第23讲 | 联盟链和它的困境

2018-05-16 陈浩

深入浅出区块链

进入课程 >

讲述：黄洲君

时长 13:49　大小 6.33M

不知不觉我已经写到了深入区块链技术部分的最后一篇，今天我们就一起来聊聊联盟链。

其实，在 2016 年的时侯，联盟链是非常火热的，当时的公链还处于探索阶段，以太坊也不够成熟，这给了很多联盟链涌现的机会。所以说，□从技术上来看，联盟链其实非常强劲，毫不逊色于著名的区块链项目，下面我们就一起来看看联盟链技术。

简介

联盟链源自于 Vitalik 对区块链的概念分类，是他第一次提出了联盟链的说法，联盟链的英文是 Consortium Blockchain。

我们回顾一下联盟链。所谓联盟链，就是这个区块链具有准入许可，不像公链，任何人都可以随时进入，准入许可意味着候选节点进入区块链时需要得到已经在网络中的节点的许可。

所以联盟链也叫做许可链，也就是 Permisson Chain，这个叫法在国外比较常见。联盟链的节点数通常不多，维护成本相比公链要低。

有关联盟链与公链的概念区别，它们的区别仅仅是看新加入的节点是否要经过全网中其他节点的许可，这决定了一个区块链是否开放，开放程度决定了项目生态的大小，这也是最直观的区别。

联盟链的技术框架□很多，其中又以□超级账本项目下的技术框架□最为知名，应用也最为广泛，它基本代表了联盟链，所以，今天我们就重点来介绍□一下超级账本项目。

超级账本 HyperLedger

超级账本在 2015 年年底被发起，吸纳了众多重量级公司加入，它们包括大家耳熟能详的 IBM、Intel、Accenture、日立、JP 摩根、Digital Asset Holdings 等公司。

超级账本的代码和组织结构都结构清晰、层次分明。可以说无论从声势还是实力上来说，它都可以完胜公链。

例如，超级账本组织是会员制的，加入超级账本需要缴纳一笔入会费，入会费决定了你的会员等级。再如，超级账本 Frabric 的架构设计简直就是教科书级别的，干净利落、□模块清楚，几乎挑不出毛病。

超级账本由 Linux 基金会主持，宗旨是构建一个面向企业应用场景的开源分布式账本技术平台。

因为企业应用场景的多样性，所以超级账本包含了不只一个项目，它是由多个项目组成的。一共 9 个项目，其中 5 个是主要的技术框架，其他 4 个是辅助性工具。

它的主要技术框架分别是下面的 5 种。

1.Hyperledger Fabric： 没有中文名，暂译【纺布克】，是 IBM 提供的，超级账本第一个项目。 纺布克旨在用模块化架构作为开发区块链程序或解决方案的基础，允许一些□组件——例如共识算法和成员□管理变成即插即用的服务。

2.Hyperledger Sawtooth：中文名【锯齿湖】，Intel 提供，是超级账本第二个项目。 锯齿湖是一个可以创建、部署和运行分布式账本的模块化平台，基于硬件依赖的 PoET 共识，可以面向大型分布式验证器群，同时也比较低功耗。

3.Hyperledger Iroha：没有中文名，暂译【伊路哈】，□由 Soramitsu 提供。 伊路哈是为了将分布式账本技术简单容易地与基础架构型项目集成而设计的一个区块链框架。

4.Hyperledger Burrow：没有中文名，暂译【掘地者】，由 Monax 提供。 □掘地者提供了一个模块化的区块链客户端，□提供了权限管理的智能合约□虚拟机，它部分建立在以太坊虚拟机（EVM）规范的基础上。

5.Hyperledger Indy：没有中文名，暂译【因迪】。 □因迪是特别为去中心化的身份而建立的一种分布式账本。它提供了基于区块链或者其它分布式账本互操作来创建和使用独立数字身份的工具、代码库和可以重用的组件。

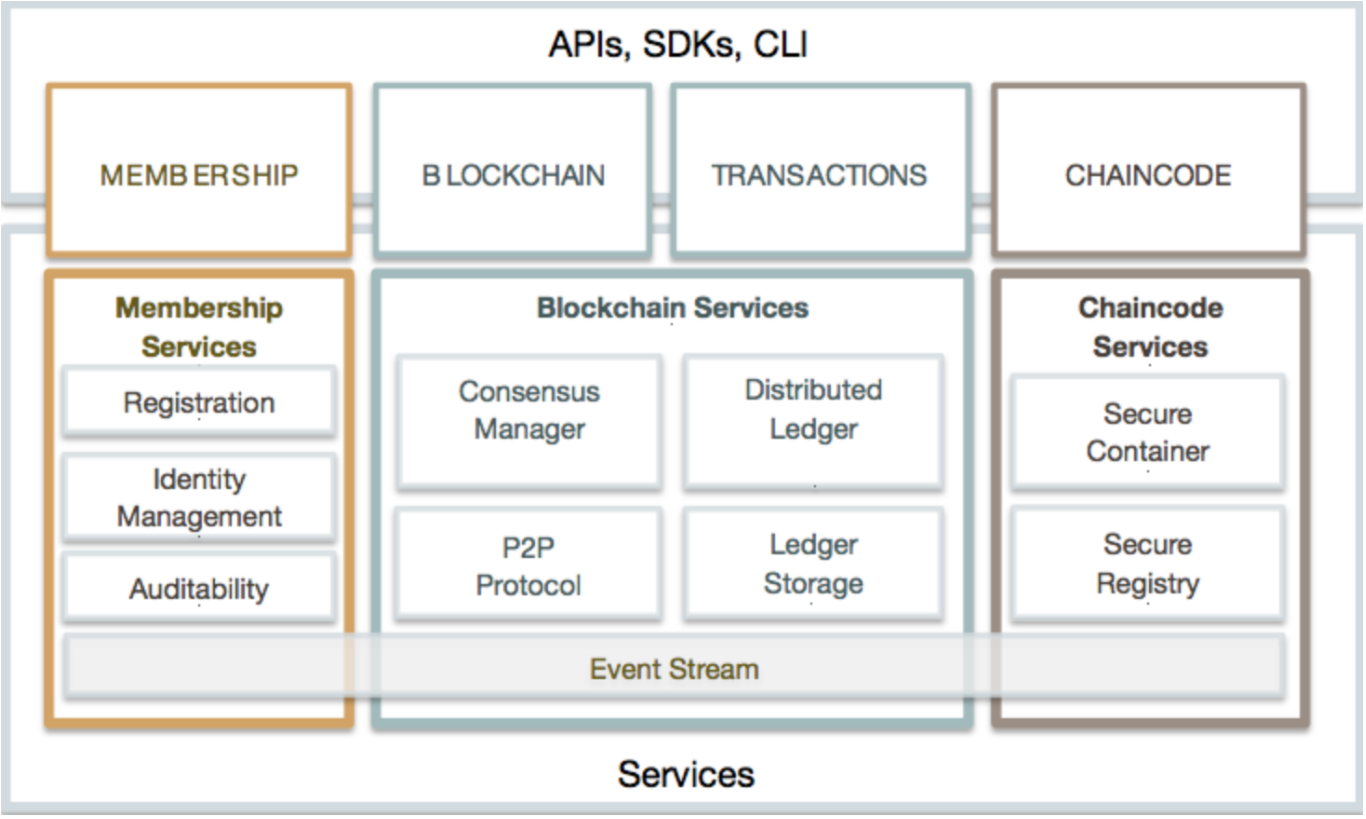
另外 4 个辅助性工具是：Cello、Composer、Explorer、Quilt，这四个辅助性工具可以对以上 5 个框架进行管理，例如 Composer 可以类比 Docker 中的 Composer，Explorer 就是区块浏览器。

我们不排除随着超级账本的发展，还有新的技术框架加入，当然，也可能存在既有的框架被市场淘汰。不过这些都不是本文的重点，所以我们不作过多介绍，你可以通过查阅超级账本官方网站获得更多内容。

1. 纺布克 Fabric

□纺布克是由 IBM 提供的，它基于 Go 语言，前身是 Openchain 项目。在□超级账本成立之初，Openchain 的代码量就已经达到 4 万行了，随着项目的推进，项目成员对 Openchian 进行了重构，也就是我们看到的□纺布克 1.0 版本。

□纺布克提供了比较完备的模块化组件，如下图所示。



我们可以看到，它的架构上分成了：成员关系管理、区块链服务、Chaincode 服务三个大模块。

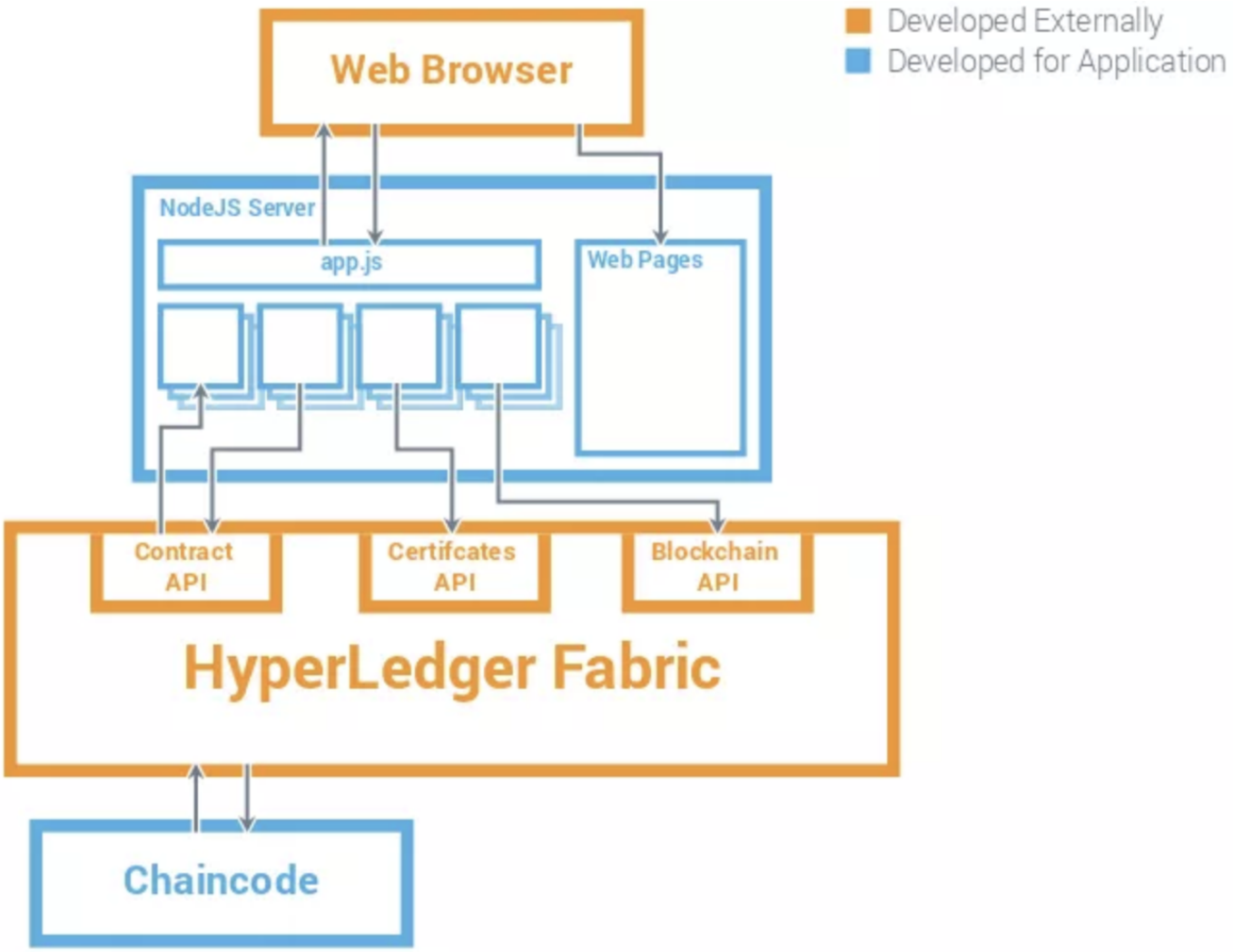
成员关系管理相当于账户和权限管理系统，区块链服务提供了区块链一样的□账本结构，Chaincode 服务相当于智能合约。

成员关系管理是基于 PKI 的成员权限管理，平台可以对接入的节点和客户端的能力进行限制。

区块链服务提供一个分布式账本平台，多个交易被可以被打包进一个区块中，多个区块□单向链接成一条区块链。区块链代表的是账本状态机发生变更的历史过程，这与公链区别不大。

Chaincode 包含核心的业务处理逻辑，并对外提供接口，外部通过调用 Chaincode 接口来改变账本数据，在纺布克中，Chaincode 是运行在隔离环境中的，也就是 Docker。

纺布克的一个可能的工作模式如下图。



如果 Chaincode 运行在 Docker 中，我们按照经典的 IT 架构来分析，可以发现纺布克基本就是经典分布式系统的升级版，它可以提供宕机容错，可插拔的共识模块让用户自行选择是否需要拜占庭容错。

2. 锯齿湖 Sawtooth

锯齿湖也是一个高度模块化的区块链技术框架，它基于 Python 语言，1.0 版本之后和纺布克一样，作为一套稳定的框架，它已经有了实际的应用了。

它是第一真正意义上提供拜占庭容错共识选项的超级账本项目，有以下□四个特点。

1. 链上治理：利用智能合约进行投票运营成员管理彼此之间的关系。
2. 高级交易执行引擎：可以并行处理交易的创建和验证，性能可观。
3. 支持以太坊智能合约：兼容了以太坊智能合约技术栈。
4. 支持主流语言编写智能合约：编写智能合约不局限 Solidity，可以是 Go、Javascript、Python 等语言。

相比以上四个特点，最引人注意的其实是锯齿湖提供了一个新的共识算法，叫做PoET（Proof of Elapsed Time），它的中文译作：时间流逝证明。

如果你熟悉 Raft 共识算法的话，我们知道 Raft 算法是一类强 Leader 的共识算法，□选举 Leader 的时候，每个节点□自己倒计时（CountDown），最先数完的那个成为候选人。

这个过程叫做超时选举（Election Timeout)。每个节点每□轮选举中得到的倒计时时间是不同的，它的代码实现为随机产生，通常是 150 毫秒到 300 毫秒。

PoET 与上述规则类似，只是倒计时时间的产生变更为硬件依赖的，这里的硬件目前是由英特尔提供的 SGX，Software Guard Extensions，它可以提供可信的程序执行环境。

SGX 提供了一种名为 Enclave 的机制，它支持两个函数“CreateTimer”和“CheckTimer”。CreateTimer 用于从 Enclave 中产生一个□计时器。

CheckTimer 会去校验这个□计时器是不是由 Enclave 产生□并验证是否已经过期。如果满足这两个条件就给该节点开具一个证明，这个证明可以被其他节点验证，验证通过则表示同意该节点成为记账节点。

我们看出，PoET 共识算法的拜占庭容错是由 SGX 保证的，具有一定的硬件依赖。

锯齿湖官方提供了的四种工作模式：开发模式、PoET 模式、PoET 仿真模式以及 Raft 模式。

可以发现，锯齿湖相当于是 Raft 协议的变种版本，选择 Raft 模式使得锯齿湖可以退化成经典分布式系统。

3. 掘地者 Burrow

掘地者也是一个基于以太坊 EVM 的智能合约执行引擎的区块链技术框架，最初项目名叫 Eris，它是基于 Go 语言构造的。

掘地者主要由下述组件组成。

共识引擎：□提供了基于 Tendermint PBFT 算法的高性能拜占庭容错共识算法。

应用程序区块链接口 ABCI：为共识引擎和智能合约引擎提供接口规范。

许可型□以太坊虚拟机 EVM：权限许可是可以通过本地安全接口强制绑定到智能合约上，其他与以太坊智能合约一样。

API 网关：□提供 REST 和 JSON-RPC 两种 API 接口。

□掘地者也是模块化的分布式账本技术，□提供许可型的智能合约执行环境，□它也基于 EVM 规范。除了 Tendermint PBFT 共识算法，没看到与纺布克的的区别。

4. 伊路哈 Iroha

以上几个技术框架，基本都是通用技术框架，不涉及业务概念。伊路哈是第一个关注资产创建和管理的区块链平台，通过名字我们也可以发现是一个日本公司主导的项目。

伊路哈具有如下特征。

可以帮助人们创建和管理多样化的复杂资产，例如货币、不可分割的权利、产品序列号和专利等等；

提供基于域名分类的账户管理机制，类似“子账本”系统；

提供权限管理；

系统本身提供验证业务逻辑规则，以及交易查询接口。

相较于纺布克和□掘地者是 Go 语言开发，□伊路哈是使用 C++14 开发的。

5. 因迪 Indy

因迪也是一个从身份出发去构建一个分布式经济系统的技术框架。

因迪具有如下的特征。

基于多冗余拜占庭容错 RBFT（Redundant Byzantine Fault Tolerance）实现的共识□算法，叫做 Plenum。

意图通过构建去中心化的身份来打造分布式账本。

全局唯一性的身份，无需中心化授权。

基于 W3C 标准的身份属性和格式；

提供零知识证明手段。

因迪与其他通用技术框架显得非常不同，对身份的研究或许会成为因迪的突破点，这点与元界的数字身份很像。

BaaS 与 BTaaS

超级账本很多技术框架是可以依托云计算来帮助企业进行快速搭建的，当然 IBM 和微软已经开始这么干了，他们将它称之为 BaaS（Blockchain As A Service)。

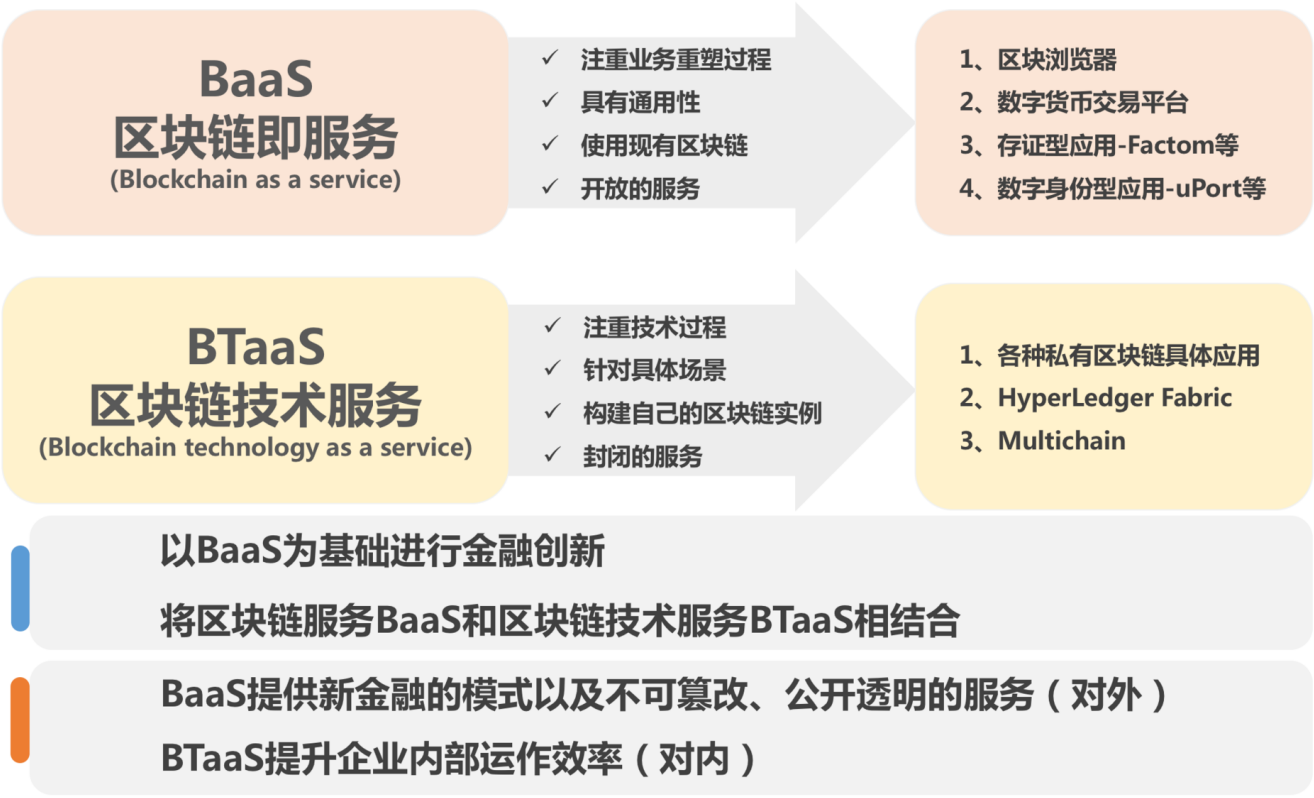
我们进一步思考，例如比特币提供了全球支付的功能，那么这种功能是否可以植入到云服务中呢?

答案是肯定的。对于诸多有支付需求的应用来说，自己搭建比特币节点，并且结构化区块到数据库中是非常痛苦的过程，毕竟比特币全节点提供的 API 有限，而我们的查询需求可能细致到交易输出和脚本签名。

所以，把比特币转化成 PaaS 服务也是另外一种 BaaS 思路。

因此，我们把原来的 BaaS 概念拆成了两种：

1. BaaS 是指把公链提供的服务转化成云计算中的 PaaS 服务的过程；
2. BTaaS 是指把区块链技术框架转化成 PaaS 服务的过程。



这两种概念还是有较大内涵上的差别的，我使用了上图来表达，我认为 BaaS 是未来区块链的发展方向，BTaaS 只是作为经典方案的补充。

联盟链的困境

超级账本系列技术框架很好地诠释了分布式账本技术走到极致是什么样子的。

这里也可以看出，几乎所有的超级账本项目都是技术主导，技术的强大也让他们忽视了市场的真实需求。

□联盟链是少数节点之间的活动，它往往退化成微观经济中的博弈，所以利用□联盟链构建少数节点之间的协作系统不是一个技术问题，而是变成了如何构造一个稳定的微观经济模型使得协作者可以达成帕累托改进，在这里，技术变成了次要的。

再好的技术工具如果不结合有效的激励和反馈机制，□那么联盟链的应用落地过程似乎变得异常艰难，它很可能最后沦落为普通的分布式系统，这个分布式系统仍然是中心化的。

这里我再提出一个问题，为什么我们不用已经成熟的技术框架，非要用联盟链技术框架呢？这就是我认为联盟链最大的困境，它是一杆加农炮，但是并没有人来告诉我们这杆加农炮可以解决什么问题。

总结

今天我们重点介绍了超级账本旗下的五个联盟链技术框架，希望可以给你提供一些技术选型上的参考。随后我们又介绍了区块链即服务这一延伸概念，最后我向你分享了我对于联盟链的观点。

今天留给你的问题是，除了超级账本之外，还有哪些有名的联盟链技术框架呢？ 你可以给我留言，我们一起讨论。感谢你的收听，我们下次再见。

参考引用：

1. https://www.slideshare.net/ormium/architecture-of-the-hyperledger-blockchain-fabric-christian-cachin-ibm-research-zurich
2. http://thesecretlivesofdata.com/raft/
3. https://intelledger.github.io/introduction.html#proof-of-elapsed-time-poet
4. https://github.com/hyperledger/burrow
5. https://github.com/hyperledger/iroha
6. https://github.com/hyperledger/indy-plenum/blob/master/docs/main.md
7. https://wiki.hyperledger.org/projects/indy
8. https://github.com/hyperledger/indy-node
9. https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_FAQ.pdf
10. https://medium.com/kokster/understanding-hyperledger-sawtooth-proof-of-elapsed-time-e0c303577ec1
11. https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf
12. http://blockchaindev.org/archives/08-on-limitation-of-private-chain.html

上一篇 第22讲 | 国内区块链项目技术一览

下一篇 第24讲 | 比特币专题（一）历史与货币

精选留言 (11)

写留言

有风的林子 4

2018-05-17

一个本质的不同，联盟链是有主的。主宰说什么是什么，而且通过安全账本保证了绝不含糊。

公链的主宰是上帝，或者市场。上帝和市场是自然规律，没有人欲的狭隘。

...

展开

作者回复: 鼓掌

SoWhat
2018-05-29

2

联盟链比公有链靠谱，政府，大公司都在用。公有链目前还都是泡沫经济，都还没落地，全是画饼。

作者回复: 你好，我们观点不一致哦。泡沫是一个新行业的必经之路，革新之始。

SoWhat
2018-05-29

2

联盟链适合政府和大公司优化一些流程，比公有链市场大得多。公有链最后可能只是一场泡沫，要落地太难了。

阿痕
2018-05-25

1

我觉得联盟链是当前阶段过渡性的区块链技术，它可以帮助企业认识和使用区块链，区块链最终的形态应该是公有链

作者回复: 我觉得未来也会共存，只是联盟链的生态不如公链家，无论是技术生态还是商业生态。

钰瀍
2018-05-17

1

我个人认为，经典分布式技术框架不适合搭建服务于网状生态系统的业务环境，这也是供应链系统一直不是很好的原因，联盟链退化自公有链，保留了区块链先天适合构造网状系统的基因，并且与现有多中心化的商业环境契合，又能发挥经典分布式系统难以依托通证实现的治理，因此更适合企业端的应用

作者回复: 有道理~

maomaosty...
2019-01-08

私有云，公有云，混合云，万变不离其宗

展开

rayeaster
2018-06-08

最近还有个新项目 clovyr.io 号称打通公链和联盟链

展开

作者回复: 挺多的，像阿希和NXT也是

rayeaster
2018-06-06

老师讲讲 r3 corda吧

展开

作者回复: 好的，看有机会我会发我个人专栏。

悟空来 |...
2018-05-26

联盟链已经好久了没有实际的运用场景

展开

作者回复: 供应链算一个吧

舍我其谁
2018-05-23

陈老师对秘猿的CITA有研究吗?
https://www.cryptape.com/#/

https://github.com/cryptape/cita

唐稳

2018-05-16

您好，关于BAAS和现有公链（比如比特币）关系，可不可以这么理解：
1）可以基于BAAS平台开发比特币应用，并将应用部署和运行在BAAS中
2）可以基于BAAS平台查询比特币公链相关的信息

而不是直接将比特币客户端部署到BAAS中

展开

作者回复: 是的，这是我的理解，也可以扩展到其他区块链，例如IOTA物联网服务也是可以的。