**【AC4\*】基于令牌的访问控制**

摘要：传统的集中式访问控制在健壮性、可信性和可循环性等方面存在不足。区块链具有容错和信任的优势。智能合约具有自动执行和灵活扩展的特点。令牌可以很好地记录凭证信息，并且易于传输。本文将区块链、智能合约和代币相结合应用于访问控制，以解决传统访问控制的不足。首先，简要介绍了访问控制、区块链、智能合约和代币。其次，给出了访问控制令牌的一般数据结构，详细阐述了访问控制令牌的等价、拆分、合并和验证算法，并阐述了基于令牌的访问控制系统结构。最后，通过一个基于令牌的访问控制仿真系统，验证了基于令牌的访问控制在健壮性、可信度、流通性、并发性等方面具有一定的比较优势。

本文将区块链、智能合约和代币统一起来，将区块链作为一个可信、安全的存储和运营环境，充分利用智能合约自动执行和代币高效智能流通的特点，提出了一种基于令牌的访问控制（TBAC）。TBAC的解决方案旨在实现以下目标：1）分布式可信访问管理模式；2）灵活高效的访问传输模式；3）高频率容错访问执行机制。

将令牌应用于访问控制，以区块链网络作为存储、认证和流通环境，以智能合约发布和应用为逻辑处理形式，以令牌为数据体，记录访问控制的规则和逻辑，执行访问控制的认证处理，确保正确的主体正确地访问正确的对象是一种称为基于令牌的访问控制的访问控制模式。

结构：分布式数据共享是一种典型的分布式应用系统。基于TBAC的分布式数据共享技术机构如图3所示。在基于TBAC的分布式数据共享体系结构中，主要有以下几个对象。

1. 数据提供程序（DP）。作为数据共享网络的供应方，数据提供者可以是数据的生产者、管理者、经营者等，数据可以分为各种类型，如结构化数据、非结构化数据、原始数据和二次处理数据。随着5G时代的来临，越来越多的数据以分布式的状态在多个对象数据库中生成和存储，这些数据库可以是一个专有的数据库，也可以是大型的共享数据中心。为了向更多的需求方提供数据服务，在该方案中，许多数据提供者通过数据服务节点在区块链上注册自己的数据，以方便对需求方的搜索和获取。
2. 数据请求者（DR）。作为数据共享网络的需求方，数据需求方可以是个人、企业、机构等。数据需求者通常需要从多个数据提供者获取数据。他们可以通过数据服务节点直接从区块链进行搜索，或者在区块链上注册自己的需求，以方便数据提供商按需提供数据。数据需求方只能根据数据提供者发布的、数据所有者授权的ACT，通过数据服务节点向数据提供者请求数据访问。
3. 数据所有者（DO）。作为数据共享网络中数据认证的主体，数据认证主要决定数据所有权的主体。未经数据所有权主体许可，数据的其他角色不能非法处理数据。数据的所有权可以是单一的独占实体，也可以是多共享的实体。同一个实体也可能有大量的数据分布在不同的数据库中。因此，在该方案中，数据认证也记录在区块链上，实现分布式授权。在现实中，DP和DO可以是同一主体，也可以是单独的主体。区别在于数据是由DO本身管理和提供的，还是由DP代表它来管理和提供的。DP和DO可以是ACT的独立或联合发布者。
4. 数据服务节点（DSN）。数据服务节点是一个区块链节点，通过TBAC程序进行发布。ACT的产生、撤销、转移和处理可以通过TBAC程序和区块链程序共同实现。通过数据提供者和请求者的连接，可以实现分布式授权和分布式权限处理的目标。数据服务节点可以在网络中进行多个分布式部署，数据提供者和数据请求者可以灵活地选择不同的数据服务节点来提供或获取数据服务。
5. 区块链。区块链作为一种分布式数据共享数据服务总线（DSB:data service bus），既是ACT的存储载体，也是ACT的执行环境。它的特点有助于形成开放的访问控制机制，突破传统访问控制机制的安全瓶颈、并发瓶颈和流程瓶颈。

基于TBAC的分布式数据共享主要通过DSN来实现。在这个节点上，不仅需要一般的区块链节点服务功能，还需要访问控制的基本功能。这些功能包括管理、判断和ACT过程。

1. ACT管理（ACTM）：主要实现ACT的产生、撤销和转移等功能。为了更方便地实现对ACT的管理，除了建立ACT数据库外，还需要创建和管理metadata数据库和ACT模板数据库。metadata是正确理解和统一整个系统语义的基础。任何授权的节点应用都可以通过该模块根据需要创建管理访问控制的基本信息，并将相应的密钥信息和原始数据以哈希的形式存储在区块链上。ACT模板是为了方便ACT的创建和统一管理而设计的，ACT的metadata、ACT模板和其他原始数据可以直接保存在区块链上，也可以保存在链下分布式数据库中。考虑到链上不能保存太多的数据，因此最好使用链下的分布式数据库。
2. ACT判断（ACTJ）：从ACT处理器获取访问请求，并根据访问请求调用相关的ACT信息、metadata信息和ACTT信息，根据访问控制规则计算逻辑，最后给出访问控制决策结果并返回给ACT处理器。
3. ACT过程（ACTP）：用于接收来自数据请求者的访问请求，调用ACTJ来决定是否以及如何开始数据访问，最终通过数据提供者提供的通道获取允许的对象数据。

为了降低仿真的复杂度和专注度，元数据、ACTT和ACT直接保存在区块链上。Fabric的默认块大小为64M，可以满足大多数数据存储需求。在实际环境中，原始数据可以保存在链外，相应的数据索引可以保存在链上。系统提供了三个基本功能：ACT发布、ACT传递和ACT应用。

1. ACT发布通过DO0和DO1进行，DO0根据许可优先permit priority规则为medicalexam DP、transportation DP和Science area DP设置ACT1、ACT2和ACT3，DO1根据拒绝优先deny priority规则为education DP和IPR DP设置ACT4和ACT5。所有ACT在链上建立并记录后，可以通过区块链浏览器进行查看，这些ACT由DO和DP共同批准，并由区块链上的其他节点见证。
2. ACT传递可分为三种类型：完全转移、分割转移和合并转移。将ACT1从DO0转移到insurance DR是完全转移，将ACT2的一部分从DO0转移到traffic police DR生成新的ACT21，将ACT4从DO1转移到employment DR生成新的ACT41是拆分转移，将ACT2和ACT3合并到DO1生成新的ACT23，ACT4和ACT5生成新的ACT45是合并转移。所有被转移或生成的ACT都可以通过区块链浏览器查看。
3. ACT应用是TBAC的目标功能。每个DR根据其拥有的ACT请求相应DP的数据。在接收到请求之后，DP首先通过区块链验证来验证请求所基于的ACT。如果ACT不符合要求，将被拒绝。如果ACT存在，则启动访问控制决策，并根据决策结果执行访问操作。在该系统中，insurance DR根据ACT1向medicalexam-DP发送访问请求，traffic police DR根据ACT21向transportation DP发送访问请求，employmen DR根据ACT41向education DP发送访问请求，DO1可以根据ACT23向transportation DP或scenic area DP发送访问请求，DO0可以根据ACT45向education DP或IPR DP发送访问请求。

总结：本文结合区块链、智能合约和ABAC的特点，提出了一种新的基于ACT的访问控制机制TBAC。与传统的集中式访问控制相比，TBAC在安全性、可靠性、流通性、并发性等方面具有一定的比较优势，TBAC在分布式数据共享中的应用有利于形成一个具有抗攻击、高容错、抗篡改、抗抵赖的数据服务网络，易扩展、高并发性，更好地促进更大范围的数据互联。

本文在讨论链上ACT的存储时，也将其透露给整个区块链网络。虽然其他节点不能使用该ACT，但通过对该ACT的分析，有可能获得一些持有者不愿意公开的信息，比如他们的权限信息。因此，本文下一步的工作就是如何保证该ACT的信息不被泄露，但可以被证实。

实际上就是把访问策略放在token中，token放在区块链上，用户根据Token中的限制确定自己是否满足访问策略。用户向区块链申请访问数据，区块链根据用户信息与数据的Token中的访问策略比对，如果满足则提供数据。

和Disac比不同之处在于：访问控制是由区块链完成的，Disac的访问控制是在每个用户本地完成的。区块链避免了风闻控制的单点失效问题，但需要构建一个相对比较完善的系统，比如需要区块链中的多个peer提供服务。并且如果数据提供方和数据所有方不是同一个体，则数据明文放在数据提供方处也有一定的风险。

**【AC7\*】AuthPrivacyChain：一种基于区块链的云端隐私保护访问控制框架**

摘要：云是一种提供共享和支持无处不在的按需访问计算的计算模式，为许多行业提供了新的数据处理和服务，显著降低了用户的计算和存储成本，提高了易用性。随着云规模的不断扩大和云计算的集约化，云安全已经成为云计算领域的一个重要问题。访问控制是保护企业和个人存储在云中的敏感数据的关键安全技术之一。由于云端采用集中访问控制机制，云中的敏感数据容易被黑客或云内部管理人员篡改或泄露。为了解决这个问题，我们提出了一个基于区块链的访问控制框架，该框架具有隐私保护功能，称为AuthPrivacyChain。首先，我们以区块链中节点的账号地址作为身份，同时重新定义云数据的访问控制权限，并对云进行加密存储。在此基础上，设计了AuthPrivacyChain中的访问控制、授权和授权撤销过程。最后，我们实现了基于authChain的授权用户访问企业资源的安全机制（authChain），并最终实现了基于授权链的用户访问隐私的安全机制。

本文提出了一种基于区块链的访问控制框架AuthPrivacyChain来解决上述问题。我们的贡献如下：

1. 分散访问控制体系结构。Authprivacychain利用去中心化、防篡改的区块链[23]-[25]存储访问控制权限，以区块链账户地址为身份，设计访问控制、授权和授权撤销流程。
2. 授权隐私保护。由于区块链的透明性，很容易泄露用户隐私。Authprivacychain在区块链中加密存储访问控制权限，有效保护用户隐私。
3. 安全。Authprivacychain不仅能保证资源的机密性、完整性、可用性、真实性和责任性，还能抵抗各种外部和内部攻击。

为了解决上述问题，我们提出了一种基于区块链的访问控制框架AuthPrivacyChain。本节包含系统模型、初始化、访问控制、授权和吊销。系统模型如图2所示，由四个实体组成：

•云。它为用户提供身份验证和数据存储。云通过区块链确定DU或DO的访问权限。

•区块链。它具有开放、透明、防篡改、不可逆等特点，与分布式数据库一样，我们将其作为访问控制的授权策略数据库。

•DO。将资源上传到云并发布资源对区块链的访问权限。

•DU。如果DU有云的许可，他可以访问这些资源。

我们假设云是半可信的，即云的软件、硬件、非对称密钥和业务流程是可信的，而云SA是不可信的。区块链被认为是可信的。首先，将资源上传到云端，然后通过区块链中的注册交易发布授权。DU向云发送资源请求，云查询区块链，判断请求是否有权限，最后回复请求。

云、DU\DO先在区块链上注册，拥有账号和私钥等信息。当有数据资源发布时，数据上传到云端，数据的metadata发布到区块链上，这两个步骤都可以通过区块链的功能完成。访问控制是用户在云中请求资源，云根据区块链中存储的权限决定用户是否可以访问资源。如果用户有权限，云将允许用户访问资源，访问记录将存储在区块链中。

授权相关信息直接存储在区块链中。访问记录也存储在区块链中。对于性能，在身份验证方面，AuthPrivacyChain优于传统的访问控制，因为它使用Addr而不是用户名和密码。在身份认证授权和访问控制方面，AuthPrivacyChain略低于传统的访问控制，因为它需要访问区块链，但可以通过选择合适的超级节点来访问区块链来缩小差距。

还是针对云存储，只是访问控制转移到区块链上了。

# 【区块链\*】基于区块链的分散存储系统中细粒度访问控制的数据共享框架

摘要：在传统的云存储系统中，基于属性的加密（ABE）被认为是解决数据隐私和细粒度访问控制问题的重要技术。然而，在所有的ABE方案中，私钥生成器（PKG）能够对云服务器中存储的所有数据进行解密，这可能会带来密钥滥用和隐私数据泄露等严重问题。同时，传统的云存储模式以集中存储的方式运行，单点故障可能导致系统崩溃。随着区块链技术的发展，分散存储模式已经进入大众视野。分散存储方法可以解决传统云存储系统中的单点故障问题，并且与集中式存储相比具有许多优势，例如价格低、吞吐量高。本文研究了分散存储系统的数据存储和共享方案，提出了一个将分散存储系统IPFS、以太坊区块链和基于属性的加密（ABE）技术相结合的框架。在该框架中，数据所有者能够为数据用户分配密钥，并通过指定访问策略对共享数据进行加密，从而实现对数据的细粒度访问控制。同时，基于以太坊区块链上的智能合约，实现了对分散存储系统密文的关键字搜索功能，解决了传统云存储系统中云服务器可能无法返回所有搜索结果或返回错误结果的问题。最后，在linux系统和以太坊官方测试网络Rinkeby上对该方案进行了仿真，实验结果表明该方案是可行的。

这类云存储系统已经非常成功，并得到越来越多的认可，但由于此类系统只依赖于存储能力较强的大公司来存储和传输数据，而大公司则被视为可信的第三方，因此不可避免地继承了依赖单点故障的缺点第三方服务。即使云存储系统是为了数据可用性而备份的，云存储服务提供商仍然可能会受到某些不可抗力因素（如政治审查）的影响，导致用户无法访问自己的数据。另外，随着存储技术的发展，存储设备的成本越来越小。集中式云存储服务的成本主要来自员工工资、法律成本和数据中心租金等，这些固定的成本不变或逐渐增加。集中式云存储服务的价格将更高。

从以上观点来看，未来需要一种去中心化的存储方式，为人们提供数据存储和共享服务。它不需要相信第三方会诚实地为我们传输和存储数据，也不需要担心数据无法访问。幸运的是，随着比特币的出现，其底层技术区块链可以为这种分散存储系统带来优雅的实现。区块链的出现使我们能够将P2P加密货币与存储空间、带宽、CPU功率等连接起来。想象一下，我们可以通过互联网免费租用额外的硬盘空间，并从加密货币中获得回报[1]。用户不必担心自己无法访问自己的数据，因为数据的可用性可以通过部署在区块链上的智能合约来保证，他们只需为自己存储的数据支付定期费用。

在传统的云存储系统中，如果用户想秘密共享存储在第三方云服务器上的数据，就需要一种技术来实现对只有特定用户才能访问和解密的数据的访问控制。在这种需求的驱动下，基于属性的加密机制[2]（ABE）被提出并迅速发展。通过这种机制，数据所有者可以根据用户的身份和属性指定数据访问策略，实现对数据的细粒度访问控制。几乎所有的ABE加密方案都需要一个可信私钥生成器（PKG）来建立系统并为用户分发相应的密钥[3]。这样的制度有很多问题。首先，在现实中很难找到一个值得信任的PKG。其次，这样的系统存在密钥滥用的问题，用户数据的所有权没有掌握在自己手中。PKG具有解密服务器中所有数据的能力，PKG可能会因为某些利益或政治审查等原因而泄露用户数据。一旦数据所有者丢失了自己的密钥，他甚至无法解密自己的数据，PKG仍然可以解密用户的数据。在实际应用中，我们需要数据拥有者能够控制自己的数据并为用户分配密钥。例如，一个医院的数据管理员应该能够为他的医生和相关人员分发密钥，以便他们能够根据他们的位置访问不同级别的数据。

为了更好地保护数据的隐私性和可用性，我们应该将数据的存储和共享从集中式的云存储系统转移到分散式的存储系统，这种存储系统的价格比传统的云存储要低，既有数据吞吐量大的优势，又不必担心单点故障。在现有的分散存储系统中，实现数据的加密和存储非常简单，但如何解决数据的秘密共享是一个亟待解决的问题。本文提出了一个能够实现对分散存储系统中数据的细粒度访问控制的框架，并基于感兴趣的关键字对数据进行搜索。

（1） 我们提出了一个将分散存储系统IPFS、以太坊区块链和基于属性的加密（ABE）技术相结合的框架，以实现对分散存储系统中数据的细粒度访问控制。数据拥有者是唯一控制自己数据的人，系统不需要可信PKG，并且数据拥有者能够为数据用户分发密钥，这比传统的ABE方案更灵活。同时，利用以太坊区块链对用户的密钥进行管理，解决了传统ABE方案中的密钥管理问题。当用户忘记了自己的密钥时，他只需要从以太坊区块链中存储相应的交易数据，并对其进行解密以获得自己的密钥信息。

（2） 通过对共享文件建立加密关键字索引，将加密后的关键字索引信息存储在以太坊区块链上，并在以太坊区块链上部署智能合约，实现分散存储系统中的关键字搜索。智能合约一经部署，就会按照智能合约的逻辑诚信运作，只有用户检索到正确的搜索结果，才会支付服务费。该方案解决了传统云存储环境下搜索服务提供商不能如实返回搜索结果的问题。

（3） 在Ubuntu-linux系统下，通过以太坊官方测试网络Rinkeby对系统方案进行了仿真，并对相应的性能和成本进行了分析。

DO为申请的用户产生解密密钥，通过区块链分发，区块链同时还有搜索密文的功能。所以是区块链分发密钥+ABE加密完成了分布式的访问控制。不适用于DVCS的点有：1）一个合作的project会有很多的DO，每个人想获取新文件都需要向DO申请key的话过于复杂，DO的操作量也很大 2）不能支持DVCS的写访问控制