Peer-to-Peer Networking and Applications
https://doi.org/10.1007/s12083-020-01023-z

A digital rights management system based on a scalable blockchain

Abba Garba[1,2] · Ashutosh Dhar Dwivedi[3] · Mohsin Kamal[4,7] · Gautam Srivastava[5,6] · Muhammad Tariq[4,7] · M. Anwar Hasan[8] · Zhong Chen[1,2]

Received: 16 June 2020 / Accepted: 28 October 2020

Abstract

Even though the Internet promotes data sharing and transparency, however it does not protect digital content. In today's digital world, it has become a difficult task to release a DRM (Digital Rights Management) system that can be considered well-protected. Digital content that becomes easily available in open-source environments will in time be worthless to the creator. There may only be a one-time payment to creators upon initial upload to a given platform after which time the rights of the intellectual property are shifted to the platform itself. However, due to the online availability of content, anyone can download content and make copies. The value of digital content slowly decreases, because the value of content can usually be determined through the difficulty of it's accessibility. There is no way to track the leakage or copyright for the spread of digital material. In this paper, a distributed media transaction framework for DRM is proposed, which is based on the digital watermarking and a scalable blockchain model. In this paper, our focus is on improving the classic blockchain systems to make it suitable for a DRM model. The DRM model in this paper allows only authorized users to use online content and provide original multimedia content. While the digital watermarking is used to reclaim the copyright ownership of offline contents in the event when the contents are leaked.

Keywords Blockchain · Digital rights management · Scalability · Watermark · Unexpanded shares · Networks

1 Introduction

Protecting the copyright of digital contents has always been very challenging. Once a digital content is uploaded to the Internet, it can be easily distributed everywhere through copies of digital files. A digital content that is widely spread may have zero value due to open access. Excessive spreading and free consumption of digital content almost always are detrimental for the owners' or content providers' benefit and causes monetary loss [27]. In areas such as photography, design, and e-commerce, the rampant spread of piracy has brought incalculable losses to the owners. The creator of a content spends plenty of time and money on legal actions to prove his/her ownership of the content. The primary challenges in Digital Rights Management (DRM) systems are as follows:

– Digital content is freely available on 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.
– The content providers have no way to track and get incentives for detecting misbehaviour or copyright violations.

In recent years, the multimedia content are used in social media to make public opinions. The well-known adage that "seeing is believing" is no longer valid due to many powerful multimedia editing tools. With the recent developments, millions of edited and tampered images, videos, audio files, and news are seen on social media that may change the perception of people regarding particular issues [24]. Transmitting and misusing the edited digital multimedia becomes a massive challenge to the original owners and creators. Such development in multimedia

This article is part of the Topical Collection: *Special Issue on Blockchain for Peer-to-Peer Computing*
Guest Editors: Keping Yu, Chunming Rong, Yang Cao, and Wenjuan Li

✉ Gautam Srivastava
srivastavag@brandonu.ca

✉ Zhong Chen
zhongchen@pku.edu.cn

Extended author information available on the last page of the article.

Published online: 12 November 2020

editing tools has decreased the credibility of audios, videos, and images as well as any other type of multimedia content. Therefore, authentication of such multimedia content is pertinent and required. Current DRM technologies such as Silverlight, Flash Air, Windows and Apple digital right managements focus on the only copyright management and content encryption. Therefore, in the case of content leakage, these services are unable to trace who should be responsible for violations. Moreover, current DRMs are unable to prove any sort of copyright violation over digital content [17]. Digital content consumption is now prevalent, and users often like to watch movies and listen to music using a mobile application or a software. These methods allow users to access content once the user makes an online profile and pays some sort of fee. The payment can be divided into different shares, platforms, and owners, etc. For such payments, DRM platforms use and trust third party payment methods such as banks, credit cards, and debit cards. From the aforementioned problems, there is a need for a new DRM framework that is reliable, efficient, tamper-resistant, and secure. This is due to the fact that multimedia content can be sold to other companies or individuals and the information regarding copyright may need to be transferred to other entities. Moreover, the proposed framework should provide a penalty for copyright violation in order to improve the security and integrity of the system. Therefore, the proposed system must allow entities to detect malicious behavior or an adversary who violates the copyright of the content. A multimedia distribution model is a necessity that preserves content modification history of multimedia content and other information regarding media distribution. For security and privacy of digital content, it is always beneficial to preserve these transaction trails in case of future investigation [8, 11, 21, 32].

An ideal DRM model should be based on a distributed peer-to-peer (P2P) network environment and be able to support a distributed ledger environment (DLT). To store transaction history and for content privacy and security issues, blockchain technology [28] could be considered as an ideal solution. The critical feature of blockchain technology is that it relies on a global P2P network instead of a central trusted authority. The blockchain can be applied for trademarks, copyright protection, supply chain management [33], healthcare [36] and other applications where distributed transaction history is required. The most popular and practical use of blockchain technology is Bitcoin [28] and Ethereum [29]. However, the primary issue with the blockchain technology is *scalability*. In this paper, the scalability issue is addressed, and a secure DRM system using blockchain technology is presented.

The rest of the paper is organized as follows. In Section 2, we present a brief related literature section. This is followed by an in-depth overview of our proposed system in Section 3. Next in Section 4, DRM challenges and solutions are presented. Our work focuses on combining our proposed system with a scalable blockchain is presented in Section 5. We give a thorough security analysis of the proposed system in Section 6. The paper is concluded with some future directions and concluding remarks in Section 7.

1.1 Our contribution

A novel blockchain-based DRM system is proposed to secure the digital content. The major issue with current blockchain system is scalability and therefore it is improved using an overlay network along with pBFT consensus algorithm. To solve the copyright issue, a digital watermark is embedded in the original digital contents. For the purpose of enhance security lightweight encryption is used to encrypt the watermark image.

2 Related work

Several DRM platforms now days are using blockchain technology. The most popular website is Ujo music [7] that uses Ethereum as blockchain consensus. The track record of digital uploaded music and digital content owner is kept by the Ujo blockchain, and with the help of smart contracts, payment is distributed. However, the biggest issue with this platform is, music content can be duplicated and there is no protection against copying the music.

Another popular DRM music website is resonate [5]. The music streaming of this platform is also based on blockchain. Any music can be uploaded and published by artists and royalties can also be managed independently. User needs to pay approximately 5 Euro to get the membership. However, samples of the music can be accessed with zero balance.

A copyright management system was presented in [26], Meng et al., where the authors presented a framework based on digital watermarking and blockchain. In this framework, watermark information was securely stored in the blockchain. However, to save the watermarked image, the system uses inter planetary file system (IPFS) instead of a centralized server.

A tamper-proof media transaction platform was presented by Bhowmik et al. [10]. Original digital contents are often tampered and spread on social media to fabricate false propaganda or some time media is edited for creative purpose. In the proposed framework, authors proposed watermarking and blockchain-based model to identify the modification histories of digital contents.

Guo et al. [19], proposed a Blockchain-enabled digital rights management system for multimedia resources contents. The system employed a whole new network architecture for distribution and managing the multimedia resources of an online education. The system was built based on the combination of public and private blockchains and also comprises three specific smart contracts approaches for the realisation of the recording of the multimedia digital right, secure records as well as verification of unmediated digital certificates accordingly.

McConaghy and Holtzman [25], employ the Bitcoin blockchain to record digital content ownership (i.e., images). Legal registry stores the terms of service and a timestamp with the help of bitcoin. The registry is stored on the blockchain with ownership information. Authors applied the concept of machine learning to identify images that have been tampered online without owner's permission.

Kishigami et al. [22] proposed a decentralized blockchain-based digital content distribution system that allows content owner to have absolute control of its digital content. Other Blockchain based digital right management proposals that supports identity and privacy protection include the followings [15, 24, 27, 37].

3 Proposed system

We divide our research problem into two parts:

- building a scalable blockchain model using an overlay network, and
- solving DRM using scalable blockchain.

In this section, we tackle the details of the scalable blockchain model while in Section 4 we propose the DRM system.

3.1 Building a scalable blockchain for DRM

The key feature of the Blockchain technology is decentralized P2P networking. Transactions in blockchain-based systems can be in the form of blocks, which are determined by miners that assist in generating blocks [35]. The key essential characteristics of blockchain are *decentralization, scalability and security*. Blockchain technology can only achieve two of them out of the three [20]. Therefore, one characteristic has to be compromised in order to achieve the other two. The first generation of blockchain technology currently in use, suffers from high latency, low throughput, high transaction cost, high energy usage, and high computational power consumption [31, 34]. In this paper, the focus is on the scalability and security and partially on the development of the decentralized mechanism by using an overlay network.

3.1.1 Addressing Blockchain scalability using overlay network

Our primary goal is to scale the throughput of the network so that system supports enough number of transactions per second. There is a necessity in our model for a network that supports fast propagation of blocks to improve throughput. In recent years, several technologies emerged, such as Bitshares [3], Ripple [6], and many others. However, in all of them, the network scales the throughput by placing its trust over the small centralised system. In the proposed framework, an overlay network (see Fig. 1) is used. This framework decreases the overhead and delay from the network. An overlay network has many cluster groups, and each cluster has one cluster head (CH) that works as a server. However, this model defeats the basic property of blockchain, i.e., decentralization. To ease this concern, we can look at other blockchain technologies who are also struggling to achieve decentralization, scalability, and privacy in a single system. Cluster heads (CH) are similar to powerful servers that are used for the fast propagation of blocks in the network. These cluster heads are connected to peers and other cluster heads in the network. Different peers in the network send encrypted blocks to cluster head for the fast propagation in the network. However, peers may not send these blocks directly to cluster head, but they can forward the blocks via neighbour nodes in the same cluster network. Due to this property, cluster head can not cheat or discriminate any block based on its source or origin. Cluster heads transfer these blocks to other networks without any information about the content of block or source of the block. Once the block has propagated, the encryption key can be revealed to the network. These cluster heads quickly propagate the blocks to other cluster networks, and therefore network can verify these blocks without any delay. The behaviour of cluster head can be audited with the help of test blocks send by peers and can be verified if these cluster heads are quickly forwarding the block to the final destination. Note that we use CH above all the networks to propagate blocks rapidly from one cluster to another cluster. CH is not working like a central distributed server for peer groups.

Cloud storage is used to store multimedia contents where identical blocks are assigned to store data, and each block has a unique block number. To identify the location of data, blockchain stores the block numbers of individual block. A single cloud storage could be assigned to each cluster. Any cryptocurrency protocol can adjust its technology with the overlay network and can solve the network bottleneck

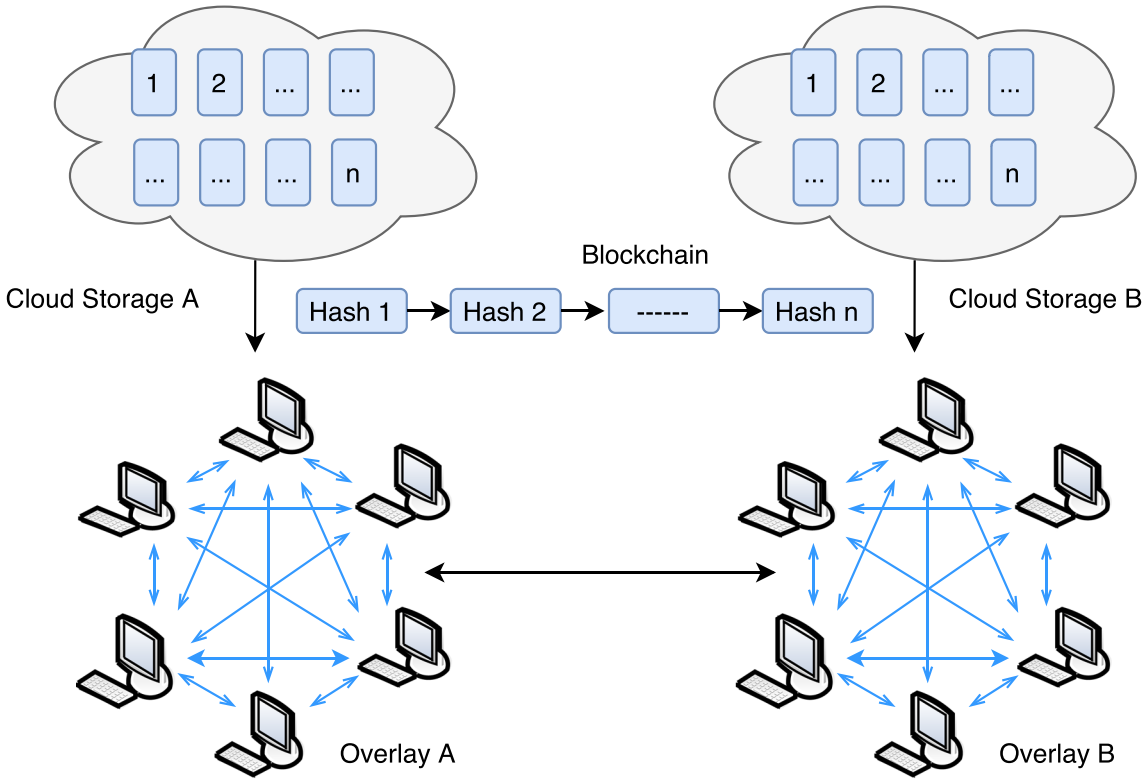

Fig. 1 Overlay Network

issue. In the proposed model, Ethereum like cryptocurrency is used for digital payments.

3.2 Consensus mechanism used in our model

A consensus algorithm is the critical component of the proposed blockchain design that is executed by network participants. Many consensus algorithms are available, and each has its own pros and cons. Some of the well-known consensus algorithms are Proof of Stake (PoS), Proof of Work (PoW), and Proof of Authority (PoA). However, most of the consensus algorithms are not scalable concerning throughput, and these algorithms have low throughput that is not suitable to meet our requirements. The best consensus algorithm in terms of high throughput is Practical Byzantine Fault Tolerance (PBFT). However, the issue with this consensus is low network scalability. pBFT is only suitable for a limited number of nodes and performance become worst when nodes increased in large amount. In the previous section, it was discussed that network scalability is increased by using distributed blockchain servers and therefore, pBFT can be easily applied to our model even for the large network. In this paper, a private blockchain with pBFT consensus protocol is used where only permitted nodes can participate in the consensus process.

3.3 Smart contracts

Smart contracts are stored programs in the blockchain that automatically execute when pre-determined conditions are met. The benefits of smart contacts are apparent in collaborations, in which they can be used to enforce some type of agreement. Smart contracts work on the very basic concept of "if/when, then.." statements that are written in the form of code inside blockchain consensus. In our model, smart contracts are used to perform voting in blockchain consensus, changing ownership of digital content, distributing reward, and the penalty for misbehaving. However, since reserved blockchains are used, these smart contracts can be re-written by authorities responsible for the private blockchain in case of any bug or changing the terms and condition based on agreements.

3.4 Scalability analysis of the overlay network

Consider the consensus algorithm with lowest throughput (PoW based Bitcoin network) and a network that consists of 9000 nodes ($N = 9000$), the majority of which are connected to 8 to 12 of their peers with a latency 110 milliseconds [1]. At the 50^{th} percentile, nodes upload rate is 56 Mbps ($bw_{50^{th}} = 56Mbps$. Let B is the size of the block,

the time required to transmit single 1 MB block to single peer (t_{hop}) is:

$$t_{hop} = \frac{B}{bw_{50^{th}}} = \frac{1MB}{56Mbs} = 0.143 \quad (1)$$

Nodes propagate blocks to their peers in sequential transfer. For 8 peers, the Bitcoin node requires $8t_{hop}$ to propagate a block to its peers. Sequential propagation is used when bandwidth is limited. In sequential propagation, nodes peer propagate the received block after t_{hop} has passed. A complete network consists of nodes with slow as well as fast bandwidth. The propagation speed depends on slow nodes, as was explained earlier. If a cluster of peers is made and the CH is used overseeing the entire network, just to propagate the blocks, then the blocks can be transferred in parallel. Instead of time $8t_{hop}$, we can propagate 8 blocks in t_{hop} time. Note that, we only use CH above all the network (see Fig. 2) just to decrease the propagation time of blocks, and we are not converting the whole network in the form of distributed centralize servers.

4 DRM challenges and solution

In traditional DRM models, DRM only considers security against unauthorized use of the content and consumption of the content without payment. In many cases, the content is encrypted, and it is very hard to verify and audit the content if it includes illegal material. Moreover, in traditional models, once the content is downloaded and potentially tampered with, there is no easy way to prove ownership of the content. Here, some issues in traditional DRM's are discussed, and a solution based on our model is proposed.

4.1 Authentication of content

It is often required to get the copyright ownership information from the tampered image for authentication purpose. Content authentication is supported by digital watermarking, and hidden information can be fetched from tampered digital contents. Once the watermark attached with the image is fetched, authentication information can be easily accessed. Therefore to identify copyright ownership or other important information from the distorted multimedia data, digital watermarking is used. However, sometimes it is also possible that watermarking is removed by attacker based on several image attacks. In such case therefore, a secured watermarking scheme should be chosen that provide enough security to protect watermark information on digital contents.

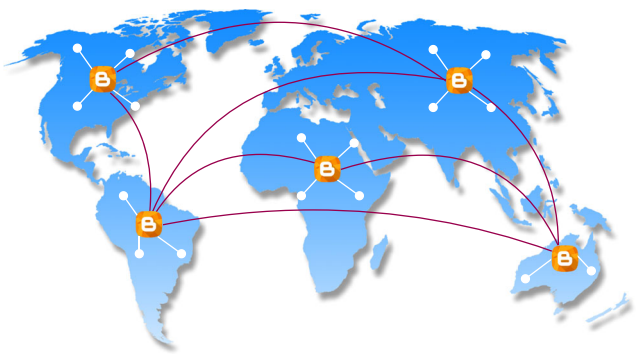

Fig. 2 Network Scalability using Cluster Heads

4.2 Data protection and usage control

Multimedia data should be protected and should not be available for download by anyone over the Internet. The multimedia data is stored over the cloud and access given only to specific users who are connected with the proposed blockchain system. Moreover, user registers themselves and buy a license for usages, such as reading books or listening to a song. This license decides the basic rights such as usage times and domain, etc. Once the user pays for the content, he/she gets the session key through the contracts in the proposed system and by using that key, the user can access the digital content at any time.

4.3 Scalable blockchain and smart contracts suitable for DRM

There should be a secured ledger or database in any DRM system to create the identity and track records of each multimedia data item. When a platform allows users to download any digital content, the income can be distributed to the owner, platform and other shareholders depending on the distribution predetermined for any given content. It is also required that the DRM may change the copyright information of any digital items when one owner sells the multimedia data to another company or individual. Due to issues mentioned earlier regarding blockchain technology, a scalable blockchain-based DRM model is proposed. This blockchain-based DRM allows users to verify authorization and keeps track of records of copyright transfer, content modification or other payment transaction history related to any multimedia content on the system. In our system, a permissioned blockchain is used and therefore, a consensus is achieved through voting between members for copyright transfer and other decisions. Note that smart contracts are run automatically using saved instructions and can not be run by individual users.

4.4 Avoid misbehaviour using scalable blockchain DRM

Traditional DRMs have no provisions for identifying and encouraging entities to detect misbehavior of copyright violation. Blockchain technology has created the new phenomenon of digital currency, which facilitates the movement of the value of the global system of payments, in a more trusted manner without the involvement of intermediaries [17]. Consequently, the payment conducted through blockchain can be a solution to the problem of compensation of content owners and incentivizes entities who detect copyright violation and give rewards using smart contracts. Smart contracts have been proposed to support the applications beyond the digital currency [39]. Smart contracts allow the execution of automatic and instantaneous payments to designated entities, including terms and stipulated time. Payment and incentivization are designed to be more inclusive providing standard terms for the digital content owner and entities.

4.5 Data storage

The size of the entire blockchain for our DRM system is only suitable for transaction storage and not for the storage of entire multimedia files. A typical multimedia file could be of the size of an MB to a few GB, while a Bitcoin block size is generally 4 MB. For instance, a Bitcoin records only data about transactions trails currently about 160 GB storage in size. The blockchain for Bitcoin comprises predominantly with metadata about transactions instead of actual heavy files. Therefore, storing digital media content poses dramatic challenges, specially when considering a large number of network participants with large amounts of potential digital content. Therefore, these multimedia files are stored using cloud storage and we only store different type of transactions in the blockchain.

4.6 User privacy and data verification of media data

The DRM should also have all identifying information of users' who upload data over cloud storage. The blockchain consensus only allows authorized users to participate in the network. These users must be verifiable by the DRM. The DRM also securely stores the content providers' identity information over the blockchain. Furthermore, data that is uploaded over the cloud storage should be verified. Many times people upload restricted contents over cloud storage, and therefore it should be verified appropriately once uploaded.

5 The proposed DRM Model using scalable blockchain network

The proposed framework consists of four parts:

1. Digital watermark encryption and authentication
2. Transaction and payment
3. Blockchain-based clustered overlay network
4. Cloud storage for storing massive multimedia data.

Figure 6 describes the general framework of the scalable blockchain DRM.

5.1 Digital watermark encryption and authentication

5.1.1 Watermark encryption

In the proposed model, invisible watermarking is used where the embedding level will be too small to notice and a robust watermarking scheme is used to secure the digital content from a designated class of transformations. An authentication procedure is provided where a content owner initiates a transaction after receiving a request from the user. In order to enhance security and robustness of watermarks into original digital content, the watermark image is encrypted before embedding. Such encryption is useful in the scenario where an attacker is able to extract the watermark, the original watermark image cannot be obtained [16]. A lightweight encryption algorithm is used to encrypt this image. Many lightweight encryption algorithms are presented in several related work for encryption algorithms [2, 4] but some of them have already been broken through cryptoanalysis. However, SPECK is used from [9] which is a lightweight encryption algorithm to secure the image from an attack. SPECK was designed by researchers from the National Security Agency (NSA) in June 2013. The cipher uses three simple ARX operations, namely, bitwise rotation, modular addition, and exclusive-OR and therefore, it is very well suited to perform on devices with low capacity. The algorithm is secured against various attacks [12–14] for the full number of rounds. This algorithm is used to add the second layer of encryption when the watermark is already embedded in the original content, therefore it does not require a very heavy encryption algorithm to change the shape of the watermark image. Figure 3 shows encryption time of several lightweight algorithms.

5.1.2 Watermark authentication

The best tools available to achieve digital authentication are watermarking or digital signatures [30]. For authentication

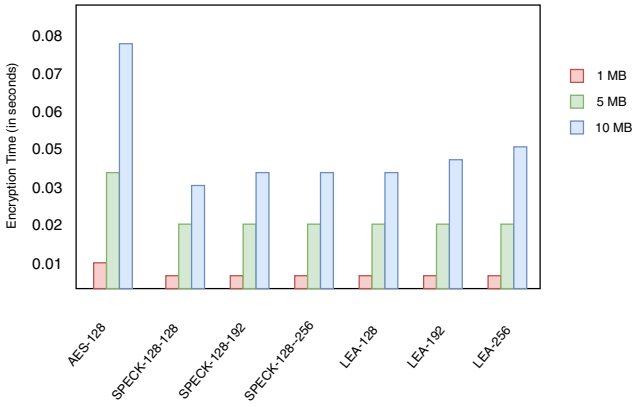

Fig. 3 Encryption time in second

of only documents or images, a digital signature can be used but on the other hand digital watermarking can be used for the verifications of documents and images as well as audio, video and files [38]. A single bit of change in the original file is not allowed in case of a digital signature. During the verification, a unique hash of the original document is generated by using a hash function and receiver of this document only accept it if the hash of the document is same on both sides of the transmission. The whole hash value will be completely different if a single bit has tampered during transmission. Therefore, in the case of a digital signature, the receiver either accept or reject the document. Therefore, digital signatures are a good way only to detect tampering or forgery of original content. One question does arise about images, audio or video that has been tampered with. It is important to prove copyright with audio, videos and image files that are modified for a purpose. In some cases, compression of multimedia data is required, and such data can also be accepted as authentic data. Some reasons for compression include Internet speed, where changing the quality of data may improve view-ability/audibility. Similarly, for images, images are edited for creative content as well as tampering with images to fabricate false propaganda over social media. Sometimes, images are compressed using standard forms such as JPEG, PNG or MPEG etc. These creative editing or lossy compression techniques are essential and should be considered.

5.1.3 Watermark embedding algorithm

Two main types of hidden watermark algorithms are "transform domain watermarks" and "spatial domain watermarks". Watermark information is hidden in the spatial domain watermarking scheme by directly modifying the original signal. However, compared to transform-domain watermarks, robustness is not as good in spatial domain watermarks. On the other hand extraction and hiding is easy in spatial domain watermarks. Few watermarking schemes under transform domain watermarks are discrete wavelet transfer (DWT) and discrete cosine transfer (DCT). Due to the formidable compatibility of the DCT algorithm with the commonly used international compression schemes, this scheme is used in the proposed model [23]. DCT represents an image as the sum of sinusoids of different magnitude and frequency. For a typical image, the DCT has the property that most of the visually significant information about the image is concentrated in a few coefficients of the DCT. Equations 2, 3, 4 and 5 represent the scenario of what DCT does to the image and also how the image is reconstructed back by applying inverse DCT. Mathematical representation of DCT represented as χ in Eq. 2 of a two dimensional matrix (MxN) β is given below:

$$\chi_{pq} = \xi_p \xi_q \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \beta_{ij} \cos \frac{\pi(2i+1)p}{2M} \cos \frac{\pi(2j+1)q}{2N}, \tag{2}$$

where

$$\xi_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \tag{3}$$

$$\xi_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \tag{4}$$

The inverse DTC is represented in 5

$$\beta_{ij} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \chi_{pq} \xi_p \xi_q \cos \frac{\pi(2i+1)p}{2M} \cos \frac{\pi(2j+1)q}{2N}, \tag{5}$$

In this work, an algorithm for the scalable DRM is created. Algorithm 1 demonstrates the generating watermark content in which DCT represents discrete cosine transform. I_level is the value for the visibility factor of watermarking. Larger the value of I_level, more visible the watermarking. W_Image represents watermarked image.

Algorithm 1 Generation of watermarked image.

Input: Image, Watermark
Output: Watermarked image, Difference of original to watermarked image
Load Image, watermark
for *i=1* $\rightarrow$ *number of pixels* **do**
x[i]=RGB_channel[i](Image);
DCT_image[i] = DCT(x[i]);
W_Image = [Watermark on DCT_image[i]] + I_level;
end
difference_value = Image - W_Image;
Save difference_value and W_Image to memory;

Algorithm 2 describes about generating the content hash in which the RGB image is converted to grey scale by averaging the three colors i.e., $\frac{R+G+B}{3}$. It sometimes produces poor results due to the variable weights of R, G and B in an image. The weighted RGB approach is used in which R,G and B channels are separated from the image. This gives us the weight of each channel. Then the equation becomes;

$$Grey\ Image = \frac{(W_R \times R) + (W_G \times G) + (W_B \times B)}{3} \quad (6)$$

where W represents the weight of R, G or B in an image. Algorithm 3 describes the content authentication of the scalable DRM.

Algorithm 2 Generation of distributed ledger.

```
Input: Watermarked Image
Output: HASH
  Grey_Image = RGB2Grey(W_Image);
  DecVal = 0;
      for i=1 → number of pixels do
    Bin_Grey[i] = dec2bin(Gery_Image[i]);
        a[i] = XOR(Bin_Grey[i], key);
        b[i] = Bin2Dec(a[i]);
        DecVal = DecVal + b[i];
  HASH = SHA3(DecVal, HASH_previous);
      Update ledger;
```

Algorithm 3 DRM authentication. IDCT represents Inverse Discrete Cosine Transform.

```
Input: Image
Output: Check Authorization of Image
y = Original_Image
x = User_Image
  for i=1 to number_of_ pixels do
    a[i] = DCT(x[i]);
    b[i] = a[i] - I_level;
    c[i] = IDCT(b[i]);
    difference[i] = y[i] - c(i);
        if difference[i]==0 then
      No rights violated;
        else
      Rights violated
    z[i] = Dec2bin(x[i]);
    j[i] = XOR(z[i], key);
    k[i] = Bin2Dec(a[i]); DecVal = DecVal + k[i];
        End;
  HASH_Image = SHA3(DecVal, HASH_previous);
      if HASH_Image == HASH values in the ledger then
    No rights violated; else
      Rights violated
        End;
```

Content owners save the encrypted watermarked image on the cloud. If a given user requests digital content, the owner will generate a hash and key from the content. This key will be used to access content from the cloud storage and also to verify whether the content is being tampered with or not. Notwithstanding that the key is kept with the owner and the original content will be stored in cloud storage, the hash will be distributed in the blockchain. Furthermore, when there is a new request from another user, the content owner uses the same procedure but generates a new key. Moreover, in this regard, the hash must be different for each user. If the content owner uses the same key definitely the hash will be the same, in this regard the key differentiates the hash. Table 1 describes the key and hash generation process. A key size equal to 10-bits was chosen for experimentation. However, for real-world applications, the size should be increased for stronger security.

5.2 Transaction and payments

In the proposed DRM model, any cryptocurrencies such as Bitcoin or Ethereum can be used for payment of any digital content access. To ensure CH obeys transactions policies a voluntary payment to CH is made that can be treated as a platform payment.

Content user pay the amount and this amount is split into *fixed shares*, e.g. some shares are given to content owner while other is given to the platform (see Fig. 4). The user do not use any bank payment but pays the amount in cryptocurrency (e.g. ethereum in this case), although recently banks are beginning to process some cryptocurrencies as well. To add a new block miner collects transactions from the network (see Fig. 5). A transaction may contain several informations like current owner, transaction details, timestamp etc. If the digital content owner is changed, in such case this information is treated as a new transaction.

Miner collect these transactions from the network and add a new block. Miner encrypt the block, once the block is added. To hide information from cluster head, this encryption is required. To prevent cluster head from any biased decision based on timestamp and wallets and to prevent cluster head from stopping any block based on

Table 1 Summary of key generation and hashes

Key	Hash
K1	BBDE59444F625CFD624A4D8A94B577ED1AFC21FB
K2	9559BBFCC7C76B263EED795ECB42E18925E7F586
K3	34FE7DFB82B86F3F2B5C4FAC9F61C027A0A4001B
K4	3779A33050E02AE5CD8645A17E08F12AC06CEEEC
K5	F19CFFAEDB4175C1D7467DE6A6BF2543F74A388A
K6	8209A63EC8D843FBE4CB9E29DE587007531C3044
K7	9DA0821B89564CCE3BA3DD4F91C84062D5AEF808

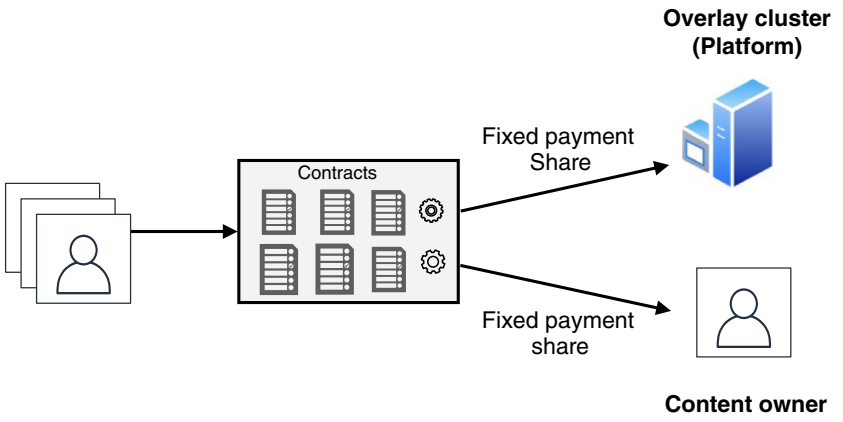

Fig. 4 Payment model

these informations; blocks are only propagated after being encrypted. The key is revealed to the network once the block is propagated.

5.3 Blockchain based overlay network

Our network consists of CHs, nodes, cloud storages, smart contracts, reserved blockchain and users. Digital content owners watermark their original image and store it in the cloud servers in the encrypted form. Once a given user needs to access content, he/she sends payment through smart contracts that are divided into two parts, one for the content owner and other for the network overlay to maintain these server services. After getting payment, a content owner sends the hash and session keys of the stored digital content to the user. By using the key, the user can download or stream the digital content from the cloud storage. In the case of a digital image, the user can verify if the hash value matches. If the hash is mismatched, the content is modified over the cloud, and the user can report such issues to smart contracts. The transactions created by these processes are sent to the network and miners store them in blocks and add a new block. Once a miner add a new block, they encrypt it and propagate to the network for verification. A block encryption key is only revealed after the block had been propagated. Once other nodes verify the block, it is stored in the blockchain. Figure 6 describes the general framework of the scalable blockchain.

5.4 Cloud storage management

Before the content is released for business usage, since digital multimedia content is very cumbersome, off-chain storage can be used to store large data. In our system, cloud storage is used that stores the data in identical blocks associated with a unique block number. To identify the location of the data, the block numbers are stored in the blockchain. Each cluster might have different or single cloud storage. The content owner uploads the digital content in cloud storage, the hash of the content or metadata will be part of the transaction and stored in the blockchain P2P network. Furthermore, the most vital aspect of the scalable DRM is to store sensitive and tamper-resistant transactions of data in the blockchain. Once the data is stored in the cloud

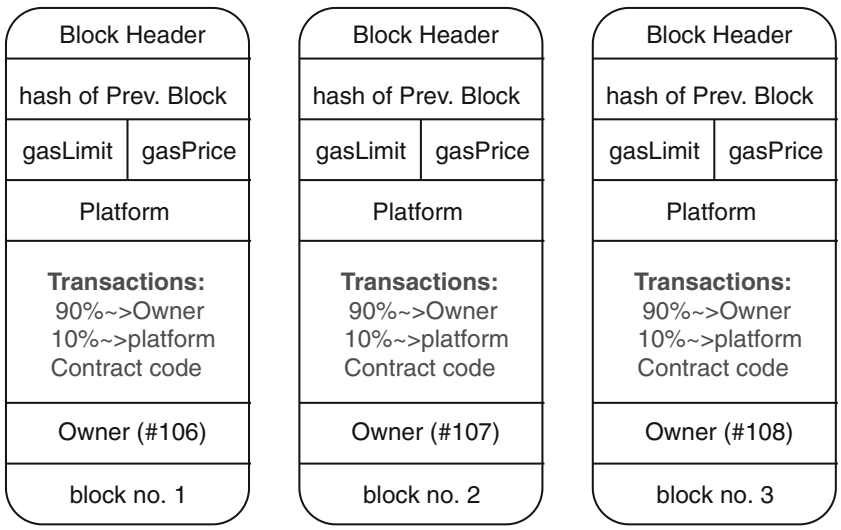

Fig. 5 Scalable DRM: General format of transactions

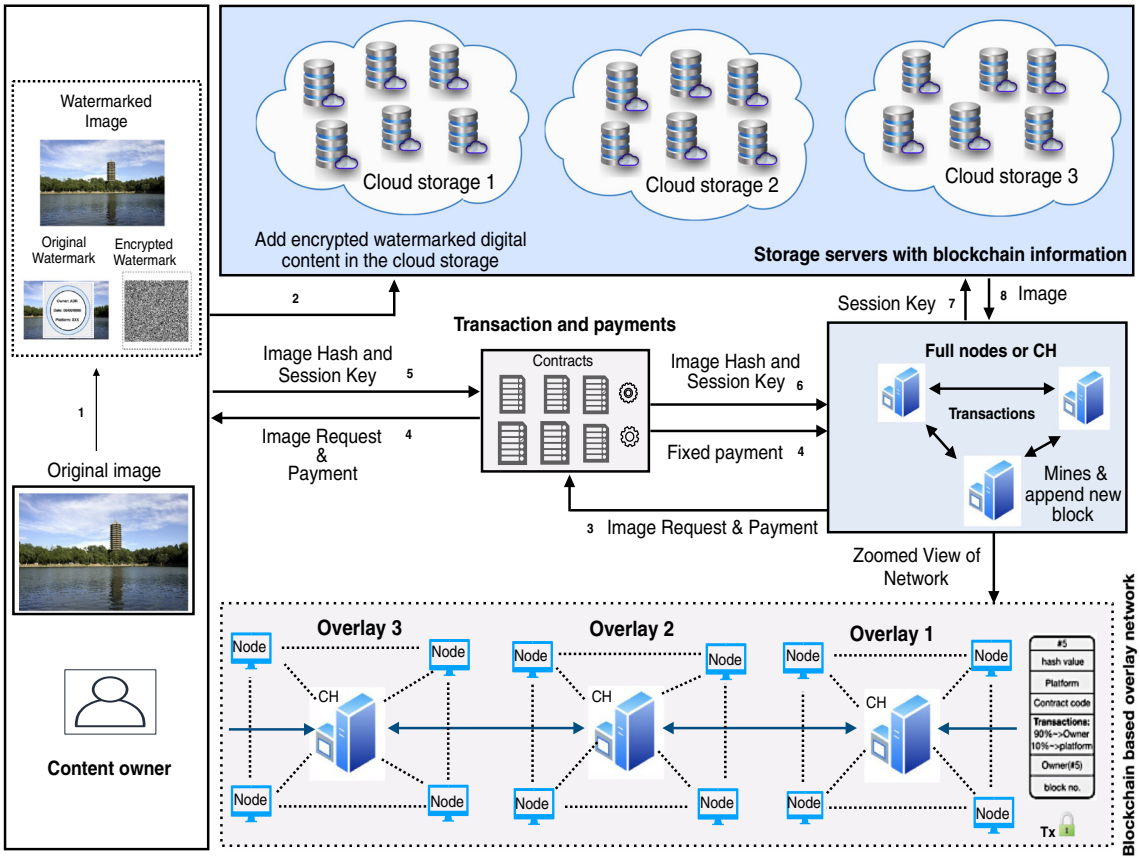

Fig. 6 General framework for scalable blockchain DRM

and its hash stored in the blockchain through transactions, it will be stored permanently and cannot be tampered with. This can provide a high level of data availability and security.

6 Security analysis

6.1 System used for the security analysis watermarking

Based on the proposed framework, the scalable blockchain for DRM is developed and implemented. The scalable DRM is built based on the overlay network and the P2P external data storage for storing massive multimedia data. In order to test the performance of the proposed system, Ali Cloud server is used. The watermark algorithms were run on MATLAB (Fig. 7).

6.2 Experimental analysis

The pixel and their corresponding decimal values are plotted for the original watermarked image as well as for the forged image. The content owner before providing it to any user applies SHA-3 algorithm on the image and generates the hash value of the watermarked image. The content owner or user determines the image digital rights violation by comparing the image provided to any user by comparing

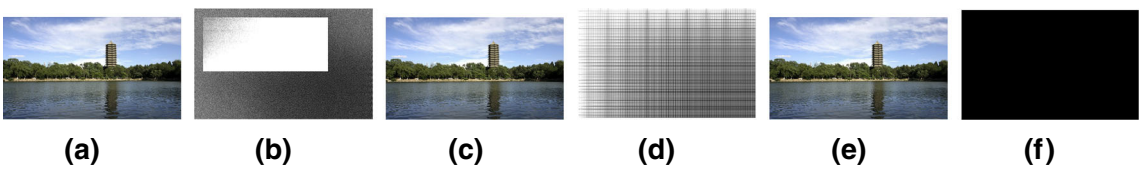

Fig. 7 General process of watermarked content authentication: **a** Original image **b** Generated watermarked channel **c** Watermarked embedded image **d** Difference between original and watermarked image **e** Retrieved original image from watermarked image **f** Difference of original image and image retrieved from the watermarked image showing all the zeros hence, no rights violated

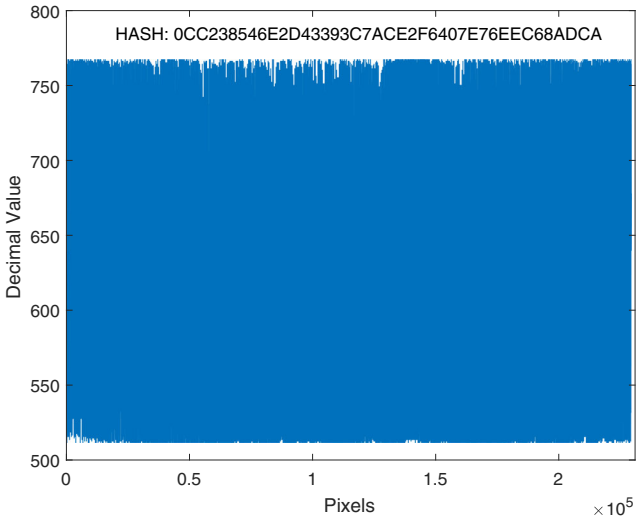

Fig. 8 Generation of decimal value for originally watermarked image

it with the originally watermarked image. The hash of an image that has been tampered with is generated and checked against all the hash values present in the ledger. Figures 8 and 9 represent the difference between decimal value of each pixel of the original and the altered images. These two figures show unsynchronized pattern and also the hash values generated for both images are different. The difference of these images are presented in Fig. 10, which does not produce all the zeros. The graphical analysis in detail is performed and presented in Fig. 11. The decimal values should be the same for any pixel values of both originally watermarked image and the image present with the user. If a single pixel value is changed, a different hash value is generated. Consequently, it can be seen that the decimal values of pixels do not overlap and are not

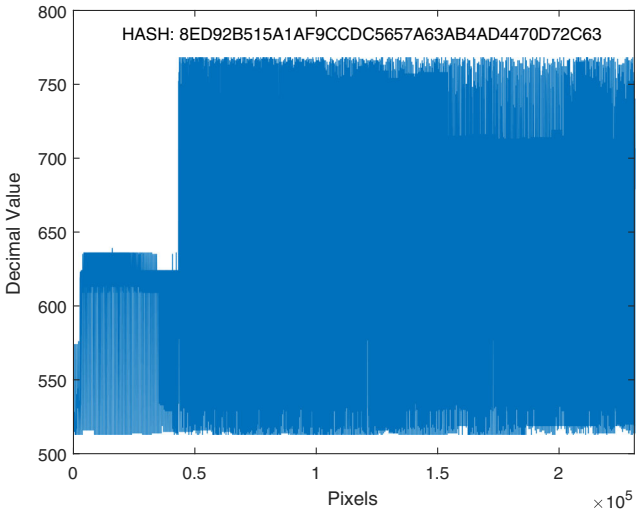

Fig. 9 Generation of decimal value for altered image

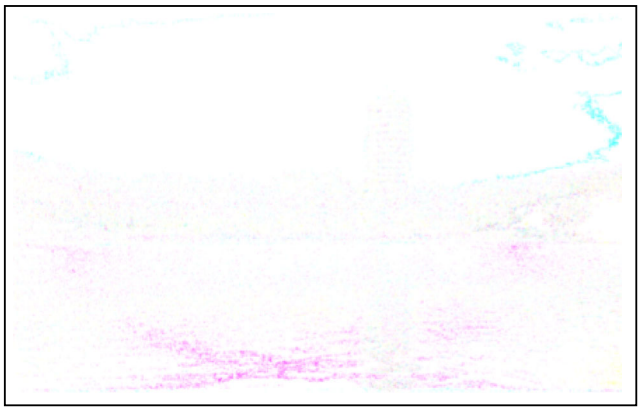

Fig. 10 Difference of watermarked image to forged image

synchronized. So, this clearly describes that the image is forged.

To evaluate the transparency and robustness, Peak Signal-to-Noise Ratio (PSNR) is used to evaluate the quality of image that can be defined as:

$$\mathrm{PSNR} = 10\log_{10}\frac{(2^d-1)^2 WH}{\sum_{i=1}^{W}\sum_{j=1}^{H}(p[i,j]-p'[i,j])^2} \tag{7}$$

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

6.3 Security analysis of overlay network

In the proposed DRM model, security is evaluated based on three categories. i.e., adversaries can be the malicious

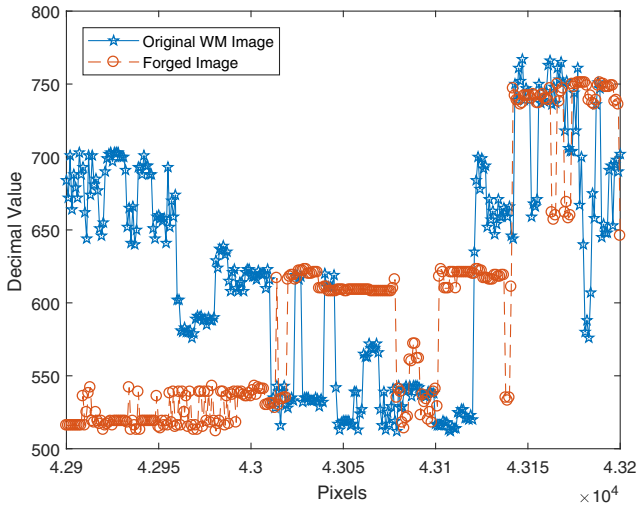

Fig. 11 Detailed analysis of digital rights violation by taking selected number of pixels for comparison.

node from the cloud storage, the malicious node from the blockchain network or the cluster head. These adversaries can modify watermark, replicate fake nodes, discard transactions delete or change information or create false transactions.

6.3.1 Incentivization for scalable blockchain

The fee is deposited by an authorized user who wants to access digital content in our system and this fee is set by platform owners and depends the contract between artists and platform owners. This fee can serve as the maintenance charges for cluster heads as well as a penalty fee in case of the content violation [18]. During the verification process, if it is found that an entity tries to violate copyright or tamper with content, then report transaction is created by the validator. The report transaction is processed through the blockchain ledger and smart contracts after the transaction is confirmed. The validator will get the corresponding reward as the time they discover misbehavior or copyright violation. These rewards will be distributed by smart contracts. Combined with transaction costs and subsequent incentives, it can be realized that the entire sources of incentives in the system mainly come from the authorized users who request for the content.

6.3.2 Storage attack

An adversary can make an attack on cloud storage and can try to modify or remove the data from the storage. However, in such cases, data is in encrypted form before uploading it to the cloud. The content owner also creates the hash of the data, and therefore if adversary make changes to the data, it can be easily verified. Many other cloud security protocols can be used to secure digital contents. However, the main goal of this paper is to secure DRM transactions. These transactions are stored in a distributed network in encrypted blocks and therefore entirely secured.

6.3.3 Denial of service (DoS) attack

An adversary can sometimes prevent authentic nodes to access the network and such attack is called Denial of Service (DoS) attack. To increase the traffic in the network and to jam the network, an adversary can launch many fraud blocks. However, the proposed model is not using a public network where anyone can join the network, and only limited users are allowed to join the network. Even after that if malicious nodes activity found, then the responsible node can be blocked from the network.

6.3.4 Encrypted blocks

In the proposed model, to prevent any discrimination based on the contents of any block like transactions, timestamp or other attribute, blocks are encrypted. During the propagation of blocks through the cluster head, blocks are encrypted. Once blocks are reached to the destination, the key is revealed that can be used to decrypt the transactions.

6.3.5 Indirect relay

It is also possible that cluster head is not honest with few nodes and do not propagate blocks for some individual node. In order to prevent cluster head to become dishonest, nodes do not directly propagate the blocks to cluster head, but they firstly propagate it to neighbour peer, and then neighbour peers pass this block to cluster head through other neighbours. This way the cluster head cannot identify the origin of the block.

6.3.6 Test block

Cluster head could be biased with individual block contents. However, the test blocks are used to check if the cluster head is working properly or not. Cluster head can receive a test block from any node who wants to monitor it. Using these techniques network nodes can examine cluster head and can stop biased decisions taken by it.

6.3.7 Dropping attack

Sometimes an intruder can attack cluster head and can control it to stop the propagation of blocks. In such case, cluster head do not communicate with any node and drops all the received blocks. However, in this case, nodes in the network can elect another cluster head.

7 Conclusion and future work

In this paper, a novel blockchain-based DRM system is proposed to secure the digital content. The scalability of blockchain is boosted significantly by using an overlay network with oversight from a CH. By solving the networking bottleneck issue, any cryptocurrency community can adjust its protocol to the proposed overlay network. To secure content with copyright issues, a digital watermark is embedded in the original digital contents. Information is added such as copyright owner, location, date of creation in the watermark image. To enhance the security of watermark images,

lightweight encryption is used to encrypt the watermark image. In future, deploying the system will be considered to conduct rigorous performance evaluation and detail security analysis of the scalable DRM. Moreover, the system will be explored further in terms of the privacy requirements of the entire entities involved in the system. e.g., content owners, users and transactions using zero-knowledge proof.

Acknowledgments The work of Ashutosh Dhar Dwivedi and Anwar Hasan is supported by University of Waterloo, Canada. Abba Garba and Zhong Chen is supported by National Natural Science Foundation of China Grant No. 61672060 and Gautam Srivastava is supported by the grant Natural Sciences Research Council of Canada (NSERC) Discovery Grant program (RGPIN-2020-05363).

References

1. Bitcion charts and graphs. https://www.blockchain.com/charts
2. Competition for authenticated encryption: Security, applicability, and robustness (2015). https://competitions.cr.yp.to/caesar.html
3. Eos (2019). https://eos.io
4. Nist competition (2019). https://csrc.nist.gov/Projects/Lightweight-Cryptography
5. resonate music (2019). http://www.resonate.is
6. Ripple (2019). http://www.ripple.com
7. ujo music (2019). http://www.ujomusic.com
8. Baza M, Mahmoud M, Srivastava G, Alasmary W, Younis M (2020) A light blockchain-powered privacy-preserving organization scheme for ride sharing services. In: 2020 IEEE 91St vehicular technology conference (VTC2020-spring). IEEE, pp 1–6
9. Beaulieu R, Treatman-Clark S, Shors D, Weeks B, Smith J, Wingers L (2015) The simon and speck lightweight block ciphers. In: Design automation conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, pp 1–6
10. Bhowmik D, Feng T (2017) The multimedia blockchain: A distributed and tamper-proof media transaction framework. In: 22Nd international conference on digital signal processing, DSP 2017, London. IEEE, pp 1–5. https://doi.org/10.1109/ICDSP.2017.8096051
11. Chen Q, Srivastava G, Parizi RM, Aloqaily M, Al Ridhawi I (2020) An incentive-aware blockchain-based solution for internet of fake media things. Inf Process Manag:102370
12. Dwivedi A (2020) Security analysis of lightweight iot cipher: Chaskey Cryptography 4(3). https://doi.org/10.3390/cryptography4030022
13. Dwivedi A, Morawiecki P, Srivastava G (2019) Differential cryptanalysis of round-reduced speck suitable for internet of things devices. IEEE Access 7:16476–16486
14. Dwivedi A, Morawiecki P, Wójtowicz S (2018) Finding differential paths in arx ciphers through nested monte-carlo search. Int J Electron Telecommun 64(2):147–150
15. Gaber T, Ahmed A, Mostafa A (2020) Privdrm: a privacy-preserving secure digital right management system. In: Proceedings of the Evaluation and Assessment in Software Engineering, pp 481–486
16. Gallardo-Saavedra S, Hernández-Callejo L, Duque-Perez O (2018) Image resolution influence in aerial thermographic inspections of photovoltaic plants. IEEE Trans Indust Inf 14(12):5678–5686
17. Goyal P, Netravali R, Alizadeh M, Balakrishnan H (2019) Secure incentivization for decentralized content delivery. In: 2Nd {USENIX} workshop on hot topics in edge computing (hotedge 19)
18. Guan Z, Garba A, Li A, Chen Z, Kaaniche N (2019) Auth-ledger: A novel blockchain-based domain name authentication scheme
19. Guo J, Li C, Zhang G, Sun Y, Bie R (2020) Blockchain-enabled digital rights management for multimedia resources of online education. Multim Tools Appl 79(15-16):9735–9755. https://doi.org/10.1007/s11042-019-08059-1
20. Im DKD The blockchain trilemma (2018)
21. Kamal M, Srivastava G, Tariq M (2020) Blockchain-based lightweight and secured v2v communication in the internet of vehicles. IEEE Transactions on Intelligent Transportation Systems
22. Kishigami J, Fujimura S, Watanabe H, Nakadaira A, Akutsu A (2015) The blockchain-based digital content distribution system. In: 2015 IEEE Fifth international conference on big data and cloud computing. IEEE, pp 187–190
23. Ma Z, Huang W, Gao H (2018) A new blockchain-based trusted DRM scheme for built-in content protection. EURASIP. J Image Video Process 2018:91. https://doi.org/10.1186/s13640-018-0327-1
24. Ma Z, Jiang M, Gao H, Wang Z (2018) Blockchain for digital rights management. Futur Gener Comput Syst 89:746–764
25. McConaghy T, Holtzman D (2015) Towards an ownership layer for the internet ascribe. GmbH
26. Meng Z, Morizumi T, Miyata S, Kinoshita H (2018) 2018 IEEE 42nd Annual Computer Software and Applications Conference, COMPSAC 2018, Tokyo, Vol 2. IEEE Computer Society, pp 359–364. https://doi.org/10.1109/COMPSAC.2018.10258. In: Reisman S, Ahamed SI, Demartini C, Conte TM, Liu L, Claycomb WR, Nakamura M, Tovar E, Cimato S, Lung C, Takakura H, Yang J, Akiyama T, Zhang Z, Hasan K (eds)
27. Mishra D (2015) An accountable privacy architecture for digital rights management system. In: Proceedings of the Sixth International Conference on Computer and Communication Technology 2015. ACM, pp 328–332
28. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system
29. RaidenGavin W Ethereum: A secure decentralised generalised transaction ledger (2014). https://gavwood.com/paper.pdf
30. Rashid A (2016) Digital watermarking applications and techniques: a brief review. Int J Compute Appl Technol Res 5(3):147–150
31. Singh R, Dwivedi A, Srivastava G, Wiszniewska-Matyszkiel A, Cheng X (2020) A game theoretic analysis of resource mining in blockchain. Cluster Computing: The Journal of Networks, Software Tools and Applications. https://doi.org/10.1007/s10586-020-03046-w
32. Singh R, Dwivedi A, Srivastava G (2020) Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors 20(14):3951
33. Singh R, Dwivedi A, Srivastava G (2020) Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors 20(14):3951. https://doi.org/10.3390/s20143951
34. Singh R, Dwivedi A, Srivastava G, Wiszniewska-matyszkiel A, Cheng X (2020) A game theoretic analysis of resource mining in blockchain. Cluster Comput 23(3):2035–2046. https://doi.org/10.1007/s10586-020-03046-w
35. Srivastava G, Dhar S, Dwivedi A, Crichigno J (2019) Blockchain education. In: 2019 IEEE Canadian conference of electrical and computer engineering, CCECE 2019. IEEE, Edmonton, pp 1–5. https://doi.org/10.1109/CCECE.2019.8861828
36. Srivastava G, Dwivedi AD, Singh R (2018) Automated remote patient monitoring: Data sharing and privacy using blockchain. CoRR arXiv:. http://arxiv.org/abs/1811.03417 1811.03417

37. Vishwa A, Hussain FK (2018) A blockchain based approach for multimedia privacy protection and provenance. In: 2018 IEEE Symposium series on computational intelligence (SSCI). IEEE, pp 1941–1945
38. Xia Z, Jiang L, Ma X, Yang W, Ji P, Xiong N (2019) A privacy-preserving outsourcing scheme for image local binary pattern in secure industrial internet of things. IEEE Transactions on Industrial Informatics
39. Zhang K, Jacobsen HA (2018) Towards dependable, scalable, and pervasive distributed ledgers with blockchains. In: ICDCS, pp 1337–1346

Abba Garba is a Ph.D Student of Computer Software and Theory at Laboratory of Network and Information Security, Peking University. Abba received his BSc(Hons) degree in omputing from University of Portsmouth, U.K., MSc in Information Systems from Kampala International University, Uganda and MBA from University of Wales, UK. Abba currently supervised by Professor Zhong Chen, his current research interest involves security and privacy especially in the Blockchain related field. Currently working on applying Blockchain Technology in Public Key Infrastructures (PKIs) domain.

Ashutosh Dhar Dwivedi is a Postdoctoral Researcher at DTU Compute (Cyber Security Section), Technical University of Denmark. His research field includes Symmetric Key Cryptography and Blockchain. He completed his PhD from the Polish Academy of Sciences, Poland. Prior to joining DTU, he worked as a full time Visiting Researcher at the University of Waterloo, Ontario, Canada, Research Associate at the Brandon University, Manitoba, Canada, Research Employee at Polish Academy of Sciences, Warsaw, Poland and Research Scholar at the Military University of Technology, Warsaw, Poland. He has made contributions to multiple journal and conference articles. Heidelberg Laureate Forum, Germany has selected him among top 100 young researchers all over the world in Computer Science to participate in the HLF-2019 event.

Mohsin Kamal (M'16) received the B.S. degree in Telecommunication Engineering from National University of Computer & Emerging Sciences, Peshawar, Pakistan, in 2008 and the M.S. degree in Electrical Engineering from Blekinge Tekniska Hogskola, Karlskrona, Sweden, in 2012. He completed his Ph.D. degree in Electrical Engineering from National University of Computer & Emerging Sciences, Peshawar, Pakistan in 2020. Since 2013, he is working as Assistant Professor at National University of Computer & Emerging Sciences, Peshawar, Pakistan. He is also the IEEE student branch counselor at the same institute since 2016. Besides that, he is elected as secretary of IEEE Peshawar sub-section from January, 2019. His research interests include the development of light-weight solutions for various IoT applications, wireless sensor networks, cooperative communication and cognitive radio networks.

Gautam Srivastava was awarded his B.Sc. degree from Briar Cliff University in U.S.A. in the year 2004, followed by his M.Sc. and Ph.D. degrees from the University of Victoria in Victoria, British Columbia, Canada in the years 2006 and 2011, respectively. He then taught for 3 years at the University of Victoria in the Department of Computer Science, where he was regarded as one of the top undergraduate professors in the Computer Science Course Instruction at the University. From there in the year 2014, he joined a tenure-track position at Brandon University in Brandon, Manitoba, Canada, where he currently is active in various professional and scholarly activities. He was promoted to the rank Associate Professor in January 2018. Dr. G, as he is popularly known, is active in research in the field of Data Mining and Big Data. In his 8-year academic career, he has published a total of 43 papers in high-impact conferences in many countries and in high-status journals (SCI, SCIE) and has also delivered invited guest lectures on Big Data, Cloud Computing, Internet of Things, and Cryptography at many Taiwanese and Czech universities. He is an Editor of several international scientific research journals. He currently has active research projects with other academics in Taiwan, Singapore, Canada, Czech Republic, Poland and U.S.A. He is constantly looking for collaboration opportunities with foreign professors and students.

Muhammad Tariq is the Director of FAST National University of Computer & Emerging Sciences (NUCES) Peshawar Campus. Before taking charge as a director, he was head of Department of Electrical Engineering in the same university. He is the author/co-author of 50+ research articles, and received many awards for his work. He has presented his research work in various IEEE flagship conferences held around the world. He rendered his Technical Committees services in various IEEE flagship conferences and transactions. He has co-authored a book on smart grids with leading researchers from Europe, China, Japan, and the U.S., which was published by Wiley in 2015. In 2017, Chinese government selected him as High End Foreign Expert through International Cooperation Project funded by State Administration of Foreign Experts Affairs China. Dr. Tariq completed his Postdoc from Princeton University as a Fulbright scholar under the supervision of Prof. H. Vincent Poor in 2016. Dr. Tariq completed his PhD as a Japanese govt (MEXT) scholar, from Waseda University, Japan in 2012. He completed his MS from Hanyang University, South Korea as an HEC scholar. He has delivered research talks as a guest/invited/keynote speaker at various forums and universities in Pakistan, China, Saudi Arabia, and the U.S. He is the programs' evaluator (PEV) of Pakistan Engineering Council.

M. Anwar Hasan is a Professor at Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is also a faculty member at the Centre for Applied Cryptographic Research. From January 2013 to April 2018, he was the Faculty of Engineering's Associate Dean of Research and External Partnerships. Professor Hasan's research interests include cryptographic computations and embedded systems, dependable and secure computing, and security for cloud and Internet of Things. He has made contributions to multiple books, journal and conference articles and has also received several awards for his many achievements in research.

Zhong Chen is a Professor of School of Electronics engineering and Computer science (EECS) at Peking University, and Director of MoE Key Lab of Network and Information security, Software Assurance, Cloud security, Director of Financial Information Research Center of Peking University. His Current research interest include Blockchain, Domain- specific software engineering, network and information security. Dr. Chen graduated and earned his Ph.D degree from Computer Science and Technology Department of Peking University in 1989, and became faculty member of Peking University. He became full professor in 1995.

Affiliations

Abba Garba[1,2] · Ashutosh Dhar Dwivedi[3] · Mohsin Kamal[4,7] · Gautam Srivastava[5,6] · Muhammad Tariq[4,7] · M. Anwar Hasan[8] · Zhong Chen[1,2]

Abba Garba
abbaggumel@pku.edu.cn

Ashutosh Dhar Dwivedi
adhdw@dtu.dk

Mohsin Kamal
mohsin.kamal@nu.edu.pk

Muhammad Tariq
mtariq@princeton.edu

M. Anwar Hasan
ahasan@uwaterloo.ca

1 Key Laboratory of High Confidence Software Technologies (Peking University), MoE, Beijing, China

2 Department of Computer Science and Technology, EECS, Peking University, Beijing, China

3 Department of Applied Mathematics and Computer Science, Technical University of Denmark, Lyngby, Denmark

4 Department of Electrical Engineering, National University of Computer and Emerging Sciences, Peshawar, Pakistan

5 Department of Mathematics and Computer Science, Brandon University, Brandon R7A 6A9, Canada

6 Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan, Republic of China

7 Princeton University, Princeton, USA

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