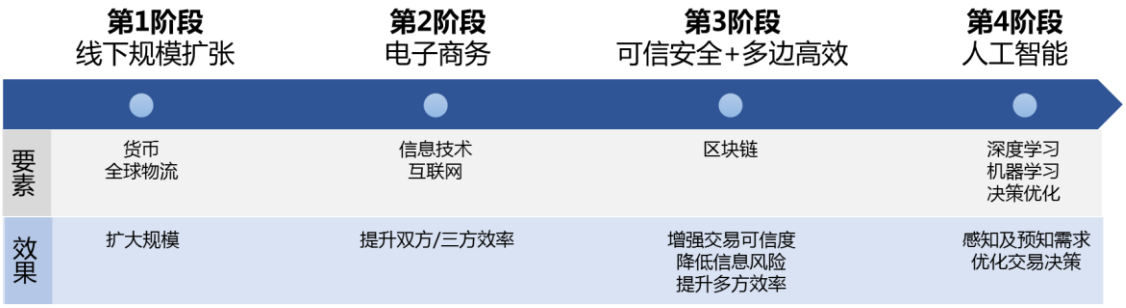
可信交易区块链技术与应用白皮书

(2017)

目录

一、可信交易与区块链技术

劳动分工的出现是人类经济史上的一大壮举，亚当·斯密的《国富论》系统阐述了劳动分工对提高劳动生产率和增进国民财富的巨大作用。其他著名经济学家如伊曼努尔·康德、卡尔·马克思等都指出社会进步伴随着分工的日益精细化；并且越发达的社会，分工则越精细。劳动分工的出现必须依赖于一个关键要素：**交易**。有了交易，每个人能够用自己生产的物品或服务换取他人生产的物品或服务，从而获取生存的必需品。回顾历史，展望未来，我们认为交易的发展可以分为四大阶段，每个阶段都是以关键概念及（或）关键技术的成熟为标志。



“线下规模扩张”阶段：以物易物是交易的最初级形态。随着社会的发展与进步，出现了中间物 – 货币。货币解放了买方与卖方的紧耦合关系，使得交易更加高效和灵活。伴随着第一次工业革命和第二次工业革命，全球物流得到了跨越式的发展。国际贸易开始兴起，重构了全球供应链与贸易格局。跨国交易也使得交易总量得到极大的提升。纵观人类经济史，以物易物、货币的出现、国际贸易的兴盛构成了人类不断扩大**线下交易的规模**的商业史书。然而供需信息的交换，仍然需要通过依靠诸如交易博览会（本质上是信息集市），抑或多级代理商（本质上是信息撮合方）等来达成。此时，信息交换成为交易发展的瓶颈。

“电子商务”阶段：随着互联网革命的到来，**交易利用信息科技与互联网通讯技术摆脱了信息交换不通畅的掣肘**。电子交易技术于 70 年代被提出后经历了近半个世纪的

发展，到 2016 年通过线上电子商务形成的销售在零售行业销售额中中占据 8.7%的比例。美国著名研究机构 eMarketer 预计这一比例在 2020 年将达到 14.7%[1]。电子商务巨头如美国的亚马逊公司，中国的阿里巴巴、京东等公司的涌现正是电子商务时代去中介化（即去信息撮合方）的一个缩影。在我国，以电子商务为代表的互联网经济正在从消费端向产业端延伸，在保增长、调结构、稳就业、促创新方面表现出强劲的动力。电子商务本质上是通过信息交换，形成高效的双方或三方参与的交易。然而我们认为，两方或三方参与的电子商务系统不是交易发展的最终形态。

“可信安全+多边高效”阶段：传统的“电子商务”交易系统具有三大弱点。第一、信息交换畅通无阻和先进的数据采集技术使得**数据隐私**荡然无存，数据泛滥正在造成诈骗、过度推销等社会恶果。第二、很多交易引入了除买卖双方以外更多的角色，如保险，代理，平台公司，银行等等。两方或者三方共享的交易系统已经滞后于**多边交易**对高效信息交换的诉求。第三、仅仅两方或三方共享的信息在越来越多要求多方参与的交易里屏蔽了数据的透明性，从而掩盖了数据背后的**风险**。概括起来，下一代的交易系统需要支持可信交易的、数据安全的、多边合作高效的系统。

“人工智能”阶段：最后，随着人工智能的发展，交易将更多地融合认知计算技术。由设备感知推断个人的交易诉求，提示交易中的风险，实现交易的**智能化**。

当前，交易系统正处于欲从电子商务阶段的第二阶段中破茧而出，进入多边、高效、安全、可信交易系统的第三阶段的关键时间点。进一步的剖析第三阶段所需求的交易系统，我们认为其应具备的特征与目前新兴的区块链技术有天然的契合。

- **健全的身份管理机制**：在可信交易中，参与交易的每一方都应该有相关的角色授

[1] https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369

权以及角色相关的权限划分。进一步的，权限应该包括参与权限、入链记账权限和数据读取权限。区块链系统中广泛应用的非对称加密技术可以将一对密钥的公钥作为身份的表征，通过智能合约来约束该公钥具备的各种权限。在私有链或者联盟链中，还可以引入证书发放机构来约束权限的授予与撤销。

- **保证网络化多边合作效率**：正如前面对交易发展的历史所回顾，在现代商贸活动中，多方参与的商品、信息和服务交换是一个十分复杂的交易过程。以跨国贸易为例，其涉及到买卖双方、买卖双方的银行、货代公司、船运公司、保险公司等等。在第三阶段，可信交易应该使得多边的信息交换可信，进而促成交易达成效率的提高。前面提到的非对称加密技术可以利用私钥签名、公钥验证的方式来形成对合约或者交易的电子签章，其余方可以在不知道签名方私钥的情况下验证签名的真伪，从而起到电子化的、快速地去伪存真、高效推进业务流程的作用。
- **释放智能合约的自动化能力**：提高多边合作效率的另外一个方式是尽量简化线下流程，自动化线上流程，这正是“智能合约”的概念所提倡的。智能合约于 1994 年首先被计算机科学家 Nick Szabo 提出，其定义是“可被计算机代码自动执行的条款[2]。”但在智能合约概念提出后的十几年，并没有系统能够真正支持智能合约的运行。区块链系统支撑的比特币生态系统，是第一个真正可执行智能合约的系统。随着越来越多的资产和货币数字化，可自动执行的场景越来越丰富。交易多方应充分利用智能合约的自动化能力缩短多边交易的达成时间。智能合约通过定义与数字化信息相关的合约条款，实现对数字化资产或者货币的自动转移。
- **可审计、可追踪**：可信交易通常需要接受国家相关部门的监管，因此必须保证交易的相关信息是可以审计，可以追踪的。区块链系统采用的区块串联方式以及分

[2] A smart contract is a computerized transaction protocol that executes the terms of a contract.

布式数据存储设计，保证了数据的不可篡改性，十分有利于审计和追踪。此外，通过设计一交易一秘钥的机制，可以使得已经封装入链的交易可以通过交易后授予数据读取权限的方式给监管部门监督监管的权力。

- **数据安全与隐私保护机制**:在传统意义上,全透明数据有利于审计与追踪。同样，在无数据隐私的情况下，也有利于多方合作效率的提高。但是实际上的协作中，各方都有部分数据是隐私的，只有在发生纠纷时才会公开。区块链系统可以通过非对称加密技术和对称加密技术的融合，保证数据以不可读的方式入链，只有被授权方才可以通过其数字身份证明查看数据明文。换句话说，区块链系统可以同时实现在数据发生篡改时任意参与方对数据进行预警，以及阻止未被授权方读取数据明文。
- **完备的可信交易协作机制**：为了确保多方交易是由多方认可的、无伪造交易或文档现象等问题，需要在交易的过程中使得相关方均可以对交易的状态进行认可，以确保交易的协作是有效的。区块链系统采用多节点的共识机制，确保只有利益相关方同意的数据可以入链，形成多边认可的交易，规避单方记账带来的数据造假风险。
- **符合国情的自主可信**：可信不只是与国际先进技术接轨，同时必须具备符合国情的自主可信的特点。在中国，国家密码管理局推出了 SM1，SM2，SM3，SM4 四种国密算法。基于国密算法的硬件密码机可以为交易系统提供更好的安全性。区块链系统可以接入基于国密算法的 SDK 或者硬件，从而实现符合国情的自主可信。

二、可信交易区块链系统技术蓝图

2.1 可信交易区块链系统技术架构

可信交易区块链系统的架构自下而上分为四个层次，分别是基础平台、标准驱动、区块链基础应用、行业解决方案，贯彻整个技术架构的是安全体系与行业标准规范适配。

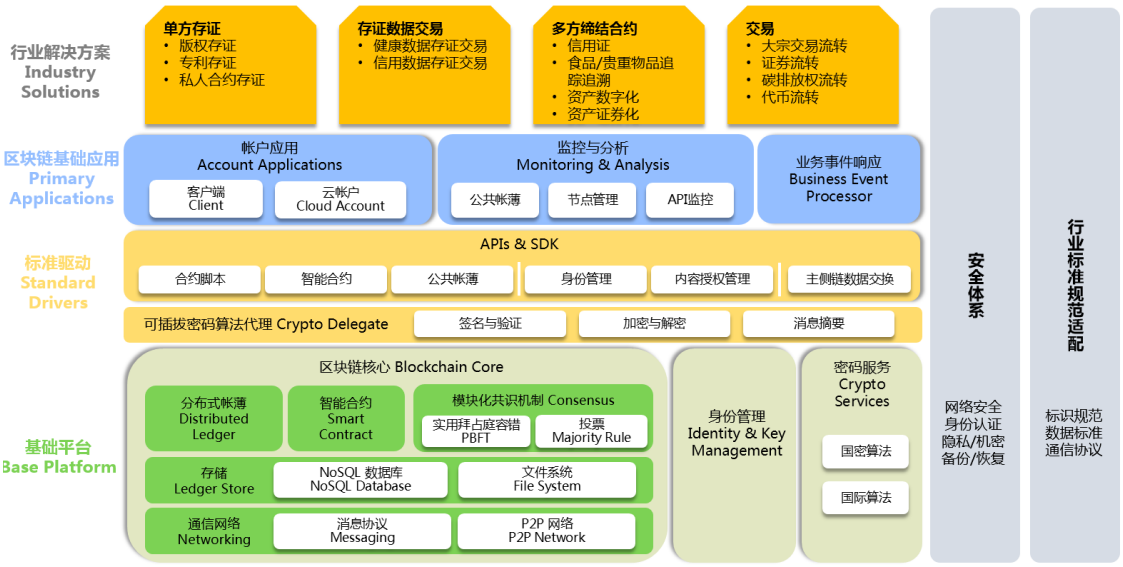


图 1 可信交易区块链系统技术架构

2.1.1 基础平台

基础平台层负责实现区块链核心功能，包括三个主要组件，分别是区块链核心组件、身份管理组件和密码服务组件。

区块链核心组件提供可信交易区块链系统的核心基础功能，

- 分布式帐薄：按照时间顺序将数据区块以顺序相连的方式组合成一种链式数据结构，并以密码学保证的不可篡改和不可伪造的分布式账本。
- 智能合约：利用由自动化脚本代码组成的智能合约来编程，从而赋予用户数据读取和操作权限。

- 模块化共识机制 :共识是可信交易区块链系统中各个节点达成一致的策略和方法。模块化共识可以根据系统类型及应用场景的不同灵活配置选用不同的共识策略。
- 存储：区块链数据在运行期以块链式数据结构存储在内存中，最终会持久化存储到数据库中。较大的文件或者数据写入区块链时，可以将原文存储在链外的文件系统里，同时将原文的摘要（数字指纹）保存到链上用以自证。
- 通讯网络：区块链采用 P2P 技术来组织各个网络节点，每个节点通过约定的消息协议实现路由、新节点识别和数据传播等功能。

身份管理组件是可信交易区块链的另一个重要基石。该组件实现对可信交易区块链各方参与者的身份认证。可信交易区块链的参与者只有获取身份和角色认证之后才可以参与到区块链的交易和共识之中。身份管理组件应支持各类第三方数字证书。

密码服务组件是是基础平台的第三个重要组成。其负责提供国密算法和国际算法实现和封装，用于区块链密码相关操作，包括对称加密、非对称加密、签名、数据摘要等。密码服务支持接入硬件密码设备，同时提供缺省软件方式实现。

2.1.2 标准驱动

标准驱动层提供 APIs，SDK 以及可插拔密码算法代理。其中 APIs 提供接口服务；SDK 提供一套围绕 APIs 的标准开发环境；可插拔密码算法代理封装密码服务的实现细节，向区块链核心功能和应用提供服务。

2.1.3 区块链基础应用

区块链基础应用，包括帐户应用、监控与分析和业务事件响应。

- 帐户应用包括客户端与云帐户。客户端实现可信交易区块链系统的所有功能，

包括对整个分布式账簿（区块链）的完整拷贝，和点对点网络中的一个完整网络节点。适用于计算、存储和网络资源充分，对可信度要求高的使用方。云帐户提供远程的用户帐户管理功能，实现帐户托管服务。适用于存储资源较少的使用方。

- 监控与分析应用提供节点管理功能，用户可以实时监控区块链网站中各个节点的状态；公共帐薄提供分布式帐薄的完整查看和查询功能；“API 监控”模块实时统计节点相关的 API 调用情况，并可以给出性能分析报告。
- 业务事件响应应用基于生产者/消费者模式提供事件注册服务。节点或者客户端可以注册区块生成事件、交易或者存证确认事件等，一旦事件被业务事件响应组件监听，所有的注册者都可以收到通知。

2.1.4 行业解决方案

行业解决方案提供四种基本类型的封装，分别是单方数据存证，多方数据交易和多方缔结智能合约及面向交易的应用。前面三种应用过程不涉及精确价值的转移。而面向交易的应用则以价值的精确转移为导向。我们指出，大多数的解决方案通常都是四种基本应用类型的组合。

2.1.5 安全体系

安全体系负责定义和实现网络安全、数据隐私、灾备与恢复相关的标准。区块链系统面临的风险不仅来自外部实体的攻击，也可能有来自内部参与者的攻击，以及组件的失效，如软件故障。因此在实施之前，需要制定风险模型，认清特殊的安全需求，以确保对风险和应对方案的准确把握。

2.1.6 行业标准规范适配

行业标准规范适配负责将行业中的解决方案落地到区块链技术中，比如行业数据规划、合规要求、通讯协议要求等，同时负责定义区块链数据与行业数据映射的标准接口。

2.2 可信交易区块链系统核心技术优势

表 1 列出可信交易区块链系统在架构各层级的技术优势。这些技术优势综合起来形成可信交易区块链系统的核心竞争力。

表 1 可信交易区块链系统技术优势

架构层级	模块	技术优势	带来的业务优势
基础平台	密码服务	适配国家标准密码算法和国际标准密码算法	国密算法是由中国国家密码局认定的国产密码算法。适配国密算法，可以使区块链解决方案符合国家信息安全标准。
	模块化共识机制	适配不同共识机制，包括实用拜占庭容错共识、投票共识。	满足多种业务场景、联盟链的共识要求，实现快速适配和部署。
标准驱动	身份管理	支持主流第三方数字证书支持	1. 将对参与方的认证由线下转移到线上； 2. 通过身份认证，确保交易数据的安全。
	内容授权管理	支持数据读取授权和再授权，实现公共帐薄的全程可审计。	1. 对交易数据进行访问授权，确保数据隐私； 2. 运行对数据权限进行接力授权智能合约，随时为加入的监管机构进行历史数据访问授权，从而保证公开帐薄的被审计性和信任度。
	主侧链数据交换	通过主侧链的方式进行可信互信的数据交换	1. 便于参与方进行分类帐（子链）之间的数据交换； 2. 保护参与方的商业机密。
区块链基础应用	帐户托管	实现对用户公钥私钥或者数字证书的托管	对用户帐户进行安全、便利的管理

2.2.1 密码服务

可信交易区块链的账本信息是通过对称加密、非对称加密、摘要算法共同实现的。采用对称加密算法对账本内容（资产、合约、账户、参与者等)进行加密，以确保交易安全；信息相关人利用非对称加密算法对账本内容进行签名，确保交易的可信性；用摘要算法对账本内容进行数据摘要，信息相关人可以实现不公开隐私数据而仅发布数据摘要到区块链上以保持内容的不可篡改。

国产密码算法是由国家密码局认定的商用密码 ,能够实现加密、解密和认证等功能。国产密码算法的应用领域十分广泛 ,主要用于对具有敏感性的内部信息、行政事务信息、经济信息等进行加密保护。比如，国产密码算法可用于企业内部的各类敏感信息的传输加密、存储加密，防止非法第三方获取信息内容；也可用于各种安全认证、网上银行、数字签名等。

可信交易区块链适配适配国产密码算法和国际标准密码算法。在标准驱动层，可信交易区块链提供可插拔密码服务代理，对外提供定制化密码服务。

表 2 国产密码算法与国际通用算法对比

	国产密码算法 国家密码局认定的国产密码算法	**国际通用算法** 国际通用的商用算法
对称加密	SM1 算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。	AES DES 3DES
公钥密码算法	SM2	ECC RSA

摘要算法	SM3	SHA256 MD5
分组密码算法	SM4	AES

可信交易区块链的密码服务组件可以对接密码学算法的硬实现和软实现。其中硬实现由硬件加密机或者云加密机提供密码服务。加密机是一种硬件设备，在自封闭的硬件中提供安全的密钥存储和加密运算功能，密钥在硬件中生成、存储、使用，保证密钥不会以明文形式出现在硬件设备之外。云加密机是支持用户安全远程密钥管理、支持虚拟化技术可供多租户的、安全共享的加密机。软实现则是在云环境中提供如密钥安全管理、数据加密保护、身份认证、数字签名、防篡改等加密服务，帮助云用户构建安全、合规的业务系统。

2.2.2 模块化共识机制

在如比特币网络的分布式系统中，共识机制是大部分网络成员就某条数据或拟定交易的价值达成一致，并就此对账本进行更新的机制。换言之，共识机制是在参与节点之间管理一系列连贯事实的规则和程序。共识算法允许多个分布式节点连接起来进行工作，并在某些成员失效的情况下，记账工作仍能正常进行。

共识机制管理为共识算法和其他组件之间定义了通用的接口，通用接口负责接收交易，并协调共识机制的各个参与方通过共识算法对交易和区块达成一致。共识机制管理使得共识算法模块化和可拔插。通过简单配置，用户可以选择不同的共识机制以适配联盟链、私有链等不同应用场景。可信交易区块链选择实用拜占庭容错共识（Practical Byzantine Fault Tolerance）和多数同意规则（Majority voting rules）作为基础共识机制。

2.2.2 身份管理

身份管理是可信交易区块链的重要组件，实现对可信交易区块链各方参与者的身份认证。参与者需要从身份管理组件获取数字证书，数字证书包括公开密码、名称、证书授权中心的数字签名、有效时间、证书序列号等。数字证书唯一标识它的持有者是某个私钥的合法拥有者。

身份管理可以实现对参与者角色的认证，只有通过认证的参与者或者节点才可以执行指定的功能。比如，交易的发起方需要有合格的数字证书，只有拥有投票认证的节点才可以参与共识机制。

2.2.3 内容授权管理

可信交易区块链采用加密方式对账本内容进行保护，确保数据的隐私安全。可信交易区块链提供了一套授权与再授权机制。其中授权机制授予账本内容参与者对区块链内容的读取权限，只有被授权的用户才可以查看账本明文内容。再授权机制保证拥有对某一个交易再授权权限的用户授权其他用户读取交易内容。这样的机制保证了帐薄内容的扩展可读和全程可审计。

2.2.4 主侧链数据交换

可信交易区块链通过主侧链技术实现跨平台、跨区块链的可信数据交换。主侧链数据交换技术组合不同平台的区块链成为一条主链，通过向区块链主链中签名打入其侧链的数据指纹来确保指纹的不可篡改性，从而实现可信的数据交换。

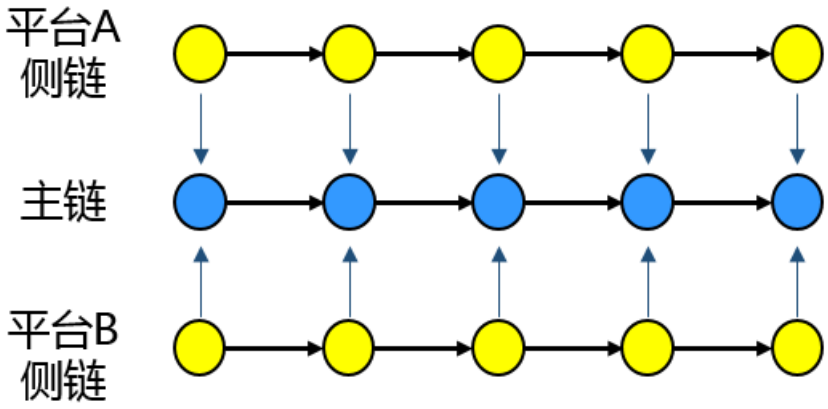


图 2 通过主侧链方式进行互信的数据交换

2.2.5 帐户托管

可信交易区块链提供帐户托管服务，参与方可以选择将数字证书、公钥私钥等存放到可信交易区块链的云帐户中。云帐户使用用户密码对数字证书等进行对称加密后保管。

三、可信交易区块链系统典型应用场景

3.1 可信交易区块链应用场景划分

我们将可信交易区块链的应用场景按照涉及方的多少及存证业务的生命周期划分为如图 3 所示的四大类。

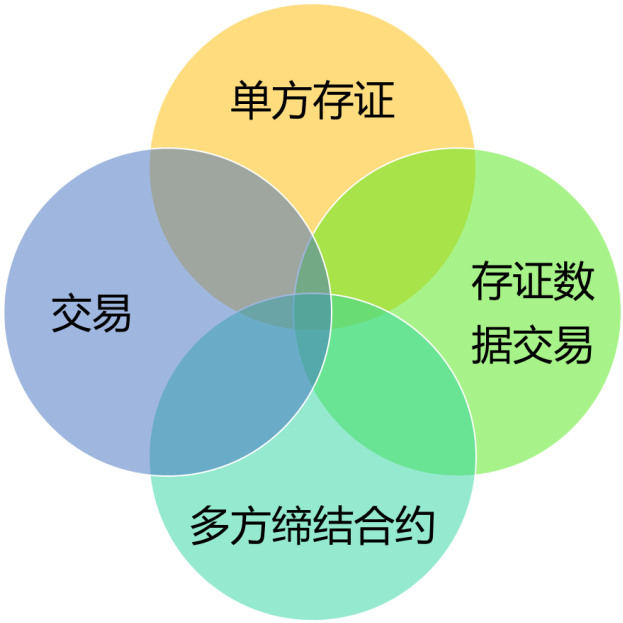


图 3 可信交易区块链应用场景分类

- **单方存证**：某一方为了证明自己对数字化文件（文本、图像、音频、视频）等的拥有，可以将相关文件存入到公开、分布式存储的区块链系统中。存证是一次性完成。
- **存证数据交易**：在存证以后，可以通过点对点数据加密互换的方式进行数据交易。该类交易保证数据只有买方和卖方可以解密。
- **多方合约缔结**：为有限的多方通过某个流程（即先后顺序）缔结数字化合约的过程服务。非对称加密算法提供的签名和验证功能辅助多方利用智能合约缔结可信合同。合同过程以合同签约流程定义的最后一方的签名、并且得到共识节点的共

识加入区块链中而结束。如果合同过程不符合智能合约中约定的流程，则诚实的共识节点会拒绝将其写入区块链中。

- **交易**：理论上为无限的多方对数字化的数量进行可拆分的流转过程。流转过程中总量守恒，并且通过智能合约约定数量转移的条件。不满足转移条件的交易不会被共识节点验证通过，也不会被写入到区块链中。

表 3 列出了三种分类单独应用时有代表性的场景。我们指出，实际的应用并不单独是上面的任何一类，而可能是通过组合以上四类的区块链应用场景才能够实现对业务的完整支撑。

表 3 可信交易区块链应用场景分类

场景分类	参与方数目	场景举例
单方存证	单方	音乐、文学著作等版权存证 专利存证 私人合约上传
存证数据交易	无限的多方	健康数据存证交易 信用数据存证交易
多方缔结合约	有限的多方	信用证 食品/贵重物品追踪追溯 资产数字化 资产证券化
交易	无限的多方	大宗交易流转 证券流转 碳排放权流转 代币流转 可信电子商务

3.2 典型可信交易区块链应用场景

在本章节中，选取六种典型的交易场景对其业务目的、业务需求及区块链针对业务需求能提供的支持予以描述。

3.2.1 单方存证

业务目的	证明某项数据归某人所有
业务需求	存证时间真实 存证不可篡改 数据不可销毁 数据可验证所有权
区块链关键支撑技术	非对称加密算法签名确保所有存证时间真实 非对称加密算法签名确保存证内容不可篡改 分布式账簿确保数据不可销毁 私钥签名公钥验证机制保证数据可验证所有权

3.2.2 信用数据存证交易

业务目的	在存证的基础上进行隐私可保护的数据交易与交换 信用数据的存证交易与交换可以形成垂直行业甚至跨行业的信用数据库及信用市场 典型垂直行业包括 P2P 借贷行业、消费金融业、酒店业、银行业、航空业等
业务需求	数据可验证所有权 数据可点对点加密交易
区块链关键支撑技术	私钥签名公钥验证机制保证数据可验证所有权； 采用身份证书与交易证书两重机制可对每个交易采用不同的交易密钥进行加密，并且授权给不同的数据买方查看。

3.2.3 信用证

业务目的	信用证是跨国贸易的一种付款方式，其付款完全是基于文件的。进口商委托银行在所有文件齐全的情况下会立刻向出口商委托银行付款。其业务过程中的主要痛点是所需要的三十多份文件需要来自包括货代、船代、海关、远洋运输商、内陆运输商、海关等十余方，周期长、验真繁复。
业务需求	快速实现多方数据的可信同步 无纸化
区块链关键支撑技术	私钥签名公钥验证机制保证数据可验证写入人的可信性； 以智能合约约束进口商委托银行的放款条件； 以天然的分布式系统提供低成本的统一信息化系统，具有天

	然的系统可拓展性。

3.2.4 资产证券化

业务目的	确保资产根据公众认可的流程形成证券
业务需求	可回溯资产证券化各方角色（包括特殊目的机构、增信机构、信用评级机构、销售机构等）认证 可检查资产证券化过程相关流程是否合法合规 确保证券化资产的唯一性
区块链关键支撑技术	将证券化资产进行密码学变换后生成唯一的 ID，同样的资产再次证券化系统将预警； 以智能合约约定资产证券化流程，避免出现不符合流程的证券化； 以私钥签名确保合约由相关方签署。

3.2.5 资产流转

业务目的	形成资产交易系统
业务需求	确保资产转移过程不可无中生有； 确保资产交易可追溯，降低不透明风险； 确保资产交易可监管； 确保资产交易可对账。
区块链关键支撑技术	以智能合约约束资产不可无中生有，无中生有的资产不会被记账节点入账； 通过交易引用串联资产交易，确保资产交易的可追踪可追溯，避免多次转手后资产不透明引发的风险； 通过交易数据授权的方式，可以追加授权监管单位对数据明文进行查看，增强交易系统的可信度； 共享账本使得对账变得非常容易。

3.2.6 可信电子商务

业务目的	形成真实可信的电子商务交易系统
业务需求	确保参与者身份真实性； 确保交易环节透明度； 确保交易的不可抵赖性，消除虚假交易； 需要一种信任机制来确权和记账。

区块链关键支撑技术	使用区块链管理和识别个人身份； 由多个业务参与方共同建设和维护一个公共的账本系统； 录入的数据由统一的共识机制保障，确保数据的时序性和真实性，并且单方不可篡改不可抵赖。

3.3 实物流相关的区块链应用讨论

由于数字化数据的真伪完全可以被以软件形式存在的算法验证，因此区块链技术对其的传播、共享与交换是无缝支撑的。而目前商业世界探讨的一部分的应用场景却是涉及到实物流的，比如有公司利用区块链追踪钻石的物流，有公司利用区块链确保食品安全，有公司希望能够利用保障数据信息的可信。在这里，我们特别对此类场景进行三个关键点的讨论。

1. **实物流向信息流的无缝转化**：在一些场景下，实物流是可以被无缝转化为信息流的。例如在某些贵重物品出厂时，可以通过硬件的方式对其密封。硬件可以以加密和签名数据的形式随时上传位置数据；任何破坏硬件的行为也会因为其上传数据的终止而被发现。一旦实物流转化为信息流，区块链系统可以通过智能合约的方式验证信息流是否满足预设条件（如预设的地域范围），一旦不满足则向区块链的所有参与方提出预警。
2. **人工智能技术的集成**：在另外一些场景下，实物流无法被端到端地转化为信息流。例如钻石的运输过程中，即使可以对运输钻石的盒子加上硬件密封，但由于其价值巨大且销售周期长，每一方接收到钻石时都会打开硬件对其进行验真。在这个过程中，经手人均是有可能可以对钻石进行掉换的。此时可以通过引入人工智能技术，如集成高清图片分析的技术，要求每一个经手人在销售时向区块链上传多角度高清图片，通过图像分析的技术进行匹配和比对，辅助业务方验真。
3. **以数据不可篡改带动可信交易**：即使有些参与方在实物流动过程中造假，基于区

块链的多方合作业务系统相当于使得任何一方在实物流动时在系统中签名认可该实物流由其经手。该签名的数据具有两个特征：1）当前采用的主流非对称加密算法的难度决定其无法破解，即只有持有对应私钥的用户可以进行签名，无法以其他人伪造为理由推脱责任；2）该数据以分布式的方式存在于合作各方的系统中，造假方无法执行单方的删除操作。

基于以上三点的讨论，我们建议对有实物流关联应用场景的用户首先考虑是否有成本合理的硬件解决方案可以在业务场景中实现实物流与信息流的无缝集成；其次考虑是否有人工智能技术、大数据技术等其他辅助手段可以帮助鉴别实物流动的真实性；在以上两种方式均无法达到的时候，则应该考量区块链分布式，不可篡改，不可推责的特性是否会对合作各方起到威慑作用，从而保证交易的可信性。

四、可信交易区块链系统应用建议

4.1 区块链应用决策

区块链是一项构建多方可信交易的关键新兴技术，但在选用区块链技术搭建业务系统之前，机构应充分评估区块链的技术特点是否匹配业务需求。本小节将从四个重要方面阐述应用区块链技术对业务系统的影响，分别是对交易系统的性能要求；是否存在智能合约；身份管理和授权是否重要；市场对流程效率、透明度与安全的要求。

4.1.1 交易系统的性能要求

对于商业应用，交易吞吐量和时延是企业最关心的性能指标。从区块链技术的实现角度，影响区块链吞吐率和响应时间的主要影响因素在于达成共识的效率、网络传输的效率、信息加解密的效率以及智能合约的处理效率。

达成共识的效率由共识算法的复杂度及需要参与共识的节点数相关。共识算法越复杂，达成共识时间越长。去中心化程度越高，会导致共识机制效率降低。也就是说，共识机制需要在一定的信任前提和利益约束下进行设计。对于高度互相信任的多方，可以减少共识节点的数目，降低共识算法的复杂度和容错能力，从而达到提升交易效率的目的。

网络传输的效率由区块链系统采用的 P2P 网络决定。每个节点机器的性能和网络情况都是千差万别的，这样的情况对交易达成速度形成一个天然的限制。对于联盟链，我们可以指定节点机器的物理配置和节点数量，并尽量以高速网络进行连接，这会很大程度改善区块链的交易性能。

其他方面，**信息加解密的效率**可以采用提升硬件处理能力或者采用专用加解密设备

来提高。**智能合约的效率**既取决于代码的质量，也取决于其实现业务的复杂度。

在选择是否应用区块链系统时应充分理解区块链系统执行效率的影响因素，然后考虑评估业务需求对区块链系统执行效率的影响，以及其影响是否是业务系统可以接受的。

4.1.2 是否存在智能合约

智能合约是区块链的核心技术。智能合约可以**自动化**不同类型的流程和操作，参与者按照智能合约规则来执行，区块链验证相关合约的执行效果，然后将执行过程自动化，真正重塑商业流程。智能合约可以执行复杂的**多方协议**，而这是任何单一组织无法做到的。

智能合约在需要高程度多方高效合作的场景中会起到提高效率，减少人为错误的作用。比如，在贸易金融中，智能合约可以推动简化全球商品转移，带来更高资产流动性。智能合约还可以防止欺诈，提高交易的透明度和效率，并加强身份的可信度。此外，智能合约还能降低审计成本。在汽车行业，智能合约可以自动化保险索赔流程，提供接近瞬时的处理，验证和付款流程。智能合约可以简化交易后的流程，消除每个交易对手履行的验证交易，在适当的贸易活动中减少重复过程。

对于存在以上业务需求的系统，可以考虑采纳区块链作为业务系统（一部分）的底层技术支撑。

4.1.3 身份管理和授权是否重要

区块链由于引入了非对称加密算法，对身份认证和授权有天然的支撑。

通过利用 hash 算法、加解密算法、数字证书和签名（盲签名、环签名）等技术，区块链可以用于创建**身份管理**系统。结合公钥基础设施（ ）PKI ）解决方案用于广义的验证，

可以形成广泛参与的区块链身份验证系统，参与方可以包括政府机构、金融部门。通过使用区块链身份管理系统，可以提高大型机构的效率，特别是可以解决当前重复验证流程问题。此外，区块链身份验证系统可以有选择的显示人身份信息，这可以有效防止身份被盗以及加强维护用户的隐私。

而当数据被放置在区块链上后，使用数字签名技术，能够让获得**授权**的人才可以对数据进行访问。通过私钥既保证数据私密性，又可以在需要的时候将数据以点对点加密的方式共享给授权机构或个人。接收加密数据方则可以利用密码学算法解密得到明文内容。这样的特性对于要求监管数据不可篡改，而在必要时候解密明文以解决争议问题或监管问题的商业场景非常有用。比如个人体检报告入链后可以以加密的形式存在，当个人与保险公司发生业务时，可以授权保险公司查看个人过去的健康状况。这样，保险公司可以验证体检报告从入链开始未被篡改，而个人可以保证体检报告不会被除保险公司以外的其他节点读取。

4.1.4 对流程效率、透明度与安全的要求

基于账本天然去中心化的特质，区块链对于处理特别多方参与的分布式、多步流程尤其高效。跨组织使用区块链这样的分布式数据库可以极大地减少人工对账需求，因此大量节约成本。此外，某些情况下（比如反洗钱领域），区块链可以让各组织获得共同能力，免除重复劳动。在多方贸易金融场景中，金融机构们将可以获得更顺畅的清算和结算流程，减短结算窗口，避免大量的资金和运营成本。在资本市场应用场景中使用区块链技术可以显著降低成本。

区块链会促进多方交易中的透明度。区块链的本质决定它是一种分布式的数据库，被多个节点维护和同步——比如，多个频繁互相交易的对手方。此外，交易数据必须在

各方间保持一致，才有可能被加入区块链。这就是说从设计上多方能访问同样的数据（某些情况下机构内部的本地数据）——因此极大地增加了透明度，而传统系统依赖于多个躲在防火墙后面的“私藏”数据库，从外部是不可见的。

区块链还可以增强安全性与互信，减少欺诈。由于每笔交易都单独加密，且这样的加密被区块链上其他各方验证，任何试图篡改、删除交易信息的行为都会被其他各方察觉，然后被其他各个节点修正。区块链依赖加密验证交易，会验证涉及交易的各方身份。这确保如果没有涉及各方的同意，一个“错误的”交易不能被加到区块链上。每次要向区块链加入一笔新的交易就需要进行一次复杂的数学计算，哈希计算，这取决于交易数据、涉及交易的各方身份和之前交易的结果。现有区块链依赖先前的区块链这一特性确保了恶意参与者不能篡改交易历史记录。这是因为如果改变之前的交易数据，现有的哈希值将受到影响，不能与账本的其它备份匹配。

4.2 区块链形态选择建议

区块链形态主要分为三大类：公有链、联盟链、私有链。

公有链属于开放网络，对公众开放，任何人、任何节点都可以参与到区块链的计算中，而且任何人都可以下载获得完整区块链数据（全部账本)。比特币是一个公有链的大规模应用，对等节点组成网络和匿名支付是它的一大特点。公有链不合适金融机构或对可控和隐私性要求更高的机构。

联盟链是一种许可型网络，具有一定的保密性质或是具有某种授权机制。每个参与节点的权限都完全对等，均可以记账。大家在不需要完全互信的情况下就可以实现数据的可信交换，R3 组成的银行区块链联盟要构建的就是典型的联盟链。

私有链同样是一种许可型网络，其记账节点由私有链中最高权限者拥有，其他参与

方只参与交易，不参与共识。对于企业用户或是个人组织来说，使用私有链，将可以使自己的帐本不暴露在公有链中，例如公司的财务数据，或是消售记录数据。

商业上的应用主要是联盟链和/或私有链，应用的核心是对于参与方的身份进行验证，通过验证后才能进入正常的交易过程中，交易通过参与方共同约定的共识机制达成一致。

4.3 区块链与新一代信息技术结合建议

4.3.1 区块链与物联网

物联网(IoT)促成了设备之间的相互连接和信息的共享，估计到 2020 年 IoT 设备数量将会达到 20—200 亿，然而，这个发展中的行业仍然缺乏一个标准化的安全体系来对抗数据被盗，以及连接设备输出被黑客攻击等安全风险。

当应用于物联网时，区块链的概念开辟了无限的可能性。区块链将使设备实现自我管理和维护，省去了巨大的云控制中心的维护费用，降低了物联网设备的后期维护成本。通过为设备生成私钥，保证用户的个人数据不被外人窃取，提高了物联网的安全性。两者若能优势融合，将能爆发不可估量的经济效益。

4.3.2 区块链与大数据分析

大数据分析是实现数据价值的核心。在进行数据分析时，如何有效保护个人隐私和防止核心数据泄露，成为首要考虑的问题。再者，在交易过程中，数据本身流通的监管比较难，对整个数据流通的全过程缺乏一种全程跟踪的手段，数据安全的保护、数据服务变现等方面都存在各种各样的困难，使得今天的大数据应用也是遇到了很大的瓶颈。

区块链技术可以通过私钥签名、加密技术来防止这类情况的出现。当数据被哈希后放置在区块链上，通过数字签名技术，允许获得授权的参与方对数据进行访问。在区块

链之上，数据可以确权、数据从可复制粘贴的资源变成有价值的数据资产，从而促进数据的交易互换，进而提升大数据分析的价值。

4.3.3 区块链与人工智能

人工智能代表一种全新的计算和决策模式，它包含信息分析，自然语言处理和机器学习领域的大量技术创新，能够助力决策者从大量非结构化数据中揭示非凡的洞察。

区块链可以打造一个人工智能驱动的网络，解决数据的信任与安全问题。人工智能从区块链网络中获取必要的数据，输出有价值的结果，通过区块链安全可靠地传递给参与方或者设备，让交互更加智能、具备更有思想，更友好的和人类及其他设备沟通交流。