分布式总账技术架构评估报告（交流稿）

——ChinaLedger 系列研究报告之一

ChinaLedger 技术委员会

2016 年 7 月

1. 前言

近年来，分布式总账技术（Distributed Ledger Technology，简称 DTL）得到了金融界和 IT 界的普遍关注。在中国，分布式总账技术的实践者们紧跟世界潮流，在金融的主战场上，银行、证券、保险、信托等各类金融机构对分布式总账技术的关注度也日益提高。

与分布式总账这个概念密切关联的另一个概念是区块链（Block Chain）。一种观点认为，分布式总账就是多边共治的、可操作并记录价值的产生和转移的区块链；另一种观点认为，分布式总账也可以不必是区块链，只要具备多边共治的技术手段（共识机制和防伪机制）和以价值为背景的数据内容，就可以纳入分布式总账的范畴。为了不带偏见地做好技术评估工作，本报告也对非区块链的分布式总账技术体系给予同样的关注。

ChinaLedger 的中文全称是“中国分布式总账基础协议联盟”。ChinaLedgerd 的目标是聚焦资产端的分布式总账应用，兼顾货币端和非金融端应用，从精选的应用场景中提取出若干具有普遍性的金融服务模式，分别通过基础账本的协议/架构层面和应用层面的技术实现对相应业务提供完整支撑。

本报告是 ChinaLedger 系列报告的第一篇，旨在评估建设 ChinaLedger 可采纳的技术架构、可选择的技术资源和需解决的关键技术。

1.1 评估范围的选择

我们选择纳入评估范围的分布式总账技术体系，主要从两方面考虑：一是是否有利于为 ChinaLedger 提供一个好的“底本”，二是是否有足够接近应用场景的特色功能。

从“底本”选择的角度，纳入评估范围的分布式总账技术体系应具有广泛的影响力、充分的运营实践考验和可持续的技术支持以及技术发展动力。

从特色功能的角度，纳入评估范围的分布式总账技术体系应具有明确的金融业务背景、金融机构的参与和支持以及初步的金融业务场景测试。

一个理想的分布式总账技术体系应该兼具底本和特色功能两方面的优势，但是现实是，同时具有这两方面优势的分布式总账技术体系是凤毛麟角。这一方面使我们纳入评估范围的标准不得不有所妥协，另一方面也说明 ChinaLedger 面临的挑战和机遇也是全世界同行的共同面临的挑战和机遇。

鉴于此，本报告拟重点考察比特币、以太坊、比特股、Ripple、HyperLedger 和 Corda 六个分布式总账技术体系。我们知道，分布式账本的技术体系博大精深，这样的范围选择难免会挂一漏万。然而，既然确定了在有限时间内集中精力完成既定目标，就必须有所取舍。

1.2 评估要点的选择

从建设 ChiaLedger 目标出发，技术架构评估将基于以下十个维度：

- **领域适用性**：该技术体系更适应货币类、资产类还是非金融类应用？
- **场景适用性**：该技术体系更适应公有链、私有链还是联盟链？
- **计算能力完备性**：该技术体系是否提供通用编程接口？是否图灵完备？

- **架构分层合理性**：该技术体系的架构分层是否清晰合理？层与层之间的技术接口是否符合“低耦合、高内聚”原则？技术性能优化和业务逻辑是否“正交”？是否方便快速响应新的业务需求？是否可与其他新兴技术共存？未来是否有希望被业内接受为协议栈标准。

- **共识达成机制与效率**：共识机制是否做到拜占庭容错？是否能够在业务场景容忍的时间间隔内达成共识？是否提供更加有效利用冗余算力的并行机制？

- **计算与存储效率**：是否能够在业务场景容忍的存储开销水平上存储分布式账本？如果不能，替代的方案是什么？

- **隐私与特权机制**：是否有途径既能对所有账户的交易流水进行共识背书，又能有效隔离无关账户彼此知晓对方的敏感数据？是否可用同一套分布式总账基础设施支持若干个“基础设施共享，但业务数据隔离”的“沙箱”式的子生态？在前两个问题都有肯定解答的前提下，是否有途径为具有法定监管职能的特殊账户提供“看穿式的”数据访问权限？

- **原生数字货币的作用和必要性**：从支付手段、汇兑手段、激励机制和资源控制的角度看，原生数字货币的作用是什么？在资产端金融应用中，哪些作用应该保留，哪些作用应该去除？

- **技术与运营支持**：该技术体系是否提供在紧急情况下的应急、纠错和实施强制措施等手段？是否方便系统的升级特别是在线升级？所采用的编程语言是否合适？是否提供方便友好的开发工具环境？

- **未来发展潜力和动向**：该技术体系在可预见的将来发展方向是什么？是否有被引入金融业务主战场的潜力？是否有被取代、被边缘化或被少数厂商和机构垄断的可能性？

我们相信，从上面这些维度来解剖纳入评估范围的分布式总账技术体系，将有助于ChinaLedger 在后续工作中做出更加符合金融主战场业务实际和中国国情的决策。

2. 领域适用性

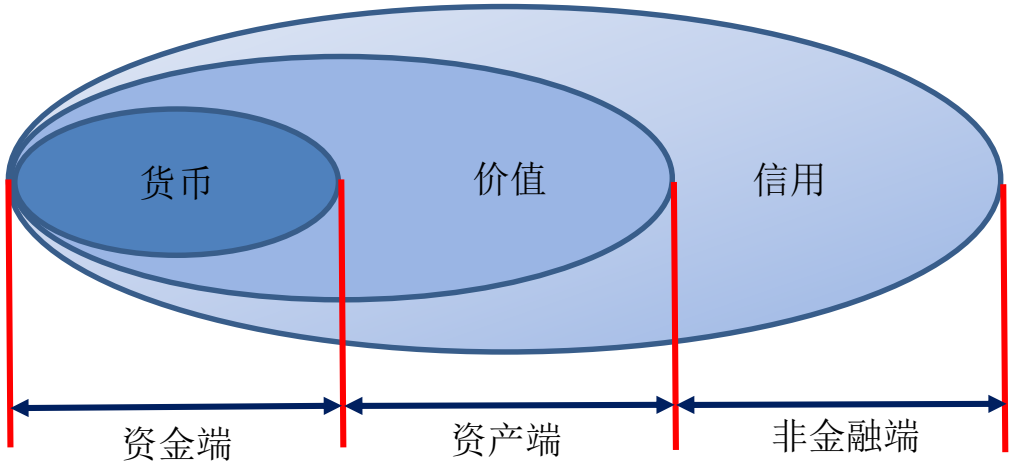
本节所说的领域，非指具体的应用领域，而是从宏观角度对具体应用领域的一种抽象。

分布式总账技术最初发源于数字货币领域。在数字货币的发行和流通中，分布式总账技术依托点对点网络和分布式架构，以数字货币的发行和转移为背景，提供了如下强安全功能：（1）身份的真实性；（2）交易的不可抵赖性；（3）时序的确定性；（4）价值的不可复制性；（5）余额的不可透支性。这些功能已被比特币的运作实践证明在技术上是成功的。

但是，该项技术用于记录守恒量在有限账户集合中的分布和转移，在转移中防止重复登记、重复消费以及透支行为，也是普遍适用的，因此凡属价值和实物资产的登记和转移，应用分布式账本技术一样可以提供上述五项强安全功能，因此，分布式账本技术还适用于包括数字货币在内的一切需要记录价值产生和转移的应用领域，故有“价值互联网”一说。

鉴于分布式账本技术本身在货币乃至价值的可信记录方面取得的成功并不特别依赖货币、价值的属性，因此在需要对信息甚至实物的变化进行可信记录的任何应用领域中，分布式账本技术也都能提供身份真实性、信息记录不可抵赖性和时序的确定性等涉及可信性的服务。所以更广义地看，分布式账本是提供的是一种信用服务。

于是，分布式总账技术所提供的货币服务、价值服务、信用服务，形成外延递进扩大的三个“圈”。仅货币服务所构成的领域，我们称之为“资金端”；除货币服务外的其他价值服务所构成的领域，我们称之为“资产端”；除价值服务外的其他信用服务所构成的领域，我们称之为“非金融端”。事实上，资金端、资产端和非金融端所对应的监管环境和市场业态，也是根本不同的。



比特币账本底层数据结构拥有的唯一一个价值字段用于描述比特币价值创造和转移的面额。换句话说，比特币技术体系如要移作他用，也只能提供单一标的资产的登记和转移。如要同时支持多种标的资产共处和交易，还需进行相应的改造。

以太坊、比特股、Ripple、HyperLedger 技术体系都能够同时提供多种标的资产（含数字货币）的登记和转移服务，天然支持数字货币和数字资产在一个区块链上共处，这对于构建具有资产交易业务逻辑的资产端应用来说是更加方便的。此外，除原生货币之外，由外部注入的数字货币（比如代币等）在技术处理上与普通的数字资产无异。外部注入的货币与原生货币之间的汇兑，其技术实现方式也与资产交易类同。

在非金融端，各技术体系一般都在底层数据结构中提供一个文本类型的信息字段，可供信息提供方签名分发，作为“经签发方确认的消息”，间接提供非金融领域的信用服务。在以太坊和 HyperLedger 技术体系中，经签发方确认的消息还可触发智能合约执行相应的动作。

如前所述，ChinaLedger 的使命是聚焦资产端应用，兼顾资金端和非金融端应用。因此我们期待被评估的分布式账本技术体系能够同时支持多种标的数字资产，能够支持外部注入的锚定法币的代币，能够支持经特定业务主体签发确认的消息来触发智能合约执行复杂的业务逻辑。

3. 场景适用性

本节所说的“场景”，非指具体的应用场景，而是对具体应用场景的一种抽象。

一个分布式总账技术体系首先是一套以软件代码为主的技术资源，同时这套技术资源又通过部署和运营形成相应的应用场景。技术体系和应用场景之间可以是一对多的，即一套技术资源可以部署多个实例。比如 HyperLedger 就是一套技术体系框架下多个项目实例，每个实例各有自己的命名。但业界在提到比特币、以太坊、比特股、Ripple 的时候，实际上都是既指一个技术体系，又指该技术体系的一个最典型、最有影响力的应用场景——它们对应的“公有链”。这或许会造成混淆。因此，我们在对分布式账本技术体系进行评估的

时候，必须严格区分二者——我们评估的只是分布式账本技术体系而并不是它对应的公有链，更不是它的社区。

根据分布式总账的技术特点，一个应用场景的参与方，既是业务的参与主体，同时又是其分布式总账本身的运营和见证主体。一般根据参与方加入应用场景是否需要获得许可，把场景分为“非许可的”和“许可的”两类。在区块链社区中也把“非许可的”场景称为“公有链”，把“许可的”场景细分为“私有链”和“联盟链”。私有链是由单边治理的业务生态，联盟链是由多边共同治理的业务生态，公有链是由整个社区共同治理的业务生态。

比特币、以太坊、比特股、Ripple 都通过自身社区共治共享的公有链体现了其技术体系对公有链场景的适用性，但也可不加改造或略加改造作为联盟链或私有链部署。据了解，以太坊有推出面向联盟链专用版本的计划，本报告后面章节还会进一步提到。

HyperLedger 目前的设计是以联盟链为出发点，但是其白皮书强调每个模块（包括身份认证和共识算法以及数据库协议等模块）的可插拔性，可以认为也兼顾了今后作为公有链的可能性。Corda 目前已公布的资料较少，但也可以从中清晰看到其非公有链的取向。

在公有链部署的场景下，参与者动态进出且构成复杂，节点无持续开机保证，对共识达成要做最坏情况的考虑，因此这类技术体系不可避免地会在应对这种最坏情况方面消耗过多资源而难以达到更高的性能和效率，但这类技术体系在强安全性保障方面更加值得信任。

在私有链/联盟链的场景下，参与者的资格审查、行为管理和运维义务等在一定程度上可通过链外的其他渠道进行管理和约束，故强安全性可以在某些方面弱化来换取更高的性能和效率。另一方面，在可以允许对共识达成、存储、应急处置、中央对手方、隐私、监管特别通道等方面进行某种带有中心化色彩的特别安排。能够方便实现这类特别安排逻辑的分布式总账技术体系，在场景适用性方面会得到优先考虑。

根据成员目前实际业务状况，技术委员会建议：ChinaLedger 的账本底层协议必须支持联盟链或私有链方式运作，并能方便引入法律法规、业务规则和监管所需要的特别安排。支持非许可的公有链部署的能力可不作为评估和考量的重点，但是从长远看，也不应排除 Chinaledger 支持公有链部署的可能性。

4. 计算能力完备性

作为分布式账本，很多区块链项目都内置了一些脚本语言，可以给用户和开发者一定的自由度。比如，比特币内置的脚本语言可以允许多重签名，或者往区块链中写入一些简短的信息，甚至生成一段谜题，提供正确的输入才可以花掉指定的资金。从解决谜题的意义上讲，将内置的脚本语言用于交易的验证只是数字签名的一个升级版本，但是内置的编程能力，允许区块链在更大的场合发挥作用，比如交易的有条件触发，实现复杂的业务逻辑，或者实现区块链与链内链外系统甚至实物的联动，就需要所谓的智能合约。智能合约给了区块链的应用很大的想象空间，使得很多复杂的商业逻辑有了搬到区块链上的可能性。

无论内置脚本也好，智能合约也好，都是为业务服务的，都是为了表达业务逻辑、方便业务逻辑的落地而存在的。因而，一个分布式总账技术体系对业务逻辑的表达能力和实现业务逻辑的计算能力自然就成为关键。在计算机科学中，衡量一个信息处理装置的能够完成什么样的计算任务、是否足够通用，有一个公认的标准，这就是图灵等价性，或者叫图灵完备性。

简单地说，一台图灵完备的计算装置可以具有一台通用的数字计算机的潜在能力，执行通用的数字计算机能够执行的任何程序。之所以说“潜在”，是因为现实的能力还要受到硬件资源配置的局限。

目前只有以太坊尝试性地实现了智能合约这一功能。比特币的内置脚本表达能力是极为有限的。Ripple 目前不支持智能合约。Bitshares 的智能合约在运用上有很多限制，并不能自定义。HyperLedger 在其框架定义中支持智能合约，在其上的智能合约又名为 ChainCode，设计了安全的运行环境来对智能合约的注册和生命周期进行管理。但 HyperLedger 智能合约功能的实现是在可插拔的底层模块之中，具体依赖于所采用底层模块的计算能力。

由于智能合约本质上是要在验证节点上运行的程序，这必然会消耗验证节点的资源，资源上的限制自然地成为了不可避免的问题。众所周知，图灵机的停机问题是不可判定的，这意味着在提供了图灵完备的脚本语言的分布式总账技术体系当中，有些智能合约在实现时需要消耗的计算资源是事先无法预知的，甚至是无限的。比特币的脚本语言并不图灵完备，从而绕开了所谓的停机问题。以太坊的脚本语言本身是图灵完备的，但是以太坊虚拟机的每个指令都需要消耗 gas 这种资源，而 gas 又和以太坊公有链上的原生货币以太币挂钩，从而必然会在有限时间内完成，通过经济杠杆限制了智能合约的无节制使用。

5. 架构分层合理性

目前，业界对于分布式账本的基础协议栈结构并无统一共识，各技术体系做法不一。无论从快速构建应用角度来说，还是从与分布式账本之外的技术资源整合的角度，甚至从未来占领标准化制高点的角度，架构分层的合理性都是一个应该引起高度关注的议题，架构分层朝着更合理方向的每一次改进，既体现了业界对分布式账本技术架构理解的深化和运营理念的升华，也往往酝酿着新的商业机会。

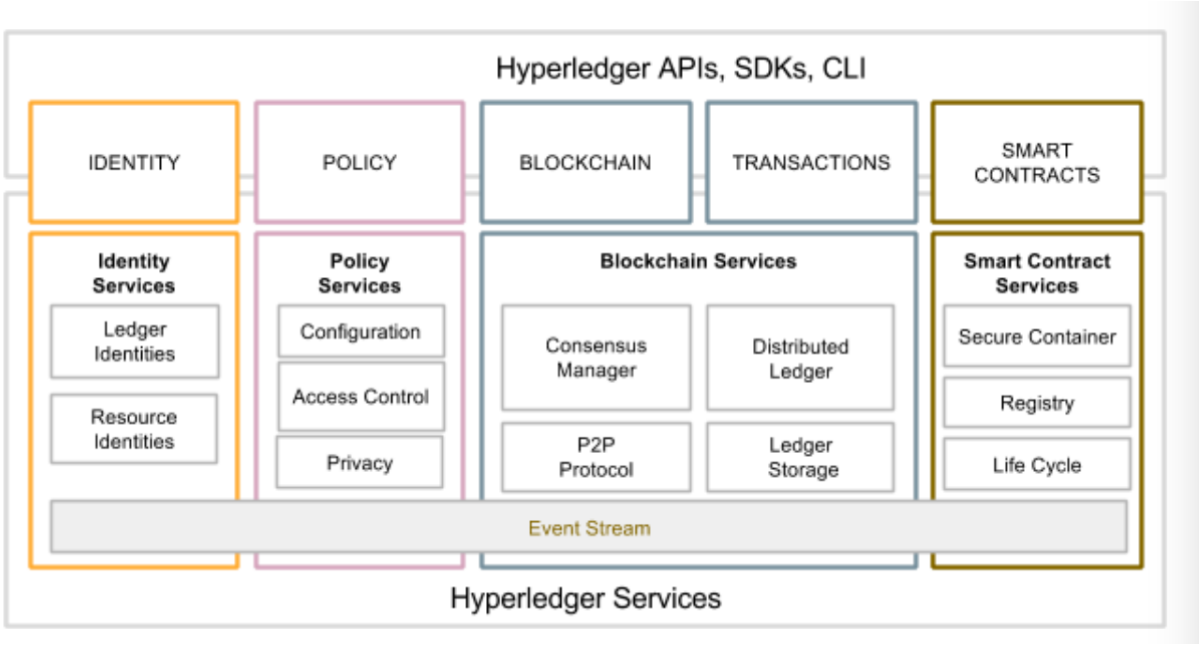
ChinaLedger 期待的分布式账本技术体系的架构，应该体现三类不同性质的节点（记账端、验证端、客户端），五个不同的协议栈层次（网络通信、基础账本、共识、智能合约、应用），四个不同的管理要素（身份、策略、数据、过程）。

对节点进行分层，就是让合适的节点做合适的事情，让共识机制、分片机制等方面的优化措施在架构层面得以施展。比如，在采用 POW 共识机制（见本报告第 6 节）的分布式账本技术体系中，所有的节点都是全功能节点，这样的机制会造成较大的资源浪费和效率损失。增强不同类别节点的差异化配置、分工协作的能力，可以更好地利用计算资源，让处于核心地位的记账端节点得到更好的资源倾斜和安全保护，让处于周边地位的验证端节点轻装上阵，让处于外围地位的客户端做好贴近用户的端到端体验和隐私保护等事情，在全网范围内形成更理想的协同工作阵形。

对协议栈功能进行分层，就是让信息合理流动，让模块间的逻辑关系借助协议栈的层次进行顺畅对接，让合适的模块有机会嵌入合适的环节，做最擅长的事。比如密码学算法包有属地管理等合规方面的限制，市场间对基础账本有沙箱隔离的限制，运行维护和应急管理有对智能合约全生命周期管理的限制等等。所有这些模块的替换、定制，既要合规合法，又要最大限度地避免对整体平台的影响。

对身份、策略、数据、过程四个管理要素进行划分，旨在对分布式总账系统的正常运营提供一个全方位的管理视图，方便对分布式总账进行日常的监控和应急处置。同时，这样的要素划分也提供了分布式总账与链外系统对接的锚点。比如，链外的物联网设备、支付设备、分布式云存储系统、交易系统的对接以及外部用户身份的绑定，都可以通过这几个管理要素与分布式总账技术体系进行受控的互联互通。

下面是引自 HyperLedger 的一张架构图：



以这张图为例，从这张图上，我们看不到节点间分工协同的阵形，也看不见对接外部系统的锚点。其他被考察的分布式账本技术体系也或多或少地存在这样那样的问题和差距，恕不一一举例。ChinaLedger 的参考架构设计还应在广泛借鉴的基础上尽快形成自己的套路。

6. 共识达成机制与效率

工作量证明机制 (Proof of Work, POW)，就是众所周知的挖矿，通过逆向求解一个函数值满足特定约束的哈希函数，计算出一个拼接于有效工作载荷上的随机数特解，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储。POW 的优点是可以达到完全去中心化，节点自由进出。缺点是消耗大量的资源，共识达成的周期较长，不适合商业应用。而且从统计角度上讲是需要 6 个或以上的确认才能认为是明确确认且不可逆。Pow 的网络容错的上限是 50%。典型应用是比特币。

权益证明机制（Proof of Stake, POS）已有很多不同变种，但基本概念是产生区块的难度应该与对应节点在网络里所占的权益（所有权占比）成反比。POS 的优点是在很大程度上缩短了共识达成的时间。它的网络容错上限也是 50%。典型应用是点点币（Peercoin）和未来币（NXT），它们都解决了谁来生产下一个区块的问题。为了达到区块明确确认且不可逆，他们分别需要多于 6 个和 10 个以上的确认。

委托授权的权益证明机制(DPOS)。当使用去中心化自治公司(Decentralized Autonomous Company, DAC) 这一说法时，每个股东按其持股比例拥有影响力。每个股东可以将其投票权授予一名代表。获票数最多的前 N 位代表成为验证者，并按既定时间表轮流产生区块。它的网络容错上限也同样为 50%。典型应用是比特股(Bitshares)。比特股需等待半数以上的验证者确认才认为区块不可逆。

瑞波共识机制(Ripple Consensus)。瑞波共识算法设定了一组特殊节点列表，只有在这个列表中的节点才是有效的验证者。这种机制达成共识的效率非常高，并且只有达成共识的区块才会写入账本。因此写入即有效，无需等待确认的时间。为了达到高可靠性，只有80%的验证者同意交易才算有效，即网络容错上限为 20%。

实用拜占庭容错算法(Practical Byzantine Fault Tolerance)。这个算法可以在异步网络中

不保证活跃度的情况下解决拜占庭将军问题. 虽然该方案不保证活跃度，但它进入无限循环的概率非常低, 在工程中是完全可用的。PBFT 依靠法定多数(quorum)，每个节点一票，少数服从多数，实现了拜占庭容错。PBFT 安全的前提之一是节点是认证过的，适用于联盟链。因为 PBFT 在效率上的优势，PBFT 已经成为了业内普遍认同的方向之一。采用 PBFT 算法的网络容错上限为 33%。

恒星共识协议(Stellar Consensus Protocol)与 PBFT 算法类似。它是基于联邦拜占庭协议(Federated Byzantine Agreement)改进而成，同样解决了拜占庭容错问题。SCP 不要求节点是认证过的，它通过节点自行选择仲裁片区(quorum slice)来达成共识。恒星网络的效率非常高，也采用只有达成共识才写入账本的方法，因此也没有等待确认的时间。网络容错上限同样为 33%。它的性能也可以作为 PBFT 的参考。

以下是选取各共识机制的公链代表项目进行对比分析：

	比特币	未来币	比特股	瑞波币	恒星币
共识机制	POW	POS	DPOS	Ripple	SCP
场景	公有链	公有链 联盟链	公有链 联盟链	联盟链	公有链 联盟链
记账节点	全网	全网	选出 N 个代表	指定特殊节点	动态决定
时间	10 分钟 6 个或以上确认	1 分钟 10 个或以上确认	3 秒左右 N*2/3 个确认	3-6 秒 无须等待确认	3-6 秒 无须等待确认
存储效率	全账本	全账本	全账本	全账本+部分账本	全账本+部分账本
吞吐量 (公网)	约 7 TPS		约 300 TPS 或更高	约 1000 TPS 或更高	约 1000 TPS 或更高
网络容错	50%	50%	50%	20%	33%

表 1：公链代表项目指标

经过对比分析，我们认为 POW 只适用于公有链。基于联盟链我们将适用的共识机制分为两类，一类是与权益证明相关的 POS 和 DPOS，另一类是与权益证明无关的 PBFT、Ripple 和 SCP 等共识。在 POS 和 DPOS 之间，我们认为 DPOS 避免了每个节点都记账，通过选举产生的记账节点也可以拥有更好的硬件，有助于提升整体效率，优于 POS。在另一类当中，PBFT 作为一个成熟已久的可靠的解决方案，也成为联盟链的优先考虑选项。

根据以太坊社区发布的技术报告，2017 年，以太坊的共识机制将转换为代号 Casper 的 Proof Of Stake（权益证明）算法，目前 Casper 算法正处在研发测试中。Casper 带来的好处是可以解决交易的确定性问题，可以降低成本，也可以让轻客户端变得可能。以太坊社区已经在着手应对这一转变可能给以太坊公有链带来的种种挑战。另外在私有链和联盟链领域，Hyperledger 也做了种种旨在提高出块速度的测试。

技术委员会建议 ChinaLedger 底层协议优先考虑支持资产端的联盟链应用。在联盟链场景下，有条件实行某种记账节点和纯验证节点差异化配置的高效共识机制，优先推荐使用 DPOS、PBFT 或它们的变种。另外根据目前 ChinaLedger 成员现有业务对吞吐量和时延的实际需求，在 ChinaLedger 项目初期，为不影响各 POC 项目进度，可暂时采用 POW 机制过渡，

待时机成熟再行替换。

7. 计算与存储效率

要实现分布式账本技术的大规模的应用，计算与存储的开销问题肯定是需要解决关键技术问题之一。以比特币的现有模型为例，由于比特币的每个区块只记录了对整个网络总账的增量流水，为了计算出整个账本的当前状态，仍需拥有整个网络的全部历史。这个特性导致了每个记录和验证交易的节点（即矿工）都要保存一份完整的总账。尽管还存在SPV（简易支付验证）节点可以只存储区块头信息，但是SPV的用途是验证某个支付是否确实存在，以及得到多少个确认等信息。涉及到交易验证时候，是否有足够余额可供支出（不可透支性）、是否存在双花（不可复制性）、脚本能否通过等等，则只能由运行全功能节点的矿工来完成。

在比特币的早期，由于交易稀少，整个区块链并不太大，但是在现在每个区块都接近最大尺寸（1 MB）的情况下，整个区块链的大小将以每年 50GB 左右的速率增加。比特币协议对区块大小的设定是 1MB，——如果按照每笔交易 250 字节来估算，每十分钟只能容纳大约四千笔交易，相当于每秒 7 笔交易。因此，有人提出放宽这一限制。但是，区块链的数据结构和必须保存全部历史的这个要求，又导致存储的开销不断增加——例如，允许每个区块 10 MB, 则区块链每年会增加 500 GB, 但这也仅仅是把平均每秒能处理的交易提高到 70 笔而已。可见，在现有模型下，比特币技术体系的计算效率的提升和存储效率的提升发生目标冲突，导致社区很难抉择。预计扩容之争还将持续一段时间，其走向也可能会决定比特币的命运。

我们再来看看其他体系。在以太坊目前的架构上，每一个节点都需要存储完整账本。自 2015 年 7 月份上线以来，以太坊的区块数据已经超过 10GB。现在的区块数据增长速率约为1GB/月。比特股中的记账节点和普通节点都需保存完整账本。比特股2.0从2015年10月份开始运行，目前区块链数据已经超过2GB。Ripple的账本，与比特币的UTXO模式不同，记录的是全网每个账户的状态。这大大缩小了保存当前状态所需的存储空间，整个总账的大小也最多不过数百MB。一个节点没有全部的历史也能正常工作，这是Ripple和比特币在存储方面最大的区别。但是，如果要保存完整的历史，Ripple所需的空间还是很大的，大约在TB级。超级账本已有的项目Sawtooth Lake与Fabric目前对存储协议并没有强调全新的扩展性方案。V0.1 版本的超级账本白皮书里只是把数据存储设计为可插拔的模块，可以支持不同的存储协议。至于R3则在最近的博客中揭露Corda没有采用全局共享数据：只有在合约范围内的合法参与主体才可见。

由此可见，按照“每个验证交易的节点保存一份整个网络的交易历史”这一简单的模型，显然是很低效且浪费的。不管存储方式怎么变，要保证区块链上的数据可审计、不可篡改的特性，总归需要有部分节点储存全部的交易数据。从根子上解决存储问题的核心在于，如何允许一部分节点在只保存了少量数据的情况下也能验证交易的有效性。解决这个问题有几个思路。

一种方式是定期保存整个网络的状态，以共同的**账本快照**（snapshot）当做整个网络共同认可的状态。这样的话，如需节约空间的节点，可以清空账本快照之前的交易历史，一切以账本快照和之后的区块为准。但是按照这种方式，全量历史记录有可能回退到云化甚至中心化存储，相当于在安全性和去中心化上做出了一定的妥协。这时谁有权发布账本快照，如何避免账本快照的发布出现冲突等，都是要进一步考虑的问题。

另一种方式，即**分片处理** (sharding). 这种方式主要出于解决计算性能问题的考虑，但是也兼顾了缓解存储问题的需要。总体思路是，每个节点只处理一部分（比如一部分账户发起的）交易，从而大大减轻节点的计算和存储负担。但是这种方式也会带来新的问题，比如不同分片间的交易有没有冲突的可能性，如何避免多个交易之间有依赖关系但却落在

不同的分片之中，如何处理依赖于多个其它交易的交易，如何保证数据的一致性和交易的原子性等等，都是新的问题。

第三种方式名为**状态旁路** (State Channels)。这种策略是保持底层的区块链协议不变，通过改变协议用法的方式来解决扩展性问题。在这种策略下，分布式账本上可见的只是粗粒度的“批发”，可以类比出入备付金操作，而真正细粒度的双边或有限多边交易明细，则不作为“交易”记录分布式账本上，而仅仅作为有争议事件发生时备查的“信息”单据，通过状态旁路的方式“曲线”执行。比特币体系下的“闪电网络”是在比特币脚本逻辑表达能力受到限制的情况下不得不借助“精巧”的设计实现的事实上的状态旁路。在以太坊体系下，借助智能合约的丰富表达能力，状态旁路的实现大大简化了。

状态旁路策略可以理解为由如下 3 个步骤组成：

（1）分布式账本的部分状态通过多重签名或者某种智能合约锁定，相当于某个特定集合的参与者各自拿出部分结算备付金放入状态旁路，参与者各自初始占比与分布式账本锁定的数额相一致。

（2）当状态旁路的参与者之间发生双边交易，记录参与者在旁路内各自结算备付金占比新变化的“单据”新版本经旁路上各参与者全体同意并进行多重签名，实现状态更新。

（3）当状态旁路无存续必要时，参与者把状态提交回分布式总账，关闭状态旁路并且再次将状态解锁，相当于按结算备付金的最新分配比例在参与者间进行清算后回到分布式总账。

由于绕开了分布式账本中为了全网检验而加在每笔明细上的巨大开销，同时又在双边或有限多边的范围内继承了相关参与者的余额信息并确保状态旁路内价值守恒，状态旁路策略成为提高分布式账本计算和存储效率的一条有效的捷径。状态旁路还有初步的隐私保护功能。关于隐私保护的更多内容请参看本报告第 8 节。

最后一种方式是记账节点**定向指派**，即在分布式账本上登记了多种资产情形下，由不同资产的发行人为其标的资产定向指派记账节点的机制。其相应模型，既可以指派到具体节点，也可以指派到规则，由符合规则的节点参与该资产的登记结算。这也是针对多资产类的业务的一个值得尝试的方向。

技术委员会建议 Chinaledger 底层协议可优先考虑能够方便实现状态旁路策略的分布式账本技术体系，在其上快速搭建并验证有实际业务背景的、适合双边或有限多边业务场景的概念验证（POC）系统，待条件具备时再做其他计算和存储性能优化方面的探索。

8. 隐私及特权机制

8.1. 隐私机制

目前分布式账本上的交易数据（包括交易内容和发送方，接受方的地址）都是公开可见的，对于某些 ChinaLedger 成员及其业务来说，这种数据的暴露不符合业务规则和监管要求。在分布式账本基础协议的框架内，寻找**既能对交易内容背书、又不让非授权人员（哪怕是背书者）获取交易内容**的技术方案。目前从公开资料中能够查阅到的，有下列三个方案：

零知识证明方案。密码学上对“零知识证明”的定义为：证明者知道问题的答案，通过出示某些信息，可以向验证者证明“他知道答案”这一事实，但是验证者不能通过所出示的信息增加有关答案的任何知识。

例子：证明者和验证者都拿到了一个数独的题目，证明者知道一个解法，他可以采取如下这种零知识证明方法：他找出 81 张纸片，每一张纸片上写上 1 到 9 的一个数字，使得正好有 9 份写有从 1 到 9 的纸片。然后因为他知道答案，他可以把所有的纸片按照解法放在一个 9 乘 9 的方格内，使得满足数独的题目要求（每列、每行、每个九宫格都正好有 1 到 9）。放好之后他把所有的纸片翻转，让没有字的一面朝上。这样验证者没办法看到纸片上的数字。接下来，验证者就验证数独的条件是否满足。比如他选一列，这时证明者就把这一列的纸片收集起来，把顺序任意打乱，然后把纸片翻过来，让验证者看到 1 到 9 的纸片都出现了。整个过程中验证者都无法得知每张纸片的位置，但是却能验证确实是 1 到 9 都出现了。

zk-SNARK 是最新研发出来的零知识证明的一个变种方案，它的全称为 zero-knowledge Succinct Non-interactive ARguments of Knowledge。目前已经有 C++实现的开源软件库。具有以下的特点：

1. 无需证明者与验证者之间进行交互。
2. 验证是简短且简单的。
3. 证明是计算上可靠的。

ZeroCash（开发中，预定 2016 年 9 月份发布）是实现了 zk-SNARK 方案的加密货币项目，可以保护交易的发送方，接收方，交易内容的隐私。

环签名方案。密码学上，“环签名”因为签名由一定的规则组成一个环而得名。在环签名方案中，环中一个成员利用他的私钥和其它成员的公钥进行签名，但却不需要征得其它成员的允许，而验证者只知道签名来自这个环，但不知道谁是真正的签名者。

CryptoNote 是一个应用层协议，实现了环签名方案，基于 CryptoNote 协议的 Monero，Dashcoin 等加密货币实现了对交易发送者的隐私保护。

同态加密方案。所谓同态加密，是一种“保代数运算”的加密形式，它能够保证两个数“先加密后运算”和“先运算后加密”得到相同的结果。这项技术可以使对余额的记加、记减、比较等操作在余额和增量都是密文状态下进行，从而可在加密状态下达到对交易流水的背书和对透支的控制两不误。

MIT 的 Enigma 项目（开发中）运用同态加密方案来保护交易数据的隐私。

以上三种方案，均在开发或者改进性能的进程之中，距离引入成熟的分布式账本体系仍有距离。另外很重要的一点，以上三种方案均严格保证所有的涉隐私计算是在分布式账本的现有协议框架内完成的，也就是说本质上是去中心化的。如果在去中心化这一点上有所妥协，比如允许有一些使用私有数据（如法定中央对手方的私钥）的计算过程在链外完成，那么就可以借助现有成熟的分布式账本技术体系来实现。鉴于私有链/联盟链场景对于去中心化的总体架构在局部基于合理的乃至法定的理由有限度地部分回归中心化的技术方案并不排斥，技术委员会建议：ChinaLedger 可以在密切关注零知识证明、环签名和同态加密方案进展的同时，优先探索链外系统加上现有成熟的分布式账本技术体系的隐私保护实现方案。

8.2. 特权机制

我国现行法律制度赋予司法机关和特定金融机构在金融业务中行使某些职能的特权。比如，业务规则不可以对抗司法冻结；监管机构可以根据工作需要，按程序查看某些涉隐私数据；交易所可以对从事杠杆交易的投资者账户实施强行平仓操作，可以对特定产品进行临时停牌，可以对特定市场实行临时停市等措施；登记结算机构可以对显失公平的交易

结果采取暂缓交收乃至取消交易等措施；等等。在赋予了私钥对操作个人资产独一无二许可作用的各分布式账本技术体系及其基础协议当中，在根据上一小节提到的某项技术对隐私实施了普遍保护措施的前提下，如何为特定有权机构行使特权职能提供技术上的方便而又不引起安全上的问题，是分布式总账技术走进金融“主战场”所必须解决的问题。目前，除 Corda 之外的其他几个分布式总账技术体系中均未见到相关的任何内容。日前以太坊公有链受到针对智能合约 DAO 的攻击，无论是暂停交易、交易回滚还是取消交易，这些在传统金融机构非常经典的应急手段，在以太坊体系内都无法实施，而只能去讨论软分叉还是硬分叉。社区无政府主义势力的阻碍是一方面，其技术体系及基础协议中没有提供相应的功能也是一个重要原因。

技术委员会建议，ChinaLedger 引入特权机制可从三个方面入手：

（1）**引入特权账号对智能合约的“刹车”机制**。研究引入特权账号对智能合约“刹车”机制的可行性，探索制作 ChinaLedger 智能合约标准模板，在标准模板中，由特权账号签发的“刹车”消息可令智能合约停止执行，进入与 gas 耗尽类似的状态。

（2）**引入特权账号对私密信息的“看穿”机制**。在探索隐私保护解决方案的同时，同步考虑特权账号的“例外”机制，探讨在上一小节推荐的链外解决方案基础上，借助中央对手方账户，建立与链内密文总账相平行的链外明文总账的可行性。

（3）**引入特权账号对状态旁路的“救急”机制**。研究引入在状态旁路中接收并执行由特权账户单独签发的应急操作单据的可行性，探索将交易回滚、交易取消、强行平仓、司法冻结等操作通过应急操作单据发送到状态旁路执行的可行性。在实验成功的前提下，探索制作状态旁路标准模板，将允许特权账号进行应急操作并接受其后果的承诺变成实现状态旁路智能合约的要件。

8.3. 沙箱（sandbox）机制

一般来说，联盟体制下的分布式总账共享可以分为三个层面：

（1）代码共享，各联盟成员各自部署；

（2）账本部分共享，各联盟成员对于账本中的共享数据可以看到明文，但是对于非共享数据只能看到密文；

（3）账本完全共享，各联盟成员可以看到账本中的全部数据。

在上述第 2 种情形下，每个联盟成员及其用户在共享数据基础上形成一个个“沙箱”，“沙箱”内的数据对其他联盟成员全是密文。基础账本的运营方则为各联盟成员提供“数据背靠背”的云服务，由于不掌握相关密钥，所有非共享数据对于运营方来说都是密文。

鉴于不排除一些 ChinaLedger 成员有可能有以上述（2）的方式实现账本部分共享的需求，技术委员会建议，如果第 8.1 节推荐的隐私保护解决方案是可行的，则探索进一步将其扩大为沙箱机制的技术方案。

技术委员会建议，本节 8.1-8.3 各节所推荐的、在其他分布式总账技术体系内尚无先例的技术方案，以尽量利用原有分布式账本基础协议为原则，如非确实必要，尽量不对基础协议进行改动；如必须改动，在改动前要审慎做好详细技术方案的专题评估。

9. 原生虚拟货币的意义与必要性

目前几乎所有的分布式账本技术体系里都有原生的加密货币。这些加密货币具有的共

同特点都是没有中心化的发行方，可以在其对应部署的公有链上自由流转。这些原生货币具有以下几点重要用途：

支付手段：当虚拟货币具有价值，就可以用来支付。在支付领域最明显的就是比特币，其本身就是为此而发明。

汇兑手段：Ripple 将其原生虚拟货币瑞波币（XRP）变为了跨国中介货币。比如 XRP/CNY 和 XRP/USD 的两个市场可以桥接成为 USD/CNY 的市场。如果各个国家的网关都使用本国的法币和瑞波币做市，那就无需再与其它国家的法币进行两两做市了。

抵押手段：将原生虚拟货币作为抵押品是比特股 BitShares 的一大特色。在比特股中可以发行价格锚定资产如 bitCNY 和 bitUSD。这些资产需用价值 2 倍的 BTS 抵押生成的，因此可以规避发行人的信用风险。

激励手段：无论是工作量证明机制 POW 还是权益证明机制 POS，原生虚拟货币都是通过俗称的“挖矿”产生，作为给这些成功记账的节点的奖励。对于公有链，原生虚拟货币的激励可以吸引更多的人加入记账，从而使网络更安全。比特股除了记账的激励外，还有对开发新功能的人的激励。通过适当的增发规则，新产生的原生虚拟货币就用来充当开发新功能的费用。当然，对于某些预分配原生虚拟货币的网络，比如 Ripple，所有的原生虚拟货币在网络运行之初就已经生成完毕，因此并没有针对记账的激励。其记账是由属于一个特殊节列表的节点组完成的。

权益证明：在这种情况下，原生虚拟货币相当于网络里所占的股权（所有权），你拥有的数量越多，你的权益就越高。采用 POS 机制的网络里，产生区块的难度与所占股权成反比。在 DPOS 中，用户还可将自己的权益委托给代表。比如比特股 BitShares 由得票最多的 N 个代表（比特股内负责这一任务的代表称为见证人）进行记账。此外，用投票的方式还能实现包含出块时间、网络运营预算等参数在内的网络参数的调整。

资源控制：分布式总账特别是其中的智能合约如被不受限制地使用，基于图灵机停机问题的不可解性，借助智能合约的恶意 DDoS 攻击和对区块链资源的无节制滥用一定会导致资源灾难。针对资源的使用收取一定数量的原生虚拟货币作为经济调节手段，可以防止攻击、制裁滥用。比如为了防止生成大量垃圾账号，可以设置激活费用；对于转账、交易收取交易费用；对于未成交的委托单，冻结相应数量代币等等。一般而言还会设置一个网络费用的动态算法，当网络越繁忙时，收取的费用也越高。

随着一套分布式总账技术体系从公有链平移到私有链/联盟链场景，前面说的关于原生虚拟货币的很多”重要意义”会变得无关紧要，一些功能会被锚定法币的代币所取代，以至于出现了一些要求在私有链/联盟链中取消原生货币机制的呼声。ChinaLedger 迟早也必然会面临这一问题。

通过以上分析，可以发现，“权益证明”和“资源控制”这两个职能，即使到了私有链/联盟链场景，仍然有存在的必要性。因此，技术委员会认为，有两种不同的思路来处理原生虚拟货币：一是将原生虚拟货币机制当作一种单纯的计量和调节工具予以保留，让其正常发挥“权益证明”和“资源控制”这两个职能，再择机去除与这两项职能无关的程序代码；二是取消原生虚拟货币，另外构建一个新的机制来实现“权益证明”和“资源控制”职能。

10. 开发与运维支持

10.1. 可升级性与升级路径

据不完全统计，比特币的核心代码库 release 了 157 次。以太坊的 Go 语言核心代码库

已经 release 了 87 次。Ripple 的核心代码库已经 release 了 55 次。比特股升级到 2.0 时区块链数据需要从头开始构建，比特股 2.0 的核心代码库目前已经 release 了 54 次。超级账本的项目 Fabric 与 Sawtooth Lake 都各自 release 了 1 次。

除了超级账本以外，其他的主流区块链技术都成功升级了多次。因为区块链网络的升级需要得到大多数节点的主动更新，所以区块链网络升级完成的准确时间很难预测。

ChinaLedger 如果选取了一个分布式总账技术体系作为“底本”，独立发展后的升级与其“底本”的后续发展是什么关系，比较耐人寻味。技术委员会建议的基调是：（1）立足金融主战场、立足中国国情；（2）如非特别必要，不改底层协议；（3）底层协议的修改如有一定的普遍意义，一定回馈社区。

虽然绝大多数升级都是平稳的，但公有链的分叉也有导致社区决策艰难的场景，比如 DAO 被攻击后的善后处置和平台升级。如果能够引入 8.2 小节所说的特权机制，会大大分流升级的压力，把升级工作做得更加安全有序。

值得指出的是，智能合约是契约但更是程序，是程序就难免会有升级问题。如何处理智能合约的升级，如何保证智能合约的状态和逻辑在升级前后有序衔接，如何保证智能合约的升级和平台的升级相得益彰而不是互相掣肘，也是全世界面对的艰难挑战。

技术委员会建议，ChinaLedger 要积极探讨智能合约的升级机制，但初期尽量避免导致智能合约升级的情形发生。数据修复尽量不要采用系统分叉的方式去做。

10.2. 编程语言、开发工具与环境

比特币、Ripple、比特股的核心代码主要由 C++编写。

HyperLedger 的 Fabric 项目核心代码主要由 Go 编写。

HyperLedger 的 Sawtooth Lake 项目核心代码主要由 Python 编写。

以太坊的黄皮书是对以太坊的形式规范描述（formal specification），即用计算机科学的形式语言来描述的以太坊系统的规范。参照黄皮书的规范可以用各种编程语言实现客户端。目前以太坊有经过大量安全审计的 Go 语言, C++语言和 Python 语言实现的 3 个客户端，另有 Java 和 Ruby 的客户端也在开发中。

既然利用现有技术进行开发，当然需要考虑现有的开发工具与环境。

基本上建议在 Linux 或者 OS X 的环境下进行开发。

比特币是历史最久，社区最为庞大的项目。github 上有公钥转换地址、区块数据浏览等大量开源的工具，中英文技术文档十分丰富。

以太坊的社区仅次于比特币社区，主要英文技术文档都在 github 上，也有专门的技术问答网站。中文技术文档则主要在 ethfans.org 网站。由社区贡献的有的网络监控，分布式应用（Dapp）的开发框架，智能合约分析器，智能合约管理平台等工具。微软提供的 Visual Studio 集成开发环境集成了 solidity 语言，方便编写智能合约。

Ripple 的网站上有开发人员中心，文档丰富，在 github 上的开源工具包括网络数据仪表盘，共识模拟器等。

比特股的技术信息在主页以及 github 上，有提供开源的网页钱包。

超级账本处于开发早期，在 github 上有 Fabric 与 Sawtooth Lake2 个项目的源码。wiki 内容繁多，但是尚未整理且修改较频繁。

技术委员会建议：一旦 ChinaLedger 选定了“底本”，在编程语言、开发调试工具与环境等方面就一定要尽量向底本靠拢，没有充分的技术理由，不要在这些方面另搞一套。这不仅可以少走弯路、多复用社区已有成果，而且可以在人才培养方面借得先机。

11. 未来发展潜力和动向

Bitcoin（比特币）诞生至今已经历了 7 年多的稳健运行，形成了完整的生态系统，有庞大的社区和技术力量雄厚的核心开发团队。可以预见，比特币社区未来还将在某些方面为区块链技术贡献出重要的思想。例如，即将正式发布的比特币闪电网络就为区块链所面临的吞吐量、确认时延、隐私保护等技术问题提供了创造性的思路。如今，比特币技术体系正在新的升级计划引领下寻求新的突破。尽管其典型公有链、单一标的资产以及 POW 共识机制等特质决定了在金融领域获得广泛应用有很大难度，我们还是希望看到新的升级计划给比特币技术体系带来新的跨越。

Ethereum（以太坊）支持图灵完备的智能合约，且创建了用户友好的脚本语言。在发布不到 1 年的时间内，以太坊的平台上已有 200 多个应用程序在开发或者运行中。目前，以太坊已经形成了以其创始人 Vitalik Buterin 为核心的开发团队，以及遍布全球的开发者社区。同时，以太坊还制订了清晰的进一步开发的路线图，具体包括：2016 年秋季发布浏览器；2017 年初发布“以太坊 1.5 版“，在该版中将共识机制改为 POS；2017 年中发布“以太坊 1.75 版“，在该版中将实现更快的虚拟机；2017 年末发布“以太坊 2.0“，初步增强可扩展性；2018 年末发布“以太坊 3.0“，最终实现无限制的可扩展性。此外，以太坊还在积极探索满足金融行业需求的各种技术路径，这些探索涉及隐私保护、吞吐量以及功能更强且更加可靠的智能合约等方面。从发展趋势来看，以太坊本来在拥抱金融主战场的需求方面处于非常积极的态势，不过 DAO 事件还是让世人清醒地看到了“草根”与“主战场”的理念融合依然任重道远，尽管这并不是以太坊基础账本和虚拟机的问题，但至少表明与“智能合约”这个新鲜事物相互配套、携手而行的生态要素培育绝非一日之功。

Ripple（瑞波）并非是由社区自行开发维护的，而是由接受了风险投资的商业机构 Ripple Inc.运营管理，因而其发展路径更多地受到单一控制主体的影响。现阶段 Ripple 公司主要致力于跟银行合作，解决汇兑类问题，而对更全面的应用于金融领域所必须考虑的隐私保护、可扩展性、合规性等问题尚未有明确的解决思路和研究计划。

Bitshares（比特股）没有形成长期、稳定的核心开发团队，其创始人 BM（Daniel Larimer）亦于 2016 年 4 月表示，他将逐步淡出比特股的开发。因此，比特股未来的发展前景并不明朗。

Corda 和 HyperLedger 分别由两家商业机构发起组建，联盟成员主要来自金融领域，将聚焦于分布式总账技术在金融行业的运用。从已披露的信息来看，两个联盟均提出了一些有创意的设想，后续能否以及如何实现这些设想是 Corda 和 HyperLedger 发展的关键。

HyperLedger 是一个支持智能合约的、底层可插拔的通用协议框架，其上项目多有很强的金融背景，包容性相对较强，又有很多金融领域传统服务商参与加盟，组件模块的不断丰富是毋庸置疑的。2016 年 5 月 19 日，Hyperledger 发布了第一版白皮书，版本号：V0.1。这版白皮书中设计的协议非常的通用，并未聚集于任何一个具体的行业或者业务场景。在区块链技术目前不成熟的状态下，超级账本项目将可扩展性（模块化），可交互性（不同区块链之间的信息交换），内部组件的可移植性作为设计的需求。另外白皮书提出的要求包括交易数据的隐秘性与合约的机密性，身份认证与可审计行，这也是符合联盟链的实际需要的。BlockStream，Digital Asset Holdings，IBM，英特尔等公司都已经各自提交了框架提案，比如 BlockStream 提供的框架是基于比特币的核心代码，其它的公司也提供了独创的框架，共识机制也各不相同。决定超级账本架构的工作组成员来自各行各业的大型机构和企业，从这版白皮书中也能看出互相妥协的成分在其中。超级账本处于第一版白皮书刚发布

的阶段，随着项目的发展，白皮书如何改进，各个公司独自提出的框架是否会整合，如何整合，如何平衡联盟内各大公司的要求，其提出的通用开放标准是否会被大多数国际金融机构采用，其协议框架和底层平台的走向如何演化，还是有很多让人看不清之处。

本报告很少评论 Corda，因为 Corda 至今为止对外公司发表的文字材料少之又少，其当事人对外表态也是慎之又慎。但从已披露的信息看，Corda 的技术体系较之前述各分布式账本体系有很大的不同，其关注的重点是打造一个企业间记录和管理合约的工具，乃至于有人认为它“不是区块链”。然而，Corda 对数据的隐私性、合规性和监管需求的考虑明显更接近金融业务主战场的视角。Corda 的定位适合于联盟链。它和区块链的共性有：共识(Consensus)、有效性(Validity)、唯一性(Uniqueness)、不可更改和可认证性(Immutability and Authentication)。在保持这五点的共性的同时，也保护数据的稳私。最终达到使联盟成员减少成本、减少交易错误、提升结算速度的目标。从以上这些方面看，Corda 与传统金融 IT 平台从理念到特性都是最接近的，不排除他们会走一条与众不同、直达金融业务本质的道路。

12. 思考与结论

根据以上分析评估，我们可得出如下初步结论：

（1）共识达成效率、计算和存储效率、隐私机制、特权机制、沙箱机制以及与链外系统的对接，同金融主战场的核心需求和中国金融监管特色需求关系密切，是 ChinaLedger 在设计阶段就必须严肃对待的关键技术问题，也是全球分布式账本技术的实践者们都在关注的共性问题。技术委员会建议 ChinaLedger 在这些方面应该有所作为，体现后发优势。

（2）从现有功能的完备性、成长性和对业务场景的综合支持潜力角度看，技术委员会初步的判断是：以太坊技术体系作为 ChinaLedger 的“底本”可能是比较合适的，但对其原生货币，除了权益证明和资源控制机制要予以保留，其余可封存不用，择机去除；对已有的将以太坊改造成联盟链的最佳实践要尽量采纳；未来与以太坊技术体系的分叉不要走得太远，既方便分享社区新成果，也方便将 ChinaLedger 的成果回馈社区。以太坊将来会支持更加灵活、更加多元化的个性化配置，共识机制、特权机制等都可以作为模块配置添加到系统架构里。这样以太坊不仅在合约层，而且在基础账本层都可以给 ChinaLedger 以支持。

（3）超级账本和 Corda 在贴近业务需求、满足合规和监管要求方面的尝试，值得 ChinaLedger 很好地学习和借鉴。

本报告是 ChinaLedger 成立后短短两个多月里形成的阶段性成果，不代表 ChinaLedger 对相关问题的最终看法，但我们期望其会对 ChinaLedger 的最终决策有所帮助。