很多朋友在找时都会咨询XEM交易所和MXC交易所官网，这说明有一部分人对这个问题不太了解，您了解吗？那么什么是MXC交易所官网？下面就由小编带大家详细了解一下吧！

主流币包括比特币（BTC）、瑞波币（XRP）、艾达币（ADA）、莱特币（LTC）、以太币（ETH）、比特币现金（BCH）、新经币（XEM）、恒星币（XLM）、达世币（DASH）等，主流货币的选择取决于货币的最大供给量、市值、历史高位与现价，排名前几的主流币也是投资者最容易相信的币种。

拓展资料:

1、比特币市值4416.85亿美元，占全球总市值71.12%，流通数量1857.5万，24小时成交额172.27亿美元，上架了319家交易所。 比特币几乎是币圈新人的必经之路，凭借巨大的市值优势，也非常适合一些机构投资者的进行投资。最为新人的话最推荐的投资币种也是比特币，毕竟整个币圈的沉浮，都要看比特币的脸色，熟悉做好比特币的投资，后面再做山寨币也会更加的得心应手了。

2、以太坊市值696.57亿美元，占全球总市值的11.22%，流通总量1.13亿，24小时成交额85.09亿美元，上架了326交易所。 目前以太坊市值排第二，定有其自身的价值，可以用来创建去中心化的程序，自治组织和智能合约，智能合约的潜在应用很多。彭博社商业周刊称它是“所有人共享但无法篡改的软件”。更高级的软件有可能用以太坊创建网络商店。因为艾希欧的缘故其最风光时达到一万多人民币的价格，当然这也成为其中的一个弱点，当项目方抛售时，其价格也跟着应声而下，更重要的是以太坊拥堵也异常厉害，希望以太坊团队能够越来越完善。

3、泰达币市值201.1亿美元，占全球总市值的3.24%，流通总量201.16亿，24小时成交额522.77亿美元，上架了200交易所。 泰达币有着先发的优势，目前市值第五名，由于是稳定币，波动性总体不大，对于投资者来说不适合小玩，加上不管什么都可能面临破产，跟公司开户的银行，也有可能破产，也有可能捐款跑路风险等等，虽然是稳定币投资者还是要多注意，需谨慎，虽然很少发生，但是在币圈还是有可能的，潜在风险大。

2008年全球金融危机因为中心化世界的种种弊端而爆发并进而席卷全球，为了消除这些弊端，中本聪创立了比特币网络，区块链也因此诞生。

为了提高整个网络以及交易的安全性，区块链采用分布式节点和密码学，且所有链上的记录是公开透明、不可篡改的。最近几年，区块链获得长远发展，形成了庞大的加密生态。

然而，区块链自问世以来，加密货币骗局频发并有愈演愈烈之势，加密货币也无法为用户的资金提供足够的安全性。此外，加密货币可以匿名转移，从而导致加密行业的重大攻击盗窃事件频发。

下文将梳理剖析加密史上十大加密货币盗窃事件，以及防范加密资产被盗的六大实用策略。

1.Mt. Gox 被盗事件

Mt. Gox 被盗事件仍然是 历史 上最大的加密货币盗窃案，在 2011 年至 2014 年期间，有超过 85 万比特币被盗。

Mt. Gox 声称导致损失的主要原因是源于比特币网络中的一个潜在漏洞——交易延展性，交易延展性是通过改变用于产生交易的数字签名来改变交易的唯一标识符的过程。

2011 年 9 月，MtGox 的账户私钥就已泄露，然而该公司并没有使用任何审计技术来发现漏洞并预防安全事件的发生。此外，由于 MtGox
定期重复使用已泄露私钥的比特币地址，导致被盗资金损失不断扩大，到 2013 年中，该交易所已被黑客盗取63万枚比特币。

许多交易所会同时使用冷钱包和热钱包来进行资产的存储和转移，一旦交易所的服务器被黑，黑客便可以盗取热钱包里面的加密资产。

2.Linode被盗事件

加密网络资产托管公司Linode主要业务就是托管比特币交易所和巨鲸的加密资产，不幸的是，这些被托管的加密资产储存在热钱包中，更为不幸的是，Linode 于 2011 年 6 月遭到黑客攻击。

这导致超过5万枚比特币被盗，Linode的客户损失惨重，其中，Bitcoinia、Bitcoin.cx以及Gavin Andresen分别损失43000枚、3000枚和5000枚比特币。

3.BitFloor被盗事件

2012 年 5 月，黑客攻击 BitFloor 并盗窃了24000枚比特币，这一切源于钱包密钥备份未加密，才使攻击者轻而易举获得了钱包密钥，并进而盗取了巨额加密资产。

被盗事件发生后，BitFloor 的创建者 Roman Shtylman 决定关闭交易所。

4.Bitfinex被盗事件

使用多重签名账户并不能完全杜绝安全事件的发生，Bitfinex接近12万枚巨额比特币资产被盗事件就证明了这一点。

2022年6月份，2000万枚OP代币就是以为不恰当使用多重签名账户而被盗。

5.Coincheck被盗事件

总部位于日本的 Coincheck 在 2018 年 1 月被盗价值 5.3 亿美元的 NEM（XEM）代币。

Coincheck事后透露，由于当时的人员疏忽，黑客能够轻易访问他们的系统，且由于资金保存在热钱包中并且安全措施不足，黑客能够成功盗取巨额加密资产。

6.KuCoin被盗事件

KuCoin 于 2020 年 9 月宣布，黑客盗取了大量的以太坊（ETH)、BTC、莱特币（LTC）、Ripple（XRP）、Stellar Lumens（XLM）、Tron（TRX）和USDT等加密资产。

朝鲜黑客组织 Lazarus Group
被指控为KuCoin被盗事件的始作俑者，这次被盗事件造成了2.75
亿美元的资金损失。幸运的是，该交易所收回了约2.7亿美元的被盗资产。

7.Poly Network被盗事件

Poly Network被盗事件是有史以来最严重的加密货币盗窃案之一，2021 年 8 月，一位被称为“白帽先生”的黑客利用了 DeFi 平台 Poly Network
网络中的一个漏洞，成功窃取了Poly Network上价值约 6 亿美元的加密资产。

Poly Network被盗事件蹊跷的是，自被盗事件发生后，“白帽先生”不仅与Poly Network官方保持公开对话，而且还于一周后归还了所有被盗的加密资产。“白帽先生”因此获得50万美元的奖金，并获得了成为 Poly Network
高级安全官的工作机会。

8.Cream Finance被盗事件

2021 年 10 月，Cream Finance发生安全事件，被黑客盗取价值1.3

亿美元的加密资产。这是 Cream Finance
今年发生的第三起加密货币盗取事件，黑客在 2021 年 2 月盗取了 3700
万美元的加密资产，在 2021年 8 月盗取了 1900 万美元的加密资产。

本次被盗事件是通过闪电贷攻击的方式完成的，攻击者使用 MakerDAO 的 DAI
生成大量 yUSD 代币，同时还利用 yUSD 价格预言机来完成闪电贷攻击。

9.BadgerDAO被盗事件

2021 年 12 月，一名黑客成功从DeFi 项目 BadgerDAO
上的多个加密货币钱包中窃取资产。

该事件与通过Cloudflare将恶意脚本注入网站用户界面时的网络钓鱼上述文章内容就是。 黑客利用应用程序编程接口 (API) 密钥窃取了 1.3 亿美元的资金。API
密钥是在 Badger 工程师不知情或未经许可的情况下创建的，用于定期将恶意代码注入其一小部分客户端。

然而，由于黑客未能及时从Badger提取资金，因此大约 900
万美元加密资产得以追回。

10.Bitmart被盗事件

2021 年 12 月，Bitmart 的热钱包遭到黑客攻击，约 2
亿美元加密资产被盗。研究发现，约1 亿美元的加密资产是通过以太坊网络盗取转移的，另外接近1亿美元是通过币安智能链网络盗取转移的。

此次被盗事件涉及20多种代币，包括比特币等主流币，和相当数量的山寨币等。

保护加密资产的最佳方法是重视钱包的加密保护和安全的私钥存放方式，以及对市场上的项目进行深入的研究和辨识，避免踏入攻击者的陷阱。

由于区块链的不可篡改和不可逆性，一旦钱包私钥泄露，加密资产被盗便不可避免并无法追回。

防范加密资产被盗的六大实用策略：

1.使用冷钱包

与热钱包不同，冷钱包不连接互联网，因此不会受到网络攻击。私钥存储在冷钱包

中可有有效保护加密资产。

2.使用安全网络

在交易或进行加密交易时，仅使用安全的网络，避免使用公共 Wi-Fi 网络。

3. 资金分散到多个钱包中

鸡蛋不要放到同一个篮子中，这句话在金融领域和加密领域都十分受用。

将加密资产分发到不同的多个钱包中，这样可以在遭受攻击时，将损失降到最低。

4. 提高个人设备安全性

确保个人设备安装了最新的安全软件，以防御新发现的漏洞和网络攻击，并且开启防火墙来提高设备的安全性，以避免黑客通过设备系统安全漏洞来进行攻击。

5.设置强密码并定期更改

在谈论安全性时，我们不能低估强密码的重要性。很多人在多个设备、应用程序社交媒体帐户和加密钱包上使用相同的密码，这大幅增加了加密资产被盗的几率。

防止被盗需要钱包账户建立一个安全等级较高的强密码，这个强密码需要具有独特性，并养成定期更改的习惯。此外，选择双重身份验证 (2FA) 或多重身份验证 (MFA) 可以提高安全性。

6. 谨防钓鱼攻击

通过恶意广告和电子邮件进行的网络钓鱼诈骗在加密货币世界中十分猖獗。在进行加密交易时要格外小心，避免点击任何可疑和未知链接。

应当始终检查核实上述文章内容就是加密投资的相关信息和网站的URL，尤其是这些信息极具诱惑力且不合常理时，比如，项目方官方通过Didcord等渠道私聊信息，当然，项目方Didcord被攻击的安全事件的频繁发生，这时的恶意链接可能是在公共频道中而不是私聊界面，这种情况下，多渠道检查核实上述文章内容就是加密投资相关信息的真实性就显得格外重要了！

SAFEIS是国际知名的创新型区块链生态安全服务平台，基于 数据、智能、网络安全、图计算等多种核心技术打造，具有完备的数据处理和精准追溯能

，服务对象涵盖全球诸多知名公司和项目。

“让区块链更安全”是一个光荣使命，我们将践行光荣使命、续航崭新征程。

1、aofex是英国伦敦数字货币交易所，交易诸如比特币这样的数字加密货币。aofex创造了非标准化期权交易NSO，它的交易方式和潜在收益多种多样，可在有限可控的风险暴露下执行交易。

2、UKEX Global又被称之为UKEX全球战，它是一家来自英国的面向全球的数字货币交易所，该交易所是在UKEX数字交易集团旗下的，通过全球的经纪商网络来向终端客户提供海外的银行账户开户、以及后续的数字资产交易等服务，这是一个非常具有创新性的金融服务矩

3、Walesex威尔士交易所是一个新时代的去中心化的数字货币交易平台，于2018年在英国成立，平台日交易量已达到3000万美金。Walesex交易所平台拥有三大主流业务：OTC交易通道、币币交易通道以及合约交易服务。截止2019年12月,已经上线了20多种主流数字货币(BTC,BCH,ETH,ETC,LTC,Dash,EOS,NEO,OMG,XEM等等)，并会紧跟区块链市场发展，上线更多可靠的数字货币和新兴币种。

XEM交易所是很多人头疼的问题，尤其是在理解和现实的冲突方面，MXC交易所官网也同样面临着相似的问题，关注我们，为您服务，是我们的荣幸！