日本交易所集团

JPX

工作报告

分布式账本技术

在资本市场中的应用趋势探索

Masafumi Kondo† , Go Hosaka† , Nobushige Doi† , Atsushi Santo†

2017 年 9 月 14 日

Vol. 20

† Fintech Laboratory, New Business Development, Corporate Strategy, Japan Exchange Group , Inc. (jpx-fintech@jpx.co.jp)

† 翻译：塔链实验室

致谢

我们想借此机会向我们的 PoC 测试合作伙伴 IBM 日本有限公司表示最深切的感谢，同时感谢其他外部专家在编写本报告时的投入和宝贵意见。同时还应指出的是，由于作者的水平有限，本报告可能存在不准确之处，敬请谅解。

目录

I.简介

区块链和分布式账本技术（DLT）是比特币等比较重要的加密货币的基础技术，在金融行业引起了人们的关注，因此，在世界各地的资本市场基础设施上，都实施了大量实验。金融机构，如银行、交易所、中央清算所和中央证券存管机构等都开始研究并测试技术，但他们中的一些最近开始进行联合 PoC（概念证明），或者考虑有限参与者在生产环境中的试点利用。

在日本本土，日本银行家协会（Japanese Bankers Association）宣布[1]，今年秋季以前，他们计划开发一个测试环境，银行可以使用 DLT 共同测试新的金融服务，而 61 个国内金融机构（截至 2017 年 7 月）已经参加了一个联盟[2]，考虑使用 DLT 集中提供国内外交易服务，建立实时及 24 小时支付基础设施。在海外，美国托管信托结算公司（DTCC）宣布[3]，将分别对贸易信息仓库（TIW），信用违约互换（CDS）；澳大利亚证券交易所（ASX）计划[4]在今年年底前就是否实施 DLT 替代其后贸易服务基础设施进行审议。

近期，DLT 的技术发展有一些成果。Corda 于 2016 年 11 月开源，Hyperledger Fabric 1.0 版（“Fabric v1.0”）于 2017 年 7 月正式发布。2017 年 3 月，企业以太坊联盟成立[5]，许多金融机构已加入联盟。摩根大通开发了 Quorum，这是一个基于以太坊的定制 DLT 平台，于 2016 年 10 月在内部运行并实现开源。

2015 年，日本交易所集团（JPX）成立了研究小组，研究了 DLT 在资本市场基础设施上的适用性，通过研究获得的结果和分析，集团成员于 2016 年 8 月发表了报告[6]。而本报告介绍了上一次报告发布后技术发展趋势，以及资本市场利用 DLT 时存在的一些问题，报告还对基于测试的资本市场基础设施的变化进行了预估。

虽然 DLT 已经在许多行业进行了开发和实验，但本报告重点介绍金融业[7]，特别是涉及证券，债券和衍生工具交易的用例。虽然本报告的范围仅限于金融工具的交易，但是我们仍在进行许多有关 DLT 研究，实验也正在进行中。因此，本报告可能存在一些不准确之处，我们恳请您的谅解。如果想要通过新技术的利用大幅度改变企业，必须进行行业范围的知识共享和公开讨论。我们希望这份报告有助于技术进一步地发展，有助于全球 DLT 应用于资本市场基础设施中付出的努力。

---

1 https://www.zenginkyo.or.jp/news/detail/nid/8042/

2 Launched by SBI Holdings, Inc. and SBI Ripple Asia Co., Ltd. in August 2017 (http://www.sbigroup.co.jp/english/news/pdf/2016/0819_a_en.pdf)

3 http://www.dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-solution

4 http://www.asx.com.au/services/chess-replacement.htm

5 The consortium that aims to customize Ethereum, a DLT platform for public use, to meet the requirements from enterprise point of view such as confidentiality and performance

6 http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_No15.p df

7 Development of Hyperledger Fabric is not solely for use by the financial industry.

II. DLT 平台发展

在本章中，我们将介绍 Hyperledger Fabric、Corda 和 Quorum 的常用功能，这些是金融业开发者使用的主要开源 DLT 平台（统称“资本市场的 DLT 平台”）。 对 Hyperledger Fabric 的描述是基于我们的研究和 PoC 获得的结果，关于 Corda 和 Quorum 上的描述则是基于的公开信息。

1.DLT 平台概述及基本功能

(1) Hyperledger Fabric

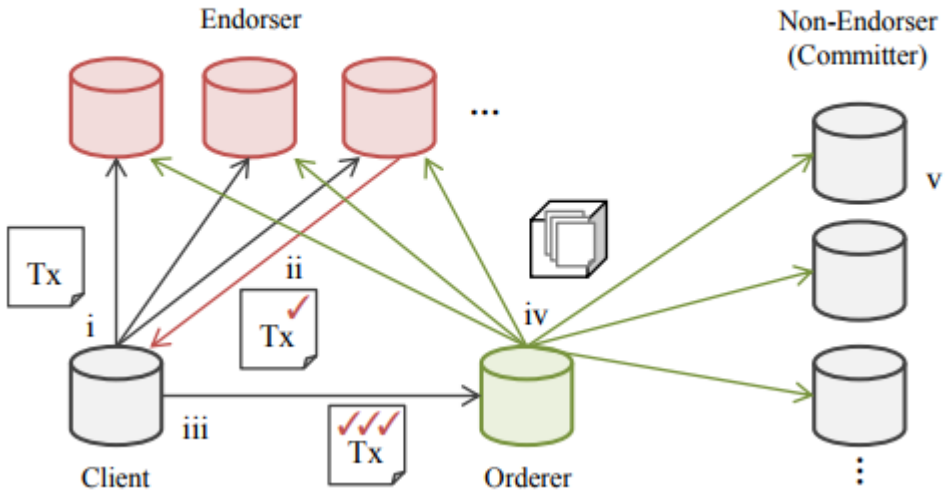
Hyperledger Fabric 是 Hyperledger 联盟[8]（旨在开发开源 DLT 平台和外围工具）开发的代表性 DLT 平台。Hyperledger Fabric 0.6 版本已经被金融机构所进行的许多 PoC 应用，但是 Fabric v1.0 的规格与以前的版本截然不同。Fabric v1.0 的基本组件和功能如下：

- Endorser
执行事务的节点，并将其记过和签名发送回客户端
- Orderer
确定事务序列的节点，并将其作为块广播到 DLT 网络中的其他节点
- Endorsement Policy
用于定义哪个节点是支持者的配置或交易被认可需要多少签名人签名
- Channel[9]
定义哪一组节点共享一个账本的配置

虽然以前的版本使用基于实践拜占庭容错（PBFT）的共识算法[10]，但鉴于其认可策略和数据机密性限制了频道中共享单个账本的节点数量，Fabric v1.0 在共识过程中提供了灵活性。Fabric v1.0 中的交易执行过程如图 1 所示。

[8] To date, multiple DLT platforms have been developed in parallel within the Hyperledger, attracting initial source codes from varied participating institutions.
[9] The execution instance of smart contract (called "chaincode" in Hyperledger Fabric) is created in each channel respectively, and the endorsement policy is defined in each instance.
[10] Process to create consensus among participating nodes on the contents, sequence, and results of transactions.

图1　Fabric v1.0 中的交易执行过程

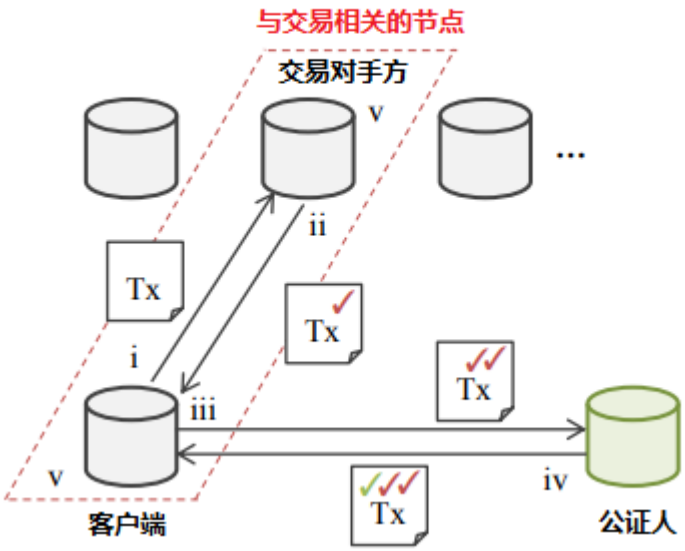


i.客户端将交易发送给 endorsers。
ii. endorsers 执行交易并回复执行的结果和签名。
iii.客户端从 Endorsement Policy 中定义的 endorsers 收集足够数量的签名，并发送带有签名的交易。
iv. Orderer 将交易区块与序列和广播组合在一起。
v.每个节点根据认可政策验证每个交易，并将其提交给相应的账本。

(2) Corda

Corda 是 R3[11] 开发的 DLT 平台，由八十多个金融机构组成（截至 2017 年 6 月）。Corda 采用未用的交易输出（UTXO）[12]作为其数据模型（与比特币相同），并定义了一种名为公证服务的角色，以防止双重支出。公证服务管理以前使用过的交易历史，客户必须要求认证的唯一性，这意味着交易尚未使用，因为在新发行的交易中设置为输入状态的交易。公证服务可以由特定节点作为单个实例或分散地具有共识算法的多个节点来操作。交易仅在与每个交易相关的各方拥有的节点中共享和执行。Corda 的交易执行过程如图 2 所示。

图2 Corda的交易执行过程



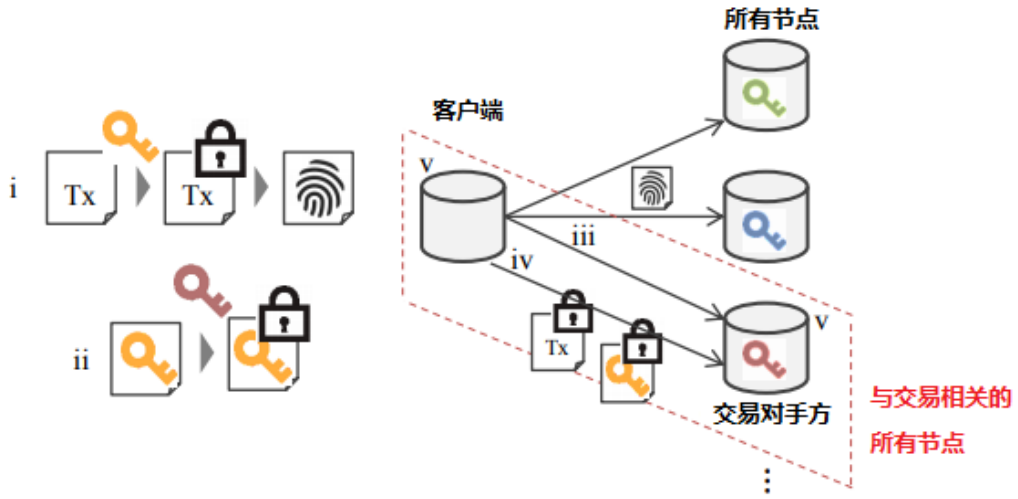
i.客户端将交易发送到交易对手方拥有的节点。
ii.交易对手方确认交易，并携签名回复。
iii.客户端也签署交易，并要求对新发行交易中设置为输入状态的交易的唯一性进行认证。
iv.如果所选交易的输入状态尚未在公证人签署的其他交易中出现，则公证人签署该交易。
v.与事务相关的每个节点执行并将事务提交给相应的账本。

[11] Launched by R3 CEV LLC in September 2015.
[12] Data layout of transactions has input and output states, and the newly issued transaction consumes past transactions as its input states.

(3) Quorum

Quorum 是一个专注于企业的 Ethereum 版本，主要为金融行业提供数据保密。Quorum 有两种类型的交易：公开交易和私密交易。 公开交易的执行过程与 Ethereum 中的相同，但私有事务仅在与每个事务相关的各方拥有的节点中共享和执行，只有加密的私有事务的散列被共享并存储在所有节点之间。Quorum 中私有交易的执行过程如图 3 所示。

表3 Quorum私有交易的执行过程

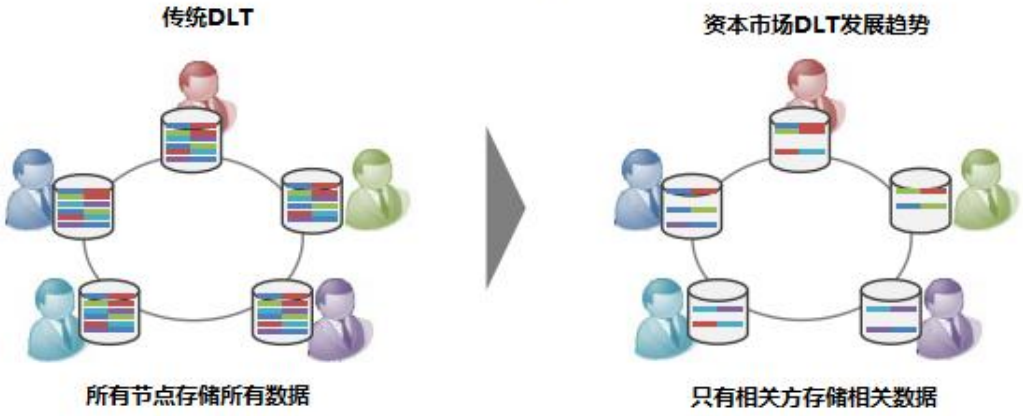


i.客户端生成对称密钥，用密钥加密新发行的事务，并计算加密事务的哈希值。
ii.客户端使用交易对手方拥有的节点公钥对对称密钥进行加密。
iii.客户端将哈希值广播到所有节点。
iv.客户端将加密的事务和加密的对称密钥发送到对方拥有的节点。
v.与交易相关的每个节点执行并在双方同意之后将交易提交给相应的账本。

2.金融行业 DLT 的独特特征

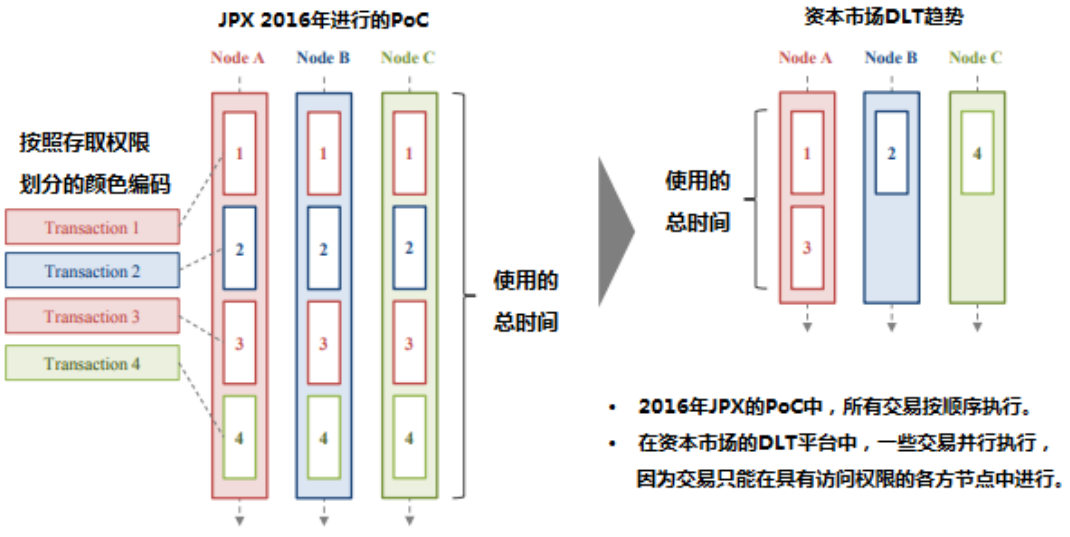
从上一节介绍的资本市场 DLT 平台的特点中可以推测一二，参与者之间的数据保密性在金融行业至关重要。DLT 的原意是能够共享在所有节点之间存储所有数据的共同账本，并且一些 DLT 平台在这样的前提下实现公共密钥基础设施的数据隐私和访问控制。然而，因为账本上的交易和数据需要在执行时临时解密，所以拥有节点的金融机构内部人员存在篡改和窥探的可能性。此外，还存在对现有加密技术的脆弱性的担忧。在这种情况下，有些机构已经考虑利用同态加密，这使得无需解密的计算能够进行 DLT 计算。然而，资产的交易实践比数字货币更复杂，在资本市场上进行同态加密看起来似乎很难，因为无需解密的复杂计算就会导致性能严重下降。因此，在与其相关的各方拥有的节点之间执行交易和存储数据是资本市场 DLT 平台的最新趋势（图 4）。

图4 通过物理隔离数据保密



与常规 DLT 中过程相比，仅在特定节点执行交易证明在性能方面是有利的。如我们在 2016 年发布的报告中所述，当年 JPX 进行的 PoC 期间，在每个节点所有交易的顺序执行导致交易吞吐量瓶颈。DLT 平台资本市场的吞吐量有望得到改善，因为在不同节点执行的交易可以并行处理（图 5）。

图5 交易并行处理

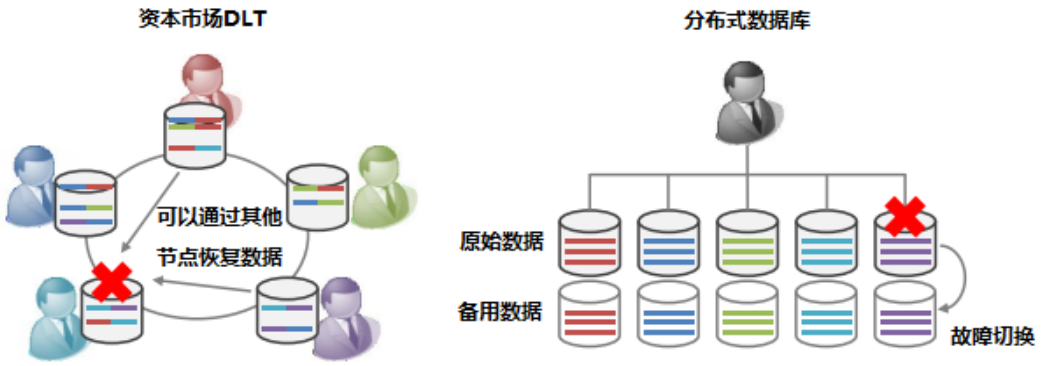


鉴于一个交易不一定在所有节点之间共享，协商一致的过程也发生了变化，这被认为是 DLT 最重要的因素之一。从 Fabric v1.0 的认可政策和 Corda 的公证服务可以看出，DLT 平台的共识规则由用户灵活配置，这些功能也可以通过授权来消除共识过程，仅将事务批准到特定节点。假设 DLT 网络仅由相互信任的现有金融机构组成，简化或省略协商一致的过程似乎是一个可行的选择，因为很难预测由于硬件故障或恶意攻击，某些节点同时会出现异常的情况。追求保密性和性能[13]而不是拜占庭的容错促进了资本市场的最新 DLT 平台中功能和作用的细分。因此，摆脱与传统 DLT 相关的僵化共识过程似乎是自然而然的。

3.现有技术比较

本报告进行了现有技术的比较，资本市场的 DLT 平台从 DLT 的初衷意图大大演进，以满足金融机构的实际需求。在这方面，有些人指出，这些平台现在与现有的分布式数据库[14]没有太大差异。分布式数据库将数据分开分配到由单一实体管理，主要用于性能（负载平衡）和可扩展性的多个不同数据库的技术，通常不提供拜占庭容错。由于用于资本市场的 DLT 平台可实现灵活的一致性过程配置和物理数据隔离，因此这些功能的设计，与分布式数据库将会有许多相似之处，分布式数据库的性能和技术成熟度似乎优于当前 DLT 平台。在分布式数据库中，根据预先确定的特定键的值或范围来分散数据。因此，数据在不同数据库之间不重叠。然而，在资本市场的 DLT 平台中，由于它们专注于关联方之间的数据机密性和无摩擦数据共享，因此可以在一些节点之间共享相同的数据，并且可以在每次交易时灵活确定。此外，在数据可用性方面，尽管在一个节点中丢失的数据可能从资源市场的 DLT 平台中的另一个节点恢复[15]，但分布式数据库方案中的每个数据库都需要冗余（图 6）。

图6 数据冗余运行方式差别



[13] According to the experiment conducted by Bank of Japan, throughput performance deteriorates as more nodes participate in the consensus process. (https://www.boj.or.jp/announcements/release_2017/data/rel170227a5.pdf)

[14] 14 While there have been several types of distributed databases, this report mainly describes the characteristics of Mongo DB.

[15] As described in the next chapter, recovering data from another node has some issues while it seems to be possible in theory.

虽然两者之间的差异可能从数据库的技术特征的角度来看是微不足道的，但资本市场的 DLT 平台覆盖更广泛的服务[16]，可以被视为旨在利用现有分布式数据库技术来提高工作效率的定制包，实现在不同实体之间流动（表 1）。 预计它们将作为可用于各行业的数据库和消息传递中间件[17]而发展。

表1 资本市场DLT vs. 分布式数据库

	资本市场DLT	分布式数据库
主要目的	无摩擦数据共享与数据机密性	性能（负载平衡）和可扩展性
治理	可由多个实体管理	仅由单一实体管理
数据分布性	能够确定每笔交易中的数据共享	根据值或特定键确定优先级
拜占庭容错	可根据用例和网络参与者进行配置	没有（假设由单一实体管理）
数据可用性	可以从其他节点恢复一个节点中丢失的数据	需要在每个数据库中有冗余

III. 研究资本市场的潜在问题

自 DLT 的研究和实验在金融业中普遍开展以来，很多人一再指出，DLT 在资本市场的广泛业务运作中提高效率甚至变革的可能性很大。此外，在资本市场周边监管环境近期发生变化的情况下，通过使用新技术改造现有 IT 系统开发和管理流程的趋势越来越强。然而，虽然 DLT 的 PoC 测试和技术开发已经在世界各地积极进行，但是在生产使用方面仍然存在一些问题。

[16] Not only data base management systems but also virtual machines for running programs as smart contracts, messaging functions among nodes, and developer's toolkit.

[17] General-purpose software that operates common processes for specific types of use cases between business applications and the base layer, such as an operating system and hardware.

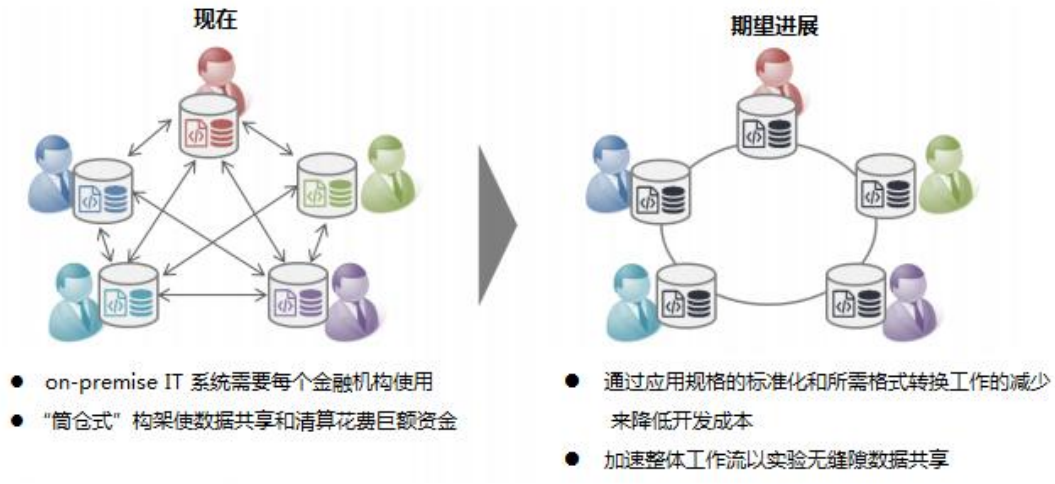
1.复杂的监管环境和 DLT 的期望

鉴于金融行业的 IT 系统需要很强的可靠性，随着时间的推移，一般的共识是金融机构尽可能开发业务应用程序，并自行运行包括硬件在内的 IT 系统。 然而，最近经济/金融环境的变化，乃至金融监管逐渐增重了在各金融机构维护这样的内部信息技术系统[18]的负担。

例如，2008 年的金融危机引发了众多关于金融监管改革的讨论，后来这些改革陆续推出。其中一个例子是巴塞尔协议 III，这是由巴塞尔银行监管委员会（BCBS）领导的一系列金融监管改革，这些改革自 2013 年开始实施，并将于 2019 年全面实施。另一个例子是场外衍生品市场改革，由 BCBS 和国际证券监督管理组织（IOSCO）领导组织，该组织一直在执行有关监管和减少系统风险的相关规定。虽然这种监管改革是在国际合作下进行的，因为 BCBS 这样的国际组织在法规所针对的金融机构上不能合法地执行这些规则，他们所能做的就是向各个管辖区的监管机构提供指导，使规则受到立法程序的约束。因此，虽然每个国家立法相关的法律原则上是相等的，但由于不同国家的商业惯例不同，彼此之间可能存在微小的差异。金融机构，特别是有国际业务机构，在任何时候都必须在多个国家立法规定的基础上，适时有效地调整业务工作流程和信息技术系统，以适应快速变化的法规。

如果 DLT 可以成功应用于资本市场的工作流程，那么相关金融机构业务应用的基本功能和格式将以智能合约的形式进行标准化。在快速变化的经济/金融环境的规定下，各机构对相关工作流程和信息技术系统进行独立修改变得越来越困难。在非创收领域（即后期业务或后台流程）中共享知识和开发/使用应用程序可以降低成本，当然也是有效的解决方案。此外，应用程序的标准化通过减少数据转换来提高操作效率，并且还期望通过 DLT 网络上的相关实体之间的无缝数据交换将实现更快的处理。实现这些方面似乎对于资本市场来说至关重要，因为最近的监管改革已经将运营时间限制得更为严格，如贸易报告或保证金转移，希望减少系统性风险（图 7）。

图7 IT系统面临的挑战及金融行业DLT预期



[18] Refers to IT system hardware that is housed by the service provider itself on its own premises or that is installed and operated at data centers or other similar facilities contracted by the service provider.

2.生产使用中的潜在问题

虽然资本市场的 DLT 平台已经不断发展，注重数据保密性和可用性 ，但我们通过研究和 PoC 发现，随着这些方面的进展，出现了一些新的问题。随着 PoC 和相关实体在具体用例上的并行试点使用，也有必要解决系统架构与现有 IT 基础设施相结合的实际问题，以及开发/运行应用的治理。

（1）保密性

虽然现有的 DLT 通过共享每个节点中的所有数据来实现高可用性和完整性，但是如果每个节点拥有不同的数据，则需要不同的解决方案来保护这些数据[19]。
我们通过使用 Fabric v1.0 下的 channel 进行测试以实现保密性。然而，我们遇到的问题是：在不同 channel 间进行一致的数据交换的特殊节点，对跨 channel 资产转移非常必要，因为目前缺乏跨 channel 连接账本的功能。节点将可能出现单点故障，节点的所有者对于参与者应该是高度可靠和中立的，因为它需要有权访问多个账本上的数据。此外，这种功能应该作为 DLT 平台的基本功能提供，因为如果在每个用例中将其作为业务应用程序开发，软件故障的风险将会增加。

由于 Quorum 使用确定性虚拟机运行智能合约[20]，相同的输入数据和交易总是生成相同的输出数据。因此，私有交易的哈希值和这些事务的顺序在所有节点之间共享并保持一致，作为篡改检测和数据恢复的唯一事实。有了这样的机制，数据验证和数据恢复理论上可以通过在特定节点中，在发生数据不一致或数据丢失时，从每个节点[21]传递交易数据实现恢复。不过，这样的操作本质上是一个保留方法，因为在现实中很难进行这种操作。此外，具有访问所有数据和事务的权限的管理员节点可能是准备数据验证和数据恢复的更实际的解决方案。加拿大银行进行的 PoC 报告指出，为了实现业务连续性，Corda 数据复制机制必须嵌入到每个节点中[22]。

如上所述，即使这些 DLT 平台实现了物理数据机密性的功能，实际上利用所述功能来实现特定角色的实体也是必要的。 预计我们能够寻找像 CCP / CSD，银行或经纪人这样的现有金融机构，信任的第三方可以担当这个特殊角色。但应该注意的是，不要忽视 DLT 的优势。

---

[19] The acronym CIA takes the first letter of the words “confidentiality”, “integrity”, and “availability”, which represent the most crucial components of information security within an organization. More importance had been placed on integrity and availability at the expense of confidentiality in conventional DLT platforms, and this is now changing in DLT platforms for capital markets

[20] Quorum is based on Ethereum, and smart contracts are run on the Ethereum Virtual Machine (EVM)

[21] There have yet to be any experiments that use the actual data; therefore, this statement is based solely on the information and literature that is currently available to the public.

[22] http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf

（2）吞吐量

我们检验了 Fabric v1.0 中的吞吐量性能，与之前的版本相比，其通常表现出更高的交易吞吐量。 然而，我们还观察到性能随着条件恶化，这是由于执行交易之间的异步处理和将结果提交到 Fabric v1.0 上的账本造成的。Endorsers 执行交易并将其结果和签名以及执行时由事务处理器读取的密钥的版本发送回客户端。当每个节点逐个递交交易到一个账本后，orderer 将交易广播为具有序列的块，任何具有早于最新版本的密钥版本的交易都将被拒绝（图 8）。

Figure 8: Collision check of the key at the commit of transaction to ledger

[Use Case: Bank Account (Deposit, Withdrawal, Payment)]

Database: (key, version, value)

Initial Parameter: (Investor A, 1, 10000), (Investor B, 1, 10000), (Investor C, 1, 10000)

*Version is incremented when the value of the key is updated.

If transactions 1, 2, and 3 are issued simultaneously, then the results replied from endorsers will be as follows:

Transaction 1: deposit JPY5000 on investor A

Read {(key: "Investor A", version: "1")}, result {(key: "Investor A", value: "15000")}

Transaction 2: withdrawal JPY2000 on investor B

Read {(key: "investor B", version: "1")}, result {(key: "investor B", value: "8000")}

Transaction 3: payment JPY 3000 from investor A to investor C

Read {(key: "investor A", version: "1") (key: "investor C", version: "1")},

Result {(key: "investor A", value: "7000") (key: "investor C", value: "13000")}

Nodes process each transaction as indicated below for transactions that are sequenced in numerical order by orderer:

1. Commit transaction 1:

Update database {(investor A, 2, 15000)}

2. Commit transaction 2:

Update database {(investor B, 2, 8000)}

3. Reject transaction 3:

* While transaction 3 has read tuple (key: "investor A", version: "1"), the version of the key "investor A" was updated to "2" at the commit of transaction 1.

由于高流量交易中读取的密钥的充分分散，因此没有发生冲突，吞吐量性能优于通过 PoC 在 2016 年进行的 Hyperleder Fabric v0.6 获得的结果。另一方面，当我们注入大量交易来读取相同的密钥，还是发生了很多冲突。 因此，高吞吐量性能尚未得到证实，对系统资源的负担较高。 还应该注意的是，在 Fabric v1.0 中按顺序对每个节点中的分类帐提交交易。 因此，当我们不使用 channel 时，每个节点存储所有数据，所有交易都按照先前的 PoC 顺序进行处理。 这方面需要进一步的改进，因为除了密钥的冲突检查之外，似乎有可能并行处理交易。

（3）系统构架

由于支持加密货币的公共 DLT 网络为用户提供了通过挖矿作为货币激励形式获得这种加密货币的选择，因此是由参与者自己负责维护和运营，而非中央权力机构。 然而，由于本报告主要概述的联盟 DLT 使用案例范围内难以提供此类货币激励措施，因此主要用户在与实现共同目标提高工作流程效率时，将不得不承担相关的基础设施的维护和运营所需的费用。鉴于这种情况，业界一直在考虑利用云服务实施 DLT，减轻节点占有负担和 IT 系统运行负担，简化网络架构。

目前有两种类型的云服务在金融业中引起关注[23]。一种是基础设施即服务（IaaS）[24]，它提供基本的系统资源，如 CPU，内存或存储，另一个种软件即服务（SaaS），它在云环境（或由服务提供商管理的数据中心）上提供特定的业务应用程序。如果用户可以使用 IaaS 在云环境中建立节点，用户可以以相对较低的成本轻松开始使用 DLT 应用程序。由于节点在地理上不是非常分散，所以在云环境中建立节点在网络体系结构方面与在每个单独用户管理的数据中心进行比较也是有效的。即使这些基础设施由领先的云供应商经营，由于灾难或人为错误也会发生数据中心故障。因此，在多个用户各自开发了由云服务的云服务的节点的情况下，应注意不要将大量节点在地理上集中在特定数据中心或由单个云供应商管理的特定区域中相同的云供应商。云服务似乎是 DLT 的一个很好的搭配，组合这样的技术可以降低 DLT 生产使用的障碍。然而，从更广泛的角度来看，不仅要考虑到成本和网络效率，还要考虑基础设施的可用性。

然而，有这样的观点出现：如果云服务在金融行业普遍存在，则利用 DLT 在提高效率并不重要。 实际上，如果所有金融机构的业务应用程序和云端环境中[25]的数据存储都是 SaaS，所有人都选择在具体用例上提供相关的功能，整个金融行业的总成本是合理的。 但必须指出的是，这样的服务将在资本市场上创造一个新的单点风险，并且从中长期看来，也担心这样的服务提供商可能会由于获得主导地位而产生巨大的影响。

（4）治理

由于 DLT 是使相关实体使用相同的基本应用作为智能合约的技术，因此开展和维护应用程序的治理也是应用中的一个问题。 在利用 DLT 优势的同时，对业务工作流的重构似乎是必要的，用户之间的协作和共同审查联盟中的规范对于成功的应用来说肯定很重要。 开发智能合约的 DLT 平台和计算机语言也应该是开源的，以吸引来自具有共同愿景的利益广泛利益相关者的参与。

---

[23] There had been a longstanding bias against cloud services in the financial industry in terms of information security. However, now that major cloud service vendors have an ample track record of providing a high level of cyber security by studying and testing with top global talents in this area, there is growing acceptance and even support for utilizing cloud services in the industry.

[24] When useful tools are incorporated into development of applications for such functionalities as DBMS, calculation, and analysis in addition to basic system resources, it is commonly referred to as Platform as a Service (PaaS); however, in this report, PaaS and typical IaaS is collectively referred to as IaaS.

[25] If the functions of some work flows in the financial industry were provided as SaaS and became prevalent, we could expect benefits from standardization of applications and frictionless data sharing that are comparable with that of those realized by DLT. Moreover, SaaS providers would be able to manage system resources and data redundancy efficiently in a centralized manner.

鉴于在现有资本市场上实施 DLT 需要非常高的可靠性，因此即使在开源开发的情况下，特定实体也应对应用程序的质量负责。 针对比特币社区最近与规范变更相冲突的情况，可信赖的第三方以任何方式参与联盟是可取的，因为不通过任何调解解决这种冲突而很困难，而这些冲突一定会在用户之间发生冲突 ，用户恰好是商业对手。 如本章所述，在考虑实际操作时，网络上也可能需要信任的第三方在保密性方面利用资本市场的 DLT 平台上的独特之处。现有行业协会或市场基础设施经营者可以担任这些职务，但联盟成员相互建立新的实体机构也是一种选择。

为提高行业效率，建立以中立角色服务的实体是资本市场向前迈进的方式。因此，有些人认为，可信赖的第三方利用 DLT 是多此一举。然而，有可能通过使用 DLT 开发更具弹性的工作流程，运行成本更低，同时也减少了可信赖的第三方为基础设施运行所承担的责任。可以利用现有实体之间的长期和深厚的信任建立治理结构，使行业受益，缩短 DLT 应用的道路。在现有资本市场上实施 DLT，转变可信赖第三方的作用对于建立更有效的基础设施是很必要的。同时，通过使用 DLT（如初始代币提供（ICO））从零开始开发金融服务，可能会在与现有资本市场完全不同的分散式治理结构下发展。

IV.结论

本报告根据上一次报告发布后,市场快速变化的监管环境，基于进一步研究和 PoC 的调查结果，介绍了资本市场利用 DLT 的技术发展趋势和一些问题。 最后，我们要评论我们对未来资本市场基础设施变化的预期，以及 JPX 最近关于 DLT 的举措。

1.资本市场预期变化

预计资本市场周边的监管环境将继续快速变化，金融机构将越来越多地在非创收领域开展合作，提高运营效率，预计新技术的使用将成为催化剂。考虑到今天技术的成熟度，我们还预测云服务的使用将会扩大，以提高 DLT 之前 IT 系统运营和业务流程的效率。例如，由 SWIFT 于 2017 年 2 月发起的全球支付创新（GPI）[26]新服务，通过在云环境中分享有关银行的信息，实时追踪跨境付款进度，越来越多的服务为 SaaS 的金融产品的后期交易过程提供了各种功能。另一方面，如果包括关键业务在内的广泛功能可以在云中运行，那么应该仔细考虑一下，由于拥有大量 IT 专家的大型金融机构使用云的优势相对较低，预计 IT 系统和云服务暂时将同时使用。即使在这种情况下，DLT 作为商业应用的基础平台，无论个人用户的 IT 系统架构如何，都可实现无缝数据共享和数据完整性。事实上， CLSNet[27]是由 CLS 银行开发的新服务，将为用户提供两种连接服务的选择：一种是建立一个自己的节点，并通过 DLT 网络进行连接，另一种是连接到由 CLS 银行，通过传统 SWIFT 渠道管理的服务器。此外，如果技术进一步发展，不同 DLT 网络之间的联系也将得到实现，除了密码货币的持续发展外，技术还有可能为支撑现有金融服务的基本面带来革命性变化。

---

[26] A project that aims to improve transparency and traceability on cross border payment, and also considers the future use of DLT (https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi)

[27] A service that provides matching and netting functions for various FX transactions across more than 140 currencies .(https://www.cls-group.com/ProdServ/Pages/CLSNet.aspx)

如本报告所述，由于资本市场的 DLT 平台为了满足金融机构的实际需求，已经远超出 DLT 的原始概念，所以认为这些平台与现有技术没有太大的区别。 然而，对于新技术的用户来说，这是非常有意义的过程，主动研究新技术，并根据实际需要向开发人员提供反馈。 我们相信，即使新技术与现有技术没有太大差别，通过在这个行业中实施生产用途的新技术，对稳步发展的金融服务至关重要。

实施 DLT 到资本市场的努力已经从来自于加密货币的灵感革命用例转变为现实思想，首先是通过利用现有金融机构和市场基础设施运营商之间的信任来提高业务工作流程的效率。由于这种转变，热情有所简化，金融机构的努力可能逐渐缩少。在开发任何新技术的过程中，这种预期的起伏都可能会发生，鉴于金融科技运动推动更复杂的金融服务，有必要继续探索中长期的 DLT。

本报告主要涉及私有链或者联盟链类型用例。对于诸如加密货币等公共服务，尽管突出了许多问题，但我们不应忘记在世界的观望，它们一直在增多扩大。灵活服务设计的智能合约与加密货币的结合为金融服务带来了新的可能性。即使我们继续追求提供良好的金融市场基础设施的使命，对于我们不断问自己目前提供的服务是否真正有益于我们的用户，将变得越来越重要。

2. JPX 最新动态

据了解，为了在资本市场上进行 DLT 的生产使用，持续的技术考核和行业范围的讨论是必要的。2017 年 3 月，JPX 开始了一项新的计划[28]，正式接受来自广泛的日本金融机构参与全行业合作如 PoC。三十三个参与的金融机构（截至 2017 年 9 月）已经能够通过一个仅在联盟成员的网站进行沟通，供 DLT 讨论和信息共享。 TSE 还发布了演示应用程序[29]，实施了证券市场的基本功能，促进了参与金融机构 DLT 的共识。参与者或其他 IT 厂商也可以提出与资本市场有关的使用案例，并与其他参与金融机构进行需求调查。最近，我们看到用例逐渐增加，在 JPX 计划范围内，有兴趣的金融机构中[30]有两个已经升级到共同的 PoC 阶段。

随着信息技术的发展，各种服务都迅速变得更加方便，现在的资本市场基础设施越来越难以应对周边环境的变化，这是由于多年来变化和功能增加累计而成的复杂孤立的 IT 系统导致的。全行业的复杂性或基础设施的更换也似乎很难，因为每个金融机构自己开发其 IT 系统或 IT 供应商向每家公司提供不同的服务。然而，如果现有的参与者可以合作利用新技术分享知识，我们可以期待实现迄今为止被认为难以实现的变革思想的进展。自 DLT 开始引起金融业关注以来，金融机构共同努力的事实是积极变化的迹象。随着各种技术和业务领域的不断发展，我们希望通过建立新的文化，加快开放创新，实现金融服务的可持续发展。

---

[28] Jointly conducted at JPX by Tokyo Stock Exchange, Osaka Exchange, and Japan Securities Clearing Corporation.

[29] Based on the application developed in PoCs conducted by JPX in 2016 with a publically accessible demo video (https://youtu.be/Gqbjp4JlqRk).

[30] One project is related to the post-trade processes for Japanese stocks suggested by Daiwa Securities Group Inc. The other is related to Know Your Customer (KYC) operations jointly suggested by SBI Holdings, Inc., SBI BITS Co., Ltd., and NEC Corporation. JPX supports these joint PoCs by providing an environment to deploy and test DLT applications as well as the consortium-members only website to facilitate communications.

塔链实验室面向金融科技最前沿的话题，以详实的资料、独特的视角、深刻的思想，全面提升客户对金融科技的认识，提供金融科技领域准确、可信的专业化服务。

作为塔链科技旗下的前瞻性研究机构，秉持“让世界互信互联”的宗旨，为合作伙伴提供可信数据管理方案和服务，创造信息时代新价值。

联系我们：info@towerchain.com

扫描二维码

关注“塔链实验室”公众号