补充材料一

一，推荐警方做什么？

（简单方案，不需要牵扯不相干的细枝末节）

一，一，调查与立案：

询问受害人，让受害人提交材料，做笔录，最后立案。

一，二，侦查与破案：

1，准备任意邮箱，警官证，向上级请示。

（请示能否允许向交易所提交警官证照片，和手持警官证照片，用于币安交易所执法请求认证。）

2，通过以下链接，联系交易所，注册，并向交易所提交执法请求。

需要VPN，才能访问：（需要在这里阅读说明）
https://www.binance.com/zh-CN/support/law-enforcement

不要VPN，直接访问：（需要在这里注册）需使用谷歌浏览器访问，且手机访问需开启"桌面版网站"选项，电脑访问则无需。
https://app.kodex.us/binance-cn/signup

3，警方将注册邮箱告知受害人，受害人凭借警方邮箱，联系交易所，获取案件调查进展。

4，警方通过受害人的身份证号码（受害人已用身份证号码通过交易所KYC认证），

锁定受害人账户，与交易所合作，调取数据，侦查，破案。

5，警方锁定证据，追踪责任，明确民事与刑事的责任归属。

一，三，执法与结案：

最终追回并返还，加密货币资产，到受害人的币安交易所账户，

追究责任，结案。

二，王天佑对交易行为的补充陈述

1，黑客盗币事件的性质

黑客盗币事件的性质是：网络盗窃，金融犯罪。金融犯罪是手段，网络盗窃是目的。

2，受害人王天佑没有超出两个平台既定的规则和功能

Fast API授权是机器人提供的功能，受害人王天佑没有超出机器人提供的功能。

API第三方授权是交易所提供的功能，受害人王天佑没有超出交易所提供的功能。

3，受害人王天佑没有超出他的能力圈做事，因此，王天佑不应对其能力圈之外的事情，承担额外的责任

合约交易，王天佑不懂，所以受害人王天佑不做合约交易。

至于信息安全和软件工程，王天佑也不懂，所以王天佑外包给经纪商（机器人）和托管方（交易所）了。

4，王天佑授权了API，但是王天佑没授权非法的交易和划转行为

5，亏损是金融风险，盗币是安全风险，这是两个性质

作为投资者和做市商，王天佑只负责承担金融风险，至于安全风险，是经纪商AntBot和托管方Binance应该承担的责任。

王天佑的工作是投资组合管理，以及作为做市商的流动性提供。所以，王天佑可以承担金融风险，但王天佑不应该负责和承担安全风险。

王天佑在发生盗币事件之前，只懂投资组合，和做市策略。至于软件工程，编码实现，信息安全，网络安全和密码学，不是王天佑的专业范围，所以王天佑外包给专业人士了。既然王天佑已经外包出去了，王天佑就不应该负责和承担这个安全风险了。

6，"翻墙"行为，"C2C买卖USDT"行为，是否违法，存在争议

注：参见后文，第五，第六

6-1，王天佑对"翻墙"行为的指控，强调几点：

6-1-1，"墙"的这个概念，在当前中国的一切公开的规范性法律文件中，都是不存在的。

6-1-2，"墙"的本质是，入侵检测手段，和非法的网络攻击手段，"墙"本身是违法的。

6-1-3，"翻墙"行为是，架设专用网络，进行数据加密，抵御或避免"墙"的网络攻击，并使用中国国家批准的合法互联网物理基础设施，访问境外的合法网站，因此"翻墙"并不是非法行为，并不违法，也不违反相关规定。

6-1-4，"翻墙"与"墙"的行为没有发生在物理层以及物理信道，个人翻墙亦不是企业行为，因此"翻墙"行为不在相关文件的约束范围内，因此所谓个人的"翻墙"，并不是非法行为，并不违法，也不违反相关规定。

以上参见后文：五，有关"翻墙"的法律法规和科技术语解释，5，有关"翻墙"是否违法的解释。

6-2，王天佑对"C2C买卖USDT"行为的指控，强调几点：

6-2-1，在币安交易所，USDT个人间的交易，是C2C交易，不是OTC交易，之前的相关法规没有禁止C2C交易，只是禁止了OTC交易，因此C2C交易没有被法规禁止，是合法的。

6-2-2，C2C交易中，平台撮合式交易方式，订单随机匹配，承兑商在交易前客观上根本无法知晓其交易对手的身份以及收取的款项的性质，不可能与对方形成共谋的意思表示，主观上也不可能是明知。

6-2-3，行为人以真实身份信息以及银行卡实名注册，从侧面也能说明其没有犯罪主观故意。

6-2-4，行为人已经币安交易所在进行KYC审核，有理由相信对方是合法交易。

6-2-5，行为人的交易价格无明显异常。

6-2-6，行为人的交易，在行为人家中发生，行为人性格内向，在交易过程中，没有向公众提及自己的交易行为，也没有干扰其他人，因此，没有违反公序良俗。（注：违反公序良俗的情形主要包括：危害国家公序、危害家庭关系、违反两性道德、射幸行为、侵犯人格尊严、违反竞争秩序、违反消费者与劳动权利保护、暴利行为等。）

6-2-7，USDT是一种加密货币，属于虚拟商品，不是货币、外汇、有价证券。购买USDT个人间的的银行或支付宝转账，也遵守银行和支付机构的相关管理规定，没有违反金融机构，支付机构和银行的管理规则。因此在币安交易所，个人间C2C交易USDT，不构成破坏金融管理秩序罪。

6-2-8，非法经营不属于洗钱罪的上游犯罪，因此，即便假设上游真的存在非法经营，交易USDT也不构成洗钱。

6-2-9，如果怀疑是，存在其他上游犯罪，构成洗钱，或者怀疑是，诈骗罪，帮信罪，掩隐罪，可以参考如上所述的6-2-1，6-2-2，6-2-3，6-2-4，6-2-5，6-2-6。

6-2-10，如果怀疑是，开设赌场罪，王天佑强调，对于加密货币的投资管理与做市交易，属于投资与交易行为，并非赌博行为，且币安交易所是加密货币交易平台，并非网络赌博平台。

7，王天佑认为，在国外网站发生的币币交易行为，不违反国内法律。个人的投资与交易行为亦不属于经营行为。

币安交易所位于国外，因此在币安交易所进行的现货币币交易行为，实际在国外的网站上发生。

因此，在国外网站上发生的币币交易行为，不违反国内法律，亦不违反国外法律。

王天佑个人的投资与交易行为，亦不属于经营行为，不涉及非法经营。

但是黑客针对加密货币的未授权交易，导致的网络盗窃和金融犯罪的行为，不论发生地点在国内还是国外，均属于违法行为。

8，王天佑认为，笔录中的民间口语化表述，仅供警方参考理解。

但不能作为判决依据，如“翻墙”等。

王天佑认为，之前的笔录过程中，警方说，笔录要便于警方上级领导理解。

因此，王天佑的表述，经过警方的引导后，可能会口语化，从而牺牲准确性和公允性。

如“翻墙”，是口语和民间的表述，仅供警方参考理解，但不能作为最终的法律判决依据。

有关相关问题的，准确表述，本材料的下文中，会进行明确的解释说明。

9，王天佑认为，笔录中的个人猜测，仅供警方参考理解。

个人猜测，不能代表或代替，政府和机构的官方意见。（问题问错人了）

对于相关问题，王天佑个人说了不算，没有法律效力，不能作为判决依据。

王天佑认为，之前的笔录过程中，对于警方询问，有关“加密货币是否属于个人财产”，“加密货币在中国的财产类型属性”，“加密货币是否受中国法律保护”，“交易加密货币是否合法”，“币安交易所经营地点在哪”，“中国是否承认币安交易所对加密货币的定价和估值”，“币安交易所在中国是否合法”等问题：

王天佑不是相关中国政府部门或相关机构的工作人员，王天佑在笔录过程中的意见，只是个人的猜测，王天佑个人的猜测不能代表或代替，相关中国政府部门和相关机构的官方态度和意见，因此没有法律效力，不能作为判决依据。

相关问题，警方可以去咨询，中国政府有关部门（比如，中国人民银行、中央网信办、最高人民法院、最高人民检察院、工业和信息化部、公安部、市场监管总局、银保监会、证监会、国家外汇局、财政部、国家工商总局、国务院法制办、国家互联网信息办公室、中央网信办、中国互联网金融协会、中国银行业协会、中国支付清算协会、发改委等中国政府有关部门），币安（Binance）加密货币交易所，资产评估机构，会计师事务所，国际密码研究协会（IACR），国际金融密码协会（IFCA），国际会计准则委员会（IASC），国际刑警组织（ICPO），国际期货业协会（FIA Global），国际金融管理协会（FMA），世界银行（WB），国际清算银行（BIS），国际货币基金组织（IMF）等，政府部门和相关机构的，法律，规定，标准，准则，解释，态度，意见，以便进一步明确。

王天佑在笔录中的回答，只是个人猜测，不属于相关中国政府部门和相关机构的回答，所以，王天佑说了不算，没有法律效力，不能作为判决依据。

三，币安交易所客服对警方疑问的解释

1，报警时效问题：

币安交易所客服回应，没有报警时效。不论什么时候联系币安交易所，币安交易所都会全力配合警方调查。

2，为啥币安不报警问题：

币安客服回应：AntBot属于第三方程序，币安与AntBot没有直接关系，相关程序是王天佑在使用，所以币安不是受害者。

关于资金存放在币安的问题，币安客服说，王天佑在币安的资金是通过王天佑授权给AntBot的API发起交易的，而AntBot的API被黑了，所以主要问题点在于，王天佑与AntBot之间的利益损失。所以，币安不报警。

（之前王天佑和警方说过了，如果王天佑去找AntBot客服，AntBot客服就说，因为王天佑的资产存放在币安，因此责任在币安。）

3，为啥私人去注册，币安的执法请求提交系统链接，不能通过认证：

在大多数情况下，为了保护客户的机密信息，币安只会配合由政府部门提交的执法请求。法律不允许币安披露任何正在调查的信息。

警方成功注册后，用户王天佑可以提交警方的邮箱给币安客服，联系币安执法相关部门，以获取有关案件的机构更新信息。

四，涉区块链业务相关人员名单

注：以下内容不构成任何投资建议，亦不代表当事人王天佑的态度，排名不分先后，仅供参考。

中国人与海外华人，经营区块链业务的，有很多人，有一些还在国内：

加密货币交易所

- 赵长鹏，何一（币种：BNB）（涉嫌：交易所，ICO）

赵长鹏是币安创始人，之前在国内的公司是比捷科技，赵长鹏曾任OKCoin交易所CTO，后来去了海外，做了目前世界最大的加密货币交易所币安，发了交易所代币BNB，目前BNB在世界加密货币中，市值排名世界第三，市值仅次于BTC和ETH。

- 孙宇晨（币种：TRX，BTT，HT）（涉嫌：交易所，ICO）

北大与宾大毕业，曾拍下巴菲特午餐，发了TRX波场币，上了币安，收购了BitTorrent，发了BTT币，后来控制了HuoBi火币交易所，并改名“火必”。由于其控盘水平太高，被网友称为“孙割”。

- 李林（币种：HT）（涉嫌：交易所，ICO）

HuoBi火币交易所创始人，发过交易所代币。

- 杜均（币种：HT）（涉嫌：提供信息服务，投资，交易所，ICO）

HuoBi火币交易所投资者，目前在区块链媒体：金色财经。

- 徐明星（币种：OKB）（涉嫌：交易所，ICO）

OKCoin与OKEX交易所创始人，发过交易所代币。

- 雷臻（涉嫌：交易所，ICO）

雷臻是Bibox 交易所创始人，也是原OKCoin 交易所创始人。Bibox 交易所联合创始人是Aries Wang，具体姓名未知。

- 唐珂，甘醇（币种：KCS）（涉嫌：交易所，ICO）

甘醇是KuCoin交易所创始人，发了交易所代币KCS，KuCoin交易所的多层营销模式被怀疑是金字塔传销。

- 韩林（币种：GT）（涉嫌：交易所，ICO）

韩林是Gate.io交易所创始人，发了交易所代币GT。

- 陈建/陈龙杰（币种：MXC）（涉嫌：交易所，ICO）

本名陈建，真名为陈龙杰，抹茶交易所MEXC创始人。

- 张健（币种：FT）（涉嫌：交易所，ICO）

前HuoBi火币交易所CTO，FCoin交易所创始人，后来FCoin交易所暴雷跑路了。FCoin发过交易所代币，张健曾是工信部区块链专委会委员。张健著有《区块链：定义未来金融与经济新格局》和《金融科技重构未来金融生态》书籍。

- 赵翼（币种：WAL）（涉嫌：交易所，ICO）

赵翼是鲸交所创始人，鲸交所WhaleEx采用了慢雾科技安全系统，同时启用了EOS超级节点多重签名机制。 鲸交所WhaleEx已经跑路。

加密货币矿业

- 吴忌寒（币种：BCH）（涉嫌：矿业，ICO）

比特大陆创始人，比特大陆生产蚂蚁矿机，比特大陆曾被红杉资本投资，比特大陆也经营BTC.com和Antpool矿池业务，经营云算力挖矿业务BitDeer比特小鹿，曾分叉BTC发了BCH币，长期来看，BCH相对BTC一直下跌。

- 毛世行（涉嫌：矿业，钱包）

网名神鱼，F2Pool矿池创始人，Cobo钱包创始人。

- 江卓尔（涉嫌：提供信息服务，投资，矿业）

莱比特矿池BTC.TOP 创始人，比特币的布道者、矿工和长期投资人，提出了：江卓尔60日累计BTC涨幅指标。

- 许浩扬（涉嫌：矿业，钱包）

许浩扬是 ViaBTC 矿池和 ViaWallet 钱包创始人。

- 潘志彪（涉嫌：矿业，钱包）

潘志彪，币印钱包和币印矿池创始人。

著名投资者

- 李笑来（涉嫌：投资）

比特币早期投资者，著有《韭菜的自我修养》和《大佬的自我修养》两本书。

- 郭宏才（币种：ETHW）（涉嫌：投资，ICO）

网名宝二爷，比特币和以太坊早期投资者，分叉ETH发了ETHW币。

- 杜均（币种：HT）（涉嫌：提供信息服务，投资，交易所，ICO）

HuoBi火币交易所投资者，目前在区块链媒体：金色财经。

- 薛必群（涉嫌：投资）

薛必群，网名薛蛮子，UT斯达康创始人之一，区块链早期投资者。

- 沈南鹏（涉嫌：投资，ICO）

红杉资本中国，曾对P2P项目有投资，曾公开拒绝区块链，后来看到区块链领域可以盈利，才对区块链领域有投资，主要投资项目包括：BCH（比特现金），CFX（树图链），FIL（Filecoin），CTK（CertiK）。

- 徐小平（涉嫌：投资）

真格基金，投资了DDEX.io交易所，后来暴雷跑路了。真格基金也与顺为资本和高榕资本投资了Pionex嵌套量化交易所，目前Pionex在新加坡仍然运营。币安交易所曾发文表示，嵌套交易所是不合规业务。

- 蔡文胜（涉嫌：投资）

美图秀秀，其隆岭资本对OKCoin进行了投资，公司投资比特币。

单纯ICO

- 陈昊芝，王哲（币种：COCOS）（涉嫌：ICO）

触控科技，购买并继续开发了COCOS开源游戏引擎，发了COCOS币，上了币安。

- 陆扬（币种：VET）（涉嫌：ICO）

陆扬，唯链VeChain或VET币，联合创始人兼CEO。

- 帅初（币种：QTUM）（涉嫌：ICO）

帅初，量子链QTUM创始人。

- 达鸿飞（币种：NEO）（涉嫌：ICO）

达鸿飞，Neo创始人，分布科技CEO。

- 姚期智（币种：CFX）（涉嫌：ICO）

姚期智院士是清华教授，图灵奖获得者，曾担任CFX树图链首席科学家。

CFX树图链，曾被红杉资本投资，曾和中国电信，小红书，快手合作，曾标榜自己根正苗红。

CFX已经在币安交易所上市，CFX树图链是联盟链，且没有投票权。

CFX最开始在AWS亚马逊云上运行实验，而后，投资方撤资，一直阴跌，项目团队单方面修改经济模型后暴拉，随后暴跌，因此有项目方控盘嫌疑。

CFX在币安的简介上，踩ETH捧自己，姚期智也常拿CFX的TPS高说事。但是TPS高，常和中心化程度高有关，并不能衡量区块链的去中心化程度和价值。

CFX抄了以太坊的智能合约功能，只是众多以太坊杀手之一，没见过以太坊创始人V神因为众多以太坊杀手的TPS高而改代码。

DeFi 与 GameFi

- 汤洪波（涉嫌：DeFi）

汤洪波是 DeFi 聚合器 DeBank 创始人。

- 王东（币种：LRC）（涉嫌：DeFi，ICO）

王东是 Loopring 路印协议创始人。发了 LRC 币。

- 雷达熊（币种：DODO）（涉嫌：DeFi，ICO）

网名雷达熊，真名未知，代世超、雷达熊、王琦是去中心化交易所 DodoEx 联合创始人。发了 DODO 币，上了币安。

- 代世超（币种：DF）（涉嫌：DeFi，ICO）

代世超，dForce 创始人。发了DF币。

- 韩元桢（币种：MBOX）（涉嫌：GameFi，ICO）

韩元桢是 MOBOX 创始人，MOBOX 是一个区块链游戏平台，连接多款区块链游戏。

MOBOX 上面曾有赌博业务，实际是 NFT 资金盘。

MOBOX 具有复杂的经济系统，发了 MBOX 币，上了币安。

加密货币钱包

- 付盼（币种：TPT）（涉嫌：钱包，ICO）

付盼是 TokenPocket 钱包创始人，发了 TPT 币。

- 文浩（涉嫌：钱包）

文浩，是比特派 BitPie 钱包创始人。

- 何斌（涉嫌：钱包）

何斌是 ImToken 钱包创始人。

- 葛越晟（涉嫌：钱包）

葛越晟，理财钱包 Matrixport 首席执行官。

- Eric Yu（币种：MATH）（涉嫌：钱包，ICO）

只知道是中国人，姓余，网名 Eric Yu，Math Wallet 麦子钱包创始人，具体姓名未知。发了 MATH 币。

- Kevin（涉嫌：钱包，DeFi，ICO）

只知道是中国人，网名 Kevin，BitKeep 钱包创始人，BitKeep 钱包也做了 BitKeep Swap 跨链交易，Kevin 具体姓名未知。

- Veronica Wong（币种：SFP）（涉嫌：钱包，ICO）

只知道是中国人，网名 Veronica Wong，曾是腾讯的大数据安全团队，是 SafePal 钱包创始人，具体姓名未知。

- Jacob，Gary（涉嫌：钱包）

只知道是中国人，网名 Jacob 和 Gary，他们是 HyperPay 钱包创始人。

提供信息服务

- 刘志鹏（币种：BTM）（涉嫌：提供信息服务，投资，ICO）

区块链媒体：巴比特创始人，比特币早期投资者，原来是科幻作家，笔名长铗，巴比特旗下设置有投资机构时戳资本，发了BTM币：比原链，BTM币曾上了币安交易所，后来BTM币一直阴跌，最后从币安交易所退市。

- 陈勇（涉嫌：提供信息服务，第三方授权，嵌套交易所）

陈勇是加密货币量化交易软件BitUniverse创始人。

BitUniverse原来只是做区块链数据与媒体，后来转为量化交易软件。

BitUniverse属于第三方授权，币安交易所认为第三方授权是不合规业务。

后来BitUniverse又孵化了Pionex量化嵌套交易所，总部位于新加坡。

币安交易所认为嵌套交易所是不合规业务。

- 林嘉鹏（涉嫌：提供信息服务）

林嘉鹏曾创立区块链行情平台AICOIN

- 刘洋，余芳（涉嫌：提供信息服务）

刘洋，币看创始人。余芳，币看联合创始人。

- 郭楠（涉嫌：提供信息服务）

郭楠，网名Larry Guo，是MyToken创始人。

- Pxstar（涉嫌：提供信息服务）

Pxstar是区块律动BlockBeats创始人，真名未知。

- Alyssa Tsai（涉嫌：提供信息服务）

Alyssa Tsai是PANews创始人，真名未知。

- ？（涉嫌：提供信息服务）

？是ForesightNews创始人，真名未知。

- ？（涉嫌：提供信息服务）

？是非小号创始人，真名未知。

- ？（涉嫌：提供信息服务）

？是深潮TechFlow创始人，真名未知。

区块链安全

- 钟晨鸣（涉嫌：网安）

钟晨鸣，网名余弦， 知道创宇公司，钟馗之眼，区块链安全公司慢雾科技创始人。

- 顾荣辉（币种：CTK）（涉嫌：网安，ICO）

顾荣辉是区块链安全公司CertiK创始人。CertiK曾被红杉资本投资。CertiK曾发行CTK币种，上了币安。

- 张振宇（涉嫌：网安）

张振宇是极验验证（GeeTest）创始人，很多加密货币交易所都使用了极验验证（GeeTest）作为人机验证方案。

五，币圈有哪些死亡方式?

骗局/欺诈/失误/偷盗/被割

1，交易所跑路 2，钱包被盗 3，DeFi被黑 4，跨链桥被黑 5，币种暴雷 6，量化机器人被黑 7，做合约爆仓 8，追热点被套 9，出金冻卡冻钱 10，稳定币暴雷

11，貔貅盘 12，庞氏骗局 13，金字塔传销 14，资金盘骗局 15，GameFi骗局 16，DeFi土狗盘 17，空投骗局 18，夹子机器人骗局 19，NFT骗局 20，ICO骗局

21，云算力挖矿骗局 22，质押挖矿骗局 23，P2P骗局 24，带单群骗局 25，量化程序骗局 26，卖课程骗局 27，区块哈希值赌博（哈希盘）骗局 28，赌博游戏骗局 29，交易挖矿骗局 30，X2E（X To Earn，边X边赚）骗局

31，第三方授权骗局 32，嵌套交易所骗局 33，私钥碰撞 34，增发盘骗局 35，密码泄露丢币 36，改税点 37，老鼠仓 38，私募预售 39，项目方预挖 40，项目方预分配

六，有关币安Binance和小蚁AntBot使用的加密算法是否安全的补充陈述

1，Binance的对称加密使用的加密算法是——HMAC

1-1，关于HMAC，币安客服的回应

这个是在API上的请求签名（Signature）签名的生成是以密钥（secret key）和请求参数进行生成的。

关于这个签名的生成，可以查看这个文档链接。

https://Binance-docs.github.io/apidocs/spot/cn/#signed-trade-user_data-and-margin-endpoint-security

1-2，关于 Fast API，币安客服的回应

这个是给予第三方平台提供的一个功能。这个是用户同意以币安登录第三方平台并在第三方平台上自动生成的API并进行绑定（以应有的权限设置）。可以查看以下链接。

https://www.Binancezh.jp/zh-CN/support/faq/%E5%A6%82%E4%BD%95%E5%B0%8D%E6%8E%A5fast-api-6aa7e2253c544d91b60746bfd03fd75d

2，AntBot的非对称加密使用的加密算法是——RSA

由《应用密码学：协议，算法与C源程序》知，对RSA算法，有选择密文攻击，公共模数攻击，低加密指数攻击，低解密指数攻击等攻击方式。

在使用RSA的时候，e不能特别小，d也不能特别小。现在建议e至少大于65537，d至少大于n^{1/4}

与RSA算法本身的实际缺陷相比，更多的是操作员错误问题。

使用低级的随机数生成器（RNG）的结果是，它们生成的随机数是很差的质数会导致生成私钥，而私钥更容易受到破坏。

KeyFactor的研究表明：

RSA是安全的，但是在很多情况下，IoT制造商都在错误地使用RSA；

由于分解式攻击，每172个RSA密钥中有超过1个有遭受危害的风险；

ECC是RSA的更安全替代方案；

ECC密钥比RSA小，但更安全，因为它们不依赖RNG；

ECC由于其较低的计算开销而可以很好地扩展；

ECC对量子计算的抵抗力更大；

相关企业和物联网设备制造商都需要在安全性方法上提高加密敏捷性。

3，由上信息，可推出，此次事件可能的攻击原因

3-1，AntBot 使用了低级的随机数生成器（RNG），造成 RSA 加密算法被破解。

3-2，AntBot 没有使用可信任的 RSA 开源库，造成 RSA 加密算法被破解。

3-3，AntBot 自行开发 RSA 加密算法，导致其有漏洞，造成 RSA 加密算法被破解。

3-4，AntBot 的 RSA 参数设置（e不能特别小，d也不能特别小）不符合安全标准，造成 RSA 加密算法被破解。

3-5，AntBot 的 RSA 密钥长度太短，不符合安全标准，造成 RSA 加密算法被破解。

3-6，AntBot 没有及时将落后的 RSA 加密算法，更新换代为 ECC 加密算法，造成 RSA 加密算法被破解。

4，总结：AntBot单方面宣称，“API接口密钥，存储于云服务器，且经过区块链非对称加密RSA算法，理论上无法被破解。”一说，是不真实的。RSA加密算法有很多可能被黑客利用的操作失误和漏洞。

七，有关"翻墙"的法律和科技术语解释

1，"墙"的定义：

防火长城（英语：Great Firewall，常用简称：GFW，中文也称中国国家防火墙，中国大陆民众俗称墙、网络长城等等），是对中华人民共和国政府在其互联网边界审查系统（包括相关行政审查系统）的统称。此系统起步于1998年，其英文名称得自于2002年5月17日Charles R. Smith所写的一篇关于中国网络审查的文章《The Great Firewall of China》，取与Great Wall（长城）相谐的效果，简写为Great Firewall，缩写GFW。

2010年年初，中国信息产业网、《人民邮电报》曾公开报道了，原北京邮电大学校长方滨兴院士的身份，为“中国国家防火墙（GFW）之父”。

来源1：https://zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E9%95%BF%E5%9F%8E（维基百科）

来源2：https://zh.wikipedia.org/wiki/%E6%96%B9%E6%BB%A8%E5%85%B4（维基百科）

注："墙"的这个概念，在当前中国的一切公开的规范性法律文件中，都是不存在的。

2，"翻墙"的定义：

"翻墙"行为是，架设专用网络，进行数据加密，抵御或避免"墙"的网络攻击，并使用中国国家批准的合法互联网物理基础设施，访问境外网站，因此并不是非法行为，并不违法，也不违反相关规定。

3，"墙"的原理：

3-1，"墙"的技术包括：

3-1-1，IDS检测+基于UDP域名解析劫持+DNS劫持+域名污染。

3-1-2，IP地址或传输层端口人工封锁，BGP劫持（黑洞路由）。

3-1-3，TCP RST重置，TCP旁路阻断，中间人攻击。

3-1-4，协议检测→根据流量协议拆包→关键词匹配→封锁。

3-1-5，深度包检测（机器学习识别翻墙流量+直接阻断）。

3-1-6，篡改HTTP响应+对特定网站进行DDOS攻击。

3-2，"墙"的技术总结：

3-2-1，"墙"的运行涉及非法的网络攻击手段，因此"墙"本身是违法的。

4，"翻墙"的原理：

"翻墙"的技术包括，VPN，Tor，Vmess（含ShadowSocks，V2Ray，Trojan），Clash等。

以上技术的手段和目的是，架设专用网络，进行数据加密。因此以上技术，并不是用于侵入计算机信息系统的程序工具。

"翻墙"行为的本质是，抵御或避免"墙"的上述网络攻击，并使用国家批准的合法互联网物理基础设施，访问境外网站。因此"翻墙"并不是非法行为，并不违法，也不违反相关规定。

5，有关"翻墙"是否违法的解释。

5-1，国际出入口信道是物理信道，现行法只规定不允许非法架设物理信道，而翻墙必定使用合法物理信道。

5-2，“墙”的基本原理是：网络攻击或入侵检测。

5-3，“翻墙”的基本原理是：抵御网络攻击或入侵检测，而非网络入侵。

5-4，“个人翻墙访问境外网站”的禁止性规定是不存在的，无论是从技术角度还是法律方面，访问境外网站和境内网站没有任何本质区别。现行法律没有禁止访问境外网站。

5-5，现行法律禁止的是企业违规跨境经营以及无资质企业非法经营网络服务，但与个人访问境外网站皆无直接关系。

5-6，一切翻墙行为都必须使用国家批准的合法国际出入口信道，全球互联网的本来面貌就是所有国家网络基建的互联互通。

5-7，"翻墙"与"墙"的行为没有发生在物理层以及物理信道，个人翻墙亦不是企业行为，因此"翻墙"行为不在相关文件的约束范围内，因此所谓个人的"翻墙"，并不是非法行为，并不违法，也不违反相关规定。

总结："翻墙"并不是非法行为，并不违法，也不违反相关规定，不在相关文件的约束范围内。

6，涉"翻墙"的相关规定文件，汇编，与解释

6-1，国务院与邮电部1996年文件（文件性质：规定，办法，通知）

> 《中华人民共和国计算机信息网络国际联网管理暂行规定》（国务院令第195号）（1996年1月23日）
>
> 第六条 计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网。
>
> 第十四条　违反本规定第六条、第八条和第十条的规定的，由公安机关责令停止联网，给予警告，可以并处15000元以下的罚款；有违法所得的，没收违法所得。
>
> 北大法宝 【法宝引证码】 CLI.2.13908 （现行有效）

> 关于发布《计算机信息网络国际联网出入口信道管理办法》的通知（邮部〔１９９６〕４９２号）
>
> 第二条 我国境内的计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。
>
> 任何单位和个人不得自行建立或者使用其它信道（含卫星信道）进行国际联网。
>
> 北大法宝 【法宝引证码】 CLI.4.14832 （现行有效）

解释1："翻墙"行为是先通过运营商提供的中国服务器的信道与境外的服务器进行的国际联网，然后在通过境外服务器获取网站信息，这并不违反国务院1996年文件第六条，因为并没有建立或者使用其他信道进行国际联网。

解释2：普通个人进行"翻墙"行为，并未也没能力建立，如光缆或微波通信的物理通道，因此不可能违反邮电部1996年文件第二条。

6-2，1998年国务院信息化领导小组文件（文件性质：办法，部门规章，通知）

> 关于印发《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》的通知
>
> （国信［１９９８］００１号）
>
> 第三条 本办法下列用语的含义是：
>
> （三）国际出入口信道，是指国际联网所使用的物理信道。
>
> 北大法宝 【法宝引证码】 CLI.4.19760 （现行有效）

解释3：上述文件规定，邮电部国家公用电信网提供的国际出入口信道是物理信道，现行法只规定，不允许非法架设物理信道，而"翻墙"必定使用合法物理信道。

解释4："翻墙"与"墙"的行为，发生在OSI模型的，传输层、网络层、会话层、应用层，而非物理层，因此不在上述文件的约束范围内。

6-3，工信部2017年文件（文件性质：通知）

> 工业和信息化部办公厅关于深入推进互联网网络接入服务市场清理规范工作的通知
>
> 但随着清理规范工作深入开展，一些深层次矛盾逐步浮出水面，部分企业违规自建传输网络、非法经营传输业务及违规经营跨境数据通信等问题仍较为突出，……（省略）……有关事项通知如下：
>
> 四、各基础电信企业要加强网络资源和用户台账管理，采取技术、管理、法律等措施，防范网络资源被用于非法经营。要配合各通信管理局做好违规线索核查，及时关停被用于非法经营、违规使用的网络资源。
>
> 北大法宝 【法宝引证码】 CLI.4.314373

> 工业和信息化部关于清理规范互联网网络接入服务市场的通知（工信部信管函[2017]32号）
>
> 二、工作重点
>
> （二）严格资源管理，杜绝违规使用
>
> 4.违规开展跨境业务问题。未经电信主管部门批准，不得自行建立或租用专线（含虚拟专用网络VPN）等其他信道开展跨境经营活动。基础电信企业向用户出租的国际专线，应集中建立用户档案，向用户明确使用用途仅供其内部办公专用，不得用于连接境内外的数据中心或业务平台开展电信业务经营活动。
>
> 北大法宝 【法宝引证码】 CLI.4.289332

解释5：相关文件的出台，针对的是企业行为，包括违规跨境经营以及无资质企业非法经营网络服务。但与个人行为，访问境外网站，皆无直接关系，因此不在上述文件的约束范围内。

参考链接：https://Billchen.Bid/jekyll/update/2020/05/02/is-bypassing-gfw-illegal/

原文链接：https://mp.weixin.qq.com/s/cndzW_oXClkSdwOtam0qUw

来源：微信订阅号“不能使用该名称” ForBiddenSpeech，作者为王宇扬

八，有关“C2C交易USDT”的法律和科技术语解释

八，一、什么是USDT?

USDT是Tether公司于2014年7月发行的加密货币,是一种将加密货币与法定货币美元挂钩的虚拟货币。USDT号称严格按“美元本位”发行，每发出一个USDT，都会有1美元存在银行账户，以维持其稳定，因此被称为稳定币。

八，二、是否可以交易USDT？USDT交易违法吗?

USDT是一种虚拟货币，我国不允许平台交易，允许个人之间的场外交易。

虽然针对比特币及其他通过代币融资、投机炒作行为，中国人民银行等部委曾发布《关于防范比特币风险的通知》（2013年）、《关于防范代币发行融资风险的公告》（2017年）（以下简称《公告》）等文件，实质上否定了此类“虚拟货币”作为货币的法律地位，但上述规定并未对其作为商品的财产属性予以否认。

因此，主流观点认为，比特币等“代币”或“虚拟货币”具备权利客体特征，符合虚拟财产的构成要件，虽然不具备货币的合法性，但应赋予其作为虚拟财产或商品的合法属性。

《公告》规定：任何所谓的代币融资交易平台不得从事法定货币与代币、“虚拟货币”相互之间的兑换业务。因此，交易平台无法再参与加密货币与法币的OTC兑换，只能进行个人与个人之间的C2C交易。

八，三、如何交易USDT?

一种是交易所目前的C2C撮合交易，一种是场外OTC交易。

1，C2C交易：目前主流交易平台，虽然仍在加密货币交易过程中发挥作用，但其并不直接进行兑换，而是广泛采用信息平台的撮合机制。平台撮合式交易是指，交易双方在平台上注册为平台服务商，出售方将其持有的USDT的数量以及价格挂在平台上销售，而买方则根据自身需购买USDT的数量以及价格下单，平台则根据双方的买卖情况进行匹配，双方在交易之前不知道对方的身份以及相关信息。在平台匹配成功后，买方按照卖方在平台上的银行账户给对方转款，卖家确认收到款项后，平台会依照订单数量的USDT划到买方账户内，至此，平台的撮合交易模式完成。在整个过程中，平台不直接参与交易，本质上仍属于买卖双方之间一手交钱一手交币的形式。

2，加密货币的场外交易简称为OTC交易（Over-the-counter），其本质是脱离于交易平台进行法定货币与加密货币之间的兑换。

通过QQ群、微信群等场外交易的方式进行这种C to C，C2C的交易，产生了专门赚取USDT差价的“OTC承兑商”。

八，四、USDT承兑商

USDT在不同的交易平台上有不同的价格报价，由此产生了一类专门利用USDT在不同交易平台价格差异来赚取利润的人员，即USDT承兑商。 他们通过以美元实时汇率的比例，收取用户人民币，并兑换给用户USDT。而当用户需要将盈利换成人民币时，他们还提供将USDT换成人民币的逆向服务。通过手续费，交易点差，汇率波动等方式，这些服务商获得相应的巨额收益。

“OTC承兑商”经常通过QQ群、微信群等场外交易的方式进行这种交易，或是在火币网，OK平台上买USDT，然后到其他平台，通过平台撮合C2C交易出售USDT以赚取差价。

“USDT搬砖”是指行为人在两个不同平台低买高卖USDT，以赚取其中差价的交易行为。

八，五、USDT的刑事风险点

自出现以来，USDT的交易额长期处于全球逾千种数字加密货币交易量的最前列，并逐渐代替比特币成为洗钱的主要渠道。在东南亚和非洲被主要用于博彩；在其他资本管制国家，如东欧、俄罗斯，主要用于传销和违法活动。

1. 线下交易缺乏有效的KYC审核

KYC（Know your customer）即“充分了解你的客户”，是在加密货币OTC交易中一种常用的审查资金安全性的方法。

《关于防范比特币风险的通知》要求：“ 提供比特币登记、交易等服务的互联网站应切实履行反洗钱义务，对用户身份进行识别，要求用户使用实名注册，登记姓名、身份证号码等信息。”

而火币网和OK平台虽然支持实名制，但是并没有进行一对一的KYC（了解你的客户）验证。USDT买卖双方无法识别对方资金或USDT来源，交易时对方仅提供一个实名账号、一张银行卡（或微信、支付宝账户）。可能绑支付的是一个账号，然后交易的时候可能被替换成另一个账号，账户信息则是另一个人的银行卡。

而对于线下交易则风险更高，由于缺乏平台的KYC审核机制，如果自己不承担起严格的KYC审核义务，与之进行USDT“搬砖”的对手来自五湖四海，极有可能会是给你“黑钱”或者潜在的违法犯罪之人。

公安部门曾要求火币网和OK平台在交易过程中增加一些视频验证，来加大反洗钱力度，以保证交易者的实名手机账号和实名银行卡是一一对应的。 2020年8月，火币网完成本年度最大的反洗钱风控策略升级，以协助警方反诈、反洗钱的破案工作。

2. 固定交易方交易

目前，虚拟货币交易市场五花八门，交易对手也是良莠不齐，空气币、传销币大量存在，买币不交币也大有人在。因此，从事USDT“搬砖”业务，若能够建立彼此的信任机制，成为固定的交易方，那么交易既高效便利，又省去了必要的担忧。但是，难免会有违法犯罪分子用谎言建立“信任”，利用固定的交易方，大量输入“黑钱”和“黑币”。

作为正常的USDT“搬砖”，交易对手都是随机匹配，自由撮合，并不能形成稳定的交易对手。如果每一次的买币卖币都是有稳定的交易方，而且频繁交易，就打破了“搬砖”的随机性。随机性和自由撮合，本是“搬砖”的“护身符”，但却由于固定的交易，而摧毁了这一“护身符”。

在司法机关看来，在固定的时间、固定的价格与固定的交易方交易，极有可能形成了共谋，否则不可能如此默契。因此，如果是固定交易方交易，也面临极大的风险。

3. 冻卡之后仍然交易

自从“冻卡”行动的开展，不少币圈人被频繁“冻卡”，出现了“冻卡”高潮。其中有部分人，熟知“冻卡”的规则，知道“冻卡”并不意味着构成犯罪，有可能是误冻或者错冻。于是更换了银行卡，仍然进行交易，但这无非是给自己增加了双重风险。
在已经出现“冻卡”的前提下，一方面，自己已经明确知道有卡被冻，那么很有可能是资金出现了问题；另一方面，司法机关已经做出了冻结的强制措施，以实际行动告知其可能涉嫌违法犯罪活动，那么此时应该自行检查风险，暂停交易，如果仍执意而为，就不得不被司法机关推定属于明知，进而以犯罪论处。

另外，无限制的高频大额交易，频繁换卡或换钱包地址交易，也极易让司法机关产生怀疑。

八，六、涉嫌罪名

虽是说个人私下交易自由，但并不代表不被犯罪份子利用作为犯罪工具，尤其是成为洗钱，诈骗、赌博等违法犯罪活动转移资金，支付结算的工具，这就有可能构成犯罪。因为从客观上看，利用USDT接受了转来的资金卖出了币，就是提供了帮助行为；从主观上看，如果明知他人是在进行违法犯罪活动，仍然提供卖币服务，那么此时就会构成相应犯罪的共犯，或者是帮助信息网络犯罪活动罪。

1. 洗钱罪

《刑法》 第一百九十一条 明知是毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪的所得及其产生的收益，为掩饰、隐瞒其来源和性质，有下列行为之一的，没收实施以上犯罪的所得及其产生的收益，处五年以下有期徒刑或者拘役，并处或者单处洗钱数额百分之五以上百分之二十以下罚金；情节严重的，处五年以上十年以下有期徒刑，并处洗钱数额百分之五以上百分之二十以下罚金：（一）提供资金账户的；（二）协助将财产转换为现金、金融票据、有价证券的；（三）通过转账或者其他结算方式协助资金转移的；（四）协助将资金汇往境外的；（五）以其他方法掩饰、隐瞒犯罪所得及其收益的来源和性质的。

USDT交易主要是用来掩饰资金流向，如果资金来源是毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪、金融诈骗犯罪，则涉嫌洗钱罪，如果是其他来源，则涉嫌掩饰、隐瞒犯罪所得、犯罪所得收益罪。

2. 掩饰、隐瞒犯罪所得、犯罪所得收益罪

《刑法》第三百一十二条 明知是犯罪所得及其产生的收益而予以窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；情节严重的，处三年以上七年以下有期徒刑，并处罚金。

USDT交易方如果明知是犯罪所得及其收益而掩饰、隐瞒的，可能涉嫌掩饰、隐瞒犯罪所得、犯罪所得收益罪。

如何判断明知?

《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》第十一条：“（一）多次使用或者使用多个非本人身份证明开设的收款码、网络支付接口等，帮助他人转账、套现、取现的；（二）以明显异于市场的价格，通过电商平台预付卡、虚拟货币、手机充值卡、游戏点卡、游戏装备等转换财物、套现的；（三）协助转换或者转移财物，收取明显高于市场的 “手续费”的。”

3. 帮助信息网络犯罪活动罪

《刑法》第二百八十七条之二　明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

目前网络诈骗形式多样，基于加密货币隐蔽性强、不易追踪的特点，有大部分的网络诈骗平台将骗取的款项兑换成USDT用于购买加密货币，而后进行二次出售后再兑换成为USDT，再将USDT兑换成人民币，从而实现整个诈骗的闭环。对于以经营USDT为业的平台或承兑商，如果未履行严格的审查义务，若无法核实资金的合法来源、无法核实USDT的合法来源而兑换，就有可能被认为涉嫌帮助信息网络犯罪活动罪而受到司法机关打击。

2021年5月12日，杭州西湖区人民法院审理了一起涉嫌非法经营罪、帮助信息网络犯罪活动罪案件，被告人包括币圈大佬赵东等在内的12人。赵东是圈内赫赫有名的“OTC承兑商”，他的审判具有重要的里程碑式意义。据报道，检方在庭审中主要根据其仅履行了姓名+身份证号码的简易KYC审核，且资金主要来自境外博彩平台“跑分”的第四方支付平台交易，进行了诉讼说明，并建议判处三年以下有期徒刑，并处罚金。

4. 上游犯罪（诈骗、开设赌场、非法经营等）的共犯

USDT交易方如果与上游犯罪份子事前存在共谋，仅是分工不同，那么，USDT交易方就与上游犯罪成为共犯。这里所涉及的罪名就很多。

4-1，诈骗罪

根据《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》第四条第（三）款之规定：“明知他人实施电信网络诈骗犯罪，具有下列情形之一的，以共同犯罪论处，但法律和司法解释另有规定的除外：1．提供信用卡、资金支付结算账户、手机卡、通讯工具的；2．非法获取、出售、提供公民个人信息的；3．制作、销售、提供“木马”程序和“钓鱼软件”等恶意程序的；4．提供“伪基站”设备或相关服务的；5．提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供支付结算等帮助的；6．在提供改号软件、通话线路等技术服务时，发现主叫号码被修改为国内党政机关、司法机关、公共服务部门号码，或者境外用户改为境内号码，仍提供服务的；7．提供资金、场所、交通、生活保障等帮助的；8．帮助转移诈骗犯罪所得及其产生的收益，套现、取现的。

4-2，开设赌场罪

据币圈人士介绍，用USDT操作跨境赌博有两种模式：一种赌客直接充人民币，跑分平台的会员兑换USDT；还有一种是赌博平台要求赌客直接用USDT充值，然后平台去提现时，让跑分的人来洗,“现在马来西亚的一些赌博平台就是这么做的"。

如果USDT交易方资金来源于博彩行业，交易方固定，容易给司法机关产生事前串通的印象。因此无论是USDT交易平台还是USDT承兑商在从事USDT交易过程中，均应严格注意风险，避免“瓜田李下”之嫌。

八，七、出罪辩点

1，USDT个人间的交易是合法的。

USDT是类似比特币一样，在我国的法律地位是一种网络虚拟财产，普通民众对这类财产可以依法进行占有、使用、收益以及处分的；我国民众在自担风险的前提下，可以在网络上进行自由交易、买卖，这种买卖行为应当是合法、有效的，而非公安机关认为的涉嫌违法、犯罪。

因此，USDT是作为合法虚拟商品性质，以及行为人在各个平台上正常交易行为合法性，是无罪辩护的前提。

2，平台撮合式交易方式，订单随机匹配，承兑商在交易前客观上根本无法知晓其交易对手的身份以及收取的款项的性质，不可能与对方形成共谋的意思表示，主观上也不可能是明知。

平台的撮合交易，类似于“滴滴打车”订单匹配模式，在平台交易之前，买卖双方的身份都是隐匿的，双方的交易完全由平台进行随机匹配与撮合，行为人在出售USDT时，无法知晓对方身份信息，即使对方客观上确实是通过与行为人买卖USDT时进行诈骗、洗钱等犯罪活动，行为人主观上也不可能与对方进行共谋或者明知对方是犯罪行为而提供帮助。这种随机的撮合模式中，也会在行为人收款的情况有所体现。双方是随机的交易，行为人银行卡往往只有一两笔是接受到了上游犯罪人员的赃款，而不可能是经常性、大量的接受到了赃款，这个客观事实从侧面证明了行为人不可能与对方形成共谋或者明知对方犯罪而提供帮助。

假若这种交易行为被认定为违法犯罪，那么就意味着，在日常生活中，任何商家在收到以犯罪所得支付的消费或者购买商品的款项时，都会被认定为是上游犯罪人员的帮助犯。这将造成日常交易变得极为不稳定，极大的阻碍社会、经济的发展。

3. 行为人以真实身份信息以及银行卡实名注册从侧面也能说明其没有犯罪主观故意。

若是为了违法、犯罪，必然不会用自己实名注册，这样就相当于自己“裸奔”。在故意犯罪中，行为人必然绞尽脑汁切断犯罪行为与自己任何联系，以确保自身不被办案机关查处，而非故意将自身暴露，这才符合日常逻辑。

4. 已经进行KYC审核，有理由相信对方是合法交易。

要求相对方手持身份证、银行卡录制视频，在视频中明确自己的身份，保证资金来源合法正当，并愿意承担任何法律责任，此外还需提供该银行卡的交易流水，保证银行卡的安全性。

通过这种方式，交易所C2C商户可以了解交易对手的信息，应当认定为交易所C2C商户已经尽到了审慎审查的义务，交易所C2C商户为个体，不具有金融机构、司法机关的多种查控系统，无法对交易对手资金安全性有进一步的审查能力。

且交易对手已经以视频的形式提供了身份信息，若该笔交易涉及到赃款，则交易所C2C商户可以马上提供交易对手的身份信息给公安机关，交易对手也难逃法律的制裁，以此可以反推出，交易对手既然愿意做KYC，那么他可以保证他的资金是合法的。

5. 交易价格无明显异常。

USDT作为稳定币，价值相对较为稳定，波动较小。交易所C2C商户通过USDT的买进与卖出，从中赚取几分钱的差价。

随着“断卡行动”的推进，C2C交易被冻结的情况越来越多，火币网推出了蓝盾认证商户，这些商户通常经KYC认证，信誉较高，交易相对安全，因此这样的商户价格相对较高，甚至比一般的商户高出0.05元。但这是因为泰达币市场的交易特性，并不能以此认定交易价格畸高，从而推定商户的主观明知。

参考链接：

https://zhuanlan.zhihu.com/p/399791139