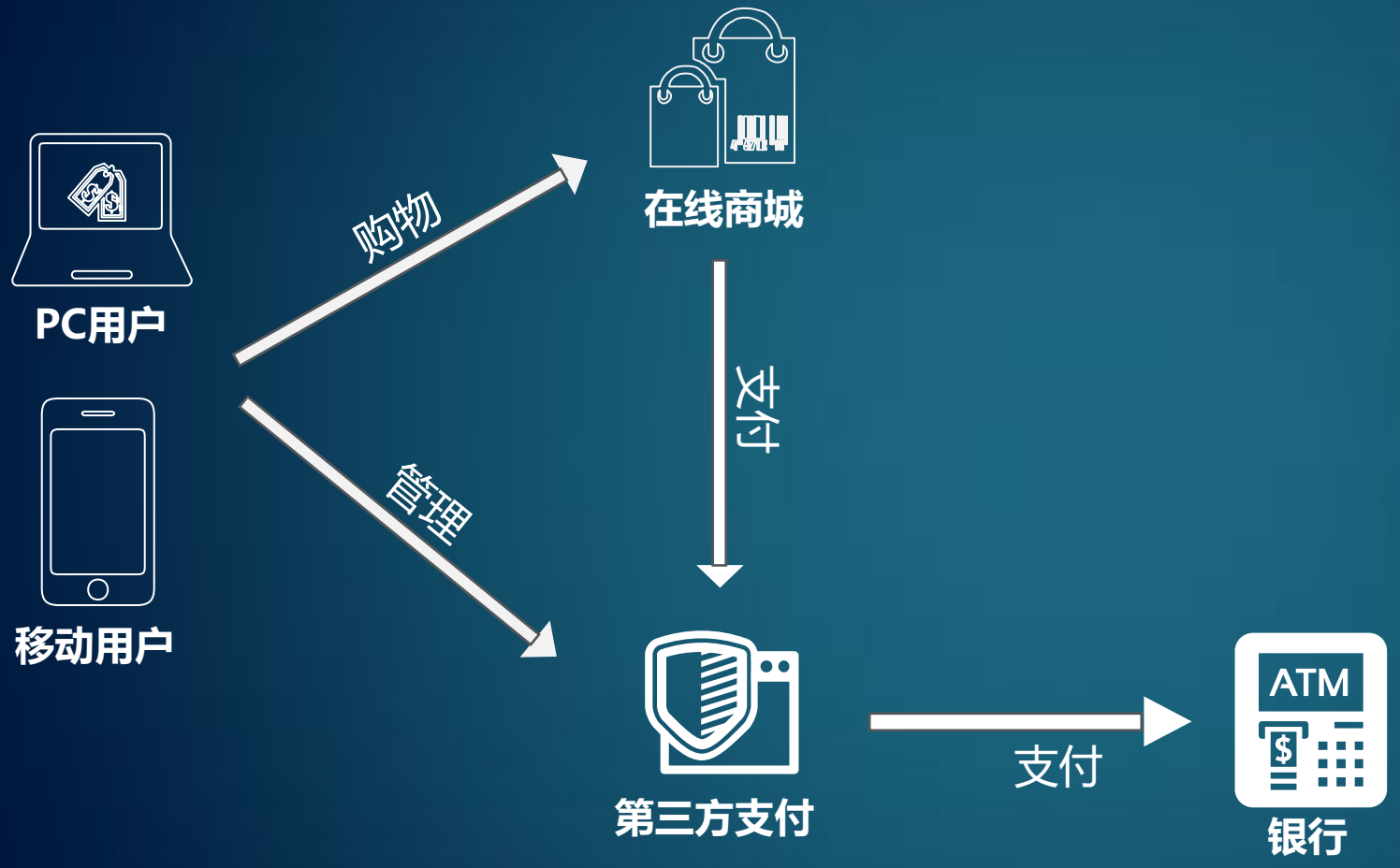
第三方支付系统设计与实践

唐贵斌

目录

CONTENTS

概述



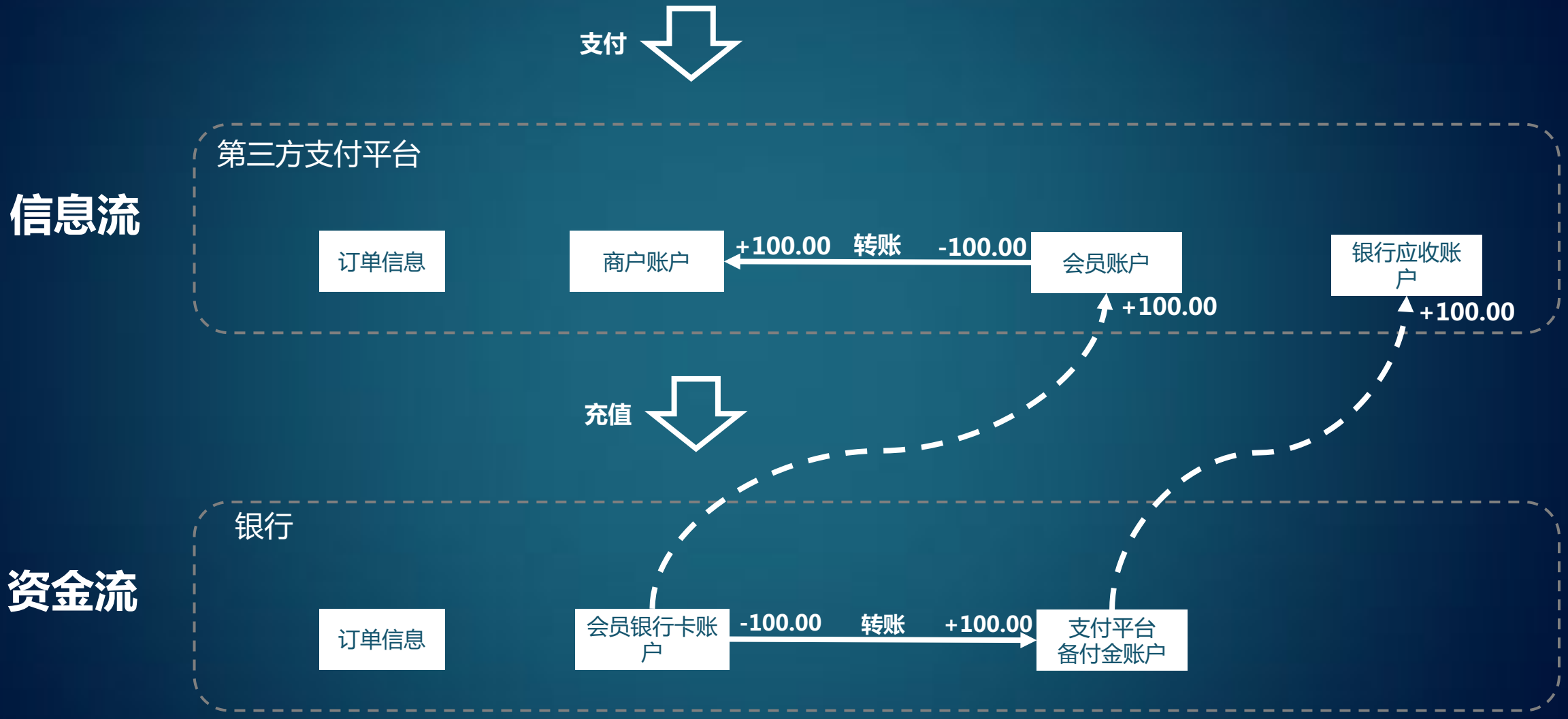
第三方支付平台

- **牌照**：中国人民银行核发的非金融机构从事支付业务的从业资格证书
- **第三方支付平台**：取得牌照的从事支付业务的非金融机构
- **非金融机构支付服务**：非金融机构在收付款人之间作为**中介机构**提供下列部分或全部货币资金转移服务：
  （一）网络支付；
  （二）预付卡的发行与受理；
  （三）银行卡收单；
  （四）中国人民银行确定的其他支付服务。

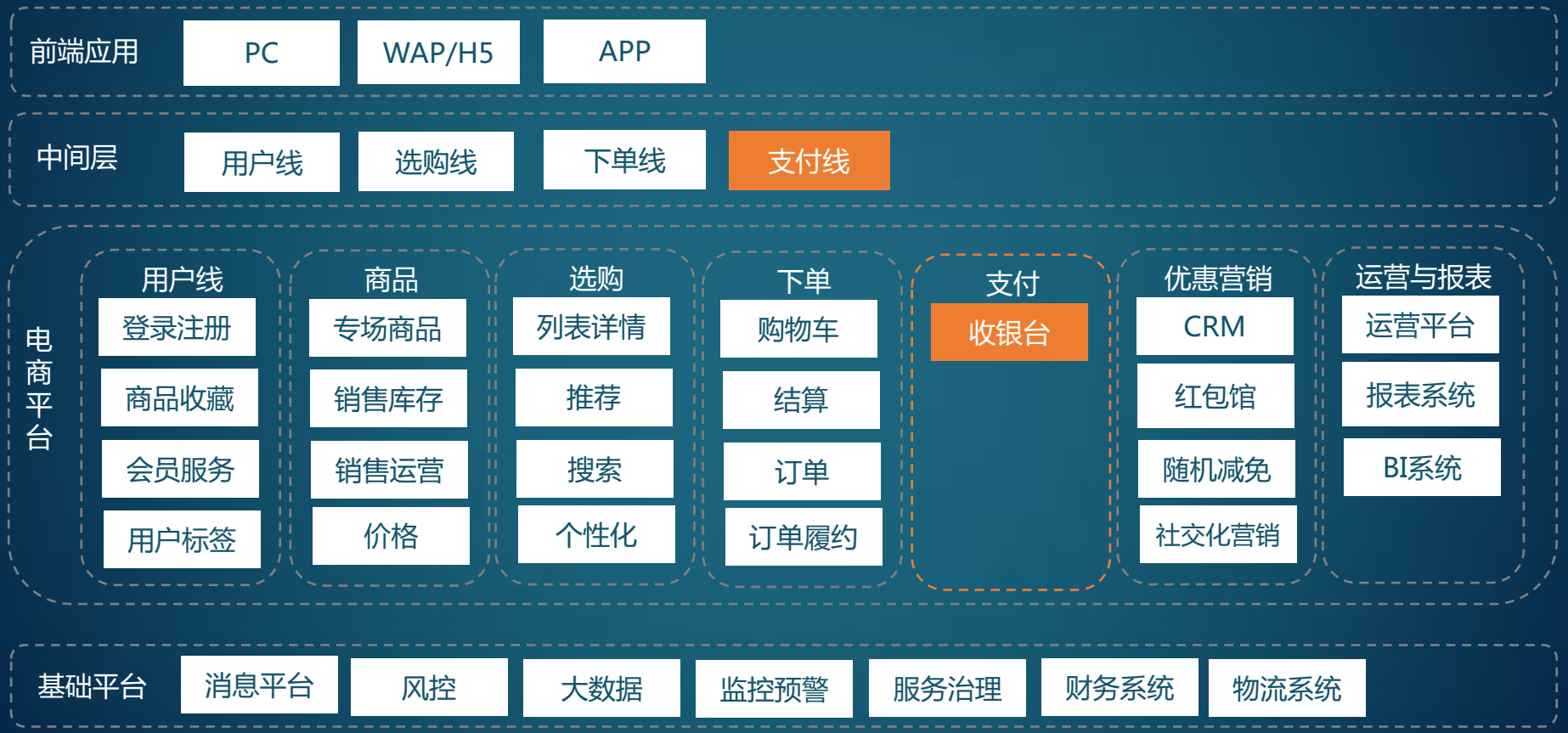
名词解析

信息流	资金信息在第三方支付发生的流转。举例：支付宝用户A的账户划转500元到用户B的账户。实际没有银行账户资金的转移。
资金流	资金在银行发生的实际流转。举例：从用户A的银行账户划转500元到企业B的银行账户。
发卡行	支付交易中，资金流出银行卡所属的银行。
收单行	支付交易中，资金流入的银行。一般也指商户的收款银行。
收单机构	在传统线下收单中，指部署/维护POS机的机构，如：拉卡拉。线上交易中，如支付宝、微信（财付通）等。
转接机构	建立公共平台，提供统一的清算和结算。如：银联，网联。
账户支付	在支付时，用户先登录第三方支付平台，然后才能做支付。可以使用余额支付，也可以选择银行卡支付。
网关支付	由商户直接把用户的银行卡信息提交到第三方支付平台，支付平台发给银行做扣款。也就是用户不需要登录第三方支付平台。
担保交易	买家先付款到第三方支付平台，卖家发货，买家收货后，再确认付款。支付宝最先引入。
备付金	也称支付准备金，商业银行或第三方支付平台为保护存款人利益，满足存款支付，确保资产流动性所做的资金准备。
支付牌照	中国人民银行核发的非金融机构从事支付业务的从业资格证书。
一清	执牌的第三方支付平台或银联把资金直接结算给商户。
二清	执牌的第三方支付平台或银联把资金结算给商户，商户再把资金结算给下一级商户。风险高，重点打击。

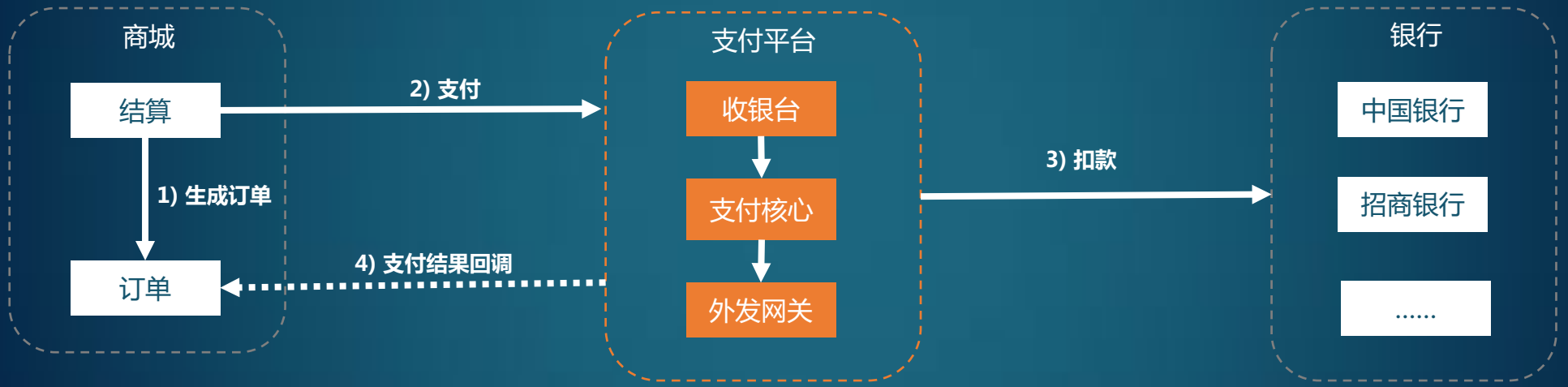
资金流与信息流


支付
信息流
第三方支付平台
订单信息
商户账户
+100.00
转账
-100.00
会员账户
银行应收账户
+100.00
+100.00
充值
资金流
银行
订单信息
会员银行卡账户
-100.00
转账
+100.00
支付平台备付金账户

与商城关系架构图


前端应用
PC
WAP/H5
APP
中间层
用户线
选购线
下单线
支付线
电商平台
用户线
登录注册
商品收藏
会员服务
用户标签
商品
专场商品
销售库存
销售运营
价格
选购
列表详情
推荐
搜索
个性化
下单
购物车
结算
订单
订单履约
支付
收银台
优惠营销
CRM
红包馆
随机减免
社交化营销
运营与报表
运营平台
报表系统
BI系统
基础平台
消息平台
风控
大数据
监控预警
服务治理
财务系统
物流系统

核心流程



目录

CONTENTS

原则

高内聚

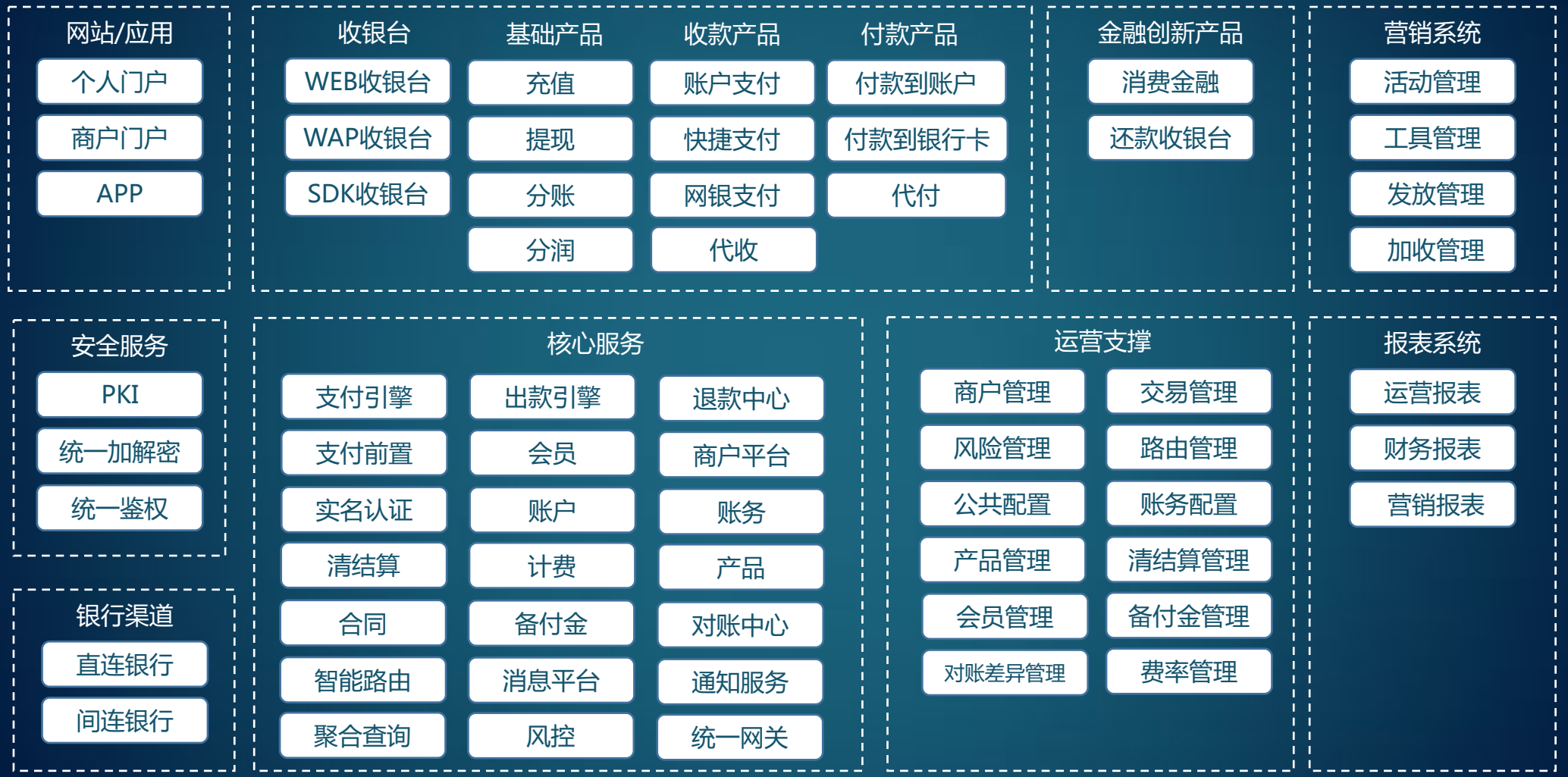
- 单一责任原则
- 一个模块或子服务只负责某特定的功能

低耦合

- 模块与模块之间，或子服务与子服务之间，尽可能独立
- 弱依赖

模块（单个大系统）=子服务（服务化）

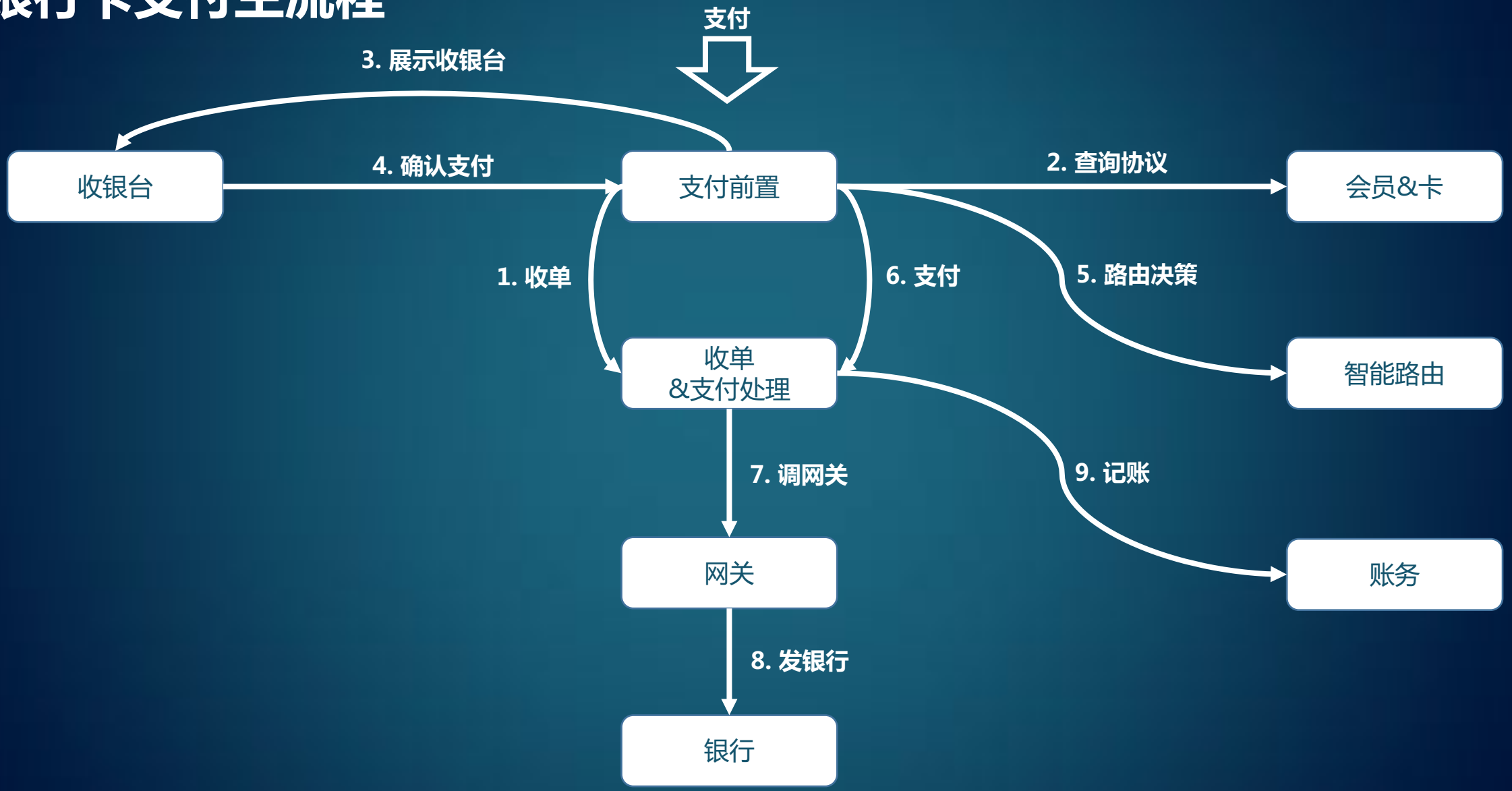
业务架构


网站/应用
个人门户
商户门户
APP
收银台
WEB收银台
WAP收银台
SDK收银台
基础产品
充值
提现
分账
分润
收款产品
账户支付
快捷支付
网银支付
代收
付款产品
付款到账户
付款到银行卡
代付
金融创新产品
消费金融
还款收银台
营销系统
活动管理
工具管理
发放管理
加收管理
安全服务
PKI
统一加解密
统一鉴权
银行渠道
直连银行
间连银行
核心服务
支付引擎
支付前置
实名认证
清结算
合同
智能路由
聚合查询
出款引擎
会员
账户
计费
备付金
消息平台
风控
退款中心
商户平台
账务
产品
对账中心
通知服务
统一网关
运营支撑
商户管理
风险管理
公共配置
产品管理
会员管理
对账差异管理
交易管理
路由管理
账务配置
清结算管理
备付金管理
费率管理
报表系统
运营报表
财务报表
营销报表

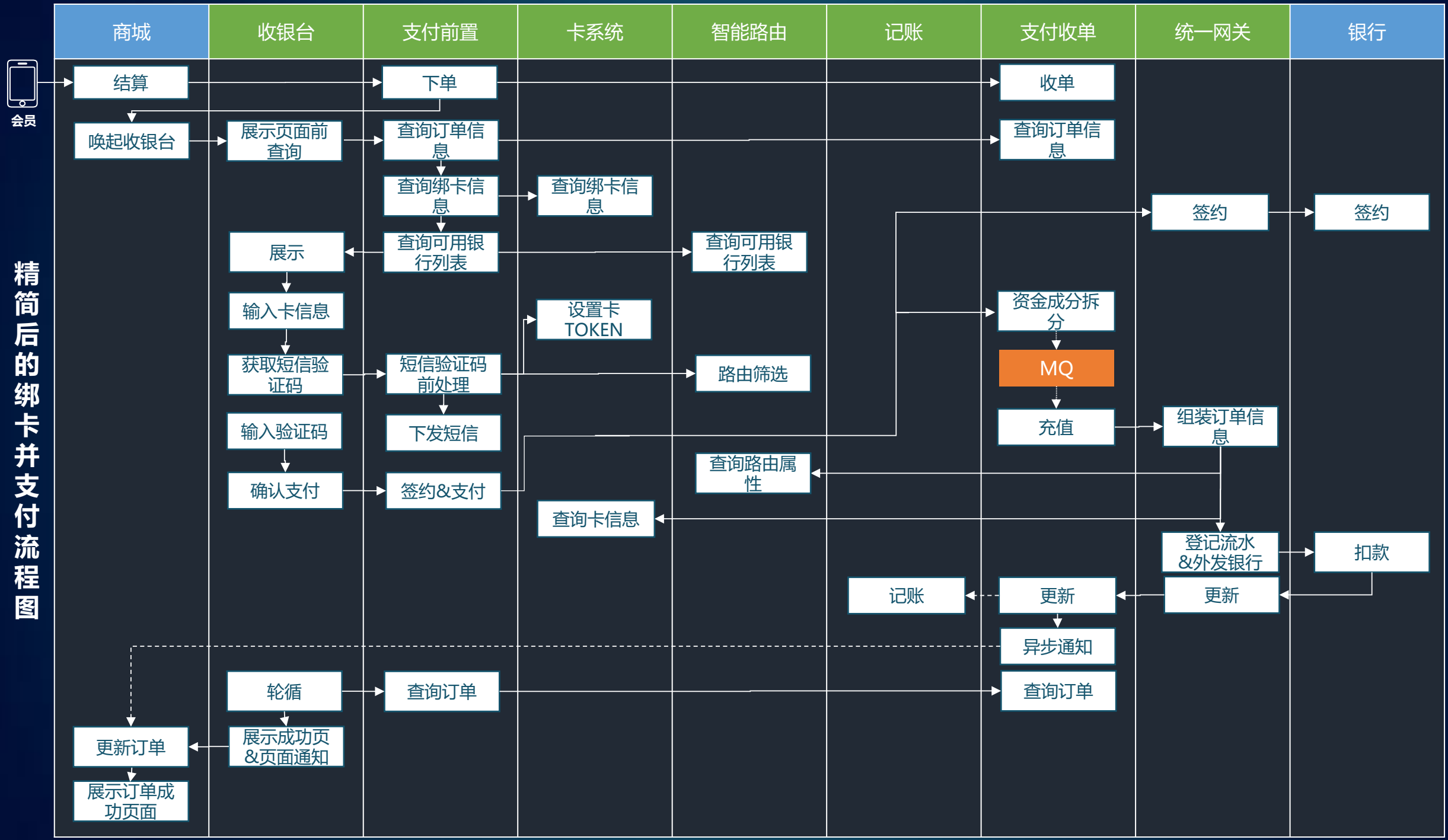
分层模型


前端应用
PC
WAP/H5
APP
商户
商城应用
代收代付
网关层
收银台
个人门户
商户门户
代收代付
实名认证
应用层
会员服务
商户服务
充转提
收单服务
收银台服务
城市服务
核心引擎
支付引擎
出款引擎
运营支撑
管理平台
报表系统
基础服务
会员
卡系统
智能路由
风控
会计
计费
产品中心
渠道网关
备付金
商户
合同
对账
基础设施
统一安全
统一加解密
PKI
消息平台
商户通知
监控系统
第三方服务
银行渠道
实名认证渠道

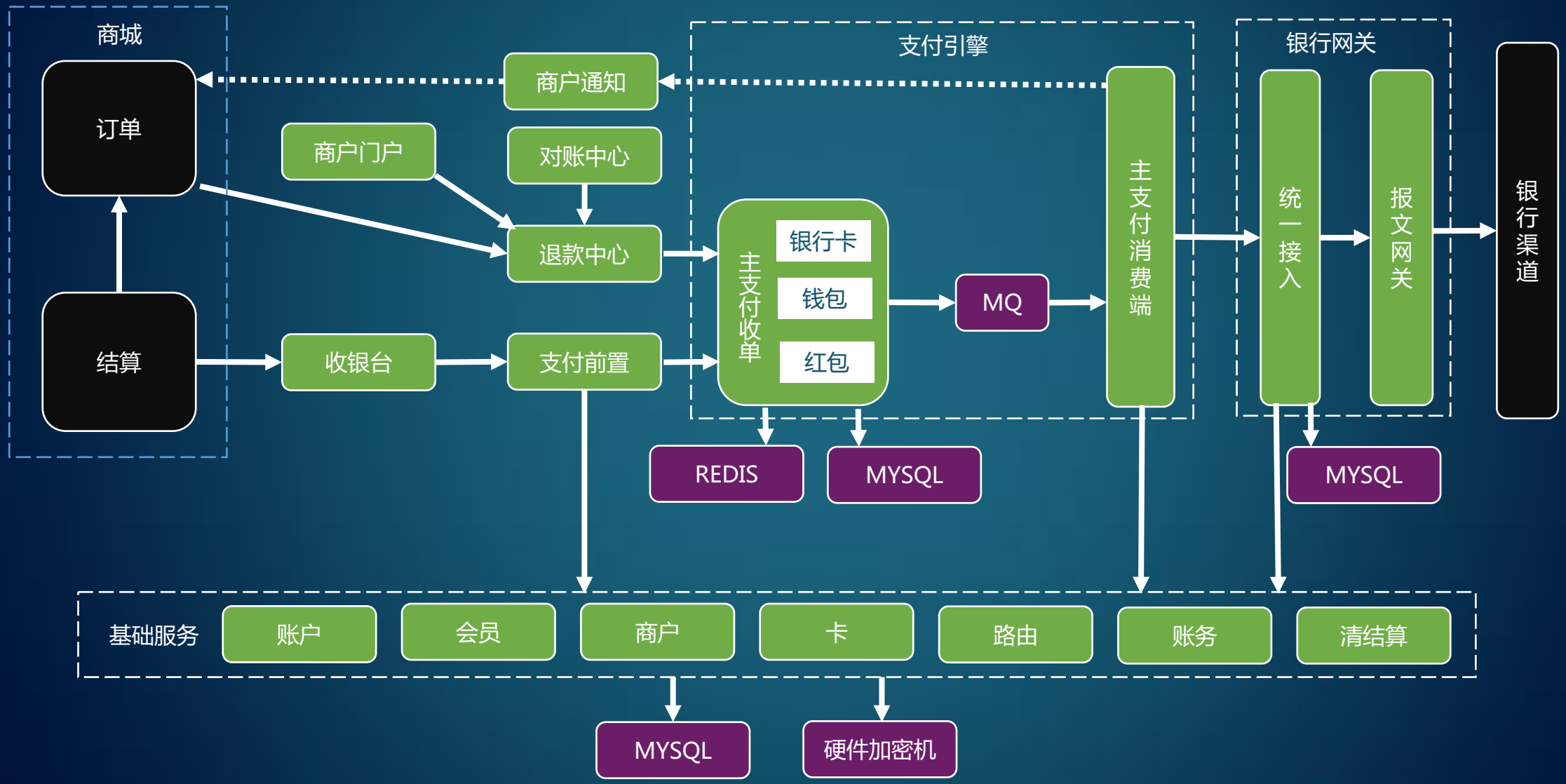
银行卡支付主流程


支付
3. 展示收银台
收银台
4. 确认支付
支付前置
2. 查询协议
会员&卡
1. 收单
6. 支付
5. 路由决策
收单
&支付处理
智能路由
7. 调网关
9. 记账
网关
账务
8. 发银行
银行

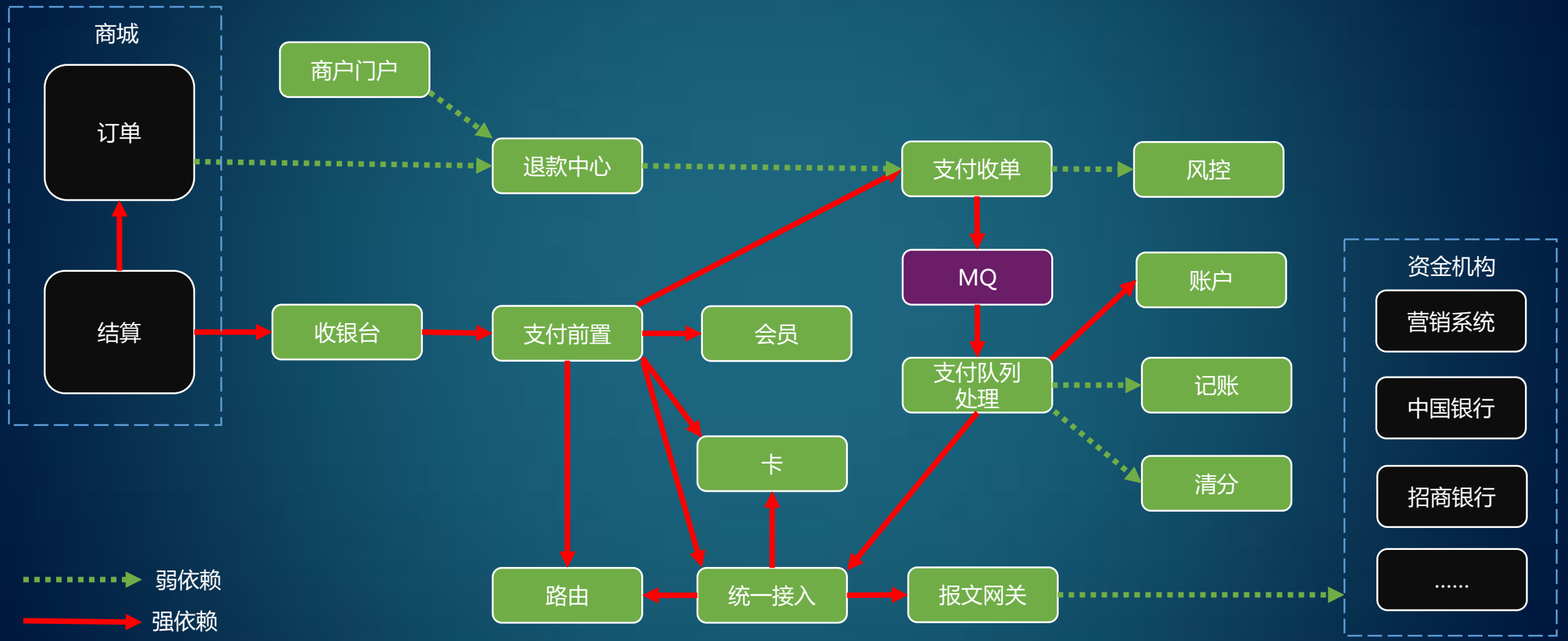
精简后的绑卡并支付流程图



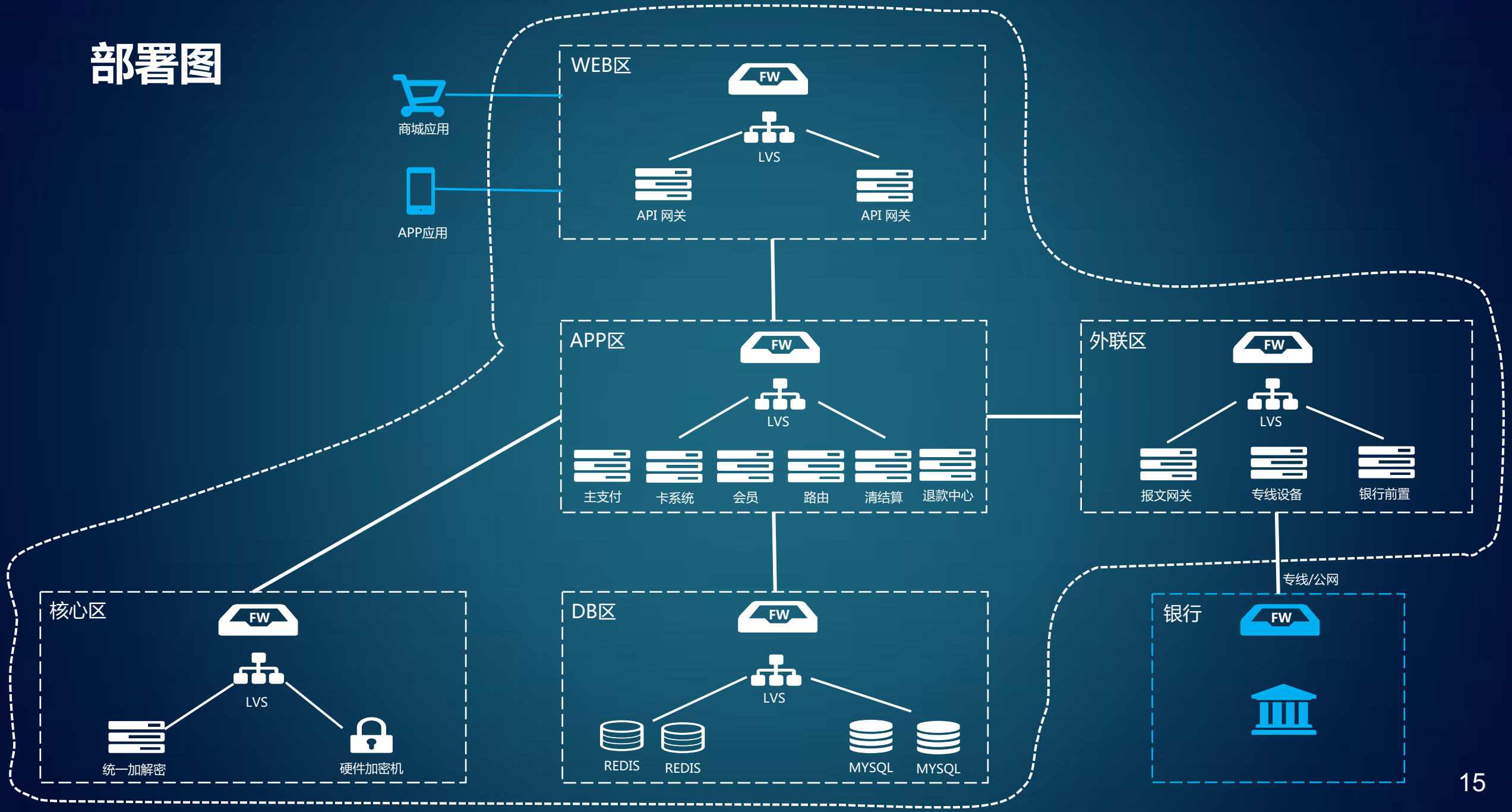
核心模块图


商城
订单
结算
商户门户
对账中心
退款中心
收银台
支付前置
商户通知
支付引擎
主支付收单
银行卡
钱包
红包
MQ
主支付消费端
银行网关
统一接入
报文网关
银行渠道
REDIS
MYSQL
MYSQL
基础服务
账户
会员
商户
卡
路由
账务
清结算
MYSQL
硬件加密机

核心模块依赖图


商城
订单
结算
商户门户
退款中心
收银台
支付前置
会员
卡
路由
统一接入
报文网关
支付收单
MQ
支付队列
处理
风控
账户
记账
清分
资金机构
营销系统
中国银行
招商银行
.....
弱依赖
强依赖

部署图


商城应用
APP应用
WEB区
FW
LVS
API 网关
API 网关
APP区
FW
LVS
主支付
卡系统
会员
路由
清结算
退款中心
外联区
FW
LVS
报文网关
专线设备
银行前置
核心区
FW
LVS
统一加解密
硬件加密机
DB区
FW
LVS
REDIS
REDIS
MYSQL
MYSQL
专线/公网
银行
FW

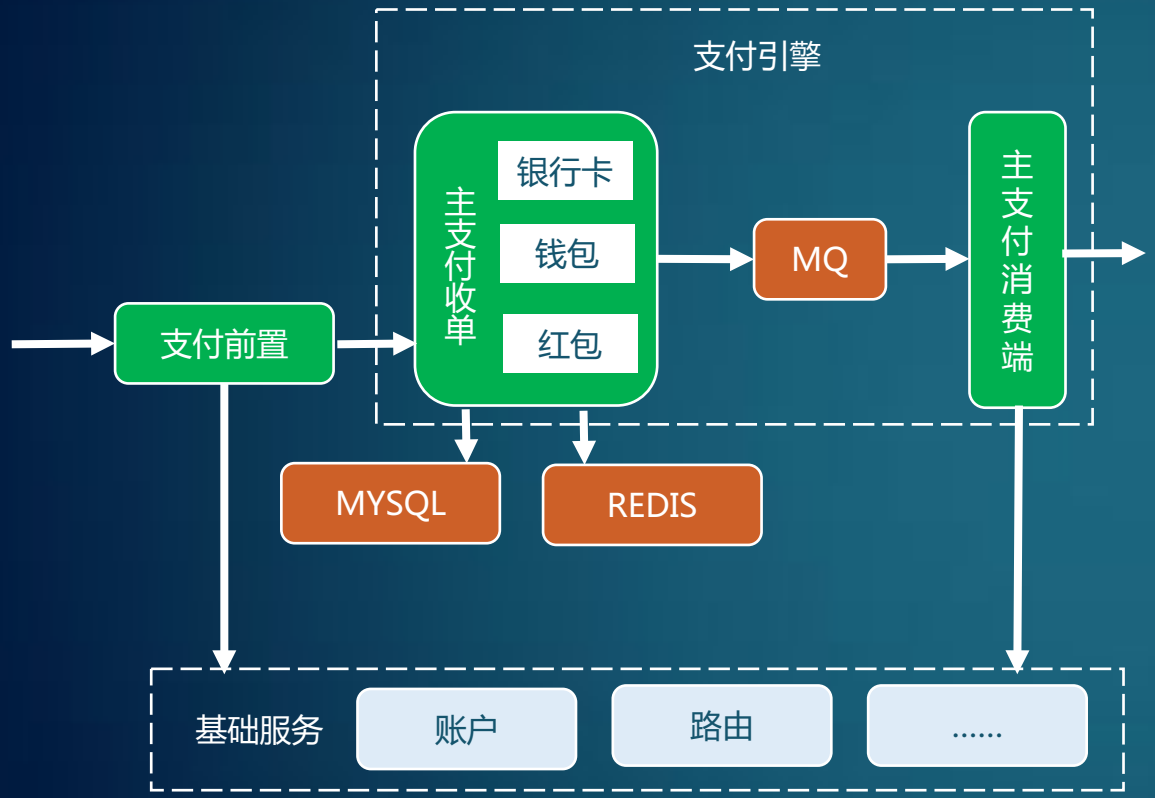
目录

CONTENTS

订单表模型

- **商户订单表**：保存商户订单信息
- **支付订单表**：保存支付内部生成的订单信息，代表一次支付行为
- **充值订单表**：保存单个资金成分支付的订单信息
- **银行流水表**：保存银行流水信息

支付核心



使用MQ实现异步化

- **支付前置**：负责串所有的流程，包括查询银行列表，校验方式等；
- **主支付收单**：落商户请求单，生成消费订单，生成充值订单，并把支付请求发到消息队列；
- **主支付消费端**：从MQ获取支付信息，发给渠道网关进行充值服务

智能路由

业务规则

根据运营策略，控制不同渠道的分流比例（部分渠道有全年累计交易额指标）

分流比例

区分新签约用户、已签约用户，根据渠道验证信息强度，提供用户最优的渠道

用户标签

不同支付金额分流到不同的渠道，以降低成本

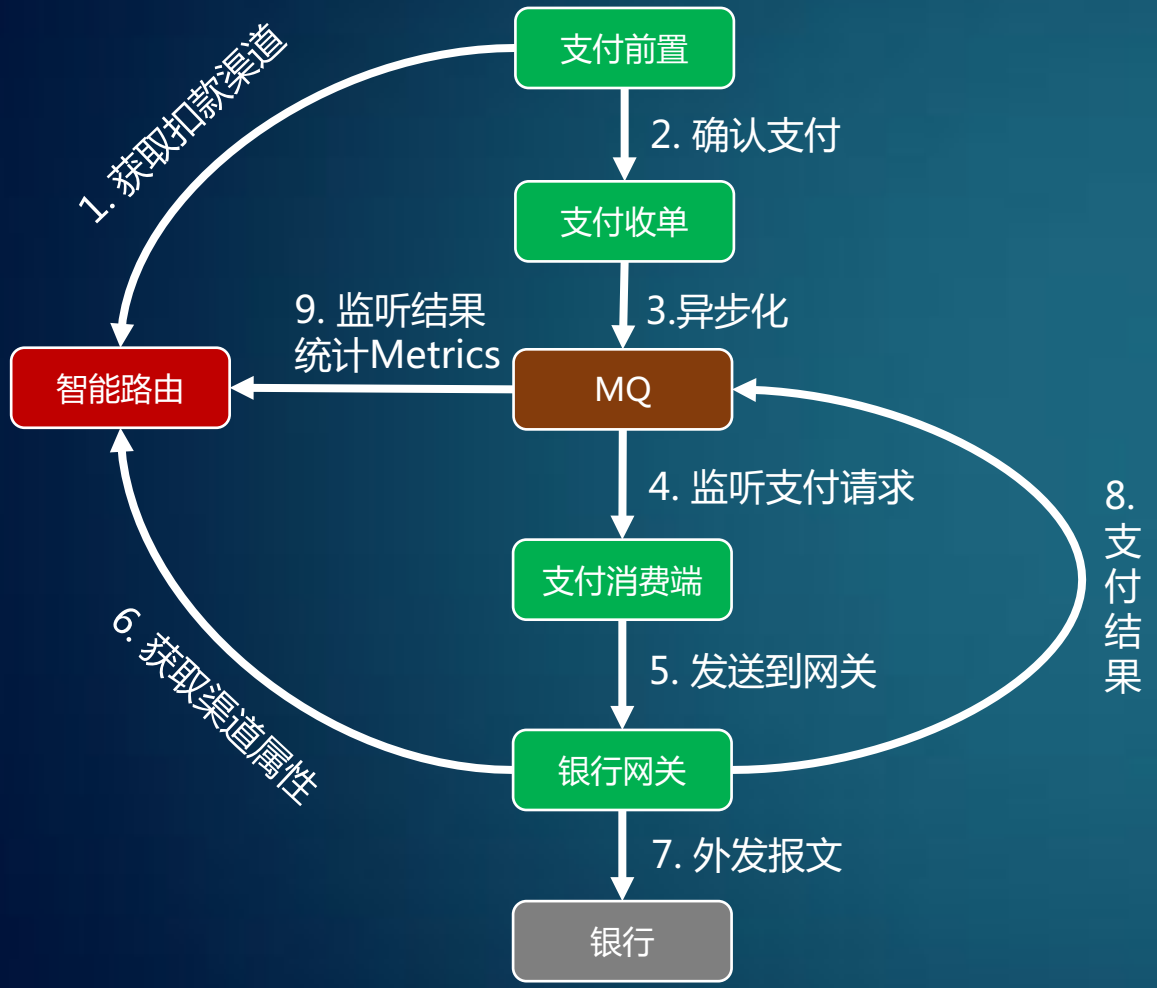
额度范围

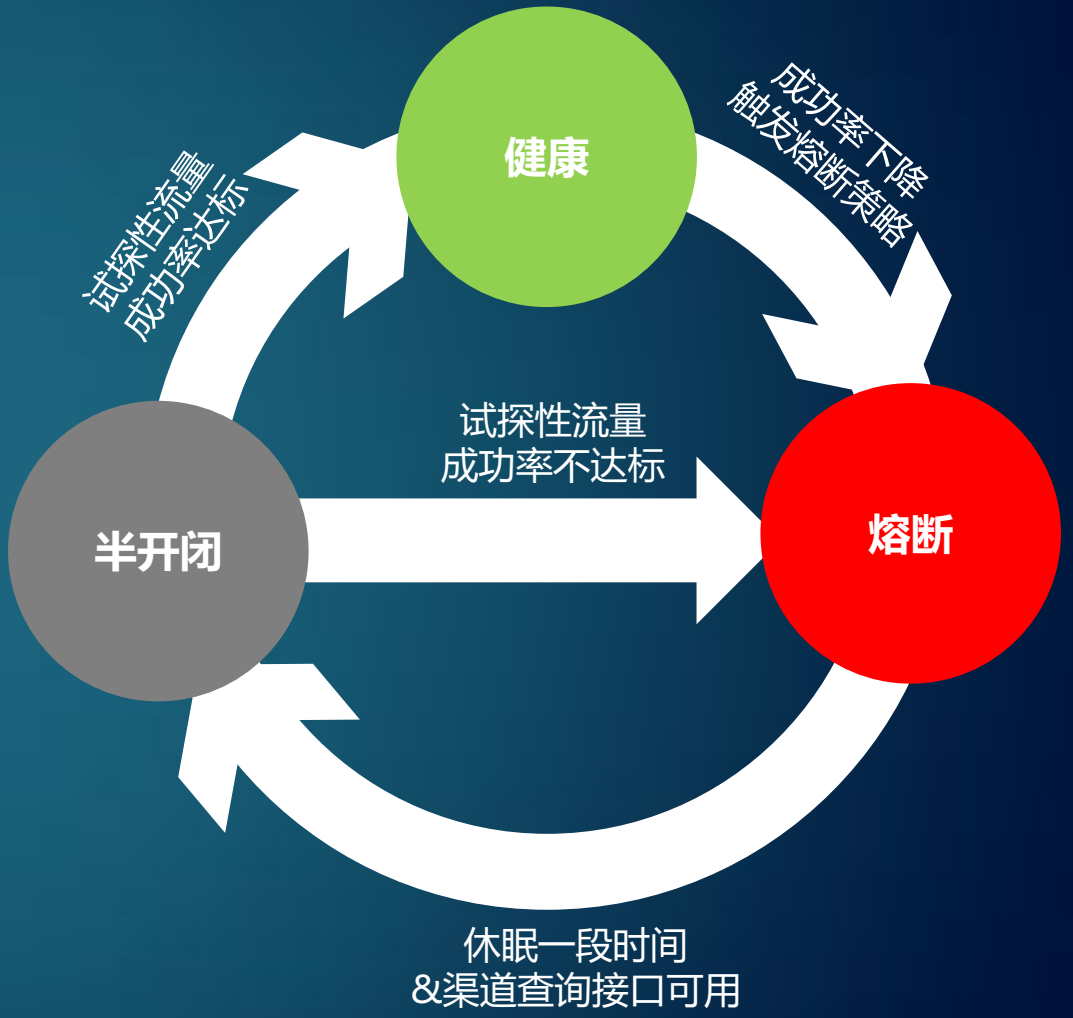
可用性规则

自动过滤渠道状态为不可用的渠道

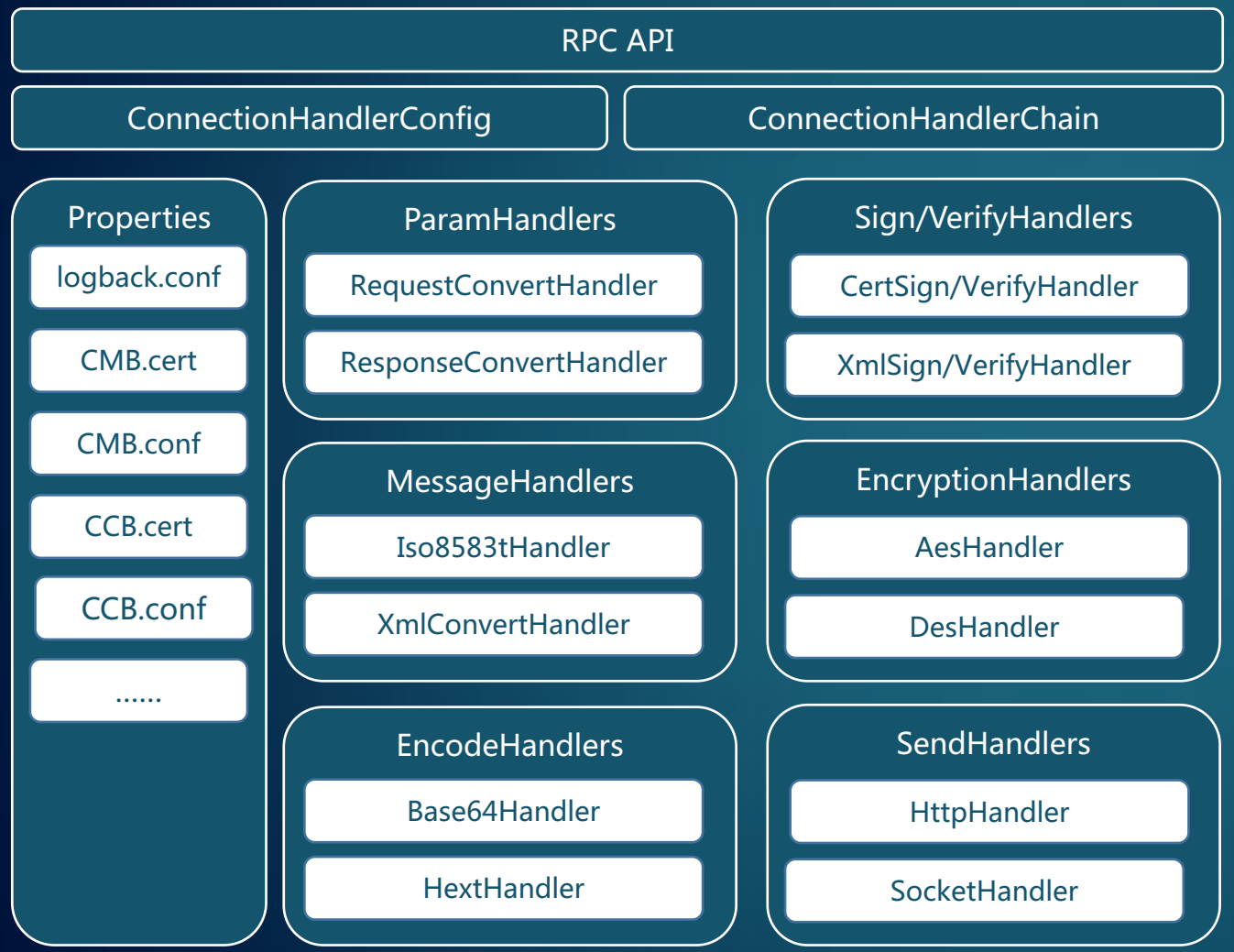
渠道状态

智能路由


支付前置
2. 确认支付
支付收单
3.异步化
9. 监听结果
统计Metrics
智能路由
MQ
4. 监听支付请求
支付消费端
5. 发送到网关
银行网关
7. 外发报文
银行
1. 获取扣款渠道
6. 获取渠道属性
8. 支付结果


健康
成功率下降
触发熔断策略
试探性流量
成功率达标
试探性流量
成功率不达标
半开闭
熔断
休眠一段时间
&渠道查询接口可用

统一网关



1. **责任链设计模式**
   组合各种不同的HANDLE来处理复杂多变的银行接入流程
2. **使用配置文件方式开发**
   屏蔽开发人员技术能力的差异，减少绝大部分的重复工作和出错可能
3. **提高效率**
   渠道接入开发工作量平均耗时由一个月缩短到两周
4. **快速修复**
   下发配置文件立即修复线上BUG

记账

复式记账法	对每项经济业务按相等的金额在两个或两个以上有关账户中同时进行登记的方法。
记账方法	**借贷记账法**、收付记账法和增减记账法。
记账原则	有借必有贷，借贷必相等。
记账依据	会计恒等式：1. 资产 = 负债 + 所有者权益；2. 利润 = 收入 - 费用。
账户	具有一定的格式和结构，能够用来连续、系统、全面的记录反映某种经济业务的增减变化及其结果。
科目	账户变化的会计要素分类，是账户的名称，也是设置账户的依据。
账户和科目区别	科目只有名字，账户包括结构与格式，通常情况不进行区分。
复式记账必要性	账务数据与业务数据一致；异常数据定位；

借贷简要公式

【借记类】账户（如资产，应收款），【增加】为【借】，【减少】为【贷】；
【贷记类】账户（如负债和所有者权益，应付款），【增加】为贷，【减少】为【借】；

记账实例

支付平台记账

充值账

借：应收-平台托管-银行渠道-银行B	500
贷：应付-平台托管-网关账户	500

消费账（实时）

借：应付-平台托管-网关账户	500
贷：应付-平台托管-商户账户	500

消费账（批量）

借：应付-平台托管-网关账户	500
贷：应收-平台托管-商户账户-暂结算款	500

日终清分

借：应收-平台托管-商户账户-暂结算款	500
贷：应付-平台托管-商户账户	500

其它

支付平台流水

消费订单表	1笔
充值订单表	1笔或多笔
银行流水	1笔或多笔

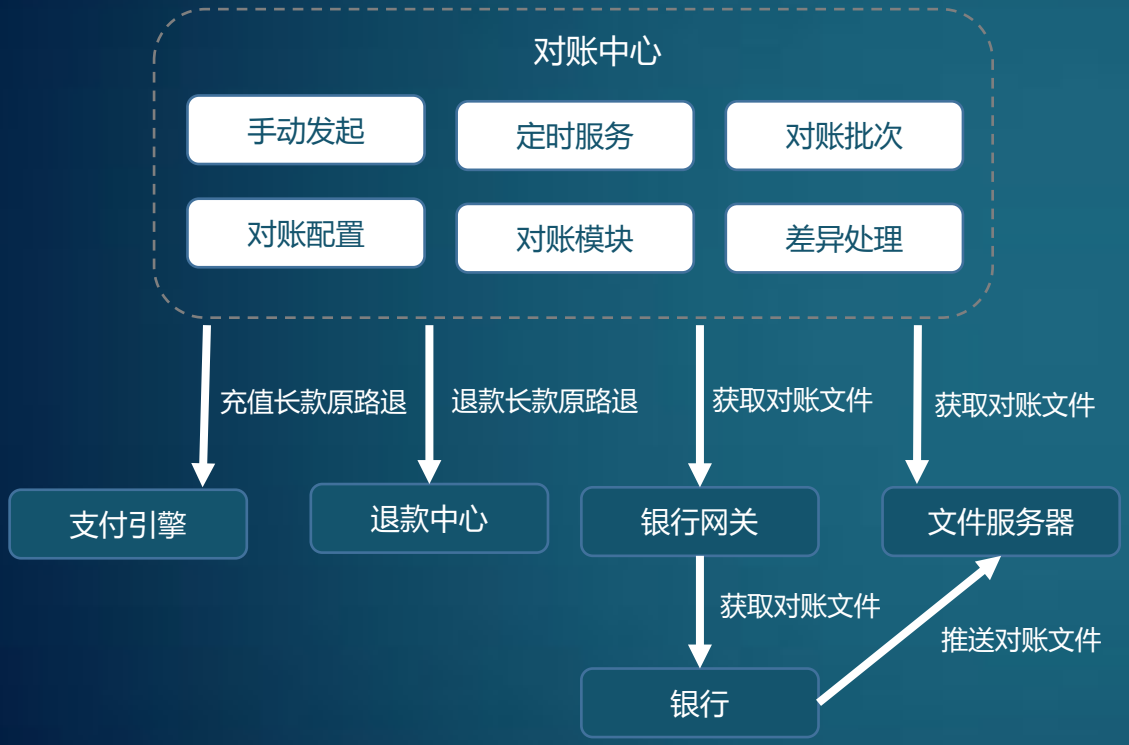
银行资金流转-同行

银行A-用户账户	减少 500
银行A-支付平台账户	增加 500

银行资金流转-跨行

银行A-用户账户	减少 500
银行B-支付平台账户	增加 500

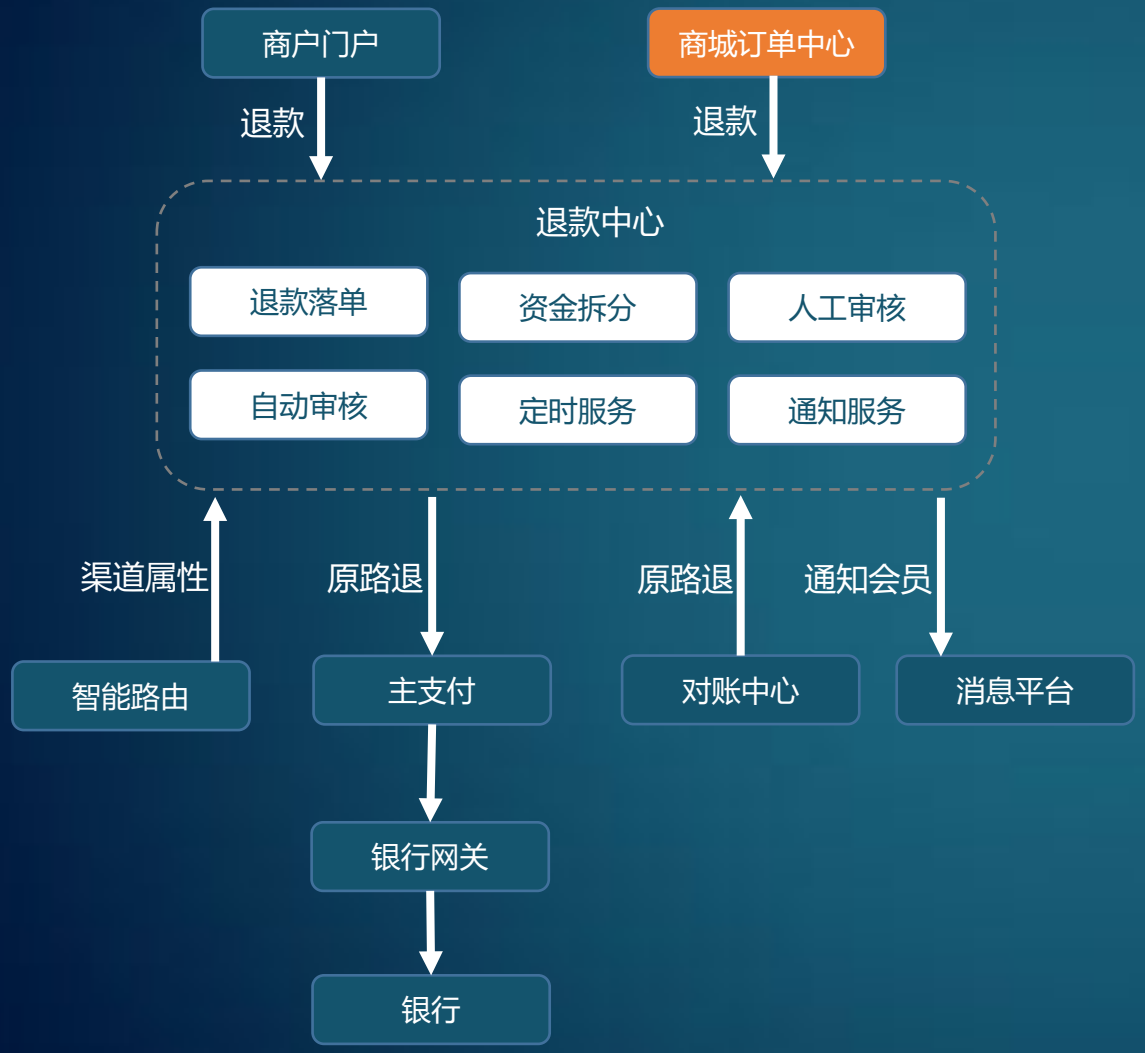
对账



概念

- **支付长款**：我方无/失败 银行有/成功；需退回；
  支付短款：我方有/成功 银行无/失败；需追回，否则资损；
- **退款长款**：我方有/成功 银行无/失败；需再次退回；
  退款短款：我方无/失败 银行有/成功；我方置为成功，取消差异；
- **存疑**：我方和银行之间的会计日期不准，在跨天时有可能计算为不同的会计日导致对不上，需要隔天再对；
- **对账以出对账文件方为准**：第三方支付平台一般以银行为准，商户一般以第三方支付平台为准；

退款中心



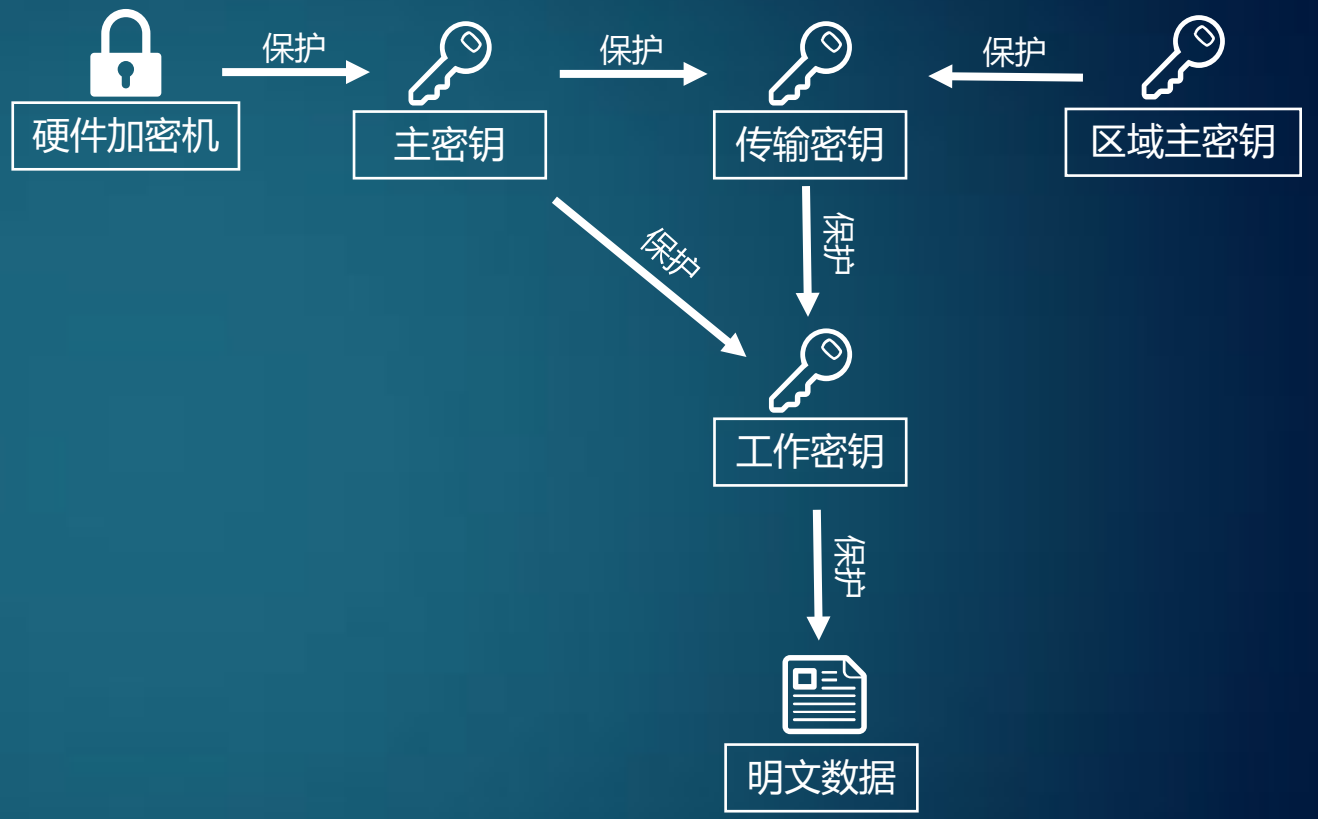
概念

- **正交易退**：当天支付总金额大于退款总金额；
- **隔日退**：当天的交易需要第二天才能退；
- **指定时间段退**：每天有个时间段银行可能在跑批，无法受理退款；
- **串行退**：银行不支持并发退款，比如1S只接收1笔退款，超过的就退款失败；
- **余额退**： 从结算账户的余额做退款；

统一加解密

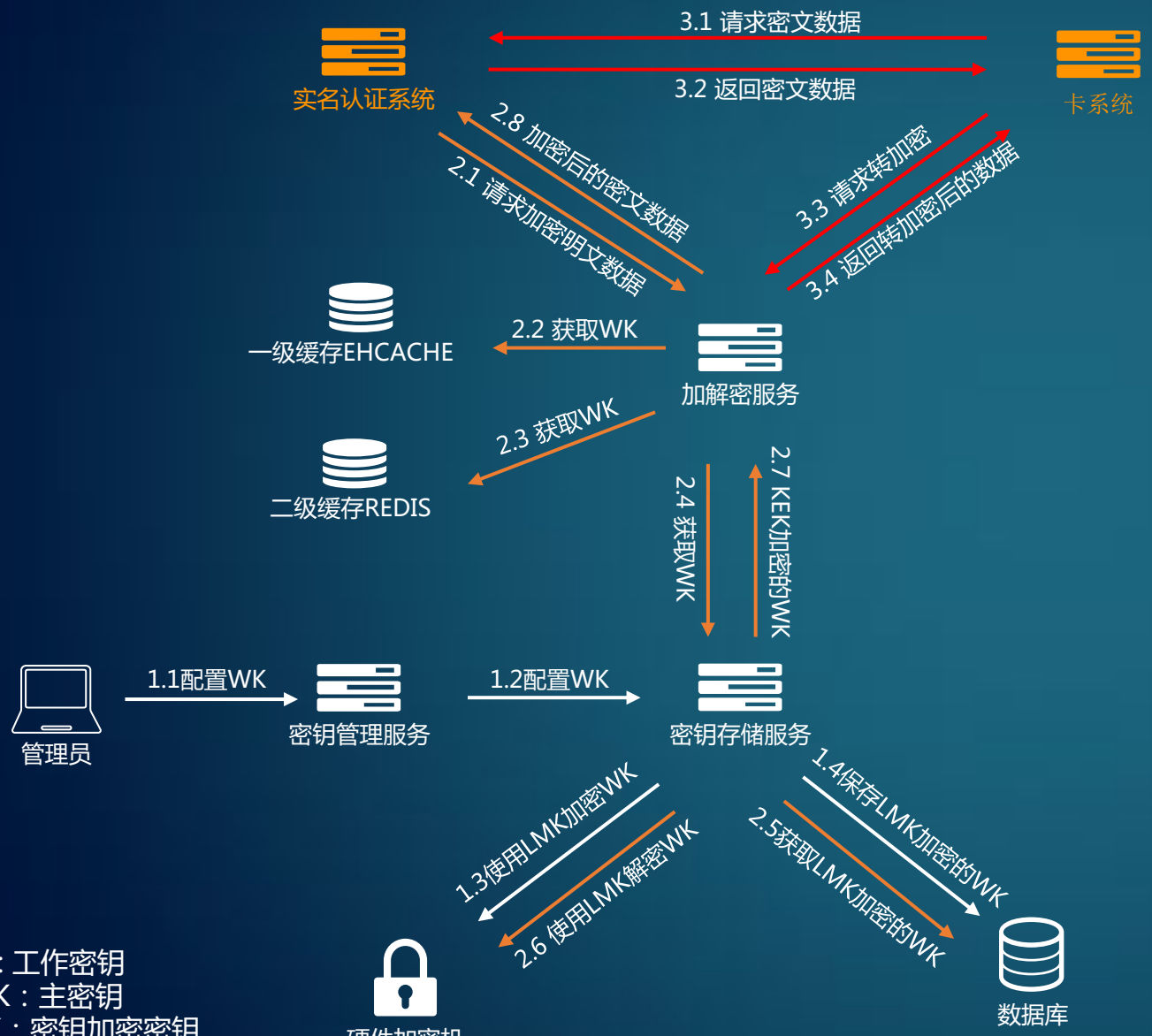
密钥的价值 = 数据的价值

数据值100W = 密钥就值100W



密钥逐级保护体系

统一加解密

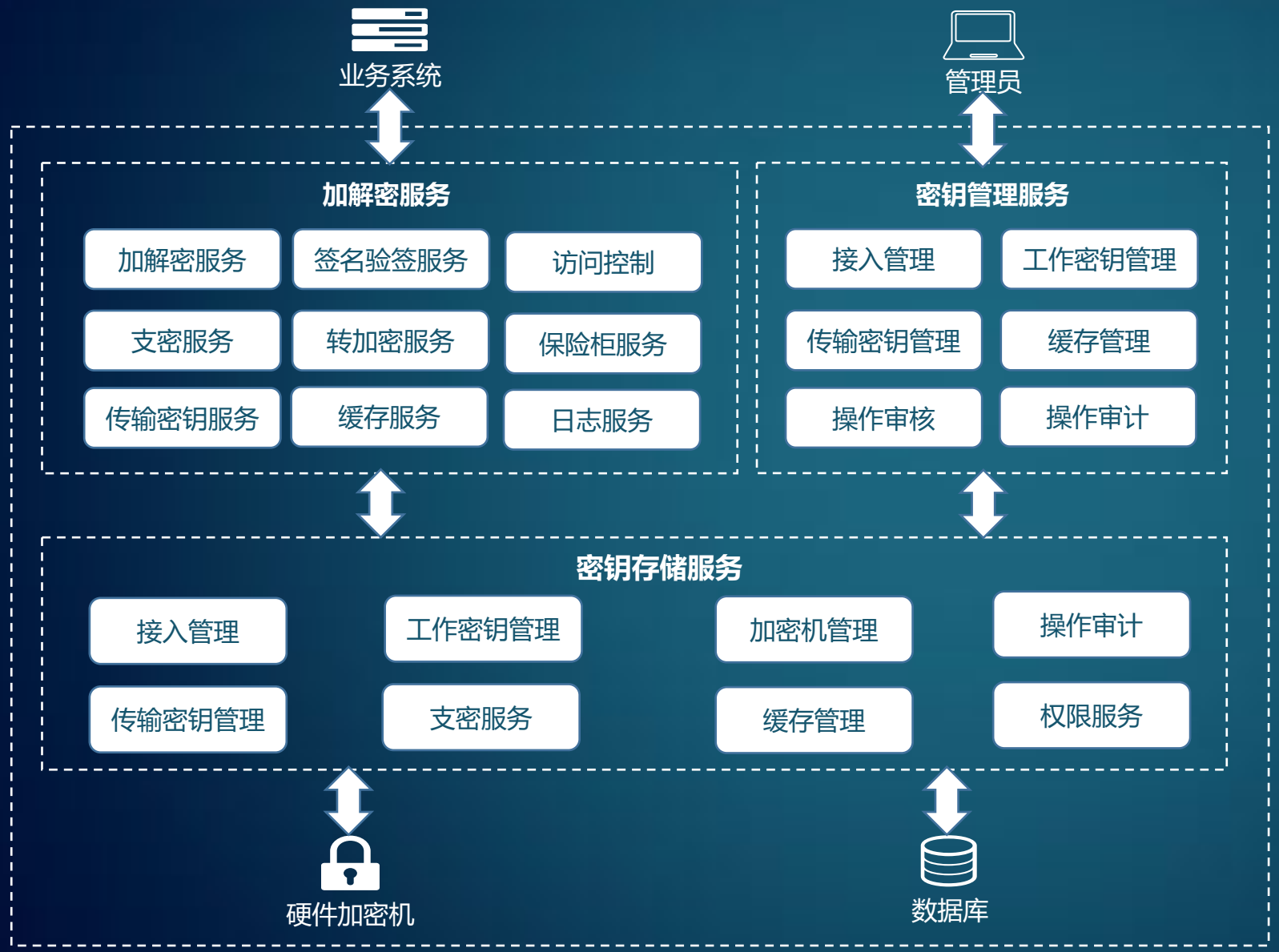


WK: 工作密钥
LMK：主密钥
KEK：密钥加密密钥

核心功能

- **密钥统一存储**：避免密钥存储在配置文件、DB、环境变量；开发、测试、运维都无法接触生产密钥
- **金融级安全**：工作密钥使用硬件加密机加密后存储，最供金融级安全防护
- **统一加解密及验名验签**：业务系统无需写重复代码
- **统一管理密钥版本**：业务系统无需实现复杂的密钥版本管理
- **本地缓存服务**：加解密服务达到异地多活和水平扩展

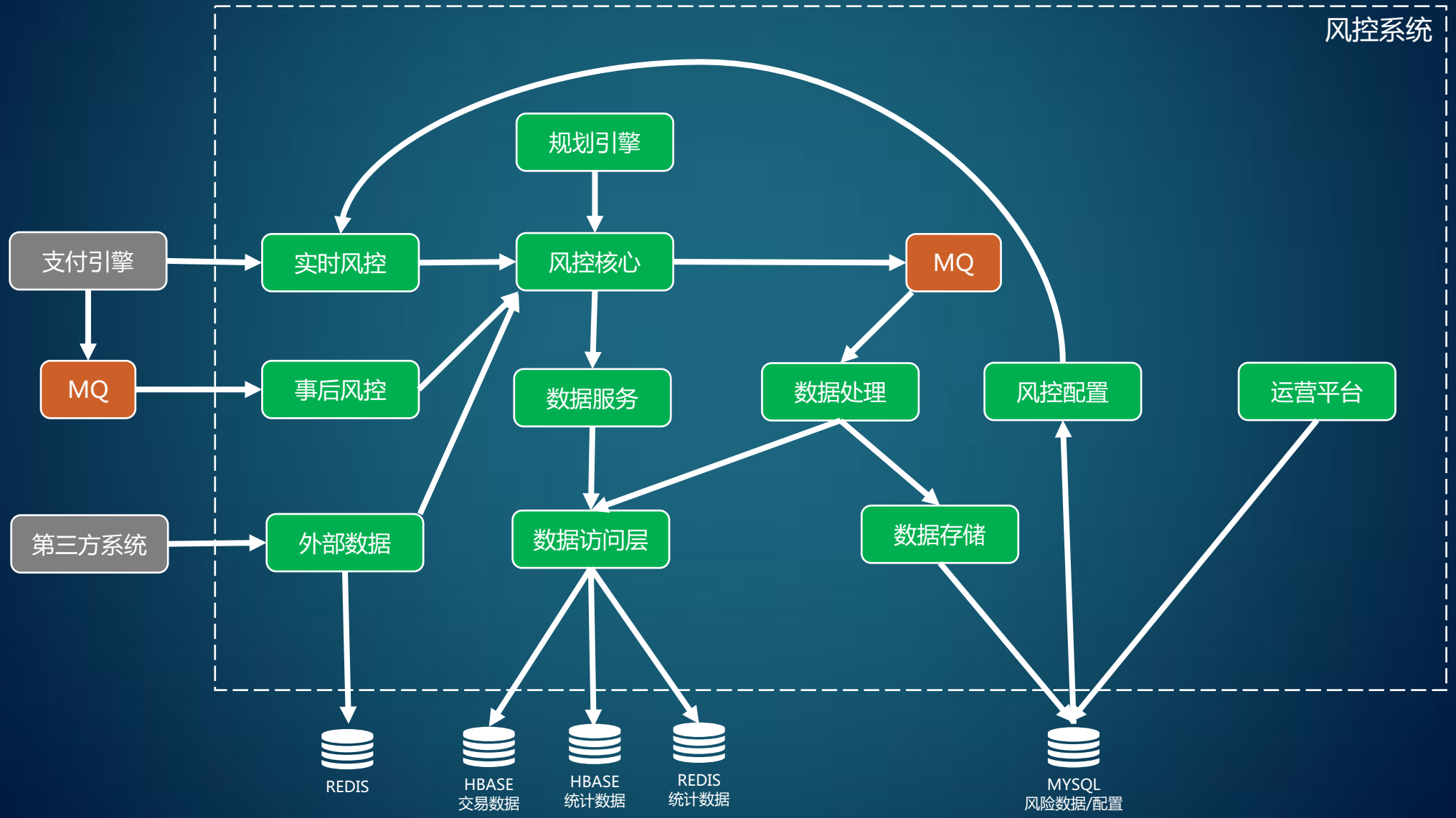
统一加解密



职责说明

- **加解密服务**：对外提供加解密、签名验签等服务
- **密钥管理服务**：管理接入方、工作密钥等
- **密钥存储服务**：负责存储工作密钥、接入方信息等
- **硬件加密机**：保存主密钥，对工作密钥进行加密
- **数据库**：保存接入方，使用主密钥加密后的工作密钥密文等

风控


风控系统
规划引擎
支付引擎
实时风控
风控核心
MQ
MQ
事后风控
数据服务
数据处理
风控配置
运营平台
第三方系统
外部数据
数据访问层
数据存储
REDIS
HBASE
交易数据
HBASE
统计数据
REDIS
统计数据
MYSQL
风险数据/配置

目录

CONTENTS

预防雪崩/过载保护

慢响应比想象中可怕

只处理自己能力范围内的请求

- **入口限流**：只处理系统负载内能处理的请求。使用排队机制或直接拒绝。
- **快速失败**：各子服务的调用需要设置合理的超时时间，并且确保是生效状态，避免过多的慢调用导致线程耗尽。
- **熔断与资源隔离**：可参考Hystrix实现。
- **合理超时设置**：上层服务的超时时间理论上要小于下层的服务超时时间。

资源隔离

保证核心业务的高可用

- **线程池**：进程级隔离，不同请求不同业务类型，使用不同线程池处理
- **系统拆解**：使用微服务化隔离不同的业务系统
- **服务分组**：不同等级的服务分发到不同的集群
- **DB读写分离**：主从模式
- **静态资源**：保存到CDN
- **热点**：热点读使用缓存
- **环境**：预发布、测试、生产
- **资源**：大数据集群和应用集群隔离（带宽使用不一样）

强弱依赖

前提：**A服务依赖B服务**

强依赖：B服务宕机后，A服务无法提供正常的服务；
弱依赖：B服务宕机后，A服务能提供完整或部分有损服务；

例：

1. 当使用REDIS做缓存时，如果没有使用try&catch，读取REDIS失败，直接抛出异常，导致主流程中断，就属于强依赖。需要修改为弱依赖。

2. 在支付过程中，调用实时风控服务，如果超时，就拒绝支付，就属于强依赖；如果超时后仍能正常支付，就属于弱依赖；

垂直拆分和水平扩展

垂直拆分：把一个大系统的模块拆分成子服务；例：把会员模块从支付核心中拆出去。

水平扩展：会员服务开始只有2台服务器，扩容到10台服务器；

注：
1、垂直拆分需要充分考虑【高内聚、低耦合】的原则；

2、水平扩展需要考虑数据库最大连接数的问题。比如有台mysql最大只支持1500个连接，如果有50应用，那么每台应用的最大连接数应该不超过30；

异步化

最常用方法：使用消息中间件做异步化。

优点：提高并发性能；削峰填谷；

缺点：
1、增加系统复杂性；

2、需要使用额外的机制确保数据的最终一致性；

流量均衡

流量不均衡的后果：高负载下的应用处理变慢，容易形成雪崩。

可能存在流量不均的情况：
1、F5开启长连接，且使用了session保持；解决：关闭session保持，开启按请求包分发。如果需要使用session，就引入redis做分布式session存储。

分库分表

算法1：根据ID取模，优点：算法简单；缺点：扩容需要停机，数据需要重新分布。

算法2：使用映射表，优点：不停机扩容；缺点：映射表是热点数据。

监控和降级

新业务上线基本要求：
1、要有监控方案，及时发现线上问题；
2、要有降级方案，减少线上BUG导致的损失；
3、要有回滚方案，线上验收不通过时做回滚；

重构项目上线基本要求：
1、要有监控方案，及时发现线上问题；
2、要有灰度方案，逐步扩大灰度比例；
3、要有回滚方案，线上验收不通过时做回滚；

过度设计

反例：
1、未来2年内单表数据不越过3000W，却使用了分库分表。
2、并发最高只有50个，同步能满足需求，又没有特殊要求，却设计成异步化。
3、并发最高只有50个，使用微服务架构。

大促准备

1、**确定流量模型**：根据历史数据，推算入口数据，再根据流量模型推算各系统的流量。
2、**线下压测**：确定单机性能，推算集群性能。
3、**线上单机压测**：通过调权重确定线上单机性能，推算集群性能。
4、**线上复制流量压测**：复制真实流量到测试集群，需要解决安全问题。
5、**线上流量回放压测**：把历史真实流程回放到生产集群，需要解决数据染色和隔离。
6、**扩容**。
7、**健壮性梳理**：强弱依赖梳理。把可以修改为弱依赖的强依赖优化为弱依赖。
8、**大促演练**。

目录

CONTENTS

互联网金融

消费金融

现金贷 - 乱象环生 通过奇高利息弥补风控缺失 严监管 17年底开始走下坡路

消费贷 - 依托消费场景，只能用于消费，风险较低，收益也低

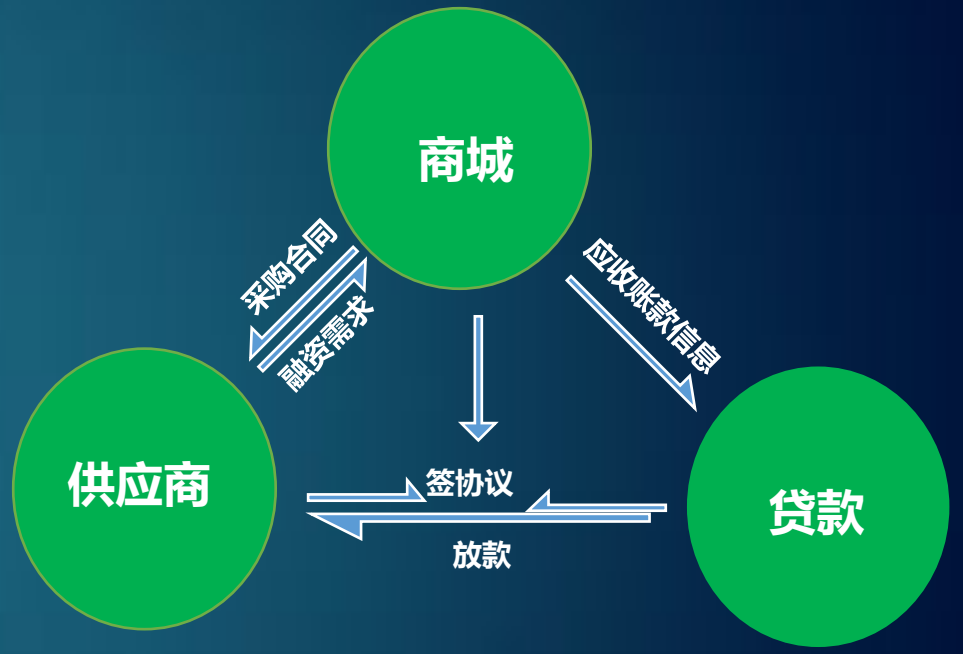
两者最大区别：
现金贷是资金直接支付给实际借款人，借款人拿到资金后具体用途并不限定。
消费贷所承担的资金基本上支付给店铺或者其他消费场所，直接用于支付消费者在消费商品或服务过程中所需费用。

供应链金融

供应链金融是基于对供应链上下游的数据分析，为系统内的企业成员提供融资解决方案。

供应链金融相比其他金融解决方案的特点：

- 基于供应链系统内的真实交易，并且熟知系统内的交易规则、商品特点、物流方式等
- 以与交易相关的资金流信息、物流信息、商务信息、仓储信息等为主要风险控制变量
- 主要以供应链交易产生的现金流作为第一还款来源



供应链金融


审核是否满足申请条件
核实信息的完整性、真实性
调查企业的经营、信用情况
审批通过后进行放款
供应商收到贷款资金
提交申请（供应商）
业务调查
风控审批
放款
选择产品、申请金额
填写企业相关信息文字
提交企业相关授信材
风控人员审核供应商及业务人员提交的申请材料
确定是否通过申请，并出具审批意见

Thanks