效用树

|  |  |  |
| --- | --- | --- |
| 质量属性 | 属性求精 | 场景 |
| 可恢复性 | 数据恢复 | 数据库恢复时间不超过10分钟（H,H） |
| 系统故障恢复 | 重启、从错误中恢复的时间小于1分钟(H,H) |
| 可伸缩性 | 并发量 | 可支持的用户的并发量不低于30000(H,H) |
| 可支持单车的并发量不低于10000(H,H) |
| 并发请求响应速度 | 用户请求服务的平均响应时间不超过5秒(M,M) |
| 并发请求成功率 | 最高并发中，用户成功获得响应的概率不低于95%(M,M) |
| 能成功报告自己位置的单车不低于95％(M,M) |
| 安全性 | 机密性 | 系统验证用户身份，拒绝不在用户权限范围内的服务和数据，并通知用户(H,M) |
| 完整性 | 拒绝未授权的访问(H,H) |
| 互操作性 | 数据接口 | 与用户所选的支付APP进行数据传输，交互成功率达到100%(H,M) |
| 与GPS全球定位系统交互，误差在20米之内的交互成功率到达99%(H,M) |
| 易用性 |  | 用户完成操作时间如注册，借车操作时间不超过3分钟（M,M） |
| 用户操作成功率高于99%(M,M) |
| 可用性 | 可用时长 | 单车端嵌入式系统无故障运行时间大于1个月(M,H) |
| 故障处理 | 系统发生故障可以在1分钟内恢复，单车发生故障可以及时通知维修人员维修(M,M) |
| 可扩展性 | 扩展后大小 | 更新APP大小不超过原有的10%(M,M) |
| 扩展影响 | 所影响到的源代码量不超过2%(M,M) |
| 性能 | 服务请求响应时间 | 用户正常使用客户端，操作响应的时间小于1秒(M,M) |
| 用户使用客户端通过网络访问，在不涉及外部系统的情况下获得服务器响应时间小于2秒(M,M) |
| 用户使用客户端通过网络访问，涉及外部系统的情况下，服务器中转响应时间小于2秒(M,M) |

敏感点列表

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 架构决策 | 相关质量属性 | 场景编号 |
| S1 | 采用分布式数据库保存部分区域数据和全部数据的完整拷贝 | 可恢复性 | A1 |
| S2 | 纪录余额数据库每次变化的日志，根据日志恢复数据 |
| S3 | 本地提前开发相应应急服务 | A2 |
| S4 | 本地购买备用主机 |
| S5 | BigTable | 可伸缩性 | A2 |
| S6 | 数据库水平分区 | A3 |
| S7 | 数据库读写分离 |
| S8 | 数据对城加密存储 | 安全性 | A5 |
| S9 | 传输全程延迟检测 | A6 |
| S10 | Tokenisation |

权横点列表

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 架构决策 | 相关质量属性 | 场景编号 |
| T1 | 采用分布式数据库保存部分区域数据和全部数据的完整拷贝 | 可恢复性、可伸缩性 | A1 |
| T2 | 数据对称加密存储 | 性能、安全性 | A3 |
| T5 | 传输延迟检测 | 性能、安全性 | A3 |
| T6 | Tokenisation | 性能、安全性 | A3 |

有风险决策列表

|  |  |  |
| --- | --- | --- |
| 编号 | 架构决策 | 风险 |
| R1 | 采用分布式数据库保存部分区域数据和全部数据的完整拷贝 | 数据量大，维护副本成本高 |
| R2 | 纪录余额数据库每次变化的日志，根据日志恢复数据 | 短期恢复数据困难大，有失败的可能 |
| R3 | 传输全程延迟检测 | 降低系统性能，时间监测成本高 |
| R4 | Tokenisation | 降低系统性能，信息传输中异常检测撤回机制较复杂，可能会影响性能 |

无风险决策列表

|  |  |
| --- | --- |
| 编号 | 描述 |
| N1 | 数据库水平分区 |
| N2 | 数据库读写分离 |
| N3 | 本地提前开发相应应急服务 |
| N4 | 本地购买备用主机 |
| N5 | 用户－服务器身份认证 |
| N6 | BigTable |
| N7 | 使用高精度的GPS定位服务 |
| N8 | observe模式+备忘录模式 |