Genex 券交易平台 - 软件需求规格说明书

> *基于《券的金融本质与短期资金募集机制白皮书》提炼的软件开发需求*

---

1. 项目概述

1.1 项目定位

构建一个**券类资产的金融交易平台**，实现券的完整金融生命周期管理：

```
发行方发行 → 一级市场销售 → 二级市场流通 → 估值定价 → 清算兑付 → 到期管理
```

1.2 核心技术优势：区块链作为基础设施

> ***Genex 是协议，更是平台*** *—— 区块链是底层基础设施，平台在其之上提供集中化的运营、审核、评级与交易服务*

中心化与去中心化的分工

去中心化（区块链基础设施）	中心化（平台服务）
券的发行（链上铸造）	发行方入驻审核、资质认证
券的流通（P2P自由转移）	交易撮合、订单管理
券的消费结算（合约清算/销毁）	发行方信用评级
券的防伪验证（链上天然保证）	风控与合规监管
券的所有权记录	用户体验、搜索、推荐
交易记录不可篡改	数据报表、分析

关键创新：合约清算保护企业客户

> ***消费者使用券时，通过智能合约直接与发行方结算/清算/销毁，全程不经过平台***

这意味着：

- **企业无需担心客户被平台抢走**：消费环节平台不介入，客户数据不经过平台
- **企业无需担心为平台引流**：消费者与企业的结算关系是直接的
- **消费者隐私得到保护**：消费行为记录在链上，平台无法获取消费明细

```
传统模式：消费者 → [平台验证] → 企业兑付（平台掌握全部消费数据）

Genex模式：消费者 → [智能合约清算] → 企业兑付（平台不介入，不获取消费数据）
```

平台服务对象

- **发行方**（企业、政府、机构）：简单发行券、管理券、融资
- **消费者**：折扣购买券，即时支付消费
- **金融机构/投资者**：券资产交易、投资、做市
- **监管机构**：合规审计、链上数据报表
- **第三方开发者**：基于协议构建应用

市场定位：First Mover

目前市面上**没有**基于区块链基础设施的券交易平台：

- **闲鱼/淘宝**：中心化平台，券只是数据库记录，企业客户数据全部被平台掌握
- **礼品卡交易平台**（Raise、CardCash）：中心化架构，同样的客户泄露问题

- **NFT市场**（OpenSea）：技术可行，但无人专注券品类
- **DeFi协议**：做代币交易，不做券

Genex = **券交易领域的区块链基础设施平台先行者**

券的核心特性（基于区块链）

- **链上发行**：券在链上铸造，天然具备唯一性和防伪能力
- **自由流通**：持有人之间可P2P直接转移，天然具备流动性
- **合约清算**：消费者用券时通过合约与发行方直接结算，平台不介入
- **不可篡改**：所有发行、流转、兑付记录链上可追溯

1.3 核心价值主张（基于白皮书）

- **发行方**：通过平台简单发行券，实现短期无息融资、现金流提前回笼；消费结算走合约不走平台，**客户数据不会被平台获取**
- **消费者-买方**：以折扣价购买券，即时可用于支付消费，与现金、信用卡同等使用
- **消费者-卖方**：将持有的券折价变现，释放流动性
- **投资者/金融机构**：在可信的交易市场上进行券资产买卖、做市、投资
- **平台**：提供券自由买卖的交易市场、发行方信用评级，以及区块链基础设施让各方安全结算

1.4 券的金融本质（白皮书定义）

> "*券是由发行方（企业、政府、机构）发行、以未来商品或服务兑付为担保的短期无息融资工具，其现金流特征与商业票据高度一致。*"

券的五大金融要素：

要素	说明	金融等价
发行	发行方发券，持有人支付现金	信用创造
流通	券在用户间转让、交易	债权转移
估值	券在市场中折价交易	折现定价
清算	消费者使用券购买商品/服务	债务兑付
到期	券超过有效期未使用	债务注销

1.5 券的证券属性风险分析（SEC Howey Test）

> ***关键风险：白皮书将券定义为"短期无息融资工具"，具有"信用创造""债权转移"特征，这些描述可能触发SEC证券分类***

Howey Test 四要素分析

要素	判断	说明
投入资金	**是**	用户购买券需支付资金
共同事业	**可能**	券价值与发行方经营状况相关
期望利润	**关键**	消费者买券是为了消费折扣（非证券）；投资者买券是为了转售获利（可能是证券）
依赖他人努力	**可能**	券的价值取决于发行方的兑付能力

SEC Project Crypto（2025）四类数字资产分类

分类	是否证券	券的可能归属
网络代币/数字商品	否	不适用
数字收藏品	否	不适用

数字工具（Utility）	**否**	**消费型券可能归此类**（可兑换商品/服务的功能性工具）
代币化证券	**是**	**金融化券/投资型券可能归此类**（二级市场交易、期望获利）

合规策略

- [ ] 聘请美国证券律师出具券的法律属性意见书
- [ ] 消费型券：强化"功能性工具"定位，弱化"投资工具"表述
- [ ] 金融化券/投资型券：按证券合规处理（Reg D/Reg A+/Reg CF豁免）
- [ ] 平台根据券类型实施不同合规级别
- [ ] 白皮书措辞审查：避免"融资工具""信用创造"等可能触发证券分类的表述

---

2. 用户角色定义

角色	描述	核心需求
发行方	企业/政府/机构，在平台发行券	简单发券、资金回笼、客户数据不泄露
消费者-买方	折扣购买券用于消费	低价购买、即时用于支付（链上天然有效）
消费者-卖方	持有券希望变现	快速出售、合约保证安全收款
投资者/金融机构	券资产投资、做市	可信交易平台、信用评级数据
平台运营方	管理平台运营	发行方审核、信用评级、交易风控、合规
监管机构	监管合规审计	数据报表、链上可追溯

---

3. 功能模块需求

3.1 发行方入驻与发行管理模块（B端核心）

3.1.1 发行方入驻

- [ ] 发行方资质审核（营业执照、政府批文、机构证明）
- [ ] 品牌认证与初始信用评级
- [ ] 发行额度审批（基于发行方信用）

3.1.2 信用成长与额度机制（零保证金入驻）

> *入驻不收保证金，通过信用评级动态控制发行额度，降低企业入驻门槛*

```
入驻审核 → 初始信用评级（低额度）→ 发行 → 兑付表现 → 信用提升 → 额度提升
                                                    ↓
                                              违约/差评 → 降级/额度缩减/冻结
```

- [ ] 新发行方零保证金入驻，初始给予低发行额度
- [ ] 信用评级基于：兑付率、Breakage率、用户评价、经营年限
- [ ] 信用评级与发行额度直接挂钩，动态调整
- [ ] 信用评级数据公开透明，消费者/投资者自行判断
- [ ] 违约触发机制：降级、额度缩减、暂停发行、冻结账户
- [ ] 可选：发行方主动缴纳保证金以快速提升额度
- [ ] 可选：销售款部分冻结作为兑付保障（发行方自愿开启，可提升信用评级）

3.1.3 券发行管理

- [ ] 券模板设计（面值、有效期、使用条件、使用场景）
- [ ] 批量发行券（链上铸造，券ID即唯一标识）
- [ ] 发行定价策略（折扣率设定）
- [ ] 发行审批流程
- [ ] 发行上架管理

3.1.4 券的类型支持（白皮书分类）

类型	描述	金融属性
实物券	印制券、礼品券、月饼券	实物兑付负债
数字券	电子优惠码、App储值券、电子礼品卡	电子化储值负债
金融化券	可交易礼品卡、积分券、平台抵扣资产	短期无息债券

3.1.5 发行方数据分析

- [ ] 发行量/兑付率/Breakage率统计
- [ ] 二级市场流通分析
- [ ] 融资效果分析（现金流时序图）
- [ ] 券生命周期追踪

3.2 券生命周期管理模块

3.2.1 券的状态流转

```
已发行 → 已上架 → 已售出 → [流通中/已兑付/已过期]
```

- [ ] 状态流转跟踪与记录
- [ ] 过期自动处理（状态变更、Breakage收益计算）
- [ ] 历史记录留存（≥5年）
- [ ] 券有效性链上自验证（无需平台介入）

3.2.2 券信息字段

字段	说明
券ID	链上唯一，天然防伪
发行方ID	关联发行方信息
面值	券的票面价值
发行价格	发行方定价（通常折价）
有效期	起止日期
使用条件	使用限制与规则
使用场景	适用范围
当前状态	生命周期状态
当前持有人	所有权记录

3.3 交易市场模块

3.3.1 一级市场（发行方→持有人）

- [ ] 发行方券上架展示
- [ ] 消费者购买流程
- [ ] 支付对接（稳定币/加密货币 + 法币通道）
- [ ] 券所有权链上转移（自动记录）

3.3.2 二级市场（持有人之间自由交易）

- [ ] 卖方挂单：设定售价、有效期
- [ ] 买方求购：设定求购价、数量
- [ ] 一口价模式
- [ ] 竞价/拍卖模式（可选）

3.3.3 撮合引擎

- [ ] 价格优先、时间优先撮合规则
- [ ] 实时撮合与延时撮合
- [ ] 部分成交支持

3.3.6 做市商与流动性激励

> ***二级市场冷启动阶段如果没有做市商提供流动性，用户挂单无人接，市场即死***

- [ ] 做市商准入：KYC L3 + 最低保证金/资金要求
- [ ] 做市商激励：手续费减免/返佣（Maker-Taker模型，做市方手续费低于Taker方）
- [ ] 做市义务：维持最小挂单深度（买卖双边）、最大价差限制
- [ ] 做市商API：低延迟专用接口、批量挂单/撤单
- [ ] 流动性挖矿（可选）：早期阶段对提供流动性的用户给予平台激励
- [ ] 做市商监控：防止做市商操纵价格、虚假挂单（Spoofing/Layering检测）

3.3.4 定价机制（白皮书公式）

```
P = F × (1 - dt) × (1 - rc)

其中：
- P：市场价格
- F：券面值
- dt：时间折价率（距有效期越近，折价越高）
- rc：信用风险溢价（发行方信用越低，溢价越高）
```

- [ ] 智能定价建议
- [ ] 历史成交价参考
- [ ] 折价率实时计算与展示
- [ ] 发行方信用评级影响定价

3.3.5 交易流程（链上原子交换）

卖方挂单 → 买方下单 → 平台风控审查 → 智能合约原子交换（券⇔资金同时转移） → 交易完成

> *智能合约保证交易原子性（要么全部成功，要么全部回滚），平台负责风控审查与AML监控*

3.4 清算与支付模块

3.4.1 资金与资产托管（两种模式）

	方案B（默认）	方案A（定制服务）

券资产	用户自托管（自有钱包）	平台托管（平台钱包）
法币	平台托管（隔离账户）	平台托管（隔离账户）
消费结算	合约直接清算，平台不介入	经平台验证后清算
P2P流通	用户间直接转移	需经平台
适用场景	所有用户默认模式	企业与平台签订托管服务协议
启用条件	注册即可	需签订服务协议

- [ ] 默认方案B：券在用户自有钱包，平台只托管法币
- [ ] 方案A：企业与平台签订托管服务协议后开通，平台代管券资产
- [ ] 法币通道对接（出入金）
- [ ] 可选：保障资金链上锁定（发行方自愿缴纳的保证金/冻结款，见3.1.2）

3.4.2 清算规则

- [ ] 交易手续费计算（平台收益）
- [ ] 买卖双方资金划转
- [ ] 退款机制
- [ ] Breakage收益计算与分配

3.4.3 兑付清算（合约直接结算，平台不介入）

> *消费者使用券时，通过智能合约直接与发行方完成结算/清算/销毁，**平台不接触消费数据，不介入消费环节***

- [ ] 合约清算：消费者调用合约兑付，券自动销毁
- [ ] 发行方履约记录（链上可查）
- [ ] 债务清算会计处理
- [ ] 兑付率统计

3.4.4 链上对账

- [ ] 链上数据即账本（无需日终对账）
- [ ] 异常交易链上可追溯
- [ ] 链上流水实时可查

3.5 风控模块

3.5.1 发行方风控（核心）

- [ ] 发行方信用评级（基于兑付率、Breakage率）
- [ ] 发行额度动态调整
- [ ] 兑付能力监控
- [ ] 风险预警机制

3.5.2 券真伪风控（链上天然解决）

> *链上券天然防伪、防双花，无需额外验证机制*

- [ ] 链上验证券合法性（合约地址 + 券ID）
- [ ] 链上状态检查（是否已兑付/过期）

3.5.3 交易风控

- [ ] 异常交易监测（大额/高频/异地）
- [ ] 欺诈行为识别

- [ ] 黑名单管理
- [ ] 交易频率限制（防止高频小额洗钱）
- [ ] 单用户持券/持仓限额

3.5.4 用户风控

- [ ] KYC分级强制认证（见3.6.1）
- [ ] 信用评分体系
- [ ] 交易限额管理（与KYC等级挂钩）

3.5.5 AML反洗钱专项（核心风控）

> ***券是有面值的价值载体，P2P可自由转移，天然具备高洗钱风险，必须严格防控***

已识别的洗钱路径：

路径	手法	防控措施
买券洗钱	脏钱买券 → P2P转给另一账户 → 卖出提现	出入金来源审查、大额交易审核
分散洗钱	一个账户买券 → P2P分散转给大量小账户 → 各自小额提现	P2P转移监控、关联账户检测
发行方自洗	发行方发券 → 关联账户自买自卖 → 虚构交易套取资金	发行方关联交易检测、自买自卖识别
跨境洗钱	A国法币买券 → P2P转给B国用户 → B国卖出提现	跨境交易额度限制、地域异常检测

AML具体需求：

- [ ] **出入金来源审查**：法币入金需验证资金来源合法性
- [ ] **大额交易审核**：单笔超过阈值需额外人工审核
- [ ] **P2P转移监控**：虽不经过平台，但链上数据公开，平台持续监控异常模式
- [ ] **P2P转移限额**：单日/单月P2P转移次数和总额限制（与KYC等级挂钩）
- [ ] **发行方关联交易检测**：检测发行方与买方的关联关系，识别自买自卖
- [ ] **链上行为分析**：分析链上转移模式，标记异常地址（扇出/扇入/环形转移）
- [ ] **可疑交易自动标记**：触发规则后自动生成SAR（可疑交易报告）
- [ ] **交易图谱分析**：构建用户间交易关系图谱，识别洗钱网络

3.6 用户系统模块

3.6.1 账户管理（钱包为核心）

- [ ] 钱包连接（WalletConnect / 内置钱包）
- [ ] 可选：手机号/社交账号绑定（便于找回）
- [ ] **KYC分级强制认证**（见下表）
- [ ] 法币通道绑定（出入金，需完成KYC L2）

钱包丢失与恢复方案（方案B下核心风险）：

> *方案B用户自托管券，私钥丢失 = 资产永久丢失，必须提供恢复机制*

- [ ] **内置MPC钱包（推荐）**：平台提供MPC（多方计算）钱包，密钥分片存储（用户设备 + 平台 + 第三方），任意两方可恢复
- [ ] **社交恢复**：用户预设3-5个可信联系人（Guardian），丢失时多数Guardian确认即可恢复钱包权限
- [ ] **助记词备份提醒**：首次创建钱包时强制提示备份助记词，定期提醒验证
- [ ] **账户抽象（AA钱包）**：支持ERC-4337账户抽象，用邮箱/手机号作为账户入口，降低Web3门槛
- [ ] 方案A用户不受影响（平台托管，平台负责恢复）

KYC分级制度：

等级	要求	权限
L0（浏览）	仅钱包连接	浏览市场、查看行情，不可交易
L1（基础）	手机号 + 邮箱验证	小额交易（日限额X元）、持券上限Y张
L2（标准）	身份证/护照 + 人脸识别	正常交易、法币出入金
L3（专业）	企业/机构认证 + 合规审查	大额交易、做市、发行

> *不完成KYC不能交易。发行方必须达到L3。*

3.6.2 个人中心（链上资产视图）

- [ ] 我的券库（链上钱包持有的数字券）
- [ ] 我的订单（链上/链下订单记录）
- [ ] 我的钱包（链上余额 + 法币余额）
- [ ] 交易历史（链上可验证）

3.6.3 消息通知

- [ ] 交易状态通知
- [ ] 券即将过期提醒
- [ ] 价格变动提醒
- [ ] 发行方公告推送

3.7 合规与报表模块

3.7.1 美国联邦金融监管合规

FinCEN / BSA（银行保密法）：

- [ ] FinCEN MSB（Money Services Business）注册（Form 107，每2年续期）
- [ ] BSA合规计划：AML程序、KYC流程、SAR申报、CTR（大额现金交易报告）
- [ ] 交易记录留存（≥5年）
- [ ] 大额交易报告（超过阈值自动上报）
- [ ] 可疑交易报告（SAR）

OFAC制裁合规（强制）：

> ***不执行OFAC筛查在美国运营MSB属于联邦犯罪，这是零容忍红线***

- [ ] 接入OFAC SDN（Specially Designated Nationals）制裁名单
- [ ] 用户注册时筛查：姓名、地址、国籍与SDN名单比对
- [ ] 每次交易时筛查：交易双方实时比对制裁名单
- [ ] P2P转移筛查：链上地址与已知制裁地址库（Chainalysis/Elliptic）比对
- [ ] 制裁名单更新同步：OFAC名单更新后24小时内同步至系统
- [ ] 命中处理：冻结账户 → 上报OFAC → 禁止任何资产操作
- [ ] 覆盖范围：SDN、Sectoral Sanctions、Non-SDN Menu-Based Sanctions、阻断法规

SEC相关（视券的证券属性而定，见1.5节）：

- [ ] 如券被归类为证券：Broker-Dealer注册 + Form ATS申报
- [ ] 如券被归类为数字工具：按CLARITY Act向CFTC注册数字商品交易所
- [ ] 反欺诈合规（无论券是否为证券，SEC反欺诈条款均适用）
- [ ] 发行方信用评级系统的合规审查（评级不得误导投资者）

GENIUS Act（2025年签署，稳定币法）：

- [ ] 平台使用第三方合规稳定币（USDC/USDT），不自行发行
- [ ] 稳定币出入金通道合规对接

FATF Travel Rule（加密资产转移规则）：

> ***加密资产转移超过$3,000时，发送方服务商必须向接收方服务商传递发送方/接收方身份信息***

- [ ] P2P转移≥$3,000时，强制通过平台合约路由（记录双方身份信息后放行）
- [ ] 接入Travel Rule协议（如TRISA/TRP/OpenVASP）实现跨平台信息传递
- [ ] 低于$3,000的P2P转移：链上转移自由，但平台持续监控异常模式
- [ ] 设计约束：方案B下用户自托管券，但P2P转移大额时必须回到平台合约执行，确保Travel Rule合规

消费者保护法合规：

- [ ] FTC Act Section 5：禁止不公平或欺骗性商业行为（券描述、定价不得误导）
- [ ] Dodd-Frank UDAAP：禁止不公平、欺骗性或滥用行为（适用于消费金融产品）
- [ ] 券信息披露义务：面值、有效期、使用限制、发行方信用等级必须明确展示
- [ ] 退款政策透明化：一级市场购买后的退款权利与流程
- [ ] 发行方虚假宣传监控：平台对券描述与实际兑付内容的一致性负审核责任
- [ ] Gift Card相关法规：CARD Act（信用卡法案中礼品卡条款）——有效期不得少于5年、不得收取休眠费

州级合规：

- [ ] 各州Money Transmitter License（MTL）——49个州+DC
- [ ] 纽约BitLicense（如服务NY用户）
- [ ] 加州DFAL牌照（2026年7月生效）

3.7.2 税务合规

- [ ] 用户税务报告（IRS Form 1099-DA/1099-B）
- [ ] 发行方税务报告
- [ ] Breakage收入税务处理
- [ ] 跨境税务合规（FATCA）

3.7.3 数据隐私合规

- [ ] CCPA（加州消费者隐私法）
- [ ] GDPR（如服务欧盟用户）
- [ ] 用户数据存储与删除策略

3.7.4 数据报表

- [ ] 平台交易日报/月报
- [ ] 发行方兑付率报告
- [ ] 用户行为分析
- [ ] 券类别分析
- [ ] 风险指标监控仪表盘
- [ ] 监管报表自动生成（SAR/CTR/1099）

3.8 争议与纠纷处理模块

3.8.1 交易争议

- [ ] 买方申诉：购买的券无法兑付、券信息与描述不符
- [ ] 卖方申诉：买方恶意投诉、付款争议

- [ ] 平台仲裁流程（提交证据 → 平台审核 → 裁决 → 执行）
- [ ] 链上证据采集（交易记录、转移记录不可篡改）

3.8.2 发行方违约处理

- [ ] 发行方无法兑付：降级 → 冻结发行 → 启用保障资金（如有）→ 公示
- [ ] 发行方跑路：冻结账户 → 链上券标记为风险券 → 通知所有持有人
- [ ] 用户赔偿机制：保障资金优先赔付，不足部分公示损失

3.8.3 券的取消与召回

- [ ] 发行方申请召回未售出的券（链上销毁）
- [ ] 问题券紧急下架（平台主动 + 发行方申请）
- [ ] 已售出券的退款流程

3.8.4 客服系统

- [ ] 在线客服（工单系统）
- [ ] 发行方专属客服通道
- [ ] 投诉处理时效要求（24h响应，72h处理）

3.9 平台商业模式

收入来源	说明
交易手续费	二级市场每笔交易收取买卖双方手续费
发行服务费	发行方在平台发行券时收取服务费
增值服务	券推广置顶、数据分析报告、信用评级加速
方案A托管服务费	选择平台托管模式的企业收取托管服务费
API/开发者服务	第三方接入API收取调用费

3.10 开放平台与国际化

3.10.1 API/SDK开放平台

- [ ] 券发行API（第三方系统对接发行）
- [ ] 交易API（做市商/量化交易接入）
- [ ] 券验证API（商户验证券有效性）
- [ ] 开发者文档与沙箱环境

3.10.2 多语言与国际化

- [ ] 多语言支持（中文/英文/日文 优先）
- [ ] 多币种支持（法币 + 稳定币）
- [ ] 多地区合规适配

3.10.3 发行方管理后台

- [ ] 券管理（查看、下架、召回）
- [ ] 兑付管理（确认兑付、查看兑付记录）
- [ ] 财务管理（销售收入、提现、对账）
- [ ] 数据仪表盘（实时发行/兑付/流通数据）

---

4. 技术需求

4.1 系统架构要求

- 高可用：99.9% SLA
- 高并发：支持万级TPS
- 低延迟：交易响应 < 500ms
- 数据安全：金融级加密

4.2 技术栈建议

层级	技术选型
前端	React/Vue + 小程序 + App
后端	Go 微服务架构
数据库	PostgreSQL + Redis
消息队列	Kafka/NATS
搜索	Elasticsearch
区块链（核心）	EVM兼容链 / L2 / 应用链
智能合约	Solidity - 券发行、转移、兑付合约
钱包集成	WalletConnect / 内置MPC钱包 / AA钱包（ERC-4337）

4.2.1 区块链选择标准

> *链的选择直接影响用户成本、交易速度、合规可行性*

评估维度	要求	说明
Gas成本	单笔交易 < $0.01	券面值可能只有几十美元，gas不能比券本身贵
交易确认速度	< 5秒	消费者兑付需即时确认，不能等15秒以上
TPS	≥ 1000	支持平台规模增长
EVM兼容	必须	降低开发与生态对接成本
监管友好	优先	链本身不在OFAC制裁名单内，有合规工具支持
生态成熟度	优先	钱包、浏览器、预言机、审计工具等生态完善

候选链评估（需MVP阶段最终确认）：

- [ ] **L2方案**（Base/Arbitrum/Optimism）：低gas、高速、EVM兼容、背靠主流生态
- [ ] **应用链方案**（Avalanche Subnet/Cosmos App Chain）：可定制gas策略、独立出块
- [ ] **Polygon PoS/zkEVM**：低gas、成熟生态、企业级案例多
- [ ] 排除：Ethereum L1（gas太贵）、Solana（非EVM）、BSC（监管风险）

4.3 区块链核心架构

4.3.1 数字券标准

- [ ] 基于ERC-721/ERC-1155设计数字券标准
- [ ] 券元数据：面值、发行方、有效期、使用条件
- [ ] 券状态管理：可流通、已兑付、已过期
- [ ] 批量发行优化（gas效率）

4.3.2 智能合约体系

合约	功能
CouponFactory	券发行工厂，发行方调用发行新券
Coupon	数字券合约，管理所有权与转移
Marketplace	挂单/求购/撮合（可选，支持链下撮合）
Redemption	兑付合约，验证并销毁已使用券
Treasury	资金托管合约，管理交易资金流

4.3.3 Gas费策略

> ***谁支付Gas直接决定用户体验。消费者不应为使用一张50元的券支付gas费***

操作	Gas承担方	说明
券发行（铸造）	**发行方**	发行成本，计入发行服务费
一级市场购买	**平台代付**	平台通过Paymaster（ERC-4337）代付gas，从交易手续费中覆盖
二级市场交易	**平台代付**	同上，gas成本内含于手续费
P2P转移	**发送方**	用户自主行为，平台不补贴；或设每日免费额度
券兑付（消费）	**平台代付**	消费环节不应有额外成本，通过Paymaster代付

- [ ] 接入ERC-4337 Paymaster合约，实现用户无感Gas体验
- [ ] 平台预充Gas池（Paymaster存款），定期补充
- [ ] Gas成本监控：当链上gas spike时自动暂停非紧急操作
- [ ] 备选：L2/应用链原生低gas（< $0.001），则无需Paymaster

4.3.4 P2P流通机制

- [ ] 用户钱包间直接转移券（无需平台）
- [ ] 链下签名 + 链上结算（降低gas）
- [ ] 批量转移支持
- [ ] 转移历史链上可查
- [ ] 大额P2P转移（≥$3,000）强制通过平台合约路由（Travel Rule合规，见3.7.1）

4.3.5 混合架构（链上+链下）

```
链上（不可篡改）          链下（高性能）
├─ 券所有权              ├─ 订单簿
├─ 转移记录              ├─ 撮合引擎
├─ 兑付记录              ├─ 用户资料
├─ 发行方信息            ├─ 消息通知
└─ 清算结果              └─ 数据分析
```

4.4 安全要求

- [ ] HTTPS全站加密
- [ ] 敏感数据加密存储
- [ ] 接口签名验证
- [ ] SQL注入/XSS防护

- [ ] DDoS防护
- [ ] 资金操作多重验证
- [ ] 智能合约审计（第三方）
- [ ] 私钥管理方案（MPC/HSM）

4.5 灾难恢复与业务连续性（DR/BCP）

> ***金融交易平台必须具备灾难恢复能力，Nasdaq上市审计也会审查BCP***

4.5.1 灾难恢复

- [ ] RPO（恢复点目标）< 1分钟：数据库实时同步至备用区域
- [ ] RTO（恢复时间目标）< 15分钟：备用系统15分钟内接管
- [ ] 多区域部署：主用区域 + 至少1个热备区域（不同地理位置）
- [ ] 数据库主从复制 + 自动故障转移
- [ ] 链上数据天然灾备（区块链本身是分布式存储，不会丢失）
- [ ] 链下数据（订单簿、用户资料）定期快照 + 增量备份

4.5.2 业务连续性计划

- [ ] 交易系统故障：自动切换至备用撮合引擎，未完成订单状态保护
- [ ] 链节点故障：多节点冗余（≥3个自有节点 + 第三方RPC备用）
- [ ] 法币通道故障：对接多个支付服务商，自动切换
- [ ] 密钥管理灾备：MPC密钥分片存储于不同地理位置
- [ ] 年度DR演练：每年至少1次全量灾难恢复演练并记录
- [ ] BCP文档：灾难分级、响应流程、通知链、恢复步骤（SOX审计要求）

---

5. 未来扩展需求（白皮书第八章）

> *注：券的数字化已作为核心架构实现，见4.3节*

5.1 券的资产证券化

- [ ] 券收益流打包
- [ ] Coupon-Backed Securities (CBS)
- [ ] 信用评级与收益曲线模型

5.2 跨境券流通

- [ ] 多币种支持
- [ ] 跨境支付对接
- [ ] 国际化合规

---

6. Nasdaq上市准备（GoGenex Inc.）

> *IPO前18-24个月启动准备*

6.1 牌照与注册（上市前必须完成）

牌照/注册	监管方	说明
MSB注册	FinCEN	法币托管与价值转移，Form 107
州MTL	49州+DC	各州货币转移牌照，或通过持牌合作方

NY BitLicense	NYDFS	如服务纽约用户
Broker-Dealer（视情况）	SEC	如券被归类为证券
Form ATS（视情况）	SEC	如券被归类为证券
数字商品交易所（视情况）	CFTC	如CLARITY Act通过且券被归类为数字商品

6.2 SOX合规（Sarbanes-Oxley）

- [ ] **Section 302**：CEO/CFO个人签署财务报告准确性认证
- [ ] **Section 404(a)**：管理层评估内部控制有效性（ICFR）
- [ ] **Section 404(b)**：外部审计师审计内部控制（加速申报人要求）
- [ ] **Section 906**：虚假财报的刑事责任条款
- [ ] 数字资产托管内部控制（钱包安全、密钥管理、MPC/HSM）
- [ ] 智能合约部署与升级审计追踪
- [ ] 链上记录与GAAP财报对账

6.3 财务与审计

- [ ] 聘请PCAOB注册审计师（具备加密资产审计经验）
- [ ] 2年以上经审计GAAP财务报表
- [ ] 数字资产会计：FASB ASU 2023-08（公允价值计量）
- [ ] 收入确认：ASC 606（Breakage收入、递延负债、手续费）
- [ ] 链上数据与链下账本对账机制

6.4 Nasdaq上市标准

- [ ] 满足最低股东权益/市值/收入门槛
- [ ] 独立董事（至少多数）
- [ ] 审计委员会（全部独立董事）
- [ ] 薪酬委员会
- [ ] SEC注册声明（Form S-1）
- [ ] 完整风险披露（券的证券属性风险、监管风险、技术风险）

6.5 商业保险需求

> ***Nasdaq上市公司几乎必须持有以下保险，也是机构投资者尽调的标准项***

保险类型	覆盖范围	说明
D&O保险（董事及高管责任险）	董事/高管个人因管理决策被诉的法律费用与赔偿	上市公司标配，IPO前必须购买
E&O保险（专业责任险）	因平台服务失误（如信用评级错误、交易撮合问题）导致用户损失	金融服务平台必备
网络安全险（Cyber Liability）	数据泄露、黑客攻击、勒索软件导致的损失与响应成本	加密平台高风险，保费较高
忠诚保证金（Fidelity Bond）	内部员工欺诈、盗窃数字资产	金融机构监管常见要求
商业综合险（General Liability）	一般商业责任	基础商业保险

- [ ] IPO前12个月完成所有保险采购
- [ ] D&O保险覆盖额度需匹配公司市值
- [ ] 网络安全险需覆盖数字资产托管风险（方案A模式下平台托管的资产）

6.6 上市后持续合规

要求	频率
10-K年报（SOX合规）	年度
10-Q季报	季度
8-K重大事件披露	实时
SAR/CTR申报	持续
州MTL续期	年度/两年
FinCEN MSB续期	每2年
智能合约审计	每次升级

---

7. MVP阶段优先级

Phase 1 - 基础发行与交易（MVP）

1. KYC分级认证（L1/L2/L3）
2. 发行方入驻与基础审核
3. 券发行与上架
4. 一级市场购买
5. 基础二级市场挂单/购买
6. 支付与清算
7. 基础风控与AML
8. 基础客服与争议处理

Phase 2 - 体验优化

1. 智能定价建议
2. 搜索/筛选优化
3. 消息通知
4. 信用评分体系

Phase 3 - 发行方端增强

1. 批量发券
2. 完整数据分析
3. 融资效果报告

Phase 4 - 合规与扩展

1. 完整合规报表
2. 高级风控
3. 跨境券流通

---

8. 关键指标（KPI）

指标	描述	目标值
交易成功率	成功完成/发起交易	> 95%
发行方兑付率	已兑付/已售出券	> 85%
链上确认时间	从交易发起到链上确认	< 30秒

用户投诉率	投诉订单/总订单	< 1%
平台折价率	平均成交价/面值	80-90%
发行方留存率	持续发行方比例	> 70%

---

9. 术语表（白皮书定义）

术语	定义
Breakage	消费者购买后未使用或遗失的券金额，最终转化为发行方利润
折价率	券的市场价格与面值的差额比例
兑付率	已使用券数量/已发行券数量
信用利差	基于发行方信用风险的额外折价
递延负债	发行方发行券形成的预收账款

文档版本: v3.4 生成日期: 2026-02-09 来源: 券的金融本质与短期资金募集机制白皮书 (draft v0.1) 更新: 补齐OFAC制裁筛查、FATF Travel Rule、Gas费策略、钱包恢复方案、做市商激励、灾难恢复BCP、消费者保护法、链选择标准、商业保险