荣泽区块链数字存证系统
（DCS）
产品白皮书

目录

1 前 言 2

2 概 述 4

2.1 亟需解决的数字资产安全问题 4

2.2 区块链数字存证系统保护数据安全 6

2.3 产品优势 7

3 产品概述 9

3.1 功能架构 9

3.2 功能介绍 9

3.2.1 产品服务 9

3.2.2 底层服务 10

4 应用领域 11

4.1 政务领域 11

4.2 供应链领域 11

4.3 物联网领域 11

4.4 数据服务与共享 11

4.5 数字版权领域 12

5 联系我们 12

1 前 言

当今社会，随着企业的信息化程度越来越高，数据已经成为企业、个人最重要的资产之一。 然而近年来围绕着数据安全发生的事件却越来越频繁，尤其是个人与企业的隐私信息保护是行业关注的热点话题。

据调查分析，企事业单位中的办公电脑、工作站与个人桌面机中的海量数据有 65%的数据完全没有保护措施，20%的数据没有完整的保护方案，而只有 15%的数据做了专业的保护。计算机病毒、服务器硬件被盗或损坏、离职员工的恶意删除、数据库文件损坏等人为误操作或物理安全隐患因素等，时刻威胁着企业的数据安全。

GDPR 法案的推出，在一定程度上推动了全球数据安全相关法规、标准的建立和完善，也使得企业的数据安全合规压力陡增，多数企业把数据安全摆在了整个信息安全体系提升的最重要的位置。然而，数据安全牵扯到了信息化的各个层面，在企业探究构建完善的数据安全体系时发现：数据安全体系建设是一项体系化工程，而非简单的技术工具运用。它是个复杂的大工程，从信息安全单个部门基本无法推动，尤其是一些 IT 建设有诸多历史问题的企业，如果要达到法规和标准的合规要求，甚至要考虑信息系统的重构。当前，摆在企业信息安全管理者面前的问题是：如何平衡合规压力和无法改造的复杂业务和信息系统。企业应该构建哪些必备的模块化的数据安全能力，实现数据治理，即保障核心数据安全的同时又做好与权限相符的隐私数据保护工作。

荣泽区块链数字存证系统（Data Coffer Service，DCS）是一套集区块链、非对称式加密、分布式存储等现代核心技术于一体的数据存管服务产品。保证数据存储后永不丢失、永不泄漏；并且利用已存储数据的相关行为信息，结合可信时间戳（支持国家授时中心提供的航天级时间戳），将所有行为记录进行串联，组成一条完整的，不可篡改的溯源链；区块链数字存证系统还可结合大数据分析的风控模型，用全流量分析技术实现对关键行为事件的感知、理解并预测，快速响应可疑事件。

相对于传统的数据存证系统，荣泽区块链数字存证系统具有更好的安全性、更高的私密性与更强的容灾能力，能够为企业提供更高安全系数的核心数据和文件加密的存储服务，协助企业实施高效、便捷、安全的数据治理工作，建立合规

的数据安全体系。

2 概 述

2.1 亟需解决的数字资产安全问题

数据资产安全保障在日常工作中会因为很多问题而收到威胁，因此我们收集和汇总了企事业单位在数据安全建设过程中遇到的一些问题，归纳下来，比较突出的有以下六个方面：

2.1 数据资产清册问题

数据资产清册问题主要体现在如下三个方面：

1）资产状况不清

到底拥有多少数据资产？数据资产的变化情况是怎么样？是否有不明资产和违规资产？实际资产与在册资产是否存在差异？差异情况如何？敏感数据有哪些？都存储在哪里？

2）访问状况不清

访问热度如何？有哪些静默资产？哪些是高频资产？敏感数据都在被谁访问？是否存在僵尸库？

3）权限状况不清

数据资产的权限变化情况是怎么样的？在某时段内是否发生了提权操作？都有哪些数据帐号？帐号都在被谁使用？帐号的权限是否与登记的有差异？是否有弱口令帐号？是否存在帐号权限过大、违规的情况？

以上三个方面的问题都是资产不清的具体问题。数据资产梳理是一个持续的过程，数据和业务是不断发生变化的，因此，需要借助工具来开展数据资产管理工作。准确掌握数据资产状况，是开展数据安全体系建设的基础条件。

2.2 管理责任不清

目前国家施行的法律法规通常都会要求明确数据责任，通过加大惩罚力度，来提升数据安全防范意识，规避“数据资产无人管、数据资产随意用”的现象，数据资产责任不清主要体现在如下两个方面：

1）数据资产未认责

数据资产体量大，且使用复杂，贯穿整合业务流程，涉及多个部门和岗位的人员，数据的所有权，使用权，安全责任等无法清晰划分；同一资产涉及多个部门或团队使用，且使用频率和重要性无法量化，导致资产认责工作无法开展；

2）管理角色的职责边界模糊

数据安全管理角色包括数据资产管理员、数据库管理员、安全审计员、安全检测工程师、数据运维工程师、权限管理员等，一般情况下这些角色可能会由研发、运维、安全、运营人员来兼任，没有独立的团队或虚拟团队，导致权责不清，不利于整体提升数据安全防护能力。另外，一旦发生数据安全事件，很难开展追踪溯源工作。

2.3 制度不完善

1）制度规范未落实或难落实

制度规范是数据安全管理和安全技术落地的依据。在开展制度规范编写工作时，由于没有对现状进行充分的调研，管理制度规范与实际技术措施无法对应，导致数据安全体系无法落实。

2）缺少稽核手段

建立了一套切实可行的制度规范，进行了相关的贯彻与执行，但由于缺少稽核手段，安全管理部门无法及时掌握执行情况。数据安全管控措施无法按照管理制度体系要求严格执行。

2.4 数据交换管理混乱

随着数据应用的快速发展，企事业单位内部向外提供的功能越来越多（小程序、公众号、APP、Web 等），数据会向外部、内部和合作伙伴进行交换共享，随着开放的接口越来越多，交换关系越来越复杂，若未将交换共享的方式和接口标准化，则会出现功能重复、调用复杂、多点登录等现象，运维人员和应用系统负责人的压力也会倍增，影响数据应用的发展。

2.5 安全技术措施零散

1）数据安全产品功能分散

现有的数据安全产品，大多都是单一数据安全功能，如：脱敏，加密，防泄密，企业部署了很多数据安全类产品，再加之企业数据分布也相对分散，导致各各网络区域各数据安全产品间无法形成有效联动和和整合机制,导致数据安全管控能力分散，无法形成统一数据安全管控体系。

2）安全能力孤岛

由于组织内部的应用会按照部门划分,数据安全能力的建设也会以部门为单位开展，没有形成整体的防御体系，造成安全短板，容易被不法人员利用。

另外一个维度是角色和职责不明确，IT 各部门没有将安全责任进行清晰的划分，当发生数据安全事件时才考虑防护。即便是有主动建设的意愿，也是各自申请各自建设。

2.6 审计能力不足

通过对全栈日志的收集与分析，能够有效的制定安全规则，在大量的访问中自动发现违规和高危行为，降低了数据安全管理员的工作量和风险识别的难度，同时也提升了准确率。

但是，当遇到“心脏滴血”、APT 这类攻击时，由于这种攻击是用真实的身份、合规的操作，做非法的事情，所以攻击的操作轨迹和规律很难被发现，加之这类攻击并没有触碰到现有的规则，导致安全攻击一直在发生，管理人员却一直不知道。

2.2 区块链数字存证系统保护数据安全

区块链数字存证系统的核心功能是基于许可区块链的数字资料管理器,通过便捷的图形化界面提供数字资料创建、浏览、保存、状态变更、行为追溯等功能，通过对基于区块链的数字资料的各种操作实现数字资料的可信存储与管理,为构建可信体系提供技术实现手段。

区块链数字存证系统对数据的防护主要表现在防泄露、防篡改、防滥用三个基础方面。

防泄露：数据被违规违法窃取，可能用于商业分析、诈骗、骚扰营销、倒卖等，造成数据主体和运营方的名誉损失或财产损失，甚至造成刑事案件的发生，因此，防止数据泄露是数据安全防护的重点。

防篡改：数据篡改一般发生在内部，由于利益的驱使，数据管理人员、运维人员、开发人员等具有较高权限且了解数据逻辑的人员对数据进行非正常修改，达到为他人或自己获利的目的，例如违章信息删除、摇号信息换人等等。如果没有很好的控制数据防篡改，则将会导致业务运转混乱，大大降低公信力。

防滥用：数据是企事业单位的核心资产，合理使用数据可以带来新的机遇。反之，如果没有严格的控制数据使用，使数据泛滥，将会降低数据价值，丧失竞争力，甚至会在生态中被淘汰。数据被滥用场景举例：a.项目的建设方或运营方在业主方不知情的情况下利用身份的便利条件分析数据;b.产品侧没有很好的做数据规划，导致数据使用场景过多、可接触到数据的节点过多。

区块链数字存证系统未来将打造数字资产生态,为可信数据的流动提供支持,帮助企业把可信的数据转变为资产，让数据资产在生态间相互流转，从而使企业的数据资产转变为企业提供的服务，更好的为企业赋能。

2.3 产品优势

区块链数字存证系统解决释放数据价值过程中面临的诸多问题,区块链数字存证系统以体系化的方式实现数据的可存、可得、可用、可追溯、可预警，用较小的成本获得较大的数据收益，具体体现在以下六个方面：

一是保障数据存储安全。数据的存储安全是数据资产管理的底线，与集中式的云存储服务不同，比如 Google Drive（它存储了所有文件，包括系统中删除的文件）。区块链数字存证系统将数据文件存储于分散的区块链网络，数据文件被分解并分布在多个节点上,这个过程叫做分片,并且这些文件是用私钥加密的,这使得参与网络的任何其他节点都不可能查看该文件。分片确保文件只是原始自

我的一小部分，这意味着读取它们的全部内容是不可能的。

二是全面掌握数据资产现状。数据资产管理的切入点是对数据进行全面盘点，为业务应用和数据获取夯实基础。从资产化管理和数据权属分类的角度出发，快速的检索和链式结构的追溯帮助业务人员快速精确查找他们想要的数据，成为对数据资产管理进行有效监控的手段。

三是保障数据隐私安全。数据的隐私安全是数据资产管理的底线，区块链数字存证系统在技术层面，采用加密、去标识化等安全技术措施保障数据隐私。融合多方计算、区块链、联邦学习等敏感数据隐私处理技术，保障数据授权隐私化使用，达成隐私数据“可用不可见”，实现数据价值发挥和个人隐私保护之间的平衡。

四是完整的行为追溯。完整不可篡改的行为日志数据是区块链解决方案的一部分，每次对链上数据产生的检索、查看、修改等行为信息，都保证有可信的时间戳，并且永久被存储在区块链上，不能更改。产生安全事件时，通过对历史行为的追溯，可以有效的发现漏洞，找出事故源头。并且基于可信的行为日志，结合大数据分析的风控模型，用全流量分析技术实现对关键行为事件的感知、理解并预测，快速预知响应可疑事件。

五是将实现数据互联互通。数据资产管理通过制定企业内部统一的数据标准，建立数据共享制度，完善数据登记、数据申请、数据审批、数据传输、数据使用等数据共享相关流程规范，打破数据孤岛，实现企业内数据高效共享。

六是将对接司法系统。使数据资产得到司法级认证，享受司法保护。使企业在遇到行权、维权等相关法律诉讼中，可由司法系统快速调用出具有法律效应的证据与证明。保护企业自身权益不被损害。

3 产品概述

3.1 功能架构

荣泽区块链数字存证系统主要业务架构如下：

区块链数字存证系统以荣泽区块链技术 RBC+RBaaS 为基础，用哈希链的数据结构改变了电子数据易被篡改的属性，用“区块+共识算法”解决分布式系统的数据一致性问题，拜占庭容错能力保证跨实体运行的系统不受少数节点恶意行为的影响，从而解决业务层面的信任难题，保障了企业数据资产管理的全流程安全。

3.2 功能介绍

3.2.1 产品服务

3.2.1.1 WEB

支持企业用户通过区块链数字存证系统提供可视化控制 Web 窗口，完成数据在区块链存证系统中各种业务的操作。包括文件存证、数据存证两大主要存证业务。

3.2.1.2 API

提供通用的 API 接口，方便企业现有系统、设备的对接。

3.2.1.3 存证芯片/继承电路

荣泽自主研发的通用区块链登记模组，利用 5G+物联网+边缘计算技术，快速使现有设备具备上链登记数据的功能，保证端到端的数据可信。

3.2.1.4 认证的智能设备

通过认证的区块链采集设备一体机，直接将采集数据进行上链登记，如执法

记录仪、工业摄像头、审讯记录仪、摄像扫描一体机等。

3.2.2 底层服务

3.2.2.1 底层公共服务

底层公共服务是建立在区块链一体机基础上提供的公共的、通用的、基础的底层业务基座，在区块链技术基座之上，业务基座包括可信企业身份与通用存证两大基础服务。可信企业身份与通用存证两大基础服务可包括的服务有：电子签名、存证服务、认证服务、时间戳服务、CA 证书、公证节点、个人/企业认证、可靠时间源等。

3.2.2.2 存证综合服务平台

存证综合业务平台，是基于原有的基础服务向外拓展的面向于各具体业务线的服务平台，相对于基础的存证服务，存证综合业务平台的范围更广、内容更多、功能更强。业务方向包括有：产业线内的人/机/物的管理与溯源、数据/文件的管理与授权、公证/出证的电子网络、基于行为的态势感知安全预警、可信的数据资产交易、全面的配置中心等。

3.2.2.3 区块链一体机

荣泽国产区块链软硬件一体机是一款高性能分布式全量账本服务器，集成了荣泽自主可控区块链底层技术平台 RBC，与帮助用户创建、管理和维护企业级区块链网络及应用的服务平台 RBaaS。

旨在降低政府、企业用户使用区块链的难度，轻松一键部署高可靠、高可用的区块链网络。具有强隐私、高性能、高安全的技术优势。真正做到开箱即用，将用户从复杂的安装部署与调整优化中解放出来，大幅度降低规划难度，节省成本、简化运维。

4 应用领域

4.1 政务领域

政务信息化发展的难点在资源整合与应用，打破“各自为政、条块分割、烟囱林立、信息孤岛”的问题。由于业务烟囱的存在，其业务系统间不同数据格式、不同数据标准、不同数据管辖权造成了数据鸿沟，以及行政资源的浪费与行政效率的低下，无法实现政府内部纵向或横向协同，跨部门业务由业务申请人在数个政府部门之间奔跑传递。利用可信企业身份平台管理数据的所有权、管理权、使用权等，更好的服务于政务，有助于打破信息孤岛、促进协同、降低成本提高效率、提升政府透明化治理等作用。

4.2 供应链领域

供应链是一个商流、物流、信息流、资金流所共同组成的，并将行业内的供应商、制造商、分销商（零售商、批发商）、终端用户串联在一起的复杂网链结构。这种复杂的网链结构需要统一的识别码将不同系统中的组织、人、机、物等关联起来，而可信企业身份作为一种统一的数字身份平台，结合可信存证，与生俱来地适用于供应链领域。例如：物流、溯源防伪等。

4.3 物联网领域

物联网（IoT）蓬勃发展的今天，它不仅给个人消费带来变化，还给整个社会发展带来了深刻变化。目前，大型的物联网平台依靠中心化模型控制各个电子设备之间链接与交互，但是在很多场景下，这种方法变得不是那么实际。而可信身份平台正好可以解决这一问题。可信身份平台可以帮助管理物联网平台的各电子设备的关系、管理电子设备的所有权、管理权、使用权以及其产生的数据的所有权等，保证数据的安全性和可信性。可以企业身份在工业设备、智慧交通与智慧城市等领域都可以有很好的应用。

4.4 数据服务与共享

数据作为数字经济的生产资料，只有流通起来才能产生社会价值与经济价值。目前数据的流通面临数据的权属问题，即数据的所有权、管理权、使用权、受益权等。利用可信企业身份可追溯、不可篡改的特性，可以确保数据权属的真实性，同时保证身份的不可伪造性。同时利用智能合约，数据可用不可见，进一步保护

用户隐私以及数据生态的利益。

4.5 数字版权领域

版权领域的痛点还在于维权门槛高，传统数字内容的版权维护路径，需要内容生产者向监管部门提出版权认证申请，需要耗费较多的时间与金钱。但处于区块链的环境下，内容生产者或机构都可以通过加入区块链网络社区，方面快捷的实现内容上链，版权登记。版权内容生产者将自己的作品传到区块链平台上，平台为作品生成一个不可篡改、准确原创证明的唯一 ID，证明版权的归属和完整性，并同时记录到链上，维权成本和门槛极低。

在维权门槛较低的同时，区块链数字版权的法律效力也能得到保障。相比传统的维权取证来源，监管部门更看重维权取证的证明力，而区块链的数字维权证明有别于人为的信用委托，更趋向与数据代码构成的技术背书，同时公信力更有效。

通过区块链技术，还可以对作品进行鉴权，证明文字、视频、音频等作品的存在，保证权属的真实、唯一性。作品在区块链上被确权后，后续交易都会进行实时记录，实现数字版权全生命周期管理，也可作为司法取证中的技术性保障。

5 联系我们

官网：http://www.rongzer.com/

地址：南京市浦口区江北新区研创园腾飞大厦 B 座 17 楼

电话：18551702841

邮箱：ding.dan@rongzer.com