electronics

MDPI

Article

Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities

Kasun Moolikagedara, Minh Nguyen, Wei Qi Yan * and Xue Jun Li *

Citation: Moolikagedara, K.; Nguyen, M.; Yan, W.Q.; Li, X.J. Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities. *Electronics* **2023**, *12*, x. https://doi.org/10.3390/xxxxx

Academic Editor: Yolanda Blanco Fernández

Received: 21 July 2023
Revised: 21 August 2023
Accepted: 24 August 2023
Published: date

School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland 1010, New Zealand; kasun.moolikagedara@autuni.ac.nz (K.M.); minh.nguyen@aut.ac.nz (M.N.)
* Correspondence: weiqi.yan@aut.ac.nz (W.Q.Y.); xuejun.li@aut.ac.nz (X.J.L.)

Abstract: In this paper, we explore video blockchain for establishing connectivity among vehicles in a smart city through utilizing blockchain technology. By leveraging intelligent vehicular systems that provide location-based visualization through multiple deployed cameras in vehicles, we expand the scope of collecting video surveillance data for observation, thereby enhancing overall situational awareness. We utilize the decentralized nature of blockchain to implement a vehicle-based surveillance system across a smart city. To ensure reliability, the integration of two cryptographic functions, hashing and signing, with the blockchain is employed. This integration ensures secure and tamper-proof solutions for the existing intelligent surveillance system. In this paper, our primary focus is on combining blockchains to achieve sustainable and robust smart solutions for intelligent vehicular distributed video networks while eliminating the need for third-party intermediaries. Through extensive experiments and analysis, we demonstrate the effectiveness and feasibility of our proposed video blockchain approach. The results indicate that this innovative framework provides enhanced security, privacy, and scalability for intelligent vehicular distributed networks in smart cities, paving the way for a connected and efficient urban environment.

Keywords: video blockchain; distributed network; intelligent vehicular

1. Introduction

The rapid advancement of blockchain has significantly impacted multiple facets of society, necessitating the careful consideration of the complexities that play a vital role in community development and that enhance our daily lives. As we navigate this area, addressing both its positive and negative aspects becomes imperative. Therefore, in the context of contemporary technologies, ensuring security is of paramount importance. Particularly in smart cities, where sensitive information is abundant, the establishment of a highly secure repository is necessary.

The concept of a "smart city" represents an ambitious goal pursued by cities worldwide, driven by the intricate nature of urban environments and the potential offered by intelligent technologies. Within this context, it is crucial to thoroughly examine digital surveillance systems, as they hold significant importance today. Furthermore, prioritizing the safety and security of individuals by reducing crime rates and accidents stands as one of the primary objectives of smart cities [1,2].

In video surveillance [8], the primary objective is to capture video footage using vehicle cameras and securely store it onsite, leveraging blockchain to ensure data communication integrity and resistance against tampering and cyberattacks. Video surveillance serves multiple purposes, including crime solving, anomalous event detection, and privacy policy enforcement, making recorded video footage highly valuable for diverse applications. However, there exists a potential risk of malicious attackers, savvy hackers, or unauthorized third parties manipulating cameras and video repositories, rendering them ineffective in crime scenarios. These attacks may include false frame injection, data tampering, and privacy violations within a surveillance system. To address these challenges and enhance the security of video data captured using intelligent surveillance systems, we propose the following hypotheses:

- The utilization of a video blockchain framework will significantly enhance the security and integrity of video data;
- The integration of enhanced cryptographic functions, such as the Schnorr signature and hash (SHA256), within a video blockchain, along with the implementation of

Merkle trees, will establish a comprehensive security mechanism that ensures the robust storage, retrieval, and data integrity of video records within a network;

- The combination of vehicle cameras, blockchain, and third-party certificate authority (CA) verification will ensure the secure and sequential storage of video data and protect it from tampering and unauthorized access;
- The proposed video blockchain will effectively mitigate the risks associated with malicious attacks, data tampering, and privacy violations in "intelligent vehicular distributed video networks", thereby improving its effectiveness in crime scenarios.

In this paper, our focus was driven by our intention to combine video blockchain [3] with an enhancement of intelligent vehicular systems. We aimed for an evaluation of a novel method for capturing and storing video data using vehicle-mounted cameras and blockchain. Building upon existing work and implementing enhanced cryptographic functions, our objective was to enhance the security of vehicle videos in smart cities.

The rest of this paper is organized as follows. Section 2 provides a survey of related work, followed by a detailed presentation of our proposed method in Section 3, as well as a demonstration of the experimental results in Section 4 to assess the validity and effectiveness of our hypotheses. In Section 5, we discuss the results and conclude this paper, with the limitations and future work in Section 6.

2. Related Work

2.1. Theoretical Frameworks for Blockchain

In this paper, we explore how computational methods can be applied to video surveillance, focusing on the video blockchain approach that predominantly protects user identification by using hashed public keys [23]. Previous work [8] stored video footage from surveillance cameras and ensured the integrity of video data. However, the work did not cover the storage of real videos in the blockchain, which plays a significant role in simplifying human lifestyles across various sectors, including energy, healthcare, and supply chains [9,10].

The key feature of blockchain is to enable a decentralized community and reach consensus on a transparent transaction history without relying on pre-established trust, thus mitigating double-spending attacks [11,12]. The use of hash functions, particularly in the context of proof-of-work, has proven effective in resisting distributed denial-of-service (DDoS) attacks, as demonstrated by bitcoin.

In the process of calculating blockchain data, cryptographic encryption is employed to establish connections between preceding and succeeding blocks [26]. Each block has a block header, which contains the information necessary to establish the link between adjacent blocks and a block body that typically stores transaction details and records [19].

In a blockchain, each block contains specific information, including a local number indicating the block position in the chain, the identity of the source or creator, the hash value of the previous block, a timestamp, and a Merkle root. The hash value of the preceding block is critical for maintaining the integrity and continuity of the blockchain. The timestamp serves multiple purposes, ensuring the reliability, authenticity, and traceability of the data while preventing tampering [20].

2.2. Surveillance System for Smart Cities Approaches

The concept of smart cities [1] emerged during the 2008 economic crisis when the world sought to leverage information and communication technologies (ICT) to become more intelligent and resource-efficient. Smart cities aim to achieve cost and energy savings, improved service delivery and quality of life, and reduced environmental footprints [24].

A smart city includes a surveillance system that captures videos and aims to enhance the integrity of the recorded data. In [14], using Blocksee, through the method of using the event of a car accident, detected through built-in accelerometers, relevant videos were

cryptographically hashed and recorded through distributed storage on the blockchain. To ensure the integrity of the recorded videos, we leveraged the unique features of the distributed and tamper-proof characteristics offered by blockchain technology. In the blockchain, timestamping features are applied to verify and transfer unaltered data to a distributed repository. Similarly, Ref. [11] explored the use of blockchain-based systems to guarantee the storage of recorded data from closed-circuit television (CCTV) cameras in smart cities, preventing alteration or tampering. This mechanism assists law enforcement and clients in securing data recordings from digital surveillance systems by utilizing the metadata recorded in the blockchain. To ensure data security in a smart city, it is crucial to adhere to the principles of confidentiality, integrity, and availability (CIA) [5,17] in both video surveillance and video blockchain. Although video surveillance lacks built-in mechanisms to ensure secure data transfer, we can sort the videos in the correct order [22] and ensure their proper storage in a video blockchain without tampering. The video blockchain mechanism organizes the videos accurately in ascending or descending order from the video website and stores large data in the blockchain [28–30]. Additionally, blockchain addresses data integrity in systems such as medical record keeping and intelligent gas monitoring in smart cities [4,6,7].

2.3. Extracting Cryptographic Functions: Advances and Limitations

While considering smart cities worldwide, infrastructure security and data privacy emerge as two critical aspects. A distributed ledger, such as blockchain, offers enhanced security for connected electric vehicles [13]. Blockchain eliminates single points of failure and employs various cryptographic algorithms to ensure data integrity. Bitcoin, implemented with blockchain since 2009 [14,15], has extended its support to sophisticated sectors like smart cities. Blockchain has also eliminated the need for third-party involvement in transactions, providing a secure and transparent mechanism [18].

Hashing, a one-way function, guarantees transaction information without tampering. By converting plain text to irreversible hash data, the blockchain employs hashing algorithms such as SHA for data encryption. The blockchain encrypts transaction data in blocks using a hash algorithm and saves a unique string of 32-bit numbers mixed with an arbitrary three-column string. The integrity of the stored data is ensured through comparisons between hash values. To create a high-confidence smart city, we propose an approach that combines a (k, n) secret-sharing mechanism and software-defined networking (SDN) framework to secure data transportation among smart cities [16]. Data security is guaranteed by using the (k, n) secret-sharing scheme, while SDN-based transmission strategies leverage SDN's advantages in network management and are scheduled to overcome challenges posed by unstable network states. Extensive experiments demonstrated that this approach significantly reduces attack success rates with reasonable overhead.

A cryptographic hash function plays a crucial role in a blockchain by mapping arbitrary data to a fixed-size string. The security requirements for hash functions include one-way characteristics and collision resistance [22]. To ensure a minimum of 80-bit security, the output length of hash functions should be at least 160 bits. In blockchains, the general hash function is SHA256, which belongs to the SHA (secure hash algorithms) family of cryptographic hash functions. Hash functions in blockchains are utilized for various purposes, such as proof-of-work (PoW), address generation, block generation (as part of the Merkle-tree paradigm), signature validation, pseudorandom number generation, and other essential components, like the Fiat–Shamir mechanism.

A Merkle tree is employed to organize and represent the primary transaction data in a bottom-up manner. Each leaf node corresponds to a transaction, and the hash value of two transactions is computed to obtain the hash value of the intermediate node. This process continues until a final hash value, known as the Merkle root, is derived. Each set of transaction data has a unique Merkle root associated with it.

The Schnorr signature scheme reduces the computation required for signature generation, especially during idle time. The main computational work for generating signatures is independent of the message, and it involves multiplying a 2n-bit integer with an n-bit integer. The scheme is based on a prime modulus, p, where p-1 has a prime factor, q, of an appropriate size, satisfying the condition p-1 = 1 (mod q) [16]. Typically, p is chosen to be approximately 21,024, and q is approximately 2160, resulting in a 1024-bit number for p and a 160-bit number, which matches the length of the SHA-1 hash value [15].

In the field of cryptography, the Schnorr signature scheme is well known for its simplicity and security based on the intractability of discrete logarithm problems [25]. This scheme minimizes the computational effort required to generate a signature, and it is widely utilized in public-key cryptography for digital signatures. Digital signatures provide message authentication among communicating parties, protecting against fraudulent message creation or denial. Digital signatures involve the use of public-key algorithms among the communicating parties. The sender's private key is harnessed to encrypt either the entire message or a hash code of the message, forming the digital signature. Confidentiality can be further achieved by encrypting the entire message along with the signature using public or private key schemes. To resolve disputes, the signature function and the message must be accessible to a third party. However, the security of these approaches relies on the protection of the sender's private key against forgery, loss, or theft. Digital certificates and certificate authorities, along with timestamps and key revocation mechanisms, are commonly employed to address these security threats.

3. Proposed Video Blockchain

In this paper, a descriptive research design is employed to investigate a secure mechanism for linking vehicle-mounted cameras in a smart city. Both primary and secondary video data are utilized to achieve the research objectives. For primary data collection, videos from vehicle-mounted cameras were collected, and the images extracted from these videos were used for experimentation. This implementation was part of our studies in the visual blockchain [~~33~~] [21]. During the image encryption process, the raw image data were converted into a sequence of bytes, and the original data of the raw image could not be accessed once the encryption process was completed [21,27].

The main objective of this paper was to create a chain of blocks using vehicle videos and connect them in a distributed manner to ensure the correct video sequence without tampering, while minimizing the involvement of third parties in a smart city. To attain secure surveillance data communication using blockchain technology, a combination of a SHA-256 hash function and Schnorr signature was employed. The hash function ensures collision resistance, while the Schnorr signature scheme enhances the security of the communication.

Let (G', S', V') represent a signature scheme, and H (·) denotes a hash function with collision resistance properties. We utilized these components to achieve the desired security requirements for the communication of surveillance data over our blockchain.

Key Generation (G')**:**

- Generate a private key, s_k, randomly from the set $\boldsymbol{G}$;
- Compute the corresponding public key v_k as $v_k = g^{sk}$.

Signing (S'):

- Take a message, m, as input.
- Generate a random value, b, from the set of integers modulo, $|G|$;
- Compute u as $u = g^b$;
- Calculate a by applying the random oracle H (·) to u and the message m: $a = H(u, m)$;
- Compute s as $s = a * s_k + b \bmod q$, where q represents the modulus of the group **G**.
- Output the signature (a, s).

Verification (V'):

- Take a message, m, and a signature (a, s) as input;
- Retrieve the public key v_k;
- Compute u' as $u' = g^s * v_k^{(-a)}$;
- Calculate a' by applying the random oracle $H(\cdot)$ to u' and the message m: $a' = H(u', m)$;
- If a' is equal to a, the signature is considered valid. Otherwise, it is invalid.

In the context of blockchain data processing, the calculation involves generating both hashing and signature functions. This dual process ensures the integrity and security of the data. In this paper, we calculated the hash value using a specific hash function, such as SHA-256. This hash value acts as a unique identifier for the data, helping to ensure its integrity and prevent tampering.

To enhance the data protection of the vehicle-based video surveillance system in the smart city, we employed a third-party certification process. This involved collaborating with a certificate authority (CA) to verify the authority and authenticity of the data. The involvement of a trusted third party, such as a CA, adds an extra layer of security and credibility to the data.

Moreover, a private blockchain was employed to transmit the video data. By utilizing a private blockchain, we ensured that the data sent through the CA were received without any tampering. The private blockchain serves as a secure and decentralized platform for transmitting and storing video frame data, ensuring its integrity and protection. This mechanism, which combines the calculation of hash values, third-party certification, and the use of a private blockchain, effectively enhances the security and integrity of data in the vehicle-based video surveillance system in the smart city. It offers a reliable and trustworthy approach to guarantee the authenticity and integrity of data originating from vehicles.

In Algorithm 1, we assume the availability of a blockchain web service (Blockchain Web Service) and aim to process incoming requests (R_i) from authenticated nodes (N_i). The steps involved in the process include:

Algorithm 1: Blockchain-Based Image Encryption Process

Require: Blockchain Web Service
Ensure: Genesis Block
(1) while T has not expired do
(2) if node N_i is authenticated == **True** then
(3) if request R_i is matched == **True** then
(4) if Ri is identified as a processed request == **False** then
(5) process the response to C_i
(6) *Hash* (*video_frame_metadata*)
(7) *Sign* (*video_frame_metadata*)
(8) Update chain
(9) else
(10) Response to N_i that R_i is not a valid request
(11) end if
(12) else
(13) Deny the request
(14) end if
(15) Validate and add block into chain
(16) end if
(17) end while

In this updated version of Algorithm 2, a certificate authority (CA) has been introduced to provide certificates for the hashed features. The algorithm outlines a process for image encryption using blockchain and assumes the availability of a blockchain web service. Authenticated nodes can submit requests for image encryption, which are then vali-dated and processed according to specific conditions. Valid requests undergo the encryption process, which includes generating a response for the requesting node, hashing the video frame metadata, and signing it for integrity. The algorithm updates the blockchain by adding a new block containing the encrypted image or relevant information. Invalid requests are responded to accordingly, either by notifying the node of the issue or denying the request outright. The algorithm ensures the integrity and security of the blockchain by validating and adding processed blocks. It continues processing requests until a specified time has not expired. A certificate authority has also been introduced to generate certificates for the hashed features, enhancing security and verification capabilities.

Algorithm 2: Hashed Features Authentication Procedures

(1) **Function**: *hash_feature* (*features_set*)
(2) *string_features* [*empty_string*]
(3) for *feature_vector* in *features_set.items* do
(4) *feature_string* = *Convert_to_string* (*feature_vector*)
(5) *string_features* = (*string_features* || *feature_string*)
(6) end for
(7) *bytes_features* = *Convert_to_bytes* (*string_features*)
(8) *feature_hash* = *Convert_to_hash* (*bytes_features*)
(9) *feature_id* = *features_set.name*
(10) **return** {*feature_id: feature_hash*}

(11) **Procedure**: *record_hashed_feature* (*features_set*)
(12) *feature_tx* = *hash_feature* (*features_set*)
(13) *certificate* = *CertificateAuthority.generate_certificate* (*feature_tx*)
(14) *tx_result* = *transaction_commit*(*feature_tx*, *certificate*)

(15) **return** *tx_result*

(16) **Procedure**: *verify_hashed_feature* (*features_set*)
(17) *feature_tx* = *hash_feature* (*features_set*)
(18) *query_feature_tx* = *transaction_query* (*feature_tx*)
(19) if *query_feature_tx* == *feature_tx* then
(20) *verify_hash* = **True**
(21) else
(22) *verify_hash* = **False**
(23) end if
(24) **return** *verify_hash*

4. Results

The process involves converting captured videos into individual video frames, each ranging from 50 KB to 1024 KB. These frames were utilized to establish a private blockchain system using Microsoft Windows 11 Pro 64 bit. An experimental setup was executed to assess the efficacy of the proposed approach against various attacks. The experimentation led to the creation of innovative computational techniques for video blockchains, combining specific cryptographic algorithms with video blockchain technology. This article serves as a valuable contribution to the realm of video blockchain by introducing a fresh method for safeguarding video data in surveillance setups. The study's outcomes can serve as a cornerstone for forthcoming endeavors in both video blockchain and cryptographic algorithms.

Each root structure within the Merkle tree ensures the integrity of the connection between video frames and their respective hashing order. This safeguards against any alteration to the image sequence without modifying the entire root structure of the tree. Overall, these findings offer valuable insights into the advancement of web interfaces for video blockchain systems, and their implications can be harnessed to augment the dependability and security of such systems in the future.

The results in Figure 1 reflect Merkle tree-based approaches for data verification. The evaluation was conducted by measuring the computational time and amount of data for each experiment, with each experiment being repeated 100 times to minimize errors caused by outliers.

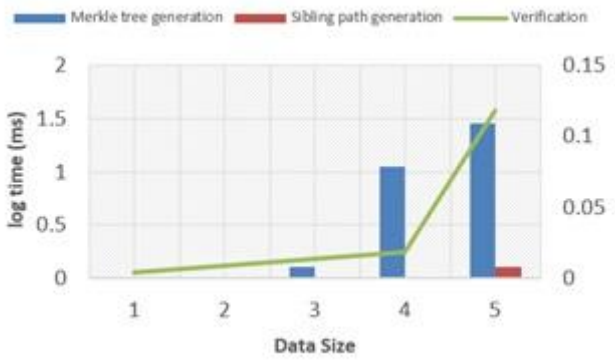

Figure 1. Average computational time (millisecond) for authentication based on Merkle tree by data size.

However, beyond 100 KB of data, these approaches exhibit only marginal differences. For instance, while generating a Merkle tree for a 1 MB data file, the prover's computational time is dominated by the process, accounting for approximately 99.9% of the total time, and the results are presented in a plot. The execution time varies based on

different input sizes and block sizes, and we analyzed this variability to ascertain the function's time complexity. Figure 2 illustrates the relationship between execution time (on the *y*-axis) and input size or block size (on the *x*-axis). This comparison encompasses various input sizes and block sizes, providing insights into the function's performance.

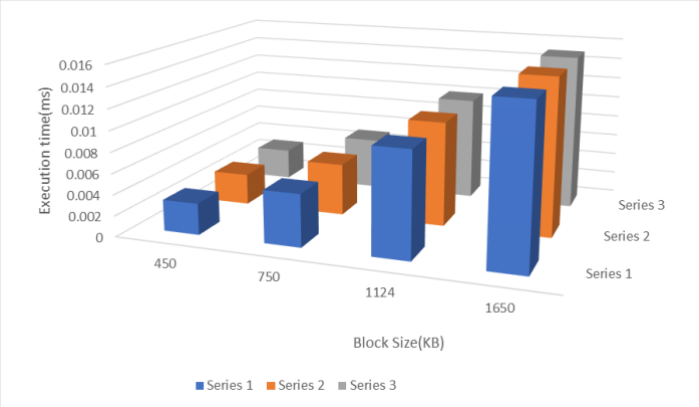

Figure 2. Execution times for different input sizes and block sizes.

In Figure 3, we also compare the computation time and data size metrics with those of other similar work. Our results show a significant change after a data size of 100 KB, indicating that the study's outcomes are comparatively reliable. These findings can be applied to improve the efficiency and accuracy of Merkle tree-based approaches for data verification.

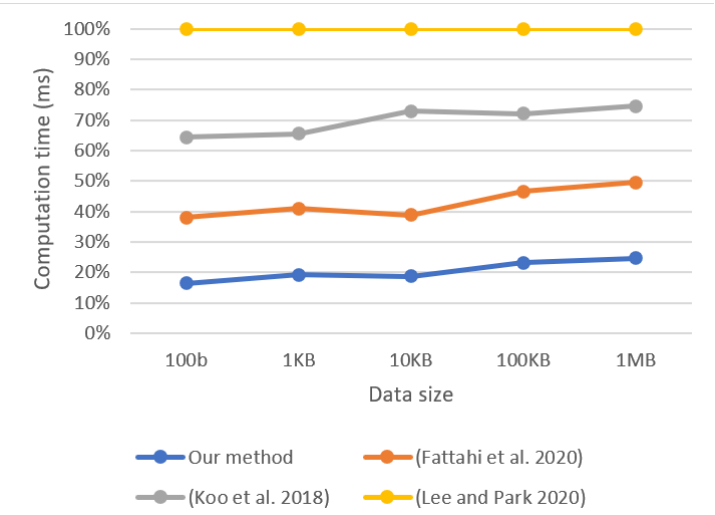

Figure 3. Comparison of the computational time between ours and other similar work.

The use of blockchain technology in intelligent surveillance faces many challenges, such as scalability, interoperability, and regulatory compliance. Scaling blockchain to handle large volumes of data and transactions, integrating it with the existing systems, and navigating regulatory frameworks are crucial areas requiring attention in this domain. In our future work, we plan to address these issues.

5. Discussion and Result Analysis

In this paper, our primary findings are rooted in videos captured from vehicles. To evaluate our video blockchain system, we established a blockchain environment using visual coding and the Hyperledger Fabric private blockchain platform. Hyperledger Fabric, designed for distributed ledger research and experimentation, facilitated the

creation of our private blockchain, enabling us to conduct comprehensive analyses. Additionally, we harnessed the integrated development environment (IDE) in MATLAB to gather computational results and compare them against video frame encryption. The MATLAB IDE was also employed to measure the success rates of our proposed method.

This paper contributes valuable insights into the evolution of web interfaces for video blockchain systems, outlining avenues for bolstering their reliability and security in forthcoming developments. Our recorded videos yielded results for the number of pixels change rate (NPCR) of 99.6021% and the unified averaged changed intensity (UACI) of 33.4065%. Table 1 shows a comparison with other results, indicating our method outperforms others. In Equation (1), *M* denotes the width (i.e., number of columns) of the images, and *N* signifies the height (i.e., number of rows) of the images.

$$\boldsymbol{P} = \boldsymbol{M} * \boldsymbol{N}. \quad (1)$$

Let I1(i, j) and I2(i, j) represent the pixel values at position (i, j) in the first and second images, respectively. Equation (1) calculates the normalized pixel difference rate (*NPCR*) as a percentage. It quantifies the proportion of pixels that differ between the two images and is computed by summing the absolute differences between corresponding pixel values ($|I1(i,j)-I2(i,j)|$) and dividing it by the total number of pixels ($M * N$), multiplied by 100.

$$NPCR = \frac{\Sigma\, |\mathrm{I1(i,j)} \neq \mathrm{I2(i,j)}|}{(\mathrm{M} * \mathrm{N})} \times 100 \quad (2)$$

where *UACI* provides an indication of the average changing intensity difference between the two images. Higher *UACI* values indicate greater average changing intensity differences, while lower *UACI* values suggest that the images have more similar average intensities. In this context, Σ represents the summation over all pixel positions (*i*, *j*). Additionally, $|I_1(i, j)–I_2(i, j)|$ denotes the absolute difference in pixel values between corresponding positions (*i*, *j*) in the two images.

$$UACI = \frac{\Sigma\, |I_1(x,y) - I_2(x,y)|}{(\mathrm{M} * \mathrm{N} * \mathrm{L})} \times 100 \quad (3)$$

Table 1. Comparisons of deferential attack.

Type of Test	This Work	Belazi et al. [31]	Muhammad et al. [30]
NPCR	99.6021	99.6098	99.61
UACI	33.40	33.4384	33.44

We also established a peer-to-peer (P2P) network to interconnect the vehicle cameras and created a blockchain network using the required vehicles category in the smart city. For instance, the blockchain model can be applied to monitor city activities. Compared to the traditional client–server model, this P2P model offers numerous benefits. On the other hand, current surveillance systems heavily depend on service availability. However, a client–server architecture cannot guarantee high availability [31] because of its inherent nature. This structured P2P network continues to function even in the event of a node failure because of its distributed nature. Thus, we ensure the system's availability for users and maintain the security of the system's data.

It is noteworthy that while the results largely align with our expectations, there exist slight discrepancies when compared to the results of other studies. These variations can be attributed to several factors. Firstly, the choice of blockchain platform and encryption algorithms can lead to nuances in the results because of their inherent characteristics. Additionally, differences in the types of videos, varying frame rates, and even environmental conditions during recording could contribute to these deviations. These

discrepancies are not unexpected within the realm of research, as the uniqueness of each approach and experimental setup can inevitably lead to divergent outcomes.

In conclusion, our discussion of the results highlights the alignment between our anticipated outcomes and the actual findings of our study. Moreover, the comparative analysis against other related research lends credence to the effectiveness of our video blockchain system. The minor discrepancies identified can be attributed to a combination of methodological choices and contextual variations. This discussion, thus, reinforces the value of our research in advancing the field of video blockchain systems while also acknowledging the nuanced nature of the experimental results in a diverse research landscape.

6. Conclusions

This paper presents a video blockchain framework that validates the hypotheses formulated in the study. The results underscore the significant enhancement in security and data integrity achievable through the utilization of a video blockchain within smart city surveillance systems. This outcome posits that the integration of a video blockchain establishes a robust security mechanism for the storage and retrieval of surveillance camera video records. Moreover, the inclusion of Merkle trees in the video blockchain architecture further bolsters the security and data integrity of the surveillance system.

The combination of vehicle cameras, blockchain technology, and third-party certification authority (CA) verification ensures the secure and sequential storage of video data, protecting it against tampering and unauthorized access. Lastly, the proposed video blockchain approach effectively mitigates the risks associated with malicious attacks, data tampering, and privacy violations in surveillance systems, enhancing their effectiveness in crime scenarios.

This paper contributes to the field by establishing a link between video frames captured by intelligent surveillance systems and blockchain. By leveraging cryptographic functions and decentralized storage platforms, the security of vehicle camera transferring video data is significantly improved. The proposed blockchain-based approach not only enhances the security and integrity of vehicle video data but also promotes trust, reliability, and controlled disclosure in smart cities. Throughout this paper, one of the identified limitations pertains to the necessity of maintaining a minimum number of connected nodes to enhance the system's availability. Additionally, our method is not resistant to quantum computer attacks. Taking into account these limitations, we plan to extend our research in future endeavors to enhance the system's resistance against attacks from quantum computers. This approach is of significant value to law enforcement monitoring, autonomous vehicles, insurance providers, and traffic management systems, providing increased security and adaptability for an advanced vehicular distributed video network in smart urban environments.

Author Contributions: Conceptualization, K.M and W.Q.Y.; methodology, K.M.; software, K,M.; validation, K.M.; formal analysis, K.M.; investigation, K.M.; resources, K.M and W.Q.Y.; data curation, K.M.; writing—original draft preparation, K.M.; writing—review and editing, K.M., W.Q.Y., M.N., and X.J.L.; visualization, K.M.; supervision, W.Q.Y. and M.N.; project administration, X.J.L., W.Q.Y., and M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript.

NPCR	Normalized pixels change rate

UACI	Unified average changing intensity

References

1. Aldairi, A.; Tawalbeh, L. Cyber security attacks on smart cities and associated mobile technologies. *Procedia Comput. Sci.* **2017**, *109*, 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391.
2. Alketbi, A.; Nasir, Q.; Abu Talib, M. Novel blockchain reference model for government services: Dubai government case study. *Int. J. Syst. Assur. Eng. Manag.* **2020**, *11*, 1170–1191. https://doi.org/10.1007/s13198-020-00971-2.
3. Gedara, K.; Nguyen, M.; Yan, W. Visual Blockchain for Intelligent Surveillance in a Smart City. In *Blockchain Technologies for Sustainable Development in Smart Cities*; IGI Global: Hershey, PA, USA, 2021.
4. Chen, J.; Ruan, Y.; Guo, L.; Lu, H. BCVehis: A blockchain-based service prototype of vehicle history tracking for used-car trades in China. *IEEE Access* **2020**, *8*, 214842–214851. https://doi.org/10.1109/ACCESS.2020.3040229.
5. Chen, Y.C.; Chou, Y.P.; Chou, Y.C. An image authentication scheme using Merkle tree mechanisms. *Future Internet* **2019**, *11*, 149. https://doi.org/10.3390/fi11070149.
6. Chen, X.; Xing, Z.; Karki, B.; Li, Y.; Chen, Z. Blockchain simulation: A web application for it education. In Proceedings of the IEEE Annual Computing and Communication Workshop and Conference 2021, Virtual, 27–30 January 2021; pp. 486–491. https://doi.org/10.1109/CCWC51732.2021.9375934.
7. Chukwu, E.; Garg, L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access* **2020**, *8*, 21196–21214. https://doi.org/10.1109/ACCESS.2020.2969881.
8. Deepak, K.; Badiger, A.N.; Akshay, J.; Awomi, K.A.; Deepak, G.; Harish Kumar, N. Blockchain-based management of video surveillance systems: A survey. In Proceedings of the International Conference on Advanced Computing and Communication Systems 2020, Coimbatore, India, 6–7 March 2020; pp. 1256–1258. https://doi.org/10.1109/ICACCS48705.2020.9074197.
9. Engelhardt, M.A. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. https://doi.org/10.22215/timreview/1111.
10. Fill, H.; Haerer, F. Knowledge blockchains: Applying blockchain technologies to enterprise modeling. In Proceedings of the Hawaii International Conference on System Sciences 2018, Waikoloa Village, HI, USA, 3–6 January 2018; pp. 4045–4054.
11. Fitwi, A.; Chen, Y. Secure and privacy-preserving stored surveillance video sharing atop permissioned blockchain. In Proceedings of the International Conference on Computer Communications and Networks 2021, Athens, Greece, 19–22 July 2021; pp. 1–8.
12. Fu, J.; Qiao, S.; Huang, Y.; Si, X.; Li, B.; Yuan, C. A study on the optimization of blockchain hashing algorithm based on PRCA. *Secur. Commun. Netw.* **2020**, *2020*, 8876317. https://doi.org/10.1155/2020/8876317.
13. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5760–5772.
14. Gallo, P.; Pongnumkul, S.; Nguyen, U.Q. BlockSee: Blockchain for IOT video surveillance in smart cities. In Proceedings of the IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (2018), Palermo, Italy, 12–15 June 2018. https://doi.org/10.1109/EEEIC.2018.8493895.
15. George, R.V.; Harsh, H.O.; Ray, P.; Babu, A.K. Food quality traceability prototype for restaurants using blockchain and food quality data index. *J. Clean. Prod.* **2019**, *240*, 118021. https://doi.org/10.1016/j.jclepro.2019.118021.
16. Gergely, A.M.; Crainicu, B. Randadminsuite: A new privacy-enhancing solution for private blockchains. *Procedia Manuf.* **2020**, *46*, 562–569. https://doi.org/10.1016/j.promfg.2020.03.081.
17. Gřivna, T.; Drápal, J. Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digit. Investig.* **2019**, *28*, 1–13. https://doi.org/10.1016/j.diin.2018.12.002.
18. Mayer, H. (2016). ECDSA security in bitcoin and ethereum: a research survey. CoinFaabrik, June, 28(126), 50.Hasan, O.; Brunie, L.; Bertino, E. Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey. Ph.D. Thesis, University of Lyon, Lyon, France, 2023.
19. Hou, L.; Zheng, K.; Liu, Z.; Xu, X.; Wu, T. Design and prototype implementation of a blockchain-enabled lora system with edge computing. *IEEE Internet Things J.* **2021**, *8*, 2419–2430. https://doi.org/10.1109/JIOT.2020.3027713.
20. Gedara, K.M.; Nguyen, M.; Yan, W.Q. Enhancing privacy protection in intelligent surveillance: Video blockchain solutions. *BLOCKCHAIN'23 proceedings published by Springer LNNS*
21. Khan, P.W.; Byun, Y.C.; Park, N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics* **2020**, *9*, 484. https://doi.org/10.3390/electronics9030484.
22. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022.
23. Khrais, L.T. The combination of iot-sensors in appliances and block-chain technology in smart cities energy solutions. In Proceedings of the International Conference on Advanced Computing and Communication Systems 2020, Coimbatore, India, 6–7 March 2020; pp. 1373–1378. https://doi.org/10.1109/ICACCS48705.2020.9074362.
24. Koo, D.; Shin, Y.; Yun, J.; Hur, J. Improving security and reliability in Merkle tree-based online data authentication with leakage resilience. *Appl. Sci.* **2018**, *8*, 2532. https://doi.org/10.3390/ap.
25. Kullig, N.; Lämmel, P.; Tcholtchev, N. Prototype implementation and evaluation of a blockchain component on IoT devices. *Procedia Comput. Sci.* **2020**, *175*, 379–386. https://doi.org/10.1016/j.procs.2020.07.054.
26. Kumar, M.; Kaur, G. High performance scalable recursive block matrix inverse for multicore architectures. In Proceedings of the International Conference on Parallel, Distributed and Grid Computing 2022, Solan, India, 25–27 November 2022; pp. 45–49.

27. Lee, D.; Park, N. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. *Multimed. Tools Appl.* **2020**, *80*, 34517–34534. https://doi.org/10.1007/s11042-020-08776-y.
28. Li, T.; Chen, Y.; Wang, Y.; Wang, Y.; Zhao, M.; Zhu, H.; Tian, Y.; Yu, X.; Yang, Y. Rational protocols and attacks in blockchain system. *Secur. Commun. Netw.* **2020**, *2020*, 8839047.
29. Majdoubi, D.E.L.; El Bakkali, H.; Sadki, S. Towards smart blockchain-based system for privacy and security in a smart city environment. In Proceedings of the International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (2020), Marrakesh, Morocco, 24–26 November 2020. https://doi.org/10.1109/CloudTech49835.2020.9365905.
30. Belazi, A.; Abd El-Latif, A.A.; Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **2016**, *128*, 155–170. https://doi.org/10.1016/j.sigpro.2016.03.021.
31. Muhammad, K.; Hamza, R.; Ahmad, J.; Lloret, J.; Wang, H.; Baik, S.W. Secure surveillance framework for IoT systems using probabilistic image encryption. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3679–3689.