JUGUGU：分布式私钥加密托管系统

绪论

现在的区块链技术就像1990年代初期的互联网技术：很有潜力，但十分不亲民。JUGUGU的诞生目的是**消除进入Web3元宇宙的障碍。**让新手用户不更改习惯，30秒创建账户，无感登录，并轻松的使用区块链应用。无论在微信小程序中，公众号中，网页中，使用起来像登录微信一样简单。当前区块链应用面临的困境：

- **私钥管理复杂。**需要了解私钥相关知识并自行保管私钥，虽然保证了去中心化特性，但新用户对于私钥的不谨慎存储也存在很大的安全隐患。
- **私钥托管不安全。**大部分项目方缺乏密码学方面的技术支持，私钥的存储存在很大的安全隐患。
- **政策合规困难。**由于当前国内政策原因，完全去中心化的应用无法实名认证并且无法绕开“数字货币”，不仅使得应用难以推广，而且存在极大的政策风险。

关键词：密码学、区块链、智能合约、多重鉴权、分布式存储、云安全

一、简介

JUGUGU 是链接Web2 用户到Web3 世界的友好登录工具，带给新用户近似于传统互联网产品的使用体验。**在不牺牲安全性的前提下**用户**使用手机号注册**，注册一次可**跨平台登录所有支持的区块链应用**。注册过程与**传统互联网体验一致**，无需用户下载插件，无需配置私钥，无需购买数字货币，无需互联网用户更改过多使用习惯。**登录支持无感登录，支持手机验证码登录**。注册一次可通行于web3世界。目前支持Conflux 树图公链**Conflux Core**、**Conflux eSpace**。

JUGUGU由密码学专家，安全专家、高级工程师、大学教授等多位开发者维护。JUGUGU系统为**非盈利**开发，完全**免费开放**接入接口。

二、使用场景

并支持微信**小程序**，微信**公众号**，**App**，移动端**网页**、**游戏**等移动互联网高频场景接入JUGUGU登录系统，跨平台使用web3区块链身份登录。

三、开发者

1.JUGUGU适用于**更多场景**，更符合传统开发者的开发与设计习惯。根据JUGUGU接口，开发者只需进行简单地**接口调用**，即可实现JUGUGU服务整合进区块链应用。

2.开发者实名认证后，可通过JUGUGU平台内置工具“**GUGU Box**”完成**一键智能合约部署**，将合约地址与项目信息提交JUGUGU，获取项目API密钥和RSA4096 Public.pem。前者作为开发者合约绑定的鉴权，后者作为JUGUGU加密通信的公钥。

3.JUGUGU对于传统互联网企业，只需要专注前端和业务端开发，使得Web2开发团队**轻松进军Web3区块链应用**。

四、安全

（一）密钥存储安全

①采用AES256、ECC256、RSA4096**混合加密**、**同态加密**、**分片存储**等技术。

②采用**短密钥**机制，用户与JUGUGU各执一半私钥。

（二）服务器安全

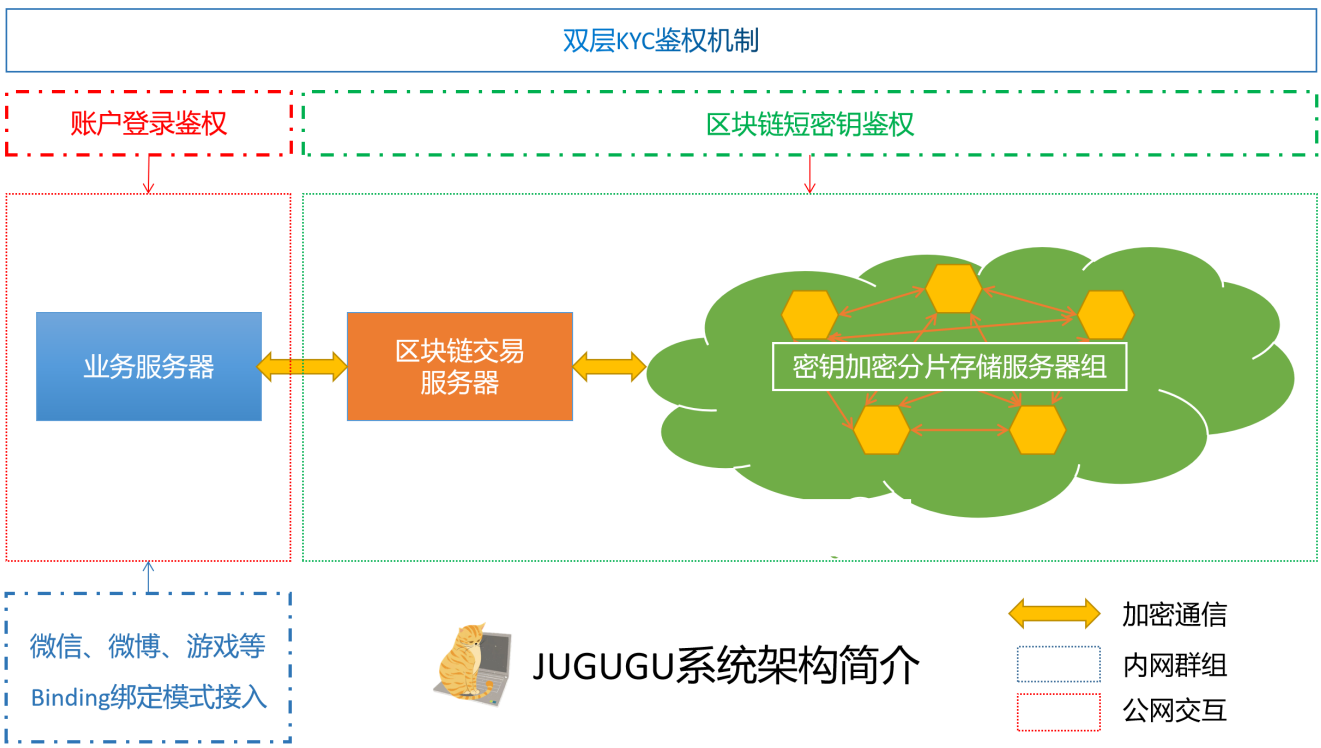
①采用**分布式云服务器**技术和**组内通信**机制。服务器数据与通信全部进行了安全组配置限定群内互通，不依靠单一服务器安全。

②云服务器配置文件、数据库等信息进行了**多重加密处理**。

③分布式云服务器组采用WindowsServer、Linux等不同操作系统，即使存在操作系级**"0day"漏洞**，也不会使得整个JUGUGU分布式密钥托管系统陷入危险之中。

④JUGUGU服务软件进行了混淆、加密、加壳处理**防止逆向工程破解**。增加安全**组策略与端口限制**，加装**阿里云安全服**务，保证安全性。

⑤当任意一台服务器的软件异常时，服务器组通过**风险预警**“**心跳检测**”切断所有组间通信，保证密钥系统安全。



（三）软件安全

针对字典暴力破解、弱口令、DDOS、SQL注入、CC/XSS攻击进行了加固防护。

（四）区块链交易

①升级扩展的**ERC721**合约，作为标准合约兼顾**中心化管理**、**去中心化运行**，支持中心化的发放型NFT与中心化自由mint型NFT、去中心化自由mint型NFT

②改进go-conflux-sdk、go-ethereum，大幅提升区块链交易处理性能，拥有**更高的并发能力**。

③支持多链、多合约同时交易处理；支持同一地址在同一区块链上同时发送>100笔区块链交易，不同地址同时在不同区块链不同合约上执行>10万笔交易。

④**Rollup交易打包**技术有效降低交易Gas费用，提升交易速度，相对于单笔**交易速度提升240倍**。

⑤支持**ERC20**接口合约交互

⑥支持**ERC721**接口合约交互

⑦支持**ERC1155**接口合约交互

⑧支持基于EVM技术的**全部区块链**

⑨一个用户绑定多链地址，使用独有的**地址转换技术**仅需一个密钥拥有多个区块链地址，便于维护整个密钥系统。

⑩支持多区块链的ERC20和NFT资产的**跨链**。

五、政策合规

1.可选支持**动态实名校验**，信息0.6毫秒级动态校验，不存储用户敏感信息。

2.可选支持**面部识别校验**，信息仅毫秒级动态校验，不存储用户敏感信息。

3.可选支持**用户赎回私钥**，当用户随着使用和学习渐渐熟悉区块链和去中心化机制后，自由切换至非托管模式，自行管理自己的加密资产安全。

4.可选支持**绑定Web3地址**，用户资产可在JUGUGU系统和指定Web3地址之间**自由流通**，可作为**Web2与Web3的桥梁**。