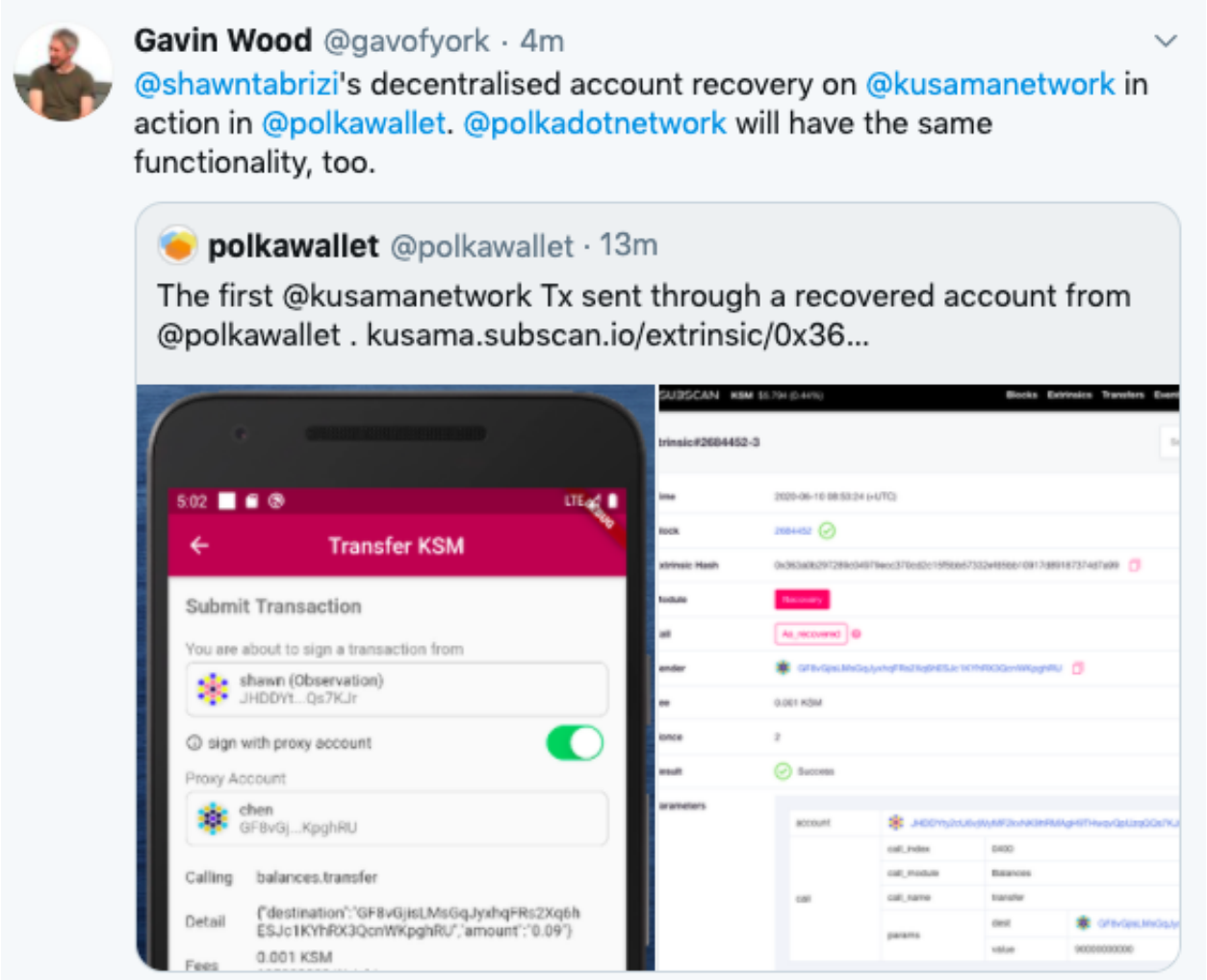
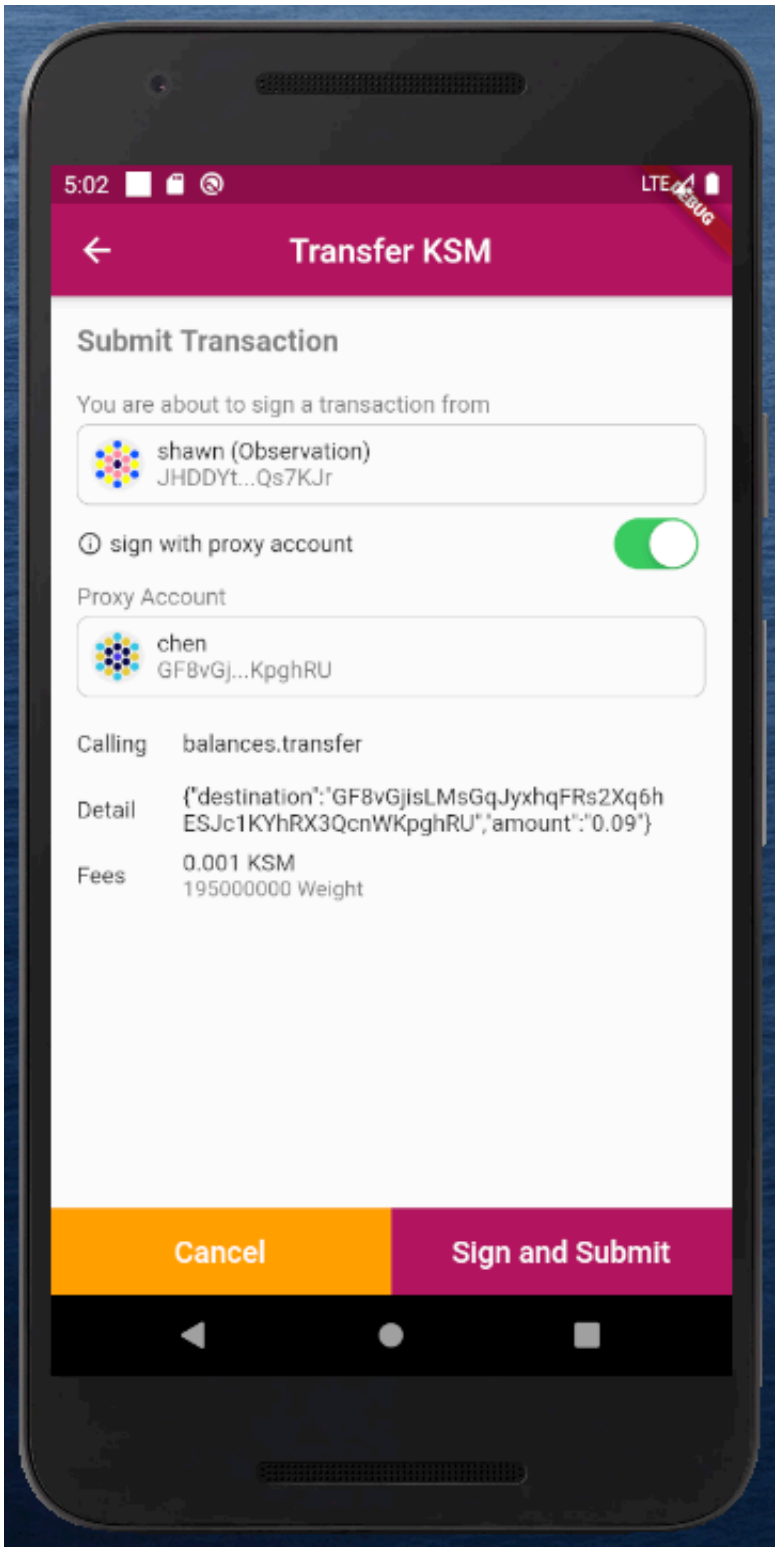
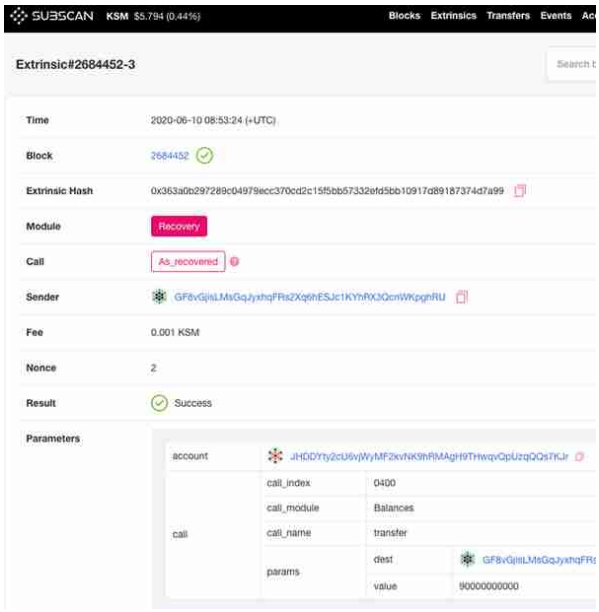


*twitter.com

6月10日，Polkadot 联合创始人、Web3 基金会主席 Gavin Wood 博士转发 Polkawallet 官方推特并称 Polkadaot 网络也将集成社交恢复账号功能，Polkawallet 开发团队成为 Kusama 网络中首个完成社交恢复功能集成的移动端钱包，Acala 网络同样集成了 Substrate 的社交账户恢复模块，所以 Polkawallet 已为波卡 DeFi 生态用户带来私钥保护伞。


5:02
LTE
DEBUG
Transfer KSM
Submit Transaction
You are about to sign a transaction from
shawn (Observation)
JHDDYt...Qs7KJr
sign with proxy account
Proxy Account
chen
GF8vGj...KpghRU
Calling
balances.transfer
Detail
{"destination":"GF8vGjisLMsGqJyxhqFRs2Xq6h
ESJc1KYhRX3QcnWKpghRU","amount":"0.09"}
Fees
0.001 KSM
195000000 Weight
Cancel
Sign and Submit



*zhihu.com

社群里经常能看到软件更新之后找不到账户，忘了保存私钥和助记词的求助信息，Substrate 的 Social Recovery pallet 为此而生，它让你可以通过多个好友来恢复你的区块链账户，恢复原理类似于微信密码可以通过好友来恢复。

Substrate Social Recovery 是什么？

Substrate Social Recovery 基于多签钱包的 M-of-N 社交恢复工具。它允许用户在私钥或其他身份验证机制丢失时恢复其帐户。Substrate 最值得称道一点是能让用户在冗杂的区块链公私钥对中解脱，直接在用户选择的身份验证机制中添加恢复模块。简单来讲就是你可通过指定其他几个用户验证来帮助自己再次获得账户的使用权。

在 Substrate 社交恢复功能中，用户可以通过设置好友总数、最小好友阈值和延迟时间来帮助自己恢复账户。最初的押金数额与每人最多可关联好友账户数是由 Substrate 开发人员来设定，后续该两个参数可通过链上升级模块自动更改。

Polkawallet 私钥社交恢复实现步骤

步骤 1：设置恢复配置

用户最多选择 N 个信任的朋友

用户选择阈值 M，建议大于7/10

用户为恢复进程选择最小延迟时间，建议 6 个月至 1 年

用户存入可退还的配置押金

步骤 2：启动恢复进程

用户创建新帐户

用户用足够的资金为这个新帐户支付恢复保证金和交易费

用户通过声明丢失的帐户和带有存款的新帐户来启动恢复进程

用户联系朋友验证你的恢复请求，至少需要有 M 个朋友发送验证

等待延迟期过去，最后使用新账户声明代理使用丢失的账户

完成这些步骤后，你现在可以使用你丢失的账户了。恢复模块允许你访问所有其他模块。这样，如果恢复模块是在链上实现的，那你正在使用的区块链 runtime 配置的每个模块都不需要进一步配置。

步骤 3：清理旧账户

关闭恢复进程，以退还押金

删除恢复配置，它将退还另一笔押金

通过恢复模块调用其他模块，例如解绑、删除身份信息

最后，把你所有的钱从丢失的帐户转到你的新帐户

如果有人恶意恢复我的账户怎么办？

可能会出现这样的情况，即使你的账号没有丢失，但会有恶意黑客试图抢走你的账户进行“恢复”，因此从恢复机制上 Substrate Social Recovery 设置了保护措施来防止该情况的发生。

首先，恢复的启动需要最低阈值数量的好友批准，简单的理解就是你规定范围内的朋友们都同意才可以进行下一步。那么，如果黑客冒名顶替诱骗你的朋友，多半这里你就会被朋友告知，但即使这样他也成功了会怎样？

如果有足够的朋友批准启动了恢复进程，黑客仍然需要等待你设置的延迟时间过去才能转移你的资金。但是，在此期间内你只要登陆并检查账户，就可以立即取消并且获得黑客账户内的存款，所以如果你能够及时发现并且抓到黑客，他们就是一个蜜罐啦。

所以，当你注意到有人恶意恢复，建议你更改朋友群并删除那些容易上当受骗的朋友，并且定期更新朋友列表。

社交账户恢复对于 Acala 用户来说意味着什么？

起初对于私钥的社交恢复最早只是一种设想，以太坊创始人 Vitalik Buterin 在内的开发者们只是将社交恢复功能当作是一种社会实验，早些年手机制造商 HTC 的 Exodus 也有类似的社交密钥恢复机制，但用户仍然无法通过支付费用来确保其他人保管好自己的密钥。

随着 Polkawallet 已在 Kusama 网络中完成首次 Substrate Social Recovery ，同样的功能也可在 Acala 网络上使用，确保用户能够在安全稳健的金融环境下使用跨链 DeFi 产品，让用户私钥的整个生命周期连接到现实社交生活，彻底摆脱私钥丢失的烦恼。