第7章 网络安全应用

董建阔

南京邮电大学

主要内容

网络安全应用解决方案
- 基于安全IP的安全解决方案
- 基于SSL的安全解决方案

电子邮件安全应用技术
- PGP安全技术
- S/MINE安全技术

万维网(WWW)安全应用技术
- 万维网攻击分析，SDL注入攻击、XSS攻击
- 万维网的安全防范技术

区块链及其应用

网络安全应用概述

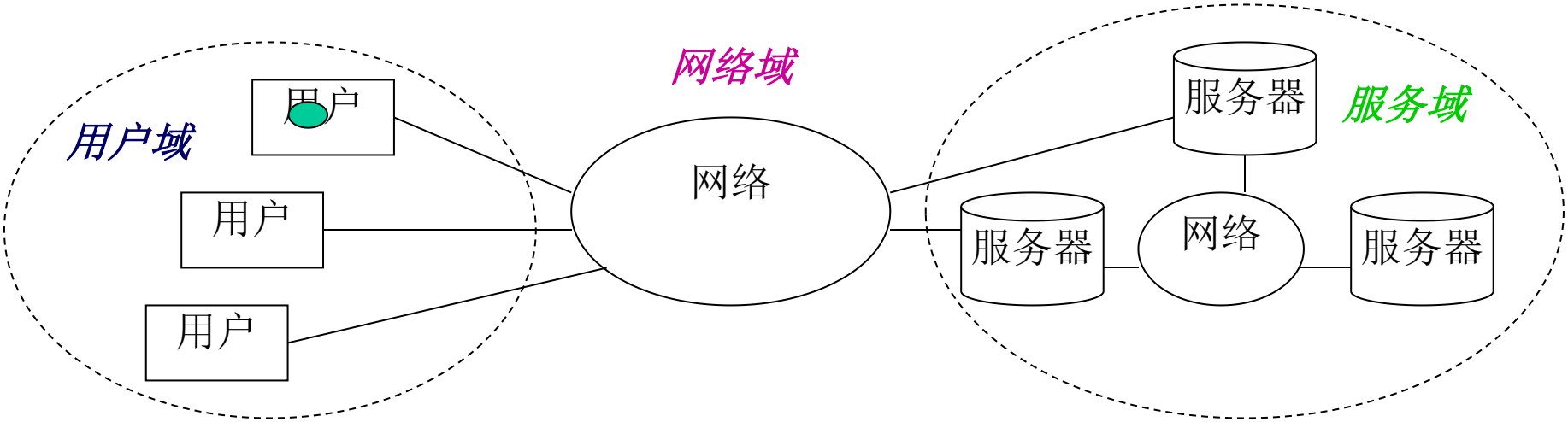
- 网络安全的目标(内涵)包括：保密性、完整性和可用性。因此，网络应用安全技术需解决以下两方面问题：

  1）一方面，需要解决网络应用相关数据的保密性和完整性问题，这方面的责任方包括：应用系统管理员、用户。

  2）另一方面，需要解决网络应用系统本身的可用性问题，这方面的责任方包括：网络系统和应用系统管理员。

C/S网络应用的抽象结构

- 客户端/服务器(C/S)的网络应用结构包括了用户域、网络域和服务域。
- 对等网络(P2P)的网络应用结构是C/S应用结构的组合

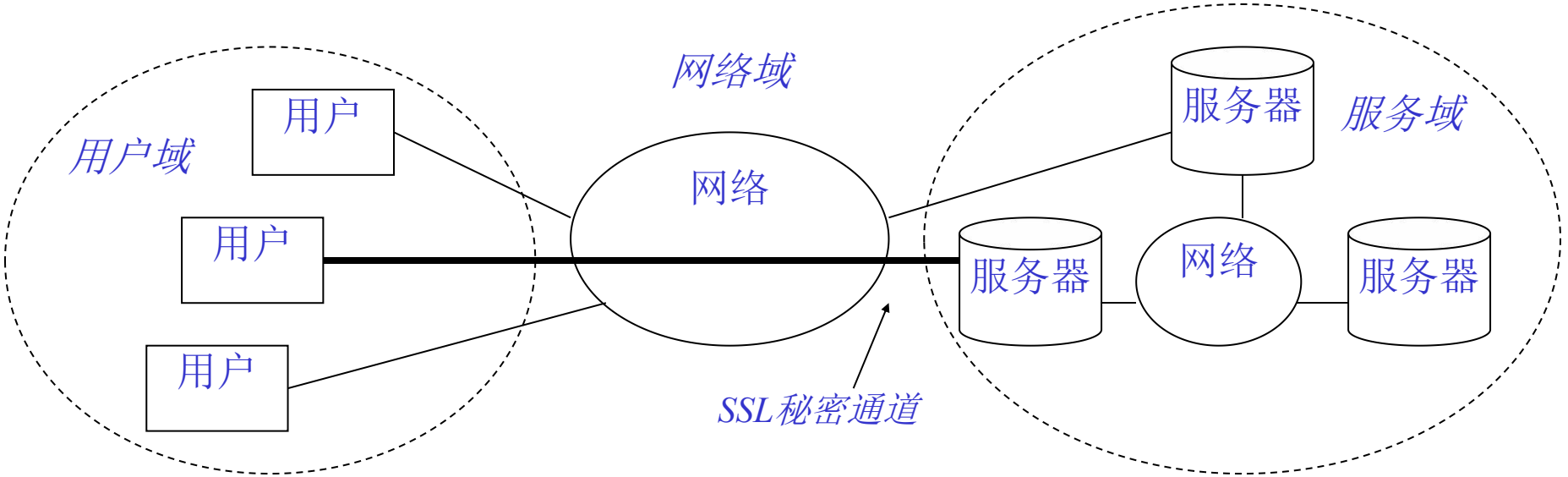


客户端/服务器(C/S)网络应用抽象结构

网络应用保密性和完整性解决方案

（1）传送层安全技术：

– 基于SSL安全数据传递技术：适用于用户域或服务域都可能不安全的应用环境。

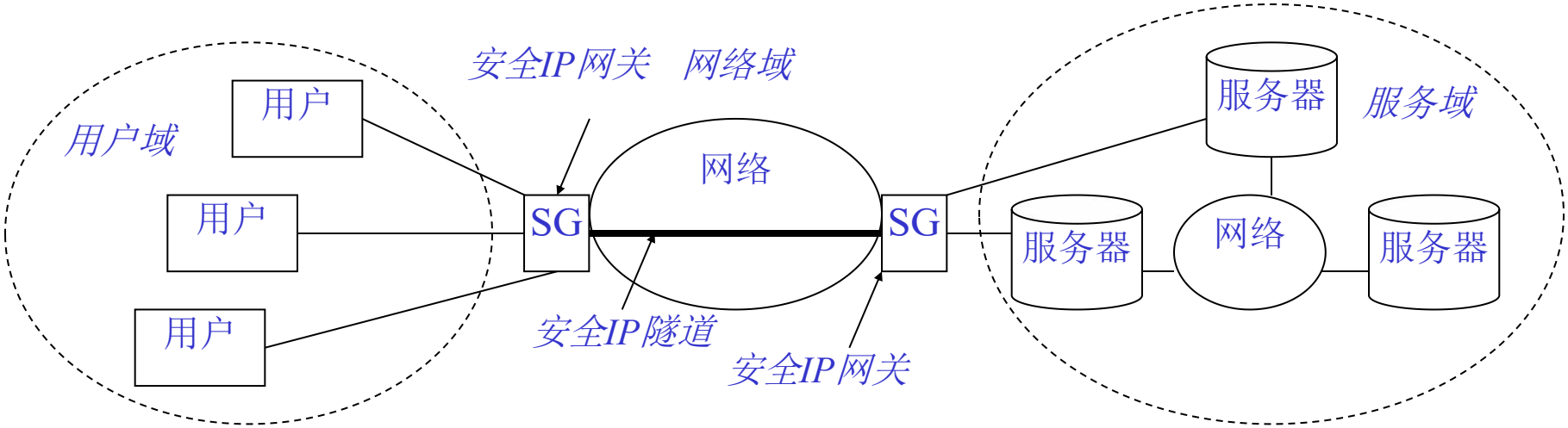


基于SSL的网络应用安全方案

网络应用保密性和完整性解决方案

（2）网络层安全技术：

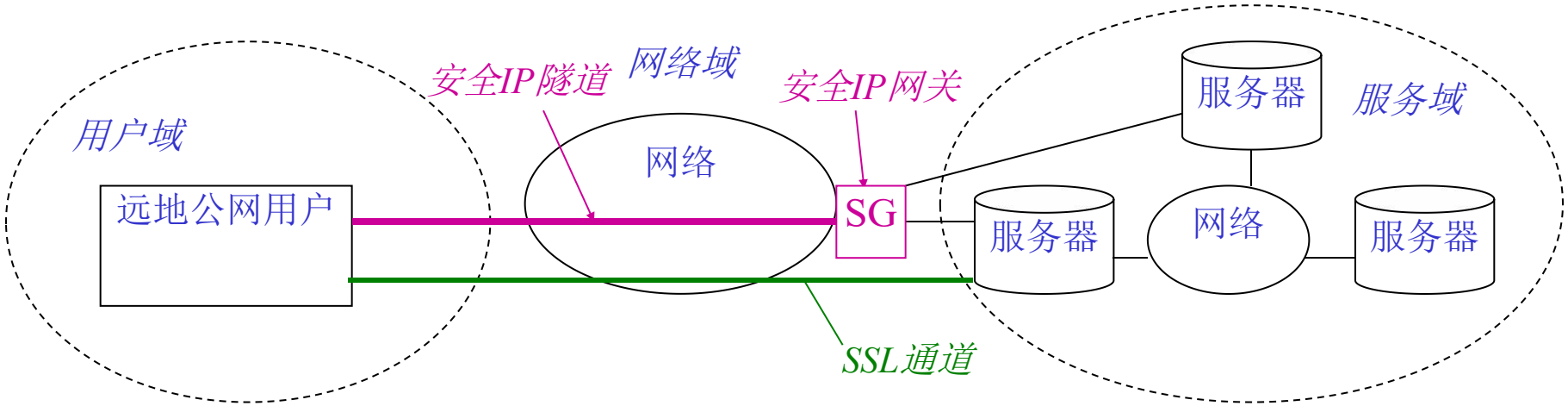
– 基于安全IP隧道的方案，适用于用户域和服务域都安全的应用环境。



基于安全IP隧道的网络应用安全方案

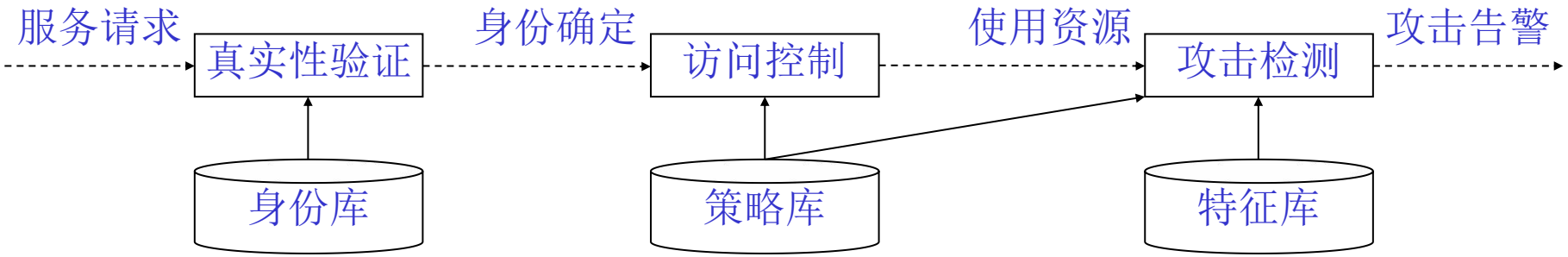
远地网络用户的安全解决方案

- 单个远地用户：可以采用基于SSL的安全方案(由应用服务提供)，也可以采用安全IP隧道 方案(由网络服务提供)。



网络应用的可用性解决方案(1)

- 网络应用安全中的可用性需要综合运用真实性验证、访问控制和攻击检测技术进行保护(防攻击技术)。
- 基于真实性验证、访问控制和攻击检测的网络应用的可用性保护模型(防攻击模型)。



网络应用的可用性保护机制

网络应用的可用性解决方案(2)

- 真实性验证的结果可能是合法的网络实体，也可能是匿名的网络实体，或者非法的网络实体对网络进行访问。
- 按照真实性验证的结果进行访问控制：
  - 如果访问控制策略表中没有匿名用户或者匿名实体项，则说明该安全系统不对匿名用户开放；
  - 如果访问控制策略表中没有指定合法用户，则说明该安全系统不对合法用户开放。
- 用户在访问网络、使用网络资源过程中，攻击检测将进行实时检测和事后检测。攻击检测是按照访问控制策略库和网络攻击特征库，采用智能算法进行的。

检测符合攻击特征的行为

检测违反安全策略的行为

电子邮件安全应用技术

- 电子邮件是因特网上使用最为普遍的网络应用之一。
- 从网络安全角度看，目前电子邮件是造成网络安全威胁的一个主要渠道。研究和开发电子邮件安全技术不仅具有很大的实用价值，而且具有较大的研究意义。
- 目前电子邮件安全技术主要解决完整地、保密地传递电子邮件。
- 目前常用的安全传递电子邮件的技术包括完美隐私(英文缩写PGP)技术和安全多用途因特网邮件扩展(S/MIME)技术。

完美隐私(PGP)技术

- 完美隐私(Pretty Good Privacy, PGP)技术是一个典型的面向网络应用的安全技术，它是报文身份验证技术和报文加密技术在电子邮件和文件存储方面具体的应用。
- PGP技术是美国麻省理工学院(MIT)软件工程师Phil Zimmermann个人发明并且推广应用的网络安全应用技术。

完美隐私(PGP)功能与应用

- PGP技术目前已经在所有常用的计算机操作系统上实现，其中既有PGP实现的自由软件，又有PGP实现的商业软件。
- PGP提供了5种与网络应用安全相关的服务：报文真实性验证、报文加密、报文压缩、安全电子邮件、以及报文分段服务。
- PGP服务也可以在网络环境下的非电子邮件应用中提供。

PGP报文真实性验证的发送方

- PGP采用SHA-1报文摘要算法与RSA公钥加密算法结合，实现对报文的真实性验证。具体的过程如下：

$$M1: A \rightarrow B: M \,||\, VK_A\{H(M)\}$$

- 说明：发送方A对报文M执行报文摘要算法SHA-1，得到H(M)，然后利用A的私钥VK_A对H(M)进行加密(数字签名)，得到$VK_A\{H(M)$，将其附加在报文M后发送给接收方B。
- 目的：杜绝假冒的电子邮件

PGP报文真实性验证的接收方

- PGP采用SHA-1报文摘要算法与RSA公钥加密算法结合，实现对报文的真实性验证，过程如下：

$$M1: A \rightarrow B: M \,||\, VK_A\{H(M)\}$$

- 接收方B收到报文M之后，利用发送方A的公钥解密报文验证码，获得发送过来的报文摘要H(M)。B同时利用SHA-1算法重新计算收到的报文M的摘要H'(M)，如果H'(M) = H(M)，则B可以验证报文M是真实的。
- 数字签名的安全性是由公钥的真实性保证，而这种真实性的保证可以通过一个实名群的公开发布实现。

PGP的报文加密方法

- PGP的报文加密方法不需要协商密钥
  - PGP的报文加密方法不采用安全IP技术和SSL安全技术中的密钥协商方法，而是利用公钥加密方法传递传统加密算法使用的对称密钥(称为会话密钥)，利用传统加密算法加密报文。
- 每个会话密钥只用于加密一个报文。所以，PGP是采用“一次一密钥”的方法加密报文，这是最为安全的报文加密方法。

PGP的报文加密过程

- PGP对报文的加密过程如下：

（1）对于某个等待发送的报文M，发送方A随机产生一个对称密钥$K_{A,B}$，并对M加密：

$$M1: A \rightarrow B: K_{A,B}\{M\} \,||\, PK_B\{K_{A,B}\}$$

（2）接收方B收到报文M1之后，首先用自己的私钥解密$PK_B\{K_{A,B}\}$，得到本次加密报文的对称密钥$K_{A,B}$，然后，再利用$K_{A,B}$解密$K_{A,B}\{M\}$，得到报文M。

PGP的报文压缩

- PGP采用ZIP算法进行报文压缩。
- PGP对报文的操作处理顺序：
  - 报文签名→报文压缩→报文加密
- 选择操作处理顺序的考虑：
  - 如果加密或压缩后签名，无法直接验证明文。
  - 压缩后加密提高加密效率及数据保密性。
  - 电子邮件加密/解密是客户端到客户端应用，客户端的身份验证无需防范DOS攻击！
- 安全IP技术的操作处理顺序：
  - 报文加密→报文签名 （防DOS攻击）
  - 安全IP技术属于网络层安全防范技术，必须防范DOS攻击

PGP的安全电子邮件服务

- 将报文加密算法和报文真实性验证算法应用于电子邮件存在的障碍：
  - 传统电子邮件系统只能传送7bits的ASCII码正文字符。
  - 加密算法和真实性验证算法都是生成以8bits为单位的任意数据流。
- 采用radix-64转换算法，将3个8bits数据转换成4个7bitsASCII码字符。

PGP的报文分段服务

- 传统因特网上的电子邮件系统会限定电子邮件的长度，为解决这个问题，PGP提供了报文分段的服务。
- 发送方PGP将较大的电子邮件分为较小的电子邮件，然后将分段后的电子邮件逐一发送出去。接收方PGP将分段电子邮件进行合段后再做其他处理。

PGP对电子邮件报文的处理流程

- 电子邮件发送方处理流程：
  - 发送用户数据 → 签名 → 报文压缩 → 报文加密 → 密文转换为ASCII码字符流 → 分段大报文 → 发送电子邮件
- 电子邮件接收方处理流程：
  - 接受电子邮件 → 报文合段 → ASCII字符流转换为密文 → 报文解密 → 报文解压缩 → 报文真实性验证 → 用户提交数据

安全MIME（1）

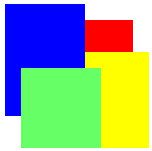
- 安全MIME
  - Multipurpose Internet Mail Extension (多用途因特网邮件扩展)
  - 是IETF指定的有关电子邮件的安全规范。虽然因特网上许多安全电子邮件软件采用PGP技术，但是，工业界倾向于采用安全MIME(英文缩写S/MIME)作为安全电子邮件产品的标准。
- 功能上与PGP基本相同。它可以支持电子邮件的加密、签名(真实性验证)和压缩。
- S/MIME提供的服务包括：安全封装服务，数字签名服务、数字签名+安全封装服务。

安全MIME(2)

- 安全封装服务可以为一个或者多个电子邮件的接收方加密任何类型的邮件内容，以及对加密邮件内容的密钥进行加密。
  - 安全封装服务并不显式提供报文真实性验证服务。(与PGP提供的加密服务相同)
- 数字签名服务就是生成电子邮件内容的报文摘要，利用签名者的私钥对报文摘要进行加密，将加密后的报文验证码(即数字签名)附在电子邮件后面，发送给接收方。

安全MIME(3)

- 数字签名和安全封装服务综合了电子邮件的数字签名和安全封装。
- S/MIME 3.1将RSA公钥加密算法作为必须实现的算法，将Diffie-Hellman密钥生成算法作为必须实现的算法。
- S/MIME 3.1将AES对称密钥加密算法作为应该实现的算法，将SHA-1作为建议应该实现的报文摘要算法。



万维网(WWW)安全应用技术

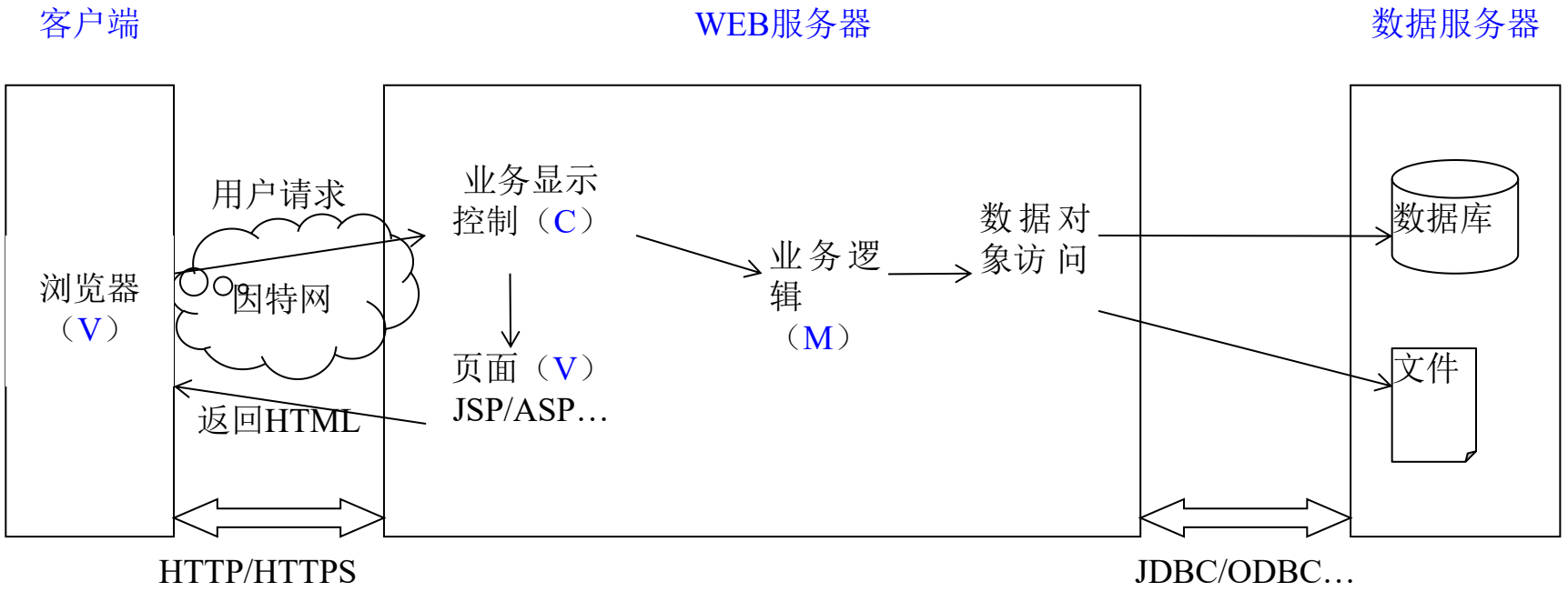
- 万维网面临的安全威胁
- 万维网安全防范技术
- 万维网攻击检测技术
- SQL（结构化查询语言）注入攻击
- XSS（跨网站脚本编写）攻击

万维网(WWW)安全技术

- 万维网应用由三个部分构成：
  - 提供万维网服务的万维网服务器
  - 使用万维网服务的万维网浏览器
  - 传递浏览器和服务器之间服务请求和响应报文的网络。
- 这三个部分都面临安全的威胁。
- 为何特别讨论万维网的安全技术？

万维网(WWW)应用系统框架

- 基于MVC（Model-View-Controller, 模型-视图-控制器)设计模式的万维网应用系统框架



基于MVC模式的万维网应用系统框架

万维网服务器安全漏洞

- 万维网服务器安全漏洞主要源于两个方面：

  其一，万维网服务器软件错误产生的安全漏洞

  其二，万维网服务器配置不当产生的安全漏洞

- 这些安全漏洞都会允许远地网络用户非法进入万维网服务器，窃取非公开的数据和文件，执行非授权的修改系统的命令，发起“拒绝服务”攻击，使得万维网服务器泄露敏感数据或处于“不可用”状态。

针对万维网服务器的攻击举例

（1）身份真实性验证类攻击：以攻击万维网服务器的真实性验证系统为目标。如：

- 穷举口令类攻击
- 破译弱强度口令类攻击
- 口令恢复验证类（保密问题或口令暗示）攻击

针对万维网服务器的攻击举例

（2）授权访问类攻击：以攻击万维网服务器的访问控制系统为目标。例如：HTTP会话劫持攻击。

- 用户第一次通过身份真实性验证与web服务器建立连接后，服务器会产生一个会话标识S-ID保存在cookie中，以此作为后续通信的验证信息来区别各类用户的访问权限。
- 攻击者可以通过ARP(地址解答协议)等欺骗手段，将双方交互的报文发送至攻击者，截获S-ID，冒充真实的用户获取非法的授权访问能力，劫持已建立的会话。

针对万维网服务器的攻击举例

（3）注入代码类攻击：以攻击万维网服务接口为目标。

– SQL注入、SSI注入、Xpath注入、LDAP注入等， 如：

select * from products where productID = ‘+用户输入ID号+’

如果用户输入16，则该语句在执行时变为：

Select * from products where product_id = ‘ 16 ‘

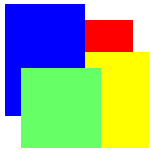
数据库会将ID为16的商品信息返回给用户。

如果攻击者输入： ’ or ‘1’=‘1 结果？获取所有商品信息

select * from products where ‘’ or ‘1’=‘1’

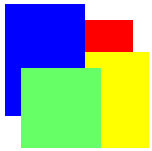
针对万维网服务器的攻击防范措施

- 针对服务器验证类攻击，可以采用强用户密码、限制猜测次数、多类型真实性验证机制等防范措施。
- 针对授权访问控制类攻击，可以采用基于角色的访问控制、cookie加密传输等防范措施。
- 针对注入代码类攻击，可以采用输入数据强验证等防范措施。
  - 软件编程人员一定要养成对于所有输入数据进行检查的编程习惯，这样才能编制出“可信”软件



安全漏洞的不可避免性

- 根据目前的软件技术水平，复杂而庞大的软件系统一定会有软件错误。万维网应用就是一个复杂而庞大的软件系统，确实已经发现了不少软件错误。
- 复杂而庞大的软件系统配置相应也比较复杂，很容易产生配置错误。
- 在这种软件错误和配置错误存在的情况下，对万维网服务器进行安全保护，是一项目前尚没有成熟的技术，只能通过一些技巧处理。
  - 无论是软件研究，还是软件开发都有很多机会。

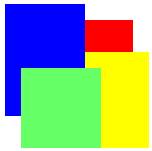


对浏览器的安全威胁

- 万维网浏览器是在公共互联网上发现、浏览和下载所有万维网服务器上有价值信息的客户端。
- 由于现在浏览器都支持Java语言和Java脚本这类移动代码编制的程序（注：这也是网络传播的恶意代码编制的方法），这些程序可以在浏览器上运行。
- 如果这些程序中嵌入恶意代码，则会渗透到浏览器所在的计算机系统、窃取浏览器所在的计算机系统中用户的敏感数据、僵尸化、或破坏该计算机系统。

SQL注入攻击定义

- SQL（结构化查询语言）注入攻击，是目前最为有效的入侵网站数据库、窃取用户敏感信息的攻击。
- SQL注入攻击：利用万维网应用软件（主要指与数据库相关的SQL编程语言）中没有严格过滤或验证输入数据而产生的漏洞，通过万维网应用提供的SQL的用户参数输入的功能，注入恶意代码。
- SQL注入攻击目的：窃取网站上的用户登录账户和密码，进一步假冒网站合法用户登录网站；直接窃取网站后台数据库的敏感数据。



SQL注入攻击分类

按照注入SQL命令不同，SQL注入攻击可分成以下类型：

- SQL操纵类攻击，利用不同的SQL操作，例如SQL的条件判断语句操作，修改SQL语句的攻击过程。
  - 例如：通过更改WHERE语句的相关判定条件，使得WHERE语句总是为真，或者总是为假，实现SQL注入。
- 语句插入类攻击，插入新的SQL语句的攻击过程。这类攻击方式仅当单个数据库的查询请求支持多个SQL语句时才能够发起攻击。
  - 例如在易攻击的SQL语句后面附加一个SQL服务器的EXECUTE（执行）命令。

SQL注入攻击分类(续)

- 功能调用类攻击，在某个易攻击的SQL语句中插入不同数据库功能调用的攻击过程。这些插入的功能调用可以发起操作系统的调用或者操纵数据库中的数据。
- 缓存溢出类攻击，针对网络应用软件的漏洞常用的一类攻击。在SQL注入攻击中，这类攻击借助于SQL的功能调用注入，利用系统中的漏洞，导致缓存溢出，进而发起攻击。
  - 这类攻击仅仅对存在漏洞、并且没有及时打补丁的服务器才能发起有效的攻击。

重复式查询的SQL攻击

- 重复式查询属于SQL操纵类攻击，攻击者可以基于SQL的条件语句，在查询语句中注入恶意代码。例如一个登录的查询如下：

SELECT * FROM User_Info WHERE UserName = 'Bob' and Password='123456'.

- 在这条登录查询语句中，可以注入OR 1=1'，结果的登录查询语句如下：

SELECT * FROM User_Info WHERE UserName = 'OR 1=1';-- and Password='123456'.

逻辑错误查询的SQL攻击

- 逻辑错误查询也属于SQL操纵类攻击，在这类攻击中，攻击者利用数据库服务器返回的出错消息，获取有关数据库内部的敏感信息。
- 例如以下查询语句可获取有关数据库表结构的敏感信息，例如数据库的表名、表的属性名（表的列名）等信息。

SELECT * FROM User_info WHERE UserName = ' HAVING 1=1';-- and Password='123456'.

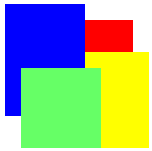
  - 返回出错消息“*列 'User_info.UserID' 在选择列表中是无效的，因为它既没有包含在一个汇聚函数中，也没有包含在GROUP BY语句中.*”，由此可获得该数据库的表名：User_info，以及该表对应的属性名：User_info.UserID

合并查询的SQL攻击

- 合并查询属于语句插入类和SQL操纵类组合攻击。它在安全的查询上附加恶意代码，用于获取其他的表信息。例如可以获取表属性的数据类型信息。例如数据库服务器执行以下的查询语句：

```
SELECT * FROM User_info WHERE UserName = ' UNION
SELECT SUM(Username) from User_info-- BY UserID
HAVING 1=1';-- and Password='123456' .
```

- 返回出错消息："*对于SUM操作符，操作数的数据类型VARCHAR无效.*"，该出错消息就泄露了Username的数据类型是VARCHAR的信息。



背驮式查询的SQL攻击

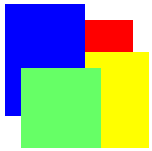
- 背驮式查询攻击属于语句插入类攻击。攻击者在传统的查询语句中注入恶意代码，并且也执行数据库操纵类操作，例如INSERT（插入）、UPDATE（更新）、DELETE（删除）语句，操纵某个数据库中的记录。例如以下查询语句：

```
SELECT * FROM User_info WHERE UserName =
';INSERT INTO User_info VALUES('Bob','123'}-'
```

- 这样就可将某个非法的记录插入到数据库的User_info表中。

真实性验证防范SQL攻击

- 基本思路：SQL注入攻击中的SQL语句都是假冒的SQL语句，通过在SQL语句中关键操作符和用户相关信息进行加密，防范假冒的SQL语句，以此防范SQL注入攻击。
- 具体方案：每个用户赋予一个传统加密算法的密钥，服务器则赋予用于公钥加密算法的公钥和私钥。对于SQL的登录查询，采用两级加密：
  - 采用传统加密算法和用户的密钥，加密用户名和登录密码；
  - 采用公钥加密算法和服务器公钥，加密查询模式。

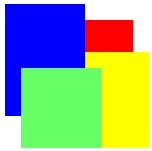


真实性验证防范SQL攻击(续)

- 执行过程包括三个阶段：
  - 注册阶段，用户注册服务器，获得赋予的用户密钥；
  - 登录阶段，采用加密算法加密SQL登录查询语句；
  - 验证阶段，服务器接收到用户的SQL登录查询语句之后，通过解密算法进行SQL登录查询语句的真实性验证。
- 只有通过真实性验证的SQL登录查询语句，才提交SQL服务器执行，以此防范SQL注入攻击。经过测试，这种真实性验证方案十分有效，加密和解密过程可以在不到一秒钟时间内完成。
- 方案的不足：无法防范基于链接的SQL注入攻击；难以维护客户端的传统加密算法的密钥、以及服务器端的公钥加密算法的密钥；在注册阶段缺少安全保护机制。

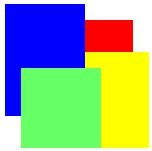
SQL查询属性值移除方案

- 基本思路：在用户提交的SQL查询语句的属性值中，移除SQL查询语句的方案，消除攻击者通过SQL查询语句属性值的代码注入，防范某种类型的SQL注入攻击。
- 采用“异常检测”的方法，通过统计分析，获取正常用户的SQL查询的特征样本(查询简本)。通过正常用户的SQL查询简本与攻击者动态产生的SQL查询进行比对，检测并识别SQL注入攻击。
- 方案不足：采用统计方法获取正常用户使用SQL查询的行为特征，行为特征描述不完整、不准确，可能产生误判，影响正常的SQL查询操作。



跨网站脚本编写(XSS)的攻击

- 跨网站脚本编写(Cross-Site Scripting, XSS)是另一种常见的万维网应用攻击技术，通过用户浏览网页，或者用户点击网页中的链接，将攻击者的恶意代码传回到该用户的浏览器或客户端。
- 包括恶意代码的脚本将在该用户浏览器的安全区域运行，可以读取、更改、传送该浏览器可以访问的任何关键数据。



XSS攻击的分类

- XSS攻击可以分成两类：持续式XSS和非持续式XSS
  - 当恶意代码成功地植入某个万维网应用（网页邮箱、论坛等）中，则就会出现存储式/持续式XSS攻击。持续式XSS攻击不需要引诱用户点击任何网络的链接。
  - 当服务器没有很好地检测和清除万维网页面中隐藏的恶意网络链接时，就可能发生反应式或非持续式XSS攻击。恶意链接包含的恶意代码，在用户点击后就可以下载到用户的浏览器并且运行，使得攻击者可以获取用户敏感的数据

XSS攻击举例

（1）持续式XSS攻击

例如：跨站点脚本攻击

跨站点脚本攻击过程

XSS攻击举例(续)

（2）非持续式XSS攻击

例如：某页面所在地址为

<frame src = ”http://truth.example/file.html ”>

该地址也可以通过URL参数形式定义为

http://truth.example/page?frame_src=http://truth.example/file.html

攻击者可以将frame_src参数替换为

<frame_src=http://attacker.example/spoof.html>

当用户点击链接后

浏览器地址栏中显示http://turth.example

而实际链接却指向了http://attacker.example。

万维网浏览器的攻击防范措施

- 利用浏览器防火墙或其他安全工具，过滤试图利用浏览器漏洞侵入计算机的恶意代码和病毒。此外，用户应及时更新浏览器软件，培养良好的安全浏览习惯。
- 从浏览器角度防范恶意代码，属于端系统防范网络攻击问题，是目前比较难以解决的安全问题。很大程度上依赖于用户的自觉和自律。

针对传输网络的安全威胁

- 网络的安全威胁来自于对万维网浏览器和服务器之间传递数据的窃听、篡改、假冒和重播报文攻击。这也是网络安全最主要研究的问题。

基于SSL/TLS的攻击防范措施

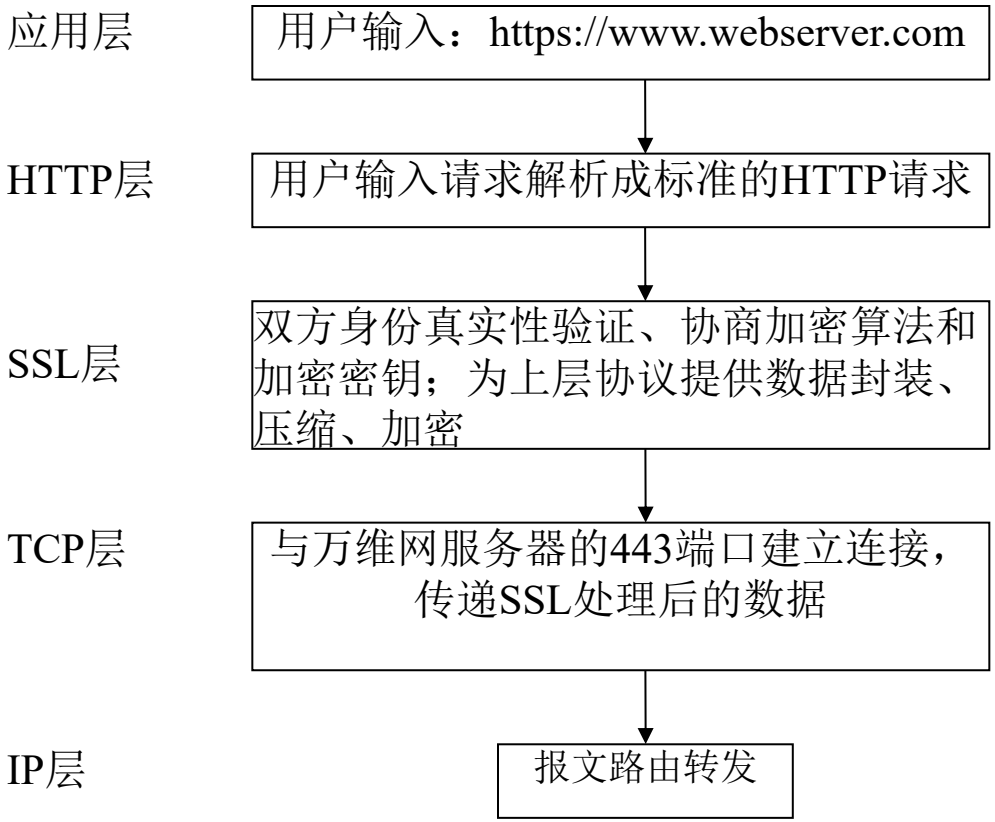
- 这方面目前已有比较有效的安全技术。例如，传送层安全技术中的安全套接层(SSL)技术就是针对万维网浏览器和服务器之间保密、完整地进行数据交互而设计的。
- 传送层安全协议（TLS）建立在SSL 3.0协议规范基础上，1999年IETF将其标准化为RFC2246 (TLS1.0)，后又标准化RFC4346 (TLS1.1)，最新标准化RFC5246(TLS1.2)。TLS独立于应用协议，采用的密码算法与SSL不同，侧重于对安全性的改进。

攻击防范措施的具体应用

- 在万维网环境下，重要数据通常采用安全超文本传送协议（HTTPS，Hypertext Transfer Protocol Secure）进行传送，它在不安全的互联网络上构建了一个安全通道。
- HTTPS是HTTP协议和web安全传送协议的联合体，它将SSL协议或TLS协议作为HTTP协议的可选安全子层，对用户请求页面和web服务器返回页面进行加密和解密，有效防范窃听、篡改、假冒、重播和中间人攻击。

HTTPS客户端处理流程

- HTTPS使用443端口，而不是HTTP的80端口与下层协议通信。
- 采用SSL协议提供web安全传送服务的HTTPS客户端协议栈处理流程如图所示：



HTTPS客户端协议栈处理流程

万维网服务的保密性和完整性

- 保证万维网服务的保密性和完整性技术比较成熟。可以采用在前面介绍的SSL技术或TLS技术，在万维网浏览器和服务器之间建立一条秘密通道，所有在浏览器和服务器之间传递的报文都经过加密和签名后才在网络环境下传递。
- 浏览器用户保管好自己的私钥，就可以防范网络攻击者对万维网浏览器和服务器之间传递数据的窃听、篡改、假冒和重播攻击。

万维网服务的可用性

- 目前的网络安全技术尚不能保证万维网服务器、浏览器和网络的可用性。即无法完全防范“拒绝服务”类的网络攻击、以及探测系统漏洞的“网络蠕虫”攻击。
- 目前对网络最大的安全威胁来自于分布式“拒绝服务”攻击，和“网络蠕虫”攻击。
- 目前设计了一些保护万维网浏览器和服务器可用性的技术。

保障万维网服务器的可用性

- 在公共万维网服务器前端设置一个万维网服务器防火墙，用于过滤异常的万维网服务请求，保护万维网服务器不受“拒绝服务”这类攻击。
- 万维网防火墙是专门针对万维网服务器设计的一个访问控制系统，它本身携带安全策略库和审核数据库，用于控制进出万维网服务器的报文。
- 比一般的网络防火墙针对性强，可以制定较为详细的、有针对性的安全控制策略，并且可以通过及时调整安全控制策略，防范潜在的网络攻击。

保障万维网浏览器的可用性

- 防范措施：用于过滤进入浏览器的数据，包括Java脚本等移动代码，通过特征分析剔除可能的恶意代码。 例如：

（1） 管住自己，不要随意访问不熟悉的网站；

（2） 禁用ActiveX插件、控件和Java脚本

（3） 安装防病毒软件

（4） 注册表加锁

（5） 禁用远程注册表操作服务

（6）及时升级万维网浏览器或选用安全浏览器

区块链及其应用

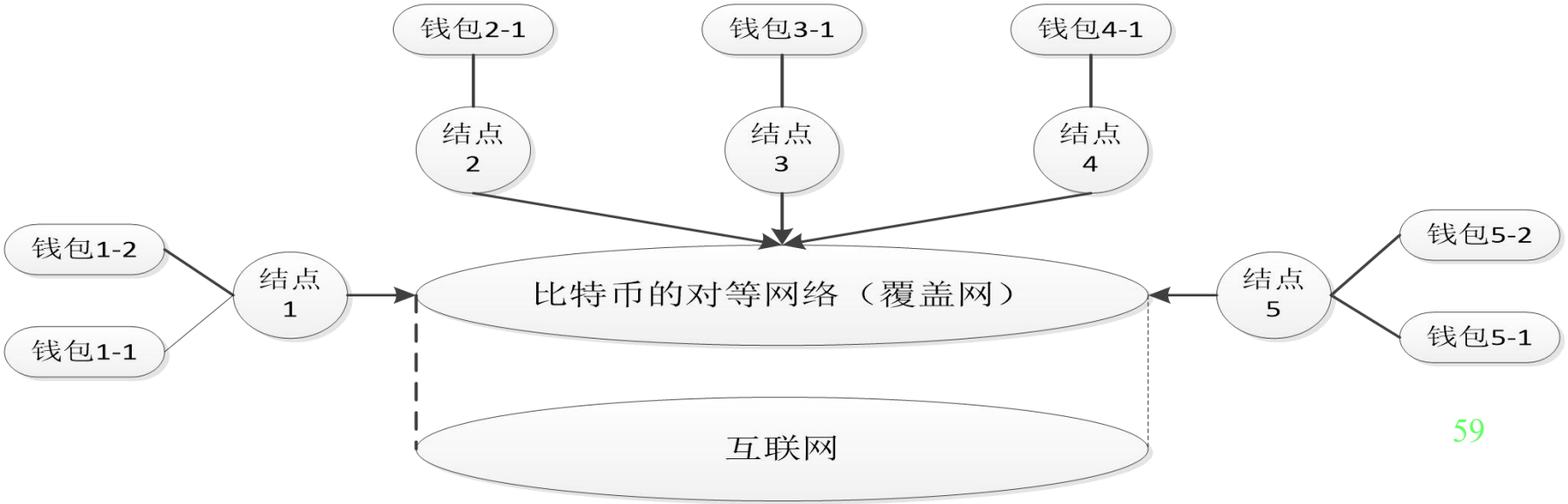
- 比特币与区块链
  - 比特币是全球首先成功使用区块链构建的去中心化数字货币系统
- 区块链的“块”和“链”
  - 区块链的“块”是具有真实性验证能力的块
  - 区块链的“链”是具有真实性验证能力的链
- 区块链的应用
  - 比特币是区块链在金融领域的成功应用
  - 区块链可以在互联网其他领域得到应用
  - 区块链应用目标：去中心化的信任管理

面向比特币的区块链概念和原理

- 起源：区块链不是现在的网络权威或者网络安全权威发明的，而是由自称为“中本聪”的一个人或一个团队，在构建全球去中心化数字货币体系——比特币的过程中设计和实现的一种去中心化的信任管理机制。
- 基础：面向比特币的区块链分析是研究区块链的基础。目前最为成功的区块链应用就是比特币系统，这个去中心化的互联网数字货币系统已经正常运行将近十年。

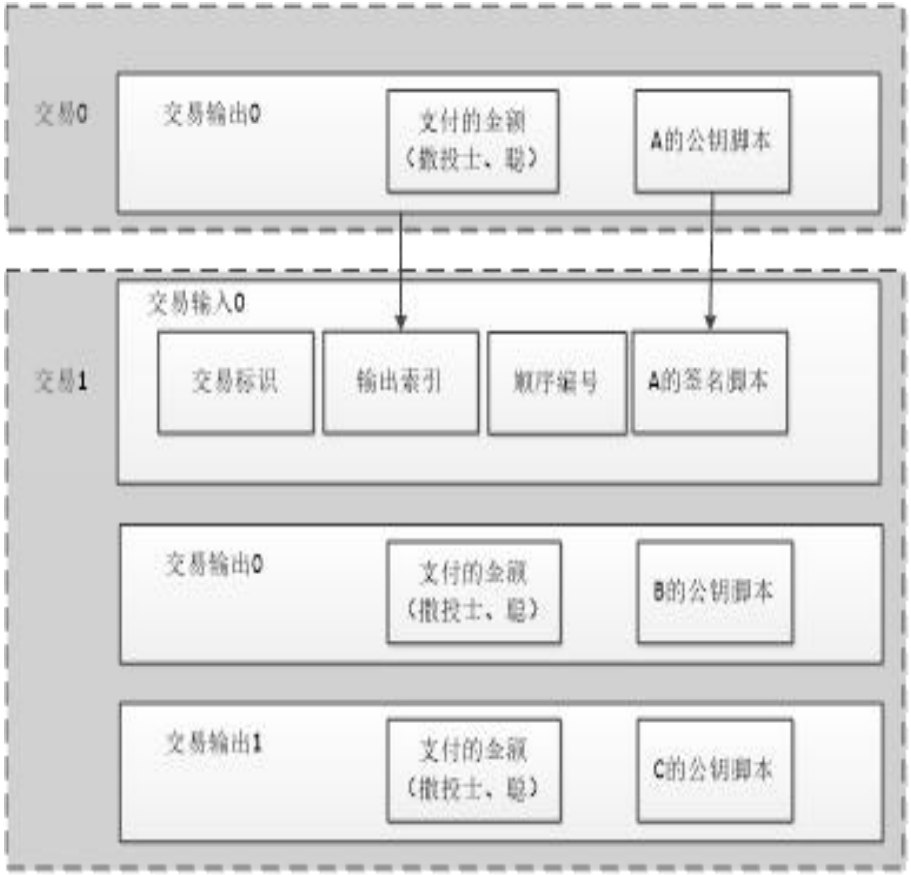
比特币的网络和对等结点

- 构建对等网络：比特币系统是基于互联网的对等网络、用于数字货币交易的网络数字货币应用系统
- 对等结点的交易：通过在对等网络上广播比特币的交易，提交比特币系统其他结点验证完成的交易
- 通告一次成功的“淘金”：广播已经验证成功的块



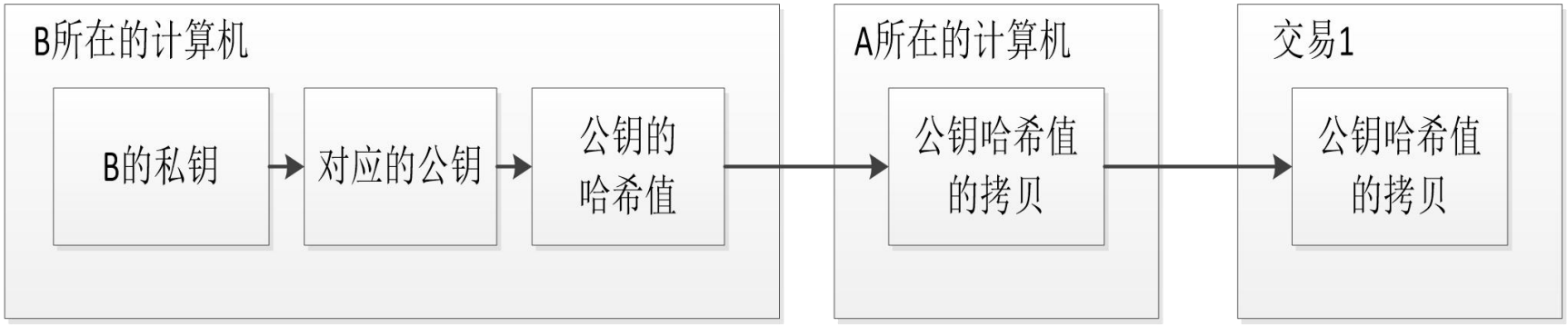
比特币的交易

- 比特币的交易就是将一定数额的比特币从一个钱包转移到另一个或多个钱包的过程。并通过交易输入和交易输出记录过程。
- 每个交易可以有多个输入，也可以有多个输出。每个交易输入通过数字签名验证这个交易输入有权使用比特币，每个交易输出必须明确指示接收比特币的目的钱包



比特币的钱包

- 钱包：比特币系统中定义的概念，在比特币的用户参与交易之前，用户首先要在比特币的系统中创建自己的“钱包”，这个虚拟钱包由一对公钥和私钥构成。
- 作用：用户运行钱包程序，生成钱包的私钥，并基于私钥推导出公钥；将钱包公钥的哈希值作为钱包的地址，接收付给自己的比特币；采用钱包私钥的数字签名，花费钱包里的比特币。



比特币：去中心化数字货币系统

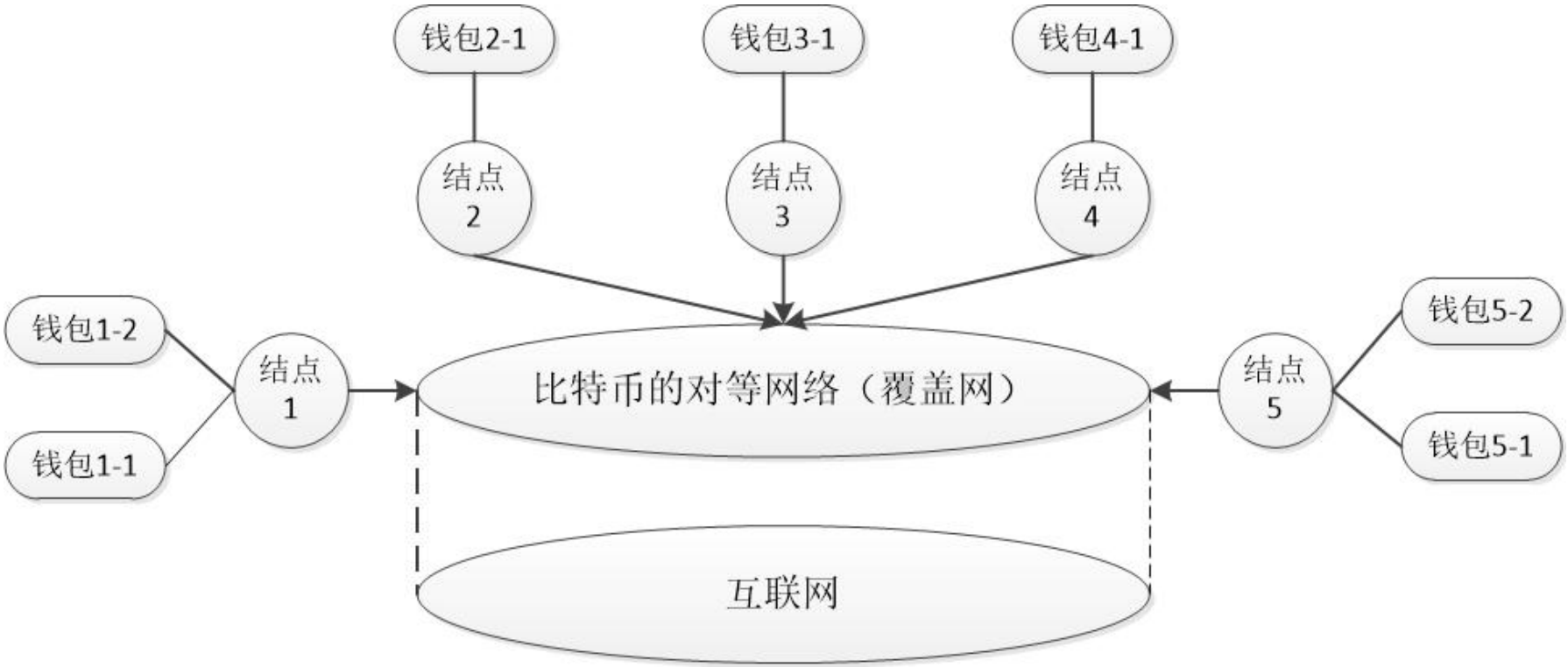
- 比特币是一种基于互联网之上的覆盖网络、采用分布式控制方法构建的自治的、网络数字货币系统。
- 每个比特币系统的结点采用对等网络(P2P网络)方式接入比特币的网络，构成了一个对等的比特币的应用网络。
- 每个比特币系统的用户通过设立自己的钱包，将自己的公钥作为钱包地址，用于接收比特币；采用数字签名，花费自己钱包的比特币。
  - 用户在比特币系统结点设立钱包时获取密钥对，无需PKI。

比特币与区块链

- 比特币系统巧妙地集成了四十多年来在密码学、数据真实性验证、以及对等网络等方面的已有研究成果，采用高度复杂的、原创的、实际可用的方法解决了去中心化的数字货币的女巫攻击和重复花费的难题。
  - 重复花费（双花）：将一个数字货币花费两次或多次
  - 女巫攻击：单个实体假冒多个实体投票，形成假冒多数
- 比特币系统采用区块链解决以上两个难题：
  - 采用对等网络通告所有交易，通过区块链记录有效交易
  - 当区块链出现分叉时，选择最长链；利用工作证明方式限制每个实体投票(验证)数目，防范假冒的有效交易验证。

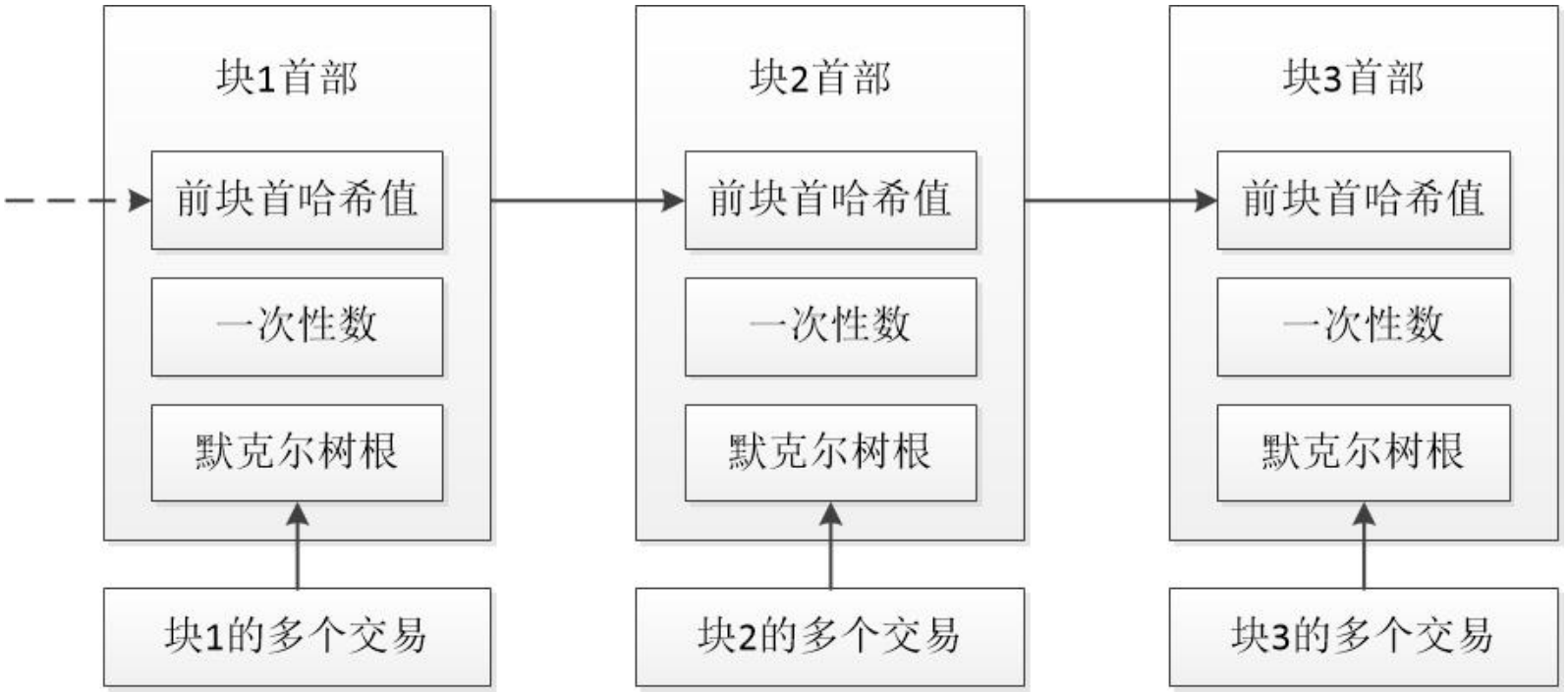
比特币系统的示意图

- 结点就是一台连接到比特币对等网络系统的计算机
- 每个结点可以有多个钱包



区块链是比特币的公共账本

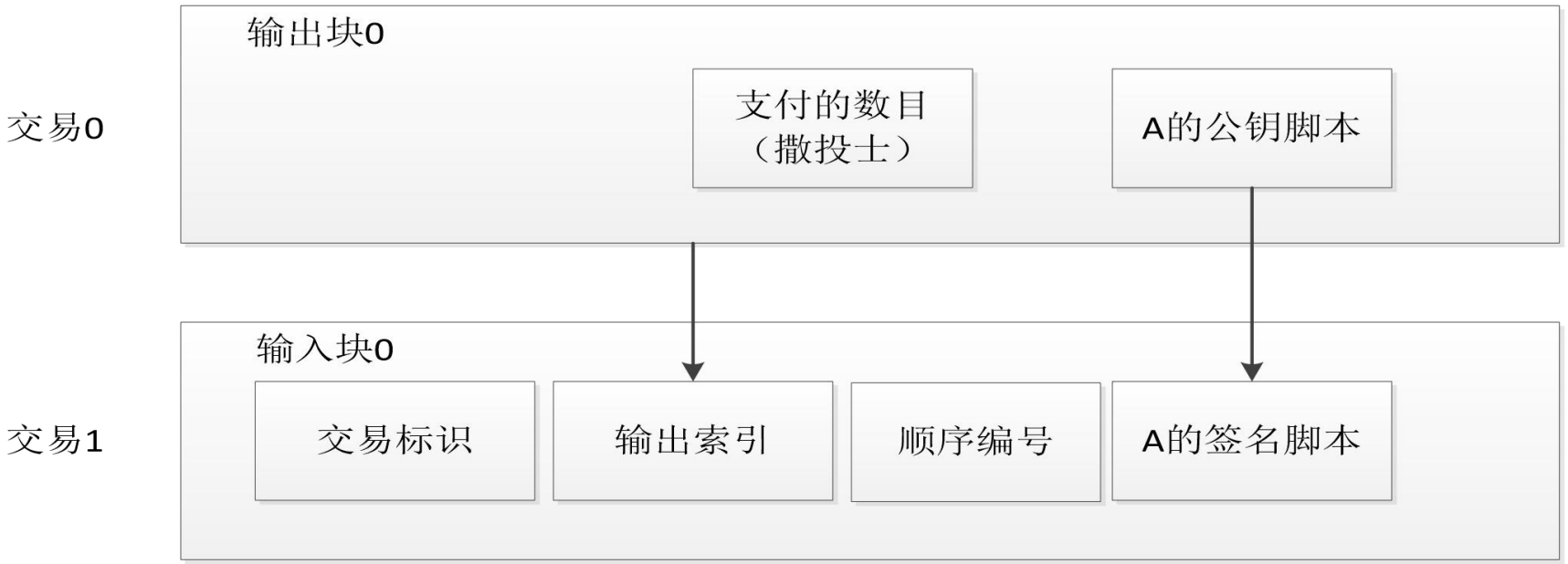
- 区块链记录比特币的所有的交易账单。
- 比特币系统的每个结点保存和维护有效的所有区块链。
- 每个块记录了一次或多个交易。



输入块和输出块——交易

- 输入块验证拟花费的比特币钱包所有者
- 输出块指定拟支付的比特币数目和对象

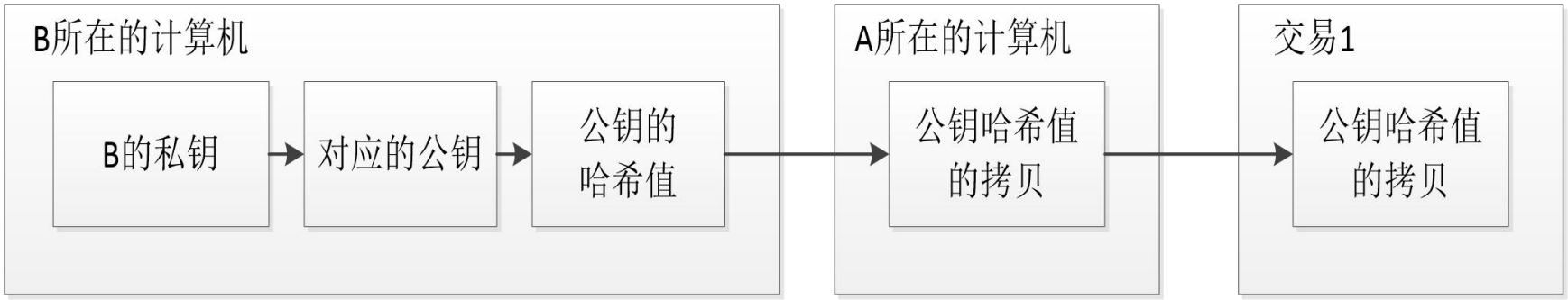
输出块举例：支付给A的公钥脚本



输入块举例：花费支付给A的输出块

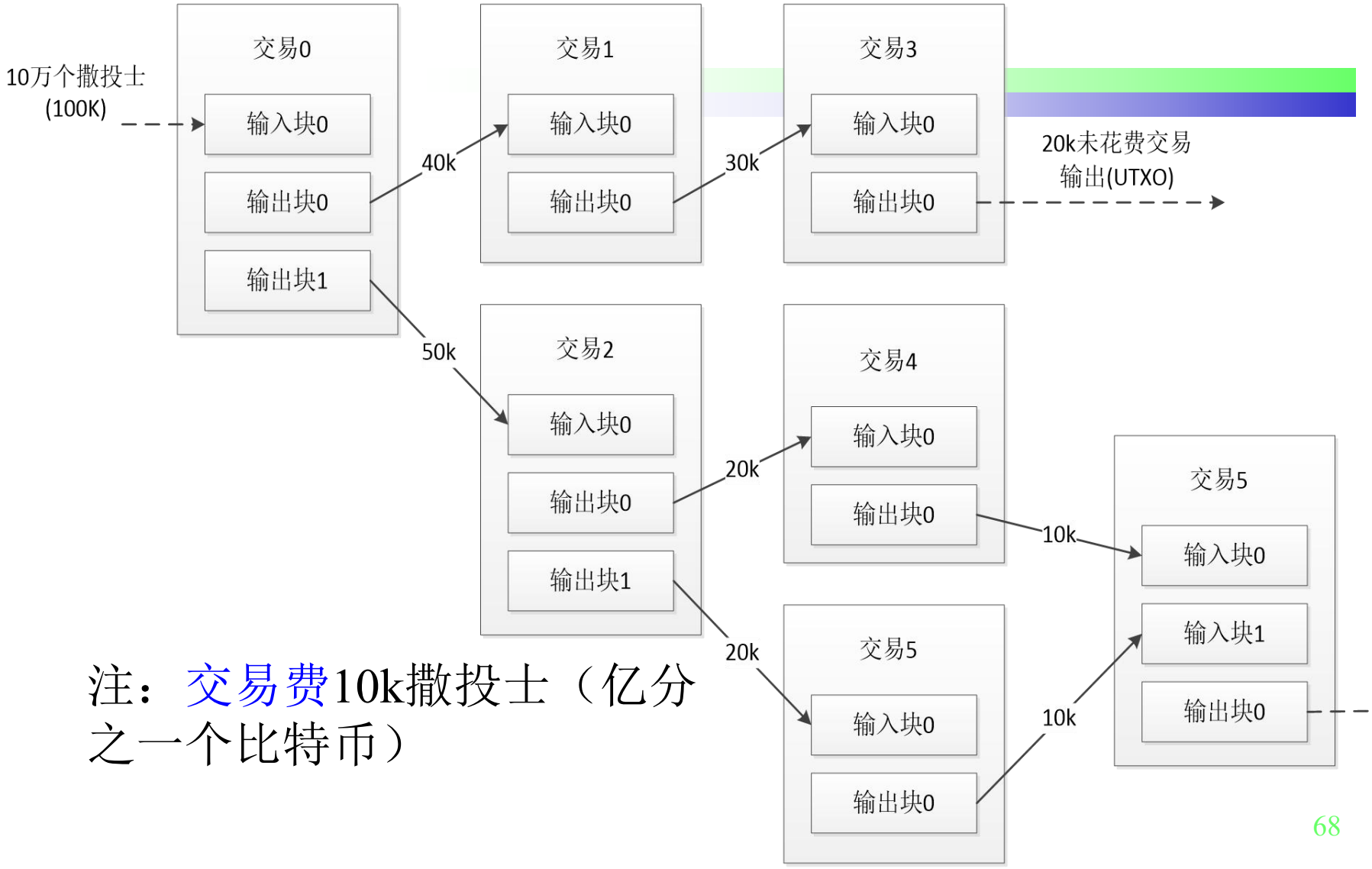
比特币的交易类型

- 付给公钥哈希值（P2PKH）是一种标准的交易类型：利用接收方公钥作为地址
- 付给脚本哈希值（P2SH）交易是2012年提出的标准交易，使得支付方可以把赎回的脚本也包括在哈希值内。



付给公钥哈希值（P2PKH）交易（A付给B）的示意图

一个典型交易的举例



注：交易费10k撒投士（亿分之一个比特币）

工作证明：防止二次使用比特币

- 工作(量)证明（POW）是一个低于某个目标值的哈希值的尝试过程(淘金，也称挖矿)，它必须通过执行一定数量的计算才能获得。
- 比特币的工作证明充分利用了密码哈希算法中的随机特性，使得对于哈希值对应的数据有任何修改或者重新执行哈希运算，只会产生新的哈希值。
- 由于可能在不同计算时间，产生不同的哈希值，所以，最为困难的事情是找到低于某个值(目标值)的块首哈希值——不断修改“一次性数”，进行淘金

在物联网隐私保护中应用

- 采用对等系统设计方法，可以从设计层面解决物联网的隐私保护问题。而区块链是作为构建这类具有隐私保护的、对等系统的技术。
- 区块链被作为防止篡改的、存放真实数据的技术。基于这种考虑，所以，区块链技术被应用于医院的医疗记录保存、艺术品的拍卖、以及房地产的销售等。
- 物联网的一种隐私保护涉及方案：区块链+对等存储系统
- 与对等存储系统结合，区块链可以注册和真实性验证对物联网装置数据的所有操作，无需将数据托管给服务器。

[参考文献] Marco Conoscenti; Antonio Vetrò; Juan Carlos De Martin. Blockchain for the Internet of Things: A systematic literature review. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016: 1 – 6.

在物联网中应用的疑问

- 其一：是否物联网一定需要一个无信任中心的网络？如果无信任中心，则物联网服务由谁提供？物联网服务如何收费？
- 其二，比特币中的区块链是依赖于“工作证明”达成共识，而取得对于交易的信任。这种“工作证明”需要花费巨大的计算资源，物联网计算资源不富裕的装置，能够采用这种信任方法吗？
- 其三，如果不采用比特币分布式竞争的共识规则，则在物联网环境下可以采用何种轻量级的、满足物联网应用需求的“共识规则”？

在物联网中应用的疑问(续)

- 其四，比特币的系统中的可信概念，是物联网应用需要的可信概念吗？比特币的系统毕竟属于网络数字货币系统，比特币系统需求的“可信”具有“金融”意义的含义，而物联网的可信更多应该是可靠、稳定、可适应、可恢复的概念。
- 其五，物联网上一定需要“智能合同”吗？物品与物品之间的交互是依赖物品之间的合同进行的吗？这种“合同”与物联网讨论的“服务协商”是一个概念吗？

区块链应用的建议

- 应用区块链技术应该针对特定应用领域的去中心化信任管理需求，明确需要解决的问题。
- 在解决问题中，要灵活应用区块链综合的数据加密、真实性验证、对等网络的技术和实现方法，而不可拘泥于比特币系统中采用的区块链相关方法。
- 面向物联网的区块链应用，更加侧重于去中心化的数据可信管理，必须解决数据可信自动(必须限制可能的人工介入)采集、传递和存储的技术问题。