Corda 分布式□本平台：□介

Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn

2016 年 8 月

Abstract

由相互不信任□点□成的分布式□本可提供一个全局性□一数据□，用于存□机构与个人之□交易和□□的状□。目前□了保持各个独立□本之□数据同步，需要大量耗□的人工工作，而分布式□本可淘汰其中很大一部分。□也将提高金融□内□行的代□共享水平，以降低大众使用金融服□的成本。本公司推出 Corda—一个□了□□以上目□而□□的平台。本文□一般□者提供高水平的介□，而即将□布的技□白皮□会□□□述 Corda 的□□理念与基□框架。

Contents

1 引言

我□ R3 □信，分布式□本技□有潜力□金融服□行□□来□革，使□内客□与相关公司□益。我□的愿景是：未来金融□□将得到准确的存□与自□管理，每个人都能无□无□地□理任何契□或合□。我□相信未来市□□□将是：参与方达成的金融合□一旦被□□，就可以被准确无□地持有和共享。重复、□□、匹配失□和数据□坏都将成□□史。以□□□代表的孤□将不再出□。

我□期望依□已□被□明的技□，在□有的法律框架内，□金融服□□景□建一个共享□本架构。我□的理念可分□以下三□：□足机构的工程需要、关注非功能性的需求、可□展性。

本文介□了 Corda 平台的□□特点，我□相信□个平台□金融机构会是非常不□的□□。[a]

2 背景

□行□敢于突破□□思□，□早地利用信息技□，将手工□理精确地自□化，将物理□理精确地数字化。然而，我□仍有机会改善□些新□架构的成本与效率。

□得一提的是，每个金融机构都以自己的角度□□着□□客□群和交易□方□□、地位的□本。同□，交易□方也以自己的角度□□着□□一个□本。□种重复会□致□□的不一致，需要交易各方耗□高昂成本来□行□□、□□和□□。□同一笔交易，双方□知存在差异也是一个□□，并且可能是系□性□□。

多个金融机构的存在会促□□争，多个技□平台的存在□会增加复□性，□生运□□□。然而一直以来，□些□□不可避免，除非采用集中化的市□基□□施。由此看来，□□依靠合作公司提高技□而不提高自己的水平是行不通的。

集中化市□基□□施在提高机构□数据与商□□□共享度方面已有成效，但整体上看，金融交易□域的整合水平仍然□□低于网□□代的信息交□水平。

我□相信加密技□的□步，例如通常□到的区□□技□，提供了一个新的机遇：机构□安全共享□□的□威性系□。通□建立一个□□金融交易、□理商□□□的全新共享平台—一个可□□企□□所有□□的、□威性的全局性□□□本，□金融机构□（特□是但不限于交易后服□）的□□活□□来□革。□个架构会□金融行□□来一个全新的共享平台，□个平台之上的新老参与者及第三方都能展开□争，□相提供□新□品和服□。

[a]□者可通□□件□系作者：Richard Gendal Brown (richard@r3cev.com), James Carlyle (james@r3.com), Ian Grigg (iang@r3.com), Mike Hearn (mike@r3.com)

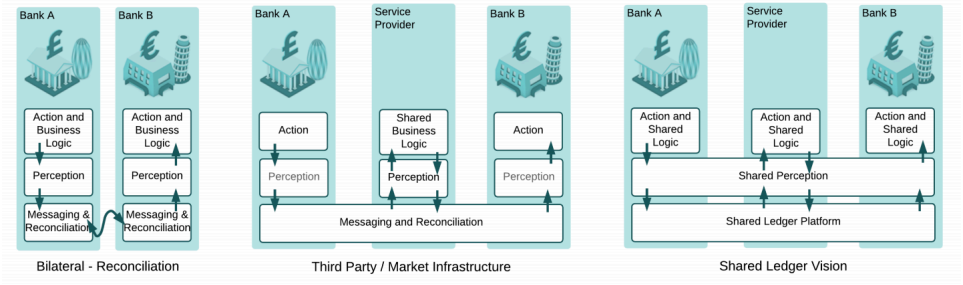


Figure 1: 上□所示，我□展示了三种状□的□化□程。第一种是参与方各自□□并管理自己的□本，□理所引□的不一致性和重复□□（“双□－□商”），第二种是参与方将关□□理□程的□□委托□集中化服□商（“第三方／市□基□□施”），□化到第三种，□是各方在开放性与□争性基□上，使用新老服□提供商及市□基□□施提供者的服□，合作□□一个共享□本，保□各方□□的一致性。

我□相信，更高□量的数据、更少的差异和更快的企□达成□□速度，将□来成本的大幅□□。而且，各个企□若使用□个共同架构，会形成一个新的平台□新老金融服□商展开□争，更好地服□客□需求．未来，□□的平台也有可能在企□内部□用，□在企□内部用多个系□□□同笔交易，也是造成成本上升、操作复□的一个主要原因。

3 愿景

□期来看，我□可以□想借助“全局性□□□本”，使所有□□活□参与者充分互□，任何参与方均可通□一种安全、一致、可靠、私密、□威的方式，来□□和管理彼此之□的□□。之所以称之□全局，是因□呈□□每个人的数据都是一□的；之所以符合□□，是因□其物理方式的□□会有所差异。最□可能形成的状□，将会是企□内部□□的□威□本系□被淘汰，由企□□可共享的全局性□威□□系□取而代之。

3.1 □□原□

如果使用分布式□本技□，□□原□包括：

- □本上□□的事□无□在任何争□□合，都可被各方看作具有法律□束力的可用□据。
- □□在□本上的事□是具有□威性的，而非存□在□□的□威数据的”影子“，因此直接通□平台便可达成决定。
- 参与方一旦达成□□，□本上的□□就是最□且不可□的。□□或解□唯有通□后□交易来□□。□将促使公司不得不通□改□内部工作流程来提高准确度和□量□准。

- 原□上，任何授□参与方都可以直接□□□本，并通□□本来□□与交易□方达成的□□。任何参与方都不用被迫与其他方打交道，但是分□或等□制的市□模型可能会越来越少。

- 通□提倡开放式的□准和私密性的□□，新老金融服□提供商都可以□□互□，展开□争，提供差异化的服□，从而利于客□自由□□，促□□内□争。

- 唯一能□□金融交易内容的是参与方本人，和其他具有合法知情□的人。

然而，□个愿景的最□□□需要□渡状□，比如最初只关注共享商□□□的参与方。□有的系□在可□□的未来将会一直存在，意□到□一点，在□□解决方案的□候就需要把□有系□的共存、整合与移植作□一个基□。□些□渡状□也可□来可□的价□，同□□期愿景的法律和其它非技□性□□也可着手解决。

需要□□的是，我□的□期目□是□□一个全局性□□□本，但是最后□□的可能是多种形式的分□□本。也□最后的情况是一种□□□□□□一个□本，□本的匹配具□自主性和灵活性，又保□不同商□服□□功能上和操作上的独立性。

支撑□个愿景的架构和□略□□包括：

- 只有□其管理的□□与□□有法定□益的人□能□□□此系□管理的□□。

- 此系□管理的□□的□□将由□算机代□描述，□段代□必□□得相□法律文件的合法授□。

- □了确定如何□理合□失□□□，此系□提供了□合□代□升□的支持，以及关于争□解决流程的明确参考。□是因□就算在自□□定下，技□和人□因素也会□致出□合□争□情况。

- 成本、□□和□管□担（包括□本、流□□金和运□□□）的降低，□新□品和服□的出□，就意味着我□的愿景得到了成功□□。

- □了□□整个金融界的广泛□用，本系□的一部分必□且将会保持开放：开放源□、开放研□，开放□准。

- □然此愿景使用到了□如一个”平台“或”系□“的□□，我□□□□□□□仍是多□□的，可能由多个技□提供商□争或合作提供不同□成部分。□者不□□想象我□把□个系□□□成了一个完全□一垂直整合的模式。

- 此愿景□意味着，□品高□□所包含的知□□□可由参与建□的企□或□□持有。

- 基于日益□重的网□犯罪和□峻的网□安全形式，本系□会采用高□准的安全□□来□□。

我□□□，□□此愿景所必需的基□技□□明已□存在，包括但不限于：□达的加密技□，全球通信网□，金融工具定□的□准以及保□全局一致性的有效算法。

最近公众□分布式□本和区□□系□大□关注，□造了使□一愿景能被公开□□的□境，而且多个金融机构已□建立了□同行□的合作□盟关系，□些都□此愿景的□□成□可能。在此愿景的□定下，□个网□的参与者□有一个身份□□的基□架构，但是至于架构的复□程度于操作方式尚无□定。□管□的参与是□个平台□□□程的关□因素。

我□□□存的分布式□本平台□行了需求分析和□估，得出□□：目前尚没有任何平台能□足我□提出的需求。本□上来□，支撑□□分布式数据□系□□□的威□模型并不适用于我□目前面□的状况：□互不信任的法律□体达成一致（就是□区□□技□可以做到交易可信□而不需要第三方担保）。□行的区□□系□架构也不适用于我□的要求，无法做到在□独法律□□□面上□行有限制且□慎定□的数据共享。所以，我□□□并着手开□了 Corda 平台。

4 Corda 平台

Corda 是一个用于□□和□理金融□□的分布式□本平台，它的□□就是□了□□本文所描述的愿景。

Corda 平台支持智能合□，符合 Clack，Bakshi，Braine 的定□。智能合□既可由□算机代□自□□行，也支持人工□入及控制的□作，其□利和□□由法律条文明确表述，具有法律效力。智能合□把商□□□和商□数据关□到相关的法律条文上，以保□平台上的金融合□能□力根植于法律上、具有□行效力，若各方存在模糊性、争□性或不确定性□，就有相关的法律依据可循。

4.1 主要特性

Corda 平台尤其适用于受□管的金融机构。它很大程度上是受到区□□系□的启□，但又摒弃了很多不适合金融□景的□□区□□□□□□。

Corda 提供了一个运行智能合□的框架，具□以下关□行□和特点：

- 通□基于□有合法框架并与□有和新□法案兼容的方式，□□和管理两个及以上可□□参与方的金融□□和其它共享数据的□化。
- 去中心化控制的公司□工作流□□；
- 在个人交易□面而非全局系□□面上，支持企□□达成共□；
- 支持□入□管以及□督性□□察者□点；
- □在交易参与方之□□□交易的有效性；
- 支持多种共□机制；
- □□自然□言法律文□与智能合□代□之□的□性关□；
- 使用符合□□□准的工具；
- □格控制数据□□□，□□有明确授□或□□上有□□□的用□开放；

Corda 平台的□些□□特性，适合复□的金融服□机构。□注意，此□□没有使用原生加密数字□□，也未□全局性交易□置速度限制。

4.2 概念

我□首先是使用了全局性□本的概念：可靠的□一数据源。然而，在我□的模型里，交易和□本条目并未全局可□。当交易□□生在小部分参与方之□，我□努力把相关数据□置□□□部分人可□。

在我□的的□念里，基□□象是一个状□□象，是一份□□两个或多个参与方之□□□是否存在、以及□□内容和当前□□状□的数字化文档。□文档□与有合法理由□看的用□共享。在一个各参与方无法可□全部数据的全局化共享系□中，要保持数据的一致性，我□主要依□安全的加密哈希算法来□□参与方和数据。□个□本，□被定□□一个不可改□状□的□象集。

我□依据□□状□来□□和思考，我□的目□是□了确保在□□状□□化□程中，所有□□的参与方能□保持共□。可以□□□是区□□概念的本□：确保不同角色持有的数据，在数据更新中持□保持一致性，□是保□可靠交易完成的基□：从□□的□□支付到复□的智能合□交易。

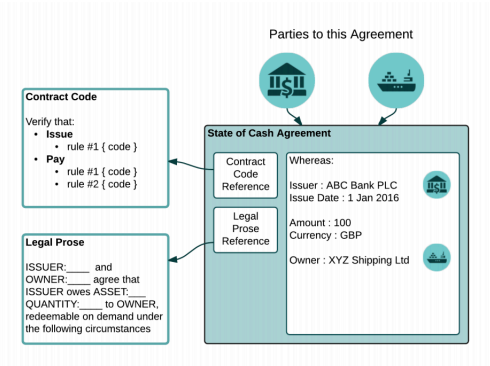


Figure 2: 上□所示的状□□象，代表某个虚□的航运公司在一家商□□行□有一□ 100 英□的□金索□□。状□□象通□哈稀算法□□其□□的法律文件和合□代□之□的□性关□关系，同□通□合□代□控制其□□。

与其他系□相比，我□□注于□□状□，而其他系□中参与方必□达成共□的数据是整个□本的状□或整个虚□机的状□。Corda 平台提供三种主要工具来达成全局分布式共□：

- 智能合□□□，根据□先□定的□□，确保状□□化的有效性；
- 唯一的□□戳服□，以消除冲突同□保□事□□序性；
- 一个□□流程□理框架，以□化多个参与方之□复□多步□□定的□写□程。

4.3 共□机制

在 Corda 平台中，□□的更新要通□”交易“，交易会覆盖已有的状□□象，生成新的状□□象。共□机制可分□两个方面：

1. 交易有效性：参与方通□□□相关合□代□成功运行并持有全部必需的数字□名，便可以确□□期更新的可定□□出状□的交易是有效的，并且任何与之相关的交易都是有效的；

2. 交易唯一性：参与方如果确□□交易是所有□入状□的唯一使用者，即可确□其唯一性。也就是□，没有其他交易可以推翻我□之前达成的共□（有效性和唯一性），使用同一状□。

参与方通□独立运行相同的合□代□并□□其□□性，便可□交易有效性达成一致。然而，就交易唯一性达成共□，需要一个□先□定的□察者，很多情况下要求□察者具□独立性。

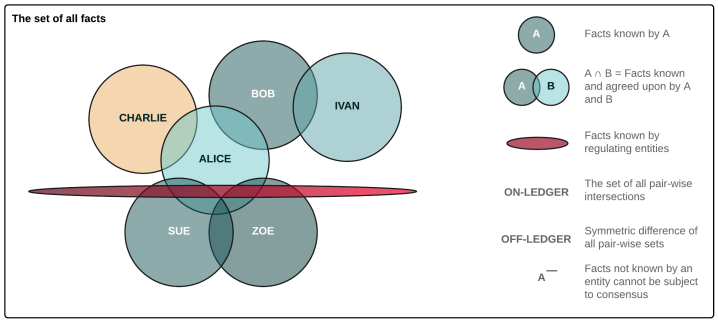


Figure 3: 上□所示，□□交易参与方才能就交易有效性达成共□。因此，数据□□需要□看的参与方共享。而其他平台一般在□本□面达成共□。所以，Corda系□中的任何角色，都只能看到整个系□管理的全部数据的子集。如果系□中至少两个角色就一份数据是否存在和□□□□达成共□，我□就称其□“□本上的数据”，系□允□任意□合的角色参与到所有指定数据的共□建立□程中。□被唯一角色□有的数据，被称作□“□本之外的数据”。

Corda 提供”可插拔“的唯一性服□，旨在提高□私性、□展性、法律系□兼容性和算法的敏捷性。□一服□可能由众多相互不信任的□点□成，□些□点通□一种拜占庭容□算法□合在一起，或可能非常□□，像一台□独的机器。在某些情况下，例如状□的□化需要全部相关参与方□名，□□候可以不需要唯一性服□。

需要重点指出的是，□些唯一性服□□用于□明某个状□的□化是否是因□某个特定交易的□生引起的；它□不需要□明交易本身的有效性，那是交易参与方的□任。□意味着，唯一性服□不需要□□任何交易的完整数据，与其他分布式□本和区□□□□方案相比，大大提高了系□的□私性和□展性。□□□□决策，是在共享□本框架中做出□衡的重要抉□，我□即将□布的技□白皮□会□其作更□□的□明。

4.4 商□□□

Corda 平台通□智能合□代□□行商□□□，由一段□函数构成，只用来接受或者拒□一次交易，可能是由更□□和可复用的函数□成。□些函数将交易解

□□，通□□用（智能合□）命令来使用□入状□并生成□出状□，如果□期操作有效，□接受□□交易。合□定□了□本的部分商□□□，而且具有灵活性：某些配置里各个□点将会在沙箱内下□并运行合□，并不需要□□，尽管我□的□想是□管□境下的 Corda 平台配置将使用□名代□。

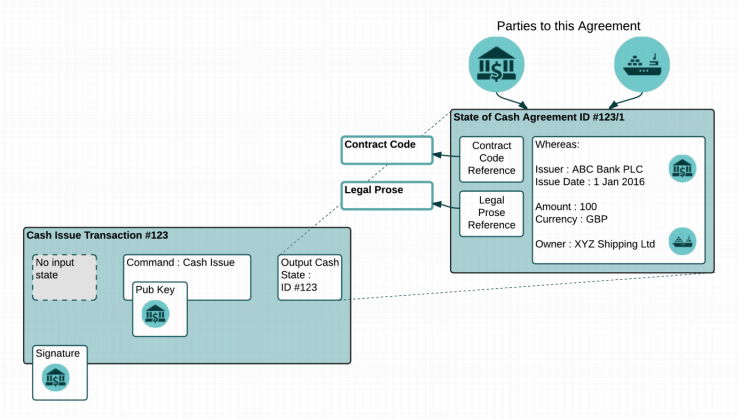
我□□□ Java 虚□机来□行合□及□□有效性，因□ Java 虚□机有多个已有□和丰富的技□□累，并且利用已有□□□准，便于□行重复利用□有合同内代□。不□，我□□ Java 虚□机增加了一个定制沙箱，比普通的 JVM 沙箱□格得多，不□□行安全需求，□支持确定性□行。跟以太坊一□，□□□准化字□□集 Bytecode 集而不是某一□□程□言，可允□用□在合□□言□□方面□行□新，或根据自身喜好复用已有□程□言。□也便于用□直接使用内部程序的合□代□，一旦合□通□□□便可使用，□将大大□化□用开□□程。

4.5 核心金融概念

Corda 的基□架构深受三个架构□域影响深□的用例影响，被□□具有代表性的共同□□，也可能是有所□□性的。□三个用例包括：□金，□券托管和衍生品合□。在所有三个用例中，我□□想它□□金融□□的案例：

- □金余□（例如："我与以下□行达成一致，□行欠我一百万美元"）
- □券托管（例如："我与以下托管□行达成一致，我□有以下公司的 1000 股股票"）
- 双□衍生品□□（例如："□行 A 和 B 同意他□是以下利率互□□□（IRS）的参与方，□意味着他□在□定□□根据□商一致的清算公式□以下□金流□行互□"）

就□些例子中的一个而言，Corda 的□金□□□商□□□□行了明确建模，"□存在□行中的□"的概念不复存在，只有所有者□一家指定机构的□金索取□的概念。所以，我□的核心□金合□极其□□却不失□大：我□□□□金□行者的法律身份、□□种□、□金数目、□金所有者（其他信息比如索取□的性□，明确指定管理此□□的法律条文，法律条文也会□明□生争端后的解决流程），在□些基□上建立其他所有与□金相关的概念（支付、□算和其他）。



上□展示了一种最□□的 Corda 平台交易：□行交易。我□□□生成一个新的□金状□，由一家商□□行□行□一家虚构的航运公司。□□行交易由□行□行□名。从□个□□模型，可以构建出更复□的交易，例如支付、□□□付合□和期□。

Corda 模型□□我□模型的核心概念是：

- 状□□象：代表两个及以上参与方之□的□□，由机器可□的合□代□控制。合□代□引用并旨在□行人□可□的法律条文。交易：通□生命周期□化状□□象。
- 交易□定或商□工作流：在无中心控制的情况下□参与方可□□操作。

有□□性地□格限制可用的□程技□，□决定□最大化，但是可共享的状□数量必□最小化。

状□□象（数据）的□合、合□代□（允□性操作）、交易□定（商□□□□排）、任何必要的 API、□包插件、UI □件，都可以被□□是一个共享的□本□用程序，或 Corda 分布式□用程序（CorDapp）。□是一个核心的□件集，是平台上任何一个合□开□者都期待去□建的。

5 Corda 平台与其他平台的□比

Corda 平台的□建得益于我□与金融从□者的广泛合作，□□更是始□□□着他□的需求。当然，Corda □□灵感也来自于以往的成果，包括 Todd Boyle 和 Ian Grigg 在□文中关于三式簿□的介□[1]，以及已有分布式□本平台（例如比特[2] □和以太坊）的相关因素。因此□也便于不了解 Corda 的人借助□些平台来更好地理解 Corda。

5.1 与比特□的□比

Corda 与比特□有以下几个□著相似点：

- 通□交易□建和使用的状□不可□的，□是一□的；

- 交易有多□□入和□出。比特□有□会用“未使用的交易□出集”（UTXO 集）指代□本作□□果□出；
- 合□是□函数；合□并无存□功能，也不能与任何其他事物□行交互。□于同一□交易，合□的“□□”函数永□□出相同□果。

然而，比特□交易有□一且□格的数据格式，而且除了比特□数量和相关使用□□（脚本），只能保存极少的数据。曾有人□□打破□种限制：通□在合□代□的半□准化□嵌入数据，以便可以通□模式匹配来提取数据，但□种方法并不有效。相比之下，Corda 平台内的状□可以包含任意□型的数据。另外，Corda 平台上的交易不□可以□用□入合□，也可以□用□出合□。比特□交易的确□机制□由已使用□入状□的合□代□控制。而 Corda 的“合□”概念，指的是可以□理各种任□的一系列商□□□，而不限于交易□□。比如，□在 Corda 上的合□□包含生成有效交易的代□（一般在比特□中被称作“□包代□”）。

比特□脚本只能□取一串固定的字□数□作□□入□。□意味着合□无法判断整个交易的□构，□合□的功能造成了极大限制。而我□的合□是□灵完整的，可使用任何普通□程□言在 JVM 上工作。Corda 允□在交易中指定任意精确的□□□界，而不依□挖□□生区□的□□。□至关重要，我□□想的□多合□□型也支持必要精准□□，同□也因□我□主要的共□机制□行方案是使用区□自由的冲突解决算法。□里需要□□的是，Corda 并未使用工作量□明机制（POW），也没有“挖□”的概念。

5.2 与以太坊的□比

和以太坊相似，Corda 平台上的代□运行在相□□大的虚□机上，并能包含复□的□□。可用非□□程序□□□言□写合□程序。二者都旨在□不同□型的金融合□建模。

然而，以太坊中的“合□”是指程序的□例化，每个参与□点都□其□行复制和□□。□种□例化非常像面向□象□程中的□象：可以接收和□送消息，更新本地存□等等。相比之下，我□□智能合□的□行方法用代□表示是一□函数，其中□有一个函数用来保持系□同步（□□函数）。□函数是□函数而且无状□（比如，它不可能与系□的其他部分□行交互）。因□合□没有任何□型的可□存□器，因此没有“消息”的概念。以太坊宣称自己是不限于金融□□的平台，理□上可以□用于各行各□。而我□的 Corda 平台□不考□非金融□用，至少前期如此。

6 路□□

□了达成□□□□□方案，我□首先用代□模□并□制了 Corda □件的□品原型□，以□□□□概念的方方面面。Corda 模型有望在中短期内交付，以下是 Corda 模型的部分（并非全部）□展方向。

- 交易分解与□化唯一性服□：整合多种机制以有□□地□藏部分交易，包括唯一性服□的模糊□理；
- 合□□□沙箱：□式□接最小的 Java □白名□；

- 基于插件的□包，用于位置推理；
- 数据□或网关□□所属（或其他）商□□□□行者（比如中央机构或估□代理方），参与方在□本上可□□□行者身份。
- 使用 Corda 模型来管理用□身份;
- 互操作性和数据集成：尤其参照 FpML 和 ISO20022，支持其他数据格式和其他平台的集成或互操作性；
- □涉及的数据构建□用程序；
- 使用技□来□化□私性，比如不□□分布地址、零知□□明和□□□行方案等；
- 未来金融工具的参考合□；
- 原生支持□□□合□□的商□□□，比如状□□象的聚合。

7 □□

相比□有的分布式□本和区□□平台，Corda 平台的□建有着明确的目的，即□□和□行注册金融机构的□□□□，而并非□所有□□提供解决方案。因此，Corda 的数据分配和交易□□均独辟蹊径，但仍保持了分布式□本的特性，金融机构也正是因□□□特性才□ R3 之□□目□生□趣，□而言之，就是采取一种自□化且可□施的方式来确保金融□□的可靠□行。

Bibliography

[1] Grigg. Triple Entry Accounting. `http://iang.org/papers/triple_entry.html`, 2005.

[2] Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. `https://bitcoin.org/bitcoin.pdf`, 2008.