



区块链

共识

价值互联的不变协议

kpmg.com

作者介绍



Sigrid Seibold

咨询资本市场主管, KPMG LLP

Sigird拥有25年银行业和资本市场工作经验。她主要运用其在数据管理和数字化技术(如金融和区块链领域)方面的专长为大型投资银行提供服务。作为一位备受尊崇的行业思维领袖,她曾多次发表涵盖不同资本市场主题 of 白皮书,其中包括区块链在投资银行中的应用,并在《华尔街日报》等主要报纸上发表文章。



George Samman

区块链顾问及咨询师

Geoge是一名区块链顾问/ 咨询师, 并是Startupbootcamp中专注于区块链及比特币的企业家。他撰写了一个关于区块链技术的博客, 并为SAMMANTICS编写使用案例。从2013年起, 他已与伙伴共同创办并服务于多家专注于比特币及区块链技术的初创公司。他亦为多个区块链刊物供稿, 并是一家华尔街公司的组合基金经理、市场分析师和技术分析师。他拥有特许市场分析师(CMT)认证。

与毕马威中国联络



麦高仕 (James McKeogh)

合伙人, 咨询

麦高仕是毕马威咨询行业的合作人, 已经在毕马威工作17年, 并有3年在伦敦巴克莱财富公司的工作经历。

麦高仕主要从事金融领域, 也从事过制药、制造业、石油和天然气工业、公共部门和零售业等行业。詹姆斯在香港工作已经超过6年, 专门从事在数据分析、数字和支付等毕马威服务的新兴技术。麦高仕同时领导着涉及该生态系统各个方面的毕马威金融科技项目—从业务孵化器和加速器, 到投资者和大型企业。



张峻铭

合伙人, 金融科技创新

张峻铭先生有25年银行业咨询经验。在核心银行、企业转型、业务流程重组和信用风险管理方面具有丰富的业务和技术专长。从事过大规模的转型项目, 包括IT战略规划、网点运营、客户关系管理、精益运营改善, 电子银行、KPI和数据分析等, 最近几年主要参与金融科技和区块链技术相关工作。

目录

- 1 抓住机遇 – 区块链及其它
- 2 区块链的基本要素
- 3 共识
- 10 主要发现
- 14 区块链适合您的企业吗?
- 15 掌控前方的道路
- 17 附录一: 主要术语
- 19 附录二: 共识机制评估问卷
- 24 附录三: 问卷反馈集锦
- 25 鸣谢



抓住机遇—区块链及其它



区块链是比特币的核心技术，是一个去中心化的数据库账本。起初，区块链技术并没有得到人们的广泛关注，但如今，世界上很多大型银行和科技公司都已逐渐意识到区块链将会是继互联网之后的另一个颠覆性的科技发展技术，并开始对其进行大量投资。

区块链技术有望实现数字身份的建立，并使传统的纸张密集型流程自动化，这使得区块链技术成为未来金融服务的万灵丹。尽管有一些人对区块链技术持审慎态度，但有一件事是明确的，那就是毕马威中国将会继续研究和分析不同的案例，这也是毕马威中国与客户约定的一部分。我们相信，随着金融服务机构逐步意识到区块链的影响和作用，他们将会逐步把区块链技术应用到日常操作中。



术语

区块链、分布式账本以及共识机制有可互换使用。本刊中，下列术语具有以下定义：

区块链：一种管理持续增长的、按序整理成区块并受保护以防篡改的交易记录的分布式账本数据库。

分布式账本：不同于传统数据库技术的数字化所有权记录（因不需要中央管理员或中央数据存储）；这种账本能在点对点网络的不同节点之间相互复制，且各项交易均由私钥签署。

共识机制：区块链或分布式账本技术应用的一种无需依赖中央机构来鉴定和验证某一数值或交易的机制。共识机制是所有区块链和分布式账本应用的基础。

节点：保存账本副本的共识网络或服务器的成员或系统，并可担任不同角色，如发出、验证、接收和通知等。概括而言，节点可被视作虚拟机实例。

区块链的基本要素

区块链作为分布式账本的其中一种，将交易以区块的形式进行排序和验证，并施以保护以防篡改。电脑网络通过加密的审计线索来保存和验证交易的共识记录。分布式账本意味着不存在单一的中央机构（如结算所）来验证和执行交易，而参与者的电脑则被用作网络内的节点。

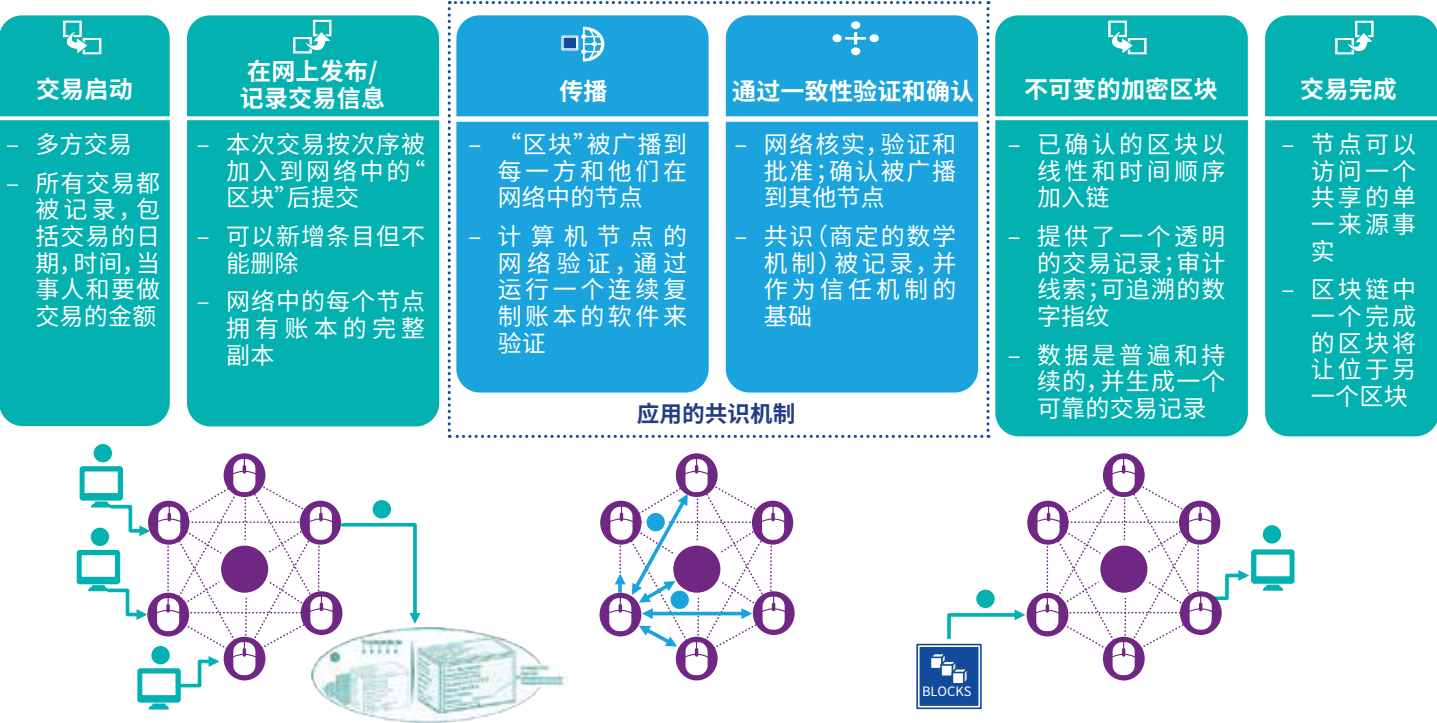
这些节点的部分或全部将按商定算法（即共识机制）来验证，并在合适的情况下，执行拟定交易。这些交易随后被加密并储存于节点的关联区块中，形成审计线索。

由于该技术在参与者的节点上运行，能提供所需保密度，因此交易各方之间无需设置中间人，点与点之间亦无需进行信任验证。在有效执行的情况下，区块链具有快速、保密、可靠和低成本的优势。

区块链的核心是参与者之间的共识（参见图1第三、四步）。共识之所以是关键，是因为在没有中央机构的情况下，参与者必须就规则及其应用方法达成一致；并同意使用这些规则来接受及记录拟定交易。

图1: 区块链是什么？

区块链是在分布式账本中排序及验证交易的方式。应用区块链时，电脑网络以加密的审计线索来保存及验证交易的共识记录。



共识

共识概念：昨日与今天

建立共识当然不是一个新的概念。共识在人类开始群体生活之时便已存在。从最基本的层面上说，共识只是一种让一个多样化团体在不发生冲突的情况下作出决策的方法。根据Edward Shils的“共识理念”，共识的达成需以下三个条件：

- 团体成员共同接受法律、规则和规范
- 团体成员一致认可实施这些法规的机构
- 身份认同或团结意识，这样团体成员才会承认他们就达成的共识而言是平等的。

共识开始时作为社会运作的一个概念，但如今已成为计算机科学的重要组成部分。在过去30多年，电脑世界中的共识机制已从一个抽象概念发展成分布式账本技术的重要支柱。

在分布式账本中，共识机制是大部分（或全部）网络成员就某条数据或拟定交易的价值达成一致，并就此对账本进行更新的机制。换言之，共识机制是在参与节点之间管理一系列连贯事实的规则和程序。¹

共识算法允许关联机器连接起来进行工作，并在某些成员失效的情况下，工作仍能正常进行。这种容错能力是区块链和分布式账本的另一主要优势，并有内置冗余余量以作备用。

共识协议或共识平台是分布式账本技术的核心。用以建立共识的算法多种多样，并建基于性能、可扩展性、一致性、数据容量、治理、安全性和失效冗余等方面的要求。

如图1所示，交易一经创建和发布，即署有交易发起人的签名，签署表示获得授权以支付金钱、订立合同或传递与交易相关的数据指标。交易在签署后即可生效并包含执行需要的所有信息。

交易被发送至区块链网络的一个节点，该节点将根据预先设定标准来验证交易。无效交易会被废弃，而有效交易则会被传送到另外三到四个关联节点，这些节点将进一步验证交易并将交易传到其对等端，直至该交易到达网络中的所有节点。这种蔓延式的方法确保有效交易在数秒之内到达网络中的所有节点。只要发送者使用多于一个节点来确保交易传播，那么它就不需要信任用来传播交易的节点。接受者亦不需要信任发送者，原因是交易已被签署，且不包含任何机密信息或证书，如密钥。

一旦交易被验证并纳入区块，该交易便会在整个网络中传播。在整个网络达成共识和网络中的其他节点接受新区块后，该区块就并入区块链中。一经区块链的记录和足够多的节点确认，该交易将成为公共账本的永久组成部分，区块链网络中的所有节点亦会视之为有效。

可建立共识的机制很多，程序员和企业亦一直致力于开发新的机制。区块链采用何种共识机制是如何定义一个区块链的核心。

我们将于下文介绍当前最主流的共识机制。您会看到并不是所有这些共识机制都是区块链。某些机制在“链外”仍可作为双边协议运作，对此我们将进行更详尽的分析。注：刊末附有术语表，为非专业人士解释某些常用术语。

¹ <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>

共识

共识机制如何运作

共识机制的基本决定参数：

- 去中心化治理:单一中央机构不能提供交易不可改变性。
- 节点结构:节点通过既定方式来交换信息,可分多个阶段或层级。
- 身份验证:此流程验证参与者的身份。
- 完整性:验证交易的完整性,如通过加密算法。
- 不可否认性:验证假定发送者确实发送了信息。
- 隐私性:协助确保只有既定接收人才能读取信息。
- 容错性:即使某些节点或服务器失效或运行减慢,网络仍能高效、快速地运行。
- 性能:包括吞吐量、实时性、可扩展性和延迟。

不同共识机制中的参数会存在巨大差异。我们在描述下列特定机制时将分析这些差异。

上述参数的一部分通过加密法中四个主要方法来执行,这四个方法使用数学公式来尝试确保安全性和隐私性。这四种方法包括公钥、私钥、散列法以及分层确定性密钥。

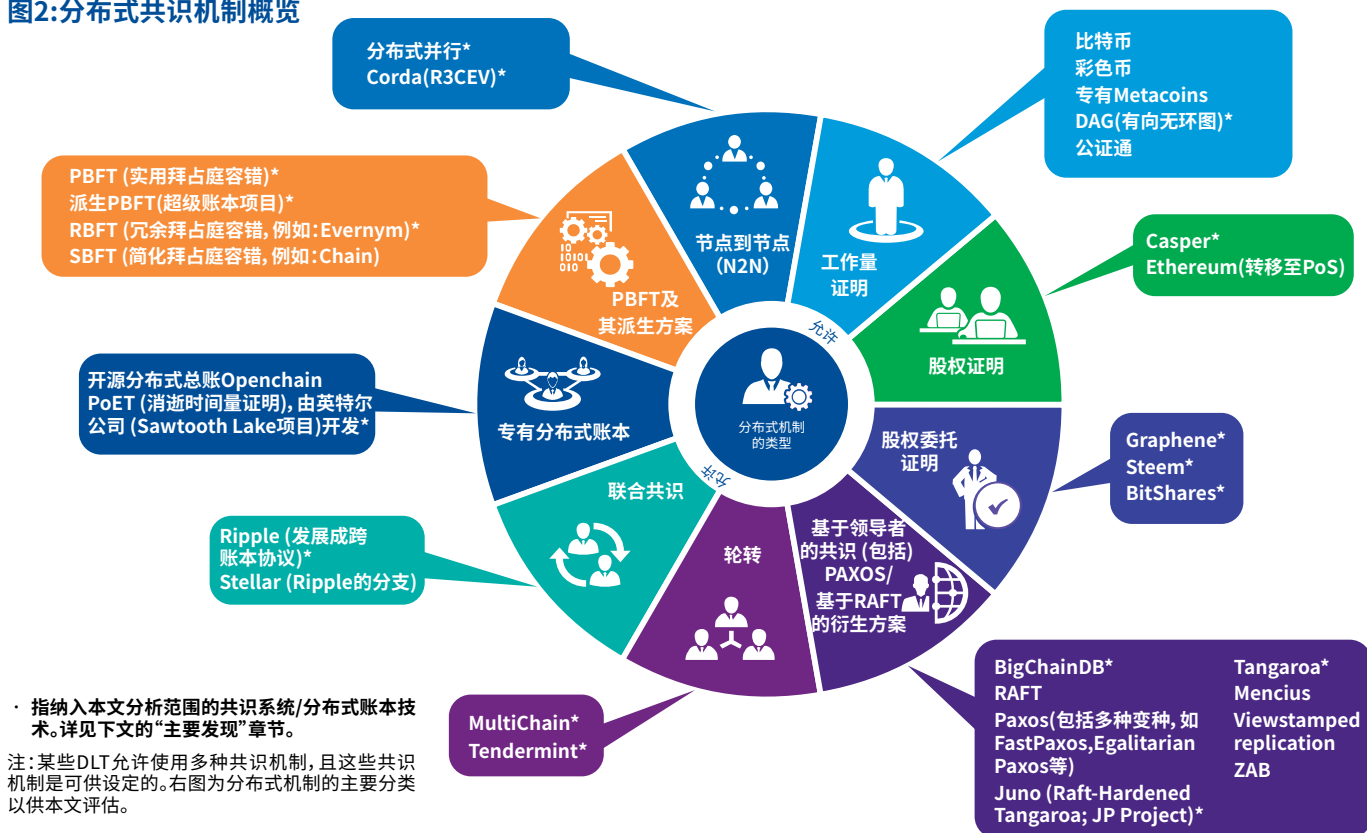
共识机制和分布式账本技术概况

图2展示了当前市面常见的分布式账本技术。

注:主要术语定义请见附录1

因技术更新日新月异,以下共识机制的种类和描述仅是近期某一时点(2016年4、5月)的概览。本文的目的并不是完整展示当前所有共识机制,而仅描述那些当前作为区块链建立的技术选项而被热切讨论和探索的机制。我们特此说明,这些共识机制中的大部分在区块链和分布式账本产生前已被应用。我们的分析中未包含任何传统的集中化数据库。

图2:分布式共识机制概览



拜占庭将军问题

现代共识机制的基础于1962年提出。RAND Corporation的一名工程师Paul Baran在论文《论分布式通讯网络》中提出了加密签名的概念。这些数字化签名不久就成为了系统对修改数据或文档的用户进行验证的方法。

二十年后，三名学者发表了一篇关于去中心化系统可靠性问题的论文。在《拜占庭将军问题》³中，作者Leslie Lamport、Robert Shostak、和Marshall Pease提出了一个思维实验：假设有一组将军，各自统领着拜占庭军队的一部分，包围了一个敌军城市。将军之间只能靠信使进行通讯。但为了攻占这个城市，他们必须就作战计划达成一致。

问题在于，一个或多个将军已可能发生叛变，并试图误传信息以破坏作战计划。对此，我们的问题是，这支军队可存在多少已叛变的将军而仍可正常地统一作战？

此情景可与在没有中央机构验证相关资产和交易的情况下的数字货币、资产托管和价值转移进行直接类比。在分布式账本中，不同的参与者节点就像将军，需确定一个可接受的失效水平：在系统不需要拒绝交易的情况下，可容许多少恶意交易（可容许多少已叛变的将军）？这是因为一定数量的失效可能不会损害系统整体的可靠性。

在这些作者提出的情景中，由于每两个将军由信使联系，我们可以制定一套算法，在肯定三分之二或以上将军是忠诚时，该系统（拜占庭军队）便是可靠的。

对于计算机上的分布式金融交易而言，问题更为复杂；有一段时间，业界甚至认为这个问题是不可解决的。

拜占庭将军问题的解决方案以及比特币

Miguel Castro和Barbara Liskov在1999年提出实用拜占庭容错算法（PBFT），成为该问题的解决方案。PBFT可以最小延迟处理大量的直接点对点（或分布式）信息。这意味着程序员可建立安全和适应性强的私人分布式网络。从1999年起，PBFT已通过多种途径得以实施，并进一步发展成各种技术迭代。

首先在1999年发展起来的是“工作量证明”。工作量证明是指系统用户须重复运行算法以验证系统内其他参与者的交易。到目前为止，该方法仍然是最受业界认可的共识实现方法。

工作量证明系统以去中心化的点对点加密协议来运行区块链。这些系统不设中央机构，但假定“忠诚”节点至少控制系统的大部分计算能力。（至少半数军人受忠诚将军掌控。）这些系统是公开或无需设置权限的系统，即系统内节点不需要知道其他节点的身份。

比特币是工作量证明系统的最知名应用。一个名为Satoshi Nakamoto的个人或团队于2008年10月以一篇名为《比特币：点对点电子现金系统》的论文提出了比特币技术。⁴该技术随即作为开源代码被应用，并于2009年1月发布，成为当前最有名的电子货币。比特币技术基于“挖矿”，即参与者电脑验证交易并将其加入公有账本，就此赚取新的比特币。

很多其他方法紧随比特币陆续涌现。图3（下页）展示了比特币出现前后的技术发展。我们将于下文探讨其他技术分支。

开采比特币的其他途径

股权证明产生于2012年。此方法旨在创建一个机制，以惩罚那些不遵循共识协议的节点。参与者必须以预设数额的电子资产（比特币）对共识结果下注。如果结果没有实现，恶意节点将损失这些资产。

在股权证明系统中，比特币挖矿要求参与者“下注”，参与者需根据他们已拥有的比特币数量来开采新币或输入新交易。在工作量证明系统中，能否成功挖矿则取决于实际的计算工作。

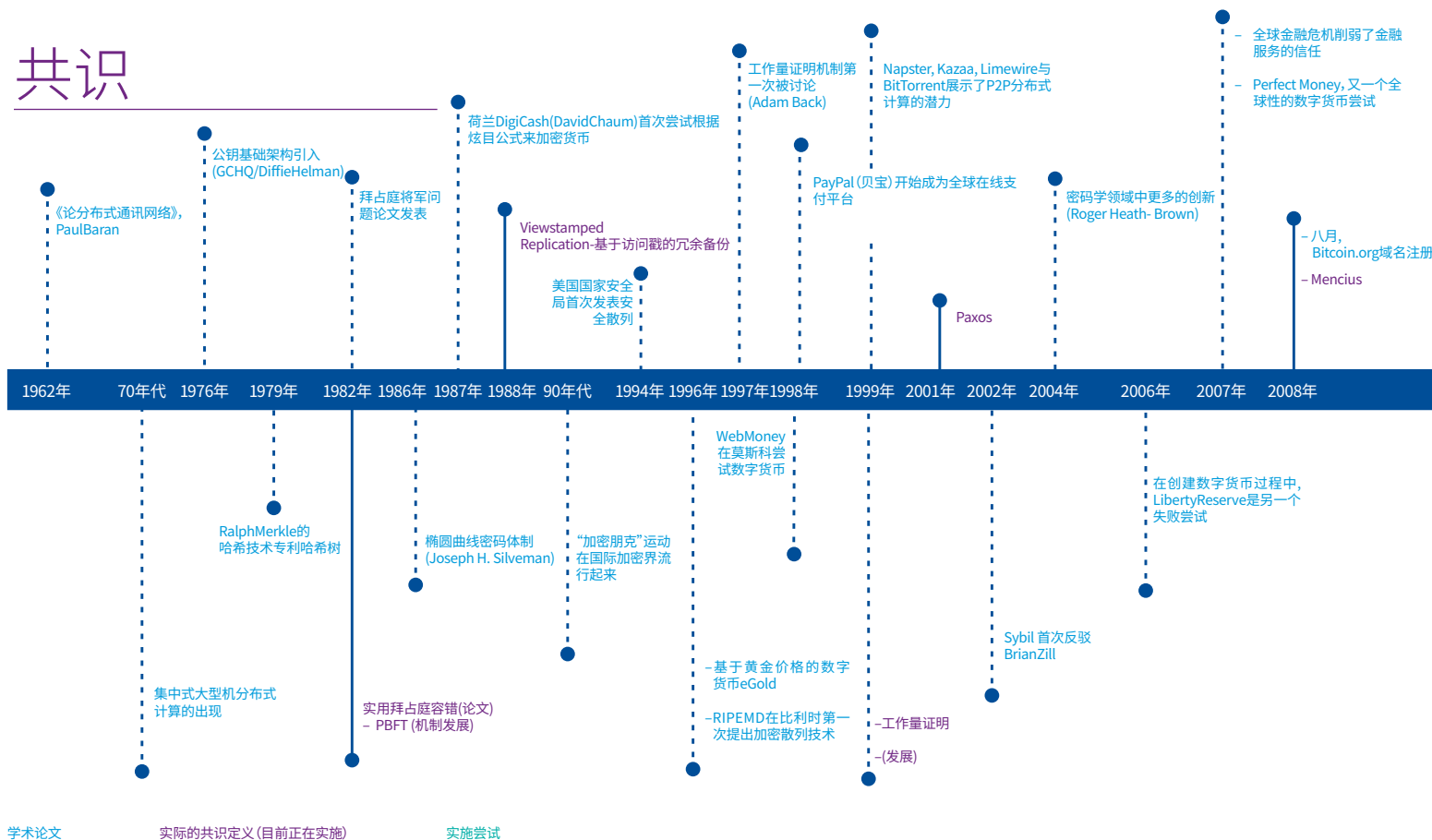
与工作量证明系统对比，股权证明系统的优势在于其要求更少的计算工作。由于相关计算需要高昂成本，计算量的减少可降低系统成本和准入门槛。⁵参与者拥有越多比特币和更高受控计算能力，开采新区块的可能性就越高。

3 LAMPORT, L., Shostak, R., and Pease, M.《拜占庭将军问题》，美国计算机学会程序语言和系统汇刊，4, 3 (1982年7月), 382–401

4 <https://bitcoin.org/bitcoin.pdf>

5 <http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf>

共识



另一个名为股权委托证明 (DPOS) 的系统尝试结合股权证明系统和工作量证明系统的特点。DPOS通过所谓“见证人”来执行一个去中心化的投票程序, 以防止潜在的网络中心化

比特币之后的发展

开发者一直致力于提出新的机制以提升比特币应用。2014年, 法国企业家Flavien Charlon创建了Coinprism, 通过使用名为“彩色币”的开源协议在比特币区块链基础上创造数字化资产, 使比特币区块链可用于货币以外的用途。某些大型金融市场企业 (如花旗集团⁶和美国纳斯达克⁷) 已于2015年开始尝试使用彩色币。

同时出现的还有Metacoin, 一种以新层级形式建立于另一种区块链基础上的币种。⁸

尽管这些技术拥有各种显而易见的潜力, 但将其应用于高度监管的金融机构仍是不可行的, 原因如下⁹:

5 <http://www.ibtimes.co.uk/codename-citico-in-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759>

6 <https://www.theguardian.com/technology/2015/may/13/nasdaq-bitcoin-blockchain>

7 <http://explainbitcoin.com/what-is-a-meta-coin/>

8 <https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/564ca429e4b0a9e90a947ba2/1447863337472/watermarked-tokens-and-pseudonymity-on-public-blockchains-swanson.pdf>

9 https://ripple.com/files/ripple_consensus_whitepaper.pdf

– 源自比特币及其它基于工作量证明的区块链的安全系统不适用于受监管的金融结算 (其激励被扭曲)

– 结算的法律终局性不足

– 监管风险仍较高。

区块链之外的技术方案

为寻找能可靠应用于金融机构并被监管者接受的共识机制, 开发者将注意力投向不是基于比特币或工作量证明系统的技术方案。于2012年开发的Ripple就是首个有重要影响的新方案。Ripple的代码库基于比特币区块链, 但并非使用工作量证明共识。Ripple网络使用的是“Ripple共识账本”, 具有以下特点:

– 该系统由参与者和历史记录定义, 并非由基础技术定义。

– 通过开放式点对点广播来传播信息。

– 其货币使用XRP标记系统, 而不是依靠挖矿。

– 总网内存在称为“独特节点列表” (UNL) 的集合信任共识子网, 整个系统如同一个联合体。

– 各参与服务器根据其管理员的设置方式来管理自身UNL。

共识

2016年2月, Linux Foundation的Hyperledger项目发布了基于模板的PBFT以作为区块链的创建基础。该项目意图通过建立一个跨行业、开放标准的开源开发程序库,使商业用户可建立自定义的分布式账本方案。Hyperledger的模板可自定义特定交易,并通过私有区块链或其他注册表进行记录。

大企业的参与度增加

今年3月,摩根大通发布了自身的共识机制,该机制的研发从2015年已开始。像RAFT和Tangaroa(启发了该项目)一样,这个名为Juno12的项目通过选举一个临时领袖来实现共识。客户端节点向领袖节点发出指令,后者再将该指令发布到系统中。^{11,12}

Intel®亦在今年发布了Sawtooth Lake项目详情,该项目基于分布式账本的PoET平台。Intel 对该项目作如下介绍:

“Sawtooth Lake抽取了共识的核心概念,使共识从交易语义中分离,并提供两个附带不同绩效权衡的共识协议:第一个是消逝时间量证明(PoET):这是一个抽彩式协议,建立于由Intel的SGX提供的可信执行环境,以回应数量巨大的参与者的需求;另一个是群体投票:这是Ripple协议和SCP的修改版,作用是满足要求立即获取交易终局性的应用的需求。¹³

中国企业也在该领域不断发展。ChinaLedger Alliance在五月初宣布成立:在万向区块链实验室带领下,11家商品、股权和金融资产交易所致力创建一个开源区块链协议,并制定跨行业标准以确保监管合规。¹⁴

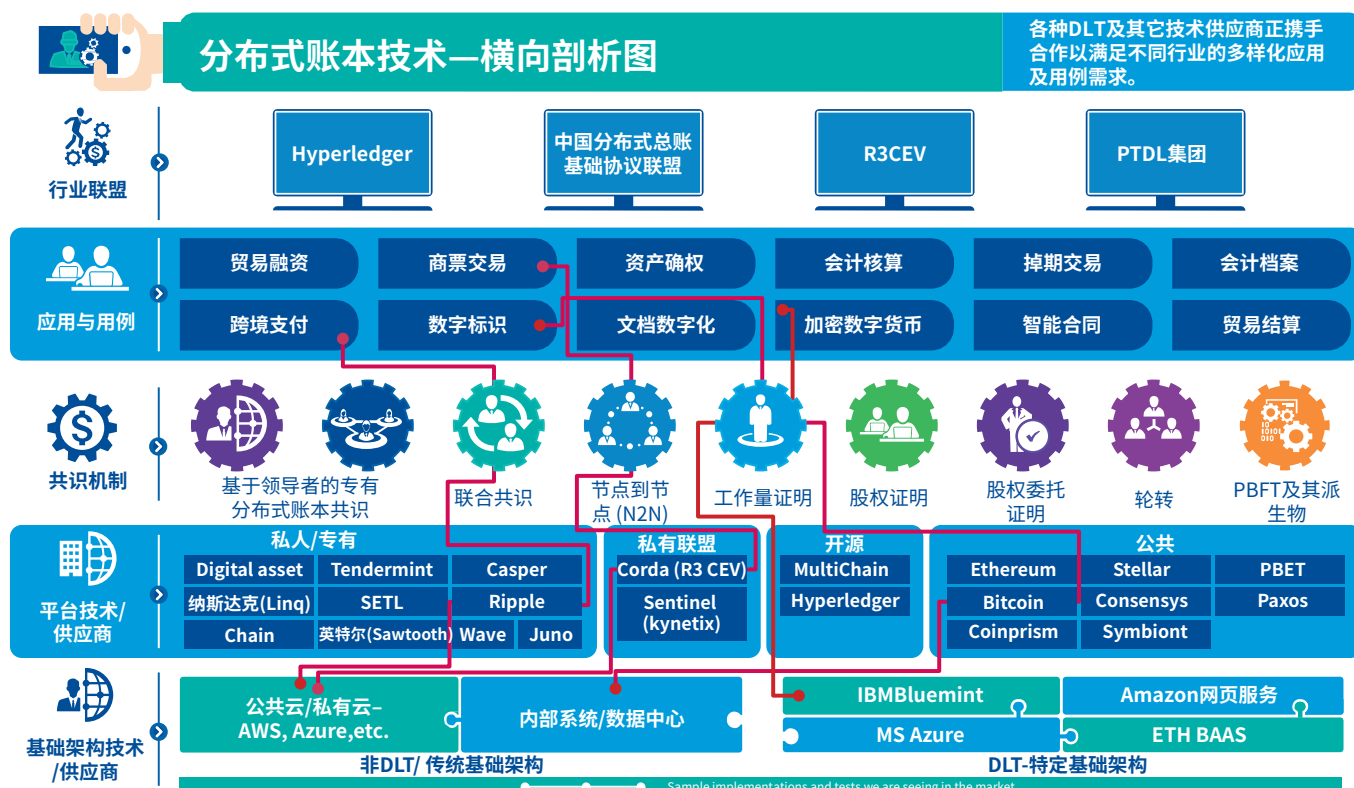
11 <http://www.the-blockchain.com/docs/JP-Morgan-Juno-Distributed-Cryptoledger.pdf>

12 <http://www.coindesk.com/jpmorgan-juno-hyperledger-blockchain/>

13 <http://intelledger.github.io/introduction.html>

14 https://bitcoinmagazine.com/articles/china-joins-the-blockchain-race-with-chinaledger-alliance-1462204569?q=&hPP=5&idx=articles&p=0&is_v=1

图4: 分布式账本技术图示



硅谷初创公司Chain亦在五月发布了¹⁵ Chain Open Standard 1, 该标准由Chain在九家大型银行和支付企业(包括第一资本和花旗集团)¹⁶ 协助下建立。Open Standard 1是一项开源技术, 意在协助金融公司在已设置权限的区块链网络中运行大规模金融应用。

Chain声称Open Standard 1可在一秒内完成大量交易, 亦可加密数据并选择性地为交易对手和监管机构提供访问。该方案提供了一个智能订约框架, 以支持简单规则的执行和关键值储存。

不同企业的开发成果将很快形成一个数字化账本生态系统。某些供应商(如初创企业)提供针对特定用途的平台, 另一部分供应商则提供通用方案。更多开放标准协作团体将会出现, 回应各种复杂需求的共识机制亦会不断涌现。

15 http://www.americanbanker.com/news/bank-technology/with-banks-help-startup-chain-rolls-out-open-source-blockchain-1080785-1.html?utm_content=socialflow&utm_campaign=amerbanker-tw&utm_source=twitter&utm_medium=social

图4展示了各种区块链、分布式账本技术和技术供应商是如何紧密合作, 以回应不同用例的市场需求。

图 5描述了共识机制的发展成果以及当前发展速度。

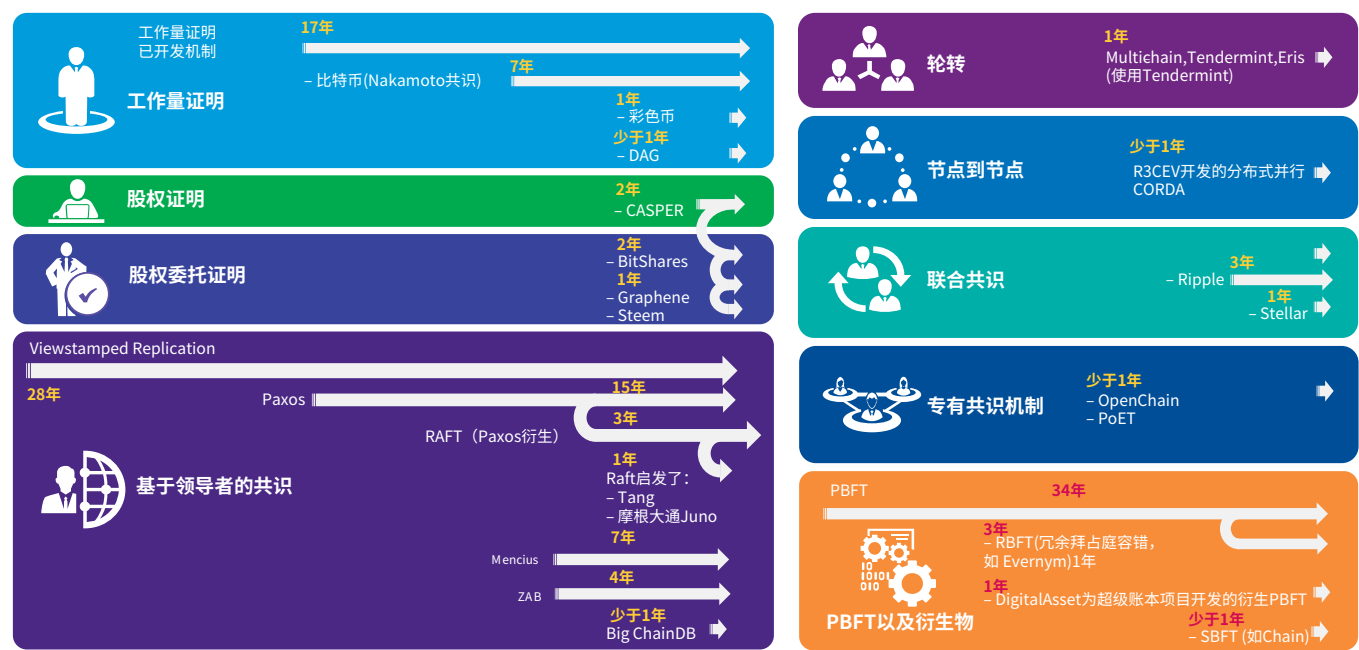
针对特定需求的共识机制

我们相信共识机制将发展为针对特定需求, 其中包括特定用例的需求、技术执行可能性的需求或监管环境的需求。针对后者需求的其中一个例子是MultiChain, 其权限管理系统具有七种权限设置, 允许不同参与者进行连接、发送、接收、发出、挖掘、激活或管理等操作。

仅有连接权限的节点可具有只读访问权限。若节点没有挖掘权限, 则其仅可能读写, 而不能验证。一个只能写不能读的节点不会有太大价值, 原因是若节点不知道从何处接收资产, 那么它也不能建立任何交易。

16 Capital One Financial, Citigroup, Fidelity Investments, First Data, Fiserv, Mitsubishi UFJ Financial Group, Nasdaq, State Street and Visa

图5: 共识机制的历史比较



主要发现



图6: 分布式共识评估架构

我们在为本文进行的调研的过程中, 调查了超过20位区块链和其他共识机制的开发者和企业用户。

图6, 汇总了我们在评估当前市面最重要的共识机制和分布式账本技术时涵盖的框架与主要话题。

注: 应用该评估框架编制的具体调查问卷请见附录2。

下文是我们从调查中获得的主要发现。

共识方案概述

- 需设置权限的分布式账本技术越来越受金融服务机构的欢迎, 因该方案的参与者可被预先确定。上文图2汇总了当前正针对不同用例被执行或测试的各种共识机制。
- 共识机制要求交易方通过节点对节点通讯来验证交易。不同分布式账本技术在验证一项交易时所需的节点数不同, 从一个节点(如OpenChain)、过半数(如Juno)、绝对多数(如Ripple)到全部节点(如Casper)或节点数可设置; 譬如, Stellar可就可信节点网络设置为要求51%或就不可信节点网络设置为要求67%。

- 虽然所有技术供应商均看似具有一定程度的抵抗力/容错性, 并不需要所有节点在线, 但在多数情况下, 系统将要求一定比例的节点上线以推进共识。该比例取决于分布式账本技术及其相关的共识机制。某些分布式账本技术(如Casper)仅需一个节点在线即可运行, 另一些分布式账本技术则要求最少五个节点或预设的多数节点在线。节点对节点分布式账本技术是个特例, 因其要求所有交易方在线。

- 我们看到了各种类型的节点角色和节点数量面世。举例说, MultiChain的权限管理系统包含七种权限设置: 连接、发送、接收、发出、挖掘、激活和管理。系统内的节点若仅有连接权限, 其亦有可能具备只读访问权限。若节点不具备挖掘权限, 则其仅可能具备读/写权限, 而不能进行验证。一个仅能写不能读的节点不会具有太大价值, 原因是若节点不知道从何处接收资产, 那么它也不能建立任何交易。具备权限改变功能似乎是分布式账本的一个合理选择。

- Graphene和Bitshares 2.0等无权限账本应用DPOS, 并采纳与MultiChain类似的主要概念(不同点是这些无权限账本是开放式区块链): 灵活性。在本类方案中, 区块链参数的

灵活性(如费用、见证人数量、区块间隔和区块报酬等)可由一个委员会设定。该委员会由另一群与见证人不同的、被选出的股东组成;这些股东不会获得任何报酬,仅能通过投票来控制全域区块链参数,并在维护窗口中执行。

- 参与节点的数量取决于方案应用的概念。工作量证明不对初始竞争验证(挖掘)的节点设置限制,但现在亦有一些仅应用两个交易方节点来验证交易的极端方案(Corda)。
- 多数共识机制设有三个验证流程,但亦有例外,尤其是投票流程。
- Juno允许用户以任何方式加密信息,而Corda则提供节点对节点数据加密服务。这使交易方能在保密的情况下进行交易,不会将交易内容泄露给无关方。
- 共识机制的不同在于它们如何将交易定义为“已承诺”、“安全”或“生效”。但多数共识机制均要求大多数参与者接受交易,以实现交易终局性。
- 权限系统内参与节点的激励如何定义取决于金融服务用例。一般而言,参与者之间会通过法律合同、运营目标等方式对节点进行外部激励。某些分布式账本技术仍可被设置为应用工作量证明激励或股权证明反激励。

治理、风险和控制

- 系统中的节点通常为网络参与者所有,但对某些分布式账本技术而言,节点将被共识供应商拥有或管理,如Evernym。在某些情况下,供应商可占有一定比例的节点,但整个网络仍保持开放,以让其他参与者提供节点。
- Ripple起初设定为占有所有验证节点,但就权限系统而言,市场逐渐认为节点应由网络参与者占有。
- 治理模型取决于不同的账本设置。但外部法律合同、监督/监管/观测节点以及一体化权限模型均是分布式账本技术常用的治理机制。
- 多数分布式账本技术希望继续依赖现行的法律及监管架构来识别恶意操作和执行法律行动。此外,某些分布式账本技术(如MultiChain、Hyperledger和Corda)仅是平台或服务,不对参与者的恶意操作负责。
- 方案采用不同方法来限制恶意活动,其中包括将节点加入黑名单、锁定并发账本、保护访问控制系统、断开正进行恶意活动的对等节点以及允许客户中断领导权(对基于领导权的

分布式账本技术而言)。大部分这些方法类似于非分布式账本技术应用中使用的方法。

- 多数分布式账本技术使用公钥架构来确保其他参与者的可信度。上述共识机制大多建立于发布区块链所使用的密钥均为安全这一假设。
- 在我们评估的分布式账本技术中,管理员节点功能各不相同。对某些分布式账本技术而言,管理员节点的应用是可设置的。
- 不同软件方案使用不同的方式在(权限)网络中加载或解除节点。某些方案把整个强制的了解客户和反洗钱流程交由参与者完成,另外一些方案则在加载节点时承担一部分这些责任。
- 节点的行动者已知使恶意节点的访问权限能被更直接地限制。系统可迅速地通过投票排除这些节点或对其进行删除。
- 交易对手风险的管理继续在外部进行。但多数分布式账本技术均通过使用实时交易终局性、可验证真实性和其他分布式账本功能来缓释交易对手风险。

主要发现

性能

- 吞吐量、延迟及节点数是分布式账本技术可延伸性及性能的一般衡量标准。只有某些资本市场业务才需要很高的吞吐量。许多区块链用例允许交易延迟。
- 从比特币实施以来，分布式账本技术在性能方面取得了显著提升。大多数分布式账本技术现在都能够在毫秒至秒之间完成交易，处理量在每秒500至5000宗交易之间。此外，在有些分布式账本技术中（如分布式一致），单个账本的交易速度（非分布式共识）达每秒100,000之高。
- 大多数分布式账本技术对数据量或场的个数不实施限制。尽管如此，有些实施受到有效载荷或元数据大小的限制。由于更多的节点被添加进网络，很多分布式账本技术的性能（主要是延迟及吞吐量）因规模越来越大而受到负面影响。尽管如此，我们复核的分布式账本技术中有较高比例显示，规模对系统的性能不存在影响。
- 可扩展性对依赖大量的交易吞吐量的金融服务业务而言十分重要。大多数待建的分布式账本系统遵循行业特定的设计规则，以满足可扩展性和速度以及数据隐私方面的要求。

安全

- 共识机制的安全性尚处于早期阶段，并在不断变化。不同供应商之间的安全功能存在多样性，这是由它们的基础架构和使用的共识机制导致。在大多数情况下，安全测试正在开展的过程中，但还没有达到实施安全强化的程度。从回应结果看，对审计的聚焦似乎已让位于共识机制、安全及其他组成部分。目前采取的方法是建立一个全功能模型并在问题和障碍的基础上对产品进行调整。
- 关于攻击的各种风险和漏洞继续存在。大多数分布式账本技术积极识别此类风险和漏洞，提高技术予以解决。
- 并不是所有分布式账本技术提供商都考虑了其账本解决方案在高度监管的环境中实施所要求的大量安全测试及认证。尽管如此，我们发现一些例子，显示客户已经开始要求安全测试及审计。
- 丢失私钥仍然是分布式账本解决方案的关键风险之一。人们考虑了很多缓解措施，如复位/重新发出钥匙、钥匙磁盘加密、多人签署、将违规的钥匙列入黑名单等。私钥管理服务在未来应有一席之地。

- “重复支出”是一个公认的风险。大多数提供商设计了复杂程度不同的机制，能够在本质上最小化或防止这一风险。

- 很多账本解决方案建立了大量的系统安全性记录，其他的解决方案未来会增加系统安全性记录。

加密/算法强度

- 有些分布式账本技术（如Juno）允许用户按自己喜欢的方式对每个信息加密，CORDA支持N2N数据加密服务。这使得交易对手可以按照隐秘的方式进行交易，不向任何其他方透露内容。其他分布式账本技术（如Chain）不仅对元数据加密，还使用零知识证明来加密隐藏交易中的资产及金额。业界试图寻求共识机制的标准框架。
- 共识机制的主要是在标识待处理交易的“提交”、“安全”或“激活”状态之方法上存在差别。总体而言，共识机制是为所有参与的交易主体提供最终的“完成交易”。
- 针对已许可系统中参与节点的激励的定义取决于金融服务中的用例。通常使用如参与者之间的法律合同、运营目标对节点进行外在的激励。有些分布式账本技术仍然可以通过配置以使用工作证明激励或股权证明抑制因素。这可以通过配置实现。
- 分布式账本技术及其提供商提供钥匙生成编码及数据库，用之可以生成公钥和私钥。在设置节点时可以生成钥匙。私钥可以在本地存储，不需要与节点交换，这与今天大多数公钥架构实施相同。在许多观察案例中，钥匙在现有硬件安全模块架构上生成和存储，以维持适当的控制。
- 分布式账本技术广泛使用了多重错误跟踪的机制，包括监控：失败率和信息处理等，某些分布式账本技术能够提供满足实时需求的错误跟踪和监控功能，另外一些分布式账本技术有订阅机制，可以为所有节点方便读取其他节点的行为变化。
- 很多已实施设计的共识方法属于PBFT的衍生品，允许对很多设置进行修改，以便在某些用例中有更好的表现。

标记化

- 在各种共识机制中, 存在不同程度的自我执行规则, 以确保激励机制使节点的行为诚实和合作。在没有这些激励的情况下, 创造者们走上Ripple/Stellar路线或依靠声誉。大多数分布式账本技术专注于提供跨不同资产的技术层。一些分布式账本技术利用本地加密货币 (如Casper使用Ether, Ripple使用XRP), 而其他分布式账本技术不使用本地加密货币, 但仍然可以提供标记不同资产的能力。Chain使用主传输节点, 以加快处理速度。
- 几乎所有分布式账本技术使用数字签名 (或等价物) 签署交易。因此我们认为这是分布式账本技术的主要参数之一, 有助于人们采用分布式账本技术。

隐私

- 分布式账本技术采取各种措施以保障隐私, 包括:
 - 不将客户数据包括在分布式账本中;
 - 匿名地址

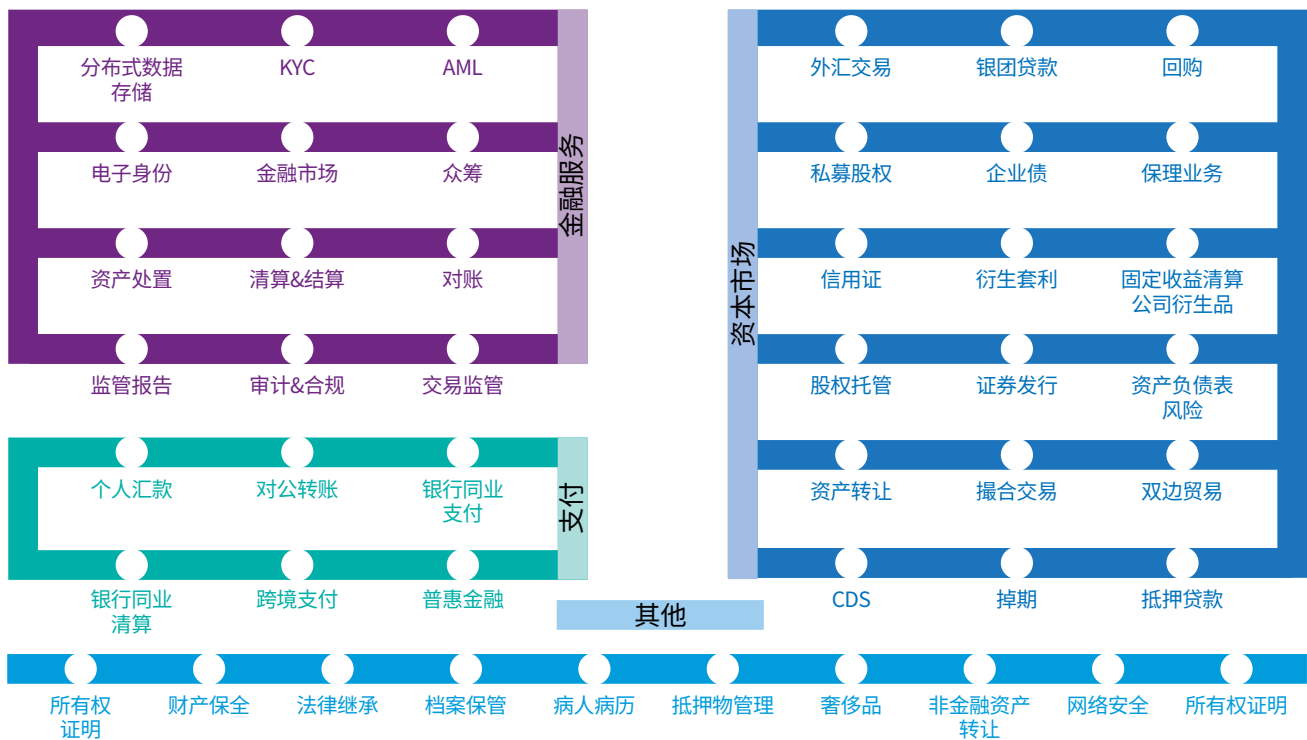
- 加密及权限管理模型
- 零知识证明
- 环签名
- 几乎所有的分布式账本技术都需要通过数字签名等来使用可验证的真实性。
- 节点一般都有一定程度的所有其他交易的透明度, N2N分布式账本技术除外。

执行方法

- 实施成本和时间表主要取决于特定的用例, 虽然许可和部署技术的整体实际成本似乎是可控制的。然而, 针对市场上整个资产类别的分布式账本解决方案的实际总实施成本是很难判断的。
- 不同的用例包括固定收益清算公司 (FICC) 类资产场外交易衍生品和抵押的数字现金、国际收支、加密货币、积分和关于国际互换和衍生工具协会衍生品掉期的智能合同的使用。

图7说明了目前在测试并部分实施的用例的各种例子。

图7: 目前在测试及实施的用例



区块链适合您的企业吗？

很多金融机构正在设法利用分布式共识机制，但是存在很多挑战。监管繁重，成本也是一个问题，金融服务业整体也在快速变化。在进行大量投资之前，金融机构应考虑一些重要问题：

- **范围**：需要考虑哪些因素？
- **交易对手**：哪些实体创建并发布交易？
- **流程**：今天实施的流程与DCL应用相比如何？业务及数据层面的一致意见/共识如何达成？谁被允许验证交易的有效性？
- **数据**：哪些数据需要分享？与谁？什么时候？哪类资产将被转让？应该在何处储存数据？是否需要验证及公证？
- **技术**：现存的基本技术格局如何？将受到何种影响？基本的技术成本如何？
- **人员**：需要哪些技能及组织变革？
- **监管**：该解决方案是否能够帮助我的企业以更有效的方式满足监管要求？
- **行业**：是否有行业驱动的时间要求重新聚焦当前业务，更快更具信任地处理事务？
- **业务案例**：什么是整体业务案例，包括对事实成本的考虑？投资回报如何？是否有充分的规模效应？
- **性能/安全**：解决方案是否满足我的需要？是否满足了我的安全要求？
- 交易记录是否需要引发进一步的事件（智能合同）？

方法：

- 解决关注的问题的最简单方法是什么？
- 分布式账本技术是否是你正在寻求解决的问题的正确的解决方案？你是否甚至需要区块链？如果是，对应的资产类别是什么？处于使用周期的哪一阶段？
- 你正在寻求解决的具体问题是什么？
- 使用分布式账本技术的设计假设及目标是什么？
- 你的用例是否需要不可变性？
- 目前的业务状况是否涉及到第三方？

- 是否了解并信任他们？
- 是否实施了中央权限？
- 用例是否可能需要治理控制框架？
- 你是否同意交易的不可变记录（共识）？

执行：

- 你怎样开头，如何在概念验证以外实施？
- 根据可扩展性、安全性、性能等方面的要求，什么是合适的技术工具包？
- 私人或公用区块链或脱链解决方案？
- 你是否需要一个以上的区块链？
- 你的工作流程是什么？
- 你在何处需要何种共识机制？（或根本不需要？）
- 共识机制需要满足哪些要求？（附录三的问卷可能有帮助）
- 快捷方法中需要测试哪些情景？
- 你如何与监管机构展开接触？

鉴于严格的监管框架、严格的投资预算及大多数企业已经有非常复杂的技术格局的事实，这些措施可能很难成功。同等重要的是，大多数当前的分布式共识账本技术仍然是处于研究中的项目，不可能简单插入来提供解决方案。

任何分布式账本技术都必须确保功能，并为监管者所接受，必须能够与不断变化的需求及技术一道成长——必须“抗未来变化”。鉴于IT部门警惕未来不断增加的成本及技术，任何新增项都必须比现有系统更具成本效率。

目前，不能说哪个共识机制明显优于其他。有的共识机制可能在某个用例上更好，另外的共识机制可能在另外的用例上表现更好。公司需要开展逐例分析，而且这些分析还得考虑到新的机制在不断涌现。

掌控前方的道路

关注哪个共识机制对公司个体最有用，即哪个共识机制能够创建为监管机构所接受的真实及可扩展的解决方案，这极为重要。

分布式账本技术及其基础共识机制已经呈现多样化，但是随着不同用例的制定，还在快速变化。虽然种类繁多，有些东西却是清晰易见的。

与以往一样，如何最好地满足可能不信任他人，但仍希望在没有第三方参与的情况下执行安全交易的交易对手还是最重要的问题。谁是参与者或节点？他们想要完成什么？这些交易对手可能需要一定的隐私保护功能。他们可能想要控制其他节点被允许读或写的内容。在某些情况下，交易对手希望交易中涉及的所有节点都信息对称，或者想确定不同节点的不同级别的信息。

关注哪个共识机制对公司个体最有用，即哪个共识机制能够创建为监管机构所接受的真实及可扩展的解决方案，这极为重要。因此，问题不是工作证明分布式分裂账或许可分布式账本更优，而是特定用例是否需要共识或何时需要。如性能及容量等交易验证及非功能性要求在这一决策过程中也扮演着重要角色。

这意味着确定什么时候真正需要分布式账本，技术使得不再需要中间商，但是在很多情况下，代价是保密性及隐私降低。

因此，对于很多资本市场业务而言，当保密性及隐私极为重要时，区块链将无法在某些要求。只有参与的交易对手可以互动的封闭式系统将依然是受偏爱的选择。

虽然，出于本报告所提及的原因，与开放式公共系统相比，大部分金融服务用例偏好许可分布式账本系统。我们发现，进入公测的公有链应用非常少见，悉尼股票交易所最近也发布公测通告。随着技术能力不断演变以满足严格的行业要求，开放式公共系统在金融服务中的情景如何，尚不清楚。

目前为止，大多数共识模型基于不同行业及行业以外的学术圈提出的理论，在金融服务交易方面的可扩展性上存在困难。金融服务需要每秒处理数以十万计的交易。网络稳定性是主要问题之一。网络必须不停运行，哪怕是停止一秒钟也不行，这极其关键。我们预计，分布式账本技术的性能及延迟将持续改进。但是区块链及分布式账本最终还是存在结构性限制。这可能将其应用局限于在延迟及交易量方面要求不是非常高的用例。

掌控前方的道路

在生产环境中，选择合适的共识机制非常困难。因为大多数理论属于学术性质。真实的世界可以证明理论有误，特别是涉及到像资本市场这样复杂的系统。目前尚处于早期。

大多数分布式账本技术正在被银行用于降低成本，自动化和简化后台操作。应用层以区块链为基础的技术将创造收入。

放弃一种技术而使用另一种技术，在集中和分散账本之间选择，总会做出权衡。隐私及保密性是以透明度为代价换来的，而且因此产生了一套完全不同的要求，可能导致不需要区块链。今天的金融服务业，特别是资本市场，在过去几年是在各种标准上建立的。虽然我们看到财团成立，而且监管机构表示出兴趣，区块链及分布式账本技术的不断扩散还没有显示出真正的标准化迹象，这可能对其应用及监管接受十分关键。

数据存储也是另一个争议的来源。区块链上的每个节点是否需要存储每一份记录？一个具有一定规模的区块链要求节点存储大量节点根本没有参与的交易数据。这是不是在浪费精力和空间？调和不同节点并确保一致性，是否会存在困难？存在区块链上的数据百分比是多少？哪些数据将被散列并在本地存储？如何在区块链上存储数据及将数据复制至区块链是关键的设计特性。

监管机构、财团及行业集团最终可能需要在协议及标准基础之上规定需要哪类共享“编写”数据库。

如果数据存储不能在所有账本节点上复制，而是在某些节点及N2N上复制，这样系统变得更加集中，失去了透明度，尽管保密性及隐私得到提高。尽管如此，如果数据及交易不是分布式，不是时刻需要共识，那么我们就得问一下区块链与现状相比是否具有优势。

尽管如此，有大量用例显示，共识模型及分布式账本（包括区块链）具有根本性优势：

- 当各方需要知道向谁传输了何种数据
- 当相关方需要查看信息并向其市场开放数据

- 然而，这个清晰的价值链，能够有设置权限、资产证券化、风险量化、精准预算、资产分拆等功能。作为一个状态机，它具备了确认交易方的权限和优先级，这里的优先级主要是指：节点的业务处理过程是按照价值链事先确定的业务处理顺序来完成的。

- 当需要不可变的企业间审计痕迹

- 当多方需要直接向数据库编写内容，而无需相互信任，也不需要中间人

什么时候需要共识？系统什么时候应该是集中，什么时候应该是分布式？讨论还在进行中。但是正如我们所证明，存在有效的原因支撑使用这两个系统，具体用哪个取决于单个案例的需要及实施的可能性。

此外，本报告调查的企业同意这一看法，这是明显的。被调查企业根据其所属行业及其需要，采取不同的方法。但是，在所有情形中，它们密切关注安全性、隐私、性能及风险管理。

与此同时，我们发现明显的迹象显示分布式账本技术带来的可能性引起的兴奋正在向金融行业之外蔓延，渗透到大范围的经济环境中。基于区块链的新业务模型正在被开发。区块链及分布式账本技术带来的兴奋将为对资本市场及金融服务中效率低下的流程进行根本性改造铺平道路。这一改造的一部分将超越区块链/分布式账本技术的使用，而是将归于同一框架下。

最后，能否在不同行业开展业务，最终将由哪些共识机制、区块链能够存活下来并被广泛采用所决定。

附录一

主要术语

验证

通过私钥/公钥证明交易对手身份及资产存在性的流程

区块链

维持不断增长的交易记录清单且带有各种防篡改及修改保护措施的分式数据库

共识机制

验证一组价值或交易的真实性及有效性的方法，无需信任或依靠集中的权威；可以在区块链上或没有区块链的情形下建立；存在多种方法

加密

通过Quorum结构及保密码，实施交易完整性验证及密码验证的过程，无需信任或依靠中央权力

加密签名

在用户保留私钥签署交易安全的情况下对数据所有者进行数学验证的一种方法

股权委托证明

股权委托证明利益相关者选择“证人”命令及提交交易，选择“代表”负责协调软件更新及参数修改

分布式账本

与传统数据库不同的一种所有权数字记录，因为没有中央管理权或中央数据存储。反而，账本在对等网络虚拟私人网络中在多个不同节点之间进行复制，且每个交易均使用私钥进行唯一签名

容错

即使在有些组件出现故障的情形下支持系统继续正常运行的属性

联合共识

实现拜占庭协议（共识）的一种方法，其中节点能够分享另一个节点，并在没有直接了解所有其他节点的情况下达成共识

附录一：主要术语

治理

建立分散控制——没有中央权限命令，达成共识时无需其批准。有些类型的共识机制使用选举的领导负责验证及维护在节点之间分享的数据。治理还包括节点进入或退出许可网络。

散列函数

一个应用编程界面通过名为散列的流程为每个文件创建唯一的钥匙或数字指纹。

分级确定键

确定性钱包是指从名为种子的单一起点获取钥匙的系统。种子能够让用户简单备份，在无需任何其他信息的情况下恢复钱包，在有些情形中，允许在不知道私钥时创建公共地址。

账本间协议

将过去遗留的账本与未来的分布式账本连接。

基于领导者的共识

在这种共识中，选举一位领袖并掌控局面直至投票选举一位新的领袖。在这一模型中，领袖负责验证交易的有效性并将数据传送至其他节点。

实时性

指正在发生的数据传输，不是之前发送的数据记录回放。通过混入无法再次复制的数字，使安全传输具有实时性。如果一个节点可以再没有任何失败节点的参与下将新的价值外化，这个节点就具有实时性。有些节点可能会失败。只要大部分节点可用，网络依然能够运营，可以处理延迟性（一个或两个慢速服务器将不影响共识反应的整体时间）。此外，对正在分布的越来越大的账本的网络宽带的影响也需要考虑。

Merkle树形多人签名

支持一群用户使用多个私钥签署一份文件的验证功能。

节点

共识网络的成员或系统；持有账本复制本的服务器；能扮演不同角色：签发、核实、收取、通知等。无论从哪点看，节点可以是一个虚拟机实例。

节点对节点 (N2N)

只有交易涉及的两个节点参与的机制；事实上，它回避了传统的共识机制。

现实标志编号

用于仅一次进入网络的唯一识别器。

已许可

在一个私人网络中，用户设定关于访问、共识机制、治理及参与等的规则。

实用拜占庭容错

这是分布式计算系统的一个特征，容忍一定程度的错误，而且支持该系统继续运行并达成协议。今天，传统的拜占庭共识协议在概念验证设置中扮演着一定角色。在此类设置中，所有节点均相互认识（已许可系统。网络中的已验证及受信任的验证人随机选取，但总是需要大多数通过，对拜占庭伪装者及Sybil攻击有很好的防护性能）。

公用区块链

在这一网络中，所有人都可以通过读取数据、提交交易及参与验证流程参与到这一网络中。

公钥

其他钱包将交易金额发送至这一公共地址。

私钥

唯一与所有者连接且只有交易参与方知道的加密钥匙；秘密地锁在数字钱包中。

隐私

确保只有意向收件人能够读取信息。计算加密领域通过在对应用的沟通中，使用针对特定安全沟通要求的数学公式，解决众多关于分布式共识的安全性及隐私问题。

专有共识机制

唯一的共识模型，用不用现有一致性算法作为基础皆可。

附录二

共识机制 评估问卷

Quorum结构

网络中的节点用于交换发表声明的信息的风格及阶段(可以通过以下因素进行区别:如(节点)领袖选举、领袖类型、验证交易有效性的方法、容错水平、符号的使用、算法的严密性、实时性保障及许可管理)。

远程程序呼叫

一个协议。一个程序可以用它向位于网络中另一台计算机上的程序请求服务,不需要了解网络详情,也叫功能呼叫或子程序呼叫。

轮询调度算法

节点轮流担任领袖的共识机制。

可扩展性

在受到大量运营请求测试时,能够应对、完成逐渐增加的吞吐量并保持甚至提高性能水平或效率的能力。延迟性指交易处理延迟。

安全性

分布式账本的安全性是指保护业务及个人数据以及交易信息的过程。按照非拜占庭式故障,结果的验证应该准确无误;还包括完整性(向接收信息的节点保证收到的信息没有任何修改)及不可否认性(证明发出信息的节点确实发出了该条信息的机制)。安全性可以在其功能中包括数字签名。

Sidechain

将资产从一个机制转移至一个单独的挂钩机制;特殊目的账本。

吞吐量

衡量在规定时间内可以处理多少宗交易的标准。

标记化

在对损害安全性的前提下,使用保留所有必要数据信息的唯一识别标志替代敏感数据的流程。

UTXO:


未花交易,资产可以直接从一个交易的产出传输至下一个效益的投入,每个产出只可使用一次。

附录二: 共识机制评估问卷

框架类型	问卷
 总体共识方法	共识机制使用的基本方法是什么？
	验证一个交易的有效性需要多少节点？(百分比V个数)
	是不是所有节点必须在线系统才能运行？
	算法是否存在网络中的参与者可以提前知晓这一基本假设？
	谁对节点拥有所有权(如共识提供商或网络参与者)？
	共识机制中涉及哪些不同阶段？
	如适用, 进入及退出共识机制的每个阶段需要满足哪些条件？
	如适用, “提议”阶段后是哪个表决流程？
	一宗交易什么时候被认为是“安全”或“实时”？
	是否存在多轮审核, 确定哪组交易能够进入下一轮的共识？
	节点需要多少时间来做出决定？
	在添加一个新的块之前, 确切地说需要多少时间建立共识？
	系统是否包含同步节点决策功能？
	目前及已规划的验证器数量是多少？
	什么是容错?在一切关闭之前, 需要多少个节点同步决定？
	是否存在分叉漏洞？
	对参与节点而言, 许可系统中激励的定义是什么？
	系统在接收数据时遵循什么流程？
	目前如何存储数据？
	一方如何拥有一项资产？


框架类型	问卷
 <p>治理、风险及控制</p>	如何实施治理/控制？
	谁是负责人？网络中发生恶意事件时他们负责什么？法律行动如何发生？
	对于试图更改共识的行为，是否存在内部惩罚机制？
	共识机制怎样允许访问权限？
	对于恶意行为，共识机制如何限制访问权限？
	什么是许可管理流程？添加或删除节点的流程是什么？
	协议如何评估其他参与者的可信度？
	是否有单独的管理/管理员特权？由谁管理？
	是否有节点定义并执行的限制/隐私权利？
	节点或用户是否可以拥有“读取”或“编写”访问权限？在只履行一种功能时（如后台外包），是否要求特定的节点访问权限？
	实施了哪些措施来降低风险？
	对于许可系统，谁管理KYC/AML流程？数据存储在哪里？
	如何处理交易对手结算风险？
 <p>性能</p>	验证交易和/或达成共识需要多长时间？
	关于共识机制能够或将要处理的数量，有哪些一般标准（如交易数量）？
	关于共识机制能够或将要处理的金额，有哪些一般标准（如以美元计的交易金额）？
	如何衡量可扩展性？
	交易中场域的个数是否存在限制？
	如果提高系统的可扩展性，系统速度是否会受到影响？
	同步是否会影响可扩展性？

附录二: 共识机制评估问卷

框架类型	问卷
<div>  <p>安全性</p> </div>	怎样追踪交易活动？
	共识机制是否使用数字签名？
	共识机制如何处理假设的行业标准？
	目前正在解决哪些风险/安全问题？
	是否有计划让应用/共识机制通过认证 (如ISO、SOC等)？
	基础设施的托管选项有哪些 (如云、数据中心托管等)？
	你如何描述目前为止实施的安全测试 (如有)？
	你计划怎样实施/整合数字钱包? (包括私钥管理？
	发生违规时, 哪些数据面临风险？
	系统如何防止签名欺诈 (如钥匙被盗)？
	共识机制是否有全面的记录？
	系统将如何处理一般服务器问题？
	共识机制如何处理“重复支出”的风险？
	系统如何确保网络同步?节点与网络同步需要多长时间？
	节点是否能够访问内部钟表/时间机制以保持足够准确？
	在什么条件下会发生锁定/开启? (即什么是证明安全?)
	灾难恢复的流程是什么？
	正在进行测试的威胁模型是什么?什么被定义为“正常”?如何监控欺诈？

框架类型	问卷
 隐私	系统如何确保隐私？
	系统是否要求节点间传送的信息具有可验证的真实性？
	是否所有节点能够看见其他所有交易？
	如何在应用之间界定和确保隐私？
	数据加密模型的工作方式是什么？
	如果许可网络中发生共识, 是否为每个交易签发随机公钥以增加隐私, 或产生随机CUSIP翻译因素？
	参与者的身份是否向对方隐藏 (如Blackpool)？
 加密/算法强度	密钥如何生成？
	密钥生命周期管理怎样？
	什么是密钥库方法 (library approach)？
	什么是HSM整合方法？
	共识机制是否需要领袖？
	共识机制的严密程度如何？(系统严密程度是硬编码还是弹性编码?)
	目前, 是否通过度量节点行为来发现潜在的系统错误？
 标记化	如何对资产进行符号化 (如适用)？如何简单介绍符号化概念及术语？
	向符号分配了哪些安全机制？
	如何简单介绍符号的生命周期管理流程？
	共识机制是否使用交易签名？

附录二: 共识机制评估问卷

框架类型	问卷
 执行方法	目前正在探索、测试及实施的用例有哪些？
	实施成本有哪些？
	实施需要多长时间？
	是否存在被审核的业务案例，以便将实施成本（包括解决方案成本）与现有流程进行比较？
	你目前与谁合作（如风险投资人、银行、信用卡公司等）？
	参与者的身份是否向对方隐藏（如Blackpool）？

附录三: 问卷反馈集锦

请访问kpmg.com/us/blockchain-consensus-mechanism，
下载问卷反馈集锦。

鸣谢

区块链网络中的很多人士复核并核实了本报告的部分内容,我们想在此对他们的贡献表示感谢:

毕马威: Bob Hayward、KiranNagaraj、Walter Murphy、Mihai Liptak、Roshan Rao、BurakKarvan和Francis Sam Yesurathinam

BigChainDB: Trent McConaghy – gtrent@gmail.com

Bitshares 2.0: Ryan R. Fox – ryan@ryanRfox.com

Casper: Vlad Zamfir – vldzmfr@gmail.com

Directed Acyclic Graphs: Aviv Zohar – avivz@cs.huji.ac.il

Distributed Concurrency: Dan Conner – dan.conner@disledger.com

Evernym: Jason Law – jason@evernym.us
Timothy Ruff – timothy@evernym.us
Drummon Reed – drummond@respect.network

Graphene: Ryan R. Fox – ryan@ryanRfox.com

MultiChain: Gideon Greenspan – gideon@coinsciences.com
Maya Zehavi – mayazi@gmail.com

OpenChain: Flavien Charlon – flavien.charlon@coinprism.com

Ripple: Bob Way – bob@ripple.com

Steem: Ryan R. Fox – ryan@ryanRfox.com

Stellar: Jed McCaleb – jed@stellar.org;
Joyce Kim – joyce@stellar.org

Tendermint: Jae Kwon – jae@tendermint.com

注: Ryan Fox不代表Cryptonomex, Inc., Steemit, Inc.或区块链网络中的任何其他实体。他的回应是其本人在独立研究基础之上的观点。

注: 此版本以英文版本(Blockchain Consensus – Immutable agreement for the Internet of value)为准。

联系我们:

李世民 (Simon Gleave)

毕马威亚太金融服务区域主管

电话: +86 10 8508 7007

电邮: simon.gleave@kpmg.com

北京

张峻铭 (Raymond Cheong)

合伙人

电话: +86 10 8508 5458

电邮: raymond.cheong@kpmg.com

香港

麦高仕 (James Mckeogh)

合伙人

电话: +852 2847 5018

电邮: james.g.mckeogh@kpmg.com

冯翰时 (Simon Phipps)

合伙人

电话: +852 2143 8813

电邮: simon.phipps@kpmg.com

上海

张龙华 (Longhua Zhang)

合伙人

电话: +86 21 2212 3378

电邮: longhua.zhang@kpmg.com

本刊提及的部分或全部服务可能不适用于毕马威审计客户及其附属机构。

本刊所载资料仅供一般参考用,并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料,但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

kpmg.com/socialmedia



© 2016毕马威会计师事务所 — 香港合伙制事务所,是与瑞士实体 — 毕马威国际合作组织(“毕马威国际”)相关联的独立成员所网络中的成员。版权所有,不得转载。香港印刷。毕马威的名称和标识均属于毕马威国际的商标或注册商标