****

**本科生毕业论文（设计）**

|  |  |
| --- | --- |
| 题目： | 基于TEE和区块链的 |
|  | 隐私保护计算平台 |

|  |  |
| --- | --- |
| 姓名 | 王明业 |
| 学号 | 17343107 |
| 院系 | 计算机学院 |
| 专业 | 软件工程 |
| 指导教师 | 郑子彬 教授 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2021 | 年 | 4 | 月 | 10 | 日 |

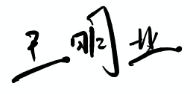
|  |
| --- |
| 基于TEE和区块链的隐私保护计算平台 |
| A Privacy-Preserving Computing Platform based on TEE and Blockchain |

|  |  |
| --- | --- |
| 姓名 | 王明业 |
| 学号 | 17343107 |
| 院系 | 计算机学院 |
| 专业 | 软件工程 |
| 指导教师 | 郑子彬 教授 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2021 | 年 | 4 | 月 | 10 | 日 |

**学术诚信声明**

本人郑重声明：所呈交的毕业论文（设计），是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文（设计）不包含任何其他个人或集体已经发表或撰写过的作品成果。对本论文（设计）的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本论文（设计）的知识产权归属于培养单位。本人完全意识到本声明的法律结果由本人承担。

作者签名：

日 期： 2021年 4月 10日

摘要

TEE（Trusted Execution Environment）即可信执行环境，它保证加载到其中的代码和数据在保密性和完整性方面受到保护[1]。区块链本质是一个数据结构，储存于区块链中的信息具有不可伪造、可追溯和公开透明的特征[2][3]。本文给出一种计算平台的设计，该平台使用当下流行的加密方法如RSA[4]、AES[5]，并结合TEE和区块链技术，可以全程保护用户的隐私。

**关键词**：TEE、可信执行环境、区块链、隐私保护、服务计算、计算平台、代码运行平台

Abstract

TEE (Trusted Execution Environment) guarantees that the confidentiality and the integrity of the code and data loaded into it are protected. The essence of the blockchain is a data structure, and the information stored in the blockchain has the characteristics of unforgeability, traceability and transparency. This paper presents a design of a computing platform. The platform which uses popular encryption methods such as RSA and AES, and integrates with TEE and blockchain technology, can protect the privacy of users throughout the process.

**Keywords**: TEE (Trusted Execution Environment), Blockchain, Privacy Preserving, Service Computing, Computing Platform, Codes Running Platform

目录

[一、 绪论 1](#_Toc69218416)

[二、 TEE工具和区块链工具详述 2](#_Toc69218417)

[（一） TEE工具详述 2](#_Toc69218418)

[三、 整体架构与流程 3](#_Toc69218419)

[（一） 整体架构 3](#_Toc69218420)

[（二） 类图 3](#_Toc69218421)

[四、 TEE和区块链使用详述 3](#_Toc69218422)

[（一） 添加题注 4](#_Toc69218423)

[1. 使用工具栏插入题注 4](#_Toc69218424)

[2. 直接使用域代码插入题注 4](#_Toc69218425)

[（二） 引用题注 5](#_Toc69218426)

[1. 引用某一题注 5](#_Toc69218427)

[2. 使用书签引用题注 5](#_Toc69218428)

[五、 表格相关 6](#_Toc69218429)

[（一） 插入表格 6](#_Toc69218430)

[（二） 续表标记 7](#_Toc69218431)

[1. 使用文本框 7](#_Toc69218432)

[2. 使用页眉 7](#_Toc69218433)

[六、 图片相关 7](#_Toc69218434)

[（一） 插入普通图片 7](#_Toc69218435)

[（二） 插入引用图片 7](#_Toc69218436)

[1. 使用工具栏插入引用图片 8](#_Toc69218437)

[2. 直接使用域代码插入引用图片 8](#_Toc69218438)

[七、 公式相关 8](#_Toc69218439)

[（一） 公式标号 8](#_Toc69218440)

[1. 插入标号 8](#_Toc69218441)

[2. 自动标号 8](#_Toc69218442)

[3. 引用公式标号 9](#_Toc69218443)

[八、 参考文献相关 9](#_Toc69218444)

[（一） 插入参考文献 9](#_Toc69218445)

[（二） 引用参考文献 9](#_Toc69218446)

[（三） 其他的参考文献管理方案 10](#_Toc69218447)

[1. Word自带的文献管理 10](#_Toc69218448)

[2. 第三方管理方案 10](#_Toc69218449)

[九、 导出 10](#_Toc69218450)

[（一） 另存为PDF 10](#_Toc69218451)

[（二） 使用 Microsoft Print to PDF 虚拟打印机 10](#_Toc69218452)

[（三） 使用 Adobe PDF Converter 虚拟打印机 10](#_Toc69218453)

[十、 参考文献 11](#_Toc69218454)

[附录 A. Word域操作 12](#_Toc69218455)

[附录 B. Seq 域代码开关 13](#_Toc69218456)

[附录 C. 一些Word排版技巧 14](#_Toc69218457)

[十一、 致谢 15](#_Toc69218458)

# 绪论

当下的一些计算任务，如深度学习，需要很高的算力[6]，个人电脑的配置无法满足在可接受时长内完成这些计算任务并得到结果，很多用户会使用大公司的云计算平台运行这些计算任务。比较流行的一种云计算服务平台做法是：在物理机器上运行虚拟机，用户与虚拟机实例进行交互，用户对虚拟机有完整的访问和操作权限[7]，使用体验等同于以管理员身份在使用一个操作系统。例如，虚拟机实例的操作系统是Ubuntu，那么用户的使用体验等同于以管理员身份在使用一个完整的Ubuntu操作系统。并且，公司监听虚拟机的使用以记账收费。

这样的云计算服务平台做法可能会有以下问题：

在物理机器上运行多个虚拟机，虚拟机的运行会占用资源。考虑到机器最主要的功能是运行计算任务，那么相对于计算任务占用资源，运行虚拟机占用资源可以看成是一种浪费。

小企业或者个人，如果有空闲计算资源想供他人使用，由于技术限制，他们可能无法像大公司一样在物理机器上运行多个相互隔离的虚拟机实例供用户使用，并进行监听与记账收费。并且，小企业或个人的空闲计算资源可能不够充裕，无法支持运行多个虚拟机并同时运行计算任务。

对于不熟悉系统操作的人员，面对一个虚拟机实例，需要花费时间精力去学习虚拟机系统的使用。而他们想要的服务，只是上传代码文件到服务器运行，然后得到结果。

本文给出的基于TEE和区块链的隐私保护计算平台，只用在物理机器上运行一个带有在TEE中执行代码的功能的系统，然后在该系统中执行一套程序。这套程序会生成并管理密钥，接收客户端发来的代码，然后执行代码完成计算任务，最后把计算结果以及计算过程信息记录在区块链上。加密算法保证了客户端和服务端数据传输的保密性；在TEE中执行程序保证了计算任务运行时的保密性；区块链上储存加密后的计算结果和计算过程信息，保证了计算结果的不可篡改性、保密性和匿名性，实现了全程的隐私保护。

本文给出的基于TEE和区块链的隐私保护计算平台只用在物理机器上运行一个操作系统，不会有运行多个虚拟机占用过多资源的情况。并且，运行本文提出计算平台的技术门槛和开销，相比运行上述云计算服务平台要低。此外，用加密算法、TEE和区块链实现的全程隐私保护，可以让用户足够信任。而用户需要做的只是通过HTTP请求与计算平台进行交互，无需操作一个完整的系统。

# TEE工具和区块链工具的使用

TEE工具和区块链工具的使用是本文提出的隐私保护计算平台的关键所在。先了解TEE工具和区块链工具，有助于理解平台的架构、流程和模块功能。在此先给出TEE工具和区块链工具的描述，并提及其在本平台中的大致使用方式。

## TEE工具

比较流行的TEE开发工具是Intel Software Guard Extensions (SGX)[8]。但Intel SGX相对比较底层，使用Intel SGX的SDK开发程序，过程非常繁琐：需要花费大量时间学习相关接口、编程模型以及SGX SDK的编译系统。

Youren Shen等提出的Occlum，是一个针对Intel SGX的内存安全、多进程的库操作系统[9]。Occlum的最大优势是其易用性。使用Occlum，可以不用编写任何额外的SGX相关编码，仅需要使用一些shell命令就可以使程序在SGX保护下运行，也即是在TEE中运行。此外，Occlum还支持运行多种不同编程语言的程序，包括C/C++、Python、Go和Java。

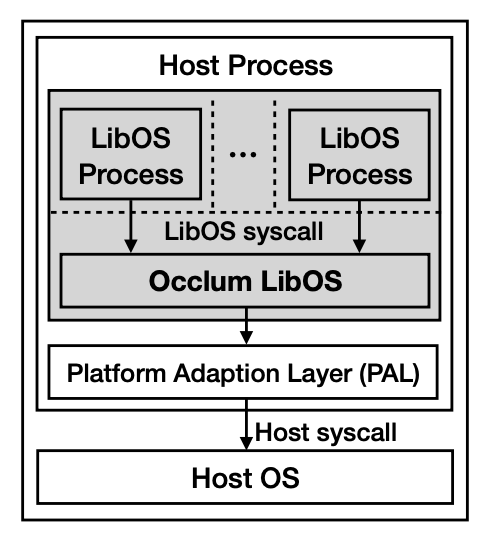


图 1 Occlum库操作系统概述

如图 1所示，Occlum是建立在主操作系统（Host OS）上的库操作系统（LibOS即Library OS）。其具体使用方式是：在安装有Occlum的主系统上，使用Occlum的相关命令运行代码文件，即可实现代码在TEE中执行。事实上，Occlum作者给出了一个内置Occlum的Ubuntu 18.04系统镜像，使用该镜像安装Ubuntu操作系统，即可在Ubuntu中使用Occlum命令，无需额外安装。该Ubuntu系统的其他使用，如文件系统、系统命令等，与一般的Ubuntu系统一样。

由于主系统是Ubuntu，所以平台代码的部署、服务器维护等操作，跟使用一般Ubuntu机器的操作一样。要让平台和计算任务运行在TEE中，只需要编写shell脚本，使用Occlum命令，让相关代码运行即可。

## 区块链工具

区块链本质是一种按照时间顺序将数据区块用类似链表的方式组成的数据结构[10]。一个基本的区块链，每个区块会包含[11]：索引（index）、时间戳（timestamp）、交易数据（transactions）、校验（proof）和前一个区块的散列（the hash of the previous block）。

本平台会在代码中自行实现一个适用本平台需求的区块链。该区块链的区块中的交易数据实际记录的是每次计算任务的信息，包括这次任务的标示、计算结果和运行信息，具体将在后文讲解。并且，因为只有服务端运行计算任务并将相关信息写入区块链，所以该区块链只会在服务端增长，而不是多方共同作用使得区块链增长，所以省去了工作量证明机制和校验。

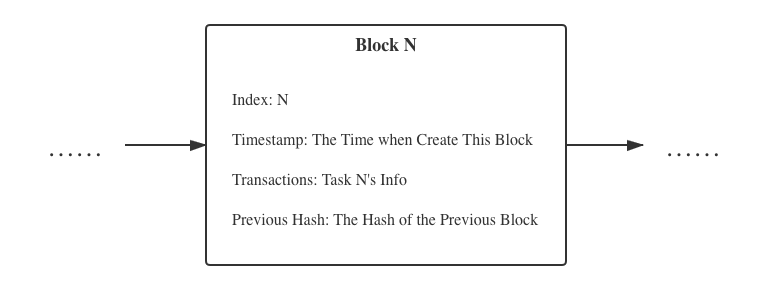


图 2 本平台所用区块链示意图（第N个区块）

# 整体架构与流程

## 整体架构

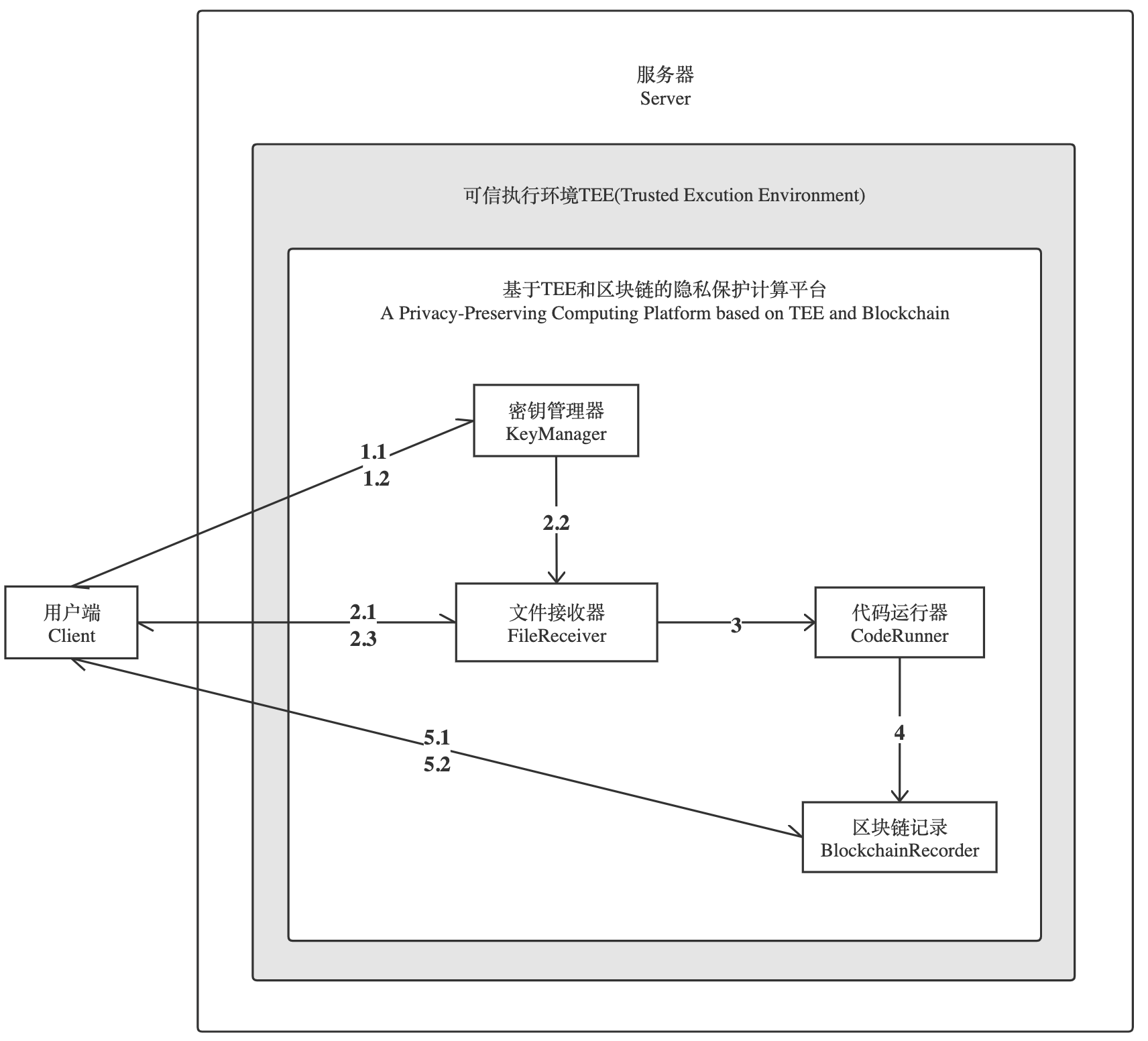


图 3 基于TEE与区块链的隐私保护计算平台 整体架构示意图

如图 3所示，本平台运行于服务器的TEE中。平台包括密钥管理器KeyManager，文件接收器FileReceiver、代码运行器CodeRunner和区块链记录BlockchainRecorder。图中个模块间的连线表示模块间有交互；连线上的标号表示具体交互过程或具体流程，详情可见下一部分（二）流程详解。

## 流程详解

本部分标号、指代等请参考：图 3 基于TEE与区块链的隐私保护计算平台 整体架构示意图。流程的标号代表流程发生的先后顺序，数字越小，代表流程越先发生。

流程中非对称加解密算法采用RSA，对于一对RSA密钥KRN，称其中公钥为KRN pub，私钥为KRN pri；

流程中对称加解密算法采用AES，AES密钥称为KA；

流程中信息摘要算法采用SHA-256；

用户端A的第n次计算任务记为An，如A的第1次计算任务记为A1；

那么，用户端A执行计算任务A1的流程如下：

### 用户端与密钥管理器进行密钥传递的一系列过程

## 引用题注

### 引用某一题注

选择工具栏的 引用 > 题注 > 交叉引用。

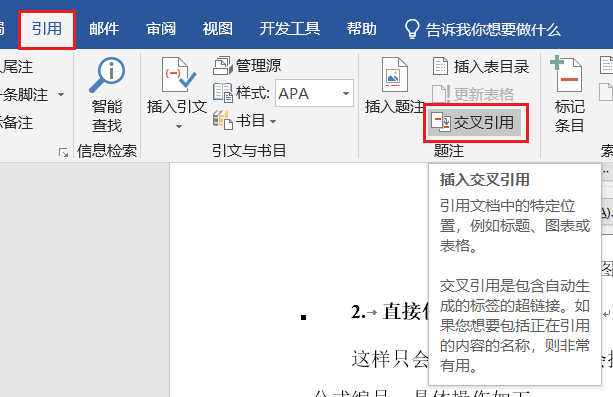


图 6. 交叉引用

选择希望引用的项目，以及引用内容后点击插入即可。

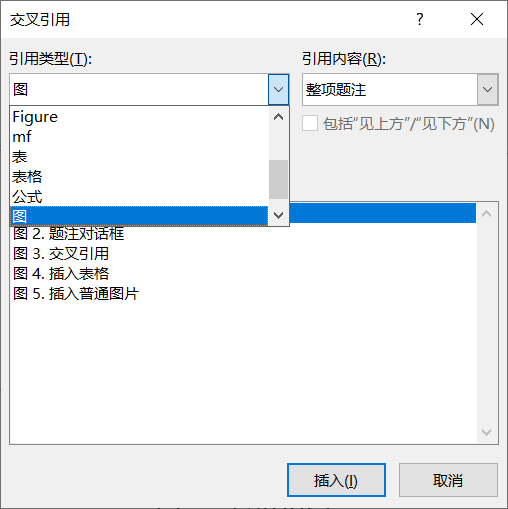


图 7. 交叉引用对话框

### 使用书签引用题注

要利用书签插入题注，首先需要为题注添加书签，再引用书签内容。

#### 添加书签

TODO

#### 使用工具栏引用书签

TODO

#### 直接使用域代码引用书签

TODO

{ REF 书签名 \h }

# 表格相关

## 插入表格

选择工具栏中的 插入 > 表格，再选择需要的大小即可



图 8. 插入表格

模板默认的表格样式为三线表。若希望插入Word默认的表格样式，请选中表格后选择工具栏中的 设计 > 网格型。如希望始终插入默认表格，对 网格型 选项右键，在菜单中选择 设为默认值。

## 续表标记

目前在Word中插入续表标记的操作比较复杂，建议在文章完成后再进行相关操作。

### 使用文本框

TODO

### 使用页眉

TODO

# 图片相关

## 插入普通图片

选择工具栏中的 插入 > 图片 或 插入 > 联机图片，再选择图片即可。



图 9. 插入普通图片

当然，你也可以直接将图片拖动到文档中或复制粘贴。

## 插入引用图片

引用图片实际上是一个Word域。使用引用图片可以做到当引用的图片改变时，更新文档可以同时更新图片而不需重复插入。但是与此同时，你也无法在Word中对引用图片使用某些编辑功能。

### 使用工具栏插入引用图片

TODO

### 直接使用域代码插入引用图片

TODO

{ INCLUDEPICTURE "图片路径" }

# 公式相关

Word 默认插入公式的快捷键为 Alt + = 。具体的公式编写规则参见**错误!未找到引用源。**-**错误!未找到引用源。**]。下面只说明添加自动标号以及引用公式的方法

## 公式标号

### 插入标号

在要插入标号的公式后，添加“”，

并回车，效果如下图所示：

也可以直接使用公式

效果是相同的。

### 自动标号

自动标号实际上是利用了Word的题注功能实现的。因此方法与TEE和区块链使用详述一章的操作大同小异。

#### 使用工具栏插入自动标号

TODO

效果如下所示：

#### 直接使用域代码插入自动标号

TODO

{ SEQ mf }

效果如下所示：

### 引用公式标号

公式必须使用书签引用。TODO

#### 使用工具栏引用公式

TODO

这样就引用了式。

#### 直接使用域代码引用公式

TODO

{ REF 公式书签名 \h }

如

{ REF inverse\_fourier\_transform \h }

这样就引用了式。

# 参考文献相关

Word 的参考文献管理有很多方案，但是能做到开箱即用而且功能齐备易用的却寥寥无几。出于灵活性和简便性的考虑，本模板使用的是最原始的手动管理方案。下面简单介绍手动管理的操作方式以及其他文献管理的方式。

## 插入参考文献

TODO

## 引用参考文献

TODO

## 其他的参考文献管理方案

### Word自带的文献管理

这一方案胜在开箱即用且功能齐全。而且相比手动管理，Word提供跨文档的文献数据整理，更为方便。但不足的是Word并不自带对最新的参考文献著录规则GT/7714-2015的支持，只有GB/7714-20 05的支持。如果要使用自带的管理功能，必须自行编写繁复的XSL样式文件来支持新标准。这导致我们几乎无法使用自带的文献管理。日后若有对GT/7714-2015的完整支持（无论是官方还是社区编写文件），本模板可能转向使用内置的文献管理方案。

### 第三方管理方案

目前已经有很多与Word集成的第三方文献管理方案。如Endnote、Mendeley、NoteExpress、Zotero等。有需要可以自行引入使用，这里不再赘述。

# 导出

这里的“导出”指的是导出PDF，有三种方式，各有其利弊。

## 另存为PDF

TODO

## 使用 Microsoft Print to PDF 虚拟打印机

TODO

## 使用 Adobe PDF Converter 虚拟打印机

TODO

# 参考文献

1. Sabt M, Achemlal M, Bouabdallah A. Trusted execution environment: what it is, and what it is not[C]//2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015, 1: 57-64.
2. Yaga D, Mell P, Roby N, et al. Blockchain technology overview[J]. arXiv preprint arXiv:1906.11078, 2019.
3. Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.
4. Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
5. Daemen J, Rijmen V. Reijndael: The Advanced Encryption Standard[J]. Dr. Dobb's Journal: Software Tools for the Professional Programmer, 2001, 26(3): 137-139.
6. 余凯, 贾磊, 陈雨强, 等. 深度学习的昨天, 今天和明天[J]. 计算机研究与发展, 2013, 50(9): 1799.
7. 吴吉义, 平玲娣, 潘雪增, 等. 云计算: 从概念到平台[J]. 电信科学, 2009, 25(12): 23-30.
8. McKeen F, Alexandrovich I, Anati I, et al. Intel® software guard extensions (intel® sgx) support for dynamic memory management inside an enclave[M]//Proceedings of the Hardware and Architectural Support for Security and Privacy 2016. 2016: 1-9.
9. Shen Y, Tian H, Chen Y, et al. Occlum: Secure and efficient multitasking inside a single enclave of intel sgx[C]//Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems. 2020: 955-970.
10. 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.
11. Van Flymen D. Learn blockchains by building one[J]. The fastest way to learn how Blockchains work is to build one, 2017.

# 附录 A. Word域操作

表 A1. Word域操作的快捷键

|  |  |  |
| --- | --- | --- |
| 操作 | 流程 | 快捷键 |
| 插入域 | 工具栏 > 插入 > 文档部件 > 域 | Ctrl + F9 |
| 更新选定域 | 菜单 > 更新域 | F9 |
| 切换选定域的域代码显示 | 右键菜单 > 切换域代码 | Shift + F9 |
| 切换所有域的域代码显示 | — | Alt + F9 |
| 编辑选定域 | 右键菜单 > 编辑域 | — |
| 锁定选定域 | — | Ctrl + F11 |
| 解锁选定域 | — | Ctrl + Shift + F11 |
| 跳转到下一个域 | — | F11 |
| 跳转到上一个域 | — | Shift + F11 |

详细的Word域操作参见**错误!未找到引用源。**-**错误!未找到引用源。**]

# 附录 B. Seq 域代码开关

Seq 域的详细介绍参见**错误!未找到引用源。**]。

\c

重复最近一次使用的编号，这对在页眉和和页脚中插入章节编号十分有用。

\h

隐藏域结果。 使用它来不显示数字地引用交叉引用中的Seq字段。 例如，您可能要引用编号的章节，但不希望显示章节编号。 如果还存在格式开关 (\\*)，则\h开关不会隐藏域结果。

\n

插入指定项目的下一个编号。这是默认开关。

\r n

将编号重置为指定的数字n。如{ SEQ figure \r 3 } 会将figure的编号重置为3。

\s

在开关指定的标题级别后重置编号。例如{ SEQ figure \s 2 }会在二级标题样式处开始编号。

# 附录 C. 一些Word排版技巧

* 使用 Ctrl + \* 可以切换空白字符的显示与否。这对于排版效果查错十分有效。
* 开始 > 段落 > 查看网格线 可以显示隐藏的表格边框，这对于表格格式调整以及排版效果查错也十分有效。
* 在Word中使用矢量图，最好使用EMF格式。否则导出时会被导出为位图。
* 段落设置中 换行与分页 下的 与下段同页 和 段中不分页 在需要控制内容布局时非常实用。
* 建议将插入题注，插入书签，交叉引用等常用功能添加到快速访问工具栏，这样可以直接通过 Alt + 数字 来便捷地使用相关功能。

# 致谢

致谢应以简短的文字对课题研究与论文撰写过程中曾直接给予帮助的人员(例如指导教师、答疑教师及其他人员)表达自己的谢意，这不仅是一种礼貌，也是对他人劳动的尊重，是治学者应当遵循的学术规范。内容限一页。