A Scalable Blockchain Based Digital Rights Management System

Ashutosh Dhar Dwivedi

Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada

Keywords: Blockchain, Digital rights management (DRM), Scalability, Watermark

Abstract. The internet has the main advantage of transparent and sharing, but on the other hand, it has a disadvantage that digital contents are not protected. Due to the online environment, it is not easy to achieve a well protected Digital Rights Management System. Any digital content that is freely allowed to spread online have zero value. The content provider only gets a one-time profit when they upload their work to a platform and transfer the right of the production to the platform. Now the platform is assumed to hold the right. But due to the online availability of content, anyone can download it and can make various copies. After this, the value of the digital content becomes zero, because the value can only be determined by the difficulty of access to the content. There is no way to track the leakage or copyright to the spread of digital material. Anyone is allowed to use it for their purpose. In this paper, we propose a distributed media transaction framework for digital rights management(DRM) scheme based on digital watermarking and scalable blockchain network model. The first generation of blockchain technology is suffering from high latency, low throughput, high transaction cost, high energy and high computational power consumption as well as centralization due to mining pools. In this paper, we mainly focus on removing or improving all these issues from the original blockchain system to make it suitable for our digital rights management model. Our model allows only authorized user to use online contents and provide original multimedia contents. The DRM also take care of digital contents and keep track records of required content modification, copyright transfer or other transaction trails related to multimedia data. We use digital watermarking to reclaim the uniqueness and copyright ownership of the off-line content once it is leaked.

1 Introduction

With the development of internet and online environment, it is not easy to protect the copyright of digital contents. Once a digital work is uploaded to the internet, it could be easily distributed to everywhere by making the duplicate copy. Digital contents that are widely spread have zero value because of its free availability to everyone. Excessive spreading and free consumption of digital contents always hurt the owners' or content providers' benefits and causes business loss. In areas such as photography, design and e-commerce, snaking of piracy has brought incalculable losses to the creators. The victim spends plenty of time and money for legal actions to prove his ownership against pirated, tempered or edited contents. The basic challenges in Digital Copyright Management Systems are:

- Digital contents are freely available somewhere over the internet without any restriction to download.
- Users are unable to authenticate the content available on the internet since the content sources are often unknown,
- Content providers have no way to track copyright violations.

Nowadays, multimedia content are also used for making social media influence over public issues. The well-known adage that "seeing is believing" is no longer valid due to many powerful multimedia editing tools. With the development of this internet generation, we see millions of edited and tempered images, videos, audios and news on social media to change the perception of people regarding particular issues. Transmitting and misusing these edited and tempered digital multimedia bring a great challenge to original owners or creators. Such development in multimedia editing tools has decreased the credibility of audios, videos, images or any other type of multimedia content and therefore authentication of such multimedia content is required. Current DRM technologies such as Silverlight, Flash Air, Windows and Apple digital right managements focused on only copyright management and content encryption. Therefore, in case of leakage content, they are unable to trace one who should be responsible for the violation. Also, current DRMs are unable to easily prove copyright violation over any edited or tempered digital content. Digital content consumption is now prevalent, and people often like to watch movies and listen to songs through the mobile app or web browser. These apps or web browser allow users to access contents once the user makes an online profile and pay some charges. The payment can be divided into different shares, platform, owner etc. For such payments, the DRM platforms use and trust over third party payment methods, e.g. Banks, credit card, debit card etc.

Upon the above problems, we need a new DRM framework that is reliable, efficient, tamper-resistant and secure. Also, the new DRM framework should securely store multimedia information and other payment histories in the form of transactions. In many cases, the owner of the multimedia content sell items to some other company or individual and the information regarding copyright may need to change. Therefore we also need a multimedia distribution model that preserve content modification histories of multimedia contents and other information regarding media distribution. For security and privacy of digital contents, it is always beneficial to preserve these transaction trails. The best model could be based on a distributed P2P network environment and support a distributed ledger environment (DLT). To store transaction histories and for content privacy and security issues, blockchain technology[19] could be a perfect solution. The critical feature of blockchain is relying on a global peer to peer (P2P) network instead of a central trusted authority. Blockchain can be applied for many models such as trademarks copyrights protection, supply chain management and other applications where we require distributed transaction history etc. The most popular and practical use of blockchain is bitcoin and Ethereum. However, the primary issue for blockchains is *scalability*. We mainly focus on solving this scalability issue and trying to model a secure DRM system using blockchain technology.

2 Related Work

Currently, few platforms created a digital rights management system using blockchain technologies. The one music website based on Ethereum is Ujo music[9]. Ujo keeps a track record of the digital content owner and creates an identity of each uploaded music. The payments of music are distributed using Ethereum smart contracts. However, the music contents are not protected against duplication.

Another music platform is Resonate[8]. It is blockchain-based music streaming platform to publish music. Artist can upload and publish their musics and can also manage royalties independently. Members pay credit of 5 Euro or more for full access. With zero balance, listeners can only access samples of the songs.

In the paper[18], authors presented a new design scheme of a copyright management system based on blockchain and digital watermarking. In this model, blockchain is used to store watermark information securely. In the model, authors use Inter Planetary File System (IPFS) to store and distribute watermarked images without a centralized server.

In the paper[11], authors proposed a tamper-proof media transaction framework. Original media is often edited for creative content preparation or tampered with to fabricate false propaganda over social media. The proposed blockchain model is based on watermarking that can easily retrieve either the transaction trails or the modification histories of tempered images.

Numerous research is going on nowadays to improve scalability issues in the blockchain. The new cryptocurrency application now days are Ripple[7], Monero[5], Algorand[1]. These are some Proof-of-Work(PoW) and Proof-of-Stake(PoS) based applications.

3 DRM requirements and our solutions

In traditional DRM models, DRM only considers security against the unauthorized use of contents and consumption of content without payment. In many cases they encrypted contents, but in such situation, it is very hard to verify and audit these contents if it includes illegal and bloodcurdling materials. Also, in traditional models, once the content is downloaded and tempered, there is no such easy way to prove ownership to the content. Here, we discuss some issues in traditional DRM's and propose a solution based on our model.

3.1 Authentication of contents

Several times it is required to get this information from the tempered image to identify ownership of the copyright. Digital watermarking support content authentication and can fetch hidden information from the distorted multimedia data and also check the authenticity based on watermark attached in the multimedia. Therefore we use digital watermarking with multimedia data to identify ownership of the copyright or to identify other information from the tampered data. However, the attacker always can remove watermarking based on various type of attacks over the image. Therefore we require a secured watermarking scheme with enhanced technique to protect watermark information with the multimedia data.

3.2 Data protection and usage control

The multimedia data should be protected and cannot be downloaded by anyone over the internet. We store the multimedia data over the cloud and give access to it to only a specific user who uses our copyright-based multimedia application. These audios, videos cannot be played by other media players. Our multimedia tool fetches the watermarking information from the multimedia and if matches with the original watermark information, then it only allow playing. Also, the user registers himself and buy the license for usages, such as a listening song or reading books. This license decides the basic rights such as usage times, domain etc.

3.3 Scalable blockchain suitable for DRM

There should be a secured ledger or database in any digital right management system to create the identity and track record of each multimedia data. Mostly when a platform allows us to download any digital content, the income can be distributed by the owner, platform and other shareholders depends on the percentage of shares. Many times it is also required that DRM change the copyright information of any digital items when one owner sells the multimedia data to other company or individuals. Blockchain could be the best solution to keep records of these transactions. However, the primary issue for blockchains is *scalability*. Due to problems as mentioned earlier, we propose a scalable blockchain-based digital rights management (DRM) model. This DRM allows users to verify authorizations and keep track

records of content modification, copyright transfer or other payment transaction histories related to the multimedia contents. In this paper, we mainly focus on creating a scalable blockchain DRM for a multimedia system.

3.4 Data storage

Blockchain size is only suitable for transaction storage but not for the storage of images, audios or videos. A typical multimedia file could be of the size MB to few GB, while a bitcoin block size is generally 1 or 2 MB. Therefore we store these multimedia files over the clouds. We want to create a secure model for payment transactions, copyright information and copyright modification histories of the digital contents. Therefore we only focus on preserving these transaction trails using decentralized blockchain while multimedia contents still rely on third-party service like a cloud.

3.5 User privacy and data verification of media data

The DRM should also have all identifying information of users' who upload data over the cloud. The content provider always makes an account and provide users' identity to the DRM. These identities must be verifiable by DRM. The DRM also securely store the content providers' identity information over the blockchain. Furthermore, data that is uploaded over the cloud should be verified. Many times people upload restricted contents over the clouds, and therefore it should be verified appropriately once uploaded. Using Machine learning or AI, this could be easily done. AI algorithms can spot patterns and take action by themselves without human intervention. These algorithms automatically delete videos before they got any views. Once the content provider uploads any politically sensitive or illegal content, the DRM easily identifies and block the content provider to upload content again and also close his account.

3.6 Privacy in transactions using Zero Knowledge

Privacy is always an essential component of any transaction-based model. Consider a credit card applicant in a bank want to prove that they have maintained an average minimum balance in their bank account in the last six month. The traditional way to prove this, applicant share the six-month statement. This conventional way will of-course reveal a lot of personal information about the applicant, which is not needed for the company. However, somehow applicant can prove the balance requirement without sharing private details using some technique. In cryptography, such technique called Zero-knowledge proofs (ZKPs). In Zero-knowledge proofs technique where a *prover* provides a verifiable proof to a *verifier* that certain property holds true without revealing any additional information. The use of Zero-Knowledge could make really a game-changer in blockchain technology.

4 The proposed DRM Model

The major problem with PoW based blockchain is a scalability issue while other drawbacks are Increasing complexity and energy wastage. With the increase over time, the complexity of mining increases. On the one hand, this property can be seen as a strength of PoW based blockchain because it protects the network against new hardware. But on the other hand, as complexity increases, there are only a few nodes with high computational power that can mine new blocks. This can lead to the problem of pushing the network into the centralization of mining power. Therefore, contrary to the idea of decentralization. Also, as the difficulty level to mine, a new block increases it requires more hashing power and thus

can be seen as more energy used. The problem of energy consumption in bitcoin mining and its solution using a game-theoretic approach is discussed in the paper[20]. In our proposed model, we mainly focus on creating blockchain-based DRM and trying to solve scalability with respect to throughput and other above-mentioned issues of blockchain and also try to solve copyright issues of digital contents using secured digital watermarking schemes.

4.1 Scalable blockchain for DRM

The blockchain and cryptocurrency initiated by Satoshi in 2008[19]. The key feature of this technology is decentralized peer-to-peer (P2P) network instead of central authority. Due to decentralized and distributed property of blockchain, it is believed that such a system have potential in many areas beyond finance, including healthcare, insurance, government etc. However, the major problem of blockchain is scalability. The major scalability issues in blockchain can be explained as below:

Throughput scalability The blockchain system throughput is measured in terms of the number of transactions per second (TPS). Currently, the average throughput of Bitcoin is 3.00 TPS (transactions per second) and for Ethereum throughput is 9 TPS (transactions per second) approximately. To understand this scalability issue lets take an example of Visa's centralized system processes and compare it with bitcoin. The maximum capacity of Visa's centralized system is $56,000$ TPS while the average throughput is 2000 TPS for a country like the US, and daily peak time this could be $4,000$ TPS. The throughput provided by Bitcoin or Ethereum is not enough for our model.

The system throughput[2] depends on two parameters: the block size (B), *i.e* the number of transactions in a block and the inter-block time interval t_B, *i.e.*, time to mine a new block. If a block contains 2000 transactions and the average time is 600 second then, throughput will be 3.33 TPS. Therefore to increase throughput either we increase block size B, or we decrease t_B. However, these parameters cannot be changed arbitrarily that we discuss below.

Block size (B) To increase the size of blocks is not practically feasible due to the restricted capacity of the P2P propagation. A modern processor can support thousands of transaction per second while disk input-output can support hundreds of thousands of transactions per second. A miner once mines a new block; it propagates the block for verification to all nodes in a P2P network. P2P network consists of many nodes, and propagation speed might be slow due to the slowest computer in the network. Therefore increasing the size of the block will also increase the time required for a block to propagate[13]. Now, let's see below what happens when the block propagation time increases due to the large block size.

Increasing block propagation time (t_B) Increase in block propagation time might cause *fork*. A fork occurs a miner mines a new block on the previous block, rather than on the top of the recent block. This happens because miner has not yet received the most recent block (see Figure 1). Therefore the time required by a new block to propagate throughout the network defines the opportunity window in which forks may occur.

The longer the propagation time, the higher the probability for the fork to occur. Consider if the block propagation time is 600 second ($t_{B=600}$) and consider the time required for a block to reach full network is $t_{network}$, then the probability of the fork to occur is[17]:

$$P(\text{fork}|t_B = 600) = 1 - \epsilon^{\frac{-t_{network}}{600}}$$

From the above equation, the probability for the fork to occur $P(fork) = 1.95\%$ for propagation time $t_{network} = 11.6$ seconds. If the $t_{network} = 126$ second, the $P(\text{fork}) = 17.58\%$, which is unacceptable for real world usability.

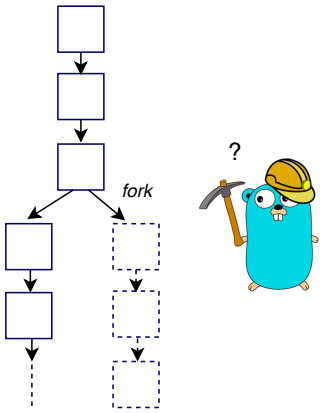

Fig. 1. Blockchain Fork.

Shorting the block propagation time (t_B) Decreasing Block Propagation Time (t_B) might stop many nodes from participating in the network. A P2P network consists of many nodes that also include slow processing of peer computers (see Figure 2). Network speed depends on these slow peers. All the nodes in the network must be capable of receiving and processing blocks faster than they are produced.

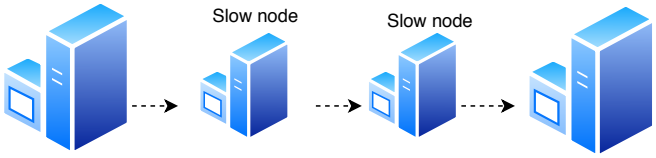

Fig. 2. Peer to Peer Network.

Nodes in the network cannot verify the blocks if they have a slower speed and therefore excluded from the network. To allow maximum nodes to remain to participate in the network, the propagation time of the network must be shorter than block propagation time (t_B).

$$t_{network} < t_B$$

Therefore, we need to maintain the ratio between block propagation time (t_B) and network propagation time $t_{network}$. To increase the throughput of blockchain, we can reduce the inter-block time interval (t_B), but in such case, our requirement is to decrease the $t_{network}$. In our proposed model, we try to decrease ($t_{network}$) for the whole network.

4.2 Blockchain based overlay network

Our primary goal is to scale the system with thousands of on-chain transactions per second. As we discussed in the above section that long propagation time would not allow high throughput blockchain network. We need a network that allow fast block propagation to scale the throughput. In the past, we have seen many examples, Ripple[7], Bitshares[4] etc. where network places its trust over a small centralized system and scale throughput very

well. In our model, we use an overlay network that decreases network overhead and delay. These overlay network grouped in the form of clusters and each cluster has one cluster head (CH) that work like a server. However, this model defeats the essential property of blockchain: decentralization. But if we look at other blockchain technologies, they are also somehow struggling to achieve all three properties in a single system that is decentralization, scalability and privacy.

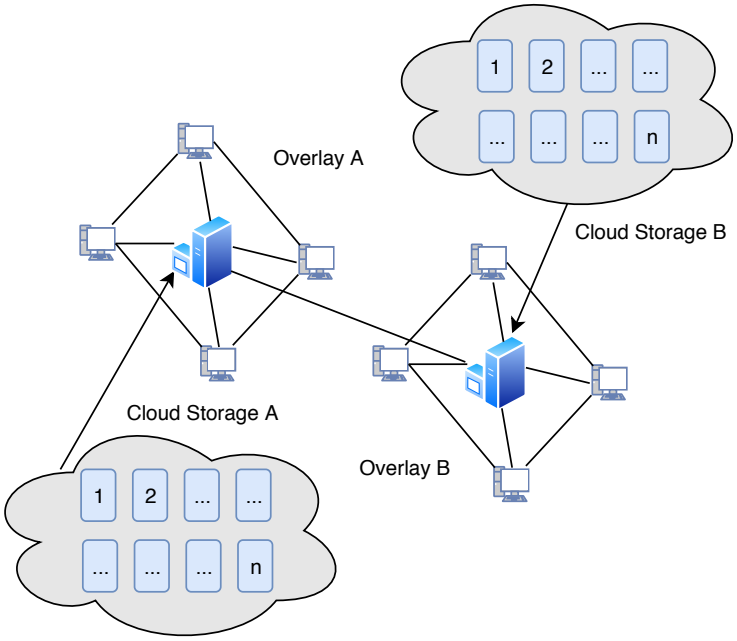

Fig. 3. Overlay Network.

These cluster heads (CH) works like a server (with fast processing speed) that is connected with many peers and other cluster networks in the blockchain system. Cluster heads receive the nodes from the different peer in encrypted form. Also, peers don't need to send encrypted blocks directly to the server, but they send the block to other peers in the same cluster. Due to these properties of the overlay, CH cannot cheat any particular peer. CH blindly serves the peers without the knowledge of the source and information about encrypted block contents. Due to fast propagation speed, these CH forward blocks quickly to other clusters in the network for the verification without any network delay. To audit the behaviour of any CH, the peers in the network can send test blocks to CH and validates if their peers quickly receive them.

To store the digital multimedia contents, we are using cloud storage that stores data in identical blocks associated with unique block-number. The block numbers are stored in the blockchain to identify the location of the data. Each cluster might have different or single cloud storage.

By solving the networking bottleneck issue, any cryptocurrency community can adjust its protocol to our overlay network. In our DRM model, we can use cryptocurrency like bitcoin for the payment of any digital content access. To assure cluster head performance transactions include a voluntary payment to CH that can be treated as platform payment.

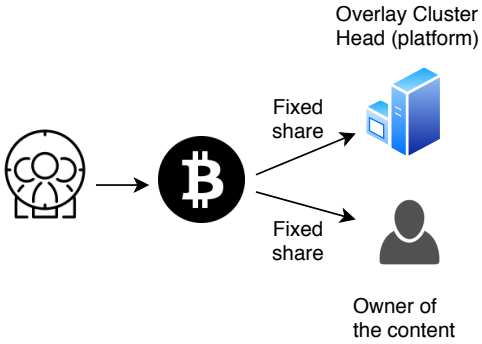

Fig. 4. Payment model

The paid amount by the content user is divided into fixed shares, e.g. some part of the income goes to the platform like cluster head in our case, and some part will go to the owner of the digital content. The user pays the amount in the form of cryptocurrency and does not use any bank payment method. The miner nodes collect these transactions from the network and try to mine a new block. The general format of a transaction might contain information like timestamp, current owner, transaction details, etc., depends on the requirement. In many cases, the owner of digital content might be changed; in such a situation, this information is also treated as a transaction and saved in the ledger.

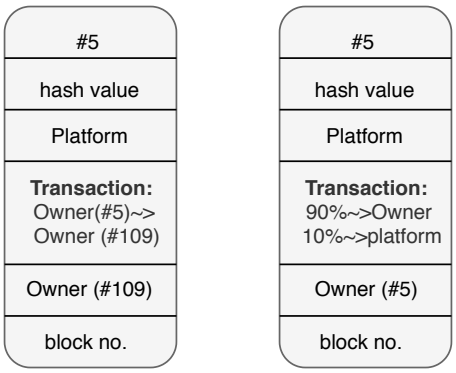

Fig. 5. General format of transactions

These transactions are collected by miners to mine the block. Once a miner mine a new block, it encrypts the block. The encryption is required to hide information from CH. To prevent CH from stopping any block based on the original node, wallets and timestamp; blocks are only propagated after being encrypted.

4.3 Digital watermarking scheme for DRM

The best tools available to achieve digital authentication now days could be the watermarking or digital signature. However, a digital signature can only be used for complete authentication of images or documents while digital watermarking can be used for content

verification of videos, audios, images or document file. Adding a digital signature to the original content does not allow a single bit of change in the image or file at the receiver end. A unique hash value is generated from the original file and during the verification process, the receiver's computer only authenticates the image or document if it is not modified during transmission. A single bit modification in the original image changes the whole hash value of the original file, and this is the reason digital signature either accept or reject. Therefore digital signature is a good way only to detect forgery or tampering. Now the question arises about the tempered images, audio or videos. How to prove copyright with images, videos and audios that are modified for a purpose. In many applications, it is required to compress multimedia data, and these compressed data are accepted as authentic data, e.g. depends upon internet speed, people like to change the quality of data when watching movies, songs or listening audios. Similarly, for the image, apart from tempering images to fabricate false propaganda over social media, images are edited for creative content also. Sometimes, images are compressed using standards such as MPEG, JPEG or PNG etc. We consider these creative editing or lossy compression's as essential in our model.

Digital watermarking[12] is a technique to embed copyright information with original content in the form of digital multimedia information such as an image. In the case of copyright disputes, the embedded watermark digital information can be extracted from the original content and verify the ownership of copyright. A watermark can be visible or invisible depends on requirement. Digital watermarking has two stages: watermarking embedding and watermark extraction. Watermarking schemes are divided into three types: robust, fragile, and semi-fragile. A robust watermarking is used to detect copyright information in case of malignant transformations in the original files, while for slight modifications in original contents, fragile or semi-fragile can be used. In our model, we prefer invisible watermarking where embedding level will be too small to notice and robust watermarking scheme to secure digital contents from the designated class of transformations.

Watermark encryption In order to enhance security and robustness of watermark into original digital content, we first encrypt watermark image before embedding. Such encryption is useful in case if any attacker is able to extract the watermark, the original watermark image cannot be obtained. We use a lightweight encryption algorithm to encrypt this image. Many lightweight encryption algorithms are presented in several competitions for encryption algorithms[6, 3]. However, we use SPECK[10] lightweight encryption algorithm to secure our image from attack. SPECK was designed by researchers from the National Security Agency (NSA) of the United States of America (USA) in June 2013. The cipher uses three simple ARX operations, namely, modular addition, bitwise rotation, and exclusive-OR and therefore very well suited to perform on IoT devices. The round function of SPECK is shown in Figure 6. In the figure, r_1 and r_2 are rotation constants while K_r is round key. The full description of cipher can be found from the original paper[10].

However, we only use four-round encryption to secure our digital watermark image. The algorithm is secured against various attacks[14, 15]for full number of rounds. We are using this algorithm just to add the second layer of encryption when the watermark is already embedded in the original content, therefore do not require very heavy encryption algorithm to change the shape of watermark image.

Watermark embedding algorithm Two main types of hidden watermark algorithms are "transform domain watermarks" and "spatial domain watermarks". In spatial domain watermarking scheme, watermark information is hidden by directly modifying the original signal. The process of hiding and extraction is easy, but robustness is not as good as transform-domain watermarks. Few watermarking schemes under transform domain watermarks are discrete cosine transfer (DCT) and discrete wavelet transfer (DWT). Due to the good com-

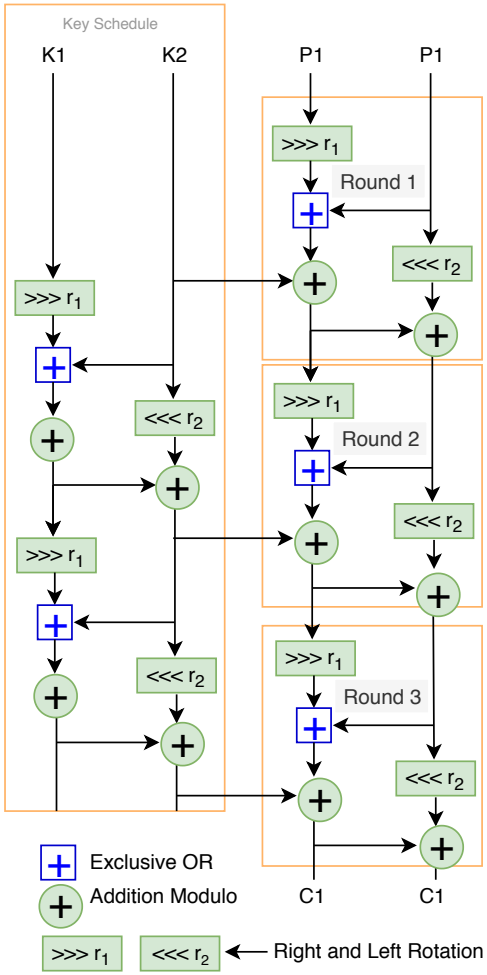

Fig. 6. The round function of SPECK.

patibility of the DCT algorithm with the commonly used international compression schemes, we use this scheme in our model[16].

In order to evaluate the robustness and transparency, Peak Signal-to-Noise Ratio (PSNR) is used for evaluating the image quality that is defined as:

$$\mathrm{PSNR} = 10\log_{10}\frac{(2^d-1)^2WH}{\sum_{i=1}^{W}\sum_{j=1}^{H}(p[i,j]-p'[i,j])^2} \tag{1}$$

where W the image width, d is the bit depth of pixel, H the image height, and $p[i,j]$, $p'[i,j]$ is the ith-row jth-column pixel in the original and watermarked image respectively.

5 Security Evaluation

In any model the security evaluation can be addressed by three factors: Confidentiality, Integrity, and Availability. Confidentiality ensures that only authorized users are able to access the system. Integrity ensures that there is no change in original message when transferring

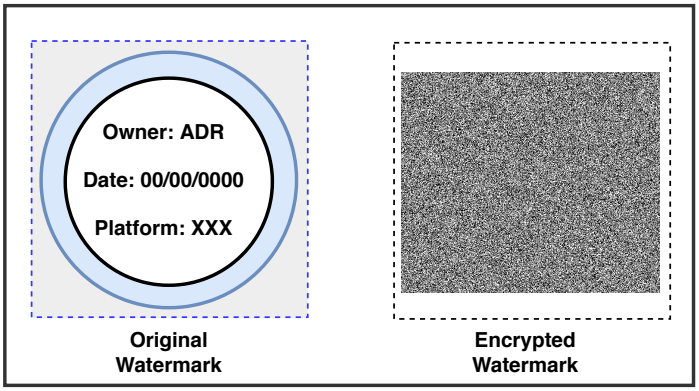

Fig. 7. Watermark image encryption.

data from sender to receiver. Availability ensures that data is always available to the user when required. We evaluated security in our DRM model. In our case adversary can be any cluster head, any node in the network or a part of cloud storage. These adversaries can create false transactions, delete or change informations, discard transactions or modify watermark. We also considered few attacks that could be possible in our model and find the security margin against them. Our cluster heads can propagate all blocks to its Gateways fairly without any discrimination due to auditing performed by other P2P nodes.

5.1 Encrypted Blocks

In our model, we encrypt all transaction blocks to prevent any discrimination based on contents like timestamp, transactions and other attributes. Please note that we are encrypting transaction but not multimedia data over the clouds. Once it is propagated through the gateway or cluster head, we reveal the encryption key.

5.2 Indirect Relay

In order to ensure not preventing individual nodes from propagation, nodes do not propagate blocks directly to the cluster head, but it propagates firstly to its peer neighbour and then peer neighbour transfer it to CH through other peers.

5.3 Test block

To check if CH is working properly or not, any node can send a test block directly to CH and monitor if CH is working properly or not. By using this technique, they can continuously monitor the cluster heads in the network to stop any biased decision by CH based on individual block contents.

5.4 Denial of Service (DoS) Attack

In such type of attack, the attacker tries to prevent an authentic user from accessing the network. Generally, the attacker launches many fraud transaction blocks to increase traffic in the network. However, in our model, we do not allow random users to join the network without proof of authenticity, and once a node is detected for doing a malicious activity, it is directly blocked by peer networks.

5.5 Storage Attack

This is also possible that an adversary can make a cloud storage attack and try to remove data, or modify data from the storage. However, in such case, we are using robust watermarking schemes, and others already made security algorithms to protect multimedia data. To secure multimedia data from unauthorized access, we can use many other cloud security protocols. Also, our primary focus is to secure DRM transactions that are saved in encrypted blocks in the distributed network and therefore, they are entirely secured.

5.6 Dropping Attack

In such attacks, the attacker can control the cluster head, and cluster heads are not able to do anything in the network. Generally, in such case cluster heads drop all received blocks and stop communicating with any other node. In such case, peer networks can elect other nodes as a cluster head.

6 Conclusion

In this paper, we presented a novel blockchain-based Digital Rights Management System to secure digital contents. We boost the scalability of blockchain by using an overlay cluster head. By solving the networking bottleneck issue, any cryptocurrency community can adjust its protocol to our overlay network. To secure the contents with copyright issues, we embedded a digital watermark in the original digital contents. We add information such as copyright owner, location, date of creation in the watermark image. To enhance the security of watermark images, we used lightweight encryption to encrypt the watermark image.

References

1. Algorand, year=2019,. "http://www.algorand.com"
2. Bitcion charts and graphs. "https://www.blockchain.com/charts"
3. Competition for authenticated encryption: Security, applicability, and robustness, year=2015,. "https://competitions.cr.yp.to/caesar.html"
4. Eos, year=2019,. "https://eos.io/"
5. Monero, year=2019,. "http://www.getmonero.org"
6. Nist competition, year=2019,. "https://csrc.nist.gov/Projects/Lightweight-Cryptography"
7. Ripple, year=2019,. "http://www.ripple.com"
8. resonate music. "http://www.resonate.is" (2019)
9. ujo music. "http://www.ujomusic.com" (2019)
10. Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., Wingers, L.: The simon and speck lightweight block ciphers. In: Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. pp. 1–6. IEEE (2015)
11. Bhowmik, D., Feng, T.: The multimedia blockchain: A distributed and tamper-proof media transaction framework. In: 22nd International Conference on Digital Signal Processing, DSP 2017, London, United Kingdom, August 23-25, 2017. pp. 1–5. IEEE (2017), https://doi.org/10.1109/ICDSP.2017.8096051
12. Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J., Kalker, T.: Chapter 5 - watermarking with side information. In: Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J., Kalker, T. (eds.) Digital Watermarking and Steganography (Second Edition), pp. 137 – 182. The Morgan Kaufmann Series in Multimedia Information and Systems, Morgan Kaufmann, Burlington, second edition edn. (2008), http://www.sciencedirect.com/science/article/pii/B9780123725851500085
13. Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: 13th IEEE International Conference on Peer-to-Peer Computing, IEEEP2P 2013, Trento, Italy, September 9-11, 2013, Proceedings. pp. 1–10. IEEE (2013), https://doi.org/10.1109/P2P.2013.6688704

14. Dwivedi, A.D., Morawiecki, P., Srivastava, G.: Differential cryptanalysis of round-reduced SPECK suitable for internet of things devices. IEEE Access 7, 16476–16486 (2019), https://doi.org/10.1109/ACCESS.2019.2894337
15. Dwivedi, A.D., Morawiecki, P., Wójtowicz, S.: Finding differential paths in arx ciphers through nested monte-carlo search. International Journal of electronics and telecommunications 64(2), 147–150 (2018)
16. Ma, Z., Huang, W., Gao, H.: A new blockchain-based trusted DRM scheme for built-in content protection. EURASIP J. Image and Video Processing 2018, 91 (2018), https://doi.org/10.1186/s13640-018-0327-1
17. Marshall, A.W., Olkin, I.: A multivariate exponential distribution. Journal of the American Statistical Association 62(317), 30–44 (1967), http://www.jstor.org/stable/2282907
18. Meng, Z., Morizumi, T., Miyata, S., Kinoshita, H.: Design scheme of copyright management system based on digital watermarking and blockchain. In: Reisman, S., Ahamed, S.I., Demartini, C., Conte, T.M., Liu, L., Claycomb, W.R., Nakamura, M., Tovar, E., Cimato, S., Lung, C., Takakura, H., Yang, J., Akiyama, T., Zhang, Z., Hasan, K. (eds.) 2018 IEEE 42nd Annual Computer Software and Applications Conference, COMPSAC 2018, Tokyo, Japan, 23-27 July 2018, Volume 2. pp. 359–364. IEEE Computer Society (2018), https://doi.org/10.1109/COMPSAC.2018.10258
19. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
20. Singh, R., Dwivedi, A.D., Srivastava, G.: Bitcoin mining: A game theoretic analysis. IACR Cryptology ePrint Archive 2018, 780 (2018), https://eprint.iacr.org/2018/780