面向中国资本市场应用的

分布式总账白皮书

ChinaLedger

2016 年 10 月

1. 前言

近年来，金融领域的技术创新不断涌现，以金融科技（FinTech）为代表的一系列影响深远的技术创新，正在改变着金融服务业的业态。其中，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，依托民间数字货币的各类创新性应用方兴未艾；“主战场”上的各类传统金融机构关于分布式总账技术的各类高质量的研究、有意义的探索和尝试越来越密集，力度也越来越大；金融监管机构和 IT 产业政策管理机构也对这项技术给予了高度关注。

与分布式总账概念密切关联的另一个概念是区块链（Block Chain）。一般认为，区块链是一种典型的分布式总账，在其上可以以多边共治的方式，靠密码学原理的保证来不可更改地记录价值的产生和转移行为，以可编程的方式实现与价值有关的业务逻辑，当然更一般意义下的区块链还可以可靠地记录价值以外的其他信用状态并实现相应的业务逻辑。我们也注意到另外一种观点，即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。在本白皮书中，尽管我们提出的框架性方案基本上还是落在区块链范畴之内，但我们将主要使用“分布式总账”这一提法。

“中国分布式总账基础协议联盟”（简称 ChinaLedger）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。与“互操作型的”联盟组织不同，ChinaLedger 成员机构间基本上不存在横向的互操作关系，更多地是统一维护一套共享的共性基础平台、各自基于平台建设自身应用系统的“资源共享型的”联盟组织。

ChinaLedger 成立以来，组织成员单位系统交流了中国资本市场的法律与监管环境、典型业务场景的功能需求和分布式总账技术应用的推进顺序，认真评估了建设 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，广泛参考了海外推进分布式总账技术在资本市场应用的最佳实践。在此基础上，制定此白皮书，作为推进 ChinaLedger 下一步工作的纲领和依据。

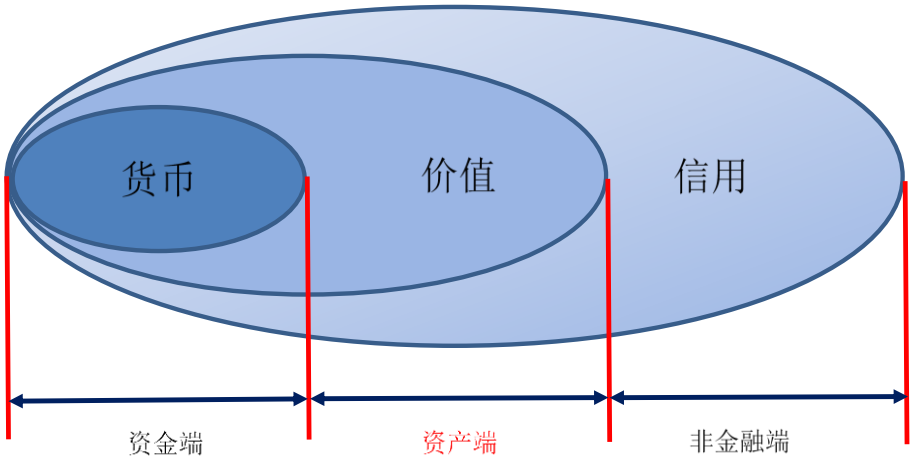
2. 业务需求与推进顺序

本节聚焦中国资本市场，考察在“资产端”引入分布式总账技术的必要性、

可行性和先后顺序问题。

2.1 “资产端”的具体范围

分布式总账技术最初发源于数字货币领域，但目前已可提供货币服务、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。



具体到“资产端”，其外延包括一切具有价值属性的非货币的财产，大致分成四类：

（1） 有价证券类：股票、债券、基金、期货、期权、资产证券化产品、结构化理财产品、非标私募产品等；

（2） 大宗资产类：土地（地契）、房屋（房契）、大宗商品（仓单）、贵重奢侈品、艺术品等；

（3） 权益类：矿业权、碳排放权、数字版权等；

（4） 积分类：各种奖励积分、折扣抵用券等。

其中，（2）-（4）类业务基本上属于“场外业务”，（1）类业务中，既有适合“场内”开展的竞价类业务，也有适合“场外”开展的报价类业务。交易所、外汇交易中心的固定收益类产品和仓单类产品，中证协下属的机构间报价平台和各地的区域性股权交易市场均属于“场外业务”。

一般来说，“场内业务”在交易环节涉及到比较复杂的时序逻辑关系和匿名

的交易对手方，在清算环节涉及中央对手方净额担保交收制度，还涉及到复杂的即时行情披露，流动性好，对实时性能和系统可用性要求高，对交易差错的纠正比较困难，因此对全局性风险的容忍度极低。特别是，“场内业务”各类职能角色已通过法律、部门规章和业务规则等形式确定了相应的特许经营主体（例如：交易场所、登记结算机构、市场经营机构等），除非修法，否则此类职能角色几无可能发生变化。

相对而言，“场外业务”在交易环节大体上具有相对简单的时序逻辑关系，交易对手方是相对实名的，在清算环节往往采用非担保交收制度，流动性较差，交易相对离散因而对实时性能要求不高，对交易差错的纠正相对容易，因此相对于场内业务而言对全局性风险的容忍度较高。场外业务各类职能角色的定义层级相对较低，对其进行变动涉及到的流程相对简单。

在中国，从事场外业务的机构大都使用自建的技术平台。相对于平台的实际业务负载而言，平台的开发、维护、运行成本因必要的冗余配置而在全局看略显重复，跨机构的平台整合虽然从经济上是合理的，但所涉及的机构间面临信任基础不足的问题。新设立的从事场外业务的机构在平台的技术路线选型上也面临是否选择“云服务”和“分布式总账”的问题。

2.2 业务功能

基于分布式账本开展“资产端”业务，大约有如下几类功能：

2.2.1 发行

这是价值通过非挖矿的形式从无到有、从聚到散的过程，可能有两种形态：一种是确权发生在链下，当确权完成时将相应资产份额转到链上登记托管。这种业务类型相对简单，除资产份额数据外，登记托管职能机构对确权相关的电子文档资料的数字签名也应放到链上备查。另一种是确权本身通过链上“认购”智能合约的业务逻辑执行过程产生，本身就是分布式应用的一部分。这种业务类型较为复杂，在中国资本市场的场内业务中经常见到。如果不仅认购份额、连“发行价”也要以“众人参与、众人见证”的可编程的方式确定，相应的智能合约将更为复杂，目前中国资本市场无论场内还是场外都还没有先例。

发行后的资产总份额一般情况是守恒的，但在分红派息、配股等场合，资产也会发生并非由交易/转让导致的变动（公司行为）。这些公司行为也属于“发行”的一部分。

ChinaLedger 应能支持通过智能合约在链上“认购”的发行方式，支持发行后通过公司行为引起的资产变动。

2.2.2 交易/转让

交易涉及资金和资产的双向流动。目前做法有二：

（1）资金在链下、资产在链上，资金通过分布式总账平台与资金系统之间的“支付网关”进行。在真正的支付发生之前，资金通过链上开设的“虚拟头寸”进行记账管理。

（2）资金、资产都在链上，交易即支付。

无论哪种情况，必然涉及到分布式总账对交易完整性的管理，也就是说，一笔交易要么资金、资产之间的双向流动均已完成，要么均未完成，不应出现一方完成、另一方未完成的情形发生。

普通的资产交易不允许“买空”和“卖空”。在分布式总账中，这涉及有关透支控制的余额检验。

除非明确规定交易信息公开，否则交易信息是交易双方隐私的一部分，分布式总账中应避免除交易双方之外的普通账户看到或容易推测出这类隐私数据。

场内交易的主要形式是连续竞价。连续竞价的时序逻辑是“订单驱动、价格优先、时间优先”。场外交易的主要形式是“报价驱动、双边报价、点击成交”。部分产品具有远期的反向操作，比如股权/债券的“质押式回购”。

ChinaLedger 应能同时支持资金和资产在链上双向流动，支持交易完整性，支持买空卖空控制，支持交易数据的隐私保护。ChinaLedger 应优先支持报价驱动的场外交易模式，之后酌情考虑支持订单驱动的场内交易模式以及“回购”模式。

2.2.3 结算

直接使用基础账本记账的场合，交易即结算。

使用智能合约处理交易的场合，可在智能合约内部完成净额轧差，在回到基础账本的环节实施交收。

在使用分布式总账平台仅处理场内交易业务的交易后环节的场合，交易信息需依赖一个前置于分布式总账平台的消息基础设施（待建设）来汇集，由分布式

总账平台在基础账本或智能合约的层面来完成相应的清算和结算动作。

如果担任“中央对手方”的职能机构由法律明确规定，分布式总账平台不应改变这一职能。

ChinaLedger 将优先考虑实时使用智能合约进行净额轧差、在回到基础账本的环节批量实施交收的业务模式。

2.2.4 交割/行权

数字权益的行权可直接在基础账本上执行过户。

实物权益的交割一般在线下执行，但使用分布式账本技术可以依据业务逻辑直接变动权益凭证（如电子仓单）的权限状态，提高线下执行的安全性和自动化水平。

ChinaLedger 将支持使用分布式账本平台进行数字权益的行权，为实物权益的交割提供更好的保障。

2.3 监管功能

中国资本市场的法律、法规、行政规章和业务规则赋予各类带有监管功能的主体各自依法合规行使监管职能以及特定的操作特权。比如：

司法部门有依法冻结指定账户交易的特权。

监管部门有依法“看穿”所有账户的开户、交易、持有数据的特权。

交易所有依法对特定交易产品实施“停牌”、对特定市场实施“停市”、对显失公平的交易予以取消、对达到特定风控警戒标准的仓位予以强行平仓、强行减仓的特权。

登记结算机构有依法对特定的已达成交易实行暂缓交收或拒绝交收的特权。

目前尚未看到有分布式账本平台完整支持这一系列含有明确“中心化”特征的特权。ChinaLedger 将支持这些特权在分布式账本平台上“落地”。

2.4 推进顺序

根据对中国资本市场各类不同交易结算机制的法律定位和业务特点的分析，结合它们在分布式总账平台上落地的技术难度，ChinaLedger 建议中国资本市场

的分布式总账应用按如下顺序来推进：

（1）**场外业务**。场外业务是与分布式总账业务场景契合度最高的业务，也是法律监管环境最容易随着技术进步调整适应的业务。对于已经存在的场外市场，可以尝试在单市场利用分布式账本技术去单独支持个别新推出的业务，也可以联合多市场利用分布式账本技术进行云化整合，在云化整合的场景下要注意技术上保障市场间交易信息的有效隔离。对于正在筹建的场外市场，则建议直接把业务建立在分布式账本技术之上。

（2）**场内业务的交易后业务处理**。这是资本市场最核心的业务之一，目前各相关机构（证券公司、交易所、登记结算公司）花在交易后清算结算和对账处理上的时间很长，采用分布式总账技术可以大大缩短这一时间，同时也为相关机构节约大量 IT 开支。

（3）**业务沙箱**。在指定的资本市场业务“特区”内，封闭运行由分布式账本技术支持的场内业务，在鼓励技术创新的同时，审慎观察市场表现，严格控制风险范围，使之不会扩散。

（4）**国际化业务**。随着世界各国对分布式总账技术认知的不断加深和应用的不断推进，中国的资本市场在今后的对外开放中一旦与境外资本市场对接，使用分布式总账技术促进对接将成为一个可能的选项。

上述推进顺序还与央行数字货币工作推进进度密切相关。如果央行数字货币工作提速，可能会进行一些局部调整。

3. 技术选型评估

为满足前述业务需求，ChinaLedger 对目前世界上有影响的六大分布式账本技术体系（比特币、Ripple、比特股、以太坊、HyperLedger 和 Corda）进行了深入的考察和评估。需要指出的是，其中前四个技术体系是平台、货币、社区三位一体的，后两个技术平台是“纯平台的”，但我们的评估仅针对平台，不涉及货币和社区。

考察评估的维度涉及领域适用性、场景适用性、计算能力完备性、架构分层合理性、共识达成机制与效率、计算与存储的效率、隐私与特权机制、原生货币的作用和必要性、技术与运营支持、未来发展潜力与动向十个方面。

3.1 领域适用性

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。

3.2 场景适用性

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”。私有链是单边治理的业务生态，联盟链是多边共同治理的业务生态，公有链是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，鉴于公有链社区人员组成的复杂性和博弈的高度对抗性，能够在公有链环境下生存下来的分布式总账技术平台，在安全上是经得起考验的，不加改造或略加改造作为联盟链或私有链部署也具有可行性。

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，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。

3.3 计算能力完备性

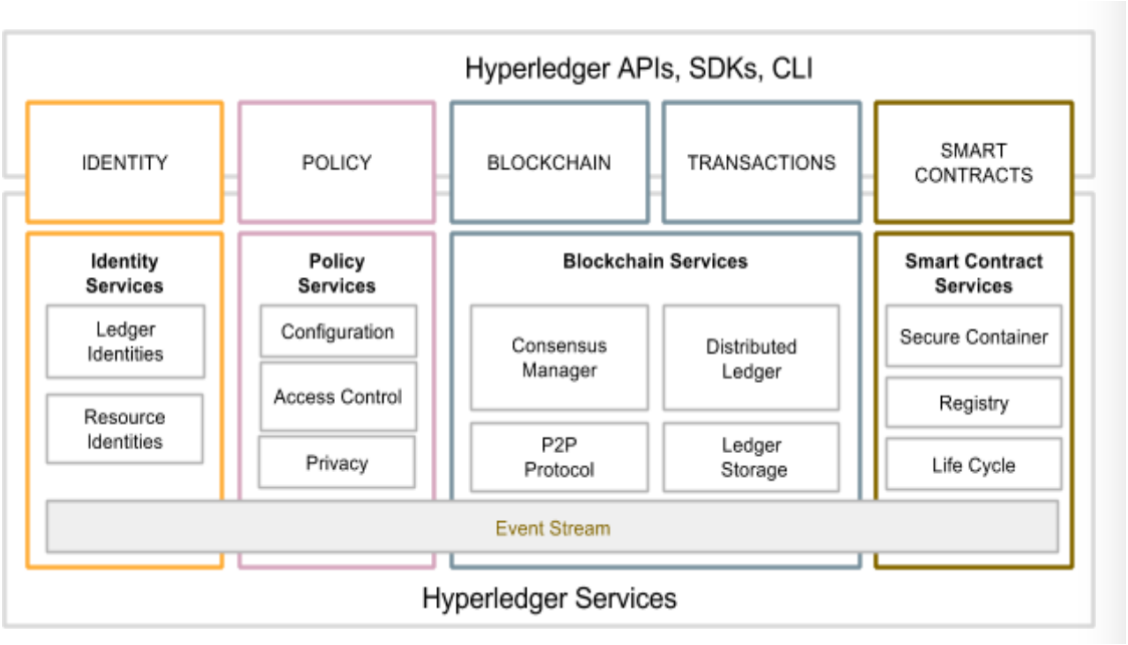
价值可编程是分布式总账技术的一个重要的本质属性，直接决定平台对业务逻辑的表达能力，具体体现在“智能合约”上面。比特币的内置脚本表达能力是极为有限的。Ripple 目前不支持智能合约。Bitshares 的智能合约在运用上有很多限制，并不能自定义。以太坊和 HyperLedger 支持智能合约且达到“图灵完备”程度。

3.4 架构分层合理性

目前，业界对于分布式总账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来看，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）。从长远来讲，有些共性技术（如 P2P 通信和执行智能合约的虚拟机环境）或许应该交给更合适的主体来做。从现实情况看，六大体系中，Hyperledger 的架构分层显示出更多的包容性和更大的弹性，其各组成模块有灵活的可插拔性，便于支持各种法律和监管环境下分布式账本技术的落地，各模块间的相互关系也较为合理。该架构的优点值得 ChinaLedger 吸取。

Hyperledger 的架构总体布局由下图所示：



3.5 共识达成机制与效率

目前可供选择的共识达成机制有工作量证明机制、权益证明机制、委托授权的权益证明机制、Ripple 共识机制和实用拜占庭容错机制等。

工作量证明机制 (Proof of Work, 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，不适合在资本市场的“主战场”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。其网络容错的上限是 50%。典型应用是比特币和以太坊。

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）。以太坊计划在未来使用的 POS 算法叫 Casper，验证人数最多 250 人，并且区块一旦达到最终状态（final）就完全不可伪造。

委托授权的权益证明机制 (DPOS)。它其实是 POS 的变种，由全部节点记账变为选出代表节点记账。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。采用 PBFT 算法的网络容错上限为 33%。在私有链/联盟链的部署方式下，实用拜占庭容错算法（PBFT）具有较大潜力。

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 通过节点自行选择仲裁片区(quorum slice)来达成共识，增减节点非常灵活。网络效率也很高，也采用只有达成共识才写账本的方法，因此也没有等待确认的时间。它的网络容错上限同样为 33%。其性能也可以作为 PBFT 的参考。

3.6 计算与存储效率

目前运行着平台+货币+社区三位一体的公有链上，我们所观察到的计算与存储效率受到很多因素的制约，而且计算与存储之间存在目标冲突，并非技术上完全不能实现更高的效率，所以参照意义并不是很大。

要实现分布式账本技术的大规模的应用，在计算与存储方面做进一步的性能优化是不可避免的。目前可选择的技术方案有：

一种方式是以定期保存的**账本快照**（snapshot）当做整个网络共同认可的状态。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，这在公有链上是相当于在安全性和去中心化上做出了一定的妥协。我们也可考虑以诸如 IPFS 等分布式文件存储方案来降低中心化存储的风险。

另一种方式是**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，如在复杂时序逻辑下数据的一致性、交易的原子性和交易的相互依赖对性能的影响等。

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”记录在分布式账本上，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。

三种优化思路并不是彼此排斥的，可以组合使用。

3.7 隐私及特权机制

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，对于中国资本市场业务来说，这种数据的暴露往往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**的技术方案是非常重要的。

目前从公开资料中能够查阅到的较为彻底的、既适合公有链又适合私有链和联盟链的密码学解决方案有零知识证明、环签名和同态加密三种技术可供选择，相应的技术实现虽已接近可用水平但与实际需要尚有差距。

作为临时性的解决方案，有人建议使用“状态旁路”。用状态旁路提供隐私服务，其前提是所有用户均按同样的脚本使用智能合约。如果有用户故意使用恶意的智能合约，就有可能把在正确的智能合约内存中解密的明文交易信息泄露出去。因此，状态旁路只适合于双边或有限多边的场景，不适合大量用户同时使用。

特权机制是一个全新的问题。以太坊公有链受到 The DAO 被攻击事件的影响至今仍在持续，类似事件如果出现在资本市场“主战场”上是不堪设想的。但评估过程中，我们没有发现所考察的技术体系在这一问题上有可供选择的解决思路。

3.8 原生数字货币的意义与必要性

目前几乎所有部署在公有链上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。这些原生货币的用途包括：支付手段、汇兑手段、抵押手段、激励手段、权益证明和资源控制等。

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，前面所

说的关于原生虚拟货币的很多用途会被消解，一部分功能会被锚定法币的代币所取代，因此在私有链/联盟链的建设过程中，“去币化”已成为一道标配的工序。但是，“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。原生数字货币或许仍不失为在私有链/联盟链场景下履行这两个职能的一种单纯的计量和调节工具。

3.9 开发与技术支持

据不完全统计，比特币的核心代码库、以太坊的 Go 语言核心代码库、Ripple 的核心代码库、比特股 2.0 的核心代码库等均已进行了多次升级，超级账本的项目 Fabric 与 Sawtooth Lake 都各自进行过升级。应该说这些平台的核心代码都积累了大量的在线升级经验。

相比之下，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。

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。

除 Corda 之外，其他平台都是开源项目，项目文档比较丰富。但最近 Corda 发布了非技术白皮书，使业界对其理念和技术路线有了较多的了解。

3.10 未来发展潜力和动向

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，但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）制订了清晰的进一步开发的路线图，具体涉及浏览器、

共识机制、虚拟机和可扩展性方面的重大改进。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。

Ripple（瑞波）现阶段主要致力于与银行合作，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 分别由两家联盟组织发起建设，联盟的成员机构主要来自金融领域和 IT 领域。它们将聚焦于分布式总账技术在金融行业的运用，重点放在私有链、联盟链上。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。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，不排除会走一条与众不同、直达金融业务本质的道路。

4 技术路线

4.1 领域、场景和运营模式选择

ChinaLedger 将为在中国资本市场推进分布式总账技术应用提供符合中国国情、适应中国法律与监管需要的基础平台，聚焦资产端应用，兼顾资金端、非金融端应用。

鉴于中国资本市场分布式总账技术应用场景更多地呈现出“同质化、小生态”的特点，ChinaLedger 将针对这一特点积极探讨带有隔离墙机制的“云化”解决方案。

针对中国资本市场的现实环境，ChinaLedger 优先考虑提供联盟链解决方案，在联盟链上忠实体现和反映中国资本市场职能机构的业务范围和职能边界。在运营模式的设计上，支持技术层面的专业化运营服务和业务层面的自主化运营服务既互相剥离，又有机结合。

4.2 平台策略

根据前面的技术选型评估，大致可以得到关于平台的一组基本的策略。

4.2.1 借鉴

分布式账本技术的核心就是对算法的充分信任，而在算法代码开源条件下，通过在广泛应用和反复博弈中取得公众信任，是对一个分布式账本技术体系强安全性的最好诠释。因此从近期看，ChinaLedger 的分布式账本基础平台不可能凭空产生、从头做起，而必须首先选择合适的开源分布式账本技术体系作为主要借鉴，在其基础上搭建符合中国国情、适合中国法律与监管需要的基础平台。

从前面的业务需求分析中不难看出，高安全性、强表达力、多资产类别、良好的未来发展潜力和性能优化前景，去除原生数字货币副作用小，是中国资本市场对基础账本选择的基本要求。而在我们所考察的六大技术体系里，最有借鉴价值的，是以太坊和超级账本两个平台。

但随着技术的发展，新的平台也在不断出现。另外从长远考虑，自主可控底本的研发也应提上日程。因此，初期的借鉴不是最终目的，ChinaLedger 还必须对长远的底本选择做出战略性安排。

4.2.2 改造

从前面的业务需求分析中不难看出，ChinaLedger 为适应中国资本市场要求而拟在后续对分布式账本基础平台的主要修改工作，核心是在中心化的“特权”机制的引入、“隐私”机制的实现、原生数字货币的去除和业务处理性能的优化。它们都几乎不约而同地集中在智能合约层面。我们判断，合约语言的未来趋势一定是跨平台，即使在同一平台下，合约模板也完全有可能对基础账本层的细微版本变化无感。如果再加上技术实现方案上的刻意努力，这就意味着，近期的借鉴和长远的自主开发可以兼顾，我们在合约层面拟开展的改造工作不仅在近期会快速得到应用，在未来也会得到最大限度的复用。因此，ChinaLedger 的目标是：在智能合约层提出一套“合约模板”，尽量把所有改动封装在“合约模板”中，这样就可以在某种抽象意义下同时既支持近期以借鉴为主的基础账本，又支持远期以自主开发为主的基础账本。

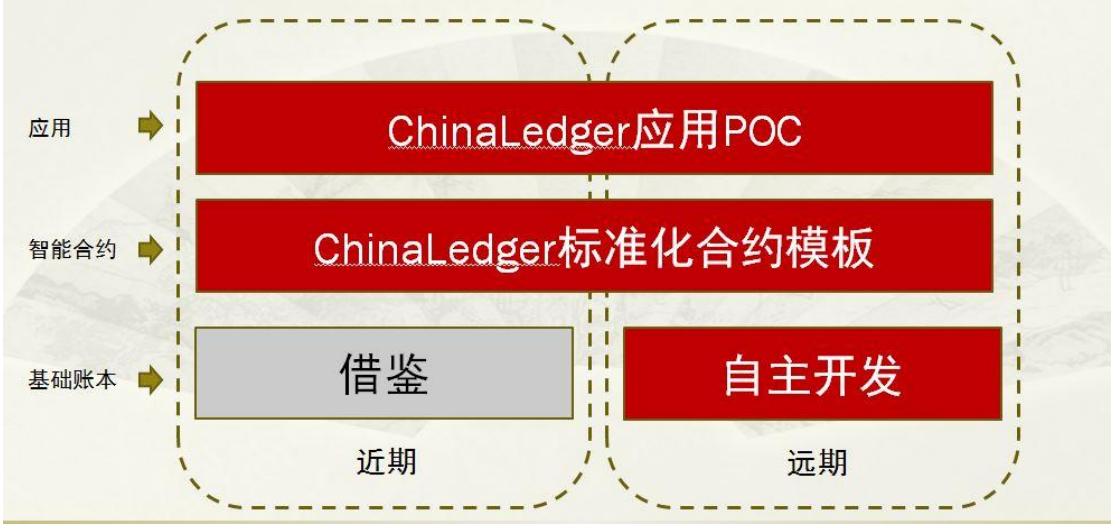
4.2.3 自主研发

分布式总账技术具有强安全性，资本市场又是国民经济的命脉。从长远战略考虑看，ChinaLedger 应在充分掌握底层账本核心技术的前提下，自主开发出一套含基础账本在内的整个分布式总账技术体系。

涉安全技术模块的自主掌控、涉资本市场模块的合法合规、架构的充分模块化和架构组件的充分可插拔是 ChinaLedger 未来自主研发的分布式总账技术体系的设计所应遵循的基本架构准则。

在数据的加解密算法和摘要算法上，ChinaLedger 应支持国密算法。

以上关于平台选择策略的借鉴、改造和自主研发三原则，可用下图表示。



4.3 共识机制选择

根据选型分析的结论，PBFT 所能达到的性能指标在各类共识机制中名列前茅。据我们了解，目前，在以太坊平台和超级账本平台上都有引入 PBFT 共识机制的尝试。ChinaLedger 内部也进行了在以太坊平台上引入 PBFT 共识机制的测试。应该说，引入 PBFT 已经不存在本质上的技术障碍。

但是也要看到，PBFT 不适于节点可动态加入的场景。针对这种情况，ChinaLedger 还将深入研究 PBFT 的替代方案。

5. 特权[1]方案

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。这些措施具有鲜明的中心化色彩，虽不被社区认同，但却是资本市场得以正常运行的根本保证。

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，在基础账本层面均未见到这种合法支配技术意义下属于他人名下财产的中心化技术安排。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，而只能去硬分叉。这一方面源于社区无政府主义势力的阻碍，另一方面也源于必要的中心化特权机制的缺失。

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。本节介绍 ChinaLedger 关于一些特权机制在分布式账本上实现的技术方案。

5.1 特权账户

ChinaLedger 平台上将设立特权账户，包括但不限于司法账户、监管账户、交易业务操作账户、结算业务操作账户等。

特权账户的地址（公钥）将被特别明示出来，其他参与者可以通过所附签名验证操作指令是否为其所发。

5.2 特权操作

特权操作指令以私钥签发的消息的方式送达指定的智能合约，触发相应的特权操作动作。以下各小节所述，均为 ChinaLedger 将提供的特权操作指令。需要说明的是，目前本白皮书中所介绍的特权操作指令只是完整履行法律法规所需特权指令的一小部分。ChinaLedger 还将继续研究并提供其他中国资本市场所需的特权操作指令。

[1]本白皮书中“特权”一词对应的英语是“special permission”而不是“privilege”

5.2.1 冻结-解冻

冻结指令由司法账户签发。指令中含有冻结类型信息、被冻结资产对应的智能合约地址和被冻结账户的地址。

冻结指令生效后，特定账户向智能合约发出的后续指令将被拒绝执行。除非收到解冻指令，冻结指令将持续生效。

解冻指令亦由司法账户签发。指令中含有被冻结资产对应的智能合约地址和被冻结账户的地址。

在收到解冻指令后，被冻结的特定账户恢复正常权限状态。

在需要区分单边冻结（禁止价值转出）和双边冻结（既禁止价值转出也禁止价值转入）的场景，ChinaLedger 将增加双边冻结指令。考虑到价值转入的指令是将对手方账户信息加密传输的（见后文关于隐私方案的部分），对双边冻结指令的执行，需要具有对手方账户信息解密权限的中央对手方账户的配合。

5.2.2 停牌-复牌

ChinaLedger 考虑每个智能合约对应单项资产交易的情形。这时，对单项资产交易停牌，就等价于对智能合约“刹车”。

停牌指令由交易业务操作账户签发，指令中含有停牌参数和被停牌资产对应的智能合约地址。

停牌指令生效后，相应智能合约不再接受除特权指令外的任何普通交易指令，合约运行进入类似以太坊智能合约中 GAS 耗尽的状态。

复牌有自动复牌和手工复牌两种。

对于手工复牌，需由交易业务操作账户签发复牌指令。指令中含有被停牌资产对应的智能合约地址。在收到复牌指令后，被停牌的单项资产对应的智能合约恢复正常运行状态。

对于自动复牌，由业主根据自身业务规则来设定复牌时间，通过停牌参数编入停牌指令。被停牌资产对应的智能合约将于指定的复牌时间恢复正常运行状态。

5.2.3 停市-恢复交易

在 ChinaLedger 中，一个“市场”可以看做一组标的资产对应的智能合约群体。所谓“停市”，目前可供选择的有三种实现方式。

第一种方式是停牌指令的“群发”，可通过一个具有群发功能的超级智能合约——停市合约来实现。在这个停市合约中预设了被视为一个特定“市场”组成部分的所有标的资产对应的智能合约地址的列表。一旦这个停市合约被启动执行，它就向列表上的所有智能合约地址发送分解停牌指令。收到分解停牌指令的智能合约检验指令来源地址，确为停市合约所发则执行停牌。

这种方式的优点一是原子性好，不会出现一部分标的资产被停牌成功、另一部分停牌不成功的情况，二是只在停市发生时有计算和通信开销，平时不发生此类开销，三是标的资产如何组成市场，只在停市合约一处维护。缺点是群发的分解停牌指令是由智能合约向智能合约发出，不再携带交易业务操作账户的签名，这样的指令安全性稍弱。

第二种方式是通过一个智能合约来集中维护市场状态，我们称这个合约为“状态合约”。正常情况下，组成市场的每个标的资产对应的智能合约在处理每一笔普通交易指令之前，均需向状态合约确认市场状态为“交易”才予以处理。需停市时，由交易业务操作账户签发停市指令，发送给状态合约，由状态合约将市场状态置为“停市”。组成市场的每个标的资产对应的智能合约在处理下一笔普通交易指令之前，如果检查到“停市”状态，即可启动本身的停牌。

这种方式的优点一是无需分解停牌指令，因而也无需交易业务操作账户批量签发的或直接免签名，可达到同样的安全性，二是市场状态只在一处进行维护。至于缺点，一是不仅在需停市情形而且在正常情形都需发生计算和通信开销，二是有可能不保证停市操作的原子性，三是一个单项标的资产属于哪个市场，需要在它自己对应的智能合约中予以设定，维护工作过于分散，集中度不够好。

第三种方式是在客户端编写批量签发停牌指令的简易脚本。这种办法优点是安全性好，标的资产如何组成市场也是在一处维护。缺点是本属于平台的功能在客户端编程实现，不够理想。

ChinaLedger 将进一步研究上述三种方案如何改进。

恢复交易指令的实现方式也同停市指令一样有三种对应的方案。收到恢复交易指令（或其分解复牌指令）后，各项标的资产恢复正常交易状态。

5.2.4 强制划转

强制划转指令由结算业务操作账户签发，指令中含有转出方账户、转入方账户和具体划转额度的信息。这些信息具有较强的隐私性，因此和普通交易指令中的转入方账户、划转额度信息一样，需纳入隐私保护的范围，具体详见后文。

需进行强制划转的情形可能包括但不限于显失公平交易的回滚冲正等。

5.3 特权滥用问题

引入特权账户和特权操作这样一些“中心化的”机制后，分布式账本会不会因为特权滥用而受到损害，成为很多人担心的一个问题。从技术上如何防止特权滥用，ChinaLedger 一直十分关注。在特权机制的设计上，也对此有所考虑，主要体现在几个方面。

（1）**留痕**。特权操作均通过特权操作指令进行。所有特权操作指令均需特权账户私钥签名并在智能合约中予以验证。这些带有数字签名的特权操作指令将在分布式总账中永久保存，成为实施特权操作的证据。

（2）**分权**。不同特权操作须由不同特权账户签发执行。特别是，负责强制划转资产的特权账户和负责停牌停市的特权账户应赋予不同自然人。这样，即使发生不当的强制划转资产的操作，划走的资产仍然从总体上留在价值守恒的智能合约当中。这时，只要实施紧急停牌，仍有可能追回不当划走的资产。同时，对于特权账户，均可考虑通过多重签名的方式增加安全性。

（3）**授权关系**。特权用户的操作权限仅针对智能合约，暂不涉及基础账本。在基础账本上，私钥持有者支配相应账户资产的原则并未发生变化。在智能合约中，特权账户的操作权限是明示的，加入智能合约、参与智能合约中相应资产交易的参与者是知情的。知情仍加入，意味着同意合约，包括同意合约中的特权安排。因此，从法律关系上看，特权用户是在被参与者授权的情况下履行特权的，也要对参与者承担滥用特权的后果。

6. 隐私方案

在第 2 节里，我们对交易数据的隐私特性进行了分析，提出了应对隐私数据予以保护的需求。

在第 3 节里，我们分析了外界提出的与分布式账本配套的隐私保护的可能方

案。通过分析，得知保持全部去中心化特性和基于密码学最新成果的、较为彻底的隐私保护方案还达不到实用水平，而基于状态旁路的临时性隐私保护方案，难以防止通过恶意智能合约截听隐私数据。

在这一节里，我们提出基于中央对手方的双链隐私保护方案。这个方案带有明显的中心化色彩，但是对于法律本来就有明确“中央对手方”职能安排的资本市场来说，这一方案又是从法律到技术的一个很自然的延伸。

由于报价驱动模式下和订单驱动模式下的隐私保护方案有许多细节上的不同，而 ChinaLedger 优先考虑在报价驱动模式占主导的场外市场应用分布式账本技术，因此以下仅讨论报价驱动模式下的隐私方案，订单驱动模式下的隐私方案我们将另行发布。

6.1 交易指令

在报价驱动的模式下，交易指令含有交易对手方和交易内容的信息。具体到通过智能合约在分布式总账平台上的实现，交易对手方信息和交易内容的信息既是需要分布式节点予以见证的关键信息，同时又都是隐私信息。如果对交易内容加密，仅有交易对手方能够解密，那么见证者就无法通过交易内容的密文确定这笔交易是否涉嫌透支（买空或卖空），而且交易对手方必需通过链下的另外途径得知这笔交易是与自己有关的。

一个自然的解决方案就是：引入中央对手方（CCP）。交易指令用中央对手方的公钥加密。这就意味着，真正的余额，只有中央对手方才知道；是否涉嫌透支（买空或卖空），只有中央对手方才能判定。对交易的见证主体，和对透支与否的判断主体，在此进行了分离。

6.2 双链模型

真正的余额明文，放在另一个分布式账本中。为区别起见，我们把所有参与者都能访问的分布式账本记为“链 A”，把只有中央对手方和监管者能访问的分布式账本记为“链 B”。

在链 A 上，交易指令以密文形式出现。交易发起方将对手方信息和交易内容

信息用自己的私钥签名，然后打包用中央对手方的公钥加密，发给智能合约。所有参与人均可通过分布式账本技术平台，在链 A 上见证这一笔内容被加密了的交易。如果交易是资金和资产在链上对流，双方都需提交这种格式的交易指令。

中央对手方用自己的私钥解密后，将明文的交易指令发到链 B 上，检验交易指令中发起者签名的有效性，并获得链 B 做出的是否透支的判断。

如果透支检查正常通过，中央对手方在链 B 上为双方完成交易后余额的维护。

上述手续完成后，中央对手方在链 B 上生成、在链 A 上向发起方发送交易确认消息。

整个过程如下图所示：

6.3 看穿式监管

在双链模型下，普通参与者在链 A 上看不到交易的细节。如有需要，被法律赋予监管职能的监管者可通过开设在 B 链上的监管者账户，看到从链 A 发起的所有交易细节的明文。

6.4 隔离墙

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。

在一个分布式总账平台为多个机构提供云化服务的场景下，被服务的机构不

希望其他机构看到己方的非共享数据，也不希望对方的技术性能瓶颈或其他异常影响自己的市场服务质量。这种机制在技术上也被称为“沙箱”。但为避免与第2节中谈到的业务“沙箱”相混淆，我们把云化服务下的“背靠背”数据隔离机制称为“隔离墙”。

在云化服务的初期，隔离墙可参照本节所介绍的双链模型，通过设定一个A链、多个B链，各个B链之间完全不能互相访问的策略来实现。如果一个A链不能满足隔离要求，可进一步对A链实施分层隔离，比如在基础账本层面共享，在智能合约层面进行隔离等等。

7. 原生数字货币的处理

在资本市场金融服务的大背景下，初期借鉴来的分布式总账技术体系中所建立的原生数字货币，其激励机制已经不具有继续存在的意义，因此，挖矿只有总账维护这一单一目的，应与原激励机制脱钩。

另一方面，以某种度量单位（如以太坊中的GAS）为纽带建立的原生数字货币的资源控制机制，在资本市场金融服务的大背景下仍有继续存在的意义。一方面，它可以精准计量智能合约对虚拟机资源的消耗，引导用户把有限资源用于有价值的服务，另一方面在极端场景下也可以对虚拟机的运行安全形成必要的保护。由于ChinaLedger的选型策略决定了其智能合约的表达能力较为强大（图灵完备），相应地就要对其局限（停机问题的不可判定性）做好防范准备。

考虑到原生数字货币代码涉及面广，内在逻辑复杂，在代码级别去除原生数字货币的激励功能同时保留资源控制功能，可能隐含较大风险。因此，ChinaLedger在其分布式总账平台的设计中将采用较为温和的方案，保留代码，通过参数设置方式将原生数字货币与资源控制功能脱钩。

此外，ChinaLedger 在面向资本市场应用场景中，将有可能会按需引入锚定法币的代币充当“结算币”。它将有助于提升面向实时逐笔结算和交易后清算交收的处理效率，甚至可助力建设数字社区生态。

在未来自主研发版本的分布式总账技术平台中，ChinaLedger 的联盟链版本将不再包含原生数字货币及相关的激励机制。

8. 性能优化目标

根据中国资本市场常态和峰值数据，ChinaLedger 将持续优化平台性能，希望最终能达到如下目标：

（1）吞吐率目标：每秒 100,000 笔以上；

（2）时延目标：同城 1 毫秒以内；

（3）存储目标：按每日 80,000,000 笔的容量，重节点能存储全量数据，轻节点能存储当日数据。

这些优化目标，在初期仅针对场外市场阶段是没有必要的。达到这些目标，主要是为了验证 ChinaLedger 后续支持场内业务交易后业务处理和进一步推进分布式总账在资本市场应用的需要。

9. 展望与总结

本白皮书仅代表 ChinaLedger 在现阶段对自己使命、对在资本市场应用分布式总账技术的认识，以及对今后一段时间内平台开发工作的设想。随着项目的推进，我们的认识将会深化，一些观点可能会有所修改，一些方案可能会有所调整和完善。

分布式总账技术是涉及强安全性的技术，资本市场又是国民经济的命脉所在，因此自主研发高水平的分布式总账技术平台，是 ChinaLedger 全体成员单位包括观察员单位的共识。同时，我们也了解到，我们关于分布式总账技术平台的总体思路，跟国内其他一些联盟组织也是高度一致的。我们将不辱使命，在凝聚共识、整合资源、求真务实、开放开源的基础上，逐步加大自主创新的步伐，做强 ChinaLedger 的基础平台。