信息安全概论课程设计（2020 春）

截止时间：2020-06-30，24：00 之前给教师发邮件。

学号：1183710109

姓名：郭茁宁

教师信箱：zhaijh_hit@126.com 和 Conandor@126.com 两个邮箱各发一份，提交形式（学号-姓名.pdf）

成绩：

题号	(1)	(2)	(3)	合计
成绩				

课程设计要求

目前国内区块链技术发展应用迅速，且有广阔的前景，区块链最初应用起源于比特币，其实现与密码学紧密相连。

认真回答下列问题，注意格式规范，结构合理，语言流畅、图表清晰。如果格式排版混乱，总分成绩可减 5 分。(小标题黑体小四号，正文宋体五号，图表名及内部字体小五号，长度不限，可自由调整。)

1. 简述区块链原理及安全机制，分析其有哪些特点，并说明该特点的实现是否与密码学相关，说明如何相关。（5 分，）

区块链技术是一种去中心化、去信任化的分布式数据库技术方案。该数据库由参与系统的所有节点集体维护，具有去中心化、不可篡改、透明、安全等特性。在典型的区块链系统中，数据以区块为单位产生和存储，并按照时间顺序连成链式数据结构。所有节点共同参与区块链系统的数据验证、存储和维护。新区块的创建通常需得到全网多数（数量取决于不同的共识机制）节点的确认，并向各节点广播实现全网同步，之后不能更改或删除。

特点：

- 可靠开放性：区块链的设计使它能够有效预防故障与攻击，５１％攻击除外（如果攻击者拥有网络中５１％的算力，他就可以对区块进行伪造，然后自己又最快地计算出正确的解，造成区块链分叉，达到攻击的目的）。所有参与系统的用户共享一个公共区块链，

不会存在因为单点失效而导致系统故障的情况，从而保证了系统的可靠性和数据的可获得性。

- 信息透明性：网络上的任何节点都可以查看整个账本。由于记录的交易信息不包含任何隐私，因此任何记录在册的信息都可以被查看，保证了数据的透明性。
- 不可更改性：区块链系统采取的是完全冗余的策略，所有完整节点都有一份完整数据，要想更改某一区块的数据，必须保证所有完整节点数据被修改，这个情况几乎不可能发生，因此降低了欺诈的风险。
- 不可逆转性：交易不存在撤销操作，交易一旦被验证认可，就不可再逆转。

在区块链中，使用的密码学的技术成果主要包括：哈希算法、对称加密、非对称加密等。哈希算法技术保证区块链账本的完整性不被破坏。哈希（散列）算法能将二进制数据映射为一串较短的字符串，并具有输入敏感特性，一旦输入的二进制数据，发生微小的篡改，经过哈希运算得到的字符串，将发生非常大的变化。此外，优秀哈希算法还具有冲突避免特性，输入不同的二进制数据，得到的哈希结果字符串是不同的。区块链尤其是联盟链，在全网传输过程中，都需要 TLS（Transport Layer Security）加密通信技术，来保证传输数据的安全性。而 TLS 加密通信，正是非对称加密技术和对称加密技术的完美组合：通信双方利用非对称加密技术，协商生成对称密钥，再由生成的对称密钥作为工作密钥，完成数据的加解密，从而同时利用了非对称加密不需要双方共享密钥、对称加密运算速度快的优点。

2. 方案设计（共 20 分）

设计一个彩票中心销售服务方案，包括发布、销售、兑奖等环节（兑奖：视频摇奖，直接公布获奖号码列表），彩票销售、兑奖等环节均线上实现，线上交易模仿 SET 协议，充分利用课内相关知识，也可参考区块链安全解决方法及自己合理发挥。（20 分）

彩票销售过程参考：

（1） 彩民线上购买彩票，选择彩票号码及投注数，购买资金汇入彩票中心的银行账户；

（2） 彩民保存购买彩票号码和投注数，重要信息加密签名后提交彩票中心保存；

（3） 彩票开奖过程，视频直播开奖，网上公布获奖彩票号码列表；

（4） 彩民依据购买彩票信息，向彩票中心申请兑奖；

（5） 彩票中心验证无误，提交奖金转账信息给银行；

（6） 银行核对信息无误，将奖金转给彩民账户。

前置条件：

（1）实体：彩票中心 TC（TicketCenter），顾客 User，认证中心 CA（绝对安全可信），兑奖银行（Bank）

（2）User、TC 和银行均已在 CA 认证中心注册，拥有证书 CA_{user}、CA_{tc} 和 CA_{bank}。

（3）User 和 TC 均已以在银行 Bank 注册，拥有账户（BankAccount）BA_{user} 和 BA_{tc}；

(在方案设计区的相应小标题下，填写你的相关设计说明即可，长度不限，随意调整；彩票销售兑奖等过程步骤，大家需做需求调研，具体方案内容大家可以合理发挥)

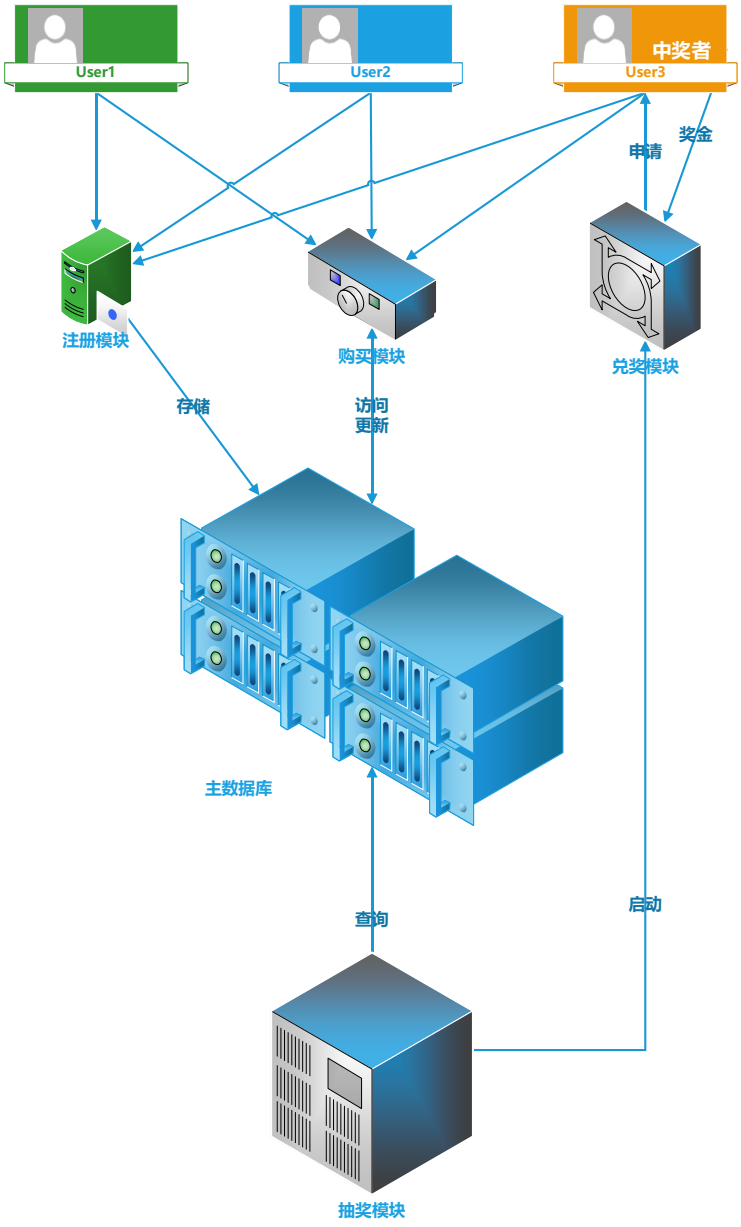
方案设计区

一、基于区块链的彩票销售系统整体架构（本问题 5 分）

（1）系统功能描述

该系统能够基于区块链进行用户、彩票中心和银行三方之间的交易。用户注册确保隐私，并能在需要时使用用户的信息；系统能够支持用户购买彩票，在不泄露隐私的情况下用户申请兑奖，在银行账户中交易，防止各种攻击。

（2）物理拓扑结构示意（建议使用 Visio 画图）



（3）功能模块划分与定义

- 主数据库：存储用户加密信息和购买记录；
- 注册模块：提供用户注册功能并载入用户加密信息；
- 购买模块：提供购买彩票功能，在主数据库中记录购买信息；
- 兑奖模块：提供兑奖功能，在用户申请兑奖时启用；

（4）区块链技术在彩票销售过程中的作用（解决的问题）

- 所有中奖地彩票和金额都可以公开备查同时又能保证中奖者身份的保密性；
- 保证兑奖的实时性；
- 保证彩票发行的公正性；

二、用户在彩票中心注册过程与说明（协议描述格式与形式，模仿 Kerberos 双向交互形式写法，后边要有注释说明，具体的密码使用可以采用对称密钥密码，也可以采用公开密钥密码）（本问题 3 分）

用户和彩票中心之间使用私钥$PriKey$和公钥$PubKey$；用户和银行之间使用对称密钥$KeyU1$和$KeyBA1$。

0. 用户和彩票中心分别获得了 CA；
1. 用户向彩票中心提供CA_{user}和用私钥$PriKey$加密后的用$KeyU1$加密后的用户银行账户$E_{KeyU1}[BA_{user}]$；

$$User \rightarrow TC: CA_{user} || E_{PriKey}[E_{KeyU1}[BA_{user}]]$$

2. 彩票中心使用公钥$PubKey$验证CA_{user}后，保存加密后的用户银行账户$E_{KeyU1}[BA_{user}]$，并向用户提供响应消息Ans_{TC}和用户唯一标识ID_{user}；

$$TC \rightarrow User: E_{PubKey}[Ans_{TC} || ID_{user}]$$

三、彩票销售购买过程与说明（参照 Kerberos 写法，后边要有注释说明）（本问题 3 分）

用户和彩票中心之间使用私钥$PriKey$和公钥$PubKey$；用户和银行之间使用对称密钥$KeyU1$和$KeyBA1$；彩票中心和银行之间使用对称密钥$KeyTC2$和$KeyBA2$。

0. 用户、彩票中心、银行相互拥有对方 CA，每次传输中均验证一次；

1. 用户向账户BA_{user}存款；

$$User \rightarrow Bank: Cash$$

2. 用户从彩票中心获得彩票信息，并选择彩票号码Num和投注数Bet，与用户唯一标识ID_{user}和用$KeyU1$加密的支付指令Pay_{user}通过私钥加密后传给彩票中心；

$$User \rightarrow TC: E_{PriKey}\left[Num||Bet||ID_{user}||E_{KeyU1}[Pay_{user}]\right]$$

3. 彩票中心用公钥解密，向银行申请将ID_{user}对应的（已加密）账户签名$E_{KeyU1}[BA_{user}]$（注册时已知）扣款，即$KeyTC2$加密：应付金额$Money_{user}$、用户账户签名$E_{KeyU1}[BA_{user}]$、彩票中心账户BA_{tc}和加密后的用户支付指令$E_{KeyU1}[Pay_{user}]$（与银行间使用对称加密技术）；

$$TC \rightarrow BA: E_{KeyTC2}\left[Money_{user}\left||E_{KeyU1}[BA_{user}]\right|\right| BA_{tc}||E_{KeyU1}[Pay_{user}]\Big]$$

4. 银行使用$KeyBA2$解密以上信息，再用$KeyBA1$解密出BA_{user}和Pay_{user}，结合BA_{user}验证用户支付信息Pay_{user}，验证成功后向中心发送授权相应消息$Arth_{BA}$；

$$BA \rightarrow TC: E_{KeyBA2}[Arth_{BA}]$$

5. 彩票中心解密获得授权信息后，给用户发送加密授权信息$Arth_{BA}$的确认信息$Conf_{tc}$；

$$TC \rightarrow User: Conf_{tc}||E_{PubKey}[Arth_{BA}]$$

6. 用户解密出银行授权信息$Arth_{BA}$进行确认，通过$Conf_{tc}$回复$Conf_{user}$确认进行交易；

$$User \rightarrow TC: Conf_{user}$$

7. 彩票中心获得确认信息$Conf_{user}$后，通知银行进行转账；

$$TC \rightarrow BA: Conf_{user}$$

8. 银行获得彩票中心信息后，将BA_{user}账户上$Money_{user}$金额转入BA_{tc}，向两个银行账户发送交易完成的信息；

四、彩票兑奖过程与说明（参照 Kerberos 写法，后边要有注释说明）（本问题 3 分）

0. 彩票开奖得到中奖号码集合Num_0，冻结购买彩票行为，向用户广播；

$$TC \rightarrow User: Num_0$$

1. 用户得知自己中奖后，向彩票中心发送私钥加密后的兑奖申请，内容包括CA_{user}；

$$User \rightarrow TC: E_{PriKey}[CA_{user}]$$

2. 彩票中心获得兑奖申请后用公钥解密，通过查询CA_{user}对应的ID_{user}，以及ID_{user}对应的彩票号码Num、投注数Bet和加密银行账户$E_{KeyU1}[BA_{user}]$，确认$Num \epsilon Num_0$且为被标记

后，将Num标记为“已兑奖”，并向银行发出加密的交易申请：包括支付指令Pay_{tc}，BA_{tc}，$E_{KeyU1}[BA_{user}]$，$Money_{tc}$；

$$TC \rightarrow BA: E_{KeyTC2}\left[Money_{tc} \left|\right| E_{KeyU1}[BA_{user}] \left|\right| BA_{tc} || Pay_{tc}\right]$$

3. 银行使用$KeyBA2$解密以上信息，再用$KeyBA1$解密出BA_{user}，，验证CA_{tc}、BA_{tc}和Pay_{tc}，向彩票中心发送授权相应消息$Arth_{BA}$；

$$BA \rightarrow TC: E_{KeyBA2}[Arth_{BA}]$$

4. 彩票中心收到交易授权信息解密后，向银行发送确认交易消息；

$$TC \rightarrow BA: Conf_{tc}$$

5. 银行获得彩票中心确认信息后，将BA_{tc}账户上$Money_{tc}$金额转入BA_{user}，向两个银行账户发送交易完成的信息；

五、系统风险分析（分析是否存在“用户隐私信息泄漏”、“重放攻击”、“身份欺诈”、“冒名兑奖”、“彩票中心否认用户获奖”、“用户谎称没有收到奖金”等威胁，系统是如何应对这些威胁的，一一说明。）（本问题 6 分）

- 用户隐私信息泄漏：需要同时有CA_{user}、私钥$PriKey$和ID_{user}才能得到加密后的用户信息，其中加密银行账户BA_{user}还要有对称密钥才能解密。
- 重放攻击：每个中奖号码在申请兑奖时，会被标记为“已兑奖”，因此若用户重复申请兑奖，会在彩票中心验证是驳回。
- 身份欺诈：每个用户在注册之后会获得唯一的ID_{user}和私钥$PriKey$用于与彩票中心进行身份验证，若在购买彩票或兑奖时，使用的CA_{user}和ID_{user}不匹配、或错误私钥加密后无法解密，都会被彩票中心视为身份欺诈。
- 冒名兑奖：每个用户持有不同的CA_{user}，只有指定的CA_{user}对应的Num才能为中奖号码，即彩票中心能够通过证书确认用户是否中奖。
- 彩票中心否认用户获奖：在彩票中心公开中奖号码后，若彩票中心否认中奖，用户可以以加密在彩票中心的购买信息为证，即用户通过私钥解密Num证明自己所购买的彩票号码。
- 用户谎称没有收到奖金：若在银行汇款后，用户谎称没有收到奖金，彩票中心可以以用户申请兑奖的记录、银行授权消息$Arth_{BA}$、银行提供的彩票中心确认信息$Conf_{tc}$和银行转账记录为证。

3. 在你设计彩票中心销售系统时，如果彩票中心领导要求可以查看用户购买彩票情况（号码），以及用户相关信息，便于管理及公安等部门依法处理有关事宜，希望你开发这样的功能。（共 5 分）

一、你将如何做，谈谈你的想法，为什么？（此问题 3 分）？

设计一个带锁的权限，只由最高领导层知晓密码，拥有这个权限可以跳过CA_{user}获取所有用户的ID_{user}，以此获得所有用户购买的彩票号码Num，并且设置为只读模式。这样可以将隐私保护的责任人范围缩小，并且将“泄露隐私”与“利益损失”捆绑，可以有效约束责任人的行为；此外可以在需要的时候为公安等部门提供数据。

二、你准备采取何种技术措施，简单描述。（此问题 2 分）

使用对称密钥密码，一个密钥交给领导，一个密钥在系统程序里，领导需要的时候可以输入密钥打开权限。打开权限后，获得认证协议，请求访问数据库时，数据库检查协议，提供只读数据接口。访问完毕后，销毁认证协议，关闭访问接口。