元宇宙与区块链

518021910740 池彦廷

2022.1.14

1 背景介绍

1.1 元宇宙

” 元宇宙”(“MetaVerse”), 意为虚拟的世界, 人们在其中可以拥有自己的虚拟形象. 元宇宙是在传统网络空间基础上, 加上多种数字技术, 构建形成的既映射于、又独立于现实世界的虚拟世界。元宇宙并非一个简单的虚拟空间, 而是把网络、硬件终端和用户囊括进一个永续的、广覆盖的虚拟现实系统之中, 系统中既有现实世界的数字化复制物, 也有虚拟世界的创造物。[2] 在 Roblox 的招股书中对元宇宙的概念进行了更具体的描述。它认为一个真正的元宇宙产品应该拥有 8 个属性：身份、朋友、沉浸感、低延迟、多元化、随地、经济系统和文明

由以上八个要素, 目前认为元宇宙的发展依赖于以下技术:

1. 全球互联网覆盖
2. AR、VR 技术
3. 5G 等新一代信息通信技术。

而目前以上三者的技术水平仍无法实现基于虚拟空间的元宇宙技术.

元宇宙将会是去中心化的（没有中央统管机构）, 将有许多公司和个人在元宇宙内经营自己的空间。元宇宙的其他特色包括数字持久化和同步, 这意味着元宇宙中的所有事件都是实时发生的, 并具有永久的影响力。

1.2 区块链

区块链是由密码学 (hash 算法等) 为数学理论基础的, 串接并保护内容的串连文字记录, 这些文字记录又称” 区块”, 目前的区块链常用于加密货币中, 如比特币与以太坊.

区块链的最大特征之一是可以提供去中心化的服务, 具有 “轻所有权、重使用权” 的特点. 所有用户可以公平的访问区块链, 故区块链在元宇宙的应用可以使得去中心化元宇宙, 即更公平, 更市场化的元宇宙成为可能.

2 区块链技术在元宇宙中的应用

由于区块链体现出极强的去中心化的思想, 区块链在元宇宙中的应用可以体现在如下方面

2.1 数字身份与数字货币

人们在元宇宙中生活需要有一个区别于现实身份的虚拟身份. 虚拟身份的实现需要实现身份的存储, 认证等方面, 同时元宇宙的去中心化特点, 用户的数字身份必需去中心化的定义

区块链本身具有去中心化, 不可篡改、可追溯特性、隐私安全性等特性, 利用区块连与公私钥技术能很好的为用户创造虚拟分身.

此外, 目前区块链条在数字货币中的应用已经相对成熟, 以区块链为基础的数字货币已经有不错的市场. 不同于各国的货币, 数字货币是世界通用的, 在元宇宙中使用有利于打破不同国家的隔阂.

2.2 数字资产

元宇宙的一大特点为" 经济体系与文明", 而完成这点需要将现实物品映射至元宇宙中并合理的定义价值, 形成经济体系

类似于现有的 NFT 技术, 区块链技术可以将现有资产转化为数字资产.NFT 的唯一性是得其标记的资产具有排他性与不可分割性, 并利用数字货币进行交易.

2.3 智能合约

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易， 这些交易可追踪且不可逆转。在区块链中, 智能合约可以实现为在区块链中的代码, 触发该合约程序能够自动执行.

元宇宙中的事务可以设置为智能合约的形式, 智能合约可编程, 开源并且强制执行, 有利于元宇宙的去中心化发展.

3 应用于元宇宙的 POW 协议

POW 协议是应用于区块链的一种公式算法, 用于使得不同主机的区块链保持一致. 在比特币中,POW 协议保证了挖矿的公正性以及区块的安全性, 但是交易速度慢并会造成不必要的计算资源浪费. 这使得比特币的 POW 协议无法直接用于元宇宙中

在元宇宙中, 我们需要一个更高效而同样安全的 POW 协议

3.1 POW 简介

在 POW 协议中, 区块生成端需要做一定难度的工作得出一个结果以证明自己的工作量, 利用工作量令其他节点信服该区块是合理的. 验证端很容易通过结果来检查工作端是不是做了相应的工作, 以将其加入自己的链中. 这种**不对称**计算往往由 Hash 函数实现, 即

$$Hash(func(C, X)) < D$$

其中 C 为数据,X 为随机值,D 为工作量阈值,D 越小所需的工作量越大.

区别与比特币, 我们需要在保证区块链能同步的情况下尽可能的减少资源浪费, 加快区块生成速度.

3.2 元宇宙中的 POW

POW-BC[1] 是一种轻量级的 POW 协议, 其运用了压缩机制对 POW 进行了三方面的优化.

3.2.1 区块压缩

POW-BC 使用 DEFLATE 算法对区块进行了无损压缩. 该操作能减少运算的复杂度

3.2.2 共识参数 D

在比特币的 POW 协议中, 共识参数由区块生成速度决定与调整, 而在 POW-BC 中, 矿工节点可以自行调整参数 D

$$D_{adjusted} = D_{base} \times \frac{T_{blockInterval}}{T_{baseBlockInterval}}$$

其中,$D_{adjusted}$ 为调整后的难度系数，D_{base} 表示调整前难度系数。$T_{baseBlockInterval}$ 是上一次区块的生成周期，在比特币中是 10 分钟。而 $T_{blockInterval}$ 由以下公式计算

$$T_{blockInterval} = T_{const} + T_{transVerify} + T_{consensus}$$

其中 T_{const} 是最小的时钟周期,$T_{transVerify}$ 是 POW-BC 链达成共识的时间, 而 $T_{transVerify}$ 是新区块传输消息至整个网络并使消息中的区块得到验证的时间.

最终得到公式:

$$D_{adjusted} = D_{base} \times \frac{110 + T_{transVerify} + (490 - T_{\text{transVerify}}) \times R_{\text{blockCompress}}}{600} \tag{1}$$

其中 R 为区块的压缩率

3.2.3 共识模型

POW-BC 中, 共识模型将达成共识的过程分为四步: 交易预处理, 包装交易, 区块生成和储存.[1]

1) 预处理: 预处理过程包括交易验证, 即检验签名与广播该交易, 交易优化并将交易放入交易池中等待处理.

2) 包装: 包装过程将交易池中的交易包装入区块中, 并对区块进行压缩.

3) 区块生成: 区块生成步骤首先调整挖矿的难度, 挖出区块后广播该区块.

4) 区块储存: 在各个区块被 P2P 的广播至通信网络后, 接受到的节点验证该区块并将其存入这个节点的区块链中. 相比与普通的 POW 协议,POW-BC 在这一阶段需要解压缩区块并验证 $D_{Adjusted}$ 的正确性.

POW-BC 模型通过以上的方式简化了运算步骤, 使得区块链技术能更好的应用于元宇宙中.

4 元宇宙与智能合约

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议, 可用于构建区块链的事务逻辑. 区块链货币交易中往往会用到智能合约技术, 当货币交易时, 智能合约自动履行.

智能合约在元宇宙中有至关重要的作用, 智能合约是区块链系统内所有行动发生的引擎。区块链功能为每个去中心化的应用程序进行编码。Metaverses 利用区块链中的智能合约, 助于确保 Metaverse 活动的安全. 区块链上的智能合约实现了 Metaverse 社区内的互动，同时实现了交易的冗余性。它们允许技术的进一步发展，而不增加中心化技术中的成本因素。工作中的智能合约几乎没有附带的维护成本。它允许快速开发并降低项目开发者的运行成本。此外，智能合约可以在不改变 Metaverse 代码库的情况下为 Metaverses 创造额外的功能。

5 总结

元宇宙是一个人们可以以虚拟形象在其中生活的虚拟世界是, 当下热门的概念区块链. 在元宇宙的实现中, 区块链起着很大作用. 利用区块链技术, 人们在元宇宙中可以有去中心化的, 保密的虚拟身份, 并利用区块链货币进行交易, 拥有类似 NFT 的虚拟资产. 共识技术中,POW-BC 技术能够简化比特币中 POW 的计算步骤, 使得区块计算加快. 智能合约技术也能广泛的用于元宇宙中, 加强其安全性, 自动性与可扩展性.

参考文献

[1] Bin Yu, Xiaofeng Li, and He Zhao and. Pow-bc: A pow consensus protocol based on block compression. *KSII Transactions on Internet and Information Systems*, 15(4):1389–1408, April 2021.

[2] 左鹏飞. 最近大火的元宇宙到底是什么？, 2021.