HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Journal of King Saud University - Computer and Information Sciences

journal homepage: www.sciencedirect.com

Enhanced computer vision applications with blockchain: A review of applications and opportunities

Najmath Ottakath [*], Abdulla Al-Ali, Somaya Al-Maadeed, Omar Elharrouss, Amr Mohamed

Department of Computer Science and Engineering, Qatar University, Qatar

ARTICLE INFO

Keywords:
Blockchain
Computer Vision
Video surveillance
Video integrity
Video and image sharing
Privacy

ABSTRACT

Videos and image processing have significantly transformed computer vision, enabling computers to analyse, and manipulate visual data. The proliferation of cameras and IR equipment has facilitated the collection of valuable information about individuals and their surroundings. These technologies find applications in various domains, ranging from biometric entry cards and high-security clearances to surveillance. These applications form part of the Internet of Things (IoT), forming a centralized network. However, the proliferation of data and its sharing brings challenges related to security, privacy, and storage. Interactions with third-party systems may introduce vulnerabilities. To address these issues, researchers in computer vision have explored the integration of blockchain technology into various applications. This paper presents a comprehensive survey of blockchain applications in computer vision, focusing on image and video data sharing, video surveillance, biometrics, and video integrity protection. The aim is to explore how the blockchain can enhance the security, privacy, and authentication of them. It also discusses tools and techniques employed at the edge to achieve these objectives while highlighting opportunities for further improvements. Overall, this review provides insights into the integration of blockchain and computer vision, advancements, challenges, and future directions in leveraging image and video data in a blockchain-enabled environment.

1. Introduction

Tamper proof and immutable record, safe and secure are features of distributed ledger technology revolutionizing not just cryptocurrency but also integrated to a multitude of fields that enable smart public security, smart health care, smart cities, and further intelligent systems (Drescher, 2020).

Due to the massive growth of new Internet of things devices (IoT) and sensors networks in almost all industries, catering to the need of the now, has caused a rapid rise in inter-connectivity (Shafique et al., 2020). Computer vision applications like surveillance, face recognition systems, fingerprint recognition systems, etc. has become part of this huge interconnected network of the internet of things (Patel and Thakkar, 2020). These devices, which are often controlled by a central station/authority, might be vulnerable in terms of security, privacy, and even counterfeiting (Zheng et al., 2018). A centralized control no matter how secure, with the multitude of encryption methods available can be easily hacked or corrupted by tampering at the control centre. A single failure without countermeasures may damage the whole system. The centralized system can be an easy point of entry to several security vulnerabilities justifying the requirement of a distributed, decentralized system (Sunyaev, 2020). Here we harness the advantages of the distributed ledger technology (DLT) called blockchain which provides a decentralized architecture for safety, privacy, and immutability (Sunyaev, 2020). Computer vision applications are enabled by cameras and sensors; images or videos are captured and then processed to make meaningful data based on the application. Intelligent and automated systems are facilitated by artificial intelligence (AI) (Hafiz et al., 2023). Machine learning and deep learning further subsets of AI have enabled better efficiency as well as exponentiated application scenarios in this discipline (Patel and Thakkar, 2020). However, the

[*] Corresponding author.

E-mail addresses: no1912348@qu.edu.qa (N. Ottakath), abdulla.alali@qu.edu.qa (A. Al-Ali), s_alali@qu.edu.qa (S. Al-Maadeed), elharrouss.omar@gmail.com (O. Elharrouss), amrm@qu.edu.qa (A. Mohamed).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.101801
Received 8 June 2023; Received in revised form 4 October 2023; Accepted 13 October 2023
Available online 18 October 2023

content captured is very sensitive in terms of privacy laws, theft of data, creating fake images or videos (Mayer and Stamm, 2020), spoofing (Kamble et al., 2020) among many other vulnerabilities. Numerous opportunities in identity management, indexing records, content management, privacy management, and several other applications can be accomplished through blockchain with image data. With no existing survey on computer vision applications with blockchain or vice versa, this review summarizes the applications of blockchain with computer vision and how it is used to solve the issues of privacy, security, and centralized control. This paper reviews the latest state of the art in detail, summarizes their applications, and categorizes them based on their main task.

The main contributions of this paper are:

- A comprehensive review of state-of-the-art applications of blockchain with computer vision.
- A review of applications of its architecture, components, limitations and implementation.
- Opportunities for future work and the most common trends in applications with computer vision are then presented based on analysing the limitations and opportunities.

The organization of the paper is as follows: Section 2 provides a background on blockchain and computer vision. Section 3 presents the methodology for article selection. Sections 4–7 review the state of the art in video surveillance, biometrics, video and image data sharing, and video integrity. Section 8 provides an overview of all the applications of blockchain with computer vision and the tools used for deployment, as well as some limitations and opportunities. Then we conclude the paper with key highlights of this survey and future direction.

2. Background

Distributed ledger technology (DLT) is a decentralized database that holds transactions between entities in a tamper-proof and immutable ledger, with each entity maintaining a transparent copy of the ledger (Hughes et al., 2019a). Blockchain is one such DLT that keeps a record of the transaction validated by several peers based on a consensus mechanism (Drescher, 2020). Bitcoin a type of blockchain that solved the double-spending problem in a paper authored by a pioneer with the pseudo name Nakamoto and Bitcoin (2008); it brought forth a new interest in this technology which led to a rise in applications from security, data storage, and privacy among many others. To cater to the different needs of applications and control over the network, the blockchain developed into public, private, and consortium blockchains (Andreev et al., 2018).

Due to the increasing use of blockchains in several applications, their requirements compared to conventional methods are usually questioned. Conventional methods or a centralized relational database model put their trust in a few or a single entity to secure the data. Blockchain is incorruptible, and since each peer of the network contains a copy of the ledger, trust need not be given to a single authority but rather to trustless peers with a complete ledger of the transaction, which may include any type of data secured on their drives (Peck, 2017). A blockchain system consists of a set of linked blocks that contain transaction data, a private key, a hash, and a nonce secured with a public key. Each block is linked to the previous block, which contains the hash value of the preceding block and a nonce. The time of the transaction is registered in each block. A block is added by validation through a consensus mechanism. A transaction in blockchain can have any kind of data stored, however, with limited capacity based on the type of blockchain platform used. The fact that a blockchain hash cannot be modified or changed and that it is cryptographically secured enables the property of security and trust. In addition to that, smart contracts can be deployed to automate, control access, and execute a contract or agreement. Smart contracts play a pivotal role in automated tasks in the blockchain. Automation through smart contracts improves processing speed, reduces cost, and forms a non-repudiated network, enabling the integrity of data to be kept safe (Abuhashim and Tan, 2020). This enables access control and contract enforcement (Mohanta et al., 2018), reduces risks, and cuts down on any third-party costs. With that comes better efficiency of the process involved (Cheng et al., 2018). This property makes it suitable for user control management, access control, or encryption, enabling applications like safe and secure data sharing, enforcement of automated contracts, etc. providing safety, security, and privacy for many diverse applications (Haiwu et al., 2018; Hughes et al., 2019b).

The blockchain can be classified based on its architecture and mode of access given for validation (Chowdhury et al., 2019). Public blockchain allows the creation and validation of blocks by the public. Modification of the data is performed using transactions. This creates a transparent and open access framework, raising privacy issues (Guegan, 2017). Private blockchain on the other hand is restricted, where only authorized parties are allowed to take part in the activities within the blockchain. This can be leveraged for computer vision use cases where unauthorized entities should not be able to access any transaction of activities thereby achieving security and privacy (Guegan, 2017). A consortium blockchain is a blockchain where the consensus mechanism is controlled by a pre-selected set of nodes. Several organizations can come together to form a consortium or a federated blockchain Sunyaev (2020).

With all these advantages, there are also drawbacks in terms of its security risks, computational costs, scalability, high energy consumption, integration with other systems and inter-operability with other blockchains, and so on. Careful planning needs to be done to choose the application area of blockchain and mitigate the risks involved. There is an inherent trade-off where you get an immutable, more secure, tamper-proof, timestamped record but with some modifications required for scalability, computational costs, and latency involved. Different types of blockchain solve different limitations such as off-chain storage for improving scalability, third-party applications for inter-operability, and so on. These trade-offs should be taken into consideration when designing an architecture for a specific application.

Pattern recognition, image processing, object identification, object recognition, and classification have been broadly termed computer vision problems. These tasks have applications in several industries from autonomous driving to robotics vision applications (Feng et al., 2019).

Recent developments in intelligent cameras (Rebecq et al., 2019), where the analytics and inference can be performed on embedded chips can be utilized for faster results. With the development of machine learning and deep learning techniques, particularly Convolutional Neural Networks (CNN), there has been a huge increase in the number of applications in computer vision that operate with image and video data.

The architecture of a computer vision setup usually involves an image capturing device and a device that performs the image processing. The image processing device performs the inference on the captured data (Gollapudi, 2019). This leads to networks of devices and layering of the hardware components. Fig. 1 illustrates a Wireless Sensor Network (WSN) (Peixoto and Costa, 2017) or Internet Of Things architecture where edge computing or fog computing is enabled (Shi et al., 2016). The things here are the capturing devices. Typically, the data processing and interface work on the edge. Cloud computing is required for storage and heavy computations which happens on the cloud layer. This necessitates the use of blockchain to safeguard the transfer of photographs and video, to safeguard the privacy with integrity during information transfer, and to enable authentication and authorization of access, to the information in these edge devices (García et al., 2017). Emerging opportunities in blockchain with computer vision, enhance many current applications from video surveillance to biometric identification.

The next few sections of this paper will detail the applications of computer vision with blockchain producing a review on the methodology, applications, tools used, and problems solved with some of the

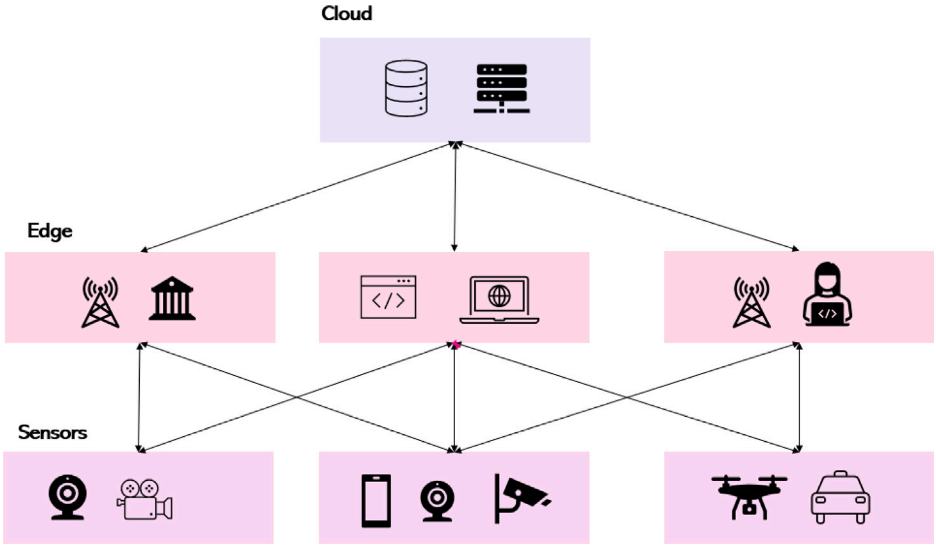

Fig. 1. Sensor network in surveillance systems.

limitations of those methods. With these, we can infer the guidelines for creating applications of Blockchain with Computer Vision. Section 3, is the methodology of the review which details the process applied for literature selection. Fig. 2 is an overview of the core applications discussed in this review. We review current trending applications that perform image and/or video processing that use blockchain such as Video surveillance systems being first in Section 4, was found to focus on security, content protection and providing access control to view and/or modify the video footage. Biometrics in Section 5 on the other hand focused on better feature extraction, multi modal biometrics and fusion methods for encryption of private keys in blockchain as well as storing biometric hashes in the blockchain enabling access control using identity management using authentication, and security. Video integrity were taken as point of focus in Section 6 where preservation of integrity of videos through identifying fake images and/or videos, archiving for preserving history and content verification was performed. Video and/or image sharing in Section 7 explores the state of art on secured sharing, medical image sharing and video streaming applications, functioning with a blockchain or distributed layer.

Many concepts and architectures are charted out, however there is need to implement this in practice. The evaluation metrics for each vary on the application, however there is a need for specificity for measuring performance. Nevertheless, it can be proved that images can be secured, users made accountable, time stamped and uneditable through use of blockchain. Most of the applications are based on public security where images or videos of people or property are bound by laws. Blockchain can now enable secure monitoring of these without the need to overcome these limitations in terms of access. Computer vision process can further be enhanced with distributed learning opportunities, secure encryption of training data as well as the trained weights. Sharing has become more secure and safe within limits of the privacy laws.

3. Methodology

The aim of this research is to identify applications related to computer vision and image processing using blockchain in several domains. For this purpose, the literature was surveyed on topics related to blockchain and possible applications such as video surveillance, biometrics, video integrity preservation and video/image sharing. Further survey was performed on how blockchain is involved in each and what are its advantages and limitations. To conduct this study prominent databases were surveyed, such as Scopus, IEEE explore, Google Scholar, and Web of Science. Duplicates in each were eliminated. Relevance to the study was examined from the selected literature and those inadequate were discarded. The main key terms used for this survey were ’Blockchain in computer vision’, ’Blockchain image processing’, ’Blockchain video surveillance’, ’Blockchain Biometrics’, ’Blockchain video integrity’, ’Blockchain content sharing’ e.t.c. The following flowchart in Fig. 3 summarizes the process.

4. Video surveillance systems

Surveillance and monitoring are essentials for any safe and secure community. It enables prevention of crimes as well as reduces the damage that may be caused due to late response. A perceptive view of the happenings in a surrounding can enhance the action taken (Tsakanikas and Dagiuklas, 2018). Smart surveillance through AI has achieved this objective (Sreenu and Durai, 2019). Cameras captures multitude of images that can be viewed and stored as well as accessed for future use. However, safety, privacy, and vulnerability caused by unauthorized access is a big concern.

In a typical surveillance system, multiple surveillance devices capture the videos. These videos are then processed on a single central server, or a control station. This forms an edge/fog network kind of architecture as illustrated in Fig. 1. The data is eventually stored in the cloud or sometimes even processed there. However, the Internet of things paradigm given to the multi-surveillance systems brings forth a lot of security and surveillance risks (Wang et al., 2019).

Centralized storage has a single point of entry which when infiltrated can cause sensitive and private image data to be accessed as well as tampered with (Mittal et al., 2020). Even though cryptographic mechanisms and security tools are available to share or store the data, any vulnerability in them can be taken advantage of, and can bring down the whole system resulting in the loss or damage of it. Blockchain provides a decentralized storage as well as mechanisms to control access to the stored information. Adding to that blockchain can safeguard privacy and keep away from tampering.

In the following section we review the applications of video surveillance system using blockchain for content protection, security and access control enabled systems.

4.1. Content protection

Video and image data that are captured, often is sensitive information. Content generated or captured need to be protected with respect to laws related to privacy and individual freedom of choice

Applications of Computer Vision with Block Chain
Video/Image Sharing
Video Integrity
Video Surveillance
Biometrics
Video/Image Sharing
Video Integrity
Video Surveillance
Video Surveillance
Biometrics
HOSPITAL
Library
LIBRARY
MUSEUM
SCHOOL

Write, secure video and image sharing, distributed learning, distributed video storage for video streaming.

Cataloguing videos for historical records in museums, combating fake through tamper proofed identity for cameras, saving video evidence for video forensics, content verification and validation.

Securing privacy, enhancing public security, and controlling access to stored data through distributed computing.

Single identity for security, access control, authentication and authorisation. Securing blockchain with biometric crypto keys.

Fig. 2. Overview of common computer vision applications with blockchain.

if the individual is not a significant party in the video. Unauthorized access and tampering of video/image are some of the major flaws in a centralized system. Available devices in a centralized system are not equipped to monitor and be selective within a wide range of coverage. A scheme to protect the content as well as privacy of those involved are the main focus in the following state of the art where blockchain is used to mitigate this. Some of the implementations also point out the requirement of a scalable and light weight blockchain Chauhan et al. (2018).

Video and/or image content can be protected by utilizing feature of the blockchain where modification is monitored as any transaction is time stamped. Fitwi et al. in Fitwi et al. (2019), used lightweight blockchain named Lib-Pri for privacy protection where tasks like checking integrity of the videos, blurring keys management, feature sharing and video access sanctioning was performed. Edge computing was performed for real time video analytics in this paper for identifying suspected individuals (Fitwi et al., 2019). Video is split into frames and a reverse chaotic mask is applied to images which is then stored in an off-blockchain storage. The suspected individual's facial features

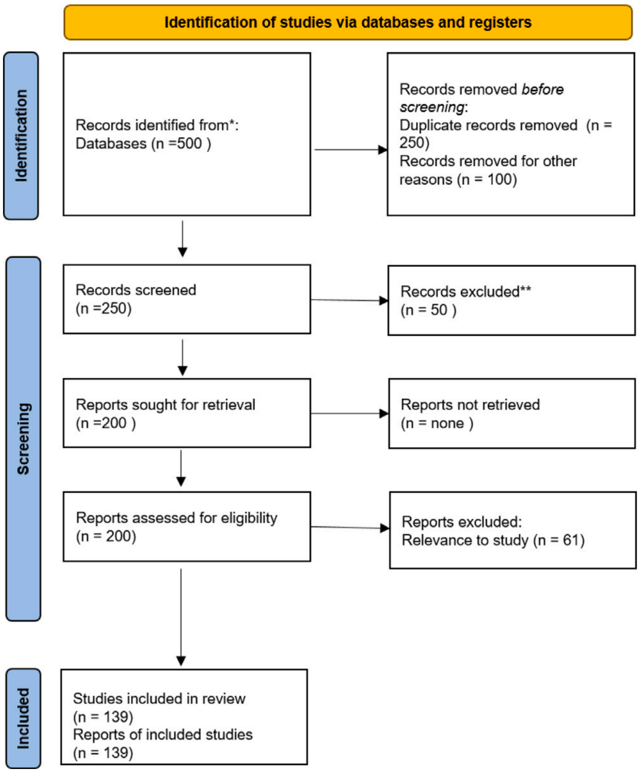
Identification of studies via databases and registers
Identification
Records identified from*:
Databases (n =500)
Records removed before screening:
Duplicate records removed (n = 250)
Records removed for other reasons (n = 100)
Screening
Records screened
(n =250)
Records excluded**
(n = 50)
Reports sought for retrieval
(n =200)
Reports not retrieved
(n = none)
Reports assessed for eligibility
(n = 200)
Reports excluded:
Relevance to study (n = 61)
Included
Studies included in review
(n = 139)
Reports of included studies
(n = 139)

Fig. 3. Article selection process.

are compared with the original and pushed to the blockchain node to identify the location and identity. Thus preserving the privacy of those involved.

In the same context, camera identity stored as transaction data on the blockchain was used to preserve the privacy of individuals in Gallo et al. (2018). The authors in paper designed Blocksee which is a video surveillance system in smart cities where vulnerability caused by malicious users manipulating the video content was solved. Camera identity enabled validation and immutability where camera settings were stored, which contained camera ownership details enabling privacy through blockchain. Preserving the camera details safe-guarded the content and enhanced privacy of the images captured by the owner of the camera. Further authorization to access to the images were also controlled in this process.

A case of privacy and security for a person of interest detected on camera in surveillance systems was taken into consideration by authors in Fitwi and Chen (2021). Video sharing was performed using a private permissioned blockchain authorized using smart contracts. Video frames were enciphered using a discrete cosine transform and advanced encryption mechanisms. This enhanced layered security enabled better security and privacy preservation along with access control.

4.2. Security

Security is the key factor in credibility of data generated and shared in surveillance systems. Blockchains provide a secure means of sharing and storing data through encryption and the use of hashing algorithms. Credibility of video content as well as its integrity are preserved.

Evidence gathering through footage stored in blockchain where its feature of timestamped storage and immutable record is taken advantage of in several applications. Video credibility was the point of focus in Liu et al. (2018) where the authors used Video-Chain which is a blockchain for video evidence storage. Video integrity evidence is saved on the blockchain. It follows a consortium blockchain, where the entities were given tokens based on privilege of access. The application layer of the video chain updates and verifies the evidence. A new data storage mechanism was built called Trusted Video Evidence Storage (TVES); it stores both evidence and original data (Liu et al., 2018). A high transaction rate protocol the VideoChain consensus protocol was used for validation. In the video processing part, the evidence was collected by cutting it 10 min apart and then compressed. A hash of the video was computed as evidence of video integrity. Reliability is thereby improved by adding backup to the original video. Analysed based on security and efficiency video chain proved to be a suitable option for implementation in real time.

A blockchain network was setup through several application domains such as, Unmanned Aerial Vehicle (UAV) and dam surveillance. It was utilized for security of data stored and accessed. The authors in Youssef et al. (2019) devised a secure IoT solution for dam surveillance where a distributed and long term security solution is accomplished through blockchain technology by providing authentication, data storage, integrity and traceability of data delivery through the UAV cloud. The performance was measured based on the data delivery ratio.

A real time surveillance requires not just video storage but also an intelligent and most relevant video frames or images to be stored which seemed to enhance the inference and fast action for surveillance applications. A combination of CNN, Inter-Planetary File Storage system (IPFS), edge computing and a permissioned blockchain was utilized for massive data storage, real-time monitoring and large scale information acquisition (Wang et al., 2019). Content oriented surveillance was accomplished by identifying dangerous individuals using sensors to identify malicious activity and tracking them after identification. Passive imaging and detecting concealed objects were performed and secured where data integrity was kept valid using blockchain (Qi et al., 2020).

Multilayered network is usually used with a private blockchain for secure surveillance in addition to a secure storage. The term IBSS(independent blockchain surveillance system) is introduced in Singh (2020) where high level layers formed the block chain layer in which the data is hashed and stored in an IPFS storage. The sensors (cameras) act as nodes to the blockchain where the video content is hashed and saved to the IPFS which is validated through a consensus mechanism. With the IPFS system, a secure large data storage was achieved with blockchain preserving privacy and security of the video data captured from the sensors. Authors in Nyaletey et al. (2019) used an IPFS system and to secure this peer to peer network a block chain is proposed.

4.3. Access control

Controlled access to the blockchain transaction secures privacy of the individuals as well as restricts the access to unauthorized individuals or organizations to use images or videos of entities not involved in the surveillance incident (Gallo et al., 2018; Fitwi and Chen, 2021). Jeong et al. in Jeong et al. (2019) surveys blockchain based management of surveillance systems and Deepak et al. (2020) surveys the use of hyperledger fabric (Vukolić), a type of private blockchain managed with IPFS and CDN in surveillance applications. In Islam and Shin (2019), to secure the data acquisition during an UAV surveillance, the data was stored in a blockchain at the mobile edge computing server.

Storing surveillance footage and controlling access can be performed by blockchain smart contracts. Bálint (2020) introduced a blockchain based system for storage of video footage where data was stored off-chain, where storj platform for storage was found to have an elaborate encryption method which secures the data along with storing it. Several types of decentralized storage were also compared in this paper for use as off-chain storage for blockchain. Nikouei et al. in Nikouei et al. (2018) identified the problem of collecting data at the edge along with feature extraction. The closest fog nodes then classify

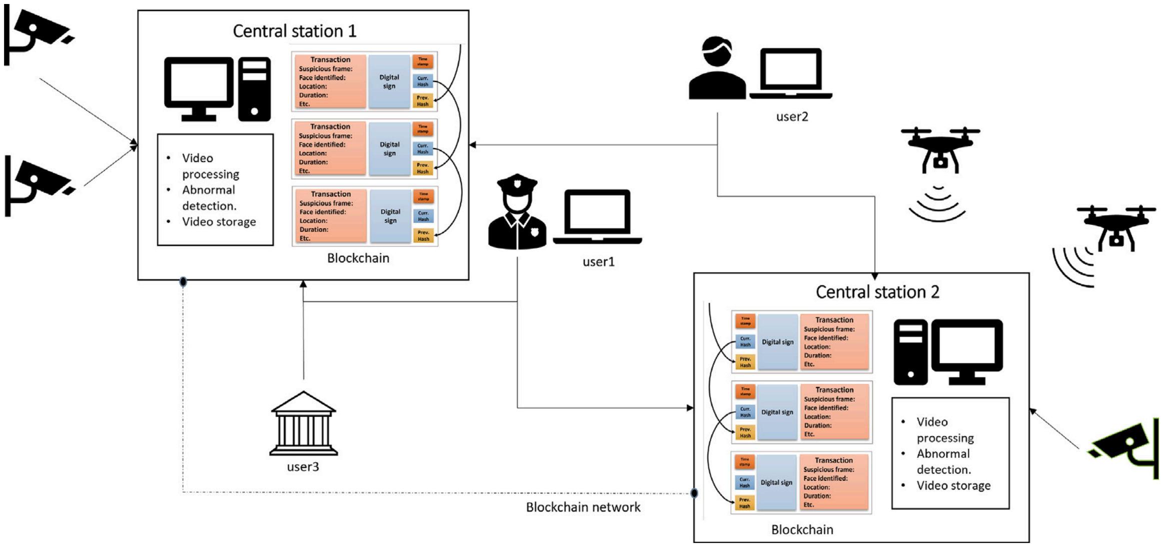

Fig. 4. Overview of surveillance system with blockchain.

the features. Misleading the surveillance system can be easily done at multiple layers where tampering can happen in the cloud system. A blockchain enabled scheme was applied to protect the index of the data stored at the cloud, at the edge and fog, to secure the data and smart contracts can be used to authorize access to that data.

Considering the requirements of a real time model, Singh et al. in Singh et al. (2020) created a lightweight mechanism named ODOB, which was used for surveillance with drones. ODOB decouples the block ledger from the block header to form a distributed architecture. Here each drone can access only their own block and this makes it simple, trustworthy, and lightweight. Another lightweight implementation of blockchain with surveillance was achieved in Michelin et al. (2020) where video metadata was stored on the blockchain to support video integrity. The Video metadata such as frame rate, video position sequence, video frame and Storage address was stored as transaction. The video was stored in a distributed storage system called IPFS. The setup of the device included a video camera module connected to a raspberry pi3 with IPFS storage running on a private instance. After evaluating for latency it was found to only take 8 ms for the whole process from capturing to storage in IPFS system. Thus achieving video integrity in surveillance.

Apart from the human aspect of suspicious behaviour, Farr et al. in Farr et al. (2020) used surveillance for autonomous detection of stolen car and inspections where a blockchain based platform was used for verification. To identify suspicious vehicles, camera feed was processed both remotely and locally. Verification of the suspected was achieved by blockchain validation system. Anomaly was determined by an open source licence plate recognition model—DeepANPR (Deep learning based Automatic number-plate recognition) using the SUN database for licence plate detection. Car recognition was achieved using a ResNet-152 architecture and trained using Cars dataset (Ke and Zhang, 2020). Once an anomaly was detected and verified a local authority can be alerted and published in the blockchain. This system ran at a fault free time of 40 s producing fast results (Farr et al., 2020).

With delay and latency taken into account, Al-Sahan et al. (2020) utilized hyperledger fabric as a private permissioned blockchain for public security. Access control was accomplished through chain code or smart contract. Machine learning and blockchain were combined in this method where real time surveillance was used to identify and track suspected faces. Here the latency was used as evaluation metric to identify its effectiveness in reporting a suspect. Surveillance events were notified and embedded on to the permissioned blockchain, specifically hyperledger fabric which further enabled access control through smart contracts or chain codes in this application. Scalability was achieved due to the consortium architecture. Real-time suspect monitoring was achieved successfully with minimal delay. Access control through smart contract enables restricted access to private and confidential information shared through different organization with integrity and confidentiality.

4.4. Discussion of video surveillance systems

With safety and security preserved on the blockchain for surveillance and with a general overview of the systems used, Fig. 4, illustrates a general architecture of block chain in surveillance. The video surveillance system can be part of an edge network or sensor network. The sensor data (video and/or image captured) is typically stored in a central station at the edge of a wireless sensor network for further processing which can be treated as a blockchain node (Nagothu et al., 2018). Fig. 5 contains the key components in the surveillance system with blockchain with a modular architecture of a blockchain based system.

The Central station where the image and/or video processing is done can be considered as nodes to the blockchain network which stores the video hashes either as a transaction or onto a secure blockchain based storage such as IPFS (Nyaletey et al., 2019). Most surveillance systems were found to be private or consortium blockchain to control access. Access can be coded with a smart contract restricting access to different users of the system enabling privacy for the required parties. Thus blockchain enables security, safety and privacy (Destefanis et al., 2018).

As with every application in blockchain, tamper proof record and immutable record is guaranteed. The surveillance system is prone to many video integrity and privacy issues that can be solved by blockchain. Access control which can be programmed through smart contracts using private and consortium model blockchains can enhance privacy of those involved. Smart contracts were applied to the block chain for controlling the image retrieval or viewing capability of different entities enabling privacy and security of the video data. They were programmed to validate or to verify the authority of the entities in the blockchain for image and/or video viewing and image and/or video retrieval. Encryption of the videos used in surveillance further improves safety of the videos.

Table 1, lists out the existing literature on video surveillance system with blockchain, The use of each are listed with the computer vision problem solved and the type of blockchain used to secure and provide privacy and access control.

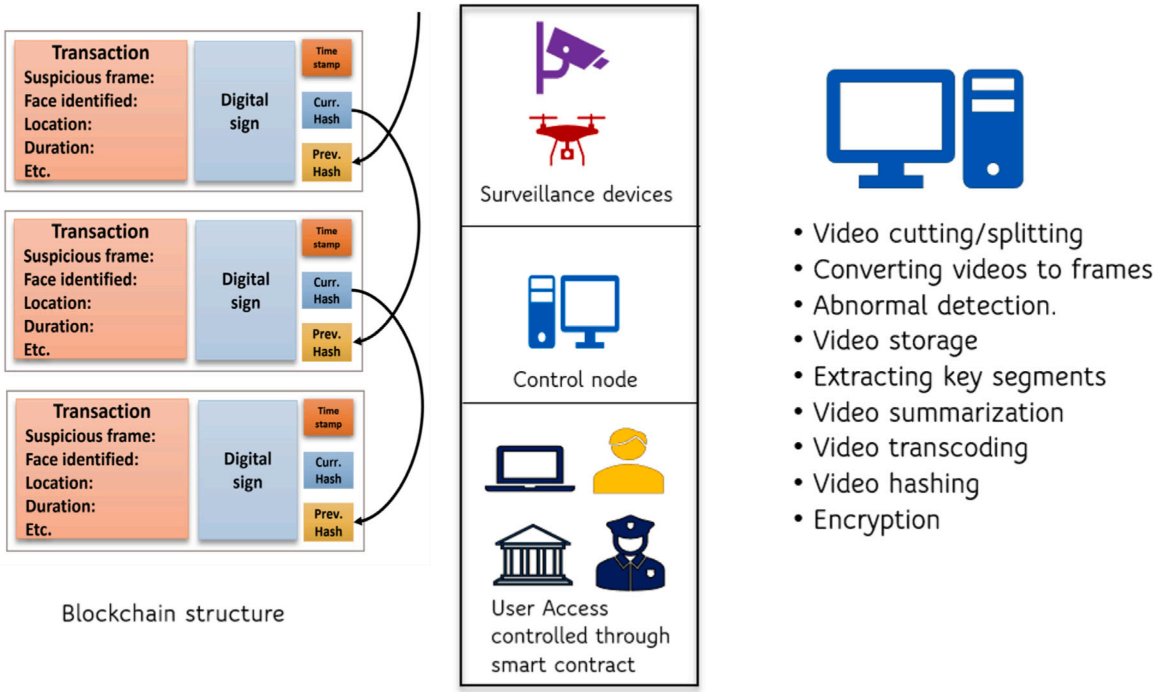

Fig. 5. The key components of the blockchain system with video surveillance including the modified blockchain structure, the infrastructure and the image/video processing involved.

It can be clearly noted that most of the applications that were integrated for national security and general suspicious activity or object identification, used a consortium blockchain or private permissioned blockchain. Here access control is administered using smart contract. Image processing or video processing tasks are mostly done independent of the blockchain at a separate layer. Blockchain is used to provide privacy, security and with that, access control to the already processed or stored data. Most applications, stored the video data on distributed storage systems such as Storj and IPFS. On other hand, lightweight applications hashed metadata and in some cases video frame of interest, and stored as transaction on the blockchain. This resulted in an efficient blockchain system with lesser latency compared to others as on-chain storage was enabled.

The limitations of the blockchain mimic the limitation of blockchain with surveillance. Scalability issues, storage issues, cost depending on type of blockchain, are some of the limitations of blockchain Wang et al. (2019). The efficiency of most video surveillance models rely on real time processing. Latency is vital for this role. With a centralized system and single storage multiple access system, latency can be improved risking privacy and security. However, the sensitivity of the applications reiterates the need for blockchain. The question arises, can the blockchain model be enhanced for latency through modification of the block. Some states of arts have brought forth modification of the blockchain block. How far can the model be modified so that there is significant change in latency and transaction time with the amount of data that is to be stored and processed. Edge computing and storing data on the edge as a node of the blockchain is still a research direction in its prime.

5. Biometrics

Biometrics is a person's unique identity; numerous elements of a person, such as their physical and, in some situations, behavioural identities, can be unique, allowing a person to be identified and recognized (Jain et al., 2007). Biometrics has its applications in several fields which involve identity management, public security and other applications that need an unique identifier using human biological features (Bolle et al., 2013). A biometric system typically consists of a biometric device used to extract the biometric features of a person that are unique like that of physical features as well as behavioural features of a person (Jain et al., 2011). These features are used as templates then matched during the process for authentication or verification tasks. The physical features of a person may include, face, palm, iris, finger print and hand veins whereas the behavioural features may include the gait, voice, signature, key stroke dynamics etc. of a person (Zhang et al., 2011; Elharrouss et al., 2020; Jain et al., 2011).

The following section details the applications of biometrics with blockchain with security and access control as the main point of focus.

5.1. Security

Like any image, biometric images can be modified and meddled with, thus it needs to be secure. Biometrics like iris and fingerprint can undergo spoofing attacks (Hadid et al., 2015). The risks involved in biometric can even lead to fake identities, thefts, impersonations and frauds. Using blockchain with biometrics for several applications, provide that integrity by having an immutable and trustable record. A biometric authentication system that is traditionally centralized, may be prone to attack and can extract information to steal identities of people. Most systems involve third party identity providers. They broker authentication protocols which is one of the main vulnerabilities leading to loss of personal information and biometric data (Jain et al., 2008).

Authors in Reddy et al. (2020) extracted face and body expressions using a 3D CNN algorithm, which were stored in blockchain called BigchainDB which is a blockchain for big data. Information extraction was performed by detecting the faces, recognizing faces and object re-identification. 3D CNN used here improved the identification of moving objects where spatial and temporal features were both determined from the video surveillance system. Face and body expression features were extracted from a pre-processed video sequence. These feature containing objects (person of interest) were then tracked and the behaviour of the person of interest's gestures are identified. These features if relevant were hashed and stored in the blocks as transaction data which also

Table 1
Video surveillance system with blockchain applications.

Method	Application	Technique	Blockchain type	Simulation	Smart contract	Limitations
Al-Sahan et al. (2020)	National security	Suspicious face detection	Consortium	Hyperledger	Yes	Camera has to be at a fixed angle to capture frontal face images. System requires security testing. Scalability issues
Youssef et al. (2019)	UAV based Dam surveillance	Fault detection	Hybrid	Bitcoin	No	Highly complex system with proof of Work consensus which causes high energy consumption
Fitwi et al. (2019)	Identification of suspicious activity, detection and recognition	Frame splitting , Object	Private	lite-federated blockchain	Yes	off-chain storage vulnerabilities
Farr et al. (2020)	Vehicle detection	Licence plate and car recognition	Public	Modified block	No	Miners are and uses a cloud based DMV)
Qi et al. (2020)	Multi-surveillance sensors	Person identification and tracking, object detection	–	–	Yes	Blockchain end to end evaluation is not provided
Wang et al. (2019)	Suspect identification	Monitoring using CNN	Private	Permissioned	Yes	Scalability and security is not tested
Singh (2020)	Multi-surveillance network	Video storage	Private	Permissioned	Yes	Requires off-chain storage, cost and scalability is not measured
Michelin et al. (2020)	Person surveillance and forensics	Video streaming and splitting	Private	Speedy Chain	–	Requires off-chain storage
Liu et al. (2018)	Video evidence gathering	Integrity	Private	videochain	Yes	Not considered processing requirements of the video
Lopes et al. (2019)	Robot monitoring	Person identification	Consortium	Robot chain	Yes	Complexity analysis of the face recognition is required
Gallo et al. (2018)	Smart city monitoring	Segmentation and feature extraction	Private	Permissioned	Yes	scalability of the approach is not analysed
Nagothu et al. (2018)	Smart surveillance	micro-service architecture	Private	Permissioned	yes	Security measures and computational overhead is not discussed
Islam and Kundu (2018)	Indoor surveillance IP cam	Preserving privacy	Public	–	Yes	Evaluation of the system is not performed
Lee and Park (2020)	CCTV surveillance	Preserving privacy	–	–	–	Transaction speed and size required to be quantified for merkle tree approach
Bálint (2020)	Video footage	Encryption or hashing of video footage	–	–	–	Employs complex consensus mechanisms such as proof of work and proof of stake
Fitwi and Chen (2021)	video storage	Preserving privacy and security	Private	Permissioned	Yes	Requires evaluation of transaction time while network scales

contains the timestamp as well as the location of incident. A chain of blocks was formed with several blocks containing these features (Reddy et al., 2020).

In the blockchain network a separate copy of each transaction is kept and each block contains the block of the previous. This makes it harder for any tampering of data by unauthorized personnel. And so the face and gesture information is secured in the blockchain. Proof of work (PoW) was identified as the preferred consensus mechanism where the nodes in the blockchain, compete to find a nonce value in the blockchain to produce a hash value. The node that finds the hash value creates a block which was approved by the consensus which accepts the biggest chain with largest total problem increasing the blockchain network. The BigchainDB here is a distributed database which incorporates all features of a typical blockchain where data can be stored both off-chain and on-chain McConaghy et al. (2016) .

Self-sovereign identity is a concept that brings privacy and security in identity management in the decentralized systems. The users are responsible for their own identity data. Blockchain technology is employed in this system to establish a web of trust, creating a resilient and secure storage environment for identity information. This information is stored in the blockchain, eliminating the need for a vulnerable central database susceptible to hacking. The identity is stored in blocks which accumulates the transactions created by many devices. In Othman et al., A horcrux protocol, a decentralized authentication method for self-sovereignty of identification using biometric credentials, eliminates the need of third party identity providers for authentication in blockchain technologies (Othman and Callahan, 2018).

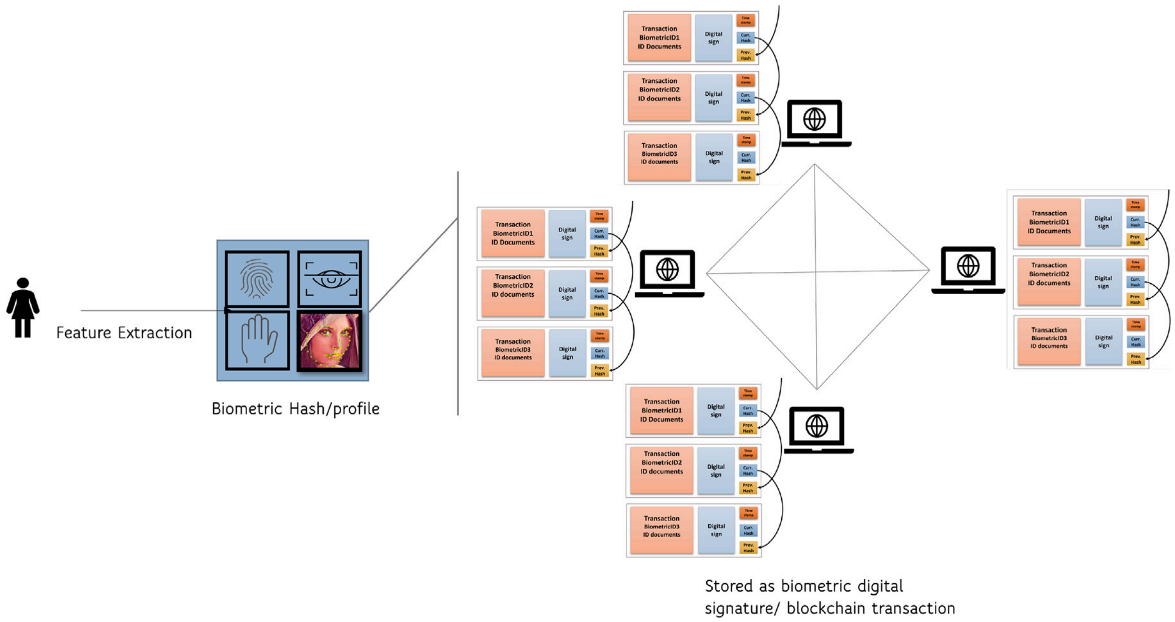
Feature Extraction
Biometric Hash/profile
Transaction BiometricID1 ID Documents
Transaction BiometricID2 ID documents
Transaction BiometricID3 ID documents
Digital sign
Time stamp
Curr. Hash
Prev. Hash
Stored as biometric digital signature/ blockchain transaction

Fig. 6. Typical biometric blockchain architecture for identity security with three nodes as peers of a blockchain network. Biometric hash is stored in each peer as a block transaction.

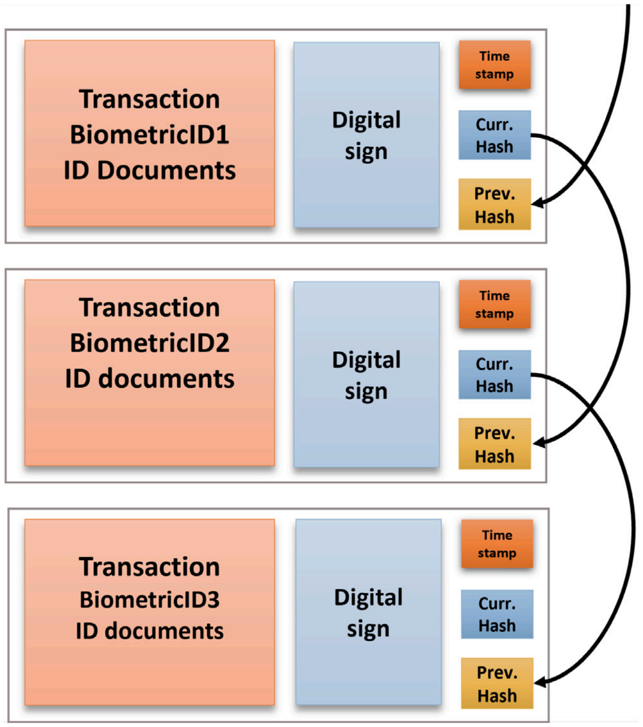

Fig. 7. The block structure of a modified block for blockchain system with biometrics and vice versa along with common biometric profiles used with blockchain in state of art.

The horcrux protocol is a protocol that works with the 2410-2017 biometric open protocol standard (BOPS) (Othman and Callahan, 2018) which contains a client device, a trusted BOPS server, and an intrusion detection system for biometrics systems. BOPS can be a single or multi-distribution model having a secret scheme. The multi-distribution scheme enables the storage of biometric data, which can be accessed through verification using the Horcrux protocol and a biometric authentication process. The data was divided into n templates using a secret scheme which are then stored using a multi-distribution scheme. Blockchain was then utilized to store the reference of the decentralized storage. This scheme allows portability, inter-operability and protection with that self-sovereignty over a persons own biometric information. Full control can be achieved by the owner to perform tasks such as editing, modifying and providing access.

Encryption techniques are prevalent in biometric security. Iovane et al. in Iovane et al. (2018) presented an encryption system using information fusion with face biometrics and prime numbers for public key cryptography and face biometrics for digital currency exchanges. The fusion was performed using a face information fusion algorithm (FIF) also called bio-hashing. This process is employed in several non-blockchain applications like palm hash, digital finger prints and face fusion which are later fused with pseudo random codes (Lumini and Nanni, 2006). Here face recognition and finger print recognition was the main technique used. Smart contracts were employed in blockchain as self executing contracts and rely on the users in the peer to peer system. An authentication system is required for the purpose of identification of the user especially in a private blockchain like the hyperledger.

Storing biometric templates in a blockchain was presented in Delgado-Mohatar et al. (2019), where face and hand written signatures were stored after merkle hashing. The face and hand written features were extracted from a pretrained model. Ethereum architecture equipped with smart contracts developed in solidity was used for this purpose. Delgado et al. experimented on several techniques in blockchain storage such as direct and hash based. It was identified that merkle tree hashing was more efficient in terms of cost performance trade-off.

Biometric for security can be elaborately used for several applications. Mohsin et al. in Mohsin et al. (2019) used a hybrid, biometric, steganography, blockchain model to secure medical data. Steganography is the process of hiding data inside another data (Hassaballah et al., 2020a; Hameed et al., 2023; Hassaballah et al., 2020b, 2018; Hameed et al., 2023). Finger vein (FV) biometrics which is contactless biometrics system can be applied for access control, authentication and electronic passport application. The finger vein extraction technique works by acquiring data through contactless means such as infra-red imaging. This image data is processed, and then matched to existing finger vein database for person identification. A verification framework for patient authentication was designed and implemented for the information transfer between the access point and the database where the information is stored.

A combination of RFID and FV biometric was used using a merge algorithm to create a hybrid biometric pattern model which increased randomization and security. Then a combination of blockchain, steganography, encryption and blockchain was used for transporting the biometric data from image acquisition side to the database. After hybrid and random binary patterns were generated by merging, the features were stored on the blockchain with particle swarm optimization (PSO), steganography and advanced encryption technique (AES) encryption. The node of the blockchain contains an immutable copy of the data with a ledger of user hash. While any user access to a patients documents is required to be authenticated, reverse of all the procedures can also be performed. This architecture was impervious to brute force attack as well as spoofing attacks, providing, confidentiality and integrity. This entire system provides comprehensive security measures, successfully meeting all security requirements.

5.2. Authentication

For public services, security of national identity is essential, which is a record of a persons biometrics along with other fundamental details of the person. Access to sensitive information needs authentication and cannot be shared publicly without the required permissions. Blockchain provides secure universal access to biometric information for identity management for public security and public services (Jacobovitz, 2016). Blockchain is used in Mudliar et al. (2018) to decentralize the current centralized system for security and transparency for voting applications. A smart contract was used here to input the data; validated and extracted data is then stored in blockchain. This information can be viewed by multiple governmental entities and can be used for several applications like voting identity as performed by authors in Garg et al. (2019).

Breeder documents being a personal profile document containing all essential information about a person are used for authenticating identity of an individual and their credentials. Authors in Buchmann et al. (2017) stored breeder document and electronic travel documents in a decentralized bitcoin blockchain. Breeder documents with biometric information was converted into bar-coded information and with that personal information was integrated onto a barcode or a chip. This was added on to the documents like birth certificate and national ID. These documents were further stored on to the blockchain as a transaction. With the use of image compression on iris and fingerprint images as identifiers, there is significant reduction in the storage space when stored onto a stacked 2D barcode. This efficiently identifies and secures the documents. Biometrics embedded with the breeder document provides enhanced recognition and authentication. This authentication system enables secured access control.

A multi-modal biometric authentication system was another technique for this purpose which is incorporated in the blockchain Sawant and Bharadi (2020). Sawant et al. suggested a fused iris and face for biometric identification. A CNN architecture was used for classifying apart from that fusion can be performed by a fully connected layer with input from CNN layer which extracts the required features. This was planned to be used as a cloud based software. Hyperledger fabric architecture was suggested for a execute-order-validate architecture which also enables use of smart contracts namely chaincodes. Authentication was achieved by the biometric SaaS (software as a service application) containing biometric template. The authenticated peer (node) was then allowed to perform transactions based on a consensus in the permissioned blockchain.

Another method for implementing secret keys for blockchains is using biometric fuzzy systems (Naganuma et al., 2020). Management of secret key was used for authenticating the user and the cryptographic digital signature, using biometrics based digital signature scheme. A secret key was generated from users' biometric and then erased after it was used. The keys were thus not saved enhancing safety of the key. Here the risk of loss of key can be reduced. The overhead was found to be reasonable in this architecture. However, automatic transactions such as smart contracts were not supported in this implementation. Immigration and border control are applications where biometric with blockchain can be used as stated by Patel et al. in Patel et al. (2018). Gateless entry was achieved with hyperledger fabric architecture. The decentralized architecture offers security and privacy by enabling control over document access, determining who has permission to access the documents. Biometric storage can be safeguarded by this approach.

Several encryption techniques were used to improve the safety and security of the biometric information. Toutara et al. in Toutara and Spathoulas (2020) presented a biometric authentication scheme for blockchain where the data from sensors once acquired was homomorphically encrypted, transformed and then uploaded on to a IPFS system. The smart contract also stores the address of the files in IPFS. This was further connected to the Ethereum address of the user. Ethereum /IPFS combination was used to achieve privacy as well as security of biometric template. The user additionally saves an encrypted copy of the transformation parameters and the pair of encryption keys for the template. This mechanism goes through a registration phase where the biometric data was acquired and stored. After the registration phase, authentication can be performed against a third party service through his/her biometric data. In their experimentation, Toutara et al. observed that they achieved minimal time overhead.

5.3. Discussion of biometrics

Biometrics being a unique identification in itself has achieved security, however prone to spoofing and theft, blockchain acts as an added security to any system. With several modes of use of biometrics with blockchain from managing identities to authentication and cryptography, decentralized systems, safety, and security through biometrics can be achieved.

Fig. 6 and Fig. 7, describes a general architecture of biometric storage with blockchain identity with key components of this blockchain network. Uni-modal or multi-modal biometric data can be stored as a key alone. It can also be fused with numerology using encrypting methods. Biometric hash can be stored on the blockchain system as transactions. The biometric key can also serve as a digital signature.

Table 2, tabulates the applications of biometrics in literature with type of biometric used with computer vision techniques used to extract the biometric features for creating template. The most common biometric scheme used was multi-modal biometrics. Iris images coupled with fingerprint was the most popular form of biometric. Smart contract is deployed for access control as well as authentication in most of the applications.

Biometrics added authenticity to the blockchain network when used as an encryption method or as digital signature. It enhanced the security of the blockchain when used as an access key or public key. Its use as identity management, made a reliable person identification and recognition system. Security to the biometric templates was enhanced when template was stored in the blockchain. Several applications related to national identity, national security, voters identification, identity documents are main focus for biometrics with blockchain application.

Finger vein authentication scheme was the most notable of the available approaches for patient document security where the data was encrypted by merge algorithm and re-encrypted using steganography and Advanced Encryption standard (AES) which then was stored on the blockchain. This technique was most efficient against known threats as well as for identity management and integrity of the data even though multiple phases were required to achieve this. However efficient in security and safety, it may result in high computational cost and time. There is a trade-off between security and performance overhead

Table 2
Biometrics with blockchain application.

Method	Application	Biometric type	Technique	Blockchain type	Validation	Smart contract	Limitations
Mudliar et al. (2018)	National Identity	Multi-modal biometrics	Feature extraction, Biometric recognition	Public	Ethereum	No	Privacy, Many legal formalities, interoperability, implementation complexity and infrastructure is not considered, cost.
Buchmann et al. (2017)	Securing identities	Iris and Fingerprint	Compression of biometrics, stored as 2D barcodes	Public	Bitcoin	No	Bitcoin consensus mechanisms complexity, interoperability, scalability, cost
Iovane et al. (2018)	Encryption	Iris	JDL method to fuse prime numbers and biometric data	Public	–	Yes	Time complexity will add to the latency of the end to end system
Sawant and Bharadi (2020)	Biometric Authentication	Multi-modal Biometrics	Fusion of multi-biometric, VGG16 on fused features for classification	Consortium	Fabric	Yes	Storage limitation and control within a few organizations, Not network fault-tolerant
Naganuma et al. (2020)	Digital	Multi-modal Biometrics signature	Features extraction	Consortium	Fabric	No	Storage limitation and control within a few organizations
Li (2020)	Distributing	Fingerprint images	Finger print chaotic image encryption	–	–	–	Storage constraints and scalability
Delgado-Mohatar et al. (2019)	Template storage	Face and hand images	VGG-face pretrained written signature	–	Ethereum	Yes	Transparency and accessibility of information to all participants, cost and performance trade-off
Toutara and Spathoulas (2020)	Authentication	Any biometric	Extract data from sensor, apply homomorphic encryption	Public	–	Yes	Limitations of storage with respect to scalability

of multi-modal biometrics with blockchain where several steps are involved in a transaction being processed such as hashing, encryption, consensus mechanism, miner validation among a few.

The use of multi-modal biometrics and fusion techniques may increase the overhead of the overall system. Storage capacity may increase with multi-modal systems, along with complex encryption techniques increasing computational complexity. This although secure may need high processing power. There lies a trade-off which needs to be addressed based on the priority of the requirements of the applications it is eventually utilized for. A standardized wholesome model for an optimum biometric system need to be determined for a safe and secure performance withstanding faults like that of spoof attacks and template ageing without the complex computation.

6. Video integrity

One of the most striking properties of blockchain is data integrity as it is uneditable and time is stamped upon transaction creation (Drescher, 2020). This enables the data to be trustable leading to many applications in combating fake videos and/or images, cataloguing images for history as well as collecting non tampered evidence. The following section details the current literature in video integrity preservation for videos and images including the processing of the images prior to blockchain layer.

6.1. Combating fake videos

Fake videos being a major cause of concern in the current era, Hasan et al. in Hasan and Salah (2019) used blockchain with which history tracking and provenance of videos were safeguarded. The history of digital content was traced and tracked using Ethereum smart contracts. This approach utilized the Ethereum blockchain to provide a decentralized proof of authenticity. IPFS storage, Ethereum name service(ENS) and a reputation system were the main components of this system. The new source and the artist create the smart contracts. The metadata requires the artist's Ethereum address as well as the smart contract address. This information with video content were stored in an IPFS storage which generates a unique hash, addressing the files that contain the video on the distributed storage.

Smart contract embedded in the Ethereum blockchain contains access functions to edit, share and distribute based on the terms and conditions which was authored by the digital art creators. Any edited video of the original video was named as a child video which were added on to a list in the smart contract. Thereby enabling tracing of the edited version of the videos.

The Ethereum address of an artist and his/her real identity are correlated with an ENS service, where the artists name, company and profile matched to their Ethereum address were stored in a decentralized fashion. In addition, off-chain resources can be utilized where Ethereum address of a video and the owner can be linked. Artists reputation can also be tracked using a decentralized reputation system. The profile of the video creator was linked to this system which enabled reputation to be quantified. Smart contracts are used to add reviews and comments and was then stored onto a decentralized storage system. With these feature set, video provenance was secured as well as its value was calculated based on a reputation system enabling a solution for wholesome integrity protection.

Upon evaluation of this system, it was found that the cost changes with the changes in smart contract. Each function executed in the blockchain has a cost, which includes, transaction and execution charged as gas currency in Ethereum. The security of this system encompasses the integrity, accountability, authorization, availability and non repudiation thus making it resilient against several attacks like Man in the middle, replay and DDoS attacks.

A similar approach to identifying manipulated videos were by leveraging the uniqueness produced while hashing. Dhiran et al. used this feature where their features were hashed using cryptographic algorithms like MD5 and AES and video was stored in the hashed format. Once the tampered video was uploaded a modified hash was generated. This can be used to detect a video's authenticity (Dhiran et al., 2020).

Like Dhiran et al. and Hasan et al., hashing was performed on the video by Yatskiv et al. in Yatskiv et al. (2019). Video integrity can be preserved by protecting the video from unauthorized changes with this approach. Here the hash function of each video frame was computed rather than the incident video frame, the hash sum of the first video frame and the second video frame was consequently added up to get hash function. Further this hash was added onto the hash of the next video frame and so on to form a blockchain transaction. Video file processing was performed using ffmpeg where video and audio materials are packaged into container formats. As the hashes are dependent on the previous hash function, modification of a frame will change the hash sum which will detect any tampering in the video frames. This was evaluated on time spent to generate the hash, which was found to be proportional to video resolution and the number of frames selected.

With the emergence of false news on the internet, Chen et al. in Chen et al. (2020a) proposed an incentive-aware blockchain-based solution based on smart contracts and a consensus algorithm tailored for authority verification. They not only focused on images but also a combination of types of media involved. This was a preventive approach to fake news propaganda. The customized algorithm used in this approach used a form of dynamic weighted ranking evaluation score. Integrity and location privacy while sharing dash cam videos were taken as a matter of concern pointed out by authors in Kim et al. (2020). An automatic dash-cam sharing system was accomplished using deep learning and smart contracts, where the encryption of the accident location was performed with that maintaining the location privacy. Deep learning was used to choose and select the accident videos, and share only necessary information. To improve accuracy, audio and image data training was performed together. This not only improved the integrity of the video but also integrity of the accident report.

6.2. Video cataloguing

Preserving history through video archives is one of the applications that blockchain can be used for its uneditable and time stamped feature. This data not only catalogued and verified but also secured with hashes on the blockchain. Striking example of one of its use is in Bui et al. where an international record of historical videos were preserved using blockchain through collaboration between several countries.

Bui et al. in Bui et al. (2019) designed ARCHANGEL for preserving integrity of digital video fusing computer vision and blockchain. A deep network architecture was implemented using a hierarchical attention auto encoder for computing the temporal content hashes (TCH) for the video content. The TCH's are secured using a proof of authority blockchain. This was distributed across multiple archives. The application was used to safe-guard against modification of content that includes frame truncation or corruption when format shifting occurs. To ensure future accessibility, format shift was done on the videos. Therefore the original video was transcoded and then compressed using ffmpeg. The processing happens in such a way that given an input video, its TCH generates hashing in each block, from audio and visual content. These hashes were then stored on the blockchain which is immutable and tamper proof.

Integrity verification was done using the TCHs, SHA-256 hashes and threshold values set, which are stored in a SIP, then stored in a blockchain as a smart contract transaction. The smart contract manages the access of the data. User access was validated through smart contract using API's. The transaction was processed and verified with the data stored on the chain. Here Proof of work mining was not required which is computationally expensive thus reducing the computational overhead due to mining.

Video captured from a streaming IoT device was used for video forensics where hash of video frames were sent and stored on nodes of permissioned blockchain in Danko et al. (2019). Connection between the video and storage device was established using TCP based tool. In terms of the video quality, resolution of videos were a major concern. Moderate resolution videos could only be implemented and there was a need for further investigation into higher resolution images. Hyperledger fabric was used as the blockchain platform which is a permissioned blockchain. The access was restricted to stakeholders utilizing chaincode, smart contracts for hyperledger blockchain.

6.3. Content verification

Several implementations like that of Cremona et al. (2019), Chen et al. (2020a), Yatskiv et al. (2019), Hasan and Salah (2019), Dhiran et al. (2020) and Bui et al. (2019) used content verification apart from identifying fake images, video evidence or cataloguing and preserving videos.

With the amount of data prevalent, there is a inherent task to verify and analyse them. Video content is very abundant; available on several devices like mobile phones, tablets, Personal Computers (PCs), Closed Circuit TV (CCTV) etc. which are equipped with cameras. Authors in Zelensky et al. (2018), stressed the need for video content verification where the need for data confirmation was a necessity at several public security as well as governmental institutions. A swype code was used to detect the movement of the camera which was utilized for verification along with other sensor data of the device. A decentralized application was implemented named PROVER app where it was initiated when camera was turned ON. Ethereum platform was used with smart contract enabled for verification.

In order to safeguard video integrity and content verification, several parts of the video surveillance system can be utilized. Authors in Kerr et al. (2018) used a combination of blockchain and a digital watermarking application to secure video evidence. A prototype camera was used where it takes part in the creation of blockchain in real time. End to end protection of video evidence was achieved. Digital watermarks were embedded on to the video prior to transmission. A communication system was introduced between the devices and the blockchain nodes which provides a reliable queuing system. This allows a scalable and adaptive infrastructure for this system. A video management system coupled with blockchain enables proper content verification with the digitally water marked images.

6.4. Discussion of video integrity applications

Video integrity applications require a tamper proof and time stamped record enabled by blockchain and specifically automated unedited smart contracts. Consensus mechanism were used to verify images and further voted out if fake. Video forensics, content verification, content filtering, history preservation through cataloguing were solutions to preserving video integrity. In terms of public blockchain, transparency was enabled as all the nodes participating had a copy of the ledger. Private blockchain enabled a private network where only specified participants were allowed through a core validator. Commonly used blockchain was permissioned blockchain where the participant need to be verified to take part in the transaction.

Table 3, tabulates the applications in which video integrity preservation is one of the main gains. As noted from the tables, Video content processing mostly dealt with the hashing the video and then storing it as a transaction in blockchain. Watermarking was the procedure used in state of the art to identify cameras and verify the content. Blockchain was modified in some instances to cater to the storage requirements

Table 3
Video/image sharing with blockchain.

Method	Application	Technique	Blockchain type	Smart contract	Main storage	Limitations
Kumar et al. (2021)	Image sharing	RCNN training with CT images	Ethereum	Yes	IPFS	Cost of transaction, limited capacity, Non Upgradeable smart contracts
Zerka et al. (2020)	Privacy	Encryption of the trained weights using Radiomics dataset	Ethereum	Yes	Cloud archive	Cost of transaction, centralization due to cloud, interoperability between institutions, Non Upgradeable smart contracts
Tang et al. (2018)	Storage	Denying fake medical image share	Ethereum	Yes	–	Cost of transaction, interoperability between institutions, Non Upgradeable smart contracts, limited capacity
Shen et al. (2019)	Image retrieval	Extraction of medical image features and encrypted data storage	–	Yes	On-chain	Scalability-transaction time increases with number of images, Non Upgradeable smart contracts
Mehta et al. (2019)	Copyright protection	Stock photos, P2P sharing	Ethereum	Yes	IPFS	Time complexity increases with number of images, cost, Non Upgradeable smart contracts
Esmaili and Javidan (2020)	Copyright protection	Video sharing systems	Ethereum	Yes	Swarm	Time complexity increases with number of images, Storage costs, Non Upgradeable smart contracts, infrastructure requirement
Xu et al. (2019)	Data sharing with access control	Micro-services	Ethereum	Yes	Database	Incomplete decentralization, Complexity, performance overhead in terms of latency, edge and fog computing challenges

and security demands to safeguard integrity. The most common type of blockchain used here was Ethereum and some efficiently used smart contracts and chain codes to restrict access or automate the verification process. The flaw in most of the applications is that they require high computational resources and are expensive in terms of monetary costs based on the type of blockchain used, as each smart contract execution is considered a transaction. There are multiple steps involved including, transaction validation, authentication and authorization with consensus execution if any, adding to that the computer vision tasks that are performed, eventually having high latency. For a real time process, there is need for a study on light weight, low latency techniques. Watermarking, hashing and storage in a third party storage, adds on to the processing time. Nevertheless, it has been observed that the majority of applications are effective in ensuring data integrity. However, the issue of data reliability and availability remains a concern in this context

With latency, real time data may not be available at required speed thereby time, however integrity of the data received even though late can be reliable due to blockchain protection. There is a requirement to boost the efficiency in terms of reliability and availability in achieving an optimum model for video integrity.

7. Video/image sharing

Content creation through videos and images have seen a boom in need due to the different video and image sharing platforms like Youtube, Netflix, Vimeo etc, being most popular means of entertainment, news and even education (Esmaili and Javidan, 2020). Video content proliferation is existent at the current times. Multiple open platforms are available to upload video content. Open platforms receive low profit, and consumers are at risk in terms of privacy. Centralized storage is one of the factors that effect the privacy of the consumers where data can be accessed by third party and be vulnerable to several attacks. This content may also be prone to copyright violations and can be manipulated (Chen et al., 2017). Solution to this was distributed storage through blockchain.

Decentralized storage being a solution for storage, Esmaili et al. in Esmaili and Javidan (2020) used swarm, an ethereum blockchain supported distributed storage platform that produced no downtime, is secure, non tampered and resistant to censorship. Video access was controlled by the smart contract which provides the validity, transparency, immutability and integrity of the transactions. A merkle tree of video hashes were also stored on the blockchain for immutability and verification. Li et al. in Li et al. (2020) used image information from wireless sensors and converted them to intelligent blocks which were encrypted. The intelligent encrypted algorithms were used to securely transmit the images where signature verification was done and then stored. Medical image data sharing has been one of the most relevant application that requires blockchain protection. The following subsection reviews applications of blockchain for medical image sharing and further advances in deep learning with medical images.

7.1. Medical image sharing

Medical data and medical images have been at a rise due to the increase in internet of medical devices facilitating better health care through proper diagnosis and enhanced treatment (Seo and Cho, 2020). These medical images are often stored on a centralized network which makes it prone to privacy being compromised or even data being poisoned leading to faulty diagnosis and improper treatment (Guo et al., 2021). Blockchain based decentralized data with distributed storage has become popular in recent researches for secure medical image storage and sharing.

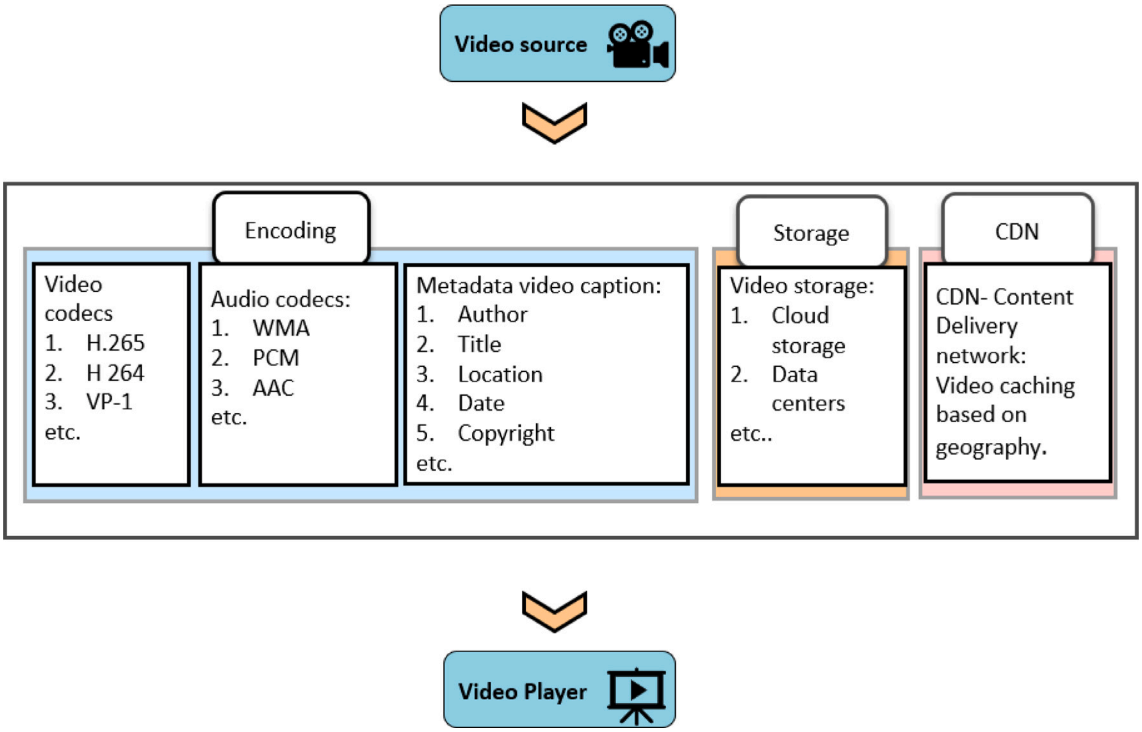

Fig. 8. Typical video streaming process.

Seo et al. in Seo and Cho (2020) modelled a hyperledger fabric architecture a permissioned blockchain for sharing medical images which are retrieved from a hashed and stored picture archive and communication system (PACS). Image sharing was invoked through smart contract.

Image retrieval from IoT systems was safe-guarded through use of blockchain after image was encrypted and stored as transaction in the blocks, which can be retrieved using a retrieval request using smart contract (Shen et al., 2019). Ethereum based medical record storage was one of the applications utilized in Tang et al. (2018) where smart contracts were used to deny fake records ensuring security of medical images.

Due to the high need of large scale medical image data for accurate AI modelling such as in Abdel Hameed et al. (2022), which is strictly protected under the GDPR privacy laws, distributed learning or federated learning is implemented (Predd et al., 2006). With distributed learning, images can be shared through an encryption or stored in a distributed framework as blockchain. Blockchain not only provides security as it cannot be tampered with but also privacy is implemented on a private or consortium blockchain.

7.1.1. *Distributed learning*

In distributed learning the data is not shared but the weights of the process is shared between institutions, this not only secures the data through distributed learning but also distributed computational costs among institutions involved (Predd et al., 2006).

Zerka et al. in Zerka et al. (2020) presented a scheme for secure medical data sharing where radiomics dataset images were trained and their weights were encyrpted using AES encryption and with a validated smart contract token, was saved to a archive model cloud, This was implemented using ethereum blockchain.

Kumar et al. in Kumar et al. (2021) used IPFS system for sending the local weights and stored the IPFS hashes on blockchain. Smart contracts were used for distributing the weights. CT images from different hospitals were trained using RCNN, where (ROI) region of interest was identified and trained in a distributed manner. This enabled a privacy preserving artificial intelligence(AI) with blockchain.

7.2. *Video streaming*

Entertainment, music, journalism and currently education, have exponentiated its need for video streaming applications. The Fig. 8 from Ghat (2017) shows how a video streaming process occurs in a traditional manner. There is a video source that records the information that is encoded and then saved in a storage location. This is then cached onto to a content delivery network based on the video content needs, later to be accessed by the end users video player. A video data may contain a video codec and an audio codec, accompanied by meta data of the video with its caption; encoded in several formats and transcoding for this is made to be suitable for end users' video player. This may charge high costs and consume high computational power. This process is usually done by a single central storage. Thus there is an increasing need for decentralized storage and due to the ever increasing need for video streaming applications plummeting the online traffic blockchain is a solution.

Peer to peer content distribution and blockchain based payment system have been implemented in several startups. A distributed system was introduced in Ghat (2017) that improves the cost and decreases the computational overhead on a single entity by having a distributed system of storage. A distributed encoding was also applied where large scale video processing can be overcome by re-using unused storage space at data centres. Problem of high computational complexity and high cost of the current encoders have motivated the videocoin Ghat (2017), a distributed video processing platform that splits the video into encoding tasks and to convert them to subtasks and parallelly processing them. Open source media framework (ffmpeg) (Cheng et al., 2012) were run on a secure container, which was safe and cannot damage host computer. Miners were paid by the clients based on the processing completion (Ghat, 2017). A video storage network is also adopted where the storage miners form a storage area network using their disk space. Distribution miners and storage miners both take part in delivering the video with lesser computation and cost which can be negotiated between clients and miners as the videos can be split into payable segments (Ghat, 2017).

Table 4
Video integrity preservation applications.

Method	Application	Technique	Blockchain type	Sim.	Smart contract	Modification	Limitations
Kerr et al. (2018)	Cataloguing	CCTV video evidence through video watermarking	Public	–	No	No	Scalability, partial decentralization
Xu et al. (2019)	Data tampering security	Micro-services	Private	Ethereum	No	No	Partial decentralization, Complexity, performance overhead in terms of latency, edge and fog computing challenges
Hasan and Salah (2019)	Combating Deep fake	Tracing video origin	Public	Ethereum	No	No	Decentralized Storage Costs, Data privacy, Complexity of using multiple technologies
Cremona et al. (2019)	Content verification	filtering illegal content	Public	Bitcoin	No	No	Privacy Concerns as filter may require analysing content, centralized control, need to adapt to dynamic content
Yatskiv et al. (2019)	Content verification	Video file processing, Preventing fake	–	Naive chain	No	No	High network latency, Processing overhead, security of cloud service
Zelensky et al. (2018)	Content verification	Video analysis and verification	–	Ethereum	Yes	PROVER app	Lack of scalability for large amount of videos
Danko et al. (2019)	Video forensics	Video hashing	Consortium	Fabric	Yes	No	scalability constraints, Resource intensive, data transfer security
Lee and Park (2020)	Video integrity	Efficient transmission of data by merkle tree hash	–	–	No	Merkle tree hash	Resource intensiveness, scalability challenges, latency
Bui et al. (2019)	Cataloguing and preservation	Hierarchical attention auto-encoder for temporal hashes	Public	Ethereum	No	No	Resource intensiveness, interoperability across countries, scalability challenges
Chen et al. (2020a)	Combating fake	Data verification	–	–	–	Customized consensus	Scalability challenges, resource intensiveness, complex consensus

In another implementation of video streaming, video transcoding was decentralized, where video segments were sent to transcoders through a smart contract which was programmed to select a transcoder based on the job and fuel or bitcoin deposited for the transcoding job (Liu et al., 2020b). It not only gives access but decides the validators, judges, referees based on delegated Proof of stake (PoS). After the transcoding process is done, a video streaming and distribution system verifies through a verification protocol which guarantees that transcoding is done correctly. Delivery of videos is performed after transcoding through mobile edge computing and blockchain Liu et al. (2020b).

Satish et al. in Sathish et al. (2019) employed microservices, which encompassed video stream processing for feature extraction from frames, the enforcement of security policy services, and data access control with verification. Their objective was to prevent unauthorized service requests and tampering by utilizing a permissioned blockchain network for video sharing. Chen et al. (2020b) and Gu et al. (2018) used blockchain based smart contract for crowd sourcing video transcoding. This enhanced efficiency thereby leading to lesser computational resources with distributed computing. In Liu et al. (2020a) a deep reinforcement learning (DRL) algorithm was used for selecting the transcoder, where videos were converted into multiple formats to provide fast and reliable service. This was decentralized using blockchain, where transcoding process was assigned to bidders. This scheme provided quality of service with increased revenue, however, does less in terms of saving energy (Liu et al., 2020a).

Chen et al. (2020b) has four components, the employer, the worker, the payment scheme and the task allocation mechanism for video streaming and/or peer to peer video sharing. Employer issues the smart contracts for distributing tasks, the workers receive and complete the tasks and are given incentives. This model was tested on a private chain for performance in both bidding and task execution performance.

7.3. Discussion of video/image sharing

Video and/or image sharing require security and privacy, like every other application in computer vision, is one of the prime tasks. Storage of the videos were implemented in the blockchain as content hashes or an index of the storage on storage systems namely swarm and IPFS. As video content being too large, merkle hashes were used to store as transaction, At some point only an event in a video is registered. Image retrieval, copyright protection while sharing or using stock photos were some of the applications safeguarded by blockchain through smart contract implementation. Based on the type of images shared, medical data seemed to have the most significant number of literature where data privacy was enabled by distributed learning, new learning approach where several organizations do their training with their data and share the weights for combined inference. Distributed learning was secured by blockchain, however data poisoning is one of the possibilities at the edge which may make it vulnerable to poor training.

Table 4, describes the applications of video and/or image sharing with blockchain. It can be noted that the video sharing systems used

Table 5
Overview of common types of blockchain used in the applications.

Blockchain	Type	Advantage	Disadvantage	Method
Ethereum	Public	Transparent Decentralized storage and processing, Fault tolerant and has its own coupled storage (swarm).	Has cost called ether/gas. Has limit for scalability, Vulnerabilities in smart contract,	Mudliar et al. (2018), Iovane et al. (2018), Delgado-Mohatar et al. (2019), Tang et al. (2018), Hasan and Salah (2019), Zelensky et al. (2018) and Bui et al. (2019)
Ethereum	Private	Single validator, Uses smart contract, Privacy protected	Can risk centralization	Xu et al. (2019), Esmaili and Javidan (2020) and Zerka et al. (2020)
Hyperledger Fabric	Consortium blockchain	Controlled by a consortium, User access programmed by chaincode, Has an orderer peer and endorser peer, There is control with decentralization, secure and private	Prone to network attacks, Not post quantum secure	Naganuma et al. (2020) and Sawant and Bharadi (2020)
Bitcoin	Public	Transparent, Available, Secure, Decentralized storage and processing	Prone to rewritten chain and is costly	Buchmann et al. (2017) and Danko et al. (2019)

ethereum for their transaction. Smart contract was efficiently used to automate the process as well verify and give access for retrieval or verify a image or video data. Due to the low capacity of storage on-chain, Off-chain storage was widely used. This is a safe alternative to centralized storage. However with the number of steps involved in this process, there is delay involved increasing latency. Cloud storage was used to store the weights, although encrypted, is vulnerable to security threats in cloud.

Video streaming applications with blockchain improved the transcoding process and decreased computational cost with the use of miners who compete to provide storage space as well as perform transcoding. Video processing was done in a distributed manner by miners. Through deep learning methods with blockchain, quality of service, security and privacy was guaranteed for a trustable video streaming service. Even though, the cost and computing power is distributed, it can lead to delay in video streaming process. Quality of service (QoS) can be a determining factor in terms of choice of video streaming service along with quality of experience (QoE). Is there a possibility of a model that is optimized for the performance, in terms of QoS and QoE fulfilled fairly is a task for future research.

8. General discussion

Data security, integrity and even processing can be safeguarded and accounted for through blockchain systems (Kirillova et al., 2020; Shrier et al., 2016; Zikratov et al., 2017). Computer vision is one such application that can leverage the immutability, both transparency and private nature of different types of blockchain. Several applications requiring public as well as private network can be leveraged to be used in applications such as securing image data, sharing images as well as video processing information among many other. Tables 1–4 lists out the applications of computer vision with blockchain available in current literature. On the type of blockchain used, there is a huge popularity for use in Ethereum blockchain as a public blockchain where anyone valid can join the network, as well as a private blockchain where access control can be restricted (Lee et al., 2020). Hyperledger fabric is used for exercising access control at situations where constrained access need to be given for certain nodes (Shalaby et al., 2020). Table 5, lists out in detail the performance of Hyperledger fabric and Ethereum.

In terms of the applications used in computer vision, the dominance of machine learning and deep learning approaches for image processing is noted. CNN are widely used in image processing part (Kumar et al., 2021; Farr et al., 2020; Qi et al., 2020,?). Most of the applications involved feature extraction stage in terms of biometrics. Multi-modal biometrics, that uses multiple biometrics as identity enhanced the security. Further enhancement was put forth with biometric and numerical fusion approach for cryptography which was then used as a digital signature (Sawant and Bharadi, 2020; Naganuma et al., 2020). Image encryption proved to not only secure identities but also secure blockchain in some applications (Naganuma et al., 2020).

With a unique representation of a person, several literature's focused on using biometrics with blockchain as an identity for governmental activities (Buchmann et al., 2017). Video integrity overlapped its application in all fields of computer vision. Combating fake seemed to be the prime focus for many applications where content verification, watermarking cameras, tracing origin of videos were some of the ways to prevent fake. Hashing video content was noteworthy for its use in content verification and video forensics. Video integrity can be preserved within many applications during surveillance, video sharing, evidence gathering, and video processing. Securing medical images and distributed learning for medical data sharing was point of focus in most applications. CT images and X-ray images were shared through blockchain transactions (Seo and Cho, 2020) Applications in video streaming, such as distributed video transcoding, not only reduced the computing cost of the process, but also enabled distributed storage enhancing the sustainability of storage through delegating tasks to peers and renting only the required storage (Sathish et al., 2019; Chen et al., 2017; Cheng et al., 2012).

Storage of big data is a challenge in blockchain as public blockchains that have limitations in terms of block size with some limiting to 1MB which is too low for video content. Several methods like video hashing using merkle hash and other hashing algorithms were utilized, however selectivity of content was to be performed. Table 6 summarizes the different off-chain storage solutions available with blockchain enabling a decentralized architecture in balint et al. for storage. Off-chain storage was found to be optimum for video storage where high resolution image and video files were to be stored. A separate physical drive may contain the whole data which is leased from miners. The hash data is only available in the blockchain with a link to the physical storage location (Hepp et al., 2018; Bálint, 2020; Esmaili and Javidan, 2020; Bálint, 2020).

Some of the computer vision applications in deployment require a middleware to deal with blockchain network as well as an user interface to retrieve information. Several architectures with computing

Table 6
Off-chain storage for large video footage.

Name	Description	Advantage	Disadvantage	Method
IPFS	All computer systems are connected by a common file system. Contents are stored worldwide. Index of content is transaction data.	Mutual trust is not required to protect users data	Failure to provide data protection, that is strong enough	Toutara and Spathoulas (2020), Bálint (2020), Kumar et al. (2021) and Mehta et al. (2019)
FileCon	Based on IPFS protocol, storage miners lease out storage. Retrieval miners	Secure storage with endpoint encryption.pass clients data to the storage miners. Miners are renumerated with crypto coins.	High cost of transaction.	Bálint (2020)
Sia	Similar to FileCon, it is a cloud based	Secure storage with endpoint storage encryption. Redundant sharing.	Computationally complex Reed–Solomon error-correcting scheme.	Bálint (2020)
Swarm	Peer to peer storage service. A torrent like service, incentive drive and coupled with Ethereum network.	It has zero downtime and DDoS resistant. Appropriate for IoT networks. Its fault tolerant and censorship resistant.	Coupled with only Ethereum.	Esmaili and Javidan (2020)
Storj	Slicing of data to segments and separated into stripes which are grouped into new erasure codes then uploaded. Uses asymmetric encryption.	Data is secured by private keys. Can store video footage.	Cost of 1GB is 0.01 dollars/month which is comparatively high.	Bálint (2020)
RIFT	Larger block size creation achieved through testing only.	Block size of 5Gb is available.	Not widely implemented.	Bálint (2020)

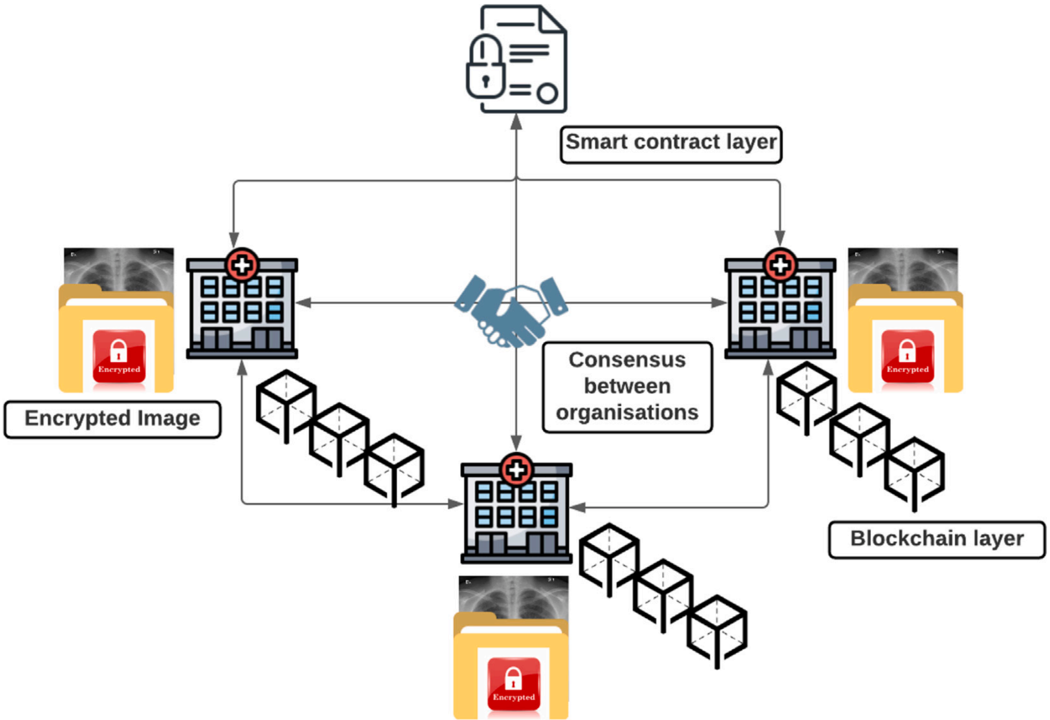

Fig. 9. Medical sharing between organization .

at the edge and fog and at the cloud is implied in several papers. Fig. 9 illustrates a general architecture of medical image sharing with blockchain that can be deployed at the edge level. The organizations form a consortium blockchain where the identity or access to information is validated by smart contract. Video and/or image data can only be shared based on a consensus and transactions created, stored as encrypted data on the block (on-chain) or on the cloud (Shen et al., 2019). The image can be retrieved through smart contract as in Shen et al..

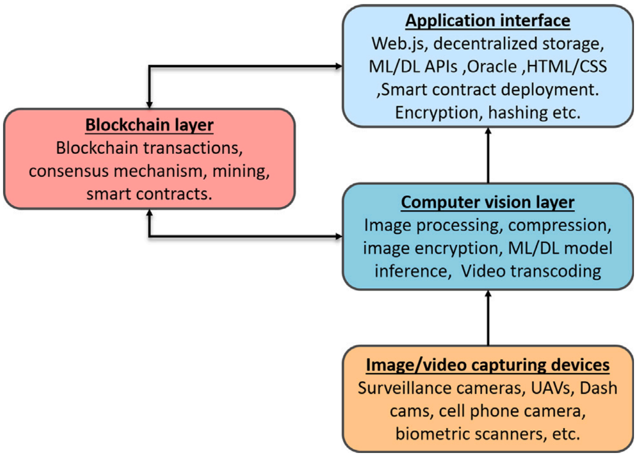
Application interface
Web.js, decentralized storage, ML/DL APIs ,Oracle ,HTML/CSS ,Smart contract deployment. Encryption, hashing etc.
Blockchain layer
Blockchain transactions, consensus mechanism, mining, smart contracts.
Computer vision layer
Image processing, compression, image encryption, ML/DL model inference, Video transcoding
Image/video capturing devices
Surveillance cameras, UAVs, Dash cams, cell phone camera, biometric scanners, etc.

Fig. 10. Layered architecture of blockchain with computer vision applications with common and potential components.

Storing Video metadata is the most common method of protecting video integrity. Metadata is an important information stored in an EXIF (Exchangeable Image File) format. The metadata has information on device captured, the settings of the video captured like shutter speed and focal length, the history of capture that includes the time and location of the capture. Apart from this information that are similar to images, they have container formats like AVI and MP4, that hold the codec information, video, and audio streams. This information does not require high storage capacity but is very crucial to identification of authenticity, origin and formatting of the image or video. This when added with blockchain security by storing the metadata on the block can enhance the provenance of videos.

8.1. Blockchain-computer-vision implementation layers

It can be evident that a generalized layered architecture can be charted from all the models. In Ramachandran and Krishnamachari (2018), a generalized blockchain for IoT is layered with a server and back-end layers, edge device and the end device. The server and back-end constitutes the part of the application layer that performs the application layer functions. Edge computing is performed in a separate layer with network connections in another layer. With this in perspective and summarizing the application uses cases, Fig. 10 is an overview of layers of blockchain with computer vision applications and common tools used in each layer of network. The layers are divided into four layers, Image/video capturing layers, computer vision layer, blockchain layer and application interface. The following describes each layer in brief.

Image/video capturing layer: There can be several image capturing devices like of that PTZ cameras, CCTV cameras, mobile phone cameras, dash cams and UAV's/drones equipped with cameras all forming part of the blockchain network. This layer is at the core of the blockchain where data is captured. There can be three ways this data is used for the applications.

- The captured data is sent to the computer vision layer where large scale image/video processing is performed. Machine an d deep learning inference can be done at this layer where the pretrained models are stored for inference.
- The captured data is stored in a decentralized storage where the index is hashed on to the blockchain.
- The captured devices can also be embedded with image/video processing capability that can then use an oracle or middle ware to store the data/metadata as transactions on the blockchain Mendki (2019).

Recent developments in hardware and embedded computing has enabled possibility of embedded blockchain where the device at the edge can be used as a blockchain node along with performing computer vision based computations. Some of the devices that are equipped for general purpose computations are as seen in the Fig. 11.

Raspberry Pi is most common tool used for this purpose but has restrictions on capacity of storage and GPU computing (Xu et al., 2018). NVIDIA corporation has released a series of embedded boards named JETSON nano, Xavier that can be used for heavy GPU computation enabling deployment of more accurate models which are trained on larger datasets for tasks like object detection, classification, abnormal detection, object recognition and so on. etc (Basulto-Lantsova et al., 2020). Current developments in light weight models called TinyML (Banbury et al., 2020) has further enhanced the computational speed and reduced complexity of the computations on the edge (Ramachandran and Krishnamachari, 2018).

Blockchain layer: Depending on the type of blockchain and the network architecture it is integrated with, the blockchain can be implemented in various formats. One approach is to have the blockchain running on nodes as part of the edge network, while another method is to deploy it within the fog network. If the blockchain is part of a surveillance system controlled by a regional control station, the blockchain nodes is several control stations. In the case of a national identity containing blockchain, it would be the public institutions. Smart contracts are used to control access to the blockchain in several levels.

Computer vision layer: The computer vision layer is where the image processing, pattern recognition, object detection is performed. Deep learning and machine learning models are deployed in this layer. The images captured are inferred for object recognition , detection, and identification or matching based on the application use case. Core information is extracted and encrypted. With the use of an application interface (API) and decentralized applications (dAPPs) they are stored on to the blockchain or a decentralized storage later to be hashed on to the blockchain Paralkar et al. (2018).

Application interface layer: The application interface acts as the link between the blockchain and the computer vision application. Decentralized applications are created where blockchain API's and Computer vision application API's are visualized. Smart contracts are deployed on this layer and communicate with the blockchain using an oracle or a middle ware. Applications like Infura, Ganache are used for interfacing with blockchain through private blockchain simulations and applications (Hu et al., 2018; Zupan et al., 2017; Taş and Tanrıöver, 2019). Scripting languages like solidity and Golang are used to program smart contract and dApps. The decentralized storage like IPFS and swarm use API's to interface with the blockchain and other applications. Using Application interface, a micro-service architecture can also be created where different tasks can be done at different nodes, performing varied tasks as in Nagothu et al. (2018). A typical usage of blockchain with access control using smart contracts for person re-identification as illustrated in Fig. 12. Other forms of layered architecture for blockchain based application can be moulded based on use case. Two layered federated learning architecture with hyperledger fabric blockchain for security can be seen in Feng et al. (2021). MNIST data was trained at several nodes and weights shared through secure hyperledger fabric blockchain.

8.2. Evaluation metrics

As with every application, the success or usability depends on its efficiency and effectiveness to perform task assigned. Performance of blockchain is commonly measured based on the success rate, average latency, throughput, cost, and resource consumption (Dabbagh et al., 2020; Pongnumkul et al., 2017). Image and/or Video processing part efficiency depends on the type of task it performs. Tasks like object detection and image segmentation have metrics related

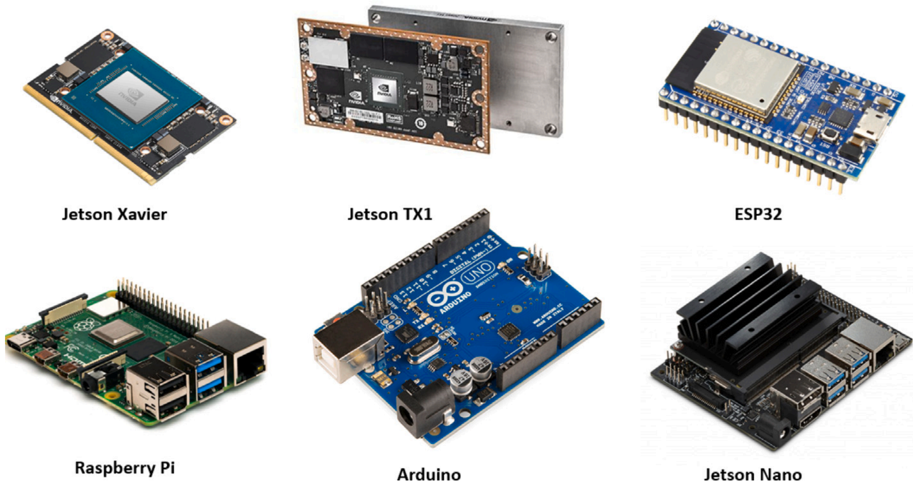

Fig. 11. Commonly used experimental edge devices for camera embedded computing.

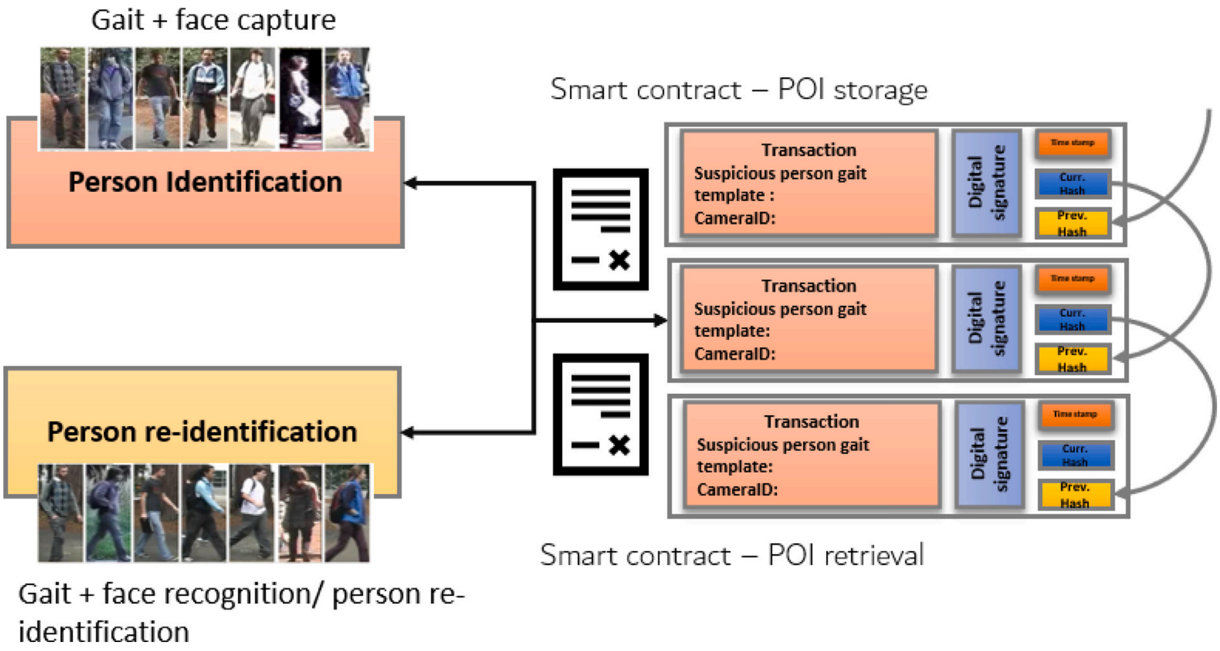

Fig. 12. Person Re-identification using smart contracts for image retrieval and storage to provide access control.

to the process it performs like accuracy of detection measured by mean average precision, number of frames processed per second etc. The following are common evaluation metrics that can be used in blockchain applications with computer vision:

Success rate: The Success rate is typically measured in the blockchain layer as the number of successful transaction performed out of 100 transactions (Dabbagh et al., 2020).

Average latency: The time taken to execute the code after initialization is usually measured as latency. With smart contracts involved and an added layer of image processing, the latency is found to usually increase in applications. Latency can be predicted using architecture modelling and using testnets and simulations for which framework was proposed in Yasaweerasinghelage et al. (2017).

Throughput: The measure of number of transactions performed per second is termed as throughput. Several blockchains have a predefined number of transactions set. The addition of another layer of computation in terms of smart contract, verification and inference on the computer vision layer, this may vary (Gupta et al., 2020).

Resource Consumption: Resource consumption is a key factor in usability of the system. The memory used and the CPU usage are averaged to quantify the resource consumed during the blockchain process. Storage capacity and overall complexity in computation both time and memory are measured for this purpose (Dorri et al., 2017).

Scalability: The number of nodes that be part of a blockchain is essential in designing an efficient blockchain application. Most private blockchains can control the number of nodes in the network thus maintaining the smaller chain and improving latency. Public blockchains on the other hand can be unlimited, however each blockchain model has its own set scale. Multi-chain approaches are used in some applications for enhancing scalability (Badr et al., 2019).

Security metrics: Applications like video integrity, data sharing and biometrics are most vulnerable to security threats although mitigated in terms of architecture by blockchain. There are loopholes in the system that need to be addressed. Quantifying how secure is the blockchain with computer vision model requires security be dealt with in all the phases of the process starting form where AI is applied, to identifying or capturing the required data to be stored or indexed. The type of blockchain influences the blockchain model used and so the security implications too. Abdelwahed et al. in Abdelwahed et al. (2020) provides methodology for measuring cyber-security risks involved in blockchain applications. Security in micro-services architecture were divided as mining services and security policy services (Shen et al., 2019). Access control in blockchain provides authorization, the cryptographic keys provide authentication, the immutability provides reliability and consensus mechanism provides validation and verification.

In terms of the mining services present in blockchain used for validation and verification provides security for the private permissioned blockchain from unauthorized miners and transaction. The security policies are defined by micro-services each orchestrating policies that involve authentication and access control. This was advantageous in enhancing scalability and heterogeneity in surveillance systems through light-weight security solutions that are flexible and inter-operable.

Performance evaluation of most of the models in the applications surveyed were based on security, throughput, latency and scalability. Each layer of the blockchain with computer vision model had its own evaluation metric. Al-Sahan et al. (2020) measured the latency for the whole model, where as (Bálint, 2020) compared the security of off-chain storage with cost involved. Esmaili et al. performed security, scalability and time complexity analysis as performance metrics (Esmaili and Javidan, 2020).

8.3. Advantages of blockchain for computer vision

Computer vision applications with blockchain enhance the application in several ways. The striking features of blockchain that enable this enhancement are the following:

Integrity: Video evidence is kept and can be traced back to its origin, all transaction are verified and hashed enabling trust in video content in the blockchain. Smart contracts are used to control access, verify content and automate the process which in itself is uneditable after deployment even by the author themselves (Christidis and Devetsikiotis, 2016).

Accountability: Every video catalogued or stored can be traced back to its origin as blockchain is an uneditable ledger which is time stamped, which makes the blockchain network accountable for the transactions.

Non-repudiation: As the ledger is uneditable and cryptographically signed by the author as private key as well as public key there is no contest in the origin of videos. Biometric keys provide an even more secure key where the author can be identified.

Authorization: Smart contracts can be programmed to perform authorization as well function with authorization, where a certain authority can only execute the functions in a contract. This enables accountability as well as access control in some situations where privacy and security of the video information need to be taken care of as in video integrity applications as well as video surveillance.

Availability: Public blockchain network is transparent, all nodes have access to the ledger and provenance data is available for the participants. Denial of service(DoS) and Distributed denial of service(DDoS) are prevented in this network due to its global placement. As there is no single point of failure, there is availability of data all the time.

Replay Attacks:

Replay attacks occur when a communication is captured and played at a later time (Smith et al., 2015). In the case of blockchain, transaction data can be subjected to replay attacks after a hard fork occurs. Two distinct blockchain branch out for the original chain. In this case replay attack materializes when malicious nodes intercept a valid data transmission on one chain and replicate and re-transmit at a later juncture . In the case of computer vision applications, this could be harmful when data such as biometric templates, image hashes are replayed by malicious nodes compromising integrity resulting in erroneous data and falsified information. It is imperative that replay attacks should be recognized and thwarted as they provide unauthorized access to sensitive information and enable malicious activity. The existence of private keys in blockchain serves as one of the defence mechanisms in the blockchain architecture. Signed transactions ensure validity of the information. Nodes performing mining mechanism can reject a transaction of an unauthorized entity (Li et al., 2020). Supplementary measures on the blockchain network such as timestamps, nonces and unique chain identification such as the chainID incorporated onto the ethereum network mitigate any replay attack ensuring integrity of the data secured (Anita. and Vijayalakshmi., 2019; Chalaemwongwan and Kurutach, 2018). Timestamp, nonce and chainID are included in the transaction data of the blockchain. Every new transaction on the blockchain undergoes scrutiny to verify the uniqueness of the nonce, a unique number, and the timestamp, which records the time the block was created. These values are embedded in the header of the block within the blockchain. If the uniqueness of the nonce and timestamp is not valid, the transaction is rejected, thus preventing a replay attack.

Impersonation and Sybil Attacks: Impersonation and Sybil attacks can be thwarted on an Ethereum framework as the Ethereum holds a decentralized Ethereum name system (ENS) which contains all the public keys generated. This with the use of biometric keys can enhance the security of Ethereum.

Privacy: With consortium blockchains, valid parties can be given access to images or videos based on their authority level as seen in many applications with biometrics and video surveillance. Restricting access to unauthorized parties safeguards privacy of the content.

Decentralized storage: Huge amounts of data retrieved from Video footage and video streaming need not be stored at one infrastructure. Several secure non-cloud, decentralized storage systems are available to store the videos.

Decentralized processing: Secure sharing of gradient of machine learning models enables federated or distributed learning which provides opportunities for secure big data analysis and collaborative training producing much more accurate results as seen in distributed learning for medical images.

Fault tolerance: Duplication of records enables fault tolerance in an decentralized network (Esmaili and Javidan, 2020).

Transparency and Trust: Visibility of all the transactions in each node provides trust to the participants despite being decentralized (Esmaili and Javidan, 2020).

8.4. Challenges and future directions

Blockchain has brought forth many advantages to computer vision as stated above, however every application has its own challenges and limitations as stated in columns of Tables 1–4.

Real time analysis: Most state of art applications of computer vision with blockchain involve architectures that need to be implemented in real time for further analysis. Although decentralized architectures, some of the applications are prone to centralization due to the use of a central node as validator such as in private blockchains.

Scalability: Scalability being its first challenge, blockchain architecture's capacity for transaction processing is very low as of now along with its block size amounting to 1Mb like that of bitcoin Wu et al. (2020). With most of its applications in identity management, there is a need for high scalability of the blockchain architecture. Public blockchains like Ethereum and Bitcoin was calculated to be 200 GB as its scalable limit (Delgado-Mohatar et al., 2019). As with the popularity of many blockchains, the size of blockchains have been growing which can be a bottle neck for several applications (Delgado-Mohatar et al., 2019). To over come scalability limitation of the blockchain, parallel processing was a solution put forth in Akbari et al. (2017), which can be used for several applications such as video transcoding.

Unexpected Security risks: Security with biometric keys can be a added fortress to blockchain, however there is a possibility of attack that is not studied yet. This being an individuals key can make them vulnerable to frauds and thefts. The type of blockchain may determine the cost involved in the process and some smart contracts when executed need to be rewarded accumulating cost (Albert et al., 2020). Implementation of a single national identity with biometric data and breeder documents. Further enhancing security through quantum proof blockchain like IOTA as in national identify breeder documents (Buchmann et al., 2017). Furthering research for more safer multi modal biometrics for encryption keys in blockchain and so on (Iovane et al., 2018). Biometric key can merge for copyright protection in video streaming and video transcoding through water marking the segments of the videos for safety of the video from tampering in the process of transcoding (Kerr et al., 2018).

Immutability of smart contracts: Smart contracts being implemented in almost all applications of computer vision for automation, verification or access control, need to be checked carefully to avoid potential bugs (Mohanta et al., 2018). Frauds and attacks are malicious behaviours that should be taken into consideration when smart contract developers need to be aware of the contract's interaction patterns to mitigate potential loses due the malicious behaviours (Destefanis et al., 2018). It is impossible to make revisions once deployed (Mohanta et al., 2018). Careful planning needs to be done in order to have secure functioning blockchain system. Time and assets are also involved in keeping up contracts along with system expenses of the whole framework (Michelin et al., 2020).

Computational Cost: Computer vision applications require high performance hardware and high computational cost in most applications (Afif et al., 2020). This causes an overhead in processing along with the latency involved in the computer vision with blockchain applications where transactions are exchanged, validated and confirmed with an consensus algorithm along with automated smart contracts and in some architectures API's which bridge between the different layers of the architecture. Enhancing security can be cause of high latency and thereby delay in output (Gupta et al., 2021). Although, some image processing applications implemented have had minimal delay as in Al-Sahan et al. (2020). Removing one property of blockchain like mining where it is not necessary can be a point forward for future applications.

Proactive Predictive surveillance: In terms of surveillance systems, a proactive predictive surveillance is a future work described in the state of art with blockchain protection. Although light weight models are utilized for blockchain in video surveillance in terms of security, feature sharing can be a direction in terms of person re-identification and gait recognition tasks. Secure video summarization (Elharrouss et al., 2019) for suspect capturing from multiple cameras and privacy preservation through this approach with blockchain can enhance suspicious activity tracking and immediate response to critical incidents. Biometric encryption of images and videos for content preservation and video integrity preservation can be used with blockchain for authentication of video content.

Need for Standardization: Once the application is deployed, there is a need for privacy, security and storage, and evidential data storing procedures to be standardized for law enforcement through watermarking camera vendors, using cameras with embedded chips for creating on-camera blocks etc (Kerr et al., 2018). There is a need for further research in applications related to video sharing in sensitive applications like educational videos, videos that contain protected content, videos that have minors involved etc.

Storage: Cloud storage is often used in this systems due to large amount of storage required for video content (Zerka et al., 2020). Several peer to peer centralized storage are analysed for this that can be leveraged for future applications (Bálint, 2020), Table 5 describes the types of storage applications available that are decentralized and commonly used with blockchain. Storage can be costly, insecure and some computationally complex codes for error checking which needs to be dealt with as future work.

Biometrics template ageing: Biometric being an unique identity of a person is applied for authentication as well as digital signature; it should be noted that certain features are effected by ageing such as face. This leads to ageing of biometric templates which can cause high error rate in recognition and consequently effect efficient access control and identity management (Buchmann et al., 2017). Losing the key to blockchain can cause considerable data loss.

Post quantum Security: Post quantum security is a big concern for the unexpected security risks that can arise for blockchain applications as well as computer vision. Current applications are not quantum secure. Buchmann et al. in Buchmann et al. (2017) suggested a hard fork on blockchain for applying a post quantum resistant digital signature in the metadata that is the integrated biometric embedded breeder document. An example of post quantum resistant digital signature as stated in Buchmann et al. (2017) would be XMSS and SPHINCS. XMSS (eXtended Merkle Signature Scheme) where private key changes with every signature generation (Hülsing et al., 2018). SPHINCS is a stateless long term hash-based signature scheme which is resistant to quantum threats (Bernstein et al., 2015). Blockchain architectures viable for IoT like IOTA which is quantum secure can be used for Computer vision applications deployed at the edge.

With all these taken into consideration, the processing capability of the blockchain depends on type of blockchain used. Ethereum for example, can run only 12 transactions per second which when compared to large amount of real time video footage generated is not sufficient. And so the type of blockchain used should cater to the application requirements (Delgado-Mohatar et al., 2019). Specific to the applications involved, for an image retrieval system, encrypted image features for data modelling was suggested as a future work in Shen et al. this is predicted to preserve privacy and security further. Rewarding members based on contribution based on shapely method was a future direction (Shen et al., 2019) to implement. Image processing systems in computer applications can be further enhanced for specificity as noted in Al-Sahan et al. (2020). Image frauds have been dealt with in many applications using hashing. However, image transformation was found to be an issue for future research (Mehta et al., 2019).

Distributed learning is an application that is blooming in the current. However there is trust involved in the image data and the weights shared among two entities at the edge which leads to need for better encryption methodologies for securing the data and safeguarding which can be done by enhancing blockchain Kairouz et al. (2019).

Light weight accurate mechanisms are the need for now due to the lack of storage and security issues of off-chain storage, where on-chain storage need to be used (Singh et al., 2020). In addition, latency involved in large systems need to be mitigated with use of several front-end and back-end applications adding to the delay time. A comprehensive robust system without trade off in terms of latency, throughput and computational overhead, accuracy of output should be the aim for computer vision applications.

9. Conclusion

This paper, provides a overview of blockchain applications with computer vision and potential future works. It discriminates the applications based on the use cases and then elaborates each application. An overview and generalized model was constructed for each application with that there was a deep delve into performance metrics, layered architecture, and the pros and cons. Compared to a centralized architecture a trade-off is eminent in terms of security, throughput and scalability as well as latency based on the application scenario. Several generalized architectures are presented in this paper as well as some future directions to mitigate the drawbacks. Discussion in each section summarizes, and presents the challenges that need to be overcome to optimize the blockchain performance with computer vision applications. In conclusion there is more room for research in each category reviewed and there is need for the use of this revolutionary technology, blockchain, to merge with computer vision into more research paths. Several applications can further be used with the introduction of distributed or federated blockchain and encryption techniques with fusion biometrics to secure the training of massive amount of data captured by different organizations.

Future direction: In the context of establishing a secure and private data transmission and communication system, blockchain emerges as a promising solution for computer vision applications. Nevertheless, there exists a crucial need to address scalability issues and accommodate the storage of large datasets with real time processing a fundamental requirement for computer vision tasks. Future research should investigate the trade-off between these requirements and optimizing solutions for a more efficient system. Blockchain technology applications in computer vision include various domain of those in public and private systems. A critical area for future exploration is achieving interoperability between these diverse blockchain networks. Access in a controlled and timely manner of real time data secured on blockchain such as surveillance video footage, biometrics identification data, medical images and live streaming data. Additionally, analysis of the data and availability of the resultant data in a secure network.

As the field evolves, it becomes imperative to develop and update security mechanisms and build advanced cryptographic methods that can withstand potential post-quantum security breaches, ensuring the long-term security of blockchain-based systems. Further research avenues include the creation of decentralized image databases, the integration of AI-generated smart contracts, and the seamless incorporation of image and video analysis capabilities facilitated by blockchain technology. These areas represent exciting opportunities for innovation and advancement in the intersection of blockchain and computer vision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research work was made possible by research grant support (QUEX-CENG-SCDL-19/20-1) from Supreme Committee for Delivery and Legacy (SC) in Qatar.

References

Abdel Hameed, M., Hassaballah, M., Hosney, M.E., Alqahtani, A., 2022. An AI-enabled Internet of Things based autism care system for improving cognitive ability of children with autism spectrum disorders. Comput. Intell. Neurosci. 2022.

Abdelwahed, I.M., Ramadan, N., Hefny, H.A., 2020. Cybersecurity risks of blockchain technology. Int. J. Comput. Appl. 975, 8887.

Abuhashim, A., Tan, C.C., 2020. Smart contract designs on blockchain applications. In: 2020 IEEE Symposium on Computers and Communications. ISCC, pp. 1–4. http://dx.doi.org/10.1109/ISCC50000.2020.9219622.

Afif, M., Said, Y., Atri, M., 2020. Computer vision algorithms acceleration using graphic processors NVIDIA CUDA. Cluster Comput. 1–13.

Akbari, E., Wu, Q., Zhao, W., Arabnia, H.R., Yang, M.Q., 2017. From blockchain to internet-based voting. In: 2017 International Conference on Computational Science and Computational Intelligence. CSCI, IEEE, pp. 218–221.

Al-Sahan, L., Al-Jabiri, F., Abdelsalam, N., Mohamed, A., Elfouly, T., Abdallah, M., 2020. Public security surveillance system using blockchain technology and advanced image processing techniques. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies. ICIoT, IEEE, pp. 104–111.

Albert, E., Correas, J., Gordillo, P., Román-Díez, G., Rubio, A., 2020. GASOL: gas analysis and optimization for ethereum smart contracts. In: International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Springer, pp. 118–125.

Andreev, R., Andreeva, P., Krotov, L., Krotova, E., 2018. Review of blockchain technology: Types of blockchain and their application. Intellekt. Sist. Proizv. 16 (1), 11–14.

Anita., N., Vijayalakshmi., M., 2019. Blockchain security attack: A brief survey. In: 2019 10th International Conference on Computing, Communication and Networking Technologies. ICCCNT, pp. 1–6. http://dx.doi.org/10.1109/ICCCNT45670.2019.8944615.

Badr, A., Rafferty, L., Mahmoud, Q.H., Elgazzar, K., Hung, P.C.K., 2019. A permissioned blockchain-based system for verification of academic records. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security. NTMS, pp. 1–5. http://dx.doi.org/10.1109/NTMS.2019.8763831.

Bálint, K., 2020. Modern, decentralized blockchain-based solutions for saving video footage. In: 2020 IEEE 18th International Symposium on Intelligent Systems and Informatics. SISY, IEEE, pp. 11–14.

Banbury, C.R., Reddi, V.J., Lam, M., Fu, W., Fazel, A., Holleman, J., Huang, X., Hurtado, R., Kanter, D., Lokhmotov, A., et al., 2020. Benchmarking tinyml systems: Challenges and direction. arXiv preprint arXiv:2003.04821.

Basulto-Lantsova, A., Padilla-Medina, J.A., Perez-Pinal, F.J., Barranco-Gutierrez, A.I., 2020. Performance comparative of OpenCV template matching method on Jetson TX2 and Jetson nano developer kits. In: 2020 10th Annual Computing and Communication Workshop and Conference. CCWC, IEEE, pp. 0812–0816.

Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O'Hearn, Z., 2015. SPHINCS: practical stateless hash-based signatures. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 368–397.

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W., 2013. Guide to Biometrics. Springer Science & Business Media.

Buchmann, N., Rathgeb, C., Baier, H., Busch, C., Margraf, M., 2017. Enhancing breeder document long-term security using blockchain technology. In: 2017 IEEE 41st Annual Computer Software and Applications Conference, Vol. 2. COMPSAC, IEEE, pp. 744–748.

Bui, T., Cooper, D., Collomosse, J., Bell, M., Green, A., Sheridan, J., Higgins, J., Das, A., Keller, J., Thereaux, O., et al., 2019. Archangel: Tamper-proofing video archives using temporal content hashes on the blockchain. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

Chalaemwongwan, N., Kurutach, W., 2018. A practical national digital ID framework on blockchain (NIDBC). In: 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology. ECTI-CON, pp. 497–500. http://dx.doi.org/10.1109/ECTICon.2018.8620003.

Chauhan, A., Malviya, O.P., Verma, M., Mor, T.S., 2018. Blockchain and scalability. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion. QRS-C, IEEE, pp. 122–128.

Chen, T.Y., Biglari-Abhari, M., Kevin, I., Kai Wang, A., 2017. Trusting the computer in computer vision: A privacy-affirming framework. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. pp. 56–63.

Chen, Q., Srivastava, G., Parizi, R.M., Aloqaily, M., Al Ridhawi, I., 2020a. An incentive-aware blockchain-based solution for internet of fake media things. Inf. Process. Manage. 57 (6), 102370.

Chen, Y., Yin, H., Xiang, Y., Ren, W., Ren, Y., Xiong, N.N., 2020b. CVT: A crowdsourcing video transcoding scheme based on blockchain smart contracts. IEEE Access 8, 220672–220681.

Cheng, J.C., Lee, N.Y., Chi, C., Chen, Y.H., 2018. Blockchain and smart contract for digital certificate. In: 2018 IEEE International Conference on Applied System Invention. ICASI, IEEE, pp. 1046–1051.

Cheng, Y., Liu, Q., Zhao, C., Zhu, X., Zhang, G., 2012. Design and implementation of mediaplayer based on ffmpeg. In: Software Engineering and Knowledge Engineering: Theory and Practice. Springer, pp. 867–874.

Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., Kayes, A., Alazab, M., Watters, P., 2019. A comparative analysis of distributed ledger technology platforms. IEEE Access 7, 167930–167943.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the Internet of Things. IEEE Access 4, 2292–2303.

Cremona, K., Tabone, D., De Raffaele, C., 2019. Cybersecurity and the blockchain: preventing the insertion of child pornography images. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. CyberC, IEEE, pp. 197–204.

Dabbagh, M., Kakavand, M., Tahir, M., Amphawan, A., 2020. Performance analysis of blockchain platforms: Empirical evaluation of hyperledger fabric and ethereum. In: 2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology. IICAIET, pp. 1–6. http://dx.doi.org/10.1109/IICAIET49801.2020.9257811.

Danko, D., Mercan, S., Cebe, M., Akkaya, K., 2019. Assuring the integrity of videos from wireless-based IoT devices using blockchain. In: 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops. MASSW, IEEE, pp. 48–52.

Deepak, K., Badiger, A.N., Akshay, J., Awomi, K.A., Deepak, G., Kumar, H., 2020. Blockchain-based management of video surveillance systems: A survey. In: 2020 6th International Conference on Advanced Computing and Communication Systems. ICACCS, IEEE, pp. 1256–1258.

Delgado-Mohatar, O., Fierrez, J., Tolosana, R., Vera-Rodriguez, R., 2019. Biometric template storage with blockchain: A first look into cost and performance tradeoffs. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., Hierons, R., 2018. Smart contracts vulnerabilities: a call for blockchain software engineering? In: 2018 International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 19–25.

Dhiran, A., Kumar, D., Arora, A., et al., 2020. Video fraud detection using blockchain. In: 2020 Second International Conference on Inventive Research in Computing Applications. ICIRCA, IEEE, pp. 102–107.

Dorri, A., Kanhere, S.S., Jurdak, R., 2017. Towards an optimized blockchain for IoT. In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation. IoTDI, IEEE, pp. 173–178.

Drescher, D., 2020. Blockchain Basics: A Non-Technical Introduction in 25 Steps. Gildan Audio.

Elharrouss, O., Al-Maadeed, N., Al-Maadeed, S., 2019. Video summarization based on motion detection for surveillance systems. In: 2019 15th International Wireless Communications & Mobile Computing Conference. IWCMC, IEEE, pp. 366–371.

Elharrouss, O., Almaadeed, N., Al-Maadeed, S., 2020. LFR face dataset: Left-front-right dataset for pose-invariant face recognition in the wild. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies. ICIoT, IEEE, pp. 124–130.

Esmaili, M., Javidan, R., 2020. A distributed blockchain-based video sharing system with copyright, integrity, and immutability. In: 2020 8th Iranian Joint Congress on Fuzzy and Intelligent Systems. CFIS, IEEE, pp. 86–92.

Farr, Z., Azab, M., Samir, E., 2020. Blockchain-based cooperative autonomous detection of suspicious vehicles. In: 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference. IEMCON, IEEE, pp. 0188–0192.

Feng, X., Jiang, Y., Yang, X., Du, M., Li, X., 2019. Computer vision algorithms and hardware implementations: A survey. Integration 69, 309–320.

Feng, L., Yang, Z., Guo, S., Qiu, X., Li, W., Yu, P., 2021. Two-layered blockchain architecture for federated learning over mobile edge network. IEEE Network 1–14. http://dx.doi.org/10.1109/MNET.011.2000339.

Fitwi, A., Chen, Y., 2021. Secure and privacy-preserving stored surveillance video sharing atop permissioned blockchain. arXiv preprint arXiv:2104.05617.

Fitwi, A., Chen, Y., Zhu, S., 2019. A lightweight blockchain-based privacy protection for smart surveillance at the edge. In: 2019 IEEE International Conference on Blockchain. Blockchain, IEEE, pp. 552–555.

Gallo, P., Pongnumkul, S., Nguyen, U.Q., 2018. BlockSee: Blockchain for IoT video surveillance in smart cities. In: 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe. EEEIC/I&CPS Europe, IEEE, pp. 1–6.

García, C.G., Meana-Llorián, D., G-Bustelo, B.C.P., Lovelle, J.M.C., Garcia-Fernandez, N., 2017. Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in smart cities, smart towns, and smart homes. Future Gener. Comput. Syst. 76, 301–313.

Garg, K., Saraswat, P., Bisht, S., Aggarwal, S.K., Kothuri, S.K., Gupta, S., 2019. A comparitive analysis on e-voting system using blockchain. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages. IoT-SIU, IEEE, pp. 1–4.

Ghat, D., 2017. VideoCoin-a decentralized video encoding, storage, and content distribution network.

Gollapudi, S., 2019. Deep learning for computer vision. In: Learn Computer Vision using OpenCV. Springer, pp. 51–69.

Gu, Y., Chen, J., Wu, X., 2018. An implement of smart contract based decentralized online crowdsourcing mechanism. In: Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence. pp. 195–199.

Guegan, D., 2017. Public blockchain versus private blockhain.

Guo, H., Dolhansky, B., Hsin, E., Dinh, P., Ferrer, C.C., Wang, S., 2021. Deep poisoning: Towards robust image data sharing against visual disclosure. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. pp. 686–696.

Gupta, S., Hellings, J., Rahnama, S., Sadoghi, M., 2020. Building high throughput permissioned blockchain fabrics: challenges and opportunities. Proc. VLDB Endow. 13 (12), 3441–3444.

Gupta, R., Kumari, A., Tanwar, S., 2021. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. Trans. Emerg. Telecommun. Technol. 32 (1), e4176.

Hadid, A., Evans, N., Marcel, S., Fierrez, J., 2015. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process. Mag. 32 (5), 20–30.

Hafiz, A., Hassaballah, M., Alqahtani, A., Alsubai, S., Hameed, M.A., 2023. Reinforcement learning with an ensemble of binary action deep Q-networks. Comput. Syst. Sci. Eng. 46 (3).

Haiwu, H., An, Y., Zehua, C., 2018. Survey of smart contract technology and application based on blockchain. J. Computer Research and Development 55 (11), 2452.

Hameed, M.A., Abdel-Aleem, O.A., Hassaballah, M., 2023. A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. J. Ambient Intell. Humaniz. Comput. 14 (5), 4639–4657.

Hasan, H.R., Salah, K., 2019. Combating deepfake videos using blockchain and smart contracts. IEEE Access 7, 41596–41606.

Hassaballah, M., Aly, S., Abdel Rady, A.S., et al., 2018. A high payload steganography method based on pixel value differencing.

Hassaballah, M., Hameed, M.A., Alkinani, M.H., 2020a. Introduction to digital image steganography. In: Digital Media Steganography. Elsevier, pp. 1–15.

Hassaballah, M., Hameed, M.A., Aly, S., AbdelRady, A., 2020b. A color image steganography method based on ADPVD and HOG techniques. In: Digital Media Steganography. Elsevier, pp. 17–40.

Hepp, T., Sharinghousen, M., Ehret, P., Schoenhals, A., Gipp, B., 2018. On-chain vs. off-chain storage for supply-and blockchain integration. it-Inf. Technol. 60 (5–6), 283–291.

Hu, Y.C., Lee, T.T., Chatzopoulos, D., Hui, P., 2018. Hierarchical interactions between ethereum smart contracts across testnets. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. pp. 7–12.

Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V., Akella, V., 2019a. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. Int. J. Inf. Manage. 49, 114–129. http://dx.doi.org/10.1016/j.ijinfomgt.2019.02.005, URL: http://www.sciencedirect.com/science/article/pii/S0268401219302014.

Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V., Akella, V., 2019b. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. Int. J. Inf. Manage. 49, 114–129.

Hülsing, A., Butin, D., Gazdag, S.L., Rijneveld, J., Mohaisen, A., 2018. XMSS: eXtended Merkle signature scheme. In: RFC 8391. IRTF.

Iovane, G., Bisogni, C., De Maio, L., Nappi, M., 2018. An encryption approach using information fusion techniques involving prime numbers and face biometrics. IEEE Trans. Sustain. Comput. 5 (2), 260–267.

Islam, M.N., Kundu, S., 2018. Preserving IoT privacy in sharing economy via smart contract. In: 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation. IoTDI, IEEE, pp. 296–297.

Islam, A., Shin, S.Y., 2019. BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things. J. Commun. Netw. 21 (5), 491–502. http://dx.doi.org/10.1109/JCN.2019.000050.

Jacobovitz, O., 2016. Blockchain for Identity Management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva.

Jain, A.K., Flynn, P., Ross, A.A., 2007. Handbook of Biometrics. Springer Science & Business Media.

Jain, A.K., Nandakumar, K., Nagar, A., 2008. Biometric template security. EURASIP J. Adv. Signal Process. 2008, 1–17.

Jain, A.K., Ross, A.A., Nandakumar, K., 2011. Introduction to Biometrics. Springer Science & Business Media.

Jeong, Y., Hwang, D., Kim, K.H., 2019. Blockchain-based management of video surveillance systems. In: 2019 International Conference on Information Networking. ICOIN, IEEE, pp. 465–468.

Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., et al., 2019. Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977.

Kamble, M.R., Sailor, H.B., Patil, H.A., Li, H., 2020. Advances in anti-spoofing: from the perspective of ASVspoof challenges. APSIPA Trans. Signal Inf. Process. 9.

Ke, X., Zhang, Y., 2020. Fine-grained vehicle type detection and recognition based on dense attention network. Neurocomputing 399, 247–257.

Kerr, M., Han, F., van Schyndel, R., 2018. A blockchain implementation for the cataloguing of cctv video evidence. In: 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance. AVSS, IEEE, pp. 1–6.

Kim, T., Jung, I.Y., Hu, Y.C., 2020. Automatic, location-privacy preserving dashcam video sharing using blockchain and deep learning. Hum.-centric Comput. Inf. Sci. 10 (1), 1–23.

Kirillova, E., Bogdan, V.V., Filippov, P., Tkachev, V., Zulfugarzade, T., 2020. The main features of blockchain technologies classification. COMPUSOFT: Int. J. Adv. Comput. Technol. 9 (10), 3900–3905.

Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W., Ali, I., 2021. An integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. Comput. Med. Imaging Graph. 87, 101812.

Lee, X.T., Khan, A., Sen Gupta, S., Ong, Y.H., Liu, X., 2020. Measurements, analyses, and insights on the entire ethereum blockchain network. In: Proceedings of the Web Conference 2020. pp. 155–166.

Lee, D., Park, N., 2020. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimedia Tools Appl. 1–18.

Li, R., 2020. Fingerprint-related chaotic image encryption scheme based on blockchain framework. Multimedia Tools Appl. 1–21.

Li, Y., Tu, Y., Lu, J., Wang, Y., 2020. A security transmission and storage solution about sensing image for blockchain in the Internet of Things. Sensors 20 (3), 916.

Liu, M., Shang, J., Liu, P., Shi, Y., Wang, M., 2018. VideoChain: trusted video surveillance based on blockchain for campus. In: International Conference on Cloud Computing and Security. Springer, pp. 48–58.

Liu, M., Teng, Y., Yu, F.R., Leung, V.C., Song, M., 2020a. A deep reinforcement learning-based transcoder selection framework for blockchain-enabled wireless D2D transcoding. IEEE Trans. Commun. 68 (6), 3426–3439.

Liu, M., Teng, Y., Yu, F.R., Leung, V.C., Song, M., 2020b. A mobile edge computing (MEC)-enabled transcoding framework for blockchain-based video streaming. IEEE Wirel. Commun. 27 (2), 81–87.

Lopes, V., Pereira, N., Alexandre, L.A., 2019. Robot workspace monitoring using a blockchain-based 3D vision approach. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

Lumini, A., Nanni, L., 2006. An advanced multi-modal method for human authentication featuring biometrics data and tokenised random numbers. Neurocomputing 69 (13–15), 1706–1710.

Mayer, O., Stamm, M.C., 2020. Exposing fake images with forensic similarity graphs. IEEE J. Sel. Top. Sign. Proces. 14 (5), 1049–1064.

McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., Granzotto, A., 2016. Bigchaindb: A Scalable Blockchain Database. White Paper, BigChainDB.

Mehta, R., Kapoor, N., Sourav, S., Shorey, R., 2019. Decentralised image sharing and copyright protection using blockchain and perceptual hashes. In: 2019 11th International Conference on Communication Systems & Networks. COMSNETS, IEEE, pp. 1–6.

Mendki, P., 2019. Blockchain enabled IoT edge computing. In: Proceedings of the 2019 International Conference on Blockchain Technology. pp. 66–69.

Michelin, R.A., Ahmed, N., Kanhere, S.S., Seneviratne, A., Jha, S., 2020. Leveraging lightweight blockchain to establish data integrity for surveillance cameras. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency. ICBC, IEEE, pp. 1–3.

Mittal, V., Tyagi, A., Bhushan, B., 2020. Smart surveillance systems with edge intelligence: Convergence of deep learning and edge computing. Available at SSRN 3599865.

Mohanta, B.K., Panda, S.S., Jena, D., 2018. An overview of smart contract and use cases in blockchain technology. In: 2018 9th International Conference on Computing, Communication and Networking Technologies. ICCCNT, IEEE, pp. 1–4.

Mohsin, A., Zaidan, A., Zaidan, B., Albahri, O., Albahri, A., Alsalem, M., Mohammed, K., 2019. Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. Comput. Stand. Interfaces 66, 103343. http://dx.doi.org/10.1016/j.csi.2019.04.002, URL: https://www.sciencedirect.com/science/article/pii/S0920548918304793.

Mudliar, K., Parekh, H., Bhavathankar, P., 2018. A comprehensive integration of national identity with blockchain technology. In: 2018 International Conference on Communication Information and Computing Technology. ICCICT, IEEE, pp. 1–6.

Naganuma, K., Suzuki, T., Yoshino, M., Takahashi, K., Kaga, Y., Kunihiro, N., 2020. New secret key management technology for blockchains from biometrics fuzzy signature. In: 2020 15th Asia Joint Conference on Information Security. AsiaJCIS, IEEE, pp. 54–58.

Nagothu, D., Xu, R., Nikouei, S.Y., Chen, Y., 2018. A microservice-enabled architecture for smart surveillance using blockchain technology. In: 2018 IEEE International Smart Cities Conference. ISC2, IEEE, pp. 1–4.

Nakamoto, S., Bitcoin, A., 2008. A peer-to-peer electronic cash system, 4. Bitcoin.–URL: https://bitcoin.org/bitcoin.pdf.

Nikouei, S.Y., Xu, R., Nagothu, D., Chen, Y., Aved, A., Blasch, E., 2018. Real-time index authentication for event-oriented surveillance video query using blockchain. In: 2018 IEEE International Smart Cities Conference. ISC2, IEEE, pp. 1–8.

Nyaletey, E., Parizi, R.M., Zhang, Q., Choo, K.-K.R., 2019. BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In: 2019 IEEE International Conference on Blockchain. Blockchain, IEEE, pp. 18–25.

Othman, A., Callahan, J., 2018. The horcrux protocol: a method for decentralized biometric-based self-sovereign identity. In: 2018 International Joint Conference on Neural Networks. IJCNN, IEEE, pp. 1–7.

Paralkar, K., Yadav, S., Kumari, S., Kulkarni, A., Pingat, S., 2018. Photogroup: Decentralized web application using ethereum blockchain. Int. Res. J. Eng. Technol. 5, 489–492.

Patel, D., Mistry, V., et al., 2018. Border control and immigration on blockchain. In: International Conference on Blockchain. Springer, pp. 166–179.

Patel, P., Thakkar, A., 2020. The upsurge of deep learning for computer vision applications. Int. J. Electr. Comput. Eng. 10 (1), 538.

Peck, M.E., 2017. Blockchain world-do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectr. 54 (10), 38–60.

Peixoto, J.P.J., Costa, D.G., 2017. Wireless visual sensor networks for smart city applications: A relevance-based approach for multiple sinks mobility. Future Gener. Comput. Syst. 76, 51–62.

Pongnumkul, S., Siripanpornchana, C., Thajchayapong, S., 2017. Performance analysis of private blockchain platforms in varying workloads. In: 2017 26th International Conference on Computer Communication and Networks. ICCCN, IEEE, pp. 1–6.

Predd, J.B., Kulkarni, S.B., Poor, H.V., 2006. Distributed learning in wireless sensor networks. IEEE Signal Process. Mag. 23 (4), 56–69.

Qi, X., Yu, K., Wen, Z., Katsuyama, Y., Sato, T., Tokuda, K., Sato, T., et al., 2020. Blockchain-based content-oriented surveillance network. In: 2020 IEEE 91st Vehicular Technology Conference. VTC2020-Spring, IEEE, pp. 1–6.

Ramachandran, G.S., Krishnamachari, B., 2018. Blockchain for the IoT: Opportunities and challenges. arXiv preprint arXiv:1805.02818.

Rebecq, H., Ranftl, R., Koltun, V., Scaramuzza, D., 2019. Events-to-video: Bringing modern computer vision to event cameras. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. pp. 3857–3866.

Reddy, R.V., prakash Reddy, V.J., Reddy, E.M., 2020. Automatic face expressions and gesture detection system using blockchain security. In: 2020 International Conference on Intelligent Engineering and Management. ICIEM, IEEE, pp. 296–300.

Sathish, S.K., Patankar, A.A., Khanna, H., 2019. Aurum: A blockchain based decentralized video streaming platform. In: 2019 IEEE Wireless Communications and Networking Conference. WCNC, IEEE, pp. 1–8.

Sawant, G., Bharadi, V., 2020. Permission blockchain based smart contract utilizing biometric authentication as a service: A future trend. In: 2020 International Conference on Convergence to Digital World-Quo Vadis. ICCDW, IEEE, pp. 1–4.

Seo, J., Cho, Y., 2020. Medical image sharing system using hyperledger fabric blockchain. In: 2020 22nd International Conference on Advanced Communication Technology. ICACT, IEEE, pp. 62–64.

Shafique, K., Khawaja, B.A., Sabir, F., Qazi, S., Mustaqim, M., 2020. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. IEEE Access 8, 23022–23040.

Shalaby, S., Abdellatif, A.A., Al-Ali, A., Mohamed, A., Erbad, A., Guizani, M., 2020. Performance evaluation of hyperledger fabric. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies. ICIoT, IEEE, pp. 608–613.

Shen, M., Deng, Y., Zhu, L., Du, X., Guizani, N., 2019. Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach. IEEE Network 33 (5), 27–33.

Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L., 2016. Edge computing: Vision and challenges. IEEE Internet Things J. 3 (5), 637–646. http://dx.doi.org/10.1109/JIOT.2016.2579198.

Shrier, D., Wu, W., Pentland, A., 2016. Blockchain & infrastructure (identity, data security). Mass. Inst. Technol.-Connect. Sci. 1 (3), 1–19.

Singh, A.K., 2020. A multi-layered network model for blockchain based security surveillance system. In: 2020 IEEE International Conference for Innovation in Technology. INOCON, IEEE, pp. 1–5.

Singh, M., Aujla, G.S., Bali, R.S., 2020. Odob: One drone one block-based lightweight blockchain architecture for internet of drones. In: IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops. INFOCOM WKSHPS, IEEE, pp. 249–254.

Smith, D.F., Wiliem, A., Lovell, B.C., 2015. Face recognition on consumer devices: Reflections on replay attacks. IEEE Trans. Inf. Forensics Secur. 10 (4), 736–745. http://dx.doi.org/10.1109/TIFS.2015.2398819.

Sreenu, G., Durai, M.S., 2019. Intelligent video surveillance: a review through deep learning techniques for crowd analysis. J. Big Data 6 (1), 1–27.

Sunyaev, A., 2020. Distributed ledger technology. In: Internet Computing. Springer, pp. 265–299.

Tang, H., Tong, N., Ouyang, J., 2018. Medical images sharing system based on blockchain and smart contract of credit scores. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking. HotICN, IEEE, pp. 240–241.

Taş, R., Tanrıöver, Ö.Ö., 2019. Building a decentralized application on the ethereum blockchain. In: 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies. ISMSIT, IEEE, pp. 1–4.

Toutara, F., Spathoulas, G., 2020. A distributed biometric authentication scheme based on blockchain. In: 2020 IEEE International Conference on Blockchain. Blockchain, IEEE, pp. 470–475.

Tsakanikas, V., Dagiuklas, T., 2018. Video surveillance systems-current status and future trends. Comput. Electr. Eng. 70, 736–753.

Vukolić, M., Hyperledger fabric. Genesis 1.

Wang, R., Tsai, W.-T., He, J., Liu, C., Li, Q., Deng, E., 2019. A video surveillance system based on permissioned blockchains and edge computing. In: 2019 IEEE International Conference on Big Data and Smart Computing. BigComp, IEEE, pp. 1–6.

Wu, H., Ashikhmin, A., Wang, X., Li, C., Yang, S., Zhang, L., 2020. Distributed error correction coding scheme for low storage blockchain systems. IEEE Internet Things J. 7 (8), 7054–7071.

Xu, Q., He, Z., Li, Z., Xiao, M., 2018. Building an ethereum-based decentralized smart home system. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems. ICPADS, IEEE, pp. 1004–1009.

Xu, R., Nikouei, S.Y., Chen, Y., Blasch, E., Aved, A., 2019. Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety. In: 2019 IEEE International Conference on Blockchain. Blockchain, IEEE, pp. 564–571.

Yasaweerasinghelage, R., Staples, M., Weber, I., 2017. Predicting latency of blockchain-based systems using architectural modelling and simulation. In: 2017 IEEE International Conference on Software Architecture. ICSA, IEEE, pp. 253–256.

Yatskiv, V., Yatskiv, N., Bandrivskyi, O., 2019. Proof of video integrity based on blockchain. In: 2019 9th International Conference on Advanced Computer Information Technologies. ACIT, IEEE, pp. 431–434.

Youssef, S.B.H., Rekhis, S., Boudriga, N., 2019. A blockchain based secure IoT solution for the dam surveillance. In: 2019 IEEE Wireless Communications and Networking Conference. WCNC, IEEE, pp. 1–6.

Zelensky, A., Voronin, V., Semenishchev, E., Svirin, I., Alepko, A., 2018. Video content verification using blockchain technology. In: 2018 IEEE International Conference on Smart Cloud. SmartCloud, IEEE, pp. 208–212.

Zerka, F., Urovi, V., Vaidyanathan, A., Barakat, S., Leijenaar, R.T., Walsh, S., Gabrani-Juma, H., Miraglio, B., Woodruff, H.C., Dumontier, M., et al., 2020. Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (C-DistriM). IEEE Access 8, 183939–183951.

Zhang, D., Guo, Z., Lu, G., Zhang, L., Liu, Y., Zuo, W., 2011. Online joint palmprint and palmvein verification. Expert Syst. Appl. 38 (3), 2621–2631.

Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J., 2018. Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services. Healthcom, IEEE, pp. 1–6.

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., Yalansky, L., 2017. Ensuring data integrity using blockchain technology. In: 2017 20th Conference of Open Innovations Association. FRUCT, IEEE, pp. 534–539.

Zupan, N., Zhang, K., Jacobsen, H.A., 2017. Hyperpubsub: a decentralized, permissioned, publish/subscribe service using blockchains. In: Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. pp. 15–16.