基于区块链的货币市场中套利和做市的风险与机遇。第一部分：风险

Vittorio Astarita
vittorio.astarita@unical.it

https://www.researchgate.net/profile/Vittorio-Astarita

意大利卡拉布里亚大学

摘要
本研究对基于区块链的货币市场中的高频交易进行了实用性介绍。这类市场具有一些有别于股票市场的特定特征，例如交易所数量众多（包括中心化和去中心化交易所）、资金在不同交易所之间转移相对简单，以及大量新兴货币的流动性极低。本研究分析了此类交易操作特有的潜在风险、可能的机遇以及最常用的算法，并提供了相关信息，可供有意通过提供（并承担风险）流动性参与这些市场的从业者参考。

1. 引言

基于区块链的加密货币是交易活动的基础，证券和大宗商品全年无休、每天24小时进行交易。此类持续不断的市场活动发生在600多家中心化交易所和400家去中心化交易所（据CoinGecko，2023年）。截至2023年4月，基于区块链的货币总市值约为1.23万亿美元（CoinGecko，2023年）。占主导地位的加密货币比特币被美国证券交易委员会视为大宗商品，其总市值约为5420亿美元（维基百科，2023年a）。

每日交易额在500亿至1000亿美元之间。不过，这一数字可能并不完全可靠，因为许多交易所或发行方会进行刷量交易，人为夸大交易量。刷量交易是股票市场上的一种违规行为，指同一实体通过同时买入和卖出相同的金融工具来制造交易。这会营造出市场活跃的假象，却不会带来市场风险，也不会改变该实体的市场头寸（维基百科，2023b）。

这个市场存在的问题之一是缺乏监管规定。中心化交易所（CEX）在全球各地设有本地运营，有时是为了规避特定的监管规定；而去中心化交易所（DEX）据称甚至没有明确的所在地。根据 CoinGecko 的数据，截至2023年4月，交易所交易的基于区块链的金融工具数量惊人：中心化交易所和去中心化交易所平台上交易的“币”约有 10800 种（CoinGecko，2023年）。

2. 交易者面临的风险与机遇

交易者可以在 1000 多家交易所交易 10000 多种金融工具（CoinGecko，2023年）。每家交易所也会为每种金融工具列出不同的交易对，由此形成数量惊人的可交易市场。不同平台上交易的不同交易对之间自然会出现价格差异（尤其是在波动性较高时，或者更简单地说，价格随时间快速变化时），从而为套利和做市等交易实践创造机会。交易者可以运用下一节介绍的技巧，通过提供流动性获利。此外，随着比特币价格不断上涨，整个市场似乎也在持续扩张，因此整个环境对交易者而言似乎十分有利。不过，这个市场竞争激烈，而且充斥着不诚信的参与者。

并且随着比特币价格不断上涨，市场似乎一直在扩张，因此整个环境对交易者而言似乎十分有利。不过，这个市场竞争激烈，而且充斥着不诚信的参与者。

平　均加密货币交易者面临着若干潜在陷阱。主要风险包括：

1）在不了解底层经济细节和技术层面的情况下投资并持有基于区块链的货币的风险（Investopedia，2023年a）。2）在自主管理钱包中处理金融工具时操作不当的风险（Cointelegraph，2023年）。3）在区块链上转移资金时使用错误参数，可能导致转移的资金损失的风险（CoinDesk，2023年）。4）将资金留在去中心化交易所（DEX）和中心化交易所（CEX）的风险；这些交易所可能遭到黑客攻击或被欺诈性经营，导致资金永久损失。5）与交易操作相关的风险。

通过接受适当的计算机科学教育并了解基于区块链的货币如何运作，可以降低前三种风险，但第四种和第五种风险无法完全避免。下一节将讨论如何降低第五种风险，因为它与所采用的交易策略有关。

2.1 在不了解所选金融工具的经济细节和技术层面的情况下投资并持有基于区块链的货币。

在未全面了解经济细节和技术层面的情况下投资并持有基于区块链的货币，会使交易者面临重大风险。这些风险包括持有价格可能突然意外下跌的金融工具。

2.1.1 基于区块链的货币风险

一些基于区块链的货币看似去中心化，实际上却由单一实体控制；这些实体自初始发行以来便掌握发行权或持有大部分资金。在第一种情况下，控制实体可以通过制造不受欢迎的通货膨胀，稀释金融工具的供应量。这些实体有多种手段实施此类欺诈，包括更改发行规则或利用现有监管规定。例如，一些基于区块链的货币没有设定代币生成数量上限，或者其代币发行和通胀监管规则含糊不清，结果对较小的投资者不利（Nakamoto，2008年）。

2.1.2 所选金融工具应具备的技术细节

Th以下货币特征有助于保护投资者免受潜在损失　　es:

-有限供应：供应量无限的货币容易受到通货膨胀的影响。通货膨胀会使货币贬值，在短时间内降低其价值。相比之下，明确且稳固的供应上限可确保货币不会贬值（Nakamoto，2008年）。

去中心化治理和交易验证流程：中心化治理和／或中心化区块链账本可能使货币受到供应规则变更、任意引入新规则或潜在欺诈的影响，从而损害较小投资者的利益（Mazieres，2015年）。

-明确的货币政策：　　透明且易于理解的货币政策有助于保护人们

免受不透明政策所带来风险的影响，因为这类政策可能会随意施加可变规则。由数学算法确立的固定规则能够提供一定保护，但无法彻底解决这一问题。例如，Terra Luna 系统就体现了这一问题：UST 稳定币通过算法与 LUNA 币挂钩以维持稳定，但最终还是失去了与美元价值的挂钩，因为 UST 的总价值已不再由 LUNA 支撑。随着 UST 稳定币开始脱钩，持有者纷纷抛售，逐渐失去对该系统的信心。这导致套利者利用原本旨在让 UST 维持美元挂钩的算法，在交易所公开市场以低于美元价值的折扣买入 UST，再将其转入 Terra Station（Kwon & Shin，2018）。在 Terra Station 上，可以按与美元等值的价格将 UST 兑换为 LUNA 币。LUNA 币转回交易所后，则按市场价格出售。这种套利行为持续了几天，使 LUNA 和 UST 的价值都接近于零。Terra-Luna 系统基于算法规则，而这些规则在特定条件下可能不稳定，从而形成了一个未曾预见的自我强化贬值循环，即使是经验丰富的投资者也未能预见这一点（Kwon & Shin，2018）。算法规则和数学可以为投资者提供支持，但无法保证投资没有风险。

-开放且无需许可： 当货币由自行任命的政策制定者管理时，资金可能面临无法使用的风险。可靠的货币应始终可用且可互换，任何人无论身处何地，都应能够使用它（Nakamoto，2008年）。应避免使用那些控制方能够施加影响并限制访问权限、限制使用（甚至撤销和/或阻止交易）的货币，因为较小的投资者迟早可能因此蒙受损失。

2.2 在自主管理钱包中持有金融工具的违规操作风险。

推出自主管理钱包的初衷，是让用户摆脱代为托管投资者资金的中介机构。此项创新背后的理由是，交易所企业、银行和投资公司等中介机构可能会挪用或丢失资金；正如这些市场中屡次发生的那样，它们也可能遭到黑客攻击（或谎称遭到黑客攻击），从而无法再访问客户资金。使用专用软件或纸钱包进行自主托管，可以消除下一节讨论的风险。遗憾的是，情况并非总是如此，因为自主托管要求用户了解这些数字工具的运作方式，而许多用户很难掌握这种知识。

自行管理托管的主要风险包括永久丢失秘密支出密钥，以及因盗窃或计算机黑客攻击而丢失支出密钥。存储在联网计算机上的密钥，其安全性取决于计算机本身的安全性。在未联网设备上以实体形式保存密钥同样存在风险，因为冷存储设备可能会丢失或损坏。记忆关键词则会使用户面临忘记关键词的风险。

降低托管钱包的计算机遭受黑客攻击风险的最佳方法，是将密钥保存在冷存储中，并使用隔离设备为交易签名。然而，并非所有基于区块链的工具都适用这种做法，因为并非所有金融工具都配备易于使用、可用于离线签署交易的钱包软件。

2.3 在区块链上使用错误参数转移资金，导致转出的资金丢失。

在区块链上转移资金时使用错误参数，是一种常见的错误，可能是由于缺乏经验或一时分心造成的（Medium，2023年）。这种错误可能导致使用错误的目标地址，并造成资金永久损失（Chainalysis，2023年）。了解在区块链上转移资金的各个方面以及其中可能涉及的风险至关重要，这有助于避免此类错误。

转移资金时，使用正确的区块链传输协议至关重要。不同的区块链可能采用独特的协议和地址格式，因此很容易误将资金发送到不兼容的地址（Chainalysis，2023年）。. 例如，将比特币发送到以太坊地址，或反过来操作，都会导致资金损失。为避免这种情况，务必仔细核对目标地址，并确保其与相应的区块链协议匹配。

另一个可能导致资金损失的问题，是使用过时或不受支持的软件（Investopedia，2023b）。未更新至最新协议版本的钱包或交易所可能无法识别较新的地址格式，导致交易失败或资金损失（Investopedia，2023b）。务必确保所使用的软件已更新至最新版本，并与目标区块链网络兼容。

人为错误也可能在转账过程中造成重大资金损失（Chainalysis，2023）。输入错误、复制粘贴失误或看错地址，都可能导致资金被发送至错误或不存在的地址（Chainalysis，2023）。为尽量降低人为错误的风险，务必仔细核对输入的信息；如果可以，也可以使用二维码输入目标地址。

总之，在区块链上使用错误参数转账可能导致资金永久损失（Chainalysis，2023）。为避免这种情况，必须了解所用区块链协议的具体特性，确保使用最新且兼容的软件，并在输入目标地址时格外谨慎。遵循这些最佳实践，用户可以降低区块链转账过程中资金损失的风险。

2.4. 将资金留存在去中心化交易所和中心化交易所的风险：这些交易所可能遭受黑客攻击或被欺诈性管理，进而导致资金永久损失。

在去中心化交易所（DEX）和中心化交易所（CEX）交易数字资产存在固有风险，包括遭受黑客攻击、欺诈性管理以及资金永久损失的可能性。本文作者亲身经历了这些风险，曾卷入近期发生的 Polarity 去中心化交易所黑客攻击事件，可能因此损失约50万美元资金。这一事件鲜明地提醒我们，此类事件可能造成怎样的后果。尽管去中心化交易所平台声称能够免受此类风险，但许多平台仍设有中心化的入口和出口，因此可能面临与中心化交易所类似的威胁（Putz 和 Pernul，2019年）。

近期发生的多起去中心化交易所黑客攻击事件造成了重大资金损失，例如 Hedera（2023年3月9日）、Platypus（2023年2月17日）和 Orion 协议（2023年2月3日）[3]。据 ChainSec 统计，截至2023年3月，共发生132起去中心化金融漏洞攻击，损失资金总额约达42亿美元[4]。其中规模最大的一起是 Ronin 跨链桥黑客攻击，造成价值6.25亿美元的损失。

中心化交易所平台也曾遭受用户资金重大损失，其中臭名昭著的 Mt. Gox 在2014年2月遭遇黑客攻击是最早且最突出的案例之一（Decker和Wattenhofer，2014）。去中心化交易所和中心化交易所平台相关的风险，凸显了谨慎考虑资金存储和交易实践的重要性（Fantazzini和Calabrese，2021）。

为降低这些风险，投资者可以考虑使用硬件钱包或冷存储方案来存放长期投资，同时仅在交易所保留少量资金用于主动交易。此外，务必了解所使用交易所的安全功能和声誉，并启用双因素认证（2FA），以增加一层安全保障。

为了帮助个人了解加密货币市场，HedgewithCrypto 等资源提供实用指南、公正的评测，以及对各种加密货币交易所和平台的比较（Hedgewithcrypto，2023年）。HedgewithCrypto 于 2019年6月创立，已吸引全球超过 160 万名读者，旨在帮助他们轻松进入加密货币市场，无须担心被海量信息淹没或遭遇诈骗（Hedgewithcrypto，2023年）。

为了帮助人们在加密货币市场中顺利前行，HedgewithCrypto 等资源提供了实用指南、公正的评测，以及对各类加密货币交易所和平台的比较（Hedgewithcrypto，2023年）。HedgewithCrypto 于 2019年6月创立，全球读者已超过 160 万，旨在帮助他们轻松进入加密货币市场，不必担心不知所措或遭遇诈骗。据 HedgewithCrypto 称，自 2012 年以来，加密货币交易所累计被盗资金近 27.2 亿美元，近期发生的事件之一是 FTX 在一次黑客攻击中损失了 6 亿美元。此外，该网站指出，加密货币交易所遭黑客攻击造成的损失约占总市值（9040 亿美元）的 0.3%，且至少有 47 家比特币交易所因重大网络安全漏洞而损失资金。以下是相关名单：

Date	交易所 ge	黑客攻击原因	被盗金额（美元）
022, 11月12日	FTX	未经授权的交易	6亿美元
2022年，1月17日	Crypto.com	未知9700万美元	3400万美元
2021, 12月11日	AscendEX	获得热钱包的访问权限	8000万美元
2021, 12月5日	BitMart	获得热钱包的访问权限	1.5亿美元
2021年8月19日	Liquid	获取了热钱包的访问权限	9700万美元
2021年4月29日	Hotbit	获取热钱包访问权限	Nil
2020年12月23日	Livecoin	系统/服务器遭入侵	未知
2020, 12月21日	EXMO	获得热钱包访问权限	400万美元
2020, 12月1日	BTC Markets	内部员工失误	270,000 用户的个人隐私信息
2020年9月25日	KuCoin	数据泄露	2.75亿美元
2020年7月11日	Cashaa	恶意软件	310万美元
2020年6月29日	Balancer	协议漏洞	50万美元
2020年4月19日	Lendf.me	漏洞和重入攻击	2450万美元
2020年4月19日	Uniswap	漏洞和重入攻击	50万美元
2020年2月5日	Altsbit	获取了热钱包的访问权限	70,000 美元
2019, 12月19日	Youbit	获取了热钱包的访问权限	未知
2019年11月26日	Upbit	获得热钱包的访问权限	4900万美元
2019, 11月5日	Vindax	未知	50万美元
2019年7月11日	Bitpoint	系统/服务器遭入侵	3200万美元
2019年6月27日	Bitrue	系统/服务器遭入侵	450万美元
2019, 6月6日	Gatehub	未知	950万美元
2019年5月7日	币安	获得了访问热钱包的权限	4000万美元
2019, 3月29日	Bithumb	未知	2900万美元
2019年3月25日	Coinbene	疑似可信内部人员	4000万美元
2019年3月24日	DragonEX	未知	100万美元

2019年2月15日	Coinmama	数据泄露	450,000名用户的个人隐私信息
2019年2月1日	Cryptopia	未知	1600万美元
2019年1月26日	LocalBitcoins	虚假网站上的网络钓鱼数据	27,000美元
2018年10月28日	Maplechange	疑似可信内部人员	9700万美元
2018年9月14日	Zaif	获得热钱包的访问权限	6000万美元
2018, 6月18日	Bithumb	未知	3100万美元
2018, 6月10日	Coinrail	未知	4000万美元
2018年4月13日	CoinSecure	疑似可信内部人员	350万美元
2018年2月10日	Bitgrail	疑似可信内部人员	1.46亿美元
2018年1月27日	CoinCheck	未知	5.6亿美元
2017年12月20日	EtherDelta	服务器 DNS 遭入侵	140万美元
2017年7月5日	Bithumb		700万美元
2017年4月22日	Yapizon	获得了对热钱包的访问权限	530万美元
2016年8月2日	Bitfinex	未知	6.23亿美元
2016年5月9日	Gatecoin	获得热钱包的访问权限	214万美元
2016年4月7日至9日	Shapeshift	疑似可信内部人员	23万美元
2016年2月16日	BTER	未知	175万美元
2015年12月11日	Bitstamp	恶意软件	500万美元
2015年8月15日	BTER	疑似可信内部人员	165万美元
2014年7月13日	Mintpal	获得热钱包的访问权限	200万美元
2014, 3月4日	Poloniex	获得了热钱包的访问权限	5万美元
2014年2月	Mt. Gox	多种方法	4.6亿美元
2013年11月11日	Bitcash	系统/服务器遭入侵	100,000美元
2012年9月12日	Bitfloor	系统/服务器遭入侵	250,000美元
2012年3月1日	Bitcoinica	系统/服务器遭入侵	87,000美元

Ta表 1. 根据以下来源整理的中心化交易所列表： https://www.hedgewithcrypto.com

总之，去中心化交易所和中心化交易所平台都存在固有风险，包括黑客攻击和欺诈性管理，可能导致资金永久损失。为尽量降低这些风险，投资者应采取预防措施，例如使用冷存储方案、尽量减少存放在交易所的资金，并了解所用平台的安全功能。

3. 运营交易风险。

本研究的第二部分讨论了运营交易风险，以及可用于降低风险的交易算法。

4. 结论

本研究对基于区块链的货币市场中的高频交易作了实用介绍，并阐述了此类交易操作所特有的潜在风险，指出这些新型金融工具带来的风险可能会完全抵消其机会。第2部分将完成这份初稿。本研究不鼓励或推广任何交易活动。这类金融工具是新兴事物，基于先进的技术概念，因此需要充分理解。此外，即使充分了解风险，也不足以完全规避风险，尤其是第2.4节所述的失灵的中介机构风险。

5. 参考文献

Chainalysis。（2023年）。检索于2023年4月11日，来源：https://blog.chainalysis.com/reports/common-blockchain-analysis-mistakes-cryptocurrency-investigations/

Coingeko.（2023）。检索于2023年4月12日，来源：https://www.coingecko.com/CoinDesk.（2023）。检索于2023年4月14日，来源：https://www.coindesk.com/learn/

Cointelegraph。（2023）。检索于2023年4月13日，来源：https://cointelegraph.com/explained/crypto-wallets-security-explained

Decker, C.，& Wattenhofer, R.（2014）。比特币交易延展性与 MtGox。载于计算机安全—*ESORICS 2014*：第*19*届欧洲计算机安全研究研讨会，波兰弗罗茨瓦夫，*2014*年*9*月*7*日至*11*日。会议论文集，第*II*部分 *19*（第313-326页）。Springer International Publishing。

Fantazzini, D., & Calabrese, R. (2021). 加密货币交易所与信用风险：关闭概率的建模与预测。《风险与金融管理杂志》, *14*(11), 516。

HedgewithCrypto.（2023年）。检索于2023年4月10日，来源：https://www.hedgewithcrypto.com

Investopedia.（2023年a）。检索于2023年4月12日，来源：https://www.investopedia.com/terms/b/blockchain.asp

Investopedia.（2023b）。检索于2023年4月12日，来源：https://www.investopedia.com/crypto-investment-mistake-6504260。

Kwon, D., & Shin, N. (2018). Terra：稳定性与采用。检索自 https://terra.money/Terra_White_paper.pdf

Mazieres, D.（2015年）。恒星共识协议：一种用于互联网级共识的联邦模型。检索自 https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Medium，（2023年）检索于2023年4月14日，来源：https://medium.com/emiswap/the-4-most-common-mistakes-people-make-when-using-blockchain-bridges-f3371a842b8d

Nakamoto, S.（2008年）。比特币：点对点电子现金系统。检索自：https://bitcoin.org/bitcoin.pdf

Putz, B., & Pernul, G.（2019年）。许可型分布式账本中的信任因素与内部人员威胁：对热门分布式账本技术框架的分析研究与评估。《大型数据与知识中心系统汇刊》第42卷，25-50。

维基百科。（2023年a）。检索于2023年4月12日，来源：https://en.wikipedia.org/wiki/Bitcoin维基百科。（2023b)。检索于2023年4月12日，来源：https://en.wikipedia.org/wiki/Wash_trade