2010年，以太坊创始人维塔利克布特林(VitalikButerin)在《魔兽世界》中有一个术士账号。有一天，暴雪决定裁掉术士&#039；的作用，并移除生命虹吸法术的达摩伤害部分。他哭着睡着了而在那一天，他意识到集中式服务器会带来怎样的恐怖，于是决定退出，并创建了去中心化的网络以太坊。2022年11月，FTX，世界&#039；美国最大的衍生品交易所被曝盗用用户资金&#039；资金，其创始人SBF被巴哈马警方逮捕。，准备移交美国审判。

从13年前莫名其妙被暴雪的背刺中的术士玩家到今天维权的FTX受害者。我们越来越意识到句子&quot不是你的钥匙，不是你的硬币&quot:即使有第三方审计/监管机构，集中式服务器仍然可以随意篡改和粉饰数据，但在去中心化的网络上。链条上的账本都是透明的，不可篡改。只要我们有自己账户的私钥，我们就对自己的个人资产有绝对的控制权。

去中心化是美好的，但代价是什么？

我们生活在区块链网，是个人资产的第一负责人。。当大部分用户选择链上钱包的时候，最关键的权衡就是我愿意为我的资产承担多大的风险和责任。以传统金融机构为例：

回到web3，我们有两种方式在web3中存储资产。、托管钱包和非托管钱包，但在此之前，我们需要简单介绍一下钱包的原理：

账户的生成就是创建私钥的过程。在以太坊，有两种类型的帐户：EOA帐户(外部拥有的帐户)、外部账户)和合约账户(通过EOA账户部署在链上的智能合约):

以EOA账户为例，

3。创建帐户后，如果没有私钥的参与，我们就不能参与链上的任何活动。

在去中心化的网络中，不存在像银行这样的信托机构。为了在两个节点之间达成交易，需要实现零信任的安全交易机制。

Let&#039；假设小明和小红希望做笔交易。一种创造交易的方式是小红声称小明给了他一万元，显然不可信；

还有一种创建交易的方式：小明声称自己给了小红一万元，只要能验证这个说法确实是小明所为。而小明真的有一万元，那么交易才算有效。

？

钱包中的一切都是围绕私钥构建的。钱包本质上是1。创建私钥，请按2。保留私人密钥，请按3。使用私钥和4。备份私钥。5.恢复私钥的工具。目前主流的私钥备份/恢复方案是助记符，即注册钱包时出现的12/24字组合：

因为私钥是我们与区块链网络交互的唯一凭证。我们的责任是保管好我们的钱包私钥和助记符。创建账户最安全的方法当然是在离线环境下，通过运行随机数(私钥)和SHA256算法生成自己的地址，但这个门槛无疑太高了。，不适用于大多数用户。所以在钱包的选择上，用户需要考虑三点：安全性、门槛、反审查：

以硬件钱包为例，黑客只能获取用户&#039；的私钥，通过钓鱼或离线窃取

。

用户在Metamask的注册过程中需要记录12个助记符，更换设备时需要重新输入12个助记符，而币安的兑换注册和设备更换登录则可以通过一键邮箱登录完成

。

如果钱包app会保存用户导入的助记词并上传到服务器，黑客就可以窃取用户&#039；破解了服务器。即使没有黑客攻击，也存在斜坡项目方自盗，无法抵御审查的可能。

有两种主要类型的钱包：非托管钱包和集中式托管钱包。

a.以主流钱包MetaMask为例。元掩码是一种非托管(或自我管理)的加密货币钱包。。非托管意味着元掩码不&#039；不存储任何有关钱包的数据，但私钥数据在本地浏览器或移动应用程序中。当用户需要在链上签名时，Metamask会从本地文件调用私钥进行签名。。但是，如果用户&#039；的私钥和助记符丢失/被盗，元掩码将不会帮助用户找回它，并且用户&#039；s资产将永远失去

B.公认最安全的硬件钱包(如账本)。，使用硬件设备离线生成私钥和钱包地址，然后将地址的公钥导入到Metamask之类的web钱包中，需要签名时，由Ledger硬件离线确认。因为私钥完全脱离了互联网，黑客很难窃取硬件钱包中的私钥。但如果用户丢失助记符或被钓鱼，硬件钱包的保护功能也将为零，用户&#039；美国的资产仍然会被窃取。

交易所钱包，如比特币基地/币安，采用托管钱包的方式，不同的是比特币基地显示的账户不是用户&#039；自己的私钥。，但只是比特币基地程序中显示的会计数字而不是以太扫描上显示的链条上的资产，可以理解为用户信任比特币基地，将资产

委托给比特币基地，而不是自己拥有。因此，coinbase&#039的账户可以&#039；t与Uniswap等dAPP交互

一般来说，在托管钱包中，项目方代为保存助记符，注册和恢复钱包的门槛较低，但钱包的安全性取决于项目方而非用户本人。，且项目方对钱包有实际控制权；非托管钱包的助记符掌握在用户手中，注册和恢复钱包的门槛高，但安全性和反审查性高。

随着WEB3的不断发展，越来越多的需求和应用场景出现。链家的生态正在蓬勃发展，尤其是2021年，DefiSummer吸引了大量以前只在交易所交易的用户将资产搬到链家。截至2022年3月，MetaMask月活用户已达3000万。与此同时，作为最主流的助记符账户恢复方案，助记符成为了黑客的主要攻击目标：对于普通用户来说，最常见的钱包被盗事件就是将助记符复制到剪贴板上，或者从钓鱼网站窃取本地存储的私钥文件。

以Metamask为例，黑客可以在两个地方获取保存的助记符和私钥：

a.钱包创建后，用户需要妥善保管生成的助记符，一般建议用纸笔复制在白纸上，妥善保管。但是有些懒人会用剪贴板复制粘贴保存在doc文档甚至微信聊天记录中。

B.如果黑客在用户身上安装了恶意软件&#039；手机/电脑，监控用户&#039；的剪贴板在任何时候。您可以窃取刚刚创建的私钥。比如QuickQVPN就被曝抄袭用户&#039；的剪贴板窃取记忆术。

a.同时，Metamask一般会对私钥进行加密，并保存在创建钱包的本地设备中，以便随时调用。，如果是Chrome上安装的Metamask插件：

一、存储位置在Windows上，Metamask的存储地址&#039；的私钥是

。

C:\Users\用户名\AppData\Local\Google\Chrome\USERData\Default\Local扩展设置

kbihfbeogaaoehlefnkodbefgpgknn.

于MacAufdemSpeicherort:库

应用程序支持

Google

Chrome

Default

LocalExtensionSettings

nkbihfbeogaeaoehlefkodbfgknn

b.即Metamask的安全性取决于Chrome的安全性。一旦Chrome的防火墙被黑客攻破，黑客可以获得用户&#039；s地址私钥并转移所有资产。这也是硬件钱包在安全性上优于Metamask等插件钱包的原因。[XY002][XY001]除了元掩码，一些非托管钱包可以&#039；甚至没有达到很高的审查阻力。比如Solana身上的Slope钱包被偷的时候，Slope&#039的移动应用程序在创建幻影钱包时通过TLS向他们的哨兵服务器发送助记符，然后这些助记符以明文形式存储。这意味着任何可以访问Sentry的人都可以访问user&#039的私钥。

此外，还有更多钱包安全事故值得我们反思：

沈波&#039；钱包被偷是记忆术的泄露。被盗时使用的钱包是TrustWallet，被盗金额包括约3823万USDC，1,607ETH，72万USDT，4.13BTCs。

Profanity旨在帮助人们生成具有特殊视觉效果的帐户，例如以特殊字符开头或结尾的帐户。另一方面，一些开发人员使用它来生成以许多零开头的帐户。

获得第一个32位私钥种子private

Profanity会通过固定的算法反复迭代这个私钥，以便与所需的账户地址发生冲突。，高达200万次(数值来自1inch披露的文章)。当PublicKey已知时，我们可以通过枚举SeedPrivateKey和迭代器来获得SeedPrivateKey。计算量大概是2^32乘以200万次，计算能力强的显卡几天甚至几个小时就能完成。

根据慢雾的调查报告，黑客地址(0xf358.7036)已经获得了ParaSwapDeployer和QANplatformDeployer的私钥权限。。黑客从ParaSwapDeployer提取了1000美元，作为测试在QANplatformDeployer的地址来回转账。我们使用AML平台来分析0xf358.7036并且发现黑客还窃取了SolaVerse部署者和其他几个昵称地址。到目

前为止，黑客已经窃取了超过17万美元。

黑客发明的公司没有&#039；不存在。勾搭上了阿西&#039；通过Linkedin和WhatsApp，用新的工作机会引诱他，安排面试，最后提供优厚的待遇，但offer文件有毒，所以他成功黑进了Axie&#039s系统。，窃取工程师部署合同的EOA地址私钥。

助记符方案不仅是黑客的主要目标，也是阻止新用户进入WEB3的高门槛。

留着一张写着12个字的白纸听起来很不靠谱也很unweb3:我们憧憬着生活在元宇宙的未来，但我们的账户安全却依赖于宋朝发明的一张白纸。迄今这两步足以让大部分web2玩家望而却步。毕竟在web2的世界里，大部分注册流程都可以使用google账号/ios账号一键登录。

无需记忆单词的帐户恢复新方案

为了降低钱包的门槛，吸引更多用户进入WEB3，我们需要使用Web2这样的社交账号登录方案，同时又不失钱包的安全性和反审查性。因此，我们需要一个更方便、更安全的账户恢复方案。现在所有的讨论都指向一个终点：背单词的无奈。目前实现无奈识记的方案有两种：MPC方案和社会恢复方案。

可以理解为MPC是一个3FA，每个认证方法持有一个密钥片段。门锁没有一把钥匙。当其中一个密钥片段丢失时，用户可以通过其他验证方式找回丢失的密钥片段

目前通常将社交找回和账户抽象钱包并列讨论。应该注意的是社会恢复方案是智能契约的一个标准和功能，由EIP-2429在2019年提出，意思是用户可以通过监护人改变契约的控制私钥；最近讨论的EIP-4337是关于帐户抽象的讨论。在下一章中，我们将讨论

MPC方案是在创建EOA钱包时联合创建私钥片段。2019年，论文《基于安全多方计算的两方椭圆曲线数字签名》发表在CRYPTO2019。，正式把MPC的实现带入大家&#039；的视野。MPC是安全多方计算。

MPC方案实现了账户的创建、使用和保存。备份和恢复中没有完整的私钥。通过多方联合生成/持有私钥片段和&quottoutofn&quot，比Metamask等单点生成/持有私钥钱包更方便。。安全性和防审查性：与传统助记符方案相比，大大提高了用户的安全性，甚至可以媲美硬件钱包[XY002][XY001]A.无私钥/助记符：在钱包生成过程中，各方(钱包项目和用户)通过MPC生成私钥片段，整个过程中从未出现过完整的私钥，可以理解为MPC是一个真正的没有私钥的钱包；

b.黑客攻击的成本大大增加：即使黑客入侵用户&#039；的本地设备，他只能获得私钥片段。黑客只有掌握了钱包端服务器用户的本地设备，才能盗取用户&#039；的财产。

社交登录：用户可以通过邮件等认证方式在MPC钱包上创建账户(假设MPC钱包采用2/2签名方案，即可以同时使用两个私钥片段进行签名)。

集中式组织(钱包/备份设备)只持有账户私钥的片段，无法控制用户&#039；的账户。

智能合同帐户上部署了社会恢复方案。智能合约钱包可以理解为部署一个合约，用于管理链上的资金与EOA帐户。与普通智能合约一样，部署者的EOA钱包可以控制智能合约。EIP-2929提出两年后。2021年，Vitalik在论坛中首次提出了社会恢复的钱包应用案例：

a.创建私钥

账户抽象钱包在私钥的创建上与Metamask没有区别。

B.保管好私钥。

因为控制合同的EOA钱包仅用作&quot签名私钥&quot并且控制权可以通过监护人转移，用户不需要专门保存助记符。

c.使用私钥

合约钱包也是转账/交易。，因为需要调用合约，所以会比MPC钱包和传统钱包贵；

还因为是看涨合约。因此，USDC/USDT等非本地令牌(例如，ETH是用于在以太坊上支付燃气费的本地令牌)支持支付。这无疑将大大降低Web3中新玩家的交互难度：原则上，项目方在同一交易中将USDC互换转换为ETH后，将代用户缴纳气费。

D.备份私钥

帐户抽象wallet的私钥备份步骤被替换为&quot卫报&quot，但是，这是违反直觉的，而且成本很高：

用户在使用web3时，想第一次注册钱包，但是需要在web3中找到三个已经有EOA

钱包的信任好友。让他们交煤气费成为他们的监护人；

如果用户想补偿他的朋友&#039；的油费并用新创建的钱包进行三次转账，就会创建一个钱包，油费一共需要给六次。，而MPC钱包创建一个账户是没有成本的。

E.恢复私钥

如果用户丢失了签名密钥，此时可以申请社会恢复功能。用户需要联系他们的监护人。，让他们签一个特殊的交易(用户或监护人交燃气费)，把钱包合同里注册的签名公钥换成新的签名。这就简单多了：监护人可以访问一个网页，比如security.loopring。，查看恢复请求并签名。

然而私钥的安全性并没有达到MPC钱包的高度：

合谋：如果某些用户知道自己是某个恢复的一部分，可能会对执行恢复攻击感兴趣；

目标攻击：外部代理可能知道恢复的所有者，瞄准执行恢复攻击所需的最薄弱点；

一般暴露：如果攻击者试图感染大型用户&#039；基本的环境依赖性并获得对多个身份的访问，，或者在恢复过程中可能对未受影响的用户产生副作用。

MPC方案V.S.社会恢复方案：安全性、阈值和反审查

有了无奈的记忆账户恢复方案，我们可以期待新一代的Web3钱包。，即可以用邮箱注册登录的钱包。现在我们选取了MPC钱包和账户抽象钱包这两个具有代表性的项目进行分析：两者都达到了用户访问中无奈记忆的低门槛，我们从安全性和反审查方面对其进行了评测[XY002]。

在MPC钱包中，防审查彻底且方便的Bitizen钱包采用2/3TSS方案。让&#039；s分析一下钱包的安全性和反审查：

a.创建

。

为了实现强审查，用户在完成钱包注册后，可以使用第二设备通过蓝牙备份私钥片段，采用2/3TSS方案：Bitizen服务器、用户本地设备、用户第二设备。b.保管

因为在创建钱包时没有生成完整的私钥，所以没有助记符：用户&#039；的Bitizen帐户将与用户&#039；用户只需登录邮箱即可正常使用Bitizen钱包。c.使用

用户可以通过人脸识别认证获取存储在Bitizencloud的私钥片段和存储在本地设备的私钥片段并签名(2/3)；

第二设备通过蓝牙备份私钥碎片时，完全可以离线保存。平日里根本不需要(签名只需要Bitizen&#039s服务器和用户&#039；主要设备完成)。[XY002][XY001]D.备份

将本地私钥碎片备份给用户&#039；s云盘；

用户需要更换设备登录时。，只需要通过邮箱和人脸认证，Bitizen就会要求用户从云盘恢复私钥碎片的备份。e.还原同样，当用户&#039；s设备丢失/误删除Bitizen本地文件，私钥碎片可以通过云盘恢复；

当用户可以&#039；t即使登录云盘，Bitizen也会通过服务器和用户上的私钥片段重新计算私钥片段&#039；的第二个备份设备，以便用户可以恢复正常使用。

三分之二的TSS方案允许用户对自己的钱包有绝对的控制权(三分之二的私钥片段在用户&#039；hands)，即使Bitizen破产或跑路，用户仍然可以正常行使对钱包的控制权。

在交易中，，可以使用钱包支持的任何代币(主流、高流动性代币)支付加油费；

在私钥的存储中，采用MPC(2/2)和TSS技术，以分布式的方式生成私钥。因此，私钥不存在被黑客在单点获取的可能性。——私钥分为两块，一块存储在Unipass的服务器上，另一块存储在用户&#039；的本地设备；

低阈值-

高适用性

低门槛钱包不是钱包应用的终结，目前的Web3基础设施与Web2的传统金融还有一定距离。Visa提供的自动扣款和定期自动支付功能给用户带来了极大的便利。不过在以太坊还是很难实现的。帐户抽象帐户可能是下一个高应用区块链钱包叙述：签证发表文章&quot自助保管钱包的自动支付&quot。，探索使用账户抽象钱包Argent在星网网络上实现自动可编程支付，让用户使用自主管理的钱包自动支付，无需每笔交易签字。以及账户抽象钱包是如何实现的？这个概念其实由来已久。

随着EIP-4337的提出，账户抽象的话题又回到了每个人身上&#039；的视线。社会恢复方案和账户抽象(使用智能契约作为EOA钱包，即账户抽象)在EIP-1271之前已经提出。，而Argent等钱包已经在StarkNet等Layer2完成了落地应用。和最近社区讨论的EIP-4337方案(账户抽象)有什么区别？

从2015年的EIP-86到最新的热点EIP-4337，开发者的核心思想围绕着&quot合同是钱包&quot，帐户抽象使用户能够以直观的方式与主网络进行交互。从而使用户能够准确控制账户的密钥权限。。因为已经规定了EOA账户的代码，无法对EOA钱包进行模块化、功能化的设计，比如增加批量转账/社会回收等功能，所以大家把突破口放在了智能合约上。。与EIP-4337最接近的提案是EIP-2938，它也定义了一个新的智能契约操作协议，但需要在共识层面进行修改，所以开发者很难维护。EIP-4337的主要创新在于主网络不需要进行共识级的协议变更。

毕竟从2018年到现在，Argent已经完成了5620万美元的融资。经过四年的发展，它只有一个7.4w的地址：正如defi崛起后，币圈用户从交易所转而使用Metamask挖高APY矿，造就了Metamask的崛起。目前智能合约钱包的热潮还需要一个新的催化剂；[XY002][XY001]目前Argent上的用户存款没有融资金额多

但是随着以太网主网账户抽象的提出，意味着Argent用户可以从StarkNet无缝连接到以太坊主网，这个过程中点燃的火花也值得我们期待。

细化权限控制：细化EOA的单一签名权限：

你好，你好、自动转让合同使用权

多样化的燃气支付方式：由他人或任何代币支付

自动扣款/自动退款

老生常谈，web2用户有48亿。web3的用户数量在22年里刚刚超过1亿，我们仍然处于区块链发展的早期野蛮阶段。

回到文章开头的问题：&quot我愿意为我的资产承担多大的风险和责任？"你能不记得我的私人钥匙吗？，还要保证钱包不丢？

我一直听到传统VC的疑问：有没有什么场景是只有web3能做而web2能做的&#039；t？我们认为Web3钱包是传统Web2的例子之一：只有在Web3的去中心化网络中，我们才能期待一个满足反审查、安全性和用户体验要求的好钱包，用户不必承担风险或责任。这个钱包出现了。也是47亿Web2用户拥抱Web3未来的重要基础

：钱包不仅是Web3的第一入口，也是连锁域名(如ENS)和灵魂有界令牌。没有安全的钱包环境，Web3乐高的搭建就没有坚实的基础。我们需要更认真地思考。熊市出手的机会不多。MPC向我们展示了EOA钱包的未来，它更易用，更安全，可以适应目前所有的EVM连锁店。智能合约与dAPP连接还有很长的路要走，社会恢复计划目前也在看鸡肋。然而，智能合约的未来可能性让人充满期待。我们想赌谁赢？我们将用真金白银交上这份答卷。

2022年是加密货币黑暗的一年，但我们仍然相信未来是光明的。我们是魔兽世界中觉醒的术士。我们希望创造一个没有人能夺走我们生命的世界(除非提案被投票)。