信息安全概论 课程设计（2020 春）

学号：xxxxxxxxxx

姓名：cycleke

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，）

区块链原理

区块链起源于中本聪的比特币，作为比特币的底层技术，本质上是一个去中心化的数据库，是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。它是借由密码学串接并保护内容的串连文字记录。

每一个区块包含了前一个区块的加密哈希、相应时间戳记以及交易数据（通常用默克尔树(Merkle tree)算法计算的哈希值表示），这样的设计使得区块内容具有难以篡改的特性。以比特币的区块链账本为例,每个区块基本由上一个区块的哈希值，若干条交易，一个调节数等元素构成，节点通过工作量证明实现对交易整理为账本区块和区块安全性的维持。一个节点通过交易广播渠道收集交易项目并打包,协议约定了区块速度生成速度而产生的难度目标值,通过不断将调节数和打包的交易数据进行哈希运算而算出对应哈希值使其满足当时相应的难度目标值,最先计算出调节数的节点可以将之前获得上一个区块的哈希值、交易数据、当前算出对应区块的调节数集成为一个账本区块并广播到账本发布渠道,其他节点则可以知道新区块已生成并知道该区块的哈希值（作为下一个区块的“上一个区块的哈希值”），从而放弃当前待处理的区块数据生成并投入到新一轮的区块生成。

区块链是分布式账本，交易记账由分布在不同地方的多个节点共同完成，而且每一个节点都记录的是完整的账目,因此它们都可以参与监督交易合法性,同时也可以共同为其作证。

区块链的安全机制

由于区块链是分布式的,每个节点都存储了完整的帐目。跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。

为了防止某个节点伪造一条交易记录，区块链还具有共识机制，就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制(PoW 工作量证明、PoS 权益证明、PBFT 实用拜占庭容错和 POOL 验证池），适用于不同的应用场景，在效率和安全性之间取得平衡。比特币使用的就是工作量证明（PoW，Proof of Work）。由于哈希运算难以由输出反向推导出输入，所以所有的节点都只能使用枚举的方式来得到正确的调节数，以证明其工作量来获得对应的“奖励”。只有当某个人控制的计算能力超过整个节点网络的 50%时，才有可能伪造一条不存在的记录（即算力劫持）。当加入区块链的节点足够多时，这样算力劫持的代价过大，几乎不可能发生。以太坊则是使用权益证明（PoS，Proof of Stake），相对于 PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升。它利用世界各地的节点来验证合约的有效性。人们难以控制保证部署自己合约的计算节点，也保证了安全性。

区块链的特点

区块链技术具有以下特征：

一是去中心化。区块链技术不依赖额外的第三方管理机构或硬件设施，没有中心管制，除了自成一体的区块链本身，通过分布式核算和存储，各个节点实现了信息自我验证、传递和管理。去中心化是区块链最突出最本质的特征。

二是安全性。一般，哈希函数是单向的，通过哈希函数的逆函数来求的消息原文在计算上是不可行的。所以只能够通过枚举后验证的方法来计算。而算力劫持等方式来伪造交易记录的代价过大，这样保证了区块链的安全性。

三是匿名性。除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行。区块链使用了非对称加密和授权技术，存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。非对称加密同样基于单向函数，基于大整数分解或其他问题求解的计算困难性，难以破解。

2. 方票案设计（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（Ticket Center），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}；

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

系统需要实现用户注册、登录、彩票发布、销售、兑奖等功能。

具体而言，系统使用 Kerberos 来进行登陆认证。用户在登陆后后可以利用 SET 协议来购买彩票。此外，此彩票销售系统还使用区块链来记录和交易，用于兑奖时的验证。

（2）物理拓扑结构示意

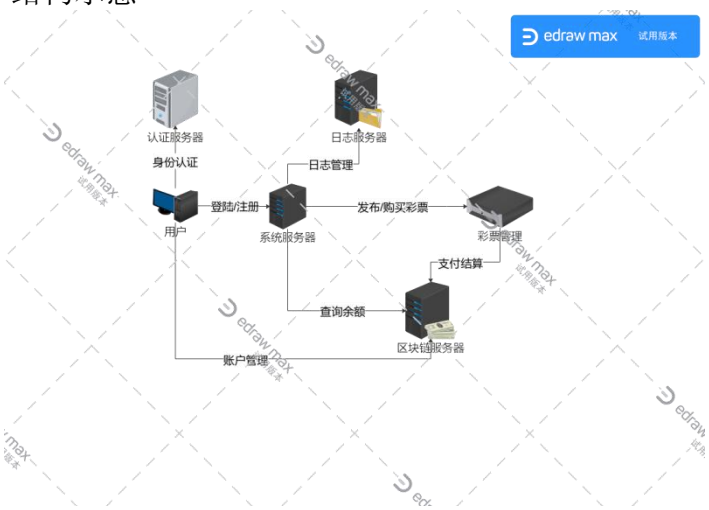

图 1 物理拓扑结构

（3）功能模块划分与定义

用户注册模块

用户在注册时需要填写用户名、密码以及手机号进行注册。用户注册成功后会在 CA 认证，同时会获得一个区块链地址用于彩票交易。

用户可以在注册时绑定银行账户（或支付宝等）用于交易、也可以在支付时再绑定。绑定时需要与第三方进行认证联动。

用户登陆模块

用户登陆使用的是 KerBeros 协议。用户在登陆时需要提供用户名和密码，首先与 AS 进行身份验证服务交换，之后和 TGS 开展票据授予服务交换，最后与彩票中心进行身份验证交换，完成登陆。

在手机 APP 上，用户还可以使用消费级的指纹、面部识别来代替密码来登陆（不过首次登陆必须使用密码）。

彩票发布模块

彩票供应商在彩票中心广播一次彩票发布。系统会记录其区块链地址用于其他用户购买彩票以及后续的兑奖。同时中心会向日志服务器添加对应的日志。

用户购买模块

用户在购买彩票时需要选择彩票号码以及投注数,之后利用绑定的第三方交易账户基于 SET 协议进行交易，同时利用区块链来记录交易。

用户会向彩票中心发送自己选择的彩票号码以及投注数。中心对此作出应答，验证受到的号码及注数是否正确。之后用户选择支付方式，核定订单。他在验证了中心的 CA 证书后,会发送包含完整订购信息和支付信息的订单。中心在接受订单后，验证顾客的身份，并向其支付账户所在金融机构(一般为银行)请求支付授权。清算机构之后会完成清算。

彩票中心会在完成清算后记录该用户购买了这份订单，存储到日志服务器，同时会在区块链服务器中记录此次交易。资金会首先到用户对应的区块链地址中，之后在区块链中将资金转到彩票商的地址中。

彩票开奖模块

视频直播开奖，使用类似双色球开奖的机制。此部分没有其他额外的要求，与一般的彩票开奖直播无异。

彩票兑换模块

在开奖完成后，系统会自动兑奖。中心会在日志中查询对应的中奖彩票，计算总奖金，之后向彩票商要求提供对应的奖金到自己的地址中。之后区块链系统会将对应的奖金发送到中奖用户的地址中。用户可以在需要时将区块链中的资金利用 SET 协议转入到自己的第三方账户中。

（4）区块链技术在彩票销售过程中的作用（解决的问题）

此系统主要利用了区块链系统难以伪造交易记录的特点。基于区块链技术，其他人难以冒领或伪造彩票。同时由于区块链是公开的，彩票商也难以抵赖，即使是中心的工作人员也无法监守自盗。

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）

实体用户 User，彩票中心 TC，认证服务器 AS

User -> TC:EK_{TC}(ID|PASSWD|INFO|K_{User}) User 利用 TC 的公钥来加密自己的注册账号、密码以及信息和一个临时密钥，发送给 TC

TC -> AS:$EK_{TC,AS}$(ID) TC 试图在 AS 中尝试创建新的认证信息

AS -> TC:$EK_{TS,AS}$($K_{User,AS}$) AS 返回后续 User 用于认证的密码

TC -> User:EK_{User}(IsSuccess|INFO|$K_{User,AS}$) TC 尝试利用提供的信息来进行注册，返回是否注册成功，如果成功有对应的额外信息（如区块链地址）和用于 AS 注册认证的密码 $K_{User,AS}$

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）

实体用户 User，彩票商 Company,彩票中心 TC，区块链服务器 BS，日志服务器 LS（此时用户已经使用 Ticket 完成认证）

User -> TC:$EK_{Ticket}(INFO_1)$ User 向 TC 发送购买信息

TC -> User:$EK_{User}(INFO_1)$ TC 再次发送订单用于确认

User -> TC:$EK_{Ticket}(IsCorrect|INFO_1)$ User 确认后再次发送

TC -> BS:$EK_{TC,BS}(Addr_{User}|Addr_{Company}|INFO_2)$ TC 向 BS 发送 User 和 Company 的区块链地址以及订单信息

BS -> TC:$EK_{BS,TC}(INFO_3)$ BS 返回交易结算信息

TC -> LS:$EK_{TC,LS}(INFO_4)$ TC 向 LS 发送日志信息

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）

中奖用户 User，彩票商 Company,彩票中心 TC，区块链服务器 BS，日志服务器 LS，银行 Bank

TC -> LS:$EK_{TC,LS}(QUERY)$ TC 在 LS 中查询中奖用户

LS -> TC:$EK_{LS,TC}(USER\_LIST)$ LS 返回用户列表

TC -> Company:$EK_{Company}(TOTAL)$ TC 向 Company 索要中奖金额

Company -> Bank:$EK_{Bank}(Auth_{Company}|BS|Addr_{Company})$ Company 要求 Bank 向 DS 转账

Bank -> Company:$EAuth_{Company}(INFO_1)$ Bank 返回交易信息

Company -> TC:$EK_{Ticket}(IsFinished)$ Company 告诉 TC 完成转账

TC -> BS:$EK_{TC,BS}(Addr_{Company}|Addr_{User}|INFO_2)$ TC 向 BS 发送 User 和 Company 的区块链地址以及订单信息

BS -> TC:$EK_{BS,TC}(INFO_3)$ BS 返回交易结算信息

TC -> LS:$EK_{TC,LS}(INFO_4)$ TC 向 LS 发送日志信息

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

彩票中心存储的所有的信息均使用加密的方式防止隐私泄露,而日志系统中的存储的是加密后的用户信息，必须通过彩票中心解密才能获得具体的信息。在信息传输的过程中，信息均使用了公钥或票据加密，无法在信道中获取信息。

而在公开的区块链中，用户使用的是一个随机唯一的交易地址。区块链具有高度的匿名性，其他人无法利用区域链来追踪用户。

重放攻击

在注册、登录、购买等环节,系统会发送当时的时间戳，如果时间戳对应的时间和服务

器时间的差距过大，那么会将该操作判定为无效操作，不会执行。而且登陆认证的票据具有有效期，如果长时间不登陆，那么该票据会失效。用户再次登陆时需要使用密码等方式来重新获得认证票据。

身份欺诈

所有的交易信息均使用密钥来加密，除非可以盗取用户的密钥/票据，那么其他人无法冒充用户或者中心来进行欺诈。

冒名兑奖

每个人的数字货币账户是唯一的，且绑定唯一的用户。而兑奖过程在线上完成且完全自动化，无法冒名兑奖。

彩票中心否认用户获奖

由于交易信息在区块链中有存储，而区块链难以篡改。用户使用公开的信息来证明自己的区块链地址购买了对应的彩票，但是没有获得奖金的记录。

用户谎称没有收到奖金

与“彩票中心否认用户获奖”问题类似，系统利用区块链来解决此问题。在第三方支付机构（如银行）的流水中也存储了转账信息，保证了这个问题难以发生。

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）？

我会依照相关的法律提供对应的服务。如果系统提供绝对的匿名和隐私，那么就可能变成违法犯罪的场所。事实上，由于比特币高度的匿名性，比特币就成为了许多犯罪份子将非法获利用于洗钱的工具，如勒索病毒 WannCry 的作者就使用比特币进行转账。

二、你准备采取何种技术措施，简单描述。（此问题 2 分）

首先在日志系统中存有所有的交易记录，在区块链中亦存储交易记录。系统可以通过将日志解密来获得交易的记录，也可以查询区块链地址对应的用户来查询交易记录。

同时整个系统是加密的，日志系统和彩票中心也是分离的，一定程度上可以防止信息泄露。