加拿大交易所QuadrigaCX的创始人Gerald Cotten去年12月在印度旅行时意外染病逝世，令人讶异的是他竟然一人掌管了储存整家交易所大部分资产的冷钱包的私钥，一夕之家1.9亿美元的加密资产瞬间石沈大海，这样戏剧化的发展令部分加密货币社群觉得像在看电影，也有人开始怀疑创始人是诈死。

QuadrigaCX没有公开遗失私钥的钱包地址

在私钥遗失、让损失用户上亿美元的资金后，这家交易所并没有将这些存有无法取出的资金的钱包地址揭露。

而创始人Cotten死前两周立下了遗嘱，妥善的安置了他大部分的财产：指定妻子为自己遗产的唯一继承人、将一家合资公司的财产遗赠给了他的姻亲、为两只狗留下了10万加元……

与ZeroNoncense对比特币交易的调查结果类似，在过去三年中热钱包的过剩资金并没有送到冷钱包中。

相反的，存款钱包的资金被发送到两个主要地址，再被发送到几个中心化交易所。此外，Elementus也指出，这些存款钱包资金在非常少量的以太币交易中被转移。这意味着QuadrigaCX希望谨慎且同时不断清算存款钱包资金。

其指出这两个主要钱包的地址为：

0x027beefcbad782faf69fad12dee97ed894c68549

0xb6aac3b56ff818496b747ea57fcbe42a9aae6218

该调查指出到在过去两周内没有资金离开这些地址。这一时期恰逢创始人逝世遗失私钥的消息的流出。然而，根据已发布的死亡证明，这与他在12月9日在印度的实际死亡并不吻合。该单位调查声称，在创始人去世后，这些交易已进入交易所很长一段时间都没有动过。

该调查也声称，发送到交易所的以太币高于QuadrigaCX宣誓书所声称的冷钱包中拥有的430,000枚以太币。Elementus表示：「发送的部分以太币资金转进了一些存款帐户，但大多数已发送到其它交易所，再也没有回来。」

这两份研究皆质疑其交易轨迹，并且怀疑该交易所的可信度。

找到一些冷钱包

BB财经日前报导，在加拿大法院指定监察人安永所发布的报告中，有103枚比特币被「意外」转入这家交易所遗失私钥的冷钱包中。

昨日一位监控区块链网路的人士Decoze在Reddit论坛发表的贴文，指出该日期收到了「多次小额转帐」，共计104.335比特币，几乎与报告中提到的数量大致相同。但自2018年4月以来，以下每个地址都处于非活动状态：

1HyYMMCdCcHnfjwMW2jE4cv9qVkVDFUzVa–收到36.37786282 BTC

1JPtxSGoekZfLQeYAWkbhBhkr2VEDADHZB–收到33.19556316 BTC

1MhgmGaHwLAvvKVyFvy6zy9pRQFXaxwE9M–收到19.54328527 BTC

1ECUQLuioJbFZAQchcZq9pggd4EwcpuANe–收到10.34268585 BTC

1J9Fqc3TicNoy1Y7tgmhQznWrP5AVLXj9R–收到4.87560516 BTC

这是该位人是在论坛中所贴出的区块链数据。

怎么确定这就是交易所遗失私钥的冷钱包？

据密码庞克，出现了一个主密钥可以再生成多个地址的确定性钱包（Deterministic wallets），虽然该钱包的子地址不能拥有独立的私钥；在出现了BIP-32提案的HD钱包后，全名是分层确定性钱包（Hierarchical Deterministic wallets），让主密钥可以包含多个子密钥。