

Monero Leads the Way Towards ASIC Resistance

WEEKLY RECAP

- Total market cap. reached \$209bn (a 0.8% decrease), and 7 day trading volume slumped 13.9% for top 100 crypto

WEEK AHEAD

- 29 Oct:** IOTA at IoT Atlanta blockchain summit
- 29 Oct:** ADA supports Trezor hardware wallet

THOUGHTS OF THE WEEK

First launched in April 2014, Monero (XMR) is a pioneer among privacy tokens, preserving user privacy using ring signatures, ring confidential transactions and stealth addresses. Recently Monero launched the "Monero 0.13.0 Beryllium Bullet" hard fork, introducing "bulletproof" technology, and updating XMR's CryptoNight proof-of-work algorithm.

Following the introduction of bulletproof technology, XMR transaction (tx) fees dropped 94% to US\$ 0.017 per tx (as observed in our Chart of the Week). Prior to bulletproof, XMR adopted "range proof" to prove that the value of a tx falls between 0 and a large number, so as to prevent the sending of negative tx amounts. The downside of using range proof technology is the resulting large data size per tx (about 4x higher than BTC), leading to higher tx fees. Bulletproof shrinks the size of cryptographic proofs used, leading to a ~80% decrease in tx size.

The latest upgrade of XMR also includes a tweak to its CryptoNight proof-of-work algorithm, increasing the memory bandwidth requirement of mining to 64 bytes (a 4x increase), in line with XMR's stated goal of pursuing ASIC mining resistance. ASIC mining devices are customized to execute a single hash algorithm, and are thus able to compute hashes 100,000 times faster than GPUs. There are several reasons why major altcoins strive to achieve ASIC resistance. ASIC mining devices are largely operated by large mining pools as they are too expensive for most home users, and this centralization of mining power can in turn lead to increased vulnerability to 51% attacks. This risk of centralization is further enhanced by the monopolistic nature of the ASIC device manufacturing industry.

The mining difficulty of XMR has dropped 24% in the wake of the Beryllium Bullet fork, primarily a result of the increased memory requirements to mine, making XMR mining an unviable option for ASIC miners. Responding to increasing pressure from altcoins, device manufacturers, and mining pools alike, ASIC manufacturer Bitmain recently launched the "overt ASICboost" update to the company's S9 Antminer devices. While the update brings about energy cost savings of an estimated 13%, competing mining pool SlushPool urged its users not to apply the update due to its incompatibility with the BIP310 standard.

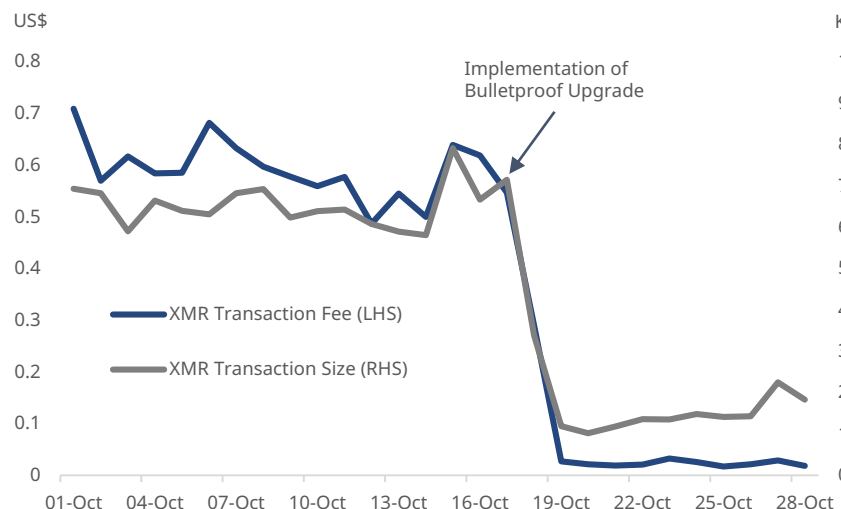
Moving forward, we expect further major altcoins to strive towards achieving ASIC resistance, with sector behemoth Ethereum pursuing ASIC resistance in its upcoming Constantinople update.

TOP CRYPTO PERFORMANCE SUMMARY

Name	Price	7D%	Vol.	7D%	Mkt Cap.	% Total Mkt
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%

CHART OF THE WEEK

Monero's Transaction Fee and Transaction Size in October 2018



TOP CRYPTO NEWS AT A GLANCE

HKEx report proposes that cryptocurrencies and blockchain should be regulated within existing legal frameworks: The report highlights blockchain's application in clearing and settlement, asset rehypothecation and private equity markets.

Intercontinental Exchange (ICE) announces the 12 December launch of BTC futures on Bakkt: The future will be physically-settled and cleared by ICE Clear US.

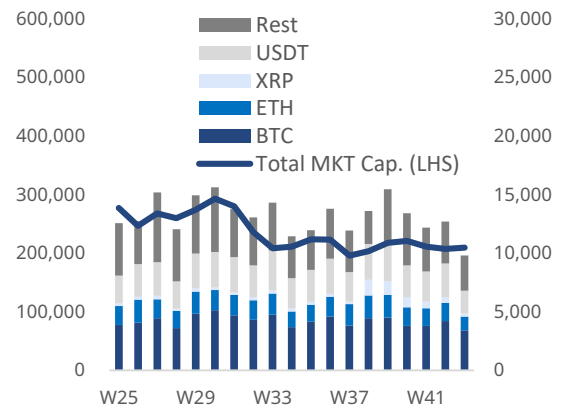
The Chinese Financial Blockchain Shenzhen Consortium (FISCO) announces coinless blockchain FISCO BCOS: The consortium is led by tech giants including Tencent and Huawei.

Tether limited burns 500mn units of USDT: The redemption is visible on the OMNI blockchain explorer. The remaining USDT (approx. 466mn) is reserved for future USDT issuances.

NETWORK FUNDAMENTALS

	BTC	ETH
Hashrate	49,886,595 TH/s (-3.4%)	244,195 GH/s (-3.0%)
# Wallet Users	29,580,712 (+0.7%)	45,232,992 (+1.4%)
Top 3 Miners	BTC.com (18%) AntPool (14%) BTC.TOP (11%)	Ethermine (26%) SparkPool (22%) F2 Pool (13%)

MARKET CAP & TRADING VOL. (US\$ MN)



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.