

# 门罗币硬分叉升级对抗ASIC矿机

## 一周回顾

- 加密货币总市值2090亿美元，环比上周下降0.8%，排名前100的币种7日交易量下降13.9%

## 一周展望

- 10月29日：IOTA于亚特兰大参加物联网区块链峰会
- 10月29日：ADA支持Trezor冷钱包

## 本周分析

于2014年4月推出的门罗币 (XMR) 是早期隐私币的代表，利用环签名，隐私环交易和隐秘地址技术来保障用户的隐私。最近门罗币进行了Monero 0.13.0 Beryllium Bullet硬分叉，启用了防弹协议 BulletProof 的同时也更新了CryptoNight工作量证明 (PoW) 算法。

防弹协议的生效使交易手续费降低94%至0.017美元。门罗币之前采用“范围验证Range Proof”技术来防止用户发出负数交易金额以确保交易的有效性。此方法会令交易区块变大 (比特币的4倍)，进而导致交易费用更高。相反地，防弹协议的使用减少了验证数据的大小，这使交易区块显著缩小约80%。

门罗币致力于对抗ASIC矿机，本次升级对CryptoNight PoW共识机制制作出了更新，将挖矿的内存带宽要求增加到64字节，为原来的4倍。为特定共识算法而量身定制的ASIC矿机挖矿速度相比GPU矿机快10万倍。ASIC挖矿设备主要由大型矿池持有，此种情况增加了挖矿中心化的风险，使51%攻击的威胁增大。而ASIC设备制造商对市场的垄断进一步增加了中心化的风险。

Beryllium Bullet硬分叉之后，门罗币的挖矿难度下降24%，这是因为挖矿的内存要求增加，使现有的ASIC矿工难以挖到门罗币。为了应对来自主流加密货币，其他设备制造商和其他矿池对ASIC矿机的对抗，ASIC制造商比特大陆最近推出了适用于S9 Antminer矿机的“Overt ASICboost”更新，此更新预计可以节约13%的能源消耗。然而其竞争对手SlushPool并不建议矿工采用此更新，因为它与BIP310标准不兼容。

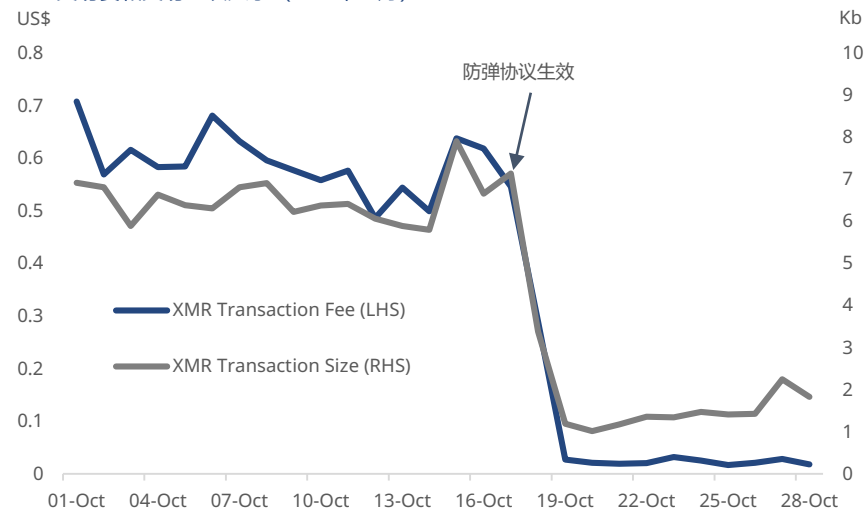
我们预计会有更多加密货币开始布局对抗ASIC矿机，比如明年将会推出君士坦丁堡更新的以太坊。

## 主要加密货币表现

币种	价格	7日%	交易量	7日%	总市值	市值占有率
BTC	\$6,477.32	-0.56%	20.43bn	-8.49%	112.35bn	53.76%
ETH	\$204.25	-1.29%	6.80bn	-15.21%	21.01bn	10.05%
XRP	\$0.46	-0.93%	1.74bn	-27.97%	18.37bn	8.79%
BCH	\$438.05	-2.68%	1.47bn	-18.52%	7.63bn	3.65%
EOS	\$5.39	-1.09%	2.06bn	-14.93%	4.89bn	2.34%
XLM	\$0.23	-6.55%	0.23bn	-30.13%	4.33bn	2.07%
USDT	\$0.99	1.25%	10.81bn	-24.39%	1.92bn	0.92%
ADA	\$0.07	-5.33%	0.08bn	-44.12%	1.89bn	0.90%
XMR	\$103.15	-1.31%	0.09bn	-14.67%	1.70bn	0.82%
DASH	\$153.99	-1.10%	0.95bn	-2.08%	1.29bn	0.62%

## 本周图表

XMR交易费和交易区块大小 (2018年10月)



## 本周主要新闻

香港证券交易所发表报告称加密货币及区块链服务应受到现有的法律监管：研究报告主要阐述了目前区块链技术在交易清算，资产再抵押以及私募股权融资等领域的应用。

洲际交易集团 (Intercontinental Exchange - ICE) 宣布比特币期货合约将于12月12日在交易平台Bakkt上线：Bakkt的期货合约将由ICE美国清算公司进行清算。

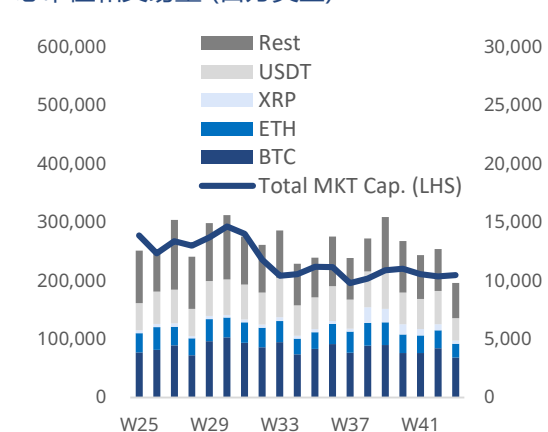
中国金融区块链深圳联盟 (FISCO) 主导的无币区块链生态系统FISCO BCOS将首次亮相：此联盟由国内科技巨头腾讯，华为等企业联手创立。

Tether公司宣布销毁5亿USDT：此次销毁信息显示在OMNI区块链浏览器上，剩余的4.66亿枚USDT将被预留供未来发行。

## 网络基础数据

	BTC	ETH
哈希率	49,886,595 TH/s (-3.4%)	244,195 GH/s (-3.0%)
钱包用户数	29,580,712 (+0.7%)	45,232,992 (+1.4%)
前三名矿池	BTC.com (18%) AntPool (14%) BTC.TOP (11%)	Ethermine (26%) SparkPool (22%) F2 Pool (13%)

## 总市值和交易量 (百万美金)



Please see important disclosure on next page.

# STANDARD KEPLER

WEEKLY SUMMARY | 22 – 28 OCTOBER

## DISCLAIMER

**Abbreviations:** ADA: Cardano; approx.: approximately; ASIC: Application Specific Integrated Circuits; BCH: Bitcoin Cash; bn: billion; BTC: Bitcoin; crypto: cryptocurrencies; ETH: Ethereum; FISCO: The Chinese Financial Blockchain Shenzhen Consortium; GPU: Graphical Processing Units; HKEx: Hong Kong Stock Exchange; ICE: Intercontinental Exchange; Kb: Kilobyte; Market Cap: Market Capitalization; mn: million; Oct.: October; Trading Vol.: Trading Volume; US\$: United States Dollars; USD: USD Tether; U.S. SEC: The U.S. Securities and Exchanges Commission; XLM: Stellar Lumens; XMR: Monero; XRP: Ripple; ZEC: Zcash

**Chart of The Week:** Sources: Bitinfocharts, Coinmetrics.io, Standard Kepler Research

**Market Cap & Trading Vol.:** Sources: Coinmarketcap, Standard Kepler Research

The horizontal axis represents the week number in 2018. For instance, W25 indicates the twenty fifth week in 2018. The primary vertical axis represents total market capitalization; and the secondary vertical axis represents total trading volume.

**Network Fundamentals:** Sources: Blockchain.info, Blocktrail, Etherchain.org, Etherscan.io, Standard Kepler Research

**Thought of The Week:** Sources: Bitcoinist.com, Bitinfocharts, Bitmain, Blockcast.it, Bloomberg, CCN, Coindesk, Cointelegraph, Compute North LLC, Ethereum World News, Github, Monero Blog, SlushPool, Standard Kepler Research

**Top Crypto News At a Glance:** Sources: Blockcast.it, Coindesk, Cointelegraph, Hong Kong Stock Exchange, Intercontinental Exchange, Standard Kepler Research

**Top Crypto Performance Summary:** Sources: Coinmarketcap, Standard Kepler Research

**Week Ahead:** Sources: Cryptocalendar.pro, Standard Kepler Research

**Weekly Recap:** Sources: Coinmarketcap, Standard Kepler Research

Past performance does not guarantee future results.

Opinions and estimates offered constitute our judgment and are subject to change without notice, as are statements of financial market trends, which are based on current market conditions. We believe the information provided here is reliable, but do not warrant its accuracy or completeness. This material is not intended as an offer or solicitation for the purchase or sale of any cryptocurrencies. The views and strategies described may not be suitable for all investors. This material has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for, accounting, legal or tax advice. Any forecasts contained herein are for illustrative purposes only and are not to be relied upon as advice or interpreted as a recommendation.

The price of Bitcoin and other cryptocurrencies are highly volatile in nature. It is suggested that clients should perform their own due diligence and consult a fully qualified independent professional financial adviser before making any investments in cryptocurrencies.

©Standard Kepler, October 2018.

Unless otherwise stated, all data is as of October 28, 2018 or as of most recently available.