KCon

有关Web3与DID的思考
资金追溯和地址画像的区块链安全应用

Plume – Bitrace 安全研究员

+1 进阶，
护航未来

KCon

+1

CONTENTS

目录

KCon

+1

DID 在区块链生态中的前景

KCon

+1

区块链地址 ≈ DID

区块链地址也可以看作是一种DID标识符的早期雏形，但其无法进行拓展或自定义使其应用场景受限。

DIDs解决了实体在网络中进行去中心化映射的问题

在现实资产数字化交易场景下，通过部署DIDs解决方案, 买卖双方可以在服务、租赁、质押等任何交易市场里，验证资产的真实性和交易对手对该标的的所有权。

W3C的DID定义尝试将去中心化标识从链上带到链下

DIDs为如何对去中心化数字资产的标识、管理和使用提供了统一的解决办法。

尝试改变由中心化授信为核心的隐私管理办法

不再依赖中心化认证等方式来获取权威性，任何人都可以通过DID标识符来辨别、追溯和验证数字资产的源头。

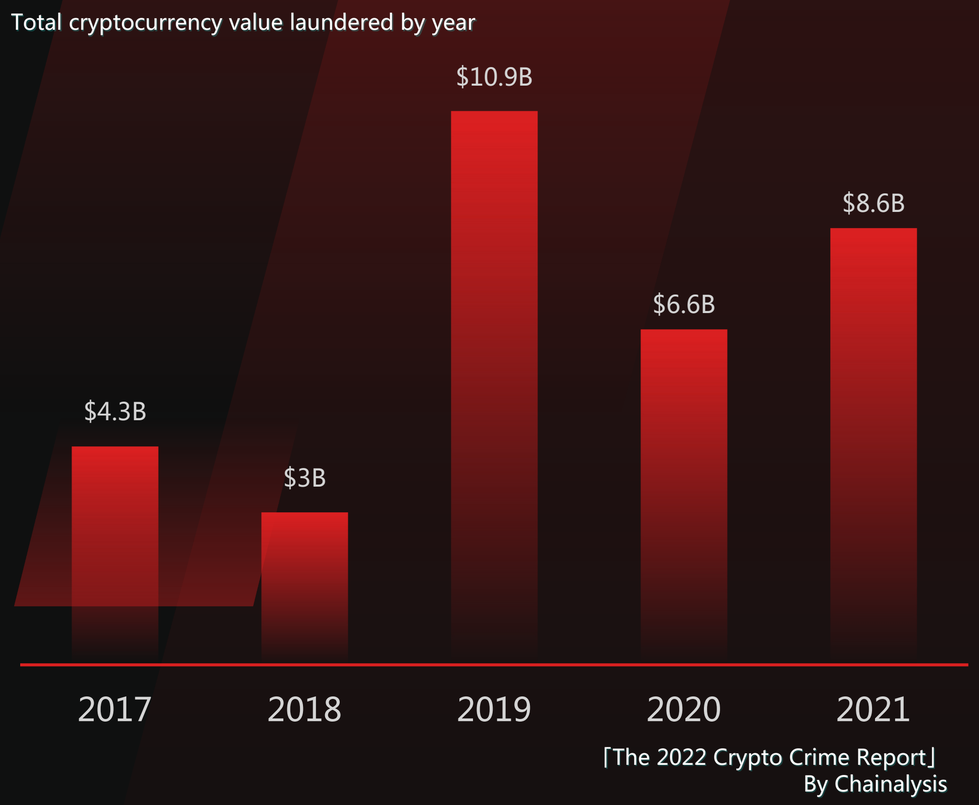
KCon

+1

区块链的安全问题

KCon

+1



「The 2022 Crypto Crime Report」
By Chainalysis

区块链生态中的犯罪活动一直在发生

根据 Chainalysis 的统计，区块链黑客威胁和犯罪活动逐年呈现增长趋势、并有越来越多的传统犯罪活动资金开始利用数字货币网络进行洗钱活动。

KCon

+1

AnySwap
2021-7-12

跨链项目AnySwap声明遭到黑客攻击，V3跨链资金池受影响，损失约240万USDC和551万MIM，超过800 万美金。黑客在将这些资产兑换为ETH后，通过混币平台tornado.cash清洗了资金。

Harmony
2022-6-24

Harmony的资产跨链桥Horizon遭受黑客攻击，损失金额约为一亿美元。攻击者将两笔18036.3ETH分别转移到多个攻击地址后，立即开始混币，截至目前已有17600ETH通过混币平台tornado.cash进行转移。

Ronin
2022-3-23

攻击者通过盗取验证人私钥的方式，从Ronin跨链桥取出173,600ETH和2550万USDC，按当前价格计算约合6.25亿美元。部分资金经过多次转账后，使用tonardo.cash混币转移。

KCon

+1

tornado

Non-Custodial anonymous transactions on Ethereum

Deposit **Wait** **Withdraw**

KCon

+1

建立DID风险评估模型

KCon

+1

实施攻击之前

找到攻击地址与其关联地址，提取相关交易以及交易链路中的相似特征。如：

手续费来源
同构公链交易链路
NFT代币交易链路
传统情报匹配
...等

实施攻击

实施攻击之后

关注转移、藏匿、清洗非法资金的模式，使用有向图进行描述和分析。并借助地址实体标签库和其它情报资源进行反洗钱追踪策略调整。

KCon

+1

地址资金来源中的风险资金评估

对地址资金来源的风险资金构成进行分析，通过来源方风险级别、风险资金占比、交易频次等特征
以及这些地址与当前地址之间是否可形成有向连通关系等作为系数来评估地址与风险资金的相关性。

$$\text{地址来源资金风险值} = \{\text{来源方风险系数}_{k}\text{、来源方风险系数}_{k1} \ldots \text{来源方风险系数}_{kN}\} \times \text{资金构成系数}_{r}$$

KCon

+1

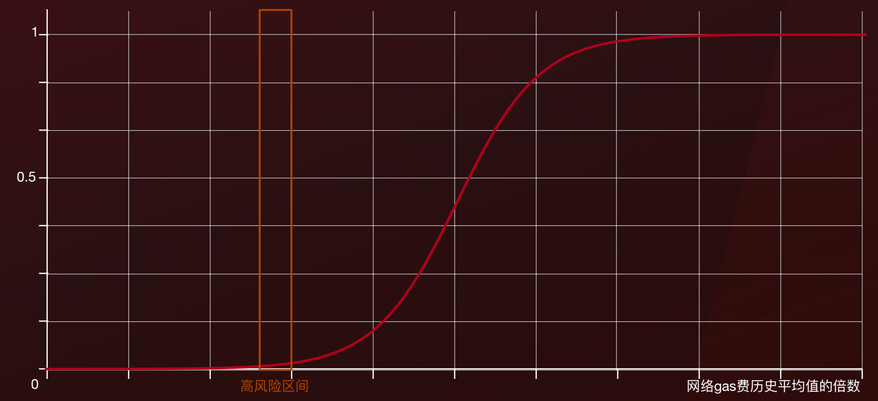
地址估值（HODL）

持有 1 类价值代币（如ETH、USDT、USDC等）的总额越大、持有时间越长。则使用该地址实施攻击的成本越高。
通常用来实施攻击的相关地址，其持币情况往往接近攻击所需手续费消耗值。

$$\text{HODL数量分值} = \text{Sigmoid}(\text{历史余额} - 100 \times \text{链上平均gas费})$$

$$\text{HODL时间评价} = \begin{cases} \dfrac{\text{HODL天数}}{365}, & \text{HODL天数} < 365 \\ 1, & \text{HODL天数} \geq 365 \end{cases}$$

$$\text{地址估值} = 1 - (\text{HODL数量分值} \times \text{HODL时间评价})$$



KCon

+1

关联地址的“真实用户”评价

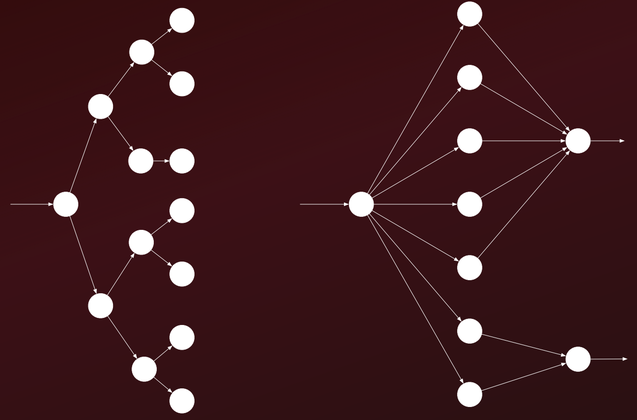
根据地址实体标签库对关联地址的交易行为进行风险评估，再判断关联地址中有“真实用户特征”的比例。
“真实用户特征”指诸如 与Defi发生交易、绑定ENS、或参与需要KYC的mint、空投等。

$$\text{关联地址真实用户评价} = 1 - \frac{\text{存在真实用户特征的关联地址数量}}{\text{总关联地址数量}}$$

KCon

+1

资金转移、藏匿、清洗过程的模式



二叉树模式

AA模式

早期阶段 – 通过延长资金转移路径或对资金进行混淆来增加分析难度和成本。

隐私协议阶段 – 使用隐私协议或隐私公链对资金路径进行截断。

Web3阶段 – 配合Web3商业设施，借助数字货币与现实商品的交易进行更高效的清洗。

资金转移过程中涉及多个相关地址的拆分、合并等情况，可使用有向图进行描述；
提取转移操作时每笔交易的频率、资金分布、层级深度等作为特征进行量化；
流入特定平台、隐私协议、隐私公链等也是权重较高的特征；
地址实体标签库对策略调整可以起到很大的辅助作用。

KCon

+1

其它DID特征（OSINT信息收集）

链上：

地址存在测试网交易记录；
在同构公链的测试网出现交易记录；
nonce/gas price/mining reward等交易详情；
已知的威胁地址（威胁情报库）等。

链下：

在社交平台中暴露地址；
在去中心化平台、网站中进行绑定、授权；
使用地址参与链上抽奖、捐赠、空投等营销活动；
更多传统情报收集方法等。

KCon

+1

DID地址画像的应用

KCon

+1

基于链上资金分析形成DID地址画像是可行的

反洗钱风控

通过DID地址画像对用户资金进行风控评估。

白名单

在无需KYC的前提下，对用户的准入门槛进行合理设计。

预言机

构建去中心化项目的外部威胁情报预言机，结合线下信息识别风险地址。

KCon

+1

DID地址画像在区块链生态的安全应用

Defi

通过DID地址画像技术增强对其用户的信用评级机制，识别资金中的异常和风险，以便更好的应对潜在的作恶行为或由此而带来的监管问题。

市场金融

DID地址画像可结合资金追溯方法对投资者、被投资者的资金来源、去向情况做进一步挖掘。也可结合资金量分析方法进行投资者行为、资金流动性等市场规律情报挖掘。

DApp

通过接入能够提供DID地址画像能力的预言机，实现合约外部威胁情报的获取，或是对去中心化的地址进行分类、聚类分析，以防范地址欺诈、黑灰产资金等风险。

钱包

作为用户的入口，钱包可以借助DID地址画像技术将有可能对用户带来威胁的地址进行识别和警示，降低用户因安全意识不足而导致的资产损失。

用户

可借助情报分析工具（如misttrack、链上天眼等）进行风险自查，或检查交易对手地址是否安全。但谨记没有所谓的绝对安全，需始终保持怀疑！

KCon

+1

MISTTRACK

https://misttrack.io/

欧科云链

https://www.oklink.com/

Etherscan

https://etherscan.io/

WalletExplorer.com

https://www.walletexplorer.com/

DeTrust 诺昕

https://detrust.bitrace.cn/

KCon

+1

缺点和不足

KCon

+1

隐私公链、协议或者隐私转账工具会中断资金流的有向结构，为资金追溯带来阻碍。

地址实体标签库和威胁情报收集的准确度对特征工程会造成较大影响。

KCon

+1

感谢您的观看！

THANKYOUFORYOURWANTCHING

KCon 2022 黑客大会