

基于 CNWW3 区块链体系标准建立的数字版权应用

白杰¹, 杨鹏飞², 孙鲜艳², 庞玉燕², 逯楠³

(1. 俄罗斯联邦总统直属国民经济与国家行政学院, 俄罗斯 莫斯科 119571;

2. 江苏数字产权交易所有限公司, 江苏 南京 210000; 3. 南京市江北新区海外知识产权维权联盟, 江苏 南京 210000)

摘要: 将区块链技术应用在数字版权的权属确定、数字版权转变为数字资产和数字资产金融和交易领域, 具有不受地域时间的限制、系统自动生成、权属申请实时完成、不可篡改结果、原件加密处理保证安全等特点, 从而实现版权申请的公平和公正。区块链技术的数字版权体系包括: 区块链底层基础设施系统、数字版权法律流程应用系统、数字版权申请流程应用系统、数字版权指纹加密应用系统、数字版权鉴权应用系统、数字版权权利确认应用系统、分布式数据存储控制应用系统、点对点控制协议。区块链数字版权资产交易应用体系包括: 区块链底层基础设施系统、数字资产交易应用系统、版权资产价值评估与估值联盟应用系统、法律律师事务所联盟应用系统、司法机构联合应用系统。区块链数字版权资产金融服务体系包括: 金融资产融资机构应用系统和中短期信贷应用系统。基于区块链的数字资产交易最根本核心是资产流动转移和信任。

关键词: 区块链智能合约; 共识算法; 防篡改; 去中心化应用; Web3.0; CNWW3; 数字资产; 数字产权; 知识产权; 资产证券化

中图分类号: TP393.03; TP311.13 文献标识码: A DOI: 10.19358/j.issn.2096-5133.2020.07.004

引用格式: 白杰, 杨鹏飞, 孙鲜艳, 等. 基于 CNWW3 区块链体系标准建立的数字版权应用[J]. 信息技术与网络安全, 2020, 39(7): 18-30.

Digital copyright application based on CNWW3 blockchain system standard

Bai Jie¹, Yang Pengfei², Sun Xianyan², Pang Yuyan², Lu Nan³

(1. The Russian Presidential Academy of National Economy and Public Administration, Moscow 119571, Russia;

2. Jiangsu Digital Property Exchange Co., Ltd., Nanjing 210000, China;

3. Abroad Intellectual Property Protection Alliance of Jiangbei New District Nanjing, Nanjing 210000, China)

Abstract: The application of blockchain technology makes the determination of the ownership of digital copyright and the transformation of digital copyright into digital assets and digital asset finance and transactions fairer and more just. Right holders only need to submit their works to the blockchain digital copyright system through the network, and the entire process is automatically completed. It has the following advantages: No geographical restriction; The whole process is automatically completed by the system; The ownership application is completed in real time; The original work or digital original is encrypted to ensure security. The digital copyright system of blockchain technology includes: the underlying infrastructure system of the blockchain; digital copyright legal process application system; digital copyright application process application system; digital copyright fingerprint encryption application system; digital copyright authentication application system; digital copyright rights confirmation application system; distributed data storage control application system; point-to-point control protocol. Blockchain digital copyright asset transaction application system includes: blockchain underlying infrastructure system; digital asset transaction application system; copyright asset value assessment and valuation alliance application system; legal lawyer affairs agency alliance application system; judicial institution joint application system. The blockchain digital copyright asset financial service system includes: financial asset financing institution application system; medium and short-term credit application system. The most fundamental core of digital asset transactions based on blockchain is asset flow transfer and trust.

Key words: blockchain smart contract; consensus algorithm; unchangeable; decentralized applications; Web3.0; CNWW3; digital assets; digital property rights; intellectual property rights; asset securitization

1 版权在现代化市场经济中的作用

版权(著作权)在传统知识产权领域占有的比重十分巨大,每年全世界范围内都会产生大量的版权(著作权),这些大量产生的版权(著作权)存在于视频领域、音频领域、摄影作品、影片、小说、书籍、图像设计、时装设计、服装设计等。

根据中国新闻出版广电网 2019 年 12 月 31 日对外发布的报道,2018 年中国版权产业增加值占 GDP7.37%;2018 年中国版权产业的行业增加值为 6.63 万亿元;2018 年中国核心版权产业行业增加值已突破 4 万亿元,达到 4.17 万亿元,同比增长 9.30%。

根据中国国家版权局 2019 年 3 月 5 日对外发布的统计数字,关于 2018 年全国著作权登记情况的通报,2018 年全国(指中国)著作权登记总量达 3 457 338 件,相比 2017 年的 2 747 652 件,同比增长 25.83%。由此可见,版权(著作权)无论是在经济中的作用或是对于 GDP 的产值,其贡献都是巨大的,而且是以每年 25% 的综合比值增长。

2 当前各国的版权申请和经济活动转化现状分析

根据国际上的经验(IPXI 美国知识产权交易所、香港国际知识产权交易中心),便捷的知识产权金融交易和高效的知识产权资产流通,能够给金融资本和研究方提供紧密的融合空间,能够为研究方提供研究成果转化所需的资金,很大程度上可以降低金融资本的项目投资风险,又可以为研究提供相应的金融工具,因此更能够促进优质的权利成果的生产和权利成果的转化。

(1)目前世界各国版权的权利确定原则是先申请先授权的原则。作品的作者依照版权管理部门的要求,向版权管理部门提交申请较为复杂的申请材料,然后需要等待较长的时间,待版权管理部门的审批,才有可能获得得到法律层面上确认的版权权利。

(2)中国相关行业协会的统计,95% 以上的作品作者在获得了版权权利证书以后不能直接转化为经济效益。以小说和音乐歌曲的作者为例:大部分的作者要将作品卖给行业投资人,行业投资人将作品卖给发行商,发行商再向市场发行。

①权利转移的路径如下:作者将版权转让给投资人。投资人将作品的使用权、发行权分别按照地区或者时间先后授权许可给不同的发行商。

②经济收益的路径如下:作者将版权转让给投资人,投资人向作者支付($X+T$,其中 T 为支付的税金)元权利转让费,净收益为 X 元。

投资人将作品的使用许可或销售放映许可按照地区或先后时间,平均分别许可给四家发行商,作品的一个市场生命周期内总收益为 $120X$ 元;

单个发行商在改作品的一个市场生命周期内平均收益为 $320X$ 元,去掉税收支出、综合成本支出以及交付给上述投资人的收益,净收入为 $98X$ 元。

根据上述的①和②可以得出,作品的一个市场生命周期内各方的收益情况如下:原始作品的作者扣除税收支出的净收益为 X ;二级投资人收益为 $120X$ 元,扣除税收支出和支付原始作者的版权转让费,净收益在 $100X$ 元;单个发行商的平均净收入为 $98X$ 元。由上述可见,原始作者的收益最为低廉,绝大部分的收益都归属于了投资商和发行商。

综上所述,目前导致知识产权经济发展的问题缺陷如下:

(1)版权(著作权)的权利确认较为繁琐,时间周期较长。

(2)目前电子化集中系统只能做到相对公平而不能做到绝对公平。根据版权的法律原则,即:作品自诞生之时,权利归属于权利人。但是,在目前的司法实践过程中,无法精确客观地判断作品的作者和产生的时间,因此现实中只能采用先申请先获得权利的原则。理论上而言,任何中心系统都是能够被篡改数据的,只能依靠制度、法律或者政府的公信力去维持信誉,所以仍然无法做到绝对的公正。如果能够出现一种机制,让各国都无歧义的确认真实的第一原始作者,那么版权(著作权)可以被全球通行。

(3)原始作者获得的收益低廉。作者不能直接获得最大的经济收益,必须要依赖于中间渠道商(上述的投资人)才能获得收益。

(4)大量的作品权利不能产生经济收益。根据 TFOSE(TORONTO FUTURES OPTIONS SWAPS EXCHANGE INC.)的预计仍然有接近 60% 的大量的优秀作品的作者因为缺少中间渠道商,无法把这些优质的作品转化成为经济效益。

(5)作品权利被侵权后法律维权成本高昂。作品被侵权后维权成本高昂,高昂的律师费用和取证成本、长期的诉讼时间、维权收益与高昂的成本倒

挂不成比例。

3 建立可信的区块链数字化确权平台和交易平台

3.1 目前区块链技术的缺陷和版权经济转化的行业难点

区块链技术是目前全球公认的防篡改、防抵赖的技术,区块链技术完成版权(著作权)的权利确定和交易,建立非人为的绝对的公信机制。目前的大多数区块链技术公信机制还处在研究过程中,并没有真正意义可被正式商用的区块链底层技术。区块链技术暂时无法被大规模商用的障碍和不足如下:

(1)因为每一笔交易或操作都需要从根源处数字验证,所以需要很大的运算量,导致不能承载高并发的大规模商用。

(2)没有统一的技术标准,没有统一的数据接口规范和调用标准、数据结构标准和标准化通用的点对点传输协议。

(3)没有一个通用的底层支撑技术平台,因此每一个试图使用区块链技术的企业都需要从最底层的区块链技术开始研发。

(4)没有区块链跨链间通信标准和协议,致使多数企业建立的区块链无法相互协同。

(5)没有任何对于原始明文的访问控制或授权访问机制,致使不希望面向所有人公开的明文无法使用区块链。

3.1.1 当前主流区块链技术平台存在问题

目前行业中各个主流的区块链平台,无论是比特币、莱特币或是以太坊,在解决具体问题的同时,仍然存在较多的矛盾冲突、特性缺陷,以及实际应用环节的问题。

(1)目前的主流区块链系统,完全无法兼顾“三性+1”原则(即:安全性、扩展性、去中心化,任何应用快速无缝部署到链上)。以比特币和以太坊为例,两者都兼顾了安全性和去中心化,但是对于扩展性就会表现出非常明显的缺失。而另一些方案(如:侧链技术),虽然解决了扩展性,但是对于安全性却又无法兼顾。所以,这些解决方案都有自身的弱点。由于都是主流的区块链平台,因此不再赘述。

(2)对于行业应用存在较大缺陷:

①单位区块创建时间周期过长,导致整体执行速度慢。如比特币 10 分钟创建一个区块的速度,且一个交易需要 6 个区块的时长确认,也就是 60 分钟

的确认时长。而以太坊的智能合约的同步调用规则,导致了所有合约都需要同步等待前一个合约/交易执行完成才能被执行,也进一步将网络的计算能力约等于了一个节点的计算能力,从而使得整体的执行效率很低。这与现实世界对于交易快速处理能力的需求和未来快速交易确认的趋势是背道而驰的;

②交易容量受限:区块的大小以及创建区块的速度,直接决定了单位区块和单位时间内所能容纳的最大交易量,对于单一区块链而言,这个限制是天生存在的。即便是现在有其他的解决方案,如 Raiden 等,也只是解决高频交易,但是对于智能合约的处理,仍然无法提高执行效率。

(3)对于分布式系统的 CAP(Consistency/一致性, Availability/可用性, Partition tolerance/分区容错性)三者处理上不够好。分布式系统的 CAP 上,虽然目前已有解决方案逼近了这个极限,但是并不是所有的区块链都已经很好地处理了。比如比特币在一致性和可用性上过多地强调,但是在分区的容错上并不能很好支持,如果进行交易验证时选择的节点出现问题,会导致错误的发生。

(4)智能合约执行效率低。以太坊智能合约的同步调用机制,以及全网共识的机制,导致执行效率低。

(5)数据和应用孤岛。几乎所有的区块链都是为解决某一个应用场景来进行设计的,因此当多个区块链平台提供了不同的能力集,但是想基于这些能力集共同构建一个去中心化应用的场景和实现,却是非常困难的。区块链技术基本上都是内生性的,所完成的工作和内容都是基于链内场景和应用,对于外部的支持非常少。但是,需求从一开始就已经出现,如 BTC Relay 将比特币区块链和以太坊智能合约综合的解决方案。但是,大部分这样的解决方案也都是一对一的,没有统一的解决方案来试图完成不同链之间的通信和交互。

(6)跨链合约交互非常困难。现实世界中的交易,或者说价值交换,类型和种类往往是多种多样的,参与方很多时候也不仅仅是买方和卖方,也可能还会有贷方、担保方、监督方等。所以对于映射到区块链上的现实交易,往往并不是局限在一个区块链,或者一个链上的智能合约,必然会有需要执行不同链上的智能合约来共同完成交易。现有不同链

的共识方式、数据的同步和处理方式以及合约本身的执行逻辑,均导致跨链合约的执行异常困难。

(7)系统共识方式消耗过多能源;区块链中的CAP三角,还是SSD三个特点,最重要的是全网的共识机制。以比特币以太坊当前的POW机制为例,通过穷举遍历计算相关信息的摘要值的方式争夺记账权(挖矿)的方式,是一种高耗能的工作过程。为了去中心化和安全性,投入如此大的代价维护一个区块链网络是否符合长远发展的可能性,一直是一个普遍的问题。

(8)容错机制缺失,没有有效的解决机制等。对于当前的区块链平台而言,升级和协议的改进本身也是一个巨大的风险。无论是比特币和比特币现金的分叉,还是以以太坊DAO事件导致的硬分叉,均对区块链本身和社区造成了巨大的分裂和影响。最根本的原因在于去中心化的网络本身,在满足安全性的前提下,往往也丧失诸多类似升级、兼容、扩展等必需的功能,从而当社区和区块链本身出现问题时,无法以一种更有效的方式(比如智能修复,平滑升级等)解决相应的问题。

3.1.2 知识产权版权(著作权)转化为经济效益的难点

(1)价值确定难。当前针对知识产权评估方法单一,知识产权种类繁多,涉及的领域五花八门,评估机构对于知识产权所属知识领域的专业能力有限,并且对于该所属的市场行业情况了解有限,使得大多数情况下评估机构只能简单地套用产权人或委托方提供的技术背景、市场情况、技术先进性等说明,以及资产财务方法、估算价值,难以形成一套成熟的估值体系和方法。知识产权成果(尤其是技术含量高,领域较为专业的权利知识产权)的真实客观价值与当前评估价值,或高或低背离。

(2)经济效益转化难。在上述(1)的基础上,当前大部分的知识产权转化的经济收益主要是许可费与权利转让费的方式。可进行转化的对象极为有限,活跃度低,成果转化率低。特定的且纵深的专业领域,特定的应用市场,维权成本和难度大,因此传统的权利许可和转让率很低。原始权利人缺少技术转化所需要的资金、市场运营能力以及相应的团队,传统的融资渠道很难与其结合。因此很多的优质作品被搁浅,具有优质潜力的知识产权资产无法被激活。

(3)知识产权资产流通难。根据金融学,有价即为资产。只有资产化,才可以证券化,即为资产证券化(香港国际知识产权交易中心(持牌机构)内部对此称为“资产份额化投资”)。只有资产证券化,才能将低频的资产变为流动性高的份额化资产。

(4)金融转化难。对于资金和其他资源都极为有限的权利人而言,缺少金融产品工具、金融手段和金融服务的介入,要想进行知识产权的价值再生和转化是极为困难的,其融资风险和付出的成本也极大。这也是目前只有巨头企业、大型企业才能够将自身的知识产权转化为市场效益、经济效益和社会效益的根本原因。

(5)版权(著作权)权利确认难。根据各国法律的原则,著作权或版权自作品产生之时,权利归属于作者或约定的权利人。但是在实践中,很难确定作品由哪个个体最先产生。而且,登记的手续繁杂,时间和空间都存在相对高的成本,因此很多的权利虽然产生,但都无法被法律意义地确定。例如,大量未登记摄影作品、音乐作品、短视频作品等,更难以实现交易和转化了。

3.2 区块链底层技术基础设施的解决方案

区块链技术提供了一种去除中心化的系统应用架构思想,通过公众共识的方式,创建一个相对客观的抗抵赖数字环境。区块链技术架构,以分布式数据技术为基础,以加密技术为手段,进行数据副本的分布存储,抗抵赖验证,以及任何现实事物的“数字”资产化及相应“数字”资产的价值转换。

但是,现有的区块链平台,无论是在理论上,或是在实际应用中,以及是否真正能够支持具体现实中的应用落地,均存在不少问题。其主要原因是这些平台只是从具体的技术架构的设计环节,并没有从系统化的角度侧重考虑对于未来任何具体应用的部署和支撑。

3.2.1 改进技术策略

在保证区块链本身的不可篡改、不可抵赖、公开透明、数据安全等特点的同时,通过搭配技术和其他策略,来有效地改进当前各个区块链解决方案中存在的问题。

(1)提供基础的公链平台,同时定义和规范有效的接口和方式,便于其他区块链进行有效对接。这是支持跨链交易共识系统中最重要的一步。同时,跨链中最重要的共识部分,需要通过统一的公

链平台进行提供。有两种构成方式,一种是非常精简的、基本上无状态化的一个公链平台,提供的能力基于跨链的一个中介平台。在公链上无法创建所谓的智能合约或者其他应用,需要依赖于第三方平台进行完成;另一种是反其道而行之,提供完整的区块链 3.0 能力的公链,除了具有支持跨链中介的能力之外,还要具有去中心化的应用和智能合约化能力。

第一种方式的优点是架构简单,容易实施,但导致部分应用必须依赖第三方平台,带来对应的局限性。第二种方式因为结构的复杂性和能力集的扩大,会导致工作量的快速扩大,也带来了更多的出错可能性;但是因为其带有天生的应用支持和智能合约支持,其适应性和可实施性会更好。

第二种方式所需要大量的资源投入和可能的较长的时间,所以更有可能的一种方式结合这两种方式的优缺点:通过快速实现第一种方式进行跨链支持,同时进行第二种方式的迭代支持更多的应用和能力。另外一个更重要的工作在于定义和规范有效的接口和方式,完成跨链对接。

(2) 提供快速建链能力,无论是行业链还是联盟链,甚至是私有链,均可以通过该平台快速搭建。

在网络层、数据层、共识层的基础上,还有最重要的跨链对接的支持能力上,基于公链平台的有效搭建和部署,可以提供一个类似模板化的平台,便于应用第三方快速搭建和部署自己的区块链平台。在应用层,第三方都可以基于开发平台快速搭建自己的区块链平台,而无需重复开发相应的模块和功能。

(3) 在保证扩展性和安全性的基础上,进行有效的去中心化。

任意的交易和智能合约都需要全网共识的要求,导致全网数万个节点,对于任意交易和智能合约来说,都等效于在单一节点执行,从而导致执行效率低,确认证效效率更低。①不是所有的交易和智能合约都需要全网进行验证的;②通过随机算法和其他诸如 xBFT 和零知识证明的共识算法,能通过部分网络节点快速确认和验证相应的交易和合约,并能最终在全网达成最终的一致共识;③通过有效的结构分层和节点定义,使得数据、交易、合约和共识进行有效的分离,减少互相之间的制约和耦合,同样能提高对应的独立性,最终提升系统和平

台的可扩展性;④安全性的保障上,一方面是来自现有各个区块链平台自身的能力,另外一方面是在平台上引入新的机制和算法。

(4) 通过创新性的技术解决方案,对跨链交易、跨链智能合约等进行便捷有效的支持。

某种程度上,跨链的交易和智能合约执行需要解决的问题除了数据交互之外,最重要的是状态的同步和一致性。对于现有的区块链平台通过以平行链加桥接的方式进行对接。需要注意的是,平行链的维护和规则,和对应的母链是一致的,同时该平行链会提供额外的对接公链的能力。

而如果基于本方案公链创建的新的区块链平台,或者是支持本方案所制定的规范的平台,在技术上,和调用标准的接口 API 没有太大的差异。

现有的区块链平台在很多情况下是不会做剧烈改动和升级的,如果发生这种情况,平行链必然也需要进行对应的升级和改动。这种情况一般都会是经过社区讨论、投票才会做相应的决定,预留的时间、前向兼容的方案等都会认真讨论,所以留给开发和升级实施的时间。

(5) 通过有效的技术手段,提供超过 100 000 TPS 级别的交易和合约执行能力。

扩展性的有效解决,安全性的有效保障,必然能支持更多的交易和合约执行能力。本质上,通过对于交易和合约执行共识的有效分区和隔离,最终通过算法确定全网的一致,从而能支持高交易量。

从另外一个角度而言,区块本身的大小和产生区块的时间实际上限制了交易数量的极值。产生的区块的时间又和分布式系统的 CAP 三角息息相关,即便是通过各种创新的算法,时间也无法压缩到很短,所以区块的大小是一个可改善的点。但无限提高区块的大小也是不现实的。大区块的全网同步和验证需要花费更多的时间。

所以在确定好区块的最大值的情况下,尝试通过交易个数和大小动态调整区块的方式,同时在区块中,将交易和合约本身的内容进行分离,主块中只存储交易和合约的某种摘要的方式,提高同一个区块中能处理的交易和合约的个数,从而提高 TPS 值。

(6) 有效地兼容现有的成熟的区块链系统,如比特币、以太坊等。

基于 UTXO 方式的比特币网络,因为状态的缺失和有限的功能支持,对于跨链支持是非常困难

的。一种可行的方案是通过某种锁定机制,在公链创建对应交易,在完成比特币主网的交易和价值转移之后,在公链进行相应的交易和价值转移,完成最终的跨链交易。在以太坊主链的智能合约带来的费用问题,从逻辑上来说,可以通过对应的交易费用覆盖。

(7)以最简单的方式实现系统,不设置过多的限制和要求。

定义一种交易共识系统模型,提出一种新的完整的系统级解决方案,通过标准化及支持自由扩展的数据接口,标准结构化的数字描述表达技术,以及从数据区块层至跨域层(数据区块层、网络交换层、平台框架层、去中心化应用层、跨域层,由低至高共计5层)的系统结构模型,提供一个可以容纳并支撑任何应用的区块链平台。任何开发者可以快速地将自己开发的任何应用部署到该区块链平台;任何个人或组织可以任意地、自由地定义创建自己的智能合约,并按照合约的定义,自动执行链上或链下任何应用系统或程序;任何组织或个人可以将其已有的、正在使用的任何应用业务系统,无缝地与主链进行对接;通过平行链和混链技术,可以双向的兼容目前任何已知的区块链主链,未来任何个人或组织新开发的任何区块链主链或行业链,都可以完全地接入并与主链相互兼容。既保证了数据的严格不可抵赖性及防篡改性,也同时保证了任何个人或组织数据的私密性,在防篡改性、开放性、完全的去中心化以及任何数据的私密性之间,达到了完全兼顾,为数字版权的所有应用系统提供了更好的落地可实施环境和区块链基础设施。

3.2.2 解决方案

目前为止行业内没有统一的底层基础、没有统一的数据标准和数据结构,应用系统很难实施区块链技术,所以建立标准的和统一的技术底层设施并可以支持所有应用快速的接入区块链底层基础设施是非常必要的。否则,多个应用难以联合协调运营,也难以产业化和商用化运营。

(1)依照 Chain NetWork WEB 3.0 (CNWW3) 建立区块链基础设施

基于块状数据结构和分布式去中心化逻辑,定

义并发布区块链标准框架模型。此模型定义标准数据接口,可扩展的结构化和格式化表达式,及由低至高的数据区块层、网络交换层、平台框架层、去中心化应用层、跨域层共5层(见图1),定义了可支撑任何应用的区块链环境。^[1]

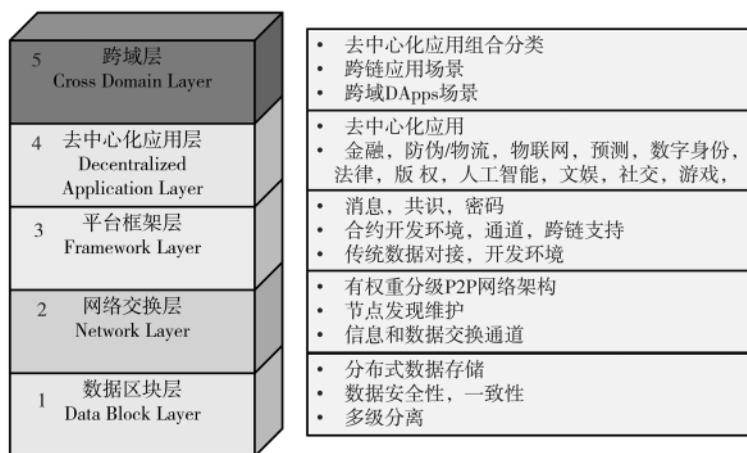


图1 区块链标准网络应用 Web3.0 模型 (CNWW3 模型)

可依据模型将应用独立部署或接入区块链网络;支持自由定义、创建和执行智能合约,并按照合约的定义自动执行链上或链下无缝接入的应用系统。模型中的平行链、侧链和混链标准,双向兼容任何主链或行业链。在防篡改、开放、完全去中心化及数据私密性之间达到完全兼顾,为行业提供了部署去中心化应用的区块链基础标准。

上述发布的区块链标准应用模型及应用部署的方法,提出了应用系统独立部署到区块链的完整系统级解决方法。该方法通过标准化及支持自由扩展的数据接口,标准结构化及格式化的表达式用以描述任何智能合约,以及从数据区块层至跨域层的系统模型,提供一个可以容纳并支撑任何应用的区块链环境。支持任何开发者快速地将自己开发的任何应用部署到该区块链平台;自由地定义并创建智能合约,并按照合约的定义,自动执行链上或链下任何应用系统或程序;支持将其已有的任何应用业务系统无缝地与主链对接;模型中的平行链和混链模式,可以双向兼容任何区块链主链或行业链。

模型既保证了抗抵赖性、开放性和完全的去中心化,同时保证了数据的私密性。在防篡改性、开放性、完全的去中心化及数据私密性之间,达到了完全兼顾。解决当前区块链技术本身存在的缺陷,为各行业提供了在区块链环境中的应用落地方法和

基础设施。

各个层级的描述和定义可以参考图 1。实现跨层的基础是提供可支持跨链的合约和共识系统。

(2) 建立公链。

用于解决跨链的方案有三种, 见证人模式 (Notary)、侧链或者中继模式 (Relay) 和哈希锁定模式 (Hash-Locking) 都需要通过创建新的区块链平台, 也就是基于新的区块链进行相应的模式开发。同时, 如果解决方案提供通用统一平台的话, 新建的区块链必然是公链, 从源代码到基础架构, 都是公开和透明的。公链的作用有如下几点: ① 提供公共区块链用于跨链中继, 完成交易验证, 数据证明, 资产转移, 智能合约执行等工作; ② 提供统一对外接口和规范, 快速接入公链进而支持跨链; ③ 提供基础的区块链平台能力, 快速完成方案部署和验证, 有效降低试错成本; ④ 提供公共开发平台, 一次性完成多个平行链智能合约协同开发和部署。

公链内容除了记录自己的区块链信息外, 最重要的内容是相应平行链的信息摘要 (交易摘要)。通过格式化的交易数据方式记录相关的内容, 同时, 通过某些类型的压缩算法, 能有效地提高区块的存储能力, 从而能记录更多平行链 (第三方区块链) 的信息。根据实际需要会增加其他的内容。行业链或联盟链或私有链, 都可以通过公链平台快速建立。CNWW3 支持调用创建链的封装快速建链。① 在不改变现有区块链的基础上, 通过提供独立平行链, 完成平行链与公链的对接; ② 提供标准的接口规范。新区块链基于对接规范适配开发即完成跨链。其中非常重要的一点是, 如果新链是基于公链创建的, 就可以认其为公链的侧链, 天然具有支持跨链的功能。

通过 CNWW3 模型 (如图 2 所示) 中交易锁定方式, 在 CNWW3 模型定义的公链发起有锁定条件的交易, 平行链监听其他区块链的交易结果并同步至公链, 完成跨链交易。对于支持智能合约的区块链网络, 调用公链智能合约, 通过平行链的智能合约桥接, 执行主链部署的智能合约进行交易。平行链监听主链交易和状态并同步至公链, 完成跨链交易。在公链中, 从最底层的网络协议、加密解密、数据存储到上层的智能合约、去中心化应用等, 从本质上是进行有效的分层管理和控制的。整个系统中存在多类型共识处理, 如数据有效性、交易有

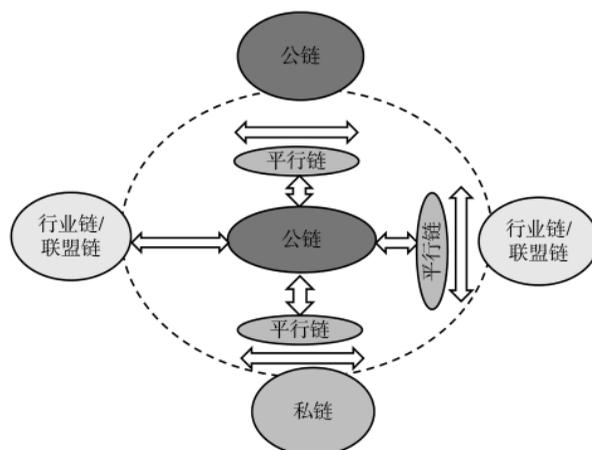


图 2 实施 CNWW3 模型示意图

效性、控制有效性。在本方案中, 在协议和软件架构层面, 将对这些内容进行有效的分层: ① 数据层、交易层、共识层、合约层、应用层等按照对应逻辑进行清晰划分; ② 在各个软件架构层面, 通过定义接口的方式, 分别对其进行独立和解耦; ③ 在共识处理上, 采用的是不同层级采用不同共识的方式, 同时互相之间不做直接强管理; ④ 通过区块的多级 hash 处理, 使得在区块同步时, 能有效快速地调整已经被验证过的区块的顺序。

支持超过十万 TPS 级别的交易和合约执行能力。通过对于交易和合约执行的共识分区隔离, 通过算法确定全网的一致, 能支持高交易量。在 CNWW3 模型中, 通过交易个数动态调整区块大小, 并在区块中将交易和合约本身的内容进行分离, 主块中只存储交易和合约的摘要值或散列值, 同时提供异步调用合约机制, 提高同一个区块处理的交易和合约的个数。

CNWW3 模型中, 交易是具有状态的, 对应的状态变迁如图 3 所示。

作为应用层面最大的支持, 在公链上回提供图灵完备的智能合约机制。系统本身的部分工作也是通过内置的智能合约来进行的, 对应的状态变迁如图 4 所示。

智能合约的调用一般都是通过交易来触发的, 如以太坊的智能合约, 通过交易携带对应参数的方式触发合约的执行。

CNWW3 模型中, 不同角色分别维护公链和平行链。为了在平行链和公链上以最简方式存储必要的数, 也提供分布存储能力, 用于存储其他类型

的基础数据。

- (1) 权益所有者(O)。具有系统 Token 的用户。
- (2) 公链维护者(M)。任意节点都是维护者。

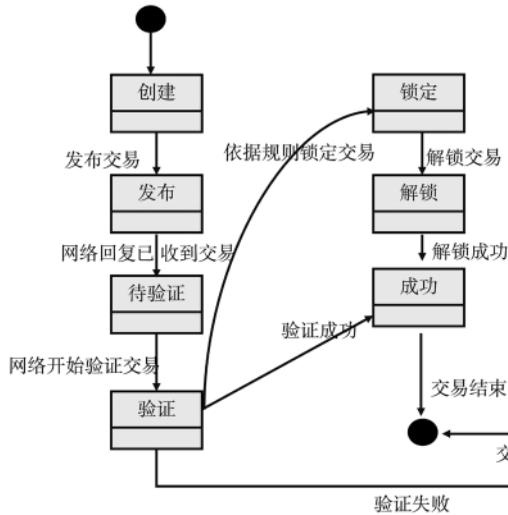


图3 交易状态变迁示意图

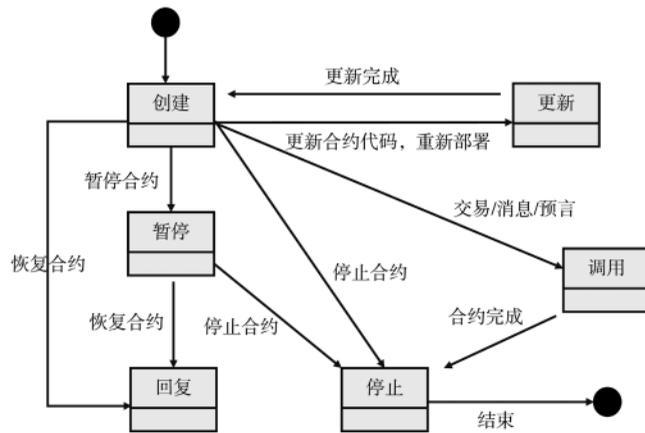


图4 智能合约状态变迁图

(3) 平行链维护者(P)。任意节点可申请成为平行链维护者。

(4) 所有的节点都自动具有监督者/候选者(C)的角色。在指定周期内未被选中承担 M 或者 P 角色的节点,可以自动作为 C 的角色进行监督和监察的工作。也可能被选中作为 M 或 P 的角色,在不同阶段承担不同角色。

(5) 公链服务提供者(S)。提供公链服务的节点。

(6) 数据存储者(D)。分布式数据存储的节点。

从基础设施网络的角色而言,多个角色的存在以及转化,对于网络的要求就比较复杂了。这和一般的区块链平台的节点/角色不太一致,各个角色在某个特定时期内并不完全对等,同时角色的状态属性也必然要求在网络层面,也有对应的区分和分层。所以在本案中,对于网络层,有对应的特殊设计和处理。目标是建立一个具有可自动伸缩能力的自适应网络平台。

ONWW3 模型对于网络层是可自动伸缩的自适应网络,分层如图5所示。

公链验证和确认。基于公链,通过创建智能合约,可以方便地定制跨链的交易和事件验证。其本质上和跨链的交易验证和确认是一致的。

综上所述,数字版权的应用业务是比较多的,需要的并发处理业务环节也很多,在正式的商业应用中用户访问量也大,因此支持数字版权的商业应用区块链的底层基础支撑必须能够满足高并发、快速数字处理能力、高用户并发访问、多扩展性、多应用系统支持。

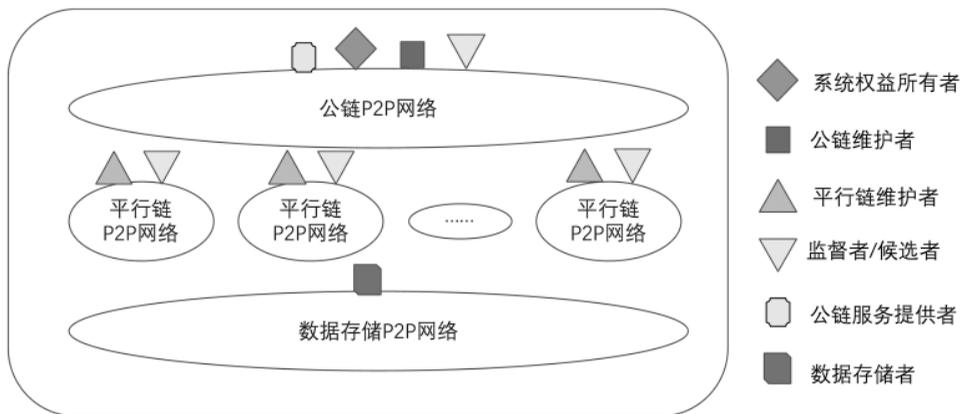


图5 网络模型层级示意图

3.3 建立应用确权系统和交易平台系统

基于上述区块链底层技术基础设施 CNWW3,开发集成功能包括权利确定、流通性数字资产登记、价值确定与权利资产化、资产交易、金融服务、维权联盟等。区块链技术可以很好解决以上功能的痛点,以及提供使用区块链技术所产生的信服力和公信力。^[2]

资产估值确定平台。由注册会计师团队、资产评估团队和金融团队,采用已经被证明过的成熟估值体系及其优点,设计出一套有效的估值体系和评估模型。该估值体系和评估模型是格式化、微分化的,且融合了证券市场关于知识产权估值的部分模型。根据区块链思维,一项估值是由多个机构共同完成的,能够完美解决上述“价值确定难”的痛点。

金融服务平台。面对两类合作伙伴:银行类金融机构,提供交易资金结算及保证金托管服务(合规性是红线),是信贷类产品的主要出资方;非银行类金融机构,提供金融产品创新方案和衍生服务(例如资产证券化、资产托管、金融科技、数据风控等)。二者互相结合弥补,围绕交易主体为核心,形成完整的产品及服务体系。

维权联盟平台。该平台引入多家世界各地及国外的知识产权机构和律所机构,按照维权联盟平台的格式化流程和方案,形成覆盖全国各地范围的强大维权联盟网,并且尝试与北京互联网法院、上海互联网法院、杭州互联网法院、广州互联网法院建立联动关系,

形成维权、司法审理一体的快捷法律通道。

国际化的知识产权金融交易平台,同时具有金融服务功能。主要功能如下:(1)知识产权价值确定服务;知识产权成果转化交易与融资性交易服务(包括整体许可和份额分拆许可融资及交易);(3)知识产权整体化权利交易服务和份额化权利拆分交易服务;(4)知识产权司法维权保障;(5)知识产权一般金融服务和新金融服务(当前知识产权领域有具有行业特性的金融需求,但没有针对性金融工具及产品支持,为此,与金融机构共同针对知识产权领域设计具有创新性的金融工具及产品)。

该平台应用系统的功能和业务架构图如图6所示,包括:(1)知识产权价值确定服务,知识产权成果转化交易与融资性交易服务(包括整体许可和份额分拆许可融资及交易);(2)数字版权整体化权利交易服务和数字资产份额化权利拆分交易服务;(3)知识产权权利稳定性指数服务;(4)知识产权司法维权保障;(5)知识产权一般金融服务和新金融服务(新金融服务是当前具有需求,但并没有相应的金融工具的产品,与部分互联网银行,为此,专门针对知识产权设计的具有创新性的金融工具产品,由相应入驻的银行机构提供服务)。

除了用区块链技术承载的各个创新平台,多数创新平台采用基于新技术的创新操作模式运行,其中最最新操作模式的数据资产操作平台是平台2、3和4,最具价值创造能力的价值创造平台是平台1、

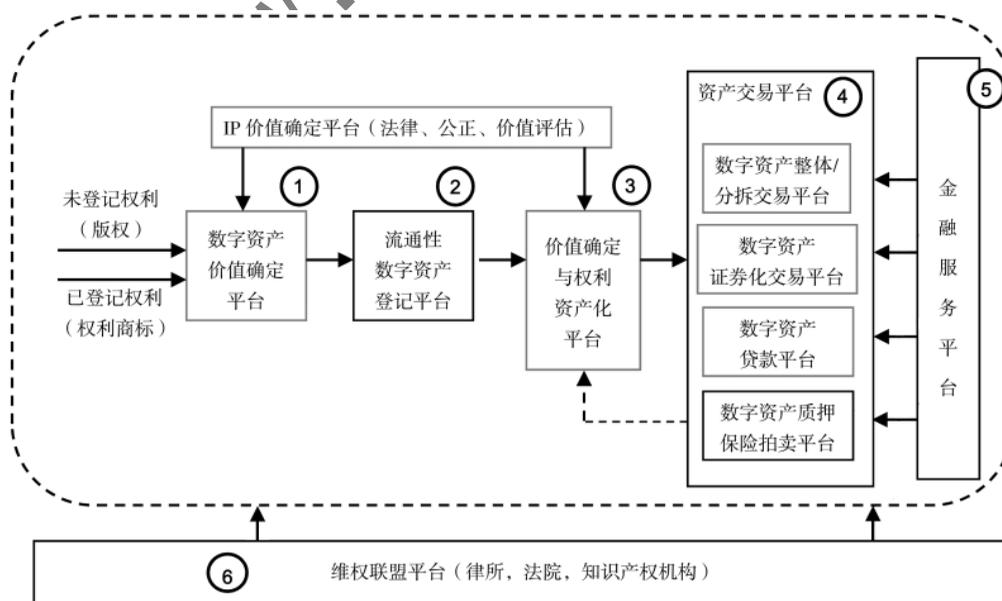


图6 业务流程和业务流转分析图

3、4 和 5。其中,平台 4 的价值评估部分和数字资产处理部分;平台 3 的拆分交易部分,平台 4 的(一、二级交易)证券化交易部分采用创新模式运行,有利于解决前述“困难”问题。而价值创造平台则有利于金融中心获得提供金融服务对价的巨大收益。

3.4 建立金融服务平台及金融服务方案

知识产权金融服务方案=

$\frac{(\text{区块链技术}+\text{新估值方法}+\text{金融过程}+\text{交易})}{\text{强维权联盟导致的第三方侵权量下降}}$

(1) 金融服务平台产品方案

知识产权金融化的整体实施思路是基于将所有的资产进行数字资产化,然后在合法合规的前提下逐步实现资产证券化,从而达到知识产权的高频流通和结算,让更多的人参与到知识产权的交易中去,实现知识产权的转化和实际落地应用,如图 7 所示。

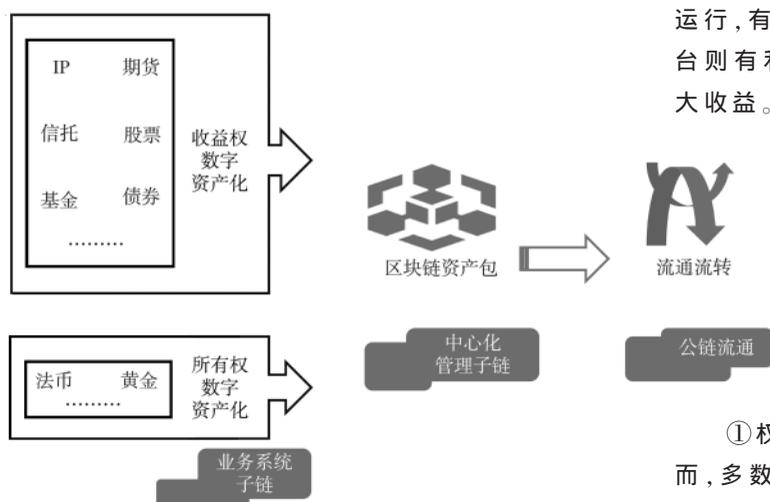


图 7 金融方案架构说明图

金融服务平台方案涵盖如下内容:

①通过交易平台完善知识产权登记、评估、交易功能,吸引金融广泛介入知识产权领域。以包括保理、融资租赁、信托、投资、证券、保险、众筹等多种产品手段在内的整体金融产品体系来全面支持知识产权从生产到交易、使用的全流程。鼓励创造者更多更好地进行知识产权的创造,提高知识产权的利用率、流通率、投产率,实现知识产权交易与金融的互相促进成长。

②完成从金融渠道商向金融科技商的身份转变,形成源于知识产权领域,向产业上下游、参与主体及关联对象延伸的、泛用性强的金融科技能力。

③扎根于知识产权领域,探索解决方案的跨行业通用性。以“赋值”为关键词,将底层资产扩大到包括 IP、期货、信托、股票、基金、债券、地产、应收账款等资产的收益权,包括各种货币、黄金、白银在内的现金及等价物的所有权,并实现跨行业的高速高频流通。

④在平台 3 的基础上实现一种具有二象性特征的区块链解决方案,其同时具有资产交易和支付结算底层工具的适用性,可以链接任意资产交易场景。

金融中心,除了采用区块链基础设施 CNWW3 承载的各个创新平台,多数创新平台采用基于创新操作模式运行,其中最具创新操作模式的数据资产操作平台是平台 2、3 和 4,最具价值创造能力的是平台 1、3、4 和 5。其中,平台 3 的价值评估部分和数字资产处理部分;平台 4 的拆分交易部分、证券化交易部分(一级交易和二级交易)采用创新模式运行,有利于解决前述“痛点”问题。而价值创造平台则有利于金融中心获得提供金融服务对价的巨大收益。

通过权利许可、转让等手段实现权利技术转化,其本质是科技资产的优化再配置,有利于使科技资产通过市场流转,被配置到最有利于其转化(或产业化实施)和获益的环境中。因此,权利的经济转化需要通过交易实现。

(1) 现有权利交易的局限性

①权利交易的前提是卖方出售自己的权利。然而,多数权利人申请权利的目的在于保护自己的市场,而非出售,这将直接导致权利交易必定是小众行为。

②权利与其伴随的实体资产(也可能是虚拟实体资产,例如包括软件著作权)具有不可分割性,对于纯正权利目的单纯的权利交易(指与其伴随的实体资产分割开的权利)通常仅限于少数有权利冲突的竞争者之间,因此,这将直接导致权利交易必定是小众行为。另外,现有权利与其伴随的实体资产分割开的交易注定难以转化。

(2)使权利成为高频交易物。只有使权利成果变成大众参与、最优转化的标的物,才能成为高频交易物。

方案 1 增加权利交易模式。在现有权利交易模式的基础上,增加产业互补或技术互补者之间的交

易模式,以及增加技术联盟的权利资产包按份许可交易模式。

方案2 权利资产包证券化交易模式。该模式以权利资产包为交易物(资产包中包括权利成果及其伴随的实体资产)。例如,一个优质企业可能有多个权利资产包,多个企业和个人权利人可以共享一个权利资产包。该模式与目前上证、深证等以企业资产为交易物的模式具有本质区别。其优势在于:

①交易对象不再受个人或企业的影响,资产包共享权利人之间通过许可交易组包,权利人享有资产包按照份额享有利益分配权,从而建立分工式转化、份额式分配利益的机制。因此,理论上任何符合资产包标准的权利成果及其当前伴随资产都可以加入权利资产包(情况不同,通过评估机制影响获得的份额),因此,有利于集合更多权利人创造的有价值的权利化成果,而不论其实施能力,从而使权利交易逐步变为大众参与的交易,最大限度地减少投资的浪费。

②使资产包被自然配置到最有利于其转化和获益的环境中,由于有利于吸收竞争者和互补者进入资产包,竞争者演变为合作者,使得资产包具有最

优化的抗市场风险能力和获益能力,成为低风险、高收益的投资品。因此,该模式有利于集合更多更有价值的权利化成果,以及实现权利成果的市场收益最大化,而风险最小化。同时,投资者的投资利益和安全性能获得最大限度的保证,有利于调动机构和个人的投资积极性,使权利成果交易变为大众参与,最佳实施者转化的投资品。

用户角色定位,规划金融产品体系如表1所示。

引入金融服务,实现数字版权资产的金融能力如表2所示。

交易与金融互相扶持,增加交易量;对金融机构实现业务引流;具备覆盖全部用户的金融产品体系。形成源于知识产权领域,向产业上下游、参与主体及关联对象延伸的、泛用性强的金融科技能力,探索实现一种跨行业的“交易+金融”区块链解决方案。将数字版权完全变化为底层资产,可以链接任意资产交易场景并实现高频流通。

4 可信的数字版权模式的数字资产金融价值优势分析

(1)数字包与资产进行唯一性创建对应时,可以赋值为任意资产,所以数字包本身在理论上可以

表1 用户角色定位,规划金融产品体系

	创造者	服务者	交易者	生产者	投资者
特色金融产品	VC及股权投资、 创作指数分析	保理、配资	经营融资、抵质押 融资、保理	经营融资、融资 租赁、保理	信托、资产 证券化、再保理
著作权领域	作者(电影、 短视频、文字)	演出经营公司、 设备及场地 经营公司、影院	版权经营公司	出版发行商	VC、PE、投行、 基金、私募、 合格投资者
特色金融产品	众筹、融资租赁、 VC、创作指数分析	融资租赁、保理	经营融资、抵质押 融资、保理	经营融资、融资 租赁、保理	信托、资产 证券化、再保理
通用金融产品	支付结算、无抵押无担保的信用类融资、估值及风控大数据服务、消费金融、保险				

表2 引入金融服务,实现数字版权资产的金融能力

运营阶段	上线初期	客户细分	用户范围	拆分交易
金融产品引入	无抵押无担保的 信用类融资	订制金融产品、保理、 融资租赁、保险、众筹、 抵质押融资、增信等 经营性融资服务	VC、PE、投行、基金、 私募、合格投资者	资产证券化、大数据 服务、配资服务
行动	覆盖范围最广的 金融服务	根据用户的细分角色 提供更多更符合其 需求的特色金融产品	建设大数据服务能力; 拓展非交易类金融服务	引导合格投资者对创作源头进行 合理投资;平台核心能力在交易 及金融撮合之外增加大数据服务
目的	信用类融资服务 和担保融资服务	交易及金融差异化需求	通过引入投资型用户, 增加交易频率和金额	良性扶持知识产权创造的目标; 长期无风险的可持续能力

支持任意底层资产进行数字资产化,区块链解决方案具有跨领域通用的能力。

(2)子领域(各个交易平台、支付结算系统、企业生产管理系统等任何有资金或贸易往来链接的子链管理系统)内的资产与资金的流通不必以实质性转移为标准,以流水表格的形式按顺序记录赋值情况即可实时反映资产的价值形态、所属者。对应的实际资产可以以信托资产或资金托管的方式在某些资产管理机构进行集中管理。

(3)数字资产包的可流通范围受赋值主体及赋值内容影响,流通性服从于子领域自身的交易管理规则,解决方案与子领域融合时阻力很小。

(4)数字资产包在不同子领域之间流通时,在两个子领域的交互点进行权属交换即可,跨链交易可以实现实时极高频互通。

(5)作者出新作品可以直接挂到交易平台,创建 N 多份使用授权,以链接或者付款二维码的方式挂出去,粉丝付款就能使用。同时不耽误将所有销售给出版商,出版商也不用担心提前销售部分影响自己收益。

(6)作品所有权交易时,只需双方商定价格就可以立即交割完毕。

(7)交易纠纷时,区块链技术实现快速举证与举证有效性。

(8)完成公证声明后,可以自行发行股权并交易,节省大量时间及成本。

(9)股权转让中的限制条款可以通过发行时权限设置来实现。

(10)股权的转让和资金兑付更为高效清晰。

(11)包括现金、现金等价物、有价证券、虚拟财产在内多种底层资产支持的,自身拥有实际价值,可以跨地区、币种、资产状态进行自由流通的数字货币在理论上存在。不触碰和不破坏,也不违反货币发行权、资金监管、外汇管制等各国现行法律和规定,容易获得各国政府的支持。拥有更多的资产支持、更高的信用等级、更大的流通范围。

(12)支持搭建一个能装入所有资产的超级钱包和对应的唯一的数字身份机制。

(13)国际间结算支付在技术上实时完成,无

用,又可以根据管制要求任意附加限制。

(14)区块链数字版权对于行业的价值。

5 数字资产交易描述

建立了以区块链为底层基础设施的数字版权为核心的金融应用,不但作品作者可以有很大的金融收益和经济收益,同时也促使各国的相关配套服务行业有了很大的提高和增值利润空间,带动了相关配套服务行业的发展。

基于区块链的数字版权应用系统,数据的私密保护与监管,可实现版权管理。任何明文(原始内容)数据都拥有唯一的数字摘要值,一点上传,多点同步分发,以及区块链智能合约的交易。

产品服务的优势:(1)数据不可篡改。分布式存储、块链式数据结构、时间戳、数字签名、非对称加密保证数据不可篡改;(2)文件安全隐私。经过 HASH 族算法将文件进行摘要值写入到区块链,同时同步到各个节点,无法篡改和伪造,只有用户自己的私钥或者授权的访问控制才能访问原始数据;(3)多方可信背书。链上的数字公正机构发放,获得可信区块链过程证书,满足法定程序的需要。如图 8 所示。



图 8 产品服务架构图

用户过程业务描述如图 9 所示。

6 结论

以区块链技术为基础的数字版权,可以达到绝对的公平和可信,符合各国的关于版权(著作权)权利确定的法律要件,并且能够实时地完成电子化版



图9 用户过程业务描述

权(著作权)权利确定,不可篡改,不可人为干预,达到了完全绝对的可信。结合金融资本服务,涵盖版权质押融资、交易转让、保险、信托及证券化等创新要素的金融服务体系,更好地破解权利估难、流转慢、融资风险大等问题。在遵守各国法律的前提下,逐步实现版权(著作权)从线下到线上的数字版权产权转化、拆分、打包、最终实现线上交易,以及为交易双方提供金融、法律、维权等服务,提高交易的成功率,降低交易的风险,从而最大限度激活市场潜在版权产权交易,真正实现了将数字版权转变为数字资产,将数字资产进行了金融化服务,促使原本固态的版权成为了高流通性的金融资产。数字版权权利人拥有了大量的资产财富,更加提高了全世界优质作品的产生和经济效益的转化。

参考文献

[1] 白杰,李东云,吴先锋.发布区块链标准应用模型

及应用部署技术研究[J].信息技术与网络安全,2018,37(8):13-18.

[2] 李东云,白杰,吴先锋.发布区块链 CNW3 标准的高并发快速交易及交易验证体系模型[J].信息技术与网络安全,2019,38(3):53-56.

(收稿日期:2020-06-01)

作者简介:

白杰(1980-),男,俄罗斯联邦总统直属国民经济与国家行政学院教授(兼职),主要研究方向:区块链技术应用。E-mail:abc@baijie.com。

杨鹏飞(1983-),男,学士,主要研究方向:供应链金融、支付结算、交易所业务、场景化综合金融解决方案的设计和和实施。

孙鲜艳(1981-),女,硕士,高级技术职称,主要研究方向:互联网项目管理和质量控制。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部
中国电子信息产业集团有限公司第六研究所