涉及中美受害人的跨国加密货币杀猪盘骗局

Bitrace*和ChainArgos†

2024年1月9日

1简介

网络诈骗犹如一场巨大的流行病在世界各地肆虐，数十个国家至少因此损失了数百亿美元（4）。一种名为“杀猪盘”[1]的加密骗局正在急剧增长，该骗局通常使用加密货币这一工具从受害人处骗取资金后进行链上清洗。（6）本文中，我们将基于中华人民共和国和美利坚合众国的受害者情况，探讨加密货币在杀猪盘骗局中的使用，并证明那些事先看起来毫不相干的案件背后具有显著的相似性。

本文将通过——列示这两个国家的骗子共用的加密货币地址，使用同一地址进行洗钱服务等事实，推断出他们很可能是同一团伙；从案件报告注明的受害者来源和诈骗钱包地址，通过加密货币链上追踪系统追踪诈骗款项，以证明其中的联系；最后，通过链上和文献研究相结合的方式，确定一系列交易所和其他服务提供商，以展示现今不法分子利用加密货币进跨境犯罪的现状，并强调全球执法机构在涉及此类骗局时面临的挑战。

1.1关于报告和文献的说明

为了便于讨论，并提供有参考价值的数字，附录中列出了所有钱包地址的详细信息。我们鼓励有专业知识的各方人士检查和复制这部作品，当然我们知道，绝大多数读者对这一细节不感兴趣。

这并不是试图混淆，或以其他方式使读者核验我们的结论变得困难。相反，它确保所有的流程图都是可读的，并且检查它们所需的所有长字符串都可以很容易从文档中复制出来。附录包含验证本文结论所需要的数据。

此外，为了本文的结论，我们对所有提交的文件进行了表面评估，在它们之间赋予同等的权重，并认为它们所包含的信息是可靠的。值得注意的是，这项分析并不是为了比较两国的法律制度或警察程序，而是为了证明中美两国活跃的骗局之间存在显著的重叠和相似性。

[1] “杀猪”骗局是一种信任骗局和投资欺诈，在与之打交道的一方消失跑路之前，受害者逐渐被诱导，对看似合理的加密货币投入越来越多的资金。

*Bitrace是一家中国区块链数据分析公司，为web3企业、金融机构、监管和执法部门提供领先的加密货币数据分析、风险管理、执法协作以及其他合规和监管工具产品和服务支持。电子邮件：bitracecn@gmail.com

†ChainArgos是一家区块链情报公司，为对冲基金、风险投资、投资公司、监管机构、执法机构、研究院和金融机构提供链上数据，以深入了解协议、交易和流程。电子邮件：info@chainargos.com

2受害者

在这里，我们探讨4种不同的受害者：

- 佛罗里达州的一个案例：佛罗里达州案例
- 一个涉及加利福尼亚州和佛罗里达州受害者的案件案例：加利福尼亚州案例[2]
- 来自中国的两个案例：中国案例

佛罗里达州的案件比其他案件要大得多，其中一名受害者被骗了200多万美元。在这起案件中，犯罪分子采用了各种各样的洗钱技术来清洗涉案资金。其余案件案值较小，使用的资金清洗手段也更少。

2.1佛罗里达州受害者

在佛罗里达案中，受害者陷入了一种较为常见的杀猪骗局，法庭文件描述如下：

> On April 15, 2022, Plaintiff and Defendant communicated through Facebook, an online social media and social networking service. Id. ¶ 10. Defendant represented that she was successfully engaged in investing in cryptocurrency and that her aunt was a prosperous cryptocurrency trading expert who managed an analyst group at Grayscale Investments, a legitimate third-party digital currency asset management company. Id. ¶¶ 11, 12. Defendant represented that, if Plaintiff were to join a margin trading platform called foundrypro.net ("Foundrypro"), Defendant would use sophisticated algorithms designed and implemented by Defendant's aunt to execute cryptocurrency trades in order to earn Plaintiff a profit. Id. ¶ 13. Neither Defendant nor Defendant's aunt had a relationship with Grayscale Investments. Id. ¶ 15.
>
> Based on these representations, Plaintiff joined Foundrypro on May 17, 2022 and began executing margin trades on that platform on Defendant's advice. Id. ¶ 17, 19. Over the course of Plaintiff and Defendant's relationship, Plaintiff invested 2,215,118 units of "Tether" (USDT), a form of cryptocurrency known as stablecoin that is pegged to the value of the U.S. Dollar. Id. ¶¶ 23, 24. From April 15, 2022 through the end of October, 2022, Defendant communicated with Plaintiff via SMS, WhatsApp, telephone calls, and email. Id. ¶ 16. Foundrypro featured a dashboard that displayed illusory investment gains which, together with Defendant's representations, encouraged Plaintiff to continue "investing" in Foundrypro. (1)

[2] 本案由佛罗里达州的一家法院出于管辖权原因处理，尽管加利福尼亚州的受害者损失了更多的钱。选择这个名字是为了减少混淆。

经过一系列司法流程后，受害者获得了缺席判决。

本案的文件提供了两类加密货币地址。首先，该文件列出了受害者最初转移资金的地址，我们将其称为受害人地址。其次，文件提供了一份加密货币交易所存款地址列表[3]，受害者的资金被发送到这些地址。详见附录A.1。

2.2加州受害者

在加利福尼亚州的案件中，两个不同的人成为了杀猪骗局的受害者，他们将加密货币发送到了附录A.2中提供的同一个骗局钱包。

第一个骗局涉及约177,502.29美元，法庭文件中描述如下：

> [Victim] met an individual known to him as “Bunny” through social media (Facebook) and started a romantic relationship with her. During the relationship, Bunny offered [Victim] a way to make money through cryptocurrency so they could afford to buy a farm and live together one day.
>
> During the relationship, Bunny convinced [Victim] to invest in cryptocurrency through “Pearcoin,” a fake cryptocurrency trading application, unknown to [Victim] at the time.
>
> Ultimately, [Victim] attempted to withdrawal his funds from Pearcoin and was told he must pay the taxes up front or he would risk a 3 per cent penalty fee for each day he did not pay. At this point, [Victim] realized he was involved in a scam and subsequently contacted the Brevard County Sheriff’s Office to report the incident. [Victim] was unable to transfer, withdraw, or access any of his funds through the investment platform. (3)

第二个骗局与此类似，涉及金额约为300,000美元：

> The victim ... reported she had been romantically involved with an individual through social media. During the relationship, she was convinced to invest in cryptocurrency. (3)

[3] 加密货币交易所提供“存款地址”，以简化为客户存款的流程。当客户打算存入资金时，交易所会为他们创建一个可以发送资金的专用地址。通过这种方式，交易所可以自动将所有转入该地址的转账分配给特定的客户账户。将“存款地址”视为一种工具，通过使用不同的外部账号确保将资金发送到正确的内部账户。

2.3中国受害者

Bitrace提供了有关中国案例的信息和数据。一名来自天津受害者称，他被诱导在加密货币交易所OKX建立账户，并将USDT提取到交易应用程序WBF和币胜。在几次较小的投资后，天津受害者获得了4,860美元的回报，随后进行了更多的投资，最终损失了大约40,000美元。这起骗局中没有情感欺诈成分的报道，更像是佛罗里达案中的杀猪盘骗局。天津受害人的资金来源se^{China}在附录A.3中，这是一个与已知骗局相关的钱包，我们稍后将详细说明。

另一名活跃在OTC市场的受害者报告了一个涉及se^{China}的钓鱼骗局。钓鱼骗局是指受害者被说服下载恶意的“特洛伊木马”软件，该木马会清空钱包，并将资金发送给骗子（7;5;9）。尽管在Bitrace接触到的受害人案件中，有两名加密货币承兑商客户遇到过这个骗局，但这个骗局似乎与一个比天津受害者更小的团伙有关。

中国没有像美国那样的法庭文件，但我们可以摘出当地对类似案件的报道，以进一步强调此类骗局。宁波（2）和温州（8）的地方当局报告了类似的诈骗案。例如，温州执法部门的一份新闻稿描述了一个涉及“特洛伊木马”软件的骗局，类似于Bitrace的一个客户报告的骗局：

> 经查，自2022年2月以来，该团伙在多个境外社交软件上发布销售打折加油卡的广告，以检测虚拟货币钱包和虚拟货币的真实性为幌子，诱骗受害者点击木马程序链接，并在暗中控制其钱包，在时机成熟的情况下，非法获取钱包中的虚拟币，短短一个月内作案30余起，涉案金额100余万元。(8)

这听起来既与世界各地报道的骗局相似，也与活跃在OTC市场的中国受害者报道的盗币骗局相似。

在中国的案例中，由于两国法律制度的差异，无法提供类似于佛罗里达州和加利福尼亚州案例的文件来进行比较分析，但这并没有削弱两国工作方式的相似性。正如我们看到的，分析的所有涉案资金都通过钱包清洗并与服务提供商的地址产生交集，这证明两起案件之间存在联系，两起案件的欺诈者属于同一个犯罪实体。

3服务提供商

佛罗里达州受害者的法庭文件提到了四家加密货币交易所：币安、Bitkub、FTX和OKX，它们都是知名的大型服务机构。币安长期以来一直是世界上最大的加密货币交易所，FTX由Sam Bankman Fried创立，他目前正在等待一场备受瞩目的欺诈案的审判结果。OKX是一家大型加密货币交易所，虽然不如币安和FTX知名，但它赞助了一些世界各地的备受瞩目的运动队和赛事。Bitkub是四家上市公司中最小的一家，是泰国最大的加密货币交易所，同样在其市场内进行着高调的赞助。

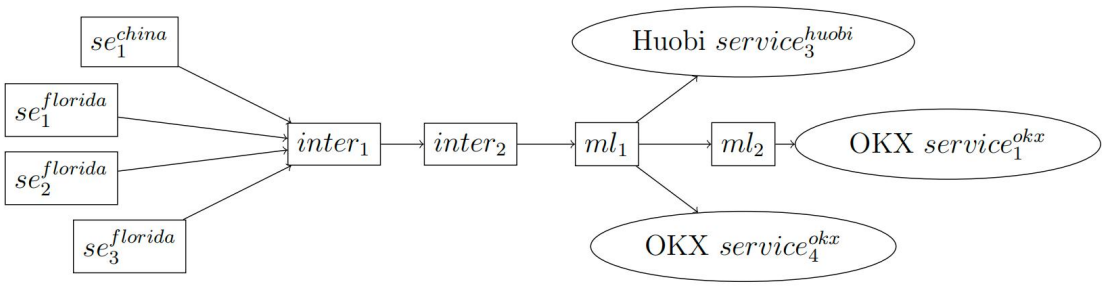

图1：佛罗里达州与中国的两名受害人的资金存在关联，并且被骗资金进入了同一组洗钱水房地址。请注意，佛罗里达州的文件中没有提到这个外汇存款地址——这是一个额外的下游地址。

进一步分析发现，Coinbase、Huobi、Maicoin、Maskex、Paribu和Peatio都是类似的知名交易所。Coinbase在纳斯达克上市，年收入达数十亿美元，目前市值达数百亿美元。Huobi是一家大型交易所，拥有多家在香港交易所上市的子公司，与许多其他亚洲交易所一样，它赞助包括西班牙国家男子足球队在内的体育项目。Maicoin称自己是台湾领先的加密货币交易所。Maskex是一家总部位于阿联酋的加密货币交易所，并持有VASP许可证。Paribu是一家土耳其交易所，与多家土耳其足球俱乐部有合作关系。Peatio是一家中国加密货币交易所，几年前关闭并开放了他们的交易软件，虽然该交易所可能已经倒闭，但其钱包地址仍然活跃。

在这里，我们只想确定这些服务提供商是大型、知名、可见的实体，不需要对其存在或参与加密货币交易进行进一步分析或提供任何形式的书面证据。

进一步的讨论将涉及在诈骗进入点和交易所之间运作的较小各方。虽然这些在新闻界和体育界不太显眼，但不难发现，交易所显然参与了诈骗收益的管理。

4下游资金追踪

本段分析中国案件和佛罗里达案件的下游地址，揭示诈骗所得资金的最终流向。在图1中，我们绘制了从佛罗里达州的三个地址和中国的一个地址通过相同的中介地址，转移到我们标记为ml_1和ml_2的两个钱包的动向。*ml*表示“洗钱者”，他们从一系列骗局中获得收益，并将钱存入交易所，其功能相当于资金汇集地址。

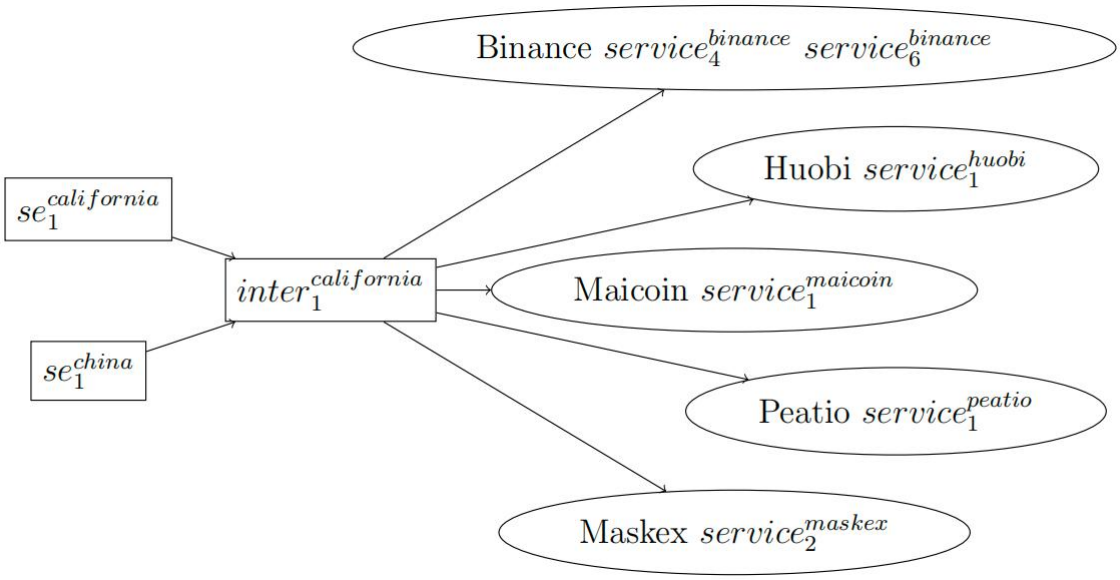

图2：将加利福尼亚州的诈骗地址与中国的诈骗地址连接起来，发现它们共享的下游中介与许多交易所有联系。

需要注意的是，欺诈收益不会以点对点的单线顺序转移方式经由洗钱地址转移，且并不是每个单位的诈骗收益都同时通过这个确切的钱包序列提供。相反，我们只是确定，这类欺诈事件及其后续洗钱活动都以相似的方式，发生在相近的时间。因此，这些团伙很可能是同一整体群体的一部分。这一点尤其令人信服，因为这些资金最后都流向了同一组通往出口的洗钱地址。

现在让我们把中国的案子和加利福尼亚的案子联系起来。在图2中，我们看到了不同案件中的资金重叠流向——同一个钱包出现在两个不同案件的下游。

还要注意的是，中介地址$inter^{\text{california}}$与加利福尼亚州案件的民事没收令（3）中给出的许多存款地址有关。此外，图[4]中的币安存款地址之一在几个月前就被路透社记者披露并引起了ChainArgos的注意，因为该地址与许多与 (6) 相关的诈骗有关。

接下来，我们将在图3中展示中间地址和交易所的联系。中国案例诈骗输入地址也与图4中的兑换存款地址有直接联系。

在se_2^{China}下游也可以看到类似的结构，在通过两个中间钱包后，资金被存入$service_5^{OKX}$。

虽然这并不是所有地址的全部展示，但它仍然表明这些骗局相互之间都存在相互联系，并波及到许多交易所。

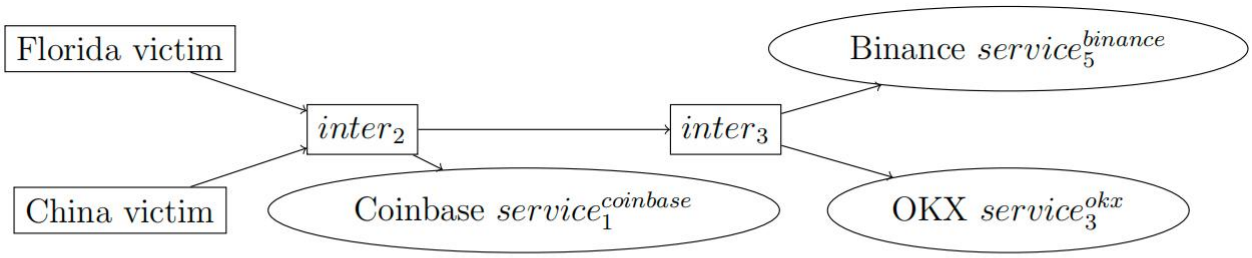

Figure 3: Further connections.

Binance	Huobi	Maskex	OKX	Paribu
$service_1^{binance}$	$service_1^{huobi}$	$service_1^{maskex}$	$service_1^{okx}$	$service_1^{paribu}$
$service_2^{binance}$				
$service_3^{binance}$				
$service_4^{binance}$				

图 4：与中国受害者的诈骗入口地址直接相连的交易所存款地址。

5总金额

到目前为止，本文通过披露单个骗局，追踪其共同的资金来源，从而确定这些骗局是某个大型欺诈组织的一部分。目前，没有足够多的信息来支撑我们记录下这一群体或相关群体实施的所有骗局。鉴于犯罪和受害者的性质，我们难以有一个可靠详尽的清单。因此，下一个合乎逻辑的步骤是查看这些案件中使用的服务提供商地址的资金总量，以确定该组织的潜在规模。对资金规模的分析提出了三个独立但相关的问题：

1.有多少钱流入了已披露的“诈骗输入”地址？

2.有多少钱通过服务提供商中转？

3.有多少钱流向了像交易所这样的资金出口？

5.1骗局规模

我们发现，从2021年年初截至撰写文本时，共有2070万美元流经前文披露的中国天津受害人案件的相关地址。由于该受害人损失了约4万美元，我们只关注到该团伙作案活动的其中一小部分，可以肯定的是，会有更多的涉案资金在该地址集中。

在佛罗里达案中，受害者声称损失约220万美元，但这三个地址的总流入额略低于650万美元，这证实受害者肯定更多。在用于映射这些流量的六个“诈骗条目”地址中，我们发现总流入量为：

$se_1^{florida}$	US$3 million
$se_2^{florida}$	US$4 million
$se_3^{florida}$	US$2 million
$se_1^{california}$	US$350 thousand
se_1^{china}	US$21 million
se_2^{china}	US$285 thousand
Total	US$30 million

在这些地址中，最独特的是，大多数流入$se_1^{alifornia}$的欺诈资金都是以以太币计价的，而不是稳定币USDT，$se_1^{alifornia}$总共收到了156.04个以太币。我们以2000美元的价格将以太币美元化，这反映了转账时的平均转换价格。

5.2服务提供商规模

接下来我们来 看看通 过 一些中间地址的流量总量。对于上述例子中的 六个中介机 构 ， 我们发现USDC和USDT的流入量为：

ml_1	US$79 million
ml_2	US$2 million
$inter_1^{california}$	US$15 million
$inter_1$	US$2 million
$inter_2$	US$6 million
$inter_3$	US$2 million
Total	US$106 million

其中一些是流经多个地址的相同代币，示例甚至显示了从ml_1到ml_2的流。根据流量合理估计，这些中介机构的处理金额在8000万至1亿美元之间。

到目前为止，最大的一笔资金流向了交易所。通过检查（1）中指定的交易所地址的存款，我们发现以下总数：

Exchange	Amount
Binance	US$159 million
Bitkub	US$27 million
FTX	US$249 million
OKX	US$13 million
Total	US$447 million

如果加上通过其他案例连接的地址，我们会得到：

Exchange	HQ	Florida Amount	Additional Amount	Total
Binance	Malta/Seychelles/?	US$159 million	US$35 million	US$194 million
Bitkub	Thailand	US$27 million	US$76 million	US$103 million
Coinbase	USA		US$2 thousand	US$ 2 thousand
FTX	Bahamas	US$249 million		US$249 million
Huobi	Seychelles		US$10 million	US$10 million
Maskex	UAE		US$ 3 million	US$ 3 million
Maicoin	Taiwan		US$177 thousand	US$177 thousand
OKX	Seychelles	US$13 million	US$28 million	US$41 million
Paribu	Turkey		US$10 thousand	US$10 thousand
Peatio	China?		US$8 million	US$8 million
Total		US$447 million	US$188 million	US$635 million

虽然这并不意味着这个犯罪组织要对所有这些资产负责，但它提供了强有力的证据，表明该地区仍有大量犯罪流动资金有待发现。

请注意，这些数据包括几个交易量较小的交易。这些都是为了数据的完整性而包括在内的，这并不是为了详尽无遗。即使在总额较大的交易所中，我们也会发现个别存款地址在总流量中会有不同的数量级。

另注意，几乎所有的交易量都发生在中国和美国以外的交易所，绝大多数由总部设在海外司法管辖区的企业处理。

5.3交易所提款

在加利福尼亚州的案件中，调查还发现了由诈骗团伙控制Tron区块上的一个交易所提款地址，通过该波场地址的资金规模约为110万美元，远远超过加州案件中损失的约50万美元，这表明对Tron和其他区块链的进一步调查可能会发现更多的关联性线索。

6讨论

该分析证明了三个关键事实：

1.类似的同时发生的骗局在中国和美国都有受害者；

2.从两个司法管辖区提取的资金通过共同的中介地址流通；

3.涉及的金额从数千万美元到数亿美元不等。

重要的是要理解分析中存在的以下局限性：

1.我们并不是说流入这些“骗局地址”钱包的3000万美元都是骗局收益收益，只是当前可以追踪到的；

2.尽管发现了6.35亿美元的外汇存款，但我们并不是说所有这些都可以归因于骗局；

3.考虑到交易的循环，上述数字可能并非完全没有重复计算。[4]

[4] 例如，存放在一个交易所的一些钱可能会被提取并重新存放在其他地方。

相反，应该从实施诈骗的范围和规模的背景来理解分析。首先，只分析了四个案件，受害者站出来并开始了某种形式的正式法律程序。其次，我们已经证明这些骗局与（6）中讨论的骗局有关，这表明此类骗局的规模和规模可能比以前所理解的更深远、更广泛。

似乎有更多的资金流动线索有待发现，通过加密货币生态进行诈骗获取的收益可能比我们目前的估计要大得多。此外，值得注意的是，虽然这些案件的受害者位于世界上最大的两个经济体，但在处理这些诈骗收益的交易所中，最多只有一小部分位于这些国家。为了解决这些问题，需要进行大量的国际合作。

参考文献

[1] Bowen v. Xingzhao Li, 23-cv-20399-BLOOM/Otazo-Reyes (S.D. Fla. Jul. 26, 2023).

[2] China Ningbo Net. A large amount of virtual currency was stolen from a ningbo citizen by a hacker., 7 2022. URL http://news.cnnb.com.cn/system/2022/07/19/030371164.shtml.

[3] Florida Circuit Court. Eighteenth Judicial Circuit In And For Brevard County, Florida Case No: 05-2002-CA- Filing 162250539 Civil Forfeiture.

[4] Global Anti-Scam Alliance. The global state of scams - 2022 report, 2022. URL https://www.gasa.org/product-page/the-global-state-of-scams-2022-report.

[5] Ledger. Security incident report, 12 2023. URL https://www.ledger.com/blog/ security-incident-report.

[6] P. McPherson and T. Wilson. Crypto scam: Inside the billion-dollar ‘‘pig-butchering‘‘ indu stry. 11 2023. URL https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/.

[7] ScamSniffer. From google to x ads: Tracing the crypto wallet drainer‘‘s $58 million trail, 12 2023. URL https://drops.scamsniffer.io/post/from-google-to-x-ads-tracing-the-crypto-wallet-drainers-58-million-trail/.

[8] Wenzhou Public Security Bureau. 743 cases were solved and 2,093 people were arrested! the results of the wenzhou clean network 2022 operation are announced!, 11 2022. URL https://mp.weixin.qq.com/s/hU5_jxtoVUHpmmKOYmg6Jw.

[9] ZachXBT. Monkey drainer twitter thread, 10 2022. URL https://twitter.com/zachxbt/status/1584955933452484613.

附录：地址

A.1佛罗里达州受害者

类型	交易所	名称	地址
受害人地址		$se_1^{florida}$	0xBA109c48264785070E35963592540324e8612d09
受害人地址		$se_2^{florida}$	0xb285CA276C96c47b546d0Ca88F77905fAdC8eb3A
受害人地址		$se_3^{florida}$	0x9800322CA41c512265A0B14C49a834C4A2c448Aa
资金存入	Binance	$florida_1^{binance}$	0x54414a636b5439b14266f1ec9504a34b50cb5b9b
资金存入	Binance	$florida_2^{binance}$	0x753173f4a680796f98e6b824a0f2da6fef191b39
资金存入	Binance	$florida_3^{binance}$	0xb90f30f9f279fc07f33c3cd3942dc028f97400a4
资金存入	Binance	$florida_4^{binance}$	0xb90a40957179711a53d09ade855bc5f45eeca1e1
资金存入	Binance	$florida_5^{binance}$	0x38f6e7dd38954102b8471e7985d2420d23b3f35d
资金存入	Binance	$florida_6^{binance}$	0x94bf1e38da59c7df90566883a3525c5fa3ca215c
资金存入	Binance	$florida_7^{binance}$	0xc52b9dfb82490d14d76f0efd7ce76e82f2b5adfc
资金存入	Binance	$florida_8^{binance}$	0xf380135d44be7e08a95c74c01c53deaec3a1701f
资金存入	Binance	$florida_9^{binance}$	0xea5331f5f39c6e3801e4fd63d99e75b2a527d032
资金存入	Binance	$florida_{10}^{binance}$	0xf1d60bb0958a79cbaf2145a929cd395173a37149
资金存入	Binance	$florida_{11}^{binance}$	0x98a3b01609867a066524f78b33c72feef598d78d
资金存入	Binance	$florida_{12}^{binance}$	0x54414a636b5439b14266f1ec9504a34b50cb5b9b
资金存入	Binance	$florida_{13}^{binance}$	0xa14e0972a9d1ecdd7b8eb3be27b3901ebb24518f
资金存入	Binance	$florida_{14}^{binance}$	0x9f7db89d141521517a553fbb704b8b05566c08a5
资金存入	Binance	$florida_{15}^{binance}$	0x5768a6c7a29cea444bbdd454b03a288d0e1d113e
资金存入	Bitkub	$florida_1^{bitkub}$	0x2bc47f91bfc8d848abfce3b81f3ce07e647fbc2d
资金存入	Bitkub	$florida_2^{bitkub}$	0xdb752832678b48e0ab53e023f054f62a09ca852c
资金存入	Bitkub	$florida_3^{bitkub}$	0xe51d0faa62f279e45938edd494f92720126bcf4f
资金存入	FTX	$florida_1^{ftx}$	0x56f60315bee850b6a212c797ee1ed43503a9536c
资金存入	FTX	$florida_2^{ftx}$	0x0f4c6cc5492dbbeb567ad752afa4ea16f44e51c6
资金存入	OKX	$florida_1^{okx}$	0x29b71e4e2d12a6aa2f3cf330f0d79e75e58f54f0
资金存入	OKX	$florida_2^{okx}$	0x967d6bc2696935b305dc42023e8e7453bbef5f6c
资金存入	OKX	$florida_3^{okx}$	0x8c379e714c01a8f8b3cb328f46bc249f918a5df4

A.2加利福尼亚州受害者

类型	交易所	名称	地址
受害人地址		$se_1^{california}$	0xcCC2F333e57cB739a3a62ED1e7A76EE17D3C3911
中间地址		$inter_1^{california}$	0x346eF244464679b031750f70D750B3FA65165443
资金存入	Binance	$cali_1^{binance}$	0x8459dd488c507b20331e0F6aC481F75Ee9f4ae97
资金存入	Binance	$cali_2^{binance}$	0x1d43DC389993cB3818724E0d06746BbaA6A9e02e
资金存入	OKX	$cali_1^{okx}$	0xc3b15B326C0eD1576f918a3B36c9dE789f936d0b
资金存入	Bitkub	$cali_1^{bitkub}$	0x5453fd1ef17c8c4F2042b07416573c3eCa19D247
资金提出	Binance	$cali_{withdrawl}^{binance}$	TWLy3aGGkRck2uoZenQQPVi7AapyTVNebC

A.3中国受害者

类型	名称	地址
受害人地址	se_1^{china}	0xe0f807bbb43ece93dde44869d9a5324d5771bd67
	se_2^{china}	0x41f0725de3f24a8ac2974a6e3a9b53567a70e0a

A.4服务提供商

描述	名称	地址
洗钱	ml_1	0xd7ee3b0fffd6a0d9d26a79129159942d29665fe1
洗钱	ml_2	0xab557fcc296231ca252857b64bd6373d8c5ed0e1
中间地址	$inter_1$	0x7ece0eff6631de8bf0717f65264945164fef019d
中间地址	$inter_2$	0x197b81d8593bC8dFbBB689DfD102E91217028baf
中间地址	$inter_3$	0x4fF0043D87900Ac1c64D63ad22f1e3cF781A9Aa3
币安存款	$service_1^{binance}$	0x4517779153917fe9342443DEA08681894a62bBe1
币安存款	$service_2^{binance}$	0x8d9e3622651E920a0Ed392d1B72a4a4F70fABB59
币安存款	$service_3^{binance}$	0x65e84F275dF40295a53CA0215720F350198De1Aa
币安存款	$service_4^{binance}$	0x101ae4fa34ae5fdb538c1e0161a3632d51a15392
币安存款	$service_5^{binance}$	0x8DaE1F79fe75A6B55d548B725973611C886496cD
币安存款	$service_6^{binance}$	0xaf9e1ff950337cb623a12467301d63c3ce803005
Bitkub存款	$service_1^{binance}$	0x08c3ae0DBd53D6E01F9e8EB21E20be2e0da97Eb8
Coinbase存款	$service_1^{coinbase}$	0x03d6cf0f90387132cbd60a3d6a4151179eb9fdce
火币存款	$service_1^{huobi}$	0x8868df97a1ce9c1a091c6836d988a430cc0ffe35
火币存款	$service_2^{huobi}$	0xeAb7461efeEFaB80ca7CC98708E5319C7F3F4B44
火币存款	$service_3^{huobi}$	0xc32eA9c68AaB7f1CDc8E251dEFFffFbC1271B092
Maicoin存款	$service_1^{maicoin}$	0x1646651e9C35Fdd8484082d37aB17d0AA4a51457
Maskex存款	$service_1^{maskex}$	0x1C8321acbe4CA3e9AD0287b8E5c262Ce343B27D2
Maskex存款	$service_2^{maskex}$	0x19231f73cdcb01c346f23c58e388f79d7480a0a9
OKX存款	$service_1^{okx}$	0x7bAF3e10BfB2177061dbc576B126Ffd605751bC0
OKX存款	$service_2^{okx}$	0x34cF51e60B2997e544Da263dfBac4562d14b7DAB
OKX存款	$service_3^{okx}$	0xCebc7962ECFe1A268810C928C467c5c4A63905c8
OKX存款	$service_4^{okx}$	0x2C72dDd368c4B50d99Aa2bBA0a7F3e49Ad346b8E
OKX存款	$service_5^{okx}$	0x90B5a0893189F9B0264e238f9EFE0df92A41BA2d
Paribu存款	$service_1^{paribu}$	0x27f72A97951135EB63aEb37d91eE02bA94fF1175
Peatio存款	$service_1^{peatio}$	0x01d05E050172ECf22A3374905822302296D71b1d