JONES DAY | One Firm Worldwide℠

白皮书

2018年9月

区块链与反垄断法：全新的科技，同样的风险？

区块链技术，特别是私有区块链，可为商业交易的进行提供技术屏障。尽管如此，在可能违反美国或世界各地的反垄断法时，任何由私有区块链滋生的限制竞争行为都要受到法律规制。

本众达*白皮书*介绍了区块链参与者如何通过实施针对区块链技术的特有属性而设计的预防措施和保护措施来管理风险。

目录

"别在意帷幕后那个人。"—《绿野仙踪》

区块链或"分布式账本"将交易的各方在一种定义会员资质与信息权限的技术屏障之下联系在一起。这种虚拟屏障在无需一中心管理者的情况下为更高效和安全的交易创造了可能性。这项技术最广为人知的实例是加密货币比特币。与以银行作为重要中介机构的传统金融体系不同，比特币的运行不需要中心管理机构，而是由用户直接交易比特币。

过去几年间，区块链及其衍生技术已由虚拟货币扩展至供应链活动和其他包含医疗、财产权与保险等领域，这些领域十分重视对价格、单位或其他关键规格信息的追踪与记录。

许多区块链运作会涉及到相互竞争的公司在公共（"公链"）或私人（"私链"）账簿中的合作。大部分商业应用的区块链为私链。这些私链以隐蔽的方式运作。

然而任何由私链滋生的的限制竞争行为仍须受反垄断法的监管。区块链与任何竞争对手共享信息的其他场合并无二致，其同样可能产生触犯美国或世界各地反垄断法的非法协同或排他性行为。当区块链跨境运作时，其可能受多个司法管辖区的竞争法管辖。因此随着此技术逐渐突出，竞争监管部门也开始对其密切关注。举例而言，2018年2月欧盟委员会发布"欧盟区块链观测站及论坛[1]。2018年3月美国联邦贸易委员会宣布成立内部"联邦贸易委员会区块链工作小组"[2]。2018年4月，经济合作与发展组织发表题为"区块链技术与竞争政策"的文件[3]。

本白皮书聚焦于区块链特别是私链的形成与运作过程中可能产生的美国反垄断法问题，并探讨企业尽可能减少反垄断风险可以采取的措施。

区块链的基础介绍

区块链是一个去中心化的电子账簿，其可以用可验证和永久的方式记录交易。交易记录将与其他交易一同储存数据"块"中，而这些数据"块"又进而彼此相互串联为"链"。该账簿或资料库由若干不同的参与者或"节点"掌管。区块链使用者会被配发独特的识别码（以比特币而言就是公共与私有的密钥）用以识别交易中的每一位参与者。每一个区块的记录都会使用一种算法，将该区块链中排在该区块之前的区块编码在该区块中。因此，一旦一个区块被加入链中，实质上便不可能对其进行修改。若要进行任何变动，将需要一并修改链中所有后续区块中的数据。同时由于区块链中的每一位参与者都有独特的识别码，其他用户可以立即验证涉及该参与者的先前交易。

区块链有两种：公链为开放且不需核准的，而私链为非公开且须经核准的。

公共区块链

公共区块链对所有人开放，但其参与者可以在网络内以独有的用户识别码的方式维持匿名。账簿用其识别码追踪每一位参与者。账簿以交易为基础，并记录先前交易历史。根据已在参与者帐户中贷记或借记的先前交易，此信息可用于评估参与者是否有完成目标交易所需的足够资金、产能、存货等。在没有中央管理机构或清算所的情况下，每个节点皆用来保存所有参与者交易的账簿。任何人皆可提出将交易区块添加至公共区块链。并不存在监督区块链的中央验证系统，以决定要添加哪些交易区块或决定在误差发生时哪些区块有效。反之，区块链使用预设规则，即"共识机制"来决定应以那个记录为准。

例如，在比特币区块链上，第一个正确解决杂凑运算的一方可以向网络提出下一个区块。这被称为"挖矿"。在验证杂凑运算被正确解决、区块中的交易有效、且每一交易中的比特币以前未被花费后，网络上的节点才将被提出的区块添加到它们的区块链复本中以示接受。若区块链的不同版本间存在冲突，则适用"工作量证明"方案，将运算量最大的链视为存有准确记录的链。在此系统下，参与者实际上不可能相较他人取得策略性的优先地位或被赋予不公平的优势。如果参与者间出现争议，则没有关于如何解决这些争议的默认规则。

当交易参与者需要匿名及与不限量的其他参与者进行交易时，非常适合使用公共区块链。然而，有些公共区块链存有技术障碍，例如速度，可扩充性和存储限制。由于商业应用中需要快速有效地进行多个交易，这些限制便带来了障碍。实际上，处理一个区块的比特币交易需要大约10分钟。其他公共区块链，如以太坊区块链网络，已经针对其中一些限制做出了改善，比方提升交易处理速度。面对这些挑战，私有区块链应运而生，以维持效率并解决公共区块链的一些基本技术限制。

私有区块链

私有区块链由一系列既定的节点管理，仅有经允许的用户有读写权限。在这些协作行为中，参与者更少、参与者间信息共享可能性更大、区块链外部对交易的可见度较低。就此而言，私有网络失去了此技术原始形下的很多特征，即能够在开放式系统中匿名交易。

与公共区块链不同，私有分布式账簿:

- 存在一位所有者负责管理或赋予会籍、采矿权和奖励，并维护共享账簿，也可能有包括覆盖，编辑或删除区块链条目的权限；
- 有所有者或指定参与者负责解决偏差，且通常不适用工作量证明机制。
- 存在有限数量会员，通常用户无法匿名；
- 存取数据无法被公众读写，因此非会员者由于缺乏权限，所以无法看到交换的信息。

这些属性使私链对许多商务应用具有吸引力。由于使用的计算密集型共识机制较少，私有区块链相较于公共区块链交易速度明显更快。同样地，私有区块链通常更适合必须遵循规定进程的受监管产业，例如通过"了解您的客户"(客户尽职调查)制度要求客户证明自己的身份的反洗钱和反恐法规。

反垄断的问题

区块链和其他"高科技"产物，如人工智能和"大数据"，与"旧科技"行为一起受相同的反垄断法和分析框架评估。在美国，使用区块链技术可能引发谢尔曼法第1条（禁止共谋）、谢尔曼法第2条（禁止垄断）、联邦贸易委员会法第5条（禁止不正当竞争）、克莱顿法第7条（禁止限制竞争并购）下的问题。

到目前为止，还没有涉及区块链的美国反垄断法执法行动。然而，在2015年，司法部（"DOJ"）对一家电子商务零售商和其两名高管提起固定价格指控，声称共谋者利用定价算法为海报和其他装饰人为设定底价（Wall Décor案）[4]。共谋者同意在定价软件的帮助下，仅在非共谋竞争者的最低价格及以上的范围内实施降价。因此，共谋者有效消除了彼此的竞争，而该竞争行为本应使消费者享受更低的价格。

与Wall Décor案中的被告使用定价算法来减少竞争类似，私有区块链参与者可以使用他们的交易数据来设定和监控价格或防止价格下降到"不利"水平。

共谋—谢尔曼法第1条

近年来，美国和世界各地的竞争监管机构和主流媒体十分关注科技公司（如Facebook，Apple，亚马逊）和"高科技"产品或服务是否应适用不同的反垄断执法规则。但正如司法部反垄断部门官员近期阐述的那样：

> 最近，人们一直在讨论某些行为—例如使用计算机算法设定价格—是否应像"传统的"定价行为一样接受相同的执法力度。需要澄清的是，当竞争者同意限制彼此之间的竞争关系时，无论是同意与街对角的加油站显示相同的油价，还是通过使用在线交易平台或算法等先进技术固定价格，都是违反谢尔曼法的行为。固定价格协议本身是违法行为；协议的执行方式并不是重点[5]。

该声明涉及谢尔曼法第1条，该条禁止限制竞争共谋，例如固定价格，串通投标或市场分割[6]。视区块链的形成和运作方式而定，它还可能涉及禁止垄断和限制竞争交易的反垄断法。 然而，对于竞争企业中的大多数区块链合作而言，实际上最大的反垄断法风险多涉及共谋。参与者可能会利用区块链技术达成"赤裸裸的"协议以操纵价格、分配市场或客户、或不当分享竞争敏感性数据。违反第1条的行为须两家或更多公司之间采取协同行为（"协议"）。单纯建构区块链而没有进一步的行动，则不会导致反垄断法律责任。私有区块链可以促进竞争。由于参与者彼此了解，此安排可以降低交易成本，改善节点之间的连接，并对链进行有组织的验证。

然而，如果竞争对手间共享诸如价格、数量和客户特定功能和规格等竞争敏感条款时，区块链则可能会增加反垄断风险。事实上，私有区块链可能提供分享信息或监控参与者是否遵守协议条款的渠道，从而促成反垄断违法行为。与Wall Décor的被告类似，竞争者可利用私有区块链促成赤裸的价格固定协议，此种协议是违反第1条的本身违法行为，即其违法定性无需考虑任何实际或声称的促进竞争效应。

即使没有价格固定协议，区块链成员若使用该技术促成竞争敏感信息的不当交换或不合理排除竞争对手访问区块链的权限，仍可能违反第1条。交换竞争敏感信息的协议可能会减少竞争，交换行为本身则可能成为非法协同的证据。

然而，与价格固定或客户/市场分配协议不同，此类信息交换行为本身并非违法。该行为则是在"合理原则"分析下进行评估，该种分析框架下需要权衡信息交换行为的限制竞争损害与促进竞争效果。

判断信息交换是否造成限制竞争损害需考虑下列因素：

- 信息提供来源（实际或潜在的竞争者）；
- 交换之信息的本质（是否含有竞争敏感性）；
- 产业结构（竞争者数量）；
- 是否交换较少或不交换竞争敏感信息仍能实现该合法的商业目标（限制较少的替代方案）。

此外，私有区块链参与者如果将竞争对手排除在区块链之外，也可能面临第1条的风险。如果一区块链对于在特定产业中的竞争至关重要，竞争者可能需要成为区块链的一部分。例如，在某些产业，规模与范围至关重要。在银行业，使用区块链技术可以显着降低交易成本。在医疗保健领域，若无法访问区块链数据网络、药品供应链或资源管理，供应商可能无法提供相同水平的医疗服务或带来必要的运营效率。

在一区块链对营业至关重要的情况下，如果私有区块链成员排除竞争对手访问区块链的权限，则非成员可能无法有效竞争。将竞争对手排除在被认为是产业中"必须拥有"的区块链之外，可能会引发使用区块链会籍规则限制竞争的指控。

区块链内也能发生排他性行为。在私有区块链中，所有者或指定区块链参与者有权解决链中的偏差。这些偏差可能无法在客观的共识机制下得到解决。相反，所有者和/或指定参与者可能得以单方面解决偏差。因此，某些参与者可能同意以不利于竞争对手且优待其他参与者的方式解决偏差[7]。虽然排除其他竞争者的协议需以合理原则分析，但仅以阻碍竞争对手的竞争能力为目的而排除竞争对手，并不是一个可以抵消限制竞争行为证据的合法商业理由。

垄断—谢尔曼法第2条

谢尔曼法案第2条禁止垄断和企图垄断。但仅具有垄断力量不足以引发第2条的法律责任[8]。反之，该实体必须利用其垄断力量，故意通过限制竞争排他性行为维持其垄断地位。法院在若干情况下皆认定了排他性行为，包括垄断者拒绝与竞争对手交易、签署独家供应或购买协议、或拒绝向竞争对手提供必要设施等。
举例说明，如果具有垄断力量的供应商要求客户使用其区块链以完成交易，且该要求将导致客户必须放弃竞争对手的区块链，则区块链将可能引发谢尔曼法第2条下的违法行为。当垄断者拒绝与竞争对手交易，亦可能违反第2条。虽然一家公司通常没有义务与其竞争对手交易，然而当垄断者拒绝向竞争对手出售其向他人提供的产品时，或当垄断者曾与竞争对手有过该等交易，却在没有任何合理商业理由的情况下终止此种关系，法院曾判定其应负反垄断责任。据此，区块链的垄断所有者若先前允许竞争对手访问其区块链，但后来在缺乏合理商业理由的情况下排除竞争对手，则可能面临第2条的法律问题。

不正当竞争—联邦贸易委员会法第5条

联邦贸易委员会法第5条禁止不正当竞争[9]。美国联邦贸易委员会对本法所定执法权限采取了广泛、且有时具有争议性的解释，其声称第5条适用于任何损害竞争的"欺骗性，合谋性，强制性，掠夺性，不道德或排他性行为"，包括谢尔曼法案未涵盖的行为[10]。联邦贸易委员会最近行使第5条权限的领域为共谋邀请—由一家公司邀请一位或多位竞争者缔结限制竞争的价格固定或市场分配协议。相对而言，根据谢尔曼法第1条，由于双方间尚未有"协议"，此种共谋邀请并不违法。

区块链能够协助所有参与者进行信息交流。如上所述，在实时交易中交换竞争敏感信息可能会导致竞争者间的价格固定或串通投标行为。然而，区块链并不局限于现行交易。区块链还能发布未来的价格或投标信息。在某些情况下，发布这些预期信息（即所谓的"发送信号"）可能被视为违反第5条的共谋邀请，特别是当有证据表明后续交易和公告价格受到发送信号影响时。

限制竞争交易—克莱顿法第7条

克莱顿法第7条禁止限制竞争交易，包括合并与收购及某些企业合营和竞争者的合作[11]。关键问题为该拟议交易是否能创造或增强市场力量或促进其行使。若相关市场进入容易或市场格局较易改变，或合并后的公司及其剩余竞争对手无法通过抬价获利或减少竞争，该交易就不太可能是限制竞争的。此外，当交易本身能够带来显著的效益时，监管部门不太可能质疑该交易。

涉及竞争区块链的合并或其他交易可能会引发反垄断法的问题。作为分析过程的一部分，司法部和联邦贸易委员会将考虑若干因素，包括与其竞争的区块链的数量和重要性、现有或新公司能够且将在未来对合并后公司造成竞争约束的可能性、以及效率。区块链仍为一种相对新生的技术。有超过1,000个区块链初创公司和数百家全新且不断扩大的企业区块链投资机构。这表明，大体上将，该市场竞争较激烈，市场进入较普遍[12]。此外，如上所述，区块链可以带来显着的效率。相竞争区块链的合并可能带来显着的成本节约和其他运营协同增益，这将在监管机构分析交易时被考虑在内。

反垄断风险的避免

绝大多数区块链项目可能是有利于竞争或中立的。区块链参与者面临的反垄断风险程度将取决于多种因素，包含区块链组成（是否涉及竞争者？），产业结构（是否集中，公司数量相对较少？），信息交换的性质（是否涉及竞争敏感信息？），信息共享制度（访问权限是否受用户限制？信息是否加密？）和效率（此区块链能否显着地节约成本或带来其他协同增益？）。区块链参与者可采取措施将其反垄断风险降至最低。

严格限制竞争敏感信息的交换

竞争者间的信息交换是在合理原则框架下分析的。许多情况下，为达成合法商业目的，公司实体交换某些交易信息是合理甚至可能是必要的。但信息交换的数量、类型和性质对反垄断分析至关重要。如果可能，参与区块链的竞争者应避免分享竞争敏感信息，特别是在集中度较高的产业。若必须共享竞争敏感信息，请考虑加密敏感数据以使竞争对手无法访问。举例而言，加密在医疗保健领域十分重要。只有区块链中作为数据目标接收者的实体才能访问和读取该信息区块[13]。

此外，各方应考虑其组织内哪些员工可以访问该信息及这些信息如何被使用。区块链中的竞争敏感信息应与负责定价，营销，战略和其他竞争重要决策的员工隔离。如此可以最大限度降低这些信息被用来减少参与者间竞争的风险。

使用明确定义、具包容性与合理的会籍认定标准

通过形成可信成员的私有区块链来减少共识机制的计算成本，能提供更高的可扩展性和效率。区块链的组成—其成员的数量、规模和竞争重要性—可直接影响其运营效率。因此，会籍标准成为区块链成功的重要因素。

反垄断问题最常出现在一位有兴趣的竞争者访问区块链遭拒的情况下。虽然可能存在合理的商业理由排除竞争者，但坚持践行几种最佳做法能最大限度地降低反垄断风险。会籍标准的缘由应有充分的文件记录和明确的定义，并应具备促进竞争的合理性。标准也不应过度狭隘定义，这容易使其被理解为有意排除某个竞争者或一类竞争者。在应用会籍标准时，区块链所有者不应以不同方式对待条件类似的竞争者。应确定排除的理由并使所有成员知悉。最后，删除任何成员的理由应该有充分的文件记录，并且符合区块链形成时拟定的既定排除标准。

区块链的规模也可能影响反垄断风险。区块链中参与者的数量越少，就越容易将竞争敏感信息追溯至特定参与者。区块链管理者可以尝试以匿名的方式模糊化竞争敏感信息，并尽量减少共谋和非法信息交换的可能性。

然而，在私有区块链中，更严格的会籍标准必然会缩小合格公司的范围。如果成员竞争者X在价格，产能，库存或其他特征方面为与其他人不一样，且该信息在区块链中交换，则竞争对手可能确定竞争者X为交易当事人。这种透明性虽然是间接的，但仍可能会增加反垄断风险。通过增加竞争者数量并使成员组成多样化，匿名在隐藏交易参与者及其数据方面将变得更加有效，从而降低反垄断风险。

使用客观共识机制

如上所述，作为会籍“守门人”的所有者、运营商或其指定人员可能具有掌控数据争议解决方式的能力。其亦可能限定有权读/写/修复偏差的参与者。这些程序规则可能允许区块链内排除性行为的发生。所有者及指定参与者可能同意将某些竞争者置于不利处境。

通过使用预先设定的客观共识机制（例如工作量证明）解决偏差，任何单个参与者都无法掌控偏差的解决方式。这降低了偏差引发竞争问题（例如特殊优待或竞争对手之间的共谋）的可能性。若必须部署不同的系统，则应建立离散参数，说明指定参与者必须如何解决偏差。比如，该系统可以是由轮转的、随机的一系列参与者解决偏差或争议。

考虑区块链数据如何被作为证据使用

反垄断监管机构经常从调查对象和其他第三方利益相关者寻求数据。这可能包含交易销售数据，赢/输单数据和定价数据。就其本质而言，区块链创建了一个长期的信息历史，与其他工具不同，在区块链参与者解决偏差后，这些信息将永久保存。反垄断监管机构能使用这些数据评估交换的信息内容，交换信息的时间，交换后竞争行为如何变化，以及数据中是否存在具有竞争重要性的趋势。

结论

在互联网，手机，电子邮件和其他现代通信技术出现之前，非法的价格固定协议和不正当的信息交换通常是由个人在隐蔽的情况下闭门暗中进行。 随着时间推移，商业通信与相关技术不断发展。 用以通信的方式爆炸性增长（电子邮件，短信，推特等）。 对话可以被“删除”、“消去”或“粉碎”。
随着区块链，特别是私有区块链的形成，商业交易可能会在这面科技之幕下进行，并形成可能为永久性的信息记录。 区块链技术除了具备非凡效用和潜在效率外，尚存在潜在的反垄断风险。 为了管理这种风险，参与者应考虑是否有必要针对区块链技术的特性而量身定制并实施预防措施和保障措施。

律师联络信息

如需了解更多信息，请联系您的公司主要代表或下列律师。 一般的电子邮件信息可以使用我们的“联系我们”表格发送，表格可至 www.jonesday.com/contactus/查询。

Ryan C. Thomas
Washington
+1.202.879.3807
rcthomas@jonesday.com

Mark W. Rasmussen
Dallas
+1.214.220.3939
mrasmussen@jonesday.com

Stephen J. Obie
New York / Washington
+1.212.326.3773 /
+1.202.879.5442
sobie@jonesday.com

Harriet Territt
London
+44.20.7039.5709
hterritt@jonesday.com

Craig A. Waldman
San Francisco / Silicon Valley
+1.415.875.5765 /
+1.650.739.3939
cwaldman@jonesday.com

Larissa C. Bergin
Washington
+1.202.879.5499
lbergin@jonesday.com

注脚

1. “欧盟委员会启动欧盟区块链观察站和论坛”，欧盟委员会(2018年2月1日)
2. “建立联邦贸易委员会区块链工作小组时机已到”，联邦贸易委员会(2018年3月16日)
3. 区块链技术与竞争政策”，经济合作与发展组织(2018年4月26日)
4. 见例如，美国司法部新闻稿，“电子商务执行官和在线零售商被指控固定海报价格”(2015年12月4日)；亦可见认罪协议，United States v. Topkin, No. 15-cr- 00201（2015年3月30日加利福尼亚中区联邦地区法院）
5. Andrew Finch，首席助理副检查总长，反垄断部门，美国司法院，于纽约金融业反垄断：热门议题和全球视角的评论(2018年3月2日)
6. 美国法典编号15 U.S.C. § 1.
7. 分布式账簿和私有区块链是否安全完全是由验证交易的实体的诚信度决定的。在私有区块链中的不可逆交易背后并没有数学上的计算保证。” Colin Thompson，“私有区块链或数据库？如何确定差异”，区块链评论（2016年10月4日）
8. 美国法典编号15 U.S.C. § 2
9. 美国法典编号15 U.S.C. § 45.
10. 见例如，诉状第31页，FTC v. Qualcomm Inc.，2017 WL 242848（2017年，加利福尼亚中区联邦地区法院）(指出第5条将纳入“谢尔曼法”第2段未规定的行为：“高通公司的做法，不论它们是否构成垄断或不合理的交易限制，都损害了竞争和竞争的过程，因此构成违反联邦贸易委员会法案第5（a）条的不正当竞争方法 。”)
11. 美国法典编号15 U.S.C. § 18.
12. “离群事业”，初创公司追踪（列出截至2018年3月29日的1,349个区块链初创公司）；“离群事业”，公司研究追踪（列出截至2018年3月29日的293区块链投资主体）。
13. 见Elizabeth Snell，“使医疗保健区块链成功的数据安全关键考虑因素”，医疗安全（2018年3月26日）。