Journal of Korea Multimedia Society Vol. 24, No. 8, August 2021(pp. 1044-1058)
https://doi.org/10.9717/kmms.2021.24.8.1044

Blockchain Technology for Combating Deepfake and Protect Video/Image Integrity

Md Mamunur Rashid[†], Suk-Hwan Lee[††], Ki-Ryong Kwon[†††]

ABSTRACT

Tempered electronic contents have multiplied in last few years, thanks to the emergence of sophisticated artificial intelligence(AI) algorithms. Deepfakes (fake footage, photos, speech, and videos) can be a frightening and destructive phenomenon that has the capacity to distort the facts and hamper reputation by presenting a fake reality. Evidence of ownership or authentication of digital material is crucial for combating the fabricated content influx we are facing today. Current solutions lack the capacity to track digital media's history and provenance. Due to the rise of misrepresentation created by technologies like deepfake, detection algorithms are required to verify the integrity of digital content. Many real-world scenarios have been claimed to benefit from blockchain's authentication capabilities. Despite the scattered efforts surrounding such remedies, relatively little research has been undertaken to discover where blockchain technology can be used to tackle the deepfake problem. Latest blockchain based innovations such as Smart Contract, Hyperledger fabric can play a vital role against the manipulation of digital content. The goal of this paper is to summarize and discuss the ongoing researches related to blockchain's capabilities to protect digital content authentication. We have also suggested a blockchain (smart contract) dependent framework that can keep the data integrity of original content and thus prevent deepfake. This study also aims at discussing how blockchain technology can be used more effectively in deepfake prevention as well as highlight the current state of deepfake video detection research, including the generating process, various detection algorithms, and existing benchmarks.

Key words: Blockchain, Security, Artificial Intelligence, Consensus, Deepfake, Video Integrity, Hyperledger Fabric, Smart Contract

1. INTRODUCTION

Blockchain is an encrypted, shareable, and decentralized ledger that enables users to record and monitor resources without relying on a single entity. It lets interested parties to interact and share resources in a peer-to-peer connection where the majority, not a single system authority, is in charge, determines distributed decision [1]. The blockchain technology has stimulated one of the most intensive bursts of research activities in latest years, but unaddressed security and privacy issues should be addressed before blockchain technologies can fully realize their capabilities.

Due to the potential of considerable commercial benefits, organizations are becoming increasingly

※ Corresponding Author : Ki-Ryong Kwon, Address: 45 Yongso-ro, Nam-gu, Busan, Pukyong National University, Daeyon campus, TEL : +82-51-629-6257, FAX : +82-51-629-6230, E-mail : kiryongkwon@gmail.com
Receipt date : Aug. 13, 2021, Approval date : Aug. 20, 2021
[†] Dept. of Artificial Intelligence Convergence, Pukyong National University
(E-mail : mamunrashid.ete88@gmail.com)
[††] Department of Computer Engineering, Donga University
(E-mail : skylee@tu.ac.kr)
[†††] Dept. of Artificial Intelligence Convergence, Pukyong National University
※ This research was supported by the Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2020R1I1A306659411, 2020R1F1A1069124), and the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2021-2020-0-01797) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

interested in blockchain technology. Increased levels of decentralization can be facilitated by blockchain, allowing suppliers to transact directly with customers, tracking assets more effectively, and ensuring data authenticity. Blockchain is considered as a significant advanced technological development, with research indicating that it has the ability to disrupt the industry by enabling authenticated and trusted decentralized safe transactions.

Blockchain isn't a stand-alone technology. The convergence of blockchain with technologies like big data analytics, IoT, and AI, in particular, will be disruptive. This convergence will have a significant impact on how businesses should approach data and gain insights from it. Organizations, regulators, and individuals will need to come up with innovative solutions and techniques to ensure that data benefits everyone in the end. We will experience this confluence in real life more frequently in the coming years [2].

Since their debut in 2017, deepfakes have appeared in our news stream more frequently than ever. It holds the potential to harm anyone's reputation if used maliciously. Deepfake combines the terms "deep learning" and "fake" to describe the advent of realistic fake videos generated by deep learning algorithms that can present disinformation by superimposing one person's face onto another person's body with no perceivable ambiguities [3].

Deepfake videos achieve face swapping by combining deep learning techniques with vast samples of video frames. The more samples there are, the more realistic the result gets. As an example, more than 56 hours of sample recordings were trained into the Obama film to make it feel very authentic and convincing. Deepfake videos are described as a data hazard and it is required the common people to make appropriate use of latest innovations and to distribute digital content in an ethical and responsible manner on social media channels [4].

Deepfake countermeasures currently available are limited. The deepfake problem is causing big tech companies to concentrate on technological solutions. However, as previously stated, the sharper the offense becomes, the better the defense becomes. Tech companies do everything they can to identify and remove bogus videos. Every day, around 5 billion videos are viewed on YouTube. There are currently no established techniques for validating the legitimacy of a digital video, audio, or image posted or broadcast on the internet. It is incredibly difficult to verify the genuine source of an uploaded digital item in a credible and trustworthy manner [5].

Our research leads to an improved comprehension of blockchain and provides a review of recent blockchain features as well as applications in many industries specially in data integrity and authenticity. We offer a blockchain-dependent generalized framework for proving the authenticity of electronic assets such as movies, audios, and photos in this article. It enables public access to reliable and verifiable data provenance, as well as the monitoring and analyzing the history of a publicly available web video. Although our proposal focuses specifically on video content, it is sufficiently flexible to be used to any other type of digital content, such as speech and images. The special characteristics and flexibility of using blockchain can help us in our battle against the deepfake. Our paper's main contributions can be highlighted as follows:

1. Briefly highlighted the features of blockchain and deepfake.
2. Summarize the relevant studies of blockchain combating deepfake.
3. Classify different deepfake detection methods as per their working process.
4. Proposed a framework that can be used to minimize the impact of data forgery.
5. Make recommendations for future study in the blockchain-deepfakes topic.

The remaining portion of this paper is organized as follows. In section 2, we present similar survey

and research works where features of blockchain technology are applied to limit the adverse impact of artificial intelligence are discussed and also few relevant papers on blockchain and deeplearning applications. Section 3 provides some explanation of the way this research was conducted. In section 4, we provide some basic information on blockchain architecture, consensus algorithms, smart contract and hyperledger fabric. Section 5 introduces the basic concept of deepfake; creation and identification techniques of deepfake are also discussed. and shows the experiment result and discussion. Generalized smart contract-based framework to protect video integrity and provide data authenticity and transparency using the decentralized and immutable feature of blockchain are mentioned in short in section 6. Section 7 comes up with the discussion of the implementation and evaluation of the proposed methodology. Finally in section 8, conclusions and future works are presented in a brief manner.

2. RELATED WORKS AND STUDIES

In reality, there are very limited works which focused on the uses of blockchain to combat against deepfake technology. Zhang et al. carried out one of the mentionable surveys related to blockchain and deeplearning. They carried out the survey on the papers published from January 2018 to August 2020. This study also covers five themes related to blockchain and deep learning, including (1) architecture, (2) trade and finance, (3) logistics and transportation, (4) smart contracts, and (5) security and privacy [6].

In one review paper, Yu et al. described the deepfake video production technique, then examine existing detection technology. Their review focuses on existing challenges with current detection algorithms as well as prospective developments. That particular review has a strong emphasis on generalization and resilience [7].

In another survey paper, David et al. offered a thorough outline of how to use blockchain as a service in today's information systems. The study provides detailed information on various blockchain researches and applications, and also their impact on blockchain and its deployment in other scenarios or applications. This study also highlighted the fact that the structure of blockchain and modern cloud and edge computing paradigms are crucial in enabling new members in today's unparalleled dynamic global market to adopt and develop blockchain technologies [8].

One of the most significant studies comes from Yazdinejad et al. [5] where they intend to be a one-stop shop for learning how to use blockchain to navigate deepfake AI. They present various use cases and methods for tackling deepfakes technology using blockchain capabilities and functionality. They also covered a variety of possible applications, including the usage of smart contracts, public and private keys, and blockchain-based distributed verification of authenticity. In their paper to combat the problem of fake news A. Qayyum et al. created a unique blockchain approach based on contracts. A publisher management protocol, a news smart contract, and the establishment of a news blockchain were all included in the proposed plan [9].

For tracing the sources of digital information, H.R. Hasan et al. suggest an Ethereum blockchain-based approach. This solution included a smart contract system, metadata of JSON objects on InterPlanetary File System servers, looking for Ethereum address in Ethereum Name Service [4].

As a result of the present explosion of interest in blockchain technology, many innovative technologies and applications have been proposed. Multiple survey studies have been prepared to demonstrate the advantages of this technology in contemporary applications. Blockchain technology for IoT, healthcare, and decentralized digital currencies are all examples of such surveys. Other

studies have looked into the obstacles, prospects, and future visions of blockchain technology. Lin and Liao [10], for example, explore blockchain security difficulties and challenges, provides a comprehensive review of blockchain security and privacy challenges, as well as potential attacks and countermeasures. In addition, blockchains and their potential uses are the focus of a recent special issue of IEEE Spectrum [11].

Various scholars have produced surveys on the various aspects of machine learning usage in blockchain-based smart apps to date. All of the main components of machine learning that can be employed in BT-based applications, such as intrusion detection, are included in the suggested survey. Gipp et al. [12] limit their use of blockchain to ensuring the video footage's integrity. The video is hashed and secured on the immutable blockchain as part of their approach. A hash mismatch will occur if the video is tampered with.

Our study looks into the applications of blockchain technology in a diversified way of combating malpractices of artificial intelligence such as deepfake that are getting momentum in recent times but have not been studied in much detail so far. We intend to conduct a thorough investigation into the usage of blockchain technology to provide digital content's authenticity and fight against deepfake. We hope through this review paper we can find a way out to effectively solve the deepfake situation as well as able to provide a way forward to future researches in this burning topic.

3. RESEARCH METHODOLOGY

For this article, a systematic mapping study was chosen as the research approach, with the goal of providing an overview of the research connected to the usage of blockchain for fighting deepfake, as well as the following essential steps.

1. Determine the necessity of the review, produce a proposal, and establish optimized procedures for the review.
2. Analyze the papers, choose the studies, evaluate their quality, take notes and extract data, and synthesize the information.
3. Summarize the review's findings and propose future research directions.
4. From our study of relevant articles, we have designed our own framework that can effectively protect the data authenticity and block any manipulation or forgery to original video/image such as deepfake.

First, we introduce the readers with the fundamental terms which is required to get the idea of blockchain and deepfake from many research papers and articles. The search for all relevant scientific papers on the research topic is the second stage and involves a title-based screening of all related papers. We summarize the key intakes from the most popular and prestigious journals that deal with technical elements of blockchain and deepfake. We also focused on peer-reviewed, high-quality articles relating to the research topic that were published in conferences, workshops, symposiums, books, and journals. Scientific databases such as IEEE, ArXiv, Springer, Semantic Scholar Science Direct, etc. were used to search the terms “blockchain” and “deepfake” in all articles' titles. Further search was undertaken using the works of relevant studies that were referenced (snowball effect).

In the next stage we critically appraised the collected literature's eligibility using a predefined set of established addition and deletion rules. Initially, all research publications' abstracts and the initial sections of literature review were evaluated. Following that, a full-text review was conducted, and several further papers were omitted from the study, with the grounds for deletion documented. Any conflicts on the relevancy of the items under review were settled by argument until an agreement was reached.

We studied a number of documents before coming up with our own research on the usage of blockchain to safeguard photos, videos, and audios

from deepfake. The features of blockchain network and its applications to protect the authentic transactions and hold-off any kind of forgery attempt through its rules and logics has inspired us to come up with the idea of designing our own framework. Our proposed framework consisting of smart contract, IPFS (InterPlanetary File System) distributed storage, Ethereum blockchain offers a way forward to protect the data integrity against any kind of data manipulation. We have used different programming languages such as Solidity, Python, HTML, CSS to design our proposed framework.

4. BLOCKCHAIN BACKGROUND

At first, a quick overview of blockchain technology is introduced in this section. After that, blockchain consensus mechanism and working procedure are explained. Another two major concepts of blockchain namely Smart Contract and Hyperledger Fabric are also discussed in short. This chapter's main objective is to familiarize readers with blockchain technology and some of its main characteristics that can be of use in our fight against deepfake.

4.1 Blockchain Architecture

Blockchain is a peer-to-peer immutable network that consists of an ordered sequence of linked and duplicated data blocks. The blockchain's integrity is maintained at its core through the usage of public key encryption for all network interactions and updates [13]. The blockchain is built around a distributed system and a decentralized immutable consensus method, which is protected by encryption protocols that govern each block in the chain.

The main distinction between a blockchain and a centralized database is the degree of centralization. While all records in a database are centralized, each blockchain participant has a safe copy of all records and modifications, allowing each user to see the data's origin. Fig. 1 depicts the architectural differences between a traditional third-party ledger-based system and a blockchain-based system. In the typical configuration, a number of ledgers or databases are directly connected to a central or trusted third-party ledger. In this arrangement, each node in the network maintains its own ledger, but the central ledger acts as the master. The blockchain topology does not require the use of a trustworthy central ledger because each node in the network has its own duplicate ledger copy that interacts directly with all of the other nodes in the network. As a result of this design, all ledgers are synchronized across the network at all times and can engage directly without the requirement for a trusted third party [14].

This specific architecture helps the blockchain to keeps its three pillars intact: Decentralization, Transparency and Immutability. Because of these

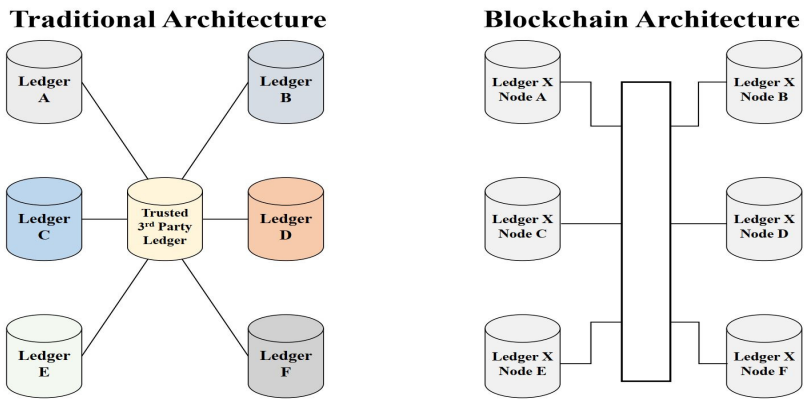

Fig. 1. Traditional vs blockchain architecture.

benefits, it has found use in practically every sector that requires data sharing among numerous parties while maintaining safe authenticity, confidentiality, and durability.

4.2 Working Procedure of Blockchain?

We already know that, a blockchain is a group of interconnected blocks, as illustrated in Fig. 2. The previous block's hash is combined with the current block's hashed content and a timestamp to create the new block. As a result, the new block will always be dependent on the prior block, and the two will be closely linked.

When one block in a blockchain is replaced by another, the chain is broken and a new, shorter blockchain is generated (whose length is determined by which block is replaced). Every block that isn't interchanged will be "thrown away" (i.e., is no longer valid) [15]. The blockchain will remain to use the blockchain that the majority of users consider is correct. If the network is permissionless, this might be the majority of the network, or if the blockchain is permissioned, it will be the majority of trusted nodes. This means that consensus-based blockchains will maintain their original state. The only method to change the blockchain is for the majority of the system's nodes to believe the new blockchain is correct [15].

4.3 Consensus Mechanism in Blockchain Networks

A consensus mechanism is a fault-tolerant technique used in blockchains to obtain an agreement across dispersed nodes on a single network state. These are algorithms that ensure that all nodes are in sync with one another and that all transactions are valid and added to the Blockchain. Their job is to ensure that the transactions are valid and authentic. When selecting a blockchain consensus mechanism, organizations and blockchain developers must make informed selections. As a result, business and blockchain executives may work backwards from desired outcomes to an appropriate consensus mechanism. On the other hand, mining refers to the process of constructing blocks that will be linked to a database. It enables nodes to generate blocks that are also validated by others. If the new block is found to be genuine, it is added to the blockchain database. Mining nodes are nodes that attempt to build blocks. To win the reward, mining nodes strive to verify transactions as swiftly as possible and generate new blocks.

Few most common consensus mechanisms are proof of Stake (PoS), proof of work (PoW), Proof of Importance (PoI), Proof of Space (PoSpace), minimum block hash, Practical Byzantine Fault Tolerance (PBFT), and Measure of Trust (MoT) [16].

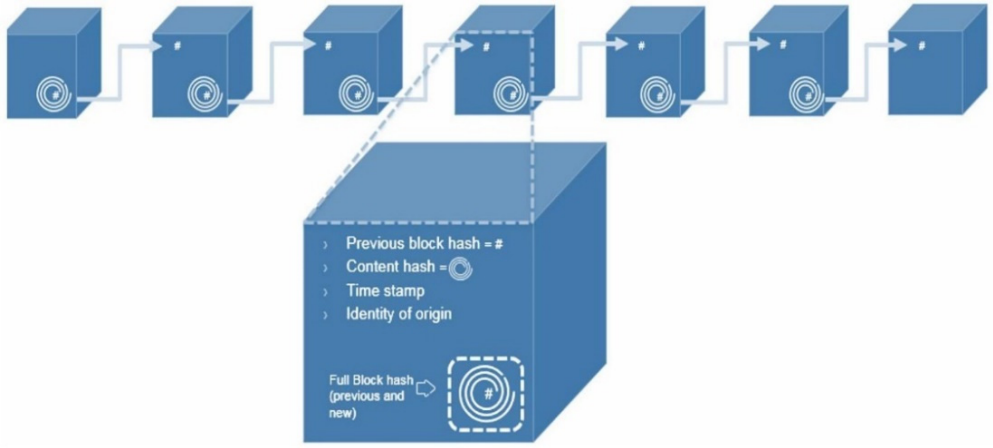

Fig. 2. Blockchaining.

4.4. Smart Contract

Smart contracts, a fascinating new blockchain application, have emerged in recent years. Smart contracts are contracts that execute themselves in which the terms of a multi-party agreements are written directly in code. A blockchain network bridges the code and the agreements it contains. To carry out reliable transactions and engagements amongst remote, anonymous parties, smart contracts do dispense with the need for a central authority, legal system, or external enforcement mechanism. Transactions are traceable, transparent, and irrevocable as a result of them. Developers have devised domain-specific languages like Solidity to make the process easier due to the inherent challenges of smart contract creation.

4.5 Hyperledger Fabric

Hyperledger Fabric is a scalable architecture-based framework for distributed ledger applications that provides high levels of confidentiality, robustness, flexibility, and scalability. It consists of a ledger, smart contracts, and some method for participants to keep track of their transactions, just like other blockchain technologies. Instead of using an open permissionless approach that allows anybody to join a Hyperledger Fabric network, members enroll through a trusted Membership Service Provider (MSP) (needing transaction validation and network security mechanisms such as "proof of work"). It also allows users to construct pathways, which allow a set of entities to create their own transaction ledger [17].

5. CREATION AND DETECTION OF DEEPFAKE

This section enables the readers with a brief introduction of deepfake technology. After that, the generation techniques of deepfake are discussed in short. Detection methods of deepfake as well as their classifications and various way preventing deepfakes are also discussed in later subsections.

5.1 What is Deepfake?

Artificial Intelligence-based image synthesis for humans is called as "deepfake,"; a name that is a combination of two unique terms "deep learning" and "fake." Using various machine learning algorithms, it integrates and superimposes existing digital media onto raw photos or videos. Deepfakes have been used to create fake news, malicious hoaxes, fake X-rated videos, and financial frauds thanks to their technological capabilities [18]. When such overlay digital materials and source footage are combined, a fake video is created that displays a person doing an action at an event that never happened in real life. Deepfakes have the potential to shape public opinion, political concerns, and difficult circumstances that could escalate to military war [18].

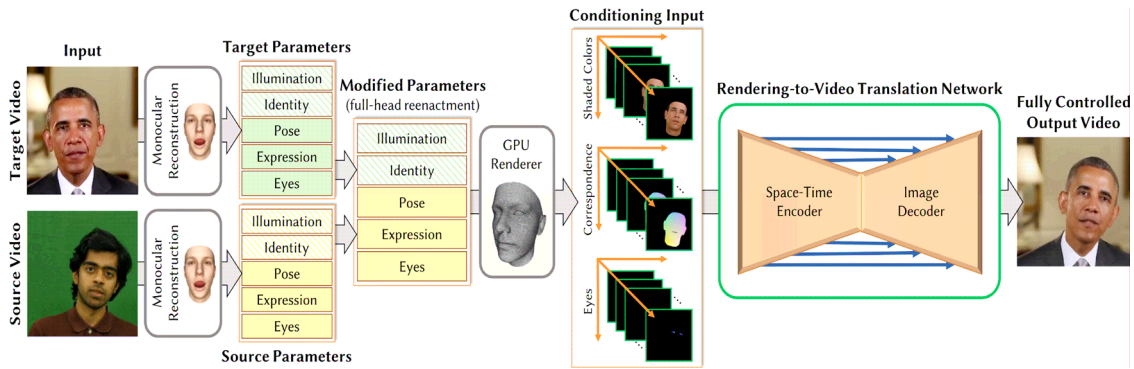

Fig. 3. Example of Deepfake Video.

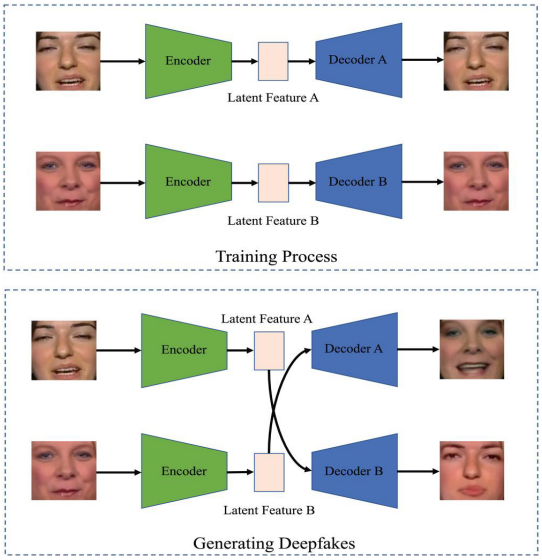

Fig. 4. Deepfake using Autoencoders (faceswapping).

5.2 Deepfake Generation Techniques

Deepfakes make use of an autoencoder, which is a form of neural network. An encoder transforms an image to a lower-dimensional spatial domain, which is then used by a decoder to recreate the image. Deepfakes employ this architecture by using a universal encoder to encode a person into the latent space. Important information can be obtained from the underlying representation of their facial features and body posture. After that, it can be decoded by a model that has been trained specifically for the target. This means that the target's individual information will be placed on the underlying face and body features from the original video in the latent space [19].

The integration of a generative adversarial network to the decoder is a popular improvement to this architecture. A GAN trains an adversarial connection between a generator, in this case the decoder, and a discriminator. The generator produces new images from the latent representation of the source material, while the discriminator determines whether or not the image is formed. As a result, the generator produces images that closely resemble reality, as any flaws would be detected by the discriminator [20]. There are many sophisticated deepfake methods such as Faceswap, Open Pose, Deekfake, and Cycle GAN available now-a-days and the comparison among them is really interesting topic [21].

5.3 Deepfake Detection

Many centralized organizations offer ways to combat deepfakes, and those that perpetrate deepfakes can be easily identified. Because of these centralized companies, users do not have access to verified data provenance of digital information [18].

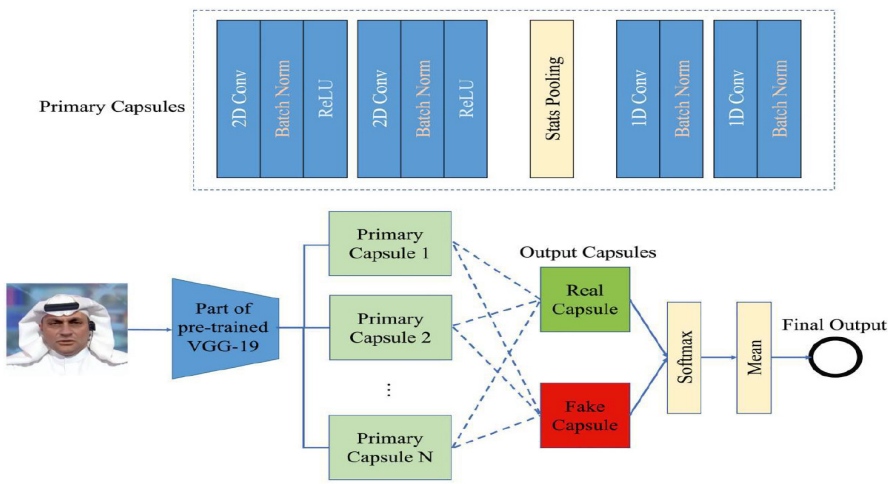

Fig. 5. Capsule-forensics architecture for deepfake detection.

To determine whether digital content is genuine, people can utilize search engines and check multiple blogs, postings, news, and other sources relevant to the false ones in order to identify the original sources and therefore avoid the spread of disinformation by deepfakes. Two examples of deepfake detection are illustrated in Fig. 5 and 6.

Deepfake video detection has been improved thanks to recent breakthroughs in image classification. In this method, the detection network is trained using face images extracted from the detected video. All of the frames in this video are then predicted using the trained network. Finally, an average or voting approach is used to calculate the forecasts. There are two types of network-based methods of deepfake detection using image classification: transfer learning and specially created networks [7].

Video has a special characteristic called time continuity. Video, unlike photographs, is a multi-frame series with significant connection and continuity between subsequent frames. Because of flaws in deepfake algorithms, yhe association between neighboring frames is disrupted when video frames are adjusted, resulting in face position shift and video flickering. Depending on this, scholars have found various methods like CNN-RNN, time-based detection etc. [7].

Yu et al. has tried to classify the deepfake detection methods in five different categories. Table 1 represents the classification of currently existing deepfake detection methods [7].

The above-mentioned techniques have helped in deepfake detection to some extent but doesn't provide the complete solution. Blockchain can be used to provide some levels of security, approval, and validation to deepfakes. Traditionally, blockchain has been marketed as a visibility and transparency play, in which once something is completed, the "when" and "who" are readily evident. When a user with a digital identity wants to accomplish anything, they may be asked to provide confirmation of their identity before being granted access to something (such as finances or movies) [18]. With tamperproof records, logs, and transactions, blockchain might be used to establish the validity and originality of digital media in a decentralized, trusted, and secure manner and is the best option for deepfakes. Many researchers have proposed Smart contract and Hyperledger Fabric based solutions to control and record the history of digital content transfers and thus helping authentication of the content and prevent deepfakes. Fig. 7 depicts one of the examples of uses of the blockchain technology in the fight against deepfake [5].

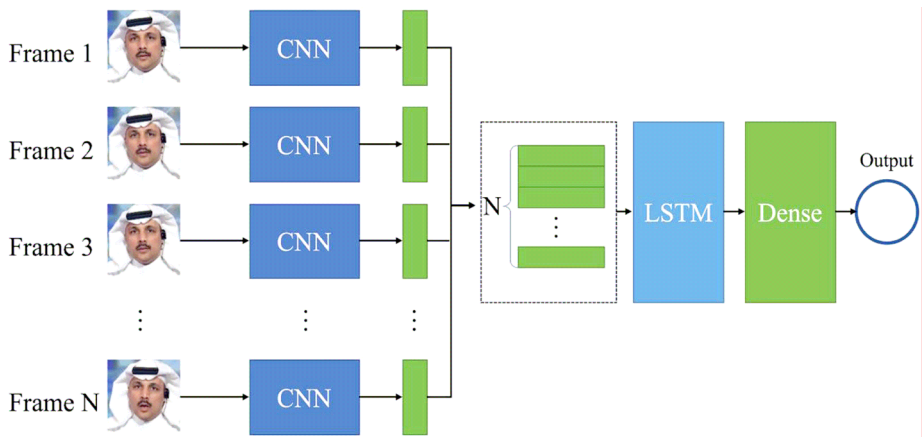

Fig. 6. Deepfake detection method based on CNN-LSTM (Temporal-consistency-based methods).

Table 1. Classification for existing deepfake detection techniques.

Methods	Description
General network based methods	CNNs accomplish the task of detection, which is a frame-level classification task.
Temporal consistency based methods	Due to flaws in the forgery algorithm, anomalies between neighboring frames are discovered in deepfake videos. As a result, RNN is used to detect such inconsistencies.
Visual artefacts based methods	Underlying image disparities in the blending boundaries would result from the blending operation in the generation process. These artefacts are identified using CNN-based approaches.
Camera fingerprints based methods	Devices leave varied footprints in collected photos due to different generation processes. Faces and background images are simultaneously detected as coming from separate devices. As a result, these traces can be used to complete the detecting task.
Biological signals based methods	Concealed biological signals in faces are difficult to interpret using GAN, making it impossible to synthesis human looks with appropriate behavior. Biological signals are extracted based on this observation to detect deepfake films.

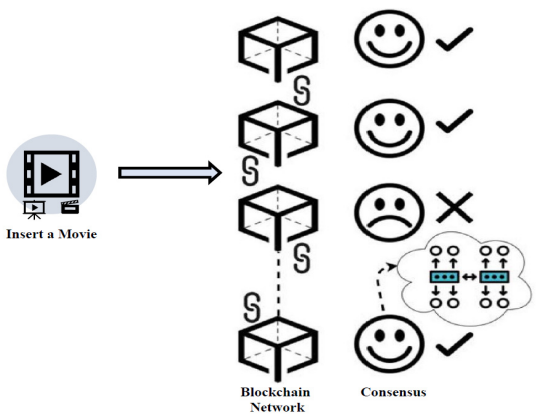

Fig. 7. Use of consensus mechanisms of blockchain against deepfake.

6. PROPOSED FRAMEWORK

In this section, a data (video, image etc.) sharing system is proposed which is unlike existing methods, is totally distributed. We proposed a Smart Contract based solution that can operate as a heart in the war against deepfake, allowing us to achieve our video content security goals while running on the blockchain as evident if Fig. 8. Blocks are formed via consensus methods in these networks, and block validation requires a majority vote. Furthermore, when employing blockchain technology, numerous identity steps are required for final clearance due to several signature transactions in the original data.

A smart contract concentrates on data content, such as video frames and metadata. Aside from the frames, information in the video, metadata can provide details such as the time and date of recording, speed, relevant logs, GPS, device information, and so on. A smart contract is activated on the blockchain when a hash for a video is generated and it contains all the important attributes as well as video metadata. According to the terms and conditions, others may change and edit this video. The smart contract can also create restricted access or roles for that video. On the blockchain, the video's content may be tracked, and a smart contract can be used to link the video's owner's legitimacy to the database. In a nutshell, confirming the authenticity of a video is simple, and it's a good way to resist deepfake technology.

A decentralized interface is incorporated in the suggested content sharing system to allow users to interact with the smart contract, and also the storage and the smart contract. When a user re-

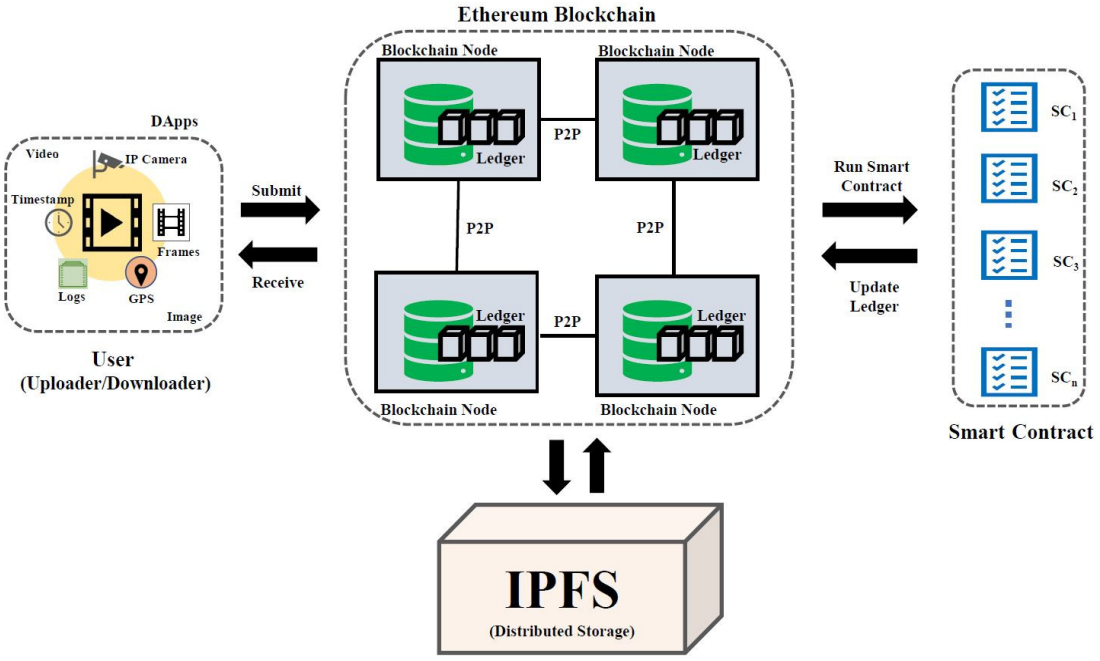

Fig. 8. Proposed framework (use of Smart Contract against data forgery)

quests to upload or download a video to the system, Dapp (Decentralized Applications) downloads or uploads the file and also sends the user system events from the smart contract.

Users who want to download a video will use the distributed application to communicate their request to the smart contract. After thoroughly examining and authenticating both parties involved in the transaction, the smart contract subtracts the video's value (Ether) from the balance of the downloader and added to the video owner's. The Dapp with the smart contract command changes the permission listing after the transaction has been verified in Blockchain, and the downloader user can then view the content.

This framework protects the content's copyright while also preventing illicit and unapproved dissemination in the system. By preventing the dissemination of untrustworthy, false, or unworthy information, it also improves the quality of content.

7. IMPLEMENTATION AND EVALUATION

The architecture provided in this study is made up of four basic pieces, as indicated in Fig. 8: smart contracts, IPFS storage, a blockchain network and distributed applications. Solidity 0.5.1 was utilized in the Remix.ide online programming environment to construct the Ethereum smart contract. To interact with the smart contract, the web3 library was used in a distributed application written in the Python 3.9.4 programming language. The development environment consists of OS (Windows 64), RAM (8GB), CPU (Intel i7), Dapp (Backend- Python 3.9.4; Front End- HTML & CSS), development languages (Python, HTML CSS, Solidity, Remix IDE).

7.1 Performance Analysis

Our proposed framework offers some remarkable attributes that bears the proof of our main purpose of this research. Few of the attributes are mentioned below:

7.1.1 Decentralized Infrastructure

Recent technologies such as blockchain are focused on removing centralization and increasing distribution. The suggested architecture eliminates resource storage centralization and substitutes it with fault-tolerant, peer-to-peer, Ethereum-compliant, and DDOS-resistant storage.

7.12 Integrity and Immutability

Modifying the content is nearly impossible due to the addition of video hashes to the smart contract. As a result, no node in the network can modify or republish content generated by other nodes. The content owners can sign or trademark their videos and leverage the immutability of the content to safeguard their ownership.

7.1.3 Transparency and Trust

Due to the usage of the smart contract, the suggested approach establishes transparency in the system. Smart contract's code and transactions are accessible and transparent to all network nodes, establishing trust in the system regardless of the fact that there is no central mediator.

7.1.4 Fault Tolerance and Zero Downtime

As previously stated, content redundancy and dispersion between nodes, as well as the absence of coding to store material, improve fault tolerance and therefore access control. Due to its decentralized nature, probability of system downtime is practically nil.

7.2 Security Analysis

Our suggested new framework dismisses the current centralized material distribution model in favor of a fully distributed framework. There is no more any central database in the network that may be hacked or manipulated, endangering the system's performance and security.

Smart contracts, under the proposed concept, allocate users to various roles, each with its own set of capabilities and responsibilities. It ensures that users can't hide their identities by functioning as "autonomous agents" and must follow the designated roles only.

Various health factors of the device are examined before data can be transferred. This assures that the device that will transfer the data is secure and up to date with the latest security updates and safeguards. Only if all of the device's minimum standards are satisfied, data encrypted and transferred to the IPFS.

As this architecture lacks a central server, censorship and distortion of content are unfeasible, and users can readily express their ideas and content on the platform. DDOS attacks are unlikely in the system due to the lack of a central server. Table 2 compares the content sharing platform provided in this paper to models found in other similar works [22,23,24,25,26].

The proposed system's assessment and comparisons to related works revealed that the new architecture is superior in terms of structure dif-

Table 2. Performance comparison of proposed and similar systems.

Methods	Decentralized Structure	Data Integrity	Security	Separated Storage	Transparency	Data Sustainability & Zero Downtime
[22]	✓	✗	✓	✓	✓	✗
[23]	✓	✗	✓	✓	✓	✗
[24]	✓	✓	✓	✗	✓	✗
[25]	✓	✓	✓	✓	✓	✗
[26]	✓	✓	✓	✗	✓	✗
Proposed	✓	✓	✓	✓	✓	✓

fusion, high availability and transparency, data integrity and immutability, system sustainability, trustworthiness, and security.

7.3 Time Complexity

Investigations with the proposed methodology demonstrated that the download time grew as the video size increased (Fig. 9). The algorithm for inserting and certifying video in the Merkel tree determines the system's time complexity and it is defined by O(log(n)).

As depicted in Fig. 9, the increase in time is evident after the video size has crossed 128 KB as the chunks are stored with that size. The time increase is almost similar as the increase in the size of the video files. This means that, the validation and upload time for large videos usually takes high time in comparison to the low size video files. But, the second time download of videos files is very fast and almost identical to each other irrespective of their size. This is one of the remarkable advantages of using blockchain because for second time download there is no necessity of validating the files or users.

8. CONCLUSION

Deepfake, which rely on deep learning technique, have progressed at an unprecedented rate in recent years. Deepfake algorithms can quickly propagate malicious face-altering videos, endangering societal stability and personal privacy. To this end, scientific institutions and research groups all around the world are undertaking studies to lessen the detrimental effects of deepfake on individuals and mankind as a whole. In this study, we described the deepfake generation techniques and examined existing deepfake detection methods as well. We also explored using blockchain technology as a possible remedy against the damaging effects of data manipulation, and how blockchain may help us reduce the impact of vicious deepfake technology. Our suggested framework can aid in the fight against deepfake videos, photos, and audios by assisting users in determining if a video or digital content can be traced back to a reliable source. In order to achieve a universally safe artificial intelligence society and ensure that future technology is produced with good intentions, we wish to apply more of the combination of state-of-the-art

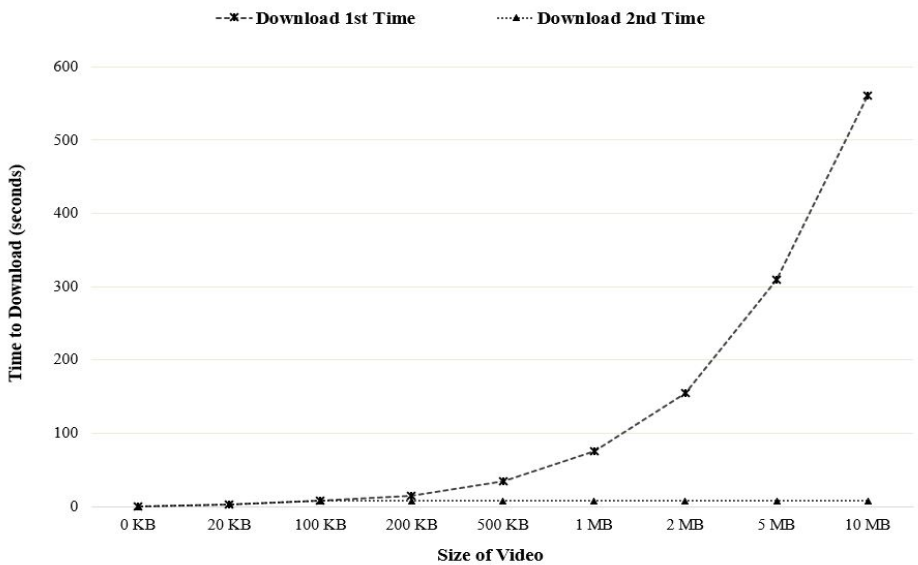

Fig. 9. Download time vs video size (first- and second-time download).

content-unique hashing methods, integrity methods, security measures, and globally adopted blockchains.

REFERENCE

[1] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Communications Surveys Tutorials,* Vol. 21, No. 1, pp. 858-880, 2019.

[2] M.V. Rijmenam, "Five Blockchain Trends for You to Consider This Year," April 2019. [Online]. https://vanrijmenam.nl/five-blockchain-trends-consider-this-year/ (Accessed 02 Aug 2021).

[3] C.C.K. Chan, V. Kumar, S. Delaney, and M. Gochoo, "Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media," *IEEE/ITU International Conference on Artificial Intelligence for Good (AI4G)*, pp. 55-62, 2020.

[4] H.R. Hasan and K. Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts," *IEEE Access,* Vol. 7, pp. 41596-41606, 2019.

[5] A. Yazdinejad, R.M. Parizi, G. Srivastava, and A. Dehghantanha, "Making Sense of Blockchain for AI Deepfakes Technology," *IEEE Globecom Workshops*, pp. 1-6, 2020.

[6] Y. Zhang, Y. Liu, and C. H. Chen, "Survey on Blockchain and Deep Learning," *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1989-1994, 2020.

[7] P. Yu, Z. Xia, J. Fei, and Y. Lu, "A Survey on Deepfake Video Detection," *IET Biometrics,* pp. 1-18, 2021.

[8] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Information Processing & Management,* Vol. 58, No. 1, p. 102397, 2021.

[9] A. Qayyum, J. Qadir, M. U. Janjua, and F. Sher, "Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News," *IT Professional,* Vol. 21, No. 4, pp. 16-24, 2019.

[10] I.C. Lin and T.C. Liao, "A Survey of Blockchain Security Issues and Challenges," *International Journal of Network Security,* Vol. 19, No. 5, pp. 653-659, 2017.

[11] M.E. Peck, "Blockchain World-Do You Need A Blockchain? This Chart Will Tell You If the Technology Can Solve Your Problem," *IEEE Spectrum,* Vol. 54, No. 10, pp. 38-60, 2017.

[12] T. Hepp, A. Schoenhals, C. Gondek, and B. Gipp, "OriginStamp: A Blockchain-Backed System for Decentralized Trusted Timestamping," *IT-Information Technology,* Vol. 60, No. 5-6, pp. 273-281, 2018.

[13] D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, *Apress,* 2018.

[14] F. Hawlitschek, B. Notheisen, and T. Teubner, "The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy," *Electronic Commerce Research and Applications,* Vol. 29, pp. 50-63, 2018.

[15] A.H. Billstrom and F. Huss, Video Integrity Through Blockchain Technology, *Master's Thesis, KTH Royal Institute of Technology*, 2017.

[16] A. Shubhani and N. Kumar, "Chapter Eleven-Cryptographic Consensus Mechanisms," *Advance Computing,* Vol. 121, pp. 211-226, 2021.

[17] A Blockchain Platform for the Enterprise (2020), https://hyperledger-fabric.readthedocs.io/en/release-2.2/blockchain.html (Accessed August 03, 2021).

[18] A. Chauhan and A. Kumar, "Establishing Environment Setup for Preventing Deepfakes Using Blockchain Technology," *Mukt Shabd Journal,* pp. 771-776, 2020.

[19] S. Charleer, "Family Fun with Deepfakes. or How I Got My Wife onto the Tonight Show," *Towards Data Science,* 2018.

[20] I. Jessica, "Defamatory Political Deepfakes and the First Amendment," *Case Western Reserve Law Review,* Vol. 70, No. 2, pp. 417-455, 2019.

[21] H.B. Jeon, H.K. Ko, S.G. Lee, B.D. Song, C.K. Kim, and K.R. Kwon, "Comparative Analysis of Four Face Transformation Technologies to be Provided to the Interactive Media Platform COX," *Journal of Korea Multimedia Society,* Vol. 22, No. 5, pp. 535-546, 2019.

[22] B.K. Zheng, L.H. Zhu, M. Shen, F. Gao, C. Zhang, Y.D. Li, and J. Yang, "Scalable and Privacy-Preserving Data Sharing Based on Blockchain," *Journal of Computer Science and Technology,* Vol. 33, No. 3, pp. 557-567, 2018.

[23] Z. Ma, M. Jiang, H. Gao, and Z. Wang, "Blockchain for Digital Rights Management," *Future Generation Computer Systems,* pp. 746-764, Dec. 2018.

[24] N. Fotiou and G.C. Polyzos, "Decentralized Name-Based Security for Content Distribution Using Blockchains," *IEEE Conference on Computer Communications Workshops,* pp. 415-420, 2016.

[25] M. Liu, F.R. Yu, Y. Teng, V.C.M. Leung, and M. Song, "Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing," *IEEE Transactions on Wireless Communications,* Vol. 18, No. 1, pp. 695-708, 2019.

[26] D. Bhowmik and T. Feng, "The Multimedia Blockchain: A Distributed and Tamper-Proof Media Transaction Framework," *22nd International Conference on Digital Signal Processing (DSP),* pp. 1-5, 2017.

Md Mamunur Rashid

received his B.S. Degree in Electronics and Telecommunication Engineering from Rajshahi University of Engineering & Technology, Bangladesh, in 2011. He worked at Robi Axiata Ltd. from 2011-2021 as a telecom professional in Bangladesh. He is currently pursuing a Doctorate (Combined Masters & Doctors) degree in the Department of Artificial Intelligence Convergence at Pukyong National University, Korea. His research interests include blockchain security, multimedia security and artificial intelligence.

Suk-Hwan Lee

received a B.S., a M.S., and a Ph.D. degree in Electrical Engineering from Kyungpook National University, Korea in 1999, 2001, and 2004 respectively. He is currently a professor in the Department of Computer Engineering at Donga University. His research interests include multimedia security, digital image processing, and computer graphics.

Ki-Ryong Kwon

received the B.S., M.S., and Ph. D. degrees in electronics engineering from Kyungpook National University in 1986, 1990, and 1994 respectively. He worked at Hyundai Motor Company from 1986-1988 and at Pusan University of Foreign Language from 1996-2006. He is currently a professor in Dept. of IT Convergence & Application Engineering at the Pukyong National University. He has researched University of Minnesota in USA from 2000-2002 with Post-Doc, and Colorado State University from 2011-2012 with visiting professor. He was the General President of Korea Multimedia Society from 2015-2016. He is also a director of IEEE R10 Changwon section. His research interests are in the area of digital image processing, multimedia security and watermarking, bioinformatics, weather radar information processing.