区块链技术——USDT分析

摘要：区块链技术快速发展，加密货币也成为引人注目的话题。本文对目前最大的稳定币USDT展开分析，从USDT项目特点和实现形式切入，详细介绍USDT的代币技术和共识机制，并从金融大环境，竞争者，法律等多方面分析USDT目前的形势并给出投资分析，供广大读者思考。

关键词：USDT；区块链；分布式记账

1 经济模型分析

1.1 项目、创始人及团队简介

1.1.1项目简介

USDT是Tether公司推出的基于稳定价值货币美元（USD）的代币TetherUSD，它是一种将加密货币与法定货币美元挂钩的数字货币，是一种保存在外汇储备账户、获得法定货币支持的虚拟货币。1USDT=1美元，用户可以随时使用USDT与USD进行1:1兑换。Tether公司严格遵守1:1的准备金保证，即每发行1个USDT 代币，其银行账户都会有1美元的资金保障。用户可以在 Tether 平台进行资金查询，以保障透明度。

1.1.2 USDT的特点

* 稳定：Tether将现金转换成数字货币，锚定或将美元、欧元和日元等国家货币的价格挂钩，从而不受大多数加密货币的波动影响。
* 透明：Tether的法定储备账户会定期接受审核，以确认其储备账户能够实际支持Tethers(USDT)流通中的价值。余额定期更新，可随时公开访问。所有Tether交易都记录在公共区块链上。
* 区块链技术：Tether平台建立在区块链技术的基础之上，利用它们提供的安全性和透明性。
* 广泛的集成：在Bitfinex, shapUNK, GoCoin和其他交易所使用tethers。
* 安全：Tether的区块链技术在满足国际合规标准和法规的同时，提供了世界级的安全保障。

1.1.3 USDT主要风险

* 公司发行无没有法律保障：USDT由 Tether 公司发行，自带中心化属性，尽管bitfinex是当前世界最大的虚拟货币市场交易所，但是也有倒闭的风险。
* 超发频繁：短短几年间，USDT超发上百次，系列产品的数量也大大提升。
* 被盗事件，无法保障安全：曾USDT被盗上千万美金，各大交易所纷纷暂停USDT充值，且事后无人为此事负责。

1.1.4创始人及团队简介

Directive team：

Chief Executive Officer： JL Van de Velde

Chief Financial Officer： Giancarlo Devasini

General Counsel: Stuart Hoegner

Chief Technology Officer: Paolo Ardoino

Chief Compliance Officer: Leonardo Real

Chief Operating Officer: Claudia Lagorio

1.2 项目的目标及实现形式

项目意在建立一个全球性的可分配网络，使得用户能够及时，安全的共享信息。希望通过计算和数字分享并使用互联网加密，区块链技术使得人与人之间的资产交换，交易等都能够用统一的方式及时，安全，低价的完成。省去第三方消去人工，提供更高效的市场是其主要思想，与共享经济的理念结合。同时也希望通过代码，保证整个交易的安全性与有效性。

USDT期望利用区块链技术，成为一个连接现实世界货币与虚拟货币的桥梁，促进世界经济的交流与沟通，加速了世界各国之间的经济交流，同时能够在数字货币下跌的行情中成为一个避险的利器。虚拟货币的普及也将改变商业变现的方式，无论人们身在何处，虚拟货币只需要任意介入一台电脑管理，就可在任何地方挖掘，购买，出售。去中心化的特点，也使得其交易费用降低。

1.3 为什么需要分布式记账

1.3.1 分布式记账的概念

分布式记账技术是分布在多个节点或计算设备上可共享，复制，同步的数据库。每个节点都可以复制并保存一个分类帐，且每个节点都可以进行独立更新，构建和记录，且不需要任何中央机构维护。为确保交易的公正性，交易者需要通过特殊节点进行投票，若利益不相关的若干节点达成共识，及说明其符合大多数人的意见，共识也就随之达成共识一旦达成，分布式分类账就会自行更新，分类账的最新的商定版本将分别保存在每个节点上。分布式记账技术解决了信任成本问题，对于银行、政府、公正处等依赖没有那么大，数据全在节点上。同时，也解决了消费者权益、财务诚信和交易速度的问题。

1.3.2 分布式记账的演变形式

如下图所示，电子记账实际是由我们的实物记账演变而来，利用区块链技术以及加密演变技术而达成电子记账的效果，确保交易的真实性和稳定性。

图一 分布式记账方法

1.3.3 分布式记账的优势

分布式账本记录参与者之间的交易，省去了调解不同账本的时间和开支，大大降低了信任成本。且账本可以存储任意金融、法律定义上的、实体的或是电子的资产。

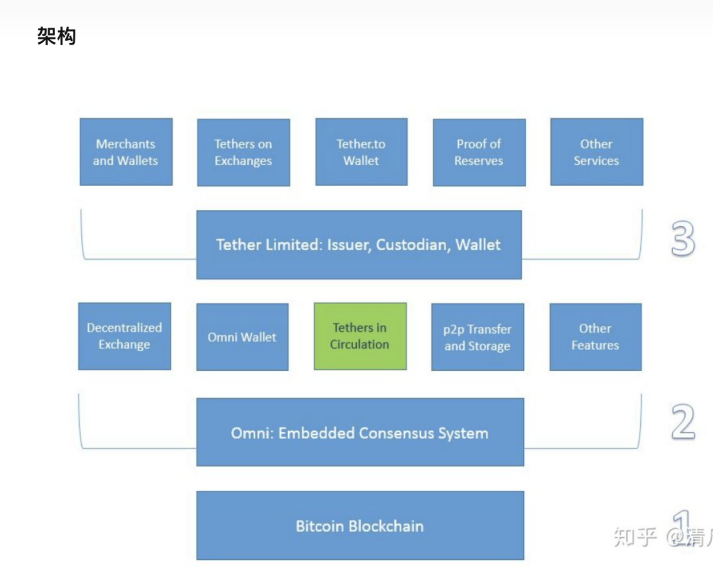
NGK账本基于密码学，通过公私钥及签名的使用访问账本，确保交易的安全进行。根据共识的规则，账本的记录可以由多个参与者共同进行更新。一旦区块发生任何篡改，在几分钟甚至是几秒内都会在所有的副本中反映出来，并通过广播机制被所有参与者了解。NGK分布式账本技术是颠覆性的创新，通过算法，密码学，省去中央机构提高效率，使得它有机会改变公共和私营服务的实现方式，有更广泛的应用场景，提升生产效率。

1.4 代币机制

1.4.1 USDT发展轨迹

USDT是由比特币的爱好者以及那些致力于促进数字化背景下的法币流通的创业者所创建的。在2014年公司发布了区块链平台旨在利用更加现代的手段取代替传统金融系统，并将Realcoin改名为Tether 。2015年2月bitfinex宣布支持USDT交易，随后Poloniex交易所也支持USDT。以太币强势崛起在一定程度上增加了USDT的交易量。USDT的发行和交易使用的是Omni协议，与初期的比特币一致，因此其交易确认等参数也相同。

1.4.2USDT的技术原理



图二 USDT架构

1.4.3 Omni协议层与USDT

USDT是基于 Omni 协议的数字虚拟货币，因而Omni对于USDT的重要性也是不言而喻。Omni是基于比特币区块链网络的数字货币通信协议，将Exodus Address作为Omni协议数据链的起点，并建立在Bitcoin之上的软件层。在BTC锁定脚本中，OP\_Return具有备注，认定功能并确保其不会被节点解析出来的，确保交易的信息在全世界唯一存在。比特币具有脚本功能也帮助Omni 协议在比特

币区块中嵌入 Omni 协议的数据，并通过 OP\_RETURN 操作码区分。

 图三 Omni与USDT关系

USDT 交易采用的是 Omni 协议的“简单发送”格式，如下：

 图四 Omni协议简单发送形式

由上图可知，我们只需要明确交易版本，交易类型，货币标识符，转账金额即可发送USDT交易，其分别由2，4，4，8个字符构成，可有分别的简单发送值。

2.技术模型分析

2.1 共识机制

区块链的共识机制可分为四大类：工作量证明机制、权益证明机制、股份授权证明机制和Pool验证池。

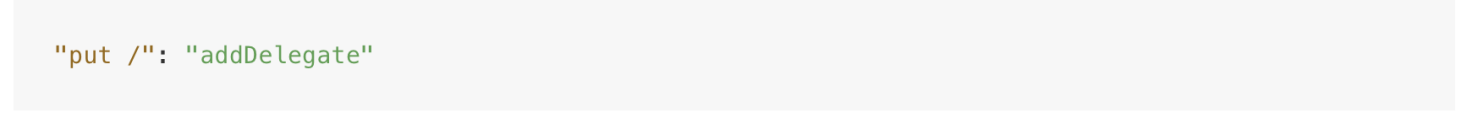
* 工作量证明机制（PoW）

由于比特币本质上是一个去中心化的账本，不存在中间机构，因而需要利用区块链技术的算法对一个特定值进行计算工作。矿工们在挖一个新的区块时，必须对SHA-256密码散列函数进行运算，区块中的随机散列值以一个或多个0开始。随着0数目的上升，找到这个解所需要的工作量将呈指数增长，因而求得正确的数值解以生成区块的能力是节点算力的具体表现。但是，基于工作量证明机制的挖矿行为还造成了大量的资源浪费，达成共识所需要的周期也较长，不适合商用。

* 权益证明机制（PoS）

基于PoW存在的问题，PoS机制试图解决存在大量资源浪费的问题。PoS根据矿工持有币的多少和时间，依据算法等比例地降低节点的挖矿难度，加快挖矿速度。这种共识机制可以缩短达成共识所需的时间，但本质上仍然需要网络中的节点进行挖矿运算。

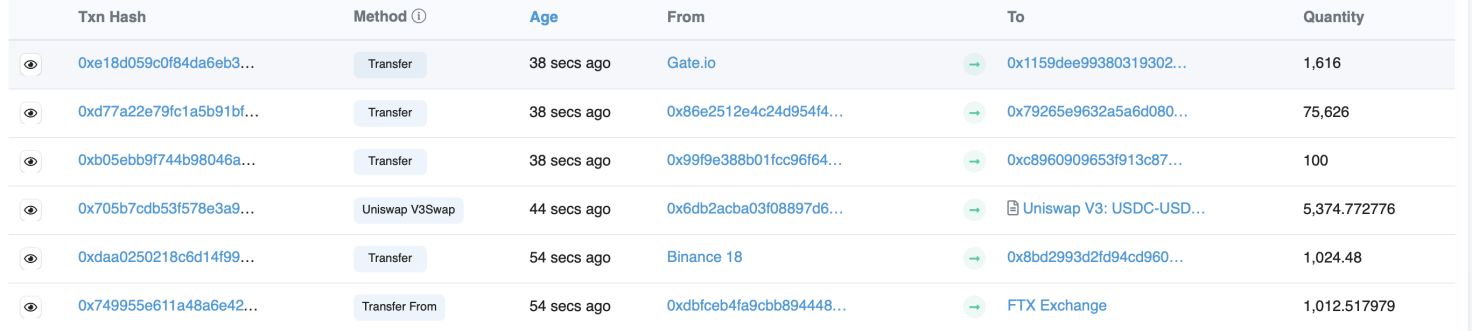
* 股份授权证明机制（DPoS）

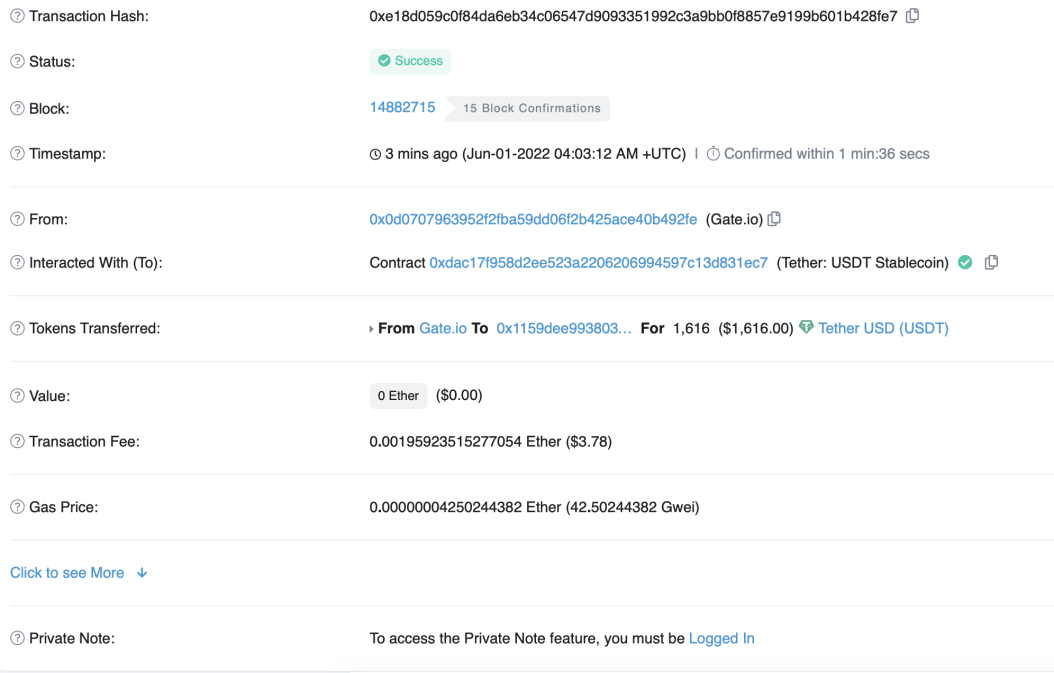
DPoS是建立在PoW机制和PoS机制存在问题上，通过选举抵消中心化所带来的负面效应，在DPoS的共识算法中，机制的正常运行依赖于受委托人。注册受委托人需要调用节点API，使用钱包，并接受投票；接下来机制会根据维持循环，调整受委托人，并根据区块链高度在某个时间点调整区块奖励；循环产生的新区块也会通过广播的方式通知大家。

图五 DPoS部分算法

* PooI验证池

Pool主要建立在Pasox、Raft基础之上，实现秒级共识验证，提升效率因而被广泛应用。

2.2交易界面



图六 USDT交易界面

从上图中我们可以清楚的看到交易的哈希值，金额等，但是私钥需要私人账号登陆，保证交易的安全。

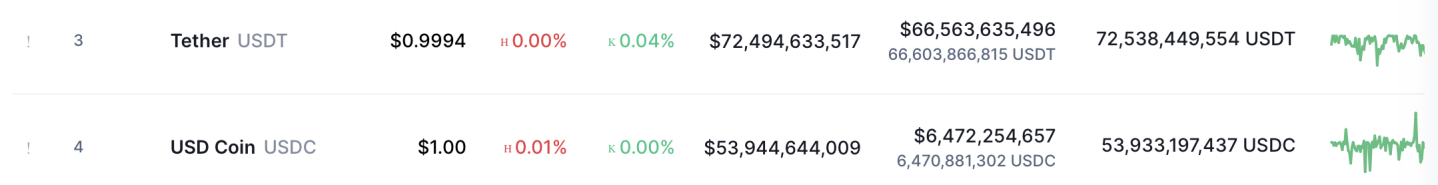
3. 项目未来

3.1 项目投资分析

3.1.1 USDT的重要意义

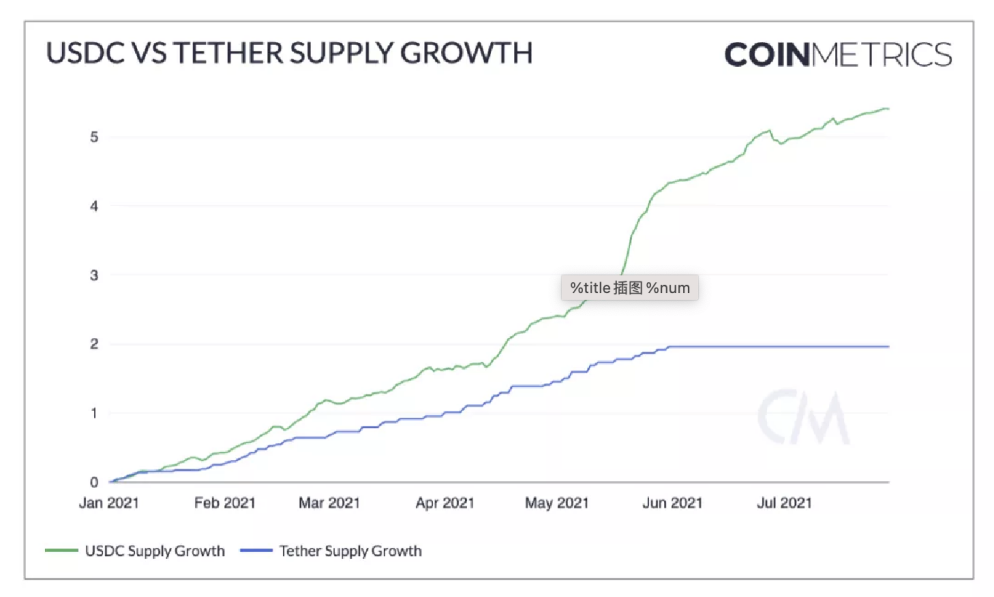
USDT作为最先出现的稳定币之一，打通了数字货币与法币的链接通道，打破了中心化世界对去中心化世界的一道枷锁，usdt是用算法技术代替中央机构的尝试者，开拓者，也是最有可能实现虚拟货币普及化的公司之一，可以说是责任重大。但我们也不可否认在USDT之后，出现了其他稳定币对其造成冲击。

3.1.2其他货币的冲击

以下将USDT与USDC进行比较：

图七 USDT与USDC市值比较

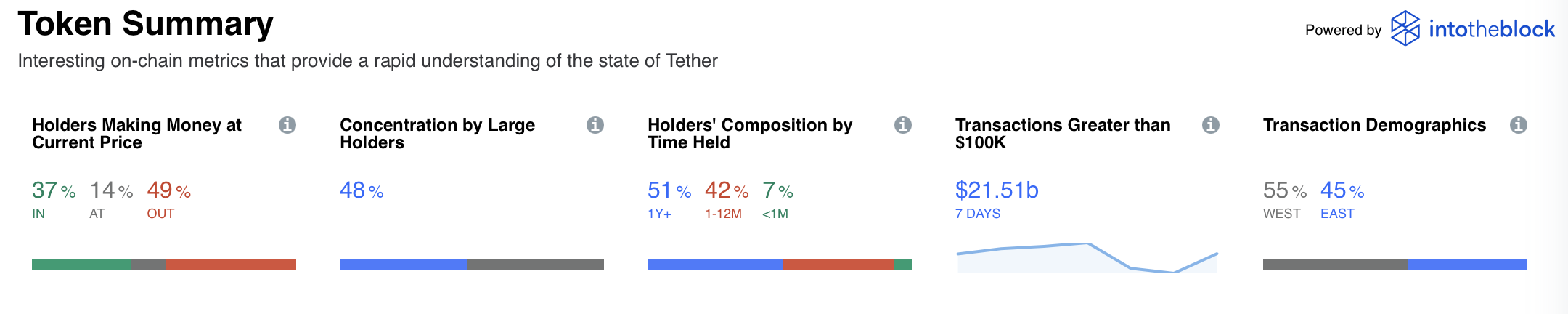
目前USDT和USDC分列虚拟货币榜单第三第四位，市值分别是700多亿和500多亿，两者占稳定币总市值的7层以上。2020年下半年，DeFi 大幅刺激了稳定币的需求，尤其是稳定币场内的收益组合可能性被挖掘，使得市场的需求量大大增加。而在经历了一年多的膨胀后，截至 2021 年底，全网稳定币总市值已突破 1600 亿美元，一年内稳定币市场体量增长逾千亿美元，在过去一年走完了过去若干年增量总和的 10 倍。

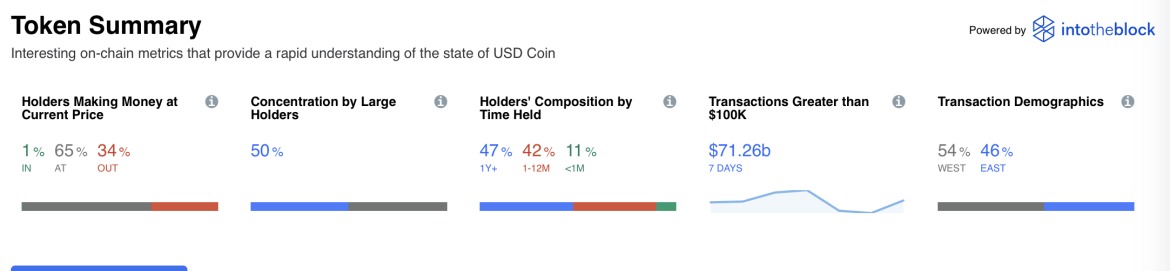


图八 USDC与Tether 的需求增长

中心化稳定币层面，由上图我们可以得出，USDC 的供应量增速比 USDT更为猛烈，而USDC的迅速扩张有力挑战了 USDT 的“霸主”地位。

深究其背后的原因，可以发现USDC背后的资本更为强大，由比特大陆、高盛集团、IDG、中金公司、光大和百度等投资的Circle公司发布，是一个完全抵押的美元稳定币，且有全球六大会计师事务所Grant Thornton也每月公开报告Circle发行的USDC的财务状况。发行公司Circle也是加密资产行业全球牌照数目最多的公司，拥有美元、英镑、欧元进出加密资产的合规通路。而目前USDT所存在的最大问题就是资金不透明，这也成为许多投资者的心头之患。





图九 Tether与USD Coin代币概况

以上两图分别是近期（2022年5月）Tether和USD Coin的Token summary情况：

由第四张图（Transactions Greater than $100K)可以很直观的发现USDC大金额交易量要远大于USDT，也可以看出USDC对于USDT的重大冲击。

3.1.3 加密货币大环境

截止5月13日，[比特币](https://link.zhihu.com/?target=https%3A//cn.investing.com/crypto/bitcoin/btc-usd)跌穿2.7万美元后艰难重回3万多美元，月度环比重挫23.79%，创2020年12月以来新低；[以太坊](https://link.zhihu.com/?target=https%3A//cn.investing.com/crypto/ethereum/eth-usd)月度环比重挫28.78%，[BNB](https://link.zhihu.com/?target=https%3A//cn.investing.com/crypto/bnb/bnb-usd)月度下跌24.85%，[狗狗币](https://link.zhihu.com/?target=https%3A//cn.investing.com/crypto/dogecoin/doge-usd)下跌33.28%。加密货币的全线加速下降必然有其原因：

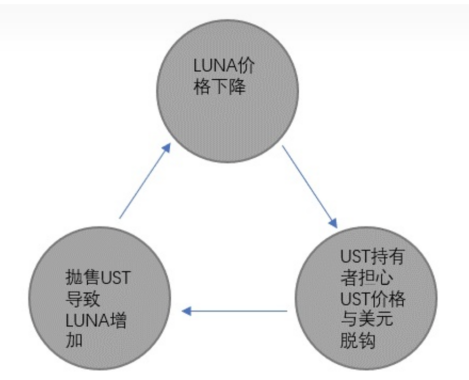
1.美联储加息缩表导致加密资产兑现为美元并大量流出到其他领域避险

加密货币火热的市场与美联储大放水有着密不可分的关系，很多投资者都拿到了政府纾困金，更有大量投资者将加密货币视为对抗美元通胀的避险工具，美联储加息毫无疑问大大降低了加密货币投资者的信心。

2.LUNA 暴跌99%至1美分以下，Terra区块链正式宣布暂停

稳定币UST与美元脱钩遭挤兑。我们知道UST与美元价格为1:1，当UST的价格低于1美元就意味着交易者可以将其从流通中永久移除，生成价值1美元的Luna加密货币。通过减少UST的供应，提高它的价格。相反，如果UST的价格超过1美元，交易员可以选择烧掉Luna并创造新的UST。这种设计期望

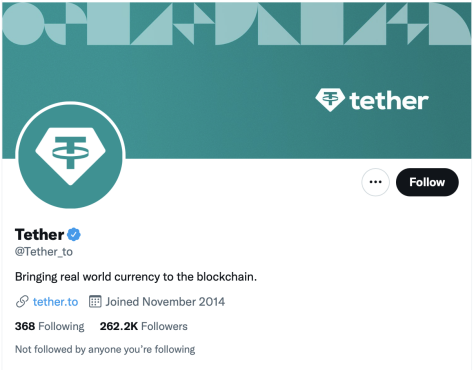
通过“烧掉”UST减少供给，达到市场供需平衡，使UST稳定在1美元，但当交易、投资者对LUNA和US缺乏信心时，更多的LUNA铸造会促使他们抛售更多UST，而随着UST供给增大需求减少，更多LUNA被铸造，从而使这两种稳定币的价格陷入恶性循环。

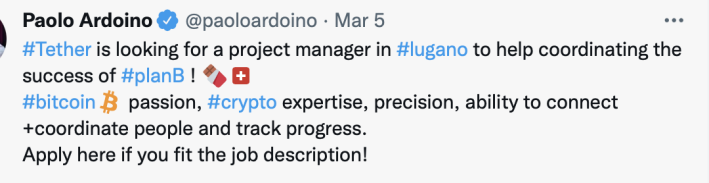


图十 稳定币关系

3.信心缺失

加密货币的部分价值来自人们对它的信任，而稳定币的波动影响了投资者的信心，因而市场也非常容易受到情绪及政策影响。

3.1.4现有社区及应用评价

以下是在Twitter的社区当中截取了部分近期评价：

图十一 Twitter社区用户评价

社区中大部分评价都是正面积极的，由此可以看出目前市场当中仍有许多看好USDT的投资者，他们对于加密货币依旧有着十足的信心，期待它越变越好。

3.1.5 法律分析

3.1.5.1USDT 的法律属性

（1）USDT是否为法定货币

《中华人民共和国中国人民银行法修订草案征求意见稿》第十九条规定，“人民币包括实物形式和数字形式。”因此，由中国人民银行发行的数字形式的人民币也是法定货币以及外国法定货币发行机构发行的数字形式的货币，能够从法律上被认定为货币。但USDT无国家信用支撑也无中央调节机制，并且缺失国家相关监管政策予以监管。因此，USDT并不是由外国法定货币发行机构发行的法定货币的数字形式，不属于货币。

（2）USDT是否为美元代币票券

根据2000年7月5日中国人民银行办公厅《关于对购物卡性质认定的函》（银办函）、《中国人民银行法》第十九条、《现金管理暂行条例》和《国务院关于禁止印制、发售、购买和使用各种代币购物券的通知》的相关规定，认定为“代币票券”一般应具备以下几个要素：

1.具备一定数量的金额；

2.在时间上具有一定的跨度性；

3.在一定范围内使用和流通，可购买不特定商品；

4.不记名、不挂失。

发行机构承诺USDT与美元一比一锚定，具有一定的金额；USDT的使用并无一定的期限要求；USDT可以在一定范围内使用和流通，在可以购买不特定的数字货币；且不记名不挂失。但目前没有相关的制度和条件来保障USDT价值的稳定。因此USDT并不能作为美元代币票券而存在。

（3）USDT是否属于美元外汇资产

根据《企业会计准则第19号外币折算》，外币是指企业记账本位币以外的货币。国内企业通常应选择人民币作为记账本位币。《企业会计准则规定》业务收支以人民币以外的货币为主的企业，可以按照本准则第五条规定选定其中一种货币为记账本位币。但是，编报的财务报表应当折算为人民币。企业对于发生的外币交易，应当将外币金额折算为记账本位币金额。可以得知，外币即以人民币以外的其他货币计价的货币。

根据《中华人民共和国外汇管理条例》中外汇是指下列以外币表示的可以用作国际清偿的支付手段和资产：

（一）外币现钞，包括纸币、铸币；

（二）外币支付凭证或者支付工具，包括票据、银行存款凭证、银行卡等；

（三）外币有价证券，包括债券、股票等；

（四）SDR；

（五）其他外汇资产。

目前USDT仅局限于数字货币领域，无法在其他金融领域进行直接兑换、在其他国家也不能无限制作为支付手段使用。所以USDT不是境外批准的金融产品，其与传统规范意义的外汇存在很大差别，不属于外汇资产。

3.1.5.2 USDT 交易过程中的其他法律问题

（1）是否涉嫌非法经营罪

根据《刑法》第二百二十五条的规定，非法经营罪是指违反国家规定，有下列非法经营行为之一的犯罪：

（一）未经许可经营法律、行政法规规定的专营、专卖物品或其他限制买卖的物品的；

（二）买卖进出口许可证、进出口原产地证明以及其他法律、行政法规规定的经营许可证或者批准文件的；

（三）未经国家有关主管部门批准，非法经营证券、期货或者保险业务的，或者非法从事资金结算业务的；

（四）从事其他非法经营活动，扰乱市场秩序，情节严重的行为。

目前国内对于USDT交易商交易虚拟货币等并无特许牌照或专营牌照的具体法律规定，也没有USDT交易商相关追究刑事责任的规定和相关刑事司法解释，因此单纯买卖USDT这一行为而言，一般不会被认定为非法经营罪。

（2）是否涉嫌非法买卖外汇的法律风险

非法买卖外汇罪是指我国的机构、单位或个人，外国驻华机构及其工作人员，其他来华的外国人，违反国家关于外汇买卖的有关法律规定，以牟取非法利益为目的，非法买卖或变相买卖外汇，情节严重的行为。同时，根据最高人民法院有关规定，非法买卖外汇20万美元以上，违法所得5万元人民币以上，即构成非法买卖外汇罪。

由于USDT无法直接出售给指定银行，也不存在外汇使用额度，所以买卖USDT不属于买卖外汇，因此将USDT视为非法买卖外汇的行为不太可能。

3.1.5.3 其他法律风险

1. 涉嫌反洗钱、反恐怖融资。

2.涉嫌违反资本管制、外汇管制。

3.涉嫌侵犯财产类犯罪，破坏金融管理秩序罪。

3.3 项目投资分析

3.2部分分析了如今金融领域大环境，将USDT与其最大竞争对手USDC的进行分析比较，并结合Tether社区用户的评价看法和法律分析，我们可以发现投资USDT在目前阶段还是存在一定的风险。虽说USDT仍然稳居稳定币第一位，但国家相关政策和竞争者的冲击还是相当之大，目前许多国家也没有非常完善的法律体系去保证相关投资者的安全。因而我认为，投资USDT还是要持谨慎的态度。

参考文献：

<https://www.jianshu.com/p/df68179a72e7>

[https://baike.baidu.com/item/共识机制/20234683?fr=aladdin](https://baike.baidu.com/item/%E5%85%B1%E8%AF%86%E6%9C%BA%E5%88%B6/20234683?fr=aladdin)

<https://zhuanlan.zhihu.com/p/432619874>

<https://coinmarketcap.com/currencies/tether/>

<https://www.qkl456.com/221468.html>

<https://zhuanlan.zhihu.com/p/37073462>

<https://blog.csdn.net/xq723310/article/details/82684595>

<https://zhuanlan.zhihu.com/p/159198681>

<https://blog.csdn.net/xq723310/article/details/82684595>

<https://zhuanlan.zhihu.com/p/31588809>

<https://zhuanlan.zhihu.com/p/477001893>

<https://zhuanlan.zhihu.com/p/514146971>

<https://www.20on.com/75675.html>

<https://www.qkl456.com/308947.html>

<https://www.163.com/dy/article/FUF4QVIO0514832I.html>

<https://coinmarketcap.com/currencies/tether/>

<https://etherscan.io/tx/0xe18d059c0f84da6eb34c06547d9093351992c3a9bb0f8857e9199b601b428fe7>