



Ethereum Colored Address Protocol

以太坊彩色地址协议

33357

以太坊地址输入问题

- 用户检查输入的以太坊地址只能一个个检查字符，容易出错，耗费精力。
- 很多用户为了方便只检查首尾几个字符，很多应用也会简化地址显示，这会导致安全风险：
 - 黑客使用显卡可以在几秒内生成首尾字符相同的假地址，替换 APP 上原本显示的真地址，只检查首尾字符很容易被骗。
 - 用户可能输错地址中间的一两个字符，就算一个个比对也很难看出来。
 - 一旦失误、受骗就是资金的直接损失，而且很难追回。

损失案例

- 利用相似地址通过伪造的token制造假的交易记录，真实地址为0xd9A1b0B1...cB2853a91，假地址为0xd9A1C378...244853a91

	0x19a2e15547...		Transfer	19824906	100 days ago	0x1E227979...a6F538FD5		OUT	0xD9A19256...e58853a91		1,155.28802767		ERC-20: Wra...BTC
	0x3374abc5a9...		Transfer	19789009	105 days ago	0x1E227979...a6F538FD5		OUT	Fake_Phishing327990		1,155.28802767		Wrapped BTC (WBTC)

- 利用相似地址通过少量真实的token制造真的交易记录，有点像小额转账测试。

From:

Interacted With (To):

ERC-20 Tokens Transferred: 50

0x2017aFE23EB6766988e2546fE88Ee4ee16B781f6 (Fake_Phishing7223)

0xD10Cc2227CC70bb067fCaA552bccaf8206dd1c1E (Fake_Phishing7231)

From

0x5aF375FA...97DA5713C

To

0x656eC290...F04c2c934

For 0

\$0.00

Tether USD (USDT)

From

0x2cf13C3f...480f1a7f2

To

0xa8b812FB...5C76aE5C6

For 0

\$0.00

Tether USD (USDT)

From

0xEF0b38b6...2A26a2749

To

0x42B4FcB6...9E2846985

For 0

\$0.00

Tether USD (USDT)

From

0xA20887A7...728A873AD

To

0x9F179837...3D5492072

For 0

\$0.00

Tether USD (USDT)

From

0x9dF5Cf84...79A028e32

To

0x405CF9f2...82e7C51e2

For 0

\$0.00

Tether USD (USDT)

From

0x3B3C632d...b76662A20

To

0x5B401f90...cc0882ee9

For 0

\$0.00

Tether USD (USDT)

From

0xb797DAF2...408422DFD

To

0xdEd2AD0e...31093ab8C

For 0

\$0.00

Tether USD (USDT)

From

0x68383b49...A50C27745

To

0x468479cF...a1C371206

For 0

\$0.00

Tether USD (USDT)

From

0x9104F917...fF5EA1490

To

0x9c21451C...F58a47CB5

For 0

\$0.00

Tether USD (USDT)

Scroll for more

以太坊彩色地址方案

- 将地址去除“0x”，剩下的进行 sha256 的计算
- 取计算结果的前 30 个字符，每 3 个为一组 RGB
- RGB数值范围映射在 50 - 200，防止颜色太白或者太黑。
- 按顺序给地址首尾 5 个字符进行染色。

方案优势

- 差异性：使用 hash 值对地址进行染色，即使只输错一两个字符，染色结果也会大不相同。
- 兼容性：兼容现有的地址显示方案，没有增加 UI 组件，技术容易实现，用户容易接受。
- 安全性：暴力计算出一个首尾 5 位数值相同、颜色排列相似的地址，使用 4090 显卡计算需要 31,688 年，如果租用 AWS A100 显卡服务器，成本高于 88 亿美元。

效果演示

<https://eth-colored-address.dnevend.site/>

☐ Simple View ☐ Auto Refresh

0x786671f5436Ec07d736Ea28B6879e832F1007356

0xa86671f5436Ec07d736Ea28B6879e832F1007356

0x786671f5436Ea07d736Ea28B6879e832F1007356

0x786671f5436Ec07d736Ea28Ba879e832F1007356

0x786671f5436Ec07d736Ea28B6879e832F100a356

☒ Simple View ☐ Auto Refresh

0x78667...07356

0xa8667...07356

0x78667...07356

0x78667...07356

0x78667...0a356



项目讨论

<https://x.com/33357xyz>





33357.xyz

@33357xyz

推广

#ETHShenZhen 公共物品项目: #以太坊有色地址协议

如何快速确认你转账时输入的 #ETH 地址是正确的? 光比对首尾字符就够了吗? 现在的黑客可以快速生成首尾相同的地址来替换掉原有地址, 光确认首尾相同不能保证地址安全。用户也容易在无意间输入错误的地址字符。但挨个数地址字符是一件很累人的事情, 看多了容易眼花。

通过 #以太坊有色地址协议, 给地址的首尾 5 个字符染色, 只需确认地址首尾 5 个字符的数值和颜色相同就能确定地址一致, 对用户非常友好。

@OpenBuildxyz @GCCofCommons
@ethpanda_org

下午11:40 · 2024年8月16日 · 3,136 查看

查看 帖子 互动量

 6

 3

 13

 4



项目源地址

https://github.com/AdamLeeeeee/Ethereum-Colored-Address-Protocol/

AdamLeeeeee / Ethereum-Colored-Address-Protocol

Q Type ↗ to search

+ ▾

🔄

<> Code Issues Pull requests Actions Projects Wiki Security Insights

Ethereum-Colored-Address-Protocol

Public

👁 Watch 1 ▾

🍴 Fork 0 ▾

★ Star 0 ▾

🔗 main ▾

🌿 1 Branch

🏷 3 Tags

🔍 Go to file

📄 Add file ▾

<> Code ▾

🔄 李洋 and 李洋 Revert "[Adam] feat: set publish config" e55ef8a · 2 hours ago 45 Commits

📁 public	styles: font	13 hours ago
📁 src	[Adam] feat: show why and how by TextCard	7 hours ago
📄 .gitignore	[Adam] init HelloWorld React Project	5 days ago
📄 .nvm	feat: demo	yesterday
📄 README.md	[Adam] docs: readme	7 hours ago
📄 package-lock.json	[Adam] add position scroll when click a menu items	4 days ago
📄 package.json	Revert "[Adam] feat: set publish config"	2 hours ago
📄 postcss.config.js	feat: use tailwind css	3 days ago
📄 tailwind.config.js	styles: font	13 hours ago
📄 tsconfig.json	[Adam] init header menu simply and change js to ts	5 days ago
📄 yarn.lock	feat: simple view	12 hours ago

About

An Introduction WebSite of Ethereum Colored Address Protocol

📖 Readme

📈 Activity

★ 0 stars

👁 1 watching

🍴 0 forks

Report repository

Releases 3

📦 third releases for test Latest

6 hours ago

+ 2 releases

Packages

No packages published

[Publish your first package](#)



项目规划

- 提交 EIP 方案，争取以太坊社区的支持
- 制作 SDK，提供方便的 UI 插件
- 优化项目方案，争取成为 walletconnet 一样的基础设施

谢谢观看