JIBREL NETWORK

2017年5月

第二版草稿

YAZAN BARGHUTHI
yazan@jibrel.network

VICTOR MEZRIN
victor@jibrel.network

摘要

Jibrel Network 旨在促进货币、债券和其他金融工具等传统资产在区块链上的数字化、上市与交易。Jibrel DAO可让平台使用者存入现金、货币市场工具或创造自己的“密码编译存托凭证 (CryDR)”，从区块链上 / 区块链外套利交易获益。过度暴露在数字货币的去中心化机构与资金，可通过稳定资产对冲持仓并保护资金。此外，Jibrel 会为开发人员提供完整平台，建构运用资产担保的代币凭证进行交易、投资与对冲的工具和应用程序。

另外，Jibrel 还能通过点对点 (P2P)、企业对企业 (B2B) 或消费者对商家 (C2M) 等渠道，以法定货币 (fiat) 对法定货币交易的形式做到实时、几乎零手续费的全球付款与汇款。

本白皮书概述了 Jibrel 的组成核心组件、组件间互动的方式，并意图展示如何使用现有基础架构高效建构网络。

1. 介绍

在 2009 年因为比特币 (Bitcoin) 而为人所熟知之后[1]，区块链 (Blockchain) 已展露巨大的价值。我们能够透过这项新科技，在无法变更的去中心化账本中验证并认可交易，还能更广泛的应用，以达成去中心化一致性。

这项令人难以置信的创新内容目前正逐渐让我们摆脱对全球各产业内中介机构、结算/清算公司与中介服务供货商的需求，一步步改变着这个世界。

话虽如此，但由于仅能在机构层级实行，因此加密经济的大部分价值仍仅限定于特定使用案例或地理区域。此外，也由于这些经济孤岛 (Silo) 在传统资产与数字资产之间转换的挑战与限制带来瓶颈，而普遍有着体系风险。

即使传统经济与加密经济之间有着差异，但前者所遭遇的难题仍困扰着后者。希望在各种传统货币之间互相转换的使用者，当合并使用加密货币兑换、传统金融机构以及付款处理单位时，同样会面临一样的时间延迟与应支付的手续费。

此外，能够促进传统资产在区块链外快速流动的传统个人与机构投资者，也由于现有的基本不兼容性（尤其是缺乏透明度与极端的市场波动）而不想参与[2]。

最后，通过众售、去中心化资金和密码编译投资人筹资的去中心化组织过度暴露于数字资产与加密货币，限制了向传统持有形式多元拓展的选项。

数字货币扮演多重角色这件事让风险进一步加剧：数字货币被用来奖励促进交易的矿工，是转让价值的手段、是投机性的投资工具，最近也被用于群众集资与去中心化组织和应用程序的营运（例如去中心化运算[3]、去中心化储存[4]）。

在传统金融中，上述各功能都使用不同的工具，且受到相应的监管。这样有助于管理体系风险。在充分建立去中心化监管共识协议之前，加密经济面临未受监管汇兑方面的安全性与诈骗风险，也由于这种极度波动的货币被用于设计目的以外的用途而产生市场风险，更由于通过这种高波动性数字货币进行群众集资以及后续受到智能合约的约束而衍生出体系风险[1]。

本报告分析了目前环境的限制与挑战，并提出运用现有基础架构为所有利害关系人提供解决方案的方法。

2.传统资产担保代币凭证

Jibrel 生态系统的核心利害关系人有：希望获得加密货币与区块链技术所创造价值（例如低汇款手续费和及时转账等）益处的非投资型使用者；希望从新兴加密经济获得高报酬的传统投资者；希望以稳定的低收益资产扩展其加密持股的去中心化组织 / 基金和密码编译投资者。

让区块链获得传统金融工具的稳定性，能成功满足所有利害关系人的需求。以他们所代表的基本传统资产一对一支持打造栓式凭证，就能达到这个目的。通过这种方法，可将栓式凭证用来表示货币[5]甚至商品[6]。

1 项目有着无法实质化的风险，因为若资金由于市场低迷而减少，可能导致无偿债能力

只要开发出能够持有传统资产同时核发基础资产拥有权凭证的“担保人”，就能让货币、商品、货币市场工具和其他金融工具广泛的在区块链上公开交易。

3.系统架构

下节概述了 Jibrel Network 的关键元素，以及有助于将传统资产放到区块链上的必备因素。

3.1公开区块链

虽然对另一个区块链的依赖会带来大量新的挑战与限制，但直到完全跨链通讯可行之前，早期版本的 Jibrel 仍需要公开而安全的区块链。

3.2加密货币汇兑

加密货币汇兑为一般使用者提供了使用当地货币的法定货币账户，以及持有加密货币的数字钱包。用户可购买、交易或传输数字货币，在加密货币与法定货币之间轻松转换。

3.3栓式凭证

若要建立传统资产担保代币凭证，需要栓式凭证。对于所持的每一笔传统资产，必须打造一个栓式凭证。基础资产售出时，凭证就会销毁。

3.4担保人

为确保栓式凭证有相应价值，需要担保人。担保人会持有传统资产并核发相应的栓式凭证，同时也会在基础传统资产的拥有权被释出 / 移转时，对凭证进行赎回或销毁的操作。

3.5应用层、链接库与范本

一旦奠定栓式凭证，就能运用其功能开发一系列应用程序，包括付款处理工具、汇款钱包与交易平台。为利于迅速的应用程序开发，需要一个专属应用层，提供易用链接库与程序代码范本。

3.6拥有权移转

核发栓式凭证后，就能以所有加密货币的类似方式，轻松交易其基础资产。高阶流程概述如下：

1. 使用者将法定货币 (FIAT) 传给担保人
2. 担保人给使用者 jFIAT
3. 使用者以 jFIAT 付款给商家
4. 商家兑换 jFIAT
5. 担保人将法定货币转到商家账户

有了担保人支持栓式凭证，保证基础资产能于未来时间点兑换，凭证就能维持在系统内，运用于区块链上与区块链外的付款。

3.7费用与收费

数字与传统资产的拥有权移转都会产生费用与收费，应予考虑。

3.8监督 / 监管

代表区块链外拥有权或价值移转的所有区块链上交易，都必须满足国际与当地法规，且必须受到相应的管理。

应拟妥法规协议 / 管理工具，确保正确的管理与监督。

所有交易必须满足 KYC / AML 规范。

4.JIBREL NETWORK 实施方式

本节概述 Jibrel Network 中实施各元素的方式。

4.1以太坊 (Ethereum) 区块链

所选区块链必须与采矿奖励以及系统参与者之间的基础交易拖钩。因此，以太坊很适合构成 Jibrel 基本架构的基础。采矿奖励会采用以太坊“Gas”（燃料，工作量衡量单位）的形式提供，而任何栓式凭证都不会与采矿流程有关[7]。

虽然 Jibrel 也适合以比特币的 Omniprotocol 当作基础来打造，但这已超出本文讨论的范围。

4.2密码编译存托凭证 (CryDR)

CryDR 是代表 Jibrel 所持有基础传统资产拥有权的栓式凭证。在本文中会以 jAsset 表示（例如 jUSD、jEUR、jGBP）。发行当时，Jibrel 会支持六种法定货币以及两种货币市场工具，日后规划新增其他金融工具。

4.2.1货币 / 法定货币

Jibrel Network 的第一个开发时程旨在支持美元、欧元、英镑、俄罗斯卢布、人民币和阿联酋迪拉姆，且会在整合策略性汇兑合作伙伴时逐渐新增其他货币的支持。

4.2.2货币市场工具

稳定的低收益资产是 Jibrel 的核心产品服务，密码编译投资人可购买“美国国库券”与“零息存款证明”的栓式凭证。在 Jibrel Network 的第一个开发时程中，所有货币市场工具都会包含*自动转仓*或*累积*机制。也就是说，从期满投资中收到的法定货币会自动重新配置到相似资产中。同样的，红利或利息也会累积到基础资产期满或售出为止。在日后版本中，将可配置货币市场工具。

4.2.3其他金融工具

在未来，随着传统金融机构整合到 Jibrel 平台，将能充分支持其他金融工具，包括上市与私募股权投资。

4.2.4智能循规

由于 CryDR 可充分编写，因此可嵌入监管成份。法定货币将不受限制，但其他资产的购入与转售将受到类别与地理区域的限制，以做到充分合规。每份 CryDR 都嵌有这样的逻辑。

4.3Jibrel DAO

Jibrel DAO 会代表传统资产的拥有者接收 / 持有资产，并核发相应的 CryDR。之后立即传送到拥有者的钱包。赎回凭证后，凭证会遭到销毁，其基础资产会移转给凭证持有人。

虽然 Jibrel DAO 以完全去中心化为目标，但在传统金融机构充分整合到区块链上之前，系统的大型元素仍必须位于区块链外。区块链外的活动需要当地与国际监管机关的投入与监督。

因此必须妥善管理利害关系人互动，确保彻底遵守法规且不致牺牲透明度与可靠性。这一点会通过*资产入口网站 (Asset portal)* 达成，也就是于各自地理区域营运、充分合法的专属实体。

4.4资产入口网站
在将传统资产转换为区块链上数字资产的过程中，资产入口网站被用来进行必要的法律与金融步骤。

法定货币入口网站将会是简单的加密货币汇兑。可以就现有交易所建立起策略性合作关系，也可打造充份分布于各地理区的 Jibrel 专属汇兑网络。此外，将一部分的 Jibrel 法定货币储备金保留在现有交易所中，能大幅降低转账时间与费用，同时为交易所提供所需的流动性。

非法定货币入口网站必须位于区块链外，才能进行必要的尽职调查，取得非法定货币存款的拥有权。

在大部分的地理区域，资产入口网站需要经纪人与资金拨付执照。若涉及管制严格的司法管辖区或更细微的金融资产，可能需要监管机关的全面介入与监督。

随着法规的演进，资产入口网站将能够去中心化并由社群主导。机构投资者与其他金融机构将能使用 jibrel 平台将其传统资产上市到区块链上。

4.5Jibrel Network 凭证 (JNT)
虽然非法定货币入口网站会以法定货币收取*脱机费用*，但 Jibrel DAO 的区块链上费用与佣金将以 Jibrel Network 凭证 (JNT) 的形式收取。

5.基础架构

用户余额和交易等关键数据会储存于区块链，其他数据则寄存于开发服务器上。

现在已开发出多种开发环境、工具与架构，能做到去中心化应用的迅速开发[8]。Jibrel 必须研发类似的开发人员组件、工具与架构，以广泛采用与散布 CryDR。

基础架构必须跨两大主要领域：区块链上 API 与区块链外 API / Utils。

5.1区块链上基础架构
网络只需要四份密钥智能合约就能有效运作。

5.1.1CryDR 智能合约
在 Jibrel DAO 注册的每笔资产，都具备一份以智能合约形式核发的 CryDR。CryDR 智能合约会符合 ERC-20 标准。在用户帐户之间转送 CryDR，会类似于在钱包之间转送其他 ERC-20 凭证。

5.1.2Jibrel DAO智能合约
会有一份专属 Jibrel DAO 智能合约规范 CryDR 智能合约的运作。

5.1.3董事会智能合约 (BODC)
董事会智能合约 (BODC) 是互动 / 影响 Jibrel DAO合约的唯一机制。

BODC 会受到投票系统管理，其中董事会成员可使用自己的以太坊帐户就 BODC 行动进行投票。成员必须对私钥的储存与使用负责。在理想状况中，董事会将由密码编译思想领导者和金融服务专家所组成。

图 1密码编译存托凭证——一般流程

5.1.4助理 / 公用程序（辅助智能合约）
我们也必须建立许多辅助智能合约才能提供辅助功能，例如在执行不同版本的合约之间转换，以及启用其他 API 功能等。

其详细描述超出本文讨论范围。

5.2区块链外基础架构
为了促进将 CryDR 广泛采用于交易、投资与对冲工具上，会发行适用于应用程序开发人员的易用链接库与程序代码模板。

图 2 Jibrel DApp API 工作流程

5.2.1链接库与范本
我们希望开发人员使用现有链接库与以太坊区块链（例如 JS web3）互动。我们会发行这些链接库与程序代码样本的包装函式，简化与 Jibrel DAO 和 CryDR 智能合约的互动方式。

5.2.2CryDR 档案总管
我们会建立开放源码档案总管，让使用者检视 CryDR 元数据、与 BODC 互动，以及手动验证 Jibrel DAO 基础资产的拥有权。

5.2.3董事会工具组
我们会建立工具，作为 CryDR Ltd 内部 IT 基础架构与以太坊区块链之间的接口。尤其会用于董事会成员与 BODC 互动的筹划，以及系统状态的运作状况监控。

6.智能型监管的实施

本节概述 Jibrel Network 内 CryDR、智能型监管与法规遵循的实施方式

6.1CryDR 架构
CryDR 本身就是部署至以太坊区块链的智能合约。为了做到稳健而可扩充的系统，CryDR 应满足多项需求：

高兼容性：应使用与现有凭证管理工具兼容的 ERC20 接口
可更新的商业逻辑：应可轻松更新，以跟上不断演进的实际规则与规范
不变性：部署之后就不应改变
可移转：事件与储存内容应分开存放
互动功能：CryDR 之间应能彼此互动

6.2现有方法
这些技术需求很难使用以太坊生态系中目前能使用的工具达成。智能合约的升级难以实施，而虽然目前已有特定工具和方法，但各有其限制。

6.2.1EVM DELEGATECALL
第一种可能的方法运用以太坊虚拟机 (EVM) 中的“DELEGATECALL”运算码。

这虽然是更新商业逻辑的强大工具，却有许多缺点。具体而言，一旦部署，整个更新过程中都必维持原始智能合约的储存架构。因此，这种方法只能用于简易可升级合约的实施，无法用于 Jibrel 的使用案例。

6.2.2智能合约删修
另一个可能的解决方案是删修合约并部署另一份新合约到相同的地址，保存事件与状态。虽然这对于 Jibrel Network 可能会是理想的解决方案，但 EVM 中尚未实施。

6.3Jibrel Network 方法
在打造 Jibrel 时，我们运用一套更加繁琐但全面化的解决方案——我们将整个系统解构为多份可彼此互动、提供流畅升级与更新的细致智能合约。

这样的实施复杂度更高，但能为 Jibrel DApp 提供强大的后端。

6.3.1CryDR 3 层系统
CryDR 可解构为其关键组件：

储存（Storage）：放置所有数据
视图（View）：第三方合约与网络应用程序的接口
控制器（Controller）：实施法律合规与商业逻辑，协调储存与视图合约

图 3阶层式架构

6.3.1.1更新法规遵循性
有了这个架构，我们就能轻松部署全新 CryDR 控制器合约，配置要使用这个新控制器的视图与储存合约。

这样能让我们有效的轻松更新支持 CryDR 的基础法规遵循与商业逻辑，我们称之为智能型监管。

图 4控制器更新

Jibrel Network 藉由促进让商业逻辑得以更新的流程，能够随着实际法规的变革一起演进，确保凭证能够充分合法。

6.3.1.2升级接口
使用此架构，还能让我们流畅升级凭证接口，例如可提供新凭证标准（如 ERC223）的其他支持。

图 5视图升级

进行这类升级时，CryDR 储存会维持不变 / 不受影响。

因为视图的阶层在控制器之前，因此所有事件在更新过程中都会维持不变。实施完善的控制器会触发所联机的所有视图，让客户端可以接收到所有事件。

图 6触发事件

6.3.2智能型监管的架构

实施 KYC/AML 措施需要严格而详尽的账户许可控制。
智能合约有着先天限制，主要是这种合约只能存取区块链上的数据，原始设计禁止合约呼叫第三方服务。

为了存取区块链外数据，必须先以交易形式将数据推送到区块链上。

简单来说，所有法律合规措施都必须通过智能合约实施于区块链上。

为了实施 KYC/AML 措施，我们必须实施两种解决方案：

数据储存：将用户数据储存于区块链上
规则实施：在各交易上套用 KYC / AML 规则

许多项目都处理第一项任务，如 Civic 和 uPort 等。但这些解决方案是专为适应性与多用途而打造，所以只能储存一般用户信息，不足以满足机构等级的 KYC / AML 处理需求。

因此，Jibrel 会建立专用的法规遵循 API，在专用 Jibrel KYC / AML 模块与目前可用第三方解决方案之间扮演联系功能。

图 7 Jibrel 法规遵循 API

6.3.3Jibrel Network 凭证 (JNT) 的角色

Jibrel Network 的其中一项关键商业需求，就是所有的 CryDR 都必须栓定于某笔基础资产。为了达到这一点，区块链外资产必须先进行证券化，这也是需要虚拟兑换货币的原因。除了要与网络进行交易，还要促进区块链外费用的付款。

比特币 (BTC)、以太币 (ETH) 等现有货币并不适合，因为这些货币的价格波动与 Jibrel Network 中的效用无关。这样的脱节带来了市场与信用风险。此外，Jibrel Network 旨在于未来提供专属区块链，须有专属凭证才能促进流畅的移转过程。

CryDR 本身由于必须一直栓定实际资产，不适合用于此解决方案。在付款流程中运用 CryDR 会导致另一方面的脱节，造成系统失衡。

Jibrel Network 凭证 (JNT) 会当作网络的“燃料”或称为“Gas”。JNT 会为 Jibrel Network 及相关 Jibrel DApp 提供的所有功能给予通用存取权。

JNT 会确保所有 CryDR 始终都栓定个别的基础资产，增加额外一层法规遵循性。

图 8 Jibrel Network 凭证互动

7.充分去中心化的运作

在短至中期内，会需要区块链外活动，以进行必要的法律与金融尽职调查，将实体资产转换为数字资产。此外，也需要董事会成员监督 Jibrel DAO，确保充分透明度与遵循法规。

长期来看，法规应会演进而能够促进资产拥有权的区块链上验证，让 Jibrel 成为去中心化自治组织。

7.1自助式入口网站
区块链上运算能力、实施复杂零知识证明的可行性[2][9]、取得相关授权的法规障碍等技术限制一旦获得克服，Jibrel 就能营运自助式入口网站网站（即托管于区块链上、与 Jibrel Network 通讯的传统兑换平台）。

这些入口网站的建立对于 Jibrel 达成充分去中心化非常重要。

7.2区块链上数位身份 / KYC / AML
虽然目前有许多区块链上数字身份与 KYC 解决方案，但其功能仍然有限。需要更先进的身份解决方案，才能做到自助式入口网站。

7.3董事会去中心化自治组织
一旦营运达到稳定状态，就能解散董事会，以自治监管实体取代董事会的功能来监督 Jibrel DAO 的营运。

8.使用案例

可轻松汇兑的传统资产担保凭证提供了广泛的使用案例

8.1传统 / 数位资产汇兑
让传统资产和数字资产得以自由互相交换，本质上就能将传统投资工具大规模销售给寻求稳定数字资产的投资者与实体，为机构投资者开发出一个促进低风险、高报酬的平台。

8.1.1投资平台
客户可将货币市场工具或商品存进Jibrel DAO，再将

这些产物 (CryDR) 以较高价格销售给去中心化组织与基金，*从区块链上 / 区块链外套利* 获益。

8.1.2对冲凭证
去中心化自治组织与基金可购买货币市场 CryDR 并存放于区块链上，有了充分透明度，可让投资者安心确认自己的资金安全无虞。去中心化自治基金可从广泛的传统资产中选择，以补足其数字产品组合，并防止加密经济衰退。

8.2全球转账
提供资产担保凭证可让平台得以提供同时具备传统资产（尤其是稳定性与全球采用）与数字资产（不变的特性、易于移转与可靠）优点的凭证。

有了这些凭证，就能实施付款网关、汇款管道与其他金钱转账等使用案例。

8.2.1汇款
Jibrel 能够让法定货币和法定货币间使用密码编译基础架构执行交易而进行转账，做到汇款功能。用户可运用数字货币提供的低廉费用新增资金并转账给世界上任何一个人，同时享有传统货币的稳定性与安全性。

8.2.2通用钱包
可建立货币不可知钱包，让使用者自由转换货币，并以任一种货币转账给任何地点的任何人，不致被收取这类交易一般需要的高额手续费。

8.3跨境付款
同样的，Jibrel 也能提供跨境付款功能。

8.3.1货币 API
有了基础凭证，Jibrel 就能提供货币 API，让使用者在各种货币间自由转换。

8.3.2商家 API
Jibrel 可为商家提供简单易用的付款网关，接受任何货币的款项，并以当地货币对外支付。无须汇兑或转账费用。

一旦建立起网络，商家就能使用 Jibrel 的易用链接库和 API，设定货币不可知付款网关。

2 虽然目前在改善可能性核对证明 (probabilistically checkable proof) 的效率方面，已经花费了很大努力，但这种方式仍高度不实用

9.引用

[1] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008 - URL - {https://bitcoin.org/bitcoin.pdf}

[2] Brennan and Lunn, Credit Suisse Equity Reports - *Blockchain - The trust disruptor: Shared ledger technology and the impact on stocks*, 2016 - URL {http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf}

[3] Golem, *The Golem Project: Crowdfunding White Paper*, 2016 - URL {http://golemproject.net/doc/DraftGolemProjectWhitepaper.pdf}

[4] Wilkinson, Shawn, *Storj Project: A Peer-to-Peer Cloud Storage Network*, 2014 - URL {https://storj.io/storj.pdf}

[5] Tether Ltd, *Tether: Fiat currencies on the Bitcoin blockchain*, 2016 - URL {https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf}

[6] Eufemio, Chng and Djie, *Digix: The Gold Standard in CryptoAssets*, 2016 - URL {https://dgx.io/whitepaper.pdf}

[7] Buterin, Vitalik, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2013 - URL {http://ethereum.org/ethereum.html}

[8] Solidity, *Solidity: A contract-oriented, high-level language for the Ethereum Virtual Machine*, Release 0.4.10 Documentation - URL {http://solidity.readthedocs.io/en/v0.4.10/}

[9] Ben-Sasson, Chiesa, Garman, Green, Miers, Troma and Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 - URL {http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf}