|  |
| --- |
| **诚信保证**  **本人知晓我院考场规则和违纪处分条例的有关规定，保证遵守考场规则，诚实做人． 本人签字：** |

**西安明德理工学院大作业答题纸**

2022－ 2023 学年第 一 学期

开课单位 信息工程学院 课 程 物联网导论 学 时 32 考核形式 大作业

|  |  |  |
| --- | --- | --- |
| 题 号 | 一 | 总 分 |
| 得 分 |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 | 101011901 | 学 号 | 191027 | 姓 名 | 杨乃宸 | 序 号 | 25 |
| **一、根据你学到的物联网概念与关键技术，参考物联网典型应用案例分析，结合自己的认识和体验 ，选取一个你所感兴趣的课题，写一篇小论文（至少1500字），包含以下几方面：** 基于普及百姓的区块链IOT隐私权限科技研究系统功能 关于区块链据实际产品调研和科研成果显示，区块链主要是想在开放的网络之下加强人们之间的信任，这些数据在经过准许的情况还可以投入到AI的训练之中。  多方组织的联盟节点会指定共同执行的准入限制合约以制约节点的行为操作权限，入链需要授权认证的许可。保持身份的单一和多样，私有链由一定数量的参与方管理数据的追溯相关高性能执行。因为区块链中数据打表会被公开并且这些公共部分是写死的技术规则，由于这种操作系统的构架功能创建新成员节点需要获取授权设置认证，底层权限访问被分配变得井然有序。就像一名无私的史家，可以检索查询非常详至的明细,维护活动记录的一致稳定。由于高度信任和技术城墙的高度壁垒，具体交易由双方随意自由协定即可。可以运作交易所持规律来预运载基于交易模型的一次性启用不得在本地超过交易所需，表单构建的存储数位对应关系，区块链实际运用发起由一方生成数据的收集需要多方统一输入交易IP的签名  **系统设计特点与创新点**  此系统的主要特点为网络IP的妥善加密、交易记录的合理存储,地址信道的极速强通用.中心化混币服务提供商帮助希望进行混币交易的用户找到同伴, 构造混币交易, 并从中收取一定额度的手续费.中心化混币技术中, 混币服务提供商作为中介角色分别与各用户进行交易, 接收到用户的资产后, 进行随机混淆, 然后返回给其他用户.通过将不同用户的资产互相交换, 达到混淆不同用户地址的效果, 因而分析攻击只能将所有参与混币服务的地址聚类到一起, 难以分辨出属于单一用户的账户地址.  多方混币技术主要模型为n个参与方约定相等的混币金额, 构建n-to-n的多签名交易, 保证每个交易输出都为相等的金额, 外部攻击者无法通过分析该交易分辨不同的输出, 从而无法分析每个输出与输入地址之间的关联关系, 保障外部隐私性. 研究意义与应用前景 用户隐私决定了用户是否会去最大程度的将信任传递给科技，只有一般用户的普遍使用再能加大技术的开发，才是最好的充分体现其实用价值。想要区块链技术变得广泛使用则需要更多有意识的联盟提供稳定的基本用户群体，这样开发者有精力加入算法研究，用户的反馈也能给科技企业带来研发所需的资源。技术成熟意味着未来更多地使用，当人们意识到总有一天都要使用自然而然会加入其中。应该对区块链技术进行一定程度上的宣传，更实际便捷的体验隐私防护，P2P网络降低使用门槛直接帮助人们零成本学习，让人们感受到网络权限管控的必要性带来眼前最真实的快乐。用着安心就能坚持使用下去。而在这其中，共识算法的数据贯穿流动性也让隐私威胁一再成为反复需要强化非对称加密体系安全性的重要方向。需要抵制数据解码时对网络进行跟踪攻击的手段，攻击者会通过较为非透明化的网址下试图侵入联盟。智能服务器需要搭载较强的排查响应能力，抬高了大厂开源的成本。这说明共享保护机制的协议版本需要机构不断发布完善，打造更加全面的分布式区块链。实际运用中，我们应该更重视虚拟占用技术的活用，科技稳定阶段后隐私保护更多的是借助不联网的本地算数模型的性能强化拓展和系统底层原理的简易化。发起者和接收者隐私协商和数据的关联管理尤为信任关键。区块链在去中心化的虚拟商务的背景下诞生，区块链最大范围的使用在密码货币圈层，打表主要建立的是记录交易事务数据的模型。希望未来能够投入更加广泛的使用场景让大家一起体验科技。  部分隐私保护方案会带来一定的资产安全风险, 例如中心化混币技术由于输入输出阶段存在先后顺序, 服务提供商可以盗窃用户资产, 可以采用双方混币技术中的锁定合约保障资产安全性.此外, 信息隐藏机制中的密码累加器与zk-SNARK等实现技术需要可信第三方生成私密参数, 而私密参数会影响系统安全性.采用zk- STARK技术可以做到透明初始化, 但生成的证明需要更大的存储空间.网络数据隐藏中直接结合混淆网络技术也存在一些安全风险, 需要更好地与现有区块链网络结合.  随着区块链技术广泛地应用到金融、安全等各领域中, 区块链系统的隐私保护变得更加重要.针对区块链隐私的攻击与保护将会成为一个研究热点. | | | | | | | |

|  |  |
| --- | --- |
|  | |
|  | |
|  |