网银在线新支付平台总体架构介绍

进步就需要变革，完美则需要经常变革

--丘吉尔

随着新兴互联网金融业务的迅速崛起，对支付服务提出更高的要求，网银在线原有系统架构很难满足快速变化、日益复杂的新兴业务需求；与此同时，随着用户量、业务量爆发式增长，系统的处理容量和稳定运行也面临考验。为此，2013 年开始新支付平台设计定位为：能快速响应业务发展，架构更清晰合理，服务更稳定可靠，具备可伸缩和扩展能力，支撑未来千万级以上的交易处理能力，为今后企业发展构建核心竞争力。

一、 总体建设原则

新支付平台秉承继承发展、集中统一、安全高效、平滑过渡四个基本原则：

- **继承发展**。要继承原业务流程和对外接口，优化系统架构，提高支付系统运行效率和稳定性；要前瞻设计和开发系统功能，以适应未来支付清算业务发展和创新需求。
- **集中统一**。要适应互联网金融发展和金融创新的需要，逐步整合统一架构，公共核心业务沉淀为基础支付平台，为上层业务系统提供便捷统一的支付服务。
- **安全高效**。系统建设要坚持安全与效率并重，科学设计业务流程，提高系统运行效率；要完善运营管理和运行维护体系，确保系统安全、稳定运行。
- **平滑过渡**。要充分考虑新支付平台系统的兼容性，实现系统上线的平稳切换，平滑过渡；要采取必要措施，确保业务的连续性和资金的安全性。

二、 总体架构框架

总体架构框架参考 TOGAF 与 Zachman（扎科曼）企业架构框架，并根据现阶段的业务特点、系统规模、发展阶段与团队结构对框架进行简化，先解决主要问题。现阶段企业架构框架如下图所示：

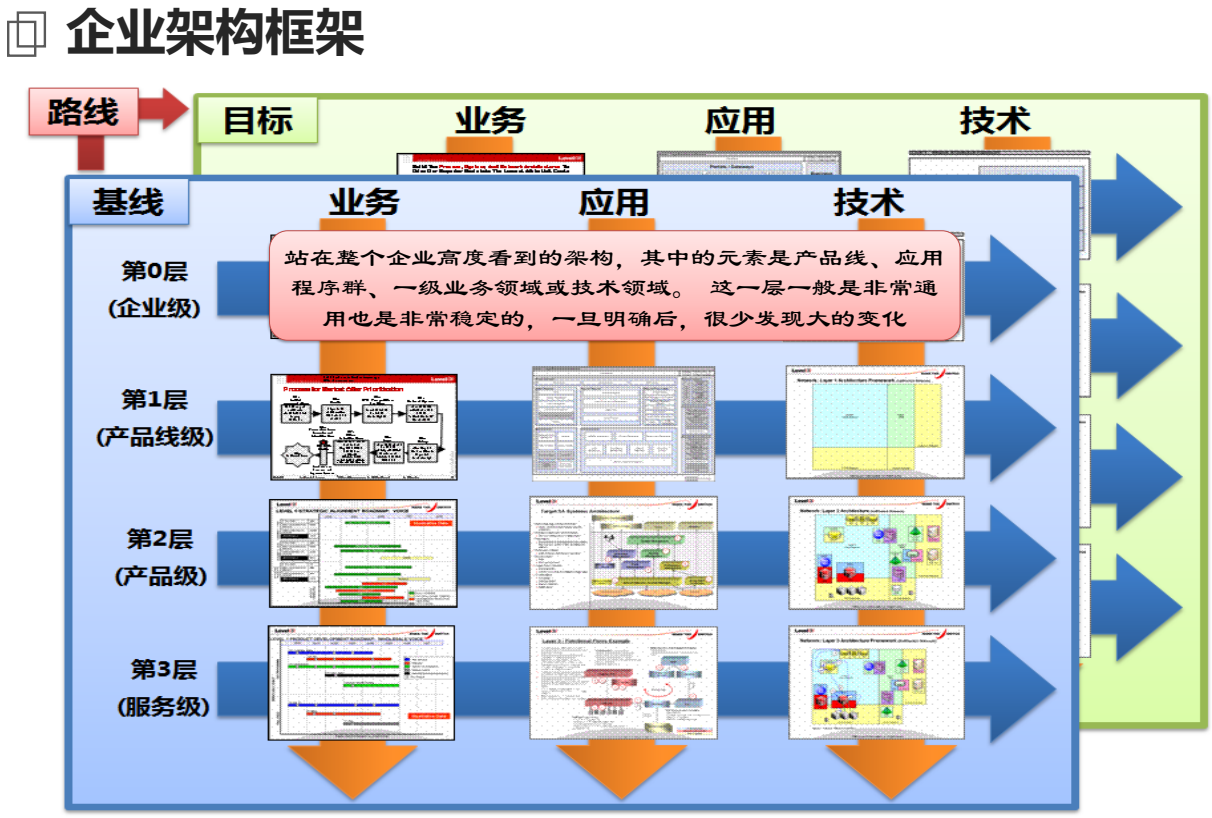

图 1 现阶段企业架构框架图

企业架构框架通过三个维度进行架构进化，首先，横向各列代表企业最重要的业务架构、应用架构、技术架构依次推进，其次，纵向至上而下分为企业级、产品线级、产品级、服务级逐级细分，最后，重大架构变革则通过规划路线由外及里，从基线架构向目标架构演进。针对新平台总体架构设计是站在全站高度看

到的顶层架构，这层在段时期内应当是稳定、通用的。

下面通过总体业务架构和应用架构来描述新支付平台架构建设及规划情况。

三、 业务架构

业务架构依据公司战略，承担描述企业的产品与服务、切分各产品线的边界职能，清晰业务之间的协作关系与流程，识别业务整体差距，逐步完善整体业务环境，支持公司的可持续发展，为业务发展提供整体业务与产品蓝图。

经过与发展战略、业务发展需求分析，当前业务架构重点解决以下三个需求：

- **基础服务抽象与封装，复用公共业务服务；**
- **核心系统稳定性需求，解决既快又稳矛盾；**
- **提供完整的数据视图，沉淀企业核心数据。**

（一）总体业务架构

从需求出发，新支付平台业务架构将各产品层的公共服务、支付工具、账务、会员、信用沉淀到基础支付平台。建成稳定可靠的基础支付平台，沉淀并积累账户、会员、信用等企业核心数据，结合灵活扩展的商户会员产品、个人会员产品、无线及线下产品组成的各产品线，形成稳中灵变的业务架构，适应未来业务发展需要，总体业务架构设计如下图所示：

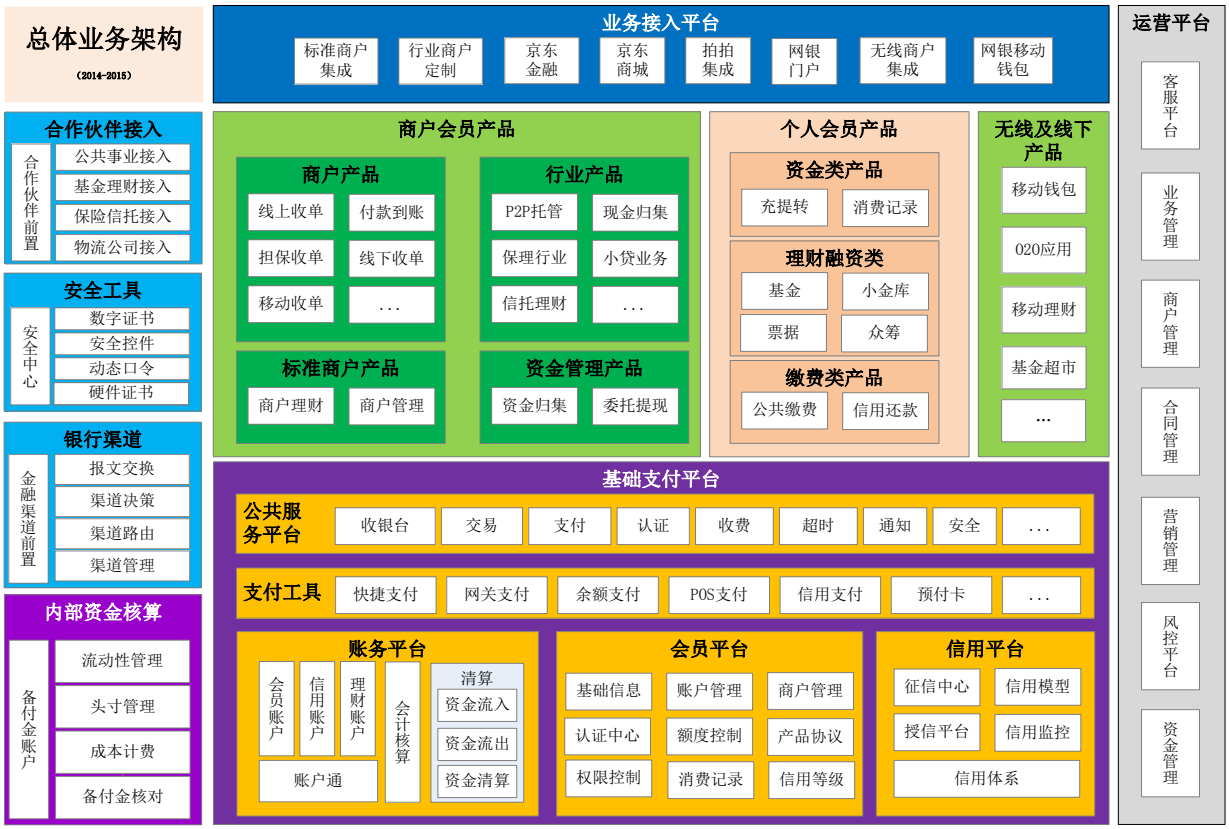

图 2 总体业务架构

（二）架构实践难点

之前系统承接各种业务需求，很好的满足当时的业务需要，但缺乏全站统一的业务架构蓝图，导致关键信息分散各处，业务流程复用困难，主要集中在会员体系、交易体系、账务会计体系三个方面，这个新老平台切换带来很大挑战。

1、缺乏统一会员体系

原先会员体系的问题主要是分散、模糊、单一。会员体系概念上的有商户和银行账户、企业站会员、个人钱包会员，彼此必须通过繁琐的映射关系才能实现业务上的互通互用；商户和银行会员与账户区分模糊，或者说就没有将会员的概念从账户中区分，

企业站会员和商户账户概念模糊；基于基本账户之上的会员体系造成客户分析失真。

统一会员体系，会员号用来存放该资金账户所隶属的会员编号，所有的注册会员都将得到唯一分配的会员号；

会员号规则如下：

会员号（18 位） = [360 固定前缀] + [2 位会员类别] + [3 位预留位 000] + [9 位生成序列号] + [1 位校验位]

格式说明：**360 XX 000 XXXXXXXXX X**

其中，会员类别分为以下四类，不同的会员类别采用不同的 9 位序列号。

00：个人会员

08：企业会员

80：银行会员

88：内部会员

按新的会员编号规则，能支持 10 亿以上，甚至万亿的会员需求，统一个人、企业、银行、内部会员，为今后的业务复用和发展建立基础。

新老会员体系的过渡采取重建、融合、兼容三种方式，内部影响的采用重建和融合，例如个人、银行、内部会员，涉及到外部影响的采取兼容方式，最大程度对外部业务无感知。

2、缺乏统一交易系统

由于历史建设时期局限，没有统一交易的概念，因此每个业务、支付工具都形成各自的交易系统，例如会员应用、企业站业

务、快捷网关、小金库等等。每个交易系统又有自身的状态体系，再加上业务与业务、业务与支付工具需要互用，则通过交易调用交易的嵌套是的业务流程变得非常复杂。

统一交易平台对业务产品中通用的复杂交易处理逻辑进行包装，降低业务产品的复杂度及重复研发的成本，统一封装各种支付工具的处理逻辑，提供组合支付的能力，降低业务系统使用支付工具的成本；此外，交易统一有利于风控统一校验，运营统一查询提供平台。

新老交易系统迁移采用逐步分流、兼容过渡的方式。建立流量分流系统，切换流量从小到大分步验证新交易的正确和兼容性；针对例如退款等此类关联交易则按同源处理原则分流到原正单处理的系统兼容过渡，如此一来，新交易既能得到充分验证，同时切换迁移时对上游系统或外部用户无感知。

3、账务体系不完善

账务体系包含清结算一代账体系包含银行账和商户账，企业站和个人站的业务形成二代账体系，二代账在一代账中创建个人总账、企业总账、小金库总账等方式虽解决了银行账、商户账在一代账的统一，但一代账务体系并不完善，清结算系统是 2005 年开始投产运行，很难胜日益复杂的业务场景，问题主要包含几个方面，第一，面向商户的账务架构局限应用范围，第二，单边记账的模式不能完整表达账务的收付关系，也很难追溯资金的流向，第三，缺乏中间账户和内部账户，无法表达资金在途情况和环节，

资金的平衡依赖业务系统的资金流程完整性，同时手续费等内部也无法得到体现，第四，没有运营会计的支持，无法对单日账户科目借贷、总分、资产负债等平衡关系准确检查。

新平台账务体系目标是整合一、二代账务，新城统一完整的账务体系，首先，对账户号重新统一规划，其次，引入复式记账会计体系，再次，建立内部中间账户，清晰记录资金流转过程，最后，通过账务核心和会计核心共同完成账务体系的完整性。

新账户号规则如下：

账户号（24 位） = [360 固定前缀] + [2 位会员类别] + [3 位预留位 000] + [9 位生成序列号] + [1 位校验位] + [2 位账套编号] + [4 位账户子类别]

= **会员号（18 位）** + [2 位账套编号] + [4 位账户子类别]

格式说明：**360 XX 000 XXXXXXXXX X XX XXXX**

其中，账套和账户子类别解决账务隔离和账户属性多样性，例如，个人会员的账户子类型：

0001：基本账户

0003：理财账户

0005：保证金户

0007：P2P 个人专户

0009：小金库账户

…

会计核心和账务核心共同构成了新支付平台的账务体系。账务核心负责外部业务系统对账务的请求，包括生产账务记账凭证，修改账户实时余额和记录账务流水。会计核心则是以会计思想来

管理账务，其职责包括把账务核心的收付账务请求转化分录并记录下来，通过日切来计算账户余额和科目余额，检查借贷平衡。

账户余额迁移是非常敏感的活动，资金风险极高；总体策略是上层业务迁移新平台交易支付调用新账务统一记账，二代账与三代账并行期共用账户余额，一代账与三代账并行期内同步记账；首先，关闭二代记账入口，最新下线二代账系统；其次，一代账与三代账并行验证资金无误后，正式过渡到三代账实现三账合一，期间需对跨账明细逐笔核对，确保每日发生额完整无误，在途资金和余额初始化则需在一段并行时间内财务核准确认；最后，新会计系统每日会计核算确保三代账务平衡准确。

（三）业务架构价值

业务架构的主要价值用规范、统一、沉淀三个词来概括，具体提现以下几点：

1、 公共核心业务沉淀为基础支付平台,统一提供基础支付服务。平台对公共处理逻辑进行抽象和封装并下沉形成统一的基础支付平台，降低业务产品的复杂度及重复研发成本；

2、 基础支付平台做到安全、稳定、可扩展，为上层业务的快速增长与创新需求提供平台支撑；从总体业务架构层面来根本解决互联网业务的“快”和支付行业的“稳”之间的矛盾；

3、 沉淀企业核心数据，随着业务数据不断沉淀积累，这些数据是企业持续发展的源动力，同时也为用户和业务提供大数据支撑；

4、 基础支付平台使业务核心更加专业化，组件式平台，使服务自身能够通过插件式体系进行灵活扩展；

5、 统一交易平台作为数据的唯一集中点，提供完整的、清晰的交易、支付数据，满足客户对支付数据展现和对账的需求；

6、 通过清结算业务向新资金平台切换，实现三账统一、会计集中，简化新业务的流程设计，降低技术研发成本。

（四）架构发展规划

虽然新支付平台两期投产上线，但业务架构的全面落实仍然处于一个布局与打基础的阶段，有以下几个方面需要加强和改进：

1、 核心业务服务进一步增强，特别是支持前方产品发展依赖度最高的资金服务，必须建设稳固支付，清算，账务，会计，核算的整套体系，一些通用服务需要进一步优化。

2、 会员体系必须加强，基础模型与会员信息纳入统一的会员信息业务体系进行设计与管理，以支持于前端产品的个性化与差异化运营。

3、 推进产品化，新产品的研发必须按产品进行设计、实现、运营与管理。原有功能必须分阶段进行梳理，形成产品。

四、 应用架构

总体应用架构模型描述了整个信息系统架构的设计思路、主要组件及其相互间的关系，以及组件、用户和外部系统之间的关系；提供了一个简单明了、清楚而易于理解的模型，帮助项目组成员就目标系统的总体架构设计达成共识；描述了为实现业务目标而要求信息系统应具有的能力，并定义了主要的系统特征和系统需求。新支付平台设计总体技术方向为：

- **建设安全、高可用、灵活的架构**
- **采用开放的面向服务架构**
- **采用基于组件、分层的架构**

（一）应用架构原则

1、 流程化原则：以流程的方式来描述支付的业务处理，通过合理及可配置的流程设计，使得支付业务灵活，易于调整；

2、 可重用原则：要打破紧耦合和竖井式的方式，将基础业务处理模块化封装，便于重用，有利于方便、快速地满足新的需求，同时降低开发和维护的成本；

3、 松耦合原则：采用松耦合的设计，使得各系统独立性增强，各系统划分和职责更加清晰，保证整个支付业务的灵活性。

除以上优流程、可重用、松耦合基本架构原则外，按高可用性、可扩展性、低成本三个方面出发总结如下应用架构原则，其中绿色文字部分是目前新支付平台已基本做到，而蓝色文字部分

是正在逐步改善和优化。

表 1 应用架构原则情况表

应用架构原则	高可用性	可扩展性	成本
无单点，N+1 设计	√		
服务可重用	√	√	√
无状态	√	√	√
避免过度设计	√	√	√
引进成熟技术	√		√
短事务/柔性事务	√	√	
并发控制		√	
异步处理	√	√	√
可复制	√	√	
可缓存		√	√
可回滚、禁用	√		
应用与数据独立	√	√	√
可水平拆分		√	√
计算可并行		√	√
分级与降级	√	√	√
支持多数据中心部署	√	√	√

【绿色表示已完成，蓝色表示进行中】

（二）总体应用架构

新支付平台实现应用系统的层次平台化，进一步提升应用架构合理性，新平台纵向有效建立支付产品层、交易层、支付层、资金层等平台化处理架构，产品层提供灵活多变快速扩展的能力

适应业务的不断变化，交易层、支付层、资金层及渠道形成基础支付平台作为支付业务关键链路系统，做到安全稳定，自治容错，易于伸缩等特性，信息集成层则促进各应用系统之间松耦合。总体应用架构设计如下图所示：

总体应用架构

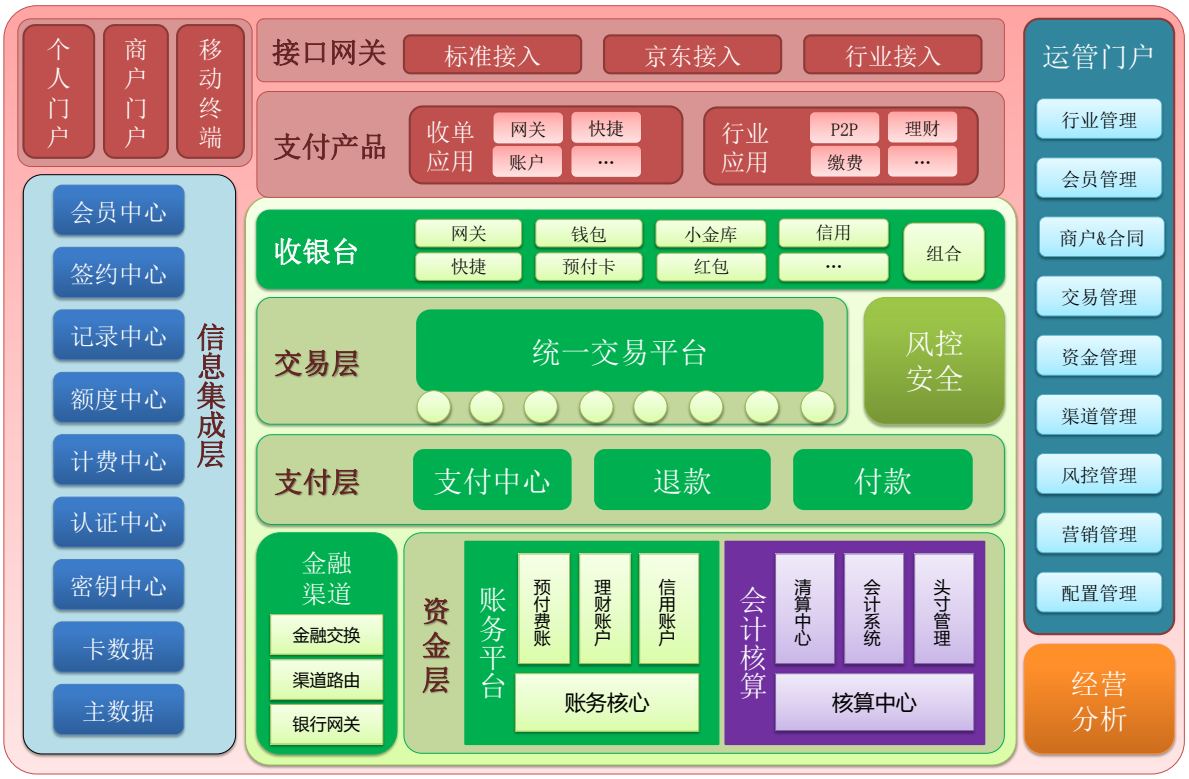

图 3 总体应用架构

总体应用架构是企业业务系统的蓝图，可以指导具体解决方案的制定、系统的开发和部署。上图所示，新支付平台的总体应用架构业务流程从架构的中部至上而下分为接口网关层、支付产品层、交易平台层、支付层、资金层；从领域上划分为七个领域，业务与产品域、基础支付平台域、资金平台域、金融渠道域、信

息集成域、运营平台域、风控及数据域。其中业务与产品域。包含会员门户及终端、接口网关、支付产品，与会员界面或系统直接交互，此域能处理各类业务需求，要求能快速响应业务变化，应对负责的支付应用；基础支付平台域包含交易层、支付层及收银台系统，此域对支付业务抽象成公共服务为业务与产品域系统提供基础业务支撑，此域要求高效，稳定，容量可扩展；资金平台域包含账务、会计、清算、核算等资金处理的核心系统，此域要求绝对的安全和稳定。

以下按高可用性、可扩展性、低成本三个方面介绍架构情况：

1、高可用性

新支付平台的高可用目标是 99.96%以上，总体策略顺序是避免发生、降低概率、控制影响和快速恢复；具体措施如下：

（1）应用系统采用无状态设计，分布式集群部署无单点；关键路径核心系统数据库进行 Failover 改造，避免数据库单点故障中断支付业务，双十一大促前核心数据库分库分表，扩展容量的同时也提高数据库可用性；

（2）系统运行可监控，可回滚，可禁用。监控系统在故障发生初期能及时预警；新上线的系统在预发布环境生产验证，如有异常及时回滚；对局部故障可进行降级禁用处理，降低故障概率，控制故障影响；

（3）业务服务采用合理超时重试和幂等性设计，提高系统的容错能力，特别是在网络异常，磁盘 IO 抖动等情况的业务完整性；

（4）业务系统合理分级，一级系统不依赖或弱依赖二级及以下系统；异步设计降低系统之间的强耦合，例如会计系统异步消息处理与账务解耦；可根据具体场景进行有序降级；

（5）多 IDC 部署，只读站的建设进一步提高系统可用性。

2、可扩展性

新支付平台的可扩展性目标是根据业务需要无限伸缩，总体策略按业务类型垂直拆分，按客户或请求编号水平拆分，按读写访问关系实施读写分离和数据复制；具体措施如下：

（1）业务与产品域各系统随业务需求垂直扩展拆分，应用和数据相互独立；

（2）CDS（Wangyin Client Database Splitter）数据库基础服务，实现数据库的分库分表、读写分离，以及 Failover 的能力；

（3）MSP 消息中心为系统间异步处理和系统扩展，以及数据异构复制及广播提供基础服务；

（4）容量与资源使用可监控，提前进行容量预警，例如服务吞吐量、响应时间、关键服务访问量等；

（5）账务的缓冲记账及汇总记账解决账务的热点账户问题。

3、低成本

新支付平台的可扩展性目标是单笔支付耗费更低的成本，总体策略资源根据业务重要和数据关键程度分级合理分配，减少或消除依赖成本较高的“IOE”，合理设计提高资源的整体利用率；具体措施如下：

（1）业务及系统分级，重要核心系统使用好的基础设施，而非关键系

统使用廉价运行环境；

（2）使用业内成熟的开源产品，例如数据库在非核心数据基本采用MySQL数据库；

（3）N+1的架构设计，降低单台机器高可靠性的要求，进而减少成本投入；

（4）基础资源虚拟化，提高资源的利用率。

（三）架构实践难点

新支付平台应用架构在项目涉及面大，几乎涉及整个基础业务系统的改造调整，同时新的业务需求继续承接，在新老系统并存期间需要很多临时过渡方案，因此，实施过程中遇到各种各样的问题与困难。事物总是先求生存，然后求发展，在这些困难当中，资损控制、高可用性始终是支付类平台始终是悬在头上的达摩克利斯之剑，是安身立命的根本，下面就这点介绍新平台遇到的难点和解决方案。

1、 资损控制

金融机构存在的意义就是承担风险、获得收益，作为第三方支付公司，资损控制是资金安全的重要指标，这里所说的资损是指交易、账务等系统因程序逻辑或系统异常导致的资产损失。

（1）幂等控制

分布式架构各系统服务间的访问难免出现处理中断或访问超时等情况，通常的做法是通过重试补偿的方式解决，对于支付系统这种重试如果没有幂等控制就会产生资损，在恶化的情况下甚

至是灾难。新支付平台从业务、交易、支付、账务、金融渠道的关键链路上增加幂等控制和唯一流水号，具体来说就是在数据库上增加一张幂等锁表对流水号控制资金转移活动重复执行。

（2）资金核算

除了联机交易期间控制资损之外还需进行资金核算，日清月结确保每日交易、账务资金无误；主要资金核算内容包含下图所示：

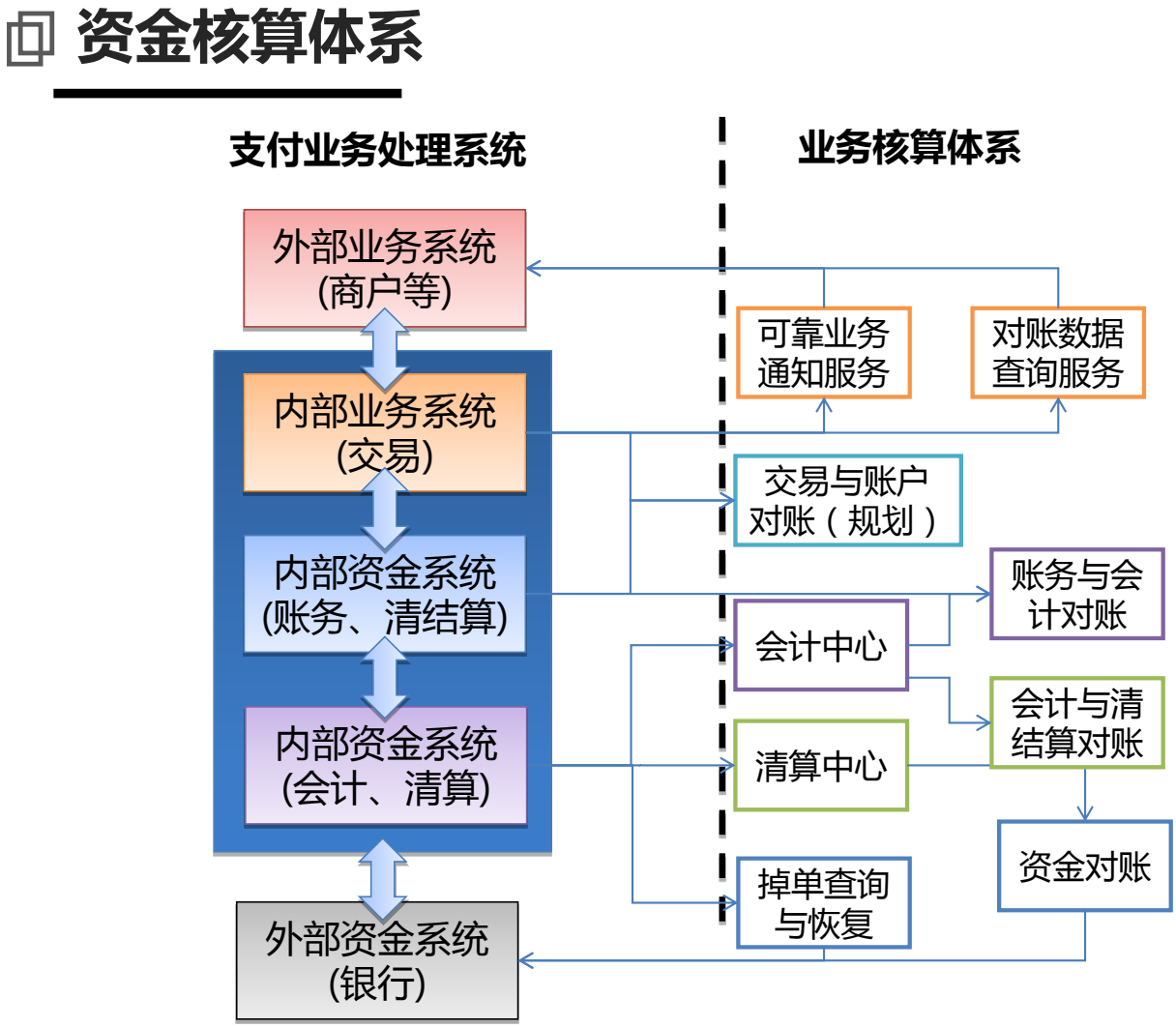

图 4 资金核算体系

（3）数据一致性

通常一次支付过程需要涉及多个支付工具或多个账户的资金转移，特别是组合支付工具的场景。以简单的银行卡消费为例需要完成三个步骤：1）渠道会调用银行扣款完整资金流入，2）账务系统会完成充值转账处理，3）交易系统给商户平台返回交易成功；若三个步骤一旦出现不一致，则会出现资金风险；新支付平台业务流程采用“先收后付不垫资”原则和“掉单补查”机制控制数据不一致产生的资损，后续规划使用最终一致性的分布式事务或称柔性事务来解决数据不一致问题。

2、 高可用性

高可用性是支付服务质量的重要指标。平台的业务量越来越大，系统越来愈多，特别是关键链路上的核心系统如账务核心，账务核心的不可用就会影响全站大面积的业务，下面就高可用性的几个方面简单介绍。

（1）缓冲记账

缓冲记账是指对于有大量并发账务请求的账户进行特别记账处理，即不实时创建账务流水和更新账户余额，记账信息登记在缓冲区，根据设置定时对一段时间内的一批缓冲账务请求进行汇总记账并更新账户余额。参与缓冲记账的账户在账务请求时系统先将记账信息登记在缓冲区，缓冲记账每隔一定时间对于当日的缓冲账务操作请求进行逐笔记账并更新账户余额。另外为了保证缓冲区内的账务请求不会被遗漏，系统还会在每日凌晨固定时间

对缓冲区中上日未处理的所有数缓冲记账据进行批量逐笔记账并更新账户余额。这样即使有大批量业务数据的账户，账户余额和账务明细每隔几分钟更新一次，在一定时间内能满足账户查询的需要，同时能解决热点账户并发引起的数据库锁超时问题。

缓冲记账主要应用在流入账户或余额不敏感的账户上，例如中间中转账户、银行应收账户等内部账户，以及大促期间特大平台商户的商户待清算账户，缓冲账户号可通过在线配置进行维护。

（2）异步记账

异步记账是在特殊业务场景下的记账优化，特别是在借贷双方余额同时增加的情况，例如商城用户用银行卡在线消费的情况，此时银行资金流入后账务处理将银行应收和商户待清算账户同时增加交易金额，这种类型的业务对账户余额的实时性要求不高，可通过异步记账，缓解高峰时段大量同步调用账务服务而产生的记账压力；同时账务服务在不可用期间也不影响银行卡收单交易。

（3）错误码规范

分布式环境下故障发生之后会迅速传导影响故障的识别和定位，为此新平台为每个应用系统分配系统号，而这个系统发生的错误码编码规范中就含有系统号，这样在上层系统中能直接定位故障的发生节点与大致原因，提高故障处理响应速度。

（四）平台运行情况

新支付平台一期和二期项目历经 9 个月完成建设投产，支付成功率从投产前后的对比来看有了明显的提高，网关成功率从原

来的 45～60%提高到 64～78%（图 5 所示），快捷/网银+成功率从 90～93%提高到 92～95%（图 6 所示）。

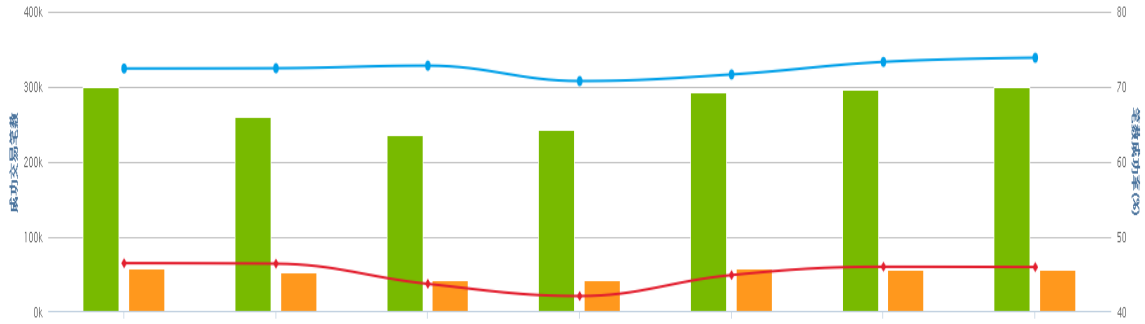

图 5 网关成功率对比

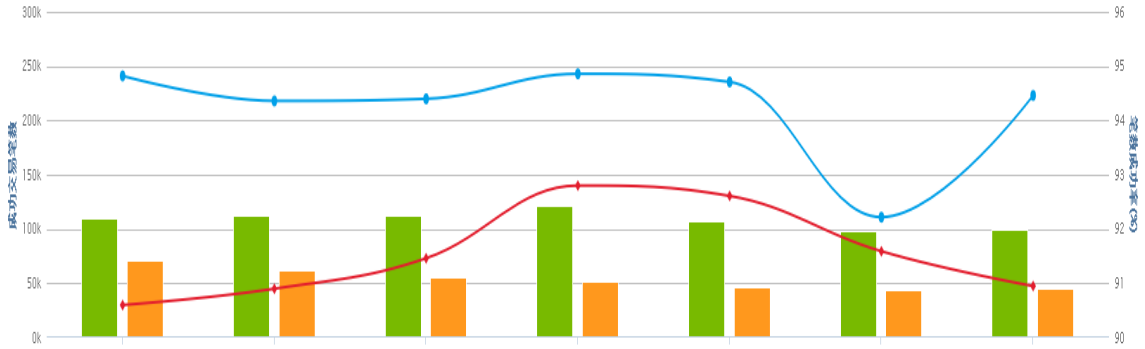

图 6 快捷成功率对比

在 2014 年大促活动期间运行稳定。“618 大促”当日交易创建破百万笔，“双 11 大促”第一次经受 294.8 万笔峰值考验，当日交易系统 TPS 峰值到达 198 笔/秒，支付关键路径上的数据库服务器总体 load 在 2～3 之间，CPU 利用率在 10%左右，总体系统没有太大压力。

五、 总结与展望

新支付平台作为支付业务的重要平台，它规范了网银在线各业务产品线的边界，清晰业务节点之间的协作关系，为京东商城、京东金融、拍拍网及外部商户提供随时，随地，快捷安全支付服务。

新支付平台还处于初级阶段，原有系统还未完成全部迁移，基础公共服务还在不断优化和建设，支付成功率还需进一步优化提高，架构建设有待不断完善、合理，难免存在不足之处恳请各位专家、领导指正。