

谁是谁？ Web3信任的灵魂拷问

w3tester

Founder, zCloak Network

2023-5-20

提纲

- Web3世界的信任危机
- Web2的解决方案和问题
- Web3原生的机构身份解决方案
- Valid ID设计剖析与示例

Web3世界的信任危机

“谁是谁”问题带来的惨案：



主题帖



吴说区块链 
@wublockchain12



吴说获悉，币追披露一起罕见案例，一名受害人连续被骗四次。受害人在火必官方 telegram 群中收到「火必客服」私信，称存入 ETH 即可获得 HT。受害者被骗后另一个客服表示可以帮忙，随后因为泄露助记词 imtoken 钱包中剩余资金被转走。随后受害者寻找 imtoken 客服遇到假客服，再次被骗32 ETH。

Web3世界的信任危机

Web3 需要信任吗？

- Trustless：通过密码学与共识机制的巧妙结合，即使没有可信第三方作为中介，也可以让两个互不认识的人完成一笔交易。
- 合约是谁部署的？文件是谁签名的？DC里的这个链接是谁发的？
- 正在跟我聊天的，真的是本人吗？声音？图像？视频？
- Web世界里，到底什么是真的，什么是假的？

Web3世界的信任危机

“谁是谁”，人与人信任的首要问题

- 前一个“谁”，是链上常见的身份标识符，如钱包地址、DID、去中心化域名。
- 后一个“谁”，现实世界的真实身份。
- 前者是赛博空间，后者是现实世界，二者怎么形成关联？
- 小问题：ENS 域名能解决谁是谁的问题吗？

Web2的解决方案和问题

互联网行业的解决方案

- 基于证书发放机构（Certificate Authority, CA）的公钥基础设施（Public Key Infrastructure, PKI）体系。
- 通过中心化的数字证书发放机构，对主体的真实身份进行审核，然后签发数字证书，以证明该机构的真实身份。
- 简单说：这个域名属于谁。
- 常见的使用了HTTPS连接技术的网站，就是用了这种证书进行网站身份验证。

Web2的解决方案和问题

CA与PKI方案的问题

1. 中心化单点认证方法，并不符合Web3去中心化的理念。
2. CA证书的申请一般面向中大型机构和组织，虽然个人也可以申请，但是几乎没有有效的身份认证机制。（广大中小网站广泛使用的DV证书根本没有任何身份认证机制）
3. 应用范围比较有限，一般只用在网站的TLS加密通信上。

Web2的解决方案和问题

CA与PKI方案的问题

twitter.com/home

主页

为你

有什么新

证书查看者: twitter.com

基本信息(G) 详细信息(D)

颁发对象

公用名 (CN)	twitter.com
组织 (O)	Twitter, Inc.
组织单位 (OU)	<未包含在证书中>

颁发者

公用名 (CN)	DigiCert TLS RSA SHA256 2020 CA1
组织 (O)	DigiCert Inc
组织单位 (OU)	<未包含在证书中>

有效期

颁发日期	2022年12月25日星期日 08:00:00
截止日期	2023年12月26日星期二 07:59:59

pseudo

solana.com/zh

SOLANA

Pov

Bring

证书查看者: solana.com

基本信息(G) 详细信息(D)

颁发对象

公用名 (CN)	solana.com
组织 (O)	<未包含在证书中>
组织单位 (OU)	<未包含在证书中>

颁发者

公用名 (CN)	R3
组织 (O)	Let's Encrypt
组织单位 (OU)	<未包含在证书中>

有效期

颁发日期	2023年2月26日星期日 11:02:11
截止日期	2023年5月27日星期六 11:02:10

Web2的解决方案和问题

PGP的基本介绍

- PGP (Pretty Good Privacy) ，主要开发者为菲尔·齐默尔曼，1991年在互联网上免费发布，目前有多种软件实现。
- 通过给用户提供一个系列对称与不对称密钥，可以完成消息加密与解密，消息签名与验证等常见操作。
- PGP是很好的密码学工具，但是在实践层面，它依然很难解决“谁是谁”的问题：交互对象的公钥是什么？
- 自由软件开发者会把自己的PGP公钥发布在社交媒体或者自己运营的网站，这的确是一种发布公钥的办法，但其安全性和可扩展性并不理想。

Web2的解决方案和问题

Web of Trust

- 为了解决可信公钥发布的问题，菲尔·齐默尔曼在PGP 2.0的使用手册里提出了Web of Trust（信任网络）的概念。
- 与CA方案依赖中心化机构的方法不同，信任网络的理念是通过熟人关系，对其他人的PGP证书（包含对方的身份和公钥）进行签名和互相验证。
- 本质：把我们对熟人的信任转移到对PGP公钥的认证上。

Web2的解决方案和问题

Web of Trust的问题

1. 技术领域熟人圈子的建立并不容易，依赖线下的聚会和会议活动。新人想要融入已有的信任圈子，难度不小。
2. 信任的建立基本依赖于口口相传，并没有明确的真实性、有效性的检查方法，对于错误的认证也没有惩罚机制。基本还停留在“君子协定”的阶段。
3. PGP技术相当复杂，设置和操作流程相当繁琐。不了解密码学基本原理、不会命令行操作几乎寸步难行。绝大多数人无法使用，很难形成网络效应。

Web3原生的机构身份解决方案

什么是身份？

- 马克思：人是社会关系的总和。身份 = 社会关系。
- 思考：现实世界的真实身份，是怎么确立的？
 - 个人：身份证、护照、学历文凭、员工卡、社保证明；
 - 机构：工商注册信息、资产证明、信用等级、技术能力、各类资质证明。
- 身份表达的本质：信任的传递。

Web3原生的机构身份解决方案

密码学与信任传递

- 如何用密码学进行信任传递？
 - DID: 确定主体的唯一标识；
 - Claim: 一份文本，描述该主体的特征；
 - Hash: 结合了主体标识与描述文本的独一无二的摘要；
 - VC: 公证方对Claim的Hash进行数字签名，签名作为后缀附加于Claim之后。
 - 验证: $\text{Verify}(\text{Claim}, \text{签名}, \text{公证方公钥}) = \text{Pass/Fail}$.

Web3原生的机构身份解决方案

聚焦机构身份

- 个人身份：zCloak zkID.app，链下优先，本地优先，隐私优先，zk上链。
- 机构身份为什么重要：
 - 个人身份的起点；
 - 互联网世界各类诈骗的主要来源；
 - 亟需简单便捷、成本低廉、跨国共识的解决方案。

Web3原生的机构身份解决方案

Web3机构信任根

- 问题：Web3去中心化世界的机构身份，依赖于中心化的社交媒体与网站，依赖TG和DC？
- Web3原生的组织形态：DAO、网络国家、数字城邦，应该以什么样的形式确定自己的组织身份和层级架构？靠工商局吗？
- 有没有可能利用已有的密码学工具，建立一套Web3原生的、完善易用的机构身份系统？

Web3原生的机构身份解决方案

Valid ID的设计理念

- 简单易用：连接钱包即可使用。zkID wallet、Metamask、Wallet Connect.....
- 安全可靠：使用简单、成熟、经过时间检验的密码学原语，如Keccak哈希，secp256k1曲线上的ECDSA签名算法等。直接支持在主流加密钱包APP与硬件钱包内进行访问。
- 标准化：工业界行业标准，如W3C的DID和VC标准“did:zk:”，VC应用于机构身份认证，兼容已有加密生态。
- 去中心化，在 Web of Trust 互验证理念的基础上，提出了基于多方认证的信任网络架构（Multi-party attestation based Web of Trust），消除单点信任问题。

Web3原生的机构身份解决方案

Valid ID的设计理念

- 数据自主可验证：入驻主体使用根密钥（rootkey）才能修改主体信息。信息更新使用基于数字签名的自验证数据结构，平台的所有的事件与日志在Arweave、EVM公链进行留存。任何人都可以独立对平台上的相关信息进行独立审核和验证。
- 易于扩展，系统架构参考Nostr协议进行了相应的密码学改造（<https://github.com/zCloak-Network/vips>），简单灵活且易于扩展。天然辐射多链，相关数据可以辐射至所有公链，直接被智能合约所调用（项目早期阶段以EVM公链为主）。

Web3原生的机构身份解决方案

与ENS等域名项目的区别

- Web3域名的本质是链上地址的助记符，而不是身份认证方法。通过域名的文字本身，并不能传递真实的身份信息。
 - 举例：timcook.eth = Apple CEO? openai.eth = OpenAI公司?
- ENS profile内写入的网站、email等信息，并没有任何检查机制，无从判断其真实性。
- Valid ID内主体信息，会经过多个第三方的独立检查（第三方：律师事务所、安全审计公司、会计师事务所），验证结果存储于AR与EVM公链，不可篡改，可验可查。


Web3原生的机构身份解决方案

与身份聚合Profile类项目的区别

- Web3身份聚合项目，专注于链上交易信息与交互的聚合展示。对链下信息缺乏有公信力的验证机制。
- Valid ID专注于机构真实链下身份的认证与锚定。通过密码学与法律声明的双重保障，不但能在机构承认自己的链上身份时证明其身份，还能在机构否认自己链上身份时反证其身份。
- 机构身份信息：官方网站、twitter账户、email等常见信息，以及注册国家和地址等工商注册信息，还可能包括链上链下的信用积分、审计公司安全报告、投研机构的评级报告等等。
- 相关认证机构无需与zCloak Network团队进行沟通，就可以自行发布符合自家标准的机构认证信息。而用户也可以根据发布认证信息机构的口碑与信誉，对其发布的内容的价值和真实性自主进行判断。

Valid ID设计剖析与示例

Valid ID: Web3 CA与PKI基础设施

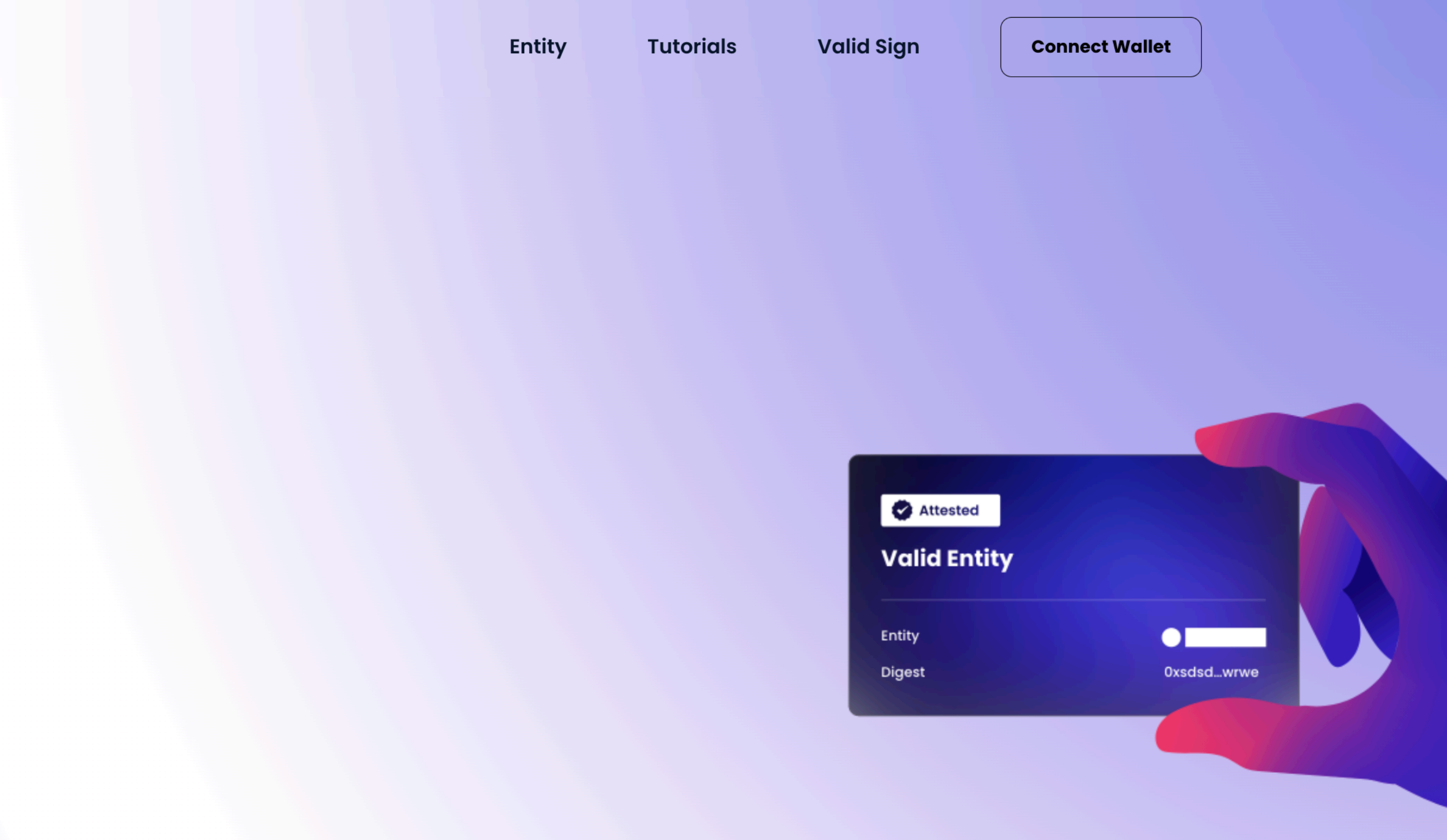


Valid ID alpha

Attested, thus **valid.**

Build the root of trust for your entity in a way that is both cryptographic and legally binding.

[Onboard](#)



Entity Tutorials Valid Sign [Connect Wallet](#)

Valid Entity

Entity

Digest

Valid ID设计剖析与示例

Valid ID的VC数据

Height 1,138,440

Confirmations 44,231

Data [🔗](#)

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "version": "1",
  "ctype": "0x4416bc7ec4ff4c79dd30c9758607a9e59aad496b7dca5d6b5a0ae596aa9b20f1",
  "issuanceDate": 1678888024687,
  "credentialSubject": {
    "Twitter Handle": "@zCloakNetwork",
    "Email": "info@zcloak.network",
    "Domain Name": "zcloak.network"
  },
  "issuer": "did:zk:0xAEd82aAc7a2c4e59357A93EA62EE4C3E9567A779",
  "holder": "did:zk:0x2F460e375d0C657CfAeF5f486bA72A989ee4A506",
  "hasher": [
    "Blake3",
    "Keccak256"
  ],
  "digest": "0x94515c99ed5b23b466117b9fe52454741ae20149672f585d68de4cac6126ab7f",
```

Valid ID设计剖析与示例

VIP协议

<https://github.com/zCloak-Network/vips>

☰ README.md

VIPs

VIPs stand for Valid ID Implementation Possibilities. This protocol aims to build an Ethereum compatible [Nostr](#) protocol for the Valid ID platform.

- [VIP-01: Event format, hashing and signatures](#)
- [VIP-02: Metadata](#)
- [VIP-03: Key](#)
- [VIP-04: Role](#)
- [VIP-05: Deletion](#)
- [VIP-06: Delegation](#)


Event Kinds

kind	description	VIP
0	Metadata	02
1	Key	03
2	Role	04
3	Deletion	03,04,05,06
4	Delegation	04,06

Valid ID设计剖析与示例

Valid ID自验证数据结构

```
{  
  "id": <32-bytes lowercase hex-encoded keccak256 of the the serialized event data>  
  "rootkey": <rootkey of the event creator>,  
  "created_at": <unix timestamp in seconds>,  
  "kind": <integer>,  
  "tags": [  
    ["e", <32-bytes hex of the id of another event>],  
    ["r", <rootkey of an entity>],  
    ... // other kinds of tags may be included later  
  ],  
  "content": <arbitrary string>,  
  "sig": <signature using ECDSA on the keccak256 hash of the serialized event data, not the same as the "id" field.>  
  "protocol": "eth-nostr"  
}
```



Valid ID设计剖析与示例


Valid Sign设计理念

- 网站：<https://sign.valid3.id>
- 多种钱包支持，可以对任意消息、文件进行数字签名。
- 签名后内容为纯文本，可以在任何社交平台、媒体网站、聊天工具内展示。
- 使用机构rootkey，或者下属人员、设备key（role关联）进行签名，可以查看关联关系。
- 支持在TG、DC、微信（zCloak Network公众号）内直接进行签名验证。

Valid ID设计剖析与示例

Valid Sign签名验证

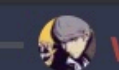
 我是官方客服，可以帮到您吗？
===
Valid Sign from [valid3.id](#)
===
name:zcloak.vid,
sig:0x6bfc524bb9ef2a4ae9941e6caf6d05c7a4f3dc58ba22b73d5cb1bde40550cb291e08d78f16ed7c9844b9b770206538ddb91f5be120f5ed109d13792faba1d52400

 Valid ID Bot
✔ [zcloak.vid](#) has signed this message (from [valid3.id](#)).
zkID:
did:zk:0x2F460e375d0C657CfAeF5f486bA72A989ee4A506
Entity Name: [zCloak Network](#)
Twitter: [@zCloakNetwork](#)
Domain: [zcloak.network](#)
Email: info@zcloak.network

[Twitter](#)
zCloak Network ([@zCloakNetwork](#)) /
Twitter
Privacy-first DID and ZKP infrastructure.
zcloak.vid
did:zk:0x2F460e375d0C657CfAeF5f486bA72A989ee4A506



我是官方客服，可以帮到您吗？
===
Valid Sign from [valid3.id](#)
===
name:zcloak.vid,
sig:0x6bfc524bb9ef2a4ae9941e6caf6d05c7a4f3dc58ba22b73d5cb1bde40550cb291e082400

 w3tester使用了Verify Signature

Valid ID Bot 机器人 今天20:58

✔ [zcloak.vid](#) has signed this message (from [valid3.id](#)).

 zCloak Network

zkID

did:zk:0x2F460e375d0C657CfAeF5f486bA72A989ee4A506

Twitter

Domain

Email

[@zCloakNetwork](#)

[zcloak.network](#)

info@zcloak.network

今天20:58

Valid ID设计剖析与示例

Valid Name设计理念

- .vid, Web3实名域名系统。
- 域名分配与机构工商注册名称相符, 同名机构域名先到先得。
- 为主流商业机构、商标预留域名。
- 支持多级域名: w3tester.zcloak.vid
- 支持zkID VC系统内显示, 多链支持。
- 目前免费。

提问?

- zCloak Network 网站: <https://zcloak.network>
- Valid ID 网站: <https://zkid.app>
- zkID wallet: wallet.zkid.app
- zCloak twitter: @zCloakNetwork
- Valid ID twitter: @valid3_id
- zCloak blog: <https://zcloaknetwork.medium.com/>
- zCloak discord: <https://discord.com/invite/j3mATwNVSH>

