11月19日，针对FTX事件，神五发文题为&quot安全的CEX:偿付能力的证明&quot，讨论了使交换更接近不可信的尝试的历史，这些技术的局限性，以及一些新的更强大的想法。这些想法依赖于ZK斯纳克和其他先进技术。

V神说使用ZK-斯纳克可以提高隐私性和鲁棒性，把所有用户&#039；存放在一棵大树上。并且用ZK-斯纳克证明了树中所有的余额都是非负的，加起来都是一些声称的值。如果我们给隐私加上一层hash，提供给每个用户的Merkle分支就不会泄露任何其他用户的余额。

此外，我们不&#039；t只是想证明交易的资金全部偿还给了用户，但也要防止交易所完全偷走用户&#039；资金。v表示，理想的长期解决方案是以自托管为主，辅以多重签名、社会回收钱包等技术，帮助用户应对突发事件。。短期内，有两种明确的选择：比特币基地等托管交易所和Uniswap等非托管交易所。

最后，V说，在短期内，交易所分为两个明确的&quot类别&quot:托管交易所和非托管交易所。今天后一类只是DEXes，比如Uniswap。将来，我们还可能看到带有&quot受限&quot加密，用户资金保存在类似于validium智能合约的东西中。我们可能还会看到半管理的交易所。我们信任他们的法定货币，而不是加密货币。

这两种类型的交换都将继续存在，提高托管交换安全性的最简单的向后兼容方法是添加保留证书。这包括资产证明和负债证明的组合。。为双方达成良好的协议存在技术挑战，但我们可以也应该尽可能在这两方面取得进展，并尽可能开放源代码软件和流程，以便所有交易所都能受益。

从长远来看，V神希望我们越来越接近所有交易所都不被管理。，至少在加密方面。钱包恢复将会存在，而且可能需要为处理小额交易的新用户和出于法律原因需要此类安排的机构提供高度集中的恢复选项，但这可以在钱包级别而不是在交易所本身内完成。