迈斯链·迈斯币

2018

迈斯链·迈斯币
MES Chain
白皮书

POINT

·权益 ·娱乐 ·影视

全球影视娱乐通证

前言

.....

目录

1 背景

.....

2 相关术语

迈斯链（MES Chain）是我们的品牌以及底层区块链平台的名称。

迈斯链（MES Chain）是一个整合影视娱乐资源的的娱乐应用主链。

对现在版权零散的影视娱乐行业，我们进行了资源整合，创建了一个全球的去中心化，可信任的安全信任链，将影视的版权信息，版权授权以及其他娱乐资源转化成了可信任的迈斯链资产。版权人，用户以及明星等等通过持有迈斯链产生的迈斯币持有版权，出售版权，购买版权，通过迈斯链可信的网络与去中心化的能力，保证了用户的利益。

迈斯链携手公众大V，明星带动行业的资源流动，让大V们获得他们影像义相当的价值回报，同时让支持他们的粉丝们获得福利。

MES Token是指迈斯链基于区块链技术发行的权益数字代币，可以在迈斯所中与其他的Token进行交易易，也可以在将来在外部交易易所与其他加密数字货币进行兑换。
MES Token也是全球影视娱乐通证，是迈斯链与第三方专业机构合作研究，所推出的面向公众的全球影视娱乐数字资产交易平台的唯一指定代币。

迈斯所是一个交易平台，在这里，可以将MES Token与其他基于影视娱乐所发行的Token进行交易，迈斯所也是迈斯链生态系统的核心组成部分。

3 优势

技术上，迈斯链在比特币以及以太坊的基础上升级了共识，独创DPOS与PBFT相结合的共识机制，既保证了去中心化，也保证了数据的完整性可信任性。同时动态轮段见证节点和区块生成策略保证了见证的利益，依旧保证了迈斯链稳定运行。
资源上，迈斯链通过与大V和明星等公众人物合作，创建明星节点，充分利用粉丝文化，最大限度的发挥了资源的利用率，资源的丰富程度保证了迈斯链的稳定发展，从而形成良性循环。
回报：迈斯链通过去中心化的节点根据节点的工作量奖励拥有迈斯币的工作节点，从而鼓励节点见证宣传迈斯链。

4 应用

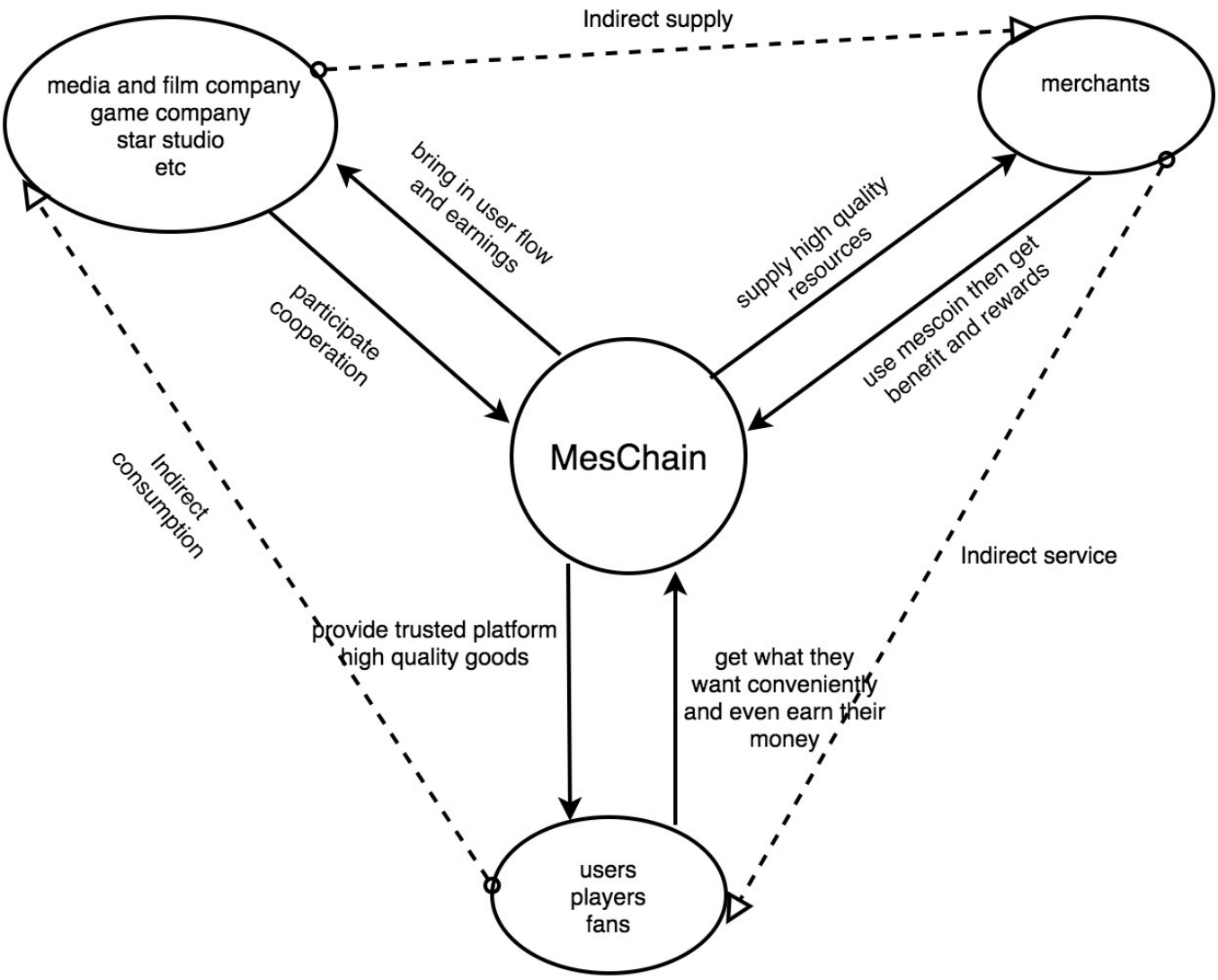
4.1 存储

得益于迈斯链的技术架构，可以存储公证信息，版权信息等信息到迈斯链上，而保证不被篡改。

4.2 交易

- 版权购买：通过迈斯链产生的迈斯币可以直接购买影视版权，同时得到迈斯链的奖励。
- 票务：通过与明星合作迈斯链，通过迈斯链可以快速购买演唱会门票，以及其他活动的入场券，可以获得和明星合影，签名，见面会等福利奖励。
- 物品拍卖：基于去中心化，以及可信任的机制我们可以公开透明的拍卖物品，以迈斯币作为抵押，避免了恶意竞拍
- 币币兑换：在交易所通过迈斯链的迈斯币也可以与其他的区块链货币相互兑换

4.3 交易流程



5 技术架构

5.1 MESChain架构

迈斯链(MES Chain)的架构与现有的众所周知的区块链相似，比如比特币和以太坊，节点通过Gossip协议传播数据。系统将数据和状态切分成不同分片。系统中每一个节点都将被包含在一个分片中。交易记录（UTXO）存储在相应分片中节点的内存中。这产生了几个新的挑战。

- 如何在大量交易的时候稳定快速的出块。
- 如何保证账本以及其副本不被篡改。
- 如何保证有大量节点时交易速度不受到影响。
- 如何随着账本的增大保证交易速度不过多的受到IO的影响

为了公平和安全的解决上述问题，避免被恶意节点利用规则，我们需要让操作随机。例如，将账本存储分配到不同的分片中，根据交易拥堵情况动态调节见证节点数量等

在本文的技术细节部分，我们将介绍用于解决这些问题的技术方案。

- 在第6.1章中，我们将详细探讨 ***DSFT 高级容错权益委托共识（Delegated proof of Stake with Fault Tolerance）*** ，。
- 在第6.2章中，我们介绍了 ***DEC 动态时间段轮换算法（dynamic epoch circle）*** ——一种动态分配见证节点控制出块速度的动态调节时间段算法
- 在第6.3章中，我们介绍了 ***SSA 存储分配算法（store sharing algorithm）*** – 利用一定的随机参数但是却能稳定定位存储片的存储分配算法

5.2 Dapp开发

MES Chain 提供标准的JSON RPC接口和Web接口方便开发Dapp，对比其他公链如ETH,EOS等，我们不限制开发语言，提供了C++,JAVA,NodeJS SDK方便广大开发者开发。

6 技术细节

6.1 DSFT 高级容错权益委托共识

MES Chain 独创DSFT（Delegated proof of Stake with Fault Tolerance）高级容错权益委托共识。将DPOS（Delegated Proof of Stake）权益委托证明共识与SPBFT（Super Practical Byzantine Fault Tolerance）高级拜占庭容错共存。

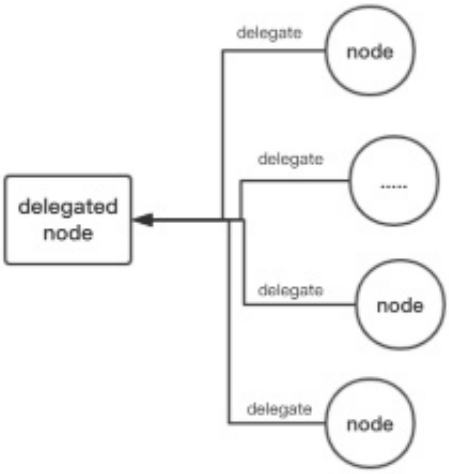
- 为什么不采用POW和POS?

POW（Proof of work）工作量证明共识解决了可信任的问题，即通过不断的计算得出的结果已证明自己的权益，但是同时也带来了一些问题，比如双花攻击，电力耗费过大等问题。

POS（Proof of stake）股权证明共识，对比POW它不需要的产生大量算力电量消耗，双花攻击所需要的代价远大于可能获得的利益。因为最有可能进行双花攻击的人就是工作的人，它们不会破坏自己的利益。但是POS的币龄也带来了一些问题，比如币龄长的节点长期离线可能会导致数据同步速度和交易速度受到影响，币龄的权重过大鼓励了这种滥用。以及还会面临账本分叉（Nothing at Stake Problem），贿赂攻击（Briber Attack）等，由此我们采用了DPOS（Delegated Proof of Stake）。

- 为什么采用DPOS?

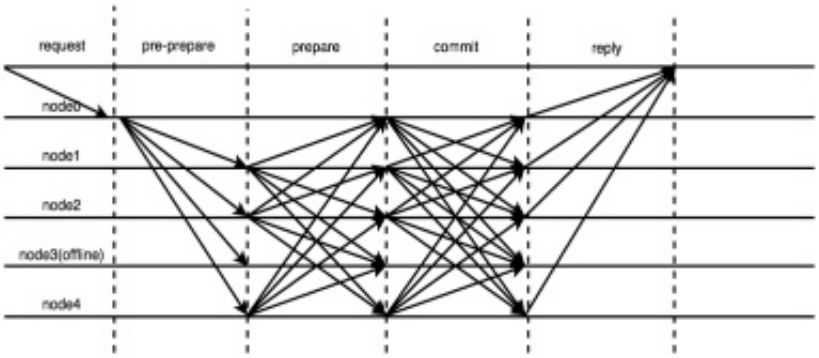
什么是DPOS（Delegated Proof of Stake）：权益委托证明共识，这个共识是目前最有效，最分散，最灵活的共识模式，如何才能快速的产生的一个块（Block），尤其是当大量的节点在链上时，想像一下几十万至几百万，甚至亿级节点分别确认最后再产生一个区块，仅仅是网络消耗恐怕急需要消耗大量的时间，这显然不是我们想要的，所以我们通过分级投票制度，节点选举出关键节点即见证节点去生成区块。



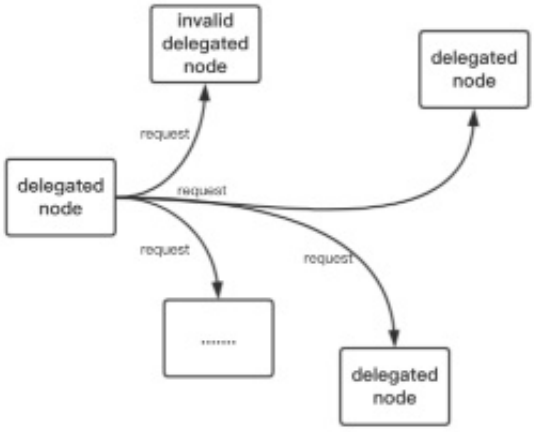
见证节点可以缩减至几百至几十的量级，此时我们就可以快速的生成区块。每当见证节点生产一个区块，它们可以获得奖励，奖励（交易费）由见证节点共同制定，如果见证节点没有在规定的时间（一个区块生成时间为一轮）产生区块，那么它们将失去见证区块的身份，同时委托节点会重现投票生成另一个见证节点，直到生成新的区块，然后会继续下一个循环，重现选举见证节点生成区块。

其次关于区块分叉，由于分叉大都是对节点有利的，所以旧的共识节点无法在新的链上进行区块生产，很快便会被投票出局，所以即便是硬分叉也可以无缝切换。DPOS对硬分叉也提供了强有力的支持。所以基于以上优势我们采用了DPOS（Delegated Proof of Stake）权利委托证明共识。

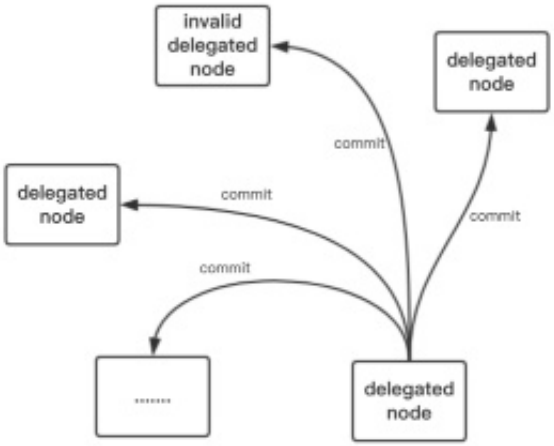
- 为什么采用SPBFT?
  SPBFT是基于PBFT的改进版，上面介绍了，我们还是用了PBFT公式算法作为保证区块一致性的优化，即当DPOS见证节点产生区块时，如果见证节点被恶意攻击或者主动叛变，会导致当前链上的内容出错，我们需要进行拜占庭容错，这个算法在保证活性和安全性（liveness & safety）的前提下提供了(n−1)/3的容错性。这也是对DPOS的改进。见证节点打包好一个区块向外广播时，会进入三个阶段（见图SPBFT三个阶段）：预准备（pre-prepare）、准备（prepare）和确认（commit），首先当前见证节点会向其它节点广播本次交易hash，以及交易内容。



自己进入准备（pre-prepare）状态，其他见证节点会对内容进行校验，校验通过则向其他节点广播prepare状态，



见证节点收集到足够的prepare状态节点（数量大于2f+1），进入commit状态，并向其他见证节点广播commit状态，



收集到足够的commit状态（数量大于2f+1）说明该区块无误，开始正常广播区块信息，其他节点则会接受区块，否则会视为该节点无产出，投票重新进行选举见证节点。

6.2 DEC 动态时间段轮换算法

DEC（dynamic epoch circle）:动态时间轮转 Epoch时间段优化，链上交易处理速度优化，见证节点数量优化，与常见的固定值轮换算法和普通轮换算法不同，基于基础见证节点会根据网络状态以及当前链上拥堵情况进行动态调节见证节点数量与交易速度。
当交易拥堵的时候会适当减少见证节点数量，提高出块效率。交易不拥堵时增加见证节点数量，维持系统稳定性，保证节点参与率。
见证周期内节点顺序优化，保证每轮的节点顺序不同，防止见证节点被挟持恶意攻击网络。

6.3 SSA 存储分配算法

SSA（store sharing algorithm）：存储分片算法，区块链扩容，这是一个区块链无法回避且极其重要的一个问题。所有主流的平台都在努力提高每秒的交易量（TPS）。事实上，当今的公共以太坊网络每秒处理20–30笔交易和比特币网络平均每秒可以处理7–10笔交易。这一数字远低于像Paypal,Alipay这样的集中支付处理器，后者平均每秒能处理约成千上万笔交易。从技术角度来看，网络中的每一个完全参与的节点都必须要验证每一笔交易，并且这些节点必须和它的其他节点保持一致，这是区块链共识的组成部分，它通过创建分布式的账本副本来保证区块链的安全。比特币设计之初限制了区块的大小为1M，这在当时看来是没有太多问题的，随着网络的拓展，1M的大小早已不堪负重了，以太坊也因为扩容问题发生了硬分叉，所以区块链扩容使我们必须解决的一个问题。为此我们提出了分片技术（Sharing），分片技术是一种基于数据库分片传统概念的扩容技术，在拥有大量数据的时候，单一数据库没办法快速的处理它们，于是我们将数据库分割成多个碎片并将这些碎片放置在不同的服务器上。这样相当于多台服务器同时处理了这些数据，在公共区块链的情境中，网络上的交易区块将被分成不同的碎片，其由网络上的不同节点组成。因此，每个节点只需处理一小部分传入的交易，并且通过与网络上的其他节点并行处理就能完成大量的验证工作。因此，随着网络的增长，区块链处理越来越多的交易将成为可能。这种属性也称为水平扩容，同时也提供了区块链每秒处理的交易数量，理论上节点越多处理速度越快。

7 发展计划

.....

8 合规和风险控制

.....

9 组织结构

.....

10 管理团队

.....

参考文献

[1] Bitcoin wiki. 15 May 2016. The wiki of Proof_of_work.Retrieved from https://en.bitcoin.it/wiki/Proof_of_work

[2] Bitcoin wiki. 10 November 2017. The wiki of Proof_of_Stake.Retrieved from

https://en.bitcoin.it/wiki/Proof_of_Stake

[3] wikipedia. 14 May 2018. The wiki of Proof_of_Stake.Retrieved from https://en.wikipedia.org/wiki/Gossip

[4] iost-official Documents. March 2018. The wiki of Proof_of_Stake.Retrieved from https://github.com/iost-official/Documents