Accepted Manuscript

Blockchain for digital rights management

Zhaofeng Ma, Ming Jiang, Hongmin Gao, Zhen Wang

PII: S0167-739X(18)30161-4
DOI: https://doi.org/10.1016/j.future.2018.07.029
Reference: FUTURE 4347

To appear in: *Future Generation Computer Systems*

Received date : 25 January 2018
Revised date : 10 July 2018
Accepted date : 14 July 2018

Please cite this article as: Z. Ma, M. Jiang, H. Gao, Z. Wang, Blockchain for digital rights management, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.07.029

Future Generation Computer Systems

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Blockchain for Digital Rights Management

Zhaofeng Ma[a,b] Ming Jiang[c] Hongmin Gao[a,b] Zhen Wang[a,b]

[a]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b]Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China
[c]3.The Third Research Institute of China Electronics Technology Group Corporation, 100015, Beijing, China

HIGHLIGHTS

- We proposed a new trusted model DRMChain for digital rights management based on blockchain
- The DRMChain builds up an external flexible storage and internal blocks creation architecture
- The DRMChain provides a DRM-protected scheme supporting for identity and privacy protection
- The DRMChain innovates a violation tracing approach with conditional identity management

ARTICLE INFO

Article history:
Received 23 January, 2018
Received in revised form
on 10 June, 2018
Accepted 16 July, 2018
Available online

Keywords:
Digital rights management
Blockchain
content protection
privacy proteciton
conditional tracing
violation checkout

ABSTRACT

Online digital content service becomes more and more easily, however, free consumption and excessive spreading without rights protection will hurt the content providers' benefits and causes business loss, another problem is once the content provider supply illegal or politically sensitive content such as terroristic opinion or multimedia content, it will cause serious social problem such as fright or social crisis. To solve this problem, in this paper we proposed a blockchain-based scheme for digital rights management(named DRMChain) ,which supports the right content serves the right users in a right way, the DRMChain can provide trusted and high-level credible content protection and conditional traceability of violation content service. In the proposed DRMChain, we use two isolated blockchain application interfaces (BAI) to respectively store plain and cipher summary information of original and DRM-protected digital content, and considering large capacity of digital content such as image, audio or video, we proposed external flexible storage of plain/cipher digital content and creates hashID of the content itself and links with the blockchain. In DRMChain scheme, we named the BAI plain interface as BAIP for summary metadata storage of original content, and the BAI cipher interface as BAIC for DRM-protected content service. In the DRMChain scheme we proposed efficient and secure authentication, privacy protection and multi-signature-based conditional traceability approaches, and thus the DRM license, usage control and constrain information can be easily retrieved form the blockchain, and customs can query all the consumption transaction lists of free or paid consumption history to prevent baleful fee-deduction. Analysis and performance evaluation manifest the DRMChain scheme provides a reliable, secure, efficient and tamper-resistance digital content service and DRM practice.

1. Introduction

Digital content consumption is now becoming popular, more and more people often visit and watch videos or images resource through web browser or mobile App-based software. However illegal content usage(such as illegal download and spread the right-reserved content) may do harm to content providers, or hurt the right-holder's business stakeholder[1-4], upon the value-added content or business data, it's necessary to use technique solutions to prevent the data being stolen or being illegally used, and together should enhance the usage control of content access. In fact, digital rights management[5-9]is an important technology for content protection of rights holder's profits or business stakeholder[1-3,6,9], upon which many institutes and researchers paid much attention and do more research work on DRM[1-5,10-20], however, current DRM technologies such Windows DRM, Silverlight, RealNetworks, Flash AIR, Apple HLS DRM focused on content encryption and license management, however it is obviously lack of original content management violation checking and tracing of the one who should responsible for the violation[12-16].

Upon the above problems, new DRM architecture should require efficient and reliable technologies that can provide creditable, tamper-resistant and high-level secure and flexible supporting[1-6]. Fortunately, blockchain is a decentralized, reliable and secure computing paradigm in P2P network environment[21-24], which provides distributed ledger technology (DLT) that store the completed blocks in chronological order with tamper-resistance and security, it allows participants to keep track of digital transactions without central recordkeeping, Each node holds a copy of the blockchain downloaded automatically, the record's authenticity can be verified by the entire community using the blockchain instead of a single centralized system[25-28]. Blockchain can be applied for IT asset management and supply chain management, trademarks copyrights protection, credit certificate proof[29-40]. The most famous and successful