
Cyber-Physical Chain (CPChain) Whitepaper 2.0

物信链白皮书 2.0

Towards the Trusted Future

智享万物，信通未来



2019 年 6 月 30 日

June 30, 2019

序言

随着互联网“下半场”时代的开启，人类社会正迈入“数据和智能商业时代”。物联网、区块链等新兴技术正在加速赋能传统行业。未来，越来越多的商业服务开始在线化，业务数据化，在传统的交通、医疗、物流运输、仓储和供应链领域，对物联网技术的需求将越来越重要。一方面，传统的中心化物联网系统面临着连接成本、商业模式落地等方面的困难；另一方面，伴随着物联网设备获取数据能力日益强大，用户隐私面临着泄露的风险日益严重，数据泄密、隐私侵犯等恶性事件正成为常态，公民“数据权”的意识正逐渐觉醒，对于用户数据隐私的保护与用户数据价值的分享与传递，正成为物联网商业化道路上不可避免的重要问题。

物信链（Cyber-Physical Chain, CPChain）深度融合区块链技术与物联网技术，实现去中心化、可信任的新一代分布式物联系统，降低系统互联互通成本、提高数据开放共享价值和确保用户隐私与系统安全。CPChain 重点围绕区块链技术应用与物联网行业所面临的扩展性、安全性和实时性问题，结合区块链—物联网—分布式加密存储与计算三大技术，构建新一代物联网体系架构，建立物联网行业数据获取、共享与应用的全流程解决方案。CPChain 专注于多方参与的数据交易和基于物联网大数据的人工智能决策应用场景，建立多方的信任和实现异构数据的互联互通，解决行业应用痛点问题。在此基础上，基于 CPChain 平台，打造新一代物联数据共享的创新型商业模式。



目录

序言	1
1. 项目背景	5
1.1 物联网产业的发展与痛点	5
1.1.1 物联网的产业需求与市场规模	5
1.1.2 物联网系统的中心化架构面临挑战	5
1.2 区块链技术为物联网带来新的发展潜力	7
1.3 物联网区块链市场规模预测与应用展望	8
1.4 商用区块链系统面临可扩展性的瓶颈问题	9
2. 核心技术	10
2.1 平行分布式架构	10
2.2 平行分布式加密存储、检索和授权共享	12
2.2.1 基于 DHT 的分布式加密存储	12
2.2.2 基于加密计算的数据共享与应用	14
2.2.3 Market: 数据交易信息聚合平台	16
2.2.4 OTP: 基于区块链的数据开放传输协议	18
2.3 DPoR 共识结构	18
2.4 大规模公有链的 LBFT 2.0 共识	19
2.4.1 二权分立委员会	20
2.4.2 LBFT 2.0 有限状态机	20
2.5 高实时性、安全性的侧链共识系统	23
2.5.1 数据网关和嵌入式加密算法	24
2.5.2 行业链共识算法激励与安全机制	24
2.6 测试与正确性验证	24
2.6.1 白盒测试	24
2.6.2 黑盒测试	25
2.6.3 DDoS 攻击	27
2.6.4 形式验证	27

2.7 性能.....	28
3. 商业应用	29
3.1 应用场景.....	29
3.1.1 智能出行	29
3.1.2 智慧医疗	29
3.1.3 公共安全	30
3.1.4 去中心化身份认证 (DID)	30
3.2 落地案例.....	31
3.2.1 无感停车.....	31
3.2.2 共享充电.....	33
3.2.3 药品溯源(Drugledger).....	34
3.2.4 驾培链.....	36
3.3 DApp 开发.....	38
3.3.1 PDash 数据共享	38
4. 经济模型及系统用途	40
5. 社区治理	41
5.1 RNode 荣誉节点生态	41
5.1.1 节点类型.....	41
5.1.2 荣誉度评估 (RPT)	41
5.1.3 节点奖励.....	42
5.2 理事会.....	43
5.2.1 人员组成.....	43
5.2.2 权利义务.....	43
5.2.3 任期.....	43
5.2.4 选举方法.....	44
5.2.5 收益.....	44
5.3 委员会.....	44
5.4 物信链基金会.....	45
5.4.1 人员组成.....	45
5.4.2 权利.....	45

5.4.3 义务.....	45
5.4.4 任期.....	45
5.4.5 入选方法.....	45
6. 发展路线图	46
7. 财务	47
7.1 通证分配计划.....	47
7.2 资金使用计划.....	47
8. 合作生态	48
9. 免责声明	49



CPCHAIN
CYBER PHYSICAL CHAIN

1. 项目背景

1.1 物联网产业的发展与痛点

1.1.1 物联网的产业需求与市场规模

物联网(Internet of Things, IoT)是信息领域的一次重大发展和变革机遇，它将先进的信息技术、通讯技术、传感技术以及计算机技术等高度整合，建立一套全球性的动态网络基础设施，网络将所有智能对象（RFID 标签、传感器、智能手机、可穿戴设备等）互联，进行信息与数据的传输与分享，实现全面感知、可靠传送和智能处理等功能。

物联网的价值在于连接真实世界和虚拟的数据世界。据知名市场研究机构 Gartner 预测：到 2020 年，全球物联网设备接入量将达到 260 亿，物联网产品和服务提供商的收益预计达到 3000 亿美元量级。物联网在无缝数据集成与数据价值链的形成中正日益发挥着重要作用。

1.1.2 物联网系统的中心化架构面临挑战

当前物联网在智能交通、智能家居和医疗护理等领域都采用中心化的技术与运营模式，即“烟囱式”物联网架构，面临着来自技术、信任、数据价值和商业模式等多个方面的共性问题。

技术瓶颈问题

- **兼容性低：**越来越多的硬件设备开始出现互联的趋势，目前存在着多种协议，而单一平台缺乏连接所有制造商设备的能力，因此设备和平台的兼容性成为 IoT 解决方案发展的关键挑战。
- **架构效率低下：**随着计算设备、存储设备以及传感器等元器件价格下跌，物联网设备迎来爆炸式增长。现有物联网解决方案成本过高，大多是“烟囱式”垂直体系架构，所有数据中心基于单个项目建设，每个 IT 系统都有自己的管理工具和数据库，形成了信息孤岛，在百亿互联设备时代，这样的架构效率低下，不能满足时代的需求。
- **成本高：**由于物联设备大多具有生命周期长的特点，且利润远低于 PC 和智能手机等具备快消品性质的智能终端，厂商却需要为这些设备长期维护相应

的 IT 系统，利润不足以支撑维护成本，设备厂商难以为继。

- **可扩展性弱：**现有的 IoT 和联网技术并没有满足技术日益增长的复杂性和互联性需求，可扩展性较弱。

用户数据隐私问题

- **隐私安全性差：**互联网需要建立在信任之上，而斯诺登等一系列事件也证明了“可信第三方”并非 100% 值得信任。在互联网进入大数据时代之后，隐私泄露成为公众关心的重大问题；针对大规模物联设备的安全漏洞的高级可持续攻击，在隐私泄露的同时将带来系统运行安全问题，导致设备损坏、人员生命安全受到威胁。因此，在物联网发展之初，隐私性和安全性必须嵌入物联网基础架构体系中，确保用户在享受更便利、更智能的服务同时不会泄露自己的个人信息，并让用户真正拥有自己创造的数据及其价值。此外，当前中心化架构中“封闭即安全”的理念也已经过时，以区块链为代表的新技术正在构建一个全新的“开放即安全”的万物互联新秩序。
- **数据所有权的归属：**随着大数据时代的到来，数据产出价值越来越重要，然而数据价值被头部平台所垄断，平台通过一系列终端设备采集个人数据，并开发更好的算法来为每个人提供定制化服务，进而获取更大的经济收益，数据价值正成为商业竞争的重要资源。与此同时，对于个人数据所有权的归属的立法与合规也开始提上日程，2018 年欧洲 GDPR 法规的颁布和执行即是一例。通过区块链技术与物联网平台相结合，将有助于建立一个既能保障用户数据所有权，又能让数据资源被有效利用的应用生态。
- **数据激励问题：**个人数据未来仍将是数据的主要来源，目前公众对于个人数据的搜集、管理的动机不足，核心在于激励不足，感受不到数据的价值。单体的个人数据虽然微小，但就像数据经济的毛细血管，占据了人体血管的 97%，只有激活个人对数据的搜集、管理和应用意识，数字经济才能获得更多新鲜的血液。目前的数据生态里，个人是数据的产生和贡献方，但是互联网公司切走了数字经济中的大部分蛋糕，如果有更好的、能获得多方共识的数据利益分配方案，不但个人能从数据的生产和分享中获得激励，企业也将合法获得更多维度的数据，做大数据经济的整体规模。

数据价值问题

物联网系统每时每刻都产生着大量数据，这些数据在商业应用与科研领域都具有极高价值。例如：基于交通出行数据，运用深度学习的方法训练更准确更高效的路径规划算法；医疗护理机构可以利用摄像头等传感器的数据更精确的判断病人的状况，从而设计更加定制化的护理方案。然而，在“烟囱式”的孤岛架构体系下，大量的交通数据掌握在几家中心化平台手中，无法实现高效的互联互通，中小公司无法利用这些资源，高校等科研机构也难以获取高质量的数据集，这严重阻碍了科研的进展，也导致数据的价值无法充分体现。此外，大部分物联网设备单独联网是没有实际意义的，只有多项数据综合分析才会产生价值，若数据无法互联互通，则无法实现价值的传递。

商业模式问题

物联网设备的联网、计算、存储等功能带来成本的增加，但是对于大部分传感器等传统设备而言，联网并不是其核心功能所在，而仅仅依靠售卖硬件的模式无法支持长期维护相应的 IT 系统带来的巨额开销。当前中心化架构下，大部分厂商对于物联网设备的 IT 功能系统无法充分利用，商业模式也仅是单纯的售卖用户数据，这一点又涉嫌侵犯用户的权益和隐私。随着物联网系统的进一步发展及开放以及用户安全意识的提高，当前商业模式必将迎来一轮大的变革。

1.2 区块链技术为物联网带来新的发展潜力

区块链作为一项新兴技术，在解决数据安全、隐私等方面展现了极大的潜力。目前，已有众多研究者和企业将区块链技术引入越来越多的领域。其中，物联网与区块链的结合是最具发展潜力的一个方向，区块链技术有机会重塑其基本架构，并解决当前中心化“烟囱式”体系中的一系列挑战。

显著降低设备互联成本

区块链技术的核心概念是分布式账本，即一个公开的、多方共同维护的分布式数据库。基于区块链构建基础物联网数据平台，可以有效解决“数据孤岛”问题，厂商无需再为自家的单一产品建立一整套数据解决方案，显著降低了设备互联成本以及后期 IT 系统维护成本。因此，基于区块链技术构建的去中心化物联网系统足以承载百亿级别的互联设备数据。

有效保护数据隐私

区块链技术最大的优势在于去中心化带来的隐私安全性，没有任何第三方控制用户数据，没有大量的数据存放在一个数据中心，降低了黑客攻击、恶意泄露等风险。利用区块链构建的物联网是一个人人参与、完全开放且安全的去中心化系统，所有用户可以掌控自己的数据，保护自身的隐私与权益。

实现数据价值传递

基于区块链的物联网系统是一个对等的去中心化网络，所有参与方可以平等地参与数据分享过程。所有用户可以对自己产生的数据进行访问授权，数据应用与服务商能以较低的成本合法获取大量有价值的用户数据，并在此基础上创建更智能化的服务，通过数据的实时流动实现价值的传递。

创造全新的商业模式

区块链技术改变了用户、物联网设备和厂商在物联网系统中的角色，不同于当前的中心化架构，在新的物联网系统中，用户可以动态制定数据授权机制以及设备之间的交互规则等；设备也不仅仅执行单一功能，区块链不止将设备简单互联，还能使得设备之间能自主交互；厂商也不再需要维护成百上千套不同体系中的 IT 系统。角色的改变将吸引更多参与者，重塑市场规则，创造全新的商业模式。

1.3 物联网区块链市场规模预测与应用展望

相比传统物联网系统而言，基于区块链技术的物联网系统通过设备之间的共识运行，无须中心验证，即使一个或多个节点被攻击整体网络系统依然可靠安全，通过数据加密技术和 P2P 互联网络保证数据的不可篡改和数据的隐私性，将有望解决传统物联网在安全、成本、商业模式等方面存在的问题。

知名研究机构 Research And Markets 最新发布一份关于区块链市场报告中提到：预计 2024 年，区块链物联网市场总值将从 2019 年的 1.131 亿美元增至 30.21 亿美元，年复合增长率达 92.92%。其中，推动区块链物联网市场增长的主要因素包括：物联网的采用率不断提高，对物联网安全、业务流程简化、透明度及稳定性的需求不断增长以及对运营效率日益关注。此外，区块链物联网市场的潜在机遇包括智能合约及数字身份的区块链解决方案获得更多的应用以及政府支持政策不断增多。

1.4 商用区块链系统面临可扩展性的瓶颈问题

区块链技术虽能实现去中心化的信任，蕴藏着巨大应用价值，但区块链技术的发展还远未成熟。在商业应用方面，区块链的数据存储能力、可扩展性、通用性、功能完备性、易用性等都还存在明显不足，现有的大型区块链系统架构，并不足以支撑高吞吐、高并发的商用系统需求。

数据存储与计算成本极高

区块链是一个大型的众多节点共同维护的分布式数据库，在区块链系统，数据只有追加而没有移除，数据只增不减，随着时间推移，区块链系统对数据存储大小的需求也将持续增大，这将导致商用区块链系统面临着极高的存储与计算成本；而大型的公有链应用平台，必然承载大规模的数据，在当前区块链的存储成本下，数据的存储能力与实际需求之间差距明显，大型公有链基础数据平台没有实际可行性。

通用性

在物联网领域，数据和业务类型多样，区块链系统需要适应多样化的业务需求，满足不同应用场景下的数据高效共享与数据安全，这意味着区块链对数据的记录方式要有足够的通用标准，才能很好地表示各种结构化和非结构化的信息，并且能够满足随着业务范围拓展所需的跨链要求。

共识机制效率低下

当前区块链以 PoW 为主流的共识算法对算力资源消耗极大，而在很多应用场景下，用户没有办法获取很强的计算能力。并且，所有以挖矿为基础的共识算法都将面临交易速度的瓶颈。若无法解决区块链系统的可扩展性问题，那么去中心化应用无法真正落地。

在上述背景下，物信链（Cyber-Physical Chain, CPChain）致力于解决物联网与区块链技术融合中的数据与交易的扩展性、安全性和实时性问题。首先，提出分布式云存储系统与区块链去中心化系统的平行分布式架构，解决大规模数据存储与分享的扩展性问题；其次，提出结合计算与通信的协同优化设计，开发全新的适用于大规模公有链的混杂共识协议；最后，融合智能物联网的端-边-云架构以及区块链的主-侧链架构，打造基于区块链的物联网设备自主身份及 DPKI 体系，以及物联网大数据共享平台。

2. 核心技术

2.1 平行分布式架构

CPChain 平台致力于构建一个面向物联网系统的基础数据平台，提供数据从获取、存储、分享到应用的全流程解决方案，突破区块链应用于物联网系统中的核心底层技术，为物联网数据的共享与交易提供基础设施；在此基础上构建数据聚合和实时数据流动应用，最大化物联网数据价值。去中心化的区块链系统要求全网节点对同一交易(数据)进行运算，从计算和存储角度来说具有很大的弊端，无法充分发挥分布式网络系统的协同能力，只能遵循“木桶原理”，因此不具有扩展性。CPChain 提出数据层与控制层分离思想，构建平行架构来增强系统的可扩展性。在保护用户隐私的同时提供开放的数据分享功能，采用分布式存储方案，将用户数据加密上传云端，降低区块链的存储负担，同时又能确保数据的完整性与准确性。

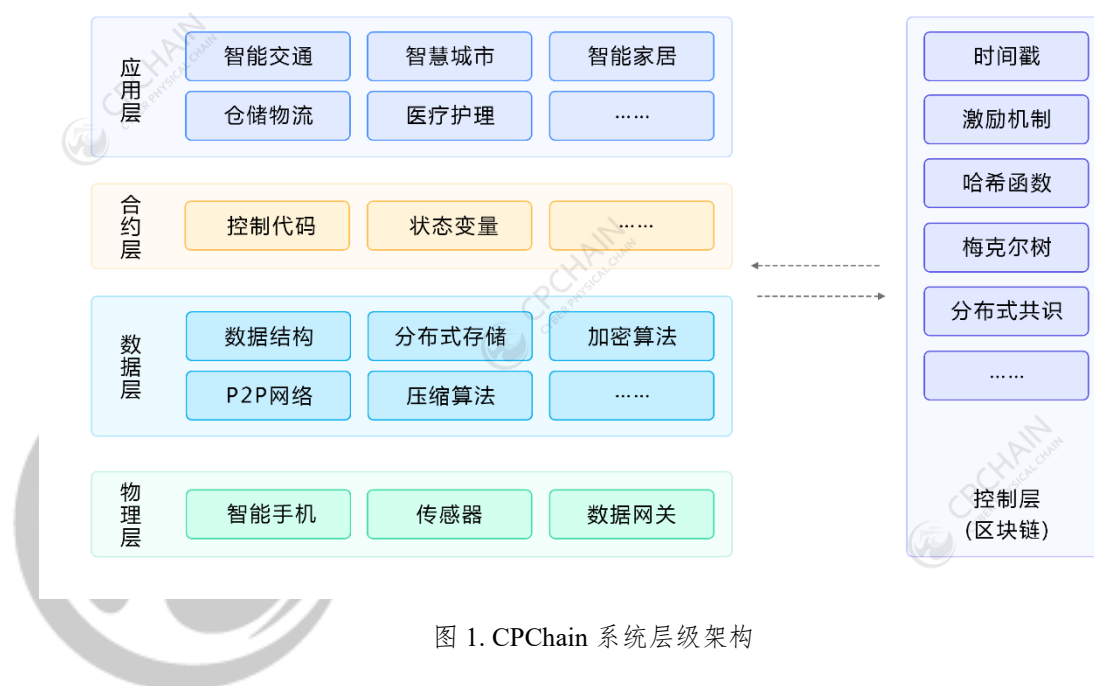


图 1 具体给出了 CPChain 系统层级结构，由物理层、数据层、合约层、应用层和控制层组成，区块链作为纵向的控制层对数据的交互进行监管。物理层是 CPChain 物联网系统数据获取的基础，主要包含智能手机、传感器、数据网关等，加入 CPChain 网络的智能设备需运行一个区块链节点或与区块链网络进行通信，同时也作为去中心化应用的运行环境，处理加密、共识等操作；数据层处理主要

的数据,针对不同的应用设计不同的数据结构与压缩算法,提高数据的读写效率,原始数据无需上链,仅上传哈希值作为数据的唯一标识以及完整性与正确性的凭证,原始数据在用户侧加密后存储在分布式哈希表(Distributed Hash Table, DHT)中;合约层是系统功能的核心,由于智能合约部署在区块链上,合约规则难以更改,因此,合约的设计应当基础且简洁,将更多的交互功能放在应用层;应用层是用户与合约交互的接口,可根据不同的需求开发不同的应用;控制层的功能由区块链完成。

基于区块链技术构建的去中心化系统与传统的分布式系统不同,去中心化系统中,计算与存储任务是冗余的,去中心化节点中的每一个节点都要存储相同的数据并执行相同的计算任务。这种冗余的存储与计算一方面使区块链系统能不依赖于可信第三方稳定的运行,确保了数据的完整性、不可篡改性以及系统的一致性;另一方面,过多的冗余数据也加重了系统的负担,使得新节点的加入成本越来越重,长远来看,这种模式不可扩展、不可持续。以比特币为例,比特币区块链的大小在 2019 年第一季度已经超过了 210GB,这使得新节点需要耗费大量的时间用于同步数据,并且随着时间的推移,新节点进入难度持续增加。冗余的计算确保了系统状态的一致性,是有价值且必不可少的,但数据的大量冗余存储却造成了系统负担加重,不具备可扩展性。为解决数据存储、分享与交易的扩展性问题,CPChain 提出平行分布式架构,如图 2 所示,将去中心化的主链、行业链网络和分布式存储系统有机组合。区块链作为 CPChain 平台的控制层,不再存储系统的全部数据,仅上传数据的标识与凭证,既极大的减小了平台的存储负担,又能确保系统的一致性。

CPChain 平行分布式架构中,分布式云存储层与区块链层作为两层平行的分布式网络,平行分布负责数据存储与计算任务。用户数据将在客户端加密后分块,各个部分进入不同存储节点,同时哈希凭证上传区块链网络的所有节点,以便后续对数据进行验证、确权等操作。平行分布式架构将数据层从区块链中剥离,既保留了区块链系统安全、去中心的特性,又提高了可扩展性,大大减小了区块大小。当前很多区块链平台都面临扩容的问题,例如增加区块容量,但仅增加区块容量会提高区块链节点维护成本,造成节点数较少,系统安全性会降低。通过 CPChain 的系统架构,在区块大小不变的情况下,单个区块可以打包的交易数量大大增加,可以极大提升平台的交易处理速度。

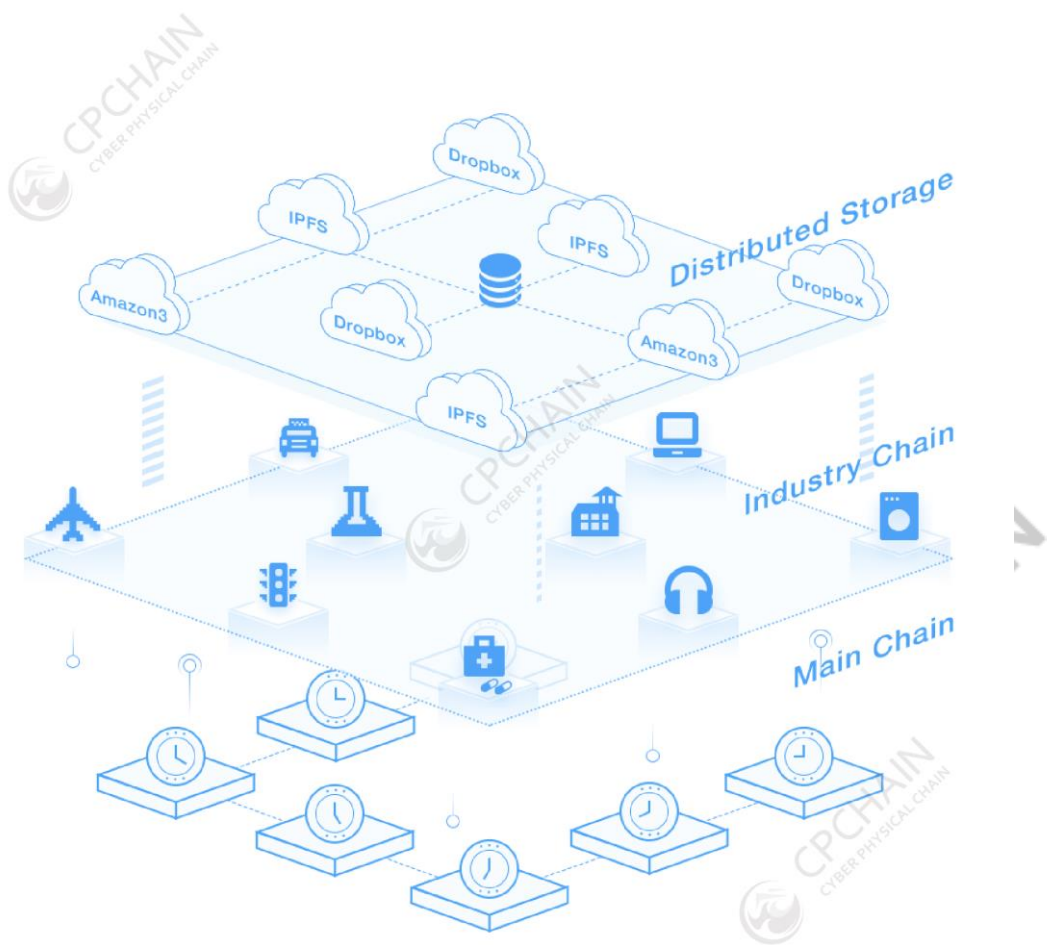


图 2. CPChain 平行分布式架构

2.2 平行分布式加密存储、检索和授权共享

CPChain 采用平行分布式架构，在该架构下，典型物联网数据上传与分享过程如图 3 所示。为保障数据安全、可靠、高效地在网络中进行分享，CPChain 创造性地将分布式存储技术与重加密技术以及同态加密技术结合起来，从而实现高效的数据访问控制机制。下面从四个方面阐述平行分布式加密存储、检索和授权共享所涉及到的关键技术。

2.2.1 基于 DHT 的分布式加密存储

物联网数据的分布式存储过程如图 4 所示。系统将数据层与控制层分离，所有原始数据在本地进行加密并由所有者签名，在进行分块后基于分布式哈希表方法保存在不同的节点中，使得宿主无法知道原始数据。同时，将数据的哈希值存

入区块链，作为数据完整性和正确性的凭证以及数据的标识。

区块链还对数据做访问控制，数据的拥有者在存储数据时，区块链会存储每一条数据记录的访问权限，可以通过发送一笔包含该数据标识的交易完成。用户想要取出数据时，需提供证明，满足数据的标识才能获取数据的访问权和使用权。若系统中存在恶意节点，其可能会无视访问权限，但数据都是加密处理的，并且在 DHT 中，每个节点只保存数据的随机一部分，因此，恶意节点的影响有限。由于所有数据均是在用户侧加密，因此需设计有效的数据授权访问机制来实现数据的分享。传统的分布式哈希表仅保存数据的 key-value 对，无法满足 CPChain 系统的需求。因此，在数据层，CPChain 提出改进的分布式哈希表方法，结合数据加密计算使用的密钥，记录密钥与数据块之间的对应关系。

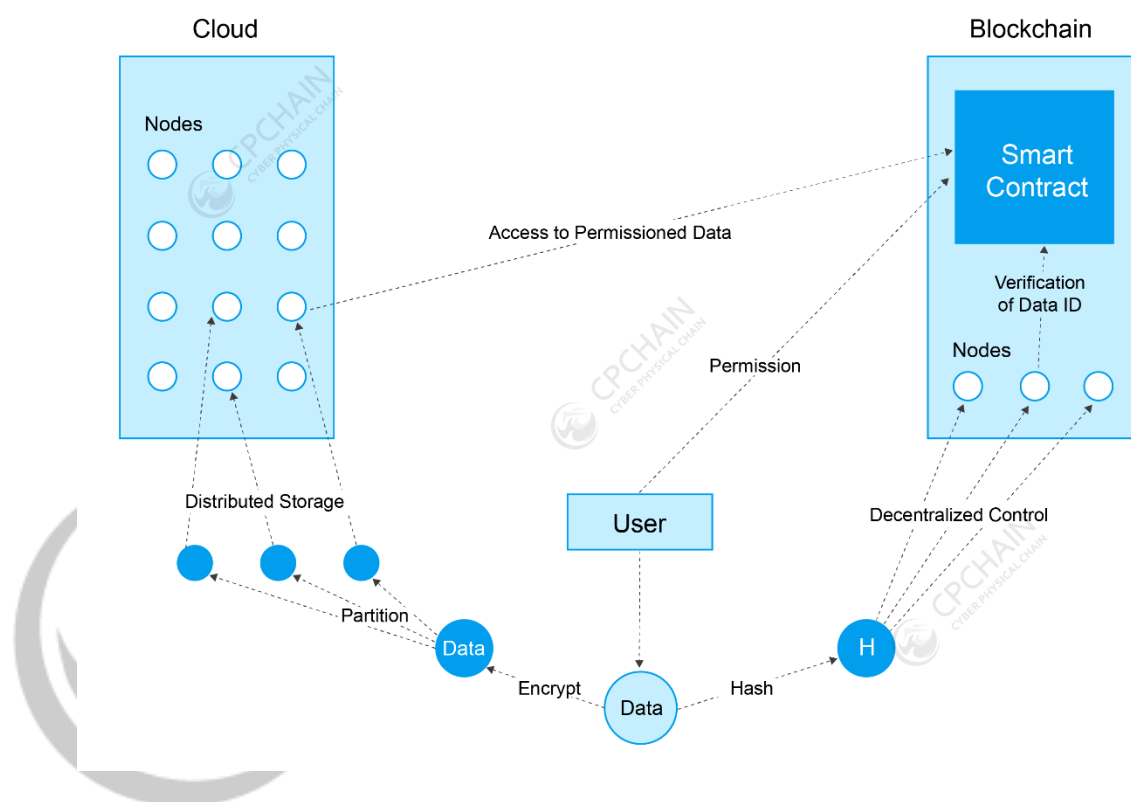


图 3. CPChain 典型物联网数据上传与分享

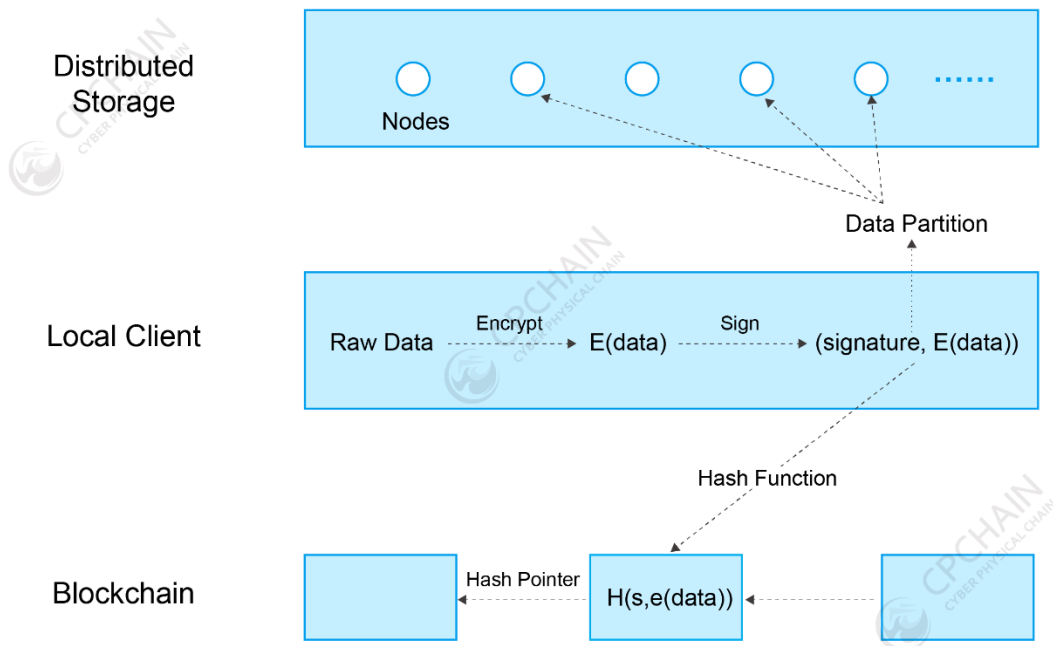


图 4. 数据分布式存储过程

数据的加密和解密均会消耗一定的计算资源，面对物联网系统每时每刻都在产生的庞大数据量，对每一条数据记录单独加密无疑是对算力资源的巨大浪费。因此，必须针对不同类型的物联网数据设计合适的数据结构和加密机制，以同时满足数据安全和处理效率的需求。CPChain 平台将产生的数据按时间顺序排列，以链式结构组织，同时设定时间周期 T ，将一个周期内的数据打包成块，在此基础上选择加密区间 e 与上传区间 u ，使一条区块链记录能保证整个区间内的 u 个数据块中数据的完整性与真实性。

2.2.2 基于加密计算的数据共享与应用

CPChain 平台将数据层从区块链中剥离，为保证数据的安全与隐私，所有原始数据均在用户侧进行加密。由于数据对第三方不可见，如何实现对加密数据的计算或分享是平行分布式架构所面临的首要挑战。区块链平台采用的公钥加密体系在引入分布式加密存储后将不再适用，因为公钥加密技术需使用接收方的公钥对数据进行加密，如图 5 所示，只能实现一对一授权。而在 CPChain 平台中，希望实现数据一次加密上传，多次授权使用，如图 6 所示。因此，CPChain 平台将深度研发重加密与同态加密技术，将加密技术与区块链技术深度结合，实现更

安全、更高效的数据分享与服务。

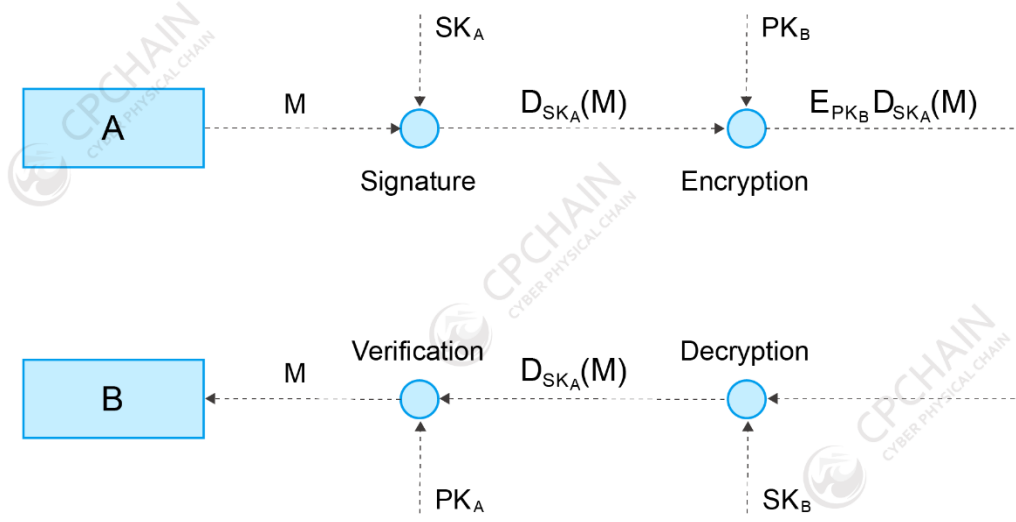


图 5. 公钥加密体系

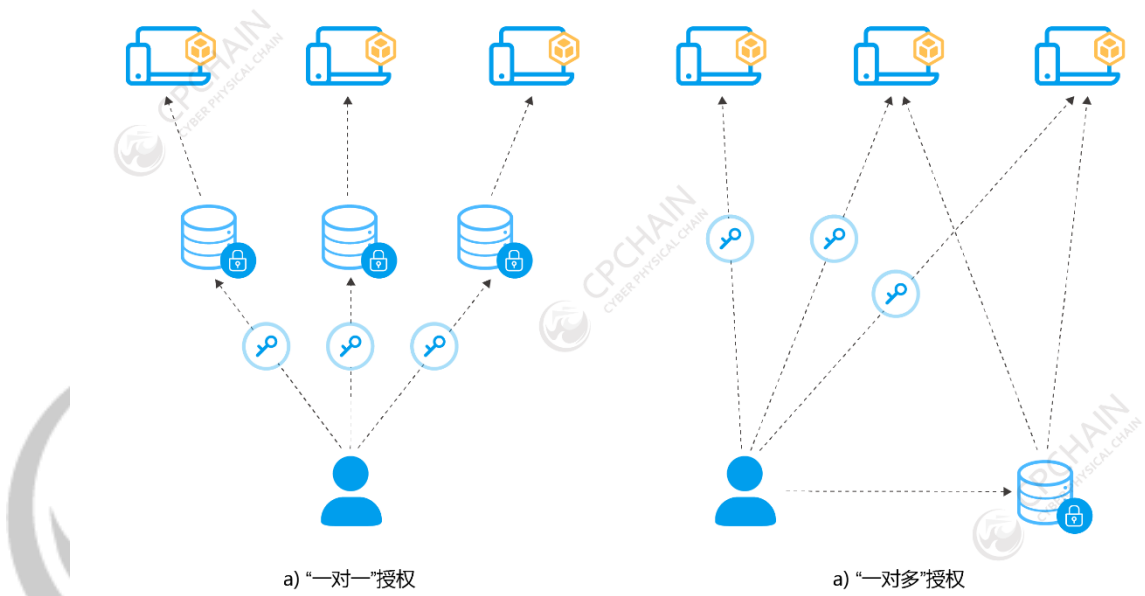


图 6. 公钥加密 “一对一”授权与 CPChain 加密 “一对多”授权

为实现一次加密多次授权，CPChain 基于重加密技术构建了一套对称加密与非对称加密结合的方案。用户在对每一个加密区间进行加密时采用对称加密的密钥，即加密和解密使用同一密钥，在改进的 DHT 中记录加密数据块与密钥之间的对应关系。为提高数据的安全性，每一个加密区间都需更新密钥。而基于非对称加密的重加密体系则用来传输加密数据所使用的密钥，这样可保证将数据的

授权限制在单个加密区间。

重加密技术可部分解决平行分布式架构下的数据共享问题，但其数据在智能合约下是可见的，面临一定的安全隐私问题。为此，CPChain 将引入同态加密技术，实现在加密数据下的计算与应用功能，如分布式加密匹配与搜索，增强对用户隐私保护。

2.2.3 Market: 数据交易信息聚合平台

PDash 是基于区块链技术设计的去中心化数据交易系统，在去中心化的前提下，通过模块化设计，将数据信息和交易信息分离，兼顾了用户的隐私和数据交易的效率，并引入代理网络保证数据可靠传输，在每一笔交易过程中，代理节点也作为卖家和买家之间的见证，结合智能合约中的一整套争议处理机制，在完全分布式的系统中实现可信的交易。

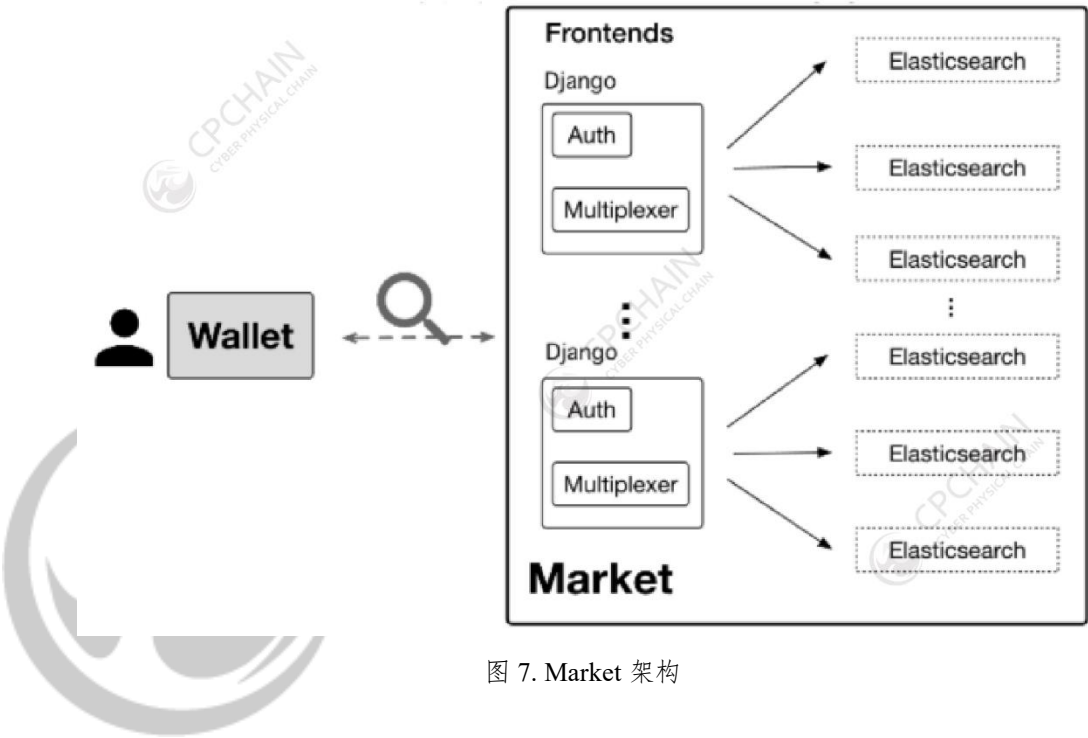


图 7. Market 架构

Market 是 PDash 的交易信息聚合平台，作为信息桥梁连接数据的卖家和买家。Market 包含身份认证、数据库、检索、链上信息同步模块等。卖家在 Market 上发布自己拥有数据的基本描述信息，这些信息以结构化的形式添加，包含标题、标签、描述、价格等字段；买家可根据实际需求检索 Market，检索程序支持自然语言检索，并匹配数据信息中所有字段。检索采用数据描述信息的哈希值做为数据索引，并将该哈希值，AES key，以及 URL 对应，储存在本地数据库。

图 7 所示的 Market 架构是传统的服务器/客户端架构，依赖于中心化的服务提供商运营。但是，Market 在 PDash 中仅仅是信息聚合的平台，整个交易的流程并不依赖于 Market，而是在 Chain 上处理交易逻辑。与比特币钱包概念类似，比特币转账是在同一条区块链上完成的，用户使用任一客户端都不会影响系统的运行，因此，Market 的架构并不违背 PDash 去中心化原则。另外，PDash 的 Market 与传统的商城系统不同，采用了与区块链账户体系兼容的椭圆曲线数字签名算法进行身份认证，用户无需注册，Market 运营方无法获取用户身份信息。尽管如此，若是 PDash 系统出现多家 Market 的运营商，则会造成数据信息的割裂，不利于数据的自由流动与聚合，违背了 PDash 的最终愿景，因此，CPChain 设计了一套基于区块链的去中心化的 Market 架构，如图 8 所示。与传统的中心化架构相比，去中心化的 Market 架构增加了 local data synchronizer 和 chain data synchronizer 等模块，分别负责将本地数据同步到链上、将链上数据同步到本地，去中心化的 Market 主要通过这些新增模块保证任意一台服务器运行一个新的 PDash Market 都能获得相同的数据信息，不会产生割裂。

去中心化的 Market 有一个 ID 生成模块，为每一份发布到 Market 中的数据生成一个唯一 ID，以便更高效、更准确地在 Market 与 Chain 之间同步数据。每当有新的数据信息发布时，local data synchronizer 就会将数据同步到链上，同时，chain data synchronizer 会周期性的监测链上数据，将新数据信息同步到本地。

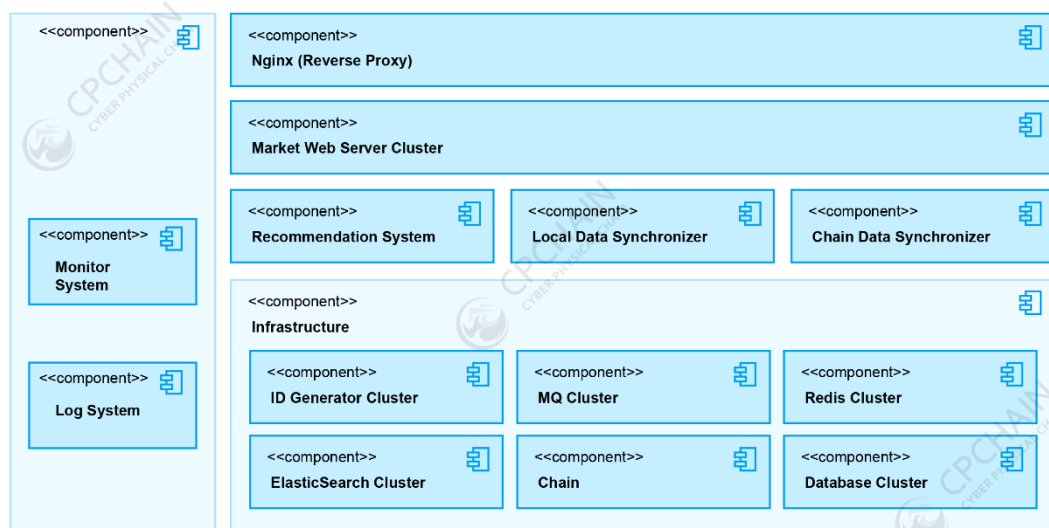


图 8. 去中心化的 Market 架构

2.2.4 OTP: 基于区块链的数据开放传输协议

Open Transfer Protocol(OTP)是基于区块链的数据传输协议,提供数据在不同客户端之间的安全可信传输。OTP 为客户端提供了一种通用方法以使用不同的外部存储系统来交换数据和消息。通过集成区块链技术,OTP 支持独立于具体用户的信任机制,使用户可以完全控制自己的数据。同时,OTP 提供注册函数,可以为用户分配 OTP 格式的 URI (唯一资源标识符)。

OTP 不仅仅在 PDash 中负责数据的传输,更是一个全新的基于区块链的通用数据传输协议。OTP 的设计目标包括:

1. 独立于具体用户的信任机制。OTP 利用区块链对数据完整性进行校验,对代理节点的身份进行验证,在数据传输过程中提供了信任机制,而不依赖于任何具体的用户或可信第三方;

- 2、高度的兼容性。考虑到不同的用户往往将数据存储在不同云存储系统中,因此,OTP 设计了兼容方案,OTP 客户端可以与异构的存储系统进行交互;

- 3、用户掌握的访问控制。OTP 集成了一套非常细致的访问控制方案,数据完全由用户自己控制,用户可以授权不同的代理节点访问自己不同的数据;

- 4、出色的可扩展性。OTP 的设计可以承受数据量、用户数和访问量的快速增长;

- 5、简单的交易逻辑。我们利用代理节点组成的网络作为数据分发网络,作为数据发送方和接收方之间的桥梁,处理复杂的网络功能,简化客户端的逻辑,使数据传输更加容易和轻量级,对于物联网设备意义重大。

2.3 DPoR 共识结构

CPChain 采用上海交通大学分布式智能系统实验室自主研发的 DPoR (Dynamic Proof of Reputation) 协议,将整个区块链系统分为三层(见图 9)。普通节点通过准入考核后,即可成为荣誉节点。系统设计了特定的选举算法,从荣誉节点中(第二层)选举出部分节点组成动态委员会(第三层),负责区块链的维护。第三层主要解决了委员会内部对区块的添加、验证、广播和上链的共识问题。总体而言,DPoR 可应对大规模网络的共识问题的三个子问题,分别为节点信誉度评估、节点选举、委员会内部拜占庭容错(Byzantine Fault Tolerance, BFT)共识。

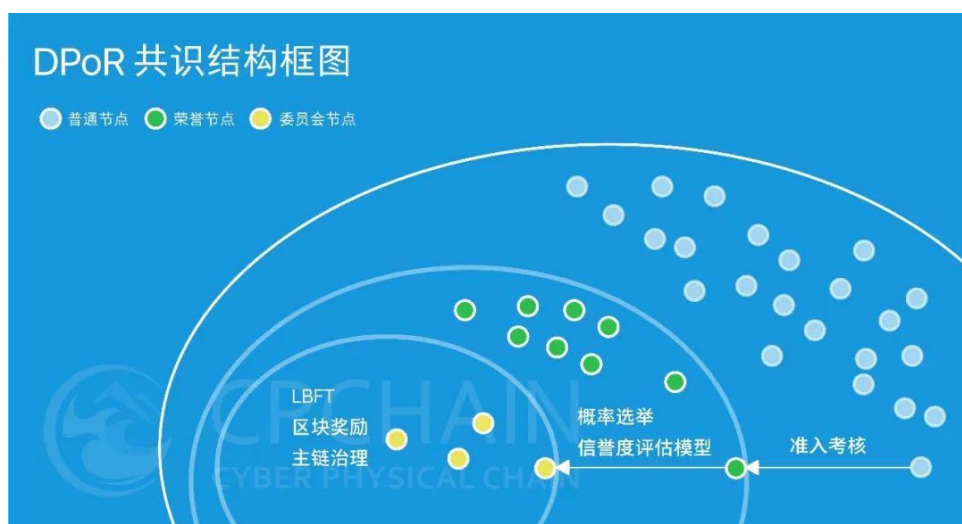


图 9. CPChain DPoR 共识结构

2.4 大规模公有链的 LBFT 2.0 共识

在大规模 CPChain 公链系统中，基于网络规模大、物联网数据量大的网络特征，节点状态一致性和分布式数据存储的实现面临诸多挑战。CPChain 将开发一种性能可扩展的混合共识协议，并提出一种动态的委员会选举机制，以解决基于 PoW 共识协议的系统可伸缩性问题。

主链结构的核心问题是确定哪些节点完成数据收集，哪些节点将链打包在块上，以及如何确保区块数据的安全性和一致性。传统的分布式故障容错算法，如 PBFT 和 Zyzzyva，更多地依赖于通信复杂度来保证节点间的一致性。例如，PBFT 算法采用三相协议确保系统的一致性，以及即使存在恶意拜占庭节点，也能保证节点故障的恢复。然而，由于该算法更依赖于通信来保证算法的安全性，以至于系统的可扩展性较差；此外，随着节点数量的增加，系统的性能下降速度加快；当节点数量超过某个阈值时，该系统将不再可用。PBFT 依赖于一个主副本，它承担向所有备份节点广播请求的职责，任何涉及主副本的错误行为都会导致其吞吐量大量下降。因此，PBFT 的吞吐量不存在下限。只要系统能在有限的时间内做出响应，该系统的活跃度就会一直保持。传统的拜占庭容错算法由于其在小规模网络中的可靠性和可用性，使其更适用于私有区块链和联盟链环境。针对这一问题，CPChain 的核心方案是为动态委员会设计一个动态投票机制，选出可信的委员会对区块的数据进行收集并打包各个区块的任务。

2.4.1 二权分立委员会

传统的拜占庭容错算法不能直接应用于大规模的公有链场景，PoW（工作量证明）共识协议消耗大量的计算资源，从而导致效率低下。CPChain 提出了一个基于二权分立委员会的三层协议 LBFT 2.0，以提高 CPChain 的共识性能。委员会由两部分组成：验证委员会和出块委员会。验证委员会指的是对可以进行出块的提案委员会成员进行验证的一组用户。它具有以下特性：

- 所有验证者共同构成验证委员会；
- 验证委员会主要由 CPChain 基金会、政府以及企业提名的节点共同构成；
- 除某些异常情况外，验证委员会中的验证节点将不会出块；
- 验证委员会遵循 CPChain 所设计的 LBFT 2.0 协议，以达成共识；
- 验证委员会成员数量总是等于 $3f + 1$ ，其中 f 是拜占庭节点的数量。

出块委员会成员由每一届内固定数量的荣誉节点选举产生，其中包含以下属性：

- 出块委员会成员根据候选人的荣誉参数和随机种子选出；
- 每一任在任期的成员轮流承担着在该任期内出块的职责；
- 出块人指的是分配给当前轮次中出新块的成员；
- 出块者的不当行为将面临来自验证者的弹劾机制，验证者将因提议的失败而惩罚该出块者。

其余用户均为普通用户。一旦一名普通用户获得荣誉节点的资格，就可以宣称自己是参与委员会竞选的候选人。候选人当选后，将于后续任期内加入出块委员会。

2.4.2 LBFT 2.0 有限状态机

LBFT 2.0 协议可以看作是一个有限状态机(FSM)，有 5 种状态：空闲状态、准备状态、提交状态、弹劾准备状态和弹劾提交状态。前三个状态是为正常情况设置的，其余状态被称之为弹劾状态，专门处理非正常情况。

图 10 展示了这五种状态以及状态之间的转换。

对于正常情况，验证者会在空闲、准备和提交状态之间切换。而对于异常情

况，则进入弹劾准备或弹劾提交状态。

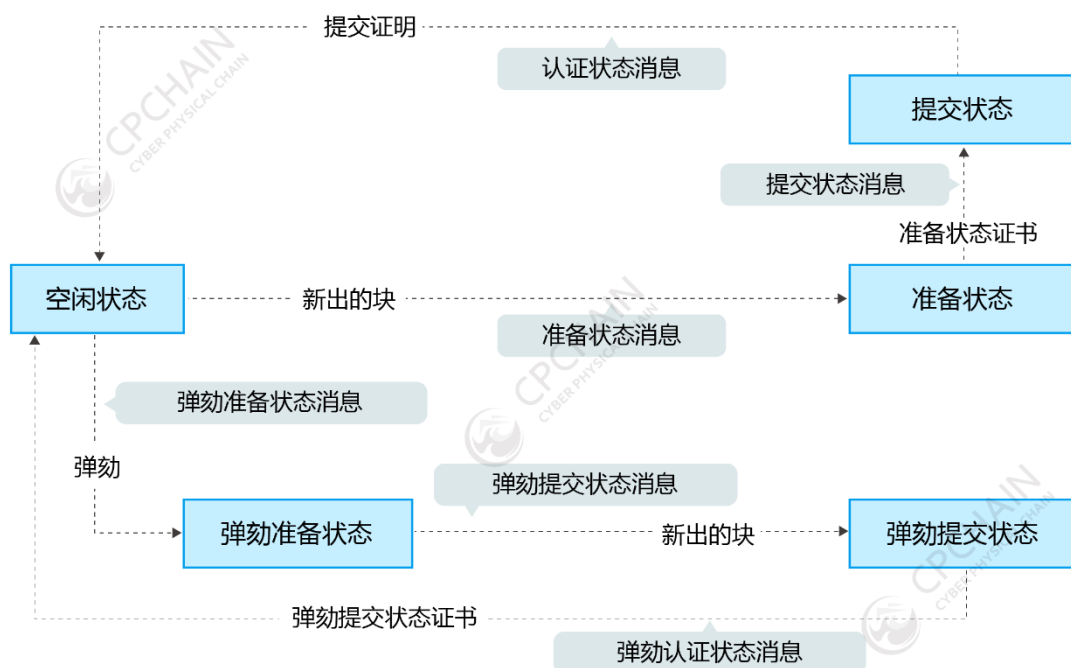


图 10. 有限状态机的 5 种状态转换

仲裁

在深入解释案例处理程序之前，让我们先介绍一个重要的概念仲裁。仲裁是验证委员会成员的子集，在特定情况下可以在仲裁中达成一致。这些群体有两个重要的特性：

- 交集：任何两个仲裁机构至少有一个共同的忠实验证者；
- 可用性：始终存在一个不会出错的仲裁验证者。

当仲裁中的成员认可来自同一区块的信息时，他们将收集仲裁证书。证书分为两种，准备证书(P-certificate)和提交证书(C-certificate)；表明存在一个仲裁机制分别就准备的消息和提交的消息达成一致。

块生成

一个普通用户要求参与竞选，获取入选资格（即成为荣誉节点），然后进入候选人名单。候选人经定期选举产生后，该用户即加入出块提案委员会。关于其出块的块号，提议者生成一个区块并广播给验证委员会的所有验证者。

常规情况处理流程

一旦接收到一个新生成的区块,验证委员会中的验证者将按照以下步骤对该块进行验证。

- 块验证过程中要仔细检查该申请人的标识、时间戳等;
- 如果验证通过,此验证者将向验证委员会中的其他验证者广播一条 **PREPARE** 消息;
- 一旦接收到 $2f + 1$ **PREPARE** 消息(**P-certificate**),验证者即向其他验证者广播提交消息;
- 一旦接收到 $2f + 1$ 条(验证通过)提交消息(**C-certificate**),验证者就将该区块插入本地链,并将验证消息连同这 $2f + 1$ 验证者的签名广播给所有用户;
- 一旦验证者在块高中首次接收到验证消息,它将向所有节点广播相同的消息;
- 任何用户收到具有足够签名的验证消息后,都将该块插入本地链。

弹劾机制

在 LBFT 2.0 中,弹劾是一个关键的异常处理程序,当提议者发生出块故障或无响应时启动弹劾机制。它是一个基于 **PBFT** (实用拜占庭容错算法) 的两阶段协议,分为准备和提交阶段。当验证者触发其弹劾机制时,它将代表出块故障(或没有响应)的提议者生成一个块。与正常出块流程相比,弹劾机制具有更高的优先级。换句话说,除了验证消息外,弹劾机制中的验证者不处理任何正常的案例消息。弹劾机制围绕以下两种情况开展:

- 验证者定时器超时;
- 处于空闲状态的验证者接收到来自提案者的非法块。

计时器超时的原因有很多,比如提案者未给予响应、双花攻击和时间戳不正确。非法区块可以是具有不正当交易和标识的区块。下面列出了弹劾程序的步骤:

- 委员会中的验证者 v 生成弹劾块;
- 此块被用作弹劾准备消息,广播给委员会中的所有验证者;
- 一旦接收到具有相同头部和主体的 $f + 1$ 条弹劾准备消息,验证者 v 就向其他验证者广播弹劾提交消息;

- 一旦接收到 $f+1$ 条弹劾提交消息，验证者将向所有用户广播携带着 $f+1$ 个签名的弹劾验证消息；
- 任何验证者第一次接收到弹劾验证消息，即插入弹劾块并向所有节点广播相同的该消息；
- 如果所有用户均接收到弹劾验证消息，则将该块插入本地链。

CPChain 主网将能支持最高每秒 1000 笔交易，即每个有效块可容纳 10000 笔交易。超过这个数字的交易将会被顺延至下一个块处理。由于 CPChain 每隔 10 秒产生一个有效块，在正常情况下一笔有效交易将会在 10 秒钟之内确认并上连。

2.5 高实时性、安全性的侧链共识系统

CPChain 作为物联网系统的基础数据平台，其主链是一个通用的物联网数据控制层。然而不同的物联网垂直应用，具有不同的性能需求，典型的对实时性要求严苛的应用包括无人车实时控制、车队协同等。在此类应用中，为完成物联网中各设备节点间的协同、高效工作，CPChain 需支持实时控制信令的安全通信与交互。数据交互若仍然通过主链完成，将面临极大的延时，无法保障各类应用对实时性的要求。物信链将选取典型的应用场景，开发轻量级侧链共识协议来满足机器数据交易高频、细粒度、高安全性和实时性等需求。具体地，CPChain 在行业链中将结合边缘计算、硬件安全方法设计侧链共识系统，确保各类应用对信息交互时延的要求得以满足，从而实现对侧链网络的高实时性和高安全性，如图 11 所示。

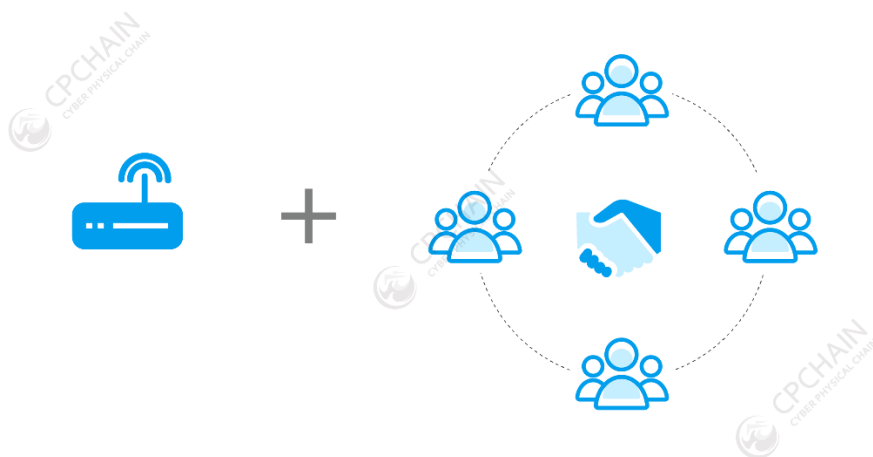


图 11. 基于硬件加速的利他合作模型

2.5.1 数据网关和嵌入式加密算法

物联网中各传感器采集的数据由于存在异构性,而传感器自身往往不具备计算能力或计算能力极为有限,若将对传感数据的处理与认知相关的计算置于各传感器节点,则将带来更大的时延,无法满足应用需求。由于物联网中部署的网关设备具有较之于传感器节点更为强大的硬件支撑,可提供更为高速的计算能力,且其设备电能不受限制。因此,通过利用物联网中部署的数据网关,将传感器数据聚合到边缘网关进行数据处理、加密计算,一方面降低了由数据处理带来的计算时延,另一方面减轻了物联网中各传感器节点的计算负荷,延长了其工作时间。

2.5.2 行业链共识算法激励与安全机制

物联网系统由 Mesh 网络或无线 Ad Hoc 网络组成,其无线通信技术包括 IEEE 802.11p、NB-IoT 等。因此,物联网中机器交易共识可充分利用无线网络系统特性,将共识过程嵌入于网络通信协议中,使得共识过程中信息交互无需涉及数据层,仅通过更加底层的通信层完成,降低了该过程中的时延。此外,考虑到机器交易的高并发性、实时性和安全性需求,CPChain 将基于演化博弈理论研发高效的利他合作激励机制和安全机制,如基于有向无环图(Directed Acyclic Graph, DAG)数据结构的利他合作激励机制,从而使得 CPChain 侧链上的应用效率更高、速度更快,也更为安全。

2.6 测试与正确性验证

自动化测试是 CPChain 持续集成 workflow 基础。CPChain 利用 Jenkins 部署自动化测试服务器,并使用 Jepsen 作为模拟测试用例框架。

在以下部分中,将从不同角度介绍 CPChain 测试框架。

2.6.1 白盒测试

白盒测试主要用于检查区块链的内部功能和结构,研发人员对于待测试的所有代码的功能有着清晰的认知。白盒测试包含三个级别:单元,集成和回归测试。

单元测试

单元测试由 Go 语言编写并附带区块链代码,这些链代码存储在 CPChain 代

码仓库中。所有单元测试文件均以`-test.go` 结尾。每个单元测试文件都包含数个测试函数，用于在给定输入的情况下，与预定的输出对比，检查其相应功能。

此外，单元测试还包括对 Fusion API 和 RPC API 功能测试。

集成测试

CPChain 中一部分 Go 文件引用并集成了多个文件，用于实现更高层的功能。这些文件同样拥有其相应的测试文件来进行集成测试。

回归测试

当远端代码仓库中更新某个分支时，Jenkins 都会激活所有测试文件进行回归测试。我们通过这种方式来重新执行单元测试和集成测试，确保现有代码中引入新的错误。

2.6.2 黑盒测试

黑盒测试指的是在并不了解内部实现的情况下检查区块链系统的功能。在黑盒测试中，会列出测试用例列表以检查系统是否正常工作。每个测试用例包含三个部分：

场景：简要描述用例；

步骤：如何重现用例；

预期结果：一个正常的链，在执行完上述步骤后的预期结果是什么。

异常共识测试用例

共识是区块链的核心。当验证者和出块者面临拜占庭错误时，需要确保链的安全性和一致性。因此，CPChain 设计了大量关于 LBFT 2.0 共识的测试用例（包括异常和正常测试用例）以测试链的功能。对于每个可能的异常情景，如面对非法行为的应对，均设计一种输入及其预期输出来模拟该情况。该测试用例采用 Jepsen 框架实现。

稳定性测试用例

稳定性测试包括启动、重新启动和终止引导节点、出块者、验证者、普通节点和智能合约管理员。该测试提供了链在极端情况下的稳定性证明，如停电，连接错误等。

挖矿测试用例

出块者有责任出块并广播。这组测试用例分为几种类型：

出块者：包含策划的测试用例，其中提议者执行不同的行为。

竞选：检查竞选日志、api、候选人列表和智能合约。

RNode：确保在不同条件下参与的 RNode 是没有问题的。

奖励：保证正确计算和分配基本和维护奖励。

准入控制（AC）：确保为最小 CPU 容量设置的阈值按预期工作。

验证者：测试验证者合约和域的有效性。

启动和停止：通过多次中止和重新启动链进行稳健性测试。

Nemesis 测试用例

我们可以利用 Jepsen Nemesis 来模拟一些异常情况，如：

- 网络包延迟；
- 网络断连；
- 节点崩坏；
- 时间漂移（错误的本地时间）；

Nemesis 测试样例可能会与其他样例重复

兼容性测试用例

兼容性是所有去中心化系统都必须面对的重大挑战，因为不是所有的节点都会更新到最新版本。类似于比特币中的软分叉与硬分叉，CPChain 也有软更新与硬更新。在软更新中，旧版本的节点依旧能参与到链中。而在硬更新中，旧版本节点将不能参与竞选，甚至不能同步。

兼容性测试保证了区块链与所有最新版本的节点不会受到旧版本节点的影响。

压力测试用例

压力测试通过提高交易量，来逼近链能达到的吞吐上限。压力测试方面主要分成不同类型：

1. 以接近我们的 tps 上限的速率发送数据，从而测试 CPChain 主链在这种压力下是否还能稳定的处理所有的交易；
2. 以超过我们的 tps 上限的速率发送数据，从而测试 CPChain 主链是否不会崩坏，超过上限的交易是否会顺延到未来的块。

2.6.3 DDoS 攻击

DDoS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击，是所有分布式系统中都必须面临的问题。DDoS 是通过操纵多台服务器，联合对一个或多个重要目标进行大量的服务请求，从而完全占据目标的计算资源或者带宽，从而达到瘫痪目标原有功能的目的。

以太坊、比特币等传统区块链，由于其完全去中心化的设计，并不惧怕 DDoS 攻击。每一个单一节点，甚至小部分节点的瘫痪都不会对其 P2P 网络造成任何影响。但在 CPChain 上，验证节点正是 DDoS 攻击潜在的目标，面对可能的 DDoS 攻击，我们采取了如下对策

1. 设立多台默认出块节点，作为备选方案；
2. 验证节点设立一个白名单，其中包含了所有默认出块节点；
3. 每台验证节点上设立一个检测器。一旦发现 CPU 长时间超负荷运转，就会默认自己遭受 DDoS 攻击，启动白名单，在防火墙的层级上拒绝除默认出块节点以外所有节点；
4. 当以下三种条件之一满足的时候，移除白名单：
 - a) 一段时间内不再检测到 DDoS 攻击；
 - b) 连续长时间开启白名单；
 - c) 手动进行解除。

2.6.4 形式验证

软件验证并不能证明一段代码是否存在缺陷，数学上是否完备。形式验证通过一定的形式或者规范，在更高的层次上描述一个程序，从而判断数学上是否正确。

形式验证在高度并行的程序上尤为重要。死锁与竞争危害都是并行程序上必须考虑的重要问题。为此我们将使用 TLA+ 作为形式验证语言，对 CPChain 进行

形式验证，从而确保算法正确性。

2.7 性能

CPChain 在不同的环境下有不同的性能。主要有两个性能尤其值得我们关注，分别是公共环境与受控环境。

2.7.1 公共环境

公共环境就是指在实际的公共网络环境下运行。它具有以下特点：

1. 节点分布在全球各地；
2. 每个节点都有着截然不同的硬件与网络配置；
3. 每个节点都由不同的用户操作，其中绝大部分用户对链的实现并不熟悉；
4. 不是所有的节点都更新到最新版本。

其中验证节点将都为 CPChain 布置，具有相同的配置：

1. 虚拟服务器类型：亚马逊云计算服务（AWS）t2.large 模组；
2. 网络：1 Gps（预估值）；
3. 地点：新加坡；
4. 处理器：3.0GHz 英特尔可扩展处理器，两个虚拟处理器；
5. 内存：8GB；
6. 数量：共计 7 台服务器；

在该配置下，CPChain 团队在 2019 年 5 月 1 日至 6 月 5 日之间进行了一次 Beta 测试。遍布全球的 795 个普通节点，70 个荣誉节点以及分布在新加坡的 7 个验证节点参与测试。最终 Beta 主链得到 70 万个块（其中包括 Beta 测试期间生成的近 30 万个块），440 万笔交易，交易峰值可达每秒 1000 笔交易。

2.7.2 受控环境

受控环境指的是一个受控的网络仿真运行环境。它具有以下特点：

1. 所有的节点分布在多台内网服务器，或者是由一台服务器发起的多个线程；
2. 各个节点之间的带宽可认为是无穷大，或者逼近网线极限；
3. 所有节点都是更新到最新版；
4. 所有节点拥有完全一致的本地时钟。

在该条件下，CPChain 主链在 1000-10000TPS 情形下均能稳定运行。

3. 商业应用

3.1 应用场景

3.1.1 智能出行

当前全球汽车保有量已突破十亿，出行行业已是庞然大物。智能出行是未来出行行业发展的重要方向，其发展趋势主要是基于智能网联电动汽车和智慧交通基础设施，实现高效的交通管理系统和灵活的出行服务。

目前，智能出行面临的挑战来自于技术和运营两个层面。技术上的挑战包括数据的采集与共享，难点为大量异构的设备和数据的有效管理；其次是服务提供商与消费者之间信任的建立，此外还需兼顾系统的安全与用户数据的隐私。

运营的挑战包括协作与激励，协作指不同服务提供商的账户体系的打通，为用户提供更集成的服务；激励指如何吸引更多用户参与到智能交通的生态中，共享个人数据，共建开放性数据平台。

区块链技术在建立信任、协作、激励与隐私安全方面具有巨大的优势，在实现用户交易去中心化的同时，采用加密算法技术，可与车载自组织网络技术形成互补，能够更好的保护用户的数据安全性和真实性的同时，实现用户数据确权。此外，通过区块链中的激励机制也可以更好的推动用户来分享个人信息，共同为用户提供强大的汽车数据服务和社区支持，将在未来智能交通共享生态以及集成的移动出行服务（Mobility as a Service, MaaS）服务建立过程中产生巨大的价值。

3.1.2 智慧医疗

医疗行业关乎民生且行业规模巨大。传统的医疗在医疗信息数据存储和共享上有很大的弊端，对于患者治疗、医情的流转的能力受到了一定的限制。“智慧医疗”开始兴起，医疗行业正朝着的“数字化”方向进化，药物（疗法）、设备、服务和商业模式的数字化转型已成为所有医疗参与者的战略。

在政府层面，大多数国家都制定了以智慧医疗为目标的政策或战略，数字健康记录（EHR/EMR）和其他健康信息技术（HIT）系统正成为新型医疗系统的核心。然而，由于医疗体系的复杂性，当前个人健康数据的安全性、完整性和访问控制依然有诸多限制，无法有效的优化数字医疗工作流程，不同的供应商、医院

和付款人、政府机构之间，仍存在着数据孤岛现象，妨碍着医疗协调的正常运行。另一方面，医疗供应链缺乏追溯性，医疗数据过于分散，对研究和服务会产生负面影响，药物研发成本持续上升，生产、贩卖劣药和假药的现象严重。

区块链技术具有可追溯性，而且准确度和可信度高，通过构建合理的数据共享激励机制协调各方利益。区块链技术及其用于健康数据无缝衔接的安全基础设施，可帮助医疗行业解决一些紧迫的问题，如网络安全、数据互操作性、药品供应链来源、保险公证和账单欺诈等问题。

3.1.3 公共安全

随着社会经济发展、技术进步和城市化进程加快，城市公共基础设施更新换代加快，对于城市公共基础设施的维护与安全防护也提出了更高的要求。

传统的智慧城市建设之中，城市基础设施如地铁、电网、地铁交通、水网、公共电梯等多采用中心化系统方案，聚焦于信息技术在各领域应用，顶层设计与统筹协调不足，产生了大量“信息烟囱”，制约了信息手段效能最大化发挥。同时，中心化系统，一旦遭受攻击，将面临系统瘫痪，无法及时响应城市公共服务，造成公共事件。

区块链技术为城市基础设施如：地铁、电网、地铁交通、水网、公共电梯数据的可信流转提供低成本解决方案，在记录、跟踪和验证设备的历史记录、保证设备的真实性、隐私性和安全性，进行设备与设备之间、设备与人之间的智能活动等方面发挥着重要作用。

基于区块链技术的智慧城市系统，融合了点对点网络、数据加密、共识机制、智能合约等技术，可有效提高城市物联系统安全性。每一笔记录与实际物联设备相关联，将保证上链数据的真实性，另一方面，由于系统的去中心化特性，有效防止了大规模关键物联网基础设施被破坏，即使单个基础设施遭到攻击，整个系统仍旧保持正常运转，避免出现城市公共基础出现大面积瘫痪现象。

3.1.4 去中心化身份认证（DID）

近年来，网络空间数字身份管理备受关注。目前，OECD 的 18 个成员国已经制定或正在考虑制定本国的数字身份管理政策，其中美国已于 2011 年 4 月正式发布《网络空间身份信任国家战略》，全面系统地提出了“网络空间可信任身

份生态系统”的战略构想。但在数字身份认证领域尚存在着一系列痛点，亟须有效解决。

个人数据真实有效性缺失：用户虽然获得了身份认证，但并没有真正掌握身份的控制权，无法真正确定数字身份的用户是否是其本人，难以从源头追溯系统中数字身份信息的真实有效性。

社会基础设施搭建不完备。身份属性种类众多，不同应用场景所需要用到不同身份认证信息，但不同中心化认证系统尚未打通，而系统之间的相互认证又需要经历非常复杂的流程，难以进行一致性协同管理。

认证技术简单使隐私易泄露。目前各大平台的身份认证手段相对比较简单，背后隐藏着较大的个人隐私信息泄露风险，可能导致用户信息被出卖，造成严重的财产及相关利益损失。

另一方面，DID 也与物联网设备的身份标识和身份认证密不可分。物联网设备的身份标识是物联网设备安全通信必不可少的前提。当前，物联网设备认证存在着如下问题：

- 大量物联网设备的存储、计算以及通信资源受限；
- 物联网设备数量规模带来的可扩展性问题；
- 边缘节点管理大量物联网设备时面临风险。

基于区块链 DID 认证体系的物联网系统遵从端-边-云架构，利用区块链作为数据的可信存证，形成 DPKI 体系，更好地满足物联网系统可扩展性的要求；同时，考虑到设备的资源限制，对于无法负担 DID 相关运算与存储要求的物联网设备，利用边缘节点辅助，协同完成 DID 生成、认证、授权以及访问服务等操作；针对边缘节点管理大量物联网设备的风险，利用 PUF 模块实现轻量级的快速认证，PUF 模块的引入也使得设备无需存储额外数据即可复现大量密钥。

使用 DID 可以最大化降低不同中心化认证系统的互联互通成本，优化用户认证流程，方便政府、机构管理，帮助用户快速且安全的实现身份认证。

3.2 落地案例

3.2.1 无感停车

3.2.1.1 背景

网络安全问题。在交通的建设中，安全从来都是首要问题，而新的智慧交通

体系架构中的安全架构更是重中之重。随着当前技术的快速发展，在新型智慧城市（如雄安新区）的交通建设中，必然需要考虑大量的自动化人工智能系统，而在这些包含众多电脑、网络、处理器组成的互联汽车互联交通系统，一旦受到网络攻击、被黑客操控，将不仅仅危害人民财产安全，更可能危害人民生命安全。

中国城市化进程飞速发展，而当前城市基础设施的建设滞后于城市化发展水平，在城市交通中出现了交通拥堵、停车困难等问题。其中，停车难、停车乱、停车贵正日益成为困扰着中国各个城市发展的重要问题，深深折射出城市管理之痛。面对老百姓停车难的问题，虽然相关部门已迅速响应、整改，但停车位发展不足、停车位利用率低事故率高仍然大量存在。近年来，随着电动汽车保有量的增长，充电设施不足和被普通车辆占用造成利用效率低下问题逐渐严重。如何通过使用信息、通信和控制技术，使停车、充电更加高效、便捷和安全是城市建设和管理中面临的重要问题。

3.2.2.2 方案

CPCChain 与知名国际汽车厂商合作，结合物联网与区块链技术，融合最新的分布式身份认证技术，创新性的提出并实现了基于分布式身份的无感停车及充电系统，解决了充电车位被普通车辆占用问题，提高了充电车位利用效率，提供即插即充、即用即走的无感支付功能，极大提高用户体验。

车辆搭载嵌入式区块链设备，可上传去隐私的车辆行驶数据到节点网络，从而获得物质财富或社会价值奖励。

当车辆达到目标车位，车内嵌入式设备与车位上的智能地锁进行蓝牙通讯，并基于付费服务器确认身份。车上设备基于区块链的智能合约自动完成押金支付，地锁确认押金后自动下降，开放车位给车辆。基于超声波传感器确认停车到位，从而开始付费计时。

当车辆离开车位，地锁基于超声波传感器确认车辆离开。付费服务器基于停车场付费规则，向区块链智能合约发起完成费用结算。结合一次性设置的小额免密支付功能，停车付费自动完成，对于已具备基于车牌识别计费的停车场，智能地锁用于充电停车位的控制，保证充电设施的利用效率。

整个过程不需要人的介入，实现无感、实时和安全的支付，不仅完成数据价值的利用，同时实现了终端快速自动交易。

不同于一般的非接触身份认证技术，车辆与车位以及充电桩的身份认证基于

DID(Decentralized Identification)技术实现。基于区块链底层的 DID 系统，默认匿名，在技术角度上具有唯一性且不可伪造性，用户可完全掌控自己的匿名身份，用户数据可以有选择的加密保存在区块链上，只有用户自己和用户授权的 DID 可以访问证明的数据，而外界只看到 DID 对需验证信息的签名即可，避免用户数据泄露。将汽车与个人 DID 绑定，当车位以及充电桩需要认证时，用户可以向访问的系统提供有限个人的信息，避免用户暴露自己大量隐私数据。

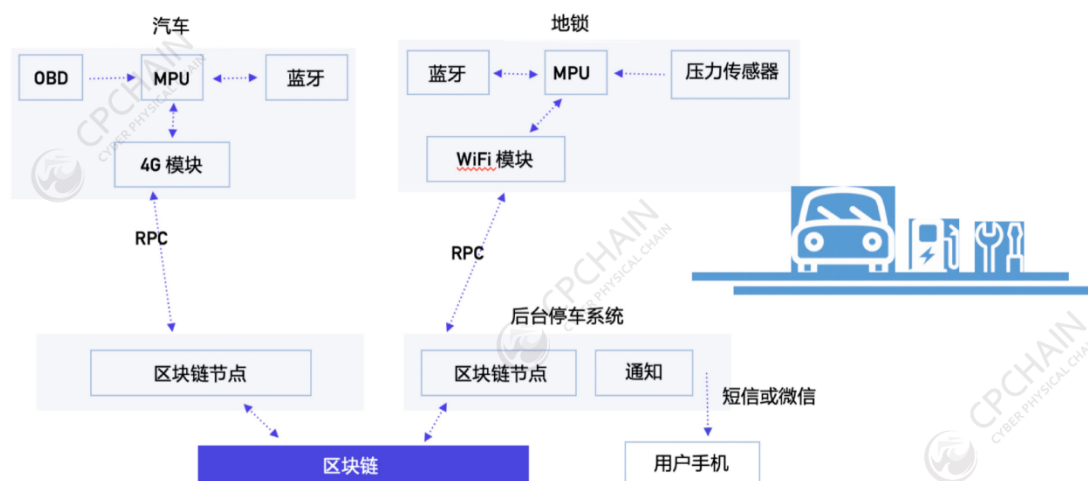


图 12. CPChain 无感停车方案

3.2.2 共享充电

3.2.2.1 背景

当前阻碍电动车推广普及的一大门槛是电动汽车充电难。

对于普通电动汽车用户而言：电动汽车用户面临着充电基础设施缺失的问题，市面上存在着众多充电平台，这些平台互不相通，电动用户每遇到一个新的平台，都需要重新注册，且注册流程繁琐。此外，充电桩市场透明性低，难以保证用户的合法权益。

对于运营商而言：共享充电行业竞争激烈，整个行业内部相互独立、彼此排斥，造成整个共享充电市场高度碎片化。此外，不同电动汽车厂商的充电设备设置各不相同，致使充电这一行为复杂化，最终影响到用户的使用体验。

3.2.2.2 方案

通过电动汽车和充电桩上的智能通信运算设备，实现以下功能：

- 验证：汽车自动连接充电桩并验证车主身份
- 即插即用：车主插上充电枪即可开始充电
- 交易：自动结算，交易安全透明

CPChain 已与知名国际汽车厂商达成合作，成为其供应商。在某车型试装了 CPChain 独立研发的具备区块链支持的 DID 功能的智能物联网设备。能够点对点的与充电桩进行通信和车辆身份信息验证。对于一次性在系统中注册的车辆，用户无需进行刷充电卡、扫二维码等操作，只需插上充电头，当充电桩内物联网设备感应到后，控制充电桩立即开始充电并开始计费等操作。充电结束之后，用户仅需拔下充电头，充电桩内部的物联网设备将立即开始结算以及小额免密支付操作，将费用信息发送至用户指定推送渠道，用户无感充电过程完成。

该解决方案得到了合作企业的充分认可，一定规模的场景化验证应用正在进一步深入中，双方将围绕交通出行领域制定区块链技术方案，推动区块链加速落地，赋能智慧出行。该解决方案还作为代表上海的五十五项科技成果之一，参加了首届“长三角一体化创新成果展”，获得一致好评。



图 13. CPChain 共享充电实景

3.2.3 药品溯源(Drugledger)

3.2.3.1 背景

中国政府自 2008 年即开始在全国推广的中国药品电子监管码制度，要求涉药企业在生产、销售、分发的过程中，将其药品具体信息进行网络登记。

美国国会于 2013 年 11 月通过了《药品供应链安全法案》，要求涉药企业，在美国境内分发的所有处方药都必须可被唯一标识和追溯。

欧盟与 2011 年通过了“假药令”，该指令对欧盟境内的利益相关者在欧盟境内药品分发和销售提出了具体技术要求，包括药品序列化，防伪技术使用，流向记录等。

传统药品的供应链追溯系统中存在着以下的问题：

- 利益相关者的商业隐私难以得到有效保护
- 数据的真实性和稳定性无法得到有效保障
- 供应链节点之间协作较为困难
- 与自身已有的 ERP 管理系统兼容问题
- 系统安全性较差，容易受到 DoS 攻击

3.2.3.2 方案

为了解决以上问题，我们建立了基于 CPChain 技术的药品溯源系统 (Drugledger)，由证书服务模块、查询服务模块、防攻击服务模块等组成。

证书服务模块(CSM)

内嵌的公钥基础设施，提供系统成员的动态管理服务（例如要求用户持有合法的证书方能进入区块链网络），起到系统监管者的作用

查询服务模块(QSM)

给利益相关者和患者提供完整的药品流追溯服务

防攻击服务模块(ASM)

检测系统中的异常活动，从而保证系统正常运行

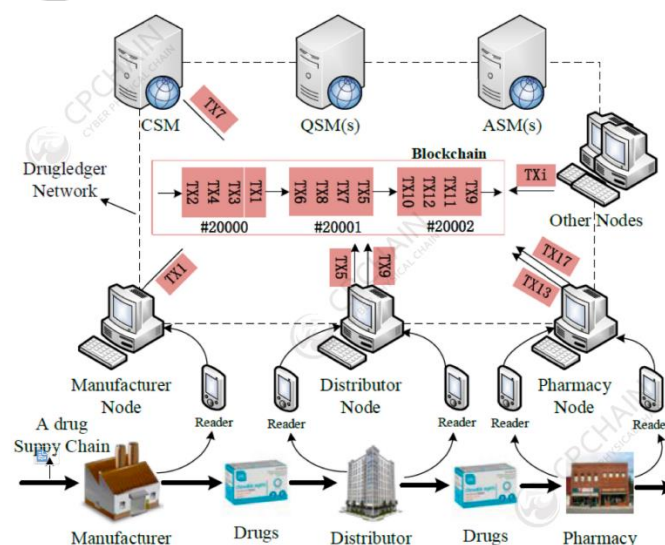


图 14. CPChain 药品溯源方案

3.2.3.3 实现

CPChain 在 PC 端为供应商、医疗机构提供了可供监控的后台页面，可以看到药品的实时流转状态。在手机端，CPChain 为供应商、医院提供了可直接操作的入库、出库、拆包、打包的功能，方便操作员操作。同时为消费者提供了可供查询药品流转信息的 APP，从而确认药品的真实性。

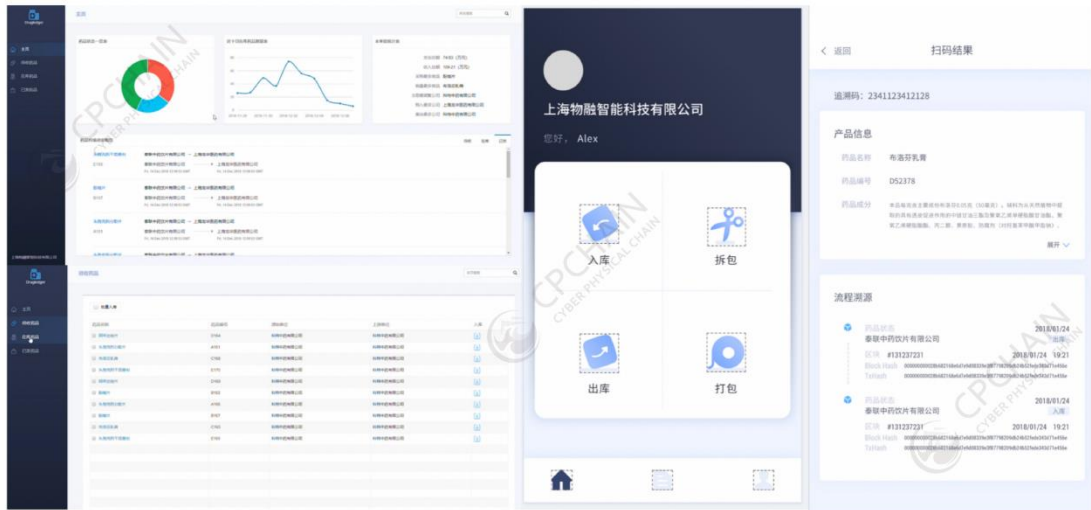


图 15. CPChain Drugledger 客户端

3.2.4 驾培链

3.2.4.1 背景

当前驾驶培训市场中，已有多款成熟的物联网设备和技术，比如通过人脸、指纹识别技术对学员身份进行识别，通过 GPS 导航来实现对驾驶轨迹和时间的记录，通过车载网关提供通讯功能，并记录音频和视频等信息，从而证明学员的学时真实性。同样，在驾驶考试系统中，目前主要通过传统的传感器检测方式和新一代的多卫星定位点检测这两种方法来监测学员考试过程。但仍有一些问题亟待解决：

- 为保证培训效果和安全，要求驾驶员培训中，参加考试之前的练习时间达到 40 小时，但学时造假情况严重；
- 现有系统配备指纹识别等人员认证手段，但培训过程中的作弊行为难以监控；
- 驾培数据存在篡改可能性，真实性没有得到保障；

-
- 缺少个性化的驾驶行为分析以及培训后的持续跟踪。

3.2.4.2 方案

在驾驶培训学时认证应用中，针对现有驾培系统中，学时造假严重，数据分散且各监管部门互不信任的问题，CPChain 联合国家安全驾驶工程技术研究中心，提出了一套驾驶培训学时保障系统。

在这套系统中，通过双方联合开发的车载物联网设备，对驾驶培训学员以及教练身份进行认证，并在培训时间段内进行抓拍，保证学员一直在车内培训。在培训过程中，通过培训过程中车载 OBD 设备获取驾驶时间、行程、学员的刹车、踩油门数据，发动机转数数据，驾驶过程中随机拍摄到学员照片等信息。在驾驶培训结束后，将以上驾驶培训过程信息通过区块链存储，在物联网终端设备直接上链，通过比对哈希值可以检验数据是否被篡改，以保证学员训练效果。当数据出现篡改时，系统会快速的找出篡改的数据，并显示正确的数据，方便监管学员驾培。同时，参与驾培的各监管部门拥有区块链节点，能够很好建立信任。

该系统还具备自动数据比对功能，对驾驶培训任何环节的数据修改能够自动识别。在这个应用中，驾驶培训的学时得到有效保障，参与方的信任得到有效维护，对提高驾驶培训效果，保障学员上路后的安全驾驶起到良好的促进作用。

3.2.4.3 实现

CPChain 与安徽三联交通应用技术股份有限公司，率先落地驾培链的应用。对于驾培系统的记录实时上链，并且每天批量比较历史数据和链上数据，对于数据不一致的情况及时预警，防止驾校对用户的学时进行造假。该解决方案获得第三届“中国创新挑战赛暨首届长三角国际创新挑战赛区块链专场赛”卓越生态创新奖。在该解决方案基础上，CPChain 和国家安全驾驶技术工程技术研究中心、上海交通大学分布式智能实验室正进行深入合作，在驾驶模拟、驾驶培训、网约车安全主动监控等方面，深度融合物联网技术、区块链技术、基于边缘计算的人工智能技术，深入合作。在后续的规划中，还将实现：基于区块链的驾培过程驾驶行为记录，进行大数据分析，给出安全驾驶建议。通过手环设备，加入学员体征监测和记录。基于对外摄像头图像分析的危險情况提醒，基于对内摄像头图像 AI 分析车内人员安全状况。

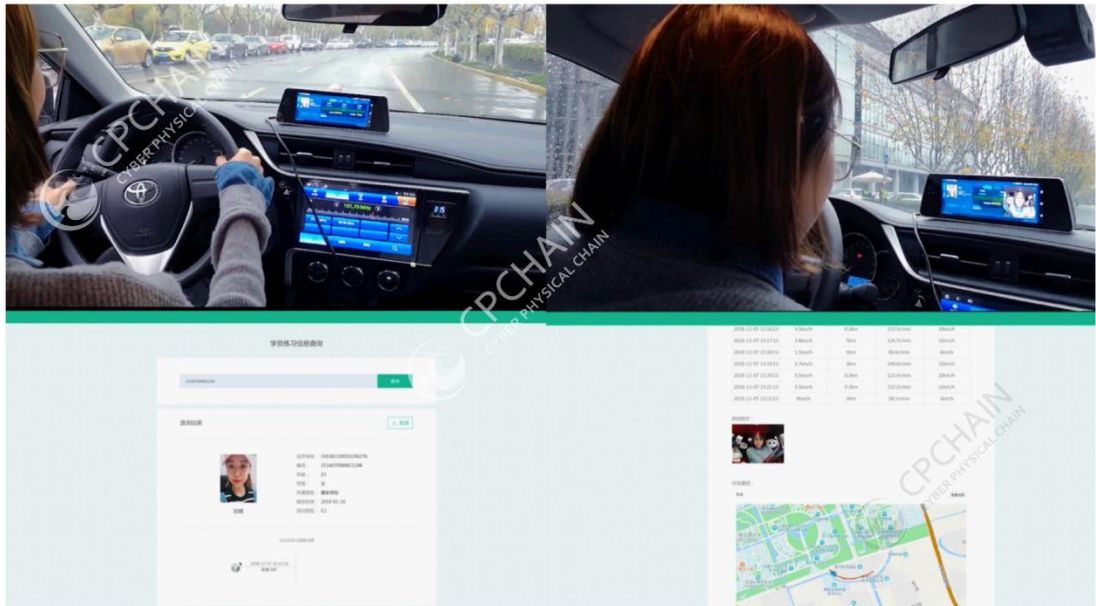


图 16. CPChain 驾培测试实景

3.3 DApp 开发

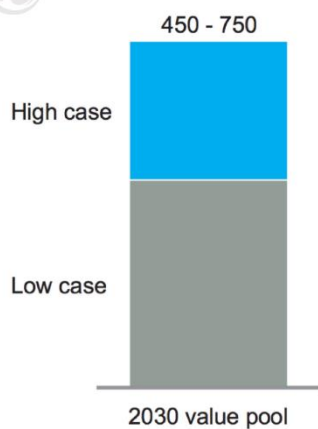
3.3.1 PDash 数据共享

3.3.1.1 背景

以汽车市场为例，汽车数据市场潜力巨大。据相关机构分析预测，将在 2030 年产生高达 4500-7500 亿美元的市场规模

Car-generated data may become a USD 450 - 750 billion market by 2030

Overall value pool (including additional revenue, savings, and societal benefits)
USD billions



Breakdown of value pool by value creation lever
Percent

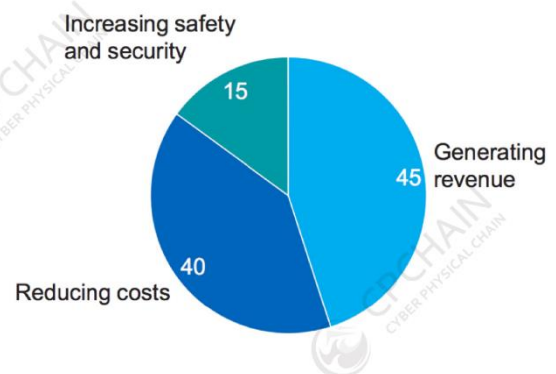


图 17. 汽车数据市场预测

3.3.1.2 方案

PDash 是一个围绕数据交易场景，消除数据提供者与消费者之间的信息差距，公正、透明、高效的数据交易平台。由以下几个重要模块组成：

- **钱包：**可为广大用户提供交易账户。
- **开放商城：**为数据提供者与数据需求者提供的交易平台。
- **分布式代理网络：**保护数据的安全与隐私性。
- **CPChain 底层公链：**连接所有数据共享参与者。

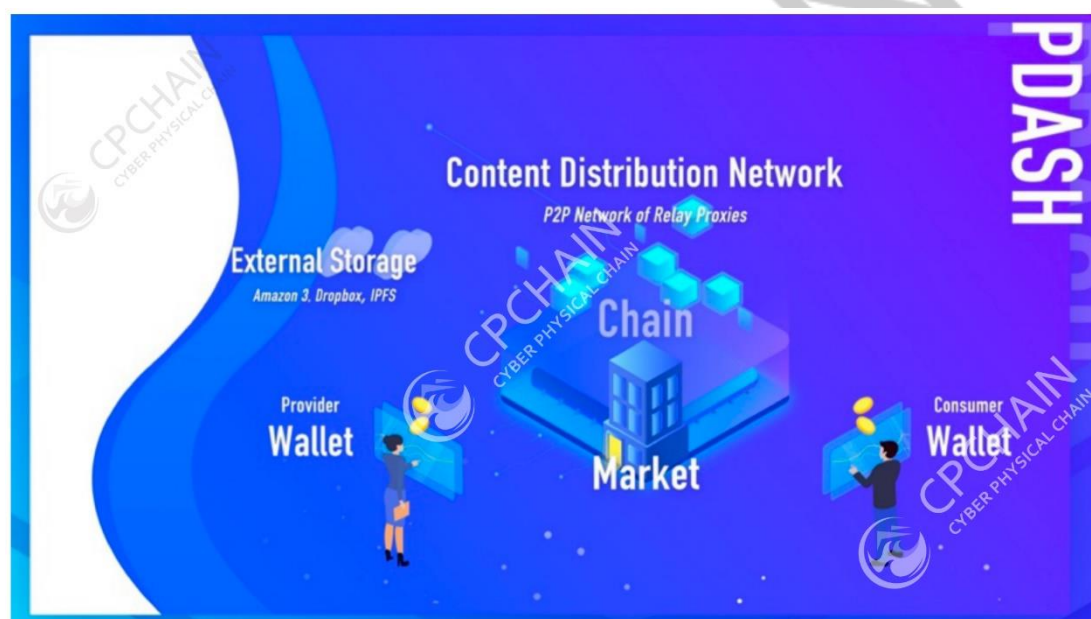


图 18. PDash 数据共享平台架构

3.3.1.3 实现

目前，PDash 已经实现了商城中的数据买卖，包括物联网的静态数据和流式数据，正在不断的吸引商家入驻并收集数据来源。（PDash 开源地址：<https://github.com/CPChain/pdash>）

4. 经济模型及系统用途

CPC 是 CPChain 上的原生资产，CPC 的价值起源是其能够方便地表征和度量 CPChain 上数字化经济活动。CPC 的价值基于两点：一是使用 CPChain 上的应用需要消耗一定量的 CPC 作为燃料；二是持有 CPC，能够参与到 CPChain 社区治理中。

1) CPC 通证总量为 10 亿，主网上线时一次性生成。

2) CPC 网络的普通节点（非 DApp 应用节点），拥有固定额度的数据存储和数据交易的权利，超过规定存储容量和交易数量，或者发送频率过快，用户将通过支付 CPC 获得额外的存储与计算资源。

3) 为保证网络和计算资源的均衡，DApp 应用开发商根据该应用将要占据的资源，必须持有相应数量的通证，若持有通证数量不足，可租赁。

4) DApp 应用产生的交易，DApp 开发者承担交易费用，并向提供租赁通证的服务提供商缴纳租赁费。

CPChain 基金会向各个智能合约的开发及服务提供商收取 CPC，支付智能合约运行所需要的 GAS 来保障各个商业智能合约的运行；所收取的 CPC 收入的大部分将作为节点奖励，支付给节点提供商，而剩余的部分用于基金会后续的日常运行、商业推广和技术开发。应用开发提供商根据最终客户企业的需求，在所获得智能合约服务的基础上进行进一步开发和加工，为其企业客户或者最终用户提供应用产品，收取 CPC 作为企业收入，最终用户可以支付 CPC 来获取企业产品和服务。

5. 社区治理

5.1 RNode 荣誉节点生态

5.1.1 节点类型

RNode 荣誉节点生态描述了包括矿工在内所有节点的权利、责任与义务。节点根据其在两种不同的奖金池中的押金和余额分为以下三类：

经济节点：在经济池中持有不低于 2 万 CPC 即可成为经济节点，在社区内享有投票权。

荣誉节点：在荣誉池中要求持有不低于 20 万 CPC，同时满足基本算力和存储要求，能够支持 CPChain Open Transmission Protocol (COTP).

行业节点：物联网行业合作伙伴，以及 CPChain 生态中的开发者可申请成为行业节点。

这里我们提到了两种不同的奖金池，分别是经济池与荣誉池

经济池：在该池中质押超过 2 万 CPC 就可以成为经济节点。经济池中的押金需要至少锁仓 90 天，且只有固定时间可以取出。

荣誉池：在该池中质押 20 万 CPC 即成为 RNode 荣誉节点。荣誉池中的押金会被锁仓 100 分钟，如果一个节点确定将会出块，将不能取出押金直至出块成功。

5.1.2 荣誉度评估 (RPT)

DPoR 使用从区块链中提取的数据，构建节点的信誉度评估模型，进而计算和评估系统中节点的信誉度值。评估模型有五部分：账户余额、交易、代理人信誉奖励、数据贡献、以及区块链维护。

账户余额 (AB)：节点账户中的 CPC 余额与节点信誉度的评估正相关，占总权重的 50%；

交易 (TX)：这里的“交易”定义为在系统中所有的交易，占总权重的 15%；

代理人信誉奖励 (PR)：节点在网络中作为代理 (proxy) 协助其他节点完成交易，会获得信誉度奖励，占总权重的 10%；

数据贡献 (DC)：节点在网络上传数据的行为会得到信誉度奖励，分为基础信誉度奖励和附加信誉度奖励。节点上传文件时，获得基础奖励；若这些文件产

生交易，则获得附加奖励。数据贡献奖励占总权重的 15%；

区块链维护 (BM)：每一轮区块添加成功后，每个委员会成员会得到相应的信誉度奖励，占总权重的 10%。

RPT 计算公式为： $RPT=50*AB+15*TX+10*PR+15*DC+10*BM$ 。

5.1.3 节点奖励

CPChain 生态的构建需要大量的物联网企业、开发团队和用户参与，不是一蹴而就的过程。因此，CPChain 分为两个阶段来规划生态激励与运营计划。第一阶段由 CPC 激励主导，主要通过 CPChain 基金会持有的运营基金来构建生态和运营维护区块链；第二阶段由市场交易主导，随着 CPChain 生态系统建设的完善和数据共享交易量的增加，荣誉节点的奖励主要来自智能合约和交易转账的费用。

CPC 激励主导阶段，节点的通证奖励包括基础奖励与出块奖励：

基础奖励：预计每年发放 500 万个 CPC 注入奖金池（每季度约 125 万个 CPC，每日约 1.37 万个 CPC），经济节点根据锁定的保证金占总保证金的比例获得对应的 CPC 奖励。

出块奖励：入选委员会的荣誉节点可获得额外区块奖励，每个区块中的 CPC 奖励数额固定，每经过 1 年（约出块 300 万个），区块奖励减少 1/4，预计约 5 年时间发放完。第一年发放约 4000 万个 CPC，第二年约 3000 万个 CPC，第三年约 2250 万个 CPC，第四年约 1700 万个 CPC，第五年约 1275 万个 CPC。

经济节点每一轮会有 90 天，具体流程如下：

每一期的长度为 90 天，其中包括最开始 3 天为募集期，中间 84 天锁定期，以及最后 3 天结算期。每一期之间没有重叠，第一期结束之后，才能开启第二期。每一期中，不同阶段没有重叠，合约始终处于确定的某个阶段，募集期，锁定期或结算期。其中募集期可以在经济池中押入通证，或者取走通证。在锁定期期间不能进行任何操作。在结算期可以主动取走利息。如果用户没有主动取走，将有管理员逐一分派。



图 19. 经济节点锁仓流程图

5.2 理事会

理事会是 CPChain 治理的核心机构，引导 CPChain 走向科学治理，同时保证效率的提升。CPChain 理事会将邀请国内外知名机构、企业、个人共同参与，集合国内外优势力量来打造 CPChain 全球化的公链社区生态，充分利用区块链、物联网创新为不同应用领域提供高效的去中心化服务，逐步吸引不同领域，及不同产业链上下游企业、用户等加入 CPChain。同时，CPChain 理事会还将承担起不断挖掘物信链创新业务，积极建立更多行业联系，为打造全球化的区块链与物联网融合发展生态体系的重任。

5.2.1 人员组成

第一届理事会成员由三部分组成，将分别由基金会提名，邀请，或通过社区选举产生。

5.2.2 权利义务

接受 CPChain 社区委托，参与制定 CPChain 战略方向和执行重大决定，推进科学治理，监督社区公共财产安全。CPChain 理事会每年将向社区披露 CPChain 的开发情况、运营情况、CPC 的使用情况等，并将引入第三方审计机构，监督项目的财务运作，审计报告将在年度信息披露中公告。

5.2.3 任期

理事会理事任期时长为 1 年，每年选举一次。

5.2.4 选举方法

除 CPChain 基金会提名和邀请的理事之外，只要拥有超过 200K CPC 账户地址的社区成员，均有被选举权，只需提交相关材料资质，即可参与每年一度的理事会选举，选举期及任期内不得出售 CPC。

5.2.5 收益

理事会每一任期总收入为 400,000 CPC，每一任期分两次分发理事会收益，每半年分发一次。

5.3 委员会

CPChain 理事会下设委员会，理事会广泛收集各方在技术研发、社区治理、生态建设等方面的意见，形成相关草案，分发给技术和生态两个委员会。

技术委员会存在的意义在于更好的利用社区资源，真正使得技术开发以多方协作方式完成。技术委员会受理理事会委托，负责整个公链技术升和迭代，确保技术适合生态的发展，生态委员会负责整个公链生态布局，包括 CPChain 上开发者的项目的投资、孵化、商业落地，交易所，节点和治理。为构建 CPChain 生态筛选合作伙伴，进行尽职调查并负责后续合作对接工作。技术委员会和生态委员会成员由 5 到 9 位构成。

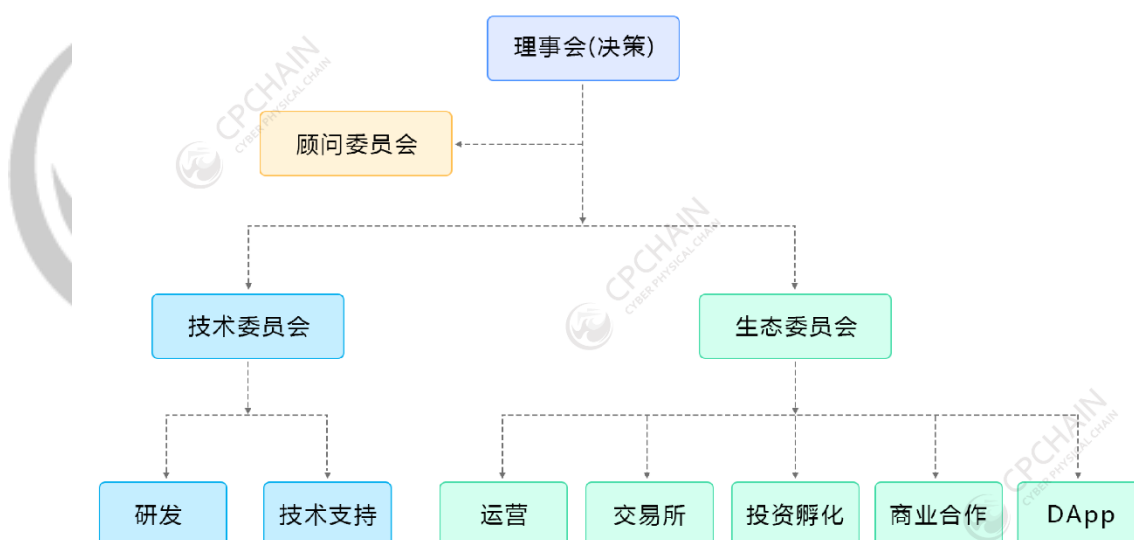


图 20. CPChain 治理架构

5.4 物信链基金会

5.4.1 人员组成

CPChain 基金会理事不少于 5 席。包括基金会主席 1 席，秘书长 1 席。旨在通过科学、合理、有效的治理机制推动并维系基金会及 CPChain 生态的建设和健康发展。

5.4.2 权利

1. 基金会内部席位的选举权和被选举权；
2. 参与基金会整体发展和生态投资等的决策。

5.4.3 义务

负责托管基金会所属资产，制定合理的资金使用提案，以维系 CPChain 技术开发、生态布局、商务拓展等业务的正常拓展。

在 CPChain 进行技术开发和生态发展等方面时提供持续强有力保障和丰富的资源。

5.4.4 任期

基金会理事任期为 1 年，可连任。

5.4.5 入选方法

基金会主席

基金会主席在基金会内部匿名推选而得。每位理事具有基金会主席被选举权和选举权。

基金会主席支持率需要过半。如果无人支持率过半，则末位淘汰后重新投票，直至符合投票规则推选出基金会主席。

罢免

当基金会成员出现渎职、危害基金会健康发展等情况时，基金会可视具体情况发起基金会内部决议罢免任意一名基金会常务理事，但结果必须向社区公示。

被罢免的基金会常务理事有权向社区公开述职，并有一次机会发起链上社区公开投票请求恢复职务。

6. 发展路线图



7. 财务

7.1 通证分配计划

CPChain 的通证发行总量为 10 亿，其中 40%用于海外社区和机构募资。

比例	分配方案	明细
40%	海外社区和机构投资	海外社区会是 CPChain 未来的发展的重要力量，此部分将用于海外社区的建设；机构投资人指在构建的物信链生态系统中的企业及为物信链早期筹备做出贡献；这些投资人会把未来 CPChain 通证(CPC)在其商业活动中的使用作为重点开拓目标。
20%	创始团队、开发团队和顾问	创始团队、以及开发团队在项目的发展过程中做出了人力、技术、资源以及物力的贡献，因此以发放 CPChain 通证(CPC)作为回报，这部分锁定期为 4 年，每年分批释放。
40%	社区治理	维持团队的持续经营和发展；商业落地推广筛选合适的行业，进行行业中的战略部署、项目扶持和通证置换，用于技术的行业应用，真正实现商业落地。

7.2 资金使用计划

日常运营	35%	包括初始团队的薪资、招募专家及开发人员、技术专利及知识产权保护，运营基金会及市场开支等
技术开发	35%	技术研发、技术与交流与分享、定期刊物发表、联盟创建或参与，社区激励等
商业拓展	20%	维持基金会扩张运营及落地的一系列商务渠道合作等
生态投资	10%	对区块链新技术和新团队的投资

8. 合作生态



北方工业大学汽车产业创新研究中心

北京师范大学认知神经科学与学习国家重点实验室脑调控认知与增强研究中心

北京邮电大学信息安全中心

9. 免责声明

- 本文档只用于传达信息之用途，文档内容仅供参考，不构成买卖 CPChain 通证相关意见。本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不构成招股说明书、要约档、证券要约、招揽投资或出售任何产品、物品或资产（不论数字或其他方式）的任何要约。本白皮书中所包含的任何内容，都不能作为对 CPChain 未来表现的代表和承诺。
- 本文档中已明确表示相关意向用户明确了解 CPChain 项目的风险，投资者一旦参与即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。CPChain 明确表示不承担任何参与 CPChain 项目造成的直接或间接损失。
- CPChain 通证并未计划在任何国家或司法管辖区构成证券或其他应受管制的产品。本白皮书非募集说明书或其他任何证券发行文件的基础，也不拟作为在任何国家或司法管辖区发行或募资证券或其他任何应受管制的产品。本白皮书并未被任何国家或司法管辖区的任一监管机构审核。
- 使用及购买由 CPChain 发售的通证，需承担高度的财务风险。CPChain 对于 CPC 在市场上的流通及交易声明免责。通证通常在交易市场上具有剧烈波动的价格区间。价格在短时间内剧烈震荡的情形经常发生。这些波动可能源于市场动能（投机活动）、法规变动、技术创新、交易可能性及其他客观因素。CPChain 并未提供投资、财务、法律意见及独立之事实验证，因为用户操作带来的经济损失；由个人理解产生的任何错误、疏忽或者不准确信息；个人交易各类区块链资产带来的损失及由此导致的任何行为均与 CPChain 无关。
- CPC 作为 CPChain 的官方通证，是平台发生效能的重要工具，并不是一种投资品，也不是一种所有权或控制权。控制 CPC 币并不代表对 CPChain 或 CPChain 应用的所有权，CPC 币并不授予任何个人任何参与、控制，或任何关于 CPChain 及 CPChain 应用决策的权利。
- 若 CPC 或 CPChain 区块链系统遭受网络攻击或通过 CPChain 提供之服务/平台存储或传输的信息可能因电脑软件故障，第三方服务厂商的协议更改、网络故障及其他不可抗力事件等，CPChain 通证可能受到不利影响。CPChain 及其关系企业，不保证能够预见、防护、减少该类攻击或对该类攻击采取适

当措施。

- 本文档无任何声明或保证确保其中所描述或传达与本计划有关的信息、陈述、意见或其他事项为正确或完整，也未对任何具前瞻性或概念性陈述的成果或合理性作出任何声明或保证，且无声明与保证之事项不限于前述事项。本文档中任一处皆不应构成或被视为对未来所作之任何承诺或声明。在适用法律充分允许的范围内，任何人按照本白皮书行动而因此产生或相关的任何损失或损害（无论是否可预见）时，不论是否系属疏忽、默认或注意不足，CPChain不会对该类损失或损害赔偿或负任何责任。



CPCHAIN
CYBER PHYSICAL CHAIN