商娱链

The Chain Of Business Entertainment

CBE，创造互联互通新世界

CBE ,Creating Interconnected World

White Paper Version 1.0

目录

第1章

背景概述

区块链背景：区块链技术是21世纪的重大创新技术，它是数字化资产的分布式账本，是构建价值互联网的基石，是驱动分享经济发展的新引擎。2009年初，比特币网络开始上线运行，由此开启了第一代区块链的序幕。支撑比特币运行的底层技术--区块链实际上是一种极其巧妙的分布式共享账本及点对点价值传输技术。各机构纷纷在比特币网络的基础，开始了第一轮的区块链的探索。2014年前后，世界开始认识到区块链技术的更大价值，并将其用于数字货币外的领域，如分布式身份认证、分布式自治组织、分布式域名系统等。在这个时期，以以太坊为代表的综合功能公有链开始出现，并以智能合约方式支持多样化业务，并衍生出了多个分布式的行业应用（DAPP）场景！运用区块链技术从各个现实行业领域诞生解决的方案越来越多，慢慢时代与发展开始从信息互联网向价值互联网（区块链）转变！

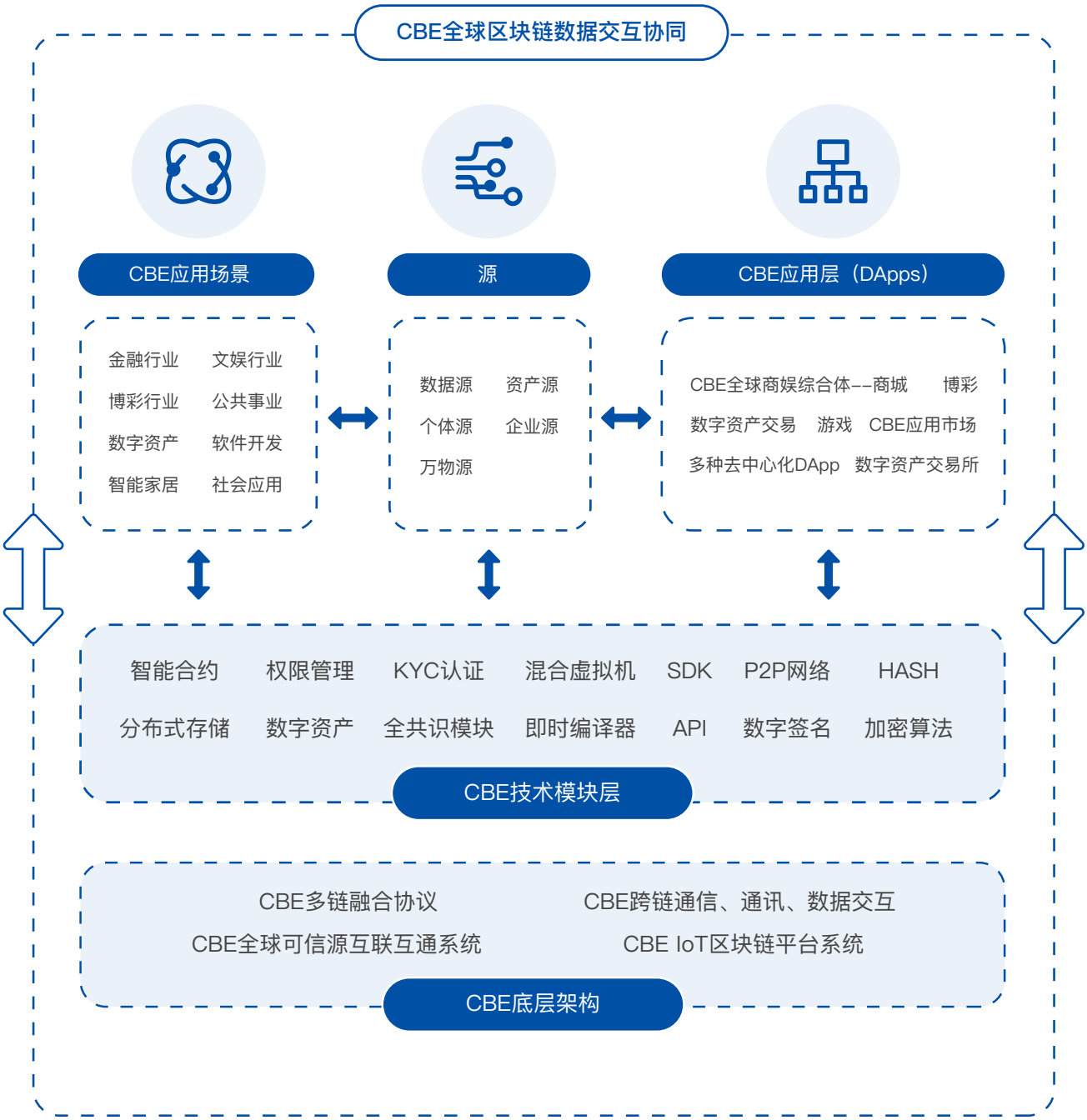
物联网背景：物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是：“Internet of things（IoT）”。顾名思义，物联网就是物物相连的互联网。物联网（IoT），物联网是让日常物品连接到互联网并且互相通讯，目的是让用户有更智能、高效的体验。物联网让一切设备互联，包括可穿戴设备、家用电器、衣服鞋帽等等，所有一切都争先恐后想连到“云端”。总体来看，我们将全面进入万物互联时代，物联网正逐渐改变我们的生活。

第一章：背景概述

数字虚拟货币背景：随着区块链市场不断增长以及越来越多的加密资产的发行引入，全球加密数字货币市值最高一度突破6000亿美元，截至2018年9月4日，全球数字货币市场总市值达到2373.12亿美元，共有1910种数字货币。时间回到一年前，2017年9月4日，全球数字货币市场总市值为1622.65亿美元，数字货币数量仅为1077种。在这一年时间里，全球数字货币市场最高值出现在2018年1月，总市值达到了8238亿美元，较2017年9月4日相比上涨407.89%。在全球对通证经济重视与认可之际，因ICO的风行，全球数字货币发行超1600种，前十名币种市值占90%，数字资产的价值与流转问题日益严重！

商娱链CBE（The Chain Of Business Entertainment）是打造区块链世界互联互通的平台，以数据交互超级社群，提供区块链技术无界交互体系及区块链跨界物联网+商业+娱乐+生态定制化服务。致力于影响整个真实世界与区块链世界的有效连接，使区块链世界各个体系之间相互贯通与链中场景交互，实现区块链多链联接，让区块链跨界交互的价值最大化；CBE将链动区块链信任数据中的每一个信任/数据源，共同打造区块链无界信任生态体系的超级社群交互。成为区块链最大的数据交互协同中心和超级社群无界交互平台，实现数据权属变现权益价值，是CBE追求的目标。

- 作为创新分布互联互通的平台，CBE将构建一个开放、协同的分布式无界融合的信任生态系统，基于区块链/分布式账本的互联互通体系，结合了分布式多维身份认证体系，实现链与链的连接、链与中心化的连接、链下与链上价值的连接的分布式点对点的可信价值体系，构建跨界无界的分布式社区交互的信任基础体系，为各类分布式DApp服务提供完整的底层技术基础、可信数据基础，让区块链世界互联，各行业各类应用都可以在信任网络的大数据库背景支持下进行跨界无界社区交互，将全球区块链的所有信任数据流通价值变现！
- CBE全球区块链数据交互协同中心将让所有区块链网络和体系无缝衔接，让分散的中心化系统（如IoT系统）相互交融并高效、便捷地连接链中及链下世界。致力于让区块链成为普惠的技术，让区块链技术和应用的创造更简单，让区块链多链链动跨界交互价值最大化，最终实现未来区块链多链高效发展的信任无界交互生态。
- 同时CBE将基于互联网平台与物联网平台（IoT），以区块链底层技术为基础，运用去中心化的大数据平台，点对点交易实现物联网万物互联互通，针对商品追根溯源，可以将数据权属化，从而解决互联网数据可以无限复制的问题，实现去中心化的信任，不依赖于任何第三方，通过数据来保证交易不会被抵赖，实现了点对点的可跨链跨界跨局域跨领域的价值传递，再结合数据资产和商家以及消费者的权益通证化，可以形成广泛的共享价值，共享流量，互换权益，数据流程对接和模式互补，创建一个可信、开放、共享、联合、协作的多层次立体的数字经济商业生态圈！


CBE全球区块链数据交互协同
CBE应用场景
源
CBE应用层（DApps）
金融行业 文娱行业
博彩行业 公共事业
数字资产 软件开发
智能家居 社会应用
数据源 资产源
个体源 企业源
万物源
CBE全球商娱综合体--商城 博彩
数字资产交易 游戏 CBE应用市场
多种去中心化DApp 数字资产交易所
智能合约 权限管理 KYC认证 混合虚拟机 SDK P2P网络 HASH
分布式存储 数字资产 全共识模块 即时编译器 API 数字签名 加密算法
CBE技术模块层
CBE多链融合协议 CBE跨链通信、通讯、数据交互
CBE全球可信源互联互通系统 CBE IoT区块链平台系统
CBE底层架构

第2章

信任、数据、价值

区块链即信任世界

区块链行业在发展过程中，发展成通过全民记账的点对点分布式账本。区块链的应用可以落地在各个领域，但是各个领域和应用场景无法实现互相融合贯通，数据的跨领域无界限交互传输也受到技术限制，区块链的应用搭建成本高，耗时长等问题仍是区块链技术的痛点。区块链/分布式账本体系的出现带来了更广层面的基础性技术信任框架，去中心化多方共同维护的技术信任， 在多方对等的情况下共同进行信息维护、数据协作、达成共识等，对各类协作中的数据、数字资产、协议进行可靠控制和技术手段下的保护，因此，区块链体系带来的新技术竞争不是单业务或单点的信任变化，而是一个体系化的生态型变化，这也是区块链具有变革性的要素所在！

区块链应用搭建成本高

在CBE上可以提供一系列的协议基础层与应用接口，简化了DAPP 的开发，组合的SDK工具包不需要专注于业务与场景的开发人员熟悉区块链的底层技术，任何应用服务提供方无需区块链底层开发能力便可以直接享受使用CBE提供的区块链技术服务。

打破单一信用体系

基于单一信息管理体系的个人认证难以对个人形成全面的、综合的的评价，难以准确获得人、物、财、事等多维度的准确认知与价值判定。而CBE可以为所有用户提供底层技术支持，用户能在平台上搭建区块，记录所有数据，加密生成数据库，资产上链与发行，资产/数据价值化，让各个区块联动交互，自动生成多维度价值体系。区别于现有区块链技术，联动各个领域、各端口、各用户，打破单一模式，实现多维度价值体系的构建。

区块链世界数据跨界交互难

CBE在分布式实体与数据信任基础上拓展生态与应用，将信任的应用扩展到很多的维度，从身份认证到数据交换，从分布式社区、分布式交易到分布式应用，结合底层的区块链分布式账本体系，联合各类服务伙伴在不同地域、不同领域提供多样化的信任服务，从而实现区块链世界的跨领域、跨地域、跨终端数据交互，联动区块链世界。

区块链各应用领域社群数据难以联通

CBE区块链的目标是实现跨领域跨界信息数据交互传输。现行区块链各应用领域社群是相对分散独立的，各社群之间的信任数据难以联动，多样化数据难以综合共识。CBE区块链致力于打造无界社群，将各个领域的社群进行联动融合，信息传输交互可以突破技术限制。各个社群的数据联动交互和透明化大大降低了入群筛选工作量，在社群入口把控时可以综合各领域信任数据，从而提高社群共性，达成社群与社群，人与人之间的共识。

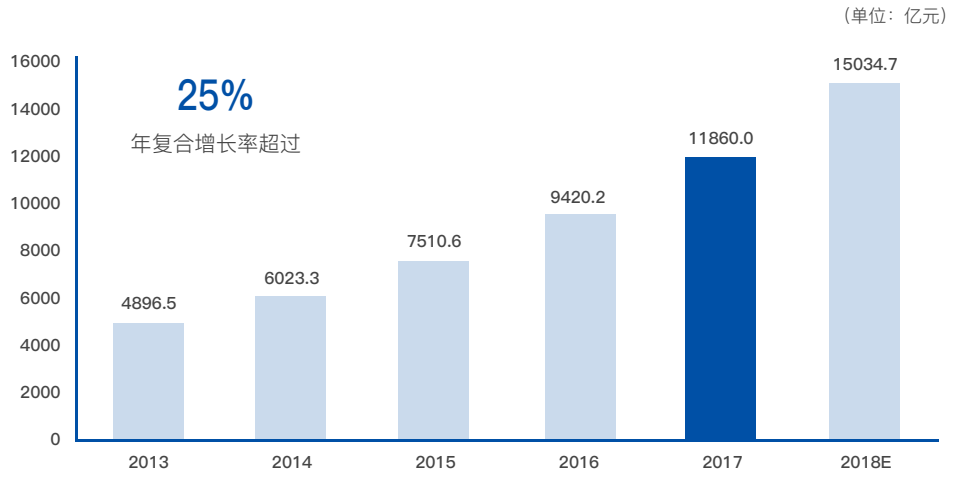
为了实现数据的采集与数据上链，让全世界的数据产出与信任数据的需求方、数据价值交易方，如：C端（Consumer 用户方）、B端（Business企业用户商家）、乃至G端（Government各个国家政府），包括万物与各行各业，可以跨界进行数据的交互协同，CBE也将结合物联网平台，以CBE强大区块链底层技术进行结合，打造数据权属化价值化后可跨领域、跨地域、跨终端数据交互，联动世界的完整解决方案！打造 信任即价值，数据即价值，共识即价值，万物价值化的全新价值时代！

物联网的新机遇

目前物联网（IOT）系统是围绕着中心化架构发展而来，设备和机器是通过集中式服务器配置在云上。随着IoT网络的快速扩展，传感器和设备节点以数十亿计的规模加入网络，集中式服务器的基础架构的维护也变得越来越昂贵，产生欺诈的机会也随之而来。数据隐私，安全和信任将成为迫切需要解决的优先事项！

IDC预测，全世界物联网解决方案的市场，将从2013年的1.9万亿美金增长至2020年的7.1万亿美金， 2019年将会到达67亿个物联设备发货量，复合年增长率61%。麦肯锡全球研究院估计，到2025年，物联网应用的经济规模将会在3.9万亿和11.1万亿之间！

2013–2018 中国物联网产业规模及预测



公众网络机器到机器（M2M）连接数突破1亿，占全球总量31%

数据来源：中国通信工业协会物联网分会

而区块链拥有去中心化、去信任和高安全隐私性三大特点，面对未来IoT设备规模的爆发性增长，应用区块链技术有望改善物联网平台的痛点：

降低交易前的验证成本：物联网区块链应用通过在区块链系统下记录不可篡改的优势，平台下的用户和设备不需要验证双方信息，只需要在交易时判断对方给予的条件与之前是否不同，区块链通过智能合约自动执行并不可篡改，保证了无需建立可信关系也可以完成交易功能。

降低运营管理成本：对于原本物联网设备来说，所有的操作都需要经过中心服务器的处理，带来了额外的管理、数据通信成本和处理时间的增加。通过区块链点对点网络技术，每个节点作为对等节点，可以不需要额外的协议、硬件支持和数据通信处理成本进行点对点的交互，从而降低成本。

保护数据安全与隐私：在区块链系统中，所有的数据传输都是通过严格的加密方式进行处理，并通过点对点的网络进行通信，不需要在交易中将数据信息委托给第三方来实现。并且根据区块链中信息不可篡改的特点，可以通过查看交易记录时间戳的方式，判断数据信息是否被窃取，保证了数据安全和隐私保护。

将物联网与区块链两大跨时代的强大技术组合--CBE，会打造以全新的强大技术与生态，与您共同迎接跨时代变革的挑战和机遇！

第3章

项目介绍

项目创新

CBE互联互通网络将结合物联网（IoT）技术平台与区块链技术，在分布式实体（终端机/用户）与数据信任基础上，将信任应用多维度拓展实现数据价值变现。从点对点，点到线，线至网，以人事财物，实现跨链、跨领域、跨系统、跨应用的互联互通体系的建立，提供万物互联互通的全球价值网络基础设施服务以及全球区块链数据的交互协作平台。

项目愿景

CBE是链动全球区块链数据的交互存储中转站，致力于影响整个真实世界与区块链世界的有效连接，让区块链世界各个体系之间相互贯通与链中场景交互，实现区块链与未来一切的连接。构建跨界无界的价值基础体系，让区块链世界互联，让各行业各类应用都可以在CBE的互联互通网络的大数据库/多终端区块链物联网的技术背景支持下进行跨界、跨领域、跨应用的分布式社区交互，将实体/虚拟/终端/IP等全领域的可信数据流通价值变现，让每一次的交互通过CBE推进价值化的滚动变现，链动整个互联互通网络中的每一个可信数据源。

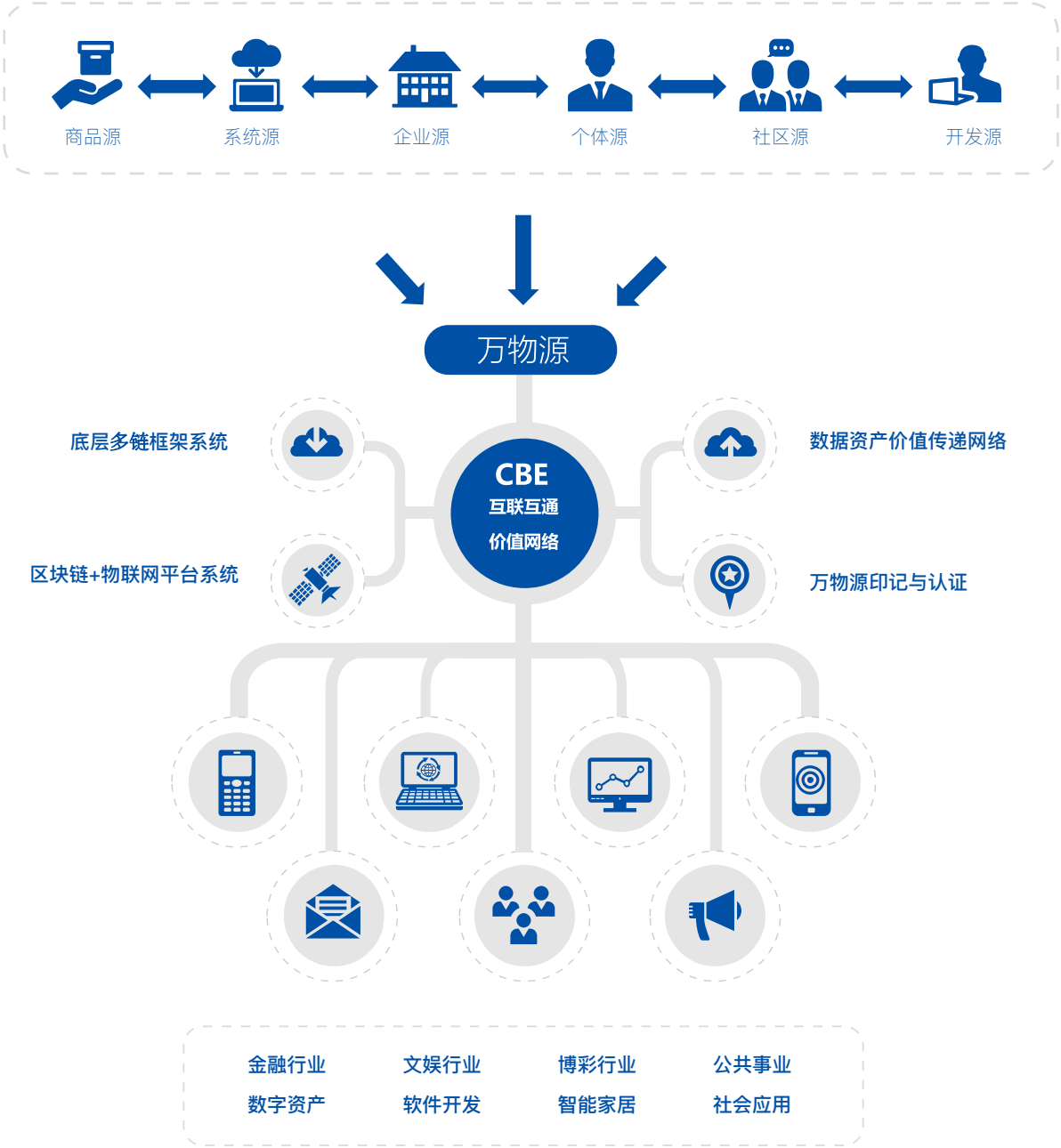
全球区块链数据交互存储中心让所有区块链网络和体系无缝衔接，让分散的中心化系统相互交融并高效、便捷地连接链中及链下世界。致力于让区块链成为普惠的技术，让区块链技术和应用的创造更简单，让区块链多链链动跨界交互价值最大化，最终实现未来区块链多链高效发展的信任无界交互生态。

第4章

CBE互联互通网络

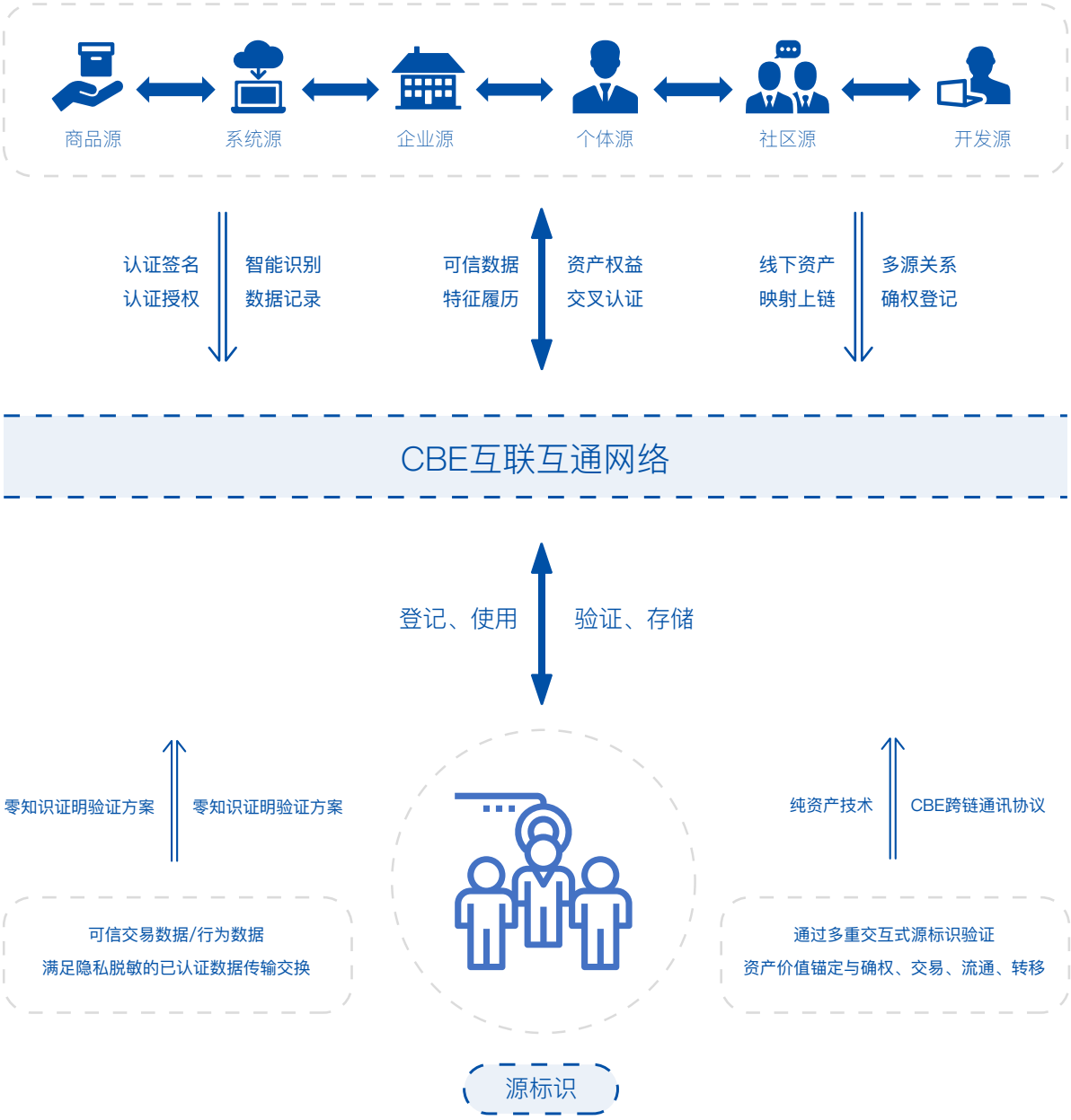
CBE通过源、互联互通网络、价值交互，建立了分布式与互联互通带来的价值自运转机制，为可信源的有效协同、为数据源的交互联通、结合互联互通分布式的多维实体价值变现体系，实现了链与链的连接、链与中心化的连接、链下与链上价值的连接的分布式的点对点的信任体系，构建跨界无界的分布式社区交互的价值互通网络。每个在参与主体网络中都存在利用PKI （Public Key Infrastructure）建立的身份标识，并且通过互联互通分布式账本进行公开信息记录与存储。各行业各类应用都可以在CBE的互联互通网络的大数据库/多终端区块链物联网的技术背景支持下进行跨界、跨领域、跨应用的分布式社区交互，将实体/虚拟/终端/IP等全领域的可信数据流通价值变现，让每一次的交互通过CBE推进价值化的滚动变现，链动整个互联互通网络中的每一个可信数据源。

■ CBE互联互通价值生态 ■



信任应用互联互通交互场景

CBE将作为互联互通生态体系的基础设施和互联互通式社区交互中枢，利用多链、多系统融合的协议网络，支持不同的业务体系，各个行业各类场景都可以进行各类应用的开展与协调，将应用在行业服务机构、金融资产/实体经济服务、社会各应用、公共事业、商业、泛娱乐行业等多场景使用，通过CBE互联互通价值网络，达到点对点协作，更是实现资产与价值的互通变现；CBE不仅支持新型的业务场景，更将为传统商业与物联网体系的流通，实现区块链一切商业相融贯通，为未来的商业提供可信数据与价值互换的基础。



互联互通源标识及价值体系

▪ 互联互通源标识 ▪

在CBE互联互通网络中所有参与源，包括万物、个人、团体、系统等在CBE网络中将使用统一的标识，CBE互联互通网络根据源标识进行价值权益管理与价值业务匹配，CBE互联互通网络将支持各类源的多重源标识管理。
源标识的登记、使用、验证、存储，都将结合CBE网络中的区块链加密技术、分布式账本技术、智能合约技术来实现各类源标识的隐私保护与安全交易。

源登记与识别：CBE将采用非对称加密 PKI 加密机制/第三方认证机构/授权服务进行各类源的身份登记与认证；

源流程：源主体将通过私钥信息与零知识证明验证方案，以CBE网络提供的分布式权益验证与交易/数据传输协同，达成网络共识，实现交易/数据传输与标识的传达，同时采用分布式账本技术，脱敏后实现标识与行为作为公开信息存储在CBE网络上；

▪ 互联互通价值体系 ▪

通过区块链技术可实现去资产数字化、数字资产价值确权、商品价值上链、归属权益化，所以登记在CBE互联互通网络上的所有资产都以特点价值的形式存在，参与各类源之间的交易，实现价值的确权、流通、转移、交易、权益。CEB网络的价值互联互通，包括：

资产价值化：CBE网络将以核心技术——纯资产，AI全局多终端数据库，从而在CBE网络中实现现实资产/数据/链上资产等的价值化。

价值流通：CBE为实现价值（数据/资产）的交互，将采用墨客原子跨链技术，来提供全局配置和调度服务，向下延展各种不同业务形态的子网，根据业务场景、隔离机制、性能开销等不同进行划务分逐层往下划分，以多链并行、CBE跨链通讯协议、多重签名账户实现链上多链与各个区块链的价值流通交换，跨链通信、共识等问题。

届时CBE网络的价值产生通过每次共识达成后释放CBE TOEKN给参与共识的节点。
此外CBE的纯资产技术将支持参与的各类源进行线下资产映射上链。产生的价值纯资产，会基于CBE实现价值的互联互通。

第5章

CBE核心技术


DApp架构体系
各类应用（dApps）
应用资产价值化
AI全局多终端数据库
SDKs
APIs
IoT平台体系
管理与加密安全
物联网协议
IoT设备接入
数据跟踪与分布式存储
APPS
IoT应用
区块链体系
可插拔式模块
纯资产协议
多链并行技术
数字资产跨链交易/交换
智能合约

CBE的底层架构将提供完整的DApp框架体系、IoT平台体系、区块链体系；

DApp框架体系：CBE提供DAPP 应用开发组件与SDK，简化DAPP 的开发，组合的工具包不需要专注于业务与场景的开发人员熟悉区块链的底层技术。此外CBE网络提分布式可信数据/资产的数据库，为分布式社群交互使用推广与价值跨界流通提供平台，进一步支持各类上层应用的实现。

IoT平台体系：CBE将根据多种不同IoT终端源提供实现端到端系统架构与管理，并将IoT平台体系的数据进行采集、上链、签名加密等一系列留存；物联网平台支持供应链跟踪和产品溯源、数据传输、云数据平台、分布式存储等内容。在IoT平台体系，终端源将使用轻量级嵌入式设备和移动设备运行的应用程序实现更高效更轻的数据采集；

区块链体系：包括纯资产技术、智能合约体系、安全体系、存储体系、跨链体系，同时对底层复杂的技术体系及异构的系统进行了融合，实现支持兼容各类主要协议、密码标准的分布式实体管理和多维认证协议，并支持对各类异构区块链和传统信息的跨链、跨系统交互映射。并提供了安全数据存储、异构智能合约、硬件密匙管理、加密数据分析等技术体系。

■ CBE区块链层技术架构 ■

CBE区块链层技术架构

子链技术：CBE链底层采用墨客子链技术，通过分层处理，由母链解决全局一致性和双花问题。DAPP的智能合约部署在上层子链中，由子链保存状态。子链采用定期刷新的机制将自己状态的hash写入底层区块链，以实现一致性。

分片技术：CBE链充分运用墨客分片技术，实现一个合约对应于一个系统分片。合约创建时自动随机选择相应数量的节点形成一个分片来处理这个合约。这个合约的生存周期包括从创建到结束合约都在这个分片中实现。中间如果需要，可以重新洗牌来选择新的分片节点，用户也可以实现自己的共识协议，作为SCS的一个插件。

项目方利用CBE多链系统创建自有区块链时，可以自定义共识协议，满足业务需求。并可以借助分片技术，实现一个业务一条区块链，TPS可以达到以太坊的100倍以上。

分片处理的节点称为SCS，其特点包括：

每个分片有自己的存储，就是子链。

SCS可以有不同于底层的共识方式，比如pos，pbft。

SCS的区块生成时间可以与底层不一致，比如可以采用快速的区块周期来进一步提高处理速度。

SCS周期性的向底层flush结果，从而获得阶段性的全局一致性。

▪ CBE区块链层技术架构 ▪

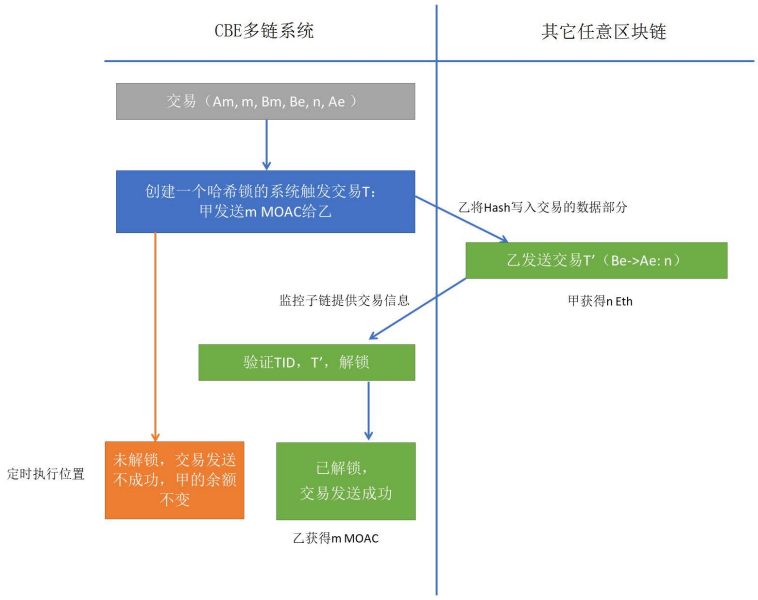
费用分担：DAPP的使用者可以采用直接调用的方式，不需要支付任何gas费用，对DAPP的应用发起调用。如果需要防止用户滥用，DAPP自己可以实现相应的处理方式。上层的共识协议不需要消耗大量的能源来获得随机数，而是纯粹处理智能合约的执行或者服务，对系统的要求非常低。节点数量增加，然后通过分片的方式支持成千上万的DAPP运行；反过来，DAPP持续的支付费用可以支持更多的上层矿工。这样就形成了一个开放的，正反馈的循环，使得CBE多链系统成为一个巨大的，适合DAPP的生态圈。

跨链：CBE多链系统采用墨客特有的系统定时触发功能和子链功能，完美解决了目前跨链方案的两个难题：1、需要跨链的每个链都支持闪电网络，也就是需要哈希锁和时间锁的功能，现有的链如果没有这个功能的话，需要进行硬分叉，很多情况下并不现实；2、整个交易的过程是个交互手动的过程。用户乙必须等待甲的公布，之后要确保在对方网络中递交合适的信息。如果需要实现自动化的话，会比较麻烦，需要额外的基础设施支持，比如类似Cosmos的拜占庭容错hub支持。

系统定时触发功能是设置在指定的未来区块位置执行某个交易。这个设置是100%会被执行。

CBE多链系统通过其他区块链的确认交易信息解锁交易，实现原子操作。

其巨大优越性在于，对其他区块链没有新的要求，只需要交易能附加数据信息，这个功能每个区块链都有。因此，跨链机制可以实现与所有的区块链的跨链操作。



CBE核心记账与共识机制

CBE链将创新性地采用超级多维分层多共识模块（SCM），通过可插拔式、多共识算法并存的机制，并通过智能合约的执行确认与区块生成各自采用独立的共识机制，以便减少区块生成过程中夹杂处理的额外环节，更合理的利用CBE平台资源，提高CBE平台整体共识性能。

同时CBE网络支持多链并行技术，由于CBE技术平台支持插件化的共识算法，每个在CBE网络发行的子链/DApp都可以采用独特的共识系统和算法。如：POW，POS，dPOS，PBFT，POC 等。

- POW是一种依赖机器进行数学运算来获取记账权（挖矿）。
- POS主要思想是节点获取记账权的难度与节点持有的权益成反比。
- dPOS节点选举若干代理人，由代理人验证和记账。
- PBFT是一种采用许可投票、少数服从多数来选举领导者记账的共识机制。
- POC 根据容量进行共识的一种协议

未来基于CBE链发行的资产/应用，可以在超级多维分层多共识模块（SCM），通过可插拔式、多共识算法并存的机制下采用独立的共识算法，未来推出的CBE全球商娱综合体可实现所有商家都是CBE的子链，都可使用各自契合的共识算法搭建分布式应用。

CBE其他关键技术和组件

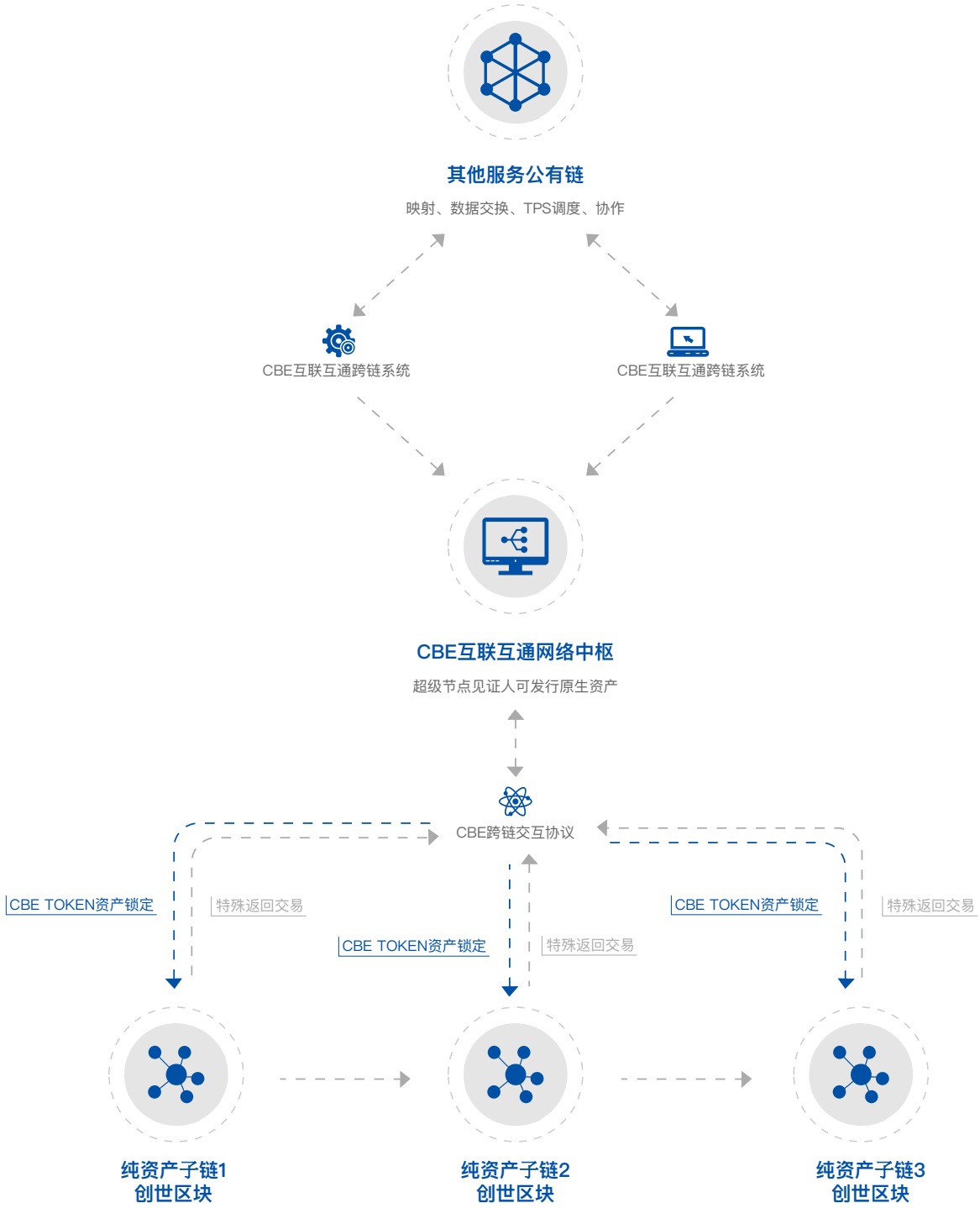
混合预言机：智能合约将应用于真实的商业环境，而且数据也将来自真实环境。“预言机”提供解决方案让区块链的智能合约获取现实世界的不确定数据信息，但这一链接链上与链外的环节存在众多无法去信任的环节。如何保证预言机读取的数据准确、如何保证预言机不受攻击和控制都直接影响智能合约的实用性和扩展性。所以CBE将开发分布式自治组织DAO功能和链外的数据交互功能（大数据/人工智能）融合的可信信用协议标准，即采用特定的共识机制对预言机提交信息的确定性做出判断，让信息知晓者在经济利益驱动下基于区块链数字身份提交现实世界的数据信息，一定的惩罚机制也在一定程度确保信息向着数据的确定性和有效性的方向。

跨链多链并行技术：CBE 能够实现跨链通信和共识。通过跨链通信和共识模块能够快速的对接不同的区块链，并形成数据交换。就像一个通用的国际空间站，能够和任何一个不同国家的空间站进行对接；CBE是区块链领域里的国际空间站。CBE不仅能够和其它的链进行通信，还能成为两个不同区块链通信的桥梁。以及能够对接无数个不同的区块链形成一个以CBE为中心的区块链通信交换中心。

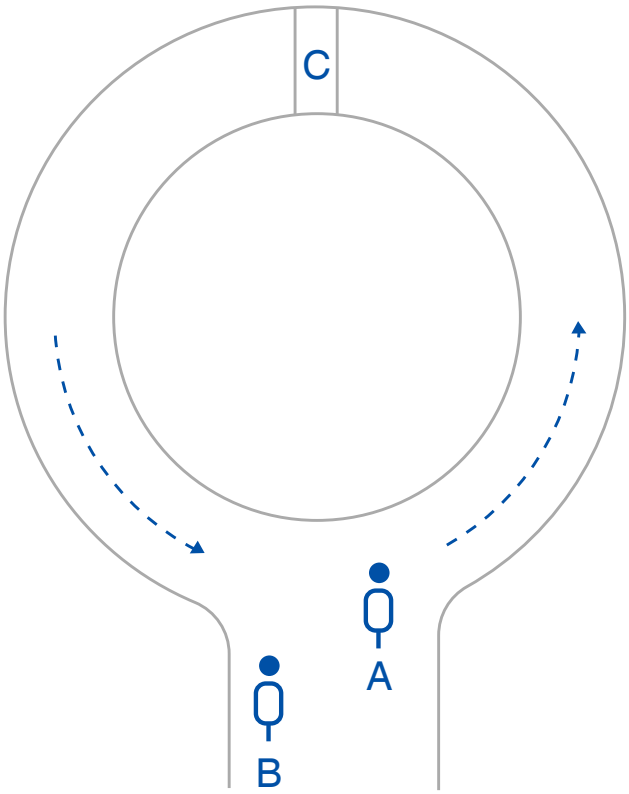
CBE跨链结构将分为多层，将实现链与链、链与传统中心系统的连接和协同工作，支持多并发的机制，以便分布式应用进行事务控制。CBE网络核心运行环境 DAPP SDK 中提供了调用其他链标准 API，也提供了调用现有主要区块链平台（BTC、ETH、Ripple、Stellar、NEO、Dash、Hyperledger 等）的 API，开发者在 DAPP 中调用这些 API 即可实现与其他链交互，也可以实现与传统中心系统的交互。功能组件层提供统一身份认证，以及链服务注册、链服务发现、链服务质量评价等功能，以便链服务与链服务、链服务与中心系统提供的服务协作运行。

- 顶层横向结构 –– 设置以STP（超级传输协议）实现多条链的交互，对应用链提供技术性服务与全局配置调配；
- 下层纵向结构 –– 针对以不同商业应用场景、不同商业逻辑、不同地域＆用户，可设置多条应用资产链，加以应用协议，实现应用链之间协作，同时使用智能合约、数据交换等基础性服务；

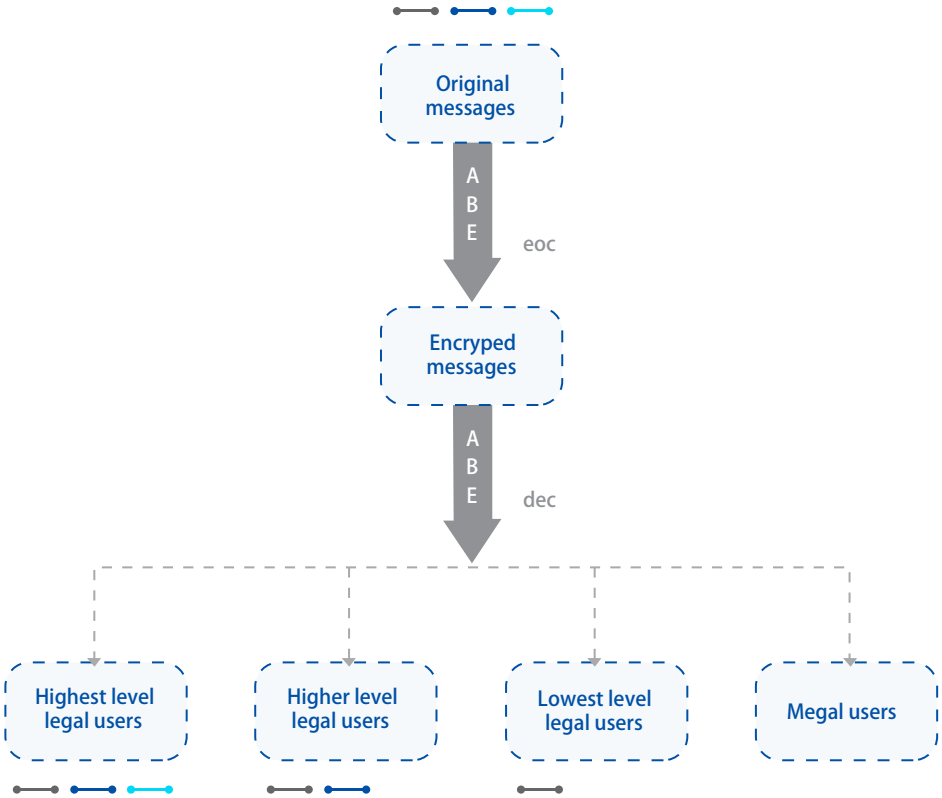
■ CBE跨链服务多链并行协作工作原理 ■



基于za-SNARKs的零知识证明的签名验证方案：CBE将基于za-SNARKs算法架构来验证交易数据，zaSNARKs是一个简洁的非互动性的零知识证明,一个SNARK执行的基本操作就是将能够解密的数据 编码到回路中，证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。比如，在图中，A要向B证明它拥有环形走廊中的那道门C的钥匙，而不能让B看到A拥有的钥匙。B可以要求A从环形走廊的入口进去，从唯一出口出来，则可证明A拥有那道门的钥匙。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程无需向验证者泄漏任何关于被证明消息的信息。



CBE属性加密分级访问控制：从安全的角度考虑，区块链上的交易信息和货物的位置数据都会泄露一定程度的隐私。因此为了确保用户有一个安全、隐私的交易环境，在区块链中需要采用合适的加密方法。数据访问控制是确保合法用户访问能力，同时阻止未经授权的用户访问数据的方法。在我们的设计中，这种技术可以支持供应链中的分级访问控制。



例如，我们可以将货物从 A 到 B 的位置信息作为原始消息，在系统中有不同访问权限的分等级的用户。如下图简化的三层结构所示，非法的用户看不到任何消息，最低等级的用户只可以看到能被所有用户解密的黑色线段。而红色线段只对最高等级的用户可见。能实现这个分等级结构的技术之一就是基于属性加密（ABE）。在 ABE 结构中，我们将身份视为一组描述性属性。这是一种一对多的公钥加密方法。这种方法不仅能解决对称加密中的秘钥分发问题， 也可以将物联网设备捕获的信息与不同用户之间共享！

AI全局多终端数据库：AI全局多终端数据库，是一个可插拔 key-value分布式数据库接口。它提供了多重后端数据库组件选择，其中包括levelDB、RocksDB、TiDB、cockroachDB 等。
AI全局多终端数据库是为区块链/分布式账本以及IPFS高度优化的数据库组件。提供了分布式处理、可扩展、实时链上索引及链外数据交互的能力，将应用在区块链与物联网、大数据、区块链与人工智能联合数据训练等计算相关的场景。

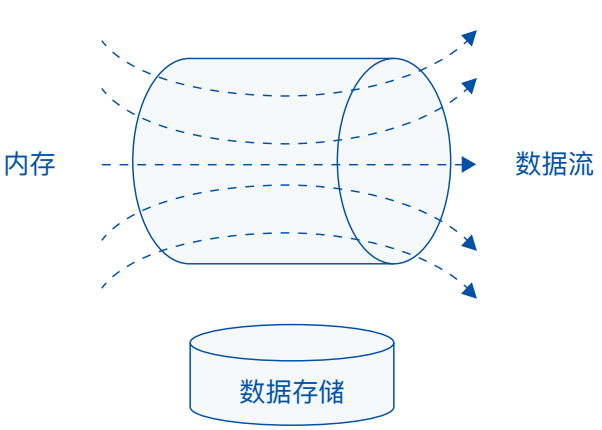
默克尔证明与SPV交易验证：采用默克尔树构造默克尔证明解决SPV的简单支付验证机制：对于比特币、以太坊等数字资产平台，客户端通常只需要关注自己的帐户信息，如果完整地同步所有帐本信息会造成效率低下。为了支持CBE的主一多子链模式,CBE采用SPV（Simple Paymem Verification）的验证技术通过构造默克尔证明，客户端只需同步区块的Block Header．就可以达到验证的目的， Block Header的大小始终不变，且占用空间极少，每年的增长也只有几兆左右，正常情况下也完全能够负载。这极大地节省了存储空间，减轻终端用户和网络传输的负担。
SPV指的是”支付验证”，而不是“交易验证”。这两种验证有很大区别。“交易验证”非常复杂，涉及到验证是否有足够余额可供支出、是否存在双花攻击、脚本能否通过等等，通常
由运行完全节点的矿工来完成。“支付验证”则比较简单，只判断用于 支付的那笔交易是否已经被验证过，并得到了多少的算力保护（多少确认数）。

SPV验证步骤：
（1）从网络上获取并保存最长链的所有Block Header至本地；
（2）计算该交易的hash值 tx_hash；
（3）定位到包含该tx_hash所在的区块，验证Block Headers 是否包含在已知的最长链中；
（4）从区块中获取构建merkle tree所需的hash值，
（5）根据这些hash值计算merkle_root_hash ；
（6）若计算结果与Block Header中的merkle_root_hash相等，则交易真实存在。
（7）根据该Block Header所处的位置，确定该交易已经得到多少个确认。

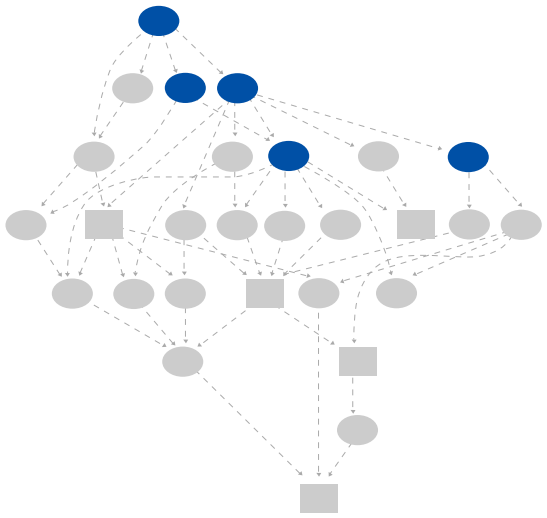
应用流式计算的动态分片技术：CBE作为基础链，要保证基础设施的畅通性．安全性和高性能，所以我们采用多子链模式来支持海量DAPP的并发运行，而海量DAPP必然带来海量的数据存储。而构建低延迟、高吞吐量、弹性伸缩且持续可靠运行的大数据流式计算来满足链上应用的实时性、无序性、无限性等特征。在流式计算中，无法确定数据的到来时刻和到来顺序，也无法将全部数据存储起来，因此，不再进行流式数据的存储，而是当流动的数据到来后，在内存中直接进行数据的实时计算。数据在任务拓扑中被计算，并输出有一价值的信息。

CBE将使用有向无环图（Directed Acyclic Graph，简称DAG）完成大数据流的计算过程，流式计算框架其核心部分采用高效流式计算函数式语言Clo-jure编写，为方便用户使用，支持用户使用任意编辑语言进行顽目开发。

数据流是流式计算框架对数据进行的抽象．它是时间上无穷的Tuple元组序列．数据流是通过流分组（Steam group-ing）所提供的不同策略实现在任务拓扑中流动，此外，为了满足确保消息能且仅能被计算1次的需求，我们的流式计算框架还提供了事务任务拓扑，并且保证每个数据流在任务拓扑中被完全执行。



数据流计算示意图



密码学：

• 私钥：非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。
• 公钥：可以公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，候选方案为 secp256r1（国际通用标准）、secp256k1（比特币标准）和 SM2（中国国标）；
• 与上面相反如果加密和解密是采用不同的密钥，也就是• 对称式加密就是加密和解密使用同一个密钥；也就是说采用这种加密方法时候，加密方与解密方需要使用同样的密钥进行加密和解密，该方式只需要一个密钥+特定算法对数据内容进行加密，加解密效率比较高，因此在对被广泛使用。但是因为解密方也需要密钥，所以保证密钥的安全也成为了一个难题。
非对称加密密钥密码系统，每个通信方均需要两个密钥，即公钥和私钥，这两把密钥可以互为加解密。如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。 非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公钥向其它方公开；得到该公钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把私钥对加密后的信息进行解密。公钥是公开的，不需要保密，而私钥是由个人自己持有，并且必须妥善保管和注意保密。
• 地址：地址是公钥的摘要，是为了用户能够方便交易而产生的，因为公钥较长约有 130 字符，而地址比较短，约有 35 或者 36 个字符。
• 私钥 >> 公钥 >> 地址。过程均不可逆。拥有私钥便拥有一切。
CBE采用的 ECC 椭圆加密算法保证了公钥无法反向推导出私钥。而Sha256 哈希算法则保证了无法从地址反向推导出公钥。
椭圆曲线密码（Elliptic Curve Cryptography，ECC）算法ECC是基于椭圆曲线数学的一种公钥的算法，其安全性依赖于椭圆曲线离散对数问题的困难性：
（一） 椭圆曲线密码算法优点
1. 短的密钥长度，意味着小的带宽和存储要求；
2. 所有的用户可以选择同一基域上的不同椭圆曲线，可以使所有的用户使用同样的操作完成域运算。
(二）Secp256k1 椭圆曲线算法
Secp256k1为基于Fp有限域上的椭圆曲线，由于其特殊构造的特殊性，
其优化后的实现比其他曲线性能上可以特高 30%，有明显以下两个优点：
1）占用很少的带宽和存储资源，密钥的长度很短。
2）让所有的用户都可以使用同样的操作完成域运算。

（三） 椭圆曲线签名与验证签名

（1）椭圆曲线数字签名生成

假定用户对消息m进行签名，他所采用的椭圆曲线参数为D=(p,a,b,G,n,h)，对应的密钥对为（k，Q），其中 Q 为公钥，k 为私钥。签名步骤：

第 1 步，产生一个随机书 d，1≤d≤n−1；

第 2 步，计算 dG=（x 1， y 1 ），将 x 1 转化为整数 x；

第 3 步，计算 r=`x mod n，若 r=0，则转向第 1 步；

第 4 步，计算 d−1mod n；

第 5 步，计算哈希值 H（m），并将得到的串转化为整数 e；

第 6 步，计算 s=d−1 （e+kr）mod n，若 s=0，则转向第 1 步；

第 7 步，（r，s）即为用户对信息 m 的签名。

（2）椭圆曲线签名验证

为验证用户对信息 m 的签名（r，s），矿工（Miner）可以得到用户所用的椭圆曲线参数以及用户的公钥 Q。矿工将按以下步骤操作。

第 1 步，验证 r 和 s 是区间[1，n−1]上的整数；

第 2 步，计算 H（m）并将其转化为整数 e；

第 3 步，计算 w=s−1mod n；

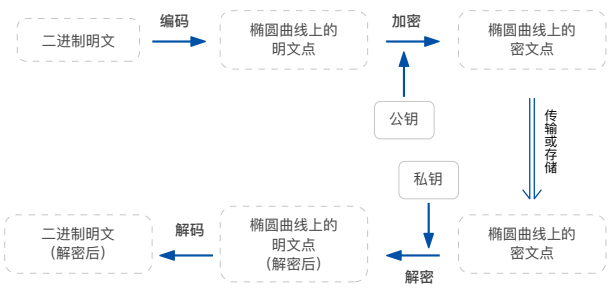
第 4 步，计算 u 1 =ew mod n 以及 u 2 =rw mod n；

第 5 步，计算 X=u 1 G+u 2 Q；

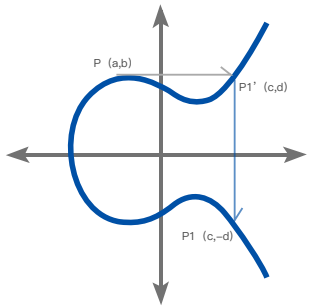
第 6 步，若 X=O，则拒绝签名，否则将 X 的 x 坐标 x 1 转化为整数`x，并计算 v=`x mod n；

第 7 步，当且仅当 v=r 时，签名通过验证。

利用椭圆曲线的签名和验证算法，一方面保证用户的账号不被冒名顶替，另一方面也能确保不能否认其所签名的交易。用户发起交易的时候，使用自己的私钥对交易签名，矿工收到信息后用用户的公钥对签名进行验证，一旦通过，该交易信息可以通过矿工进行记账，最终完成交易。



椭圆曲线密码加解密流程



Secp256k1 椭圆曲线算法

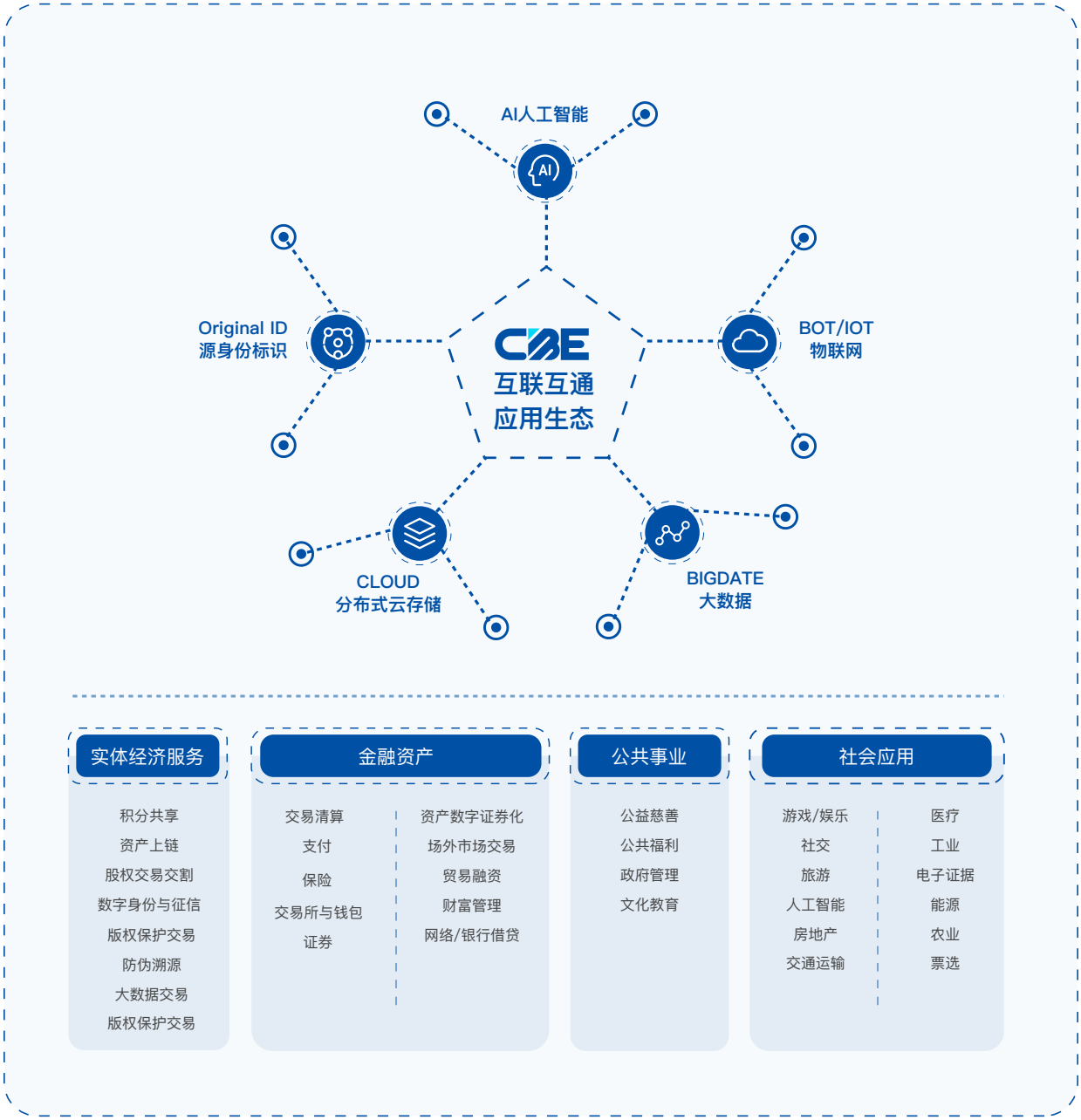
第6章

CBE生态应用领域与场景

生态运营模式

CBE是现世界世界与区块链的连接器，也是传统商业支持的基础设施，结合分布式账本技术搭建分布式社群交互平台，来自不同的链和系统可以支持不同的业务体系，并通过CBE的各类协议进行协作，不仅支持新型的业务场景，更将为传统商业进行流通，实现区块链连接一切商业，社群为未来的商业提供信任与价值互换的基础，打造万物互联互通的全新强大生态！CBE将结合物联网、云服务、人工智能、大数据等新科技，在游戏/娱乐、社交、旅游、房地产、交通运输、 医疗、工业、电子证据、能源、农业、票选、公益慈善、公共福利、政府管理、文化教育等行业推广落地应用！

CBE应用生态


AI人工智能
Original ID
源身份标识
CBE
互联互通
应用生态
BOT/IOT
物联网
CLOUD
分布式云存储
BIGDATE
大数据
实体经济服务
积分共享
资产上链
股权交易交割
数字身份与征信
版权保护交易
防伪溯源
大数据交易
版权保护交易
金融资产
交易清算
支付
保险
交易所与钱包
证券
资产数字证券化
场外市场交易
贸易融资
财富管理
网络/银行借贷
公共事业
公益慈善
公共福利
政府管理
文化教育
社会应用
游戏/娱乐
社交
旅游
人工智能
房地产
交通运输
医疗
工业
电子证据
能源
农业
票选

经济资产价值交易生态

CBE将以核心区块链技术，如纯资产技术、跨链多链并行多网层结构，提供一种可行的资产确权、流通解决方案。可记录资产流通的全过程，并形成无法篡改的链数据，建立一个全球去中心化虚拟货币交易所，并实现资产托管、资产支付等功能，同时致力于提供专门服务于资产登记和资产交易，未来交易所将会提供租借、交换、抵押、C2C交易等功能。从而解决“资产上链”、“跨链流通”等方面的难题，并实现对真实世界的传统金融产业的创新，提供区块链在不同金融/资产应用场景的底层技术支持！

从而CBE将打造一个完整的全场景区块链金融资产价值交易生态，在资产证券化、场外市场、供应链金融、财富管理、贸易融资、保险、贷款、股权交易交割、跨境支付等九大场景中带来以CBE区块链技术架构的全新模式与全新业态。

保险

CBE可设置产品规则引擎根据链上信息进行刻画、大数据用户行为分析，能够智能推荐保险产品；另一方面，各类信息上链，保障信息安全、透明性，应用CBE技术可通过智能合约简化索偿提交程序，不再需要保险代理人介入，将极大缩短处理周期。

资产证券化

CBE将构建基于区块链的智能资产证券化平台，使用区块链进行底层资产承载，并将每轮的资产评估、审计、交易信息记录在区块链上据不同的资产类型，设计不同的管理流程，包括底层资产的生成、交易、查询、打包、资金流和销毁等流程。

供应链金融

基于CBE区块链的底层技术设置“债转平台”，以供应链金融服务（应收账款融资）为核心，以债权凭证为载体，帮助入链供应商盘活应收账款，降低融资成本，增加财务收益，解决债权凭证的签发、转让、融资、兑付以及供应商对外支付及上游客户的融资需求，以此助力核心企业搭建自己的供应链金融体系。

场外市场

CBE将构建区域场外市场间联动机制，解决各地区场外市场间数据孤岛现象，通过区块链对各参与方的身份、信用、风险承受能力、投资经历等信息进行溯源管理,撮合成交的交易双方通过加密后的数字签名发布交易指令，确定交易的有效性真实性及双方的资金偿付能力!打造一个真实、公平、低风险、高效率的区块链场外市场!

财富管理

通过CBE搭建的去中心化的交易系统，各类数字化资产转让安全且有效；且财富管理的信息、数据上链，全流程透明且可溯。合格投资人认定的真实性和效率得到了提高；投后管理中，资金的事后使用情况也会加密保存到区块链中，提升信任和安全水平；

股权交易分割

CBE技术的分布式存储和运算能够确保数据的安全性和可追溯性，降低监管复杂程度；智能合约同步实时转移股权与现金，提升交易效率。设置中小企业股权交易平台，通过点对点的交易模式，实现股权交易完全无纸化。此外，后台资产转让契约完全通过CBE的智能合约实现，能够实现实时结算和交割!

贸易融资

CBE技术将实现融资文件即时审批、融资流程实时追踪，进而提高贸易融资交易的透明度，实现风险的全流程管理，满足出口商个性化的融资需求。方便银行或其他金融机构对基于贸易链条的应收应付账款或者是库存商品进行融资产品推动，降低获取原始信息的人工管理成本。通过CBE区块链技术，贸易背景项下的单据流、货物流和资金流可以实现实时更新，使得贸易金融生态系统更稳定更可靠。

贷款

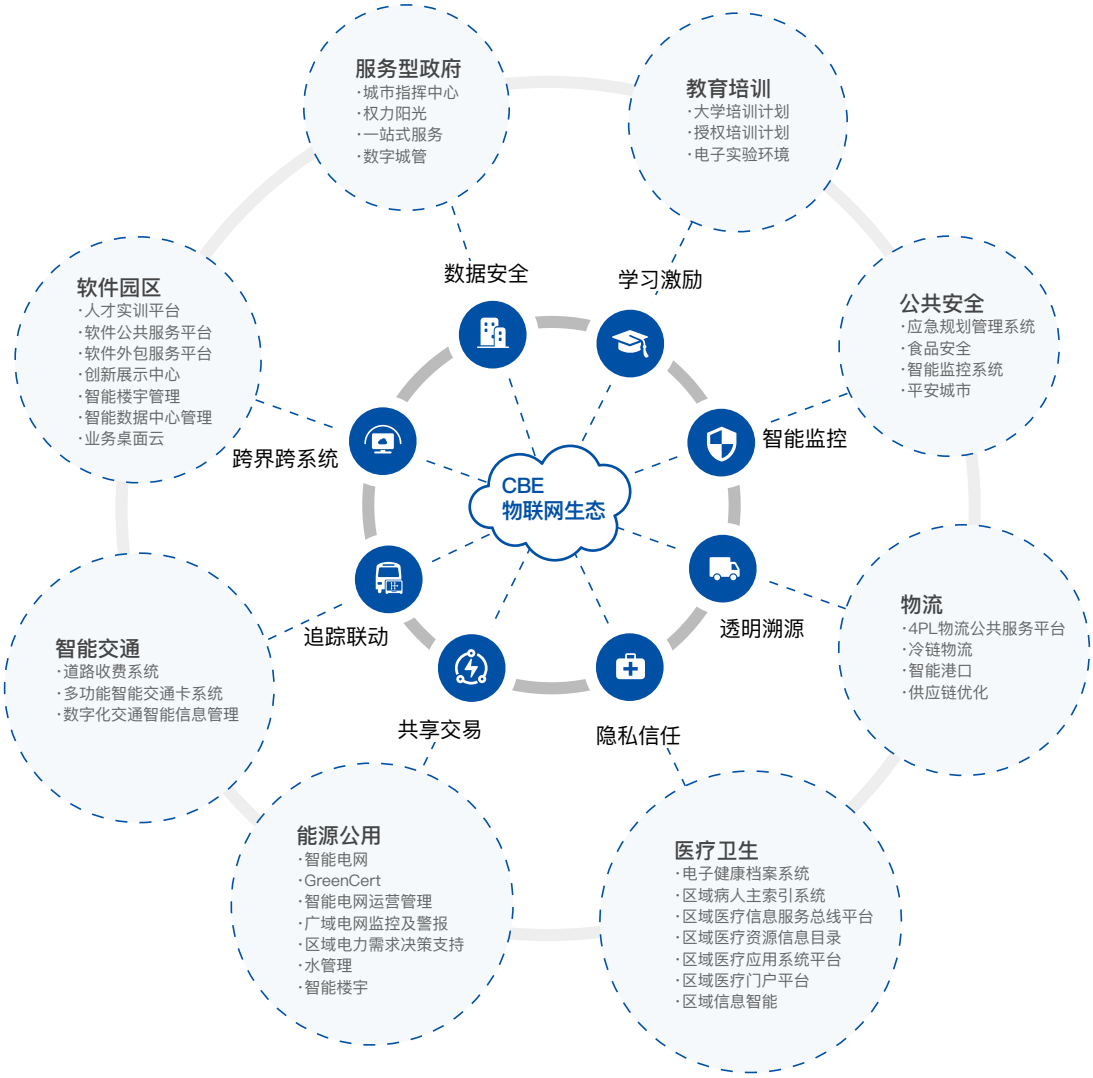
采用CBE基础技术，着力打造网贷联盟平台，有助于解决信贷成本高和坏账率高的问题；依靠技术手段打造去中心化的信用机制，进一步增强信息透明性，提升安全性，降低信用成本。共识机制和智能合约能够有效简化银团贷款流程，降低对人工的依赖程度，降低操作风险并提高支付效率，整体推动贷款进程。可以使所有参与银团贷款的机构通过系统实时查看信用协议、位置信息、应计余额等详细的交易数据。

跨境支付

利用CBE网络，将传统金融机构、外汇做市商、流动性提供商等加入支付网络，构建成为CBE支付网关。通过CBE支付网关，可以将CBE区块链上数字资产流动与现实中的法定货币相连接，实现法定货币可以转换为CBE区块链上的数字资产，便于后续的支付转账。通过CBE区块链支付网络中的网络连接器可以连接传统做市商、汇出行、汇入行等机构，摒弃中间交易环节，实现点到点快速低成本支付。

物联网(Iot)智能生态

通过运用CBE技术可让物联网内的智能设备以点对点直接互联的方式传输数据，而不是通过中央处理器，这样分布式计算就能有效分散巨量计算压力；同时，CBE技术还可以充分利用闲置设备的计算力、存储容量和带宽，大幅度降低数据计算和储存的成本。CBE技术的叠加智能合约可将每个智能设备变成可自我维护、调节的独立CBE链上网络节点，这些节点可在事先规定或后续植入规则的基础上，执行与其他节点交换信息、核实身份等功能。这样无论设备生命周期有多长，物联网产品都不会过时，节省了大量的设备维护成本。所以CBE将应用于下一代数字化智能物联网生态，以创新供应链、追踪存证溯源、共享经济、智能移动物联网等应用场景，开启万物互联新时代！



创新供应链

传统的供应链运输需要经过多个主体，例如发货人、承运人、货代、船代、堆场、船公司、陆运（集卡）公司，还有做舱单抵押融资的银行等业务角色。这些主体之间的信息化系统很多是彼此独立，互不相通的。存在数据做伪造假的问题，同时因为数据的不互通，出现状况的时候，应急处置没法及时响应。而通过CBE技术，可在供应链上的各个主体部署区块链节点，通过实时（例如船舶靠岸时）和离线（例如船舶运行在远海）等方式，将传感器收集的数据写入CBE链上，成为无法篡改的电子证据，可以提升各方主体造假抵赖的成本，更进一步地厘清各方的责任边界，同时还能通过CBE链式的结构，追本溯源，及时了解物流的最新进展，根据实时搜集的数据，采取必要的反应措施（例如，冷链运输中，超过0℃的货舱会被立即检查故障的来源），增强多方协作的可能。CBE的技术可将不同商品流通的参与主体的供应链和区块链存储系统相连接。其中包括原产地、生产商、渠道商、零售商、品牌商和消费者。使每一个参与者信息在区块链的系统中可查可看，由此为供应链上的众多参与方提供了一个管理协作平台，上下游厂商都可以根据这个平台调整自己的生产、销售计划。而CBE智能合约的使用，可以使产品交易、签收等自动执行，降低了人工操作成本，提高了效率。尽管存储在CBE区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。

商品溯源

CBE本身是一种资产，同时可发行多种资产，各类物品都可以听过CBE上链成为链上资产，在溯源领域，主要采用了CBE的“链”特性。包括食品溯源、产品溯源、奢侈品溯源、珠宝玉石溯源等。将代表实物资产的资产代码在CBE的各个环节流通，保证溯源的信息不可篡改，且可完整追溯。超级区块链在溯源领域，可通过其自身具有的备注字段，为每个溯源环节加多自定义的溯源信息（如资产故事等），以实现资产价值的提升！

共享经济

共享经济可以认为是平台经济的一种衍生。中心化平台具有依赖性和兴趣导向性，摩拜和OFO做单车共享，但并没有做摩托车的共享。另一方面，中性化平台也会收取相应的手续费，例如滴滴打车司机要将打车费用的20%上交，作为平台提成。CBE可以构建一个普适的共享平台，依托去中介化的区块链技术，让供需双方点对点地进行交易，加速各类闲置商品的直接共享，并节省第三方的平台费用。首先使用CBE区块链网关，构建整个区块链网络。资产拥有者基于智能合约，通过设置租金、押金和相关规则，完成各类锁与资产的绑定。最终用户通过DAPP，支付给资产所有者相应的租金和押金，获得打开锁的控制权限（密钥），进而获取资产的使用权。在使用结束后，归还物品并拿回押金。可完成精准计费，可以按照智能合约上的计费标准，实时精准地付费，而不是像目前共享单车的粗犷式收费（按半小时、一小时收费）。

能源交易

传统输电的线路损耗率达到5%，住户建立的微电网中盈余能源无法存储，也不能共享给有能源需求的其他住户；而CBE可以以CBE的技术开发一个点对点交易、自动化执行、无第三方中介的能源交易平台，实现了多个住户之间的能源交易和共享。主要实现方式是，刻在每家住户门口安装智能电表，智能电表安装区块链软件，构成一个CBE区块链网络。用户通过手机APP在自家智能电表区块链节点上发布相应智能合约，基于合约规则，通过本地提供的电网设备控制相应的链路连接，实现能源交易和能源供给。通过将各家住户的可再生能源存储到分布式储能设备中，通过代币的形式评估能源的占有量和消耗量，基于CBE智能合约设置能源交易规则和微电网切换主电网的策略，实现无中介的点对点能源交易。

智能移动物联网

在CBE的IoT+区块链技术的结合下，可在物联网的各类智能移动实现无限、跨界的可能，如：联网汽车（Connected Vehicle）/车联网，使车辆变成巨大的智能应用程序。汽车自动化逐年加强，包括导航、道路救援等。CBE将利用数字网络追踪这些设备，实现车辆间通信和保险条款自动追踪，车辆年检等；也可以通过车联网再联网交通。车辆网络中的应用场景很多，可以传递所有交通信息，避开交通堵塞等问题。将其延伸到全球贸易中，这个交通网络可以囊括水运、空运、地面运输网络，追踪货物运输；公共技术设施和智能城市物联网：智能设备已经用于追踪桥梁、道路、电网等的状况，CBE可以将所有这些连接到一起，共享高效率，进行维护，预测使用情况和污染情况，可帮助偏远地区监测自然灾害，防范大规模山火、病虫害等大灾害；基于CBE物联网可将治疗过程中使用的设备和服务都连接起来，对居民、病人的运动、健康等数据进行监测，获取健身、医疗、体质监测、运动监测等大数据信息，而区块链的匿名性能让患者的隐私得到保证，同时能打通医院、金融保险、药厂等其他相关部门之间的信息通道。如将病情数据匿名地传输到医院或药品厂商，以用于日后的改善；医生经过授权后可获取病人的完整的历史健康信息，更好地进行针对性治疗；而新型的药物和设备将可以在临床测试时进行追踪，并为自己的有效性和副作用提供相关证据，而无需担心有人篡改这些结果。在医保方面。监管机构通过授权实现数据共享，防止数据被篡改，便于实现精准医保控费。

更多CBE应用场景

CBE作为互联互通区块链价值网络的基础设施，可以为各行业各垂直领域等应用场景的分布式互联互通服务提供基础技术体系，让各行业各垂直领域的个人、公司、团队、应用无需掌握专业区块链技术便可便捷的使用CBE底层系统，享受分布式账本技术、分布式应用、跨链交易、资产上链发行等区块链底层服务！

消费行业Consumer

共享经济：Sharing economy
供应链管理：Supply chain
药物跟踪：Pharmaceutical tracking
农业食品认证：AgricCBEtural food authentication
物流管理：Shipping and logistics management

媒体Media

数字版权管理：Digital rights management
艺术认证：Art authentication
广告刊登：Ad placement
广告点击的真实统计：Ad click fraud reduction
正版资产的转售：Resale of authentic assets

金融行业Finance

交易领域：Trading
财富管理：Wealth management
衍生品交易：Derivatives trading
抵押品管理：Collateral management
供应链金融：Supply chain finance

软件开发Software Development

微粒化工作：Micritization of work
人工支付：Disbursement of work
面对开发者的直接付款：Ad placement direct todeveloper payments
API接口平台：Ad placement API platform
公证和认证：Ad placement notarization and certification

支付Payments

小额支付：Micropayments
B2B国际汇款：Business-to-business international remittance
税务申报和统计：Tax filing and collection
了解您的客户：Know your customer (KYC)
反洗钱：Anti-money laundering (AML)

医疗卫生Medical

病历共享：Record sharing
处方共享：Prescription sharing
多重认证：MCBEti-factor authentication
个性化医疗：Personalized medicine
DNA测序：DNA sequencing

保险Insurance

索赔申请：Claim filings
索赔处理和管理：Claims processing and admin
欺诈检测：Fraud detection
远程信息处理和评级：Telematics and ratings
数字认证：Digital authentication

资产标的Asset Titles

钻石：Diamonds
设计师品牌：Designer brands
汽车租赁和销售：Car leasing and sales
住房抵押：Home Mortgages
土地所有权：Land title ownership
实体资产数字化：Digitalization of assets

物联网IoT

支付设备：Device-to-device payments
自动化操作：Automated operations
电网管理：Grid management
智能家居管理：Smart home management
办公室管理：Office management

社会管理Government

投票：Voting
车辆登记：Vehicle registration
福利分配：Benefits distribution
版权保护：Copyrights
教育和认证：Education certificates

第7章

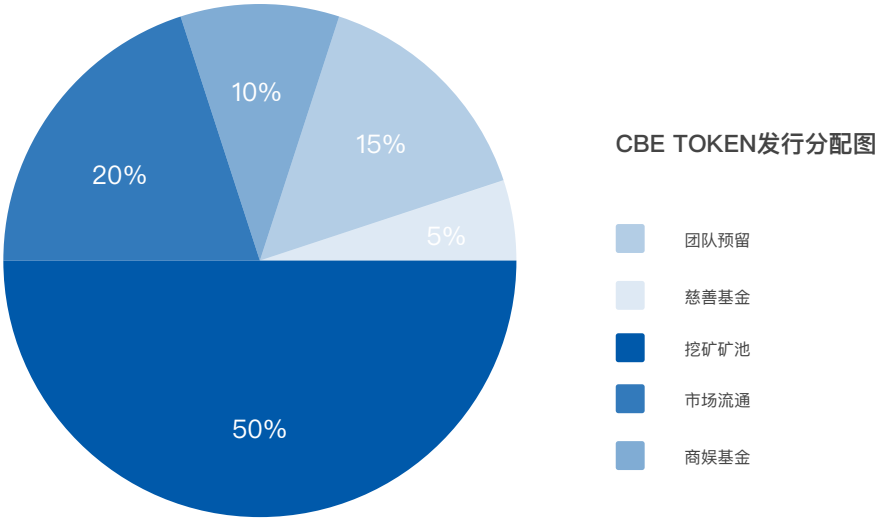
CBE TOKEN生态价值流通凭证

CBE TOEKN 生态价值流通凭证

CBE代币是CBE网络的通行证，链上的所有价值的流通都需消耗CBE代币，如：发行资产、DApp开发装载消耗、转账/交易手续费消耗、调用接口燃料费等，基于CBE的强大的技术可垂直多个领域，未来会诞生丰富的应用场景和商业模式！CBE币是基于墨客子链的原生币。

CBE 发行分配方案

代币名称： CBE；
中文名称： 令牌；
发行总量： 20亿，永不增发；



发行分配方案	比例	数量
商娱基金 用于商娱链的商业/市场拓展基金	10%	2亿
慈善基金 作为慈善基金，为慈善事业做出贡献	5%	1亿
市场流通 CBE正常启动市场流通部分	20%	4亿
挖矿矿池 冻结至CBE上线，上线后将启动挖矿激励	50%	10亿
团队预留 用于 CBE运营/创始/技术开发团队奖励激励	15%	3亿

CBE特有的回购机制

限量发行20亿枚CBE, 永不增发，共计五个阶段		
第一阶段	智能挖矿1亿枚（含首发）内	采用百分之一回购机制
第二阶段	智能挖矿1~2亿枚内	采用千分之五回购机制
第三阶段	智能挖矿3~5亿枚内	采用千分之一回购机制
第四阶段	智能挖矿6~8亿枚内	采用万分之五回购机制
第五阶段	智能挖矿9~10亿枚内	采用万分之一回购机制

CBE按五个发行阶段设定了不同的回购机制。随着回购CBE，最后直至3亿枚位置，采取万分之一回收加权的方式，对现有CBE进行权重加权。

- 在第一阶段的1亿枚（含首发）智能挖矿期间每一笔流通，其交易量的1%将被系统回购；
- 在第二阶段的1亿枚智能挖矿期间每一笔流通，其交易量的0.5%将被系统回购；
- 在第三阶段的2亿枚智能挖矿期间每一笔流通，其交易量的0.1%将被系统回购；
- 在第四阶段的3亿枚智能挖矿期间每一笔流通，其交易量的0.05%将被系统回购；
- 在第五阶段的3亿枚智能挖矿期间每一笔流通，其交易量的0.01%将被系统回购。

随着越来越多的CBE被回购，CBE将越来越稀有。系统回购CBE直至数量锐减到3亿枚为止。此后系统仍将继续按每笔交易量的0.01%收取交易手续费，同时会将收取的手续费以加权平均的方式回馈给所有持币账户。

注：回购官方将公示唯一的回购销毁钱包地址，回购的CBE将会注入该公开地址作为监督，同时除去全网的交易量，届时由CBE推出的DApp—CBE全球商娱综合体内所产生的交易也会按以上机制进行交易量进行手续费收取并用于回购CBE。

CBE TOKEN 智能挖矿机制

CBE TOKEN将于CBE链开发完成正式上线后启动智能挖矿出块，将会进行超级节点竞选，同时全网节点皆有对应挖矿激励机制，所有基于CBE的商家、企业、个人都可以成为CBE的子链设置独特挖矿机制；且由CBE推出的DApp––CBE全球商娱综合体，届时将会以持有CBE与CBE的交易使用行为，会有该DApp内的挖矿奖励。

第8章

项目创始团队

黄宥镇

软件工程师

浦项工科大学计算机工程专业，拥有LPIC国际资格证，曾参与安全程序交付、IoT机器人研究等多项目开发，个人发起WHITE HACHER活动，在区块链领域有近十年技术研发经验。

金名燮

软件工程师

高神大学，原任韩国著名IT公司工程策划师，2013年进入区块链行业，主导过多个韩国本土区块链项目的开发，作为重要嘉宾应邀出席亚洲区块链技术峰会并发表讲话，对于区块链项目技术落地具有相当研究。

？？？

全球顶级交易平台出身，CBE神秘创始人

项目顾问团队

CBE基金会

CBE基金会（以下简称“基金会”）是一家美国投资安全保障基金会，向来以多元化、高科技的投资项目被人们所熟悉，被誉为精于金融整合的机构。
致力于CBE的开发建设和透明治理倡导及推动工作，保证社群的管理、运作，以及所募资金的安全和管理。

基金会由开发人员和职能委员会组成，组织架构主要由决策委员会、代码审核委员会、运营委员会、财务委员会和商务委员会组成;

CBE致力于以分布式融合信任体系将区块链世界各个体系之间相互贯通与链下场景交互。为各类分布式应用服务提供完整的底层技术基础，将信任的应用多维度拓展延伸，构建多维度信用声誉体系，营造良好和谐社群氛围。

顾问团队

Alain · Delon

– 毕业于美国斯坦福大学，2013年进入区块链行业
– 资深微软工程师，在美国硅谷创业基地长期进行技术研究开发，参与众多优质资源项目

Gloria · Aaron

– 加州理工学院计算机专业学士
– 10年技术开发领域实际经验
– 成功创业家

Karl · Evan

– 密码学博士。加密技术和区块链技术的忠实拥护者，2012年起参与其中
– 有远见的企业家，在信息系统和产品管理方面经验丰富。

Howard · Allen

– 密歇根大学物理学教授。
– 比特币企业家，多次受邀参加北美区块链高峰论坛
– 数字营销分析专家

岛崎智

– 毕业于东京大学，后至美国哥伦比亚大学深造。
– 精通英、法、日三国语言，精通密码学、在区块链专业领域具有丰富技术经验

远藤由贵

– 毕业于京都大学
– 在亚太和东欧地区负责主持参与咨询多个国际项目，工作经验丰富

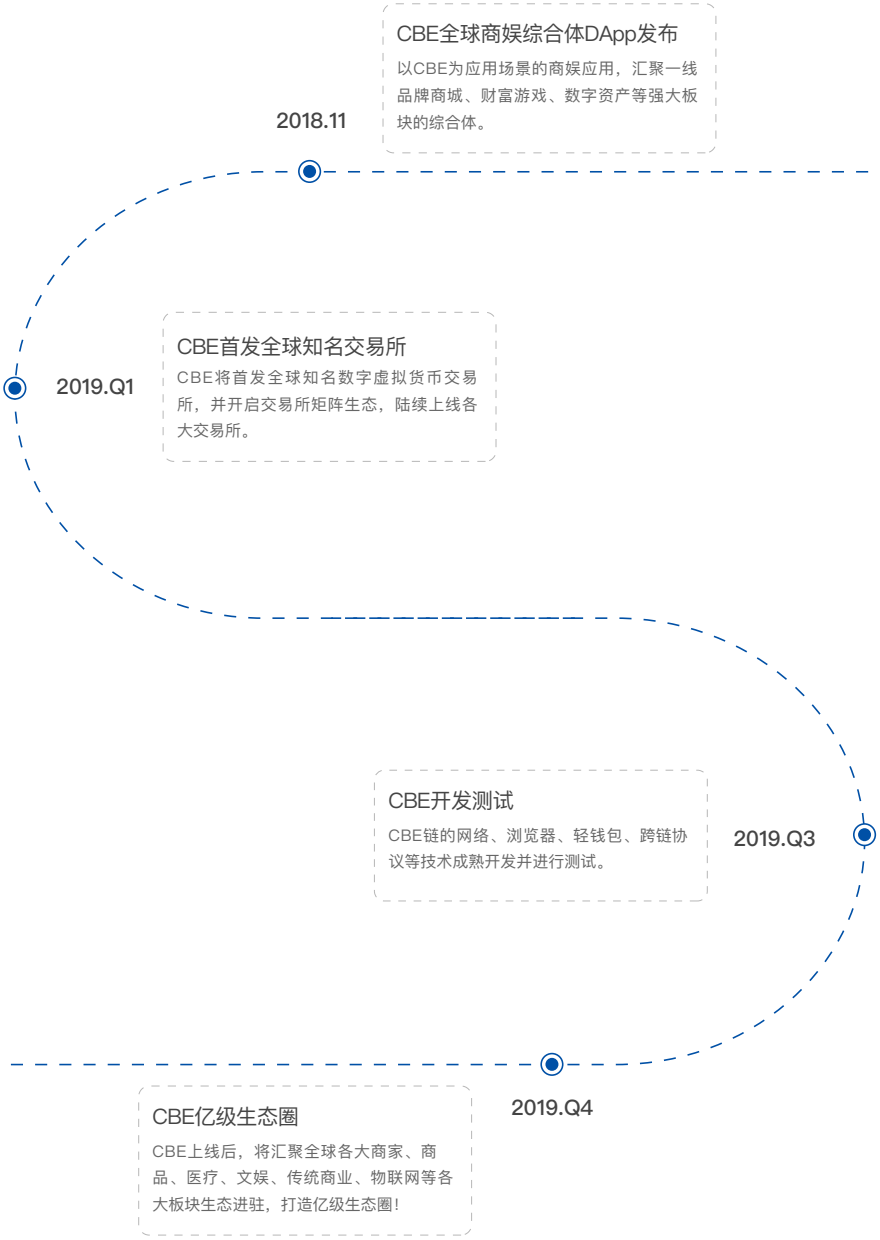
Stephen · Gino

– 毕业于麻省理工学院
– 资深产品体验设计师和前端开发工程师
– 产品设计和品牌战略实战经验丰富

Angus · Henry

– 毕业于哈佛大学
– 曾职于英特尔，Boxee和Voltaire等500强企业
– 硅谷创业家，拥有网络安全和加密货币投资经验

CBE项目发展RoadMap



第9章

风险把控与免责声明

加密资产是一种相对较新的资产类别，并具有相当大的投资风险。潜在投资者需充分了解这些风险，并根据各自的风险承受水平进行投资。

信息披露不完备的风险

截至本白皮书发布之日，CBE 仍处于开发阶段，其哲学理念、共识机制、算法、代码等技术规范和参数可能会经常且不断更新与变更。尽管本白皮书包含CBE 的特定信息，但其并不绝对完整，且出售方可能会根据特定目的不时对这些信息作出调整与更新。出售方无法，也无义务随时告知参与者CBE开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让参与者及时且充分地获悉CBE开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

监管风险

加密代币正在被或可能被各个不同国家的监管机构所监管。出售方可能会不时收到来自于一个或多个监管的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何与本次公开售卖、CBE 开发或 CBE 相关的行动。CBE 的开发、营销、宣传或其他方面以及本次公开售卖均可能会因此受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于CBE 或本次公开售卖的监管许可或容忍可能只是暂时的。在各个不同国家，CBE 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，CBE 可能被禁止交易或持有。

密码学加速发展的风险

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明 / 改良）可能给基于密码学的系统（包括 CBE）带来危险。这可能导致任何人持有的 CBE 被盗、失窃、消失、毁灭或贬值。在合理范围内，项目方将自我准备采取预防或补救措施，升级 CBE 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，项目方将和 CBE 社区其他成员一起尝试适应密码学和安全领域的不断变化。

项目失败或中止的风险

CBE 仍在开发阶段，而非已准备推出的成品。由于 CBE 系统的技术复杂性，出售方可能不时会面临无法预测和 / 或无法克服的困难。因此，CBE 的开发可能会由于任何原因而在任何时候失败或中止（例如由于缺乏资金）。开发失败或中止将导致 CBE 代币无法交付给本次公开售卖的任何参与者。

众筹收入被盗的风险

可能会有人企图盗窃出售方所收到的众筹资金（包括已转换成法币的部分）。该等盗窃或盗窃企图可能会影响出售方为 CBE 开发提供资金的能力。尽管出售方将会采取最尖端的技术方案保护众筹资金的安全，某些网络盗窃仍很难被彻底阻止。

竞争风险

CBE 的底层协议是基于开源电脑软件，没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 CBE 的源代码和 / 或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台或虚拟机从而与 CBE 竞争，或甚至赶超或取代 CBE。出售方对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台（例如 BitSharess）与 CBE 产生竞争关系。出售方在任何情况下均不可能消除、防止、限制或降低这种旨在与 CBE 竞争或取代 CBE 的竞争性努力。

第三方开发者风险

CBE 将提供一个开放平台适用于第三方（尤其是 CBE 社区成员）开发的任何类型的分布式应用和智能合约程序。所有这些应用和智能合约程序可以被接入或建立在 CBE 区块链上而不受限于审查制度、限制、控制、资格预审或准入要求。出售方既不意图也无法担当审查员在任何程度上对任何将要在 CBE 系统上开发或与之相关的程序进行审核。因此，在特定司法管辖区域被禁止或限制的程序，如涉及赌博、投注、彩票、乐透、色情等等的程序，可能利用 CBE 区块链的无准入要求来开发、促进、营销或运营。特定司法管辖区域的监管当局可能对特定程序或甚至其开发者或用户采取相应行政或司法措施。任何政府当局的处罚、惩罚、制裁、镇压或其他监管措施，或多或少会惊吓或威慑到既有或潜在 CBE 用户使用 CBE 系统并持有 CBE，从而对 CBE 的前景造成重大不利影响。

平台迁移风险

CBE 初始时将有一条独立的底层区块链作为其自有账本。然后 CBE 今后可能迁移去其他一个或多个分布式平台，只要该等平台对 CBE 上执行的交易更高效、更有价值或更适合。若发生该等迁移，所有届时存在的 CBE 将能被转换成迁移后的 CBE 上新的内置加密代币，其具有类似或同等技术规格和功能。CBE 在迁移前使用的原区块链将因此渐渐消亡。

其他加密资产的风险

CBE 中将会创建或生产并流通着各种加密资产。这些加密资产中一部分可能是由特定人士发行的，发行人将对持有人负有特定承诺或义务。其他一些加密资产可能是由 CBE 内的智能合约创建的。这些加密资产都不会带有和 CBE 一样或类似的功能。这些加密资产既不是出售方所出售或提供的，出售方也不会对它们负责，除非出售方另有特别说明。

代币通胀的风险

取决于 CBE 发布时的具体底层协议，CBE 总量可能随时间略有增加，且可能会由于采纳了CBE 源代码的补丁或升级而进一步增加。由此产生的 CBE 供应量通胀可能导致市场价格下跌，从而 CBE 持有者可能遭受经济损失。CBE 购买者或持有者并不能被保证会由于 CBE 通胀而获得某种形式的赔偿或补偿。

平台合并的风险

技术角度而言，在特定情形下，为实现协同效应或基于其他有价值的对价，CBE 可能与其他区块链项目合并。这种形式的合并可能导致 CBE 区块链被放弃或废弃，以换取新创建的其他区块链上一定数量的加密代币。该等新的加密代币将按一定兑换率分配并派发给合并前的 CBE 持有者。在特定估值模型下 CBE 持有者可能在该等合并中获得的补偿不足。

应用缺少关注度的风险

CBE 的价值很大程度上取决于 CBE 平台的普及度。CBE 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，CBE 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部 CBE 需求可能具有投机性质。缺乏用户可能导致 CBE 市场价格波动增大从而影响 CBE 的长期发展。出现这种价格波动时，出售方不会（也没有责任）稳定或影响 CBE的市场价格。

流动性不足风险

CBE 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。CBE 在市场上的流通和交易并不是出售方的职责或追求。CBE 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 CBE 持有者处兑换或购买任何CBE，也没有任何人士能够在任何程度上保证任何时刻 CBE 的流通性或市场价格。CBE 持有者若要转让 CBE，该 CBE 持有者需寻找一名或多名有意按约定价格购买的买家。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密代币交易所或其他市场上线 CBE 供公开交易。

代币价格波动风险

若在公开市场上交易，加密代币通常价格波动剧烈。短期内价格震荡经常发生，该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 CBE 交易的二级市场，出售方对任何二级市场的 CBE 交易不承担责任。因此，出售方没有义务稳定 CBE 的价格波动，且对此也并不关心。CBE 交易价格所涉风险需由 CBE 交易者自行承担。

节点处理能力不足的风险

CBE 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过 CBE区块链网络内届时节点所能提供的负载，则 CBE 网络可能会瘫痪和 / 或停滞，且可能会产生诸如“双重花费”的欺诈或虚假交易。在最坏情况下，任何人持有的 CBE 可能会丢失，CBE 区块链回滚或甚至硬分叉可能会被触发。这些事件的后果将损害 CBE 的可使用性、稳定性和安全性以及 CBE 的价值。

CBE 代币未经授权被认领的风险

任何通过解密或破解 CBE 购买者的密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意认领在本次公开售卖中所购买的 CBE。据此，购买者在本次公开售卖中所购买的 CBE 可能会被错误发送至通过购买者注册邮箱或注册账号认领 CBE 的任何人士，而这种发送是不可撤销、不可逆转的。每一购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性。

使用高安全性密码

不打开或回复任何欺诈邮件；以及严格保密其机密或个人信息。

CBE 钱包私钥丢失风险

若丢失或损毁了存取 CBE 所必需的私钥，这可能是不可逆转的。只有通过本地或在线 CBE 钱包来占有相关的独一无二公钥和私钥，才可以操控 CBE。每一购买者应当妥善保管其 CBE 钱包的私钥。若 CBE 购买者的该等私钥丢失、遗失、泄露、毁损或被危及到，出售方或任何其他人士均无法帮助购买者存取或取回相关 CBE。

系统分叉风险

CBE 是一个由出售方发起并由社区提供支持的开源项目。尽管出售方在 CBE 社区中具有影响力，但是其并不也无法独断 CBE 的开发、营销、运行或其他。任何人士均可以开发 CBE 代码的补丁或升级，而无需获得任何其他人士的授权。一旦部分的 CBE 区块链上验证者接受CBE 的补丁或升级，这可能导致 CBE 区块链“分叉”，由此将会出现两条分叉的网络，直至分叉的区块链合并或者其中某一条终止出块（这两种情况可能永不会发生）。CBE 区块链由于分叉而产生的每一分支均将有其自己的加密代币。因此，在两条分叉的分支上会分别存在拥有几乎相同技术特征和功能的 CBE。CBE 社区可能分裂成两批，分别支持两条分支。此外，分叉出的CBE 区块链分支在理论上可以进一步无限次分叉。分叉区块链的暂时性或永久性存在可能对CBE 运行及 CBE 的价值造成不利影响。在最坏情况下，可能摧毁 CBE 系统的可持续性。尽管 CBE 区块链上的该等分叉有可能经社区牵头努力后将两条分支合并而解决，但并不能保证成功且可能耗时很久。

源代码漏洞风险

无人能保证 CBE 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能、暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 CBE 的可用性、稳定性和 / 或安全性，并因此对 CBE 的价值造成负面影响。开放源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。出售方将与 CBE 社区紧密合作，今后持续改进、优化和完善 CBE 的源代码。

无准入许可、去中心化自治账本的风险

在当代区块链项目中，有三种流行的分布式账本种类，即：无准入许可的账本、联盟型账本和私有账本。CBE 底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管 CBE 初始时是由出售方所开发，但它并非由出售方所有拥有、运营或控制。自发形成的 CBE 社区是完全开放、去中心化且无准入门槛即可加入的，其由全球范围内的用户、粉丝、开发者、CBE 持有人和其他参与者组成，这些人大都与出售方无任何关系。就 CBE 的维护、治理乃至进化而言，该社区将是去中心化且自治的。而出售方仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力，不考虑其之前曾对 CBE 的诞生做出的努力和贡献。因此，CBE 在启动之后，其如何治理乃至进化将不受到出售方的支配。

源代码升级风险

CBE 的源代码是开源的且可能被 CBE 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 CBE 的运行或 CBE 的价值造成重大不利影响。

安全漏洞风险

CBE 区块链基于开源软件并且是无准入许可的分布式账本。尽管出售方努力维护 CBE 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 CBE 的核心基础设施要素之中，对这些弱点或缺陷出售方可能恰好无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的CBE 或其他数字代币丢失。

“分布式拒绝服务”攻击

CBE 被设计为公开且无准入许可的账本。因此，CBE 可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 CBE 系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入 CBE 区块链的区块之中，或甚至暂时无法执行。