TERA 平台

Yuriy Ivanov（Vtools）

中文翻译：Block

2019 年 2 月 5 日

progr76@gmail.com

内容

双花

区块确认数计算

矿工经济激励

DDOS 攻击保护

实践角度

规范

处理器线程构成

相关链接

概述

TERA 是一个去中心化应用的平台。这类似于一个‘’操作系统。TERA 由一个集成到互联网的程序和数据存储库构成。在该平台上发布程序和数据的机制不受审查，加密货币是通证经济的血液，而区块链则使其流淌。

考虑以下几层：

硬件>软件>UI>数据库>中心化网络>去中心化网络

在 21 世纪，每个人都有一个计算设备，比如一台电脑，一台笔记本，一部智能手机，一块智能手表等等。就其本身而言，这样的设备对一个人来说是没有意义的，所以它总是运行一个程序并且执行一些有用的东西。程序的结果显示在用户界面中。通常,结果持久地存储在设备的数据层中，以便能够再次访问。更大的用处是允许其他用户通过网络访问这些数据。因此，来达到为用户增加每一个连续实用性的目的。

为了相互通信，由设备组合而成的每一个节点构成了一个网络拓扑结构。将节点组合成网络的最简单方法是使用单个协调服务器。，但由于单点故障导致相应的不可靠性也表明这样的解决方案是中心化的 „。

还有一些其他的解决方案，所有的设备都是平等的，具有相同的等级和优先级，我们叫它去中心化网络。。重要的是要理解去中心化网络的整体工作原理；节点之间作为一种协调良好的机制在整个网络中进行通信。为了实现这一点，有一些特殊的算法用于节点之间的交互，我们将其称为共识。可以是:时间共识、传输

共识或数据链共识。

TERA 是人类及软件交互的下一个时代。

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——那就是它的工作缓慢。在那之后的时间里情况也并未改变。这个行业需要一种能让数亿人受益的技术并且使得世界各地的人们都来使用，这就使用了动态可扩展性。

这种技术的缺乏导致行业的停滞和交易所上加密货币的资本化损失

DApps 和中心化

Dapp 一词代表去中心化应用，但目前应用不当。它是一个通过区块链中的智能合约交互并且实际上位于一个中心化服务器的程序。集中服务器上的那部分是关键，因为没有服务器是无法使用的。这样的 DApp 只能保证用户资金的保存，因为他们在区块链上。

这种情况是由于当前的区块链在其平台上不提供托管服务 ,并且现有区块链上不存在用户界面(TERA 区块链除外)。

与网络集成

区块链对于普通用户来说仍然过于虚拟导致无法理解;他们从未能在眼中看到。

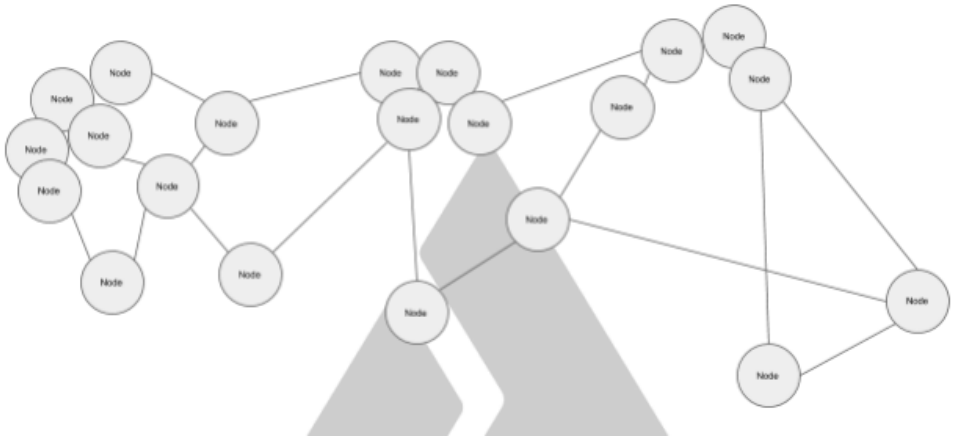
相信你从未见过的东西是很困难的。向区块链添加可视化接口将允许用户立即查看并开始使用它。软件开发的简化将有助于区块链的实际分配。为此，智能合约的语言应该尽可能简单和被人熟悉。你只需使用简单的语言和现代的通用技术(Javascript 和 HTML)，通过基本的熟练度来最大限度地提高采用率。网站程序员是 IT 行业中最大的区块链用户群体。他们将能够在区块链上快速创建流行的应用程序，并尽可能方便所有用户使用 dapps。

实施

理论角度

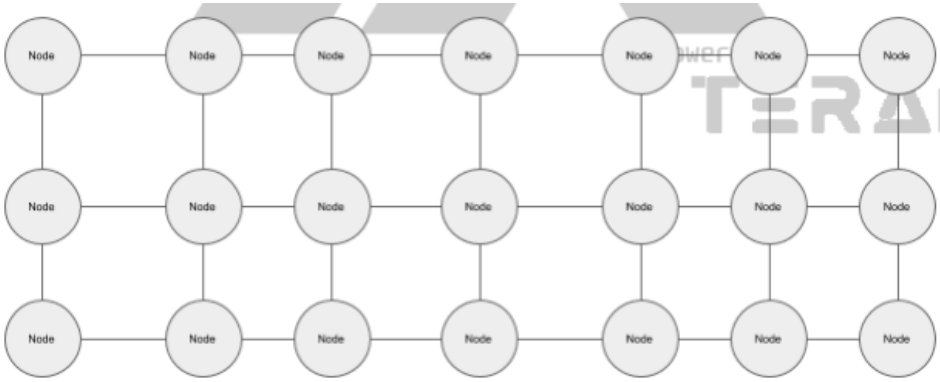
一个快速的路由网络

传统的区块链不使用节点之间的顺序。整个网络看起来是随机的，就像这样: :



这种随机的链接组织并不能保证在所有节点之间的快速传递。。

而在 TERA 中，节点自发组织成有序的通信方式: :



区块链将数据从第一个节点传递到最后一个节点的时间不超过 3 秒。

为了实现这一点，基于节点地址之间的相似性，节点之间通过特殊的连接方式进行连接。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与网络中节点的数量呈对数关系，从而实现相对恒定的交易传输时间。

因此，如果网络由 10 亿个节点组成，节点之间的传输时间仍然不超过 100 毫秒(ms)，因此最大时间将是 30*100 ms = 3 秒。节点之间传输交易的延迟时间 100 ms 是上限，但在实践中，它小于 100 ms，因为延迟较小的节点间具有连接优先级。

为了使成功的连接更加持久，每个节点会统计不同区块内容之间成功交换的信息。此统计的信息会影响连接优先级。

网络协议

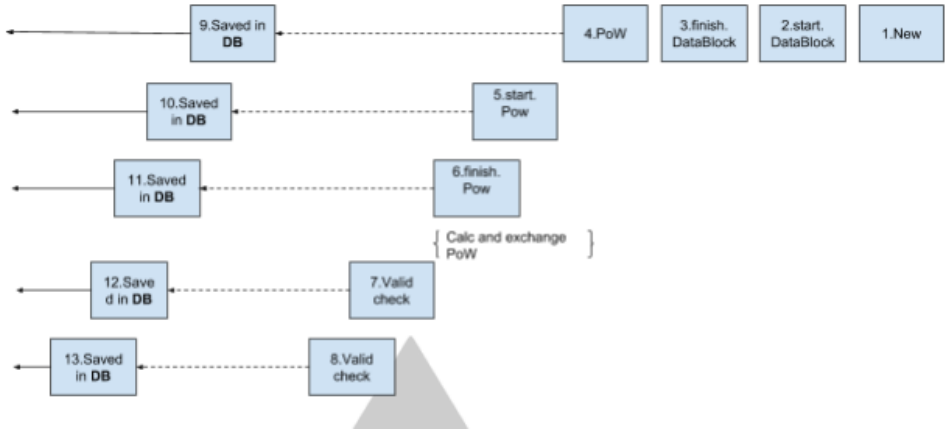
交易由用户发送到 N 个相邻节点(其中 N 是从 5 到 16)。交易被添加到新生成的区块中(当前第二个块)。当交换阶段到来时，交易开始从一个节点移动到另一个节点，并在区块中积累。如果一个块包含的交易多于它的容量，那么需要大量工

作量证明的交易会被留下——这就是 DDOS 保护的实现方式。在区块生成阶段结束时，执行签名阶段和 PoW 区块计算(1 秒)，然后开始为期 3s 的具有最大工作量证明的区块搜索。这样的区块被添加到区块链中。

区块传输处理

区块链:每秒形成块的次数 ,但区块的确认时间(即区块链中区块的接通持续时间)为 8 秒。为了使创建区块的速度比确认时间快 8 倍 ,使用了区块的流水线处理。这可以被认为是 8 个独立的区块链，形成周期为 8 秒。每一个这样的区块链相对于其他都会相对移动一秒钟。因此，我们在一秒内创建第一个区块链的区块，在第二秒内创建第二个区块链的区块，以此类推，直到第 8 个区块链。为了将这些区块链连接成一个区块链，它们被粘在一起。在传统的区块链中，前一个块的哈希包含在每个单链的区块头中。在 TERA 区块链中，为了达到这些目的，前一个区块的哈希值是基于 8 个区块链中每个的前几个区块计算出来的。在这个阶段，我们将 8 条链的逻辑绑定成一条。

几个块并行处理，处理顺序取决于当前时间(当前块):



区块上传以及上传到网络

（从网络）

时间点：

1. 新(当前)区块，从 MemPool 加载交易，计时器激活
2. 同步单元(分布式单元)的开始
3. 同步结束
4. 将数据块与前面的区块捆绑在一起，POW 运算
5. 最大 PoW 网络搜索开始
6. 最大工作量证明搜索结束
7. 检查该单位的有效性，考虑到由于下载新的区块链与大的完整的工作量证明而可能改变的之前区块。

从图中您可以看到，该区块引用前面的区块，但是增量为 8 个区块。

一旦确定有效并存储在数据库中 ,来自第 8 个节点的块就会参与到其他节点的卸载中(类似地，它们也可以从其他节点加载)。

这是在 TERA 区块浏览器页面中的区块：

数据传输与验证分离

网络中的每个节点都相等。节点的数量是无限制的。节点之间的通信通过组织单个数据链来实现，其中的信息以命令(交易)的形式记录下来。通常这样的链称为区块链，但是在这个平台中，它的应用程序被扩展。传统区块链中，交易被写到区块中。在这种情况下，不允许写入交易块，这是无效的(例如，数字签名不正确、账户资金不足、双花等)。在 TERA 平台中，区块链作为一种传输工具，可以将任意的信息写入区块中(以后我们称之为交易)。对信息正确性的解释取决于更高层次的应用。区块链有一个共识机制来确定哪个数据链为真，但是这个共识不会解释区块内交易的规则。区块数据是一个黑匣子——所有操作都是用一组字

节执行的。PoW 算法用于抵御 DDOS 攻击。交易的长度越长，PoW 的值就必须越大。在将交易发送到网络之前，客户端计算 PoW 值。

数据河

TERA 平台可以抽象地表示为一个水道，它保证了集装箱船舶通过的连续性和数理顺序。航道不对船舶和货物负责管辖。船舶的效用包括港口、渔场、仓库等，它们为船舶装载提供有用的工作。

它是如何使用的？

假设你需要把货物送到 B 港，而 A 港已经把货物装进集装箱并送到了港口。在 B 港，检查所有的集装箱是否有正确的内容，当你找到货物时就去提货。该通道仅用 8 秒就能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理顺序。区块链的目的是确保每个设备有一个区块的单一顺序和组成。如果提供了这种方法，那么读取它们的程序将在世界上所有的计算机上生成相同的结果——所以数据是相同的。因此，即使这些区块包含不正确的交易、双花等等，用户端的程序也会看到它并拒绝执行。这称为交易验证过程。为了加快整个系统的速度，我们将其从区块传输过程中分离出来。因此，我们可以在另一个时间和另一个进程中执行验证，而不影响区块链，由于大量检查，我们可以更快地执行验证——由于较少的数据库访问，我们可以对操作进行分组并加快工作速度。

自定义区块链数据库大小

对于在 1000 tps 时不可避免地会出现的大量数据，新用户应该能够快速下载区块链来验证它并开始使用它。因此，下载顺序发生了变化——如果以前是从链的开头下载的，现在将从链的末尾下载。

加载信息将取决于用户的设置——取决于他为区块链分配的磁盘内存大小。根据大小的不同，下一个下载优先级将是:

1. 账户图表
2. 区块头
3. 区块或者交易的内容

它将怎样工作：

1. 对于超轻量级客户端:只加载头文件的一部分和发票表的一部分。
2. 对于普通用户:整个帐户和标题表，以及部分块的内容
3. 对于全节点客户端-所有数据(如现在所做的)

例子：

用户为磁盘上的区块链分配空间，例如 12GB

这个磁盘空间会被分为三个部分:

•常规区块结构(从末尾开始)，例如 5GB

•其他不包含在常规结构中但需要存储在节点上的区块

(由 DHT 原则决定，即，节点地址的相似度)，例如 5GB

•最后一个常用的区块，例如 2 GB

安全

双花

TERA 区块链使用 PoW 共识机制。所有的交易都会按照一定顺序安排执行。

从账户中提现时，要核对必要的数量。在记录时，计数器“OperationID”会递增。

每个后续的支付交易必须有下一个“OperationID”号来防止同一交易被多次花费。

计算区块确认数

在比特币网络中 ,为了防止用户双花 ,至少需要等待 10 分钟 ,有时甚至一小时。

在 TERA 网络中，每秒钟都会创建一个区块，但是如果你想要具有和比特币网络一样的可靠性的话——你需要等待同样的时间。你等待的时间与可靠性的程度相关。这不存在魔法;在任何 PoW 算法中，您都要用时间来换取一定的可靠性。

在 TERA 中，我们做出了更灵活的选择。您可以等待 8 秒、1 分钟或 1 小时(例如，如果，转移价值数百万美元的资金)。

矿工经济激励

矿工平台为区块执行复杂的哈希计算，以保证区块链的不变性。

对找到的哈希块的奖励为矿工提供了经济激励。这个奖励的计算方法如下:剩余未分配货币余额的十亿分之一(0.000000001)乘以全网算力对数的平方的百分之

一。

最初,未分配的总额等于 10 亿枚硬币(tera 的总发行量),所以随着时间的推移,奖励将下降,但这将由实际交易率上得到补偿,以及反向补给由于支付交易的未分配代币余额：

•10 TERA -为限制队列之外的用户创建一个新账户

•100 TERA-创建一个智能合约/DApp

•10000 TERA -创建智能通证(即发行代币)

付款进入账户 0(即回到未分配的挖矿余额)。

通过 DAO 投票机制，交易费率将继续发生变化。

抵御 DDOS 攻击

每个区块的大小限制为 130kb;平均交易大小为 130 字节，因此平均每个区块可以承载 1000 个交易。每个交易必须有一个工作量证明字段，它记录哈希计算所做的工作。此字段用于确定该交易是否包含在该区块中。它必须至少有一个确定的值，并且必须足以与其他交易竞争。只有前(大约)1000 个工作量证明值最高的交易包含在区块中。

计算:

区块链的大容量，以及在发送的每个交易中强制执行 PoW 的要求，使您可以有效地组织 DDOS 防御，但有以下限制:

•攻击者的处理能力为普通用户的 1000 倍以内。

•平均网络负载为 50%，即每秒 500 个交易。

在这种情况下 ,攻击者每秒可以发送 1000 个交易。当您第一次在网络中发送时，将有 1000 个交易，并攻击 500 个常规用户，只有 1500 个交易。区块链只接受 1000 个交易 ,因此将舍弃 500 个交易(普通用户和攻击者将各自丢失三分之一的交易)。但与此同时，PoW 交易的平均算力将会增加，因此，在下一个块中，普通用户将花费更多的计算时间来发送交易(即两倍的时间)。与此同时，攻击者将无法增加 PoW 交易计算的能力，因为他最初工作在容量的极限(100%)。因此，一个普通用户的 PoW 交易的平均算力将增加一倍，并且在普通交易之间的区块中所占的比例也将增加一倍。攻击者的攻击将会 500 笔 500 笔的出现。也就是说，所有用户交易都将被接受。

从这些参数可以看出，区块链的工作负载越小，应用 DDOS 攻击就越困难。一旦区块链的平均负载超过 50%，我们就会增加交易的上限阈值。目前，每个矿工的节点实际上只使用一个线程支持交易处理。考虑到目前多核处理器是标准的，因此将每个节点的交易处理性能相乘并不困难。

实践角度

规范

共识机制:POW

算法:TERAhash (sha3 +优化 RAM hashing)

总供应量:10 亿

区块奖励: 剩余未分配代币余额的十亿分之一(0.000000001)乘以全网算力对数的平方的百分之一

区块大小：130KB

预挖: 5%

发展基金:1%挖矿所得

区块生成时间:1 秒

区块确认时间:8 秒

速度:每秒 1000 个交易

矿工费:免费

密码学应用:sha3 secp256k1

防止 DDoS: PoW(哈希运算)

平台:node . js

处理器线程的组成

TERA 中区块链的一个重要特点是网络的连续运行。该网络是通过创建一个具有动态结构支持的多维网格拓扑结构而形成。每秒钟进行一次交换。节点必须不断地与其邻居交换关于新区块的信息(此任务称为传输)。即使节点处于区块链加载模式(即不同步)，也应该执行这种交换。

当您启动一个全节点时，将创建以下进程(节点):

1. MAIN -程序的主线程+传输。向数据库写入新块。

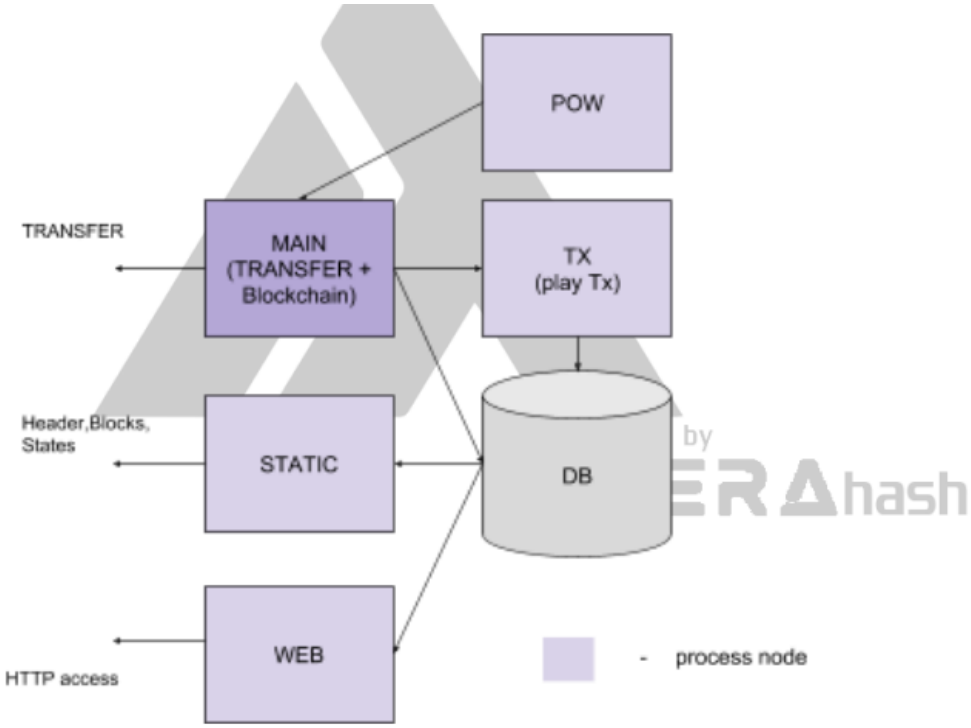
不同步时加载历史。

2. 静态——向其他节点(头、区块、状态)提供静态信息

3. TX-执行交易(更改状态表)。

4. Web-通过 HTTP 检索 WEB 数据，以便与 WEB 完全集成

5. POW-挖矿进程。哈希运算使得内存占用提升并且快速搜索给定匹配。


POW
TRANSFER
MAIN
(TRANSFER +
Blockchain)
TX
(play Tx)
Header,Blocks,
States
STATIC
DB
WEB
HTTP access
- process node

Links

Website: https://terafoundation.org/

Bitcointalk ANN: https://bitcointalk.org/index.php?topic=4573801.0

Repo: https://sourceforge.net/p/tera/code/ci/master/tree/

Tools:

TERA Decentralized Exchange: https://terafoundation.org/dapp/20

Online Node Map: https://terafoundation.org/map.html

Web Wallet: https://terafoundation.org/web-wallet.html

Top Miners: http://www.terafoundation.online/top/

API: https://sourceforge.net/p/tera/code/ci/master/tree/Doc/Eng/API.md

Constants: https://sourceforge.net/p/tera/code/ci/master/tree/Doc/Eng/CONSTANTS.MD

Docs:

DApps Paper:

https://docs.google.com/document/d/1PXVBbMKdpsAKPkO9UNB5BLMwIDjylWoHvAAzzrXjvU/edit?usp=sharing

DApps FAQ;

https://docs.google.com/document/d/1PXVBbMKdpsAKPkO9UNB5B-LMwIDjylWoHvAAzzrXjvU/edit

DEX-Guide:

https://docs.google.com/document/d/1qvVRfLq3qcYYF6dcsAAAqoGyBFF4njXUYZXZfTP

Wd2w/edit?usp=sharing

BTC for DEX:

https://docs.google.com/document/d/19vRY6tkbTP8tubZxM01llwnMyz4P6lzY0zvnargrU6k/edit?usp=sharing

Social Media;

QQ: https://jq.qq.com/?_wv=1027&k=58VsQxc

Twitter: https://twitter.com/terafoundation

Discord Invite Link: https://discord.gg/CvwrbeG

Telegram: https://t.me/terafoundation

(German) Telegram: https://t.me/terafoundation_germany

(RUS) Youtube: https://www.youtube.com/channel/UCGQeUCUKZgH0DfbakD7gjqQ