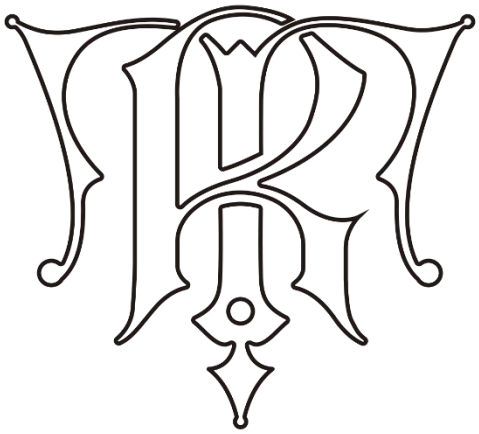
Rivet Chain

Year
2019



R T C

协议白皮书

Agreement Whitepaper

目录

1

引言

Rivet Chain

引言

区块链的诞生，为世界找到了前进的方向，共识系统产生被动信任，形成了不可篡改的共识机制。近来，对分布式共识系统的兴趣和研究显著增加，重心在于分布式的支付网络。这种架构允许快速，低成本的交易，不受中心化的控制。

开源的生态体系、去中心化的资源共享、以及加密的货币，这一系列技术的出现启发了人们，去中心化的互联网协议有潜力改善社会经济的基础框架。例如 Bitcoin、Ripple 等加密货币，以及 Ethereum 这样的开源智能合约平台，还有许多基于 EVM (Ethereum 虚拟机)和 TVM 开发的分布式应用，例如 NEST（金融平台）和 Augur（预言）。

而这里开始提到的 Rivet Chain，是基于 RTSP 协议开发，优化了 Ethereum 现有的不足，一个崭新的区块链网络系统。

Rivet Chain 不是一个单一的区块链系统，而是一个基于区块链的多项研究成果的整合。Rivet Chain 所做的是专注于开发一系列新的方法来帮助不同项目相互交流，在分布式节点上建设一个崭新的区块链互联网。

Rivet Chain 允许其他独立的区块链相互沟通和交易，并提供可拓展性解决方案——包括全新的共识机制。本文将从基本信息和技术原理层面，讨论 Rivet Chain 的相关工作。

2

概述

问题

目前的所有区块链已经涌现了许多不足，涵盖总体能效低下，性能不良或受到限制和缺乏成熟的管理机制。

虽然区块链的优势和缺点值得研究，但这里关注的是分布式支付系统必须会遇到的挑战。

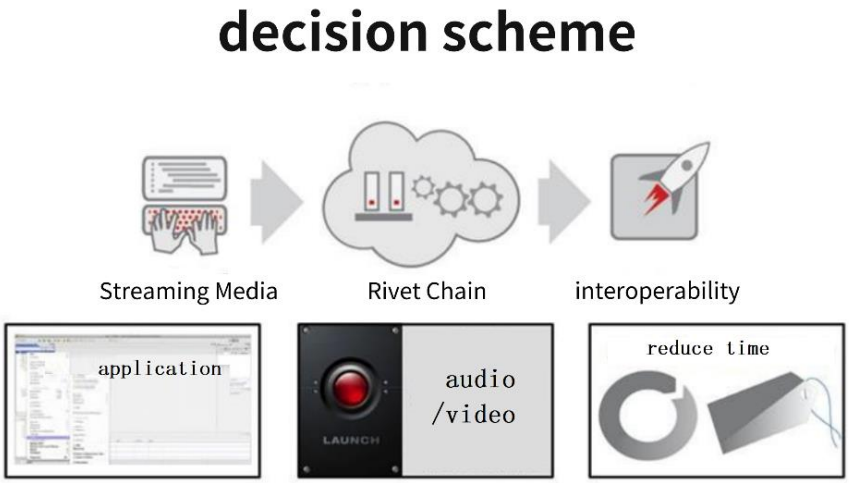
许多当下的问题其实早在许多年之前就已经被探讨过了， 比如“拜占庭将军问题”。分布式支付架构必须在遇到常规 BUG 和 “拜占庭式”BUG 时依然稳定，这些 BUG 可能因系统中的多个来源产生。

为了扩大交易吞吐量，过去的许多人已经开发了许多诸如 Segregated-Witness 和新思路的可拓展协议这样的解决方案，但这些垂直拓展解决方案仍然受到单一物理机容量的限制，以确保完整的可审计性。闪电网络能够通过部分交易完全记录在主链账本外来拓展交易容量，这种方法十分适用于小型支付和匿名保护支付通道，但是无法适用于更普适的拓展需求。

在传统区块链应用中，往往将所有交易都发送到主网，一方面增加了成本，另一方面也使得网络拥堵大大提高。在以往 Ethereum 上发生过好几次类似情况，比如我们熟知的 FOMO 3D 等。

现有区块链网络中存在大量中心化、共享不充分、交易费用昂贵等问题。这样的问题同时也导致了音频和视频这样流媒体上链相对拥堵，很难实现实时流媒体的上链。

理想的解决方案是允许多个并行的区块链交互操作的同时保持其安全特性，并具备优秀的流媒体传输能力及信息承载能力。事实证明，采用以往的证明方式很难做到这一点，但也并非不可能。例如合并挖矿，允许在工作完成的同时，确保主链在附属链上被重复使用，但交易必须通过每个节点依次进行验证，而且如果母链上的大多数哈希算力没有积极地对子链进行合并挖矿，那么就容易遭到攻击。我们会在创新工作中对其他技术和缺陷进行概括。



Rivet Chain 概述

Rivet Chain 是一个全新的区块链网络架构，能够解决这些问题。Rivet Chain 是由许多不同空间的独立区块链组成的网络。空间在 Rivet BFT 的支持下运行，Rivet BFT 是一个类拜占庭容错安全共识引擎，具有高性能、一致性的特性，并且在严格的分叉追责 机制下能够制止恶意破坏者的行为。Rivet BFT 的拜占庭容错共识算法十分适合用于 PoW+PoS 机制下的公共区块链。使用其他共识模型的区块链，包括类似基于权益证明(PoS)的 Ethereum 也能够通过使用适配空间被 Rivet Chain 连接。

Rivet Chain 的第一个空间称之为 Rivet Chain 中心。Rivet Chain 中心是一种多资产权益证明加密货币网络，它通过简单的管理机制能够对网络进行适配和升级。此外，Rivet Chain 中心能够通过链接其他空间来实现拓展。

Rivet Chain 网络的中心及各个空间能够通过 RTSP 协议进行沟通，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）。代币能够安全、快速地从一个空间转到其他空间，而无需在两个空间之间拥具有汇兑流动性。因为每个人都能够将新的空间连接到 Rivet Chain 中心，所以空间将能够兼容新的区块链条件。

理念

我们认为区块链互操作性具有很高的重要性。在现有网络中，你能够通过应用程序的 API 对大量的数据集进行访问和修改。而在区块链中，数据就被封锁在某一个链中。我们希望打破这样的数据孤岛情况，因为当数据的流畅流通与交互时，才会产生更多的价值和更大的发展空间。

我们希望通过 Rivet Chain 达成以下的现实：

1、不需要信任，不同的区块链即可直接安全地进行资产转移；

2、不同链之间的智能合约能够实现交互；

3、某些专用链可供其他区块链使用；

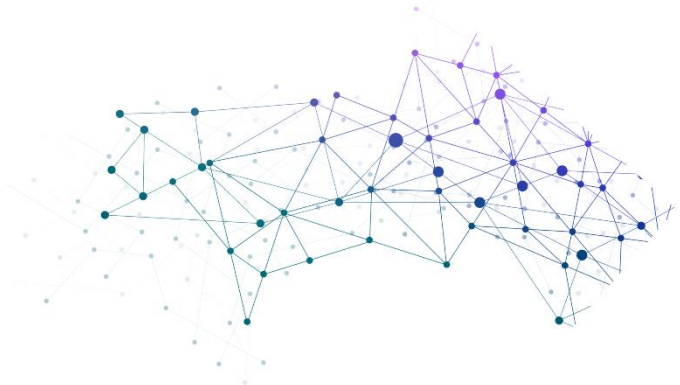
4、为无法保障安全性但能够实现沟通的链提供 bridge-slots；

5、让实时流媒体在链上低成本无阻受控点播成为可能。

利用 Rivet Chain 能够实现区块链间的互操作。这是一个具有潜力的有价值的互联网，其中的资产由不同的共识者发布和控制，并能够在不依靠需要信任的第三方的情况下实现跨链资产无缝的转移和交易，实现链下完成大部分交易，只有关键交易上链，从而大大减少主链网络拥堵的困境。

3

技术方案



Rivet Chain

在这一部分我们将阐述 RTSP 集成共识协议和用于建立其应用程序的接口。

RTSP 协议

Rivet Chain 中心是 Rivet Chain 网络中第一条公共区块链，通过 RTSP 的集成共识算法运行。RTSP 开源项旨在基于 PoW+PoS 共识算法的速度、可拓展性以及其他问题进行进一步优化。通过采用并提升已验证的 PoW+PoS 算法，RTSP 机制可解决第一代权益证明加密货币面临的相关问题。

RTSP 区块链实时流传输协议，是应用层协议升级的集成共识协议。RTSP 协议用于在空间和区块链建立和协商实时流会话。

RTSP 是应用级协议，控制实时数据的发送。RTSP 提供了一个可拓展框架，使实时数据，如音频与视频在区块链上的受控点播成为可能。数据源包括现场数据与存储在剪辑中数据。该协议目的在于控制多个数据发送连接，为选择发送通道，如 UDP、组播 UDP 与 TCP，提供途径，并为选择基于 RTP 上发送机制提供方法。

RTSP 建立并控制一个或几个时间同步的连续流媒体。尽管连续媒体流与控制流交换是可能的，通常它本身并不发送连续流。换言之，RTSP 充当多媒体服务器的网络远程控制。RTSP 连接没有绑定到传输层连接，如 TCP。在 RTSP 连接期间，RTSP 用户可打开或关闭多

个对服务器的可传输连接以发出 RTSP 请求。此外，可使用无连接传输协议，如 UDP。RTSP 流控制的流可能用到 RTP，但 RTSP 操作并不依赖用于携带连续媒体的传输机制。

RTSP 协议支持的操作如下：

从区块链上检索流媒体：用户可通过 HTTP 或其它方法提交一个演示描述。如演示是组播，演示式就包含用于连续媒体的组播地址和端口。如演示仅通过单播发送给用户，用户为了安全应提供目的地址。

共识者

在经典的拜占庭容错算法中，每个节点有相同的权重。在 RTSP，节点有着不同数量的　提交分布权，而那些拥有相当数量提交分布权的节点称之为　共识者。共识者通过广播加密签名、提交分布或者对下一个区块表决同意来参与共识协议。

共识者的提交分布权是一开始就确定好了，或者根据应用程序由区块链来决定修改提交分布权。例如，在像 Rivet Chain 中心的权益证明应用里，提交分布权可由绑定为押金的代币数量来决定。

共识

RTSP 是部分同步运作的拜占庭容错共识协议，这种协议源自 PoW+PoS 共识算法。RTSP 具有简易性、高性能。协议要求共识者固

定且被熟知，并且每个共识者都有其公钥验证身份。这些共识者试图同时在一个区块上达成共识，这些区块是一系列的交易记录。每个区块的共识轮流进行，每一轮都会有个领头人，或者提议人，由他们来发起区块。之后共识者分阶段对是否接受该区块，或者是否进入下一轮做出提交分布。每轮的提议人会从共识者顺序列表中按照其提交分布权比例来选择确定。

除了其超强的安全性外，RTSP 还具备杰出的性能。以云平台为例，RTSP 共识以分布在五大洲七个数据中心的 64 位节点为基准，其每秒能够处理成千上万笔交易，订单提交延迟时间为 1-2 秒。而值得关注的是，即使是在相对严峻的骇客环境中，比如共识者失去共识或者是恶意 BUG 的提交分布，也能维持这种每秒超过千笔交易的较高性能。

微用户端

RTSP 共识算法的主要优点是具有安全简单的用户端，使其成为移动设备和 IoT 用例的理想选择。微用户端必须同步运行头部组成的链，并且找到 PoW+PoS 最多的那一条链，而 RTSP 微用户端只需和验证组的变化保持一致，然后简单地验证最新区块中预先提交的>⅔，来确定最新情况。

这种简单的微用户端证明机制也能够实现区块链之间的沟通。

防御

RTSP 有各种各样的防御措施来防止一些明显的攻击，比如远程无利害关系双花攻击以及审查制度。

RBCI

RTSP 共识算法是在叫做 RTSP BFT 的程序中实现的。这个程序是独立于应用的“共识引擎”，能够将任何已经确定的黑盒应用转变为分布式、可复制的区块链。RTSP BFT 能够通过应用区块链接口(RBCI)与其他区块链应用连接。而且，应用区块链接口(RBCI) 接口允许区块链应用以任何语言编程实现，而不仅仅是写这个共识引擎所使用的语言。此外，应用区块链接口(RBCI) 也让交换任何现有区块链栈的共识层成为可能。

RIVET CHAIN 中心

Rivet Chain 的目标是通过协议、智能合约和 RTSP 进行集合和提升，让开发人员能够创建任意的基于共识的、可拓展的、规模化的、易于研发的和协作的应用。Rivet Chain 通过建立终极的抽象的基础层-内置有图灵完备编程语言的区块链-使得任何人都能够创建合约和去中心化应用并在其中设立他们自由定义的所有权规则、交易方式和状态转换函数。域名币的主体框架只需要很短的代码就能够实现，诸如货币和信用系统等其它协议只需要非常短的代码就能够实现。智能合约（包含价值而且只有满足某些条件才能打开的加密暗箱）也能在我们的平台上创建，并且因为图灵完备性、

value-awareness、blockchain-awareness 和多状态所增加的能力从而使其比原本脚本所能提供的智能合约高效得多。

Rivet Chain 网络中每条区块链通过 RTSP 共识算法来运行。

通过全新的区块链沟通协议，Rivet Chain 中心可连接其他众多区块链空间。Rivet Chain 中心能够追踪无数代币的种类，并且在各个连接的空间里记录各种代币总数。代币能够安全快速地从一个空间转移到另一个空间，两者之间无需体现汇兑流动性，因为所有空间之间的代币传输都会经过 Rivet Chain 中心。

这一架构解决了当今区块链领域面临的许多问题，包括应用程序互操作性、可拓展性、以及可迅速升级的能力。这些空间允许 Rivet Chain 实现高效拓展，从而满足全球沟通的需求。此外，空间也完全适用于分布式交易所，反之交易所也支持空间运行。

Rivet Chain 不仅仅是单一的分布式账本，而 Rivet Chain 中心也并不封闭或是 RTSP 生态的中心。我们正在为分布式账本的开放网络设计一套协议，这套协议将基于密码学、共识、经济、公开的原则，成为未来财经系统的基石。

容错机制

如今，实际上所有移动 wallet 都要使用可靠的服务器来进行交易验证。这是因为 PoW 机制需要在交易被认定为无法逆转前进行多次确认。而在 Coinbase 之类的服务中也已经出现双重支付攻击。

和其他区块链共识系统不同，RTSP 提供的是即时、可证明安全的移动用户端支付验证方式。因为 RTSP 被设计为完全不分叉，所以移动 wallet 就能够实时接收交易确认，从而在智能移动设备上真正实现去信任的支付方式。这一点也大大影响了物联网应用程序。

Rivet Chain 中的共识者身份类似矿工，但是他们采用加密签名来进行提交分布。共识者是专门用来提交区块的安全机制。非共识者能够将权益代币（也叫做"RTC"）委托给任何共识者来赚取一定的区块费用以及 RTC 奖励，但是如果共识者违反协议规定，那么代币就会面临被减少的风险。RTSP 拜占庭共识的可证明安全机制，以及利益相关方（共识者和委托者）的抵押品保证，为节点甚至是微用户端提供了可证明、可量化的安全性。

管理

分布式公共账本应该要有一套制度与管理系统。Bitcoin 依靠基金会以及挖矿来协作更新，但是这是一个反应缓慢的管理制度。

Rivet Chain 中心的共识者与委托者能够对提案进行提交分布，从而改变预先默认设置好的系统参数（比如区块转账费用限

制），协作更新，并对可读性的制度进行修订提交分布，从而管理 Rivet Chain 中心制度。这个制度允许共识者聚集到一起，来解决盗窃及漏洞等相关问题，并得出更快更明确的解决方案。

Rivet Chain 网络能够在制度不同的空间之间实现互操作性，这一点给客户极高的自由度和潜力而无需许可即可实验。

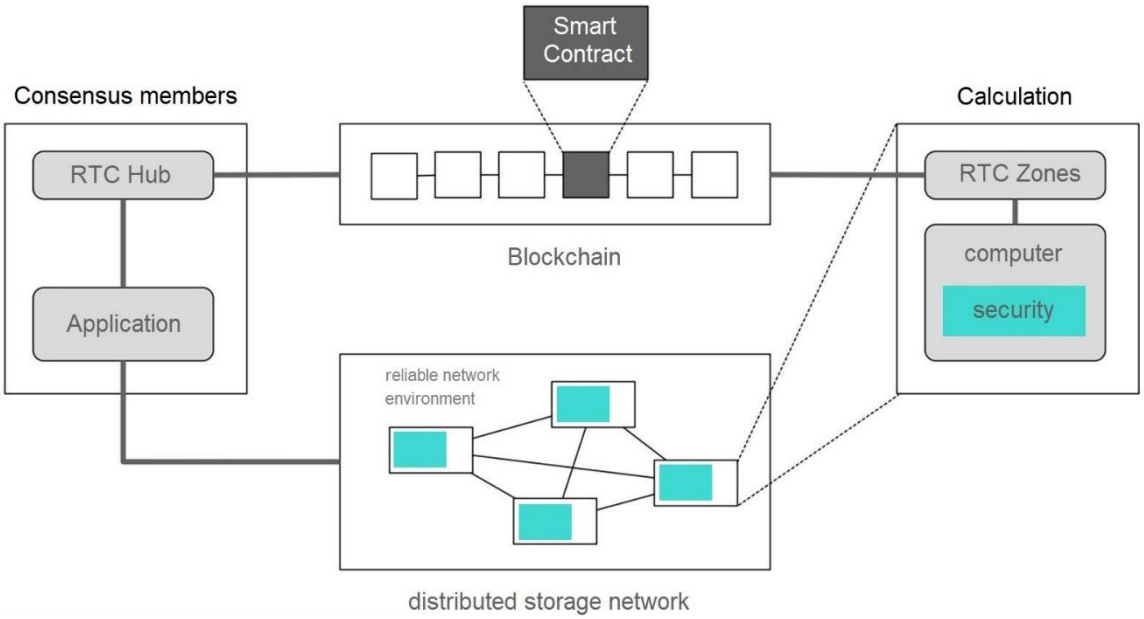
中心与空间

这里我们将描述一个全新的去中心化与可拓展性模型。Rivet Chain 网络通过 RTSP 机制来运行众多的区块链。虽然现存提案的目标是创建一个包含全球所有交易订单的"单一区块链"，但是 Rivet Chain 允许众多区块链在并行运行的同时，保持可互操作性。

在这个基础上，Rivet Chain 中心负责管理称之为“空间”的众多独立区块链。中心上的空间会源源不断地提交最新区块，这一点能够让中心同步每一个空间的状态。同样地，每个空间也会和中心的状态保持一致。通过发布证明来证明消息被接受和发送，来让消息从一个空间传递到另一个空间。这种机制叫做“区块链间沟通”，或者简称为“RTSP”机制。

任何空间都能够自行成为中心来建立自我配置，但为了简明，在这里只讨论这种只有一个中心和许多非中心的空间的配置。

Rivet Chain 空间是独立的区块链，能够和 Rivet Chain 中心进行 RTSP 消息交换。从中心的角度上看，空间是一种多重资产、动态会员制的多重签名账户，能够通过 RTSP 数据集用来发送和接受代币。就像加密币账户一样，空间不能转移超出其持有量的代币，不过能够从其他拥有代币的人那里接收代币。空间可能会被认定为一种或多种代币的"来源"，从而赋予其增加代币供应量的权力。



4

用例

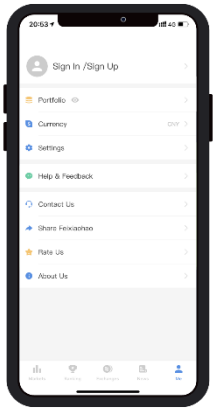
Rivet Chain

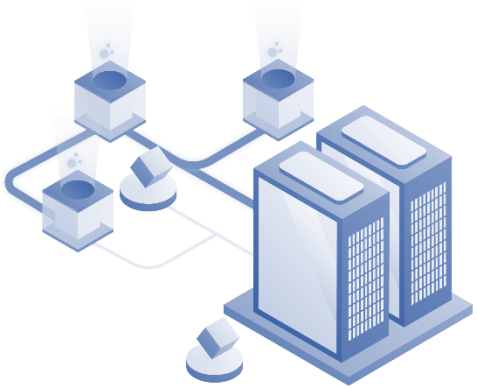
区块链音视频实时流媒体传输

RTSP 协议定义了一对多应用程序如何有效地通过区块链网络传送多媒体数据。RTSP 在体系结构上位于 RTP 和 RTCP 之上，它使用 TCP 或 UDP 完成实时流数据传输。RTSP 是用来控制声音或影像的多媒体串流协议，并允许同时多个串流需求控制，传输时所用的区块链网络通讯协定并不在其定义的范围内，RTSP 允许同时多个 Multicast，除了能够降低服务器端的网络用量，更进而支持多方 Video Conference。Proxy 的 Cache 也同样适用于 RTSP，并因 RTSP 具有重新导向功能，可视实际负载情况来转换提供服务的区块链，以避免过大的负载集中于同一区块链而造成延迟。

RTSP 使得音频与视频等实时流媒体在区块链上的的受控点播成为可能。

RTSP 协议使以自描述方式增加可选参数更容易。RTSP 信息可通过任何区块链底层传输协议携带。



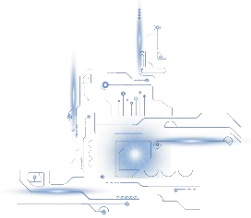


RTSP 请求能够几种不同方式传送：

- 持久传输连接，用于多个请求/响应传输。
- 每个请求/响应传输一个连接。
- 无连接模式。

拓展

拓展问题是一直以来以太坊存在的问题。目前以太坊节点会处理节点上每笔交易，并且存储所有的状态。



RTSP 基于以太坊基础，提交区块的速度比以太坊工作量证明要快，所以由 RTSP 共识推动的以太坊虚拟机分区能够强化以太坊区块链的性能。此外，它能够用来协调不同分区中以太坊合约之间的代币流通，通过分区方式为以代币为中心的以太坊扩展塑造基础。

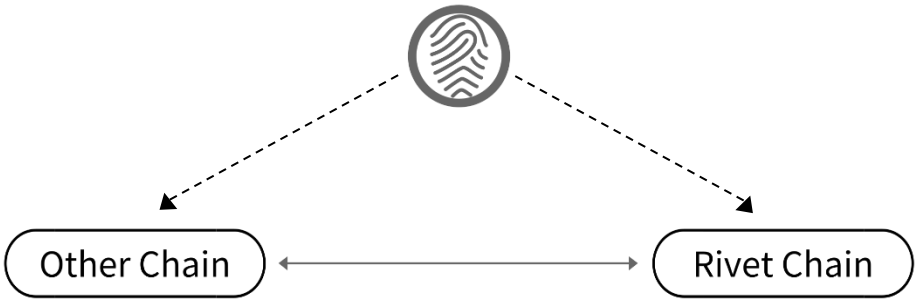
跨链沟通

我们来介绍一下中心与空间之间交互的方法。为了让数据集从这个链转换到其他的链，需要在接收方链上发布一个证明，来明确发送方已经发起了一个数据集到认定目的地。接收方要验证的这个证明，必须和发送方头部保持一致。这种机制就类似与侧链采用的

机制，它需要两个相互作用的链，通过双向传送存在证明数据集，来知悉另一方的情况。

RTSP 协议能够自然定义为两种交易的使用：一种是 RTSP Integration 交易，这种交易能够让区块链同任何观察者证明它最新的区块哈希值；另一种是 RTSP Distributed 交易，这种交易则能够证明某个数据集的确由发送人的应用程序，传输到了最新一层区块的哈希值之上。

通过将 RTSP 机制分离成两个单独的交易，即 RTSP Integration 交易与 RTSP Distributed 交易，与此同时还能确保发送方的完全自由，让其自行决定能够传出的数据集数量。

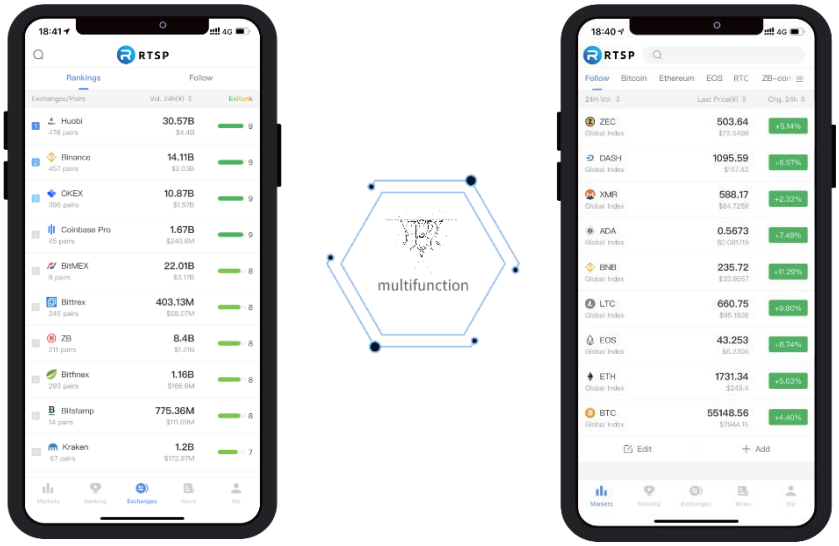


便捷多用

Rivet Chain 空间能够运行任意的应用逻辑，应用在空间创建时设定好，可通过管理者能够不断更新。这种便捷度使得 Rivet Chain 空间能够作为其他加密币的链接承载方，比如 ETH，并且它

还能和这些区块链的衍生品链接，利用同样的代码库，而在验证程序及初始分配有所区分。这样就允许多种现有加密币框架得以运行，如 Ethereum、Zerocash 等等，将其同 RTSP BFT 结合，成为通用网络中性能更优的共识引擎，为平台之间提供更多的交互机会。此外，作为多资产区块链，每笔交易都有可能包含多个输入输出项。

空间同样可成为区块链版的商业或政用系统，这些原来由单个或数个组织操作的特定服务，现在作为 RBCI 应用在某个空间上运行，从而在不放弃对底层服务控制的前提下，维持公共 Rivet Chain 网络的安全性及交互性。所以，Rivet Chain 或可为那些既想使用区块链技术，又不愿放弃控制权给分布式第三方的人，提供良好的操作环境。



谷歌架构高速区块链浏览器

Rivet Chain 使用谷歌的底层搜索架构，打造集成式区块链知识图谱、动态、可调节神经网络，信息全面的区块链专百科、拥有精选项目的“类 APP Store”、流量共享的媒体社交聚集地。

谷歌巨型 Token 化搜索引擎拥有毫秒级启动、个性化可定制、推荐区块链专属内容。“搜索即所想”——我们将区块链媒体、自媒体生产出的优质内容进行分类，用户能够第一时间找到自己感兴趣的内容。用户想要了解的区块链知识都能够进行搜索，用户想要了解的优质项目都能够通过 Rivet Chain 了解。

技术特点

Rivet Chain 谷歌巨型 Token 化搜索引擎具有网站、图像、新闻组和目录四个功能模块，搜索速录机快，开发一个对各个链之间的关系做精确分析的搜寻引擎，搜索引擎每天可处理高达亿次搜索请求，数据库存有 30 亿个 WEB 文件，提供常规搜索和高级搜索两种功能，信息条目数量，并支持多种语言，支持多达万种币种和交易所。

1、以关键词搜索时，返回结果中包含全部及部分关键词，短语搜索时，默认以精确方式进行，字母无大小写之分，不使用词干法。

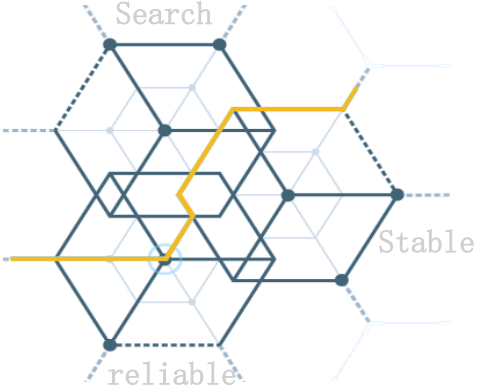
2、在我们的区块链浏览器查询时不需要使用 AND。缩小范围时，只需要输入更多的关键词，或者使用二次检索。

3、特有的 PR 技术，PR 能够对网页的重要性做出客观的评价。PR 是我们评价一个网站质量高低的重要标准，PR 分为十个等级，从容不 1 至 10，PR 越高代表网页质量和权威性越高，排名也就越靠前。

4、更新和收录，我们将是所有区块链搜索引擎收录最快的，更新也比较稳定。

5、重视链接的描述和链接的质量。

6、超文本匹配分析:我们的区块链搜索引擎同时也分析网页内容。并不采用单纯扫描基于网页的文本的方式,而是分析网页的全部内容以及字体、分区及每个文字精确位置等因素。同时还会在链上分析相邻网页的内容,以确保返回与用户查询最相关的结果。



打造自治化组织形态

Rivet Chain 让拥有共同兴趣来自地球不同肤色，不同地区的区块链热爱者在不同话题、不同热点、不同项目的圈子里聚集发声，交流互动。Rivet Chain 支持实时发帖，及时互动，让信息以最快最简洁的形式让更多人获取并得到反馈，你的声音将被更多人听到。Rivet Chain 为区块链践行者，热爱者，个人创作者、自媒体、社区、项目赋能，让更优质内容被更多人看到，实现内容生产者的收益最大化，内容资讯的价值最大化，形成内容产出、创作者受益、内容质量的良性循环。致力为区块链行业打造最专业、最开放的交流互动平台，将成为 Rivet Chain 终身事业。

数字资产信息革命

Rivet Chain 提供币交易实时提醒、高效交易、重新定义币行情资讯。透过大数据技术对海量数据进行多维度，多层级处理，将最有价值的信息及时分享给用户。在 Rivet 平台上可极速获得行情交易提醒，无论是主流代币和你所关注的代币的各种幅度涨跌，对用户任何有益有价值的交易信息，都会第一时间推送到你的身边。RTC 通过大数据技术及谷歌架构巨型搜索引擎进行高效的区块链方面的数据分析、数据挖掘，构建中立、权威的的行情数据平台及综合信息平台；为用户和区块链项目提供优质的 SNS 服务，提供及时

有价值的区块链资讯，动态等数字内容产品。Rivet Chain 通过构建新通证经济系统，在区块链应用的探索上寻求方向，让每个人都能够快速、便捷的查询币种价格，随时随地洞察掌握最新动态。力争为区块链每位体验者提供最简单便捷高效的方法来探索区块链，听见区块链，看见区块链。

5 RTC

发行与激励

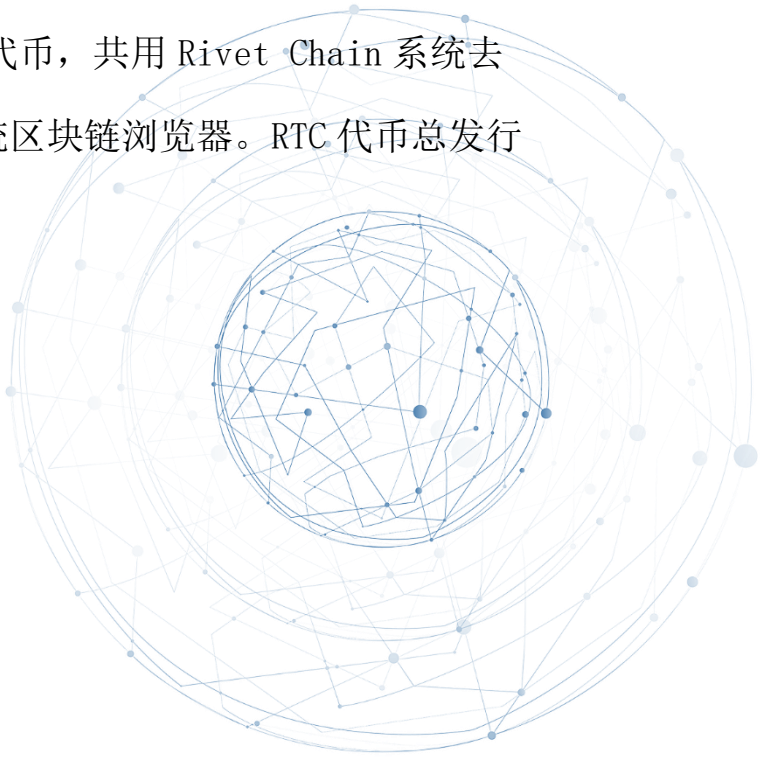
主网上线

Rivet Chain 的主网上线是指 Rivet Chain 公链应用底层系统搭建完成，而 Rivet Chain 公链是基于区块链搭建的自应用生态。

RTC

Rivet Chain 是多资产分布式账本，它有自己的代币，届时将基于 Rivet Chain 公链发行出主网代币 RTC。RTC 是 Rivet Chain 唯一的权益代币。RTC 是持有人提交分布、验证或委托给其他共识者的许可证明，RTC 也能够用来支付交易费以减少电子垃圾。额外的通胀 RTC 和区块交易费用就作为激励分给共识者及委托共识者。

作为 Rivet Chain 公链应用的结算代币，同时作为 Rivet Chain 系统第三方应用的充值结算代币，共用 Rivet Chain 系统去中心化 wallet 和 Rivet Chain 系统区块链浏览器。RTC 代币总发行量 3.5 亿枚。



分配方案及管理细则

1、创始团队　比例 20%

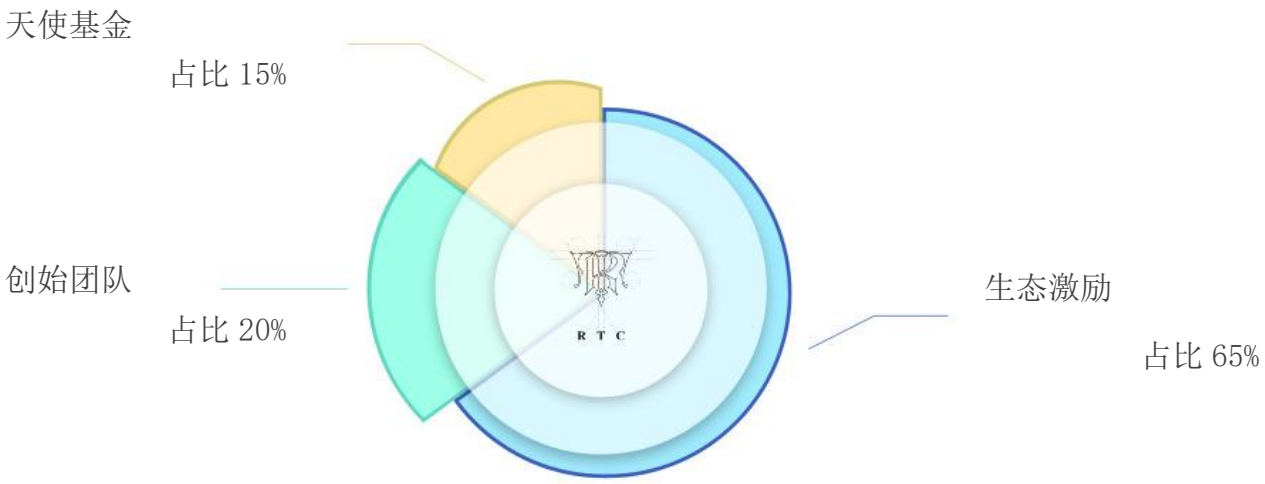
创始团队和研发团队贡献奖励，主网上线起，第一年分季度释放 40%，剩余部分第二年分季度释放 30%，第三年分季度 30%。

2、天使基金　比例 15%

天使投资，主网上线起，第一年分季度释放 40%，剩余部分第二年分季度释放 30%，第三年分季度 30%。

3、生态激励　比例 65%

为社区维护者，资源提供者、共识者等贡献者提供激励。对 Rivet Chain 有益的行为进行激励。



RTC 分配方案图例

共识者的数量限制

与以太坊或其他 PoW+PoS 区块链不同的是，由于沟通的复杂性增加，RTSP 区块链会随着共识者的增加而变慢。幸运的是，我们能够支持足够多的共识者来实现可靠的全球化分布式区块链，并具有非常快的交易确认时间。 而且随着带宽、存储和并行计算容量的增加，我们将来能够支持更多的超级共识者。

在初始日，超级共识者的最大数量将设置 100，这个数字将增长 10 年，最终达到 300 。

成为初始块后的共识者

RTC 持有者能够通过申请和提交分布成为共识者。任何人任何时候都成为共识者，除非当前超级共识者组的数量超过了最大值，需等待未来生态新增超级共识者数量。

激励骇客

Rivet Chain 中心的安全取决于底层共识者的安全性。为了鼓励发现和早期报告发现的漏洞，Rivet Chain 中心鼓励骇客发现漏洞。

管理规范

Rivet Chain 中心是由一个分布式组织管理的，需要一个明确的管理机制，以协调对区块链的各种变化，如系统的参数变量，以及软件升级和宪法修订。

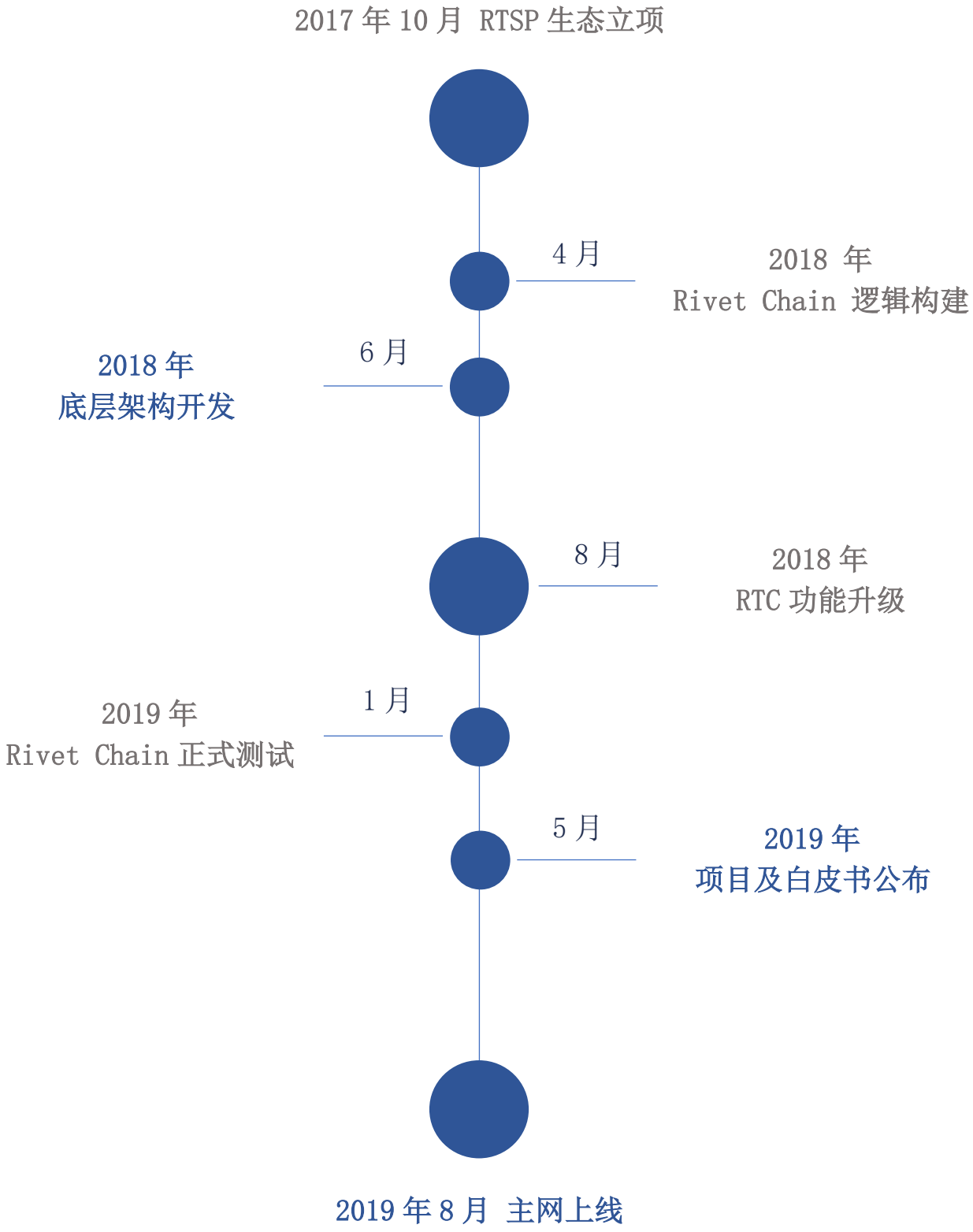
所有共识者负责对所有提案进行表决。如果未能及时对提案进行表决，将导致共识者被自动停用一段时间。

委托者自动继承其委托的共识者的提交分布权。这一提交分布能够被手动覆盖掉。

6

路线图

Rivet Chain


2017 年 10 月 RTSP 生态立项
4 月
2018 年
Rivet Chain 逻辑构建
6 月
2018 年
底层架构开发
8 月
2018 年
RTC 功能升级
1 月
2019 年
Rivet Chain 正式测试
5 月
2019 年
项目及白皮书公布
2019 年 8 月 主网上线

7

创新工作

Rivet Chain

水平拓展

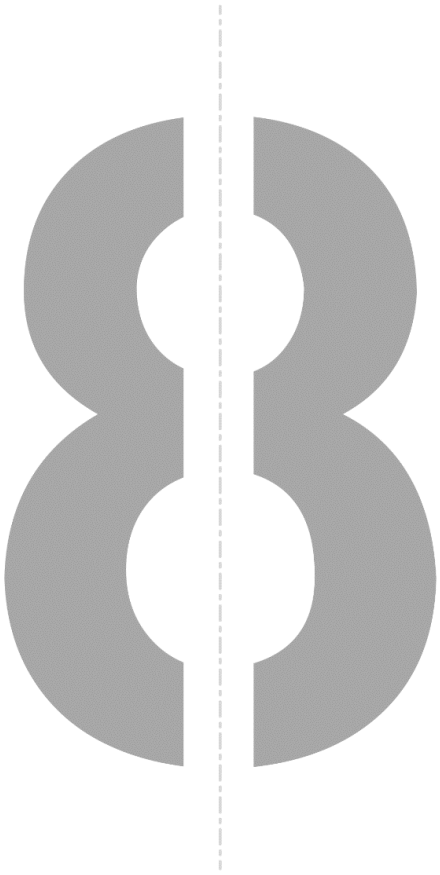
侧链使得 Rivet Chain 能够方便的在区块链和侧链间移动，并允许在侧链上验证新需求。在 Rivet Chain Hub 中，侧链和 Rivet Chain 是彼此的微用户端，在 Rivet Chain 和侧链间移动时使用 RTSP 证明。双向链接的核心机制原则上与 Rivet Chain 所采用的机制相同。

Rivet Chain 目前正在研究许多不同的策略，将区块链的状态空间化，以解决可拓展性的需要。这些努力的目标是在共享状态空间之上，维持当前虚拟机提供抽象层。目前，多项研究工作正进行中。

闪电网络

闪电网络被设计成一种代币传输网络，在公有区块链上一层运行，通过把大部分交易从共识分类账之外转移到所谓的“付款渠道”。这通过链上加密货币脚本来实现，这些脚本使双方能够进入双方持有的状态化合同，通过共享数字签名来更新状态，并且在合同结束后最终通过在区块链上发布证据，这种机制首先受到跨链原子互换交易的欢迎。通过与多方开通支付渠道，闪电网络的参与者能够成为集中点，为其他人的支付提供路径，从而使得支付渠道网络的完全联通，其代价是绑定在支付渠道上的资金。

虽然闪电网络也能够轻松地跨越多个独立的区块链，并借助交易市场实现价值转移，但它不能实现从一个区块链到另一个区块链的非对称代币交易。这里描述的 Rivet Chain 网络的主要优点是实现直接的代币交换。也就是说，我们希望支付渠道和闪电网络将会与我们的代币传输机制一起被广泛采用，从而节省成本和保护隐私。



风险声明

Rivet Chain

在 Rivet Chain 的开发、维护和运营过程中存在众多风险,这其中很多都超出了我们的控制。每个参与者应仔细阅读、理解并考虑下述风险,慎重决定是否参与我们的计划。若持有 RTC 代币，视为参与者已充分知晓并同意接受下述风险:

法律政策和监管风险

区块链技术受限于全球多个不同的监管组织的监督与控制。RTC 或受限于他们所提出的要求或行动,包括但不限于限制数字代币的使用。代币持有者必须自己进行尽责的调查,确保他们遵循所有他们当地关系到加密货币、税务、债券及其他监管的法律安全风险。

在天使或私募阶段收集到的资金都不经保险保障。若遗失了它们或它们失去了价值,买家或无法得到任何私人或公众保险的协助未经授权认领 RTC 的风险。每个人应当采取如下的措施：妥善维护其注册邮箱或注册账号的安全性；使用高安全性密码；不打开或回复任何欺诈邮件；严格保密其机密或个人信息。

技术风险

Rivet Chain 仍在开发阶段,由于 Rivet Chain 底层公链开发的技术复杂性,开发可能不时会面临无法预测和或无法克服的技术困

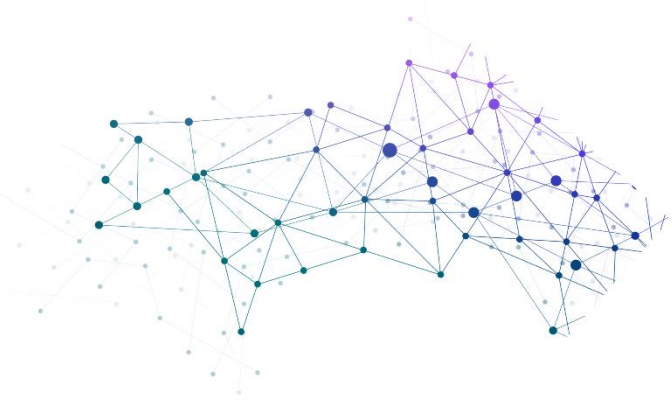
难。因此，Rivet Chain 的开发可能会由于任何原因而在任何时候失败或终止。

源代码漏洞风险，无人能保证 Rivet Chain 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞。可能将损害 Rivet Chain 的可用性、稳定性和安全性,并因此对 RTC 的价值造成负面影响。源代码以透明为根本,以促进源自于社区的对代码的鉴定和问题解决。

流动性风险

RTC 既不是任何人、实体、美联储银行或国家、超国家或准国家组织发行的货币，也不是硬资产或被其他信用所支持。RTC 在市场上的流通和交易并不是出售方的指定也没有要求。RTC 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 RTC 持有者处购买任何 RTC,也没有任何人士能够在任何程度上保证任何时刻 RTC 的流通性或市场价格。

鸣谢



Rivet Chain

我们为所有朋友欲同行们在概念成型与检查方面给予的帮助，以及对我们在 RTSP 与 Rivet Chain 工作中的大力支持，表示衷心地感谢。

- Steven Carl 在格式与措辞方面提供了很多帮助，尤其在中心与空间部分。
- Justin Johnson 在版本迭代方面的帮助。
- Avril Snow 在激励部分给予的反馈。
- Jonathan walker 对高速浏览器部分的反馈及在措辞方面的帮助。
- 同时还要感谢 Alexander Lei 在多方面的支持与贡献。
- 同时感谢您的浏览。

10

引用

Rivet Chain

- 1 Bitcoin: https://bitcoin.org/bitcoin.pdf
- 2 ZeroCash: http://zerocash-project.org/paper
- 3 Ethereum: https://github.com/ethereum/wiki/wiki/White-Paper
- 4 TheDAO: https://download.slock.it/public/DAO/WhitePaper.pdf
- 5 BitcoinNG: https://arxiv.org/pdf/1510.02037v2.pdf
- 6 Casper: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/
- 7 Ethereum Sharding: https://github.com/ethereum/EIPs/issues/53
- 8 "Bitcoin-Statistics and Facts"(October 2016)
- 9 Goldman Sachs:Blockchain-Putting Theory into Practice
- 10 Hal Finney"Reusable Proofs of Work",2005