# AMChain 白皮书

让增材制造更有智慧

V1.0.0

安世数擎（杭州）信息科技服务有限公司

2021 年 01 月

目录

# 一、AMChain 的诞生

在云计算和工业 4.0 时代，近年来我们见证了有关云制造的大量研究工作。尽管如此，诸如信任，安全，支付等问题仍然存在于这个新兴领域，这给业界采用云制造带来了更少的信心。在这方面，由于其在去中心化和安全性方面的独特优势，最近区块链技术的发展提供了潜在的可行解决方案。因此，我们通过整合区块链技术提出了一种新的云制造框架。这个框架底层便是 AMChain（Additive Manufacturing Chain）。

# 二、基于区块链的云制造（BBCM）

## 区块链技术

区块链技术通常被认为是一种处理和存储共识的分布式数据固化技术。区块链是一个数据库，也称为“分布式分类帐本”。区块链提供了谁在任何给定时间拥有财产的证据，并且可以公开获得。本质上，区块链技术是一种信任机制，由分布式技术和共识机制构成。区块链的开放属性允许所有相关人员验证交易记录的准确性。这种机制可以防止恶意的失真信息。区块链的典型应用是虚拟货币系统，其中比特币和以太坊是最受欢迎的虚拟货币。最近，涌现了大量基于区块链的应用程序。其充要条件是：

- 去中心化的分布式系统
- 对等的处理和存储共识
- 前向依赖的数据结构

解释：处理和存储共识，是区块链与既往计算技术最大不同，也是最核心特征。去中心化杜绝了特权节点对系统和数据进行倾向性干预，节点地位对等是区块链系统的重要准则。“共识”是基于特定规则和算法的公共结果（区别于传统分布式系统中的带有预设、倾向或强制性的“一致”），不受特定节点的强制约束。前向依赖是通过特定数据结构，以数学和密码学手段保证数据满足可回溯和完整性特征。结合以上三大特性，保证了“共识”可以被产生、固化并不可撤销的存储。

不能同时满足以上三大特征的区块链技术，其特性是不完整的。如：缺少完全去中心化特性，则退化为传统的分布式存储系统；缺少前向依赖的数据结构，则是传统的 P2P 对等网络；缺少共识机制，则退化为一个容错分布式系统。

# 基于区块链的云制造框架

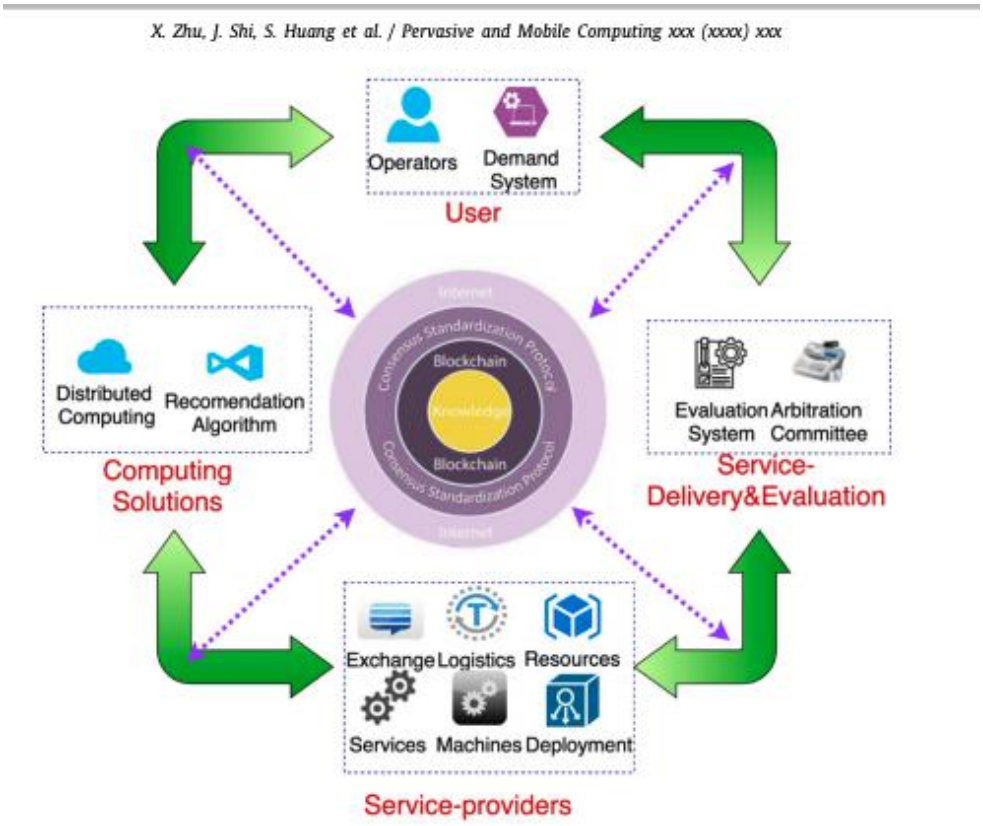


**Fig. 1.** Operation model of the proposed blockchain based cloud manufacturing system.

基于区块链的云制造的框架提议的基于区块链的云制造的系统通过将区块链技术与现有的云制造概念相结合，反映了面向共识制造的新模型。采用虚拟货币，智能合约，共识算法和 HASH256 加密技术等与区块链相关的技术来实现自动共识驱动的服务。这些服务使全球公司和组织能够拥有各种安全可靠，可信，高质量，廉价，易于支付和按需制造资源。图 1 显示了所提出的系统由四个组件组成，即用户，解决方案计算，服务提供商和交付。在中心，区块链的四个核心平台，知识，共识标准化协议，并使用互联网来保证系统的安全性和可行性。绿色箭头表示四个组件之间的交互，通讯和/或产品传输。虚线箭头显示了来自四个中心平台的支持，包括标准化支持，知识支持，网络支持以及区块链的安全性和数据支持。

**Table 1**
Comparison of traditional and blockchain based cloud manufacturing systems.

| | Traditional | Blockchain-based |
|---|---|---|
| Data storage | Internet-based traditional service | Blockchain, Oracle |
| System oriented | Service oriented | Consensus oriented |
| Payment | E-payment, Traditional payment | Uniform cryptocurrency |
| Security mechanism | Setting up security mechanism by each node itself or providing security service by the security firms [8,30] | Blockchain mechanism guarantees payment safety, and transaction safety. Oracle mechanism protects data from being stolen and juggled, |
| Trust | Identity check; authorization; isolation; access control; certificate-based authentication; user trust management; data and information flow tracing [31] | System mechanism provides trust. No independent trust is necessary. |
| Standard | No universal standards. Open communication standards proposed for research [11,32] | Consensus based global standard |
| Barriers for users | No barriers for all type of users | All providers and miners need to be pre-approved by smart contract vote. |
| Administrative tribunal | Offline local governments | Blockchain consensus mechanism-based arbitration committee |

表中列出了传统云制造和基于区块链的云制造概念之间的区别。可以看出，区块链技术实现了下一代云制造概念。通过克服现有云制造系统面临的关键挑战。拟议的 BBCM 系统采用区块链技术解决云制造的长期问题，并增强云制造能力。具有以下几个关键特征

- **没有第三方的信任**

  区块链的分散机制允许每个对等节点拥有不可更改且防篡改的完整数据。结果，用户之间的交互是可信且可追溯的。

- **开放可靠**

  以比特币和以太坊为例，两个最受欢迎和成功的区块链系统已经在全球范围内成功地在开源代码模型上运行。区块链的开放和可靠属性是 BBCM 系统吸引更多用户参与该系统的重要推动力。

- **共识标准**

  BBCM 系统的共识机制和开放属性使在完全参与的情况下定义标准成为可能。

- **轻松付款**

  密码系统为全球用户提供了一种方便的统一付款方式。而且，统一支付

系统极大地促进了仲裁结果的执行。

- **价值共享**

  BBCM 提供了一个汇总帐户和网格计算奖励机制，使所有参与者不仅可以从他们的业务中受益，而且可以从系统增长中受益。

## 三、系统的层次结构

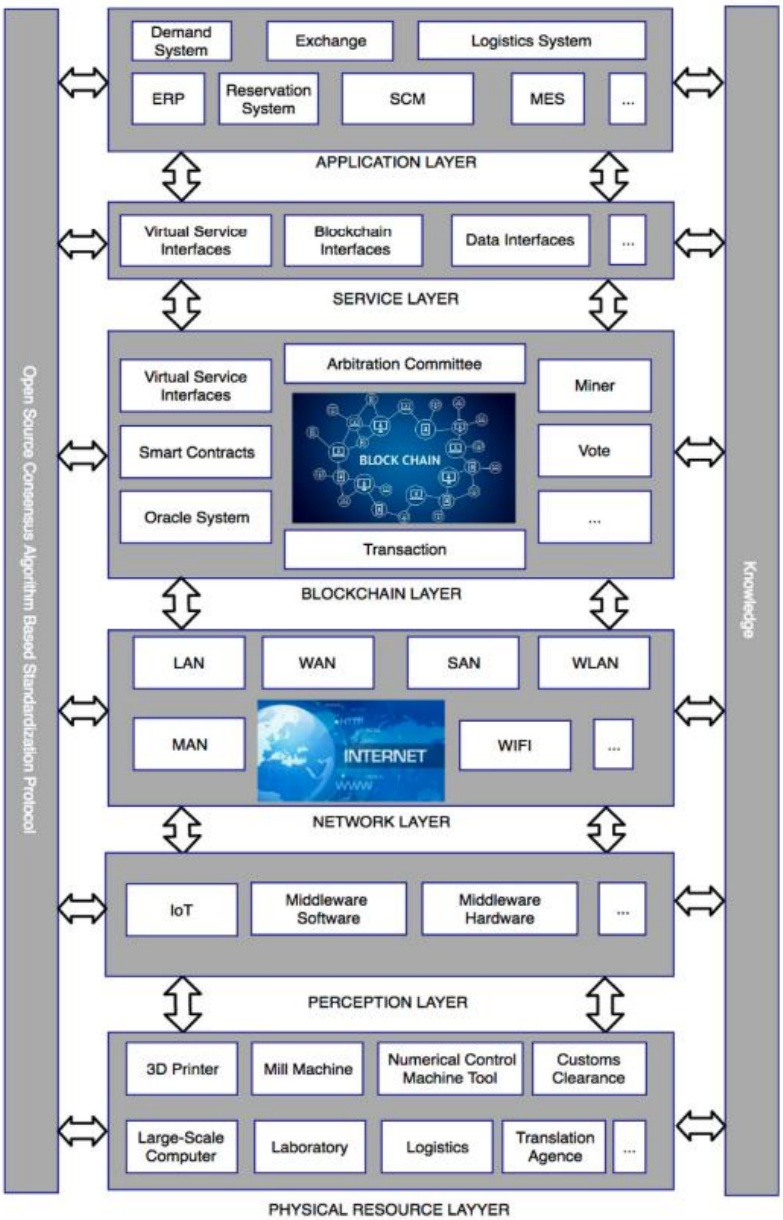


**Fig. 2.** Hierarchical structure of the proposed blockchain-based cloud manufacturing system.

如图 2 所示，基于 AMChain 提出的系统建立在具有六层的层次结构上，即物理资源层，感知层，网络层，区块链层，服务层和应用层。物理资源层包括用于完成最终用户工作的机器，资源和服务。感知层用于实现标准化工作，这使机器和服务能够为云用户服务。所有标准都遵循共识算法。该层的元素可以是 IoT 硬件或中间件软件。网络层基于互联网，为区块链提供稳定的网络服务。该层不仅包括传统的网络协议，还包括区块链协议，例如 RTXP 交易协议。区块链层提供交易，信心和云制造系统的安全性。该层包括区块链，智能合约，共识算法，Oracle，交易所等。

在现有云制造系统中，一切都被视为服务，例如基础架构即服务（IaaS），平台即服务（PaaS）和软件即服务（SaaS）。基于区块链技术，拟议的系统使用智能合约来达到开源共识标准。因此，在提出的系统中，所有事情都可以通过共识来实现。所有服务均符合标准，并通过界面设计实现。在建议的系统中可以识别所有接口，因为全局开发人员遵守本质上由他们自己设计的相同规则。服务层为应用程序开发提供了大量标准化接口，分为两类：区块链接口和常规接口。区块链接口包括读写接口，智能合约接口，共识算法接口，网格计算接口，Oracle 接口。常规接口包含虚拟服务接口，数据库接口，虚拟接口，分布式计算接口，IoT 接口和标准化接口。最后，应用层为所有参与者提供人机交互的界面。它包括应用程序和 DAPP。该层的代表性应用是 ERP，交换系统，需求系统，制造执行系统（MES），供应链管理（SCM）和预订系统。常规接口包含虚拟服务接口，数据库接口，虚拟接口，分布式计算接口，IoT 接口和标准化接口。最后，应用层为所有参与者提供人机交互的界面。它包括应用程序和 DAPP。该层的代表性应用是 ERP，交换系统，需求系统，制造执行系统（MES），供应链管理

（SCM）和预订系统。常规接口包含虚拟服务接口，数据库接口，虚拟接口，分布式计算接口，IoT 接口和标准化接口。最后，应用层为所有参与者提供人机交互的界面。它包括应用程序和 DAPP。该层的代表性应用是 ERP，交换系统，需求系统，制造执行系统（MES），供应链管理（SCM）和预订系统。

## 四、区块链的结构


- 存储层：存储系统运行过程中产生的区块链元数据和系统日志。区块链元数据采用 LevelDB 数据库存储，系统日志由文件系统存储。
- 数据层：数据层是区块链的核心，主要处理交易中的各类数据，完成数据的编码、解码，将数据打包成区块，将区块拼接成链式结构，处理区块数据签名并添加时间戳印记，将交易数据构建成 Merkle 树，并计算 Merkle 树根节点的 hash 值等。

- 网络层：主要实现网络节点的连接和通讯，又称点对点技术（P2P）。
- 协议层：提供的供系统各模块相互调用的协议支持，主要有 HTTP、RPC 协议、LES、ETH 协议、Whipser 协议等。
- 共识层：其算法称为共识机制。使用了 PoA（Proof of Authority）共识机制。
- 合约层：使用 Solidity 编程语言开发合约，编译成功后部署到 EVM 上运行执行。
- 应用层：基于以 AMChain 系统开发对应产品/平台，以完整实现基于区块链的增材制造云平台。

# 五、AMChain 共识机制 PoA（Proof of Authority）

## 权威证明 PoA 的特点

- PoA 是依靠预设好的授权节点(signers)，负责产生 block.
- 可以由已授权的 signer 选举(投票超过 50%)加入新的 signer。
- 即使存在恶意 signer, 他最多只能攻击连续块（数量是(SIGNER_COUNT / 2) + 1）中的 1 个,期间可以由其他 signer 投票踢出该恶意 signer。
- 可指定产生 block 的时间。

## PoA 的工作流程

1. 在创世块中指定一组初始授权的 signers，所有地址 保存在创世块 Extra 字段中
2. 启动挖矿后，该组 signers 开始对生成的 block 进行 签名并广播.

3. 签名结果 保存在区块头的 Extra 字段中
4. Extra 中更新当前高度已授权的 所有 signers 的地址 ,因为有新加入或踢出的 signer
5. 每一高度都有一个 signer 处于 IN-TURN 状态，其他 signer 处于 OUT-OF-TURN 状态, IN-TURN 的 signer 签名的 block 会 立即广播 ，OUT-OF-TURN 的 signer 签名的 block 会 延时 一点随机时间后再广播，保证 IN-TURN 的签名 block 有更高的优先级上链
6. 如果需要加入一个新的 signer, signer 通过 API 接口发起一个 proposal, 该 proposal 通过复用区块头 Coinbase( 新 signer 地址 ) 和 Nonce("0xffffffffffffffff") 字段广播给其他节点. 所有已授权的 signers 对该新的 signer 进行"加入"投票，如果赞成票超过 signers 总数的 50%，表示同意加入
7. 如果需要踢出一个旧的 signer，所有已授权的 signers 对该旧的 signer 进行"踢出"投票，如果赞成票超过 signers 总数的 50%，表示同意踢出