

CHAINLINK行业报告

超越通证资产发行

互操作性和现实世界数据如何解锁通证资产的真正价值



WITH CONTRIBUTIONS FROM



PAXOS



BACKED

APRIL 2024

目录

综述	1
市场机遇	2
资产通证化的优势	4
实时结算	4
公正客观的记录	4
全球流动性	4
可组合性	5
应用广泛	5
通证资产对资产管理者价值	6
通证是链上金融原语	7
预言机概述	8
通证资产概览	9
通证资产的分类	9
资产通证化的流程	9
当前的通证资产类型	10
稳定币	10
基金	10
债权	11
大宗商品	11
房地产	11
碳信用	12
Chainlink：为通证资产经济提供必要的基础设施	14
Chainlink平台	15
互操作性	17
准备金证明	19
数据服务	22
身份验证	23
自动化	26
市场对Chainlink DeFi收益指数的需求	27
抓住通证化机遇	28

综述

对于资产管理者和理财顾问来说，数字资产既是宝贵的机遇，也是巨大的挑战。一方面，客户对数字资产的需求与日俱增。数字资产通过通证化，为客户带来了创新的技术和金融服务。另一方面，许多传统资产管理者在这个领域的认知有限，很难有效评估底层基础设施的安全性和风险，也很难与数字资产交互。

通证资产是一种数字资产，是区块链上的数字化通证，用来代表实物金融资产和传统金融资产。这种资产数字化的模式有助于提高流动性、透明性、风控水平以及合规性。然而，这些资产具有一定复杂性和创新性，因此会带来挑战，尤其是较难评估资产的安全性和风险。

因此，许多资产管理者无法创建和发行包含通证资产的综合数字资产投资产品。由于客户对于通证资产的需求不断增长，资产管理者如果无法在产品组合中稳健地提供这类资产，那么客户就有可能流失到竞争对手那里。

本报告将在以下方面为资产管理者提供关键的行业洞察：

- **通证资产市场格局**，其中包括通证资产的优势，如何更好地分类和理解通证资产，通证化的大致流程以及案例分享。案例分享中会详述这类新兴资产的发展潜力。
- **通证资产的风险**，其中会详细阐述如何识别和应对通证资产底层技术的相关风险，包括在安全性和可编程性方面的关键考虑因素。
- **Chainlink可以为通证资产提供基础设施并过滤风险**。Chainlink拥有非常安全且功能全面的技术平台，可以帮助金融机构开发定制化、灵活、合规且与时俱进的区块链应用以及通证资产。

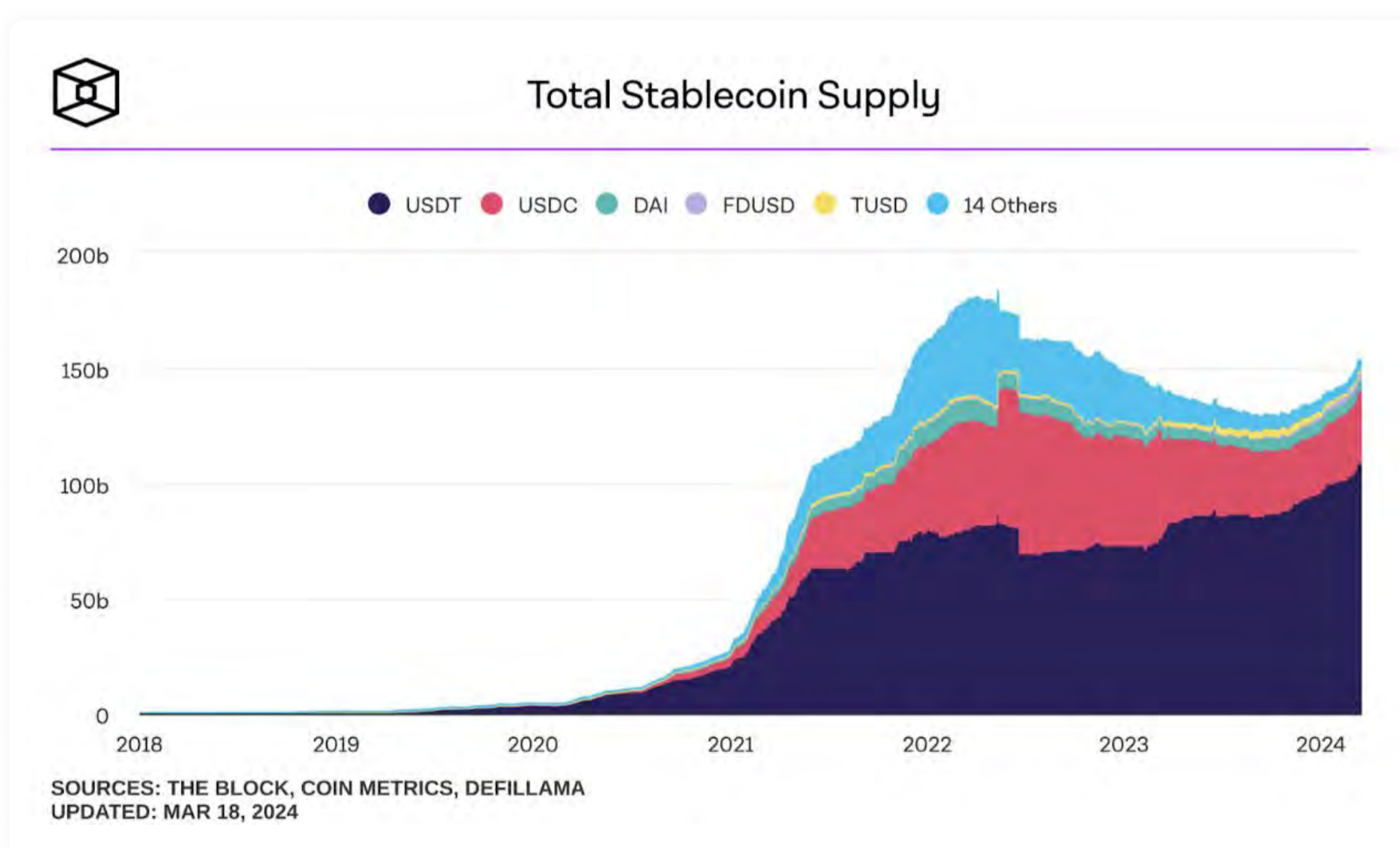
资产管理者一旦深入了解了通证资产的技术复杂性以及Chainlink风控基础设施对通证资产策略所带来的价值，就可以在创建和筛选资产的过程中做出更加理性的决策。这样做不仅可以让资产管理者有效满足目前的市场需求，还可以让他们更好地抓住通证资产的未来市场机遇。

市场机遇

[区块链](#)最初为人所知的价值是它作为一个平行的金融系统挑战了传统金融的地位。随着行业不断发展，传统金融资产开始逐渐转移到区块链上成为数字资产，而传统金融行业也开始充分意识到区块链的技术优势。因此，区块链摆脱了其最初“传统金融竞争者”的身份，并成为了现有金融生态的组成部分，传统资产和区块链上的数字资产不断融合成了一个统一的全球金融生态。这种融合是数字化时代的必然结果，区块链以及其他类型的分布式账本技术（DLT）为数字资产的存储和交易以及基于数字资产的金融服务都提供了不可或缺的后端基础设施。

这场通证化浪潮的规模不容小觑，它有望超越之前任何一种金融资产。[北方信托银行和汇丰银行](#)预计，到2030年，5-10%的资产将实现数字化。[21.co](#)发布的报告以及[BCG](#)和[ADDX](#)联合发布的研究预测到，2030年，通证资产市场规模将分别达到10万亿美元和16万亿美元。

据[DeFiLlama](#)，[Coin Metrics](#)和[The Block](#)发布的数据显示，截止至2024年3月，公链账本上的通证资产总值约为1470亿美元。另据[21.co](#)的数据显示，锚定法币的稳定币占到97%以上。这个行业势必将取得惊人增长，之后会有更多资产转型为数字通证，众多市场和行业也会在新增和原有的工作流程中加入通证资产。



虽然通证资产在私有链上的价值较难估算，但机构对于通证化的关注度却在不断增长。根据纽约梅隆银行和Celent的[调查](#)显示，97%的机构投资者都认同“通证化将颠覆资产管理行业”这一说法。贝莱德CEO Larry Fink则[认为](#)，11个现货比特币ETF的通过是“金融市场技术革命的第一步”。而下一步就是将所有金融资产通证化。另外，美国证券存托与结算公司（DTCC）的执行董事Stephen Proserpi在[DTCC的博客文章](#)中提到，DTCC与Chainlink的合作将“激活一系列应用场景，这将重新定义金融行业的运行模式”。

除金融市场之外，众多其他行业也在积极采用通证资产。这标志着全球经济将在更大程度上实现转型，向通证化迈进。世界经济论坛预估通证化已经覆盖了867万亿美元的价值，而且应用场景不仅限于金融资产。其中一个案例就是沃达丰的数字资产经纪平台（DAB）。这家公司在2023年与住友商事，Chainlink Labs以及InnoWave共同开展了一项概念验证，通过将贸易单证通证化，来解决价值30多万亿美元的全球贸易生态中长期存在的挑战。



“我们发现机构投资者及其客户对于通证资产的兴趣越来越浓。大量资金有意向投入到通证化市场中，这为传统资产管理行业带来了巨大的市场机会。资产管理者是时候积极投身于这个赛道了。”



BCG Platinion新兴技术团队全球负责人兼董事总经理 Kaj Burchardi

资产通证化的优势

要完全理解通证化的大趋势，首先必须明确[资产通证化](#)的最大优势。

实时结算

区块链可以让交易执行和结算同时发生，可以实现货银对付（DvP）结算和全天候交易，并且可以即刻进入全球各个流动性池。智能合约可以基于预定义的标准自动执行交易，金融机构可以直接在通证资产中设置复杂的规则，进一步缩短结算时间并降低摩擦。

在传统金融中，交易结算可能需要花T+2天，而且整个过程都存在对手方风险。相比之下，区块链可以实现几乎实时的交易执行和结算，为实现金融市场T+0结算奠定了基础。瑞典央行[试点](#)推出了电子货币e-krona，为支付提供实时结算。

这个转型以实现单日内结算为目的，将提高市场的可用性和效率。另外，逐渐向去中心化的金融市场基础设施（dFMI）的转型（注：指利用区块链、[智能合约](#)以及预言机网络来追踪资产所有权、执行交易并进行结算），也将实现降本增效。

公正客观的记录

将区块链作为不可篡改的共享事实来源，记录通证资产的所有权，这样做将大幅提高一系列行政流程的效率，其中包括回购，分润，净资产值发放，公司行为，股东投票以及票息支付。这将减少中间方并在各个对手方之间建立统一，可靠且不可篡改的事实来源，最终提高透明度并消除对账流程。

全球流动性

通证化采用区块链技术，为交易的执行和结算引入了通用标准，因此可以解锁大量流动性，大幅提升资本效率和速度，并创建可以即时访问的全球流动性池。最值得一提的是，过往一些资产往往会因为无法面向大众市场而缺乏流动性，通证化可以很好解决这一问题，为这类资产带来更多流动性。将这些资产转换成数字化的链上通证，不仅可以扩展市场规模，还可以更高效地应用于金融机构的各个流程中。

将高价物品通证化还有一个关键优势，那就是可以将高价值物品的所有权分割，这样做可以有效降低准入门槛，并扩大潜在的投资者的范围。在传统行业中，将房地产这类资产分割成小块来交易是不现实的，但通证化可以很好地解决这一问题，投资者可以拥有并交易分割化的资产，边际成本几乎为零。

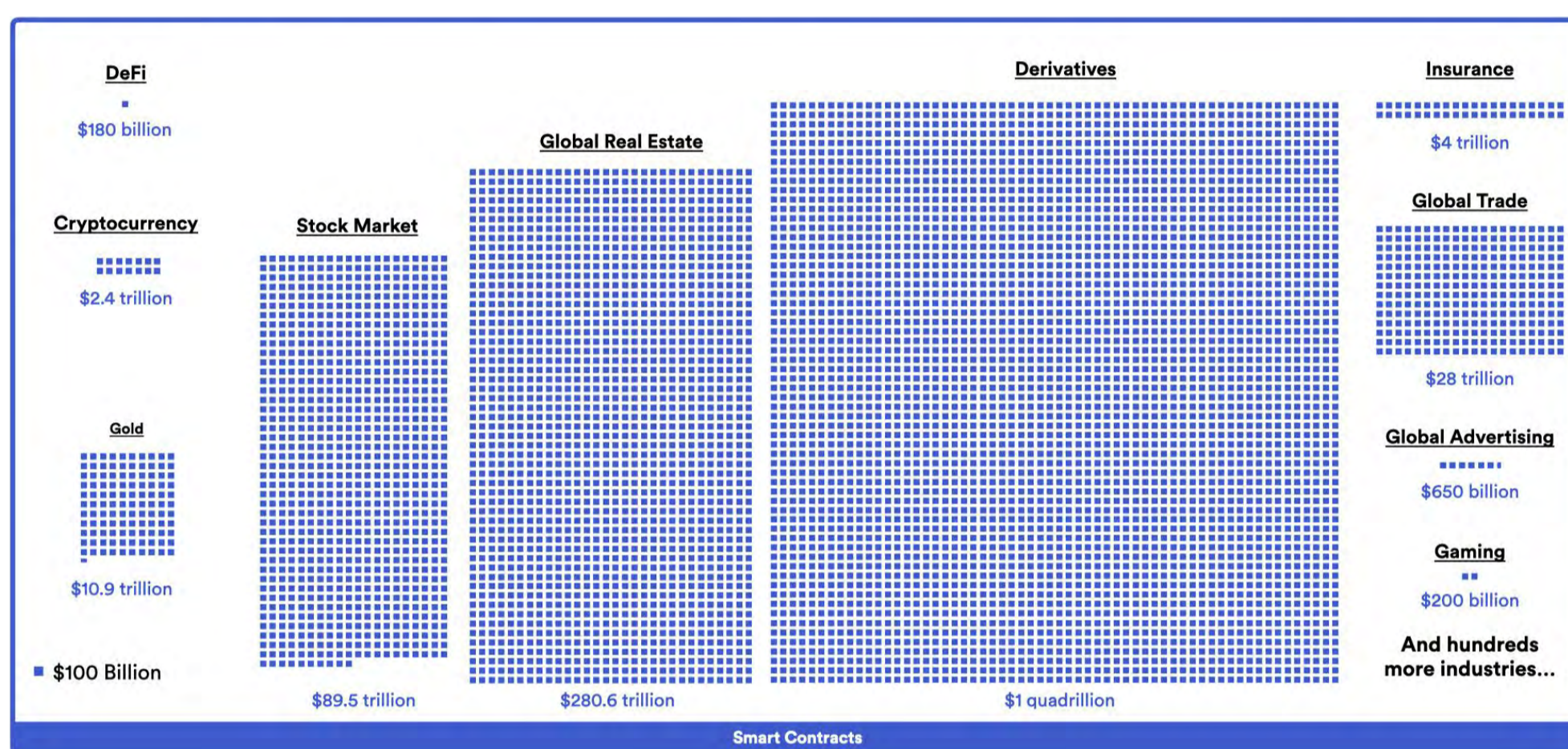
可组合性

通证化可以开创全新的金融市场和金融工具，之前分散在各个系统中无法连通的资产现在可以在区块链的标准化结算层上共存。所有通证资产都在同一个结算层上结算，这样就可以无缝接入各种链上智能合约的金融服务，功能涵盖借贷，资产互换，资产分割化以及质押（staking）。这些功能可以轻松写入链上应用中，提高资金效率并丰富资产功能。

[去中心化金融（DeFi）](#) 已经挖掘了一些可组合性的潜力，催生出了[闪电贷](#)等全新的金融原语，这个概念在传统金融领域是不可能实现的。

应用广泛

通证化不仅可以造福金融行业和大企业，任何具有货币价值或信息的物品都可以被通证化，比如艺术品，知识产权或甚至高级雇员的工作时间。因此，资产通证化常常被认为是区块链最具潜力的用例，涵盖几乎所有经济活动，总市场规模有望达到数百万亿美元。



通证化最终将拓宽可投资标的的边界。随着通证化逐渐超出传统金融资产的范畴，将大幅提升资产组合的多元性，并丰富金融市场中抵押品的种类（如：非现金类资产）。

私募股权和债券可能会成为首批被通证化的市场。而随着通证化的价值在这些市场不断得到证实，将吸引更多规模的市场也加入通证化浪潮。最终，所有具有价值的物品都会被通证化。

通证资产对资产管理者价值

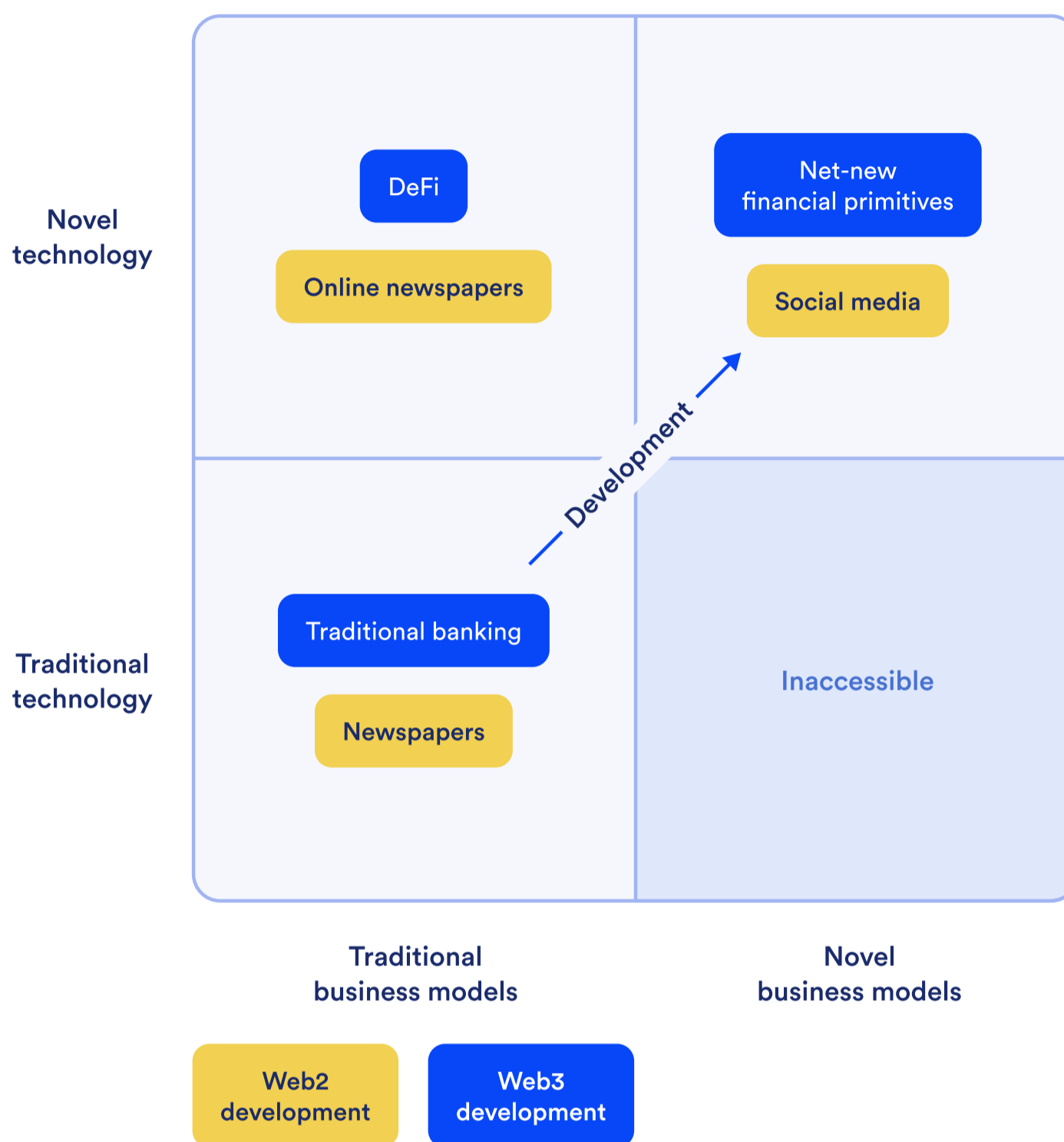
上一章我们讨论了通证化的优势，接下来我们来看看通证化对资产管理者来说有哪些特殊的价值。

- **盘活闲置资金**：通证化可以为资产管理者及其客户带来更高的回报率，让他们可以接触到之前无法触碰的市场或资产类型，以及遍布全球且全天候开放的高流动性市场。这将为资产管理者吸引来更多资金和收入。传统资产通证化还可以帮助资产管理者通过借贷、自动做市或其他低风险的增值活动，来盘活闲置资金。
- **提高资产的可用性**：通证化可以让投资者获得更多类型的资产，并让资产管理者多元化客户的资产组合，在其中添加之前无法或很难接触到的资产类别。另类投资以及比特币等新兴数字资产的兴起，证明了客户对此类多元化投资组合的需求日益增加。
- **创新收入模式**：资产管理者将通证资产放到资产组合中，将解锁独特的机会，获得新的收入来源。比如，资产管理者可以在DeFi协议中赚取收益，或代表客户在以太坊等PoS系统中质押资产。
- **为客户提供一站式服务**：资产管理者可以为客户提供一站式服务，满足客户所有的投资需求，在一个投资组合中同时提供传统金融资产和数字资产，以此来扩大在管资产规模。这样做可以提高客户留存率和满意度，客户无需委托两家不同的资产管理公司分别满足其传统资产和数字资产的投资需求。
- **提供差异化服务**：资产管理者可以利用通证化来为客户提供创新且定制化的金融产品，比如分割化的资产和通证化的基金份额；以及独特的金融产品，比如自动还款的贷款或DeFi收益类产品。
- **提高风控能力**：通证化意味着资产的全部所有权记录都保存在链上，因此可以更细致且自动化的风险评估和管理水平。另外，智能合约还可以降低金融交易中的对手方风险。增强风控能力最终将提高决策能力和判断力，并推动资产管理者更好地管理客户资金。
- **自动化后台流程**：通证化可以简化和自动化诸多后台流程，比如结算，合规和记录。效率提升不仅可以节省时间，还会大幅降低资产管理者运行成本，让他们可以减少中介雇佣。



通证是链上金融原语

通证化具有诸多优势，其潜力远不止发布链上通证那么简单。我们可以把通证和网页做一个类比。我们说通证是构成链上金融的基本要素，就好比说网页是构成互联网的基本要素。最初，网页的目的是将报纸或广播节目等模拟内容数字化并放到网上。之后，网页的概念逐步演变，引入了越来越高级的功能。如今，网页可以展示动态内容，社交网络，[游戏](#)，并催生出了全新的媒体形式。

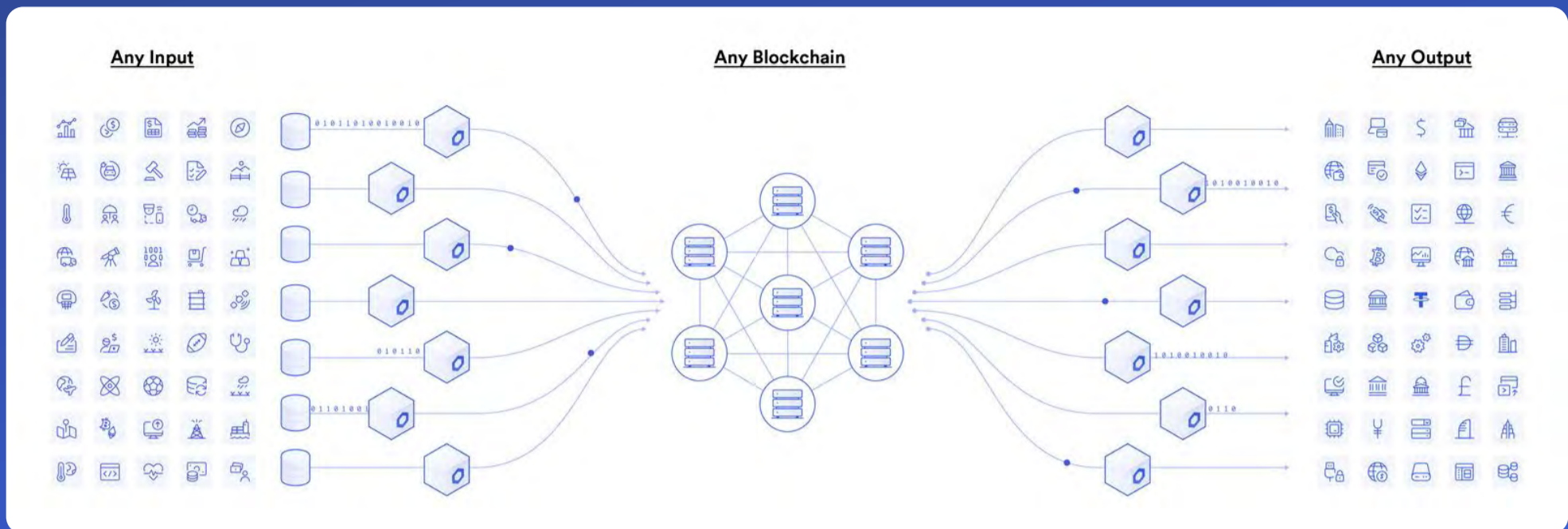


DeFi 引入了可编程性来实现通证的交互，并初步实现了产品-市场契合度。这催生出了去中心化借贷市场，永续合约衍生品以及稳定币等应用。然而，这只是一个开始。最终，我们要在链上建立全球金融系统，将资产变成数字化通证，并开发各类金融和社会服务，通过智能合约来定义资产的发行，收益，服务，治理，追踪和交易方式。

要实现可编程性，不仅需要区块链，还需要其他基础设施，尤其是预言机网络。这是因为区块链本身无法从任何外部系统获取数据，也无法将数据发送出去，因此是相互孤立的系统，就好像是没有接入互联网的计算机。要将这些链上环境与外部世界连通，就需要额外的基础设施，而这个基础设施就是预言机。

预言机概述

预言机是连接区块链网络和外部系统的基础设施，可以辅助链上应用和任何链下系统之间展开通信。将链下数据接入智能合约，可以极大扩展智能合约的功能，但同时也会带来一系列安全问题。我们通常会用预言机数据来自动触发一些智能合约功能，比如为交易提供兑换汇率，或判断是否对参数型保险进行理赔。因此，如果一方私自篡改了预言机数据，或数据无法安全及时送达，那么应用的功能和安全性就会受到严重威胁。



Chainlink发布了去中心化的预言机网络（DON），智能合约可以利用这个网络安全地连接外部数据，计算资源和系统，因此很好地解决了上述问题。Chainlink去中心化预言机网络采用了去中心化的节点网络为智能合约提供服务，比如在区块链和外部API之间传输数据，或从多个优质数据源聚合公允市场价格，并传输到链上。自2019年发布以来，Chainlink一直都维持着数字资产行业最高水平的安全性和可靠性标准，甚至在市场大幅波动期间也能正常运行。

“通证化为资产管理带来了巨大机会，但过去由于缺乏高质量的基础设施，无法解决与传统资本市场集成的相关技术挑战，因此通证化一直很难实现大规模应用。资产管理者如果要放心地参与这个新兴市场，就需要有稳健的风控基础设施，让他们能够安全地将通证资产纳入投资组合中。Chainlink制定了新的标准，为通证资产提供了功能，安全性和透明性，并帮助资产管理者更好地适应未来通证市场的发展。”

21shares

21Shares的副总裁兼数字资产战略和业务拓展负责人Eliézer Ndinga

通证资产概览

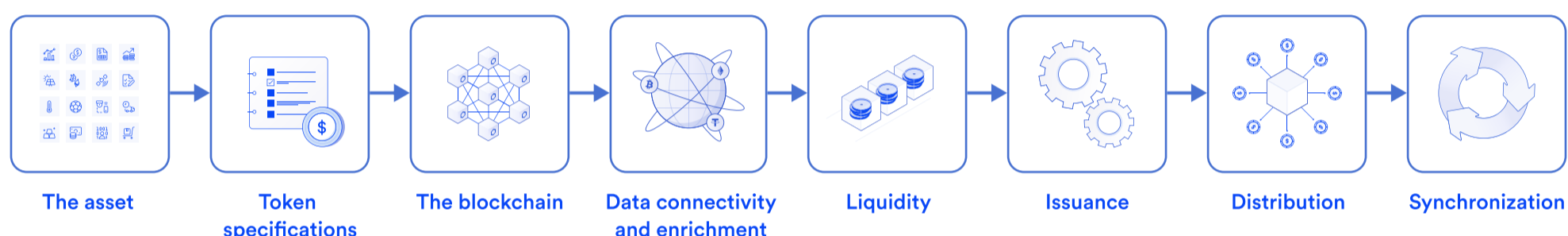
通证资产分类

在讨论如何实现可编程性之前，我们先来看一下数字资产当前的市场格局。

- **传统资产**在传统金融系统中进行发行和交易。
- **通证资产**是区块链上的数字通证，代表了实物或传统金融资产，如现金，银行存款，大宗商品，证券和债券等。通过通证化，可以针对底层资产创建相应的数字通证，在链上管理资产的所有权。本篇报告聚焦的是这类资产。
- **链上资产**是纯链上的资产，比如比特币网络的原生资产比特币，或以太坊网络的原生资产以太币。

资产通证化的流程

资产通证化流程大致包含以下几个步骤：



- **确定资产**：确定需要在链上发行通证的资产。
- **定义通证规格**：选择通证类型（同质化或非同质化），[通证标准](#)（ERC-20或ERC-721）以及其他关键属性。
- **确定区块链**：选择通证要发在公链上还是私有链上，并综合考虑每条区块链的优劣势。
- **建立数据连接性并丰富数据类型**：为通证资产建立链下连接性，以围绕资产创建安全可靠的市场。比如，通证资产可能需要接入储备金证明数据，以证明抵押率；接入汇率数据，以保障按市场计价的公允估值；以及接入身份验证服务，以检查合规性等。
- **流动性**：使通证实现跨链互操作性，让其他区块链网络中的交易对手方可以与之交互。
- **发行通证**：在自己选择的区块链网络中部署智能合约，铸造通证，最终面向用户发行。
- **分销**：在个人和机构投资者之中分销通证，为资产开拓更大的市场，并有机会实现更高的流动性。
- **数据同步**：一旦通证资产进入市场，并开始其跨链流通的生命周期，资产就需要喂价，净资产值，身份数据和储备金数据等各种数据来维持其正常运行。而这些数据必须保持同步更新，才能在资产跨链的过程中维持正常运行。要跨越各条区块链创建客观统一的记录，就必须做到这一点。

当前的通证资产类型

稳定币

由法币抵押的稳定币是首个也是迄今为止最成功的通证资产用例。[稳定币](#)相比底层法币的优势在于，它是数字原生货币，可编程，可组合，而且可以即时结算。

许多市场上最主流的稳定币，比如[Circle的USDC](#)以及由Paxos发行的PayPal稳定币[PayPal USD](#)，都主要用[现金](#)以及[短期美国国债](#)作为抵押。这样可以提高抵押资产的稳健性，并提升用户对其稳定性和可赎回性的信心。然而，一些“美元抵押”稳定币，比如Tether (USDT)，背后其实还有许多其他类型的抵押资产，比如美国国债等现金等价物，担保贷款，贵金属，比特币以及企业债券等。因此，一些市场规模最大的稳定币在结构上既像通证化的货币市场基金，又像电子货币发行商。不过稳定币通常不会为用户提供原生收益 (native yield)。

截止至2024年3月，稳定币的链上供应量达到了约[1460亿美元](#)（注：其中也包括除法币抵押的稳定币以外的其他类型稳定币）。与此同时，有超过[5000万个链上地址](#)正持有或曾经持有以太坊区块链上的通证资产，其中99%以上都是法币抵押的稳定币。虽然这些统计数据对于区块链行业来说已经非常惊人，但是稳定币在零售行业和资本市场还有更大的应用潜力。稳定币不仅可以用于零售支付，还可以作为其他通证资产交易的结算工具。由于现金和证券都被通证化了，因此可以实现原子化的货银对付 (DvP) 支付流程。

基金

随着支付型和收益型通证资产的出现，资产管理者可以完全在链上创建，投资并管理通证化基金。他们只需要一个安全的区块链互操作性协议就可以接入各个通证资产生态。

通证基金可以为资产管理者带来以下价值：

- 更快速和高效的记账
- 数字化的后台流程
- 高成本效益的基金管理机制
- 自动化的分销或公司行为
- 将资金通证用于抵押
- 个性化的投资组合

香港顶尖的金融机构裕承科金就集成了[Chainlink](#)，提升其基金通证的功能和透明性。

“裕承科金目前正在开发基于Chainlink准备金证明和跨链互操作性协议 (CCIP) 的跨链基金通证。通证受到合规监管，目的是为全球Web3用户提供流畅的投资体验。我们看到，Web3用户，传统投资者和监管者对于安全且履行社会责任的纯链上投资产品的需求越来越大”

裕承科金联席CEO Eddie Lau

债权

企业债券和政府证券等各种债务工具也可以转换成链上通证资产。比如，西门子在2023年链上[发布](#)了数字债券。通证化债权利用智能合约将债权从发布、结算、付息到到期等多个环节自动化。这样做有助于降低运行复杂度和成本，而区块链可以保障所有权和交易记录的不可篡改性。

通证化债权还可以进行分割，投资者可以买入较小份额的债权，这在传统市场上是做不到的。债权分割可以让更多投资者参与到市场中，而过去只有机构投资者或合格投资者才可以参与。

大宗商品

大宗商品也可以采用通证化手段，将[黄金](#)，白银，石油或农产品等实物商品变成数字通证，通证代表着标的资产的所有权。将大宗商品通证接入实时更新的数据，可以保障其透明性和可追溯性，这对于验证资产真实性和来源来说至关重要。

大宗商品一直以来的问题就是无法分割且市场太小众，通证化可以很好解决这些问题。将所有权分割，可以让更多投资者可以轻松投资，无需处置或保存实物资产。

另外，大宗商品通证还可以在链上交易，链上市场全天候开放，而且投资者买卖和转让所有权的体验也更加流畅。市场效率提升可以造福投资者，让资产管理者更好地多元化投资组合，也让资产发行商获得更稳定的定价机制和更广阔的全球市场。

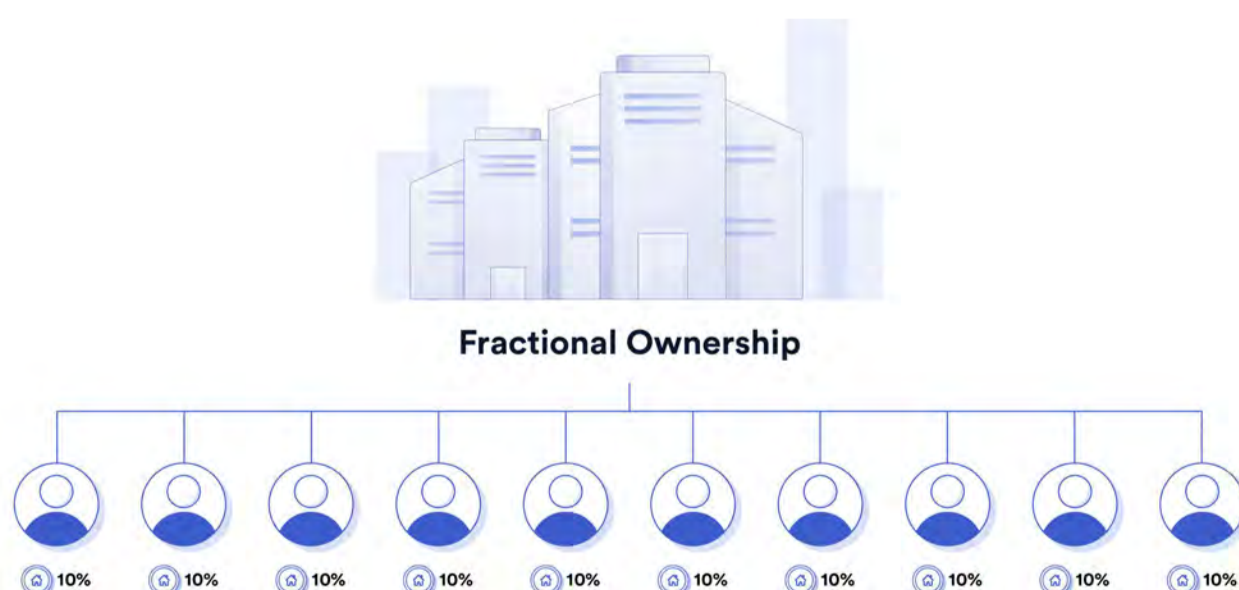
比如，Paxos推出了[Pax Gold \(PAXG\)](#) 通证，将黄金贵金属做成通证并在链上发布，通证接入了Chainlink Price Feeds，每一盎司黄金都可赎回。截止至2024年3月，链上可见的供应量超过4亿美元。

房地产

房地产是全球最大的市场之一。与其他资产相比，房地产流动性非常低，存在许多中间环节，交易往往需要耗费数周时间。

通证化可以优化房地产交易的流程，去除不必要的第三方，并降低市场准入门槛。资产交易门槛降低后，流动性和价格发现机制都会有所改善，交易成本也会降低。因此，资产管理者可以将这类通证资产纳入投资组合中，以此来吸引更多机构投资者并扩大在管资产规模。

[RealT](#)是一个房地产通证平台，可以分割房地产所有权，用户可以在平台上交易[房地产通证](#)。



碳信用

气候金融市场在过去十年中迅猛发展，吸引了大量来自企业，银行和政府的关注。然而，气候金融一直以来都面临效率和流动性的瓶颈。

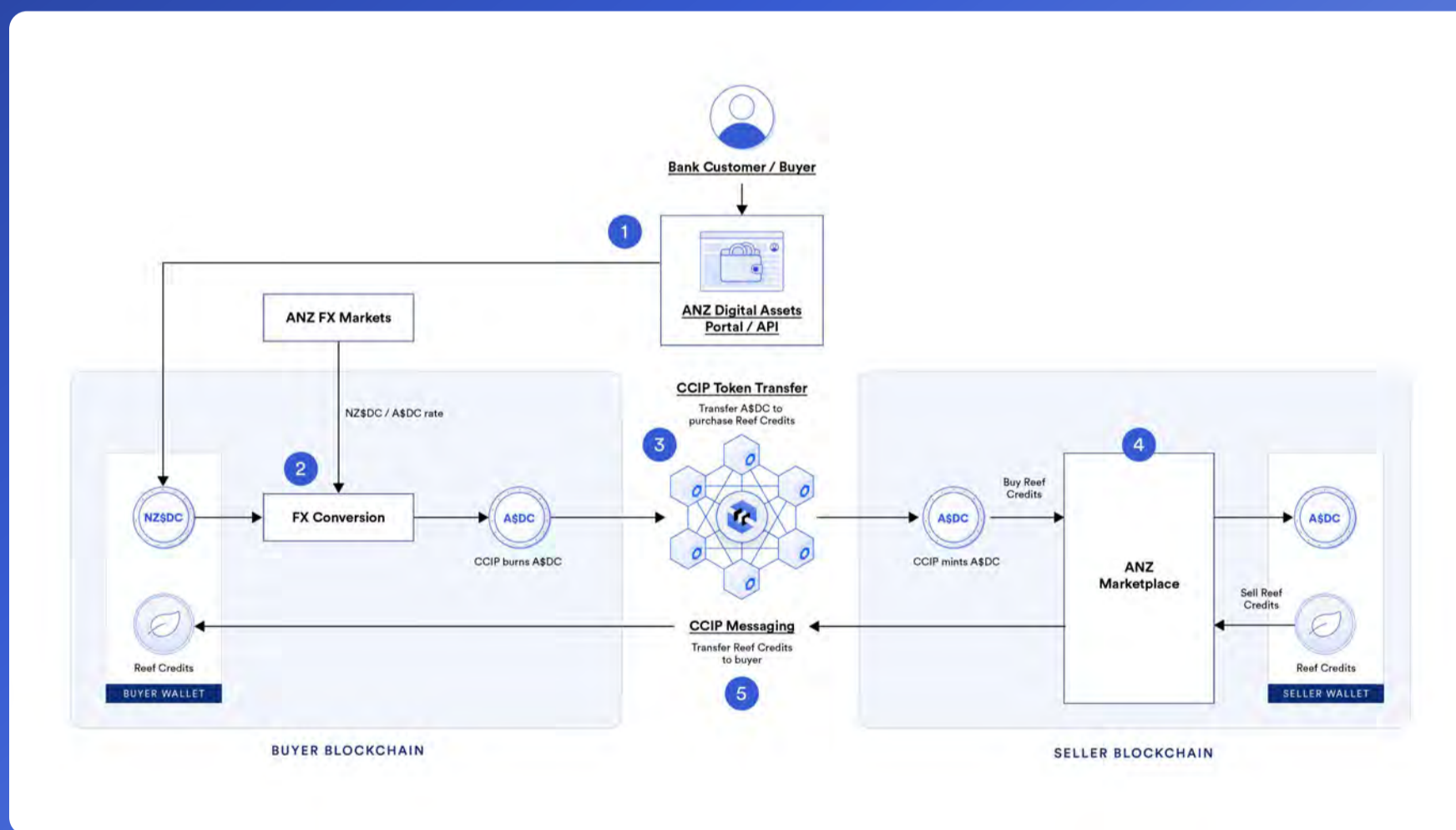
碳市场最主要的挑战是缺乏流动性。市场分化严重，资产流动性差，覆盖范围窄，而且交易分散。如果能在链上采用统一的碳信用标准将这些分化的市场整合起来，并通过区块链在全球范围内展开交易，那么碳市场的流动性和影响力都将得到大幅提升。

2022年发布的一份报告^{显示}，国际清算银行创新中心与香港金融管理局和联合国气候变化全球创新中心共同探索了如何将基于智能合约的碳信用应用到绿色债券中。

案例分享：澳新银行集成Chainlink CCIP，成功使用稳定币购买自然资源通证资产

澳新银行是一家领先的澳大利亚银行，在管资产超过1万亿美元。该银行成功开展项目，展示了银行客户如何使用CCIP安全地跨链转移澳新银行发行的稳定币来购买自然资源资产。该项目是跨币种跨链购买通证资产的典型用例。

澳新银行的技术负责人Lee Ross表示：“我们非常高兴能够采用简单好用的平台为用户流畅地接入通证资产，并推动金融创新。Chainlink CCIP是其中的关键技术，简化了通证资产跨链传输的复杂性，并保障了原子化的跨链DvP支付。”

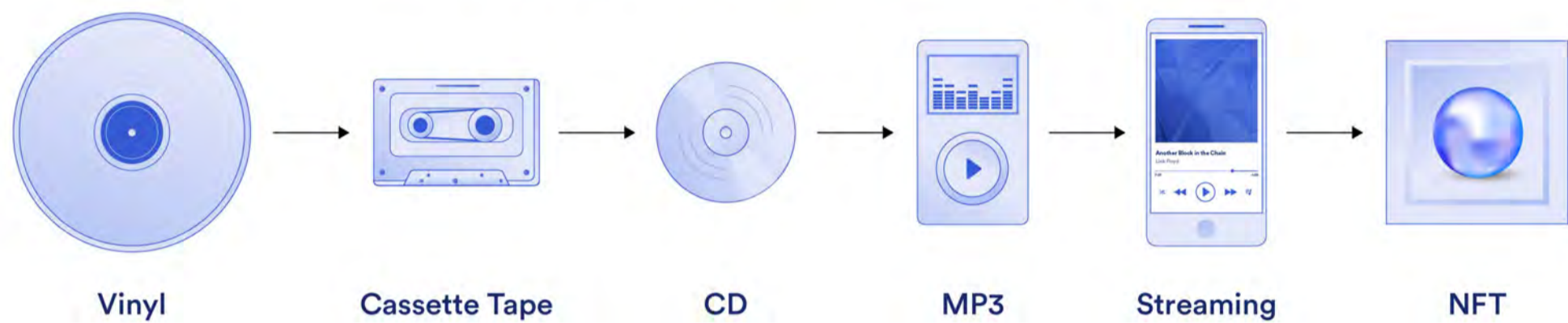


艺术品和收藏品

通证化的影响力还蔓延到了艺术品，藏品以及音乐领域，通过创建[非同质化通证 \(NFT\)](#)，将艺术品，藏品和手工艺品的所有权数字化。这一转变不仅可以让艺术品和藏品受众更广，还可以为这个市场带来前所未有的流动性。

对于艺术家和收藏家来说，通证化为他们提供了新的途径来验证真实性、来源和所有权，他们无需亲自或通过复杂的第三方中介来验证实物。将艺术品和藏品的所有权分割，消费者就可以只购买高价艺术藏品的一部分所有权，并且艺术家也可以分得预售版税。比如，艺术家或乐队可以发布新专辑的NFT，收藏者购买这些NFT，就可以分得一部分专辑版税或专属福利。

The Evolution of Popular Music Formats

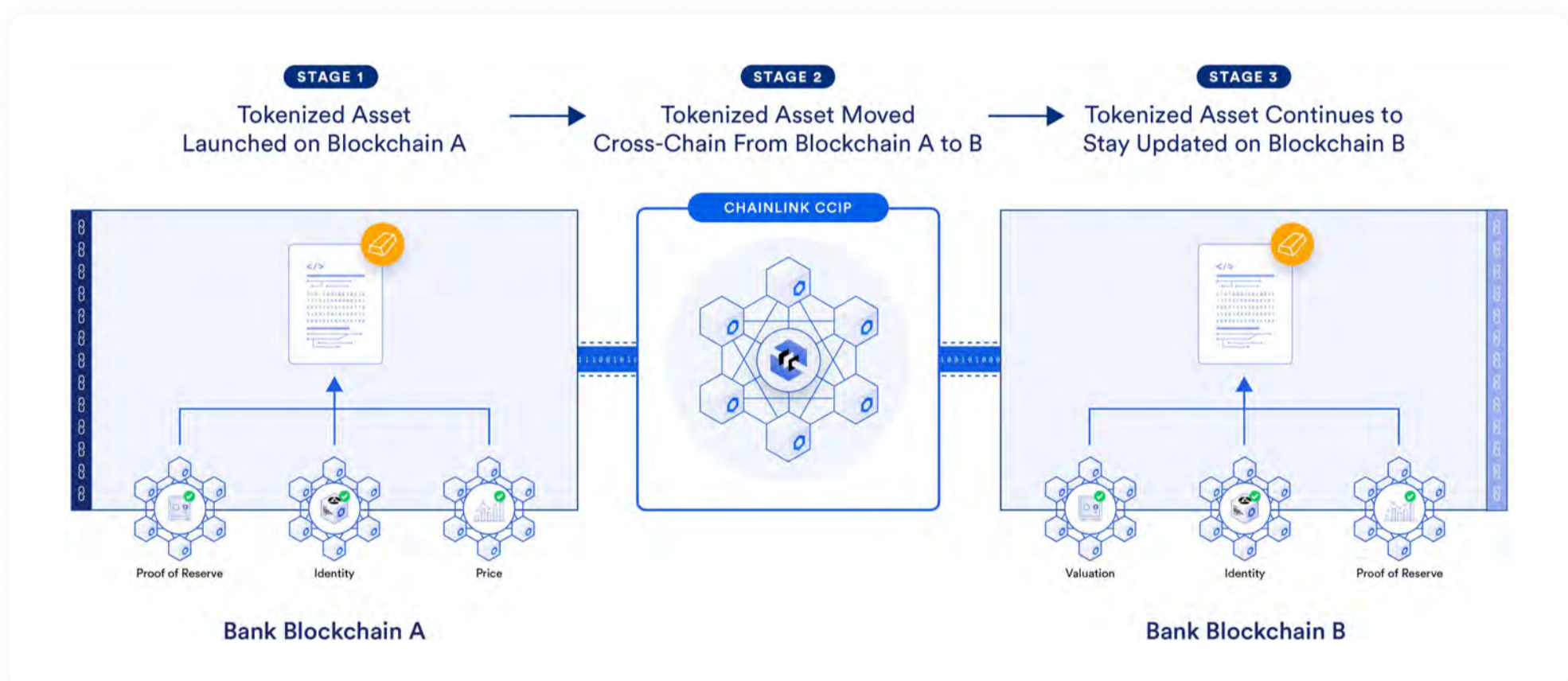


Chainlink：为通证资产经济提供必要的基础设施

通证资产可以为资产管理者和传统金融机构带来诸多价值。不过，在链上发行或购买通证资产并没有看上去那么简单。其中存在很多挑战，尤其在通证资产基础设施的开发和安全性评估方面。要克服这些挑战，机构首先得满足合规需求，建立稳健的风控框架，并制定严格的安全标准。与此同时，还要有能力应对区块链和分布式账本领域未来可能出现的各种挑战。

必须要认识到一点，那就是一旦通证资产在链上发布，必须要依靠各种服务才能保障较高水平的可编程性并建立稳健的二级市场，这些服务如下：

- **接入优质的链下数据**，提供关于资产状况或辅助交易执行的数据，比如市场定价，参考数据，KYC/AML数据以及身份数据。
- **接入可靠的储备金证明机制**，避免恶意攻击或偶然的超发攻击（over-issuance attack），并应对市值，流动性，存续期和责任等各类风险。
- **获得安全的跨链互操作性**，让通证覆盖公链和私有链上的用户和流动性。
- **与当前系统保持同步**，一旦通证资产进入市场，并开始跨链流通的生命周期，就需要喂价，净资产值，身份数据和储备金证明等各种数据来维持正常运行。而这些数据必须保持同步更新，才能在资产跨链的过程中维持正常运行。



要让通证资产充分实现潜力，跨链互操作性尤为重要。银行，金融市场基础设施和DeFi协议渐渐意识到之后会出现成百上千条公链和私有链网络，而且会针对特定的资产和地域市场出现定制化网络。如果没有安全的区块链互操作性标准，就可能导致流动性分散在各个相互孤立的系统，而这将妨碍**新的链上市场**出现。

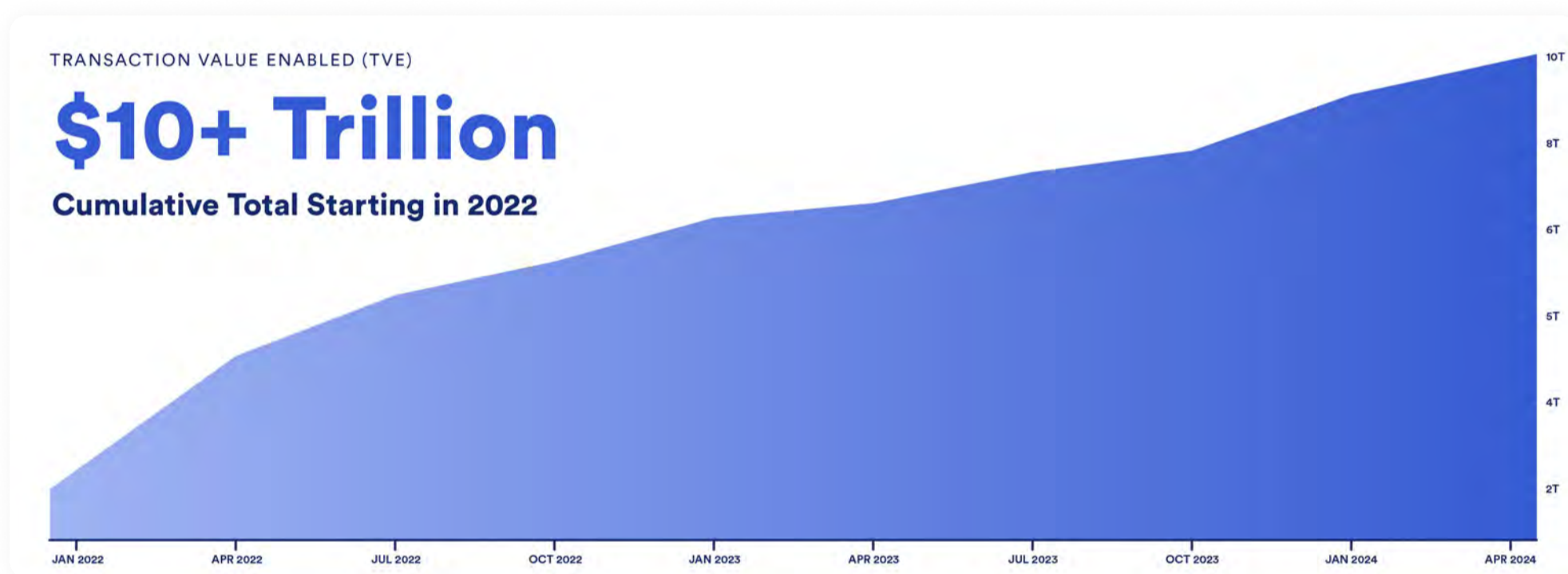
Chainlink是唯一通过建立独立风控网络来应对全球不同国家和地区合规政策的跨链互操作性平台，因此可以保证其运行符合各类监管规定和组织政策。机构可以使用Chainlink在各个交易中预定义条件和限制，比如围绕身份认证，KYC/AML，法律监管规定，通证池，出入金，组织内部规定以及各类跨链安全机制来制定政策。

Chainlink可以针对[上述所有需求](#)提供关键的基础设施服务，为通证资产创建高流动性，安全且合规的二级市场。另外，Chainlink还建立了行业领先的安全标准，为资产管理提供者提供关键的风控工具。资产管理提供者可以使用Chainlink的多层级可验证性和安全性评估框架，判断通证资产的可靠性。

Chainlink平台

Chainlink是行业标准的平台，提供链上数据，跨链互操作性以及区块链抽象化服务。Chainlink Price Feeds在2019年上线，满足了去中心化金融市场对优质，防篡改的链下市场数据日益增长的需求。自那以后，Chainlink就逐渐发展成了一个成熟的去中心化计算平台，实现了超过10万亿美元的交易额，为去中心化金融生态中规模最大的应用保障了数百亿美元的价值，并助力了数字资产行业实现初步采用。

如今，随着通证化大趋势的出现，Chainlink平台可以[帮助机构](#)实现更高水平的可编程性，在战略上拥有更多选择，将数万亿美元的资产传输到链上，并在最大程度上保障安全性和可靠性。



Chainlink服务在过去数年中一直保持高水平的运行质量和不可篡改的安全性，即使在行业最动荡和不可预测的时期也能稳定运行。Chainlink之所以能维持行业最高水平的安全性，是因为它拥有全世界顶尖的研究团队，其中包括Ari Juels和Dahlia Malkhi等世界知名研究者。另外，Chainlink的去中心化预言机网络中包含由众多顶尖企业运行的独立且抗女巫攻击的节点，这些企业包括德国电信子公司MMS，律商联讯（LexisNexis）以及瑞士电信。

Chainlink Node Operators

The Chainlink Network is powered by a geographically distributed collection of Sybil-resistant, security-reviewed node operators with significant experience running mission-critical infrastructure.

12.5B+ DATA POINTS DELIVERED ONCHAIN	12.5B+ TOTAL ORACLE NETWORKS	17+ BLOCKCHAINS & L2S SUPPORTED	10+T TOTAL VALUE ENABLED
--	--	---	------------------------------------

Enterprise Nodes

Telecommunications firms with decades of experience operating backend infrastructure for the Web2 economy.

+ MANY MORE

DevOps Nodes

Specialists in operating blockchain infrastructure such as PoS validators, PoW mining pools, and full node RPC providers.

+ MANY MORE

Community Nodes

Organizations from within the Chainlink community that have demonstrated a high level of reliability and performance.

+ MANY MORE

Chainlink平台可以为用户提供丰富的服务，增强通证资产的功能。这些服务组合在一起使用时几乎不需要添加额外的信任假设。接下来，我们将具体讨论这些服务如何增强通证资产的可编程性，并同时最大程度保障安全性。

The Chainlink Platform

CROSS-CHAIN	<div style="border: 1px solid #333; padding: 5px;"> <p>CCIP</p> <p>Move data and value between existing systems and any public or private blockchain. Architected with multiple decentralized oracle networks and a state of the art Risk Management Network, CCIP is the only interoperability protocol that operates at the fifth level of cross-chain security.</p> </div>		
DATA	<div style="border: 1px solid #333; padding: 5px;"> <p>Data Streams</p> <p>Leverage low-latency market data to power next-generation DeFi markets.</p> </div>	<div style="border: 1px solid #333; padding: 5px;"> <p>Market and Data Feeds</p> <p>Integrate ultra-secure onchain data to trigger smart contracts in DeFi and beyond.</p> </div>	<div style="border: 1px solid #333; padding: 5px;"> <p>Proof of Reserve</p> <p>Verify cross-chain and offchain reserves backing tokenized and wrapped assets.</p> </div>
COMPUTE	<div style="border: 1px solid #333; padding: 5px;"> <p>Functions</p> <p>Connect a smart contract to any API and run custom computation in minutes.</p> </div>	<div style="border: 1px solid #333; padding: 5px;"> <p>Automation</p> <p>Automate smart contracts in a decentralized way with time or event-based triggers.</p> </div>	<div style="border: 1px solid #333; padding: 5px;"> <p>VRF</p> <p>Use verifiably random numbers to ensure fair outcomes in games, NFTs, and more.</p> </div>

互操作性

关键问题：

- **通证资产是否可以跨链？**

如果不能，资产的流动性可能会非常低，而且无法覆盖许多交易对手方。

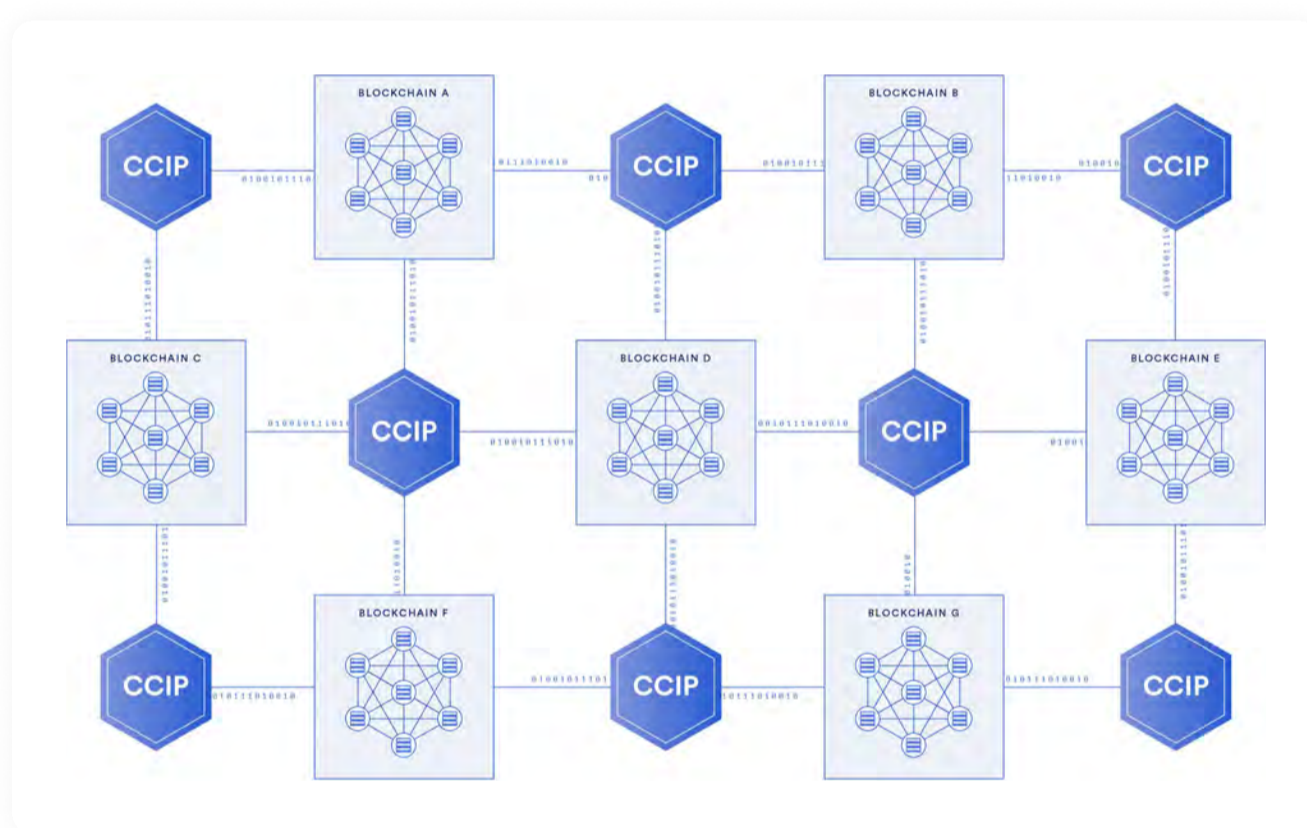
- **通证资产是否采用了最安全的跨链协议？**

如果没有，资产可能会遭受多次跨链桥攻击。

- **作为资产管理者，你的后端系统是否能通过集成中间件来接入所有区块链？**

如果不能，那么你可能需要耗费时间和资源分别接入每一条链。

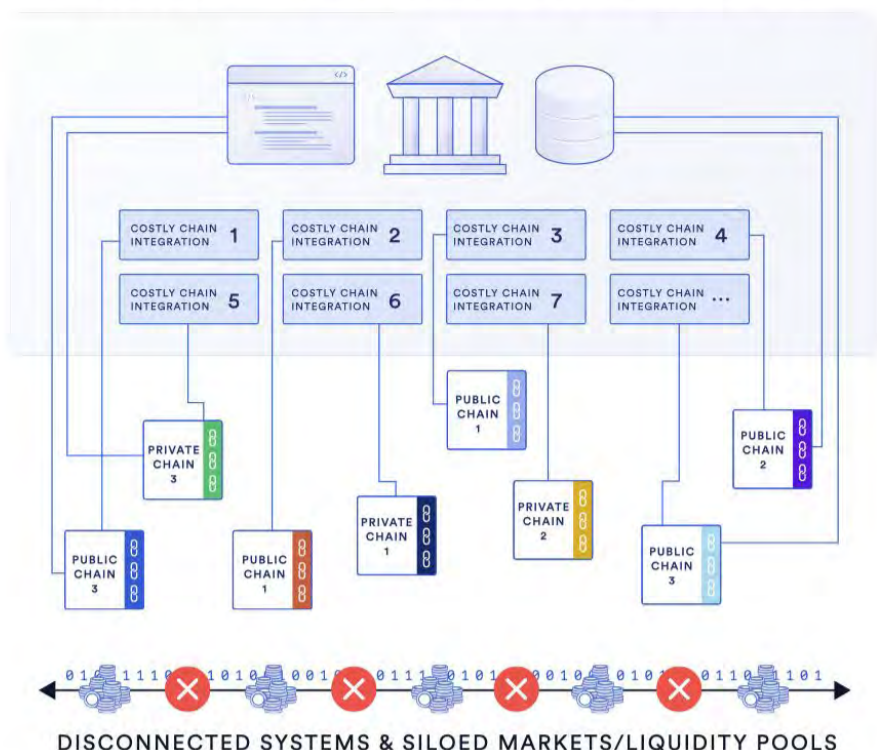
通证资产最重要的一点就是需要在公链和私有链之间转移。区块链行业正不断朝着多链格局发展，目前已经发展出了许多不同的区块链生态，而且许多银行，应用和甚至资产发行方都想要开发自己的区块链。另外，机构没必要只选择一条区块链接入，也没必要在接入区块链时重构其原有系统。因此，如果要为通证资产创建一个稳健且高流动性的市场，就必须能够覆盖各条链上的买卖双方。要实现这一点，就必须采用安全的跨链互操作性基础设施作为统一的抽象层，让机构可以利用其现有的接口和消息传输标准，与所有区块链上的通证资产进行交互。



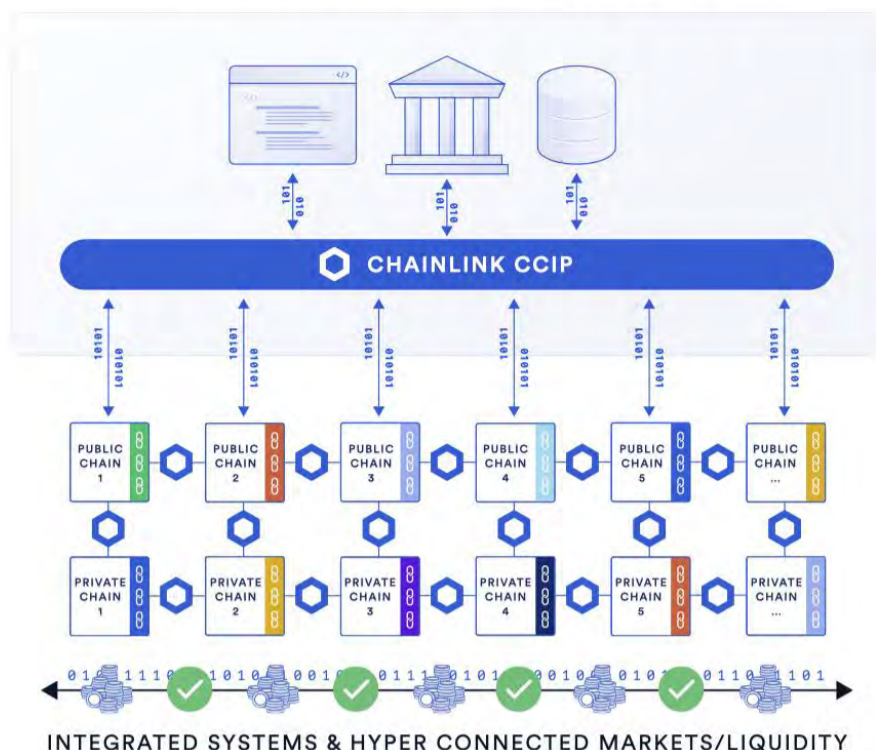
而目前的问题是，区块链互操作性实现起来非常复杂，而这也是通证资产技术栈中最脆弱也最容易被利用的漏洞。迄今为止，已有28亿多美元的[跨链资金被盗](#)。鉴于上述风险，资产管理者如果想要跨链转移资产，或是要评估某一跨链原生通证资产是否值得购买，就必须评估其底层所采用的区块链互操作性协议是否安全。

Chainlink的[跨链互操作性协议 \(CCIP\)](#) 是行业中最安全可靠的区块链互操作性协议。CCIP是区块链的抽象层，用户集成一个统一的中间件，就可以将现有后端系统直接接入各条区块链，与链上通证资产交互。同时，CCIP也是跨链消息传输协议，用户可以跨越各条公链和私有链传输数据和通证。

1000s of Costly Integrations into 1000s of Chains

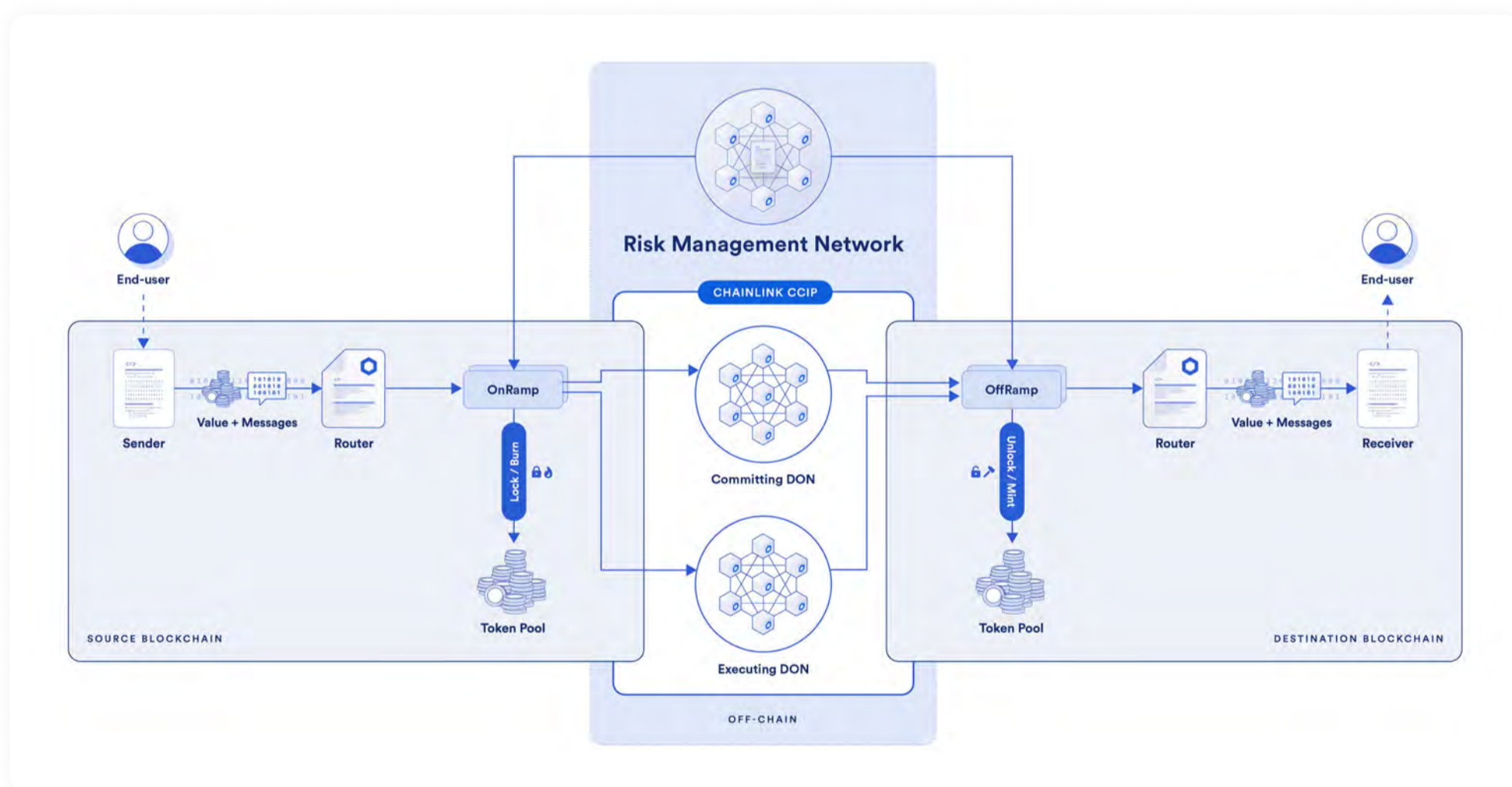


1 Integration Connects to 1000s of Chains



CCIP利用多个去中心化网络，保障每一笔跨链交易的安全，达到了[第五级跨链安全水平](#)。CCIP是唯一内置了[独立风控网络（Risk Management Network）](#)的跨链协议，这个风控网络负责监督网络异常和恶意行为，当监测到此类行为时，可以临时触发紧急关停机制。Chainlink风控网络的代码库与CCIP完全独立，无论是编程语言还是开发团队都与CCIP完全区隔开。另外，风控网络中的节点运营商与验证CCIP跨链交易的节点也完全没有交集。

值得一提的是，CCIP是唯一可以应对全球各地合规和监管政策的跨链互操作性平台。机构可以使用CCIP的风控网络在各个交易中预定义条件和限制，比如围绕身份认证，KYC/AML，法律法规，通证池，出入金，组织内部规定以及各种类型的跨链安全机制来制定政策。



主流金融机构和金融基础设施提供商已经开始与Chainlink合作，利用CCIP来探索区块链技术和通证资产，这些机构包括[Swift](#)，[DTCC](#)以及[澳新银行](#)。

储备金证明

关键问题：

- **通证资产是否拥有安全的储备金证明机制？**
如果没有，那么资产可能会遭受无限铸造攻击（infinite mint attack）。
- **通证资产的铸造机制是否安全，是否设置了熔断机制？**
如果没有，那么资产可能会遭受无限铸造攻击（infinite mint attack）并铸造没有抵押资产的通证。
- **通证资产的储备金证明机制是否透明？**
如果不透明，那么用户对于资产就会不放心。
- **风控框架中是否设置了自动熔断机制？**
如果没有，那么通证资产可能会因为储备金不足而导致坏账。

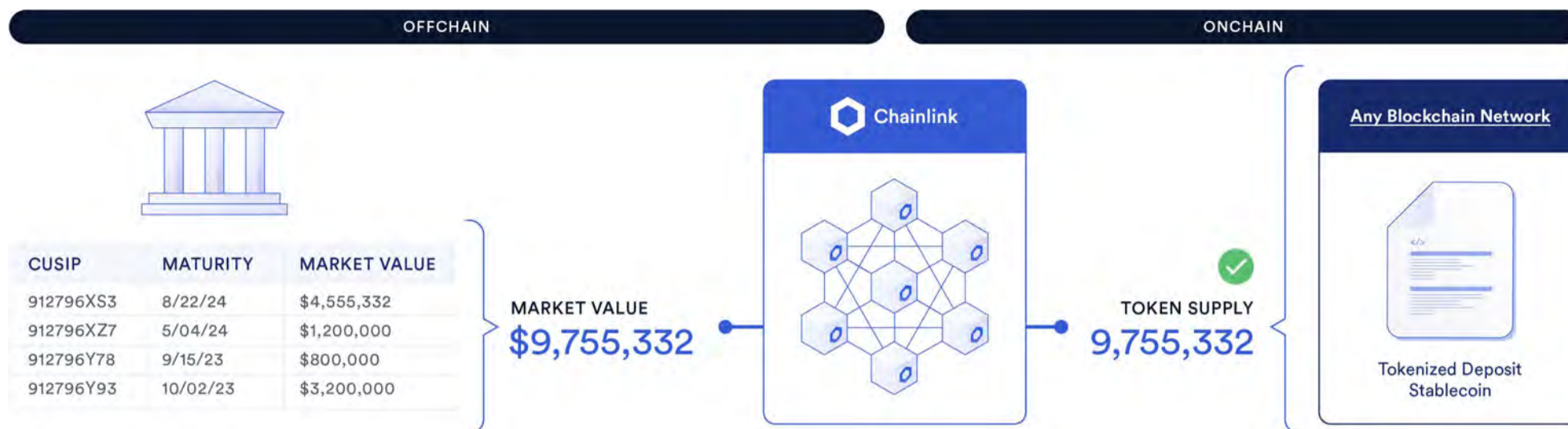
链上通证资产映射了相应的链下资产或资产组合（比如存放在银行，第三方托管方，或另一条链上的资产）。资产管理者需要获得关于链下或跨链储备金的信息，才能理性地判断是否要交易链上通证资产。因此，在链上直接验证储备金信息是非常重要的功能，对自动化的链上资产管理策略来说尤为如此。

通证资产必须考虑五个关键的储备金风险。

1. **市值风险**：资产发行方在一个或多个不同的托管账户中的抵押资产总值。
2. **流动性风险**：在不引起报价vs成交价大幅波动的前提下，市场能够吸收资产发行方大规模赎回交易的深度。
3. **存续期风险**：底层抵押资产对利率变动的敏感性。
4. **责任风险**：某一持仓是否作为抵押资产或贷款交付给了其他机构。
5. **铸造风险**：资产发行方是否能够随意铸造新通证。是否建立了安全机制，以防止过度铸造。

[Chainlink储备金证明](#)（PoR）可以自动，可靠且及时地验证通证资产的链下或跨链储备。PoR利用预言机网络来验证通证资产的跨链或链下储备，为消费者，资产发行商和其他智能合约应用实现了透明的链上审计。Chainlink PoR获取链上数据（即：WBTC等包装资产），托管方的API接口或第三方链下证明（如：来自声誉良好的审计公司）。

Chainlink PoR可以在购买资产之前自动提供关于上述风险的数据，因此可以降低通证资产的流程风险并提高效率。当资产抵押率低于某一阈值时，可以用Chainlink PoR提供的数据来触发熔断机制。Chainlink PoR可以证明通证资产的跨链和链下抵押储备金，因此能够提高资产管理者的风控能力，并预防系统性风险的出现和蔓延。



通证资产最主要的一个风险是铸造的通证价值超过链下抵押资产当前的市值。Chainlink PoR可以用来触发熔断机制，控制通证资产的铸造功能。当监测到抵押资产价值低于某一阈值时，就会禁止铸造新的通证。

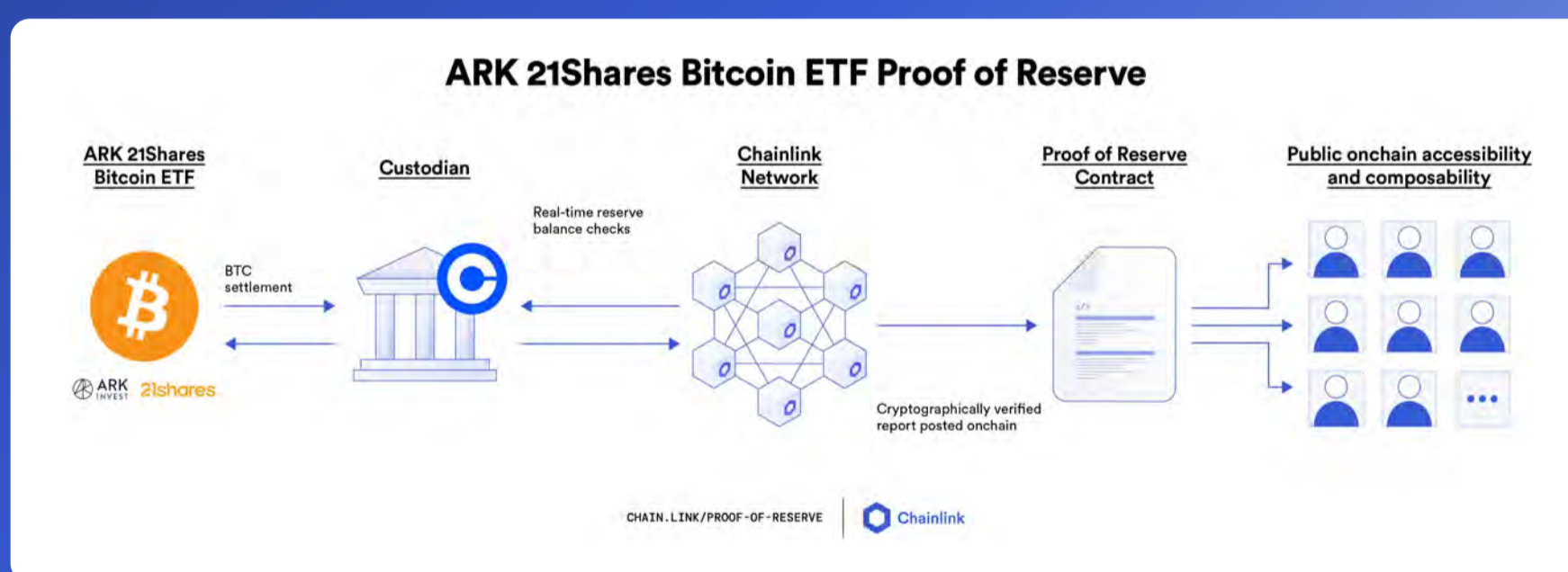
案例分享：21Shares集成Chainlink储备金证明，提高ARK 21Shares比特币ETF的透明性

资产管理公司Ark Invest和21Shares发布了ARK 21Shares比特币ETF，简称ARKB。该ETF是顶尖的现货比特币ETF，在管资产超过27亿美元。

21Shares在以太坊上集成了Chainlink储备金证明，增强ARKB比特币储备的透明性。集成了Chainlink储备金证明后，21Shares就可以清晰查看ARKB的比特币储备金。

ARKB的底层比特币储备金及其历史记录都会通过Chainlink储备金证明向公众公开。这样做可以使ARKB投资者对ETF的比特币储备金更放心。储备金数据来自链下Coinbase数据，由于Coinbase可以直接访问储备资产所在的账户或金库，因此可以计算储备金的总值并通过Chainlink预言机将数据传输到链上。

21Share US的联合创始人兼总裁Ophelia Snyder在通稿中表示：“集成了行业领先的储备金证明Chainlink PoR后，我们将为数字资产管理行业制定新的透明性和安全性标准。此次合作让我们可以为ARKB投资者提供前所未有的透明性和安全性，并让我们可以更好地为客户提供安全，透明的资产管理服务。”



案例分享：Backed Finance集成Chainlink储备金证明，提高bToken储备金的透明性

Backed在链上发布了代表结构性产品所有权的通证bToken。每个bToken都是1:1抵押，并且可以按现金价值赎回。

Backed集成了Chainlink储备金证明，以提高其储备金的透明性。此次集成将增强市场参与者对bToken抵押资产的信心。

通过Chainlink储备金证明为bToken集成链上数据后，DeFi协议就可以几乎实时查看抵押资产的情况，这将有助于降低生态风险，防范异常事件并增强投资者对bToken可赎回性的信心。

“资产管理者看到了通证化的价值，并正在迅速加入这个赛道。我们相信在未来，金融系统将充分实现全球化，操作将是实时的，而且其底层将由区块链技术支撑。Backed将作为通证化平台推动这一转型，我们致力于推动生态快速成长，而这一切都离不开安全，可靠的第三方数据基础设施。

我们非常高兴与Chainlink紧密合作，将现实世界的数据传输到链上。Chainlink Price Feeds和Chainlink储备金证明作为行业标准，将为我们的现实世界通证资产带来更强大的功能和更高的安全性。”



BACKED

Backed联合创始人Adam Levi

数据服务

关键问题：

- **通证资产是否拥有安全的储备金证明机制？**
如果没有，那么资产可能会遭受无限铸造攻击（infinite mint attack）
- **通证资产的铸造机制是否安全，是否设置了熔断机制？**
如果没有，那么资产可能会遭受无限铸造攻击（infinite mint attack）并铸造没有抵押资产的通证。
- **通证资产的储备金证明机制是否透明？**
如果不透明，那么用户对于资产就会不放心。
- **风控框架中是否设置了自动熔断机制？**
如果没有，那么通证资产可能会因为储备金不足而导致坏账。

除了储备金证明外，通证资产在整个交易生命周期里还需要接入一系列其他的数据集。如果没有数据，通证资产只能在链上表示对应的链下资产，除此之外毫无用处。链下数据不仅需要传输到链上，而且链上数据还需要传输到链下，才能够保持链下系统与区块链网络同步。

以下重要数据需要在链上和链下系统之间保持同步：

- **汇率以及按市场计价的可信估值**，这类数据的作用是正确为资产定价，确定贷款抵押率，并且展开多币种交易。
- **状态更新数据**，这类数据的作用是确保链下系统了解链上交易和资产的当前状态。
- **金融市场数据**，比如流动性，利率，融资率以及股息等。这类数据的作用是管理链上风险并展开公允市场交易。
- **合规数据**，比如KYC/AML，对手方限制，账户或资产限制以及法律法规等。这类数据的作用是遵守监管规范和组织内部政策。
- **其他数据**，比如ESG数据，代理投票以及结算规则等。这类数据的作用是为链上资产提供服务。

预言机数据可以自动触发智能合约，因此金融机构必须先仔细评估预言机协议的安全性，再将其集成至通证资产提供服务。预言机攻击是常见的攻击向量。迄今为止，DeFi行业由于预言机数据相关的攻击迄今为止损失了[5亿多美元](#)。

Chainlink为DeFi提供了行业标准的市场数据，在保障安全可靠的前提下已经为DeFi应用实现了超过10万亿美元的交易额。[Chainlink Data Feeds](#)基于去中心化的预言机网络实现，网络节点具有良好的声誉，从优质数据源聚合数据并传输到链上，中间没有任何单点失效风险。

案例分享：Paxos集成Chainlink的PayPal USD Price Feed

PayPal推出了美元抵押的稳定币PayPal USD (PYUSD)，将区块链技术集成至其支付平台。PYUSD由Paxos发行，是由美元存款，美国国债以及现金等价物抵押的可编程稳定币。Paxos是区块链基础设施和通证化平台，受到纽约金融服务部门监管。PYUSD可以传输到以太坊，并在以太坊上为DeFi协议做抵押以及用于链上支付。

PYUSD的储备金包括美元存款，美国国债和现金等价物，因此可以保障用户资金一比一赎回。另外，Paxos还会每月发布[储备金报告和验证报告](#)。

为了加速PayPal USD的采用，Chainlink在以太坊主网推出了PYUSD Chainlink Price Feed。PYUSD Price Feed可以在链上为Paxos和PayPal提供精准、可靠且去中心化的PYUSD市场喂价，并为用户提供所需数据，围绕PYUSD创建安全的市场，并集成至各种应用场景中。

PYUSD是Chainlink企业级数据基础设施的典型用例。Chainlink数据基础设施可以帮助大型企业和顶尖金融机构参与并发展链上经济，推动通证资产扩展至日常应用场景，并扩大链上金融的规模，覆盖全球几十亿用户。

“资产管理者尽早参与通证化市场将获得巨大机会，因为大量资产在未来都会转移到链上，以获得更高的流动性，透明性和市场覆盖。Paxos可以帮助金融机构和企业发行通证资产，而Chainlink平台则为行业制定了标准，为通证资产带来更强的可编程性和关键功能。”



PAXOS

Paxos的稳定币合作关系高级总监Nick Robnett

身份验证

关键问题：

- **身份信息在链上和链下之间互传的时候能否保密？**
如果不能，那么可能会削弱通证资产获得的服务质量。
- **资产发行商是否能够验证谁在与他们发行的通证资产交互？**
如果不能，那么未经许可的用户可能会与通证交互。

由于通证资产代表了链下资产的所有权，因此资产发行商，金融市场基础设施以及资产管理者必须要清楚地知道这些资产的所有者是谁，这样做既可以满足合规要求，又可以规避风险。然而，我们不能在链上公开披露这些敏感信息，因此必须要有保障隐私和安全的预言机解决方案。

许多数据库都会储存敏感数据，各类用户和机构都会使用这些数据库储存数据，其中不乏政府和大企业，而政府和大企业对于数据托管方的安全性和稳健性尤为重视。在这类应用场景中，身份预言机 (identity oracle) 可以发挥关键作用。预言机采用一种叫作零知识证明的加密技术，在可信数据库或系统中确认数据的真实性。最关键的是，在验证身份数据的过程中，外界或预言机完全无法看到数据。这种身份预言机可以验证特定的信息，比如身份数据和财务数据，或者关键的政府记录，而且整个过程中数据一直都存放在安全的数据库中无需转移。这个方法避免了数据在多个系统之间传输，因此保障了数据访问的安全性，机构可以将保密数据储存在可信数据库，并选择性地控制访问权限。

[Chainlink DECO](#) 是正在开发中的隐私保护预言机协议，利用零知识证明技术让机构和个人证明通证资产的来源并验证其所有权，同时无需在链上或向第三方透露个人信息。

案例分享：与Teller展开DECO概念验证，实现低抵押贷款

Chainlink Labs与多个关键合作伙伴展开了一系列alpha阶段的概念验证，目的是验证DECO在各个智能合约应用场景中的功能和可用性。概念验证中采用了DECO生成零知识证明，以证明来自不同数据提供方的敏感信息。整个过程很好保障了数据隐私，而且也不需要数据提供方对其服务器做任何改动。

其中一个概念验证是与Teller共同开展的。Teller是数字资产低抵押借贷协议，采用了DECO证明用户链下银行账户余额大于贷款要求的动态最低门槛。如果用户账户余额大于最低门槛，那么贷款方的风险就会相应降低，因此可以大幅降低贷款的抵押率。比如，如果贷款方希望借入5000美元，那么他就必须证明自己银行账户里至少有5000美元，以证明自己的还款能力。

DECO可以用来证明贷款人的信用，而且不会侵犯其数据隐私。最关键的是，贷款人在证明自己还款能力的同时，还可以隐藏敏感的个人敏感信息，比如姓名、财务状况以及数据访问权限等。



自动化

关键问题：

- 我是否希望使用成熟且去中心化的第三方服务来实现智能合约自动化？

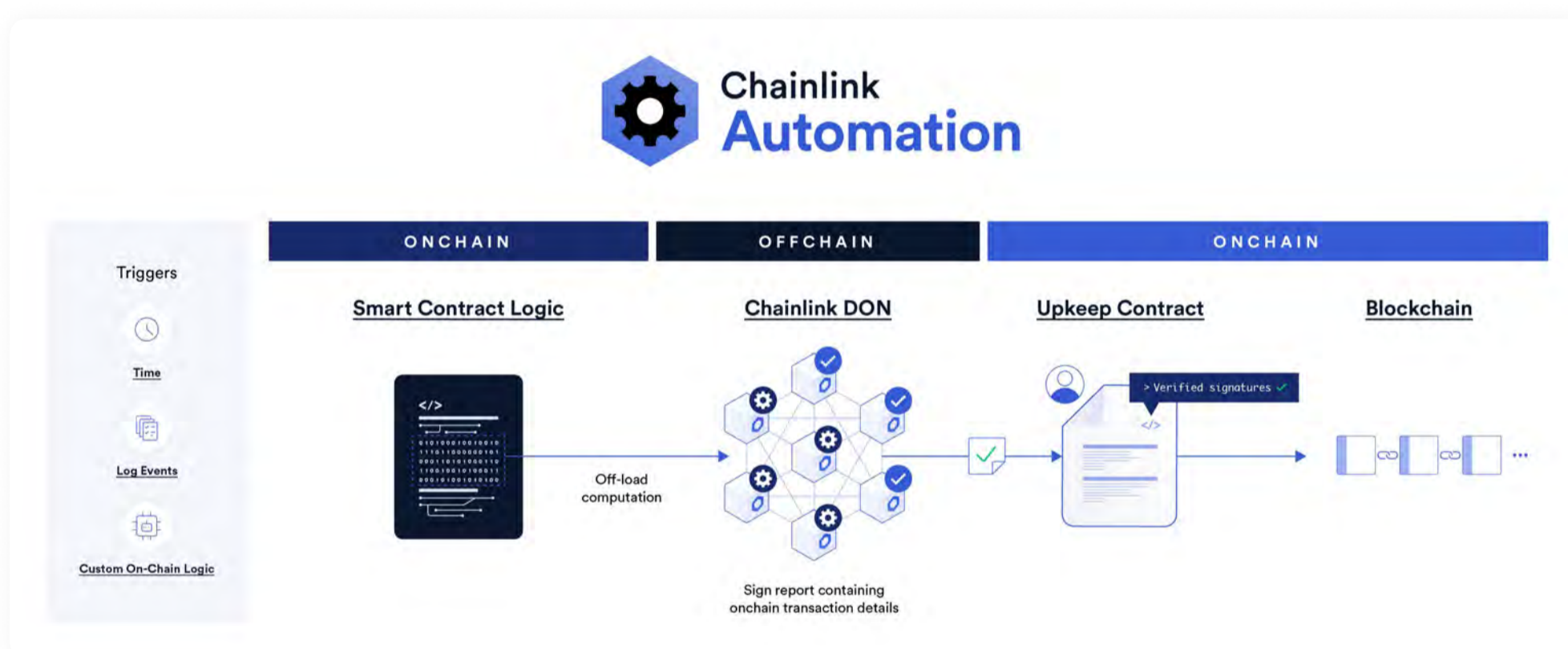
如果不是，那么我就需要花费时间和资源开发并维护内部解决方案。

- 我的公司是否能够以稳健、可靠的方式触发智能合约？

如果不能，那么链上自动化流程可能会不可靠。

自动化是支撑智能合约的底层基础设施的组成部分，既能提高效率，又能保障流程安全性。比如，资产管理者可能需要将资产交易流程自动化，或基于时间安排或市场信息自动重新平衡客户的投资组合。另外，金融机构也可能需要将数据上链的频率或智能合约的功能自动化，比如自动查看贷款抵押率或发放股息。如果满足了特定的触发条件，自动化基础设施就可以调用智能合约功能，并可靠地执行预定义的链上操作。

Chainlink Automation是可靠，高性能且gas效率极高的智能合约自动化解决方案。用户可以将成本高昂的链上计算交给链下的Chainlink去中心化预言机网络（DON）执行，大幅降低成本的同时还能保障同样水平的加密安全。Chainlink Automation是Chainlink平台的一项重要服务，可以与Chainlink Data等其他Chainlink服务组合，并实现更强大的功能。



市场对Chainlink DeFi收益指数的需求



Chainlink平台致力于开发各类稳健的金融服务。其中一个案例就是Chainlink DeFi收益指数（Chainlink DeFi Yield Index），简称CDY指数。这个数据产品目前正在开发中，在[近期发布的产品研究报告](#)中有所介绍。

CDY指数聚合了整个市场的DeFi贷款利率，并将数据发送到链上智能合约。开发CDY指数的目的是保障数据的准确性、稳健性以及市场覆盖率，这将提高链上借贷的曝光率，并提高资本效率和流动性。

Chainlink在保障安全性和可靠性方面拥有成熟的经验和往绩，深耕DeFi领域多年，其去中心化的数据聚合方法也一直运行稳健，因此完全有能力开发覆盖全市场的DeFi贷款收益率指数。包括Aave和Compound在内的几乎所有主流借贷协议都集成了Chainlink Price Feeds。

Chainlink DeFi收益指数将为各类市场参与者提供更多的机会：

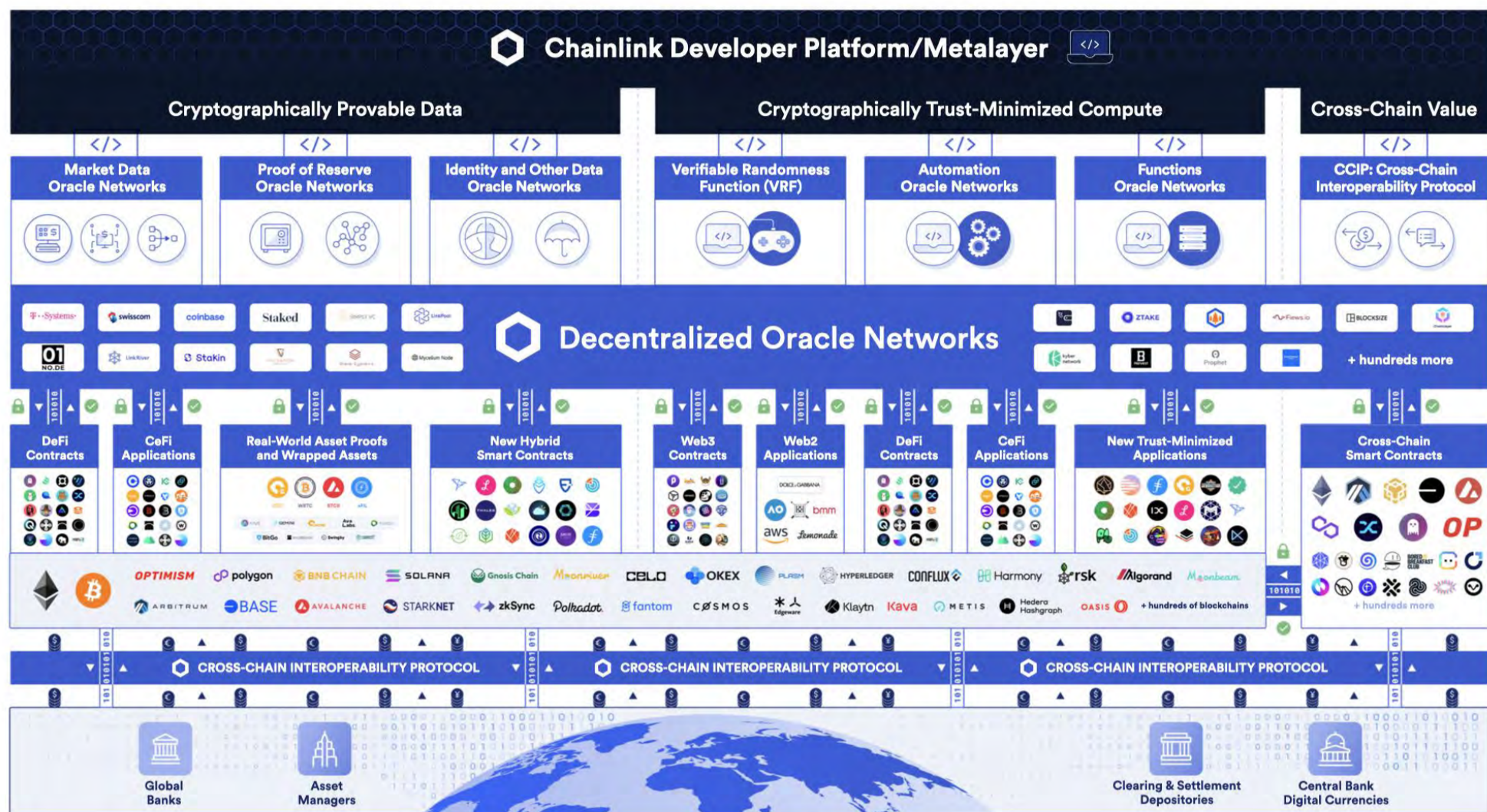
- **资产配置者**可以发现之前从没考虑过的新收益机会。CDY指数可以为传统金融机构打开DeFi世界的大门，并帮助它们寻找新的途径获得收益，管理风险并高效配置资产。
- CDY指数可以有效扩大资金流入，造福**借贷协议**。借贷协议可以获得更多资产，因此可以提高协议收入。而收入可以用来增强协议功能，安全措施以及用户体验。
- 随着更多资金流入，将加深流动性池的深度，降低滑点，**用户**也可以获得更好的贷款体验或更高效地退出仓位。这些好处将吸引来更多用户，因此可以为协议带来更多收入，并为流动性提供方带来更高的收益。

若想了解你所在的组织如何利用Chainlink DeFi收益指数实现价值，请[联系Chainlink团队](#)。

抓住通证化机遇

通证化和区块链技术在资产管理行业的不断普及势必推动金融服务行业中市场基础设施的转型。资产管理者应该为即将到来的转型做好准备，站在变革的前沿，抓住这个巨大的市场机遇。

Chainlink平台将作为桥梁，为资产管理者弥合传统金融和链上金融的差距，帮助其顺利实现转型。Chainlink平台提供了一整套通证资产服务，资产管理者可以利用这些服务为自己的通证资产投资组合实现安全且高级的编程功能，并同时在评估其他资产安全和价值的过程中使用Chainlink作为风险评估框架。



作者

Colin Cunningham

通证化与联盟负责人

colin.cunningham@smartcontract.com

Raoul Schipper

战略客户

raoul.schipper@smartcontract.com

Jimmy Haight

通证化市场营销

jimmy.haight@smartcontract.com

Wei Dai

通证化战略

wei.dai@smartcontract.com

Andras Beak

文案

andras.beak@smartcontract.com

如果你想进一步了解Chainlink可以如何帮助你实现通证化战略，请[联系Chainlink团队](#)。