

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

1.6 券类型防火墙（核心合规架构）

核心风险：消费型券一旦在二级市场被炒作获利，其性质可能从Utility转变为Security。解决方案不是贴标签，而是从平台设计上让消费型券结构性不满足Howey Test的"期望利润"要素。

双轨制：Utility Track vs Securities Track

规则	消费型券 (Utility Track)	投资型券 (Securities Track)
二级市场价格规则	转售价不得超过面值（只能折价，不能溢价）	无价格限制
转售次数限制	每张券限2-3次二级市场转售	无限制
持有目的声明	买方需确认"购买用于消费"	明确投资目的
有效期	强制≤12个月（短期工具，非长期投资品）	可更长
合规要求	MSB + FTC消费者保护	Broker-Dealer + ATS + Reg D/A+/CF
KYC等级	L1/L2	L2/L3
发行方	所有通过审核的发行方	仅通过证券合规审查的发行方
平台合规成本	低（无需证券牌照）	高（需Broker-Dealer注册）

为什么"不允许溢价"是关键

消费型券交易逻辑：

买入：100元面值券，花85元买入

卖出：不想用了，以80元卖出（折价转售）

结果：亏损5元（减损，非获利）

→ Howey Test "期望利润"要素不成立 → SEC难以认定为证券

消费型券的二级市场本质是"不想用的券找到想用的人"，不是投机市场。价格上限=面值，结构性消除了获利空间。

防火墙技术实现

- CouponFactory合约中为每张券标记类型（Utility / Security）
- Settlement合约中对Utility类型券强制执行价格上限（≤面值）
- 链上转售计数器：Utility类型券超过转售次数上限后合约拒绝交易
- Utility Track和Securities Track使用不同的交易市场界面（前端隔离）
- 合规合约中对两种类型券执行不同的KYC/AML检查等级
- 发行方发行时选择券类型，选择后不可更改（链上不可变）

MVP策略

Phase 1只开放Utility Track（消费型券），不开放Securities Track。完全规避SEC证券合规风险。Securities Track待取得法律意见书和相关牌照后再开放。

1.7 GNX原生代币合规分析

券的证券属性已在1.5/1.6中详细分析。但Genex Chain的原生代币GNX本身也可能被SEC认定为证券，其影响面比券更大——如果GNX是证券，整条链的Gas机制、治理模型、质押经济都会受影响。

Howey Test分析（GNX代币）

要素	判断	说明
投入资金	是	用户购买GNX需支付资金
共同事业	是	GNX价值与Genex平台整体发展直接相关
期望利润	关键	质押收益 = 利润预期；Gas使用 = 功能性消耗（非利润）
依赖他人努力	是	平台团队的运营和开发决定GNX价值

GNX的双重属性

用途	性质	证券风险
Gas消耗（支付交易费用）	功能性使用（消耗品）	低——类似“汽油”，用了就没了
治理投票（参与链参数决策）	功能性使用（治理权）	低——类似“投票权”，非利润导向
质押收益（验证节点质押获得奖励）	可能构成投资合同	高——质押获利 = 期望利润
二级市场交易（交易所买卖GNX）	可能构成投资合同	高——买入持有等升值 = 期望利润

合规策略

- MVP阶段GNX不上交易所：Phase 1中GNX仅用于Gas（平台补贴，用户不接触），不开放二级市场交易，回避证券风险

- 功能性优先定位**: GNX的首要用途是Gas和治理, 不宣传为“投资品”
- 质押开放时机**: 质押功能在取得法律意见书后开放, 可能需Reg D/Reg S豁免
- 代币经济设计**: 聘请代币经济学顾问和证券律师共同设计, 确保功能性消耗占主导用途
- 参考先例**: 研究SEC对ETH (非证券)、BNB (SEC诉讼)、SOL等代币的分类逻辑
- 如GNX被归类为证券: 需调整链经济模型 (如改为纯Gas代币无质押收益), 或进行证券注册

MVP策略: Phase 1中用户完全不接触GNX (Gas由平台补贴), GNX仅作为链内部运行机制。待法律意见书明确GNX分类后, 再决定是否开放质押和交易。

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

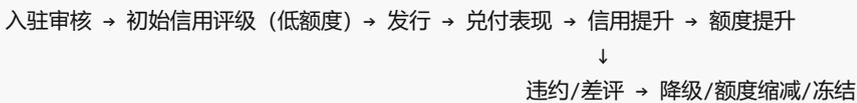
3.1 发行方入驻与发行管理模块 (B端核心)

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



- 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

发行方可配置规则 (链上合约级别执行) :

发行方在创建券时可自定义以下规则, 规则写入链上合约, 发行后不可更改。

规则	默认值	可选范围	说明
可转让性	允许P2P转移	允许 / 禁止 / 限定条件	政府福利券可设为"不可转让"
转售次数	Utility Track默认2-3次	0-10次 (0=不可转售)	0次=仅限一级市场购买, 不可二级市场交易
使用人群限定	无限定	全部用户 / 指定KYC属性	如学生券 (KYC验证学生身份)、企业员工券
单人限购	无限制	1-N张	防止囤货炒作, 如每人限购5张
使用门店限定	全部门店	全部 / 指定门店列表	连锁企业可限定券在特定门店使用
叠加使用	不可叠加	可叠加 / 不可叠加	是否允许同一笔消费使用多张券
最低消费	无	0-N金额	满X元可用 (满减券场景)

- 发行方在创建券模板时通过勾选/填写设定规则 (Web2界面, 无需了解合约参数)
- 规则在CouponFactory铸造时写入链上元数据, 合约级别强制执行
- "不可转让"券: Coupon合约的transfer函数对该券返回revert
- "限定门店"券: Redemption合约验证核销门店ID是否在允许列表中
- 平台审核时检查规则合理性 (如: 不允许设置歧视性人群限定)

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 + 三因子模型）

基础定价公式：

$$P = F \times (1 - dt - rc - lp)$$

其中：

- F = 券面值 (Face Value)
- dt = Time Discount (时间折扣) = f(剩余有效期)
- rc = Credit Risk (信用风险溢价) = f(发行方信用评分)
- lp = Liquidity Premium (流动性溢价) = f(市场供需)

示例：

面值100元券，剩余30天，发行方AA级，市场供需平衡
 dt = 0.02 (2%), rc = 0.03 (3%), lp = 0.01 (1%)
 Price = 100 × (1 - 0.02 - 0.03 - 0.01) = 94元

三因子计算规则：

因子	计算方式	取值范围
时间折扣(dt)	线性衰减：(总有效期-剩余天数)/总有效期 × 最大折扣	0% - 15%
信用风险(rc)	查表映射：AAA=0%, AA=3%, A=6%, BBB=10%, BB+=15%, <BB=20%	0% - 20%
流动性溢价(lp)	供需比：(卖单量-买单量)/总单量 × 调节系数	-5% - 10%

Utility Track券价格上限 = 面值 (见1.6)，即 $P \leq F$ 。定价公式仅用于建议价，实际成交价由市场决定但不得超过面值。

AI辅助定价引擎：

功能	算法	输入特征	输出
价格预测	LSTM时序模型	历史价格、成交量、时间特征、发行方信用变动	未来价格走势与置信区间
最优挂单建议	强化学习 (RL)	市场状态、库存深度、目标收益率	建议挂单价格
异常价格检测	Isolation Forest	价格序列、成交模式、偏离度	异常交易标记

- 智能定价建议 (基于三因子模型 + AI预测)
- 历史成交价参考 (K线图、成交量图)
- 折价率实时计算与展示
- 发行方信用评级影响定价 (信用变动自动触发价格建议更新)
- AI定价模型定期回测与参数调优

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 (平台托管为默认)

设计原则: 用户不需要知道“钱包”的存在。平台在后台自动为每个用户创建托管钱包, 用户只看到“我的账户余额”和“我的券”。

	标准模式 (默认, 所有用户)	Pro模式 (自助托管, 主动开通)
用户体验	手机号/邮箱注册即用, 与传统App无异	WalletConnect连接外部钱包
券资产	平台托管 (后台自动创建托管钱包, 用户无感)	用户自托管 (自有钱包)
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	合约直接清算, 平台不介入
P2P转移	手机号/邮箱转赠 (平台后台解析为链上地址)	链上地址直接转移
钱包恢复	平台负责 (手机号/邮箱验证即可恢复)	用户自行备份助记词/社交恢复
适用场景	99%普通用户 (消费者、发行方)	加密原生用户、技术开发者
启用条件	注册即默认开通	在设置中主动切换 (需确认风险提示)
区块链可见性	完全不可见 (用户界面无任何区块链术语)	可查看链上地址、交易哈希等

三级资产控制模型:

级别	用户画像	区块链可见性	平台控制力	消费隐私
标准模式 (默认)	99%普通用户	完全不可见	平台MPC托管	政策保证+审计保证
提取到外部钱包	想自持资产的用户	部分可见 (持有券)	平台无关	技术保证 (平台不可能获取)
Pro模式	加密原生用户	完全可见	用户完全自控	技术保证

用户可随时将券从平台提取到任何EVM兼容的外部钱包 (MetaMask等)。提取后平台无法查看、干预、冻结该券。用户可直接调用Redemption合约消费, 平台技术上不可能获取消费数据——“消费环节平台不介入”的承诺从政

策保证升级为技术保证。

- 默认标准模式**：注册后平台自动在Genex Chain上创建托管钱包（MPC托管），用户无感知
- 券提取到外部钱包**：用户可在“我的券→提取”中将券转移至任意EVM外部钱包地址（需KYC L2+）
- Pro模式可选**：用户在“设置→高级”中可切换至自托管模式（WalletConnect），需签署风险确认
- 提取后的券仍可在Genex Chain上流通、交易、消费（链上资产，不依赖平台）
- 标准模式用户的P2P转移：输入对方手机号/邮箱，平台后台解析为链上地址后执行链上转移
- 标准模式钱包恢复：通过手机号/邮箱验证 + KYC身份验证即可恢复账户（平台MPC托管，不会丢失）
- 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
- Breakage收益计算与分配

退款机制（链上资产退款逻辑）：

券是链上资产，售出后所有权已转移。退款 = 链上反向操作，比传统退款更复杂。

场景	退款流程	技术实现	时效
一级市场退款 (消费者→发行方)	消费者发起退款申请 → 平台审核 → 券从买方退回发行方（链上转移） → 资金从发行方退回买方	Settlement合约反向原子交换（券→资金同时退回）	审核通过后即时链上执行
二级市场退款 (买方→卖方)	买方发起申诉 → 平台仲裁 → 券从买方退回卖方 → 资金从卖方退回买方	Settlement合约反向原子交换	仲裁裁决后执行
已核销券	不可退款	Redemption合约已销毁券，不可逆	—
已过期券	不可退款 （Breakage已计入发行方收益）	券状态为Expired，不可操作	—
已转赠/已转售券	仅退当前持有人的购入价，不追溯前手	退款对象 = 当前持有人	—

- 一级市场退款窗口**：发行方可设定退款期限（如购买后7天内可退），过期不可退
- 退款原子性**：退款通过Settlement合约执行反向原子交换，券和资金同时退回，不存在“退了钱但券没退回”的风险
- 手续费退还规则**：一级市场退款全额退还（含手续费）；二级市场退款仅退交易金额（手续费不退）
- 退款上链记录**：每笔退款在链上记录（退款交易哈希），作为审计和争议处理的不可篡改证据
- 防滥用**：单用户退款率超阈值触发风控审查（防止恶意“买了用了再退”的欺诈）

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

信用评分模型 (量化公式) :

$$\text{CreditScore} = 0.35 \times Rr + 0.25 \times (1 - Br) + 0.20 \times \log(Mt+1)/\log(36+1) + 0.20 \times Us$$

其中:

Rr = Redemption Rate (核销率)	权重: 35%
Br = Breakage Ratio (沉淀率)	权重: 25% (沉淀率越低 = 券越有价值)
Mt = Market Tenure (市场存续月数)	权重: 20% (对数衰减, 36个月趋近满分)
Us = User Satisfaction (用户满意度)	权重: 20%

信用等级与发行额度映射:

等级	分数范围	发行额度	监控级别
AAA	90-100	最高额度, 无额外限制	常规监控
AA	80-89	高额度	常规监控
A	70-79	标准额度	标准监控
BBB	60-69	受限于额度	加强监控
BB及以下	<60	暂停发行, 整改后重新评估	重点监控

动态更新触发机制:

触发事件	更新频率	影响因子
券核销 (正常使用)	实时	+Rr
券过期 (未使用)	每日批量	+Br
用户投诉/差评	实时	-Us
季度综合审计	季度	综合调整
违约事件	实时	直接降级 (可降2级以上)

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	跨境交易额限制、地域异常检测

AML具体要求:

- 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

设计原则: 用户体验与支付宝/Zelle/Venmo一致。手机号/邮箱是账户入口, 区块链完全不可见。

3.6.1 账户注册与管理（手机号/邮箱为核心）

注册流程（标准模式，99%用户）：

手机号/邮箱注册 → 设置密码 → 短信/邮件验证码确认 → 注册成功
↓（后台静默执行，用户无感知）
平台自动在Genex Chain上创建MPC托管钱包
钱包地址与手机号/邮箱绑定映射表

- 手机号/邮箱注册**（主流程）：与普通App注册完全一致
- 可选：Google/Apple/微信等社交账号一键注册
- 注册后**平台后台自动创建MPC托管钱包**（用户不知道、不需要知道钱包的存在）
- KYC分级强制认证**（见下表）
- 支付方式绑定（银行卡/信用卡/Apple Pay，需完成KYC L2）
- 可选：Pro模式切换入口（设置→高级→自托管模式，面向加密原生用户）

账户恢复（标准模式下极简）：

标准模式用户的钱包由平台MPC托管，**不存在“私钥丢失”风险**。账户恢复与普通App一致。

- 忘记密码：手机号/邮箱验证码重置
- 换手机号：KYC身份验证（人脸+证件）后迁移账户
- 账户冻结/封禁后申诉：客服工单 + 身份验证

Pro模式用户（自托管）的额外恢复方案：

- 助记词备份（切换Pro模式时强制提示）
- 社交恢复：预设3-5个可信联系人（Guardian），多数确认即可恢复
- 账户抽象（AA钱包，ERC-4337）：邮箱/手机号作为恢复入口

KYC分级制度：

等级	要求	权限
L0 (浏览)	手机号/邮箱注册即可	浏览市场、查看行情，不可交易
L1 (基础)	手机号 + 邮箱双重验证	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、绑定支付方式、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（用户友好视图，无区块链术语）

用户界面展示	后台实际对应
我的券	链上钱包持有的ERC-721/1155代币
我的订单	链上交易记录 + 链下订单记录
我的余额	链上稳定币余额 + 法币账户余额
交易记录	链上交易哈希（用户看到的是“订单号”）

转赠记录	链上P2P转移记录
------	-----------

- 我的券（展示持有的券，含图片、面值、有效期、发行方）
- 我的订单（买入/卖出历史，状态追踪）
- 我的余额（统一展示，不区分链上/链下）
- 交易记录（用"订单号"代替"交易哈希"，Pro模式可查看链上详情）
- 转赠记录（显示"转赠给 138****1234"而非"转至 0x..."）

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: Pro模式用户自托管券或用户提取到外部钱包后, P2P转移大额时仍需通过Compliance合约路由执行, 确保Travel Rule合规(链级强制, 无法绕过)

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
- CARD Act与Utility Track有效期冲突处理:** Utility Track强制有效期≤12个月(见1.6), 而CARD Act要求礼品卡≥5年。需在法律意见书中论证“消费型券≠Gift Card”(券是发行方预付债务工具, 非零售商礼品卡), 或对符合Gift Card定义的特定券类型豁免12个月限制

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

基本要求:

- 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

核心冲突: 用户“删除权”vs 区块链不可删除

CCPA/GDPR赋予用户“删除个人数据”的权利。但区块链上的交易记录、转移记录不可删除。平台必须在架构设计上解决这一矛盾。

解决策略: 链上仅哈希/地址, 明文在链下(可删除)

数据类型	存储位置	可删除?	说明
------	------	------	----

用户姓名、手机号、邮箱、身份证	链下数据库	可删除	CCPA/GDPR删除请求可执行
KYC资料 (人脸、证件照片)	链下数据库	可删除	同上
手机号→地址映射	链下映射表	可删除	删除后地址变为"匿名地址"
交易记录 (TX Hash、金额)	链上	不可删除	但链上仅有地址, 无个人信息
Travel Rule身份信息	链上=哈希, 链下=明文	链下可删, 链上哈希不可逆	哈希不构成"个人数据" (不可逆)

- **架构原则:** 链上永远不存储可识别个人信息 (PII), 仅存储地址和哈希
- **删除流程:** 用户请求删除 → 删除链下所有PII → 删除映射表记录 → 链上地址变为无法关联到个人的匿名地址
- **法律论证:** 链上地址在映射关系被删除后不再构成"个人数据" (参考CNIL/法国数据保护局2018年区块链指南)
- **数据保留例外:** AML/BSA法规要求交易记录保留≥5年, 此期间内不得删除 (法规要求优先于删除权)
- **隐私告知:** 用户注册时明确告知"交易记录将永久保存在区块链上 (不含个人信息), 这是区块链安全性的核心保障"

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
Pro模式增值服务	自托管技术支持、高级API调用
API/开发者服务	第三方接入API收取调用费

发行方分层激励（降低入驻门槛，激励高额发行）：

层级	月发行量	平台手续费率	增值服务
白银	< 100万	1.5%	基础数据看板
黄金	100-500万	1.2%	高级数据分析 + 推荐位
铂金	500-2000万	1.0%	专属客服 + 定制报表
钻石	> 2000万	0.8%	定制开发 + 专属API额度 + 联合营销

层级每月自动根据发行量重新计算。新入驻发行方首月享黄金层级手续费（获客激励）。

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
- 开发者门户（Developer Portal）

SDK支持计划：

SDK	语言/平台	功能范围	优先级
genex-js	JavaScript/Node.js	全功能（发行、交易、核销、数据查询）	P0（MVP同步）
genex-java	Java/Android	全功能 + Android原生集成	P0
genex-python	Python	数据分析、信用查询、批量操作	P1
genex-swift	Swift/iOS	移动端核销、用户端功能	P1

genex-go	Go	高性能服务端集成、做市商接入	P2
----------	----	----------------	----

API限流策略:

调用方类型	限流	说明
普通用户	100 req/min	消费者端App调用
企业用户	1,000 req/min	发行方后台调用
做市商	10,000 req/min	低延迟专用接口
内部服务	无限制	平台微服务间调用

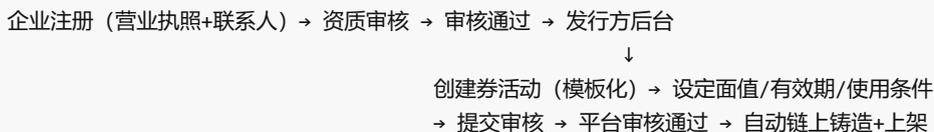
3.10.2 多语言与国际化

- 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 (B端Web2体验)

设计原则: 发行方同样不需要了解区块链。发行券 = 在后台"创建优惠活动", 链上铸造在后台自动完成。

发行方注册与操作流程:



- 券管理 (查看、下架、召回——用户看到的是"活动管理"而非"链上合约操作")
- 兑付管理 (扫码核销/在线核销, 后台自动调用Redemption合约, 发行方无感)
- 财务管理 (销售收入、提现、对账——法币视图, 不展示链上稳定币细节)
- 数据仪表盘 (实时发行/兑付/流通/Breakage数据, 可视化图表)
- 模板化发券:** 预设券模板 (满减券、折扣券、礼品卡、储值券), 发行方填表即可, 无需理解NFT/ERC标准
- 批量操作:** 批量发行、批量核销、批量导出数据
- 消费者数据隔离:** 发行方后台仅可见自己发行的券的汇总数据 (兑付率、销量), 不可见消费者个人信息 (合约清算保护)

3.10.4 商户端核销集成

发行方 (企业总部) 发行券, 但核销发生在线下门店。门店收银员需要简单、可靠的核销工具, 且必须支持网络不稳定场景。

核销方式 (三种并行):

方式	场景	说明
扫码核销 (推荐)	门店收银员用手机/平板扫消费者出示的券码	最常用, 调用Redemption合约
输码核销	消费者报出券码, 收银员手动输入	扫码设备故障时的备选

在线核销	线上商城/小程序内消费	用户点击"使用", 前端调用合约
------	-------------	------------------

商户端工具:

- 商户核销App** (iOS/Android) : 门店收银员专用, 扫码即核销, 操作≤3秒
- Web端核销后台**: 门店管理员通过浏览器核销+查看核销记录
- POS SDK集成**: 为已有POS系统的连锁企业提供SDK, 嵌入现有收银流程
- 核销API**: 第三方系统 (如企业自有App) 调用API完成核销

离线核销能力 (关键) :

门店网络不稳定时 (地下商场、偏远地区), 核销不能中断。

- 离线缓存核销**: App本地缓存已发行券的验证数据 (券ID+状态+有效期), 断网时可本地验证并暂存核销记录
- 联网后同步**: 网络恢复后自动将离线核销记录上链 (调用Redemption合约)
- 离线风控**: 离线核销设单笔/单日限额 (防止离线期间被重复核销), 超限需联网验证
- 冲突处理**: 如离线期间同一张券被两个门店核销, 以先上链者为准, 后者自动退回并通知

多门店管理:

- 连锁企业可设置门店层级: 总部→区域→门店
- 各门店独立核销权限 (某些券限定指定门店使用)
- 门店级核销数据汇总至总部仪表盘
- 门店员工账号管理 (收银员仅有核销权限, 店长有数据查看权限)

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)	Genex Chain ——Cosmos SDK + cosmos/evm (参考Cronos/dYdX v4)
智能合约	Solidity (cosmos/evm模块) - 券发行、转移、兑付、合规合约

账户系统	手机号/邮箱注册 + 后台MPC托管钱包（默认）；WalletConnect / AA钱包（Pro模式）
AI/ML	LightGBM + Scikit-Learn（信用评分）、LSTM + Prophet（价格预测）、Isolation Forest + DeepSVDD（异常检测）
监控	Prometheus + Grafana（指标）、ELK Stack（日志）、Jaeger（链路追踪）
API网关	Kong / APISIX（限流、认证、路由）

AI/ML技术栈详细:

模块	功能	框架/算法	部署
信用评分引擎	发行方与券信用评估	LightGBM + Scikit-Learn	FastAPI微服务
价格预测模型	券折价与市场波动预测	Prophet（周期性）+ LSTM（序列预测）	批量训练 + 在线推理
异常检测系统	洗钱、欺诈、异常交易检测	Isolation Forest + DeepSVDD	实时流处理（Kafka消费）
风控决策引擎	实时风险预警与自动冻结	规则引擎 + ML模型混合	FastAPI + Redis Queue
智能推荐	个性化券推荐、交易机会提示	协同过滤 + 内容推荐	P2优先级

4.2.1 自建链: Genex Chain

平台自建一条EVM兼容的应用链，承载所有券业务与合规逻辑。自建链 = 完全掌控Gas、性能、合规、升级

为什么自建链而不是用公链/L2:

维度	公链/L2	自建链 (Genex Chain)
Gas控制	受市场波动，无法保证低成本	平台完全控制Gas策略，可设为零或极低
合规执行	链层面无法强制合规	链级别内置OFAC筛查、Travel Rule、交易监控
性能调优	与其他DApp共享资源	独享资源，针对券业务优化TPS和确认速度
升级自主	依赖链治理，升级不可控	平台自主决定升级节奏和内容
数据主权	数据在公链上完全公开	可控制数据可见性（公开验证 + 隐私保护）
监管对接	难以满足监管定制需求	可为监管机构提供专属节点/API

Genex Chain 技术架构: 基于Cosmos SDK + cosmos/evm

参考Cronos (Cosmos SDK + EVM最成熟实现) 和dYdX v4 (交易平台专用链标杆) 架构

组件	技术选型	说明
链框架	Cosmos SDK (最新版本)	200+生产链验证，模块化、可定制、\$100B+资产保护

共识引擎	CometBFT (原Tendermint)	拜占庭容错共识, 即时终结性 (1个区块即最终确认, 无回滚)
EVM模块	cosmos/evm (官方Cosmos EVM)	2025年3月开源, Apache 2.0, 替代已弃用的Ethernint
跨链通信	IBC (Inter-Blockchain Communication)	Cosmos生态原生跨链协议, 120+链互通
跨链桥	IBC + Axelar跨链桥	稳定币 (USDC) 从Ethereum/其他链桥入Genex Chain
撮合架构	链下内存订单簿 + 链上结算	参考dYdX v4: 高频撮合在链下, 成交结果上链

参考链与各自价值:

参考链	价值	关键参考点
Cronos (Crypto.com)	架构最接近, Cosmos SDK + EVM最成熟实现	<1s出块、30K TPS、Block-STM并行执行、EIP-1559 Fee机制
dYdX v4	交易平台专用链标杆, 2025 H1处理\$316B交易量	链下订单簿 + 链上结算、自定义Cosmos模块、MEV防护
Injective	金融应用Layer-1, \$1.68B RWA合约	链上CLOB、RWA支持、机构级合规框架

注意: 不使用Ethernint (已停止维护)。Kava架构中的EVM模块基于Ethernint, 且Kava已转向DeAI方向, 不再适合作为金融交易平台参考。

Genex Chain 设计参数:

参数	目标
共识机制	CometBFT PoS (平台初期运营验证节点, 后期开放质押)
EVM兼容	完全兼容EVM (cosmos/evm), 支持Solidity、Hardhat、MetaMask全部EVM工具链
出块时间	≤ 1秒 (参考Cronos 2025升级已验证可达<1s, CometBFT即时终结性)
TPS	≥ 5000 (Block-STM并行执行, 独占链资源)
Gas策略	平台前期全额补贴 (见4.3.3), 后期可调整
原生代币	GNX (用于Gas、治理、质押; 前期Gas补贴不影响代币设计)
节点运营	平台自营验证节点 + 未来开放合格机构运营节点
跨链能力	IBC连接Cosmos生态 + Axelar桥连接Ethereum生态
区块浏览器	自建区块浏览器 (EVM兼容, 支持合约验证和交易查询)
监管节点	为监管机构提供只读全节点/专属API, 满足审计要求

选择Cosmos SDK的理由 (对比其他方案):

方案	优势	劣势	结论
Cosmos SDK + cosmos/evm	200+生产链验证、即时终结性、IBC跨链、完全主权、Go语言人才充裕	需自建验证节点网络	选用
OP Stack (L2)	依托Ethereum安全性	7天乐观证明争议期（金融交易不可接受）、Gas受L1影响、非独立主权	不选
Avalanche Subnet	可定制、亚秒终结性	IBC跨链弱于Cosmos、生态工具链不如Cosmos成熟	备选
Substrate/Polkadot	共享安全	Rust人才稀缺、EVM兼容需额外集成	不选
独立开发	完全定制	开发周期长、安全风险高、无生态	不选

链级合规能力（自建链独有优势）：

- 链级OFAC过滤：验证节点拒绝处理制裁地址的交易（交易级别拦截）
- 链级Travel Rule：大额转移交易必须携带发送方/接收方身份哈希，否则节点拒绝打包
- 链级交易监控：节点内置异常交易检测模块，实时标记可疑交易
- 监管API：监管机构通过专属API实时查询链上数据（无需运行全节点）
- 紧急冻结能力：平台可通过治理合约冻结涉案地址的链上资产（需多签授权）

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（ERC-721/ERC-1155），管理所有权与转移
Settlement	交易结算合约，链下撮合成交后链上原子结算
Redemption	兑付合约，验证并销毁已使用券（消费者直接与发行方结算）
Treasury	资金托管合约，管理交易资金流
Compliance	合规合约，OFAC地址过滤、Travel Rule数据哈希记录、紧急冻结
Governance	治理合约，Gas参数调整、紧急冻结多签授权

撮合引擎 (Orderbook/Matching) 不上链, 采用链下内存订单簿 (参考dYdX v4), 成交后调用Settlement合约链上结算

4.3.3 Gas费策略

Genex Chain为自建链, 平台完全控制Gas参数。前期所有Gas由平台补贴, 用户零Gas体验

前期策略 (平台全额补贴) :

操作	Gas承担方	说明
券发行 (铸造)	平台补贴	降低发行方入驻门槛
一级市场购买	平台补贴	消费者零成本购买
二级市场交易	平台补贴	交易无额外摩擦
P2P转移	平台补贴	鼓励券流通
券兑付 (消费)	平台补贴	消费环节零成本

自建链的Gas本质上是平台的运营成本 (服务器/验证节点), 不像公链需要支付ETH。平台可将Gas设为极低值甚至为零, 前期作为获客成本补贴。

后期策略 (平台规模化后可调整) :

- 根据业务增长逐步引入最低Gas (防止垃圾交易/DDoS)
- 发行方Gas按发行服务费包含
- 高频交易/做市商Gas按API套餐包含
- 普通用户日常操作保持免费或极低Gas

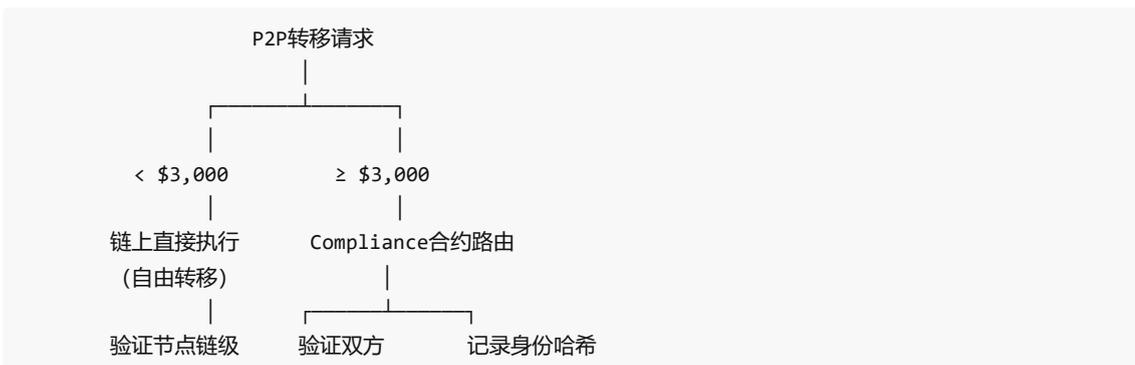
技术实现:

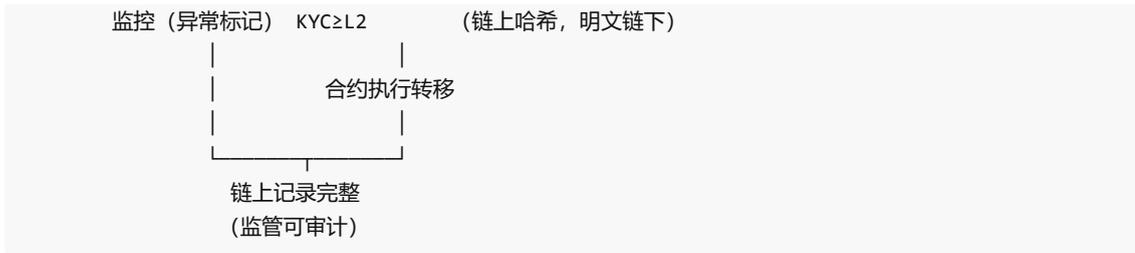
- Genex Chain创世配置中设定Gas Price = 0 (或极低值)
- 验证节点由平台运营, 节点成本 = 平台基础设施成本
- 可选: 接入ERC-4337 Paymaster作为Gas代付的标准化接口 (兼容EVM生态钱包)
- Gas参数可通过链治理合约动态调整 (无需硬分叉)

4.3.4 P2P流通机制与合规路由

Genex Chain是自建链, 所有交易对验证节点可见。P2P"不经过平台"指的是业务层面平台不介入, 但链级合规监控始终存在。

P2P转移分层合规架构:





小额P2P (< \$3,000) :

- 链上直接执行，用户体验与普通转账一致
- 验证节点内置模式识别：扇出/扇入/拆分规避 (structuring) 检测
- 发现structuring行为自动升级为Travel Rule流程
- 链上数据公开，平台持续分析异常转移模式

大额P2P (≥ \$3,000) ——Travel Rule强制合规:

- 调用Compliance合约，验证双方地址均已完成KYC L2+
- 身份信息**哈希**写入链上 (不可逆，保护隐私)
- 身份信息**明文**存储在平台链下KYC数据库 (监管可查)
- 验证节点在打包交易前检查Travel Rule数据完整性，不完整则拒绝打包
- 接入TRISA/TRP协议，支持跨平台Travel Rule信息传递

与“合约清算保护企业客户”不矛盾:

场景	Travel Rule	平台介入	隐私
消费兑付 (Redemption)	不适用 (消费不是“转移”)	不介入 (合约直接结算)	完全保护
小额P2P转移	不适用 (<\$3,000)	不介入 (链级监控)	完全保护
大额P2P转移	适用	合规合约自动路由	链上仅哈希
二级市场交易	平台天然掌握双方信息	撮合+结算	平台已知

消费者使用券消费时走Redemption合约 (与发行方直接结算)，不触发Travel Rule。平台“消费环节不介入”的隐私承诺不受影响。

- 批量转移支持
- 转移历史链上可查

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

4.3.6 智能合约升级策略

智能合约部署后代码不可修改。如果发现漏洞或需要功能迭代，必须有安全的升级机制。同时SOX审计要求所有合约变更有完整审计追踪。

升级模式：Transparent Proxy（透明代理模式）

用户/前端 → Proxy合约（地址不变，存储不变） → Implementation合约（可替换）
↓
新Implementation（升级后）

- 核心合约（Coupon、Settlement、Compliance等）均采用Transparent Proxy模式部署
- Proxy合约地址固定不变，用户和前端不需要感知升级
- 升级仅替换Implementation合约，Proxy存储层（资产数据）不受影响

升级治理流程（多签+时间锁）：

发起升级提案 → 多签审批（3/5多签） → 时间锁等待期（48小时） → 自动执行升级
↓
等待期内可紧急取消（安全委员会）

- 多签授权**：合约升级需Governance合约3/5多签批准（平台核心成员+独立安全审计师）
- 时间锁（Timelock）**：升级提案通过后强制等待48小时才执行，给社区/用户时间审查
- 紧急升级通道**：发现严重安全漏洞时，安全委员会可走紧急流程（缩短时间锁至4小时，需4/5多签）
- 升级前审计**：每次升级前必须通过第三方安全审计（CertiK/Trail of Bits/OpenZeppelin等）
- 升级日志链上记录**：每次升级的提案、投票、执行全部记录在Governance合约事件日志中（SOX审计追踪）
- 回滚能力**：保留前一版Implementation合约地址，紧急情况可回滚至上一版本（需多签）

不可升级的合约（安全红线）：

- CouponFactory中的券类型标记逻辑（Utility/Security）——类型一旦设定不可修改
- Coupon合约中的所有权记录——所有权不可被升级操作篡改
- 链上转售计数器——防止通过升级绕过Utility Track转售次数限制

4.4 安全要求

4.4.1 基础安全

- 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）

4.4.2 安全事件响应计划（Incident Response）

金融平台必须有完整的安全事件响应计划。保险公司核保、SOX审计、Nasdaq上市审查均会评估IR能力。

事件分级：

级别	定义	响应时限	示例
P0 (紧急)	资产被盗/合约漏洞被利用	立即响应, 15分钟内启动应急	MPC密钥泄露、合约被攻击、大规模资产异常转移
P1 (严重)	数据泄露/系统被入侵	1小时内响应	用户数据泄露、映射表被篡改、管理后台被入侵
P2 (中等)	局部服务异常/可疑活动	4小时内响应	单一API被攻击、异常登录行为、链上可疑交易模式
P3 (低)	潜在风险/安全隐患	24小时内评估	依赖库漏洞披露、安全扫描告警

P0应急流程:

检测到资产异常 → 自动触发紧急冻结 (Governance合约) → 安全团队15分钟内到位
 → 评估影响范围 → 链上资产冻结 (多签确认) → 取证与根因分析
 → 用户通知 (≤24小时) → 修复方案 → 事后报告 → 流程改进

- 紧急冻结能力:** 检测到大规模异常转移时, 自动触发Governance合约冻结涉案地址 (需多签确认生效)
- 数据泄露通知:** CCPA要求72小时内通知受影响用户和加州总检察长; 各州时限不同, 以最严格标准执行
- 取证与证据保全:** 安全事件发生后立即保全日志、链上记录、系统快照, 配合执法机构调查
- 用户沟通:** 安全事件发生后24小时内通过App推送+邮件+官网公告通知用户, 说明影响范围和补救措施
- 事后报告:** 每次P0/P1事件后出具事后分析报告 (RCA), 纳入SOX内部控制评估

漏洞披露与Bug Bounty:

- 建立负责任漏洞披露政策 (Responsible Disclosure Policy)
- Bug Bounty计划: 严重漏洞奖励\$10K-\$100K (智能合约漏洞上限更高)
- 与第三方安全平台合作 (Immunefi/HackerOne)

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)

4.6 UX架构层：Web2体验 + Web3基础设施

核心设计理念：用户看到的是支付宝/Zelle，底层跑的是区块链。区块链是基础设施，不是用户界面。

4.6.1 三层架构



4.6.2 翻译层核心功能

功能	Web2用户操作	翻译层处理	Web3实际执行
注册	手机号/邮箱注册	创建MPC托管钱包，绑定映射	链上地址生成
购买券	点击"立即购买"，银行卡支付	法币→稳定币转换，调用合约	Settlement合约原子交换
转赠	输入朋友手机号，点"转赠"	手机号→地址解析，Gas代付	链上P2P转移 (含合规路由)
消费	出示券码/扫码核销	调用Redemption合约	合约清算+券销毁
查看余额	打开"我的余额"	聚合链上+链下余额	查询链上代币余额
查看记录	打开"交易记录"	交易哈希→订单号映射	读取链上事件日志
发行券 (B端)	填写券模板，点"发布"	调用CouponFactory合约铸造	链上ERC-721/1155铸造

核销 (B端)	扫码/输入券码, 点"核销"	调用Redemption合约	合约清算+券销毁
---------	----------------	----------------	----------

- 手机号/邮箱→地址映射服务**: 维护手机号↔链上地址的安全映射表 (见下方安全方案)
- Gas代付服务 (Paymaster)**: 所有标准模式用户的链上操作Gas由平台代付, 用户零感知
- 法币→稳定币自动转换**: 用户用银行卡支付, 后台自动完成法币→USDC→链上结算
- 交易哈希→订单号映射**: 用户看到可读的订单号 (如GNX-20260209-001234), 后台对应链上TX哈希
- 推送通知翻译**: 链上事件 (Transfer、Redeem) 翻译为用户友好的推送 ("您的券已转赠成功")

映射表安全方案 (防篡改核心):

手机号→地址映射表是平台最高价值的安全资产之一。若被篡改 (A的手机号指向B的地址), 将导致A的券被转给B。必须防止单点篡改。

- MPC多方签名**: 映射记录的创建/修改需多方共同签名 (平台服务器 + HSM硬件安全模块 + 第三方审计节点), 单方无法篡改
- 事务型数据库 + 不可篡改审计日志**: 所有映射操作记录在append-only审计链中, 任何修改可追溯、可检测
- 映射哈希链上锚定**: 映射表的Merkle Root定期写入Genex Chain (如每小时/每日), 链上哈希 = 防篡改证明, 可随时验证映射表完整性
- 加密存储**: 映射表数据加密存储 (AES-256), 密钥由HSM管理
- 最小权限访问控制**: 映射表读写权限严格分离, 写操作需多人审批+MPC签名

4.6.3 术语映射表 (全平台执行)

所有面向用户的界面 (App、网站、邮件、客服话术) 统一使用左列术语, 禁止使用右列术语

用户界面术语	底层技术术语 (仅内部/Pro模式可见)
我的账户	链上钱包地址
我的券	ERC-721/1155 NFT资产
我的余额	链上稳定币 (USDC) 余额
转赠给朋友	P2P链上转移 (Transfer)
购买	链上原子交换 (Atomic Swap)
核销/使用	合约兑付 (Redemption)
订单号	交易哈希 (TX Hash)
交易记录	链上事件日志 (Event Log)
平台积分	GNX代币
支付	法币→稳定币→合约结算
安全验证	链上签名 (由MPC钱包后台执行)

4.6.4 Pro模式 (加密原生用户)

Pro模式为熟悉区块链的用户提供完整的链上操作能力, 但默认关闭

- 在"设置→高级"中开启Pro模式 (需阅读并确认风险提示)

- Pro模式额外功能：查看链上地址、交易哈希、合约交互详情
- Pro模式可切换至自托管钱包 (WalletConnect)
- Pro模式可直接使用MetaMask等外部钱包操作
- 标准模式与Pro模式可随时切换 (自托管→平台托管需转移资产)

4.7 关键第三方依赖与备选方案

平台依赖多个关键第三方服务。任何单一依赖中断都可能导致业务停摆。必须对每个关键依赖有备选方案。

依赖	主选方案	备选方案	中断影响
稳定币	USDC (Circle)	USDT (Tether)、PYUSD (PayPal)	用户无法入金/交易
跨链桥	Axelar	Wormhole、LayerZero	外部链资产无法桥入Genex Chain
KYC供应商	Jumio/Onfido	Veriff、Sumsudb	新用户无法注册/升级KYC
OFAC名单	Chainalysis	Elliptic、TRM Labs	合规筛查中断 (必须暂停服务)
法币通道	主银行合作方	备用支付处理商 (≥2家)	法币出入金中断
MPC钱包服务	Fireblocks/自建	Fordefi、Liminal	标准模式用户无法操作
Travel Rule协议	TRISA	TRP、OpenVASP	大额P2P转移暂停

- 每个关键依赖至少有1个已评估的备选方案
- 法币通道和OFAC筛查必须有热备 (自动切换)，因中断 = 合规违规
- 稳定币支持多币种 (USDC+USDT)，用户可选择，降低单一稳定币风险
- 跨链桥安全评估：桥是历史上最大安全漏洞源，选择时安全性优先于速度
- 年度供应商评审：评估各依赖方的财务稳定性、安全记录、合规状态

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 跨境券流通与全球节点架构

5.2.1 全球券金融网络 (GCFN - Global Coupon Financial Network)

基于Genex Chain的BC跨链能力和多区域部署，构建全球清算节点网络。

Global Coupon Financial Network (GCFN)

- 链上统一使用USDC结算，法币↔USDC转换由各本地节点的法币通道完成
- 汇率管理：使用预言机 (Oracle) 获取实时汇率，交易时锁定汇率
- 国际化合规：各节点独立满足当地监管要求

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 (标准模式下平台MPC托管的全部用户资产)

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, 仅Utility Track)

Phase 1只开放消费型券 (Utility Track), 不开放投资型券。完全规避SEC证券合规风险, 仅需MSB + FTC消费者保护合规。

- Genex Chain主网上线 (Cosmos SDK + cosmos/evm)
- 手机号/邮箱注册系统 (后台自动创建MPC托管钱包, 用户无感知)
- UX翻译层 (手机号→地址映射、Gas代付、订单号映射)
- KYC分级认证 (L0注册即可浏览, L1/L2/L3逐级开放交易权限)

5. 发行方入驻与基础审核 (零保证金, 信用成长)
6. 消费型券发行与上架 (链上铸造, Utility类型标记)
7. 一级市场购买 (银行卡/信用卡支付, 后台自动转换为链上结算)
8. 基础二级市场挂单/购买 (价格上限=面值, 不允许溢价)
9. 手机号/邮箱P2P转赠 (含Travel Rule合规路由)
10. 支付与清算 (合约直接结算)
11. 基础风控与AML (OFAC筛查、链级监控)
12. 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 - Securities Track与扩展

1. 取得法律意见书, 确认投资型券的证券合规路径
2. Broker-Dealer注册 (如需)
3. 开放Securities Track (投资型券交易市场)
4. 完整合规报表
5. 高级风控
6. 跨境券流通

8. 关键指标 (KPI)

8.1 核心业务指标

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	从交易发起链上确认	< 1秒 (CometBFT即时终结)
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%
退款率	退款订单/总订单	< 3%
核销成功率	核销成功/核销发起 (含离线)	> 99.5%

8.2 UX与用户体验指标

指标	描述	目标值
标准模式占比	标准模式用户/总用户	> 95%
注册→首次购买转化率	注册后完成首笔交易的用户比例	> 30%
翻译层API延迟	UX翻译层额外耗时	< 50ms
用户零区块链感知率	调研中"不知道平台用了区块链"的用户比例	> 90%

8.3 安全与合规指标

指标	描述	目标值
映射表完整性	链上锚定哈希校验通过率	100%
OFAC筛查覆盖率	通过OFAC筛查的交易/全部交易	100%
PO事件响应时间	检测到→启动应急	< 15分钟
合约升级成功率	升级成功/升级发起	100%
SAR提交及时率	可疑交易报告按时提交比例	100%

8.4 技术基础设施指标

指标	描述	目标值
系统可用性	平台整体正常运行时间	> 99.9% (SLA)
Genex Chain TPS	链上每秒处理交易数	≥ 5000
Genex Chain出块时间	区块生成间隔	≤ 1秒
DR切换时间	灾难发生→备用系统接管	< 15分钟 (RTO)
数据恢复点	数据丢失窗口	< 1分钟 (RPO)
撮合引擎延迟	订单撮合处理耗时	< 10ms
API响应时间	核心交易接口P99	< 200ms

8.5 容量规划

基础设施随用户规模分阶段扩展，避免前期过度投入。

阶段	用户规模	日交易量	Genex Chain节点	基础设施
Phase 1 (MVP)	10万	50万笔	3自有验证节点	单区域K8s集群
Phase 2 (商业化)	100万	500万笔	5+节点 (含合作机构)	双区域K8s + 热备
Phase 3 (金融化)	1,000万	5,000万笔	10+节点 (多区域)	多区域集群 + GCFN节点

9. 术语表

9.1 金融术语 (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

9.2 技术术语映射 (内部↔用户界面)

详见4.6.3完整术语映射表。以下为关键术语对照。

内部/技术术语	用户界面术语	说明
链上钱包 (Wallet)	我的账户	用户不知道钱包的存在
MPC托管钱包	(后台, 不展示)	平台自动创建并管理
ERC-721/1155代币	我的券	用户看到的是券的图片和信息
P2P Transfer	转赠给朋友	用户输入手机号即可转赠
TX Hash	订单号	如GNX-20260209-001234
Gas Fee	(后台, 不展示)	平台代付, 用户零感知
稳定币 (USDC)	余额 (美元)	用户看到法币金额
Atomic Swap	购买/交易	链上原子交换对用户透明
标准模式	默认模式	99%用户, 平台托管, Web2体验
Pro模式	高级模式	加密原生用户, 自托管, 链上可见

文档版本: v4.1 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: 反向补充——信用评分量化公式与等级映射 (3.5.1), 券定价三因子模型+AI辅助定价引擎 (3.3.4), 发行方分层激励体系 (3.9), AI/ML技术栈详细选型 (4.2), SDK支持计划与API限流 (3.10.1), GCFN全球清算节点架构 (5.2), 容量规划与撮合延迟指标 (8.4-8.5)