# 区块链需求文档（甲方视角）

## **1. 背景**

随着区块链技术在多个行业的应用日益广泛，我公司计划在现有区块链平台基础上，全面推进区块链技术的应用，尤其在数字门票和金融交易等核心业务场景中。为此，我们期望通过与合作方的深度合作，进一步提升现有系统的性能与安全性，并确保系统在合规性方面达到相关要求。 本项目目标是在 Fabric 联盟链的基础上，结合更高效的技术架构和系统改进，提升业务处理能力，支持不同业务场景中的全业务上链，满足当前及未来的业务需求。

## **2. 目标**

### **2.1 总体目标**

**全业务上链**：支持景区数字门票、交易所及金融系统等核心业务的全业务上链，并能在高并发、高吞吐量场景下保持系统的稳定性和处理速度。

**智能合约清结算**：通过智能合约自动执行清结算操作，确保交易的自动化和高效性。

**高性能、高安全性**：确保系统在大规模业务场景下的稳定运行，并具备抵御安全威胁的能力，尤其在数据保护和加密技术方面。

### **2.2 具体目标**

**块内并发交易支持**：系统需要具备处理并发交易的能力，特别是涉及相同关键数据的多笔交易时，能够保证数据一致性并高效处理。

**优化交易回执速度**：优化当前系统的性能，确保在高并发场景下，交易回执时间能够达到或低于 600ms，并支持每秒最多处理 1200 笔交易。

**国密算法支持**：替换现有的加密算法为符合中国国家标准（国密算法）的加密算法（如 SM2、SM3、SM4），确保系统的合规性。

## **3. 需求**

### **3.1 性能需求**

**支持块内并发交易**：系统应支持多个并发交易，特别是在涉及同一数据项时（如景区数字门票的购买、交易所的订单等）。每笔交易需要在不阻塞其他操作的情况下迅速完成，避免数据冲突和处理延迟。

**交易回执优化**：目前在高并发情况下，交易回执的响应速度存在瓶颈。我们要求通过优化交易处理逻辑，确保在高并发环境下，交易回执的响应时间能够保持在 600ms 以下。

**吞吐量要求**：系统应支持每秒处理 1200 笔交易，并确保交易处理不会受到并发交易数增加的影响。

### **3.2 安全需求**

**国密加密算法**：在区块链系统中，所有的加密操作需基于国密标准，特别是在证书生成、密钥管理、交易签名和数据传输过程中。我们要求替换原有的加密算法，采用符合中国国家标准的算法，如 SM2、SM3、SM4，确保系统的安全性和合规性。

**安全审计与合规性**：除了加密算法外，还需要对区块链平台的安全进行全面审计，确保系统在合规性和安全性上满足国家和行业标准。

### **3.3 技术实现需求**

**智能合约自动化执行**：在核心业务流程（如景区数字门票、交易所等）中，通过智能合约实现自动化清结算，支持高并发交易，并能在一定条件下自动完成结算和资金转移。

**Fabric 组件改造**：现有的 Fabric 组件需要进行国密算法的支持改造，包括但不限于：

**fabric-gateway**：调整与国密算法兼容的加密算法和签名方式。

**fabric-ca**：支持国密算法的证书签发和身份认证。

**blockchain-explorer**：支持通过国密算法进行安全连接和数据查询。

### **3.4 集成需求**

**系统集成与对接**：在项目实施过程中，需与现有系统进行对接。我们期望与区块链技术供应方密切配合，确保现有的业务流程能够无缝对接区块链平台，保证数据的一致性和完整性。

## **4. 风险控制与应急预案**

为了确保系统的稳定运行，需考虑以下风险控制和应急预案：

**技术风险**：包括技术选型风险、国密算法兼容性风险、区块链平台的扩展性风险等。需与合作方进行详细的技术调研，确保技术方案的可行性。

**安全与合规风险**：区块链系统可能面临的数据泄露、智能合约漏洞等安全隐患。必须通过安全审计、加密算法加固、代码审查等方式确保安全合规。

**应急预案**：制定紧急恢复计划，当系统出现重大故障时，能够迅速响应并恢复服务。包括故障排查、数据备份与恢复、应急通信与协调等。

## **5. 合作期望**

为确保项目的顺利推进，我们希望与合作方在项目实施过程中建立紧密合作，特别是在以下几个方面获得支持：

**技术支持与咨询**：在系统的优化和开发过程中，希望合作方能够提供针对性的技术支持，帮助我们解决区块链系统集成、加密算法替换等技术难题。

**定制化研发与功能扩展**：针对不同场景（如数字门票、金融交易等），合作方应能够提供定制化的研发服务，帮助我们根据具体业务需求优化系统功能。

**技术验证与测试**：在系统上线前，合作方应协助进行全面的测试，验证系统的稳定性和性能，确保其在高并发、大规模数据处理时仍能保持稳定运行。

## **6. 实施计划与阶段性目标**

### **6.1 交付内容**

每个阶段交付的具体内容包括：

**并发控制与MVCC改造**：确保高并发场景下的事务一致性。

**国密算法改造**：完成加密算法替换，并通过安全性验证。

**性能优化方案与交易速度提升**：优化区块链架构，提升系统吞吐量。

**完整的技术文档与改造说明**：提供详细的技术文档，说明所有技术改造的细节。

### **6.2 时间节点**

**需求确认阶段**：预计完成时间：XX月XX日。

**技术方案设计阶段**：预计完成时间：XX月XX日。

**技术实施与改造阶段**：预计完成时间：XX月XX日。

**测试与验收阶段**：预计完成时间：XX月XX日。

### **6.2 验收标准**

**并发控制和数据一致性测试**：确保在高并发场景下，系统能够处理并发交易且数据一致性无误。

**国密算法的安全性测试与符合性验证**：确保新加密算法符合国家安全标准。

**系统性能测试**：确保系统的交易吞吐量和响应时间满足要求。

## **7. 后期运维与技术支持**

项目上线后，我们期望合作方能够提供以下支持：

**运维监控与支持**：在项目交付后，合作方提供持续的系统监控和技术支持，确保系统在生产环境中的稳定运行。

**技术更新与优化**：根据市场和业务变化，提供定期的技术更新和系统优化，确保系统长期适应不断变化的需求。

## **8. 结语**

通过这次合作，我们期望能够全面提升区块链平台的性能与合规性，确保在未来的应用场景中满足业务需求，并为公司在数字化转型的过程中提供强有力的技术支持。我们相信，在技术合作方的帮助下，我们能够成功实现这些目标，并推动区块链技术的更广泛应用。