

# 以太经典51%攻击让PoW公链安全性告急

## 一周回顾

- 加密货币总市值1223亿美元，环比上周下降6.9%，排名前100的币种7日交易量上升6.4%

## 一周展望

- 1月16日: 以太坊君士坦丁堡硬分叉
- 1月16日: Cboe比特币期货XBT合约到期

## 本周分析

除了以太坊君士坦丁堡硬分叉，我们认为投资人更需留意以太经典最近的51%攻击事件。

共识算法定义了区块链协议的治理方式，并消除了第三方管理区块链的需要，同时定义如何确认区块，从而确保链上数据的完整性。遭受51%攻击标志着以太经典这条公链已经基本失去价值。

而尽管受到了51%攻击，ETC的价格仍然保持相对稳定。这说明ETC的交易很有可能正在受到操控，许多投资者并没有认识到51%攻击的严重性，并认为其与一般黑客攻击无异。所有权中心化问题和监管的缺失使得ETC价格的受操纵可能性较高。

我们认为，51%攻击会在短期内让公众对ETC的信任显著下降。长远来看，这种攻击可能会让加密货币生态环境产生恶性循环。51%攻击削弱了公众对PoW公链的信任，并导致矿工和用户逐步退出。而矿工的退出将会导致挖矿成本下降，使区块链更容易受到51%攻击，进而导致价格进一步下跌。

值得注意的是，对ETC发起51%攻击的每小时成本仅为4293美元（如本周图表所示）。而比特币的网络仍然较为去中心化，因此不太可能受到51%攻击。假设每千瓦电费为0.05美元，Bitstamp预估对比特币发动51%攻击的电费成本为550万美元，而这还没有包括挖矿设备的巨额购置成本。

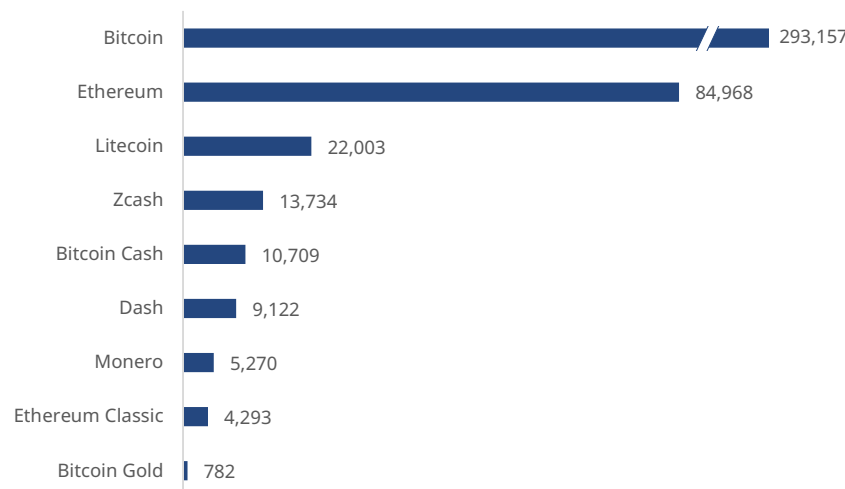
我们认为此次51%攻击使行业进一步偏离了Satoshi对公链的愿景，并且可能预示着公链未来的发展。我们可以预见，在将来用户可能离开PoW公链并转向PoS公链。而如果前20名的任何一个加密货币遭受51%攻击，用户更有可能转而使用私有链。

## 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	\$3,663.12	-4.62%	32.12bn	8.99%	64.03bn	52.36%
XRP	\$0.33	-7.25%	3.16bn	11.99%	13.57bn	11.10%
ETH	\$125.69	-18.10%	15.27bn	-14.44%	13.12bn	10.72%
BCH	\$134.68	-15.95%	1.29bn	-9.16%	2.37bn	1.93%
EOS	\$2.43	-9.72%	4.78bn	7.68%	2.20bn	1.80%
XLM	\$0.11	-3.59%	0.65bn	19.01%	2.10bn	1.72%
USDT	\$1.02	0.45%	24.05bn	3.52%	1.97bn	1.61%
BSV	\$85.71	-2.59%	0.59bn	28.26%	1.51bn	1.23%
ADA	\$0.04	-5.93%	0.26bn	57.64%	1.13bn	0.92%
XMR	\$45.19	-9.96%	0.12	31.19%	0.75bn	0.62%

## 本周图表

对PoW公链进行51%攻击所需成本（美元/每小时）



## 本周主要新闻

**以太坊将于1月16日进行君士坦丁堡硬分叉**：核心开发者Péter Szilágyi表示目前以太坊Rinkeby测试网已经成功升级至君士坦丁堡网络，挖矿奖励也会从每个区块3个ETH减少至2个。

**中央网络安全和信息化委员会办公室（CAC）公布《区块链信息服务管理规定》**：规定将于2月15日起实施，主要针对向公众提供区块链信息及技术服务的公司与组织。

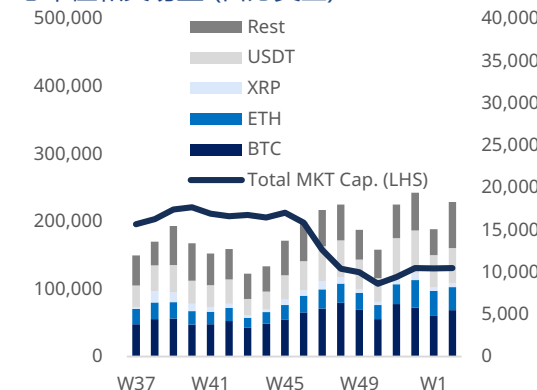
**泰国财政部向四家加密货币相关公司发出虚拟资产经营许可证**：与此同时，财政部长以电子KYC系统及资产维护系统不符合标准为理由拒绝了另外两家交易所申请。

**日本金融厅（FSA）否认有关批准比特币ETF的传言**：FSA正在考虑将加密货币归类为新的合法资产类别“加密资产”。

## 网络基础数据

	BTC	ETH
哈希率	42,014,988 TH/s (-0.9%)	182,362 GH/s (+2.1%)
钱包用户数	32,235,415 (+0.7%)	52,569,916 (+1.0%)
前三名矿池	BTC.com (14%) SlushPool (12%) AntPool (11%)	Ethermine (28%) SparkPool (23%) NanoPool (13%)

## 总市值和交易量（百万美金）



## DISCLAIMER

**Abbreviations:** ABC: Adjustable Blocksize Cap; ADA: Cardano; b/w: between; BCH: Bitcoin ABC; BCH SV: Bitcoin Satoshi Vision; bn: billion; BTC: Bitcoin; CAC: The Cyberspace Administration of China; Cboe: Cboe Global Markets, Inc.; crypto: cryptocurrencies; ETF: Exchange traded funds; ETH: Ethereum; Feb: February; FSA: Financial Services Agency; ICO: Initial Coin Offerings; Jan: January; KYC: Know your customer; Market Cap: Market Capitalization; mn: million; Nov: November; SEC: The U.S. Securities and Exchange Commission; Trading Vol.: Trading Volume; US\$: United States Dollars; USDT: USD Tether; XLM: Stellar Lumens; XMR: Monero; XRP: Ripple

**Chart of The Week:** Sources: Crypto51.app, Standard Kepler Research

**Market Cap & Trading Vol.:** Sources: Coinmarketcap, Standard Kepler Research  
The horizontal axis represents the week number in 2018. For instance, W37 indicates the thirty seventh week in 2018. W1 indicates the first week in 2019. The primary vertical axis represents total market capitalization; and the secondary vertical axis represents total trading volume.

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

**Thought of The Week:** Sources: Bitstamp, Bloomberg, Coinbase, Coindesk, Coinmarketcap, Coinmonks, Cointelegraph, Crypto51.app, Ethereum Classic, Slowmist, Standard Kepler Research

**Top Crypto News At a Glance:** Sources: Blockcast.it, CCN, Coindesk, Cointelegraph, 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, January 2019.

Unless otherwise stated, all data is as of January 13, 2019 or as of most recently available.

## ABOUT STANDARD KEPLER

Standard Kepler is Asia's leading blockchain financial services provider, offering market changing research insights, in addition to holistic advisory, brokerage, and custodian services. We take great pride in being able to offer professional services that are trusted for our honesty and driven by technology. Headquartered in Hong Kong, Standard Kepler's management team previously served in JP Morgan, Macquarie Capital, State Street, and KPMG.

Standard Kepler's research insights are distributed in collaboration with several partners, including Thomson Reuters, BTC.com, and Binance. If you are interested in exploring more of our research insights, or becoming one of our research distribution partners, visit [www.standardkepler.com/research](http://www.standardkepler.com/research) or contact us directly at [research@standardkepler.com](mailto:research@standardkepler.com).