than 2 days - which are unlikely to happen in practice. In future releases, a higher value may also help the network as a whole because stored blocks could be served to other nodes.

1.同时推荐阅读Bitcoin的wiki 整篇文档

2.解决方案原文

8️⃣BIP-322 了解一下哈！摘要：

1.证明地址的所有权，证明向现实世界供应商付款或者像简单证明匿名身份并避免欺诈

2.P2PKH地址（以1开头的旧地址），省略了使用P2SH或任何不同类型的segwit地址执行此操作的标准方法

3.提出了可以用于任何类型地址的BIP 322,不是向后兼容原始实现，但它可以使任何地址（包括遗留地址）能够签署消息

4.基本概念是一个授权的消费者，一个地址生成scriptSigs和见证数据，包括他们的签名，就像他们花费资金一样，但是他们没有签署支出交易，而是签署他们的附属消息（包括一些预定义的额外数据，以防止他们被欺骗签署真实交易）。验证者的软件验证此数据的方式与确定支出交易是否有效的方式相同。这将使比特币中的消息签名工具像任何比特币脚本一样灵活。

1.BIP-322 GitHub

2.BIP-322 Github讨论

9️⃣Bitcoin 发布0.16.3的版本之后，声称最好强制升级，因为老版本有严重的bug,直到前天为止，升级的几点也只有2/9左右（2270，截止到我写这个晚报），也就是有至少80%左右的节点还没更新最新版本，那老版本会不会被黑客利用呐？嘿嘿来看看这些文章吧！The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret!

Big thanks are owed to this dev. Great work finding and responsibly handling the bug!

不想看给你总结一下，摘要：

1.这600微秒的优化现在产生了CVE-2018-17144。当然是近年来最具灾难性的错误，当然也是比特币中最具灾难性的错误之一！

2.六百微秒。那是Matt Corallo想要通过2016年对比特币核心的拉动请求削减区块验证的时间。

1.来看看reddit的讨论

2.原文

[3.medium报道]

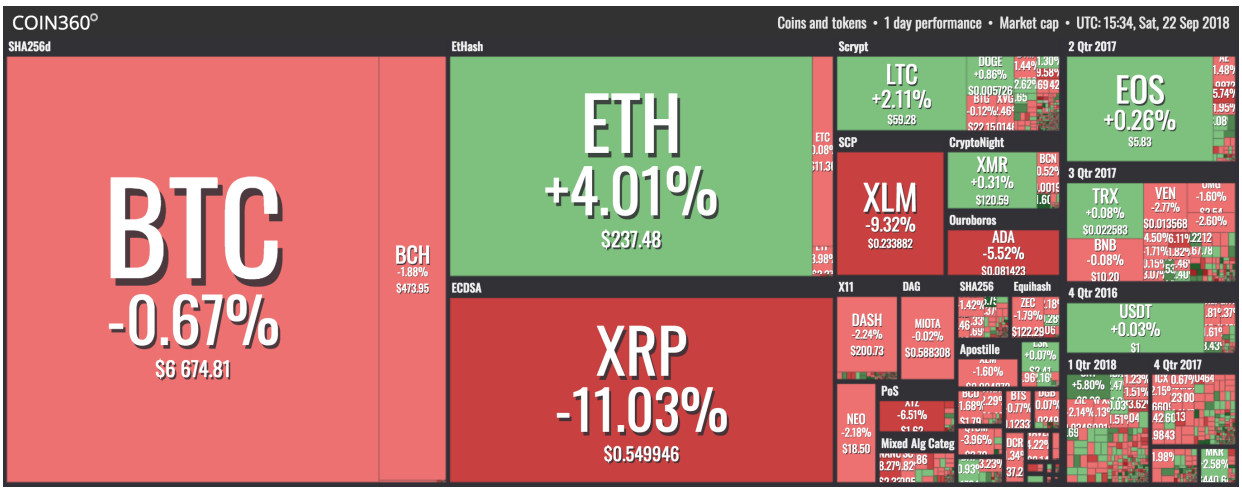
[4.CVE-2018-17144]

🔟未来是公有链成功还是联盟链成功?

推荐阅读!

[1.看看这篇]

二.货币市场24h表现

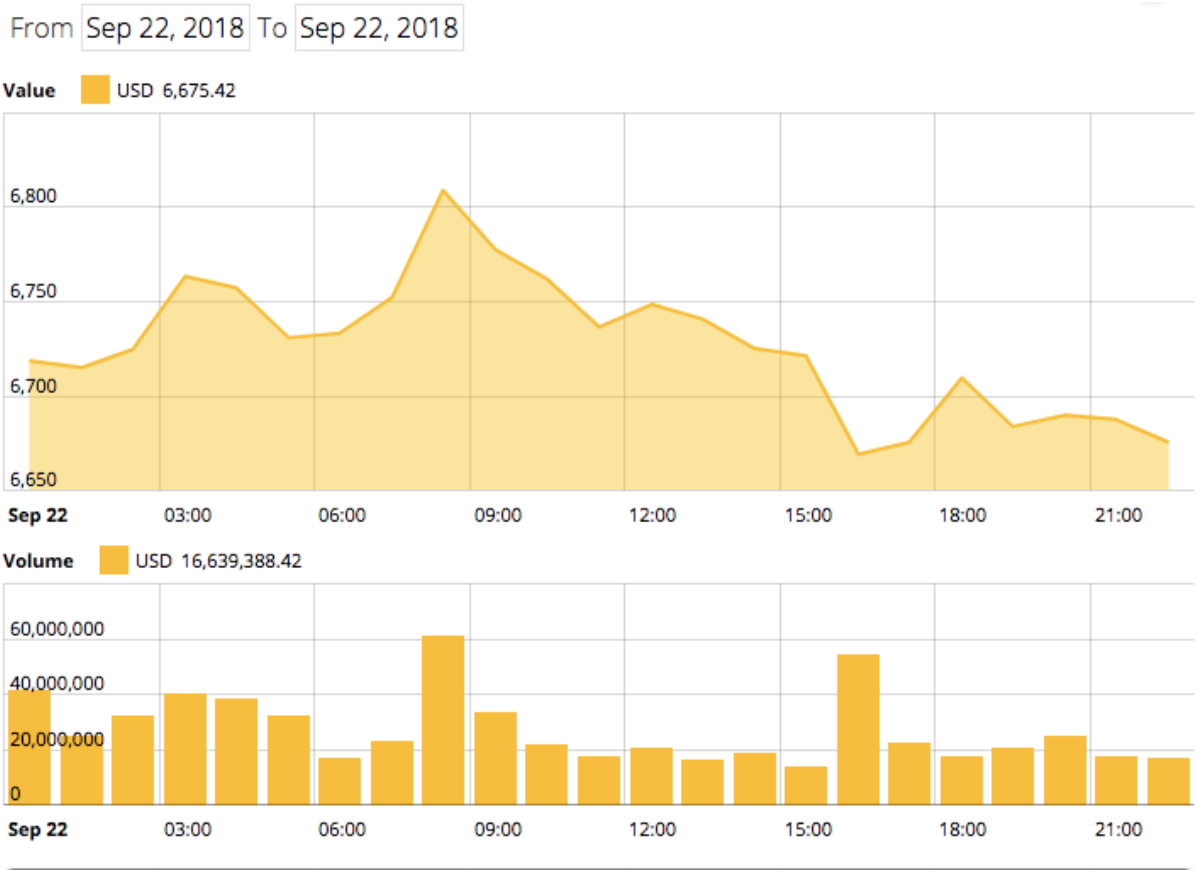


img source: coin360

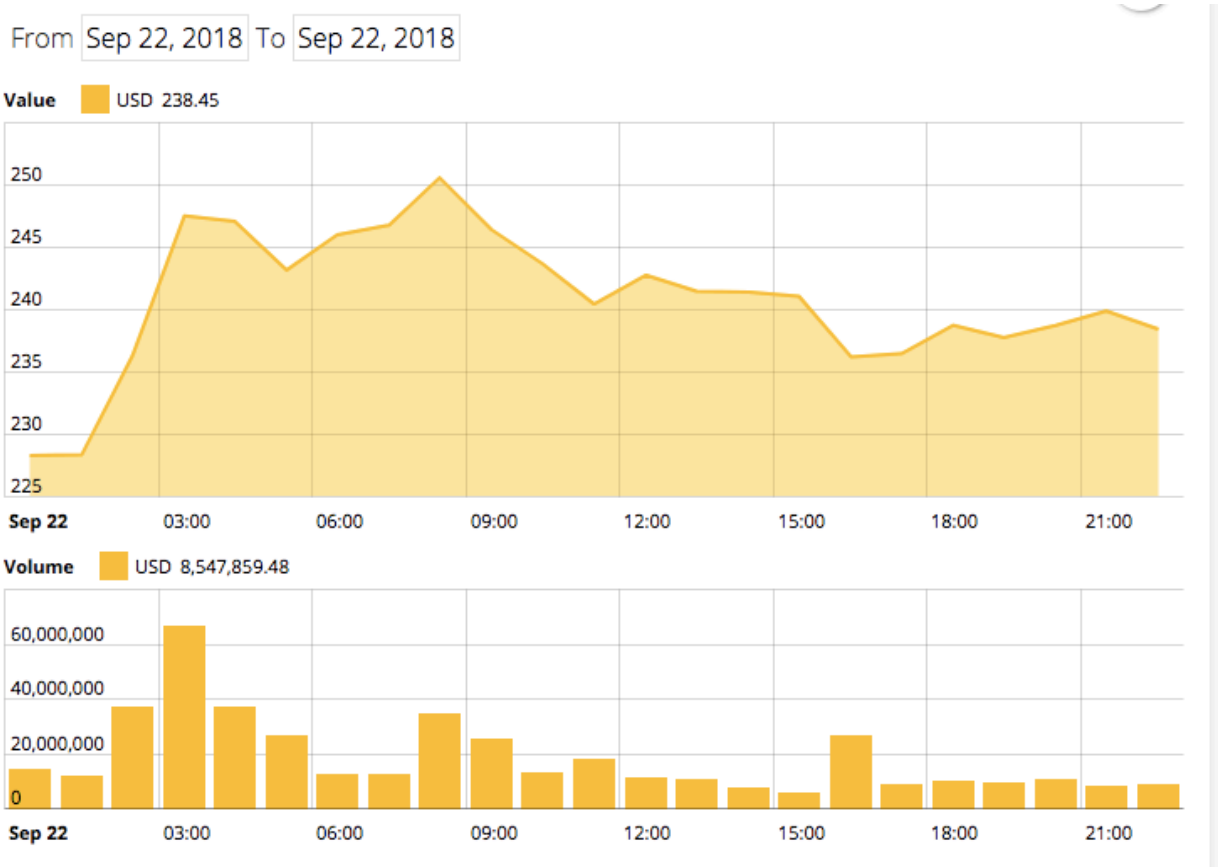
BTC & ETH & EOS 今日表现(截止发稿时间)

img source： cointelegraph

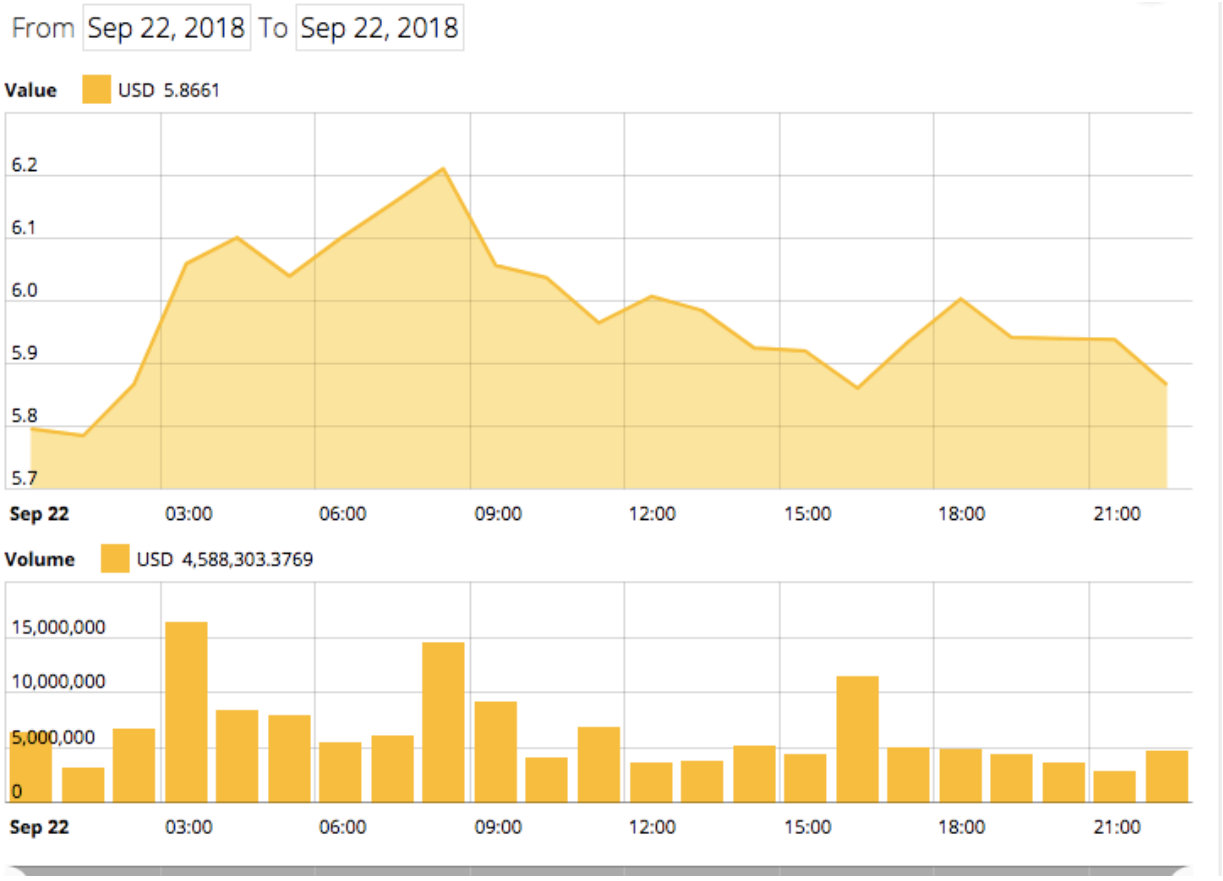
BTC:


From Sep 22, 2018 To Sep 22, 2018
Value
USD 6,675.42
6,800
6,750
6,700
6,650
Sep 22
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Volume
USD 16,639,388.42
60,000,000
40,000,000
20,000,000
0
Sep 22
03:00
06:00
09:00
12:00
15:00
18:00
21:00

ETH:


From Sep 22, 2018 To Sep 22, 2018
Value
USD 238.45
250
245
240
235
230
225
Sep 22
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Volume
USD 8,547,859.48
60,000,000
40,000,000
20,000,000
0
Sep 22
03:00
06:00
09:00
12:00
15:00
18:00
21:00

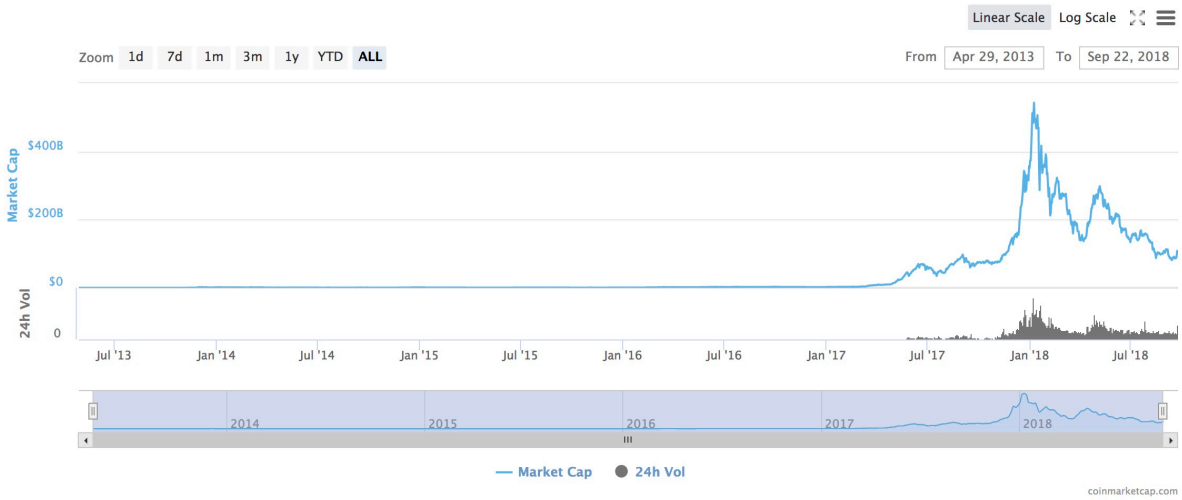
EOS:


From Sep 22, 2018 To Sep 22, 2018
Value
USD 5.8661
6.2
6.1
6.0
5.9
5.8
5.7
Sep 22
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Volume
USD 4,588,303.3769
15,000,000
10,000,000
5,000,000
0
Sep 22
03:00
06:00
09:00
12:00
15:00
18:00
21:00

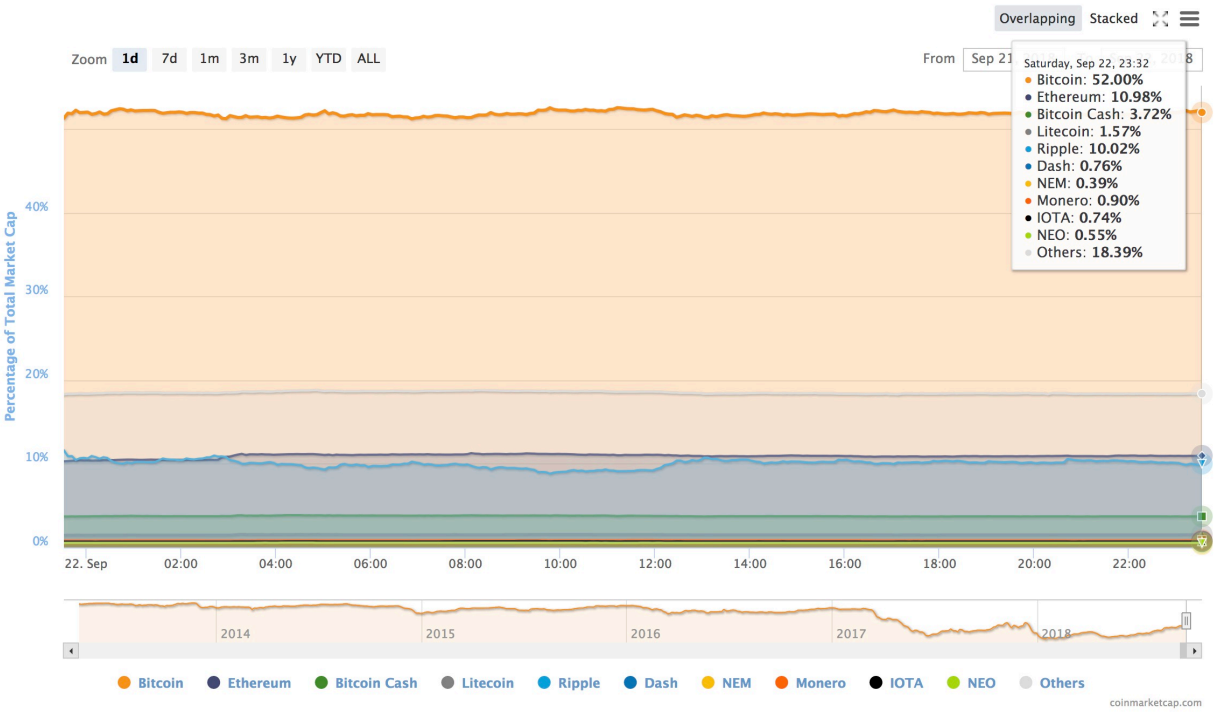
总量：

Total Market Capitalization

Total Market Capitalization (Excluding Bitcoin)



Percentage of Total Market Capitalization (Dominance)



24小时涨跌榜

Asset	Symbol	% Change 24h
electroneum	$ETN	21.04%
emercoin	$EMC	16.12%
kin	$KIN	12.14%
digixdao	$DGD	6.42%
ontology	$ONT	5.64%
ethereum	$ETH	4.27%
loopring	$LRC	3.63%
gxchain	$GXS	3.49%
bancor	$BNT	3.10%
litecoin	$LTC	3.00%

Asset	Symbol	% Change 24h
dropil	$DROP	-14.23%
aurora	$AOA	-14.06%
ripple	$XRP	-9.31%
monacoin	$MONA	-8.41%
stellar	$XLM	-8.36%
nano	$NANO	-6.75%
tezos	$XTZ	-5.86%
chainlink	$LINK	-5.24%
status	$SNT	-5.21%
cardano	$ADA	-4.47%

以上内容由火币大学整理，感谢阅读! 晚报汇聚地址为:https://github.com/HuobiUniversity/BlockChain_Daily_Report

欢迎大家star&watch!