
CTS

目录

壹

传统慈善与医疗现状

1、 传统公益项目痛点不断

2010年重庆武隆白马镇沙台小学被举报变卖救灾物资， 使人们开始怀疑捐赠物资是否真能到达了救助对象手上；2011年的郭美美炫富事件引起全社会对公益组织的质疑， 受益资金不透明化， 区块链完全可以改变这一现状；2013年嫣然基金会被质疑存在腐败， 虽然最终证明子虚乌有，但在事情澄清之前， 社会舆论几乎呈现出一边倒的态势， 严重影响了人们参与公益的热情。以上种种，都暴露了现行公益体系公信力不足的问题， 据《2010年全国慈善组织信息披露现状报告》显示， 约有75 %的慈善组织“ 完全不披露或仅少量披露信息” 。42 %的组织表示没有专门的信息披露办法。37 %的组织没有专人负责信息披露工作。更深层的问题， 则是披露的程度和方式不被高达90 %的公众所接受。造成信息披露不足的原因主要是渠道的缺乏。

公益事业的中间环节， 包括信息公布、中立评价等基础架构薄弱， 缺乏独立、专业的信息中心和中立机构对公益组织的绩效进行公开和评审， 整个公益行业缺乏统一的信息披露标准和公共信息披露平台； 公益组织缺乏信息披露所需的人力和物力投入； 同时公益组织很少对信息披露的效果进行评估； 也缺乏信息披露的动力。民间组织信息发布不足、透明度低、公信力差， 使得公益事业各方都无法做出以事实为依据的决策。但是如果用传统的物流、资金流、人力流的监控记录方式， 不但会投入巨大成本， 同时由于数据的集中化管理， 仍然缺乏让广大民众认可的公信力， 这个问题似乎无法破解， 正在人们为此绞尽脑汁时， 一个叫中本聪的神秘人物带来了新的思路。

2、 医疗信息难以公开透明

医疗行业本身痛点繁多， 老龄化、亚健康、医疗资源紧缺等诸多问题都给人类社会带来极大挑战， 而资源配置不均衡、智慧化程度较低、医疗机构之间的资讯壁垒、医生培养成本高昂,诸多因素让解决过程步履维艰。

）个人对于自身医疗资料缺乏追溯权、知情权及存取控制权

医疗资料产生于使用者， 大多却存放在医疗机构中。使用者对于自身医疗健康资料资讯既不了解， 也不具备备掌控力， 当用户就诊时， 只有有限的资讯可以参考， 这往往会提高临床决策的难度， 不利于用户的疾病诊疗过程。 并且， 使用者并不能享受由自己医疗资料研究带来的利益。在美国，2005 年有一位白血病人的血液中含有可以治癒白血病的生物机制， 治疗他的医学研究机构， 在没有通知他的前提下， 使用他的医疗资料研究出了相关治疗技术， 并且获益数十亿美金。而存储在区块链上的资料， 整个使用的链条都可以追

溯， 使用者对自己的资料有完全的控制权和知情权， 能够享受医疗资料研究带来的利益。

2 ）医疗健康资料的快速增长和中心化的存储方式使得资料安全问题日益严峻

传统情况下医疗健康资料大多以资料中心的方式进行存储， 容易遭受恶意篡改、骇客入侵、自然灾害等意外情况导致的破坏。随著医疗机构资讯化进程的加快， 资料中心这种集中化存储所存在的隐患日益加剧。

3 资料孤岛导致医疗健康资料难以得到高效共用利用

由于历史原因， 医疗机构之间存在极高的资讯壁垒， 相互之间资料不能互通， 医疗健康资料不能够得到有效的整合利用。用户在进行跨院治疗的时候， 历史医疗资料难以调用。

中心化存储也会阻碍研究资料的效率， 使用者医疗资料的录入存档和研究机构的调取因为安全的需要， 都需要冗长的手续。而区块链分散式存储资料， 既能够保证安全性， 又可以全网即时调取医疗资料。

Google 曾经通过使用者搜索行为检测到一些地区流感爆发的迹象， 提前通知了相关医疗部门准备流感药物。而目前传统的医疗机构， 需要接待有流感的病人， 诊断观察后回馈再层层上报， 耗时三个月， 已经过了最佳的防治时期。国内的非典流感， 也是暴露出中心化的医疗资料的效率底下和迟滞。

B 3、 区块链+慈善公益

区块链具有去中心化、公开透明、信息可追溯、通过智能合约自动执行四大优势。这四大优势正好对应的解决了原有慈善公益项目所被人诟病的问题。

区块链是一个去中心化的技术， 它将慈善公益项目相关的信息都是分布在网络各个节点上，目前没有什么技术能同时篡改整个网络上51 %以上的节点数据， 这样杜绝了某一个组织或个人操控一个慈善公益项目为自己谋求利益。并且区块链上所有的信息都是对全网络公开的， 相关人都可以对每一笔交易进行查询和追溯。这样我们就可以知道所捐助的每一笔款项的对应接收人是谁、是如何使用的、一共发放了几次、救助效果如何等等都可以查询和追溯相关的责任人。

区块链智能合约的使用解决了传统慈善公益项目中复杂的流程和暗箱操作等问题。我们只需要把相关的条件和要求设定后智能合约就可以自动的执行了。比如， 我们收到一个贫困儿童求助的请求， 系统自动生成一个智能合约， 智能合约确认真实性后给出救助方案。款项的金额， 款项的使用步骤， 和将会达到的效果等内容都会在合约中体现。整个合约从收款到执行都可以自动的操作， 并将执行情况自动给出反馈。整个过程不需要人工的去干预，并受所有参与当事人的监督， 通过智能合约这种全自动的模式确保了项目平稳落地。

4、 医疗数据公开信息化

CST区块链、人工智慧技术为基础， 构建智慧医疗价值链， 通过使用者体征资料创造智能硬件， 生命银行对医疗健康资料安全存储， 链上成员及机构开发资料价值并参与资料交易，AI 超能医生通过多种智慧诊断模组解析比特数位人并进行智慧诊断。

CST从医疗资料端切入， 围绕医疗资料安全、共用、使用等关键问题进行产品设计， 打通医疗电子病历、医疗 APP、物联网医疗设备之间的资料壁垒， 连接医疗平台、互助保险平台及线下机构， 为医疗生态圈中的资料需求方， 例如： 患者、医生、医院、技术服务商、保险公司、基因公司和健康管理机构提供服务。在未来将为医疗健康行业提供以区块链、人工智慧为核心底层技术的全套医疗服务解决方案。

贰

区块链未来发展与通证经济

1、什么是区块链？

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。具体来说， 区块链技术是构建在点对点网络上，利用链式数据结构来验证与存储数据，利用分布式节点共识算法来生成和更新数据， 利用密码学的方式保证数据传输和访问的安全， 利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

通俗的说， 区块链是一套多方参与的、可靠的分布式数据存储系统， 其独特之处在于：一是记录行为的多方参与， 即各方可参与记录； 二是多方参与者可以独立验证信息而不需要一个中心化机构的参与， 三是区块是在存储封存在链上的， 无法被删除或者窜改。

在应用实践中， 这种系统能够实现所有参与者信息共享、共识、共担， 从而帮助现有的经济体系脱离通过制度约束或依赖第三方机构背书的模式， 双方直接实现价值交付。这种特性可以有效降低交易成本， 提高交易效率， 减少因交易一致性所引发的摩擦。同时， 区块链具有既公开信息又保护隐私， 既共同决策又保护个体权益的特性。

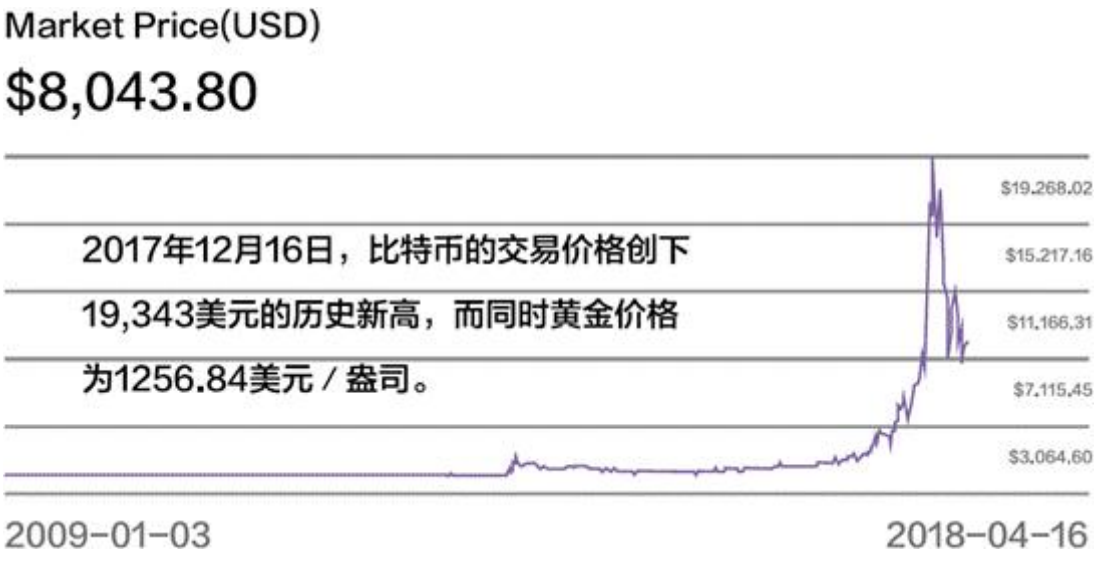
区块链技术创新加速技术创新是区块链行业深入发展的核心驱动力,区块链行业的技术创新正在经历着一个明显加速的过程。以2014-2017全球公开的区块链专利数量为例,从总体趋势来看,全球与区块链技术相关的专利公开数量呈明显上升趋势。

区块链融资增长迅猛2014 -2017年7月全球区块链领域投资金额总体呈现增长趋势。ICO的兴起,全球市场相对2014年增长幅度明显。区块链应用范围广阔得益于区块链技术的持续创新,区块链应用在全球呈现出多元广泛、积极活跃的特点。2014 -2018 ,区块链领域股权投资共计投向挖矿、钱包、虚拟货币、基础设施、底层技术、交易所、相关服务、区块链应用多个领域从占比高的区块链应用来看股权投资领域又可分为数据服务、金融、认证确权、文化娱乐等多个领域。通证经济(token economy)下一代互联网的数字经济。

2 2、数字货币发展历史

2008 年， 中本聪在比特币论坛发表了题为《Bitcoin: A Peer to Peer Electronic Cash System》的论文， 首次提出区块链的概念， 并由此构建了交易信息加密传输的技术基础和比特币网络。从 2009 年比特币数字货币平台建立至今， 比特币系统稳定运行， 自动实现了从发行到交易流通的过程。同时， 区块链作为基础支持技术， 逐渐独立出来应用于更多场景， 诞生了多种基于此概念的数字货币， 比如莱特币、狗狗币、瑞波币等。2015 年， 随着以太坊开源项目带来的智能合约平台概念， 实现了各种不同4 类型资产及合约的注册和转移， 方便了数字货币的发行和流通， 极大程度的丰富了数字货币类型。特别是从2017 年初开始， 通过 ICO 的方式， 各种代币层出不穷， 带来了数字货币市场新一轮的繁荣。截止到 2017 年年底， 在 Coinmarketcap 有统计的数字货币类型已经接近1000 种， 总市值突破 3000 亿美元。

数字货币正在被越来越多的人认知和接受， 以比特币为例，2018年2月末， 比特币价格为 9754 美元， 总市值约为 1660 亿美元， 流通量 1663.9 万 BTC。



当前区块链概念已经引起了各行业的广泛关注。之所以如此引人注目， 因为从根本上区块链将变信息互联网为价值互联网， 变信息可计算为价值可信任。这使得区块链可以通过颠覆传统的信息系统技术模型来支撑实现业务上的高可信应用。具体来说， 区块链技术在应用上的各方面特性简单总结如下：

① ） 区块链系统的使用： 通过各种加密技术使所有产生的有效信息与数据不可抵赖，不可篡改；

② ） 区块链系统的运营： 通过智能合约使系统运转与管理都按约定规则自动进行， 不受任何唯一方控制， 实现去中心化或多中心化；

③ ） 区块链系统的开发： 所有的规则与源代码， 都按约定开发完成并透明开放， 开发者无法隐藏后门；

④ ） 区块链的分类按照节点准入规则， 可以划分为公有链、私有链和联盟链。

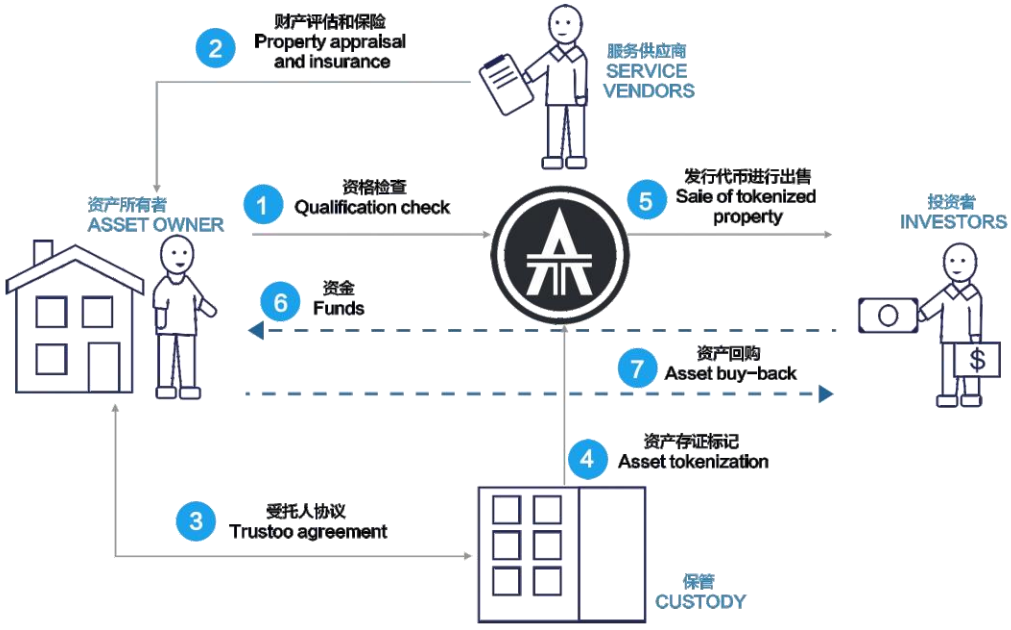
2 3、 区块链+智能合约

智能合约就是“ 可编程合约”， 或者叫做“ 合约智能化”。其中的“ 智能” 是执行上的智能,也就是说达到某个条件合约自动执行,比如自动转移证券、自动付款等,这将是区块链技术重要的发展方向。由于区块链可实现点对点的价值传递时可以嵌入相应的编程脚本,通过这种智能合约的方式去处理一些无法预见的交易模式,保证区块链能够持续生效。这种可编程脚本本质上是众多指令汇总的列表,实现价值交换时的针对性和条件性,实现价值的特定用途。所以,基于区块链的任何价值交换活动都可通过智能编程的方式对其用途、方向和各种限制条件等做到硬控制,省去了以法律或者合同约束的成本。

2 4 通证经济（token）

Token不是代币,是通证首先要把词汇表定义清楚。今天有两个意义不同的词汇被模糊混用,其一是 Cryptocurrency 一般译为“ 加密数字货币”,简称为“ 数字货币”。其二是 token”,被广泛译为“ 代币”。平时口语之中,经常只说“ 币” 字,比如说:“ 你的那个

用发不发币?” 。 那么究竟这里的“ 币” 是“ 加密数字货币(cryptocurrency)”,还是“ 代币(token)”?语义模糊。实际上这两个东西是不一样的。加密数字货币起源于比特币,它的目的就是作为互联网支付的货币。而 token 是怎么来的呢?在网络通讯中, token 的原意是指“ 令牌、信令”。其实就是一种权利,或者说权益证明德国经济学家南普认为货币,特别是信用货币,从一开始就有权力介入,实际上货币即权力,即政治,货币权力必须属于国家。然而 token 所代表的,可以是一切权益证明,岂止于货币?恰恰相反, token 的实际落地,非“ 代币” 类的应用恐怕会远远走在代币前面。比如比特币,中本聪是想让它成为支付货币,但是现在它变成了一种数字资产,并没有发挥通货的作用。尤瓦尔· 赫拉利在《人类简史》里说的,正是这些“ 虚构出来的事实” 才使智人脱颖而出,建立人类文明的核心原因。可以说人类社会的全部文明就是建立在权益证明之上的所有的账目、所有权、资格、证明等等,全部都是权益证明如果这些权益证明全部数字化、电子化并且以密码学来保护和验证其真实性、完整性、隐私性,那么对于人类文明将是一个巨大的翻新。



2 .1、通证有三个要素, 缺一不可

( ) 数字权益证明。也就是说通证必须是以数字形式存在的权益凭证,它必须代表的是一种权利,一种固有和内在的价值(Intrinsic value)

( ) 加密。也就是说通证的真实性、防篡改性、保护隐私等能力,由密码学予以保障。每一个通证,就是由密码学保护的一份权利。这种保护,比任何法律、权威和枪炮提供的保护都更坚固、更可靠

( ) 可流通。也就是说通证必须能够在一个网络中流动,从而随时随地可以验证。其中一部分通证是可以交易、兑换的。事实上,通证可以代表一切权利。

31 1、CST项目愿景

CST构建开放、平等、安全的智慧医疗链平台， 所有参与者都能够创造和分享CST上价值。 每个人在使用CST平台的时候给CST贡献了资料和资源， 并获得应有的收益。 资料， 是CST运行的基石，使用者通过感测器、智慧硬体、医疗设备向CST云端上传即时资料， 资料在CST上通过差分隐私技术进行安全加密， 实现存储、解析和流通。 Token，是CST网路中的权益凭证。使用者上传及分享资料将获得Token，购买保险、 疾病诊断、 健康助理、健康状

况即时预警服务需要消耗 Token。医疗机构需要使用医疗资料研发或者CST平台资源时， 都需要Token来作为经济手段。 CST的核心为医疗资料平台， 接入影像诊断、单据识别、心电监测等诸多模组供使用者选择使用。

①）用户： 感测器即时监测上传个人体征资料， 获得 Token 及诊断、保险等医疗服务

②）保险公司： 依托于使用者个性化的生理体征资料， 保险公司可以开发针对性的产品， 使用者的体质越健康， 需要缴纳的保险费用就越少， 对于用户体征异常的状况， 能够及时作出就医提醒， 在用户申请理赔时， 能实现急速理赔。

③）药企及药械厂商： 能够研发优化药品和器械。

④）科技公司： 能够开发个性化诊断治疗产品。AI 超能医生能为患者提供健康建议及疾病诊断见。

⑤）医疗机构： 使用者出现生理体征异常需要及时就医时， 医疗机构可调用使用者的完整历史医疗资料， 实现全面诊断。

32 2、CST医疗管理体系

目前健康类 APP 繁多， 而安全性是保障资料在网路中流畅运转的关键， 基于区块链的的分散式存储让CST具备高度的安全性，CST对使用者上传的资料通过同态加密、差分隐私（differential privacy， DP）进行资料安全保护， 并使用离散存储方式进行资料存储。CST上的医疗健康资料由整个系统中具有维护功能的节点来建立共识、共同维护、不可篡改。

CST将医疗资料与区块链协定绑定， 进行信任认证， 安全和管理的授权， 让每个人可以管理自己的医疗健康资料， 把资料的控制权归还给使用者自己， 让每个资料的贡献者获利， 用户和机构能够在安全、平等、信任的前提下， 共同分享资料、存储、算力等等资源， 构建开放的资料存储共用平台。

CST上的资料只有拥有者或者授权者才能访问， 资料的存取权限由使用者设定的智慧合约来确定， 例如： 使用者可以将自己的资料存取权限授权给三甲医院， 当用户患病之后医生可以直接调用资料进行诊断。当资料只有所有者有许可权访问的时候， 用户有突发病症状况时， 可以触发事先定义好的智慧合约将资料自动授权共用给医院。

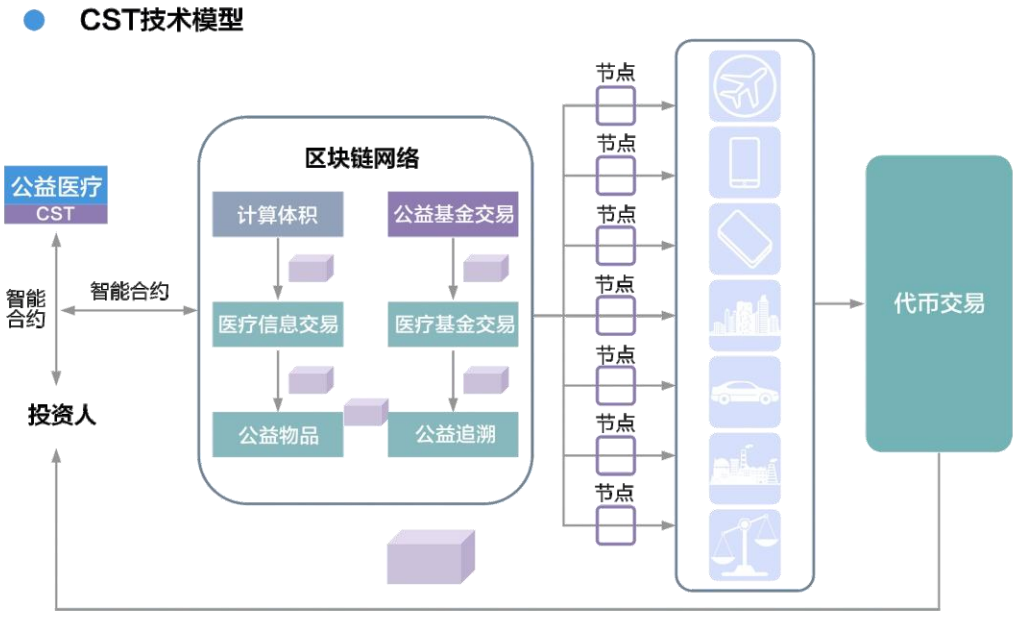
3、CST安全防篡改系统

CST把安全贯穿整个系统中， 安全是系统基石， 比如： 系统安全问题， 平台健壮性、资料安全保护、Token 安全等。 骇客一般都是发现软体缺陷进行恶意的达到自己目的，严格把控代码品质， 避免系统中代码中的缺陷， 专门设置代码评审评估部门， 部门由一线顶级公司成员组成。保证系统中的每行代码安全可信的。 使用者资料通过差分隐私进行安全保护， 差分隐私是统计资料库安全防范的典型策略， 广泛应用于隐私保护资料发布、挖掘等领域。它的工作原理， 简单点讲类似于“ 欲盖弥彰” ， 对资料库进行随机变化、资料杂讯等修饰， 在不影响总体输出的前提下对个体的资讯进行掩饰， 这样回馈出带有错误资讯的结果，从而达到保护隐私。

4、CST应用技术模型与优势

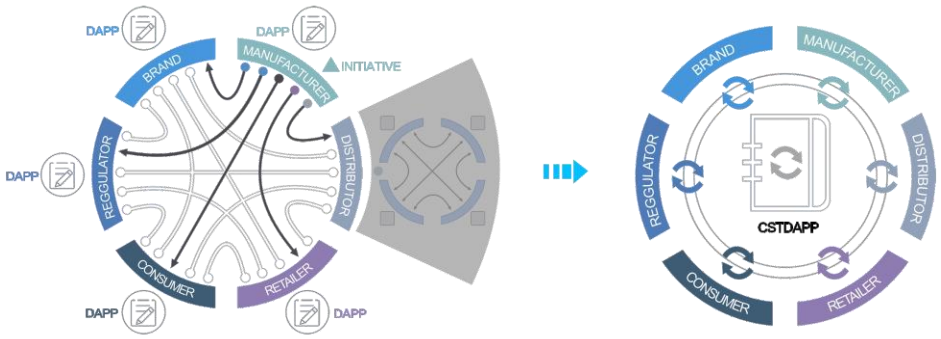
（1）国际化团队：CST的核心人员均来自原以太坊开发团队，同时曾任职Google，微软，IBM，亚马逊等全球知名公司的核心高管， 拥有全球化的视野， 可以帮助CST上的开发者搭建出更具有国际性的商业DAPP。团队多年深耕区块链领域， 更了解应该改进的方向和开发者真正的需求。

（2）安全性高：CST较以太坊在合约安全性上进行了升级和优化， 合约的接口均进行过防Dos攻击， 随机数验证， 防篡改技术验证等压力测试， 开发者可直接使用， 保障安全。



（3）不可篡改， 可追溯： 单个甚至多个节点对数据库的修改无法影响其它节点的数据库，除非整个网络超过51 %的节点同意。区块链上每一笔和以太坊的双向交易都采用密码学原理，使智能合约的每次交互全程追踪， 可追溯， 保证公平安全。

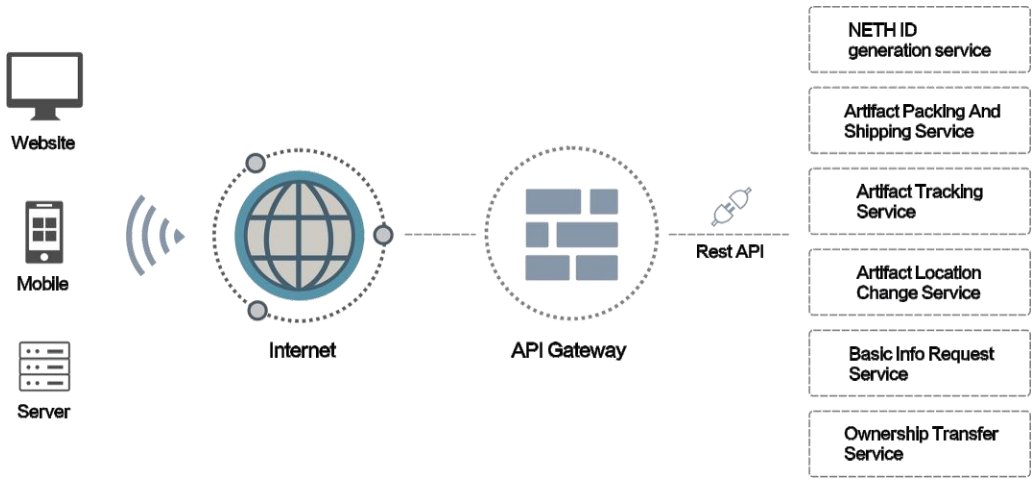
（4）更广泛的用户群体：CST不仅在区块链领域深耕多年， 在传统互联网、移动互联网领域同样拥有多款全球化的商业应用， CST将互联网的用户整合、 裂变， 通过CST将DAPP上链后可实现无国界的全球推广， 带来极致的用户体验和更广泛的用户群体。



（5））打通线上线下金融： 以区块链为核心战略， 以CST token为支付应用， 构建出全球首个基于区块链的去中心化金融， 真正实现金融平等、资产透明、达到用“ 价值” 连接一切的商业生态圈。

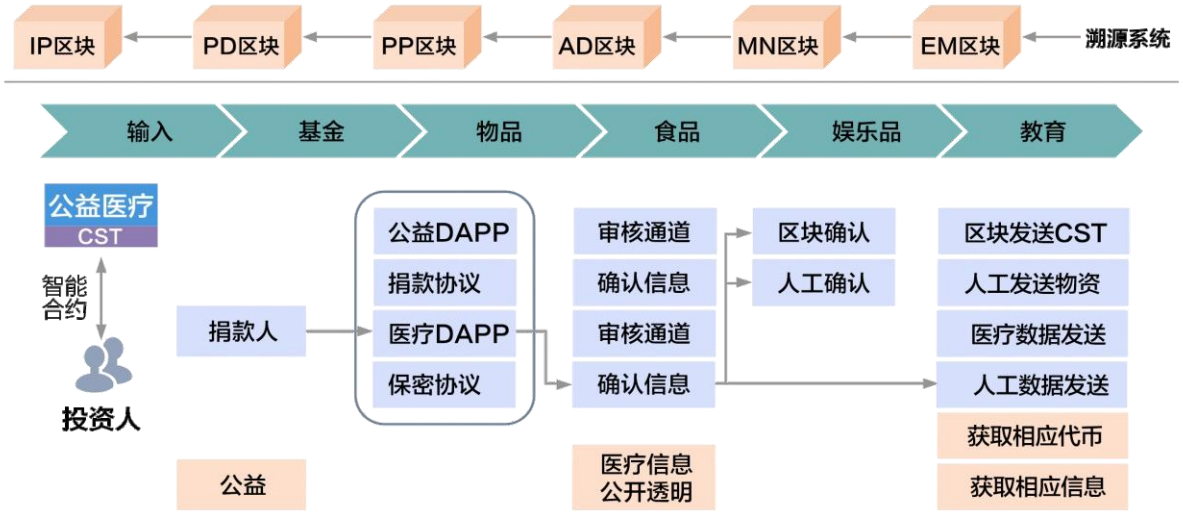
5 5、CST公益溯源生态体系

CST平台的SDK使创作复杂的溯源生态变得轻而易举。 它旨在允许独特的新支付构架可以减少会计工作增加商家和客户之间的信任。建立自己的定制网关构建类似 PayPal 网关所需的所有后端功能都将包含在平台SDK中。 作为提供商您可以通过基于开源代码和SDK中提供的示例实现自己所需的功能如购物车、网络发票、电子邮件 / 短信通知、退款等。



CST项目生态

CST是基于区块链技术所创立的一个全球领先公益溯源平台， 首先用于国际公益事业， 其性质是开放的、可信的、独立的。CST平台的运营机制中参与角色众多， 有政府及监管机构和各个部委， 行业中的大型企业机构， 公共媒体， 以及广大的消费者， 通过很多方面的角色参与， 形成多方制衡， 避免数据腐败和数据造假。



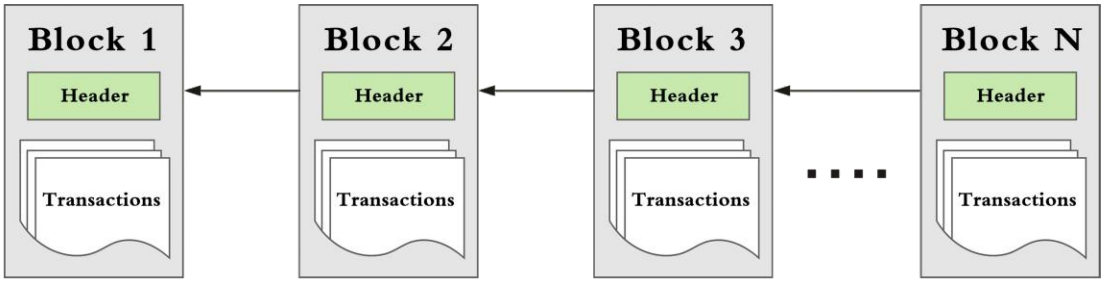
4 1、 去中心化的资产交易平台

CST坚持“ 以投资者利益为核心”的运营理念， 真正做到从投资者利益出发， 并根据已经取得实际成果的数字资产分析评估模型对现有的区块链资产进行详尽分析， 力求最大限度的排除非系统性风险。 科学、 有效、务实的为参与者提供优质区块链资产交易场所， 让源头把控并保障参与者的核心利益。

肆

CST商业应用

同时CST所开发的APP具备物资采买功能， 捐赠人可通过CST购买APP内相应物资， 并自动对接区块链交易中心， 使得够买的物资通过区块链公信系统自动完成交易并运送到有需要的用户手里，这将避免物资被随意买卖， 等不公信行为。

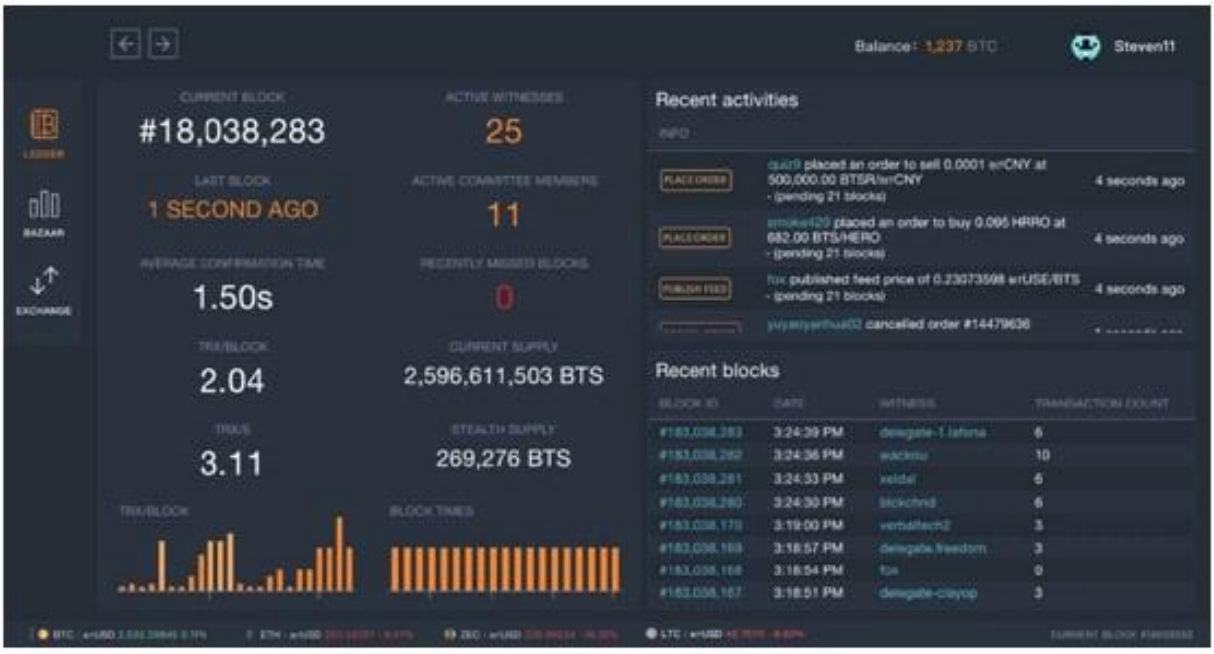


国际化专业平台介绍

1 ．支持中英日界面， 由各国爱好区块链的Native进行翻译优化， 提供原汁原味的界面用语。

2 ．不止平台界面，CST还提供中英日的咨询服务， 方便三国投资者。

3 ．将来还会支持全球任意国家等更多区块链活跃的用户。

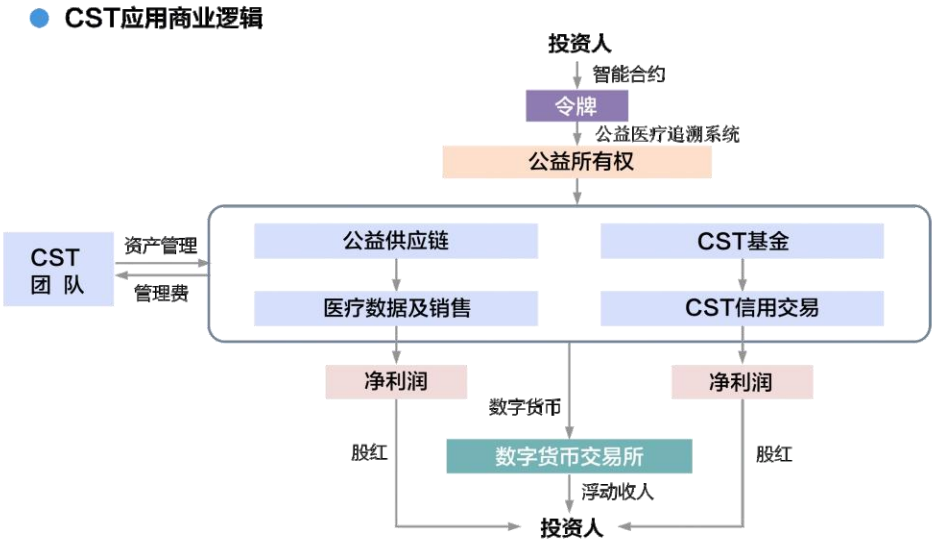


2 、CST兑换CSC稳定基金

CSC价值将牟定人民币 1：1 兑换， 并在24小时内将捐赠的CST兑换成CSC，以防止捐赠人资产因行情波动受到损失， 除CST以外， 捐赠人捐赠的如（ 比特币， 以太坊） 等主流货币也将统一兑换成CSC， CSC不仅成为了数字货币波动下的避险工具， 同时会在不久的将来奠定结算币老大的地位， 并会在各交易所形成了网络效应。

3、 公益溯源系统应用

CST是基于区块链、物联网技术所创立的一个全球领先溯源区块链平台， 主要应用于全球公益事业， 并在全球众多国家进行试点活动， 用户可以通过CST购买各种物资并统一上传到区块链系统中， 每一件上传的物品都将得到区块链的唯一认证且无法被篡改。相关款项将完全用户公益事业，实现真正意义上的公平， 公正， 公开。



4、 AI智能医生

AI 超能医生是CST中智慧诊断核心模组， 实现基于区块链网路的分散式AI超能医生， 遵循共识机制， 接入智慧 CT 辅助诊断、智慧糖网分级筛查、智慧医疗单据识别等核心模组， 整个网路具有自学习功能， 网路中的 AI 超能医生能够进行主动学习自我强化，实现分散式线上增量学习。 AI 超能医生集成了大量的智慧医疗 DAPP，它以CST底层协定为公共标准， 每个 DAPP 都可以自订自己的系统架构。

5、 全球支付的闪电网络

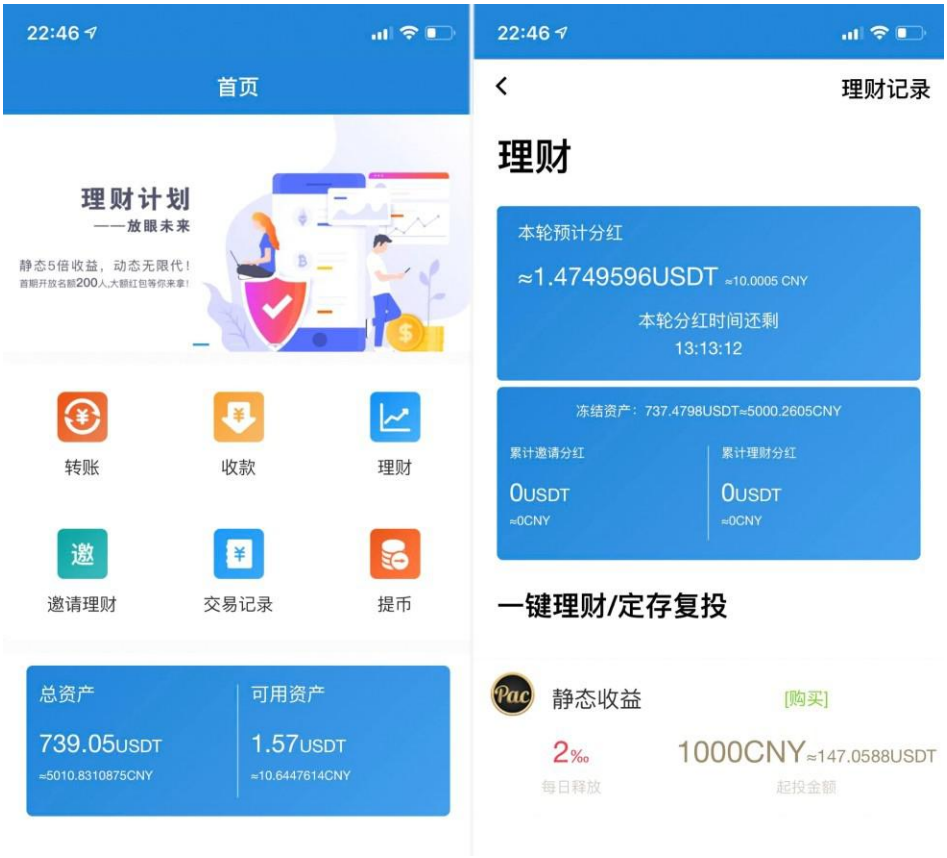
CST 是一种完全去中心化的数字货币支付落地解决方案 ， 具有支持小微支付、即时到账、手续费极低等优势。业务模型为基于BOLT协议实现了自己的「 复合决策闪电网络」， 通过上层决策网络匹配支付请求和法币兑换请求， 再由下层闪电网络建立高效、安全的支付通路， 最终通过各地支付收单方完成与商户的法币结算。 由于法币提供的模式类似于P2P代付， 全过程无任何中心化机构参与， 避免了由于Visa等卡组织停止合作而导致的商业模式崩溃， 另一方面， 上层网络的激励策略可以有效避免闪电网络的中心化倾向。

6、 慈善义卖大咖见面会

CST每天将举行大小不等的慈善活动， 其中最引人瞩目的当属义卖， 活动吸引各行业著名企业家及大咖前来助阵和义卖珍贵物品。在义卖活动中有各个合作单位， 平台捐赠的商品售卖，其得到的款项都将用于公益事业的发展。

7、 云安年化基金

英国云安集团有限公司“UK UNIVERSE GROUP CO. LTD ”位于英国开曼群岛， 是一个集社会公益， 干细胞疗法， 房地产(东南亚地区）， 游戏开发， 新型互联网+， 数字资产交易所为一体的集团公司， 而旗下的CST是全球首个将区块链技术用于干细胞存储和基因存储的数字货币， 并于不久的将来将打造全球的基因公有链， 届时， 比特币， 以太坊等国际主流货币将和CST自由流通结算， 通过CST的各种场景应用和线上转换， 线下体验， 使流量增值变现！CST团队将通过全球N个节点和每个国家的超级节点实现程序化高频交易及衍生品程序化交易， 实现资本复制， 给CST的投资者带来高额的回报！

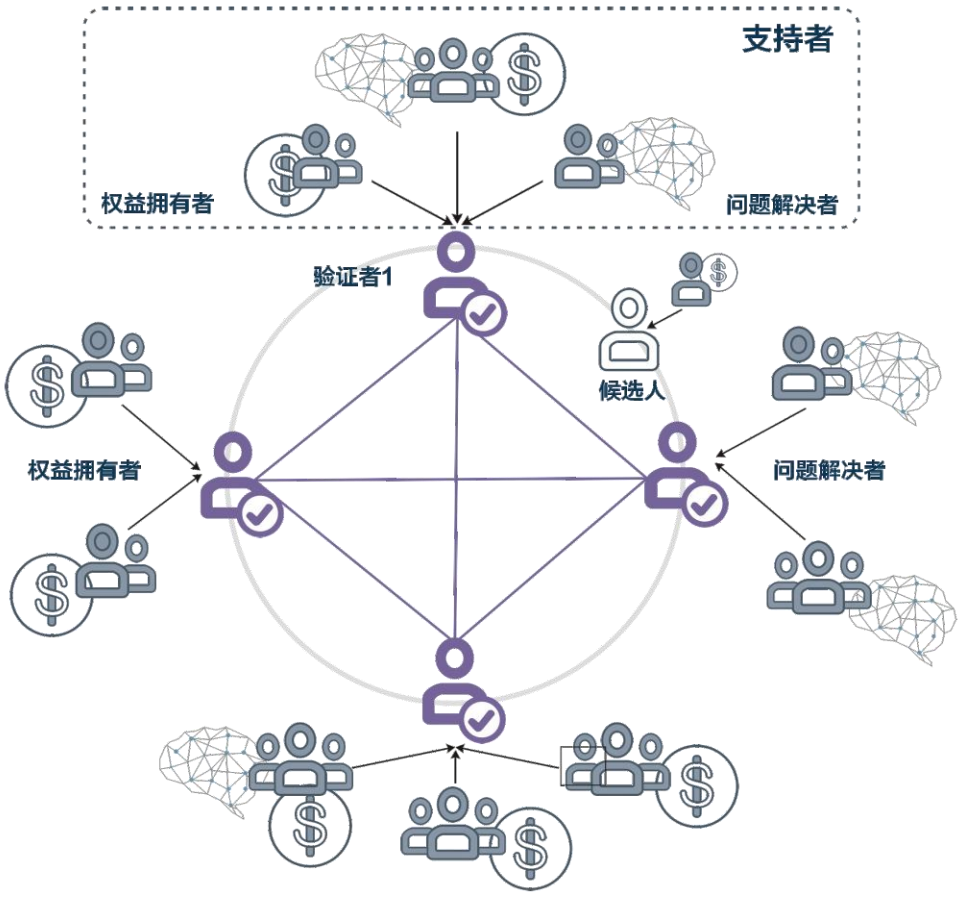


凡是拥有CST通证的用户， 都将拥有下载CST理财app进行理财的特权，2010年比特币价值一元钱， 截止到2018年比特币以突破12万元， 第一批购入比特币的用户以赚取10万倍的利润。就在去年CST作为总冠名方， 组织了世界区块链大会， 又一次证明其未来价值。理财APP作为CST第一个落地项目。势必在未来上交易所的同时， 迎来大规模的疯抢，CST的价值也会随之不断升高， 作为第一批投资者的用户， 也将获得第一个吃螃蟹的机会。

8、 节点商业竞选

CST每一个持币者都有参与社区共建的权利， 可以选择用自己手中的CST选出要采购的供应企业的物资、医疗设备。同时CST将对于每个参与投票的用户做出奖励， 真正做到社区的可持续发展共建。CST平台将

用“ 节点运营商投票” 模式替换原“ 垄断采购” 模式。全体已激活节点运营商权限的用户均拥有投票采购权限， 做到资金账目透明化， 参与CST抢购可提高上限；



1、企业商可直接对应平台需要采购的物资与设备， 提交资料申请；CST所有社区节点用户参与资料考核并投票， 选出票数最高的企业供应商， 确保其真实性与合法性， 做到真正的公开透明化。

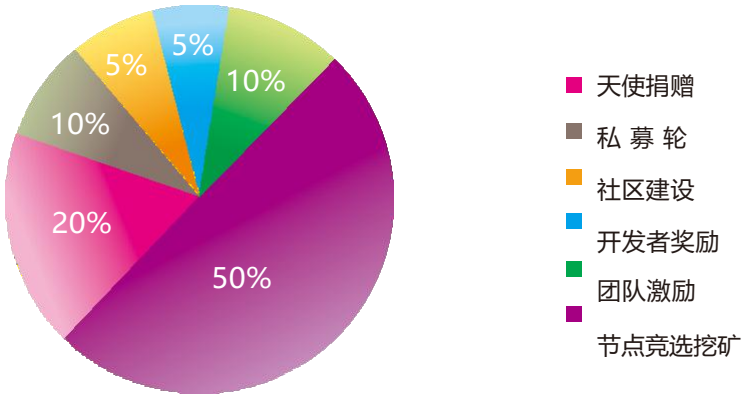
2、对于平台暂未收录的企业， 可选择参与“ 物资医疗设备捐赠”， 参与企业上链在CST全球节点进行广播宣传提高其供应商知名度。

1、CST分配计划

伍 CST项目规划

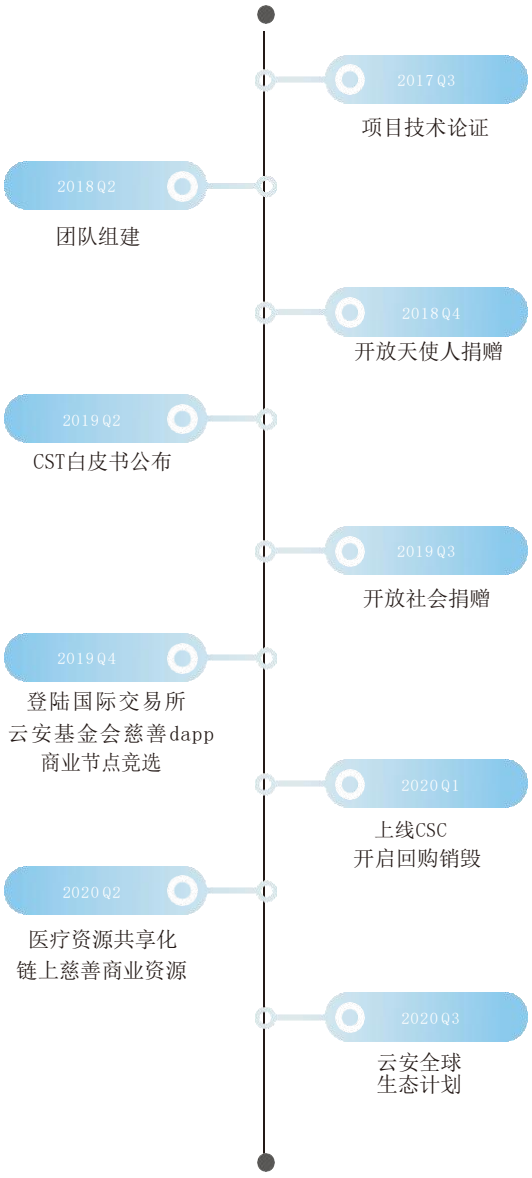
为了激励生态建设者与参与者， 云安基金发行生态通用原生 TOKEN（通证）， 用来实现项目内的奖励制度以及各方利益的分配。使整个系统中的交易更加方便、透明并可以通过智能合约实现自动执行、监管等功能， 保证了交易在没有第三方担保情况下的公平与公正。

CST的初始总量 1,000,000,000



分配比例	数量	用途
20%	200000000 CST	1/2019天使捐赠轮，锁仓90%，每六个月释放一次10%
10%	100000000 CST	9/2019社会捐赠轮，季度释放，每三个月释放一次10%
5%	50000000 CST	社区建设，5年制，用于空投奖励每年最大1000万
5%	50000000 CST	开发者奖励，每五年释放一次2500万
10%	100000000 CST	团队激励，锁仓100%，每五年释放一次5000万
50%	500000000 CST	节点竞选挖矿，持有CST参与节点竞选

2、未来发展规划



2、战略合作伙伴

Coinbase，比特币公司。2015年1月21日上午， 据美国《财富》报道， 比特币公司Coinbase C轮融资7500万美元， 比特币公司Coinbase创建的美国第一家持有正规牌照的比

币交易所。2017年1月17日， 纽约金融服务部门(NYDFS)负责人宣布， 已通过比特币交易平台Coinbase的牌照申请， 这意味着Coinbase在美国纽约州的经营终于获得了官方认证。2018年3月6日，Coinbase宣布推出首支指数基金， 进军资产管理行业。

英国保诚集团在1848年创立， 英国保诚保险成立后， 业务迅速发展，1890年初， 便成为了英国最大的人寿保险公司， 为英国人民提供周全的保障， 至今仍傲踞榜首。

Mythical Games公司成立于今年四月， 五位联合创始人分别是Cameron Thacker、Chris Downs、Jamie Jackson、John Linden和Stephan Cunningham，他们均来自于暴雪、Activision、以及雅虎等知名游戏公司和互联网公司。目前， 该公司在西雅图和洛杉矶两地设有办事处。

Struck Capital为创新型企业家提供种子阶段资本和专门知识。

洛杉矶的下一代种子风险投资公司。“ 冲击资本” 由千禧一代领导， 他们吸引年轻的创始人提供核心技术创新， 以解决世界上最大的问题。我们的目标是成为企业家最具协作性、有效性、支持性和长期性的合作伙伴。

Token Daily是一个由令牌创始人、开发者、投资者和形形色色的人组成的社区， 他们发现并讨论所有事物的最新秘密。以象征性的发布、白皮书、代币注册、学习资源、项目合作等为特色。

Algorand由密码学先驱和图灵奖获得者Silvio Micali创立， 以提供分散、可伸缩性和安全性的平台来解决“ 阻塞链三重体” 问题。阿尔戈兰为现有企业和新项目提供了一个基础， 以便在新兴的权力下放经济中在全球范围内运作。Algorand的第一个类型， 无授权， 纯粹的证明利害关系的协议支持规模， 开放参与， 和交易最终需要为数十亿用户

3、项目团队成员

首席执行官/Loi Luu

kyber网络的ceo/共同创始人，kyber网络是一种链上流动性协议， 为分散式应用程序提供动力， 包括交换、基金、贷款协议、支付钱包等等。我也研究加密货币， 智能契约安全和分布式共识算法。我的研究主要集中在加密货币的几个问题上， 从提高安全性到提高公用加密货币的可扩展性和可用性。

首席顾问/Mervyn Chng

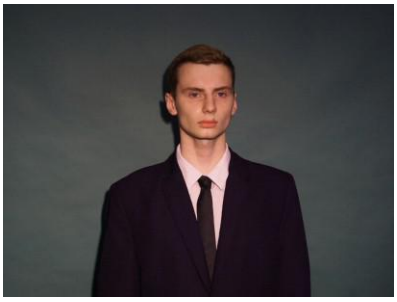
MW Partners Group合伙人， 区块链项目咨询(Loomx的基石顾问)。 专注于ICO前期/后期咨询工作， 为项目获得曝光和影响力， 并将项目与能够增值的个人/公司(如我们的子公司)联系起来。之前从业于大型风险投资基金。

Alex Batlin | 硕士 MBA

项目团队 CMO，Charlie Shrem是比特币早期开发者也是荷兰联合银行UBS区块链创始实验室负责人他担任的是金融初创公司Level 39的导师职位，并在探索分布式账本和加密货币领域有极高的地

Silvio Micali | 博士

项目团队 CTO,毕业于麻省理工大学计算机 科学和人工智能实验室任职图灵奖得主、北美区块链协会高级研究员，2013 年开始关注和研究区块链技术，10 年以上 软件开发经验， 分布式网络安全专



David Johnston | 博士

曾在 ArizonaStateUniversi AT Chain 学习工程学， 曾与包括高通（Qualcomm） 在内的大型跨国公司合作。

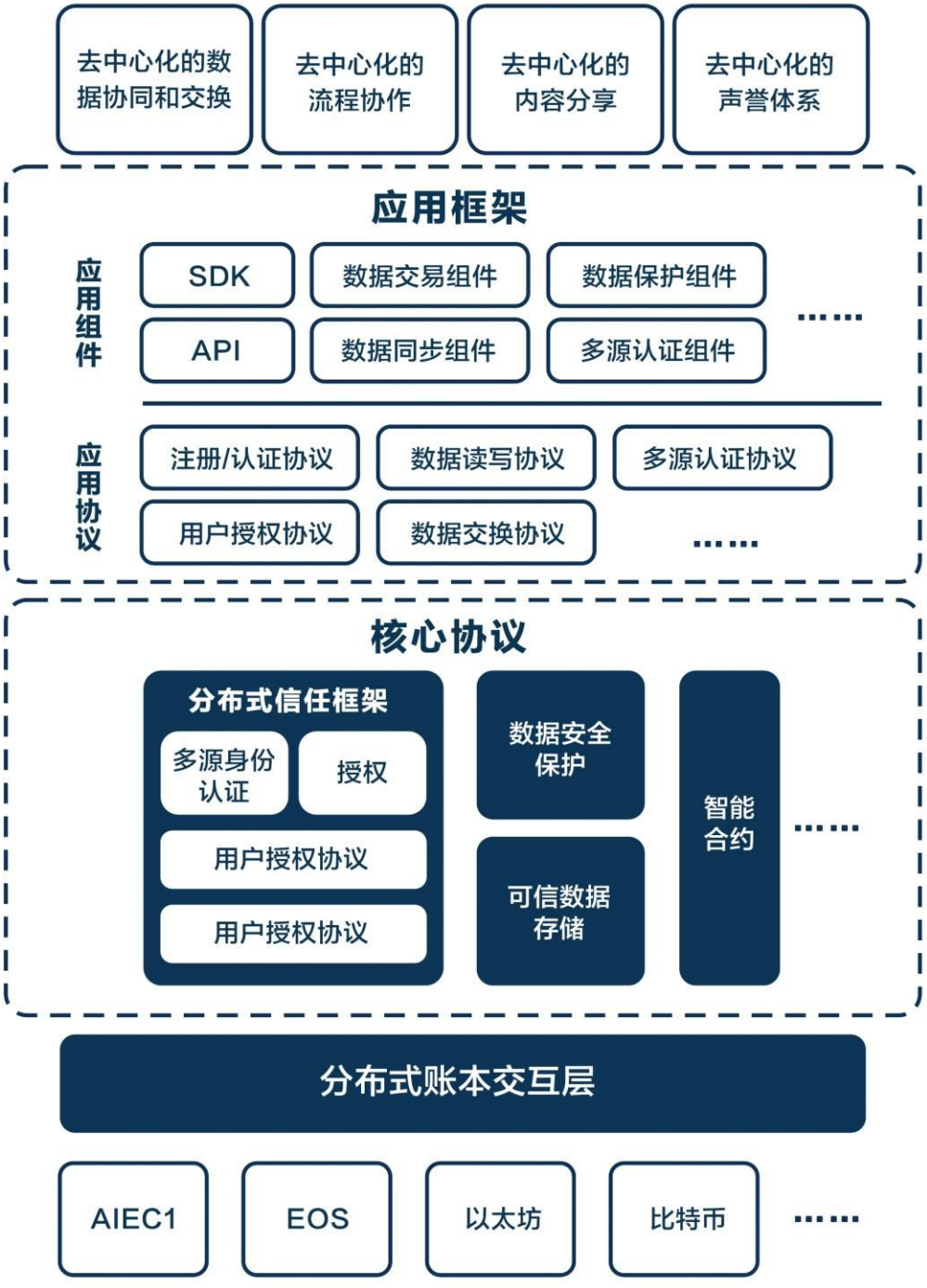
海外推广/Paulina Shafir

通过策划和执行病毒宣传活动， 建立社区， 以及为技术、区块链和视频游戏行业的公司采用传统营销和现代数字战略相结合， 对区块链，daps，加密游戏，fentnite，广播电视/广播， 纪录片制作和报道有丰富经验。

陆

CST技术架构

CST系统架构概况



6.1.1 P2P移动存储层

为了做到消息可以被传播并且系统具有去中心化的特性，CST系统利用分布式移动元数据管理系统（M3 或 M Cube）来管理节点信用值和区块链上的凭证。M3使用分布式散列表（如Chord [17]，Kademlia [18]） 协 议来管理分布式管理器中的节点。

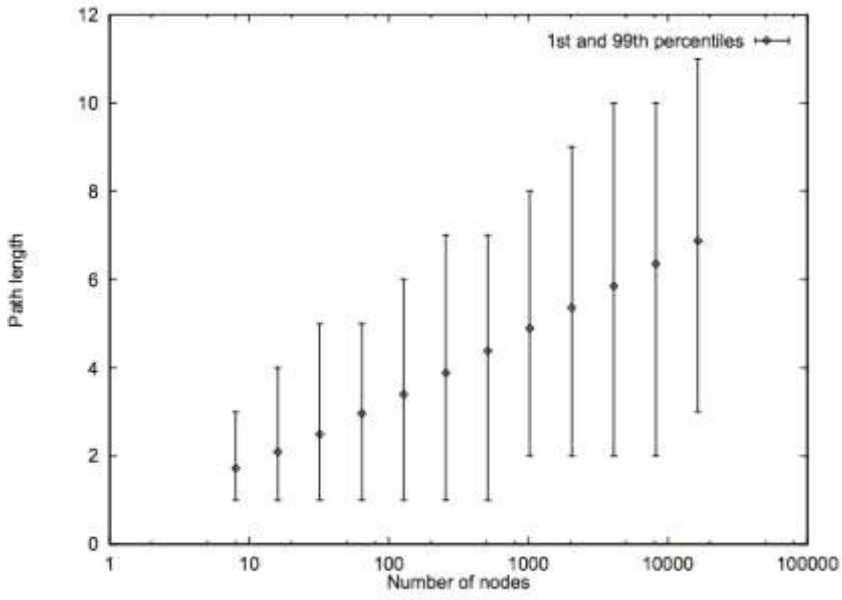


图4.1 节点的可伸缩性

6.1.2 区块链层

CST共识算法基于 Tendermint [11] 共识引擎， 本质上为具备高可扩展性的Casper机制。我们将基于Tendermint 的相耦合的以太坊项目Ether Mint【12】进行定制化研发， 一方面可以实现对于以太坊智能合约等上层应用的平滑过度， 另一方面保证了底层公链的松耦合结构，实现模块的清晰化设计。

6.1.2 信用管理

CST通过人工智能（AI） 来计算用户的信用值， 信用值可以反映用户的可信性和可靠性。CSTH同时接受来自同行的合作评级来评估广告主的可靠性。为了保证同行对信用值评估的一致性，我们将通过用户私钥对评级和行为进行加密， 并将其记录在区块链中。CST将通过SDK发布基于行为日志的AI 评估模型， 同行可以使用该模型来验证信用值。

6.2 2、安全防篡改系统

由于 CST 通过预言机在行为日志基础上来计算用户的信用值， 我们需要防止并降低恶意节点伪造行为日志篡改系统。首先， 当用户生产至少一个月有效行为日志才能被授予用户令牌，行为日志是否有限将通过 AI 模型进行验证。该策略可以防止恶意节点生成或者改变组设备ID。第二， 在将令牌授予用户之前， 链上数据可以通过比对CST管理平台
（DMP）的数据来检查行为数据和日志是否有效。

为开发者提供 ABCI（ 区块链应用程序接口） 组件。本身作为共识层实现 p2p 网络以及 Casper共识， 同时提供了应用程序接口组件。ABCI 是具体的逻辑处理层， 保证交易可以通过任何一种编程语言进行处理（ Golang, JS），并且在这一层实现交易的验证处理以及查询等操作。 对于开发者来说， ABCI 提供了友好的可定制化应用开发环境。Blockchain CST Foundation | 26DECENTRALIZED AI-POWERED TRUST ALLIANCE。

6 3、Sharding分片和Casper技术

原以太坊的这种分片方式是通过把一个单独的共识划分成许多子共识， 从而缓解系统压力，达到提升性能的作用。但实际上当一个整体的共识被分割成许多的子共识的时候， 这些被分开的子共识就会变得更容易被攻击， 牺牲掉很大的安全性或者叫真正的“ 共识”。当然也可以增加随机性等方式来复杂化路由路径， 但这种方式并不能从根本上解决被攻击的可能性， 同时还限制了挖矿节点的专门化。

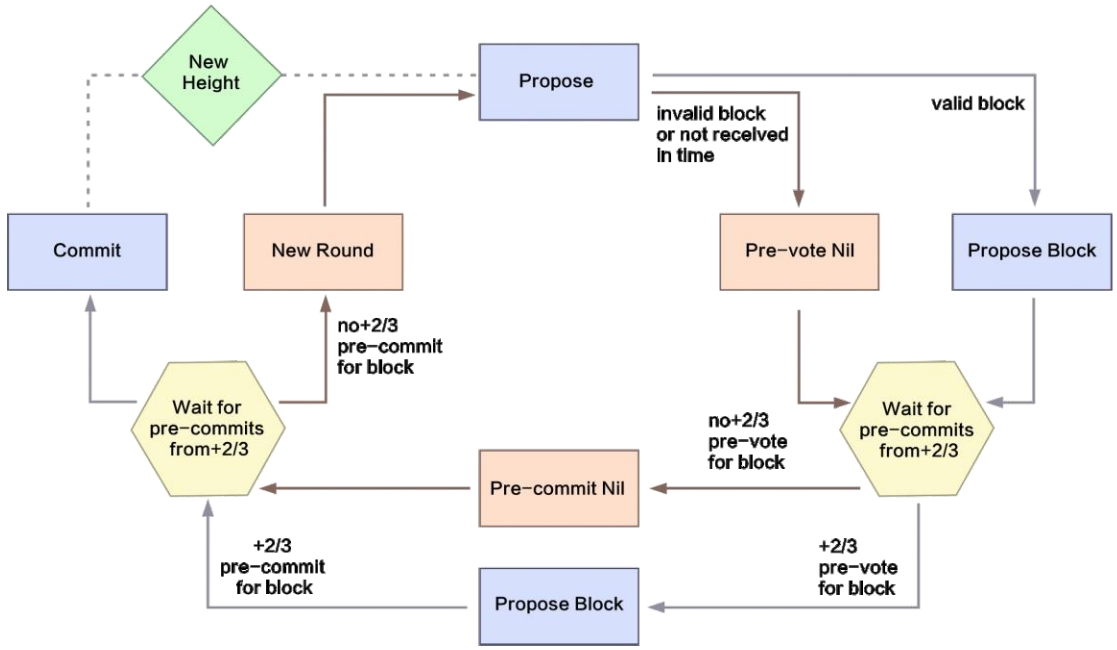
随着产业的不断升级， 现在很多的矿池都使用专门的记账系统， 这种方式逐步取代POW的挖矿节点， 使得这些节点的数量急剧减少。这些矿池能保证挖矿效率和交易的即时广播、减缓区块链的分叉， 很多的矿池也已经抛弃了官方的软件， 转而通过负载均衡和并行运行智能合约来聚集算力， 并且在全球部署节点来提高广播的效率。但是， 矿池整体的效率还是受到内部技术差别的限制， 以及每个节点的设计和协议本身的限制。所以升级某个节点， 或者某部分节点， 并不能给整个网络带来提升。

CST针对原以太坊Sharding分片技术的问题就行升级， 让提供标准服务的节点开源， 并通过Casper来达成主链上的共识。由于挖矿节点由利益相关方投票产生， 所以被委托的挖矿节点会在最大程度上保护侧链， 并且还能分享主链的强共识。这种方式会在一定程度上增加每个节点的压力， 但是效率会随着更多侧链的加入而提高， 因为被委托的挖矿节点能在集群上运行。

Casper共识

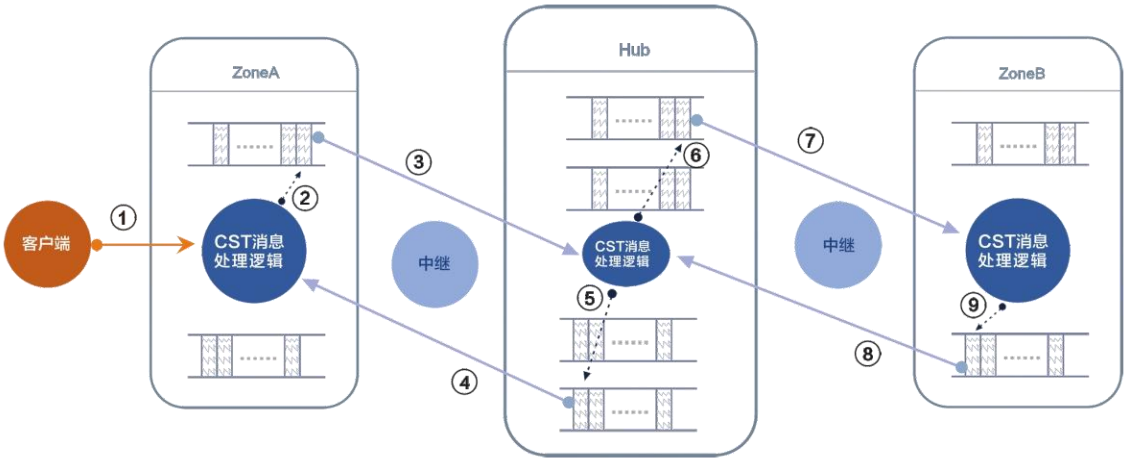
Casper是由POS衍生出来的一种共识机制， 其与POS的区别为Casper的共识按块来达成而非Pos按链来达成。而以太坊所谓会从Pow转向Pos其实是转向Casper共识， 但原以太坊因核心技术社区人员意见未达成一致， 共识机制迟迟没有更新，CST是目前所有区块链项目中最先使用Casper共识的侧链， 并且已取得了初步成果， 不仅兼容了以太坊， 同时已经在CST侧链上实现了完美运行。

Casper中达成共识包含两个活动：1， 出块；2，投注.在执行这两个活动之前的必要条件是每个验证节点已经缴纳足够的保证金。保证金在这里起到的作用之一为防止恶意节点攻击网络（ 此外， 由于出块节点的收敛， 系统吞吐量也必然会有提升）， 因此Casper有一个必备条款： 如果你有两次投注序号一样， 或者说你提交了一个无法让Casper合约处理的投注， 你将失去所有保证金。从这一点我们可以看出，Casper与传统的PoS不同的是Casper有奖惩机制， 这样非法节点通过恶意攻击网络不仅得不到交易费， 而且还面临着保证金被没收的风险。



4 分层网络结构

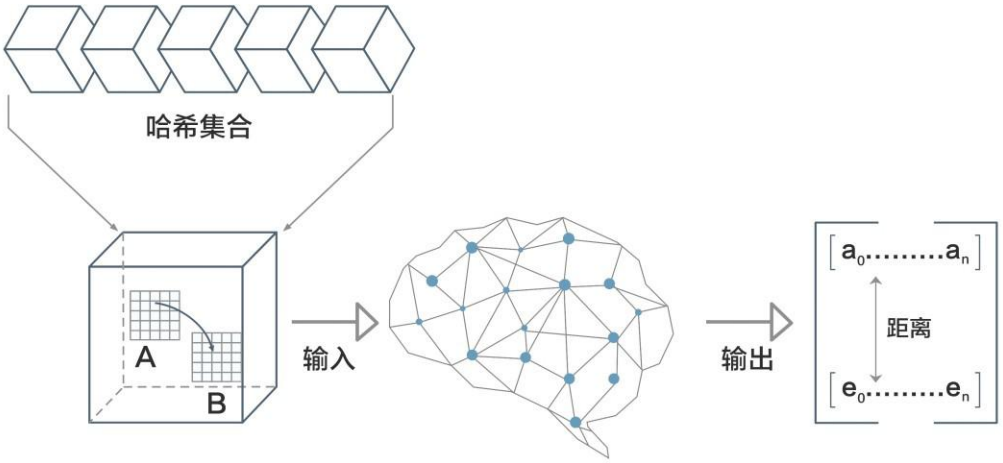
CST网络的枢纽及各个分区可以通过区块链间通信（IBC）协议进行通信， 这种协议就是针对区块链的虚拟用户数据报协议（UDP）或者传输控制协议（TCP）。



客户端想要发起一个A到B的代币转移， 消息到A处，A对消息进行处理， 然后通过中继传递到Hub空间， 在Hub空间进行处理之后通过中继传递到B，反之也是一样。通过 IBC 代币可以安全、快速地从一个分区转到其他分区， 而无需在两个分区之间拥具有汇兑流动性。相反， 所有跨分区的代币转移都会通过 CST枢纽， 以此来追踪记录每个分区持有代币的总量。这个枢纽会将每个分区与其他故障分区隔离开。因为每个人都可以将新的分区连接到 CST 枢纽， 所以分区将可以向后兼容新的区块链技术，IBC协议层的添加， 将兼容不同区块链之间的通信协议和资产交换， 为跨链实现可能。

5 5、PBFT和XO算法

PBFT意为实用拜占庭容错算法， 这个算法是卡斯特罗和利斯科夫在1999年提出来的。解决了原始拜占庭容错算法效率不高的问题， 将算法复杂度有指数级降低到多项式级， 使得拜占庭容错算法在实际系统应用中变得可行。使用拜占庭容错算法主要应用于央行的数字货币以及步萌区块链。PBFT是一种状态机制副本复制算法， 即服务作为状态机进行建模。状态及在分布式系统不同节点进行副本复制，CST在PBFT算法的基础上还引入了XO算法， 从而和PBFT算法进行互补， 既优化了社区治理结构， 又提高了CST网络的安全性。



每个状态机的副本都保存了服务的状态， 同时也实现了服务的操作。将所有的副本组成的集合使用大写字母R表示。使用0到R-1的整数表示每一个副本。为了描述方便， 假设R=3f+1。这里的f是有可能失效的副本的最大个数。尽管可能存在多于3f+1个副本。但是额外的副本出来降低性能之外不能提高可靠性。

6 6、扩容方案

以太坊区块的平均大小为21345Bytes，约为0.02M（ 平均出块时间为15秒）。比特币的转帐交易是统一格式， 可以用固定的区块大小来规范。以太坊则不同，V神（ 以太坊的创立者） 将区块链视为世界计算机， 在比特币基础上， 以太坊实现了智能合约， 这就意味着，除了和比特币有同样的转帐功能外， 以太坊网络中更多的是要为大量程序提供运算服务， 但目前以太坊因区块太小， 每秒只能完成最多20笔的交易， 根本无法运行大规模的DAPP，所以到目前为止以太坊上也没有真正的全球化的DAPP。

CST在以太坊架构的基础上， 在保证稳定性和安全性的前提下， 将CST的区块扩容到8M，同时兼容了EVM预言机， 使承载全球用户使用CST的集群级DAPP的搭建和运行提供了可能。

免责声明

本白皮书仅作为传达信息之用， 文档内容仅供参考， 不构成出售数字商品、 股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的 形式进行， 且须符合相关的证券法律和其他法律。本文档内容不得被解释为强迫参与互换。任何与本白皮书相关的行为均不得视为参与互换， 包括要求获取本白皮书的副本或向他人分享本白皮书。参与互换则代表参与者已达到年龄标准， 具备完整的民事行为能力， 与CST基金会签订的合同是真实有效的。所有参与者均为自愿签订合同， 并在签订合同之前对CST进行了清晰必要的了解。

CST基金会将不断进行合理尝试， 确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新， 包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，CST基金会将通过在网站上发布公告或新版白皮书等方式， 将更新内容公布于众。请参与者务必及时获取最新版白皮书， 并根据更新内容及时调整自己的决策。CST基金会概不承担参与者因：(i)依赖本文档内容、(ii)本文信息不准确之处， 以及(iii)本文导致的任何行为而造成的损失。CST基金会将不遗余力实现文档中所提及的目标， 然而基于不可抗力的存在，CST基金会不能完全做出完成承诺。

CST是平台发生效能的重要工具， 并不是一种投资品。拥有CST不代表授予其拥有者对CST平台的所有权、控制权、决策权。CST作为一种加密代币不属于以下类别：(a)任何种类的货币；(b)证券；(c)法律实体的股权；(d)股票、债 券、票据、认股权证、证书或其他授予任何权利的文书。

CST的增值与否取决于市场规律以及应用落地后的需求， 其可能不具备任何价值， CST基金会不对其增值做出承诺， 并对其因价值增减所造成的后果概不负责。在适用法律允许的最大范围内， 对因参与互换所产生的损害及风险， 包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，CST基金会不承担责任。

免责声明

截止到本白皮书发布日，CST仍在开发阶段， 其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了CST最新的关键信息， 其并不绝对完整， 且仍会被CST基金会为了特定目的而不时进行调整和更新。CST基金会无能力且无义务随时告知参与者CST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)， 因此必然会让持有者未能及时且充分地接触到CST开发中新产生的信息。信息披露的充分是可避免且合乎情理的。

CST平台遵守任何有利于行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时， 参与者披露用以完成此类检查的所有信息必须完整准确。CST平台明确向参与者传达了可能的风险， 参与者一旦参与互换， 代表其已确认理解并认可细则中的各项条款说明， 接受本平台的潜在风险， 后果自担。


cTs