

区块链成熟度评测报告

背景

区块链在本质上，是一个共享、可信的公共总账，任何人都可以对它进行核查，但不存在一个单一的用户可以对它进行控制。在区块链系统中的参与者们，会共同维持总账的更新：它只能按照严格的规则和共识来进行修改。区块链被视为下一代全球信用认证和价值互联网的基础协议之一。

金融业被视作区块链落地的最佳场景，根据金融业对区块链的应用需求，我们对三个区块链系统（Fabric、商业区块链 A、商业区块链 B）进行了评测，旨在为开发者选取区块链时提供参考和指导。

区块链成熟度评测模型

区块链成熟度评测模型基于金融行业开源软件成熟度评测整体模型进行建立。整体模型充分结合了开源软件的特性、系统工程领域对于软件产品质量的要求以及金融行业对于开源软件的使用需求。**整体模型涵盖开源许可证、行业认可度、产品活力、服务支持、功能性、性能效率、安全性、可靠性、易用性、可扩展性、可维护性、兼容性等 12 大类评估属性，117 个评测指标。**

区块链成熟度评测模型评测目标不限于开源软件，还包括商业软件，因此，整体模型中与开源软件相关的开源许可证、行业认可度、产品活力、服务支持等 4 大类评估属性，区块链成熟度评测模型并不包含。

区块链成熟度评测模型重点围绕金融业关注的特性以及可评测的指标进行建立，涵盖整体模型的 8 大类评估属性：功能性、性能效率、安全性、可靠性、易用性、可扩展性、可维护性、兼容性，具体包括 P2P 网络、智能合约、共识算法、账户体系、隐私安全等 34 个测试项、108 个评测指标。

评测环境

在本地局域网环境，我们测试了商业区块链 A、商业区块链 B、局域网 Fabric，此外我们还测试了广域网 Fabric。广域网 Fabric，由银联、京东、万达、招行四方组建，节点分布在北京、上海、深圳，其中银联、京东、招行为物理节点，万达为公有云节点。具体评测环境与配置如表 1。

表 1 评测环境与配置

区块链系统	机器数量	CPU/内存	主频	软件环境（操作	系统版本
-------	------	--------	----	---------	------

				系统、应用软件)	
商业区块链 A	6 台	4 核/8G	2.0ghz	CentOS 7.2	1.2
商业区块链 B	6 台	4 核/8G	2.0ghz	Ubuntu 16.04 LTS	1.1
局域网 Fabric	6 台	4 核/8G	2.0ghz	CentOS 7.2	1.02
广域网 Fabric	9 台	4 核/8G*6 2 核/16G*3	2.0ghz*6 2.3ghz*2 2.5ghz*1	CentOS 7.2	1.02

功能性对比

区块链的功能性主要考察账户体系、交易、区块、智能合约、区块链网络、共识算法、共享帐本七个方面。

（一）账户体系：商业区块链 A 账户体系健全，商业区块链 B 和 Fabric 账户体系尚待完善

账户体系主要测试七个指标：账户分级、账户分类、账户实名、账户注册、注册审批、注册形式、账户注销。七个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是通过建立二级账户体系进行验证，如果一级账户能够查到其名下的二级账户，则支持账户分级；第二个指标的测试方法是通过建立不同类别账户，检查是否具有账户分类信息进行验证；第三个指标的测试方法是通过建立账户，检查该账户是否具有实名功能，例如，是否绑定手机号、身份证号码、银行卡等信息；第四个指标的测试方法是通过在某一个节点下进行注册，检查账户是否创建成功；第五个指标的测试方法是通过在某一个节点下进行注册，检查账户是否需要审批才能完成创建；第六个指标的测试方法是检查区块链是否对任何用户均能注册，即开放式注册，检查区块链是否能够针对特定的用户做注册检查，即特定用户注册；第七个指标的测试方法是在某一节点下进行账户注销行为，检查注销后账户是否存在。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
账户分级	支持	不支持	支持
账户分类	支持	支持	支持

账户实名	支持	支持	不支持
账户注册	支持	支持	支持
注册审批	支持	不支持	不支持
注册形式	邀请注册、开放注册	开放注册	开放注册
账号注销	支持	不支持	不支持

测试结果表明,商业区块链 A 注册形式丰富,账户体系功能健全,商业区块链 B 和 Fabric 注册形式单一,均不支持注册审批和账号注销,此外,商业区块链 B 不支持账户分级, Fabric 不支持账户实名。

(二) 交易：商业区块链 A、商业区块链 B、Fabric 交易功能完备

交易主要测试两个指标：交易查询幂等性、交易持久性。两个指标的测试方法都是根据白皮书与相关文档进行专家判断,具体来说,第一个指标的测试方法是向正在运行的区块链节点发送一笔交易,再对其进行连续 10 次查询操作,比较结果是否一致判断;第二个指标的测试方法是交易成功发起后,被持久化到区块链中,并且不可更改。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
交易查询幂等性	支持	支持	支持
交易持久性	支持	支持	支持

测试结果表明,商业区块链 A、商业区块链 B、Fabric 均支持交易查询幂等性和交易持久性,三个区块链系统交易功能完备。

(三) 区块：商业区块链 A、商业区块链 B、Fabric 区块功能完备

区块主要测试两个指标：查询区块平均生成时间、查询指定区块信息。两个指标的测试方法都是根据白皮书与相关文档进行专家判断,具体来说,第一个指标的测试方法是对指定序列的区块的生成时间进行求和计算平均值;第二个指标的测试方法是通过接口判断能否获取指定区块的区块号,所含交易数量信息。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
查询区块平均生成时间	支持	支持	支持
查询指定区块信息	支持	支持	支持

测试结果表明,商业区块链 A、商业区块链 B、Fabric 均可查询区块平均生成时间和指定区块信息,三个区块链系统区块功能完备。

（四）智能合约：商业区块链 A 智能合约功能完备，商业区块链 B 和 Fabric 具备智能合约核心功能

智能合约主要测试六个指标：智能合约图灵完备、智能合约部署前需注册、智能合约发布时需审计、智能合约具备完整的生命周期管理、智能合约可见、智能合约的源码或二进制码查询。前四个指标的测试方法是根据白皮书与相关文档进行专家判断，后两个指标的测试方法是专家判断与接口判断相结合，具体来说，第一个指标的测试方法是判断智能合约是否具备图灵完备特征；第二个指标的测试方法是判断智能合约在部署前是否需要经过注册审批；第三个指标的测试方法是判断智能合约在发布的时候是否需要后台审计；第四个指标的测试方法是从编写到部署再到销毁分别进行测试，记录生命周期中各个相关操作（如设置合约的过期时间、销毁所需条件等），在智能合约生命周期中，分别测试智能合约的可用性；第五个指标的测试方法是使用不同账户部署不同数量的合约，查询某一账户下的所有智能合约、查询某一智能合约对应的部署账户地址；第六个指标的测试方法是部署智能合约，通过接口查询其源码或二进制码。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
智能合约图灵完备	是	是	是
智能合约部署前需注册	是	是	否
智能合约发布时需审计	是	是	否
智能合约具备完整的生命周期管理	是	否	否
智能合约可见	是	否	是
智能合约的源码或二进制码查询	是	否	否

测试结果表明，商业区块链 A 六项指标全部通过测试，智能合约功能完备，商业区块链 B 图灵完备、部署前需注册、发布时需审计三个指标通过测试，Fabric 图灵完备、合约可见两个指标通过测试。

（五）区块链网络：商业区块链 A、商业区块链 B、Fabric 区块链网络功能完备

区块链网络主要测试三个指标：节点的类别和能力修改和设定、节点的信息和状态获得、平台参数化。第一、三指标的测试方法是通过白皮书与相关文档进行专家判断，第二个指标的测试方法是接口判断，具体来说，第一个指标的测试方法是对不同节点进行类别与权限设定，检查设定后的各节点的类别与权限；第二个指标的测试方法是对不同节点进行状态修改或宕机重启，通过接口来检查设定后的各节点状态；第三个指标的测试方法是手动修改配置

文件，读取日志，判断配置文件修改是否生效。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
节点的类别和能力修改和设定	支持	支持	支持
节点的信息和状态获得	支持	支持	支持
平台参数化	支持	支持	支持

测试结果表明，商业区块链 A、商业区块链 B、Fabric 节点的类别和能力可以修改和设定、节点的信息和状态可以获得、支持平台参数化，三个区块链系统网络功能完备。

（六）共识算法：商业区块链 A、商业区块链 B、Fabric 共识算法各不相同

共识算法主要测试两个指标：共识算法种类、拜占庭容错算法。两个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是对支持的所有共识算法，通过交易进行逐一验证；第二个指标的测试方法是使用拜占庭容错算法作为区块链的共识算法，检查网络中节点达成共识的情况以及抗攻击能力。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
共识算法种类	RBFT	POI+多人投票	Fabric 使用交易全生命周期验证实现共识
拜占庭容错算法	支持	支持	不支持

测试结果表明，在共识算法种类方面，三个区块链系统分别采用了不同的共识算法，在拜占庭容错算法方面，只有 Fabric 不支持拜占庭容错。

（七）共享账本：商业区块链 A 共享账本功能最全面，Fabric 次之，商业区块链 B 最弱

共享账本主要测试七个指标：区块大小静态调整、区块大小动态调整、完整账本同步、部分账本同步、全量账本检索、账本选择性下载、局部账本。七个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是在网络离线状态下，根据区块链提供的配置参数调整区块大小，检查是否生效；第二个指标的测试方法是在网络在线状态下，根据区块链提供的配置参数调整区块大小，检查是否生效；第三个指标的测试方法是新增一个节点，查看账本是否完全同步；第四个指标的测试方法是新增一个节点，设定需要同步的部分账本(如区块编号 2000 至 3000 部分账本)，检查账本部分同步是否成功；第五个指标的测试方法是模拟进行第一个区块、最后一个区块以及中间任意区块的账本检索，检查是否能够检索成功；第六个指标的测试方法是对部分账本（如区块 100-1000）根据

提供的下载接口进行选择性下载测试，检查下载的结果是否正确；第七个指标的测试方法是选取测试节点后通过脚本进行局部账本的生成，测试是否可以仅同步局部账本。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
区块大小静态调整	支持	不支持	支持
区块大小动态调整	支持	不支持	支持
完整账本同步	支持	支持	支持
部分账本同步	支持	不支持	不支持
全量账本检索	支持	支持	支持
账本选择性下载	支持	不支持	支持
局部账本	支持	不支持	支持

测试结果表明，商业区块链 A 七项指标全部支持，共享帐本功能完备，Fabric 除部分账本同步不支持外，其他六项指标均支持，商业区块链 B 仅支持完整账本同步和全量账本检索两个指标。

综合来看，账户体系、智能合约、共享帐本方面，商业区块链 A 功能最健全；交易、区块、区块链网络方面，三个区块链系统均功能完备；共识算法方面，三个区块链系统分别支持不同的共识算法。

性能效率对比

区块链的性能效率主要考察区块链网络的交易吞吐量。

（一）交易吞吐量：商业区块链 A 交易吞吐量最高，Fabric 次之，商业区块 B 链最低

交易吞吐量是指单位时间能够完成交易的最高个数，测试方法如下：

1. 设 N_t 为统计时间内发送的交易笔数， N_b 为统计时间内区块上记录的交易笔数，通过频率可调的交易生成器随机生成交易，满足 N_t 可控。
2. 当测量交易吞吐量时，按照一定速率不断（可并发）生成随机交易。不断提高交易生成速率，直到 N_t 大于 N_b ，记录此时的压测系统配置参数，即为最佳压测参数。
3. 按照最佳压测参数，对区块链系统进行压力测试，测试多次，记录单位时间内区块上记录的交易笔数，并取平均值，即为交易吞吐量。

交易吞吐量主要测试一个指标：调用合约 TPS。商业区块链 A、商业区块链 B、局域网

Fabric 是局域网环境，千兆网络带宽；广域网 Fabric 是跨地域、跨网络运营商的广域网环境，十兆网络带宽，网络环境复杂，网络节点类型包含物理节点和公有云节点，网络节点硬件配置各不相同，具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	局域网 Fabric	广域网 Fabric
调用合约 TPS（笔/秒）	1599.6	12	368.8	77.3

测试结果表明，本地局域网环境下，交易吞吐量方面，商业区块链 A 大约是局域网 Fabric、商业区块链 B 的 4 倍、130 倍，交易吞吐量最高。广域网环境下，网络节点跨物理大区、跨网络运营商、公有云节点等因素产生网络时延，且网络带宽有限，造成广域网 Fabric 的交易吞吐量下降，大约是局域网 Fabric 的 1/5。

安全性对比

区块链的安全性主要考察身份验证、访问控制、加密体系和隐私、密码算法、匿名性、抗攻击能力六个方面。

（一）身份验证：商业区块链 A 身份验证功能全面，Fabric 身份验证场景单一，商业区块链 B 私钥生命周期管理不完整

身份验证主要测试五个指标：身份验证的方式、身份验证的场景、防止身份冒用、私钥具有完整的生命周期管理、节点的进出需要身份验证。五个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是对支持的所有身份验证方式通过交易逐一验证；第二个指标的测试方法是搜集身份验证的场景，对支持的所有身份验证场景通过模拟交易进行逐一验证；第三个指标的测试方法是判断是否具有防止身份冒用的功能，使用错误的身份信息进行登陆或支付相关操作，验证能够通过；第四个指标的测试方法是判断私钥是否具有完整的生命周期管理，测试私钥的生命周期管理；第五个指标的测试方法是判断私钥是否具有增删节点时的身份验证功能，若具有，增加或删除一个未经过认证的节点，测试是否增删成功，增加或删除一个经过认证的节点，测试是否增删成功。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
身份验证的方式	密钥验证	密钥验证	密钥验证
身份验证的场景	转账、查询、登陆	转账、查询、登陆	转账
防止身份冒用	是	是	是

私钥具有完整的生命周期管理	是，私钥有生成、分发、存储、使用以及销毁过程	否	是，私钥有生成、分发、存储、使用以及销毁过程
节点的进出需要身份验证	是	是	是

测试结果表明，商业区块链 A 身份验证场景丰富，身份验证功能全面；Fabric 身份验证的场景只支持转账，场景单一；商业区块链 B 的私钥没有完整的生命周期管理。

（二）访问控制：商业区块链 A 访问控制功能全面，Fabric 具备核心访问控制功能，商业区块链 B 访问控制功能缺失

访问控制主要测试七个指标：不同级别账户权限不同、不同分类账户权限不同、超级账户的权限、账户间的授权、账户授权时限控制、账户权限变更、权限变更形式。七个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是分别建立各个级别下的不同账户，模拟发起各类交易，检查不同账户支持的交易种类是否一样；第二个指标的测试方法是分别建立各个分类下的不同账户，模拟发起各类交易，检查不同账户支持的交易种类是否一样；第三个指标的测试方法是建立一个具有超级账户权限的账户，模拟发起各类交易，检查该账户是否全部支持，通过该账户查看其它账户的信息及交易，检查是否有权限能查看，通过该账户对其它账户进行审批、回收等操作，检查是否对其它账户具有管理功能；第四个指标的测试方法是建立两个不同的账户 A 和 B，使用 A 账户对 B 账户进行某项交易授权，通过 B 账户发起 A 账户的授权交易，验证是否成功；第五个指标的测试方法是建立两个不同的账户 A 和 B，使用 A 账户对 B 账户进行某项交易授权，指定授权时限为 10 分钟，分别在 10 分钟内和 10 分钟后通过 B 账户发起 A 账户的授权交易，验证两次交易是否成功；第六个指标的测试方法是建立不同层级的两个账户，使用高级别账户对低级别的账户进行权限的变更，如禁止转账，检查低级别账户是否仍能够进行转账交易；第七个指标的测试方法是对白皮书支持的所有权限变更形式通过模拟测试进行逐一验证。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
不同级别账户权限不同	支持	不支持	支持
不同分类账户权限不同	支持	不支持	支持
超级账户的权限	支持	不支持	支持

账户间的授权	支持	不支持	不支持
账户授权时限控制	支持	不支持	不支持
账户权限变更	支持	不支持	不支持
权限变更形式	高级别账户授权， 线下授权	不支持	不支持

测试结果表明，商业区块链 A 访问控制功能全面，Fabric 支持不同级别账户权限不同、不同分类账户权限不同、超级账户的权限，商业区块链 B 访问控制七个指标均不支持，访问控制功能缺失。

（三）加密体系和隐私：商业区块链 A 加密体系健全，Fabric 签名应用场景单一，商业区块链 B 交易信息不加密

加密体系和隐私主要测试四个指标：交易信息加密、签名的应用场景、签名使用的私钥保存、私钥丢失能否保护用户财产。四个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是查阅交易信息的加密情况，若支持加密，列出所有加密场景下使用的算法和加密的要素，在各个场景下，模拟发起交易，截取交易明文和加密后的密文，使用解密工具进行解密，检查解密后的内容是否与明文一致；第二个指标的测试方法是收集所有可能的签名应用场景，列出签名应用的场景，在各个场景下模拟发起交易，查看交易记录是否会记录签名后的信息，尝试调用接口的时候不签名，检查交易是否报异常；第三个指标的测试方法是获取所有的私钥保存方式与存储路径，检查私钥的保存方式和存储路径，修改私钥文件，验证私钥文件在交易过程中能否起作用，检查交易状态；第四个指标的测试方法是在私钥存储路径下删除某一个账户对应的私钥，查询该账户的资产，在私钥存储路径下删除某一个账户对应的私钥，使用该账户向其他账户进行转账交易，检查交易状态、账户财产变化情况，在私钥存储路径下删除某一个账户对应的私钥，使用别的账户向该账户转账，检查交易状态、账户财产变化情况。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
交易信息加密	支持，加密算法包括：SHA3-256，ECDSA， 国密 ，加法同态加密；	不支持	支持，加密算法包括：SHA2，SHA3，ECDSA

签名的应用场景	查询，转账，发行	查询，转账，发行	转账
签名使用的私钥保存	私钥被加密后存于用户 PC 或手机	私钥被加密后存于用户 PC 或手机	私钥被加密后存于用户 PC 或手机
私钥丢失能否保护用户财产	否，账户资产仍然存在，但是无法交易。	否，账户资产仍然存在，但是无法交易。	否，账户资产仍然存在，但是无法交易。

测试结果表明，商业区块链 A 签名应用场景丰富，加密体系健全，Fabric 签名应用场景仅支持转账，场景单一，商业区块链 B 不支持交易信息加密。

（四）密码算法：商业区块链 A 密码算法功能全面，商业区块链 B 和 Fabric 均不支持国密算法

密码算法主要测试四个指标：密码算法种类、国密算法、加密机、可插拔自定义密码算法。四个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是收集支持的密码算法种类；第二个指标的测试方法是判断该区块链是否支持国密算法，若支持，通过区块链提供的接口，调用国密算法进行验证；第三个指标的测试方法是判断该区块链是否支持加密机，若支持，通过区块链提供的接口，调用加密机进行加密验证；第四个指标的测试方法是判断该区块链是否支持可插拔自定义密码算法，若支持，通过区块链提供的接口，调用自定义的密码算法进行验证。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
密码算法种类	ECDSA，加法同态加密， 国密 ，SHA3	RSA、SHA3	ECDSA，SHA2，SHA3
国密算法	支持	不支持	不支持
加密机	不支持	不支持	不支持
可插拔自定义密码算法	支持	不支持	支持

测试结果表明，国密算法方面，仅商业区块链 A 支持；密码算法种类方面，商业区块链 A 最丰富，Fabric 次之，商业区块链 B 最少；可插拔自定义密码算法方面，商业区块链 A 和 Fabric 均支持，商业区块链 B 不支持；三个区块链系统均不支持加密机。

（五）匿名性：商业区块链 A 和 Fabric 匿名性功能全面，商业区块链 B 具备匿名性核心功能

匿名性主要测试五个指标：交易匿名、全部匿名还是部分匿名、子账户对其父账户保持

交易透明、子账户对其他父账户保持交易匿名、对审计或超级权限账户保持交易透明。五个指标的测试方法都是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是随机查询任意一个区块上任意一笔交易，使用任意一个账户，通过交易中的用户地址查询真实用户信息，若查不到真实用户信息，则代表支持交易匿名；第二个指标的测试方法是查询任意一个区块上任意一笔交易，使用任意一个账户，通过交易中的用户地址查询真实用户信息，若查不到真实用户信息，则代表支持全部匿名。查询任意一个区块上任意一笔交易，使用审计或超级权限账户通过交易中的用户地址能够查询真实用户信息，而使用普通账户通过交易中的用户地址不能查询真实用户信息，则代表支持部分匿名；第三个指标的测试方法是选取一个子账户，模拟发起一笔交易，父账户通过交易中的子账户用户地址查询真实用户信息，若能查到子账户的真实用户信息，则代表子账户对父账户保持交易透明；第四个指标的测试方法是选取一个子账户，模拟发起一笔交易，随机选取其他任意一个父账户，通过交易中的子账户用户地址查询真实用户信息，若不能查到子账户的真实用户信息，则代表子账户对其他父账户保持交易匿名；第五个指标的测试方法是判断该区块链是否支持普通账户对审计或超级权限账户保持交易透明，查询任意一个区块上任意一笔交易，使用审计或超级权限账户，通过交易中的用户地址查询真实用户信息，若查到真实用户信息，则代表普通账户对审计或超级权限账户保持交易透明。具体测试结果见下表。

对比项	商业区块链 A	商业区块链 B	Fabric
交易匿名	支持	支持	支持
全部匿名还是部分匿名	全部匿名，部分匿名	部分匿名	全部匿名，部分匿名
子账户对其父账户保持交易透明	支持	不支持	支持
子账户对其他父账户保持交易匿名	支持	不支持	支持
对审计或超级权限账户保持交易透明	支持	支持	支持

测试结果表明，商业区块链 A 和 Fabric 五项匿名性指标全部支持，匿名性功能全面，商业区块链 B 仅支持部分匿名，此外，还支持交易匿名、对审计或超级权限账户保持交易透明两项指标。

（六）抗攻击能力：商业区块链 A 和 Fabric 抗攻击能力强，商业区块链 B 抗攻击能力弱

抗攻击能力主要测试四个指标：抵御 DDOS、黑客等网络攻击、抗攻击能力程度、最大容忍节点失效个数、最大容忍节点欺骗个数。四个指标都是通过工具进行模拟评测，具体来说，第一个指标的测试方法是根据白皮书与相关文档搜集抗攻击能力，通过工具分别模拟“10%、30%和 51%”欺骗节点情况，同时欺骗节点构建虚拟网络，验证新节点加入时是否会进行识别虚拟网络，或区块链系统能够防范此虚拟网络的构建，通过工具模拟一定量节点向特点目标节点发送大量垃圾分组消息，节点和区块链系统是否有对拦截分组消息防范能力；第二个指标的测试方法是根据白皮书与相关文档搜集抗攻击能力，通过测试工具分别模拟 30%、50%、51%的节点攻击，检验共识算法的结果是否与预期一致；第三、四个指标的测试方法是根据白皮书与相关文档搜集最多容忍失效或欺骗节点数 N，通过工具模拟 N 个节点失效或欺骗，检验共识算法的结果是否与预期一致。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
抵御 DDOS、黑客等网络攻击	支持	不支持	支持
抗攻击能力程度	通过	不支持	通过
最大容忍节点失效个数	N/3 节点失效	N/3 节点失效	自定义
最大容忍节点欺骗个数	N/3 欺骗节点	N/3 欺骗节点	自定义

测试结果表明，Fabric 抗攻击能力最强，商业区块链 A 次之，商业区块链 B 不支持抵御 DDOS、黑客等网络攻击。

综合来看，身份验证、访问控制、加密体系和隐私、密码算法方面，商业区块链 A 功能最全面，抗攻击能力方面，Fabric 抗攻击能力最强，匿名性方面，商业区块链 A 和 Fabric 均功能完备。

可靠性对比

区块链的可靠性主要考察区块链网络、共享帐本、账户体系三个方面。

（一）区块链网络：商业区块链 A、商业区块链 B、Fabric 均网络可靠

区块链网络主要测试三个指标：记账节点高可用、服务节点之间高可用、区块链网络的

网络抖动是否影响系统服务等级。第一、二个指标的测试方法是通过脚本进行评测，设区块链中包含 n 个记账节点或服务节点，通过脚本依次停掉 $1\sim n$ 个记账节点或服务节点，检查区块链网络是否依然能够正确执行交易、达成共识并记账或通过服务节点对外提供服务；第三个指标的测试方法是通过工具进行模拟评测，在规定的服务等级和网络规模下，通过模拟一定量的网络节点加入或退出，获得其所容忍得比例值。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
记账节点高可用	支持	支持	支持
服务节点高可用	支持	支持	支持
区块链网络的网络抖动是否影响系统服务等级	否	否	否

测试结果表明，商业区块链 A、商业区块链 B、Fabric 均支持记账节点和服务节点的高可用，且网络抖动不影响系统服务等级，三个区块链系统均网络可靠。

（二）共享帐本：商业区块链 A、商业区块链 B、Fabric 均账本可靠

共享帐本主要测试三个指标：账本高可用、账本支持 failover 同步、账本备份恢复。第一、二个指标的评测方法是通过脚本进行评测，第三个指标的评测方法是根据白皮书与相关文档进行专家判断，具体来说，第一个指标的测试方法是假设区块链中包含 n 个记账节点，每个记账节点均有一份共享账本，通过脚本依次停掉 $1\sim n$ 个记账节点，检查区块链网络是否依然能够正确执行交易、达成共识并记账，恢复被停掉的节点，检查是否自动同步为最新账本；第二个指标的测试方法是通过脚本停掉区块链网络中的某一个记账节点，经过 10 个区块的生成时间后通过脚本重新开启该节点，恢复被停掉的节点，检查是否自动同步为最新账本并恢复记账能力；第三个指标的测试方法是判断是否有备份和恢复的工具，若有，使用该工具进行备份导出操作，经过一段时间后，使用工具进行备份恢复导入操作，检查账本是否回到备份时的状态，并正常运行。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
账本高可用	支持	支持	支持
账本支持 failover 同步	支持	支持	支持
账本备份恢复	支持	支持	支持

测试结果表明，商业区块链 A、商业区块链 B、Fabric 均支持账本高可用、账本支持 failover 同步、账本备份恢复，三个区块链系统账本可靠。

（三）账户体系：商业区块链 A、商业区块链 B、Fabric 均账户可靠

账户体系主要测试一个指标：不同节点下的账户信息高可用。测试方法是利用脚本使某一账户所在节点失效，使用脚本对失效节点的账户进行模拟转账等交易行为，检查交易是否成功；若成功，则不同节点的账户信息高可用。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
不同节点下的账户信息 高可用	支持	支持	支持

测试结果表明，商业区块链 A、商业区块链 B、Fabric 均支持不同节点下的账户信息高可用，三个区块链系统账户可靠。

综合来看，区块链网络、共享帐本、账户体系三个方面，商业区块链 A、商业区块链 B、Fabric 均可靠。

易用性对比

区块链的易用性主要考察区块链网络、智能合约、交易、账户体系、共享帐本五个方面。

（一）区块链网络：商业区块链 A 网络操作最简单，Fabric 次之，商业区块链 B 不支持删除网络节点

区块链网络主要测试两个指标：网络搭建的复杂程度、增删节点的复杂程度。测试方法是根据白皮书与相关文档收集搭建多节点区块链网络或增删节点的具体步骤，模拟搭建多节点区块链网络或增删节点，计算搭建所需时间及搭建步骤复杂程度或增删步骤复杂程度。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
网络搭建的复杂程度	不超过 10 分钟	不超过 8 小时	不超过 4 小时
增删节点的复杂程度	增删节点不需要停机	支持增加节点功能， 不支持删除节点	增删节点不需要停机

测试结果表明，网络搭建的复杂程度方面，商业区块链 A 最快，10 分钟以内，Fabric 次之，4 小时以内，商业区块链 B 最慢，8 小时以内。增删节点的复杂程度方面，商业区块链 A 和 Fabric 均支持增删节点且不需要停机，商业区块链 B 不支持删除节点。

（二）智能合约：商业区块链 A 和 Fabric 智能合约操作简单，商业区块链 B 智能合约操作需通过中心节点

智能合约主要测试三个指标：智能合约支持的语言、注册智能合约复杂程度、部署智能合约复杂程度。第一个指标的测试方法是根据白皮书与相关文档收集智能合约支持的开发语言；第二、三个指标的测试方法是通过在某一个节点下进行智能合约注册或部署行为，记录所需流程，流程需要 2 步以上视为复杂。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
智能合约支持的语言	Solidity	Go	Go, node.js
注册智能合约复杂程度	简洁，上传源代码，私钥加密	通过中心管理节点的合约管理功能，能够快速注册	简洁，上传源代码，私钥加密
部署智能合约复杂程度	部署过程简单	通过中心管理节点的合约管理功能，能够快速部署	部署过程简单

测试结果表明，三个区块链系统的智能合约分别支持不同的语言，智能合约注册和部署方面，商业区块链 A 和 Fabric 采用去中心化方式，商业区块链 B 采用中心节点方式，三个系统的过程均简单。

（三）交易：商业区块链 A 和 Fabric 交易操作简单，商业区块链 B 交易查询仅支持接口进行

交易主要测试两个指标：交易查询复杂度、交易发起复杂度。测试方法是通过在某一个节点下进行交易的查询或发起行为，记录所需流程，流程需要 2 步以上视为复杂。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
交易查询复杂度	交易查询过程简单，支持接口、sdk 进行查询	支持接口进行查询	交易查询过程简单，支持接口、sdk 进行查询
交易发起复杂度	交易发起过程简单，私钥签名，发送交易和签名结果即可	交易发起过程简单，私钥签名，发送交易和签名结果即可	交易发起过程简单，私钥签名，发送交易和签名结果即可

测试结果表明，交易查询方面，商业区块链 A 和 Fabric 支持接口、SDK 进行查询，商业

区块链 B 支持接口进行查询。

（四）账户体系：商业区块链 A 账户操作简单且健全，Fabric 次之，商业区块链 B 仅支持注册操作

账户体系主要测试三个指标：注册复杂度、销毁复杂度、授权复杂度。第一、二个指标的测试方法是通过在某一个节点下进行注册或销毁行为，记录所需流程，流程需要 2 步以上视为复杂；第三个指标的测试方法是模拟将 B 账户授权给 A 账户，记录授权所需流程，流程需要 2 步以上视为复杂。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
注册复杂度	注册简单	注册简单	注册简单
销毁复杂度	销毁简单	不支持销毁	销毁简单
授权复杂度	授权简单	不支持授权	不支持授权

测试结果表明，商业区块链 A 账户体系易用性功能丰富，Fabric 次之，商业区块链 B 仅支持注册。

（五）共享帐本：商业区块链 A、商业区块链 B、Fabric 均支持账本检索

共享账本主要测试两个指标：共享账本的检索条件限定、建立索引。两个指标的测试方法都是根据白皮书与相关文档判断，具体来说，第一个指标的测试方法是判断是否支持检索，若支持，模拟账本检索，使用脚本工具计算平均检索时间。第二个指标的测试方法是判断是否支持建立索引，若支持，模拟对共享账本进行索引建立。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
共享账本的检索条件限定	支持根据 id、关键字、时间区间、条件选择、溯源进行检索	支持根据 id、关键字、时间区间、条件选择、溯源进行检索	支持根据 id、关键字、时间区间、条件选择、溯源进行检索
建立索引	不支持	不支持	不支持

测试结果表明，三个区块链系统均支持通过 id、关键字、时间区间、条件选择、溯源进行账本检索，但均不支持建立索引。

综合来看，区块链网络、账户体系方面，商业区块链 A 最易用且功能健全，智能合约和交易方面，商业区块链 A 和 Fabric 操作最简单，共享帐本方面，三个区块链系统均支持账本检索。

可扩展性对比

区块链的可扩展性主要考察网络节点、共识算法、外围开发、云平台集成四个方面。

（一）网络节点：商业区块链 A 和 Fabric 网络节点可扩展性高，商业区块链 B 不支持网络节点动态删除

网络节点主要测试三个指标：网络节点动态增加、网络节点动态删除、网络节点数量限制。三个指标的测试方法都是通过白皮书与相关文档进行专家判断，具体来说，第一、二个指标的测试方法是使用系统提供的命令尝试在网络中动态增加或删除一个节点，检查节点增加或删除后网络状态是否正常；第三个指标的测试方法是判断是网络节点是否有限制，若有限制，限制是多少，即为区块链网络规模，通过模拟不断动态增加网络节点数，检查网络规模到达节点数限制前，是否正常，若无限制，通过模拟不间断动态增加网络节点数，检查网络是否异常。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
网络节点动态增加	支持	支持	支持
网络节点动态删除	支持	不支持	支持
网络节点数量限制	无限制	无限制	无限制

测试结果表明，商业区块链 A 和 Fabric 网络节点可扩展性功能完备，可扩展性高，商业区块链 B 不支持网络节点动态删除。

（二）共识算法：商业区块链 A 和 Fabric 共识算法可扩展性高，商业区块链 B 不支持可插拔自定义共识算法

共识算法主要测试六个指标：可插拔自定义共识算法、若采用 PoW，挖矿难度能否自定义？、若采用 PoW，需要多少个区块的确认才能保证一笔交易不会被撤销？、共识算法根据网络规模调整、共识算法根据参与方数量调整、共识算法根据交易吞吐量需求调整。六个指标的测试方法都是通过白皮书与相关文件进行专家判断，具体来说，第一个指标的测试方法是通过区块链的预留接口加载自定义的共识算法，检查网络中节点达成共识的情况；第二个指标的测试方法是通过区块链提供的接口进行自定义挖矿难度，检验不同挖矿难度下，交易达成共识所需时间是否不同；第三个指标的测试方法是判断是否采用 PoW，若采用，需要等 N 个区块后才能真正确认交易，计算 N 个区块后该笔交易被丢弃的概率；后三个指标的测试方法是检查共识算法是否能够自定义配置，配置项中是否有根据网络规模、参与方数量或交易吞吐量进行调整的参数。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
可插拔自定义共识算法	支持	不支持	支持
若采用 PoW，挖矿难度能否自定义？	不支持 PoW	不支持 PoW	不支持 PoW
若采用 PoW，需要多少个区块的确认才能保证一笔交易不会被撤销？	不支持 PoW	不支持 PoW	不支持 PoW
共识算法根据网络规模调整	支持	支持	支持
共识算法根据参与方数量调整	支持	支持	支持
共识算法根据交易吞吐量需求调整	支持	支持	支持

测试结果表明，商业区块链 A 和 Fabric 支持可插拔自定义共识算法，共识算法可扩展性高，商业区块链 B 不支持可插拔自定义共识算法。

（三）外围开发：商业区块链 A 外围开发支持丰富，Fabric 次之，商业区块链 B 仅支持 SDK、API

外围开发主要测试三个指标：可插拔 Plugin、ETL、SDK 和 API，第一个指标的测试方法是可根据已有的 Plugin 进行安装与卸载来验证 Plugin 的可用性；第二、三个指标的测试方法是根据提供的 ETL 接口、SDK、API 进行开发验证。具体测试结果见下表。

对比项	商业区块链 A	商业区块链 B	Fabric
可插拔 Plugin	支持	不支持	支持
ETL	支持	不支持	不支持
SDK 和 API	支持	支持	支持

测试结果表明，商业区块链 A 支持可插拔 Plugin、ETL、SDK 和 API 开发，可扩展性好，Fabric 不支持 ETL 开发，商业区块链 B 只支持 SDK 和 API 开发。

（四）云平台集成：商业区块链 A 和 Fabric 云平台集成支持范围大，商业区块链 B 云平台集成缺失

云平台集成主要测试三个指标：与云平台集成、与哪些云平台集成、提供相应的集成接

口，第一个指标的测试方法是使用云平台进行集成验证；第二个指标的测试方法是分别进行不同种类的云平台验证；第三个指标的测试方法是使用相应的集成接口进行验证。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
与云平台集成	支持	不支持	支持
与哪些云平台集成	支持阿里云、腾讯云、亚马逊云等云平台	不支持	支持阿里云、腾讯云、亚马逊云等云平台
提供相应的集成接口	支持	不支持	支持

测试结果表明，商业区块链 A 和 Fabric 支持与众多主流云平台集成，且提供相应的集成接口，商业区块链 B 不支持与云平台集成。

综合来看，网络节点、共识算法、云平台集成方面，商业区块链 A 和 Fabric 可扩展性高，外围开发方面，商业区块链 A 广泛支持。

可维护性对比

区块链的可维护性主要考察印记管理、系统管理、策略管理、智能合约、易部署性五个方面。

（一）应急管理：商业区块链 A 应急管理体系完善，商业区块链 B 和 Fabric 无应急管理体系

应急管理主要测试一个指标：区块链网络在出现任何故障时的应急处理能力体系，测试方法是根据白皮书与相关文档进行专家判断。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
区块链网络在出现任何故障时的应急处理能力体系	有完善的维护机制，专门的维护机构，详细的应急预案	无	无

测试结果表明，商业区块链 A 具备完善的应急管理体系，商业区块链 B 和 Fabric 没有应急管理体系。

（二）系统管理：商业区块链 A 系统管理完善，商业区块链 B 和 Fabric 系统管理尚待完善

系统管理主要测试三个指标：管理监控平台、报警系统、运维接口，第一个指标的测试

方法是根据白皮书与相关文档进行判断是否提供管理监控平台，若提供，登录管理监控平台检查其功能；第二个指标的测试方法是根据白皮书与相关文档判断是否提供故障报警系统，若提供，可使某一节点失效来验证；第三个指标的测试方法是根据白皮书与相关文档判断是否提供运维相关的接口，若提供，尝试调用接口测试其能力。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
管理监控平台	有	有	无
报警系统	有	无	无
运维接口	有	无	有

测试结果表明，商业区块链 A 系统管理最完善，商业区块链 B 和 Fabric 系统管理尚待完善。

（三）策略管理：商业区块链 A 和 Fabric 策略管理完善，商业区块链 B 不支持访问控制权限配置

策略管理主要测试三个指标：创世区块自定义、区块生成时间配置、访问控制权限配置，第一个指标的测试方法是根据白皮书与相关文档进行专家判断，若支持，自定义创世区块的文件，以此建立区块链网络，检查区块链是否建立成功；第二个指标的测试方法是根据白皮书与相关文档进行专家判断，若支持，修改区块生成时间后进行验证；第三个指标的测试方法是根据白皮书与相关文档进行专家判断，若支持，将某一服务节点的权限修改为记账节点，检验其是否参与共识记账。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
创世区块自定义	支持	支持	支持
区块生成时间配置	支持	支持	支持
访问控制权限配置	支持	不支持	支持

测试结果表明，商业区块链 A 和 Fabric 策略管理完善，商业区块链 B 访问控制权限配置支持缺失。

（四）智能合约：商业区块链 A 智能合约可维护性好，商业区块链 B 和 Fabric 智能合约可维护性缺失

智能合约主要测试两个指标：智能合约动态更新、智能合约冻结或销毁，第一个指标的测试方法是根据白皮书与相关文档进行专家判断，若支持，对智能合约进行修改并动态更新，检查更新后效果；第二个指标的测试方法是根据白皮书与相关文档进行专家判断，若支持，

对智能合约进行冻结或销毁，然后向该合约发送交易，判断是否冻结、销毁成功。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
智能合约动态更新	支持	不支持	不支持
智能合约冻结或销毁	支持	不支持	不支持

测试结果表明，商业区块链 A 智能合约动态更新、冻结、销毁等后期维护均支持良好，可维护性好，商业区块链 B 和 Fabric 智能合约不支持后期维护，可维护性缺失。

（五）易部署性：商业区块链 A 和商业区块链 B 部署管理完善，Fabric 无监控平台

易部署性主要测试两个指标：区块链节点易部署、区块链监控平台的易部署，测试方法是根据系统部署文档，通过配置参数化文件进行系统部署。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
区块链节点易部署	是	是	是
区块链监控平台的易部署	是	是	无监控平台

测试结果表明，商业区块链 A 和商业区块链 B 节点和监控平台均容易部署，Fabric 没有监控平台。

综合来看，应急管理、系统管理、智能合约方面，商业区块链 A 管理体系完善，可维护性好，策略管理方面，商业区块链 A 和 Fabric 策略管理完善，易部署性方面，商业区块链 A 和商业区块链 B 部署管理完善。

兼容性对比

区块链的兼容性主要考察区块链系统、智能合约、数据三个方面。

（一）区块链系统：商业区块链 A 系统兼容性最高，Fabric 次之，商业区块链 B 最低

区块链系统主要测试一个指标：区块链系统兼容性，测试方法是在不同的操作系统、中间件、数据库之间进行系统移植，测试是否支持。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
区块链系统兼容性	支持 suse11、12、CentOS、Ubuntu 等	支持 Ubuntu 操作系统，底层支持多种关	支持 CentOS、Ubuntu 等操作系

	Unix 操作系统，底层支持多种关系型或非关系型数据库。	系型或非关系型数据库。	统，底层支持多种关系型或非关系型数据库。
--	------------------------------	-------------	----------------------

测试结果表明，商业区块链 A 支持的操作系统最多，系统兼容性最高，Fabric 次之，商业区块链 B 支持的操作系统最少，兼容性最低。

（二）智能合约：商业区块链 A 智能合约兼容性最好，商业区块链 B 和 Fabric 不支持智能合约移植

智能合约主要测试两个指标：智能合约可移植性、智能合约向前兼容性，第一个指标的测试方法是对现有的智能合约进行平台移植，检查移植后的合约是否可用；第二个指标的测试方法是将在旧版本的区块链上运行正常的智能合约部署到新版的区块链上，检查智能合约是否可用。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
智能合约可移植性	支持	不支持	不支持
智能合约向前兼容性	支持	支持	支持

测试结果表明，商业区块链 A 支持智能合约的可移植性、向前兼容性，智能合约兼容性最好，商业区块链 B 和 Fabric 不支持智能合约移植。

（三）数据：商业区块链 A 和 Fabric 支持数据移植，商业区块链 B 不支持

数据主要测试一个指标：数据可移植性，测试方法是模拟数据的迁移与恢复，检查是否成功。具体测试结果如下表。

对比项	商业区块链 A	商业区块链 B	Fabric
数据可移植性	支持	不支持	支持

测试结果表明，商业区块链 A 和 Fabric 支持数据移植，商业区块链 B 不支持数据移植。

综合来看，区块链系统、智能合约方面，商业区块链 A 兼容性最高，数据方面，商业区块链 A 和 Fabric 支持数据移植。

总结

根据区块链成熟度评测模型，我们从功能性、性能效率、安全性、可靠性、易用性、可扩展性、可维护性、兼容性八个方面，完成了对商业区块链 A、商业区块链 B、Fabric 三种区块链系统的成熟度评测，对比总结情况如下表所示。

测试指标	测试结果
功能性	商业区块链 A>Fabric>商业区块链 B
性能效率	商业区块链 A>Fabric>商业区块链 B
安全性	商业区块链 A>Fabric>商业区块链 B
可靠性	商业区块链 A=Fabric=商业区块链 B
易用性	商业区块链 A>Fabric>商业区块链 B
可扩展性	商业区块链 A>Fabric>商业区块链 B
可维护性	商业区块链 A>Fabric>商业区块链 B
兼容性	商业区块链 A>Fabric>商业区块链 B

总体来说，商业区块链 A 在各方面均优于 Fabric 和商业区块链 B，Fabric 整体上优于商业区块链 B。建议企业优先选择商业区块链 A。此外，作为开源区块链系统基础软件，Fabric 仍处于高速发展阶段，尚不成熟。