参赛项目：疫情别链

基于智能合约的社区公共安全契约法制治理系统

“疫情别链”队成员简介

- 队长：徐鹤军　　2016年第一届中关村区块链大赛创新奖，从技术专家到区块链企业高管，具有丰富的技术开发，产品和市场开拓经验。对网络安全行业有深刻认识，当前主要从事区块链+云计算和安全领域的创新研究和商业实践。
- 队员：李乙平， 佰客云区块链总架构师， 擅长后端和底层链以及工具链的研发。曾任职于中兴通讯和上海贝尔，多年底层开发实战经验。

疫情别链项目的宗旨

以社区房屋登记和租房合同管理治理为抓手，发挥以房盯人，按人控疫情为主要社区治理手段和措施，

发挥区块链技术的资产溯源专长，协助本次疫情的社区业主和外来人员管控，生活服务支持和复工复产人员管理，同时为疫情后的基层社区管理做好基础，实现法制契约型和谐社会。

通过实施零知识证明的数据隐私计算方案，对租房登记管理，承租人的信息，疫情治理信息保护进行加强。

发挥区块链资产溯源的特点，对守法用户的信用积分奖励，鼓励社区人人参加治理，对违法行为的群防群治，

违法证据及时取证上区块链系统备案，对违规人员的信用积分处罚等治理规则。

采用基于FPGA的零知识证明硬件加速卡方案来加速隐私计算的效率和系统整体性能，达到更好的用户体验。

契约（区块链智能合约形式）要素

- 地点 ： 路标，基于IoT的GPS数据
- 时间 ： 日期,时间
- 对象 ： 契约双方
- 事件描述：文字，照片，视频，录音 等多媒体资料
- 事主：电话，编号
- 类型：事件类型

合约执行流程

1）向区块链节点部署合约

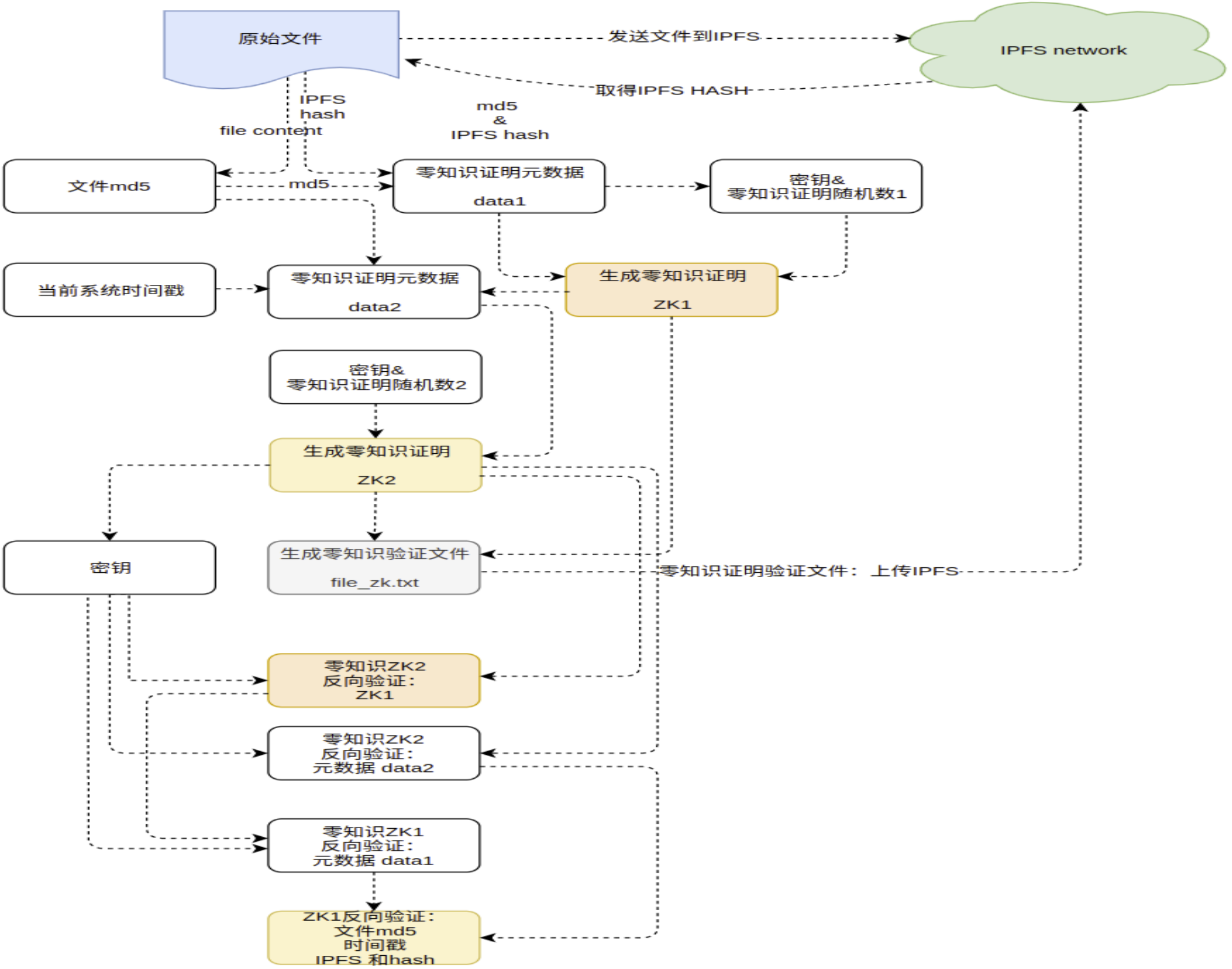
2）将合约附属多媒体资料上传 IPFS分布式文件系统存档，反馈文件存档哈希值

3）将合约要素信息上传区块链

4） 将合约地址，IPFS哈希值经过零知识证明来确权

5）查询区块链相关记录，提取合约附属哈希值

6）从IPFS文件系统提取合约附属资料用于验证


原始文件
发送文件到IPFS
IPFS network
取得IPFS HASH
IPFS
hash
file content
md5
&
IPFS hash
文件md5
md5
零知识证明元数据
data1
密钥&
零知识证明随机数1
当前系统时间戳
零知识证明元数据
data2
生成零知识证明
ZK1
密钥&
零知识证明随机数2
生成零知识证明
ZK2
密钥
生成零知识验证文件
file_zk.txt
零知识证明验证文件： 上传IPFS
零知识ZK2
反向验证：
ZK1
零知识ZK2
反向验证：
元数据 data2
零知识ZK1
反向验证：
元数据 data1
ZK1反向验证：
文件md5
时间戳
IPFS 和hash

零知识证明的FPGA加速

FPGA加速卡的初步测试效果

加速 zk SNARKs 库操作：

开发了一个 bls12-381 协处理器，能够执行 bls12-381 曲线操作 zk SNARKs 所需。协处理器

是用一个简单的指令集设计的可以从软件编程，并且在它可以执行的操作流程中是灵活的。

与 3.7GHz 处理器相比，速度提高了 3 倍.

实现更好的用户体验

本课题实现目标

- 创新拓展了区块链在社会治理场景的案例，发挥区块链智能合约助力国家基层法制建设，契约型和谐社会发展

  符合当前国家治理的重点方向

- 开发基于FPGA的零知识证明加速卡方案，具有显著优化零知识证明效率的潜力，提高云计算环境中数据隐私计算的性能，用户体验和推广效率。