[项目白皮书][简体中文版]

[内部版本:V1.0.1]

白皮书前缀说明

主流商业采用区块链技术受到限制。在本文中，我们将提出一个新的设计：

TU 网络与高并发的区块链操作系统，第三代多层系统来应对这些挑战。我们的假设核心是，在独特行业内创造许多区块链来解决独特的业务挑战。因此，TU 网络旨在支持自定义区块链体系结构，同时为跨链互操作性提供去信赖的机制。这个系统的根本是世界上第一个公认的公共企业级区块链，一种引入新的安全模式，公

平，并具有代表性的加密经济激励机制。

目录

基础介绍	第一代区块链	第二代区块链	第三代区块链	多层区块链网络
连接网络	跨链交易	注册	竞争	桥梁共识
费用分布	定义	验证者提名程序	区块链功能模块	智能合约
加密安全技术	数据存储	链外存储	应用说明	BaaS 服务
结语				

基础介绍

由于可扩展性，隐私性和互操作性方面的挑战，主流商业采用区块链技术受到限制。TU 是第一个旨在应对这些挑战的多层次区块链网络。在我们预期的将来大量特定为各行业配置的区块链将会陆续诞生。为此 TU 网络设计目的旨在支持各类自定义的区块链网络。TU 网络的核心是第一个专有的，公共的，企业级区块链：TU 是一个最先进的第三代区块链，是一种引入新的安全模式，公平，并具有代表性的加密经济激励机制。

本文:

介绍和解释 TU 网络

下一代区块链技术和第一个多层区块链网络及其必要的基础设施和协议。

1. 详细介绍 TU 的愿景和技术概念，TU，一个专用的，公共的，第三代区块链和 TU 网络中的组件。

1. 为 TU 和 TU 网络的未来实施提供路线图。

第一代区块链

Bitcoin 作为第一代区块链技术，率先创建了许多货币替代平台。这些区块链通过实施加密-安全，对等式网络，以及一个由全球分布式网络验证的数字交易公共账目解决了传统交易受限的问题。产生了一个应用数字化优势的平台，同时严格保障了价值的稀缺性

第二代区块链

随着第二代区块链，以太坊引入在区块链网络上执行应用逻辑的能力 。这启用了超出交易的新功能，将状态、业务逻辑和多方合同在区块链中存储并执行，并写入不可变的账本。这些概念已被纳入其它分布式账本技术，并导致了构建区块链和构建区块链上的区别。

基于区块链的应用程序的出现对于行业来说是积极有用的。创新的区块链应用进一步证明并验证了区块链技术的发展并不仅仅局限于作为价值转移的工具。然而，这些分离的网络由于相互孤立，只能通过中心化交易平台传输数据或进行价值转移。从某种意义上说，经济与工业之间微小王国的壁垒正在被构建。随着网络数量的增长，行业将变得越来越不连贯和稀疏。

正如在互联网的早期发展过程中，不同区块链网络还没有真正意识到相互连接的好处。虽然专门的区块链网络将，并且应该被开发，但是能够在链上与其它网络进行互通具有显著优点，特别是在确保隐私和可扩展性的前提下。一个可加入不同网络的机制将为每个参与的网络带来巨大价值。

第三代区块链

在未来，区块链将在一个类似于互联网的中心和 spoke 模型中整合数据和价值。主流区块链未来采用的方向将通过开发联合区块链来实现，以整合这些单独的 spoke。这个集成的区块链网络，即 TU。

是第三代区块链网络，将使任何公共部门或私有组织能够:

整合: 在任何与 TU 兼容的区块链和以太坊之间发送数据和值。

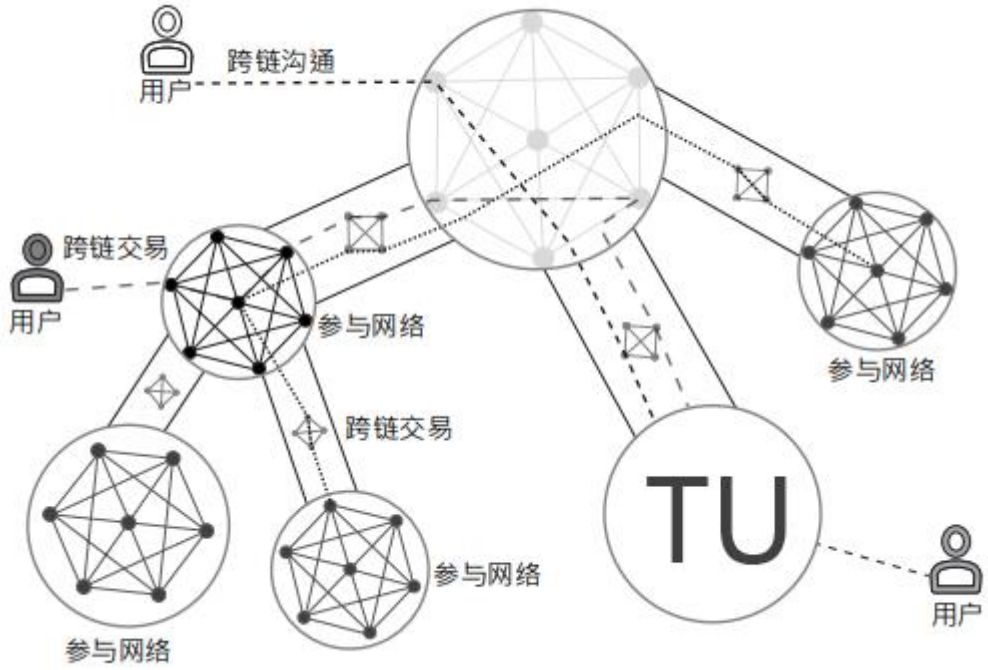
扩展: 为所有 TU 区块链提供快速的事务处理能力和增加数据容量。

Spoke: 允许创建定制的公共或私有区块链，以保持与其它区块链的互操作性，同时允许发布者选择治理，共识机制，发布以及参与方式。

TU 网络的核心是一个独特设计的，公开的，第三代的区块链，TU。设计用于连接其它区块链并管理其自身的大量链上程序，TU 还提供了激励互操作性的经济系统。

TU 令牌作为整个网络的燃料可用于创建新的区块链，货币化跨链桥梁和保护整个网络的安全。

多层区块链网络



简单的多层区块链网络，包涵所有主要参与者

多层区块链网络就像一个计算机网络，为不同的系统提供通信协议和标准来。然而，除了信息之外，tu 网络将通过在参与的区块跨链传递逻辑和价值来创建一个连续的价值链，其中每个交易都发生在链上，逻辑和价值像流动资产一样在跨链自由流动

这些基础设施，协议和概念将一起工作，以确保跨链通信从始发到目的地的传输。这些技术的价值在于它们使一个区块链与另一个区块链交互，以及一个区块链与多个连接的区块链进行交互。

连接网络

连接网络是促进多个私有或公共区块链网络之间的跨链通信和跨链事务的网络。连接网络由在 TU 上下文中指定的角色要求来定义连接网络和跨链事务提供了通用接口，使区块链开发者和用户能将消息从一个网络路由到另一个网络。具体来说，连接网络应提供以下核心功能：

- **通过通用桥接协议在不同的区块链网络之间路由消息，该最终协议涉及消息的转换和传播。**
- **提供去中心化的问责制。**
- **提供桥接协议。**

TU 网络协议规定了外部组件的标准。虽然每个连接网络的实际功能和内部组件可能因供应商和预期目的而异，但是这些核心功能应该被实现。

诸如跨链交易中继或 BTC 交易中继的点对点连接作为中心集线器存在。这样的协议虽然简单而有效，但往往导致复杂的状态可能引起争议，并且经常会依赖于运维中继网络的人员。

连接网络代替使用网桥和去信任的区块链网络来验证并确保流动交易的正确性。通过引入第三方将消息从

A 点

路由传递到 B 点，而网络本身不存在管理困难或不清楚的情况。

跨链交易

跨链交易是区块链网络之间的去信任消息，这是一个关键的基础设施组件，用于链路间通信。跨链交易允许任何已连接的区块链网络交换信息，如互联网上的计算机。

跨链交易最初是在源块上创建的，然后在最终到达目标区块链之前通过桥梁和连接网络进行处理和转发。

如前 TU 跨链交易从源块到目标网络的设计类似于数据包，即可通过多个连接网络

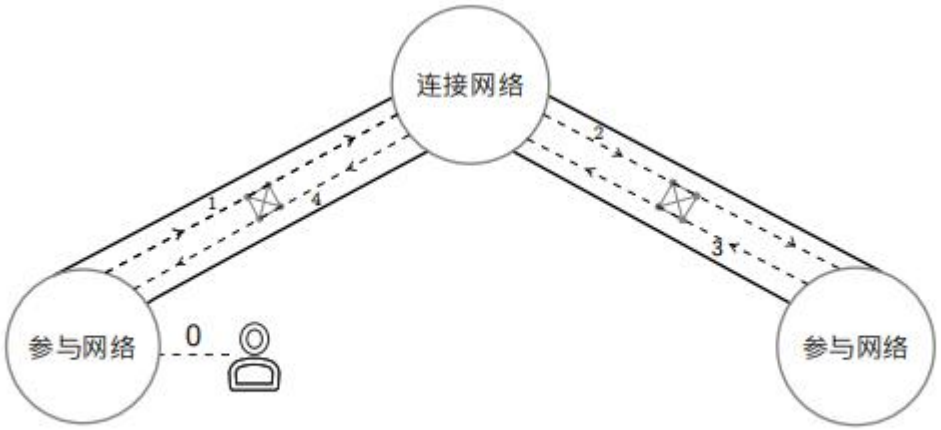
跨链交易是区块链网络之间的去信任消息，这是一个关键的基础设施组件，用于链路间通信。跨链交易允许任何已连接的区块链网络交换信息，如互联网上的计算机。

跨链交易最初是在源块上创建的，然后在最终到达目标区块链之前通过桥梁和连接网络进行处理和转发。如前所述，跨链交易的创建者必须使用 TU 令牌为通信支付交易费用，从而激励每个交叉点的参与者。跨链交易从源块到目标网络的设计类似于数据包，即可通过多个连接网络跨链交易是区块链网络之间的去信任消息，这是一个关键的基础设施组件，用于链路间通信。跨链交易允许任

何已连接的区块链网络交换信息，如互联网上的计算机。

跨链交易最初是在源块上创建的，然后在最终到达目标区块链之前通过桥梁和连接网络进行处理和转发。如前所述，跨链交易的创建者必须使用 TU 令牌为通信支付交易费用，从而激励每个交叉点的参与者。跨链交易从源块到目标网络的设计类似于数据包，即可通过多个连接网络

跨链交易的路由是一个多阶段的过程。在每个阶段，验证者验证交易，并就交易是转发还是被拒绝达成共识。如果一个交易在任何时候被拒绝，则任何由于跨链交易而导致的状态改变将被撤销，至少在连接网络中。路由路径可以分为两个子路径：前向路径和后向路径。在前向路径中，跨链交易从源链一直流向目标链。在后向路径中，跨链交易的确认被传回



生命周期，由链 A 发起，得到确认后终止

如果桥梁由于任何原因拒绝广播跨链交易，则发送方可以选择将包括证据在内的跨链交易直接传递到连接网络。

连接网络将基于参与网络的 merkle 哈希值来验证跨链交易，如果有效则将其广播。跨链交易的设计仍在考察之中，随着项目进展，将出版关于跨链交易运作的详细文件

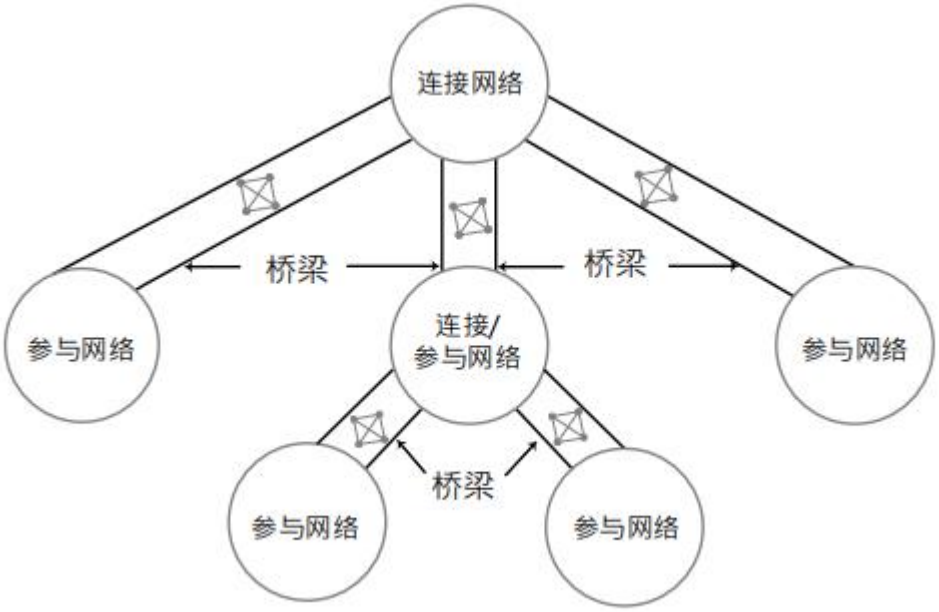
如果超过三分之二的桥梁验证者对于跨链交易投票为对，则连接网络将将跨链交易的状态更改为保持状态，这将触发事件，其中相应的连接网络令牌将被锁定，直到交易处理为止。

- **如果不到三分之二的桥梁验证者为跨链交易投票，状态将被拒绝。**
- **保持状态的交易将由连接网络和路由上的下一个区块链的桥梁验证者转发。**
- **从目标区块链接收到确认后，状态变为确认。**
- **如果没有收到确认，状态将更改为超时。**
- **对于确认的跨链交易，状态变更确定，所有锁定费用分配给连接网络和桥梁验证者**

桥梁

桥梁是通信协议，有助于参与网络和连接网络之间的通信。桥梁由自己独特的验证者网络组成，提供交易的问责和确保协议被正确执行。

桥梁是定向的; 源块链是发送交易的链，目标块链是交易到达的链



桥梁与连接网络关系俯视图

桥梁有两个主要职责：* 签署并转发已被源区块链收录并支付了跨链通信费用的跨链交易 * 通知连接网络参与网络的 merkle 哈希值更新。桥梁验证者将使用基于轻量级 BFT 的算法来达成共识。交易仅在收到三分之二以上的总票数（加权）后才获得批准

注册

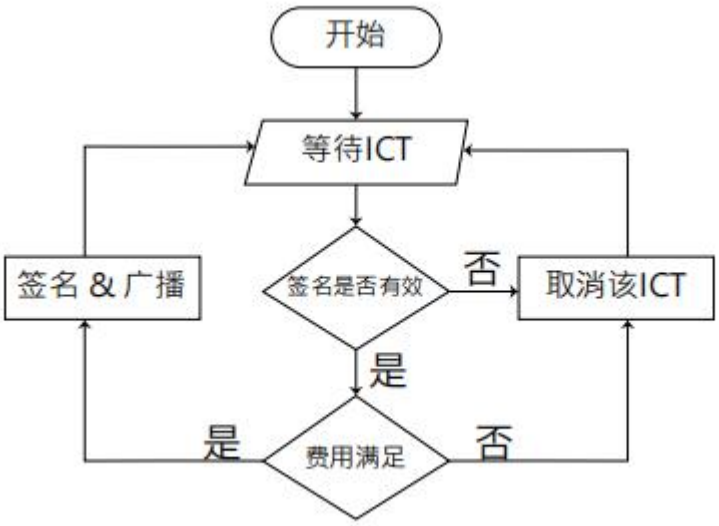
连接网络负责注册其直连桥梁。对于每个桥梁，一个专用的验证者表将保留在区块链上，按照股权排序。任何人都可以参与公共桥梁。具体来说，合同或协议的目的是保持一个全局的桥梁注册，随着节点加入或离开桥梁网络动态更新。达到了最低股权注入的桥梁才被认为是有效的。投入最多的验证者才能参与桥梁共识。

竞争

当多组验证者使用不同的标识符注册同一个区块链网络时，可能会产生多个桥梁。从连接网络的角度看，这些

桥梁是不同的，尽管它们向同一个网络传播和接收消息。

因此，用户有责任通过指定目标网络标识来确定要使用的桥梁。这里的目标是通过激励不同的桥梁网络在稳定性，声誉和价格方面进行竞争来推动开放市场，以市场需求驱动最优费用为目标



桥梁验证算法流程图

桥梁共识

桥梁验证者通过遵循轻量级的基于 BFT 的协议达成共识，其中交易处理一轮而不是多轮。每个验证者根据它们对前一个区块的视图来评估一个交易。如果三分之二或三分之二以上的验证者投票为是，则跨链交易被视为有效，此时下一个区块链认为交易有效。

从开始状态开始，需要桥梁验证者等待，直到接收到跨链交易，然后验证签名和交易费用的有效性。根据交易的有效性，它将被验证者删除（未签名），或签名并传播到连接或目标网络

费用分布

桥梁验证者可以从跨链交易费中得到奖励，并可能获得区块奖励的一部分。费用分配的目标是公平的分配政策。在内部，到桥梁的所有费用都分配给桥梁验证者。这可以按照每个验证者放在桥梁上的比例完成，也可以均分完成。在外部，桥梁与路由路径上的其他桥接器和连接网络验证者共享跨链交易费用。外部费用有两种可能的分配模式：

• 跨链交易的发送方指定了网桥与连接网络之间的费用分配。这种方法的优点是用户可以选择根据桥梁负载

和最低费率优化费用。缺点是在发送交易之前，用户需要基本了解每个桥的路由路径和费用要求。

• 发件人仅根据协议或硬编码协议规定总费用，网桥和连接网络共享此费用。该方法的优点是对用户更简单。这种方法的缺点是，如果不是很难，改变桥梁和连接网络之间的比例是缓慢的

定义

对于本文中所以用的代表共识的定义的理解，请参阅以下一组定义：

• 提名是一个节点注册成为验证者，在 tu 上参与代表共识的过程。提名必须在网络中的任何其他用户能够承诺支持之前完成。

• 排名用于确定具有最高支持的验证者。这个排名列表是一个动态的集合，这意味着选举人节点可以对共识过程作出投票。

• 动态集合是动态验证者的分层列表。动态集合中包涵验证者。

• 备份集合构成动态的候选验证者，但不在动态集合中。备份集合是下一个获得最高支持的验证者。在发生恶意行为或不活动的情况下，网络会看到此替换验证者。

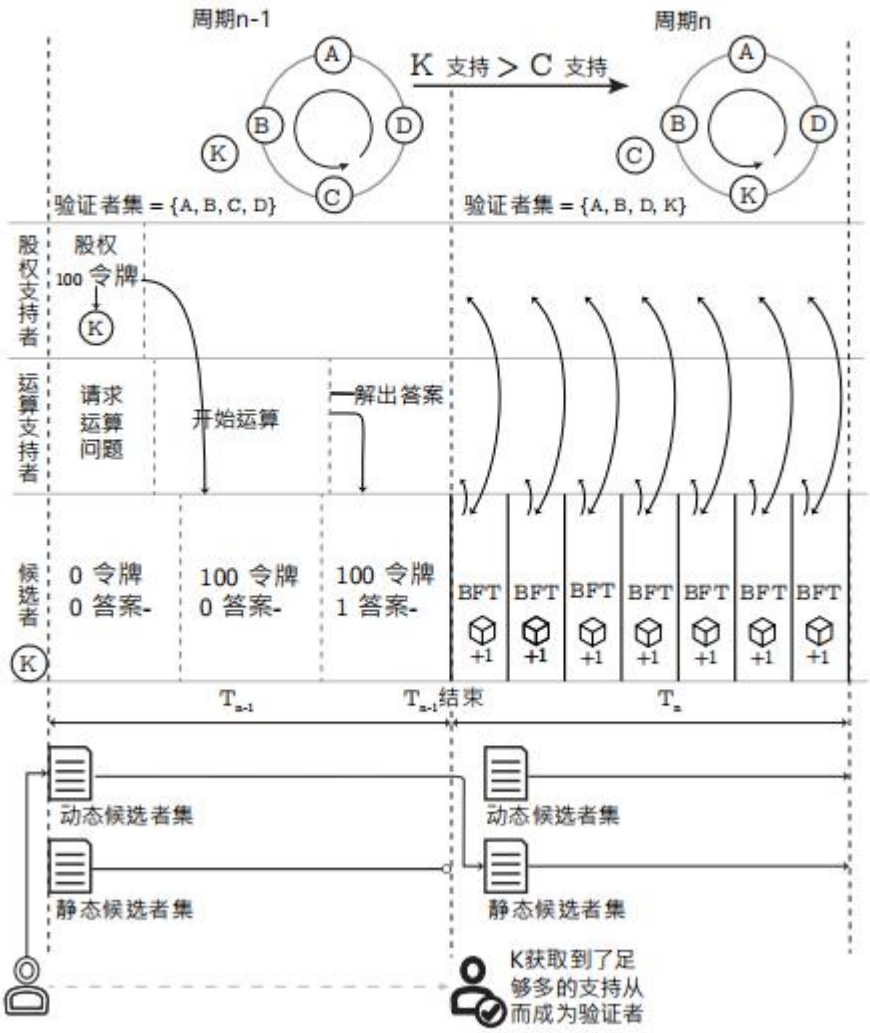
• 支持者是指支持验证者的节点。网络上的验证者将会有更多的支持者，他们的参与直接影响到动态集合中验证者的排名。此外，支持者根据其验证者的奖励比例进行奖励。支持者由两个不同的小组组成：权益者和解算者。

• 权益者是使用令牌作为承诺支持验证者，是支持者的子集。

• 权益者的令牌由网络锁定一定时间，直到它们在预定义的时间被释放回权益者为止。

• 解算者是使用智能证明来解决网络提供的算法问题的用户，然后将证明转为支持，是支持者的一个子集。

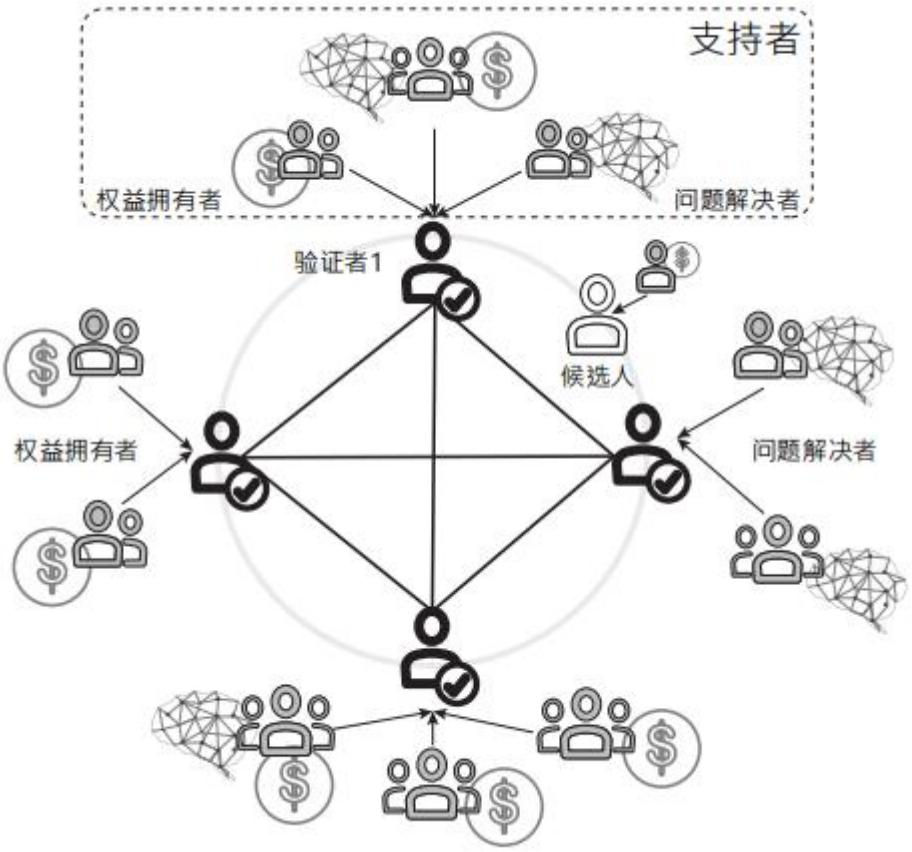
• 时期是网络为了基于 BFT 的共识而使用静态集合定义的持续时间。在每个时期中，一组静态验证者验证新的区块。在每个时期结束时，动态集合被冻结并根据利益变化生成新的静态集合。



动态 / 静态候选者集合 & 权益周期，以及候选人参与共识的过程

验证者提名程序

任何节点都可以自提名并注册成为验证者，但是它们需要足够的支持才能在 TU 上激活。网络维护并及时刷新验证集合，使用提名合同。



该图描述一个进行时的投票集合，每一个验证者被支持者通过权益或问题解决支持。候选人则需在新的轮换时拥有具备足够多支持成为正式验证者。

验证者通过网络的持续支持变得活跃。动态集合的成员始终是最高支持的候选人。为了促进这种持续的支持进程，任何时间点都有两份提名合同。网络用户返回或撤回对候选人的支持，以及静态集合的存在仅在该时期内。共识协议从静态集合中派生其动态集合。在每个时期结束时，静态集合在下一个任务期间被动态集合替换。验证者可自定义如何补偿他们的支持者。因此，验证者提出其支持条款，如果这些条款被同意，则支持者将向该验证者提供资源。这会产生一个平衡的影响，因为一个有效的验证者的排名（和随后的奖励）是基于它与其他验证者支持量的比对。

区块链功能模块

共识机制

共识机制是区块链技术的一个核心问题，它决定了区块链中区块的生成法则，保证了各节 点的诚实性、账本的容错性和系统的稳健性。常用的共识机制主要有 PoW、PoS、DPoS、Paxos、 PBFT 等。基于区块链技术的不同应用场景，以及各种共识机制的特性，主要可以从性能效率、 资源消耗、容错性、监管水平等几个方面进行评价和比较。

共识机制功能组件具备以下功能：

a） 支持多个节点参与共识和确认；

b） 支持独立节点对 区块链网络提交的相关信息进行有效性验证；

c） 防止任何独立的共识节点未经其他共识节点确认而在 区块链系统中进行信息记录或修改；

d） 应具备一定的容错性，包括节点物理或网络故障的非恶意错误，以及节点遭受非法控制的恶意错误，以及节点产生不确定行为的不可控错误

智能合约（Smart Contract）

由尼克·萨博（Nick Szabo）于 1995 年提出，他给出的定义是：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。”承诺定义了智能合约的本质和目的。数字的

形式意味着合约以计算机可执行的代码的形式运行，只要参与者达成协定，智能合约建立的权利和义务，就由计算机或计算机网络执行。

基于区块链的智能合约不仅能发挥智能合约低成本高效率的优势，而且可以避免恶意行为对合约的正常执行的干扰。将智能合约以代码化的形式写入区块链中，利用区块链技术实现数据存储、读取及执行过程可追踪透明化且不可篡改。此外利用区块链的共识算法构造的状态机系统能使智能合约高效的运行。

智能合约的功能组件包括：

a） 开发运行环境，包括：

1） 提供编程语言支持，必要时可提供配套的集成开发环境；

2） 支持合约内容静态和动态检查；

3） 提供运行载体支持，如虚拟机等；

4） 对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应

仅限于智能合约范围内，不应影响区块链系统的整体运行。

b） 存储环境，包括：

1） 防止对合约内容进行篡改；

2） 支持多方共识下的合约内容升级；

3） 支持向账本中写入合约内容。

加密安全技术

区块链中使用非对称加密的公私钥对来构建节点间信任。非对称加密算法由对应的一对唯一的密钥（即公开密钥和私有密钥）组成，任何获悉用户公钥的人都可用用户的公钥对信息进行加密与用户实现安全信息

交互。由于公钥与私钥之间存在依存关系，只有持有私钥的用户本身才能解密该信息，任何未经授权的用户甚至信息的 发送

者都无法将此信息解密。加密功能组件具备以下功能：

a） 支持国际主流加密算法，如 AES256 等对称 加密算法和 RSA、ECC 等非对称加密算法；

b） 支持我国商密算法，如 SM4、SM7 等对称加密算法和 SM2、SM9 等非对称加密算法；

c） 应具备明确的密钥管理方案，确保区块链底层安全机制正常运行；

d） 加密算法应具备抵御破解的能力，宜定期审核 加密算法的安全性，必要时采用更高破解计算复杂性的加密算法。

数据存储

区块数据结构在区块链中，数据以区块的方式永久储存。区块链的时间戳解决了区块的排序问题，新区 块生成时便记录着上一个区块通过哈希计算得到的哈希值，实现了区块密码学链接。每一个区 块记录了其创建期间发生的所有交易信息。在区块链中，如果待存储的是一些字符串、Json 对象，可以使用扩展账本结构链存储；如果是图片、视频等较大的多媒体文件，可以将文件的哈希值存储在链上，而原文件可使用云存储存储到云端。

数据存储功能组件包括以下功能：

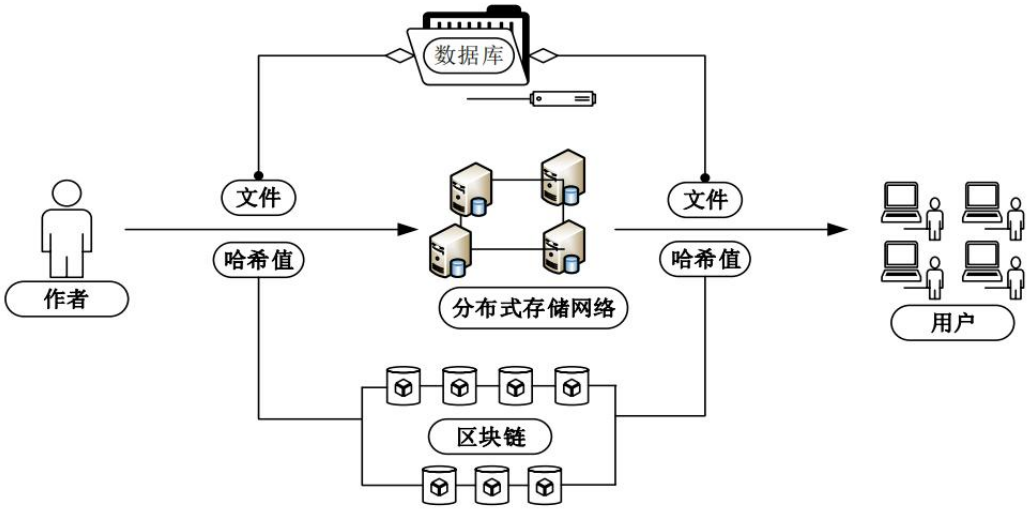
a） 支持持久化存储账本记录；

b） 支持多节点拥有完整的数据记录；

c） 支持向获得授权者提供真实的数据记录；

d） 确保有相同账本记录的各节点的数据一致性。

链外存储



在该系统中有大量的文档，图片，视频数据，不适于存储在区块链上，但是为了保证数据的完整性，我们使用现金的 hash 加密算法，将大型文件输入哈希函数中，输出一个固定长度的哈希值，并将哈希值存储在区块链上，这样既保证了系统的运行速度，又保证了大型文件的安全性。

应用说明

金融行业	非金融机构	政府	跨行业机构	
金融机构	供应链管理平台	身份管理	溯源平台	
国际支付	医院保健平台	档案管理	财务管理与会计	
资本市场	房地产	投票	股东投票管理	
贸易金融	媒体	税收	档案管理	
监管合规审控	能源	政府和非营利组织的透明度	网络安全	
保险		司法，合规与监管	大数据	
点对点交易			数据储存	
非金融机构			物联网	

BaaS 服务

基于数字身份进行对象管理：

BaaS 服务将会以数字身份作为参与的主体来服务商业用户。存在关联交易的商业用户同时在 TU 区块链上登记资产，能够为彼此的数字身份增信，提升其有效性。

对链上数据进行深度挖掘和检测

商业用户或者第三方均可以利用 TU 的数字身份数据，对相关内容和交易历史进行

深度挖掘和检测

一体化的资产管理底层服务：

BaaS 本质上是对商业用户登记在 TU 区块链上的资产加以利用，从某种程度上来说，这是一类偏底层基础设施的资产管理类服务，TU 会在客户端中供基础的应用模块框架。未来，可能还会有更多第三方介入 TU 的区块链服务，相当于一类辅助工具或者插件，以帮助使用 TU BaaS 服务的用户能够更好的实现使用和管理上的优化。BaaS 服务相当于整合了传统的一系列上下游以及周边生态的企业服

务方式，强调了一体化的数据供给和管理

应用实例

零售行业天然具有交易数据碎片化、交易节点多样化、交易网络复杂化的特点。人们通

过在线商城或者线下超市购买商品，其包装都会标注产地信息、生产日期、生产商。但我们很难判断这些信息的真实性。由于造假的利润空间很大，高价值商品，如钻石、皮包、护肤品等存在假货的可能性更高。造假不仅损害消费者利益，损害商家的信誉和品牌形象，社会也不得不消耗资金、人力来行使法律监督和法律制裁。对于商品溯源，目前存在几个痛点：一是商品溯源不仅需要追溯到生产环节、还需要流通环节。这势必增加更多主体共同背书，跨组织协作的难度可想而知；二是无论生产商还是物流商，所使用的系统必然是中心化的，存在信息孤岛问题；三是中心化系统都存在个体作恶的风险。

针对以上三个痛点，TU 提出对应的解决方案——区块链+物联网。

借助物联网，生产和物流环节的数据可通过智能设备实时采集，并通过 VEP 接入到 TU 存储在溯源网络中。区块链独有的数据存储结构和分布式账本技术，确保上链数据不可篡改。同时，非对称加密、相对匿名可确保企业核心信息不泄露。消费者需要查询商品信息时，只要知道商品编码和生产批次，即可追溯到商品的全部信息。

区块链可以解决溯源痛点，同时也不用担心泄露企业隐私。对生产商、物流商、消费者来说，信息都是透明的。更进一步来说，消费信息和物流信息可以给生产商提供决策支持，客户在哪里，生产地如何安排成本最低，生产多少最合适。物流商也同样如此。正因为区块链的存在，信息交互更透明，社会运作更高效.

发展计划

阶段性规划安排

第一阶段，创世界（2017~2018）。利用模块化的设计方法构建安全稳定的区块链网络，这一阶段即可实现智能合约及数字资产，同时我们将引入智能沙盒——一个可以智能化测

试和监测合约运行的环境，沙盒可确保即将正式运行在链上的合约足够安全。

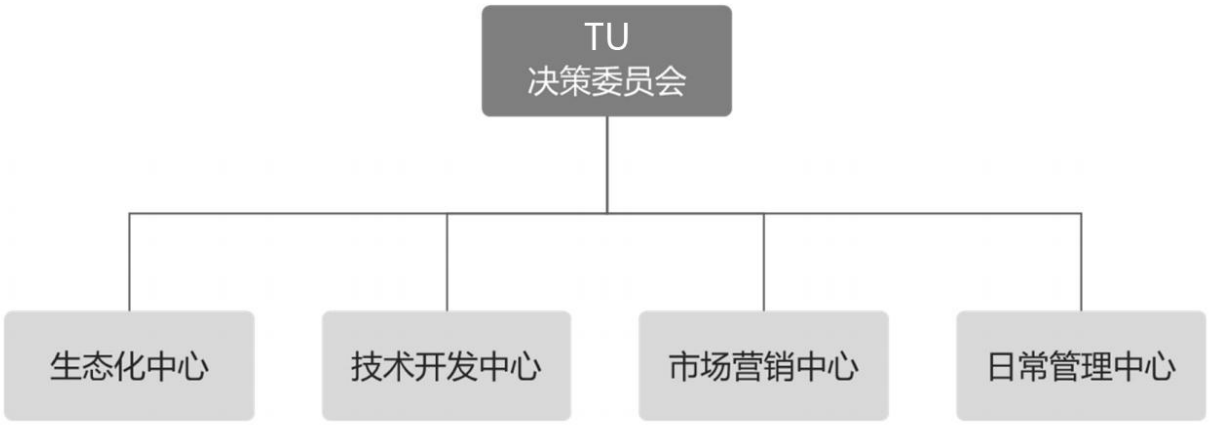
第二阶段，星系（2019~2020）。通过分叉来满足不同的商业诉求，如保险、电子文档、数字货币、溯源追踪、个人信用记录等。这一阶段将实现一个不断进化、容易使用、低成本的、适度定制化的区块链网络。

第三阶段，宇宙（2020~2018）。通过价值互换协议（VEP），将诸多分叉连接，甚至与其他网络（可能是非区块链的）打通数据交互，构建出一个相互连接、多维数据相互关联的网络世界。

治理结构

基金会（以下简称“基金会”）致力于 TU 的开发建设和治理透明度倡导及推进工作，促进开源生态社会的安全、和谐发展。基金会将通过制定良好的治理结构， 帮助管理开源社区项目的一般事宜和特权事项。基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及募集资金的安全性。基金会由生态化中心、技术开发中心、市场营销中心、日常管理中心组成。

基金会治理结构



基金会治理结构

其中，各机构的分工如下：

（1）TU 决策委员会，负责重大事项的管理与决定，包括聘任或解聘执行负责人以及各中心负责人、制定重要决策等。决策委员会成员任期三年，可以连任。委员会设主席一名，由委员会成员投票决定。首届决策委员会成员将由 TU 创始团队及投资人选举产生。

（2）生态化中心，负责探索 TU 与行业结合应用的可能性，从而实现商业落地。重点探索领域为：互联网金融、跨境交易、大数据、人工智能等领域。生态化中心成员在社区中与社区成员交流生态化的发展和未来。

（3）技术中心由负责底层技术开发、测试、上线、审核等。技术中心成员在社区中与权益人、社区贡献者沟通项目进展，不定期举办技术交流会。

（4）市场营销中心负责技术、产品、社区、开源项的推广和宣传。

（5）日常管理中心包括财务、法务、人事、行政等管理。财务负责项目资金的使用和审核；法务负责各类文件的审核与拟定，防范可能存在的各类法律风险；行政和

人事负责人员、薪酬等人事工作以及日常行政工作。

团队介绍

Co-Founder & CEO

CAjay Suryavanshi

Maria Willium

结语

随着 TU 系统不断完善，未来，TU 将会提供更多基础性的区块链服务设施，以便更多第三方开发者能够基于 TU 进行应用插件的开发，让更多普通用户能够便捷地使用我们的数字资产及数字身份的登记与管理服务

常用信息

开源社区 https://github.com/tutvle/