

D02 租户与组织域 · 设计文档

本域总览见《账号计费中心 · 结构大纲》。本文为该域完整设计：定位与边界 / 角色与依赖 / 数据模型 / 核心流程 / 接口契约 / 关键约束与验收标准。

1. 定位与边界

定位：工作区（租户）与成员归属的管理者。回答三个问题——「资源与费用归属谁」（工作区）、「谁可以操作」（成员与角色）、「用量如何切分」（组）。

核心概念

- 工作区 = 租户。个人工作区与企业工作区同构，以 `kind` 区分：两者都有组织、成员关系、钱包、默认组，权限与计费链路上不引入第二套模型。
- 组 = 额度归因与准入执行的锚点。组成员、成员角色、额度配置在本域；额度的实际扣减与执行由计量与计费域完成。
- 成员 = 关联记录，不是身份。本域只在「用户 × 工作区」上落一行成员关系与角色，不复制用户身份。

边界

- 本域只管归属与角色：工作区、成员关系、邀请、组、组配额配置、组织审计。不管身份凭证（账号与身份域）、不管金额计算（钱包与账务域）。
- 创建企业不迁移余额：个人钱包与企业钱包各自独立，无隐式内部转账。余额从企业回到个人是显式操作（余额转回），需 Owner 主动发起。
- 不判定实名：企业实名由风控与合规域判定，本域只承载企业实名状态位与等级位，并据此放行/收紧企业维度能力。
- 不执行扣费：本域维护组额度配置，不参与扣减。计费面只认工作区（钱包归属），不认组织成员——成员维度的费用归因经组的归属列为弱引用。

`kind` 语义（本域最关键的口径）

kind	语义	可变操作
<code>personal</code>	只读身份锚点：kind 不可变、不可改名、不可邀请、不可退出、不可注销、不可转让；唯一成员 = 本人 Owner	无
<code>company</code>	可变租户	改名 / 联系方式 / 邀请 / 成员管理 / 组管理 / 转让 / 余额转回 / 注销

- 没有「个人升级为企业」的路径：创建企业恒为新建 `company` 工作区，个人工作区原样保留。kind 在创建后无任何改写路径。
- 个人工作区只随账号注销关闭，不提供独立关闭入口。

2. 角色与依赖

组织角色（三级）：owner > admin > member。组织恒有主——Owner 唯一，且不可被移除、不可主动退出。

组内角色（两级）：member / admin（组管理员），与组织角色相互独立：组织 Member 可以是某组的管理员；组管理员不因组内身份获得组织级权限。

能力矩阵

操作	Owner	Admin	Member
查看工作区列表 / 组织信息	✓	✓	✓
编辑企业资料 / 邀请成员	✓	✓	✗
普通成员角色升降	✓	✓	✗
Admin 角色变更 / 移除 Admin	✓	✗	✗
建组 / 停用启用 / 设组额度	✓	✓	✗
本组组管理员	✗（除自身组）	✗（除自身组）	仅可调本组普通成员
转让 Owner / 余额转回 / 注销企业	✓	✗	✗
退出组织	✗（须先转让）	✓	✓
组织审计查询	✓	✓	✗

上游依赖

- 账号与身份域：用户身份、门户令牌、联系方式凭据（成员联系方式一律经凭据域聚合，本域不存明文）。
- 通知与触达域：邀请通知（邮件 / 短信，best-effort）、成员站内信（注销告知）。

下游被依赖（谁引用本域）

引用方	引用内容	语义
钱包与账务域	工作区 → 钱包 1:1	工作区是计费与资金归属主体
订购与支付域	工作区、组 → 账户访问密钥	密钥归属某工作区，消耗归因落到某组
计量与计费域	工作区、组、成员（弱引用）	用量归属三层切分：工作区 / 组 / 成员
发票域	工作区	发票主体与抬头归属
风控与合规域	工作区	企业实名核验与风险事件归属
账户状态与准入域	工作区状态	工作区关闭触发对应钱包的准入状态发布
运营管理	组织投影（只读）	运营面按工作区视角查看成员与组，仅读不写

3. 数据模型

3.1 域内关联总览

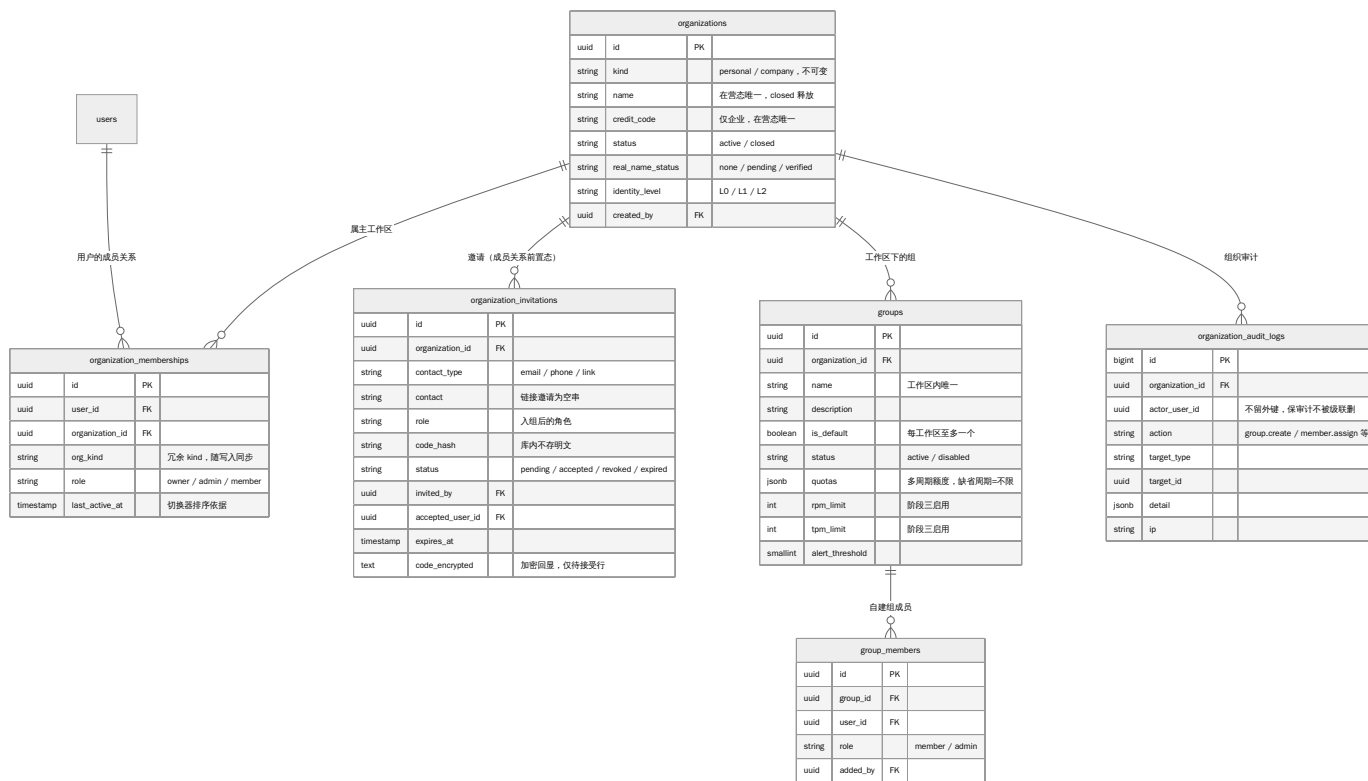


图 1

默认组的成员是派生视图 (= 工作区全体成员)，不落 `group_members` 行——从模型层消灭「移出唯一组」的边界问题。

3.2 域间引用

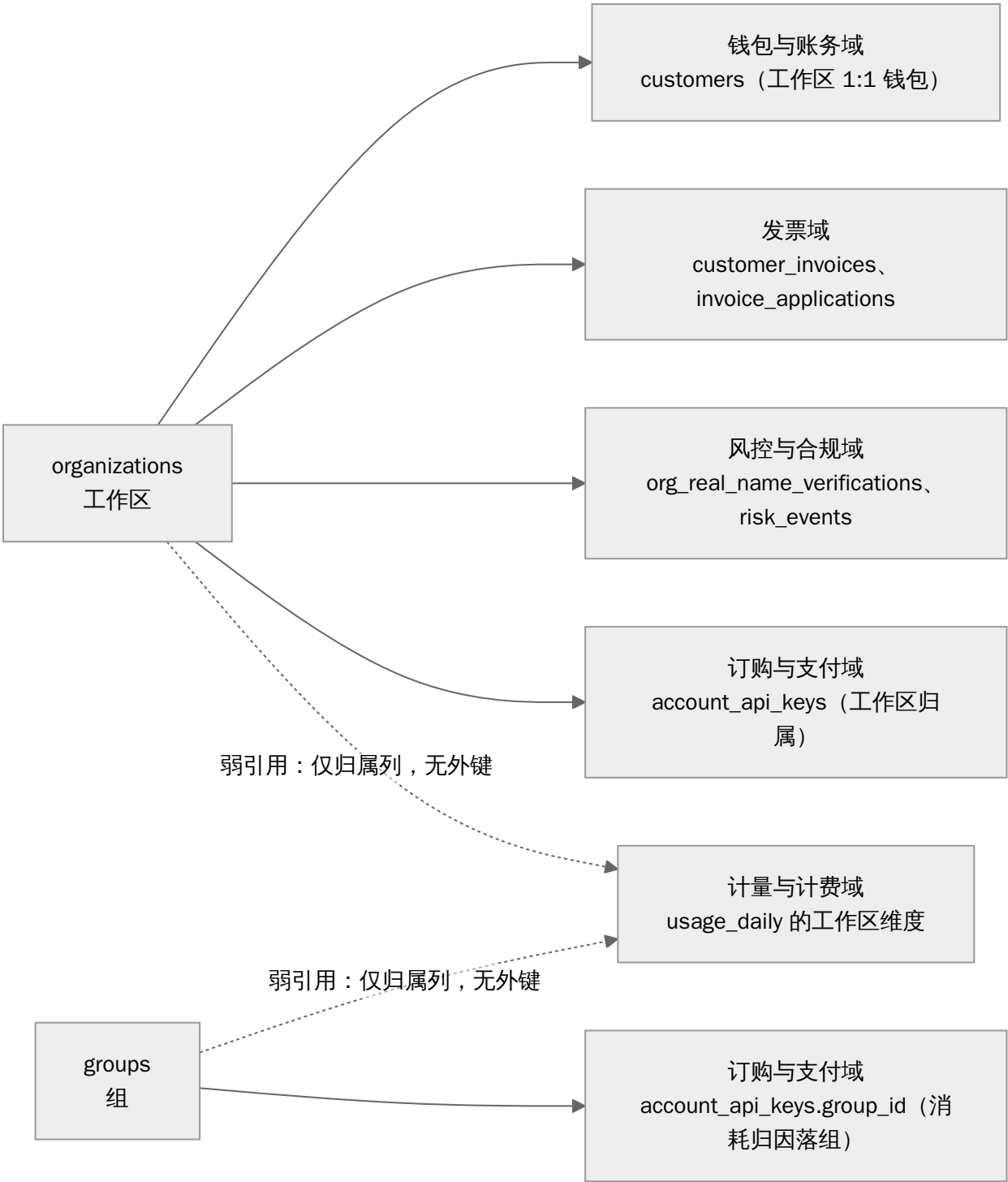


图 2

- `users` 由本域引用（成员关系的用户侧），不入本域表清单。
- 计量域刻意不建外键：用量是高频写入的事实表，归属列作为弱引用，避免删除约束拖住写入路径。

3.3 表清单 (6 表)

表	职责	关键字段
organizations	工作区（租户）主体，个人 / 企业同构	kind / name / credit_code / status / real_name_status / identity_level / created_by
organization_memberships	用户 × 工作区的成员关系与角色	user_id / organization_id / org_kind / role / last_active_at
organization_invitations	邀请（成员关系前置态）	contact_type / contact / role / code_hash / status / expires_at / accepted_user_id / code_encrypted
groups	额度归因与准入执行锚点	organization_id / name / description / is_default / status / quotas / rpm_limit / tpm_limit / alert_threshold
group_members	自建组成员（默认组不落行）	group_id / user_id / role / added_by
organization_audit_logs	组织视角留痕，Owner / Admin 可查	organization_id / actor_user_id / action / target_type / target_id / detail / ip

3.4 设计约束

1. kind 不可变：不存在改写 kind 的路径，个人 ↔ 企业之间没有翻转操作。
 2. 在营态唯一：名称仅对在营工作区唯一、统一社会信用代码仅对在营企业唯一；已关闭工作区释放名称与执照，同一执照可重新注册。预检与落库双段口径一致（并发兜底）。
 3. 组织恒有主：DB 层以「在营 owner 唯一索引」兜底，任何并发路径都至多一行 owner。
 4. 不重复加入：（用户，工作区）唯一，作为并发邀请竞态的兜底。
 5. 邀请码零明文：库内只存哈希用于比对，另存加密副本仅用于待接受行的列表回显；明文只在创建响应中出现一次。
 6. 默认组不可破：每工作区至多一个默认组，不可停用、成员不可直接设置。
 7. 组名工作区内唯一；组数上限 50（含默认组）。
 8. 审计只增：审计行与业务变更同事务写入，不提供改写或删除路径。
-

4. 核心流程

4.1 个人注册即建立工作区

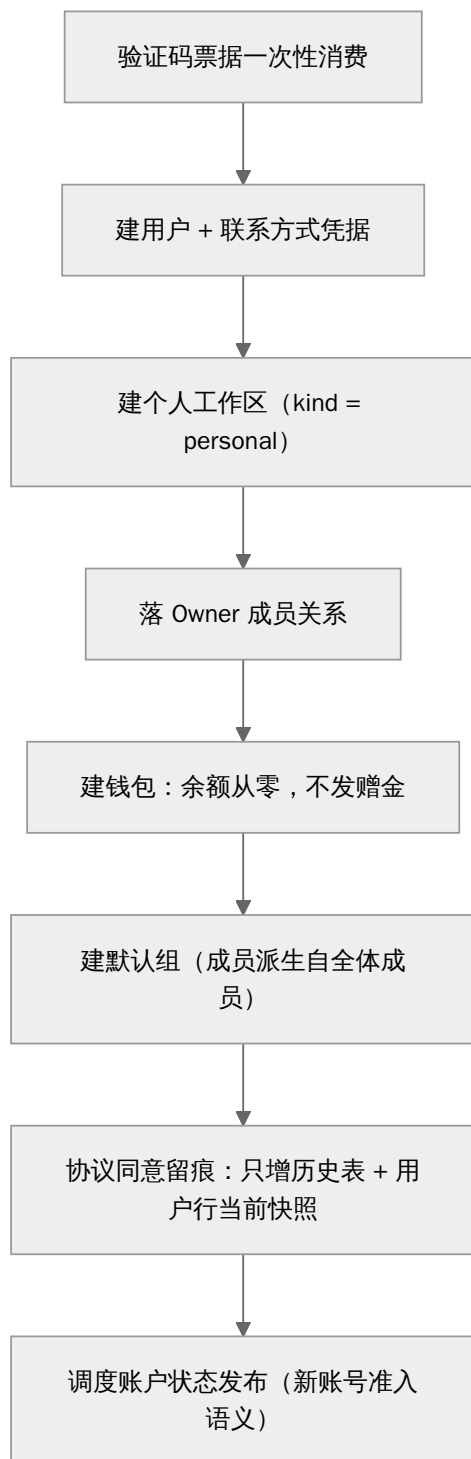


图 3

- 注册即同时具备「工作区 + 钱包 + 默认组」，故后续所有计费与归因路径都无需为空工作区做特例分支。

4.2 创建企业

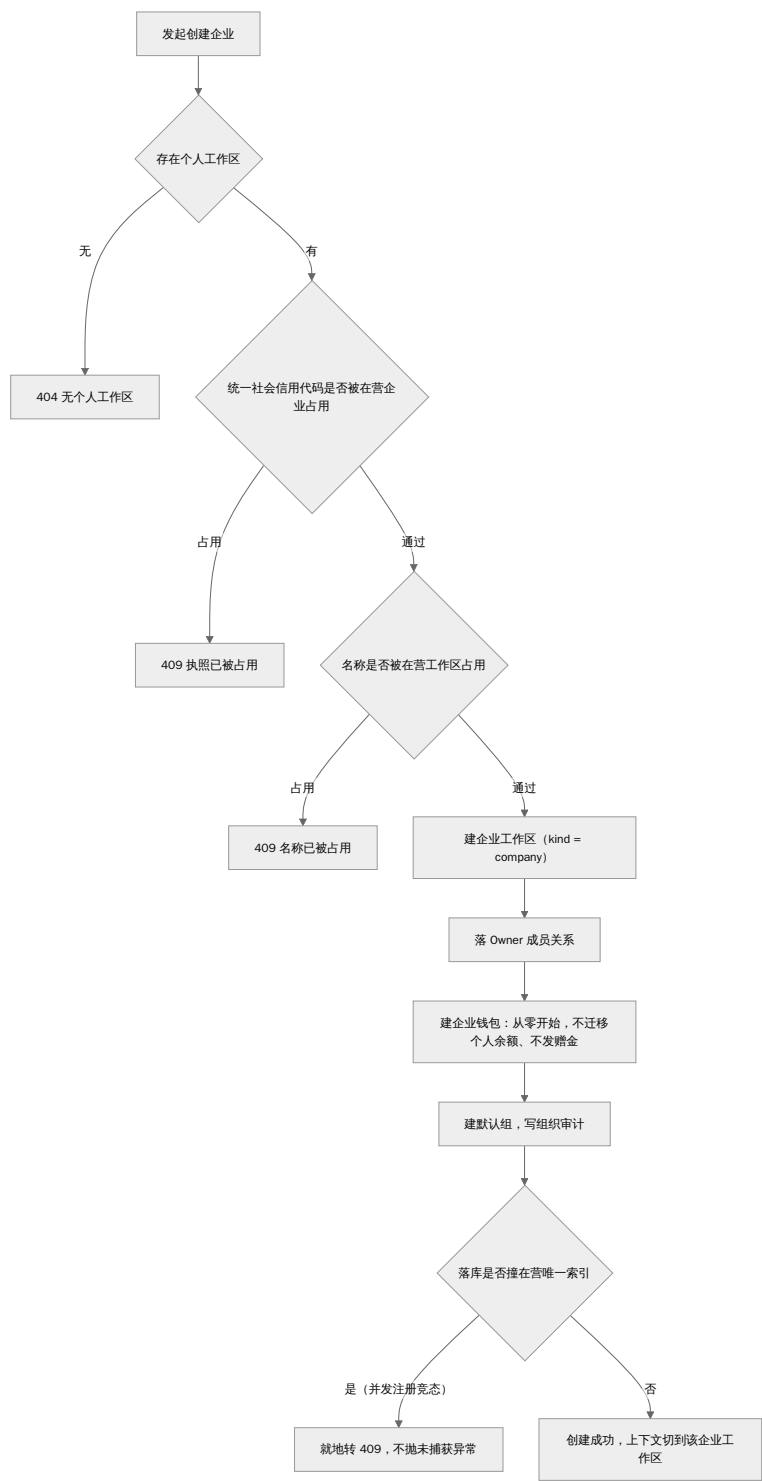


图 4

- 创建企业和个人注册同构：都建工作区 + 钱包 + 默认组，差别只在 kind、执照字段、是否发赠金。

4.3 邀请与入组

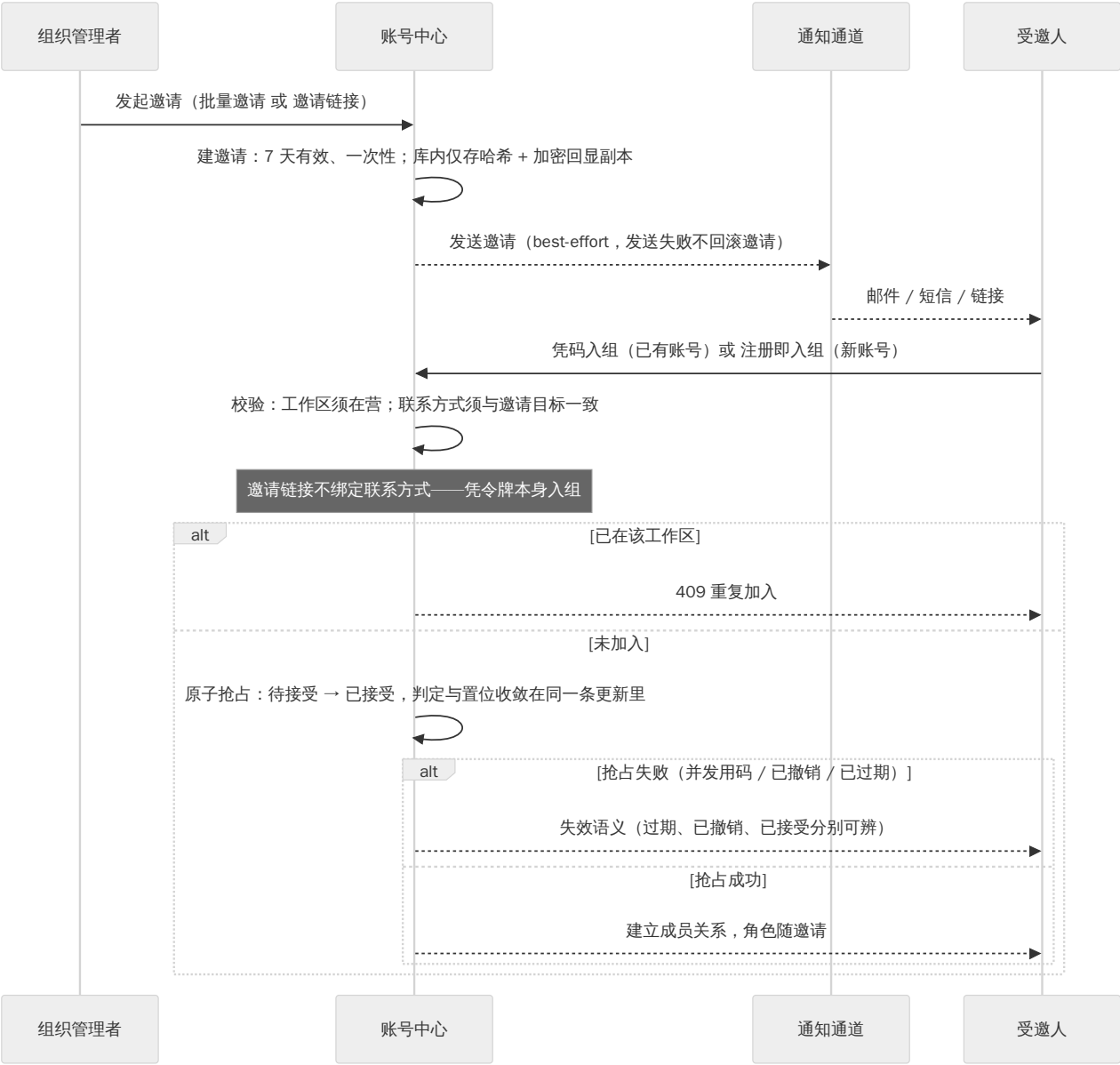


图 5

- 注册路径的抢占在建用户之前：抢占失败即早退，不产生半成品账号。
- 一个用户可同时加入多个企业；只禁止重复加入同一工作区。

4.4 成员角色变更与移除

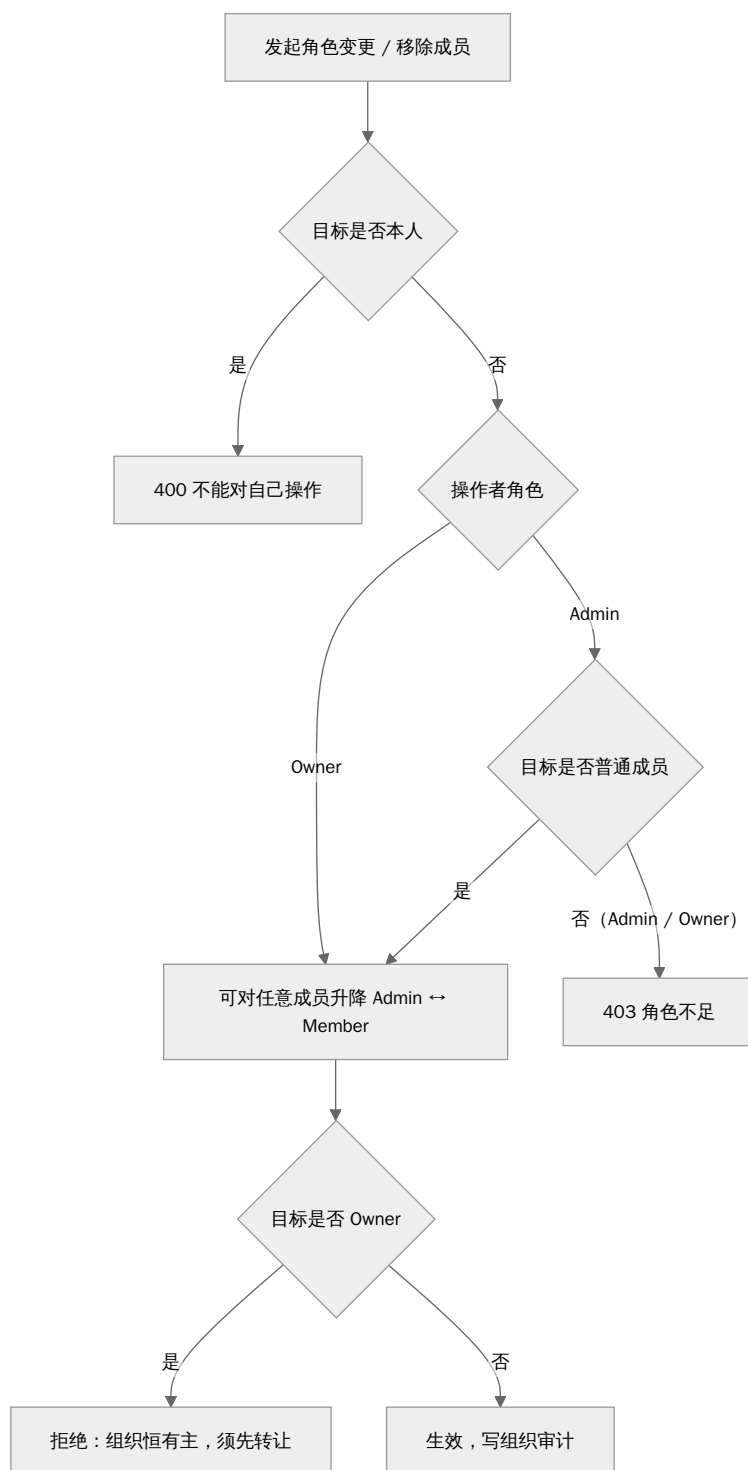


图 6

- 移除成员同时使其名下组织内的账户访问密钥失效，避免「人已离开、密钥仍可计费」。
- 变更后立即生效：目标成员在该工作区的后续请求按新角色判权。

4.5 组与组配额

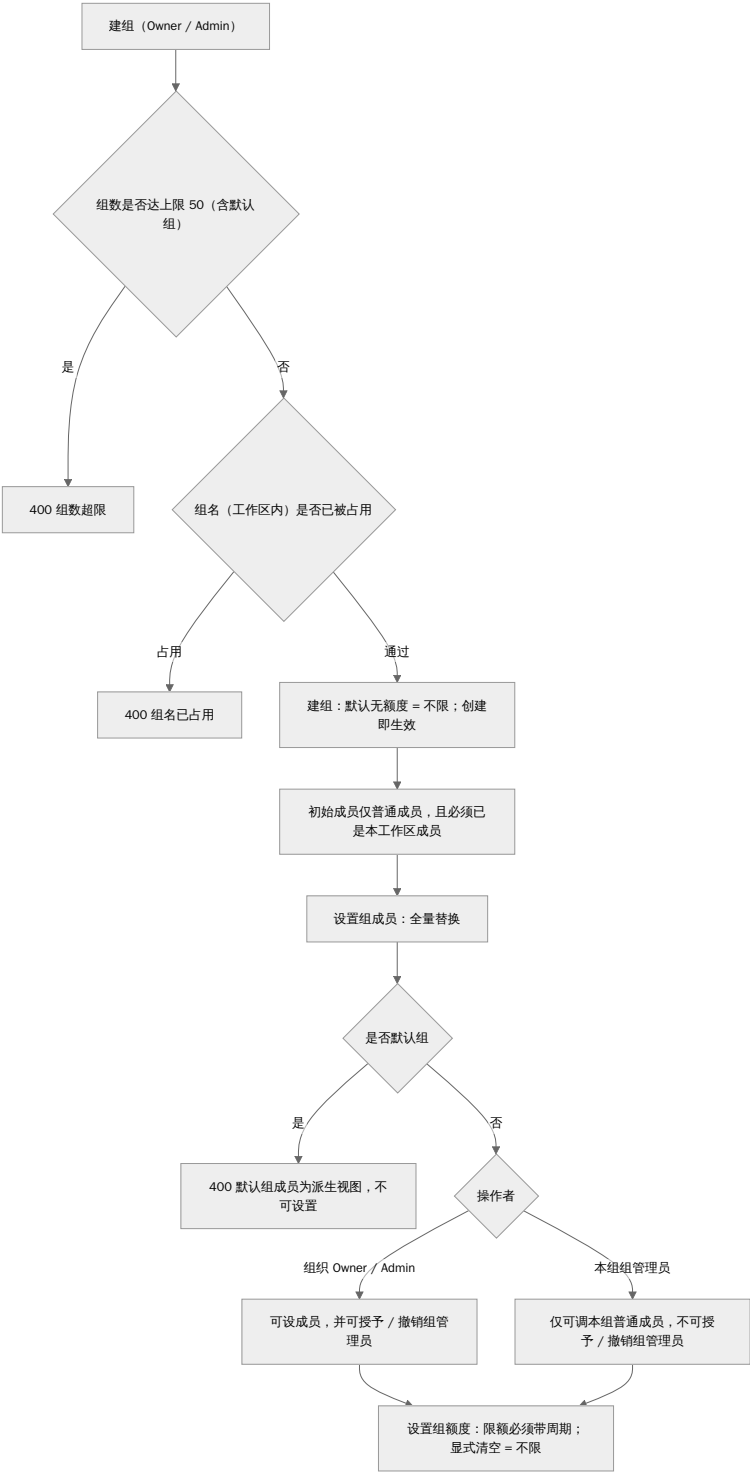


图 7

- 停用组为幂等操作；默认组不可停用。
- 组至少保留一名成员：设置成员时若结果为空集则拒绝。
- 组额度支持多周期（日 / 周 / 月 / 总计），缺省周期表示不限；限速项与告警阈值属阶段三能力，字段已就位。

4.6 所有权转让

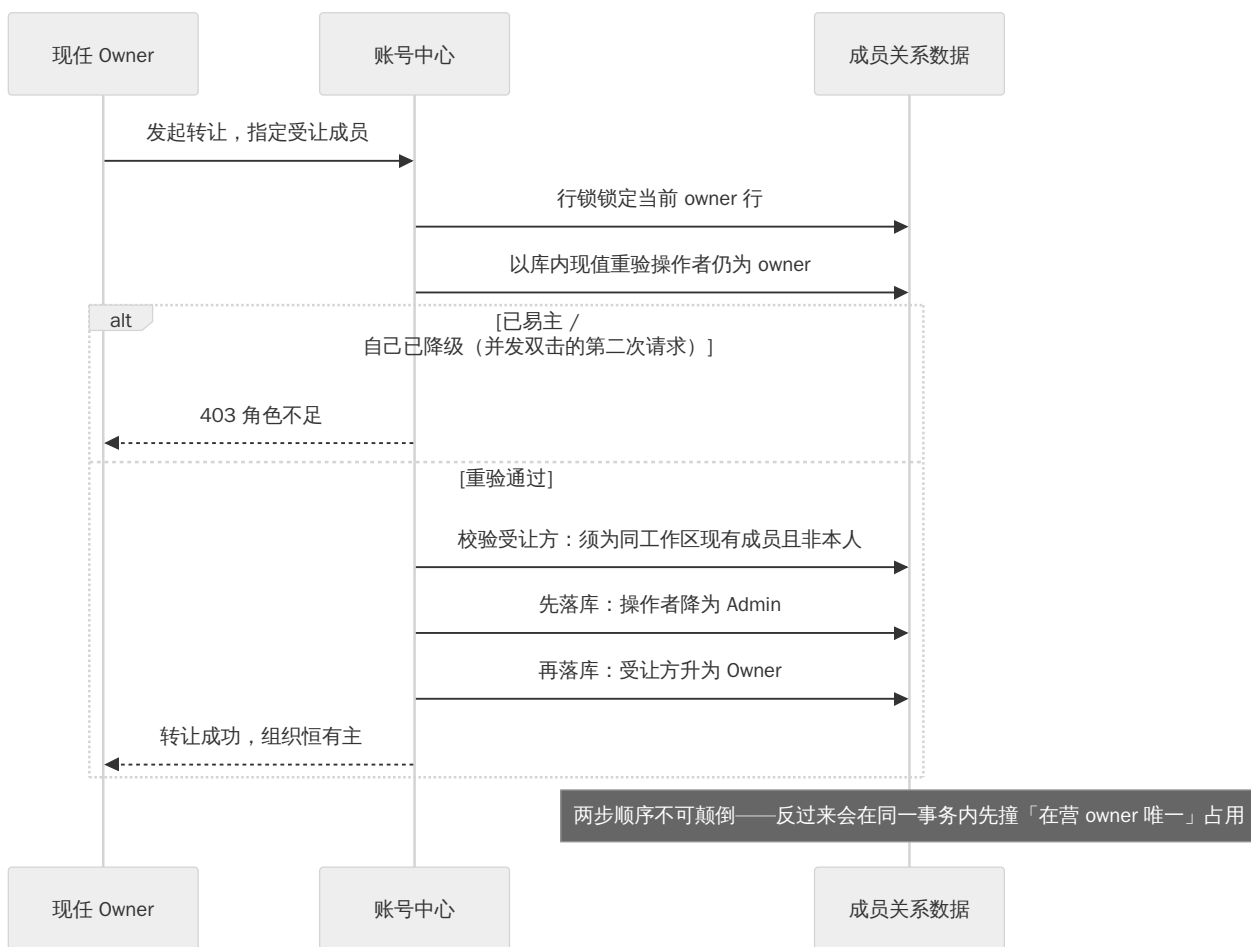


图 8

- 转让是唯一的 owner 变更路径：移除 Owner、Owner 退出均被拒绝。

4.7 企业余额转回个人钱包

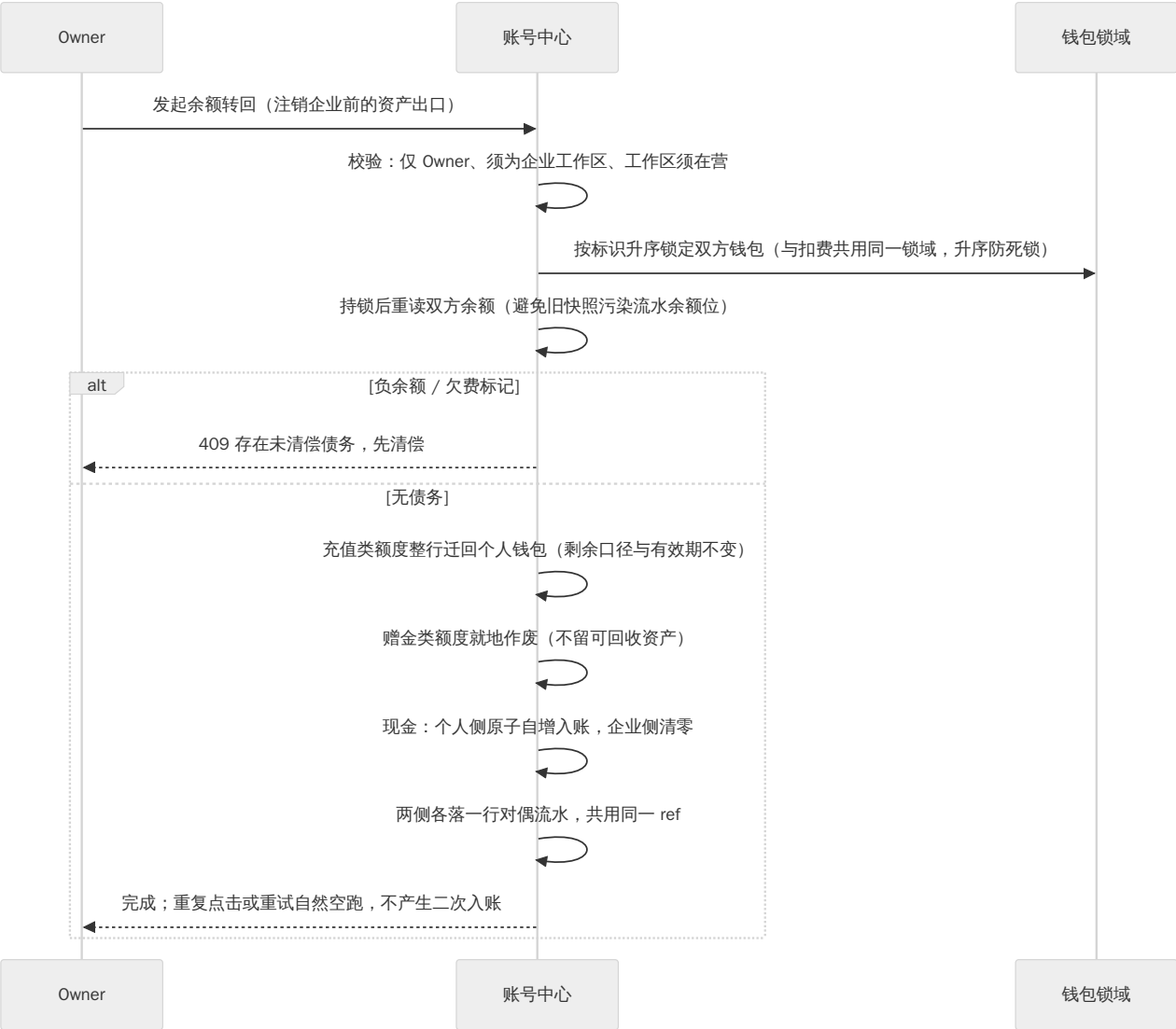


图 9

- 对偶流水是必须的：流水是资金真相源，企业侧资产不能凭空消失，迁出与迁入两侧都要各自可解释。
- 只有 Owner 可发起；企业侧清零由钱包锁串行保护。

4.8 注销企业

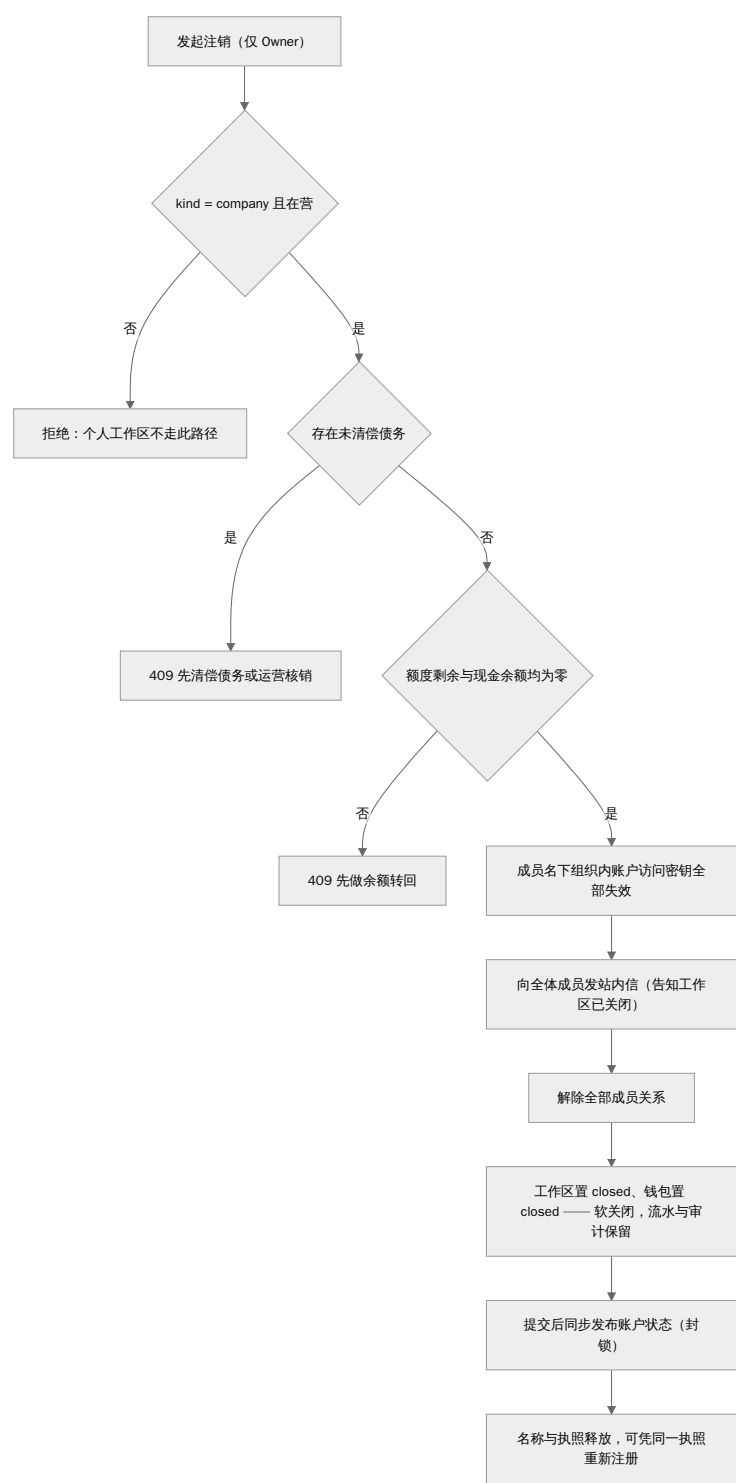


图 10

- 软关闭：不做物理删除。资金流水、审计、成员关系历史按规定保留，运营面仍可感知已关闭工作区（用于停用对应租户投影）。
- 注销前必须先处理债务与余额，堵死两条口子：「刷到负余额再注销让债务蒸发」、「资产遗留在已关闭工作区无法取回」。

4.9 工作区上下文解析（切换器与请求鉴权）

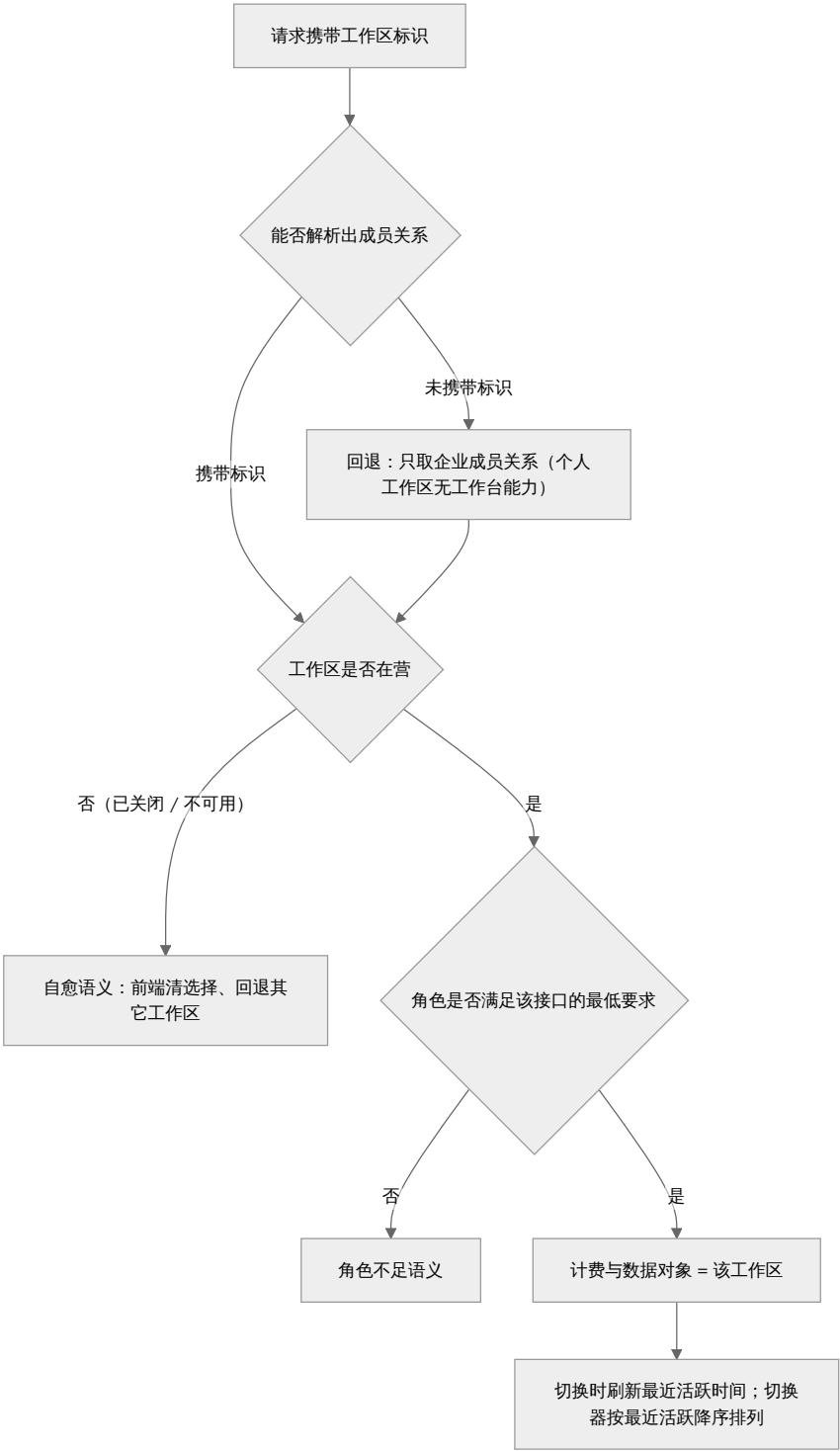


图 11

- 「工作区不可用」与「角色不足」是两种不同语义：前者前端应清选择回退（跳默认页解决不了失效工作区），后者提示权限不足。

5. 接口契约

5.1 组织与工作区 (/api/account)

方法	路径	语义
GET	/organizations	我的工作区列表：个人工作区居首 + 已加入企业，按最近活跃降序
POST	/organizations	创建企业工作区（Owner 由创建人自动获得）
GET	/organization	组织信息 + 成员列表（Member 可读，联系方式脱敏；响应带 kind 供前端分流）
PUT	/organization	编辑企业资料（Owner / Admin；个人工作区拒绝）
PATCH	/organization/touch	工作区活跃心跳（切换时调用，更新成员级最近活跃时间）
DELETE	/organization	注销企业（仅 Owner；软关闭）
POST	/organization/leave	退出组织（Admin / Member，可指定工作区）
POST	/organization/ownership-transfer	转让 Owner（受让方须为同工作区成员）
POST	/organization/balance/transfer	企业余额转回个人钱包（仅 Owner）

5.2 成员管理 (/api/account)

方法	路径	语义
PUT	/organization/members	成员角色变更（Owner 可调任意；Admin 仅可升降普通成员）
DELETE	/organization/members	移除成员（Admin 仅可移除普通成员；不能移除自己 / Owner）
PUT	/members/{membership_id}/role	角色变更（按成员关系定位的历史入口，内部换算后走同一业务校验）
DELETE	/members/{membership_id}	移除成员（同上历史入口）

5.3 组管理 (/api/account)

方法	路径	语义
GET	/groups	组列表：Owner / Admin 见全部，普通成员见默认组 + 所在组
POST	/groups	建组（组数上限 50、组名工作区内唯一、初始成员可选）
PATCH	/groups/{group_id}	改名 / 描述 / 限速（显式 null = 清空不限）
POST	/groups/{group_id}/disable	停用组（默认组不可停用；幂等）
POST	/groups/{group_id}/enable	恢复启用
GET	/groups/{group_id}/members	组成员：默认组 = 全体成员派生，自建组 = 组内成员（工作区内只读）

方法	路径	语义
PUT	<code>/groups/{group_id}/members</code>	全量替换组成员（默认组拒绝；组管理员不可授予组管理员）
GET	<code>/groups/{group_id}/quota</code>	组额度与限速查看
PUT	<code>/groups/{group_id}/quota</code>	组额度设置（限额必须带周期；显式清空 = 不限）

5.4 邀请 (`/api/account`)

方法	路径	语义
POST	<code>/invitations</code>	批量邀请（邮件 / 短信；7 天有效；通知 best-effort）
POST	<code>/invitations/link</code>	创建邀请链接（一次性令牌，随响应返回由前端拼链）
GET	<code>/invitations</code>	邀请列表（待接受 / 已接受 / 已撤销 / 已过期；过期项就地标记）
POST	<code>/invitations/{invitation_id}/revoke</code>	撤销邀请
POST	<code>/invitations/accept</code>	已有账号凭码入组
POST	<code>/register/organization</code>	企业注册（注册即建企业工作区，创建人 Owner）
POST	<code>/register/invite</code>	受邀注册（注册即入组，一次请求完成建号与入组）

5.5 内部组织投影 (`/internal/organizations`)

方法	路径	语义
GET	<code>/internal/organizations</code>	工作区列表：含成员标识与 Owner 联系方式摘要，供运营面按工作区投影
GET	<code>/internal/organizations/{org_id}</code>	工作区详情：成员（联系方式脱敏）+ 组摘要 + 钱包锚点标识
GET	<code>/internal/organizations/{org_id}/groups</code>	工作区下全部组的额度口径（与单组查询同字段）

- 鉴权：内部服务令牌（运营范围）。字段白名单，不透内部状态；联系方式一律脱敏。
- 关闭态工作区在列表中可见：运营面需感知关闭以停用对应租户。

6. 关键约束与验收标准

6.1 约束

1. kind 不可变、锚点受保护：个人工作区上任何企业维度操作（改名 / 邀请 / 成员 / 组 / 转让 / 注销 / 余额转回）一律拒绝，且系统不提供 kind 翻转路径。
2. 组织恒有主：Owner 唯一、不可被移除、不可退出；转让为唯一变更路径；并发转让由「行锁 + 在营 owner 唯一索引」双兜底。

- 3. 单次消费原子化：邀请接受与受邀注册的抢占以条件更新完成，并发凭同一邀请至多一人成功，且失败方不产生半成品账号。
- 4. 注销先清零：存在债务或余额未处理时拒绝注销；注销为软关闭，保留资金流水与审计。
- 5. 资金迁移对偶留痕：额度迁出 / 迁入两侧各落一行只增流水并共用同一 ref；额度行改挂保留，不做物理合并。
- 6. 并发互斥与锁序：钱包类变更（扣费 / 充值 / 余额转回）共用同一钱包锁域；多钱包场景按标识升序加锁，防死锁。
- 7. 两类台账分离：组织审计按工作区聚合给 Owner / Admin；本人安全日志按用户聚合（归账号与身份域）。二者不混用。
- 8. 投影只读且最小化：运营面组织投影只读、字段白名单、联系方式脱敏；不提供经投影写组织的路径。
- 9. 同一邀请至多一次有效：邀请过期即失效，过期状态在查询时就地收敛，不留「看起来仍待接受」的假状态。

6.2 验收标准

#	验收口径
1	在营期间重复注册同一名称 / 同一执照 → 409；工作区注销后，同一名称与执照可重新注册成功
2	并发两次「接受同一邀请」：仅一人成功，另一人失败，且成员关系只有一行
3	同工作区并发两次转让：仅一次成功；任何时刻 owner 行数 ≤ 1
4	余额转回：企业侧现金清零、个人侧按原子自增入账；两侧各有且仅有一行流水且 ref 相同；重试不产生二次入账
5	存在负余额或欠费标记时，余额转回与注销均返回 409
6	工作区仍有余额时注销返回 409；清零后可注销，注销后成员关系全部解除、成员名下组织内密钥全部失效
7	个人工作区上调用改名 / 邀请 / 成员管理 / 转让 / 注销 / 余额转回 → 拒绝（非 5xx）
8	组数达上限再建组 → 400；组名重复 → 400；默认组不可停用、不可直接设置成员
9	组管理员无法授予或撤销组管理员角色
10	邀请过期后接受 → 明确失效语义；列表查询将过期待接受项就地标记为已过期
11	普通成员查询组列表，只能看到默认组与自身所在组
12	内部投影接口无内部令牌不可访问；响应中联系方式为脱敏值；关闭态工作区可被列表感知
13	请求携带已关闭工作区标识时返回自愈语义（请选择回退），而非角色不足语义
14	创建企业后，个人钱包余额不变（无隐式内部转账）

6.3 待后续设计细化的开放项

- 1. 运营面组织投影的增量同步机制（现为按页惰性拉取，全量拉取需评估上限与一致性口径）。
- 2. 组级限速与告警阈值的执行时机与执行方（本域只存配置，执行在计量侧）。
- 3. 企业实名等级 L1 / L2 的正式划分——待资金权限认证通道接入后按新证据重新划分。
- 4. 成员离开工作区后的资产与密钥交接流程：是否引入「密钥归属变更」路径，或统一按失效 + 重建处理。