CHAOS

更商用的智能合约生态平台

More Commercial Ecological Platform for Smart Contract

CHAOS 基金会监制@2017

目 录

目　录

1. 背景

1.1 区块链技术

区块链技术是一种分布式的数据流通和共享的技术方案，利用去中心化方式维护一个可信数据账本，因此区块链技术也被称为分布式总账技术（DLT，Distributed Ledger Technology）。区块链技术在技术层面上解决了多方信任的问题，构建了一个可信的价值自由流通的基础设施。

比特币是区块链技术的第一代产品，是区块链技术的实践原型。从社会影响力角度而言，它是成功的，它成功地将区块链的去中心化、去信任价值理念在社会播种植根。进入 2016 年，越来越多机构和企业关注到了区块链技术的核心价值，创业企业也开始投入到区块链技术和应用研究中来。

1.2 CHAOS 的由来

随着商业领域对区块链技术的探索和钻研，区块链技术被认为可以用作商业智能合约应用的核心技术。随着以太坊的实验初步成功，区块链智能合约的前景和意义也被凸显出来。

CHAOS 团队在 2015 年就关注智能合约，并在 2016 年启动 CHAOS 区块链智能合约平台开发。结合团队在商业场景领域的积累以及对技术商业化的理解，CHAOS 初始的想法就是要建立商业易用的智能合约生态平台，而非简单的数字资产流转应用。

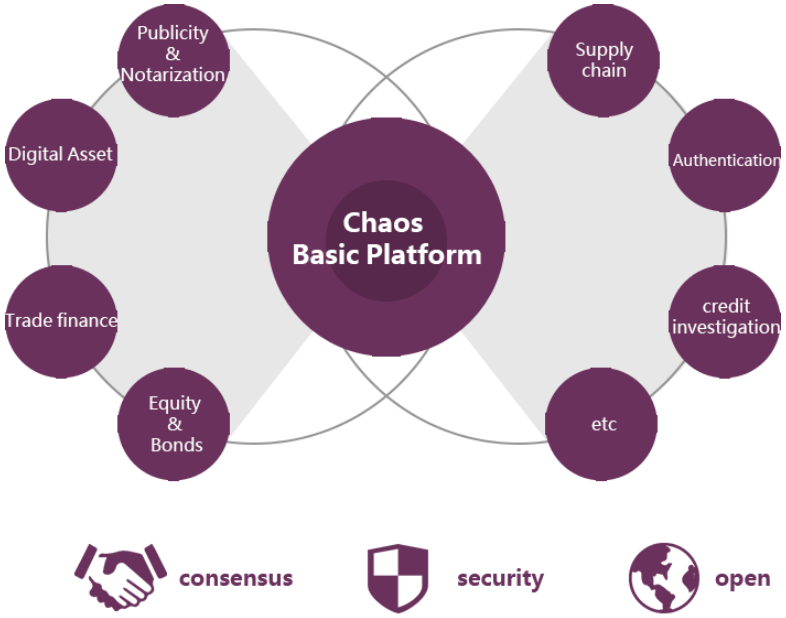
CHAOS 一词起源于卡俄斯（英语：Chaos），Chaos 是传说中的混沌之神，一切世界及概念的开始。根据赫西俄德和早期古希腊神话（公元前 8 世纪）记载：宇宙之初，只有卡俄斯，他是一个无边无际、一无所有的空间。因此卡俄斯的名字 Chaos，就成了宇宙之初的代名词。我们选择 CHAOS 作为项目的名字，是希望 CHAOS 能够成为所有智能合约商业应用的根基和信任的开始。

2. CHAOS 的定位

CHAOS 定位于提供信任缺失场景解决方案，打造一个区块链基础服务设施，也就是区块链商业智能合约生态平台。CHAOS 致力于帮助业务在区块链上快速产品化，真正实现区块链服务化。CHAOS 主要完成两个层面技术：支持服务的底层区块链基础设施，和支持高扩展的应用层业务开发环境和工具库。

目前，区块链研发主要集中在两个领域：一是专注于解决区块链底层技术，二是区块链上层应用。目前区块链底层技术主要是解决交易速度问题，闪电网络技术是针对比特币网络提出的一个解决交易速度问题的方案。区块链上层应用主要是构建一个图灵完备的可编程环

境以及配套的工具库,便于开发者在上面快速实现去中心化应用,这一领域开创者是以太坊。

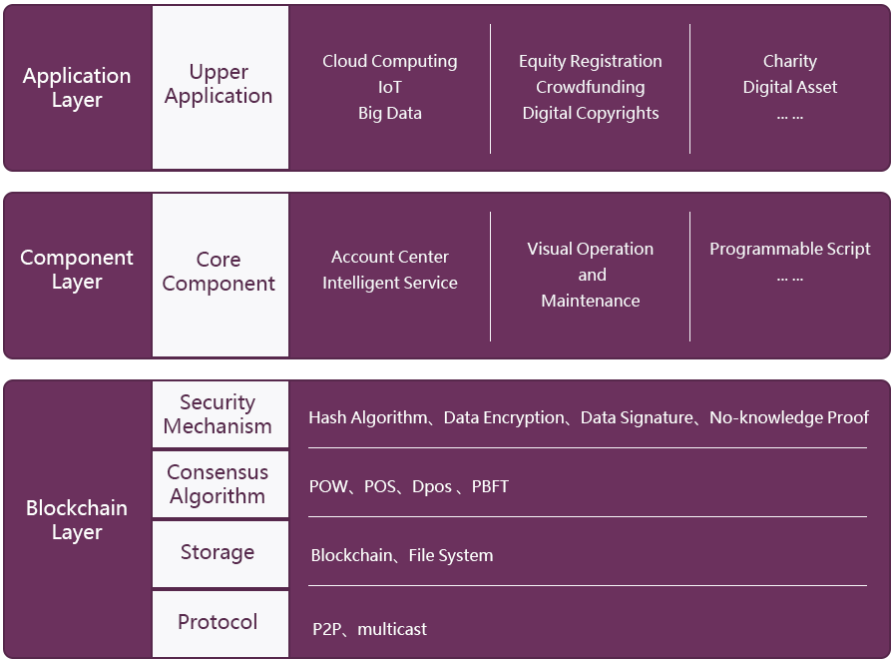


CHAOS 整体构架

与比特币相比，CHAOS 在区块链应用开发落地方面有着明显技术优势。基于 CHAOS，开发人员可以便利地开发第三方应用。相比于以太坊，CHAOS 没有硬分叉的风险和担忧。CHAOS 试图打造一个异于比特币和以太坊的区块链生态系统,并将其推广到各个商业领域，例如法律、贸易、征信、金融借贷、VC 投融资和资产确权等。

3. 技术架构

CHAOS 系统分为三部分：一是底层的 CHAOS 区块链服务，一是中间层的 CHAOS 组件层，一是上层的 CHAOS 应用层。底层提供完善的区块链服务，包含网络协议，数据存储，共识机制，安全机制四方面；中间层提供区块链开发套件，将区块链封装，方便上层应用对区块链服务进行调用和监控，以及构建智能合约；上层基于业务场景构建可信应用。

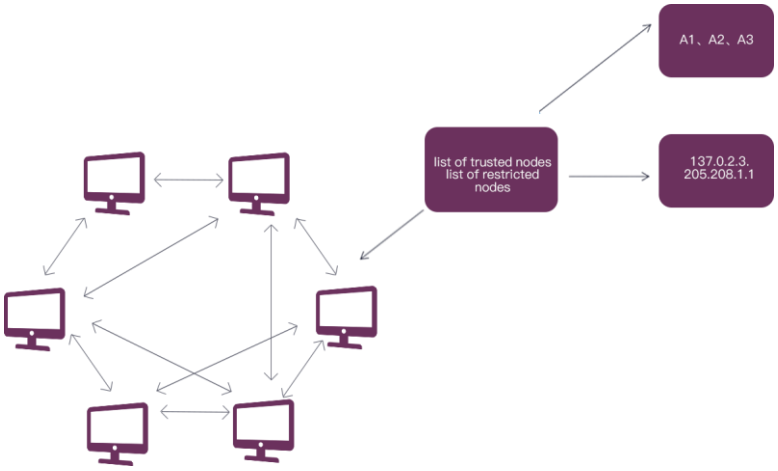


CHAOS 系统设计方案

3.1 区块链服务

3.1.1 网络协议

网络协议基于成熟的 P2P 组网协议实现，节点维护邻居节点列表，以自组织形式动态组网。除此以外，添加了可信节点列表，IP 限制等安全措施，增强网络协议安全性和健壮性。



网络协议安全机制说明

3.1.2 共识机制

CHAOS 团队在共识机制上的研究方案主要用于解决网络节点一致性信任问题，同时需要保证能抵抗恶意攻击。CHAOS 目前支持 PoW 和 PoS 算法，未来考虑开发支持多种共识算法，包括 DPoS，PBFT，DBFT 等。

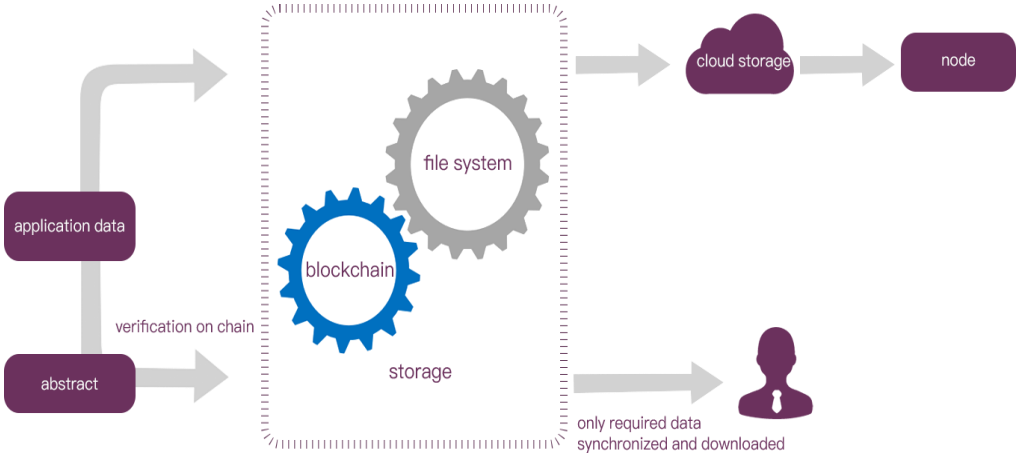
3.1.3 数据存储

数据存储包含两部分：区块链和文件系统。数据存储是区块链底层核心技术，包括数据格式定义，以及数据读写方式。区块链数据依然存储在链式数据结构之上，应用数据则存储在文件系统里，但是应用数据摘要会保存到区块链之上用于可信验证。

由于区块会不断的增长，导致应用数据所占用的空间也会不断的变大，普通电脑根本无法保存那么大的数据量。实际上，大部分用户并不需要存储全部数据，只需要下载可供基本验证的区块数据即可，大部分应用数据不必保存到本地。我们提出的解决思路是数据分片+云存储方案，具体思路如下：

数据分片：把数据分为热数据、冷数据，必需数据、非必需数据，普通用户只需下载必需数据即可快速参与区块链验证工作。

云存储：将历史数据保存到云端，并分发到世界各个节点，实现去中心化，并通过 CDN 加速，用来解决大量历史区块的存储问题，以及同步数据的效率问题。



数据分片+云存储方案

3.1.4 安全机制

通过对网络层的改造，CHAOS 设计了一套安全的加入机制，可限制了非授权用户的连接，从而增加区块链的安全性；这将意味着上新加入者需要通过现有区块链维护者超过一半（可设置）的授权允许，才能加入该网络，有点类似于投票，只不过投票人是现有区块链网络维护人。

对于私有链、联盟链来说，这是极其有用的。只有这个联盟里面的超过一半的人允许新

节点加入，这个新节点才能连接到该区块链网络，并参与挖矿。

3.2 组件服务

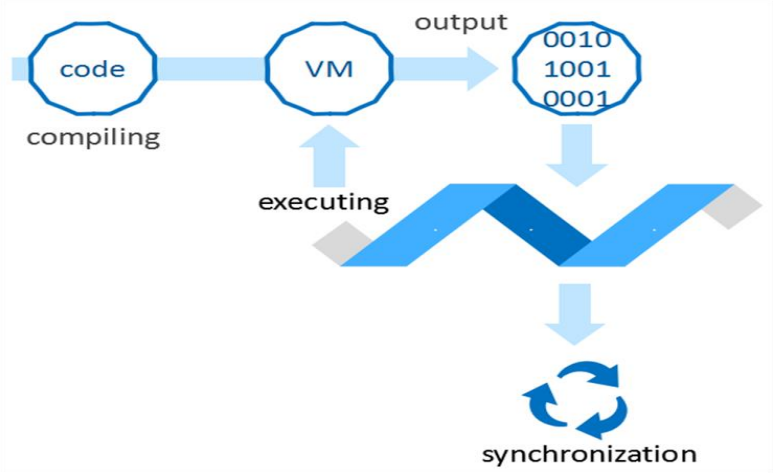
3.2.1 账户中心

提供了公私钥生成、管理功能，可使用私钥对交易进行签名、交易验证、多重签名；支持地址实名认证，同一用户支持多个地址；可针对特定用户开放高级功能权限，实现审计监管；提供应用层地址与区块链地址的映射，对于应用来说，不需要知道用户真正的区块链地址，只需知道应用的地址即可。

3.2.2 智能合约

CHAOS 合约层为上层应用提供更高层的基础组件,支持应用资产发行。开发者可基于现有区块链发行应用内部代币，并可实现应用代币跟区块链货币之间的互转。

CHAOS 可以提供商业化的大型智能合约应用服务。智能合约其实就是预先定义好的一段脚本，在发布之后就无法修改。在智能合约中支持自定义数据结构，实现复杂的业务逻辑，并通过跟自定义资产或区块链货币结合，开发出各种去中心化的应用。智能合约提供对数据进行加密处理，只有数据相关人才能看得到数据，并支持可拔插的应用共识机制，实现特定领域的特殊共识需求；开发者只需要将开发好的智能合约部署到区块链，用户即可使用该合约。



智能合约实现模型

为了更好的适应未来的区块链环境，我们系统的设计考虑到不同区块链的互通问题，考虑将其作为一组基础服务提供给开发者，实现区块链之间的资产转移，交叉验证。

3.2.3 运维中心

提供多种可视化区块链管理工具，对区块链进行监控。支持区块链参数配置;支持在线分叉投票；支持区块浏览器，可查看实时区块数据，节点分布情况，整个区块链网络运行情况；提供多维度的数据分析，可及时发现区块链异常情况，并发出警报。

3.2.4 可编程脚本

为了更方便开发者基于区块链进行智能合约编程，我们对区块链底层进行改造抽象，提供了一种更简单的方式进行编程，那就是利用脚本语言。

智能合约代码会运行在脚本虚拟机中，实现了脚本运行时的隔离，以控制脚本权限，并通过将区块链数据注入脚本虚拟机中，实现脚本可访问区块链数据实现智能合约逻辑。

脚本语言因其语法简单，易用的特性，受到广大开发者的喜爱。以语言的通用性、易学性作为考量标准，决定前期采用 lua、javascript 这两种语言作为智能合约开发的脚本语言。未来我们可能会支持更的语言供开发者选择。

4. 应用场景

CHAOS 作为解决信任问题的技术中介，在诸多应用领域可以发挥作用，将包括数字资产，征信，供应链，信息公示，保险等。下面将挑选几个应用场景说明 CHAOS 如何应用。

4.1 数字资产发行管理

金融数字资产发行在区块链上具有如下优势：总量恒定，资产自由流通，流向可溯源追查，参与者共同维护资产的可信性。传统的股票，债权，收益凭证等都可以整合到区块链上，发行相应数字资产。

发行者将资产凭证登记在区块链上，发行自己的数字资产。一旦发行完毕，该数字资产维护将不再只受发行方控制，而是由数字资产持有方和参与方共同维护，真正达到社会化运营。区块链作为一个价值自由流通的网络，数字资产可以通过这个网络在节点间自由流通交换。任何新的机构或者用户想参与进来，只需要将系统对接该数字资产的区块链系统或者成为区块链网络一个节点，这样增强了数字资产流通渠道的多样性。而资产的价值由参与该数字资产运营的机构或者用户共同决定，真正通过社会化流通实现价值定位。

4.2 互联网征信

在互联网征信领域，普通小企业由于缺少大量数据来源，其自身拥有的数据无法精确绘

制用户征信图像，只得依赖于这些大型机构。这种单中心的征信模式，往往需要依赖于企业的规模效应。对于提供征信服务的企业而言，其信息采集和维护成本也是极其高昂的。这使得征信服务往往具有垄断性。

基于 CHAOS 的互联网征信则是一个开放共享的服务模式，可以看做是一个行业内的联盟链。区块链数据的不可伪造，不可篡改属性也增强了企业间信任，参与维护这个联盟链的企业需要将数据共享在区块链上，所有企业共同参与维护和验证。

这种基于区块链的数据共享方式，也丰富了征信数据来源，增强了征信服务可靠性。多个企业共同参与维护征信系统，降低了企业成本。

4.3 供应链溯源

供应链数据在上下游企业间、政府监管机构流转，要保证数据真实性，不可篡改性。传统供应链模式，企业间，企业与监管部门之间数据往往无法自由流通，为数据造假的提供了可能性。

CHAOS 应用在供应链上保证了数据的不可篡改性，且上下游企业，政府监管机构大家共用一个网络，共同维护网络数据真实性。从产品原材料，到生产，再到入仓储，最终流转到各级经销商，分销商，全程数据都记录在区块链上，可溯源追查数据真实性。供应链上各个企业更好地明确上下游关系，使得间接上下游关系的企业间也产生关联。

4.4 信息公示

现有的信息公示模式下，信息的权威性完全来自于公示主体，这种公信力的证明方式恰恰容易滋生诸多内幕交易。

区块链数据的不可篡改、无法抵赖的属性极大地满足了公示领域要求。在区块链上实现信息公示，其可信性不再来自于单一机构，而是来自于大众节点的认可。一旦为大众认可的信息才会被记录在区块链上，然后公示于众。一旦被公示的信息，是无法被任何单一机构或者个人所篡改的。区块链从技术层面上，保证了公示信息的可靠性。

4.5 互助保险

随着互联网互助保险业务放开，越来越多平台开始开展互助保险业务。互助保险业务其核心行业痛点在于资金流向不透明问题和赔偿标准问题。现有互联网保险模式，其资金流向是无法受到公众，尤其是投保用户监控的，容易出现平台挪用现象。

基于 CHAOS 开展互助保险业务，将用户投保资金以及资金流向记录在区块链上，投保用户可以查看到自己投保资金流向。如果权限允许，甚至可以申请查看所有投保资金流向，这无形中增强了平台的公信力。

一旦出现赔付事件，可以由投保用户投票决定该事件是否应该赔付，以及赔付额度。这样可以避免大的赔付纠纷，降低平台运营风险。

5.代币 COS

5.1 价值

传统互联网商业世界，信任来源于中心化平台；CHAOS 将信任问题去中心化，将信任确定问题交给系统参与者共同决定，参与者可以获得相应资产奖励。在 CHAOS 的区块链生态体系中，虚拟世界的信任被赋予了价值。

在 CHAOS 体系里，资产奖励以及价值体现的媒介就是 COS 代币，COS 是 CHAOS 生态系统中唯一一个系统代币，充当了虚拟世界价值衡量尺度的类货币。在 CHAOS 生态中，不同的应用可以依托 COS 发行不同的资产代币，这些代币根据应用的特定需求在 CHAOS 生态系统中流转，充当应用的价值媒介或者权益凭证。

总结来看，COS 主要用作系统燃料、区块链应用价值转移媒介。具体来说是，

系统燃料：CHAOS 是一条公有链，基于其来开发部署的智能合约均需要消耗一定量的 COS。

价值转移媒介：作为 CHAOS 生态系统的唯一代币，COS 充当了价值媒介，在链上展开的智能合约应用可以基于 COS 进行交易、清算和结算，所有交易可溯源、防篡改。

我们希望 CHAOS 社区的爱好者们以及商业应用者们可以通过 CHAOS 区块链系统发行自己的智能合约应用，不断完善整个 CHAOS 生态体系，提升 COS 代币的使用价值。

5.2 分布

在 CHAOS 体系中，COS 会恒量发行，永不增发。COS 代币总量 1000 万枚，采用 POW 机制预挖生成，其分发方式如下：

天使投资：100 万枚（10%）；

ICO：600 万枚（60%）；

团队预留：100 万枚（10%）；

基金会：200 万枚（20%）。

说明：CHAOS 项目是一个社区型公有链项目，CHAOS 基金会会全面负责项目的推广和商务合作等，基金会持有的份额会用于支持媒体、第三方合作以及后续会员招募、后续战略投资方引进等。团队预留部分将锁定 2 年，第三年开始逐步释放，每年释放不超过 20%。

6. 团队

Thomas	技术总监
Breton	架构工程师
Prescott	后端工程师
Grover	系统安全专家
Micheal	商务顾问

Thomas 计算机专家，拥有 20 多年计算机软件开发与研究经验，曾就职于多家互联网巨头企业，担任技术专家，有三年多的区块链技术研究经验，是 CHAOS 项目的创始人，负责该项目整体技术工作。

Breton 软件架构工程师，专注于开源软件系统的设计，曾参与多个区块链项目架构设计与开发工作，对比特币、以太坊架构有深入理解，有丰富的系统设计经验。负责 CHAOS 项目系统架构设计与开发工作。

Prescott CIT 计算机工程毕业，14 岁开始接触计算机编程，擅长多种计算机编程语言，多次在国际计算机编程大赛中获奖，2013 年开始专门从事区块链开发工作，负责该项目技术开发工作。

Grover 软件安全专家，在计算机安全领域有大约 25 年的研究经验，曾为花旗银行、亚马逊等多家大型机构提供安全顾问的角色支持，负责 CHAOS 项目系统安全工作。

Micheal 商务顾问，曾担任互联网企业市场品牌负责人。负责 CHAOS 项目商务对接与市场推广工作。