全面概述 EOS 中的密钥丢失情况

原文：https://medium.com/@cryptolions/the-lost-key-situation-in-eos-a-comprehensive-overview-8d4064fd8f6f

问题是什么？

EOS 社区的一些成员丢失或未能接收到自己的 EOS 私钥。自此，他们一直在等待收回资金的方法。

（为了全面起见，还有另一群人也在等待获救方法。这些人从未注册过他们的以太坊密钥，也不想使用 EOS Authority 的后备流程。他们不想使用 EOS Authority 的后备流程的原因很可能是因为他们的 ETH 密钥存储在硬件设备上，如 Ledger，并且所有者不能或不想获得密钥。这个群体可能非常小。）

问题有多严重?

根据一个社区记录丢失的密钥清单有 273 个帐户，其额度总计为 891,361.74514 EOS。

应该做些什么吗?

反对帮助的观点：

- EOS 治理机构或区块生产者（BPs）的工作不是修复用户错误。
- 拯救丢失钥匙的用户将产生“道德风险”，并导致粗心大意的用户无休止的把 EOS 治理机构或 BPs 作为密码恢复者。
- 恢复密钥为恶意攻击者创造了窃取密钥的机会。这超出 BPs 权力的范围，并将引发集中化的担忧。
- 通过 BPs 没有明确或正常管理的账户进行例行交易，我们有可能破坏区块链的感知安全性和完整性。

支持帮助的观点：

- 注册过程有点令人困惑。显然，从注册过程中生成的电子邮件无效时，会有一个空窗时期。

- 我们（EOS 治理/BPs）应该提供帮助，因为我们可以。针对恶意索赔的反措施简单而有效。其范围仅限于从未在 EOS 主网上使用过的密钥。
- 正如 Liberty Block 的 Kedar 所指出的：“没有不利的派别。”

ECAF 案例＃27

12 月 14 日，ECAF 对案例＃27 进行了裁决。它的目的是创建先例。他们要求 BPs 为帐户 *hezdqnjxgmge* 创建新的密钥。在此之后，这个想法似乎通过 ECAF 为其他丢失密钥的案例提供了途径。

只有四个 BPs 支持了这项裁决，并且它已经过期，对于失去了密钥的一些社区成员而言，他们看到在丢失密钥问题上期待已久的 ECAF 的裁决。

虽然该裁决现已过期而未通过，但**批准该裁定**的**论据包括：**

- 社区成员认为 ECAF 是解决丢失密钥和支付 ECAF 费用的正确组织。据社区成员称，151 项 ECAF 索赔已经被提出。有些人（社区估计有 5 到 10 人）已经支付了申请费。我知道一份申请费是 93 EOS。

- （**谣言**）一些社区成员被告知通过 BPs 提交 ECAF 案件。
- ECAF 的裁决是及时的解决方案。丢失密钥的社区成员已等待了足够长的时间。正如 LibertyBlock 的 Kedar 所说：“ECAF 解决方案现已上市。如果用户想要利用它，直到我们的解决方案可用，他们应该可以自由使用。“
- 让 ECAF 从所有丢失的密钥恢复中收取 15%是为 ECAF 组织提供资金的一种手段。
- Ian Grigg（又名 Sun Tzu）从一开始就参与了 EOS 治理，不久前发表了一些观点以遵循 ECAF 的裁决。他的论点包括保持权力平衡，诚信，限制 BPs（BP）责任和分工。

反对通过裁决的论点包括：

- 改变密钥设置了危险的先例。一位社区成员写道：“IMO，遵守这样的命令严重破坏了 EOS 和不可变区块链的定义。仅 1000 个 EOS，ECAF 占 15%（LMAO）。如果执行此裁决，我确定我的 EOS 代币将

贬值超过$ 2,500。此外，为成千上万的这些案件做好准备。你们最好雇用一些新员工。可怕的先例 IMO。”

- “我不认为 ECAF 裁决密钥变更是合法的。”（Michael Yeats EOS Dac）
- 超越范围，正如 Aurora EOS 的 Myles Snider 所表达的那样：“问题在于 ECAF 没有明确的范围。公约规定 ECAF 应该处理的唯一问题是解决争议。让他们从人们那里拿钱并告诉他们，他们可以帮助他们重新获得丢失的帐户，这是不诚实的。既然 BPs 并没有盲目地遵从 ECAF 的裁决，那么他们就会发出含蓄的法律追索权威胁（让你的 GC 接听电话？！）。当他们发出命令说某 BP 必须取消时会发生什么？或者说某帐户的资金应该被注销？由于 ECAF 没有明确的范围，我认为现在意味着 BPs 必须评估 ECAF 决策并进行 15/21 投票。如果 BPs 投票反对代币持有人实际需要的 ECAF 裁决，他们可以为这些 BPs 投票。但是给予 ECAF 广泛的、未定义的权力是非常危险的
- 应关心的是 BPs 不应该使用他们的权力来影响任何个人账户的密钥，除非我们确信我们得到了社区的支持。

以下这些观点由 EOS 42 的 David 总结：

- 公然不相信 ECAF 是系统的仲裁员，所以拒绝遵守。
- ECAF 需要通过公民投票和公约正式批准，然后才能通过冻结帐户。
- 当前这个过程太慢而且难以推广扩展，需要另外一种处理方式。
- 相信这个系统会因错误决策让用户面临带来的风险。

ECAF 向 BPs 发送了被认为是沉重的和权威性的消息：

给 BPs 的紧急消息
这是对前 21 名 BPs 的要求。请安排您的总法律顾问在 12 月 27 日星期四 13:00 UTC 与我本人和下面列出的案件的索赔人进行电话视频会议。前 30 名的其他 9 个 BPs 可以让自己的总法律顾问作为观察员出席。
会议 ID 将在时间前（12 月 27 日星期四 13:00 UTC）提供。
会议主题：ECAF-Ruling-Case-0027-2018-12-14-AR-002
此致，
本·盖茨（Ben Gates）
ECAF 仲裁员

在对他们的语气和严厉的语言进行严厉批评之后，ECAF 软化了他们的语气并重新将会议安排至 1 月 2 日。然后他们完全取消了会议并要求 BPs 提供解释。也许这份文件可以作为解释。

软件方案

独立于 ECAF，正在构建针对丢失密钥情况的软件解决方案。这项工作由几位 BPs 的成员领导，包括：eosDAC 的 Michael Yeates，Liberblock 的 Kedar, EOS Authority 的 Rohan 和 EOS Nation 的 Daniel Keyes。

Kedar 指出：“我们承认 DPOS 正在按预期工作，现在致力于创建一个技术解决方案来帮助用户。”

本视频是关于丢失密钥恢复的软件解决方案主题的启动会议。

一般来说，所探求的过程如下所示：

1. 为了可审计性，创建丢失密钥的链上记录。
2. 确认在 EOS 主网上没有任何密钥处于活动状态。（正在研究最好的验证方法）
3. 允许 ETH 令牌持有者使用其 ETH 密钥签名。

4. 允许积极的 BPs 独立批准没有交易的密钥。

有一个程序性的问题是，通过 msig 批准处理批量的密钥恢复或个别恢复，这是否对 BPs 更好。（这是一个过程和便利的问题，没有重大的政治性后果。）

在作者的预计中，社区面前有两个主要问题：

1. **ECAF 的地位是什么？如果他们被视为合法，那么对丢失密钥的恢复将属于他们的职权范围。**
2. **如果 BPs 采用技术解决方案，BPs 是应该自己主动还是等待公投以确保社区支持这一方案。**

附录：有一个 Change.org 请愿书，有 1726 个签名，要求解决丢失密钥的问题。

附录：对于个人丢失未泄露的 EOS 私钥的解决方案

原文：https://www.change.org/p/eos-block-producers-ecaf-a-solution-for-individuals-with-lost-non-compromised-eos-private-keys

有大量的 EOS 社区成员通过适当的渠道成功注册了主网快照，但遗憾的是忘记了地方，保存失败，或者丢失了他们的私钥。这些人中的许多人拥有一种手段或机制来证明他们是这些（未泄漏）“丢失密钥”账户的合法所有者。此外，我们已经把它集中在 Telegram 群组中并与区块生产者（BPs）沟通，希望找到解决我们问题的方法。我们的理解是，一些 BPs 已花时间为未泄露的、丢失的私钥问题创建可行的解决方案，但如果没有 ECAF 的协助或批准，这个新流程就无法实施。

另外，我们要承认，由于其状况的时间敏感性，高风险性，密钥被泄露（被网络钓鱼，被诈骗，被盗等）的个人优先于我们的情况。与此同时，**我们衷心地请求，获得一些保证以确保我们的问题将在适当的时候有效直接地解决。**我们理解在分散的平台上提供此类保证的困难 —— 特别是在公约和 ECAF 的角色处于不稳定状态时。在重新制定公约中也许我们的特殊问题和潜在的解决方案对直接地解决问题有价值。无论如何，我们只提供支持，并感谢那些负责为 EOS 区块

链提供一套新指南和“结构”的人。（还应该注意的是，我们认识到，未泄露意味着安全，并且能够在处理更大问题时有不逾矩。）

我们还要感谢“EOS 911”和“EOS 官方丢失私钥”Telegram 群组成员的分享，这些成员由于掩码、“多重 tx 故障”以及其他不幸的受害者而导致丢失了私钥。我们的理解是，我们的解决方案将在一定程度上转化为对它们的解决方案。

最后，感谢所有花时间阅读我们请愿书的人。最后，我们想要的只是能够有效地重新加入我们认为足够强大的东西，以便投入时间和金钱。我们登上了船是因为我们在区块链中看到了这样的潜力，这些区块链能够为丢失的私钥恢复资金，以及其他有前途的功能。与此同时，我们并没有忘记为了实际制定这种能力的程序而固有的时间需求。与此同时，我们希望得到一些承认，甚至可能是一项计划。

EOS 官方丢失私钥群组：https://t.me/joinchat/I1ahM0iAS4M-_l0QplVh4g