

**计算机类创新创业基础课程论文**

**（2023 /2024 学年 第1学期）**

**论文题目： 当下的区块链技术**

**班 级： 计科221**

**姓 名： 董自经**

**学 号： 19222126**

**联系方式： 1995424141**

**南京农业大学人工智能学院**

**当下的区块链技术**

**摘要：**区块链技术是一种去中心化的分布式账本技术，其核心思想是将数据存储在一个不可篡改的分布式账本中。区块链技术最早被应用在比特币等加密货币中，实现了去中心化的数字货币交易，为金融领域带来了革命性的变革。随着技术的不断发展和创新，区块链技术已经被应用到了更多的领域，包括去中心化金融（DeFi）、数字身份验证、物联网（IoT）、供应链管理等。我将在此文中简述区块链技术在当下的应用、存在的问题以及未来可能的发展情景。

**关键字：**区块链技术，数据加密，数据安全

**一、区块链技术在当下的应用**

**1. 加密货币**

区块链技术最早被应用在比特币等加密货币中，将数字货币交易实现了去中心化。加密之后货币的交易不需要银行或其他中介机构的参与，而是通过区块链网络中的节点完成交易验证和记账。所有用户共用一个“大账本”，每个用户对于自己账户的操作，都会在大账本上留下相应的记录，同时系统向其他用户发送确认请求，若多数用户认可了这一笔账，则系统认可这一笔账。这种去中心化的交易方式，不仅提高了交易效率，也提高了交易的安全性和可信度。迄今为止，除了比特币之外，还有许多其他的加密货币，如天秤币等[1]。

**2. 去中心化金融（Decentralized finance，简写为DeFi）**

DeFi应用是基于区块链技术为用户提供了无需中介的金融服务，包括借贷、交易、稳定币等。DeFi应用的核心思想是将金融服务去中心化，通过智能合约实现自动化的金融服务。DeFi应用的优势在于，用户可以在不需要中介机构的情况下获得金融服务，从而降低了金融服务的成本和门槛。同时，DeFi实现了透明拱性，所有的交易和操作记录都在公开的区块链上，所有的合法用户均可以查看。用户也可以自由地将资产在DeFi与其他存储财产的账户中进行移动和使用，做到了高操作性。目前，DeFi应用已经成为区块链技术的重要应用之一，吸引了越来越多的用户和资本的关注[2]。

**3. 数字身份验证**

传统的身份验证方式依赖于中心化的身份认证机构，容易受到黑客攻击和数据泄露的风险。而区块链技术可以将身份信息存储在分布式账本中，实现去中心化的身份验证，提高了身份信息的安全性和可信度。用户身份与区块链相结合形成的链为身份链，身份链上层会应用到子链身份。身份链可以对子链身份和用户身份进行管理。应用子链如果要对其他平行的子链进行操作，就要在身份链上先注册身份，这个身份相当于子链的识别码，有了这个子链才能被其他的链所认可，并相互进行操作。直至目前，已经有一些区块链项目在数字身份验证领域有所突破，如Ethereum、Civic等[3]。

**4. 供应链管理**

区块链技术可以用于建立透明、可追溯的供应链管理系统，可以解决现有供应链融资中存在的部分问题，帮助企业提高供应链的效率和可信度。传统模式往往是用纸张记录，稍微先进的用计算机记录，但可能同时存在多个数据库，会导致数据的重复、延误等问题，增大了供应管理的难度。而区块链技术可以将供应链信息存储在分布式账本中，使得供应商都可以通过系统查看商品数据，进一步实现供应链信息的透明、可追溯，简化了记录和纸质单据的传递，提高了供应链的效率和可信度。目前，已经有一些区块链项目在供应链管理领域有所突破，如Waltonchain、Ambrosus等[4]。

**二、区块链技术存在的问题**

**1. 扩容问题**

目前大部分公有链的交易速度和吞吐量有限，难以应对大规模的交易需求。比特币网络每秒只能处理7笔交易，以太坊网络每秒只能处理15笔交易。这种交易速度和吞吐量的限制，限制了区块链技术在大规模应用中的发展。为了解决存储有限的问题，科学家提出了出了一种针对HyperLedge Fabric的环重叠存储扩展机制。该机制将所有账本节点划分为包括多个节点的簇，整个区块链数据的一部分存储在相应的簇中，许多数据块重叠存放在一起，部分解决存储不足的问题[5]。

**2. 隐私保护**

为了保持对用户的透明性，区块链上的交易记录是对所有用户公开的，难以保护用户的隐私信息。在传统的金融交易中，用户的交易信息是由银行和其他中介机构保护的，而在区块链上，用户的交易信息是公开的，容易被黑客攻击和数据泄露。而且，区块链技术采取的是“少数服从多数”的算法，在某些区块链中，如果黑客拥有超出系统网络算力的设备，就可以发动51%攻击，，从而获取到用户的隐私信息或者篡改交易记录，甚至肆意更改系统账本中的数据[6]。

**3. 安全性**

区块链系统的安全性依赖于密码学算法和共识机制，存在潜在的攻击和漏洞。区块链技术会有一个智能合约，这个合约中的漏洞可能导致资金丢失或者合约执行不符合预期导致资金被盗窃[7]。此外，如果黑客暴力破解得到用户的私钥，用户的信息包括财产的安全都会受到威胁。而且区块链技术中是所有人参与数据的决定，缺乏一定程度的监管，一些非法的行为如洗钱也可以在里面找到可乘之机[8]。区块链中的区块链系统的安全性是区块链技术能否得到广泛应用的关键因素，如果安全性无法得到保障，将会严重影响区块链技术的发展。

**三、未来可能的发展情景**

**1. 扩容技术的发展**

现有的环重叠存储机制难以充分解决区块链存储较小的问题，随着区块链技术的不断发展，将会出现更多的扩容技术，提高公有链的交易速度和吞吐量。例如闪电网络、Plasma、Sharding等技术都可以提高公有链的交易速度和吞吐量[5]。

**2. 隐私保护技术的创新**

未来将会出现更多的隐私保护技术，如零知识证明、同态加密等，保护用户的隐私信息。这些技术可以将用户的交易信息加密，保护用户的隐私信息[6]。

**3. 多链互联**

未来可能会出现多条区块链之间的互联互通技术，实现不同区块链之间的价值传递和数据交换。这种多链互联的技术可以打破不同区块链之间的孤岛，提高区块链系统的互通性和可用性。

**4. 区块链与物联网、供应链管理的深度融合**

未来，区块链技术将与物联网、供应链管理等领域深度融合，实现更多的创新应用。例如，通过区块链技术可以实现物联网设备之间的安全数据交换和价值传递，提高供应链管理的透明度和效率。

区块链技术在未来的发展中将面临诸多挑战和机遇，但随着技术的不断创新和完善，区块链技术也会愈发先进，相信在不久的未来，区块链技术将会在各个领域发挥越来越重要的作用。

参考文献：

[1]郭亚宁,尹亚丽.比特币、天秤币两种加密货币解析[J].数字技术与应用,2021,39(06):186-188.DOI:10.19695/j.cnki.cn12-1369.2021.06.59.

[2]郑妍妍.区块链技术在金融理财中的应用研究[J].产业科技创新,2023,5(04):80-82.

[3]汪宁,白伊瑞,朱芸芸等.一种面向电子证据服务体系的区块链可信数字身份认证平台设计[J].警察技术,2023(05):33-37.

[4]王道平,朱梦影,董汉玺.资金约束下基于区块链技术的供应链运营决策研究[J/OL].中国管理科学:1-13[2023-11-17].https://doi.org/10.16381/j.cnki.issn1003-207x.2023.0216.

[5]刘文选. 区块链存储扩展机制研究[D].烟台大学,2023.DOI:10.27437/d.cnki.gytdu.2023.000288.

[6]李云辉,陈家辉.基于区块链的感知数据交易隐私保护方案[J/OL].大数据:1-19[2023-11-17].http://kns.cnki.net/kcms/detail/10.1321.G2.20231012.1134.004.html.

[7]李井涵,沈国华,杨阳等.结合区块链的物联网数据安全共享机制[J].小型微型计算机系统,2023,44(08):1812-1818.DOI:10.20009/j.cnki.21-1106/TP.2021-0982.

[8]刘文娟.基于区块链技术的档案信息化与数据安全管理[J].兰台内外,2023(24):14-15+21.