**上海大学“区块链”课程论文考试**

德勤**Rubix项目分析**

姓名：孙姝 学号： **21726076**

字数：3744

摘 要：

随着比特币等数字货币热潮的涌现，支撑其的底层技术——区块链也被越来越多的人所知晓。当今信用机制的弊端显露、危机四伏，而以区块链为基础的分布式加密账本正是解决了信用缺失的难题，对当下的行业生态和运作模式产生重大影响。本文在介绍区块链技术原理和德勤 Rubix 平台的基础上，结合企业经济业务活动，将其新模式的会计应用场景与传统会计模式相对比，模拟会计信息的产生、存储、传输、处理中的循环过程，通过对比经济业务会计处理的前后差异，论证区块链技术在实际应用中对会计工作的影响，并从跨境支付、会计记账、数据存储和业务审计等多个方面对影响进行了深入探讨。

关键字：区块链，财务系统，会计业务，发展策略

论文评语：

成绩： 任课教师：吴建刚

1. 经济模型分析
   1. 项目、创始人及团队简介

德勤在2014年创建了自己的区块链团队Rubix，并通过Rubix平台创建了一个世界范围的分布式账本——Deloitte’s Perma Rec，该账本可以实现与企业的SAP、Oracle等财务系统的无缝对接，增强企业经济活动的透明度；同时，通过对账本数据的全面覆盖，可以实现实时监控、自动化报税、实时审计等，极大地提升了数据使用方和监管方的工作成果。Rubix 当前的业务模块主要有四类，如交易对手确认、实时会计和审计、土地登记、忠诚度积分等。德勤通过 Rubix 项目已经在众多领域初步实施了企业级区块链项目，主要有去中心化交易所、即时支付、医疗信息数据库建设等。目前，Rubix 平台成功的应用案例是 Deloitte’s Perma Rec——一个世界性的分布式账本。这个账本可以对接不同公司的财务管理系统，增加经济业务的透明度，明显地降低了审计和税务申报的成本。未来显而易见，区块链技术会在会计行业逐步实践探索、推广应用，而财务会计的工作模式也会因此得到改变，社会甚至可能不再需要向记账公司、会计师事务所等中介机构的存在，企业自身就可以通过区块链财务系统完成这些工作：采集会计数据、确认计量会计信息、存储财务资料、生成财务报告、自动申报纳税和审计监管等。现在，Rubix平台已经为多家公司所认同，并且在Rubix平台上建立自己的区块链应用。

* 1. 项目想要实现什么

随着企业模式的发展，会计人员正在经历由财务会计到管理会计的转型，关注会计信息的失真问题不仅是一名会计的任务，更一名管理者的工作，会计信息造假也是会计行业应该从根本上解决的问题。区块链技术由于其去中心化、去信任的独特优势而备受关注，四大会计师事务所也纷纷建立自己的研发团队来提前布局，研究区块链技术的企业应用、建设技术开发平台架构、推动区块链技术的推广应用。通过区块链技术的应用，企业可以建立一个可信度极高的会计信息保障机制，确保会计信息的真实性和可靠性，从而有效地减少会计工作的造假行为。

* 1. 为什么需要分布式记账

作为独特的分布式账本技术，区块链自身的结构就可以实现透明、共享、不可篡改等功能，与会计记账和审计具有天然的契合性，可以预知的是区块链将会是存储数据、共享信息的最佳方式。随着技术的探讨和应用，区块链在会计行业的变革作用正在一步步显现，区块链技术将会改变会计核算和计量模式、简化记账流程、完善数据结构、降低财务运作成本、降低财务风险、重塑会计审计生态。区块链对会计行业最大的贡献是解决成本和效率问题，在未来的会计业务中，很多工作都可以交给基于区块链的智能合约来完成。经过大量的研究分析，国内外相关学者都比较认同区块链技术的巨大优势，区块链技术可能是未来对会计影响最大的互联网科技。例如：Lazanis（2015）分析了区块链网络上的点对点交易、自动结算和更新账本，认为企业的资金支付可以通过区块链网络来进行，从而跨过结算中介来降低佣金费用。如果使用区块链网络自身的数字货币进行点对点的支付，降低中间成本费用的效果更为明显，可以极大地简化交易流程、降低财务的运作成本。孙玥璠（2017）在私有区块链上模拟建立了一个透明的分布式财务系统，这样的财务系统使用者可以是一个公司，也可以是一家集团企业。每一个记录节点都保存了一份完整的且不可篡改的账本，这样任一节点都可以随时查询全部数据；同时，由密码加密技术对对访入者进行限制，外部人员只有经过允许才能访问，保证了财务数据的私密性。因此，区块链财务系统在安全可靠地存储财务数据的同时，也确保了会计信息的准确性和透明度。

* 1. 代币机制

在此项目中引入了通证经济学的经济概念，在区块链网络经济中，通证经常表现为数字代币，被作为一种激励性的经济工具，推动区块链生态圈里各个角色的协同运作。通证就像目前的“打白条”，是一种“资产数字化”，个人凭借其信用背书将资产赋予权益性证明，在通证网络中流通起来。旨在鼓励大家把自己的所有权益都进行“通证化”，包括但不限于工资、存款、不动产、股票、合同、期权、证书等内容，只要市场能够赋予认可的价值，都可以在通证网络上进行通证化流通交易，并且可以在现实生活中进行兑现和消费。

1. 技术模型分析
   1. 共识机制

该机制是区块链社区各参与方统一认同的共识算法。由于在点对点网络机制下很容易存在较高的网络延迟，各个节点收到的交易数据时间可能并不相同，因此，区块链节点社区需要一个共识机制对同一时间的不同节点接受时间进行统一，最先由同一算法记录交易信息的节点获得记账员，得到记账奖励。

* 1. 帐户机制及智能合约

独特的记账模式是区块链技术迅速火热的主要原因，区块链网络内带有公开透明的分布式账本，与传统会计的中心化记账模式恰恰相反。通过与智能合约相结合，区块链技术能够弥补很多传统记账模式的不足。在德勤的 Rubix 平台上，区块链的应用管理可以归为三类：一是基础的信息存储，即用户可以在区块链网络上建立数据库，作为一种留存证明；二是较复杂的认证应用，用区块链网络来处理复杂的逻辑数据，三是交易型应用，如通过区块链网络进行不同币种之间的自由兑换。

* 1. 数据库、隐私保护、身份验证等

在 Rubix 平台上，平台可以进行访问的限制。只有拥有通证的人才能查看账本、发起交易、记录数据等。例如，甲企业与乙企业之间的业务往来会有合同或票据等信息。在交易发起的同时，网络会分别链接到甲乙企业和银行，确认双方信息的真实性，这个过程复核了贸易流程。在新的交易信息被成功写入区块链中后，网络会再次进行广播通知，其他节点则对自己的账本进行及时更新，这个过程是会留下固定的时间戳，不能再被更改。通过这样的模式，Rubix 平台上的财务数据库可以完美的重现公司业务，具有更有意义的价值存在。此外，Rubix 以基于区块链的数据库来存储管理历史数据，可以保证财务数据的安全存储、有序分类、合理披露，以保证数据的安全性。同时，Rubix 即时保存交易过程中产生的文件资料，不再需要纸质的归集。数据库的即时建立更有利于使用信息的索引、传输、共享等需求，为企业财务工作的开展提供强有力的支持。在披露程度上，区块链系统也有很大的进步。传统互联网数据的披露都趋于碎片化、低级化；在 Rubix 平台上，用户可以访问完整的分布式账本，不再有信息的不对称性。由于每个客户的访问权限不同，所以也不用担心重要财务数据的泄露。“一个钥匙只能开一把锁”，用户无法查询超过自身权限的信息。

* 1. 现有技术文档及代码评价

作为一个财务数据系统，Rubix 平台的区块链网络是极其安全的。首先加密技术的安全性可以保证数据库不被黑客轻易地攻击破解。即时在最严重的情况下，部分节点被破坏，但其他节点任然保存有完整的账本数据，不用担心数据丢失的问题。另外，Rubix 平台的数据写入机制具有极大的安全性。分布式的审核机制避免了虚假信息的录入，共识机制也让私自更改账目没有任何意义。

1. 项目未来
   1. 未来规划及激励机制

通过将区块链技术的概念和基本原理融入到德勤区块链平台 Rubix的具体应用场景中，我们分析了区块链技术对会计业务的处理方法和工作流程的影响。未来区块链技术对会计业务的改进内容可以归纳为以下几个方面：

一是可以简化会计处理程序，通过使用区块链技术改进业务流程，从源头减少了会计核算工作量，实现了会计数据从获取核算到平账报告的自动实现。

二是逾越成本效益原则的门槛，提高会计信息的准确性。

三是可以促进会计核算的标准化、规范化和会计信息的可比化、公允化。

四是区块链可保存会计报告的过程记录和操作痕迹，其不可更改性和时间戳功能为监管、自审计、实时审计等提供便利，健全了企业的外部监管环境，完善了监管手段，提高了监管效率。

* 1. 现有社区及应用评价

区块链技术的应用研究未来还有很长的路要走， 虽然区块链财务系统具有诸多优势，但是由于区块链技术正处于发展的起步阶段，研究时间较短，属于“摸着石头过河”的探索期，还有许多尚未确定的问题和不足。

例如：首先，目前的区块链基础设施架构不足以支撑大规模的商业化应用，区块链网络的分布式存在是建立在庞大数量的节点基础上的，只有大规模的统一应用才能最大化地发挥区块链技术的优势。

其次，区块链系统完全透明去中心化的模式与传统商业模式相悖。当前的会计资料还是以企业私有为主，去中心化的模式虽然让企业信息更加透明可靠，但是也无形中侵犯企业的商业隐私，必然面临着一定的利益冲突。

最后，当前与区块链会计相关的法律及行业规则有明显的空白需要完善。在区区数年里，区块链技术从技术员的小圈子产品变成各国政府和企业的关注重点，成长发展日新月异，当前的法律法规也应当顺应社会，及时更新完善，为新事物的健康成长提供更加积极广阔的发展空间。

总体来讲，随着金融科技的发展，企业需要对区块链技术给予足够的重视，密切关注和实时跟踪区块链技术在会计领域的进展，不定期评估区块链技术对自身业务流程和模式的影响，及时采取合适的战略和战术措施，以激发企业活力，获得企业的长远发展。

* 1. 项目投资分析

信息技术的进步是推动社会发展的重要力量，技术的革新不断地为企业创新发展提供强大的生命力。作为新一代互联网的基本协议之一，区块链技术对未来社会发展的影响已经初现端倪。区块链技术独有去中心化、不可篡改等优越特点，在区块链技术的基础上创建一个去中心化、去信任化的数据库，可以很好地降低中心化机构和第三方信任背书对经济业务发展的影响。在会计工作中应用区块链技术，可以实现简化记账、自动化审计、降低财务运作成本、防范财务风险等。现在，Rubix 平台已经为多家公司所认同，并且在 Rubix 平台上建立自己的区块链应用，呈现积极向好的态势。

附1：

1、请说明发起比特币交易到交易确认的整个过程。（说明中请包含：交易者如何产生地址、如何对交易签名、如何发出交易、矿工如何接受交易、如何选出记帐人、为何会使用矿池挖矿、矿池挖矿的过程、为何可能会有软分叉、为何限制区块大小、如何控制区块出块时间、区块中包含的内容，并讨论为什么使用UTXO设计）

答：交易者如何产生地址➡️比特币地址可由加密技术，私钥生成算法获得，或者是公钥经过单向的加密散列算法得到。加密技术中散列函数在比特币中被广泛使用,作为比特币地址、比特币地址脚本地址以及挖矿中的工作量证明算法。

如何对交易签名➡️通过签名生成算法，这一算法把私钥和一段消息作为输入，生成一个签名。实践中被签名的消息实际上常常是这段消息的哈希值，这样就可以对标准长度的哈希签名，由于哈希的防碰撞性，从而可以实现对任意长度的消息签名。

如何发出交易➡️比特币交易是通过脚本实现的，每笔交易的基本信息包括哈希值、输入地址、输出地址、交易信息大小、交易总价值，一个区块一般有几百笔到几千笔交易，一般交易都有若干输入地址和若干输出地址。

矿工如何接受交易➡️网络上的矿工从这些池中选择交易并将其形成“块”。除了一些元数据之外，块基本上是交易的集合。每个矿工都构建他们自己的区块，但是多个矿工可以选择要包含在他们区块中的相同交易。通过选择交易并将其添加到其区块，矿工创建一个交易块。矿工将此交易块添加到区块链该块首先需要签名，此签名是通过解决每个交易块所特有的非常复杂的数学问题来创建的。

如何选出记帐人➡️寻找符合条件的哈希值（最快的机器成为记账人，难度根据算力调整）

为何会使用矿池挖矿➡️当矿工越来越多算力越来越大的时候，单个设备挖矿是很难得到区块奖励的,于是便有人开发出可以通过协议将算力集中在一起的挖矿网站这个便是矿池,矿池把计算工作分配给到矿工，矿工则把自己的矿机里面的算力给到矿池经过算力组团之后,矿池里面的算力规模很大所以挖到币的概率也就大大提升,产量也得到了保障，矿工因此也得到了稳定的收入。

矿池挖矿的过程➡️首先是通过局域网内的其他电脑访问矿机后台,配置挖掘信息(包括要连接的挖掘服务平台-矿池,以及你在矿池)中的账号信息;然后是矿机自己的事情。它开始请求矿池通过网络进行通信。收到请求后,矿池向矿机发出了采矿任务。矿机收到采矿任务后,采矿任务由其采矿软件解决。解决后,矿机将计算结果提交给矿池,矿池通过验证后,计算出矿机的矿业收入。

为何可能会有软分叉➡️任何系统都存在“升级”，区块链也一样，因为没有中心化机构，比特币等数字资产的每次代码升级都需要获得社区的一致认可，所以分叉产生的原因可以简单理解是区块链系统升级造成的，分叉又分为软分叉和硬分叉。软分叉是指在区块链或去中心化网络中向前兼容的分叉。向前兼容意味着，当新共识规则发布后，在去中心化架构中节点不一定要升级到新的共识规则，因为软分叉的新规则仍旧符合老的规则，所以未升级的节点仍旧能接受新的规则。

为何限制区块大小➡️如果比特币的区块过小，比特币网络所能处理的交易数就会受到限制。区块链缺乏足够的空间并且也降低了比特币的竞争力；而如果比特币的区块过大，运营比特币节点的成本大大增加同时挖矿变得中心化，较低的挖矿补贴可能会影响网络的安全性。

如何控制区块出块时间➡️根据过去一段时间（或者一段区块链条）的产出区块的速度来调整目标值，或者叫调整难度：之前产出太快，就调高难度，调小目标值；之前产出太慢，就调低难度，调大目标值。

区块中包含的内容，并讨论为什么使用UTXO设计➡️一个区块包含了一个哈希值，一个计算值，然后就是一系列的交易信息。同时，还包含了区块打包时的时间戳信息。UTXO似乎天然就是为数字货币设计的，UTXO的复式记账模式为Token资产提供了货币级别的安全程度，其长达十年的稳定运行与实践测试，证明了其在安全性上的毋庸置疑。基于这一层原因，一些定位于数字货币以及服务于金融场景的区块链项目，更偏爱于UTXO。除安全性之外，UTXO还具有充分的隐私性和可拓展性。

致力于实现智能数据资产的互联基础区块链生态系统WDC智慧链，承载着金融价值和流通金融价值，所以也选择采用UTXO这种最成熟也最简单高效的账本模型。

2、请说明如果签名正确、余额足够的情况下，发出的交易迟迟没能出块，应该是什么原因，应该采取什么措施，分别说明不同措施的后果。

答：原因：平台的迅猛增长与其接受程度和比特币交易的增长速度并不相匹配。同时，还存在一些策略性原因即这一系统中的很多参与者将成千上万的交易发送给其自己，以便扩大其在区块链容量争论中的优势，这也导致了比特币交易的延迟。

措施：用户可以提高其费用或参与可以称之为“往返交易”的活动。

结果：会加快交易确认的速度。

措施：从使用动态费用模式的比特币钱包中发送交易。 如果某笔交易的优先级较高，那么就可能希望手动设置费用，以确保矿工在下一个区块中接收交易。 最终，这一切都归结于每笔比特币交易的satoshi / byte费率比。

结果：比特币用户可以获得更快的交易确认速度，可以促进矿工将某项交易纳入即将产生的区块中。

3、请说明以太坊项目的目标，它与比特币不同的技术设计及其原因。

答：目标：以太坊致力于实施全球去中心化且无所有权的的数字技术计算机来执行点对点合约。简单来说就是，以太坊是一个无法关闭的世界计算机。

不同之处：以太坊是吸纳了基于solidity语言的智能合约，并将智能合约看做一种特殊的账户，从而使得在智能合约上也可以实现具体的方法；实现了智能合约能落地执行的EVM（以太坊虚拟机），通过以太坊虚拟机，从而将solidity这样的类JS的代码变成了可以在区块链是执行的加密代码；不同于比特币技术，在以太坊transation都需要gas,一份合约或者一次交易的gas是固定的，而gas的价格则有以太坊中的oracle来决定；以太坊同时还构建了较完整的，开源的生态系统，不仅有底层的geth,编程的solidity,合约在线浏览器browser-solidity,合约钱包Mist/wallet,以太坊的前端开发框架Truffle,各种各样的开源DApp。

原因：比特币标志着一种全新的数字货币形式的出现，这种货币在任何政府或公司的控制范围之外运作。随着时间的推移，人们开始意识到比特币的潜在创新之一，区块链，可以用于其他目的。

以太坊建议利用区块链技术，不仅用于维护分散的支付网络，还用于存储可用于为防篡改的分散式金融合约和应用程序提供动力的计算机代码；以太坊应用程序和合约由以太坊网络的货币以太币提供支持；以太币旨在补充而不是与比特币竞争，但它仍然成为加密货币交易所的竞争对手。

| **平台** | **共识机制** | **状态** | **合约模式** | **交易** |
| --- | --- | --- | --- | --- |
| **比特币** | 工作量证明 | 未花输出 | 纯函数 | 支付 |
| **以太坊** | 工作量/权益 | 账户 | 图灵完备 | 智能合约 |

4、请说明以太坊智能合约的运行原理以及合约的整个生命周期。

4、请说明以太坊智能合约的运行原理以及合约的整个生命周期。

答：智能合约是一种特殊协议，旨在提供、验证及执行合约。具体来说，智能合约是区块链被称之为“去中心化”的重要原因，它允许我们在不需要第三方的情况下，执行可追溯、不可逆转和安全的交易。在以太坊，记录在区块链账本中的不仅仅是账户余额，还有函数调用后变量的新状态。在以太坊的区块中，记录的除了转账信息以外，还有可执行的代码。以太坊的每个节点都会运行虚拟机，它不仅能够执行代码，还可以读写区块中可执行的代码和数据，校验数据签名等等。如果把比特币比喻成功能手机，以太坊就像是智能手机。在以太坊中，有两种账户，一种叫外部账户，是人操作的正常账户，地址即公钥，由私钥控制；一种叫合约账户，地址随机产生，有点像游戏中的NPC。

整个生命周期：合约存储➡️合约创建➡️合约部署➡️合约执行➡️合约升级➡️合约销毁。

合约存储：首先，以太坊智能合约有两种类型的账户：外部个人账户和合约账户。这两种类型账户的功能和特点都不一样。

其次，合约在部署时, 就会创建一个合约账户, 合约代码的可执行字节码保存在合约账户中。再次, 数据主要存储在账户 storageRoot 指向的存储区域；storageRoot 对应合约存储结构的MPT树根节点hash值，通过它能够在数据库中检索到合约的变量信息。最后, 所有的基础存储目前都基于 leveldb, 一种 kv 数据库。

合约创建：用户 A 使用 solidity 等语言创建一份合约代码，A 在 IDE/钱包/其他客户端，按一定的格式填写 data，然后确认客户端会填补 account nonce(tx计数器)、compile solidity、签名等操作并将 to 字段置零。该 tx 广播到网络上，B 节点收到该 tx，B 节点检查 tx 是否有效、格式是否正确，验证交易签名是否合法。如果符合要求，计算可能的最大交易费用，确定发送者的地址，并在本地的区块链上查看发送者的余额，如果账户余额不足以支付最大的交易费用，则返回错误，对于符合要求的交易请求，B 将其放在交易存储池中，并向其他节点转发（比如转发给了C）。C 收到交易请求的节点重复用户 B 的处理过程。

合约部署：我们加入矿工B和C，B 和 C 各自从本地的交易存储池中拿到一批 TX，然后打包进行 hash 计算（挖矿）。假设 B 挖矿成功，B 会根据 A 提供的交易费用和合约代码，创建合约账户，并在账户空间中部署合约。合约账户地址在创建合约的 tx 确认后返回给 A，B 打包好的区块发送至对等节点，并在全网传播，C 接收到该区块，验证区块。

合约执行：用户 A 按照一定格式在网络中发起一个 tx 请求；该请求被网络中节点 B 收到，如果符合要求，计算可能的最大交易费用，确定发送方的地址，并在本地的区块链上从发送方账户中减去相应费用； 如果账户余额不足，则返回错误，这条交易被直接丢弃。B 同步到此交易，检查交易是否有效、格式是否正确。符合要求的交易请求，用户 B 将其放在交易存储池中，并向其他节点转发. 其他节点执行和B同样的操作过程，接下来即B 挖矿成功、C 节点收到该区块以及网络上其他矿工节点重复 C 的执行过程。

合约升级：部署在以太坊区块链上的代码是不可改变的，即无法重新部署一个新的合约到相同的地址上。智能合约升级较为困难，务必需要一次性将合约写的完美。

合约销毁：合约发起者可以调用 selfdestruct方法即可销毁合约。

一、评估要求

1、按时交稿、内容要求完整（即按本提纲内容进行）；20%

2、格式是否正确及语言是否规范（补充一下，图表都要编号和命名，如：“图1 关于什么的图”、“表3 关于什么的表”等，表命名在表上方，图的命名放图下面）；10%

3、内容是否充实（总的要求3000字-5000字左右，每一部分分析是否充实，加入了自己的分析和思考，数据和图表精确引用，如果拷贝太多则是负面评价）；30%

4、逻辑及分析是否正确（每一部分分析是否合理并准确）；20%

5、是否有新意（是否有独特的视角或超过课堂讲的内容的自学的东西的突破）；20%

二、文献要求

请在文章中用作者加年代的方式表示参考文献，比如：张某某（2009）提出什么什么。双比如，某理论（张某某，2009）提出什么什么。

请将文章中参考的文献用脚注标出。

参考文献的格式请百度“参考文献”。

1. “附1”要求

附1占整个论文30%的分数，请根据课程内容、根据自己查找的资料进行回答，回答要简洁，不要有废话和无关的话，尽量采用罗列的方式。