 

**课程报告**

|  |  |
| --- | --- |
| **课程名称：** | **企业软件项目实训** |
| **学生姓名：** | **刘浩龙** |
| **学生学号：** | **201630191933** |
| **学生专业：** | **软件工程** |
| **开课学期：** | **2018-2019第二学期** |

**软件学院**

**2019年6月**

**目录**

[**1** **区块链技术原理** 3](#_Toc13254804)

[**1.1** **什么是区块链** 3](#_Toc13254805)

[**1.2** **区块和链** 3](#_Toc13254806)

[**1.3** **分布式结构——开源的、去中心化的协议** 5](#_Toc13254807)

[**1.4** **非对称加密算法** 6](#_Toc13254808)

[**1.5** **脚本** 6](#_Toc13254809)

[**2** **公有链、联盟链和私有链的异同** 7](#_Toc13254810)

[**2.1** **公有链** 7](#_Toc13254811)

[**2.2** **联盟链** 7](#_Toc13254812)

[**2.3** **私有链** 8](#_Toc13254813)

[**2.4** **总结** 8](#_Toc13254814)

[**3** **可信计算和信任链** 9](#_Toc13254815)

[**3.1** **可信的定义和属性** 9](#_Toc13254816)

[**3.2** **信任的度量和模型** 9](#_Toc13254817)

[**3.3** **信任根和信任链** 10](#_Toc13254818)

[**3.4** **可信计算研究的发展** 10](#_Toc13254819)

[**3.4.1** **可信计算初现** 10](#_Toc13254820)

[**3.4.2** **可信计算高潮** 10](#_Toc13254821)

[**3.4.3** **可信计算在中国** 11](#_Toc13254822)

[**3.5** **可信计算研究的发展趋势** 11](#_Toc13254823)

[**3.5.1** **可信计算面临的挑战** 11](#_Toc13254824)

[**3.5.2** **可信计算待研究的领域** 12](#_Toc13254825)

[**3.6** **总结** 12](#_Toc13254826)

1. **区块链技术原理**
   1. **什么是区块链**

区块链（ BlockChain ）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。该技术方案主要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（ block ），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其信息的有效性和链接（ chain ）下一个数据库块。

通俗一点说，区块链技术就指一种全民参与记账的方式。所有的系统背后都有一个数据库，也就是一个大账本。那么谁来记这个账本就变得很重要。目前就是谁的系统谁来记账，各个银行的账本就是各个银行在记，支付宝的账本就是阿里在记。但现在区块链系统中，系统中的每个人都可以有机会参与记账。在一定时间段内如果有新的交易数据变化，系统中每个人都可以来进行记账，系统会评判这段时间内记账最快最好的人，将其记录的内容写到账本，并将这段时间内账本内容发给系统内所有的其他人进行备份。这样系统中的每个人都了一本完整的账本。因此，这些数据就会变得非常安全。篡改者需要同时修改超过半数的系统节点数据才能真正的篡改数据。这种篡改的代价极高，导致几乎不可能。例如，比特币运行已经超过 7 年，全球无数的黑客尝试攻击比特币，但是至今为止没有出现过交易错误，可以认为比特币区块链被证明是一个安全可靠的系统。

* 1. **区块和链**

关于如何建立一个严谨数据库的问题，区块链的办法是：将数据库的结构进行创新，把数据分成不同的区块，每个区块通过特定的信息链接到上一区块的后面，前后顺连来呈现一套完整的数据，这也是“区块链”这三个字的来源。

区块（ block ）：在区块链技术中，数据以电子记录的形式被永久储存下来，存放这些电子记录的文件我们就称之为“区块（ block ）”。区块是按时间顺序一个一个先后生成的，每一个区块记录下它在被创建期间发生的所有价值交换活动，所有区块汇总起来形成一个记录合集。

区块结构（ BlockStructure ）：区块中会记录下区块生成时间段内的交易数据，区块主体实际上就是交易信息的合集。每一种区块链的结构设计可能不完全相同，但大结构上分为块头（ header ）和块身（ body ）两部分。块头用于链接到前面的块并且为区块链数据库提供完整性的保证，块身则包含了经过验证的、块创建过程中发生的价值交换的所有记录。



区块结构有两个非常重要的特点：第一，每一个区块上记录的交易是上一个区块形成之后、该区块被创建前发生的所有价值交换活动，这个特点保证了数据库的完整性。第二，在绝大多数情况下，一旦新区块完成后被加入到区块链的最后，则此区块的数据记录就再也不能改变或删除。这个特点保证了数据库的严谨性，即无法被篡改。

顾名思义，区块链就是区块以链的方式组合在一起，以这种方式形成的数据库我们称之为区块链数据库。区块链是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到区块链的网络中来。

区块链是如何做到的呢？由于每一个区块的块头都包含了前一个区块的交易信息压缩值，这就使得从创世块（第一个区块）到当前区块连接在一起形成了一条长链。由于如果不知道前一区块的“交易缩影”值，就没有办法生成当前区块，因此每个区块必定按时间顺序跟随在前一个区块之后。这种所有区块包含前一个区块引用的结构让现存的区块集合形成了一条数据长链。“区块 + 链”的数据存储结构如下图所示。



我们引用《区块链：互联网金融的终局》（肖风）的一段话来总结区块链的基本结构：“人们把一段时间内生成的信息（包括数据或代码）打包成一个区块，盖上时间 戳，与上一个区块衔接在一起，每下一个区块的页首都包含了上一个区块的索引数据，然后再在本页中写入新的信息，从而形成新的区块，首尾相连，最终形成了区块链。”这个结构的神奇之处：区块（完整历史） + 链（完全验证） = 时间戳

“区块 + 链”的结构为我们提供了一个数据库的完整历史。从第一个区块开始，到最新产生的区块为止，区块链上存储了系统全部的历史数据。

区块链为我们提供了数据库内每一笔数据的查找功能。区块链上的每一条交易数据，都可以通过“区块链”的结构追本溯源，一笔一笔进行验证。

区块 + 链 = 时间戳，这是区块链数据库的最大创新点。区块链数据库让全网的记录者在每一个区块中都盖上一个时间戳来记账，表示这个信息是这个时间写入的，形成了一个不可篡改、不可伪造的数据库。我们认为，时间戳是区块链中一项伟大的技术创新，它可以证明什么呢？

* 1. **分布式结构——开源的、去中心化的协议**

我们有了区块 + 链的数据之后，接下来就要考虑记录和存储的问题了。我们应该让谁来参与数据的记录，又应该把这些盖了时间戳的数据存储在哪里呢？在现如今中心化的体系中，数据都是集中记录并存储于中央电脑上。但是区块链结构设计精妙的地方就在这里，它并不赞同把数据记录并存储在中心化的一台或几台电脑上，而是让每一个参与数据交易的节点都记录并存储下所有的数据。

1. 关于如何让所有节点都能参与记录的问题，区块链的办法是：构建一整套协议机制，让全网每一个节点在参与记录的同时也来验证其他节点记录结果的正确性。只有当全网大部分节点（或甚至所有节点）都同时认为这个记录正确时，或者所有参与记录的节点都比对结果一致通过后，记录的真实性才能得到全网认可，记录数据才允许被写入区块中。

2. 关于如何存储下“区块链”这套严谨数据库的问题，区块链的办法是：构建一个分布式结构的网络系统，让数据库中的所有数据都实时更新并存放于所有参与记录的网络节点中。这样即使部分节点损坏或被黑客攻击，也不会影响整个数据库的数据记录与信息更新。

区块链根据系统确定的开源的、去中心化的协议，构建了一个分布式的结构体系，让价值交换的信息通过分布式传播发送给全网，通过分布式记账确定信息数据内容，盖上时间戳后生成区块数据，再通过分布式传播发送给各个节点，实现分布式存储。

分布式记账——会计责任的分散化（ Distributedaccountability ）

从硬件的角度讲，区块链的背后是大量的信息记录储存器（如电脑等）组成的网络，这一网络如何记录发生在网络中的所有价值交换活动呢？区块链设计者没有为专业的会计记录者预留一个特定的位置，而是希望通过自愿原则来建立一套人人都可以参与记录信息的分布式记账体系，从而将会计责任分散化，由整个网络的所有参与者来共同记录。

区块链中每一笔新交易的传播都采用分布式的结构，根据 P2P 网络层协议，消息由单个节点被直接发送给全网其他所有的节点。

区块链技术让数据库中的所有数据均存储于系统所有的电脑节点中，并实时更新。完全去中心化的结构设置使数据能实时记录，并在每一个参与数据存储的网络节点中更新，这就极大的提高了数据库的安全性。

通过分布式记账、分布式传播、分布式存储这三大“分布”我们可以发现，没有人、没有组织、甚至没有哪个国家能够控制这个系统，系统内的数据存储、交易验证、信息传输过程全部都是去中心化的。在没有中心的情况下，大规模的参与者达成共识，共同构建了区块链数据库。可以说，这是人类历史上第一次构建了一个真正意义上的去中心化体系。甚至可以说，区块链技术构建了一套永生不灭的系统——只要不是网络中的所有参与节点在同一时间集体崩溃，数据库系统就可以一直运转下去。

我们现在已经有了一套严谨的数据库，也有了记录并存储这套数据库的可用协议，那么当我们将这套数据库运用于实际社会时，我们要解决最核心的一个问题（问题三）是：如何使这个严谨且完整存储下来的数据库变得可信赖，使得我们可以在互联网无实名背景下成功防止诈骗？

* 1. **非对称加密算法**

什么是非对称加密？简单来说，它让我们在“加密”和“解密”的过程中分别使用两个密码，两个密码具有非对称的特点：（ 1 ）加密时的密码（在区块链中被称为“公钥”）是公开全网可见的，所有人都可以用自己的公钥来加密一段信息（信息的真实性）；（ 2 ）解密时的密码（在区块链中被称为“私钥”）是只有信息拥有者才知道的，被加密过的信息只有拥有相应私钥的人才能够解密（信息的安全性）。

简单的总结：区块链系统内，所有权验证机制的基础是非对称加密算法。常见的非对称加密算法包括 RSA 、 Elgamal 、 D-H 、 ECC （椭圆曲线加密算法）等。在非对称加密算法中，如果一个“密钥对”中的两个密钥满足以下两个条件： 1 、对信息用其中一个密钥加密后，只有用另一个密钥才能解开； 2 、其中一个密钥公开后，根据公开的密钥别人也无法算出另一个，那么我们就称这个密钥对为非对称密钥对，公开的密钥称为公钥，不公开的密钥称为私钥。在区块链系统的交易中，非对称密钥的基本使用场景有两种： 1 、公钥对交易信息加密，私钥对交易信息解密。私钥持有人解密后，可以使用收到的价值。 2 、私钥对信息签名，公钥验证签名。通过公钥签名验证的信息确认为私钥持有人发出。

我们可以看出，从信任的角度来看，区块链实际上是数学方法解决信任问题的产物。过去，人们解决信任问题可能依靠熟人社会的“老乡”，政党社会的“同志”，传统互联网中的交易平台“支付宝”。而区块链技术中，所有的规则事先都以算法程序的形式表述出来，人们完全不需要知道交易的对手方是“君子”还是“小人”，更不需要求助中心化的第三方机构来进行交易背书，而只需要信任数学算法就可以建立互信。区块链技术的背后，实质上是算法在为人们创造信用，达成共识背书。

* 1. **脚本**

脚本可以理解为一种可编程的智能合约。如果区块链技术只是为了适应某种特定的交易，那脚本的嵌入就没有必要了，系统可以直接定义完成价值交换活动需要满足的条件。然而，在一个去中心化的环境下，所有的协议都需要提前取得共识，那脚本的引入就显得不可或缺了。有了脚本之后，区块链技术就会使系统有机会去处理一些无法预见到的交易模式，保证了这一技术在未来的应用中不会过时，增加了技术的实用性。

一个脚本本质上是众多指令的列表，这些指令记录在每一次的价值交换活动中，价值交换活动的接收者（价值的持有人）如何获得这些价值，以及花费掉自己曾收到的留存价值需要满足哪些附加条件。通常，发送价值到目标地址的脚本，要求价值的持有人提供以下两个条件，才能使用自己之前收到的价值：一个公钥，以及一个签名（证明价值的持有者拥有与上述公钥相对应的私钥）。脚本的神奇之处在于，它具有可编程性：（ 1 ）它可以灵活改变花费掉留存价值的条件，例如脚本系统可能会同时要求两个私钥、或几个私钥、或无需任何私钥等；（ 2 ）它可以灵活的在发送价值时附加一些价值再转移的条件，例如脚本系统可以约定这一笔发送出去的价 值以后只能用于支付中信证券的手续费、或支付给政府等。

1. **公有链、联盟链和私有链的异同**
   1. **公有链**

公有链通常被认为是真正去中心化的，通过共识决定哪个区块最终被加到链中，任何人都可以参与共识过程。

公有链是完全对外开放的，用户不需注册、无需授权就可匿名访问网络和数据，节点可以自由出入网络。公有链上的区块内数据可以被任何人查看，任何人也都可以参与发起交易或是参与共识。

公有链是真正意义上完全去中心化的区块链，通过密码学数字签名保证交易不可篡改,也通过密码学验证交易信息以及激励，在互为陌生的网络中形成共识从而建立完全去中心化的信任机制。

目前的公有链在共识机制上都存在一些限制，因为区块链去中心化的本质所以没有一个中心节点来进行保护和维持系统，所以全网的所有节点需要一起参与所有的交易并维持全状态的副本。

去中心化共识机制的优势是安全保证、政治中立和抵抗审查等等。然而，这是以扩展性为代价换来的，因为去中心化限制了区块链里全节点可处理交易的数量。

这就导致了公有链的两大性能瓶颈：

低吞吐量：区块链目前能够处理的交易非常有限

缓慢的交易速度：处理一个区块的时间很长。比如比特币的区块时间是 10 分钟，以太坊的区块时间大约是 14 秒。在高峰期里花费的时间甚至更长。大家都知道比特币拥堵的时候甚至要几天才到账，高达几百元的转账费。以太坊也好不到哪里去，一只以太坊猫就把整个网络玩坏了。

所以可扩展性、速度和效率就是限制区块链商业应用的痛点所在。

* 1. **联盟链**

联盟链一般是由若干个机构共同参与管理的区块链。

联盟链上的读写权限和记账权限都由联盟规则限定，比如由40多家银行参与的区块链联盟R3和Linux基金会支持的超级账本（Hyperleder）项目就属于联盟链项目。

联盟链的共识过程由预先选好的节点控制。一般来说适合于机构间的交易、结算或清算等B2B场景。  
例如在银行间进行支付、结算、清算的系统就可以采用联盟链的形式，将各家银行的网关节点作为记账节点，当网络上有超过2/3的节点确认一个区块，该区块记录的交易将得到全网确认。

联盟链可以根据应用场景来决定对公众的开放程度。由于参与共识的节点比较少，联盟链一般不采用工作量证明的挖矿机制，而是多采用权益证明PoS或PBFT（Practical Byzantine Fault Tolerant）、RAFT等共识算法。联盟链对交易的确认时间、每秒交易数都与公共链有较大的区别，对安全和性能的要求也比公共链高。

联盟链和私有链都是需要注册许可的区块链，所以也称为许可链。有些许可链不需要激励记账所以不会发行代币。

* 1. **私有链**

私有链是指写入权限仅在一个组织手里的区块链。读取权限或者对外开放，或者被任意程度地进行了限制。私有链则仅在私有组织使用，区块链上的读写权限、参与记账权限按私有组织规则来制定。

私有链的应用场景一般是企业内部的应用，如数据库管理、审计等。私有链的价值主要是提供安全、可追溯、不可篡改、自动执行的运算平台，可以同时防范来自内部和外部对数据的安全攻击，这个在传统的系统是很难做到的。

举个形象的例子，比如现在我们有个村子，村子里的村民采用pow等机制来进行记账权的分配，而账本是所有人都能看到的，那村子的运作是基于公有链的。如何把这个运作方式变成一个私有链呢？

只要村长发话，区块链的读写权限，记账权限全部封闭，只对村民开放，想要拥有权限必须通过他的审核和确认才行。这样外人想看村里的区块链账本必须通过村长的同意，想交易？想入村当村民？全部得由村长同意才行。账本只对村内透明。

相比中心化数据库，私有链能够防止机构内单节点故意隐瞒或者篡改数据，即使发生错误，也能够迅速发现来源。因此许多大型金融机构在目前更加倾向于使用私有链技术。  
参与节点的资格会被严格的限制，由于参与的节点是有限和可控的，因此私有链往往可以有极快的交易速度、更好的隐私保护、更低的交易成本、不容易被恶意攻击、并且能够做到身份认证等金融行业必须的要求。

私有链和联盟链之间的设计隐私权限会有不同，联盟链中的权限设计要求往往更为复杂。

联盟链平台应提供成员管理、认证、授权、监控、审计等安全管理功能。

目前看来公有链与许可链的边界逐渐开始变得模糊，开始出现混合链。特点是系统内所有节点有不同的权限，有些节点只能查看部分区块链数据，有些节点能够下载完整的区块链数据，有些节点负责参与记账。混合链可能有公有链和许可链的优点，但开发难度较大，会是未来区块链技术发展的方向之一。

* 1. **总结**

三种区块链中去中心化程度最高的是公有链。这种以比特币以及以太坊为代表的公有区块链，不受第三方机构控制，世界上所有的人都可读取链上的数据记录、参与交易以及竞争新区块的记账权等。程序开发者无权干涉用户，各参与者（即节点）可自由加入以及退出网络，并按照意愿进行相关操作。

私有区块链则完全相反，该网络的写入权限由某个组织或者机构全权控制，数据读取权限受组织规定，要么对外开放、要么具有一定程度的访问限制。简单来说，可以将其理解为一个弱中心化或者多中心化的系统。由于参与节点具有严格限制且少；与公有链相比，私有链达成共识的时间相对较短、交易速度更快、效率更高、成本更低。不过这种类型的区块链更适合于特定机构内部使用，比如Linux基金会。

而联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。链上各个节点通常有与之相对应的实体机构或者组织；参与者通过授权加入网络并组成利益相关联盟，共同维护区块链运行。从某种程度上来说，联盟链也属于私有链的范畴，只是私有化程度有所不同而已。为此其同样具有成本较低、效率较高的特点，适用于不同实体间的交易、结算等B2B交易。

总的来说，公有链的进入门槛最低，而私有链以及联盟链则在开放程度上有所限制。

1. **可信计算和信任链**
   1. **可信的定义和属性**

目前，关于可信尚未形成统一的定义，主要有以下几种说法。

可信计算组织 TCG 用实体行为的预期性来定义可信：一个实体是可信的，如果它的行为总是以预期的方式，达到预期的目标。

ISO/IEC 15408 标准将可信定义为：参与计算的组件，操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰。

所谓可信是指计算机系统所提供的服务是可以论证其是可信赖的。这就是指从用户角度看，计算机系统所提供的服务是可信赖的，而且这种可信赖是可论证的。

我们给出自己的观点：可信 ≈ 安全 + 可靠。可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统。

信任是一种二元关系。它可以是一对一、一对多（个体对群体）、多对一（群体对个体）或多对多（群体对群体）的。信任具有二重性。既具有主观性又具有客观性。信任不一定具有对称性。即 A 信任 B 不一定就有 B 信任 A 。信任可度量。也就是说信任的程度可划分等级。信任可传递，但不绝对，而且在传播过程中有损失。信任具有动态性。即信任与环境和时间因素相关。

信任的获得方法主要有直接和间接两种方法。设 A 和 B 以前有过交往，则 A 对 B 的可信度可以通常考察 B 以往的表现来确定。我们称这种通过直接交往得到的信任值为直接信任值。设 A 和 B 以前没有任何交往，这种情况下， A 可以去询问一个与 B 比较熟悉的实体 C 来获得 B 的信任值，并且要求实体 C 与 B 有过直接的交往经验。我们称之为间接信任值，或者说是 C 向 A 的推荐信任值。有时还可能出现多级推荐的情况，这时便产生了信任链。

* 1. **信任的度量和模型**

目前，关于信任的度量理论主要有基于概率统计的可信模型、基于模糊数学的可信模型、基于主观逻辑、证据理论的可信模型和基于软件行为学的可信模型等。我国学者用软件行为学来描述软件的可信性。其认为：主体的可信性是主体行为的一种统计特性，而且是指行为的历史记录反映主体行为是否违规、越权以及超过范围等方面的统计特性。主体的可信性可以定义为其行为的预期性，软件的行为可信性可以划分级别，可以传递，而且在传递过程中会有损失。

* 1. **信任根和信任链**

信任根和信任链是可信计算平台的关键技术。一个可信计算机系统由可信根、可信硬件平台、可信操作系统和可信应用组成。信任链是通过构建一个信任根，从信任根开始到硬件平台、到操作系统、再到应用，一级认证一级，一级信任一级。从而把这种信任扩展到整个计算机系统。其中信任根的可信性由物理安全和管理安全确保。

* 1. **可信计算研究的发展**
     1. **可信计算初现**

1983年美国国防部制定了世界上第一个《可信计算机系统评价准则》 TCSEC （ Trusted Computer System Evaluation Criteria ）。在 TCSEC中第一次提出可信计算机和可信计算基 TCB （ Trusted Computing Base ）的概念，并把 TCB作为系统安全的基础。作为补充又相继推出了可信数据库解释 TDI（ Trusted Database Interpretation ）和可信网络解释 TNI （ Trusted Network Interpretation ）。这些文件形成了彩虹系列信息系统安全指导文件。

彩虹系列的出现形成了可信计算的一次高潮。多年来彩虹系列一直成为评价计算机系统安全的主要准则。然而由于历史的原因，彩虹系列具有一定的局限性 :

■ 主要强调了信息的秘密性，而对完整性、真实性考虑较少；

■ 强调了系统安全性的评价，却没有给出达到这种安全性的系统结构和技术路线。

* + 1. **可信计算高潮**

1999 年， IBM 、 HP 、 Intel 、微软等著名 IT 企业发起成立了可信计算平台联盟 TCPA （ Trusted Computing Platform Alliance ）， 2003 年 TCPA 改组为可信计算组织 TCG 。TCPA 和 TCG 的出现形成了可信计算的新高潮。该组织不仅考虑信息的秘密性，更强调信息的真实性和完整性，而且更加产业化和更具广泛性。

微软提出了名为 Palladium ，后改名为 NGSCB 的可信计算计划。微软将推出新一代操作系统 VISTA ，VISTA 支持可信计算机制。 Intel 为支持微软的 Palladium 计划宣布 LaGrande 硬件技术，并计划推出相应的新一代处理器。

欧洲于 2006 年 1 月启动了名为 “ 开放式可信计算（ Open Trusted Computing ） ” 的研究计划。

IEEE 的容错专家们自 1999 年将容错计算会议改名为可信计算会议（ PRDC ）后，便致力于可信计算的研究。他们的可信计算更强调计算系统的可靠性和可用性，而且强调可信的可论证性。

* + 1. **可信计算在中国**

2000 年 6 月武汉瑞达公司和武汉大学合作，开始研制安全计算机，研究成果于 2004 年 10 月通过国家密码管理委员会主持的技术鉴定。它是国内第一款自主研制的可信计算平台，在系统结构和主要技术路线方面与 TCG 的规范是类似的，有些方面有所创新，有些方面也有差异。这一产品被国家科技部等四部委联合认定为 “ 国家级重点新产品 ” ，并获得 2006 年国家密码科技进步二等奖，已在我国电子政务、公安、银行、军队得到实际应用。

2004 年 6 月在武汉召开中国首届 TCP 论坛。 2004 年 10 月在解放军密码管理委员会的支持下，在武汉大学召开了第一届中国可信计算与信息安全学术会议。

2005 年联想集团的 “ 恒智 ” 芯片和可信计算机相继研制成功。同年，兆日公司的 TPM 芯片研制成功。这些产品都相继通过国家密码管理委员会的鉴定和认可。

此外，同方、方正、浪潮、天融信等公司也都加入了可信计算的行列。武汉大学、中科院软件所等高校和研究机构也都开展了可信计算的研究。

国家发改委、科技部、信息产业部、国家自然科学基金委等政府部门都积极支持可信计算的发展。

至此，中国的可信计算事业进入了蓬勃发展的阶段。

* 1. **可信计算研究的发展趋势**
     1. **可信计算面临的挑战**

目前可信计算已经成为信息安全领域的一个新潮流，但可信计算的发展尚存在一些问题。

1. 理论研究相对滞后

无论是美国还是中国，在可信计算领域都处于技术超前于理论，理论滞后于技术的状况。至今尚没有公认的可信计算理论模型。

可信测量是可信计算的基础。但是目前尚缺少软件的动态可信性的度量方法与理论。

信任链技术是可信计算平台的一项关键技术。然而信任链的理论尚需要进一步完善。

理论来源于实践，反过来又指导实践。没有理论指导的实践最终是不能持久的。目前可信计算的技术实践已经取得长足的发展，因此应当在可信计算的实践中丰富和发展可信计算的理论。

1. 部分关键技术尚待攻克

目前的可信计算机产品都没能完全实现可信计算中广泛认同的一些关键技术。如完整的信任链、动态可信测量、安全 I/O 等。目前的可信测量只是系统开机时的系统资源静态完整性测量，因此只能确保系统开机时的系统资源静态完整性，尚不能确保系统工作后的动态可信性。

1. 缺乏配套的可信软件系统

目前 TCG 给出了可信计算硬件平台的相关技术规范和可信网络连接的技术规范，但还没有关于可信操作系统、可信数据库、可信应用软件的技术规范。网络连接只是网络活动的第一步，连网的主要目的是数据交换和资源共享，这方面尚缺少可信技术规范。只有硬件平台的可信，没有操作系统、网络、数据库和应用的可信，整个系统还是不安全的。

1. 缺少安全机制与容错机制的结合

安全可靠是用户对可信计算的希望，因此必须坚持安全与容错相结合的技术路线。但是目前这方面的研究还十分缺乏。

1. 可信计算的应用需要开拓

可信计算的应用是可信计算发展的根本目的。目前可信 PC 机、 TPM 芯片都已经得到实际应用，但应用的规模和覆盖范围都还不够，有待大力拓展。

* + 1. **可信计算待研究的领域**

现阶段的可信计算热潮是从可信 PC 平台开始的，但是它涉及的研究和应用领域却要广泛得多。其亟待研究的领域包括以下三方面。

(1) 关键技术

■ 可信计算的系统结构，包括可信计算平台的硬件结构及可信计算平台的软件结构；

■ TPM 的系统结构： TPM 的硬件结构， TPM 的物理安全， TPM 的嵌入式软件；

■ 可信计算中的密码技术：公钥密码，传统密码， HASH 函数，随机数产生；

■ 信任链技术：完整的信任链和信任的延伸；

■ 信任的度量：信任的动态测量、存储和报告机制，软件动态可信测量；

■ 可信软件：可信操作系统、可信编译、可信数据库、可信应用软件；

■ 可信网络：可信网络结构、可信网络协议、可信网络设备、可信网格。

(2) 理论基础

■ 可信计算模型：可信计算的数学模型、可信计算的行为学模型；

■ 可信性的度量理论：信任的属性与度量、软件的动态可信性度量理论与模型；

■ 信任链理论：信任的传递理论、信任传递的损失度量；

■ 可信软件理论：软件可信性度量理论、可信软件工程、可信程序设计方法学、软件行为学。

(3) 可信计算的应用

可信计算技术的应用是可信计算发展的根本目的。可信计算技术与产品主要用于电子商务、电子政务、安全风险管理、数字版权管理、安全检测与应急响应等领域。

* 1. **总结**

目前可信计算已经成为世界信息安全领域的一个新潮流。可信计算技术是一种行之有效的信息安全技术。可信计算机与普通计算机相比，安全性大大提高，但可信计算机也不是百分之百安全。

我国在可信计算领域起步不晚，水平不低，成果可喜。我们应当抓住机遇发展我国的可信计算事业，建立我国的信息安全体系，确保我国的信息安全。

可信计算发展很迅速 , 传统计算机的误报率越来越多 , 安全投入不断增大 , 维护

与管理更加复杂 , 信息系统的使用率大大降低。产生这种局面的主要原因是不去控制不安全问题的根源 , 而只是在外围进行封堵。目前计算机采用可信计算的设计理念 , 通过对可信计算的分析和研究 , 尤其对比国外 TPM 安全芯片所经历的历程和设计理念 , 提出走自己的可信道路 , 并预测了广阔的市场前景。

**参考文献**

**[1] 蒋春凤. 非对称加密算法[J]. 内江科技, 2012(8):148-148.**

**[2] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4):481-494.**

**[3] 王晓光. 区块链技术共识算法综述[J]. 信息与电脑(理论版), 2017(9):72-74.**

**[4] 佚名. 区块链共识机制之拜占庭算法[J]. 数字通信世界, 2019, 169(01):51+57.**

**[5] 佚名. 一种基于Raft算法的区块链共识机制:, CN106878071A[P]. 2017.**

**[6] 王勇, 许荣强, 任兴田,等. 可信计算中信任链建立的形式化验证[J]. 北京工业大学学报, 2016, 42(3):387-392.**