“升级版”的Luna？案例剖析Ethena的USDe

### 简介

稳定币在加密行业中占据至关重要的地位。截至2024年7月25日，稳定币市值约为1650亿美元，占到整个加密货币市场2.417万亿美元近7%的份额。其中稳定币龙头Tether (USDT)目前是市值第三大的加密货币，仅次于比特币和以太坊。

本文将深入探讨稳定币，包括定义、分类及稳定币在数字货币领域中的重要角色。我们将通过对Ethena USDe的案例研究，探讨其运行机制、潜在风险以及USDe能否被视为“升级版”的Luna。

### 定义：什么是稳定币？

根据金融稳定委员会（Financial Stability Board）和国际清算银行（Bank for International Settlements）的定义，稳定币是“一种旨在相对于特定资产或一组资产保持稳定价值的加密货币”（"a cryptocurrency that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets"）。通常情况下，稳定币是与以美元为代表的法定货币挂钩。

### 动机：我们为什么需要稳定币？

市场不乏对稳定币的讨论。但首要问题是：我们为什么需要稳定币？

首先，在Web3大规模应用的背景下，数字资产比传统资产提供了更便捷的可交易性。稳定币作为价值稳定的交换媒介促进日常交易，同时也能够实现快速且低成本的跨境支付，避免了传统银行系统的处理延迟和高额费用。

其次，稳定币有助于减少价值波动带来的影响。由于BTC或ETH等主流加密货币具有与生俱来的价值波动性，它们并不适合作为稳定币。在市场波动时期，稳定币提供了特有的价值稳定性，充当了价值保全的避风港。

### 分类：稳定币如何保持“稳定”？

抵押稳定币完全由其他资产支持，确保其价值由其他形式的抵押物支撑。假设这些抵押物管理得当并具有可行的赎回机制，由于潜在的套利机会，这类稳定币的价值不太可能跌破其抵押资产的价值。典型的抵押稳定币包括：

算法稳定币通过算法确保抵押物的安全性，或调整市场流通（供需状态）来保持稳定。典型的方法包括：

注意

值得注意的是，这些分类方法并不是互斥的。稳定币可以同时实施多种机制来维持稳定。例如，DAI既由加密货币抵押物支持，同时也采用算法调整（即清算）。这种策略的组合可以利用多种机制的优势来减轻潜在的弱点，从而增强稳定币的总体稳定性和可靠性。

### 安全风险及解决方案

抵押物透明度

对于法定货币或商品抵押的稳定币，用户可能会怀疑抵押物是否安全保存并随时可供赎回。许多稳定币通过将抵押物托管在第三方托管人处（如银行）、进行定期审计以及发布储备证明报告来解决这一问题。这些措施可以增强抵押管理的透明度，从而在一定程度上减轻公众的怀疑。

抵押物价值波动

对于加密货币抵押稳定币，其基础资产相较于法定货币或商品的波动性更大，抵押物价值的大幅波动可能导致意外的抵押物价值缺口。为了解决这一问题，许多稳定币实施超额抵押和清算机制，以减轻抵押物价值波动造成的潜在负面影响。超额抵押在某种程度上确保了在市场波动期间，抵押物的价值能够保持在安全范围内，因为加密货币储备的初始价值超过了发行的稳定币的价值；清算机制则允许其他用户清算不足以充分抵押的稳定币，从而维持稳定币价值稳定。

智能合约漏洞

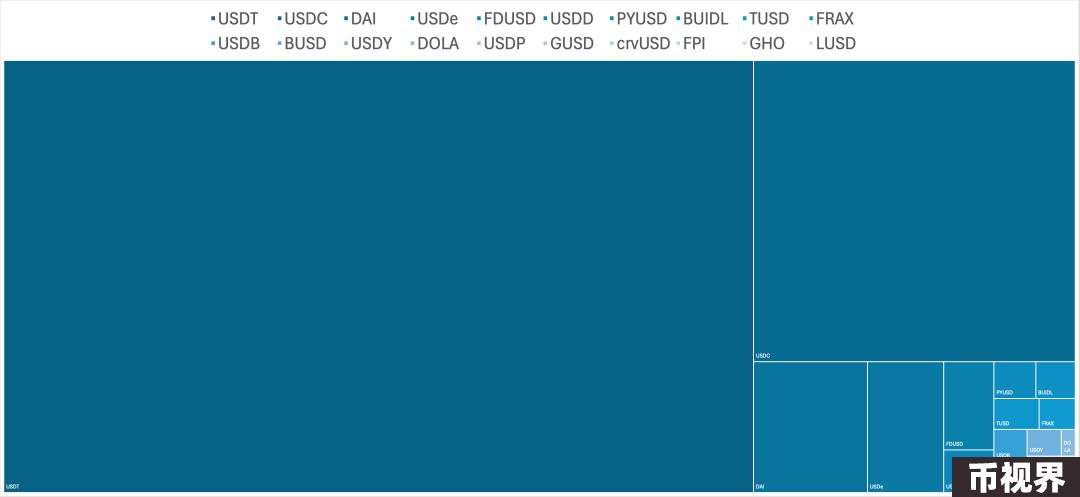
稳定币，尤其是算法稳定币，依赖复杂的智能合约来实现其稳定机制。然而，这些智能合约也可能引入代码层面的新风险，例如重入攻击、逻辑错误或治理漏洞等。因此，严格的安全审计和持续的安全监控对于确保这些协议的安全性和可靠性至关重要。

市场波动

稳定币及与稳定币相关代币的急剧波动（如在短时间内的突然崩盘）会削弱公众对稳定币的信任，并影响稳定币价值稳定。在快速变化的市场环境下（如黑天鹅事件期间），原先设计的稳定机制可能无法迅速响应和调整，从而导致大幅度的价格偏离。在高需求或恐慌情境下，自动做市商（AMM）设计也可能导致交易所流动性池中的稳定币流动性短缺，进一步加剧价格波动。流动性不足的市场尤其容易受到操纵。此外，稳定币依赖预言机来确定外部价格（如美元或以太币），不正确的预言机数据可能导致稳定币定价错误，从而产生一个新的攻击面。

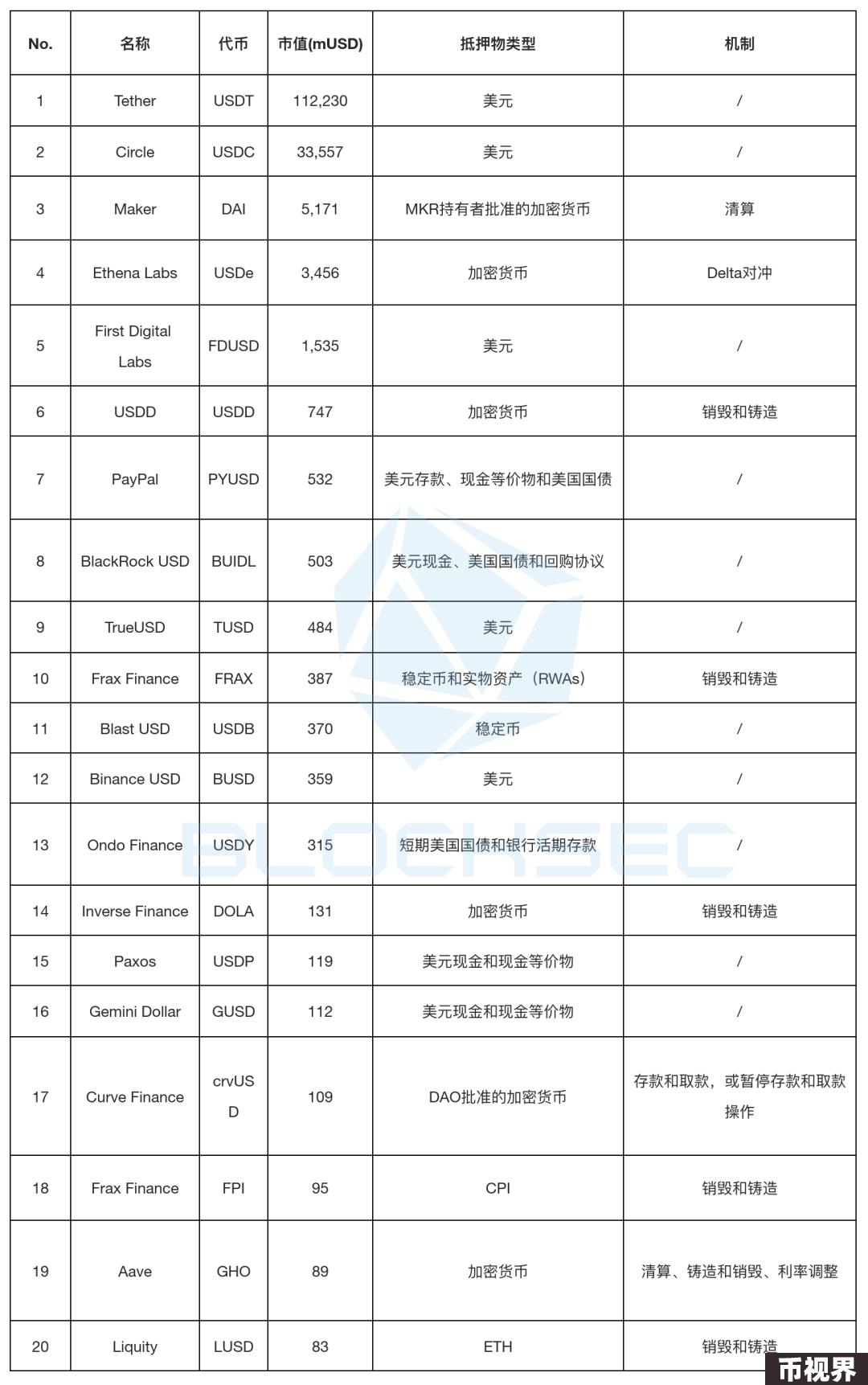
### 主流稳定币

我们从DefiLlama中选择了前20大稳定币，这些稳定币市值总和占稳定币总市值的99%以上（截至2024年7月数据），如以下图所示。



这些稳定币的市值表现出高度集中，其中前5大稳定币（即USDT、USDC、DAI、USDe和FDUSD）占总市值的96%，前20大稳定币占总市值的99%。这表明市场由少数关键玩家主导，与帕累托法则（Pareto Principle）一致。

在前20大稳定币中，所有稳定币都由某些资产（如美元、美国国债或其他加密货币）抵押。此外，这些稳定币中有9个还结合了算法稳定机制，以调整流通供应或确保抵押物安全。



这一现象表明，尽管算法稳定币声称其稳定机制设计优秀，但用户对完全抵押的稳定币，特别是由法定货币支持的稳定币，表现出明显的偏好。正如Frax创始人Sam Kazemian所说：“如果你想建立一个非常大的稳定币项目，你会希望它随着规模的扩大变得更安全，而不是相反；当人们使用稳定币时，人们也会希望它变得更安全。”（"If you want to create a very large stablecoin, you want to become safer as you get bigger, not the other way around; as people use money, you want it to be safer."）

### 案例研究：Ethena Labs - USDe

在过去的一年中，由Ethena Labs发行的USDe获得了广泛关注。截至2024年7月，根据DefiLlama的数据，它已成为市值第四大的稳定币。本节将以USDe为案例研究，探讨其设计原理和潜在风险。

设计原理

USDe可以被认为是基于中心化交易所（CEX）的稳定币，其稳定机制目前主要依赖于CEX的运营稳定性。具体来说，USDe使用主流加密货币作为抵押，并采用“delta对冲”策略来维持抵押资产的稳定性。

那么什么是“delta对冲”呢？我们可以通过以下示例来说明。如果使用1 ETH来铸造USDe，那么我们说稳定币暴露于“1 ETH的正delta”，这意味着稳定币价值对ETH现货市场价格完全敏感。理想情况下，稳定币的目标是使得这一敏感性最小化，即尽量保证“delta为0”，以更大程度上确保稳定性。为实现这一目标，Ethena通过在一个名义头寸为1 ETH的永续合约上“做空”来进行delta对冲。这一策略中和了抵押物价值对市场波动的暴露。因此，无论ETH市场价格如何变化，抵押物的价值始终保持稳定。

另外，USDe的收益包括两个主要部分：质押收益，即来自ETH质押的原生收益；以及来自delta对冲衍生品头寸的收益。第二部分又进一步分为两部分：1) 来自资金费率的收益，即CEX上多头和空头头寸之间的定期支付；以及 2) 来自基差利差的收益，即现货市场与期货合约之间的价格差异所产生的利润。根据Ethena的历史数据分析，这种收益组合在市场低迷时期（如Terra事件和FTX事件）仍保持正值。

安全风险

主要的安全问题源于对CEX的依赖以进行delta对冲以及场外结算的托管方式。我们将这一问题称为中心化风险。这种依赖关系创造了一个脆弱点，即一旦这些交易所无法正常运行——无论是由于运营问题还是银行挤兑——都可能危及稳定币的稳定性。尽管抵押物分布在多个交易所，但超过90%的抵押物仍然集中在三个主要交易所：Binance、OKX和Bybit。

此外，市场风险也不容忽视。USDe的收益机制可能会遇到持续为负的资金费率，这可能导致Ethena的收益设计中的某些部分变为负值。尽管历史数据表明这种负收益时期相对较短（少于两周），但必须考虑未来可能出现的长期不利条件。因此，应该始终准备充足的对策，例如充足的储备资金，以应对这一困难时期。

### 结语

总而言之，稳定币在市场波动中提供稳定性并促进交易，在加密货币生态系统中起着至关重要的作用。稳定币的分类从法定货币抵押到像Ethena USDe这样的算法机制，再到像Ondo这样的RWA支持的稳定币，满足了加密社区的各种需求，但也存在诸如抵押物透明度、价值波动和智能合约漏洞等风险。

随着Ethena Labs继续改进和创新USDe，一个关键问题浮现：USDe能否在市场波动中保持稳定，并避免遭遇类似Luna的崩盘？USDe的底层资产和经济模型设计与Luna还是大相径庭的，但也应该密切关注USDe能否真正保持稳定，并有可能在竞争激烈的稳定币领域中占据领先地位。

稳定币庞大的市值和影响力让我们不得不关注其安全风险，持续的安全审计和安全监控对于维持市场的稳定和信任不可或缺。