

GLOBAL MUSIC ASSET ASSURANCE DIGITAL CURRENCY: A DRM SOLUTION FOR STREAMING CONTENT USING BLOCKCHAIN

Ahmed Gomaa

Department of Operations and Information Management,
University of Scranton, Scranton, USA

ABSTRACT

*The amount of piracy in the streaming digital content in general and the music industry in specific is posing a real challenge to digital content owners. This paper presents a DRM solution to monetizing, tracking and controlling online streaming content cross platforms for IP enabled devices. The paper benefits from the current advances in Blockchain and cryptocurrencies. Specifically, the paper presents a **Global Music Asset Assurance (GoMAA)** digital currency and presents the **iMediaStreams Blockchain** to enable the secure dissemination and tracking of the streamed content. The proposed solution provides the data owner the ability to control the flow of information even after it has been released by creating a secure, self-installed, cross platform reader located on the digital content file header. The proposed system provides the content owners' options to manage their digital information (audio, video, speech, etc.), including the tracking of the most consumed segments, once it is release. The system benefits from token distribution between the content owner (Music Bands), the content distributor (Online Radio Stations) and the content consumer(Fans) on the system blockchain.*

KEYWORDS

Blockchain, Cryptocurrency, Digital Rights Management, Public Key, Private Key

1. INTRODUCTION

1.1 Streaming Content Problem

The online streaming music in the United States has been increasing in the past several years. It currently accounts for 65% of the music online share [1]. The multibillion dollar industry is constantly faced with intellectual rights infringement. For instance, in January, 2018, Spotify, a music streaming company was sued by Wixen Music Publishing Inc. for allegedly using thousands of songs, without a license and compensation to the music publisher [2].

There are two main music royalty collecting societies in the USA: the American Society of Composers, Authors and Publishers (ASCAP) and, Broadcast Music Inc. (BMI), with hundreds of thousands of members each. If two artists collaborated on the same music album, but are subscribed to different royalty collecting societies, they will receive different royalties, a fact that shows the discrepancy in how played streams are counted in different organizations. As of 2016,

ASCAP and BMI alone collect and disburse payments in the range of \$1.8 billion annually on behalf of hundreds of thousands of musicians for royalties around the world. It is not the actual value of the market. According to Institute for Policy Innovation (IPI) 2007 report, that it is costing the US economy more than 12 Billion dollars due to sound recording piracy in the US. In 2017, ASCAP and BMI announced the creation of a new comprehensive musical works database to increase ownership transparency in performing rights licensing that is expected to roll out at the end of 2018 [3]

The problem becomes more challenging when considering the online radios, and the Disk Jockeys (DJs) who are mixing music live and stream it online with audience listening around the world. The sale and distribution of media content using a digital medium provides simple and flexible production, consumption, and transmission of such content. However, it also reduces the efforts needed for unauthorized usage of this data. Thus, digital media content is more easily copied, distributed, or used in a manner not allowed by law or license agreement.

1.2 Blockchain Technology Overview

Blockchain enables secure peer to peer transactions [4]. There is a number of existing public blockchain platforms including Ethereum and Bitcoin Blockchain. Each platform has its own purpose. For instance, Bitcoin Blockchain enables a peer to peer cash system to allow online payments and allows for tracking ownership of the digital currency. On the other hand, Ethereum platform focuses on running the programming code of any decentralized application [5]. To incentivise and assure the decentralization concept, each blockchain platform rewards the platform participants, called miners, with coins, either Bitcoins on the Bitcoin Blockchain or Ether on the Ethereum blockchain. It may be viewed as a compensation for the work done. Each block on the blockchain includes a number of transactions. The blockchain platforms are designed for the entire network to consume electricity proportionate to the amount of coins given to the miners. Once a block is added, all miners compete to solve the computational problem for the new block. On the bitcoin blockchain, a new block is created every 10 minutes on average, while on the Ethereum blockchain, a new block is created every 15 seconds on average. At any given day, the amount of money spent by the entire network on electricity will be proportional to the amount of money gained by those who find the correct answer first. For instance, on a certain day in April 2018, on the Bitcoin Blockchain, 153 blocks were mined, with an average time of 8.72 minutes between every block, the 153 blocks contained 226,626 transactions. The estimated profits from the miners on that day was \$17,344,399.98, on the other hand 43% of that amount is estimated to be spent on the electricity by the entire network. In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether. Since Ethereum blockchain is designed to run programming code on decentralized application, its protocol can be used as a tool for self-operating computer programs that automatically executes when specific conditions are met.

1.3 Public Key / Private Key infrastructure

Both Bitcoin and Ethereum blockchain implementations use public key / Private Key infrastructure, where it is used in digital wallet creation and transaction generation and verification.

For instance, to generate a Bitcoin wallet, the digital wallet software will generate a new private key and a corresponding public key. These keys are later used by the owner of the wallet to send and receive coins on the platform. The concept is that someone may digitally sign an item, to confirm they are allowing an action to take place with a private key. In the Bitcoin implementation, it is sending money. Once a transaction is signed by the owner and sent to miners to be added to the blockchain, after the proof of work is done by the miners and a new block is added to the blockchain, the money is sent from one wallet to another.

The paper attempts to benefit from the proof of concept manifested in public key / private key infrastructure implemented on the Ethereum blockchain along with the capability of running decentralized programming applications on the blockchain to address the piracy problem on streamed online content on a new blockchain network, named “iMediaStreams Blockchain”. iMediaStreams Blockchain is a decentralized solution to music publishing houses as it addresses the process of validating the authenticity of the music streams.

1.4 Current Solutions and their problems:

Lawmakers recognized the growing need to protect digital media and enacted the US Digital Millennium Copyright Act (DMCA) [6, 7] to protect property rights. One approach to curbing the proliferation of illegal activity surrounding digital media content is to incorporate a form of Digital Rights Management (DRM) into the digital content. DRM can be used to detect and verify ownership of data and to control access to the data in accordance with a policy determined by the content creator or distributor. A further approach frequently incorporated in a DRM system is to embed a digital watermark in the digital media file. A digital watermark is information that is generated and interspersed in the data of the digital media file but cannot be perceived by the audience of the digital media file [8, 9, 10]. For example, to a listener, a digital audio file that contains a watermark would sound identical to the digital audio file without the watermark. However, an examination of the data (e.g., by media player software) can detect (i.e., extract) the watermark to determine if the file has been modified in some way. Possible modifications that could alter the watermark include compression of the data [11-19], cropping an image or video or attempted removal of the watermark. Watermarking can also be used to fingerprint a file; such that different recipients receive differently watermarked content. Thus, by examining the watermark, the proper owner of a file can be determined and any tampering with the file can be detected. Attempts to address the DRM in streaming music are presented in [20], [21], and [22] where the main difference in this paper lies in the usage of the blockchain technology and having a digital wallet within the browser plugin. [23] Introduced the concept of using Blockchain in controlling digital content, but did not allow for cross platform rendering and access policy control on the media file. [24] Presents an access control policy on the blockchain. The main difference in the paper in contrast with the recent publications and patents is in the way this paper includes the access control on the file header instead and the build in player, an architectural difference that allows for the destruction of the file even after being send out. Current commercial DRM solutions focus on watermarking digital media content to indicate ownership of a specific copy of the content and ways to track and prevent unauthorized reproductions and distributions. One such solution is Windows Media Rights Manager (i.e., windows media DRM 10). However, this solution is limited to a Windows environment and is not compatible or accessible on other computing platforms. Furthermore, it provides only a single layer of security, which if defeated can expose all content distributed with the system.

Currently, each major legal download services uses its own proprietary DRM algorithm, limiting which portable playback devices consumers can use with any given system. For example, music bought on iTunes can only be played on devices with an iTunes software installed. Still, the music industry is in need to protect its constituent’s rights, while promoting the music industry by not being constrained by the hardware or software played. Further, it is important to track and control the released files that are aired online. Being able to provide a control mechanism on the released songs, and a transparent reporting capability is highly valued by reporting agencies as well as by musicians and production houses.

Due to the use of such digitized media, new tools are needed by the owners of Intellectual Property and digital content to assert their rights and to prevent unauthorized usage. Content owners are interested in a number of aspects including

- Means to indicate ownership on online contents for monetization.
- Tracking digital content consumptions.
- Controlling the dissemination of the content already released.

What is needed in the art is a platform-independent DRM system for monetizing, tracking, and controlling the usage of digital media content and providing robust multi-level security to prevent the subversion of the protection system.

2. PROBLEM STATEMENT

Given the current state of piracy in the online music industry, and the current advancement in blockchain platforms, the paper is addressing how to monetize, track and control after dissemination online streamed content. This paper proposes a Digital Rights Management solution for the stated problems using blockchain and cryptocurrency technology

3. PROPOSED SOLUTION

3.1 System Architecture

To address the tracking problem of music, the relationship between the music bands, online streaming portals and the fans needs to be addressed. The proposed solution depicted in figure 1 promotes the reward of the fans for listening to their favourite music bands if the fans opted to do so. This is needed to incentivise the fans to participate in the system. The first step for the music bands is to generate their content into a portable secure format, that is self-rendering and cross platform. For streaming portals to include that content, they will need to use a Global Music Asset Assertion (GoMAA) token to allow them to stream the content on their portals. As the Fans tune in the online streaming portals, the fans will be presented with the option to install a browser plugin which includes a digital wallet, the fans will collect GoMAA tokens as they consume the content. The fans start collecting rewards for every streaming content they consume; the online radio stations provide those rewards in GoMAA tokens. All token transactions are recorded on the iMediaStreams blockchain, which includes the streaming site, the content played, and the listeners' wallet hashed address. For online radio stations, number of songs streamed will be recorded on the blockchain. For Fans, if they opted to use their digital wallet to collect coins, the number of songs they listened to will be recorded on the blockchain, using the fans wallet hashed address. Having all the information on the blockchain addresses the royalty discrepancy problem as the information is accessed by all while preserving the privacy of the streaming stations, listeners and music bands. The following sections explain the system components in details.

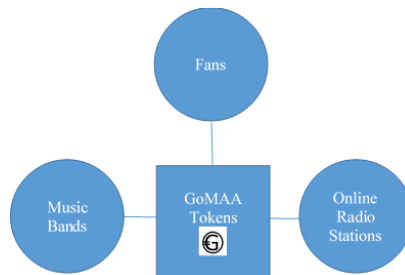


Figure 1: DRM Global Music Asset Assertion Token (GoMAA)

3.1.1 The Global Music Assets Assurance (GoMAA) Token on iMediaStreams Blockchain

The iMediaStreams Blockchain ecosystem is a safe environment for the buying, loaning, renting and selling of media streams. This environment is securely accessed through the GoMAA Tokens as the only means of exchange within the platform.

3.1.2 The Coin

The GoMAA Coin token is a cryptographic token, created to be exchanged for digital streaming content. It is the only mean of exchange on the iMediaStreams Blockchain to give all participants access to value they seek, whether they are the music producers, the online radio stations or the fans. The token is of fixed supply, fractionally divisible and non-inflationary over the long term. GoMAA Coins may be exchanged on the major cryptocurrency exchanges.

3.1.3 Protocol

The GoMAA Coin token is using an ERC20 [25] token protocol on the iMediaStreams blockchain. This token interface will enable the issuance of the GoMAA Coin token to be integrated and utilized within iMediaStreams ecosystem, which includes a Points Reward System for the media consumers. The tokens will be used by the online radio stations to buy streaming rights from Music Bands or to encourage loyal fans to explore more music or a combination of both. Every Music Band and Fan will set their value based on information provided about their value as determined by the iMediaStreams blockchain public record. A Fan may share preferences, their network of friends and followers, or even offer to share unused computing power or storage, just to name a few. All these make the Fan more attractive to both streaming radio stations and Music Bands, which will make them being valued at a higher token share. Music Brands may provide more information about their fan base, the venues, and their tours, for commanding a higher valuation for their content in terms of token required to stream their content.

iMediaStreams Blockchain creates an ecosystem where all participants are compensated through the usage of GoMAA tokens based on smart contract fulfilment, which creates a DRM environment where everyone benefits.

To be able to use the tokens on the blockchain network, Figure 2 shows the overall architecture of the DRM solution

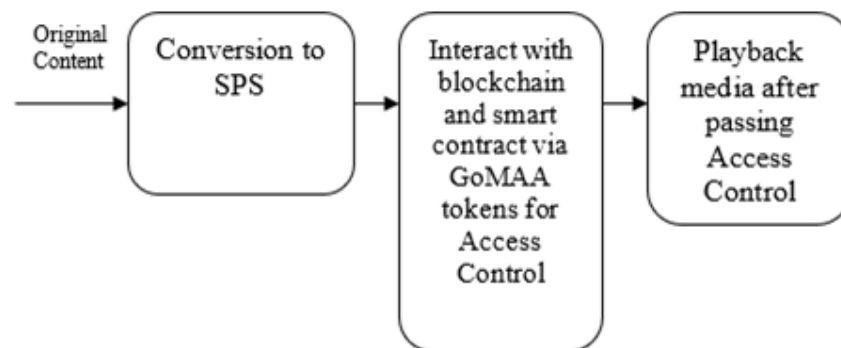


Figure 2: The overall architecture of the DRM solution

The details of the Conversion to SPS format are shown in Figure 3 and the format of the SPS is shown in Figure 4. Figure 5 shows the playback process at the receiver end whereby the content released to another party undergoes the Blockchain validation before the final rendering.

3.2 Secure Portable Streaming Format (SPS)

The first step is in converting the media file in a high level proprietary format that is both secure and portable. In addition, the content needs the options for tracking and dissemination control once released. Figure 3 shows this conversion process which converts the original content into a Secure Portable Streaming format (SPS).

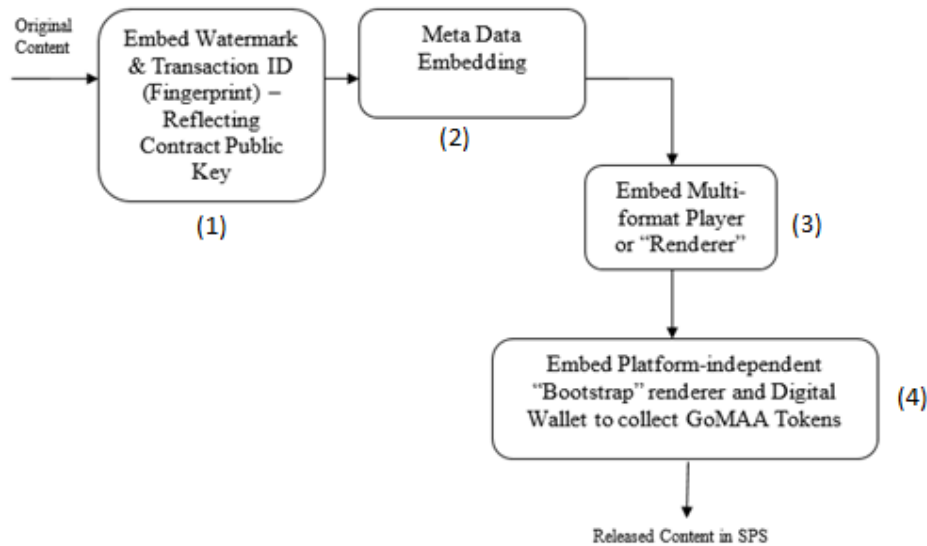


Figure 3: Conversion of original content to SPS

1. The initial content is encoded to insert a Watermark and Transaction ID (fingerprint). This is utilized when validating the transaction on the blockchain to verify privileges and rights. The fingerprint is the smart contract public key of the streaming content. Every streaming content will have its own corresponding smart contract. Prior to creating the contract address, the original content file itself is augmented with a high frequency hertz wave (> 20,000 Hz) to be outside of humans' ears capabilities, but act as a signature to the audio file, without impacting the quality of the audio. The fingerprint can be added to the audio file in intervals determined by the content owner.
2. In addition to having access control on the smart contract of the audio file, the Meta Data structure is defined based on additional usage, protection and distribution constraints as specified by the content owners. For this, the paper uses a meta-data security mechanism based on the digital content owners' requirements for protection and tracking of their content. This security mechanism is integrated into the DRM system and characterizes as a second layer in the multi-level security information flow involving permission to stream and copy, with build in instruction for access rights, including permission to stream, copy, or transfer information, "time-to-live", number of viewings allowed, even self-destruction. The security policy within the metadata on the SPS file header articulates the number of tokens needed to consume the streamed content intervals. The consumed content is published on the blockchain.

3. The renderer for the online radio streaming server is only activated based on the available tokens on the radio station wallets. Those tokens will be used to pay the content owners after the streaming is done. The renderer for the fans will be activate according to the content smart contract. If tokens are required from the fans to listen to the content, it will not be rendered to them unless they have enough tokens to pay after receiving the required stream. If no tokens are required, the plugin will enable the rendering of the files.
4. The amount and types of available tokens enables different activities. Token act as private keys that are needed. The public key represented as the streaming content id is known to everybody and the private or secret key is only known to the intended recipient who own the tokens.
 - Once a content is streamed, the smart contract clears the transactions, and the GoMAA token passes from the streaming portal to the content owners, the fans, and the iMediaStreams blockchain. If the streaming of the content cannot be validated, it is presumed to be invalid, and the GoMAA token does not transfer. The final outcome is recorded and provable. This will directly lead to the conclusion of the reconciliation debate between different tracking organizations.

3.2 Data Format of the SPS

Figure 4 shows a sample bit-stream for the SPS format. The encryption key is embedded in the machine code (which is invisible) for different players such as Win 32/64, UNIX, Mac etc. The transaction ID (or equivalently fingerprint) which contains the privilege or rights information is part of the Encrypted code.

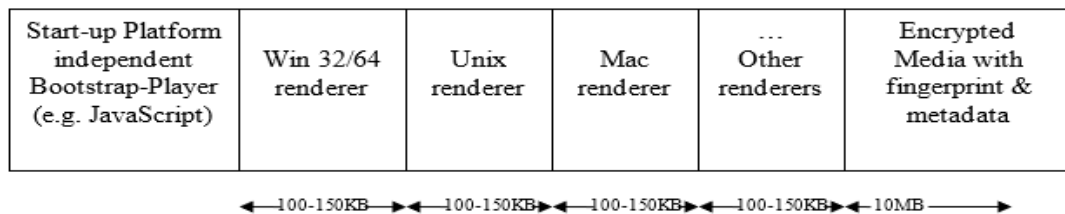


Figure 4: Sample format for SPS

The file can be self-rendered, given that a browser has a digital wallet plugin, which includes GoMAA tokens if required by the content owner and articulated in the media smart contract.

3.3 Playback/Rendering of released content or media

The renderer or player is a cross platform plugin installed on the fans' browsers. The plugin act as a digital wallet and as a media render, as depicted in figure 5 below.

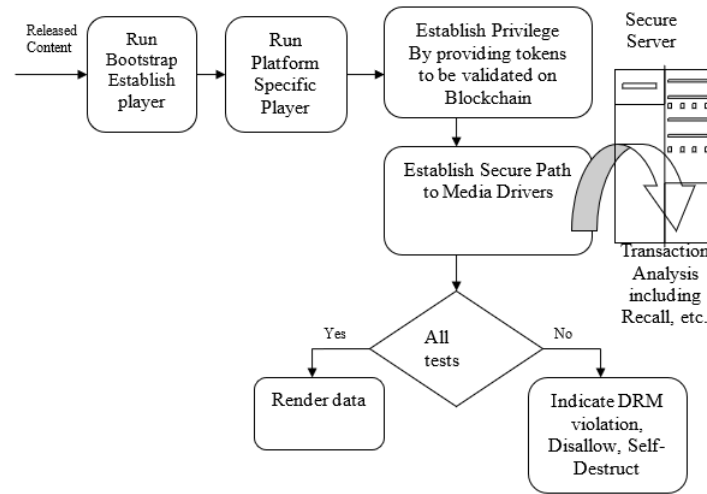


Figure 5: Playback or Rendering Process

The renderer or player aims for a self-extracting auto-executing player and digital wallet which is compatible across different browsers. This plugin prepares the content for the next step in the process, namely, the Access Control policy defined on the file header/. In order for the player to be able to control the original content after dissemination, invocation codes associated with that data are incorporated and installed on the player, where the required parameters include the predefined limitations on the data. Each time an action is taken on the content via the player (Play, FF, RW, etc.) the associated invocation code is activated and the action is counted and compared versus the original policy set at the server side. If the action is satisfied, the appropriate code is sent to the player to enable the file to play. The player consists of a *bundle* of optimized and compact platform specific players (each being machine specific binary code) along with a portable bootstrap script (for which a Java script model is used).

4. USE CASES

4.1 Buying Streaming content rights Using iMediaStreams Blockchain

iMediaStreams Blockchain provides an open ledger solution to address the discrepancy in monetising, tracking and controlling online streams. It provides music professionals with an environment where they release their music with 100% confidence that their high quality original content will be traced all the time. The transaction, once validated, is recorded to the blockchain and there is no longer any confusion or debate as to the transaction and reconciliation.

The proposed iMediaStreams Blockchain is built on an ERC-20 standard, iMediaStreams Blockchain utilizes smart contracts to enforce this transaction. iMediaStreams Blockchain, in its simplest form, is effectively a white list of legitimate online music disseminators and retailers. The smart contract quickly assesses if the song played on a domain validated by its record on the blockchain. If it doesn't appear on the blockchain and is a new domain to the environment, iMediaStreams Blockchain acts as a validation point using its data relationships to assess the played stream. Once the played stream is validated, the smart contract clears the transaction and the GoMAA Token passes from the content disseminator to the content owner. If the played stream cannot be validated, it is presumed the played stream is invalid and the GoMAA Token does not move. The final outcome is recorded and provable and any potential debate over reconciliation disappears between content owners and content disseminators. Since transactions

are validated in a short period of time, iMediaStreams Blockchain creates another change for music industry. Payment cycles can be shortened to the time it takes the smart contract to complete. If both parties desire, payment is nearly instantaneous. The option of reducing payment cycles from a few months to minutes is possible. The tracking agency collects a royalty, payable in GoMAA Tokens, on these transactions. These commissions are charged as a percentage of the transaction value.

4.2 iMediaStreams Blockchain to Compensate Listeners:

Listeners of songs are drawn to pirated content to save money. They can actually be compensated by the system if they are enjoying a higher quality song from their preferred bands. iMediaStreams Blockchain gives the content consumer ownership on how to use their tracked information, if any. The iMediaStreams Blockchain lets the listeners receive compensation. Upon consuming a digital asset, listeners receive GoMAA Tokens as a reward. These tokens can be used for many purposes within the iMediaStreams ecosystem ranging from free ad blocking to promotional offers from similar bands. Only by completing the value circle do all parties of the digital asset consumption transaction benefit. This is the value exchange missing from the online music industry today.

5. CONCLUSION

The paper presents a solution for a number of problems in the DRM space. First, it presents an overarching proposition to music monetization, tracking, and controlling. The music monetization takes place by allowing the content owners to have their content accessed using the public/private key infrastructure within the iMediaStreams blockchain. Every time the content is streamed or downloaded, GoMAA tokens are exchanged according to the rules depicted on the content smart contract.

The Tracking of the music takes place by two means, the first is by querying the iMediaStreams blockchain, where information about how many time, each content is consumed is recorded. The second mean is by checking the security server that validates the access policy on the file header. The controlling part is placed as an invocation code of the player, requiring a confirmation from the Security server to render the content or even destroy it based on the security policy as depicted on the file header. In specific, the paper presents a system for generating and controlling access to copy-protected media files. The system includes a server having a processor and a computer readable medium encoding a server software program. The server software program is configured to encode and, encrypt the media content, store the resulting data in the digital media file, embed a transaction ID, or the smart contract public address, in addition to a user-access policy stored in the digital media file header, and embed a multi-format renderer in the digital media file. The multi-format renderer is configured to render the encrypted electronic file, and is further configured to generate an invocation code in response to a requested operation on the electronic file, retrieve the transaction ID associated with the electronic file, compare the invocation code to the user-access policy, and selectively respond to the requested operation based on a result of the comparison of the invocation code to the user-access policy. Future work includes tracking subsections used in streamed online content and how to create a valuation model for the content disseminated and the Fans using their information and influential relationships within the ecosystem.

In summary, the paper presents three main advantages:

1. A DRM system focusing on the secure delivery of entertainment and information to IP devices and television set-top boxes

2. A system that accounts for files consumption in digital streaming formats and for determining usage fees such as copyright royalties.
3. Allowing content distributors the freedom to pursue new revenue opportunities made possible by digital distribution by development and licensing copy protection, electronic licensing and rights management technologies

REFERENCES

- [1] Datta, Hannes, George Knox, and Bart J. Bronnenberg. (2017) "Changing their tune: How consumers' adoption of online streaming affects music consumption and discovery." *Marketing Science*
- [2] Carlos Micames. (2018) "SPOTIFY HIT WITH \$1.6 BILLION COPYRIGHT INFRINGEMENT LAWSUIT." American University Intellectual property brief,
- [3] Lauren Iossa, Cathy Nevins, Liz Fischer. (2017)"ASCAP & BMI Announce Creation Of A New Comprehensive Musical Works Database To Increase Ownership Transparency In Performing Rights Licensing" <https://www.ascap.com/press/2017/07-26-ascap-bmi-database>
- [4] Chahbaz, Ahmed. (2018). An Introduction to Blockchain and its Applications. With a Focus on Energy Management. diplom. de. ISBN 9783960677178
- [5] Wood, Gavin. (2014) "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum Project Yellow Paper* 151 -1-32.
- [6] B.H. Turnbull, (2001) "Important Legal Developments Regarding Protection of Copyrighted Content Against Unauthorized Copying," *IEEE Communications Magazine*, pp. 92-100,
- [7] The Digital Millennium Copyright Act of 1998, US Copyright Office Summary, 1998, available at <http://www.copyright.gov/legislation/dmca.pdf>.
- [8] N. Sinha, (2000) "A Novel Watermarking Technique for digital images based on Adaptive Segmentation and Space-Frequency representation," *Proc. IEEE 2000 International Symposium on Information Theory and its Applications, ISITA 2000, Vol. II, 972-975.*
- [9] N. Sinha, (2002) "A New Digital Rights Management Platform for Digital Images," in the *Proceedings of IASTED International Conference on Communications, Internet and Information Technology (CIIT 2002)*, St. Thomas, USA, ISBN 0-88986-327-X, pp. 444-448
- [10] N. Sinha, (2005) "Secure Embedded Data Schemes for User Adaptive Multimedia Presentation", *Journal of Digital Information*, Volume 6, Issue 4, Article No. 350,
- [11] K. Bradenburg, G. Stoll, et al. (1992)"The ISO- MPEG-Audio Codec: A Generic-Standard for Coding of High Quality Digital Audio," in *92nd AES Convention, 1992, Preprint no. 3336.*
- [12] Marina Bosi et al., (1996) "ISO/IEC MPEG-2 Advanced Audio Coding," *101st Convention of the Audio Engineering Society, Preprint n. 4382.*
- [13] Mark Davis, (1993) "The AC-3 Multichannel Coder," *95th Convention of the Audio Engineering Society, Preprint n. 3774.*
- [14] J. D. Johnston, D. Sinha, S. Dorward, and S. R Quackenbush,(1996) "AT&T Perceptual Audio Coding (PAC)," in *AES Collected Papers on Digital Audio Bit-Rate Reduction*, N. Gilchrist and C. Grewin, Eds. pp. 73-82.
- [15] *IEEE Transactions on Circuits and Systems for Video Technology* (2003):Special Issue on the H.264/AVC Video Coding Standard

- [16] D. Sinha and A. Ferreira (2005) "A New Broadcast Quality Low Bit Rate Audio Coding Scheme Utilizing Novel Bandwidth Extension Tools," 119th Convention of the Audio Engineering Society. Paper 6588.
- [17] A. Ferreira and D. Sinha, (2005) "A New Low-Delay Codec for Two-way High-Quality Audio-Communication," 119th Convention of the Audio Engineering Society, Paper 6572.
- [18] D. Sinha, A. Ferreira, and, D. Sen (2005) "A Fractal Self-Similarity Model for the Spectral Representation of Audio Signals," 118th Convention of the Audio Engineering Society, Paper 6467.
- [19] A. Ferreira and D. Sinha, (2005) "Accurate Spectral Replacement," 118th Convention of the Audio Engineering Society, Paper 6383.
- [20] Ahmed Gomaa, D. Sinha (2009), Cross-platform digital rights management providing multi-level security information flow tracking, US Patent App. 12/209,893, 200
- [21] Sahita, R., & Covington, M. J. (2014). U.S. Patent No. 8,689,349. Washington, DC: U.S. Patent and Trademark Office.
- [22] Soppera, A., & Burbridge, T. (2013). U.S. Patent No. 8,533,782. Washington, DC: U.S. Patent and Trademark Office.
- [23] Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A., & Akutsu, A. (2015). The blockchain-based digital content distribution system. In Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on (pp. 187-190). IEEE.
- [24] Maesa, D. D. F., Mori, P., & Ricci, L. (2017). Blockchain based access control. In IFIP International Conference on Distributed Applications and Interoperable Systems (pp. 206-220). Springer, Cham.
- [25] Fabian Vogelsteller. 2015. ERC20. (2015). <https://github.com/ethereum/eips/issues/20>.