[](http://www.swufe.edu.cn/version3/xuexiaogaikuang/xiaohui.jpg)**西南财经大学**

Southwestern University of Finance and Economics

**课程论文**

|  |  |
| --- | --- |
| **学年学期：** | **2022-2023学年第一学期** |
| **课程名称：** | **金融科技II** |
| **小组成员：** | **贾天宇42023024，周子博42036065，周姝颖42012018，张孙楚婷42012207** |
| **学 院：** | **金融学院** |
| **年级专业：** | **2020级CFA** |

|  |
| --- |
| 评语： |

目录

[一、引言 3](#_Toc565345215)

[（一）、背景与动机 3](#_Toc1289374177)

[1、新市民已成为未来我国经济发展的新动能 3](#_Toc254310962)

[2、新市民获取基础金融服务时处于弱势地位 3](#_Toc711880804)

[3、针对新市民住房需求的金融服务和产品不足 4](#_Toc949275391)

[（二）、设计理念 4](#_Toc815482974)

[二、技术实施方案 4](#_Toc581708864)

[（一）、 准备工作 4](#_Toc1435316104)

[1、区块链 4](#_Toc673953177)

[2、CP-ABE 5](#_Toc1302291561)

[（二）、系统设计 6](#_Toc460935503)

[1、系统框架 6](#_Toc969484192)

[2、共享模式 6](#_Toc1162385155)

[3、金融数据多级访问控制算法 7](#_Toc548563326)

[4、创新算法 8](#_Toc556523511)

[（三）、系统安全性分析 9](#_Toc1199366692)

[三、 总结 9](#_Toc1474481702)

**一、引言**

国家财政部指出，要坚持以习近平新时代中国特色社会主义思想为指导，立足新发展阶段，贯彻新发展理念，构建新发展格局，紧扣做好“六稳”工作和落实“六保”任务，发挥财政资金引导激励作用，支持地方因地制宜打造各具特色的普惠金融发展示范区，增强金融普惠性，推动普惠金融高质量发展。

我国普惠金融正处于黄金发展期，而作为普惠金融重要受益群体的新市民面临着因为信息不能跨机构流通而导致的征信难题。在经济相对落后的地区，存在大量传统金融机构没有覆盖到的人群，缺乏基础数据对其信用风险进行评估，利用大数据可以为普惠金融提供最重要的技术支撑。近年来，大数据被越来越多地用于信用风险的甄别中，成为传统征信方式的重要补充。然而，在利用大数据进行征信创新和提高风控能力的同时，其发展过程中也逐渐暴露出一些问题。

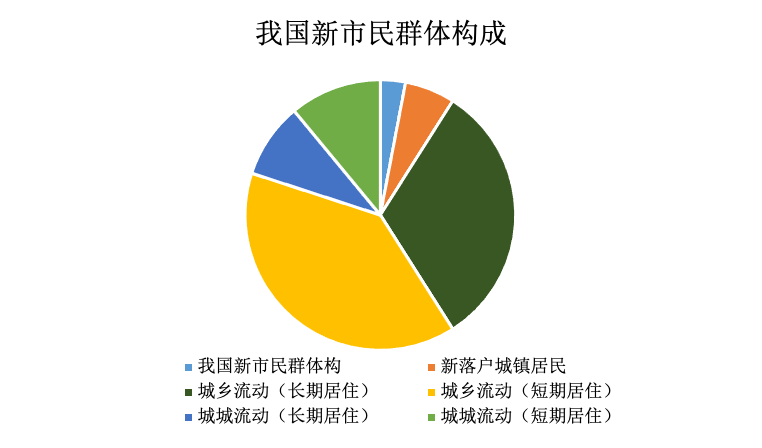
**（一）、背景与动机**

1、新市民已成为未来我国经济发展的新动能

中国银保监会、中国人民银行于近日发布《关于加强新市民金融服务工作的通知》，针对新市民在创业、就业、住房、教育、金融、养老等重点领域的金融需求，鼓励引导银行保险机构积极做好与现有支持政策的衔接，结合地方实际，因地制宜强化产品和服务创新，高质量扩大金融供给，提升金融服务的均等性和便利度。

从全国新市民的构成看，以外来务工人员为主的城乡流动人口占比最高，达71%；城镇流动人口占比20%；新落户城镇居民占比6%；高校应届毕业生占比3%。新市民逐步融入到城市，在享受相应的住房、金融和教育服务的过程中，将释放巨大的消费潜力，成为未来中国新经济、新消费中一股不容忽视的有生力量。

因此，做好新市民金融服务，从金融端服务好新市民的就业创业、住房、教育、金融、养老等实际需求，从而更好激发3亿新市民群体的消费动能，对畅通国民经济循环、构建新发展格局、实现高质量发展具有重大意义。

**图1 我国新市民群体构成**

**（来源：新市民产业与创新研究院）**

2、新市民获取基础金融服务时处于弱势地位

目前相当数量的新市民存在人户分离、抵质押资产不足、信用信息欠缺、收入与还款不匹配、金融知识和意识匮乏等问题，不符合传统金融机构的风控偏好。因此相比其他群体，新市民在获取基础金融服务时通常处于弱势地位，面临着金融服务门槛较高、获取授信额度有限、融资成本较高等问题。

3、针对新市民住房需求的金融服务和产品不足

由于尚未建立互通的金融信息系统，对新市民的征信信息获取困难。新市民进入城市不久，大多数属于灵活就业人群，城市社会保障体系暂未纳入该群体，与城市人口的社会关系和社会网络尚未建立，难以提供有效收入证明或稳定流水证明，且缺乏车辆、房产等固定资产支持，亦缺乏担保等有效增信手段，因而长期以来一直处于主流金融体系的边缘位置，导致其征信信息不完善，甚至是征信白户。而征信信息的缺失，又进一步导致传统金融机构难以对其信用状况开展有效评估，从而被挡在传统金融服务大门之外，反复如此，形成恶性循环，造成传统金融服务空白。

新市民的需求主要包括购房需求和租房需求。由于金融信息尚未实现跨机构无条件互通，非户籍人口在申请购买商品房和租住保障租赁房时面临资格认定障碍，并且在贷款时经常面临授信准入门槛高、收入认定程序复杂、还款方式僵化和利率水平高等问题。针对新市民群体的住房需求的金融产品和服务还有较大发展空间。

**（二）、设计理念**

打破金融信息互通壁垒作为实现普惠金融的必由之路，是金融行业发展的必然趋势。不同区域金融机构信息共享作为金融信息化发展的总体趋势，打破传统金融行业相对封闭的使用环境，使金融数据的收集、使用更加便捷、迅速的同时，也带来了新的安全隐患，例如个人数据泄露、勒索攻击等。金融数据安全关乎个人隐私和社会福祉。

本文提出了一种基于区块链技术的金融数据分级访问控制和共享系统。本文采用金融数据区块链上链下存储相结合的共享模式来解决区块链数据存储昂贵问题，其中链下存储原始金融数据，链上存储数据描述和数据共享日志，区块链的不可篡改特性提高了方案的可行性。通过对金融数据的属性按敏感性不同进行分级，以满足金融数据共享的灵活性需求，同时利用访问控制树、对称加密和基于属性的加密相结合的方法减小加密开销，还实现了金融数据的细粒度访问控制。另外使用密钥生成中心(Key Generation Center, KGC)和属性验证中心(Attribute Validation Center, AVC)生成用户密钥。本文最后还分析了该系统的性能和安全性，证明了本方案在金融数据共享中的安全性。

**二、技术实施方案**

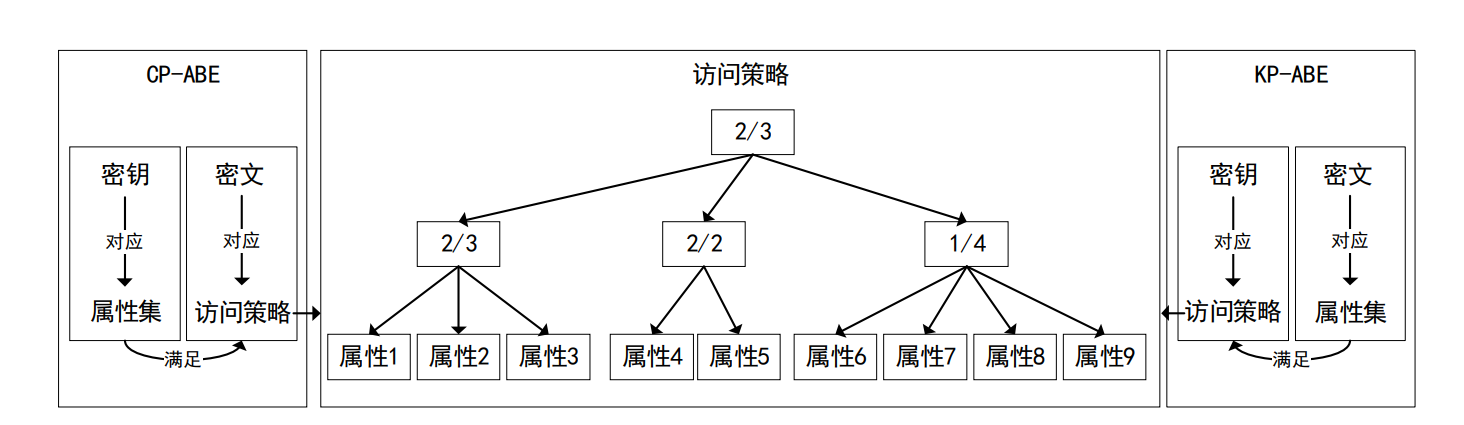
**（一）、 准备工作**

**1、**区块链

区块链提供了一种去中心化的分布式数据系统。参与系统的可信或半可信节点通过共识机制共同维护一条不断增长的链，发生过的记录均不可篡改，共识过程无需集中控制，通过Hash、数字证书、签名等密码学机制确保记录无法被伪造或破坏。因此，区块链天然具备去中心化、高可信、可追溯、不可篡改等优势。区块链按是否具有访问和管理权限可分为无许可区块链和许可区块链。无许可区块链的每个参与者均可以参与区块链的交易和数据共识过程，例如以太坊等；许可区块链为封闭网络，仅允许具有高信任度的节点来验证交易，只对特定的群体开放，例如超级账本(Hyperledger Fabric)等。传统的共识机制，例如工作量证明(Proof-of-Work, PoW)、权益证明(Proof-of-Stake, PoS)等，需要经过多个区块生成后才能确认，不可避免地存在效率低下问题。以Hyperledger Fabric为代表的许可区块链选择确认时间相对固定的实用拜占庭容错算法(Practical Byzantine Fault Tolerance, PBFT)，解决快速确认问题，提高共识效率。同时，许可区块链存在参与方的部分信任基础，性能更优；采用高性能节点作为核心节点，减弱每个节点都参与完整处理的制约，扩展性更优；用户准入和交易活动受到限制，稳定性更优；可根据不同需求进行模块化的定制，灵活性更优。因此，许可区块链更符合金融数据共享需求。

2、CP-ABE

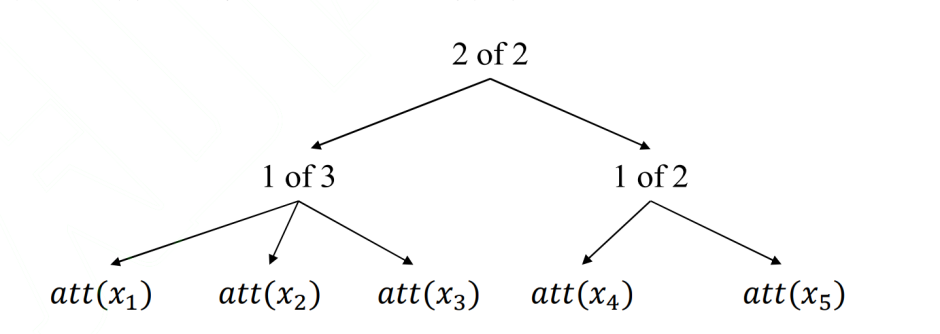
基于属性的加密算法主要分为密钥策略属性加密 KP-ABE以及密文策略属性加密CP-ABE两种。KP-ABE和CP-ABE基本结构如图2所示。传统的ABE系统是由属性来描述密文，并将策略嵌入到用户的密钥中。而CP-ABE使用属性刻画用户的资格，并且由数据的加密方来制定密文访问策略，以决定谁可以解密密文。CP-ABE中，用户的私钥与一系列属性相关，只有用户的属性符合密文的访问结构才能解密此密文。KP-ABE中，此时密文用与其相关的属性加密存放在服务器上，当允许用户得到某些消息时，就分配一个特定的访问策略给用户，其应用场景则更加偏向于付费视频网站、日志加密管理等等。

**图2 KP-ABE和CP-ABE基本结构**

KP-ABE给出了一个用户可以访问哪些信息的方案，而CP-ABE给出了那个用户可以读取密文的方案，而在金融数据共享的实际场景中，存在大量的信息需要共享给他人，这恰与CP-ABE提出的方案更加契合。以下是CP-ABE算法的四个步骤：

1）设置安全参数K：通过安全参数，生成系统公钥和主密钥 ；

2）加密首先，将访问控制策略转化为访问控制树结构t，如图3所示，结构树中的是节点表示的属性，意味着访问者必须满足该节点下j个属性中要个属性才能访问该节点中的秘密。然后，

****利用访问结构t对明文加密，得到密文

**图3 CP-ABE访问控制树结构**

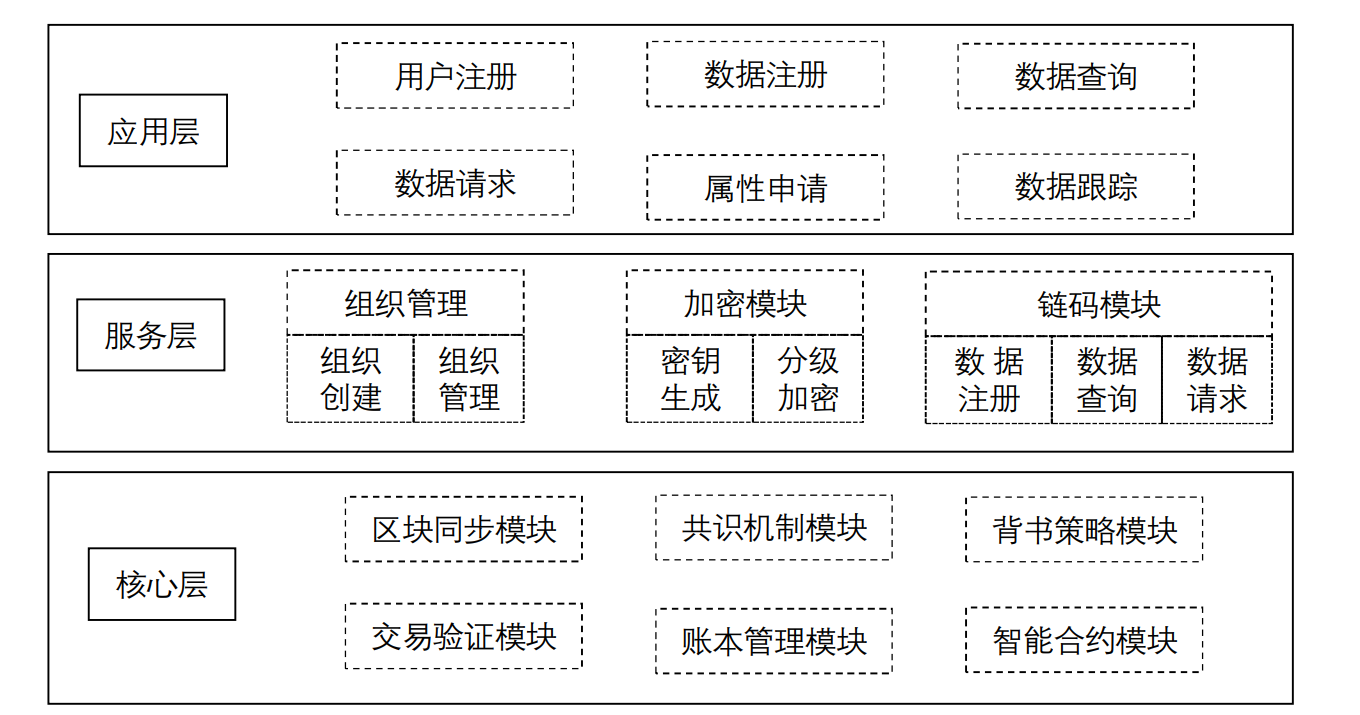
1. 生成密钥：从数据请求者的属性集合生成密钥 ；
2. 解密：利用公钥PK和自身密钥SK访问控制树，解密密文得到明文

**（二）、系统设计**

1、系统框架

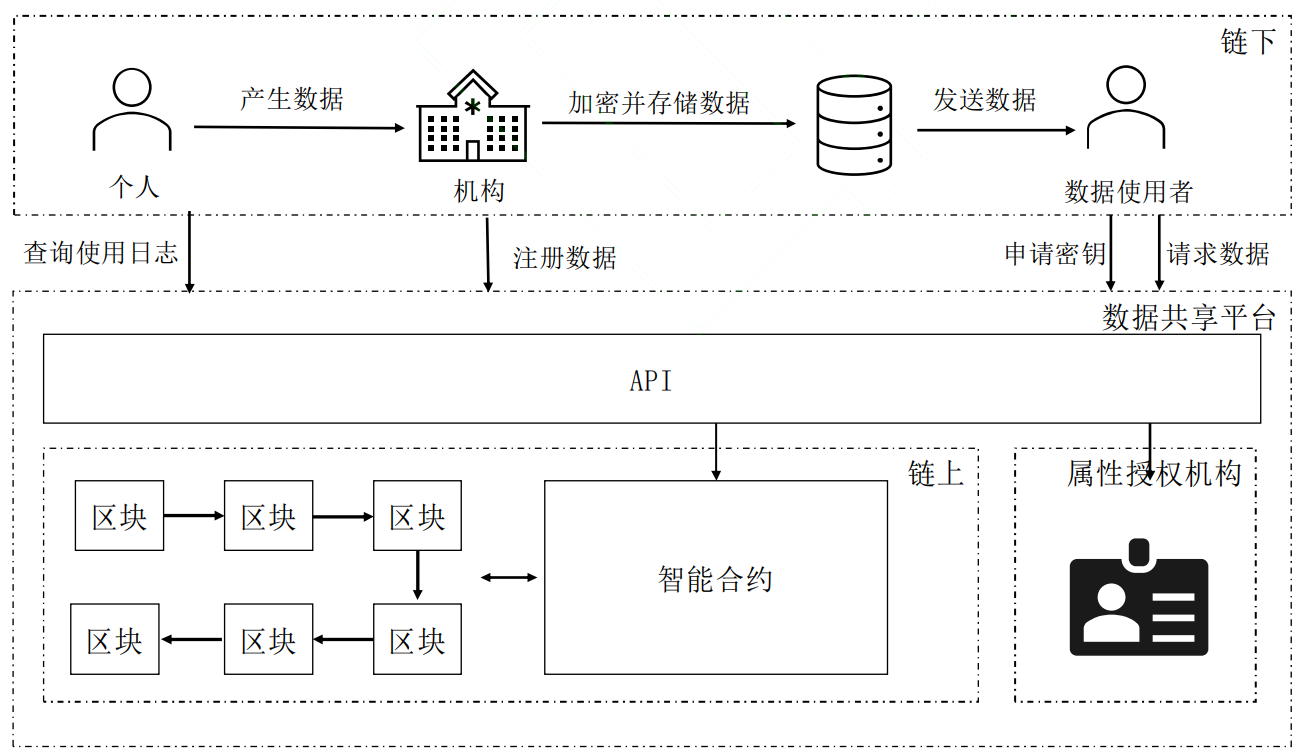
本文设计基于许可区块链的金融数据共享系统架构如图4所示，包括核心层、服务层和应用层。

1. 核心层。核心层负责许可区块链的底层运行，为数据共享服务提供核心支撑。各功能由许可区块链提供，包括智能合约、共识机制、区块同步、账本管理、交易验证和背书策略等模块。
2. 服务层。服务层负责实现数据共享平台的各服务，包括区块链模块和加密模块。区块链模块基于核心层开发的，包括组织管理模块和链码模块。其中，组织管理模块负责管理数据共享的各参与方，并为其创建共享通道，链码模块负责智能合约的创建、部署和执行，是数据共享可信执行的基础保障。加密模块负责实现CP-ABE算法，保证CP-ABE算法在各环节的稳定执行。
3. 应用层。应用层封装数据共享平台提供的各服务，使用户可以通过HTTP接口的方式调用所需要的数据共享服务，为用户使用提供便利。

**图4 数据共享系统架构**

**2、**共享模式

本文使用智能合约制定共享规则，智能合约内容公开透明且不可篡改，在满足对应条件时能够自动执行。同时，借助区块链存储数据共享记录，通过区块链本身的可审计性保障数据共享记录的可信性。但是，区块链存储成本较高，若将大量金融数据存储在区块链，不仅会大幅影响区块链性能，且一旦密钥泄露，数据安全将无法得到保证。因此，本文选择将金融数据存储在各机构的数据库中，在此基础上通过分级访问控制算法实现机构对数据的控制。本文提出的数据共享模型如图5所示，包括个人、机构、数据使用者和共享平台。其中，共享平台为个人、机构和数据使用者提供数据共享服务。



**图5 金融数据共享模型**

1. 产生数据：个人参与日常活动中会产生大量金融数据，如：日常消费、存取款操作、投资行为等。在经过个人同意的前提下，机构将会对这些数据进行采集、清洗和处理。
2. 数据存储：机构根据数据分级标准对数据进行分级，并依据访问控制策略，使用本文CP-ABE算法的加密方法对数据进行加密并存储。
3. 数据注册：机构将数据信息（包括数据描述、加密密钥、机构信息、相关个人、访问控制策略和数据地址等）上传至数据共享平台，并将数据信息存储至区块链上。
4. 密钥申请：使用者可以根据自身属性向数据共享平台申请密钥，属性授权机构验证其身份后，使用CP-ABE算法的密钥生成方法生成对应密钥，并向使用者发送。
5. 数据请求：使用者在共享平台检索数据，向平台发送数据请求，平台收到请求后向使用者返回数据信息。
6. 数据发送：使用者收到数据信息后，根据数据地址获取密文数据，使用创新算法的解密方法解密密文。
7. 使用日志查询：共享参与方可以通过向共享平台发送请求来查询数据使用情况。

3、金融数据多级访问控制算法

(1) 金融数据分级标准

金融数据的组成结构复杂多样，不仅包含用户的身份信息和资产负债数据，也包括征信数据。针对不同来源、不同敏感程度的数据，所应用的访问控制策略也应该不同。因此，为实现金融数据的高灵活性隐私保护，本文按照风险级别和重要程度，将金融数据分为以下三个等级：高敏感、中敏感和低敏感。其中，高敏感数据不参与数据共享活动。不同级别的数据可以执行不同的访问控制策略。具体的金融数据分级标准如下：

1. 高敏感数据：可以标识个人身份的信息或暴露后会给用户造成重大影响的信息，如姓名、电话、身份证号、地址、生物识别（指纹、视网膜、声音等）、照片等。
2. 中敏感数据：不能标识个人身份的信息且模糊化后仍有重要意义的数据，可以保留模糊后的结果，如年龄、地区、征信记录等。
3. 低敏感数据：其他金融数据，如年龄范围、性别、职业、资产负债、消费记录、参保保险等。

同时为实现金融数据的访问控制，需要依据数据使用者身份信息对其进行划分，包括使用者的类型和使用者的专业等级。使用者属性集合如表1所示。

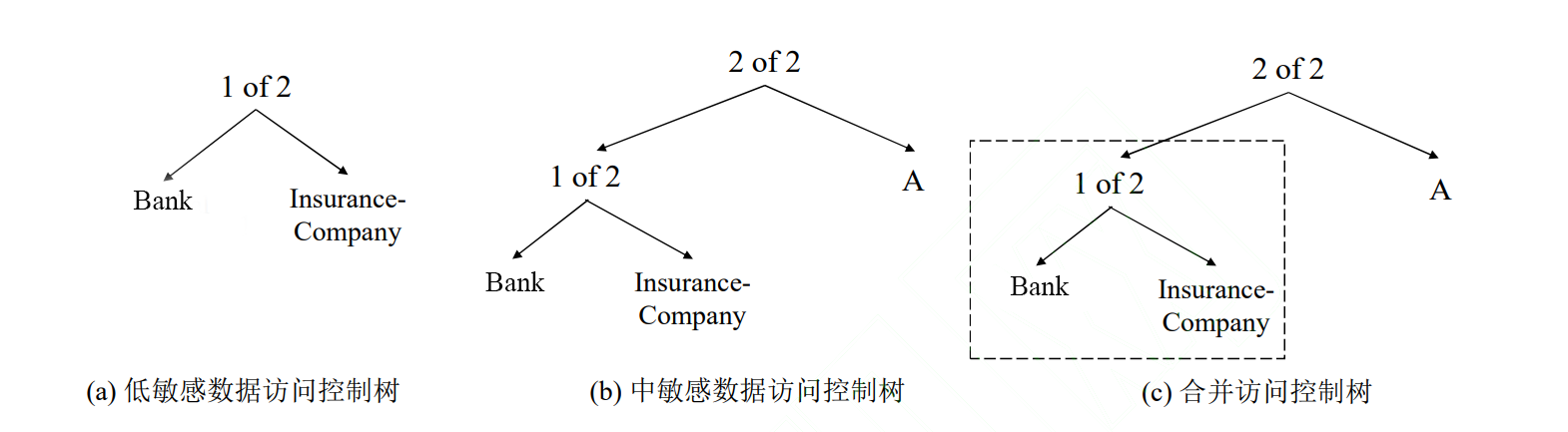
**表1 使用者属性集合**

|  |  |
| --- | --- |
| 属性分类 | 属性值 |
| 使用者类型 | Government Institute, Insurance-Company, Bank, Person |
| 使用者专业等级 | A，B，C |

使用者的类型包括以下四类：政府机构(Government Institute)、保险公司(Insurance Company)、银行(Bank)和个人(Person)，反映使用者的身份类型。使用者的专业等级从高到低分为以下三类：A、B、C，反映使用者的资质信息，不同的使用者类型应用不同的专业等级分类标准，例如：一级银行、二级银行、三级银行对应银行(Bank)使用方的A、B、C三类专业等级。

每个使用者应同时包含使用者类型和使用者专业等级两方面属性，且不得包含多个使用者类型属性或多个使用者专业等级属性，如三级银行使用者属性集合为。使用门限值连接使用者属性集合构成金融数据的访问策略，例如仅允许A级银行或A级保险公司访问的金融数据访问控制策略表示为。

4、创新算法



**图6 访问控制树转换示意图**

传统的分级数据属性加密策略针对中敏感数据和低敏感数据的两种不同的访问策略2t需要使用两次CP-ABE算法，计算繁琐。但在实际应用中，中敏感数据与低敏感数据的访问策略往往存在依赖关系，即中敏感数据的访问策略包含低敏感数据的访问策略要求。例如，低敏感数据访问策略为，即所有银行和保险公司均可访问，如图 6(a)；中敏感数据的访问策略为，即仅 A 类的银行和保险公司可以访问，如图 6(b)。考虑到中敏感数据与低敏感数据访问策略间的依赖关系，本文合并中敏感数据和低敏感数据的访问控制树，合并策略为将低敏感数据的访问控制树整体作为访问控制树根节点的左分支，并将中敏感数据访问控制策略的附加条件作为访问控制树根节点的右分支，根节点使用2of2连接，如图6(c)。访问控制树的叶子节点数量较传统方案相比减少约50%。

**（三）系统安全性分析**

金融数据中往往蕴含着患者大量敏感信息，一旦遭到泄露，将会给用户带来巨大的负面影响。本文提出的金融数据共享系统在数据生命周期的各个环节均能保证数据的安全性，包括数据存储、数据共享、数据访问。与此同时，区块链具有天然的不可篡改和可审计性，当各方针对共享数据的完整性和真实性产生质疑时，区块链中记录的金融数据共享过程可以提供可信的溯源追责。

1) 数据存储，相关机构的数据库中存放的数据为经过对称加密后的数据，即使数据库遭受外部攻击后金融数据被暴露，攻击者也无法从密文中获取任何信息。此外，共享的金融数据不包含高敏感数据，无法直接识别个人。

2) 数据共享，本文提出的金融数据共享系统以区块链为基础，通过共识机制和加密算法来保障数据共享过程的安全性，去中心化的结构避免单点故障风险，为数据共享过程提供安全保障。

3) 数据访问，金融数据通过提出的创新算法实现分级访问控制，安全可靠，可以抵御非法攻击。

1. **总结**

本文结合许可区块链与基于属性的访问控制等技术，提出了一个分级访问控制与共享方案。该方案对金融数据按敏感度进行分级，设计创新算法，在降低计算和存储开销的同时，为金融数据提供更灵活的安全保障。该方案利用许可区块链实现数据共享系统，保证了数据共享过程的可追溯性，实现更可靠的访问控制管理。为了实现稳定、高效的访问控制与共享系统，下一步将多级访问控制算法拓展到通用场景中。

这一方案使得跨机构金融数据共享成为可能，并且对于帮助新市民群体获取更加便利和完善的金融服务有着重要作用，跨区域跨机构的数据共享，使新市民的征信问题不再成为一个难题。从长远来看，对我国普惠金融的发展也有着深远影响。

贾天宇42023024占比0.25，周子博42036065占比0.25，周姝颖42012018占比0.25，张孙楚婷42012207占比0.25