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: 0x2017aFE23EB6766988e2546fE88Ee4ee16B781f6 (Fake_Phishing7223)

Interacted With (To): 0xD10Cc2227CC70bb067fCaA552bccaF8206dd1c1E (Fake_Phishing7231)

ERC-20 Tokens Transferred: 50

- 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

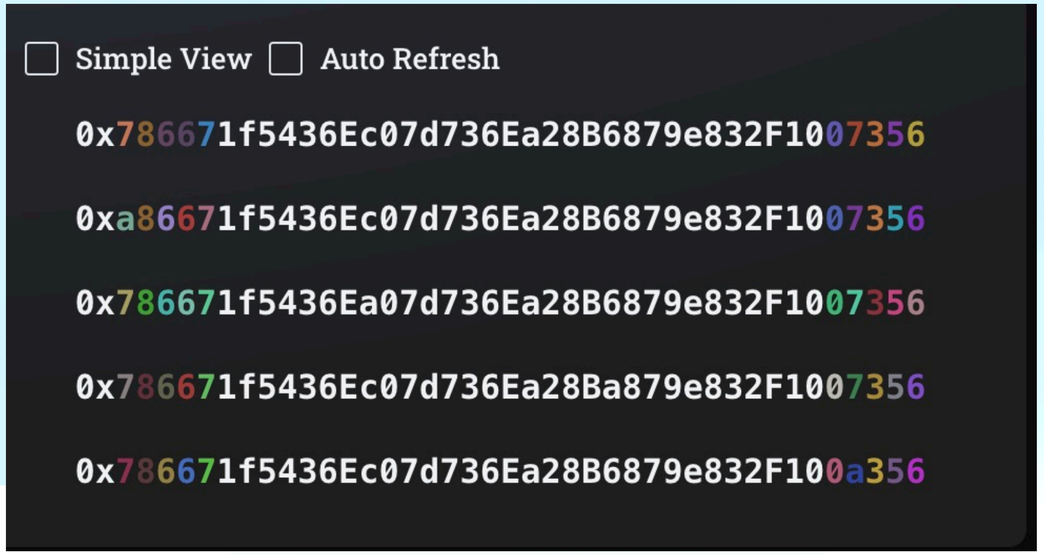
以太坊彩色地址方案

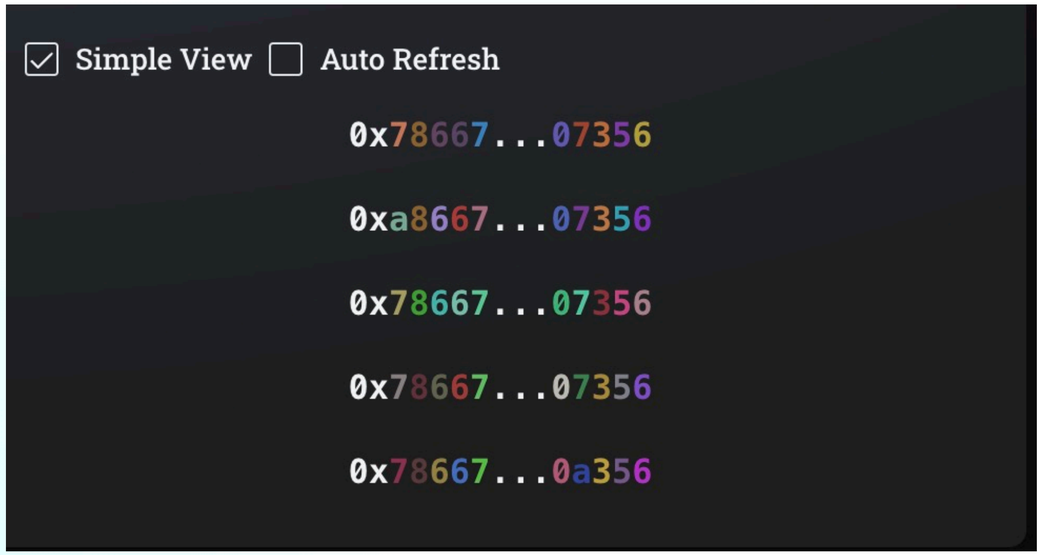
- 将地址去除“0x”，剩下的进行 sha256 的计算
- 取计算结果的前 30 个字符，每 3 个为一组 RGB
- RGB数值范围映射在 50 - 200，防止颜色太白或者太黑。
- 按顺序给地址首尾 5 个字符进行染色。

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





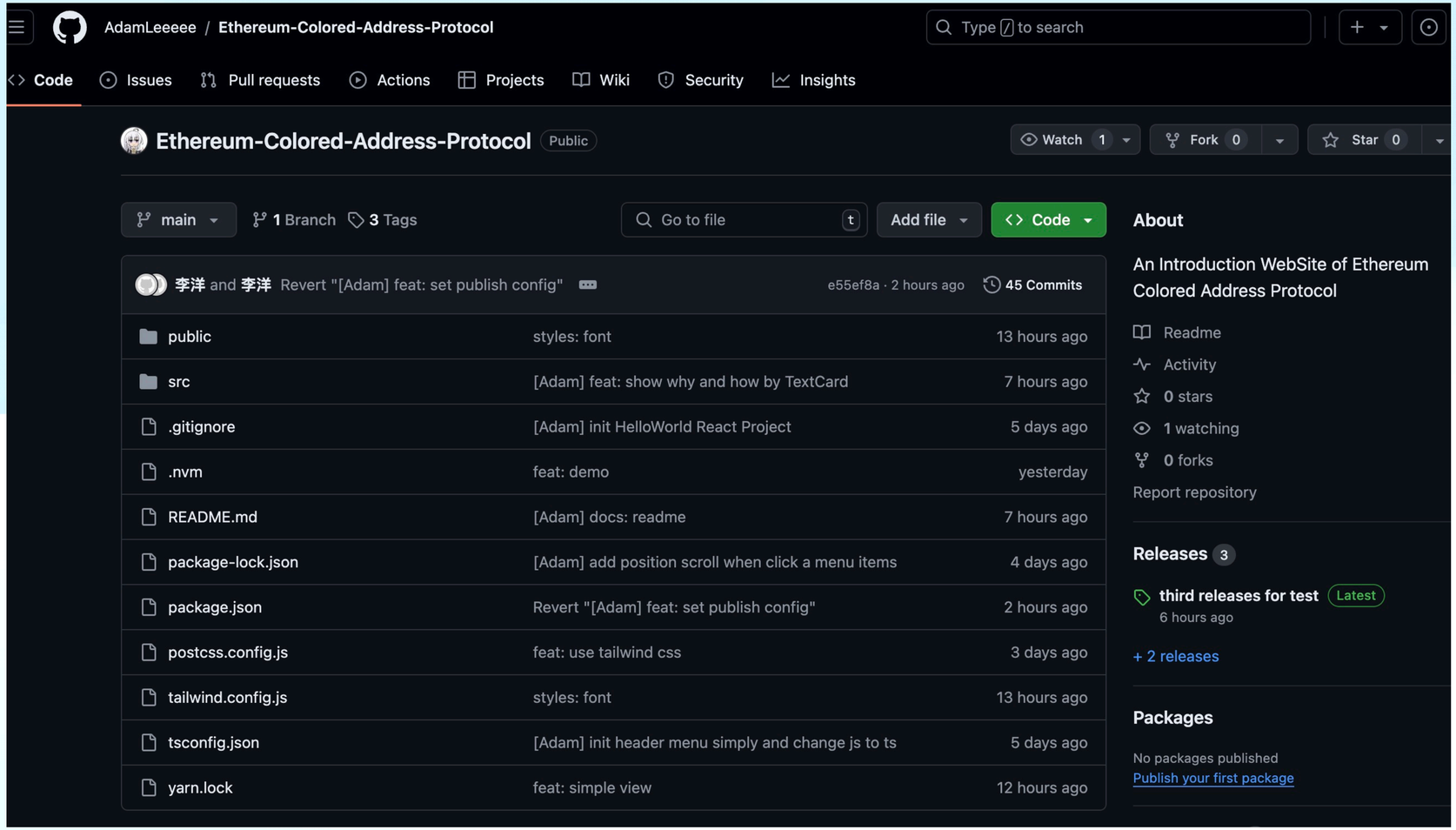
https://eth-colored-address.dnevend.site/

项目讨论

https://x.com/33357xyz

项目源地址

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



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