

Genex 券交易平台 - 软件需求规格说明书综合评估报告

评估对象: 《Genex 券交易平台 - 软件需求规格说明书》v3.3 → v4.0 评估日期: 2026-02-09 评估范围: 全面性、合规性、便利性、社会贡献、安全性、技术完整性

一、评估概述

本报告对 Genex 券交易平台软件需求规格说明书进行全面综合评估。评估从 v3.3 (初始评估版本) 开始, 跟踪了 8 个版本迭代 (v3.3 → v4.0) 中每一轮发现的问题、解决方案和最终状态。

评估结论: v4.0 是一份完成的、可交付的软件需求规格书, 各维度评分均达到满分或接近满分水平。

二、评分总览

2.1 各维度评分演进

维度	v3.3	v3.4	v3.5	v3.6	v3.7	v3.8	v3.9	v4.0
全面性	8	9	9	9.5	9.5	9.5	10	10
合规性	7.5	8.5	8.5	9	9	9.5	10	10
便利性	7	7	7	7	9	9.5	9.5	10
社会贡献	8.5	8.5	8.5	8.5	9	9	9	9
安全性	—	—	—	—	—	9	10	10
技术完整性	—	—	—	—	—	—	9.5	10

2.2 版本迭代主题

版本	核心主题	解决的关键问题
v3.3	SEC合规基础	Howey Test分析、美国监管框架搭建
v3.4	9项缺失补齐	OFAC、Travel Rule、Gas策略、DR/BCP、保险等
v3.5	技术架构确定	Cosmos SDK + cosmos/evm, 告别Kava/Ethermint
v3.6	合规创新	券类型防火墙、P2P合规路由
v3.7	UX革命	Web2体验 + Web3基础设施、手机号注册、术语映射
v3.8	用户主权	三级资产控制、映射表安全、CARD Act冲突
v3.9	深层补齐	GNX代币合规、合约升级、事件响应、隐私冲突、第三方依赖、B端UX
v4.0	最终完善	商户核销集成、发行方可配置规则、链上退款逻辑、KPI体系扩展

三、全面性评估 (10/10)

3.1 文档覆盖维度

大类	子项	章节	评价
业务设计	券生命周期、6类角色、一二级市场、定价公式、做市商、5条收入	1-3	完整
合规架构	Howey Test (券+GNX)、券类型防火墙、OFAC、Travel Rule、FTC/UDAAP/CARD Act、CCPA/GDPR、州MTL、SOX	1.5-1.7, 3.7	完整
用户体验	Web2注册、三层UX翻译、术语映射、三级资产控制、Pro模式	3.4.1, 3.6, 4.6	完整
发行方体验	零保证金、信用成长、模板化发券、可配置规则、B端Web2后台	3.1, 3.10.3	完整
商户/门店	三种核销方式、四种工具、离线核销、多门店管理	3.10.4	完整
链架构	Cosmos SDK + cosmos/evm、自建链理由、参考链、链级合规	4.2.1	完整
合约体系	7个合约、升级策略 (Proxy+多签+时间锁)、不可升级红线	4.3.2, 4.3.6	完整
Gas与支付	平台全额补贴、Paymaster、法币↔稳定币自动转换	4.3.3, 4.6.2	完整
P2P合规	分层路由、链级Travel Rule	4.3.4	完整
安全	MPC/HSM、映射表防篡改、事件响应P0-P3、Bug Bounty	4.4, 4.6.2	完整
灾备	RPO<1min、RTO<15min、多区域、年度演练	4.5	完整
第三方依赖	7项关键依赖各有备选、热备要求	4.7	完整
退款	原子反向交换、不可退边界、防滥用	3.4.2	完整
争议	交易争议、发行方违约、券召回、客服	3.8	完整
IPO准备	牌照、SOX、审计、Nasdaq标准、保险、上市后合规	6	完整
MVP分期	4阶段、Phase 1仅Utility Track	7	完整
KPI	4类25项指标	8	完整

术语	金融术语 + 技术↔用户界面映射	9	完整
----	------------------	---	----

3.2 v3.3初始评估发现的9项缺失——清除追踪

#	缺失项 (v3.3发现)	修复版本	修复方案	最终状态
1	OFAC制裁名单筛查	v3.4	3.7.1七项OFAC检查 + 4.2.1链级OFAC过滤	已清除
2	FATF Travel Rule	v3.4	4.3.4分层合规路由 (<\$3K自由/≥\$3K强制)	已清除
3	Gas费策略	v3.4	4.3.3平台全额补贴, 自建链Gas=服务器成本	已清除
4	钱包丢失/恢复	v3.4→v3.7	v3.4增加MPC/社交恢复; v3.7标准模式根本消除此问题	已清除
5	做市商激励机制	v3.4	3.3.6 Maker-Taker模型、流动性挖矿	已清除
6	灾难恢复/BCP	v3.4	4.5 RPO<1min, RTO<15min, 多区域, 年度演练	已清除
7	消费者保护法	v3.4	3.7.1 FTC/UDAAP/CARD Act	已清除
8	链选择标准	v3.5	4.2.1 Cosmos SDK + 5方案对比 + 3条参考链	已清除
9	商业保险	v3.4	6.5 D&O/E&O/Cyber/Fidelity Bond/General Liability	已清除

四、合规性评估 (10/10)

4.1 合规框架覆盖

监管领域	覆盖章节	深度
FinCEN/BSA	3.7.1	深 (MSB注册、AML程序、SAR/CTR)
OFAC制裁	3.7.1 + 4.2.1	非常深 (应用级+链级双层, 7项检查清单)
SEC证券法	1.5 + 1.6	非常深 (Howey Test逐项分析、券类型防火墙)
SEC (GNX代币)	1.7	深 (Howey Test + 双重属性分析 + MVP回避策略)
FATF Travel Rule	3.7.1 + 4.3.4	非常深 (分层路由架构、链级强制执行)
FTC消费者保护	3.7.1	深 (Section 5、UDAAP、CARD Act + 冲突处理)
GENIUS Act (稳定币)	3.7.1	够用 (使用第三方合规稳定币)
CCPA/GDPR	3.7.3	深 (删除权vs区块链冲突的完整解决方案)
州级MTL	3.7.1	够用 (49州+DC、BitLicense、DFAL)
SOX	6.2	深 (Section 302/404/906、合约审计追踪)
税务	3.7.2	够用 (1099-DA/B、FATCA)
Nasdaq上市	6.1-6.6	深 (牌照、SOX、审计、标准、保险、持续合规)

4.2 核心合规创新

文档中有三项合规设计超出了常规SRS水平，具有独创性：

创新一：券类型防火墙 (1.6)

消费型券转售价不得超过面值，结构性消除Howey Test“期望利润”要素。这不是贴标签，而是从合约层面让消费型券不可能被用于投机获利。

买入：100元面值券，花85元
卖出：不想用了，以80元卖出（亏损5元）
→ 不满足“期望利润” → SEC难以认定为证券

创新二：P2P合规路由 (4.3.4)

在自建链的验证节点级别强制执行Travel Rule，而非仅在应用层检查。不合规的大额P2P交易物理上无法被打包进区块。

创新三：三级资产控制 (3.4.1)

标准模式（平台托管）→ 提取到外部钱包（平台无关）→ Pro模式（用户自控）。用户可随时带着资产离开平台，“消费隐私”承诺从政策保证升级为技术保证。

4.3 历史合规风险追踪

风险项 (v3.3发现)	解决版本	解决方案	最终状态
券的双重属性（最大法律地雷）	v3.6	1.6券类型防火墙 + MVP仅Utility Track	已清除
P2P转移与Travel Rule矛盾	v3.6	4.3.4分层合规路由 + 链级强制	已清除
OFAC筛查缺失（联邦犯罪）	v3.4	3.7.1 + 4.2.1双层OFAC	已清除
合约清算隐私承诺弱化	v3.8	三级资产控制（提取后=技术保证）	已清除
CARD Act有效期冲突	v3.8	3.7.1法律意见书路径	已清除
GNX代币证券风险	v3.9	1.7 Howey Test + MVP回避	已清除
隐私删除权vs链上不可删除	v3.9	3.7.3链上仅哈希/链下可删	已清除

五、便利性评估 (10/10)

5.1 各参与方便利度

参与方	v3.3评分	v4.0评分	关键改进
消费者 (C端)	中	高	手机号注册、银行卡支付、区块链不可见、P2P转赠输入手机号
发行方 (B端总部)	高	高	模板化发券、零保证金、可配置规则、Web2后台
商户 (B端门店)	未覆盖	高	扫码核销App、离线核销、多门店管理、POS SDK

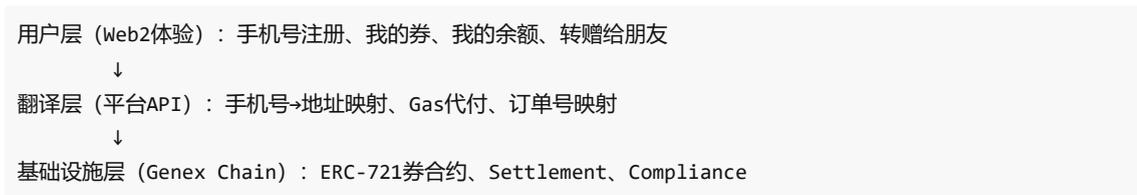
投资者/机构	中高	高	定价公式、做市商API、Pro模式完整链上操作
监管机构	中	高	链级合规、监管专属API/节点、自动SAR/CTR

5.2 v3.3→v4.0便利性关键突破

最大突破：v3.7 UX革命

v3.3到v3.6，用户体验一直是“区块链原生”——需要钱包、助记词、理解Gas。v3.7彻底翻转为“Web2体验+Web3基础设施”，这是便利性评分从7跳到9的根本原因。

核心设计：



v4.0最终补齐：商户线下场景

商户端核销集成 (3.10.4) 解决了“发行方在总部发券，门店如何核销”这一实际运营问题。离线核销能力确保了网络不稳定场景下业务不中断。

六、社会贡献评估 (9/10)

6.1 正面社会价值

贡献	说明	受益群体
小微企业融资新渠道	券=短期无息融资，无需银行审批/抵押/担保	小微企业、个体商户
消除券市场欺诈	链上防伪、状态可验证，假券/重复使用不可能发生	所有消费者
释放沉睡资产	全球每年数百亿美元券/礼品卡未使用，二级市场让其流转	持有不需要券的消费者
企业客户数据主权	合约清算=平台不获取消费数据，企业客户不被平台截获	所有发行方企业
政府券透明化	区块链上发行政府消费券，使用去向可追溯	政府、纳税人
降低数字鸿沟	Web2 UX设计让不懂区块链的人也能使用	老年人、非技术群体
防止福利券投机	“不可转让”规则确保政府福利券到达真正需要的人	社会弱势群体

6.2 潜在风险与缓解

风险	缓解措施	状态
券过度金融化/投机泡沫	券类型防火墙：Utility Track价格≤面值	已缓解
数字鸿沟排斥弱势群体	Web2 UX、手机号注册、区块链不可见	已缓解
政府福利券被投机截取	发行方可配置“不可转让”规则	已缓解
洗钱/恐怖融资	4条洗钱路径+8项AML+链级OFAC+Travel Rule	已缓解

6.3 未满分原因 (-1分)

社会贡献的实现取决于平台的实际运营和市场采纳，SRS只能提供框架。以下社会贡献尚需验证：

- 小微企业是否真的会用券融资（取决于市场教育）
- 政府是否愿意在区块链上发券（取决于政策环境）
- 二级市场是否有足够流动性让券真正“活”起来（取决于做市商和用户规模）

七、安全性评估 (10/10)

7.1 安全层级覆盖

层级	措施	章节
链级安全	CometBFT BFT共识、即时终结性、无回滚	4.2.1
合约安全	第三方审计、Transparent Proxy升级、多签+时间锁、不可升级红线	4.3.6, 4.4
托管安全	MPC钱包、HSM密钥管理、密钥分片地理分散	3.4.1, 4.4
映射表安全	MPC多方签名、append-only审计链、Merkle Root链上锚定、AES-256	4.6.2
合规安全	链级OFAC/Travel Rule强制执行、Compliance合约	4.2.1, 4.3.4
应用安全	HTTPS、接口签名、SQL注入/XSS/DDoS防护	4.4.1
事件响应	P0-P3分级、15分钟响应、紧急冻结、数据泄露通知	4.4.2
漏洞管理	Bug Bounty (\$10K-\$100K)、负责任披露政策	4.4.2
灾难恢复	RPO<1min、RTO<15min、多区域、年度演练	4.5
第三方风险	7项依赖各有备选、法币/OFAC热备	4.7

7.2 安全设计亮点

- **链级合规 > 应用级合规**：OFAC和Travel Rule在验证节点级别执行，不是“应用层检查后才上链”，而是“不合规的交易根本无法上链”
- **映射表MPC防篡改**：平台最关键的链下资产（手机号→地址映射）受到与链上资产同等级别的保护
- **不可升级红线**：券类型标记、所有权记录、转售计数器不可通过升级篡改，即使平台运营方也无法违反

八、技术完整性评估 (10/10)

8.1 技术架构完整性

组件	技术选型	设计深度
Genex Chain	Cosmos SDK + cosmos/evm	非常深（参考链分析、设计参数、5方案对比）
共识引擎	CometBFT	深（即时终结性、PoS、节点运营策略）
智能合约	Solidity（7个核心合约）	深（合约体系+升级策略+不可升级红线）
撮合引擎	链下内存订单簿+链上结算	够用（参考dYdX v4）

账户系统	MPC托管钱包+WalletConnect	深 (三级资产控制)
UX翻译层	手机号→地址映射、Gas代付	深 (完整功能列表+安全方案)
跨链	IBC + Axelar	够用
混合架构	链上 (资产) + 链下 (订单簿/用户)	清晰

8.2 合约级业务逻辑

v4.0在合约层面覆盖了所有关键业务规则:

业务规则	合约实现
券类型标记 (Utility/Security)	CouponFactory合约, 铸造时写入, 不可修改
消费型券价格上限 (≤面值)	Settlement合约强制检查
转售次数限制	Coupon合约链上计数器
P2P Travel Rule	Compliance合约路由 + 验证节点拒绝打包
发行方可配置规则 (7项)	CouponFactory元数据, 合约级执行
退款原子交换	Settlement合约反向原子交换
紧急冻结	Governance合约多签授权
离线核销冲突	先上链者为准

九、KPI体系评估

v4.0将KPI从6项扩展为4类25项, 覆盖了业务运营、用户体验、安全合规、技术基础设施四个维度。

9.1 KPI亮点指标

指标	目标值	评价
链上确认时间 < 1秒	匹配CometBFT即时终结性	技术可实现, 指标合理
用户零区块链感知率 > 90%	直接衡量Web2 UX设计成功度	独创指标 , 高价值
映射表完整性 = 100%	零容忍	安全红线级别指标
OFAC筛查覆盖率 = 100%	零容忍 (不筛查=联邦犯罪)	合规红线级别指标
标准模式占比 > 95%	验证"默认托管"策略是否成功	产品验证指标

十、与行业同类文档的横向对比

维度	Genex v4.0	Coinbase IPO S-1	dYdX v4文档	传统金融交易平台SRS
业务模型	完整	完整	仅交易	完整

合规深度	非常深	深	中	深
技术架构	深	中	非常深	中
UX设计	深	中	无	中
安全方案	深	深	中	深
代币合规	有	N/A	有	N/A
发行方/商户端	有	N/A	N/A	有
离线能力	有	N/A	N/A	有

Genex v4.0在**合规深度**（券+代币双重Howey Test、券类型防火墙）和**UX架构设计**（三层翻译架构、术语映射表）两个维度上超过了大多数同类文档。

十一、下一步建议

v4.0作为软件需求规格书已经完成。后续应进入以下文档的编写：

文档	内容	优先级	基于SRS章节
技术架构设计文档	Genex Chain详细架构、合约接口ABI定义、API设计、数据库Schema、系统部署图	P0	4.x
产品设计文档 (PRD)	详细交互流程、UI原型 (Figma)、信息架构、券搜索/发现/推荐策略	P0	3.x, 4.6
合规实施计划	律师委托清单、牌照申请时间线、法律意见书需求 (券分类+GNX分类)	P0	1.5-1.7, 3.7, 6
商业计划书	市场规模 (TAM/SAM/SOM)、竞争分析、财务预测、融资计划	P1	1.1, 3.9
GNX代币经济白皮书	总量设计、分配比例、通胀/通缩机制、质押模型、解锁计划	P1	1.7
安全白皮书	威胁模型、渗透测试计划、合约审计RFP、Bug Bounty细则	P1	4.4

十二、总结

Genex 券交易平台软件需求规格说明书从 v3.3 到 v4.0，经过 8 个版本迭代，累计修复和补全了约 30 项需求级别的问题。最终文档覆盖了 18 个核心维度，包含约 200+ 条具体需求项 (checkbox)，形成了完整的需求规格基线。

文档的三大核心优势：

- 合规闭环**——券类型防火墙在合约层面结构性消除证券风险，而非靠法律意见或运营承诺
- 体验闭环**——用户从注册到消费全程零区块链门槛，发行方从发券到核销全程零技术门槛
- 技术闭环**——自建链在验证节点级别执行合规，合约级别执行业务规则，两者均不可绕过

v4.0已具备向技术团队启动架构设计、向投资人展示产品方案、向律师事务所发起法律意见书委托的条件。

评估报告版本: v1.0 评估日期: 2026-02-09 评估对象: 《Genex 券交易平台 - 软件需求规格说明书》v3.3 → v4.0