

TERA PLATFORM

尤里伊万诺夫
2019 年 1 月
progr76@gmail.com
(草稿版本: 0.1)

内容

摘要	2
介绍	2
目前区块链的问题.....	2
低速, 没有突破性进展 (火箭科学) 技术	2
DApps 和集中化.....	3
与网络集成.....	3
实施	3
理论方面.....	3
快速路由网络	3
网络协议.....	4
块的输送机处理	5
数据传递和验证的分离	6
数据河	6
区块链数据库大小与用户环境的相关性.....	7
安全	7
实践方面.....	8
处理器线程构成	8
链接	9

翻译 (translation): KEN; weiwu
TERA 交流群 QQ 群: 692191396

摘要

Tera 是一个分散的应用程序平台。这类似于操作系统。Tera 包含集成到 Internet 中的程序和数据存储库。在此平台上发布程序和数据的机制不受审查。循环系统是区块链。

考虑以下几层：

硬件>软件>用户界面>数据库>集中式网络>分散式网络

在 21 世纪，每个人都拥有计算机，笔记本电脑，智能手机，智能手表等计算设备。就其本身而言，这样的设备对于一个人来说是无用的，因此它总是运行一个程序用于显示自身重要。程序的结果显示在用户界面中。经常，这些数据结果被持久保存在装置中的数据层，以便能够再次访问它们。而更大的用处则是通过允许其他用户通过网络进入这些数据里面。从而，每次成功的访问增加了它对于用户的有用性。

为了彼此通信，将设备组合成网络拓扑，其中每个这样的设备被称为节点。将节点组合到网络中的最简单方法是使用单个协调服务器。但由于单点故障，这种解决方案把互动不可靠性集中。还有其他解决方案，其中所有设备都是相同的，具有相同的等级和优先级，我们称之为分散式网络。重要的是要理解分散的网络作为一个整体；节点在整个网络中相互通信作为一个协调良好的机制。为实现这一目标，有一些特殊的节点相互作用算法，我们称之为共识。它可以是：时间共识，交付共识或数据链共识。

Tera 是下一代人机交互。

介绍

目前区块链的问题

低速，没有突破性（火箭科学）技术

早在 2017 年，区块链的主要瓶颈就很明显 - 工作效率低下。从那时起，情况没有改变。该行业需要一种技术，使全世界数亿人能够使用它，并使用动态可扩展性。

缺乏此类技术会导致行业停滞不前，失去加密货币在交易所的资本化。

Dapps 和集中化

Dapp 一词代表分散应用，但目前它被不正确的使用。（目前）它被称为与区块链中的智能合约交互的程序，实际上位于中心化服务器上。核心部分是中心化处理器，因为没有它就无法使用。这样的 DApp 只能保证用户资金的保存从它诞生伊始。这种情况是由于现代区块链不在其平台上提供托管服务。在现有的区块链中没有这类事情（托管服务）作为用户界面。（TERA 是例外）

与网络集成

区块链仍然太虚拟，普通用户无法理解；他们没有在眼前看到它。一个人很难相信自己从来没有看到的东西。将可视化界面添加到区块链将允许用户立即查看并开始使用它。

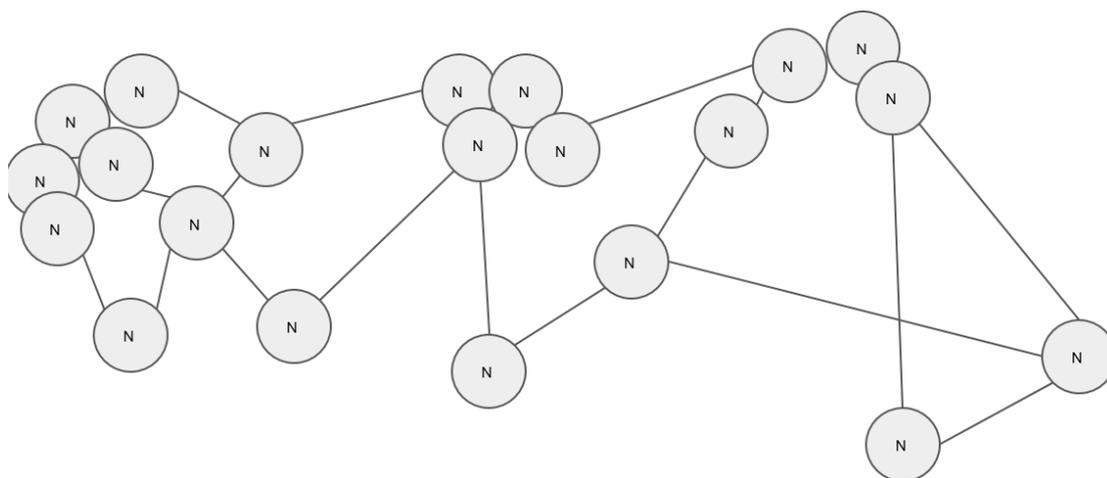
软件开发的简单性将有助于区块链的真实分布。要做到这一点，智能合约的语言应该尽可能简单和熟悉。你需要使用一个简单的语言和现代、通用技术（JavaScript 和 HTML），通过基本熟悉度以最大化接受率。在 IT 行业 Web 程序员是最大的区块链用户群体。他们将能够在区块链上快速创建流行的应用程序，并使所有用户尽可能方便地使用 Dapps。

实施

理论方面

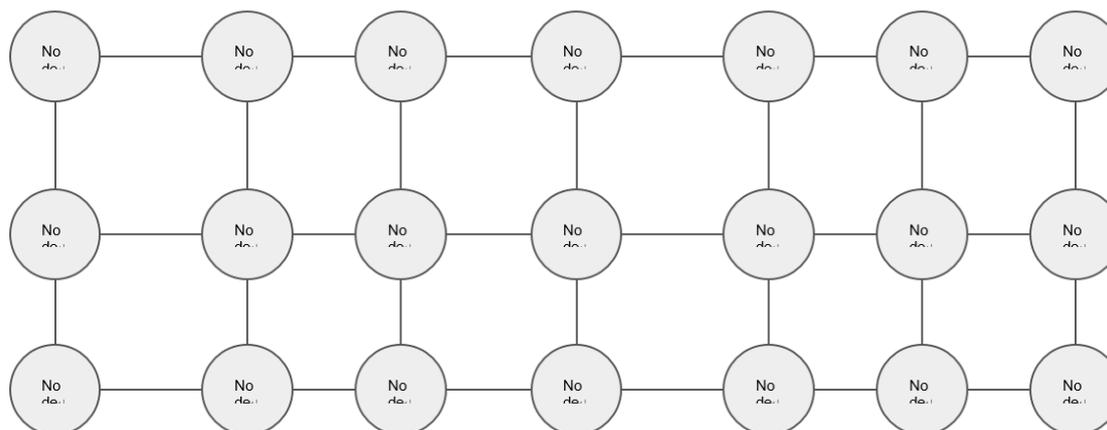
快速路由网络

传统的区块链不使用节点的顺序。网络的整体情况看起来是随机的，如下所示：



这种链接的随机组织不保证在所有节点之间快速传递块。

在 Tera 中，节点将自己组织成有序的通信方式：



区块链从第一个节点到最后一个节点传递数据的时间不超过 3 秒。为了实现这一点，基于节点的地址彼此的相似性，节点在特殊连接中彼此连接。节点地址是随机值（32 字节），在节点操作期间不会更改。与其他节点的连接数量与网络中节点的数量具有对数关系，从而实现相对恒定的事务传递时间。因此，如果网络由 10 亿个节点组成，则节点之间的传递时间仍然不会超过 100 毫秒（ms），因此最大时间将为 $30 * 100 \text{ ms} = 3 \text{ 秒}$ 。在节点之间传递事务的 100 ms 延迟时间是上限，但在实践中，这类延迟低于 100ms，因为具备相互较小延迟互动的节点拥有连接优先权。

网络协议

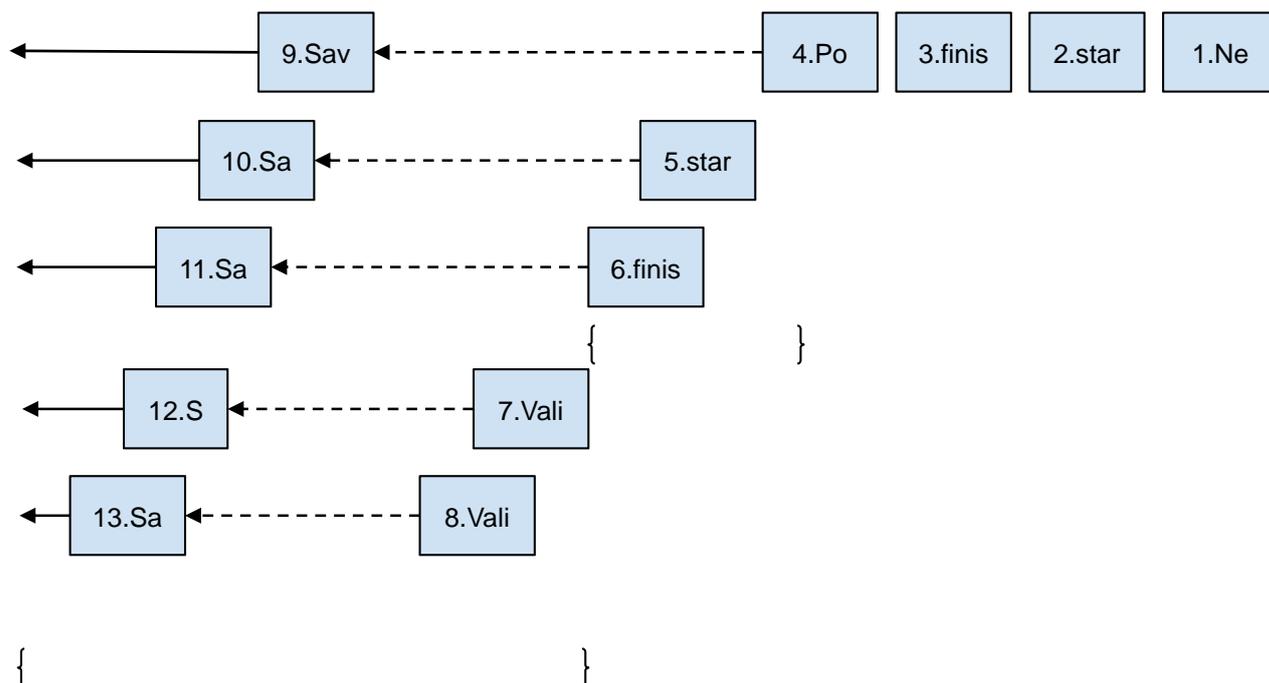
该事务由用户发送到 N 个相邻节点（其中 N 为 5 到 16）。事务被添加到新形成的块（当前秒形成的块）。当交换阶段到来时，事务开始从一个节点移动到

另一个节点，在块中累积。如果一个块包含的事务数多于它可以容纳的事务数，则剩下具有大 PoW 的事务 - 这就是 DDOS 保护的实现方式。在块形成阶段结束时，执行签名阶段和 PoW 块计算（1 秒），然后开始具有最大 pow 的领导块搜索的三秒阶段。该块被添加到区块链中。

块的输送机处理

区块链：形成每秒的块数，但确认块的时间（即区块链中块的开启时间）为 8 秒。为了创建比确认时间快 8 倍的块，使用块的流水线处理。这可以被认为是 8 个独立的区块链，形成周期为 8 秒。每个这样的区块链相对于彼此移位一秒钟。因此，我们创建第一个区块链的块一秒，第二个区块链的块为下一秒，依此类推到第 8 个区块链。为了将这些区块链连接成一个，它们粘在一起。在传统的区块链中，前一个块的散列包含在每个块的标题中的单个链中。在 Tera 区块链中，出于这些目的，根据 8 个区块链中每个区块链的几个先前区块计算前一个区块的哈希值。在这个阶段，我们将 8 个链的逻辑绑定合二为一。

并行处理多个块，处理顺序取决于当前时间（当前块）：



（区块从网络加载，加载网络）

定时：

- 1 新的（当前）块，从 MemPool 加载事务，定时器激活
- 2 同步单元的开始（分布式单元）

3 同步结束

4 捆绑数据块与前面的块，计算 PoW

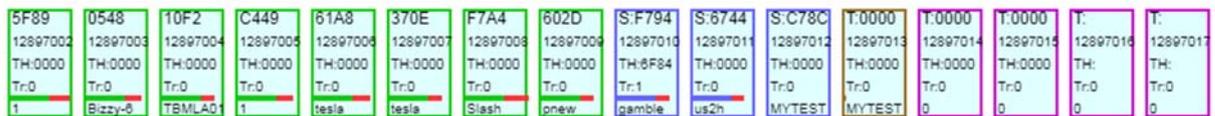
5 搜索从最大 PoW 网络开始

6 最大 PoW 搜索结束

7 检查设备的有效性，考虑到由于下载具有较大总 PoW 的新块链而可能对先前块进行的更改。

从图中可以看出，块指的是前面的块，但是具有 8 个块的 Delta。一旦确定有效并存储在数据库中，则来自第 8 个的块然后参与其他节点中的卸载（类似地，它们可以从其他节点加载）。

这就是块在 Tera 区块链浏览器页面中的样子：



5F89	0548	10F2	C449	61A8	370E	F7A4	602D	S:F794	S:6744	S:C78C	T:0000	T:0000	T:0000	T:	T:
12897002	12897003	12897004	12897005	12897006	12897007	12897008	12897009	12897010	12897011	12897012	12897013	12897014	12897015	12897016	12897017
TH:0000	TH:6F84	TH:0000	TH:0000	TH:0000	TH:0000	TH:0000	TH:	TH:							
Tr:0	Tr:1	Tr:0													
1	Bizzy-5	TBMLAD1	1	tesla	tesla	Slash	onew	gambler	us2h	MYTEST	MYTEST	0	0	0	0

数据传递和验证的分离

网络中的每个节点都与其他节点相同。节点数量不受限制。节点之间的通信是通过组织单个数据链来实现的，其中信息以命令（交易）的形式记录。通常这种链被称为区块链，但在这个平台中，它的应用程序被扩展。传统上，块被写入交易。在这种情况下，不允许写入无效的交易块（例如，具有不正确的数字签名，账户中的资金不足，双重支出等）。在 Tera 平台中，区块链用作传输，因此可以将任意信息写入块（此后，我们将其称为交易）。对信息正确性的解释取决于更高级别的应用程序。区块链具有确定哪个数据链为真的共识机制，但此共识不包含用于解释块内事务的规则。块数据是一个黑盒子 - 所有操作都像一组字节一样执行。PoW 算法用于防止 DDOS 攻击。事务的长度越大，PoW 的值就越大。在将事务发送到网络之前，客户端计算 PoW 值。

数据河

Tera 平台可以抽象地表示为水道，这保证了船舶与货物集装箱通过的连续性和数字顺序。该渠道不对船舶和货物的管辖权负责。船舶的实用性受到港口，渔船厂，仓库等的影响，它们为船舶提供了有用的工作。

怎么用？

假设您需要将货物运送到港口 B，并且港口 A 已将货物放入集装箱并将其发送到港口。在 B 口，检查所有集装箱是否有正确的内容，并在找到货物时取货。该通道仅需 8 秒即可将船只运送到目的地的所有港口。

这里的一个重要方面是数字命令。区块链的目的是确保每个设备都有单个订单和块组合。如果提供了这个，那么读取它们的程序将始终在世界上的所有计算机上产生相同的结果 - 因此数据是相同的。因此，即使这些块是不正确的事务，双重花费等等，用户端的程序也会看到它并拒绝其执行。这称为事务验证过程。为了加速整个系统，我们将其与块交付流程分开。因此，我们可以在另一个时间和另一个过程中执行验证，而不会干扰区块链，并且由于大量检查而更快 - 我们可以将操作分组并加速工作，因为数据库访问次数减少。

区块链数据库大小与用户环境的相关性

由于大量数据将不可避免地以 1000 tps 发生，新用户应该能够快速下载区块链以验证它并开始使用它。因此，下载顺序会发生变化 - 如果之前是从链的开头，则现在将从最后下载。

加载信息取决于用户的设置环境 - 关于他为区块链分配的磁盘存储器的大小。根据大小，下一个下载优先级将是：

- 1、账户表
- 2、块标头
- 3、块或交易的内容

它将如何工作：

对于超级轻的客户端：只会加载部块头和一块清单表将被加载。

对于普通客户：整个帐户和标题表，但只是部分内容块

对于完整的客户端 - 所有数据（正如现在所做的）

安全

在比特币网络中，为了保护用户免受双重花费，必须等待至少 10 分钟，有时需要 1 小时。

在 Tera 网络中，每秒都会创建一个块，但如果您想要比比特币网络具有相同程度的可靠性，则需要等待相同的时间。等待的时间是可靠度。在任何 POW

算法中，不存在魔术（即改变时间获得同等可靠性）。在 TERA 我们有更加灵活的选择，您可以等待 8 秒，1 分钟或 1 小时（例如，转移价值数百万美元的金额）。

实践方面

Tera 中区块链的一个重点是网络的连续运行。通过创建具有动态结构支持的多维晶格拓扑来形成网络。交换每秒执行一次。节点必须不断地与其邻居交换关于新块的信息（该任务将被称为 TRANSFER）。即使节点处于区块链加载模式（即未同步），也应执行此类交换。

处理器线程构成

启动完整节点时，将创建以下进程（节点）：

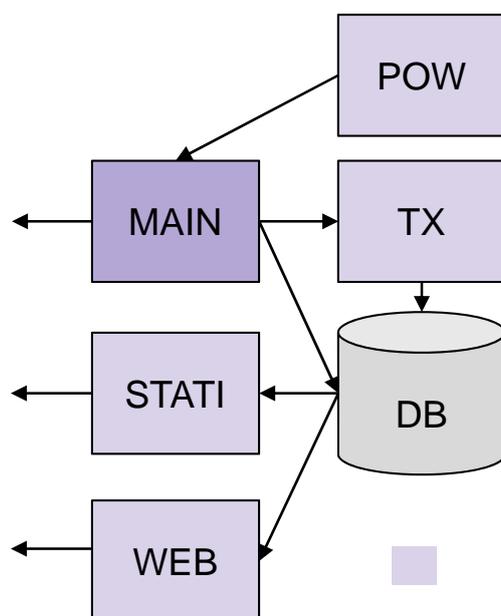
MAIN - 程序的主要线程+ TRANSFER。将新块写入数据库。不同步时加载历史记录。

STATIC- 向其他节点（标题，块，状态）提供静态信息

TX- 执行事务（更改状态表）。

Web -通过 HTTP 进行数据检索以与 WEB 完全集成

POW -mining 过程。带有哈希的记忆泵和快速搜索给定的匹配。



链接

1 网站: <https://terafoundation.org>

2 基于 TERA 平台去中心化应用的发展:

<https://docs.google.com/document/d/1PXVBbMKdpsAKPkO9UNB5B-LMwIDjylWoHvAAzrXjvU/edit?usp=sharing>

该币的细节:

名字:Tera

共识:POW

算法:TERAhash (sha3 + Optimize RAM hashing)

总量:10 亿 (TERA)

奖励:1-20 币, 取决于矿工算力 (当下总量的十亿分之一 \times 矿工算力的对数的平方取值的 1%)

区块大小:120 KB

预挖:5%

开发基金:1%的总量

块生成时间: 1 秒

块确认时间: 8 秒

速度:目前 1000 次每秒

手续费: 无