OpartChain·创链白皮书

OpartChain（创链）是比特币和以太坊之外的区块链生态系统，是一个基于分布式加密货币的去中心化应用软件,通过价值传输协议（Value Transfer Protocol）和主控智能合约技术，可以作为原创数字媒体作品的自出版和分发、交易平台，为用户提供发布出版、版权认证和保护、在线交易和分发、元数据追踪与分析的全过程一站式解决方案，简化了数字作品聚合与分享的难度和技术门槛，是数字出版领域的颠覆性创新应用。OpartChain 着眼于当前数字出版行业和传统版权制度的痛点，通过区块链技术的创新探索，致力于打造中国第一款真正落地的区块链商业应用，使普通互联网用户能真正享受区块链创新科技带来的便利。

OpartChain 系统通过良好的设计原则和设计策略来实现，例如兼容性原则、模块化设计策略、安全性策略和易用性策略。从技术角度分析，OpartChain 致力于实现首个兼容 BIP（基于 UTXO 模型的比特币演进协议 ）的 POS（Proof of Stake，权益证明机制）智能合约平台，并通过 Identity，Oracle 和 Data feeds 的引入，使其在合规性方面符合政府和行业的监管需求。在 OpartChain 的公链（Public Blockchain）系统中，在共识机制上，从去中心化程度、实用性、技术可靠性考虑，我们将以 Proof of Stake 为基础，加入节点在线激励因素（Incentive Factor）,形成 IPOS（Incentive POS）的共识协议。在 OpartChain 的联盟链中（Permissioned Blockchain），我们将采用与 Raft 融合的 Proof of Time 共识协议，使得在联盟链或者私链中，达成共识的时间大大缩短（BlockTime:250ms，Confirmation Time：750ms-3s）。

数字作品版权保护的困局（1）

通过拖拽、复制粘贴等手段，数字媒体作品非常容易在互联网上进行分享，它们会像病毒一样传播，创造者和内容所有人却很难从其中受益。 免费 MP3 下载网站、 免费 MP3 搜索引擎给传统音乐市场带来的冲击如洪水猛兽一般。此前，有一组数据让人感到无奈：国内 400 多个中型音乐网站及 1000 多个小型个人主页存在严重侵权问题， 供下载的 MP3 歌曲 50%以上是盗版。 每天有超过 45%的网民使用互联网下载音乐。唱片业年收入 2 亿元，但盗版可高达 18 亿元。

数字作品版权保护的困局（2）

7 月 25 日，多部门联合启动了打击互联网侵权盗版的“剑网 2017”专项行动，这也是该专项行动连续开展的第十三年。

虽然每年专项行动都会取得很大成效，但并不能从根本上很好地遏制网络侵权盗版，在专项行动中执法查证也存在着巨大的技术困难。

艺术家在数字时代的哀鸣（1）

“ 有许多内容的创造者 并没有得到公平的报酬，因为知识产权系统遭到了损害。在互联网的第一个时代就遭到损害。 就拿音乐来说。 音乐家们只在食物链的 末端获得一些残渣碎屑。在 25 年前，如果你是一个作曲家， 写出一首流行的歌曲， 卖出一百万首单曲，你可以获得大约 45000 美元的报酬。 而现在，作曲家的你 写出一首流行的歌曲， 被百万次播放， 你并不能得到 45000 美元， 你只能得到 36 美元， 足以买一个不错的披萨了。”

——Don Tapscott，《区块链革命》作者

艺术家在数字时代的哀鸣（2）

与国外在线音乐的发展不同，我国在线音乐行业天然面临着盈利难的问题。尤其在发展早期，整个市场版权保护较薄弱，在线音乐平台提供免费试听、下载的服务，来自用户的付费收入较少。 据《2016 年中国在线音乐行业现状与发展趋势报告》， 2016 年中国在线音乐市场规模达到了 61 亿元。 腾讯音乐、网易云音乐等各大在线音乐平台大力竞争各大唱片公司的版权独家代理，努力建立行业生态争夺市场，而仅通过下载和流媒体播放进入音乐人钱包的价值少之又少。

出版、交易与分发

出版：作者可以在 OpartChain 发布、出版作品。作品丰富的元数据、作品本身的 DNA 信息以及存储节点信息将被存入块链和 IPFS（Inter Planetary File System，星际文件系统）。

交易：我们致力于构建一个完全去中心化的点对点交易和分发网络。通过带身份认证的主控智能合约（Master Smart Contract）和价值传输协议（Value Transfer Protocol）,我们可以在 OpartChain 网络实现可监管的交易。

分发：通过加密的 IPFS（星际文件系统）协议进行内容搜索和分发，安全、高效、去中心化。

版权认证与保护

建立公链和联盟链共存的区块链系统，引入身份机制，构建信用和价值激励体系。

对于公链，可引入第三方的征信体系，建立押金体系。对存在违法违规问题如发布非法信息或者盗版内容的处以严厉处罚，违反法律的移交司法处理。采用改进的 POS（Proof of Stake）共识机制，即在传统 POS 中加入激励体系形成的 IPOS（Incentive POS）机制，防止作弊并鼓励节点在线。

对于联盟链，由于节点都是可信赖的第三方，如知名唱片公司，则采用融合 Raft 算法的 POT（Proof of Time）机制，大大缩短达成共识所需时间。

内容分发网络采用结合身份系统的公钥加密 IPNS（Inter Planetary Name Space,星际命名空间）协议，用户只有授权后才能播放流媒体作品，从源头控制盗版的产生。

全球数字作品分布式元数据数据库

OpartChain 旨在创立一个面向作品的分布式元数据数据库， 每一件作品的丰富的元数据和作品本身的 DNA 信息将记录到块链，并存储到 IPFS 网络。 这是一个全球性的去中心化数字作品数据库。

这些元数据可能包括作者创作该作品的 地点、时间，心情， 也可以包括作者自定义的版权声明等等。 通过 IPFS 协议， 用户可以在这个数据库中检索自己想要的作品和信息。

创作者与消费者的交互

通过身份系统和对区块链网络元数据的追踪，原作者可以更好地掌控自己作品的使用情况，通过反馈的数据进行更好地创作，也可以基于这些数据来与消费者进行更好地交互。基于原作的二次创作，基于粉丝贡献的激励成为可能，粉丝经济将变得更加高效。

价值传输协议（Value Transfer Protocol）

2008 年 10 月 31 日，Satoshi Nakamoto 通过一个密码学小组的邮箱发布了比特币白皮书；2009 年 1 月 3 日比特币创世区块被挖出，并在第 170 个区块发生了第一笔比特币转账交易，从此开启了比特币网络作为一种点对点的价值交换网络蓬勃发展的时代。虽然中间历经危

机，但比特币网络的价值从零开始，到今天已成为一个价值超过 100 亿美金的点对点支付网络。
点对点价值传输网络的出现有历史必然性，区块链必将成为互联网的未来。然而，当前很少有真正落地的区块链商业应用。OpartChain 密切联系实际商业场景，致力于开发能真正惠及普通百姓的区块链商业应用。

融合比特币 UTXO 模型和以太坊 Account 模型

UTXO（Unspent Transaction Output,未花费交易输出）是比特币交易的基本单位。交易时，用户使用自己的私钥签名解锁自己拥有的一笔 UTXO，并使用交易的接收方的比特币地址（公钥的哈希值）来创建并锁定 UTXO.比特币网络的全节点则会通过脚本计算哈希来检验交易的合法性。
考虑到比特币 UTXO 模型使用脚本语言，具有较高的安全性和隐私保密，OpartChain 将基于 UTXO 来构建。但考虑到现实中监管的需要，在 UTXO 模型中融合了以太坊的身份机制。

IPOS（Incentive Proof of Stake）共识机制

点对点价值传输网络中最大的难题就是“双花问题”，而解决这个问题的关键就在于共识机制的实现。共识机制（Consensus）旨在任何一个分布式系统中实现节点之间的统一性。
比特币所使用的共识机制是 POW（Proof of Work，工作量证明）机制，通过消耗大量的算力计算数学难题来达到共识，造成了不必要的能源浪费。
以太坊所使用的是 POS（Proof of Stake，权益证明）机制，通过系统代币的持有量来争取记账权。但 POS 机制较之 POW 存在一定安全风险，且可能存在记账节点不积极的情况。为鼓励节点在线，降低安全风险，OpartChain 将在 POS 机制中加入激励体系，形成 IPOS 共识机制。

主控智能合约（Master Smart Contract）

区别于以太坊的智能合约，OpartChain 中我们将采用加入线下因素（Oracle 喻言和 Data Feed）和角色机制的主控智能合约。在以太坊中，智能合约完全由代码决定，奉行“代码即法律”，这显然是脱离实际且极其危险的。The DAO 事件就是一个不幸的例子（2016 年 6 月以太坊最大的众筹项目也是当时区块链领域最大的项目 The DAO 因智能合约漏洞被黑客卷走超过 6000 万美元的以太币）。