



HBGChain

BIG DATA White Paper



什么是**区块链**

区块链(Blockchain)是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。区块链是HBG的底层技术，像一个数据库账本，记载所有的交易记录。这项技术也因其安全、便捷的特性逐渐得到了银行与金融业的关注。



HBG Block Chain

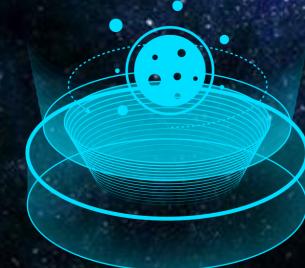
HBGChain是由马来西亚环境保护基金会共同发布成立，是世界上首个使用区块链技术，旨在促进环保事业发展、垃圾分类、减少环境污染和管理能源、监控排放的综合系统（以下简称HBG生态系统）。

目录

CONTENTS



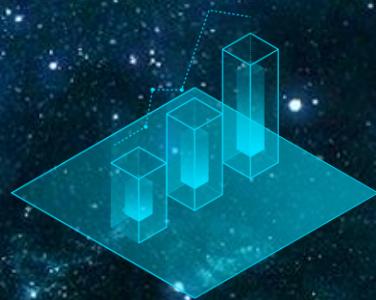
HBG简介



区块链网络



数据结构



生态系统



前景展望



HBGChain简介

区块链的定义

区块链是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。

从数据的角度来看

区块链是一种几乎不可能被更改的分布式数据库。这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者共同维护）。

从技术的角度来看

区块链并不是一种单一的技术，而是多种技术整合的结果。这些技术以新的结构组合在一起，形成了一种新的数据记录、存储和表达的方式。



「区块链的动态」

国际权威杂志《经济学人》、《哈佛商业周刊》、《福布斯杂志》等相继报道区块链技术将影响世界。

创业公司R3联合全球42家顶级银行成立区块链联盟，包括摩根大通、美国银行、汇丰银行、花旗银行、富国银行、三菱UFJ金融集团、巴克莱银行、高盛、德意志银行等。



HBGChain简介

HBG生态系统是一款致力于环保事业垃圾分类的习惯养成类应用，使用区块链的分布式技术，实现对生活垃圾分类处理的新模式，通过线上任务进行有偿奖励等方式，有效的将广大群众和会员对生活垃圾进行分配，促进再生资源产业发展，垃圾处理有机结合，环境保护垃圾分类再生资源合理利用，促进人类与环境和谐发展。





区块链网络

工作原理

发送报文时，发送方用一个哈希函数从报文文本中生成报文摘要，然后用自己的私钥对摘要进行加密，加密后的摘要将作为报文的数字签名和报文一起发送给接收方，接收方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要

区块链科普

数字签名

数字签名涉及到一个哈希函数、发送者的公钥、发送者的私钥。数字签名有两个作用，一是能确定消息确实是由发送方签名并发出来的。二是数字签名能确定消息的完整性。

区块链网络

SHA256

一种求Hash值的加密算法。

工作原理

将任何一串数据输入到SHA256，将得到一个256位的Hash值（散列值）。其特点：相同的数据输入将得到相同的结果。输入数据只要稍有变化（比如一个1变成了0）



Merkle Tree

一种哈希二叉树，使用它可以快速校验大规模数据的完整性。在HBG网络中，Merkle树被用来归纳一个区块中的所有交易信息，最终生成这个区块所有交易信息的一个统一的哈希值，区块中任何一笔交易信息的改变都会使得Merkle树改变。

工作原理

非叶子节点value的计算方法是将该节点的所有子节点进行组合，然后对组合结果进行hash计算所得出的hash value。

区块链网络

「节点网络」

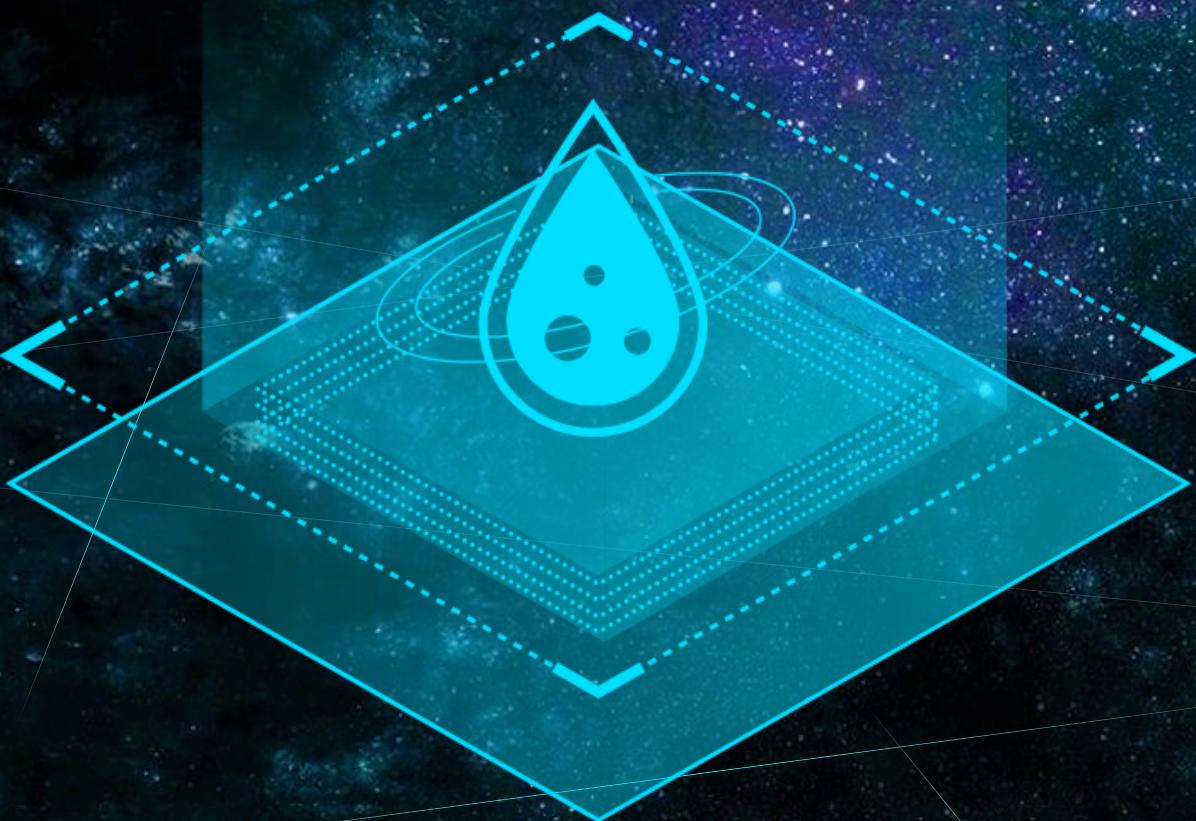
任何机器都可以运行一个完整的HBG节点，一个完整的HBG节点包括如下功能：钱包，允许用户在区块链网络上进行交易完整区块链，记录了所有交易历史，通过特殊的结构保证历史交易的安全性，并且用来验证新交易的合法性矿工，通过记录交易及解密数学题来生成新区块，如果成功可以赚取奖励路由功能，把其它节点传送过来的交易数据等信息再传送给更多的节点除了路由功能以外，其它的功能都不是必须的。



「时间戳服务器」

大多用来进行比对以及验证处理，时间戳服务器是一款基于PKI（公钥密码基础设施）技术的时间戳权威系统，对外提供精确可信的时间戳服务。它采用精确的时间源、高强度高标准的安全机制，以确认系统处理数据在某一时间的存在性和相关操作的相对时间顺序，为信息系统中的时间防抵赖提供基础服务。

区块链网络



● 节点网络第1步

所有者A利用他的私钥对前一次交易（比特币来源）和下一位所有者B签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单要点：B以公钥作为接收方地址

● 节点网络第2步

A将交易单广播至全网，HBG就发送给了B，每个节点都将收到的交易信息纳入一个区块中要点：对B而言，该枚HBG会即时显示在HBG钱包中，但直到区块确认成功后才可用。目前一笔HBG从支付到最终确认成功，得到6个区块确认之后才能真正确认到账

● 交易过程第3步

每个节点通过解一道数学难题，从而去获得创建新区块权利，并争取得到HBG的奖励（新HBG会在此过程中产生）要点：节点反复尝试寻找一个数值，使得将该数值、区块链中最后一个区块的Hash值以及交易单三部分送入SHA256算法后能计算出散列值X（256位）满足一定条件（比如前20位均为0），即找到数学难题的解。由此可见，答案并不唯一

● 交易过程第4步

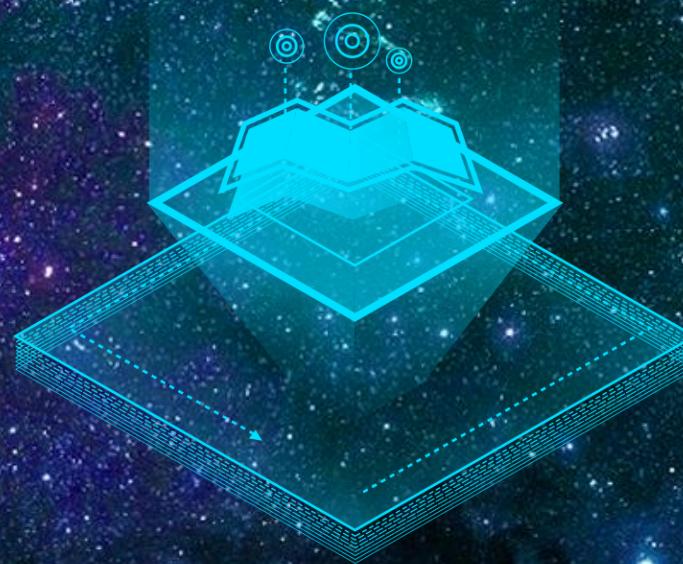
当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易，并由全网其他节点核对
要点：时间戳用来证实特定区块必然于某特定时间是的确存在的。HBG网络采取从5个以上节点获取时间，然后取中间值的方式作为时间戳。

交易过程第5步

全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块链。

要点：每个区块的创建时间大约在10分钟。随着全网算力的不断变化，每个区块的产生时间会随算力增强而缩短、随算力减弱而延长。其原理是根据最近产生的2016年区块的时间差（约两周时间），自动调整每个区块的生成难度（比如减少或增加目标值中0的个数），使得每个区块的生成时间是10分钟。





数 据 结 构

数据结构



区块链

区块链以区块为单位组织数据。全网所有的交易记录都以交易单的形式存储在全网唯一的区块链中。



数据结构



○ 区块

区块是一种记录交易的数据结构。每个区块由区块头和区块主体组成，区块主体只负责记录前一段时间内的所有交易信息，区块链的大部分功能都由区块头实现。

○ 区块头

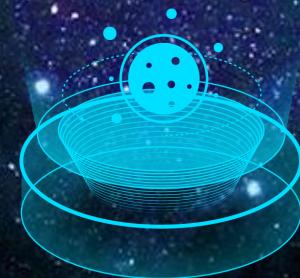
- 版本号，标示软件及协议的相关版本信息
- 父区块哈希值，引用的区块链中父区块头的哈希值，通过这个值每个区块才首尾相连组成了区块链，并且这个值对区块链的安全性起到了至关重要的作用
- Merkle 根，这个值是由区块主体中所有交易的哈希值再逐级两两哈希计算出来的一个数值，主要用于检验一笔交易是否在这个区块中存在
- 时间戳，记录该区块产生的时间，精确到秒
- 难度值，该区块相关数学题的难度目标
- 随机数(Nonce)，记录解密该区块相关数学题的答案的值



区块形成过程



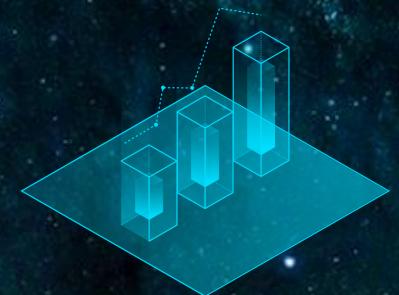
1、在当前区块加入区块链后，所有矿工就立即开始下一个区块的生成工作



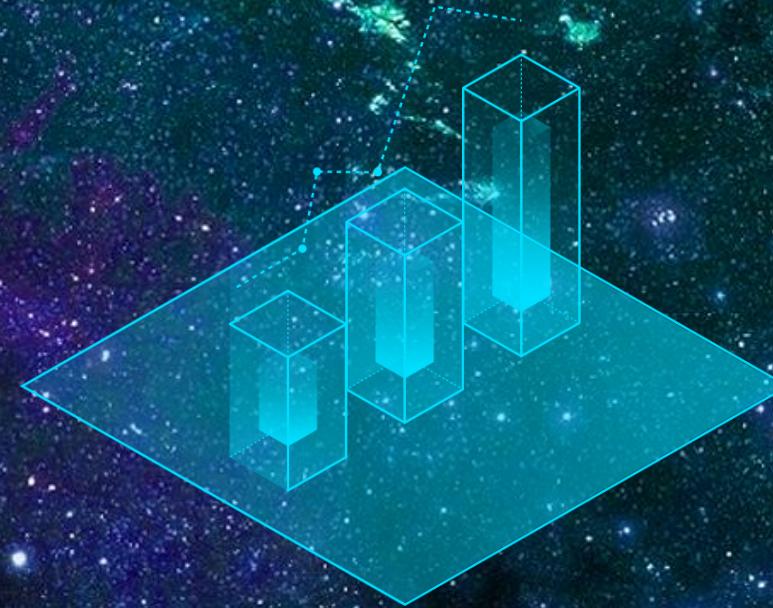
2、把在本地内存中的交易信息记录到区块主体中在区块主体中生成此区块中所有交易信息



3、把上一个刚刚生成的区块的区块头的数据通过SHA256 算法生成一个



4、难度值字段会根据之前一段时间区块的平均生成时间进行调整以应对整个网络不断变化的整体计算总量

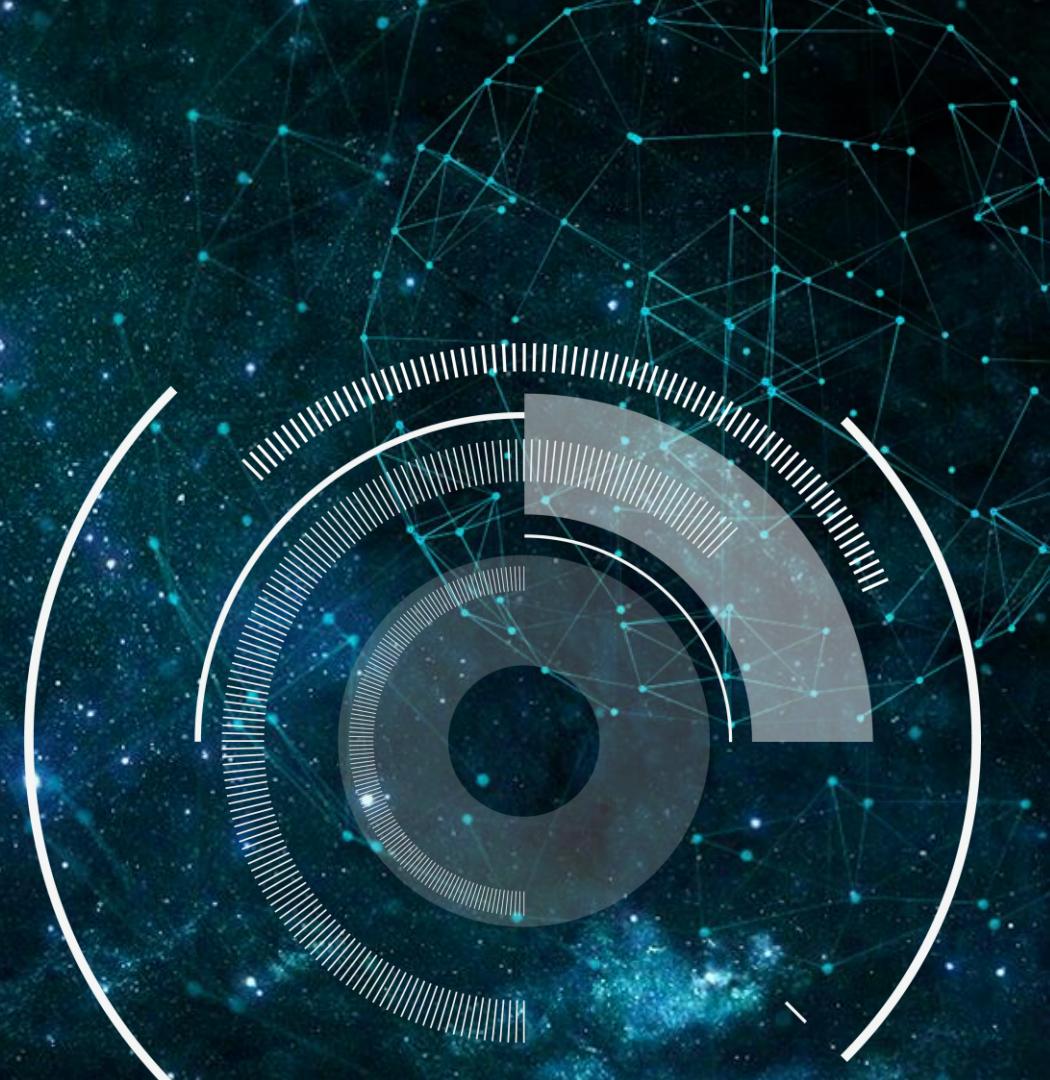


「核心问题」

核心问题

工作量证明

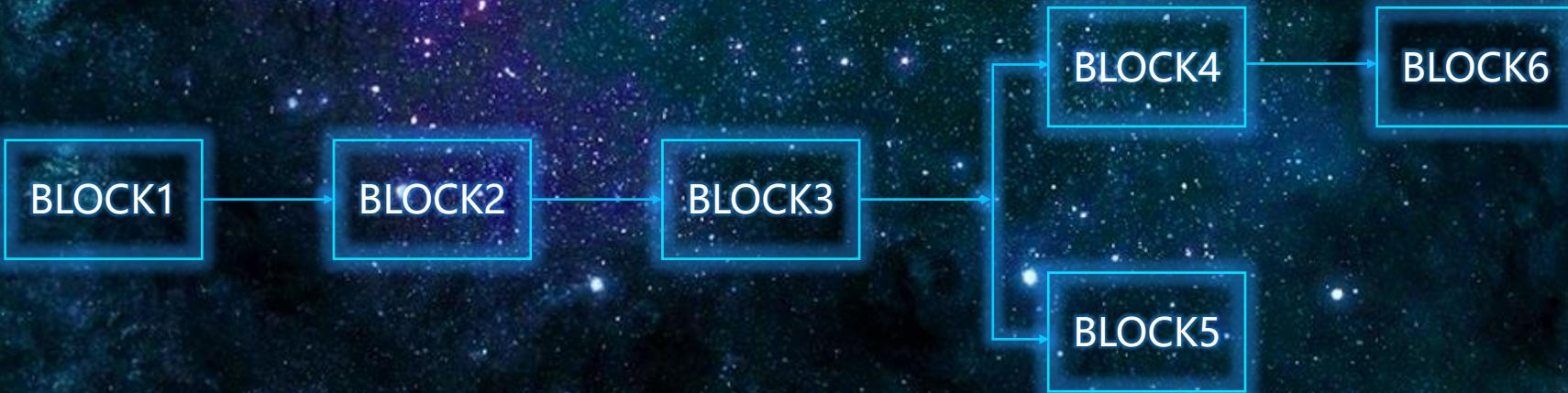
- 区块头包含一个随机数，使得区块的随机散列值出现了所需的0个数。节点通过反复尝试来找到这个随机数，这样就构建了一个工作量证明机制。
- 工作量证明机制的本质是一CPU一票，“大多数”的决定表达为最长的链，因为最长的链包含了最大的工作量。如果大多数的CPU为诚实的节点控制，那么诚实的链条将以最快的速度延长，并超越其他的竞争链条。如果想要修改已出现的区块，攻击者必须重新完成该区块的工作量外加该区块之后所有区块的工作量，并最终赶上和超越诚实节点的工作量。



核心问题

同一时间段内全网不止一个节点能计算出随机数，即会有多个节点在网络中广播它们各自打包好的临时区块（都是合法的）。

分叉

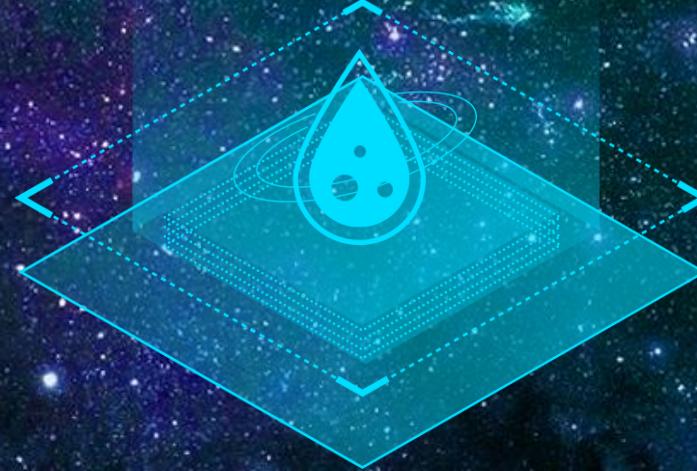


某一节点若收到多个针对同一前续区块的后续临时区块，则该节点会在本地区块链上建立分支，多个临时区块对应多个分支。该僵局的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。其他分支将会被网络彻底抛弃。

解决问题

- HBGChain在区块链和互联网的基础上，能够对目前各类主要的环保问题提出更好的解决垃圾分类的方案，帮助普通大众改善环保习惯，树立节能意识，降低企业“三废”排放，提高废弃物的再生处理效率，并能够综合监控、分析世界上一切已知的、有价值的能源使用、资源循环、废弃物再生，以及全球生态变化的重要数据。
- HBGChain以连接、转化一切可再生能源为使命。作为自然的一部分，人们在HBG系统的帮助下，让自然生态与人文生态必将重新融合，天地与我并生，万物与我为一的世界，必将得以实现。人类必将拥有一个更美好的明天！





前景展望

前景展望

从需求端来看

- 金融、医疗、公证、通信、供应链、域名、投票等领域都开始意识到区块链的重要性并开始尝试将技术与现实社会对接。

从投资端来看

- 区块链的投资资金供给逐步上升，风投的投资热情也不断高涨，投资密度越来越大，供给端的资金供给有望推动技术的进一步发展。

从市场应用来看

- 区块链能成为一种市场工具，帮助社会削减平台成本，让中间机构成为过去；区块链将促使公司现有业务模式重心的转移，有望加速公司的发展。



前景展望

从底层技术来看

HBGChain有望促进数据记录、数据传播及数据存储管理方式的转型；区块链本身更像一种互联网底层的开源式协议，在不远的将来会触动甚至最后彻底取代现有互联网的底层基础协议。

从社会结构来看

HBGChain技术有望将法律与经济融为一体，彻底颠覆原有社会的监管模式；组织形态会因其而发生改变，区块链也许最终会带领人们走向分布式自治的社会。



历史使命

HBG寓意无数个绿洲，遏制地球环境资源的恶化，创造人类与自然和谐美好未来。为此我们致力于环境保护，可再生资源的可持续利用，推动减少浪费的行为，将美丽的绿洲建立在每一个正在被污染和排放等环境问题困扰的社区中，并将分布式能源管理的技术带入我们寻常百姓的身边，为绿色生态社区建设做出贡献。





HBGChain

BIG DATA PRESENTATION