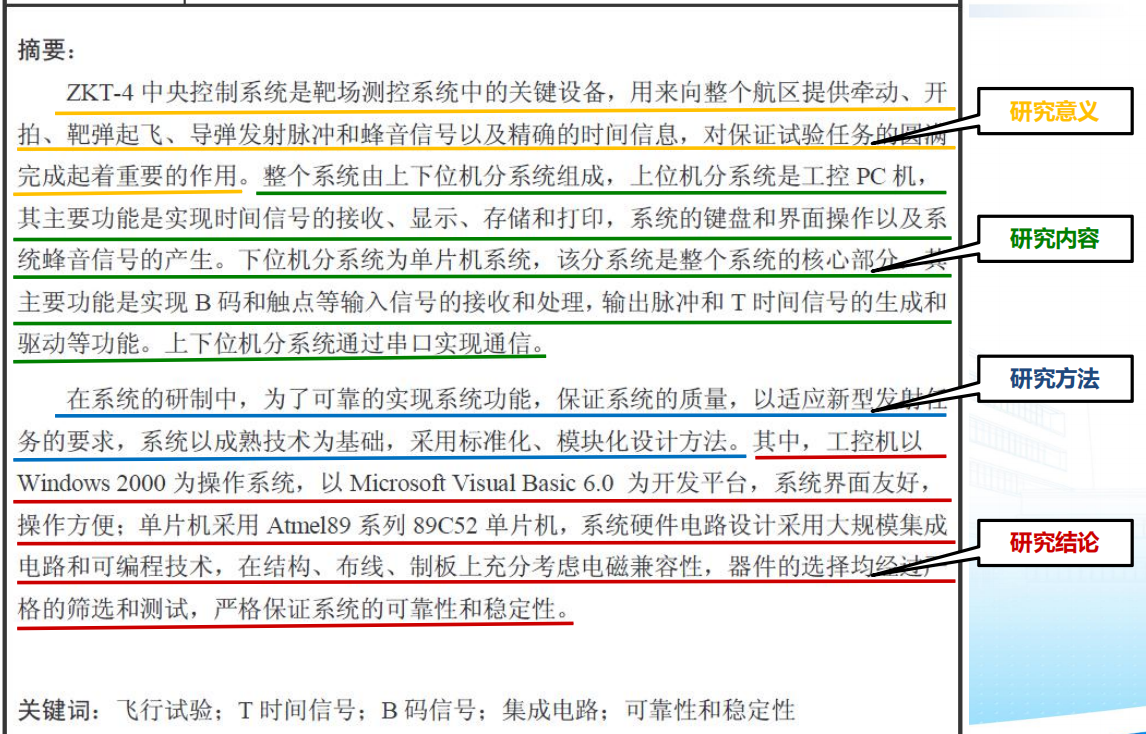
摘要（研究内容、研究方法、研究结论各提供1-2句话概括，总字数100字以内）

关键字（1-2个）



# 引言

课题X总的研究目标是。（不用写）

本年度，课题的研究内容主要包括以下2个方面。（各任务描述各自合同规定的阶段或年度研究任务的目标、内容、方法等要点。）

研究监管链共识算法的设计需求：以联盟链为基础，基于实用拜占庭容错、POA等算法，提出了满足满足监管需求的区块链设计，保证监管链安全可信、提升吞吐量、避免网络风暴、增强网络扩展性。

研究监管链共识算法的技术实现：以实用拜占庭容错、POA等算法为基础，通过优化事务元数据提取、并行化交易背书验证、角色权限动态调整、应用共识解耦等技术手段，设计满足目标需求的监管链原型。

完成2021年年度《技术进展报告》1篇。

# 研究概述

## 研究背景及意义（不用写）

。

## 课题四与其它课题的关系（不用写）

。

## 课题四研究内容

### 拟解决的关键科学与技术问题（各写1-2个）

设计满足监管需求，安全可信、吞吐量高、易扩展的监管链；并以实用拜占庭容错、POA等算法为基础，通过优化事务元数据提取、并行化交易背书验证、角色权限动态调整、应用共识解耦等技术手段，设计满足目标需求的监管链原型。

### 拟开展的主要研究内容（任务研究内容）（一段话）

研究联盟链环境下的新型共识算法，设计基于实用拜占庭容错（PBFT）等基础算法的快速共识方法，探索交易元数据提取与优化、交易背书与验证并行化、节点角色动态调整、节点信用分级与排序等机制，解决固定功能节点易遭攻击、大规模交易高并发造成的网络风暴等问题，提高监管链的安全性与效率。

### 研究技术路线（任务技术路线）（文字+至少1张图）

监管链的新型共识机制拟采用联盟链的拜占庭容错算法为基础架构，拟通过抽取交易的基础元数据重建交易的排序流程，并优化验证协议以充分实现背书策略验证等操作的并行化，大幅提高系统的吞吐率；拟构建节点候选集，利用可验证随机函数等密码学技术设计非交互式选举协议，实现背书节点等重要角色的动态更新，并引入信用模型对节点进行分级排序，实现应用层的信任机制同底层共识协议的解耦，提高系统的安全性与可扩展性。

# （各任务阐述**阶段研究的过程、技术内容、进展或阶段成果，提供必要的数据图表）**

# 信息巡查和数据处理过程的数据完整性验证（各任务名字）

## 阶段性研究内容

XXX

## 研究技术路线（技术实现方法）

XXX

## 进展或阶段性成果

XXX

## 结论

（阶段研究工作完成情况、经验和教训、下一年度或下一阶段的工作计划和建议）

参考文献

（参考文献的著录遵照GB/T 7714《文后参考文献著录规则》 的规定执行。）