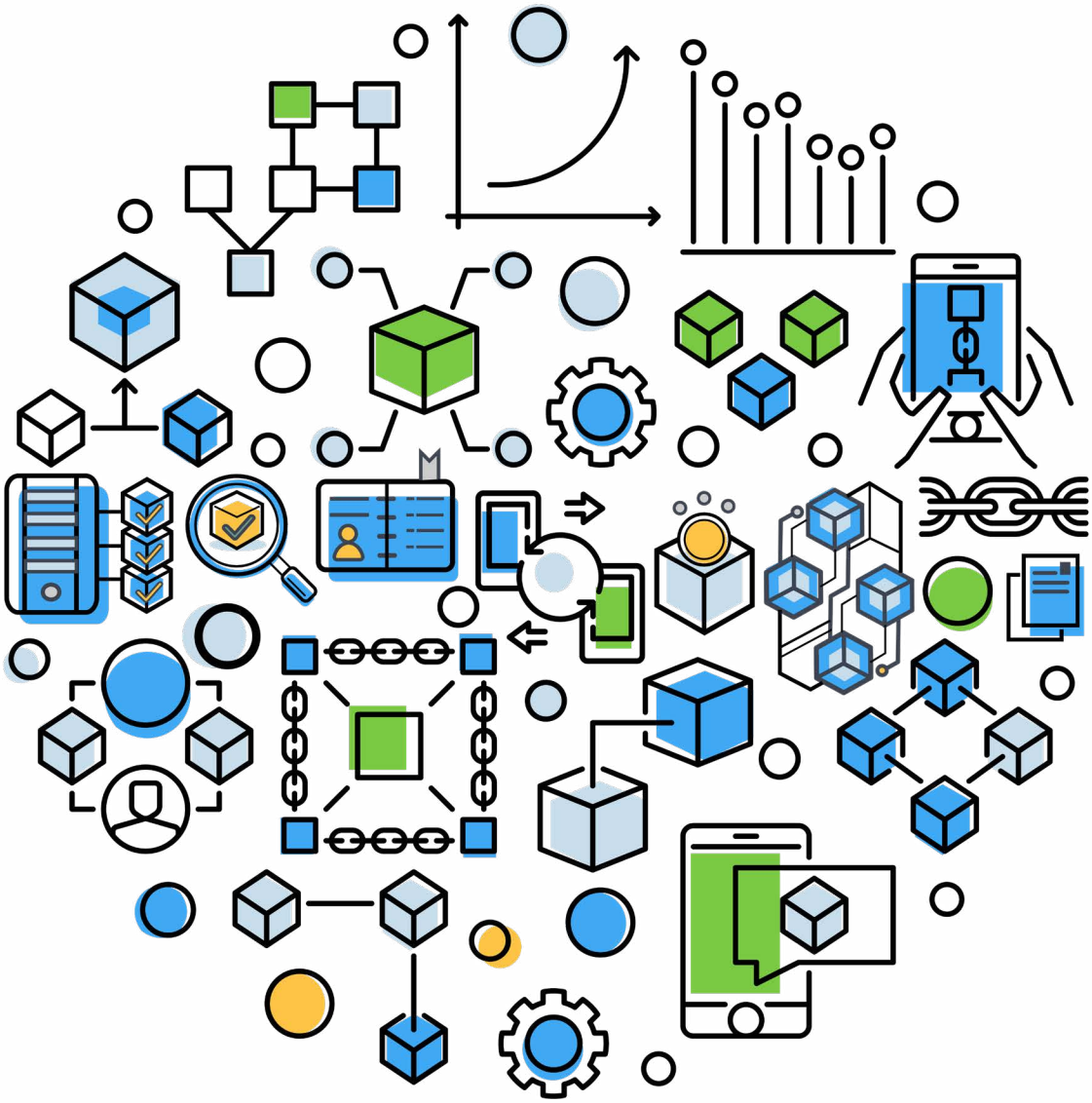
Deloitte.

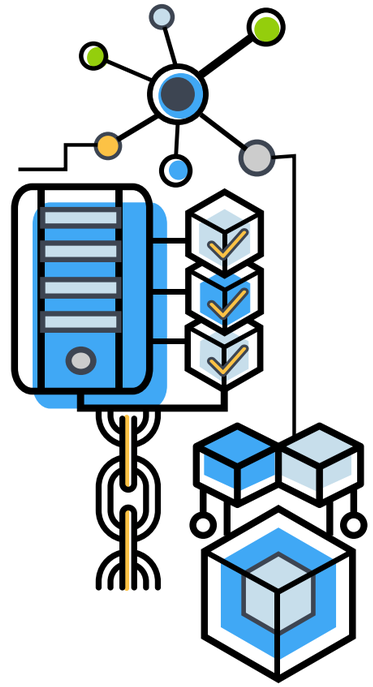
蚂蚁集团
ANT GROUP



推动风险信息共享技术

区块链融入金融犯罪合规
--德勤和蚂蚁集团联合发布

因我不同
成就不凡
始于 1845



区块链技术不再属于未来，今时今日，从金融行业到旅游服务业，区块链已经在广泛行业中占有一席之地。 为区块链技术的应用部署奠定基础的机构，就是为其未来做好准备。 对金融机构而言，必须从对区块链技术的了解、构思、投资到部署，将区块链融入其发展路线图中。

本白皮书探讨了如何将区块链技术融入金融犯罪合规领域，并阐述实施该技术的主要优势以及金融机构面临的主要挑战。

在过去十年间，我们见证了全球监管体系无论在深度和复杂性均急剧加速。因此，金融机构积极开展工作，以建立有效的金融犯罪合规控制框架来应对固有风险，并最终实现全机构的合规、诚信和声誉文化。这为金融机构及其利益相关方、监管机构和客户之间的可持续业务发展和更牢固的信任关系铺平道路。

金融机构正在调动资源向敏捷和可扩展的解决方案发展，以确保标准化、安全和有针对性的策略，旨在让每一个金融犯罪合规流程都能够针对满足监管期望而设计，并在自动化的协助下，以风险为本的方法精简运营工作。 传统的金融犯罪合规措施倾向于**人工操作**和**劳动密集型**，在持续监控客户信息和交易时，需要相对高水平的资源投入，才能建立健全的全机构金融犯罪合规框架。由于大量的人工流程，金融机构容易出现人工错误，并面临与**数据准确性**和**可靠性**相关的风险。

此外，与某些快速发展的金融犯罪类型相比，由于对人力的高度依赖，金融机构的合规项目发展速度也相对缓慢，对其风险状况构成重大挑战。因此，金融机构也开始探索新技术的使用，提高数据的准确性和安全性，并释放劳动力，使他们可以专注于重复性较低且更具战略性的任务。从对新技术的探索中，金融机构面对着一系列从运营转型到流程定制到满足机构特别需求的潜在挑战。

随着科技在金融领域的发展，促使各种各样创新型金融业务也正在发展，金融与科技之间的界线越来越模糊。金融和科技的融合正在不断扩大金融市场的广度和深度，但同时也改变了金融领域的风险管理模式。这是由于新产品和服务以及洗钱和恐怖融资手段不断变化导致的新威胁的出现。

鉴于当今的风险管理必须与上述变革同步发展，客户和股东都在寻求可信任的消费业务或服务。信任已成为受监管实体与监管机构、客户、利益相关方、员工彼此之间建立和维持关系的关键因素。我们各方都有机会在安全多方计算（“SMPC”）生态系统中，参与到以“信任”为主题的未来的建设中，尤其是在金融犯罪合规的领域。

我们可以：

1. 加强透明度，提高理解法律法规的效率；
2. 改善金融犯罪风险的管理方式；
3. 自动向高级管理层和监管报告。

蚂蚁集团 ANT GROUP

蚂蚁链是蚂蚁集团代表性的科技品牌，致力于打造数字经济时代的信任新基建。蚂蚁链坚持核心技术突破，融合包括区块链、AIoT、智能风控等技术，通过链接各个产业网络，扎实解决行业实际问题，推动区块链技术平民化。从2016到2020年，蚂蚁链连续四年区块链专利申请数和授权数全球第一。蚂蚁链坚持开放生态，与合作伙伴共建共享区块链产业带来的价值互联红利。在实际应用上，蚂蚁链已携手生态合作伙伴，解决了50余个场景的信任难题。

Deloitte.

德勤全球网络已经建立了完善的金融犯罪合规和区块链实验室的生态系统，该生态系统汇聚世界各地司法管辖区的专业人员，专注于设计创新的区块链解决方案、构思、战略，以及原型设计和开发。德勤亚太区块链实验室与该地区的技术专家合作，为金融服务行业中已部署的区块链网络举办客户研讨会、建构领先理念、开发原型、提供生产支持、以及提供创新的想法和解决方案。

德勤亚太区块链实验室负责人冼君行博士表示：“尽管亚太地区对数字资产和加密货币的监管存在不确定性，甚至全面禁止，但区块链具有得天独厚的优势，能够在不侵犯隐私的前提下，满足跨国家、跨行业的数据共享需求。跨境跟踪、追踪是可持续性和防伪工作的关键，而身份验证对于虚拟银行，中小企业贸易融资和普惠金融都至关重要。这些议题是大多数亚洲国家政府议程上的首要议题，特别是在后疫情经济中。”

区块链如何建立和维持信任?

区块链和分布式账本技术（“DLT”）由于其**不可篡改**和**分布式**的性质，在当今的数字转型时代受到了广泛的讨论。区块链技术可以帮助金融机构实现透明、可靠、而且能体现效率和成本效益的合规自动化[1]。**透明**：因为区块链技术具有去中心化的特点，即所有节点都可以访问链上的信息；**可靠**：因为该技术是防篡改的；**效率和成本效益**：通过加快流程，降低成本和优化出错率高的重复流程，提高金融行业合规自动化解决方案的整体效率和成本效益。

区块链技术为众多金融犯罪合规的实践领域提供了潜在解决方案。

了解你的客户（“KYC”）数字身份创建（识别）和认证（验证）

- 通过创建数字身份并在区块链上提交验证数据，机构可以提高客户识别和验证过程的效率

自动化交易监控

- 如果机构采用由区块链技术支持的监控系统，则每笔交易都将在链上安全记录，并具有可追溯的功能。利用区块链上的智能合约，将有助于实时监控交易，以及付款欺诈检测，同时链上交易记录均无法被篡改

数据存储与维护

- 金融机构可以考虑将其KYC数据库、交易历史记录和数字文档迁移至对数据安全有保证的区块链上

1.Deloitte, Over the horizon: Blockchain and the future of financial infrastructure Research from Deloitte & the World Economic Forum, https://www2.deloitte.com/global/en/pages/financial-services/articles/gfsi-disruptive-innovation-Blockchain.html

在亚太地区（尤其是在中国），人们一直坚信区块链的变革和战略价值，并且有许多计划开发私有/许可区块链用例。 充分发挥区块链技术的基本信任价值，为机构更好地调整其金融犯罪合规的关注点以及未来资源规划。

根据德勤发布的《2020年全球区块链调查》，中国大陆的34%和香港特别行政区的52%的受访者计划在未来12个月内至少投入500万美元在区块链技术。

在14个国家和地区的1,500位高级管理人员中，有55%的人将区块链作为前5大战略重点之一。 同时，亚太地区有89%的受访者正在招聘或计划聘用区块链专家，而39%的受访者已经在生产环境中部署了区块链。 约83%的受访者认为不采用区块链将削弱他们的竞争优势。

数据共享、对账和可追溯性是亚太地区最重要的三个区块链用例。

该报告还显示，将近89%的高管相信未来三年的数字资产潜力，而70%的高管认为监管变革的步伐非常快或有些快。 尽管数字货币已成为全球范围内的顶级用例，但数据共享、对账和可追溯性仍是亚太地区排名前三的区块链用例。

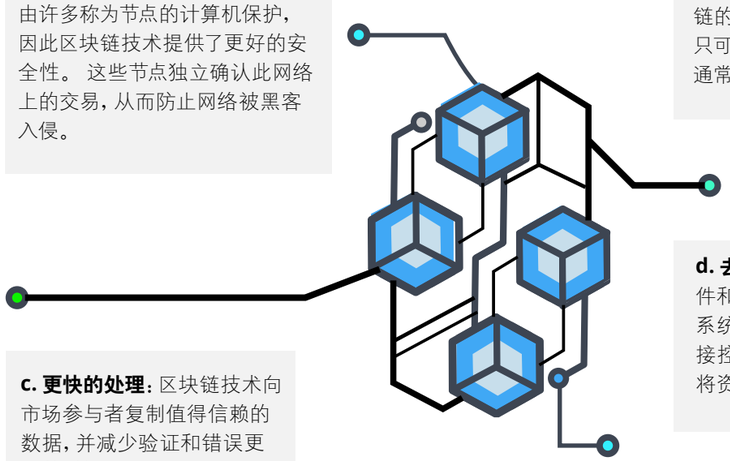
什么是区块链?

区块链在2009年比特币革命中首次受到公众关注。 比特币是一种允许点对点进行价值交换而无需第三方中介的协议，它的应用是基于使用加密技术验证交易的公共账册系统。比特币吸引了商业界无穷的想象力，但更令人感兴趣的是比特币底层称为区块链的基础技术。

区块链的四个关键特征：

a. 更高的安全性：由于该网络是由许多称为节点的计算机保护，因此区块链技术提供了更好的安全性。 这些节点独立确认此网络上的交易，从而防止网络被黑客入侵。

b. 不可篡改：不可篡改账本的创建是区块链的主要价值之一。 该技术使账本记录只可被添加而不可被删除，这意味着账册通常会保持真实状态且不可篡改。



c. 更快的处理：区块链技术向市场参与者复制值得信赖的数据，并减少验证和错误更正的时间。

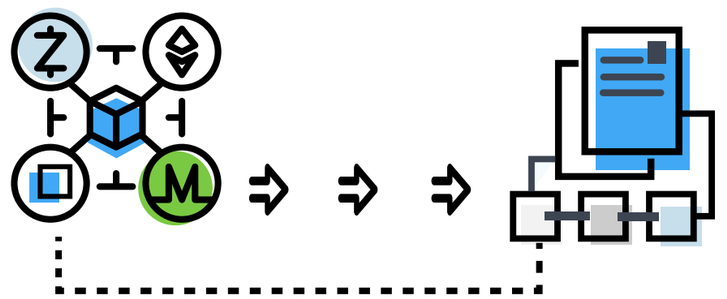
d. 去中心化系统：分布式技术允许将文件和合同等资产存储在网络上。通过该系统，所有者通过与账户链接的密钥直接控制他/她的账户，该密钥赋予所有者将资产转让给任何人的权力。

在金融服务行业中，这些特征带来了以下优势：

1. **流程完整性：**区块链的设计方式令每个节点均为独立运作，任何区块或交易添加到链后便无法篡改， 这为整个流程的完整性提供了保障。
2. **可追溯性：**可以轻松定位发生在区块链上的所有操作，从而更轻松地进行跟踪和补救操作，并创建审核跟踪。
3. **安全性：**向进入区块链网络的个人提供链接到其账户的唯一身份。 这种加密可确保只有账户所有者才能操作交易，并且使黑客很难干扰链的设置。
4. **赋能交易处理和结算：**在区块链发明之前，传统银行组织通常需要花费几天时间来启动和处理交易，但区块链则可赋能机构实现更快的交易。

如何利用区块链共享风险信息?

区块链技术的重要特点之一是它增强了信息共享。 区块链的分布式账本技术允许在网络内记录、管理和交换价值，这些价值可以是货币和知识产权，也可以是许多其他不同类型的信息。 作为信息载体，区块链在网络参与者之间创建了一层信任，而不需要第三方中介。



透明度是打击金融犯罪的关键

信息共享对于有效开展反洗钱和反恐融资计划至关重要。 今天的犯罪分子利用全球金融体系为自己谋取非法利益，并且持续尝试新型洗钱及恐怖融资方式。 尽管监管和法律框架往往只针对特定司法管辖区，但犯罪分子却不局限于在某特定司法管辖区犯案，犯罪分子在反洗钱和反恐融资程序中经常利用此漏洞来逃避定罪和执法。

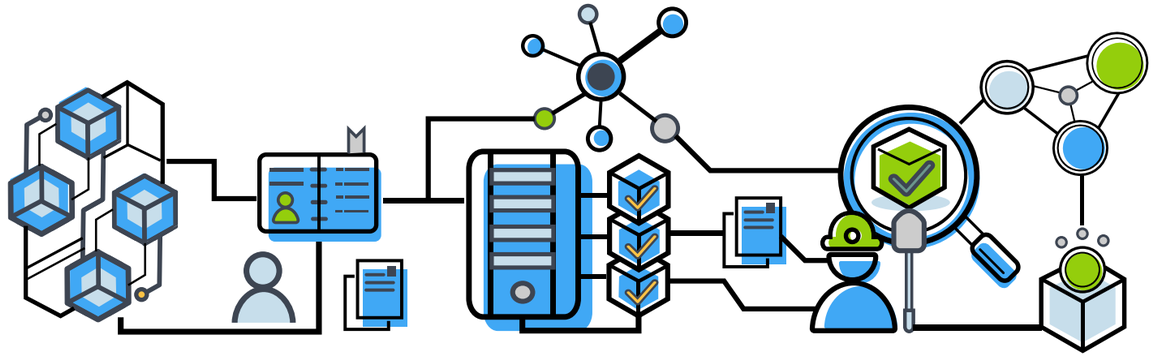
数据隐私与保密法有时会限制执法机构识别、捕获犯罪分子和破案的能力。 符合多个地方的隐私与保密法规的信息共享机制将使全球执法机构能够共同打击金融犯罪。

反洗钱主要标准设定方与国际组织，金融行动特别工作组（“FATF”）也曾指出，有效的信息共享也是打击金融犯罪一大关键，因为有效的信息共享可提高金融系统透明度，并保护金融系统的完整性。 2017年11月，金融行动特别工作组曾发布信息共享有关指引[2]，旨在突出私营机构之间共享信息的价值，指出目前此类信息共享过程中存在的挑战，并举例说明如何在金融机构内部以及非同一集团内的金融机构之间应当如何实现此类信息共享。

交易链路的信息完整性是缓解金融犯罪的关键挑战，然而，信息目前分散在众多“信息孤岛”上，包括金融机构内部、监管和执法机构、客户或其他金融机构。 如果无法获得全面的信息和数据，识别具体的威胁和类型就变得更具挑战性。在许多情况下，金融机构发现的异常交易，都是因为缺乏足够的交易信息而缺乏怀疑与洗钱犯罪有关的合理理由。

2.*FATF, Private Sector Information Sharing,* https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

推动风险信息共享技术 | 区块链融入金融犯罪合规



这情况使得全球金融情报机构（“FIU”）的负担大大增加。在全球范围内，可疑交易报告的数量近年来逐渐上升，同时，可疑活动报告越来越被认为是反洗钱/打击恐怖融资项目和制度的重要基石之一。

然而，研究表明，只有很小一部分提交给金融情报机构的可疑交易报告被实际采用——金融情报机构负责人在访谈中透露，80-90%的可疑交易报告对正在进行的执法调查没有直接价值[3]；欧盟的金融情报机构指出，提交的可疑交易报告中平均只有超过10%的使用率[4]。导致可疑交易报告使用率低的主要原因之一是金融情报机构需要审查大量没有信息或细节不足的可疑交易报告。企业与金融情报机构之间的信息孤岛互相影响，对打击金融犯罪工作产生了较大的挑战。

区块链为组织、监管机构和政府提供了以安全方式实现信息共享的机会。

因此，以往通过连接各种线索从而识别犯罪分子的传统方法效率欠缺，不足以团结各界协力应对今天快速变化的金融犯罪风险。 目前，全球已有20多个国家[5]致力于建立公私金融信息共享伙伴关系（“FISP”），通过分享信息来缩小信息差距，并建立针对金融犯罪的风险共识。[6]

3.Royal United Services Institute for Defence and Security Studies, The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017.pdf

4.European Union Agency for Law Enforcement Cooperation (Europol) Financial Intelligence Group, From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact

5.Afghanistan, Argentina, Australia, Colombia, France, Georgia, Indonesia, Ireland, Italy, Japan, Jordan, Kenya, Malta, Mexico, the Netherlands, Nigeria, Singapore, Spain, Switzerland, Trinidad and Tobago, Tunisia, the United Arab Emirates and the UK made such commitments policy at the London Anti-Corruption Summit on 12 May 2016.

6.Royal United Services Institute for Defence and Security Studies, The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, https://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_report_-_oct_2017.pdf.

私营机构如何探索“洗钱风险信息”共享?

信息共享对于定位洗钱风险尤其重要，国际上已经有许多推进信息共享的先例。我们在此列举了以下三个例子，体现不同类型的公私合作和私营机构之间的合作。

2017年4月，新加坡银行协会、新加坡金融管理局和新加坡金融情报机构所在的新加坡警察部队成立了反洗钱与反恐怖融资行业合作伙伴关系（“ACIP”）。ACIP召集了金融部门、监管机构、执法机构和其他政府实体，共同致力于风险识别、评估和最佳实践的共享。2018年11月12日，ACIP发布了一篇关于行业观点的文章《为反洗钱与反恐怖融资采用数据分析方法》，分享了针对反洗钱和反恐怖融资部署数据分析的最佳实践。ACIP专注于理解反洗钱与反恐怖融资领域的广泛问题。

1

《美国爱国者法案》（USA PATRIOT Act）314(a)和314(b)分别规定了监管部门主导的金融情报信息共享和私营机构基于自愿共享的法律机制安排。314(a)是监管主导的强制性公私信息分享机制，当执法部门需要调查洗钱或恐怖融资活动时，可通过金融犯罪执法局（FinCEN）联系14,000多家金融机构，以查找金融交易的帐户和交易可能参与恐怖主义或洗钱活动的人员。314(b)是一项义务机构自愿共享的机制，通过314(b)和其责任豁免条款，金融机构能通过反洗钱情报共享增强对客户和交易的风险判断能力，更好地为执法部门提供调查证据。[7]

2

第三个案例是荷兰的交易监控计划（“TMNL”）[8]，它汇集了荷兰最大的五家银行，建立一家企业以进行集体交易监控识别洗钱。犯罪分子在荷兰境内每年可清洗估计约160亿欧元源自人口贩卖、贩毒及恐怖融资等上游犯罪的资金。TMNL通过网络分析与异常检测等先进分析技术，实现对多家银行的交易数据联合监控，从而更有效地检测犯罪资金流和网络。类似的努力也出现在其他司法管辖区。

3

为了实现更有效和协作的洗钱风险预防和缓解措施[9]，蚂蚁集团正在与多家私营部门一起，共同积极探索和研究洗钱风险信息共享模式，希望利用区块链技术进行洗钱风险信息共享，同时保持信息安全性和反洗钱保密性。

蚂蚁集团正在利用区块链技术进行探索试行，以期在不同的受监管实体之间能够共享洗钱风险信息，帮助义务机构有效地识别高风险客户，并提高反洗钱计划的预防和控制效果。 该探索试行已取得了积极成果。

在探索试行过程中，项目团队进一步从业务和技术可行性、合法性等多个角度分析了该方案的应用价值，包括业务和技术可行性、信息安全、隐私保护、国际惯例、以及反洗钱保密性和合法性。项目团队建议在国内自愿机构中逐步推广和应用该方案模型，以提高中国反洗钱计划的总体预防和控制效果。

7.FinCEN, *FinCEN's 314(a) Fact Sheet*, https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf

8. Deloitte, *Deloitte connects 5 Dutch banks to make an impact with Transaction Monitoring Netherlands (TMNL)* , https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-dutch-banks-to-make-an-impact-with-transaction-monitoring-netherlands-tmnl.html

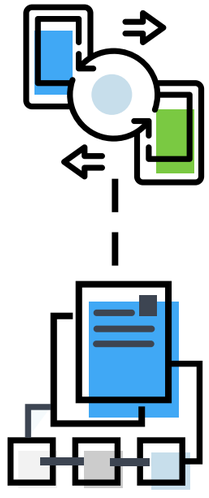
9.FATF refers to this as the Information Sharing Principle. FATF, *Consolidated FATF Standards on Information Sharing*, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf

私营机构之间共享可疑交易活动情报有何障碍？区块链如何提供帮助？

金融机构在彼此共享信息方面面临一些严峻的挑战。 以下是目前阻碍私营机构有效共享洗钱风险信息最为紧迫的问题和挑战：

1. **数据隐私、银行保密、和个人数据保护**
2. **数据安全风险**
3. **私营部门的数据质量和准确性**
4. **风险管辖权与机构相应的履职义务**
5. **信息共享的运营成本**

为了更好地面应对上述挑战，国际金融研究所（“ IIF”）和德勤在2019年发布了一份白皮书，题为《打击金融犯罪的全球框架》[10]，探讨金融犯罪监管的关键领域，包括跨境和境内信息共享，并就如何促进私营机构之间的信息共享提供了一些建议。在政策框架层面，该文件就FATF40项建议中的信息共享项提出了一些修改意见，并指出FATF成员国应当根据FATF的信息共享建议推动相应的在政策改革。 该白皮书同时指出，在这一全球信息共享框架建立的过程中，技术应当起到至关重要的作用。



在这方面，区块链技术可以成为增强信息共享过程的一种途径，帮助缓解一些上述的问题和障碍：

1. 数据隐私、银行保密和个人数据保护相关的法律框架-加强整个地区或全球的监管和法律框架对于允许非个人信息共享非常有益。同时，此类金融机构整合而来的匿名数据可以帮助识别新的风险类型、威胁和模式。通过技术创新，实体解析和风险类型共享技术可以不通过任何客户个人数据拼凑出交易模式。

2. 保护个人数据的另一种方法是在区块链上利用密码算法对相关数据进行加密处理。 这种加密功能可以基于金融机构拥有的客户数据，因此只有拥有完全相同的客户数据集的另一金融机构才能读取相关信息。如此一来，只有那些需要了解信息以理解交易全貌的金融机构才能获取有关数据。

3. 数据安全风险-在遭受攻击的情况下（假设并非所有节点都同时损坏），系统的分布式和共享性质可以促进数据和进程的恢复， 并减少对昂贵的恢复计划的依赖性。 与现有系统相比，复杂的加密技术还可以为DLT上存储的信息池提供额外的保护层。 尽管如此，在DLT环境中，我们仍然需要认真考虑网络攻击的风险。[11]

4. 整个私营部门的数据质量和准确性-DLT的关键优势在于数据的准确性，只有通过验证的信息可以被放到区块链上。

5. 信息共享的运营成本-通过利用区块链技术，授权用户可以直接取得相关信息，这一流程中去除了第三方验证要求的和成本，从而降低私营机构之间信息共享的操作和信任成本。 此外，如果在端到端的交易流程中部署区块链技术，则相关信息上链的操作成本可以进一步减少。

10. Deloitte, *The global framework for fighting financial crime*, https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html

11. ACAMS, *Distributed Ledger Technology: Streamlined CDD Examination Process through Blockchain Application*, http://files.acams.org/pdfs/2018/Distributed_Ledger_Technology_N_Zelensky.pdf

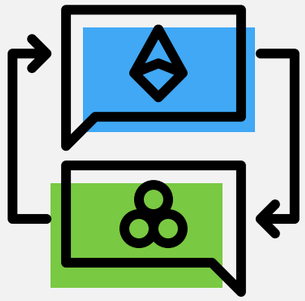
如何利用科技实现反洗钱风险信息共享?

一般来说，区块链有两种类型：公有链许可链。 两者具有不同的应用场景。

公有链主要用于加密货币，其特点是去中心化和匿名操作，链上运行的业务多样化，并且没有统一的系统访问标准。 因此，针对反洗钱风险信息共享的方案，我们不建议使用公共链。

许可链是指所有参与节点均获得许可的区块链系统，未经授权的节点无法访问该系统。 联盟链是一种构建许可链的方法，适用于需要多方合作和达成共识的业务场景。 通过加密技术和点对点传输，可以在多个业务方之间建立共享的账目（或共享的数据库）。 该方法降低了数据处理成本，提高了传输效率，同时确保了数据安全性和相互信任。 联盟链是此方案的推荐方法。

风险信息共享的范围



目前，参与机构主要探索的信息共享范围集中于洗钱高风险客户的分类信息和相关控制措施信息等。根据FATF私营机构信息共享指南，在政策和机制成熟后此范围可以考虑进一步扩展到可疑情报、高度可疑但尚未报告信息以及其他被标记的可帮助识别客户洗钱和恐怖融资风险的信息等。区块链联盟机构通过充分共享情报信息，可以进一步提高所涉机构的透明度并创建更有效的协作环境。

使用区块链和数据隐私保护技术对参与机构的数据进行保护，在实现数据信息跨机构共享的同时确保符合有关客户信息安全的法规要求。

从法律的角度来看，阐释中国大陆反洗钱法[12]的权威刊物建议，私营企业应保持基本的客户隐私和机密性（洗钱等某些对社会和商业有害的活动除外）。

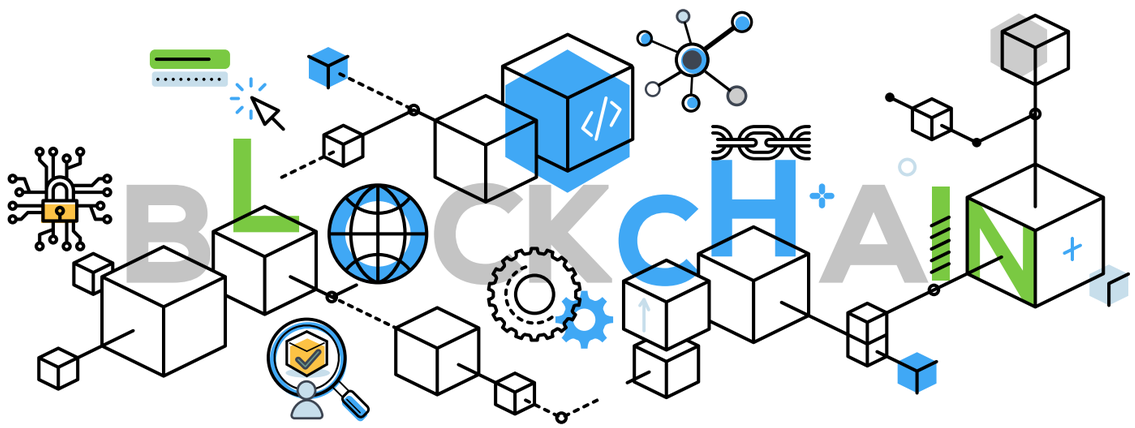
12.中国法制出版社，2007年1月，《中华人民共和国反洗钱法释义》(China Legal Publishing House, January 2007, *Interpretation on Law of the People's Republic of China on Anti-money Laundering*)

如何管理区块链联盟?

根据国际惯例，反洗钱信息共享联盟的共同模式有两种：自愿组织模式和监督协调模式。

1. 自愿组织模型：该模型是指在一个团队内部或具有紧密业务关系的合作组织之间自发建立的共享联盟。例如，在大型金融控股集团内部，或在基金销售机构与代销银行之间，可以采用此模型来实现共享，同时确保风险信息的机密性。

2. 监督协调模式：该联盟模型由主要的监管机构及其地方分支机构以及信息共享网络中的自愿机构组成。作为参与者，义务机构作为参与方以达成的共识进行共享洗钱风险情报数据； 监管机构可以充当联盟链的运营管理者，对参与方的入驻和退出进行管理，并对参与机构进行协调和监督，也可以授权参与机构作为运营管理者来行使上述权力。在此模型中，联盟链还可以将主管部门的内网用作构建环境。



我们建议的价值

我们认为，实施联盟链将为机构间洗钱风险信息共享带来以下优势：

1. 打破跨机构的洗钱情报信息孤岛，在安全和保密的基础上，建立联合防控体系，全面提升私营机构反洗钱与反恐怖融资工作的有效性和及时性。

2. 金融情报机构可以从受监管实体获得更完整、更有价值的情报和高质量的可疑交易报告，以及有关可疑客户的交易中的更多身份或数据。

3. 在反洗钱活动中实施区块链技术使该网络具有扩展的潜力，参与机构可逐步扩大至公安、海关、税务、工业、商业和执法机构参与，并形成相互信任和紧密联系的公私联盟网络，进一步提高反洗钱工作效率。

4. 形成联合防控体系将有助于降低行业内与跨行业洗钱风险，最终在国家层面降低洗钱风险。

5. 反洗钱能力较强的大型金融机构可以与规模较小的机构合作，以加强整体反洗钱措施和控制，并提高其效力以取得更好的结果。

相关推荐阅读

- ACAMS Today, *Digital Identity and Financial Crimes,* https://www.acamstoday.org/digital-identity-and-financial-crimes-2/
- IBM, *IBM Verify Credentials: transforming digital identity into decentralized identity,* https://www.ibm.com/blockchain/solutions/identity
- Frontiers in, *A decentralized digital identity achitecture,* https://www.frontiersin.org/articles/10.3389/fbloc.2019.00017/full
- Allen & Overy, *Cryptocurrency AML risk considerations,* https://www.allenovery.com/en-gb/global/news-and-insights/legal-and-regulatory-risks-for-the-finance-sector/global/cryptocurrency-aml-risk-considerations
- Global Legal Insights, *Blockchain & Cryptocurrency Regulation 2020 | 11 Cryptocurrency compliance and risks: A European KYC/AML perspective,* https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/11-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective
- 101 Blockchains, *Top 50 companies that has adopted blockchain technology,* https://101blockchains.com/companies-using-blockchain-technology/
- Finextra, *Global banks and R3 test DLT for KYC services,* https://www.finextra.com/newsarticle/29747/global-banks-and-r3-test-dlt-for-kyc-services
- Fintech Futures, *Santander and Ripple to launch blockchain-based consumer payments,* https://www.fintechfutures.com/2018/02/santander-and-ripple-to-launch-blockchain-based-consumer-payments/
- Blockchain Council, *Top 10 companies that have already adopted blockchain,* https://www.blockchain-council.org/blockchain/top-10-companies-that-have-already-adopted-blockchain/

联系人

张丰裕
德勤中国反洗钱及法证服务合伙人
北京
+86 10 85125353
chrcheung@deloitte.com.cn

Singh, **Radish**
德勤亚太财务咨询合伙人
新加坡
+65 97804580
radishsingh@deloitte.com

Zhang Hui
蚂蚁集团区块链资深技术专家
shengchu.zh@antgroup.com

李书博
蚂蚁集团区块链高级技术专家
daniel.lsb@antgroup.com

冼君行
德勤亚太区块链实验室领导合伙人
德勤中国管理咨询合伙人
香港
psin@deloitte.com.hk

Vasan, Mangala Kalyani
德勤中国法证服务总监
香港
+85 222586198
mavasan@deloitte.com.hk

杨文玉
蚂蚁集团区块链高级产品经理
wenyun.ywy@antgroup.com

王辛民
蚂蚁集团反洗钱专家
xinmin.wxm@antgroup.com

关于德勤

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体。德勤有限公司并不向客户提供服务。请参阅 www.deloitte.com/cn/about 了解更多信息。

德勤亚太有限公司（即一家担保有限公司）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100座城市提供专业服务，包括奥克兰、曼谷、北京、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、大阪、上海、新加坡、悉尼、台北和东京。

德勤于1917年在上海设立办事处，德勤品牌由此进入中国。如今，德勤中国为中国本地和在华的跨国及高增长企业客户提供全面的审计及鉴证、管理咨询、财务咨询、风险咨询和税务服务。德勤中国持续致力为中国会计准则、税务制度及专业人才培养作出重要贡献。德勤中国是一家中国本土成立的专业服务机构，由德勤中国的合伙人所拥有。敬请访问 www2.deloitte.com/cn/zh/social-media，通过我们的社交媒体平台，了解德勤在中国市场成就不凡的更多信息。

BJ-002CN-20