Towards an YouTube Verified Content System based on Blockchain Approach

Phuc Nguyen Trong, Hong Khanh Vo, Luong Hoang Huong, Khiem Huynh Gia,
Khoa Tran Dang, Hieu Le Van, Nghia Huynh Huu, Tran Nguyen Huyen, The Anh Nguyen,
Loc Van Cao Phu, Duy Nguyen Truong Quoc, Bang Le Khanh, Kiet Le Tuan
FPT University, Can Tho City, Viet Nam

Abstract— **YouTube connects people with each other through an online video sharing service platform. With the great development of the entertainment industry, content on YouTube is accessible to many people of different ages. However, verifying the content posted on YouTube is clean or not is a difficult problem. Dirty content is violent, pornographic and vulgar content that causes serious psychological harm to the segment of users under the age of 18, i.e., especially those of an age who are not yet aware of the harmful effects of content. Toxic will bring to the child's behavior. Agree that Google (i.e., YouTube) has developed a YouTube Kid application where the videos are only for children under the age of 13. However, cultural and educational differences between regions strongly influence the choice of children. Select content for children. Therefore, the content restrictions on the YouTube Kid application have not yet met all the requirements of parents around the world. There have been many development directions to identify videos containing malicious content based on deep learning. However, there is no method to build a tool to support parents of children to share and identify videos with objectionable content (e.g., violence, pornography, obscene words) on the YouTube platform. In this research paper, we introduce YVC, a YouTube-verified content platform by applying blockchain's distributed, public validation. This tool helps parents validate YouTube content and issue a report to reduce dirty content on YouTube. To demonstrate the effectiveness of our approach, we implement the proof-of-concept in the three most popular EVM platforms: Ethereum, Fantom, and the Binance smart chain. Compared to the YouTube Kids (i.e., the most common shared video platform for the under 13-year-old kid), our approach is able to capture the video preferences of the parents covering the difference areas/countries.**

Keywords—Blockchain technology; public authentication; Ethereum; Fantom; Binance smart chain platform; social media platform

I. Introduction

With the development of technology, many social media platforms are born and become indispensable parts of people's lives. Among them, the YouTube video-sharing platform is a prominent online presence that provides various types of content for today's society. With a large and wide user base, YouTube has opened a monetization policy for creators, and this policy becomes a potential monetization target not only for large companies but also for individual creators [1].

Dirty content appears to creep inside the content on Youtube in an uncontrollable way. As Hank Green notes, YouTube is "a bridge between creators who are making stuff and advertisers who want to make money. YouTube makes its money through these people but also has to keep both of these groups happy" [2]. Creators all want their video products to attract many people, the ultimate purpose is to develop media channels and earn profits. To attract more people, dirty content with erotic and violent nature gradually crept into the daily entertainment content.

Other social platforms (e.g., Reddit, Twitter) have done a lot of research regarding the issue of detecting harmful content (i.e., violence, calls to violence, pornography). For example, Tseng et al. [3] and Bellini et al. [4] highlight how forums like Reddit serve as platforms for discussing methods of intimate partner violence. Similarly, abuse, cyberbullying, and online harassment on online platforms such as Twitter was also studied by [5], [6]. For work related to malicious behavior detection on the YouTube platform, Chu et al. [1] exploits the differences used to monetize illegal YouTube content that could potentially harm viewers and other users. Thereby, the authors propose methods to prevent abuse of this service (similar findings are presented in the Related Work section of the article).

YouTube has taken a remedy by censoring and removing violent and pornographic content on the platform. In addition, the age restriction mode for adults and minors is set on the admin rights of the creator. Moreover, YouTube launched [7], a version made entirely for children to prevent children from accidentally being exposed to dirty content that causes psychological effects. However, the measures taken by Youtube have not eliminated the dirty content that is being uploaded every day. A weakness of the age limit when watching videos lies in the admin rights of the creator. If the creator intentionally does not limit the age before giving the product to the user segment older than 18, the content will still be published. open, anyone can enter. Recognizing the advantages and risks of harmful content for children's education and entertainment, Google founded YouTube Kids to serve children under 13 years old. Based on the regulations for child-friendly programs, a number of violations were identified and restricted to television programs. When a child surfs the Internet, the same rules can be automatically detected and filtered. However, content filtering on YouTube for Kids currently relies on metadata attributes, where inappropriate content can pass the [8] filter.

Blockchain technology is known for its outstanding features of transparency and immutable content. Picha Edwardsson et al. studied the possibility of using blockchain technology to create a secure, community-facing information verification database with the goal of creating a solution that could improve the reliability of verifying information and monitoring each authenticity verification process for digital content, including images and videos. The paper indicates that blockchain is not yet ready to be directly applied to fact-checking processes in a real-world scenario. The study also shows that the application of blockchain to verify a scenario is entirely possible and highly reliable and transparent [9]. Several approaches address these problems by applying Blockchain techniques in the other environment (e.g., cash-on-delivery [10], [11], [12], healthcare [13], [14], [15], supply chain [16], [17], [18], and others [19], [20], [21]).

To solve the problem of verifying dirty content through social media platforms (specifically in the research paper, YouTube). We introduce YouTube verify content system based on blockchain (YVC). YVC's purpose is to verify dirty content on youtube platform and store it on blockchain platform. The purpose of storing data on the blockchain platform is data transparency and community application. With the YVC system, we build three main user groups: Reporter, Verifier and Middleman. YVC system consists of 6 main steps from Reporter report content then to Verifier verifying dirty content and Middleman is responsible for forwarding verified data back to social media platform. Besides, to define the logical constraints in the smart contract to maintain the stable operation of the system, we also design the authorization service for the stakeholders. To design logical constraints on smart contracts, we additionally exploit Solidity language[1]. To evaluate YVC, we implemented a test model on all three of the most popular platforms that currently support EVM, including Ethereum[2], BNB Smart Chain[3] and Fantom[4].

The research problem of this article is to define the YouTube-communication channel based on blockchain and smart contract technologies, which support the parents can detect and share the violation content of the videos before reporting those videos to the Youtube. This approach also define the protocol to verify the voting from the check based on crowdsourcing approach. Therefore, the contribution of this paper is threefold: i) designing the YVC (i.e., Youtube verify content) model to support the user detect the unusual content; ii) implementing the proof-of-concept based on the blockchain and smart contract technologies; and iii) deploying the proof-of-concept on the three most common EVM-supported blockchain platform (i.e., ETH, BNB, Fantom) to select the most suitable platform.

Following this introduction, a state-of-the-art is presented to help understand the limitations and challenges of the current approaches. Then we define the architecture of the blockchain-based YVC system, and we also verify the structure of the smart contract and the database. In the next section, we describe the implementation process including the smart contract, data structure, YVC execution algorithm, and authorization. Section 6 focuses on the evaluation process based on deploying YVC in the three platforms. Finally, suggestions for future research and conclusion are made in the last section.

II. Related Work

Detect illegal activity on YouTube. The YouTube ecosystem has been studied to identify harmful content. Recent works analyzed the metadata and sharing features (i.e. keywords, hashtags) on spam YouTube videos [22], [23]. Another line of work focuses on the automatic classification of harmful activity on YouTube. Fueled by Elsagate, a controversy in which YouTube videos classified as children's content contain inappropriate themes (e.g. Elsa in the Disney movie Frozen performs the action. pique). Papadamou et al. [24] have developed a binary classifier to detect potentially annoying/harmful YouTube videos for toddlers. Similarly, several efforts have identified spam and clickbait videos by studying video metadata, comments, user activity, and video attributes [25], [26], [27]. On the contrary, we provide an overview of malicious content based on user reviews through a user-review sharing system based on blockchain technology. Our system aims to detect malicious behavior based on two aspects (i.e., content sharer and content identifier).

Based on the benefits of the blockchain-based system, more and more information verification systems are built on a blockchain platform for the purpose of transparent verification and community application. As a prime example of the application of blockchain technology in content verification, Ghimire et al propose a new method of video integrity verification method (IVM) using the blockchain technology framework. The study aims to verify data integrity and avoid tampering with video recordings in providing evidence of crime scenes or road accidents. The verification process is done by shredding the videos and comparing them with the hash value of the video previously stored in the blockchain [28].

The integrity verification method (IVM) applied by Ghimire, et al. in the blockchain platform shows that blockchain brings a new transparent and community-oriented approach to content verification in the digital age. In addition, Sathish, et al. developed Aurum [29], a new multimedia streaming platform that hosts user-generated channels with authenticated content through the use of a blockchain-driven creative process. The platform requires public content verification and the goal of community-driven development in which the research paper also mentions that the Aurum system uses effective support protocols to ensure QoS.

Aiming at community authentication and authenticity transparency, Banerjee, Prabal, et al. develop a trusted and fair platform for sharing content without a central moderator. Banerjee, Prabal, et al. have applied blockchain to manage content lists and also use smart contracts to support storage [30]. The system is built on Hyperledger Fabric and the data layer is built on Tahoe-LAFS with the goal of scalability at a lower cost than the Ethereum blockchain platform.

Besides, Zelensky, et al. also have a research paper on analyzing and verifying video data [31]. The problem of data validation to avoid interference and correct the content of violations, banking, remote management, and action confirmation. In which the algorithm will use Swype code using the movement mobile camera to verify the video content. However, the research paper by Zelensky, Aleksandr, et al. still uses a third-party intermediary to verify the content and does not really highlight the characteristics of the blockchain.

[1] Solidity is an object-oriented, high-level language for executing smart contracts. Smart contracts are programs that govern the behavior of accounts in the Ethereum state https://docs.soliditylang.org/en/v0.8.7/

[2] Ethereum https://ethereum.org/en/whitepaper/

[3] Binance Smart Chain https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md

[4] Fantom https://fantom.foundation/research/wp_fantom_v1.6.pdf

Compared with previous approaches, YouTube verified content system (YVC) builds a content authentication system applying blockchain technology on social media platforms (specifically in the research paper, YouTube). In addition, YVC aims at a transparent authentication application for the community, which also reduces the error when third parties approach.

III. YVC Architecture

YouTube verifies content based on the blockchain architecture depicted in Fig. 1. YVC consists of three main elements Reporter, Verifier, and Middleman.

- *Reporter*: The person who reports dirty content to YVC. In the YVC system, the reporter acts as an information provider, the reporter is anonymous on the system and does not need to pay gas fees when providing information.
- *Verifier*: The person who verifies the content on the YVC system. In the YVC system, the verifier acts as a content verifier, and the address information of the verifier will be public on the blockchain. However, personal information will be kept anonymous. Besides, Verifier will bear a small gas fee for verification work.
- *Middleman*: An intermediary who forwards verified and publicized reports to social media platforms (specifically in our research, Youtube).

Platforms applied in the YVC system include Website, Smart Contract, and social media platform.

- *Website*: This is the place where the information is reported and waiting for verification. In the YVC system, the website is the place where the verifier interacts with the smart contract to verify the reported content.
- *Smart Contract*: This is where the verification information of the verifier is stored. In this study, we implement smart contract deployment on the Ethereum blockchain platform and Binance smart chain platform.
- *Social Media Platforms*: These are the social networking platforms where content is stored. In the YVC system, we focus on the Youtube social networking platform.

According to Fig. 1, YVC has six steps. . In the first step, the Reporter is a viewer of the content on social media platforms (Specifically in the research paper, YouTube), if it feels that the content contains vulnerable content, the Reporter will report that content through the website of the YVC system. In the second step, the report information is displayed on the web, now everyone when accessing the website can see the reported content. In the third step, Verifier will verify content to see if the reported content contains objectionable content or not. When the verification is successful, the information about the verified content will be published on the blockchain (specifically in the research we will publish on the Ethereum blockchain platform and Binance smart chain platform). One thing to note is that, in the third step, Verifier will incur a fee to publish verification information on the blockchain, this fee is called a gas fee. In the fourth step, when the content is successfully verified, the content is also pushed to the database of the YVC system, about the storage structure we will go into details in the following section. In the fifth step, Middleman is the database administrator, Middleman has the role of getting data from the database and reporting back to social media platforms (specifically YouTube). Note that, because the information is publicly published on the blockchain, if Middleman changes the information in the database, the real information is still public and traceable. From there, it can be seen that the application of blockchain helps to reduce the intervention of third parties. In the sixth step, after successfully retrieving data from the database, Middleman reports that data to the social media platform where the reported content originated. In this step, the social media platform based on data reported by Middleman and verified on blockchain to incinerate vulnerable content on their platform. Note that, since the information on the blockchain is public and immutable, social media platforms' reporting disregard for content is minimized.

IV. Implementation

A. Smart Contract Structure

- The address (on blockchain) of verifier (`verifier`).
- The name of channel which includes on the report content (`channelName`).
- The name of video which includes on the report content (`videoName`).
- The link of video on social media flatform which includes on the report content (`linkOfVideo`).
- Duration of the start of the video containing vulnerable content (`startVulnerableDuration`).
- Duration of the end of the video containing vulnerable content (`endVulnerableDuration`).
- The verified information will be stored in the verify content with the declared struct type (`verifyContent`). The information inside the struct will be determined by two data types: boolean for true/false verification and string for storing results.

All information in the Verify field will be stored inside the smart contract (see Fig. 2). This storage will contribute to transparency between Reporter, Verifier, and Middleman. If any changes are made, the changed data will be made public on the blockchain network.

To determine whether the verified information is true or false. Verify the information is a set of variables stored inside (`verifyContent`) with data type struct. The information to verify includes (`channelName`) verified true or false by (`isChannelName`), similar to (`videoName`) will be verified by (`isVideoName`), with (`linkOfVideo`) will be verified by (`isLinkOfVideo`), with (`startVulnerableDuration`) will be verified by (`isStartVulnerableDuration`), with (`endVulnerableDuration`) will be verified verified by (`isEndVulnerableDuration`), and finally verifyResult

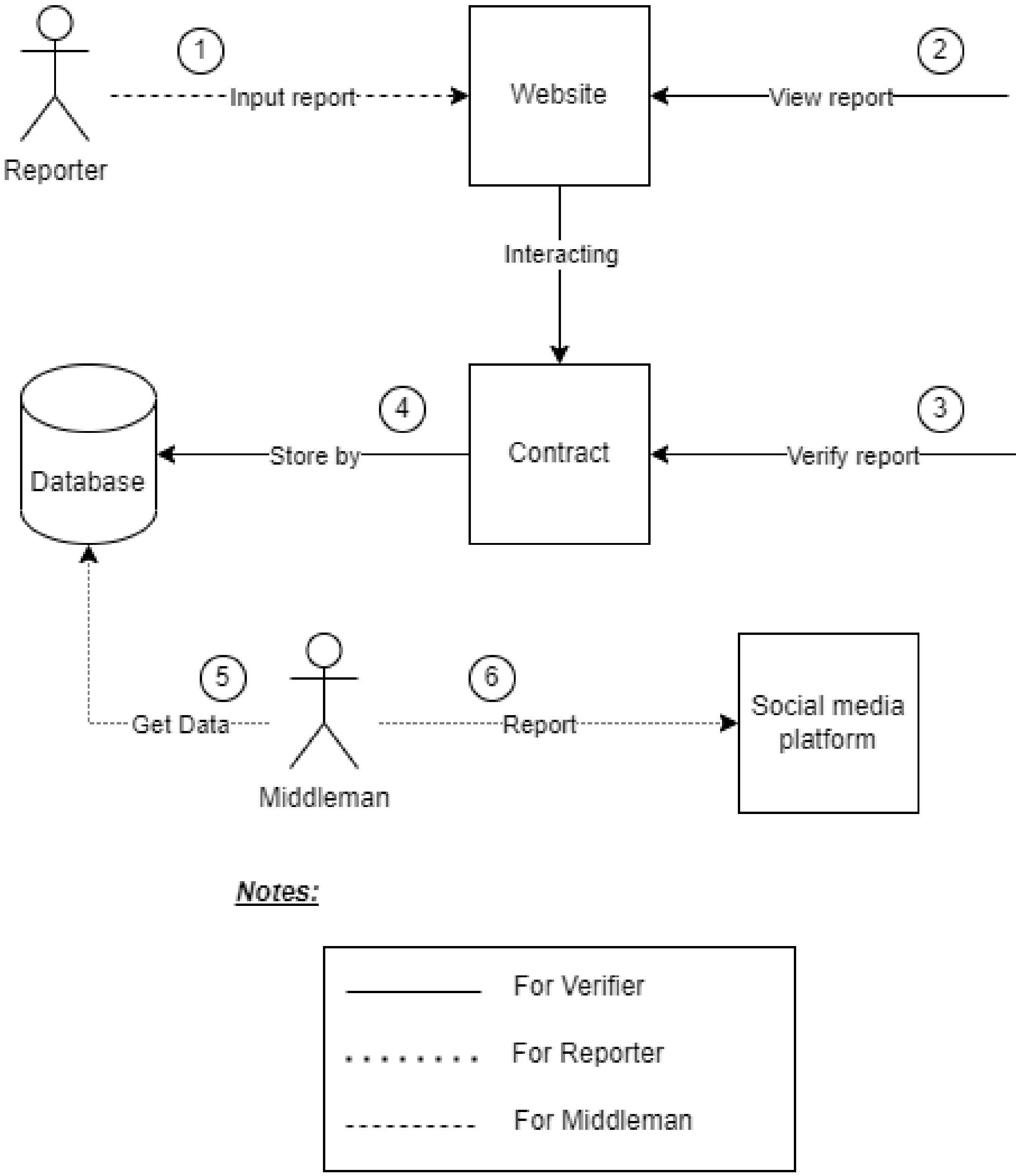

Fig. 1. Youtube Verify Content (YVC) base on Blockchain Architecture.

will save the verification result of the (`verifier`), (`verifyResult`) will be automatically programmed to display the result based on the verification result of the Verifier.

The final result received after verifying content is in the (`verifyResult`) variable. The result will be a set of true or false evaluations of the reported information and a string that evaluates the result (`verifyResult`) based on the evaluation of the (`verifier`).

B. Database Structure

Fig. 3 describes the structure of the database. The list below details the component in the structure.

- The name of channel which includes on the report content (`channelName`).
- The name of video which includes on the report content (`videoName`).
- The link of video on social media flatform which includes on the report content (`linkOfVideo`).
- Duration of the start of the video containing vulnerable content (`startVulnerableDuration`).
- Duration of the end of the video containing vulnerable content (`endVulnerableDuration`).
- The address of the contract. Is a blockchain platform where verified content is stored.

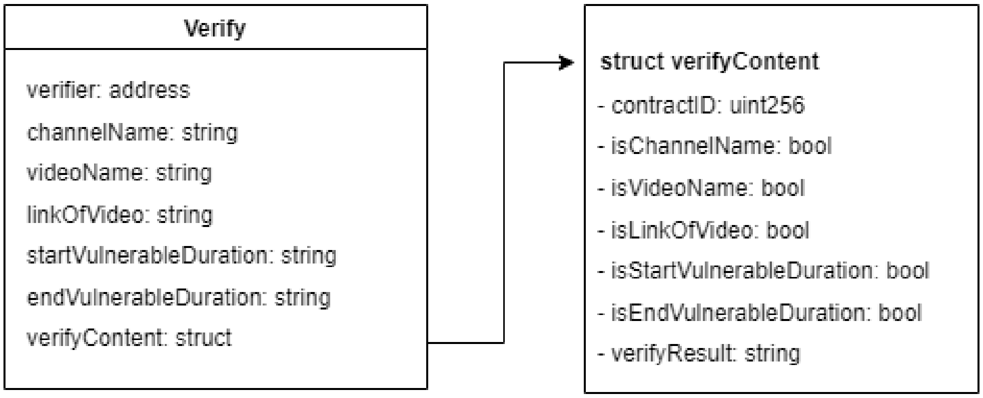

Fig. 2. Smart Contract Structure.

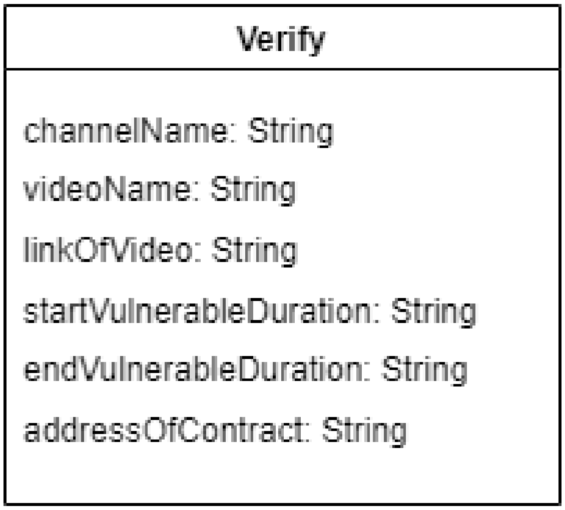
Verify
channelName: String
videoName: String
linkOfVideo: String
startVulnerableDuration: String
endVulnerableDuration: String
addressOfContract: String

Fig. 3. Database Structure.

(addressOfContract).

The database is used to store information about the content present on the blockchain platform, which means that the content has been successfully verified. Information stored inside the database includes (channelName), (videoName), (linkOfVideo), (startVulnerableDuration), (endVulnerableDuration) and (addressOfContract). The storage is to help Middleman manage the database effectively and easily transfer the reported information back to social media platforms (specifically in the research paper, Youtube). Because verified content is publicly available on the blockchain, if there is a change in the database, the information about that verified content will remain unaffected and, more importantly, unchanged. This helps the YVC system to become transparent and limit Middleman's information interference.

The database will not store the evaluation information of the Verifier, but will instead store the address of the evaluated contract on the blockchain. This storage is to streamline the database, and when Middleman reports back to the social media platform, the social media platform side can easily verify the verified contract.

C. Algorithm

Algorithm 1 YVC Execution

```
Input: verifier, channelName, videoName, linkOfVideo, startVulnerableDuration, endVulnerableDuration, verifyContent
Output: verifyContent
Begin: set isChannelName = false, isVideoName = false, isLinkOfVideo = false, isStartVulnerableDuration = false, isEndVulnerableDuration = false, verifyContent = ””
manual update isChannelName
manual update isVideoName
manual update isLinkOfVideo
manual update isStartVulnerableDuration
manual update isEndVulnerableDuration
if isLinkOfVideo == false then
    update verifyResult = ”Due to verifier, link is not correct to verify”
    update isStartVulnerableDuration = false
    update isEndVulnerableDuration = false
    print verifyContent struct
else if isStartVulnerableDuration == false or isEndVulnerableDuration == false then
    update verifyResult = ”Due to verifier, range of duration vulnerable content is not correct”
    print verifyContent struct
else if isLinkOfVideo == true isStartVulnerableDuration == true isEndVulnerableDuration == true then
    update verifyResult = ”Due to verifier, video contain vulnerable content”
    print verifyContent struct
end if
```

The algorithm executes sequentially from top to bottom of the YVC framework's execution. First, the system will take input information including the verifier as the address when the Verifier conducts content validation. channelName, videoName, linkOfVideo, startVulnerableDuration, endVulnerableDuration are the information obtained based on the Reporter's report information. verifyContent is a variable that stores the Verifier's content verification value. In the next step, the system will automatically set the values to be verified to false and the resulting string is

TABLE I. THE PERMISSION OF THE AUTHORIZED IN YVC

Function/ Method	Verifier	Reporter	Middleman
constructor	Authorized	-	-
setContent	Authorized	-	-
setVerifyContent	Authorized	-	-
getChannelName	Authorized	Authorized	Authorized
getEndVulnerableDuration	Authorized	Authorized	Authorized
getLinkOfVideo	Authorized	Authorized	Authorized
getStartVulnerableDuration	Authorized	Authorized	Authorized
getVerifyContent	Authorized	Authorized	Authorized
getVideoName	Authorized	Authorized	Authorized
verifyContent	Authorized	Authorized	Authorized

empty because Verifier has not started verifying. From lines 4 to 8, Verifier verifies the content to see if the reported content is vulnerable. After Verifier verifies the content, the system will base it on the verified data to give verification results. From lines 9 to 13, if `isLinkOfVideo` is false, the result is returned and stored in the verifyResult variable as ”Due to verifier, link is not correct to verify” and the values of `isStartVulnerableDuration` and `isEndVulnerableDuration` are set to false, then the system From lines 14 to 16, if `isStartVulnerableDuration` is false or `isEndVulnerableDuration` is false, the variable that stores the `verifyResult` result will be updated to ”Due to verifier, range of duration vulnerable content is” not ”correct”, then the system prints the `verifyContent` dataset. From lines 17 to 20, if `isLinkOfVideo` is true and `isStartVulnerableDuration` is true and `isEndVulnerableDuration` is true, the variable that stores the `verifyResult` result will be updated as ”Due to verifier, the video contains vulnerable content”, similarly the system will print the `verifyContent` dataset. and terminate the algorithm.

D. Authorization

The YVC system provides functional authorizations to the stakeholders in the system. The list of functions is described in Table I. The three main user sets inside the system include Verifier, Reporter, and Middleman. When a user joins the system, they will fit into the above user set.

We verify the actor’s authority on smart contract by account address (public key) in the Binance smart chain network. The functions and methods in smart contract are described below.

- *constructor*: The function is executed first and executes only once when verifying content on the smart contract. constructor in the YVC system will be used to validate the verifier address when performing a transaction. Therefore, only the verifier can authorize this method
- *setContent*: A function used to confirm the reported content information. This method consists of a set of variables (*channelName, videoName, linkOf- Video, startVulnerableDuration, endVulnerableDuration*) that represent the information of the reported content, respectively. When verifying content, only Verifier can authorize this method.
- *setVerifyContent*: A function used to provide content verification information. This method includes a set of boundaries (*contractID, isChannelName, isVideoName, isLinkOfVideo, isStartVulnerableDuration, isEndVulnerableDuration, verifyResult*) these variables correspond to the information to be verified. When verifying content, only Verifier can authorize this method.
- *getChannelName*: This is the method used to extract information about the channel name. This information is authorized on all 3 user sets: Verifier, Reporter, and Middleman
- *getEndVulnerableDuration*: A method used to extract information about the end time of the vulnerable video. This information is authorized on all three user sets, Verifier, Reporter, and Middleman.
- *getStartVulnerableDuration*: A method used to extract information about the start time of the vulnerable video. This information is authorized on all three user sets, Verifier, Reporter, and Middleman.
- *getLinkOfVideo*: This is the method used to extract information about the link containing the vulnerable video. This information is authorized on all three user sets, Verifier, Reporter, and Middleman.
- *getVideoName*: This is the method used to extract the information of the video name reported. This information is authorized on all three user sets, Verifier, Reporter, and Middleman.
- *verifyContent*: This is the method used to extract verified content information. This information is authorized on all three user sets, Verifier, Reporter, and Middleman.

V. EVALUATION

A. Environment Setting

We use Solidity language and Remix IDE to program smart contracts because it is pretty popular. When implementing this solution, compiler 0.8.7+commit.e28d00a7 is stable. We also use the default EVM version and don’t need optimization. The gas limit is 3000000, just enough to deploy smart contract. We also use the MIT License because we want more people to reuse our solution. Choosing a blockchain network to run smart contracts on is also an issue to be evaluated. We have measured (will be covered in the Experimental section) and decided to use the several platforms, namely, Ethereum, and BNB Smart Chain platforms.

Fantom platform contract deployed: https://testnet.ftmscan.com/address/0x9e307b1de9d4f4d3fcc3682b752f09d135490395;

Ethereum platform contract deployed: https://rinkeby.etherscan.io/address/0x51a75b578a2a64f007a728e50c2fb8b104200078;

BNB smart chain platform contract deployed: https://testnet.bscscan.com/address/0x2ad5ed1473fedf93557621dc420f7d91b39a0626.

TABLE II. The Gas for the Smart Contract Execution of the Three Platforms, i.e., Fantom, Ethereum, and BNB Chain

Gas for execution	Fantom	Ethereum	BNB Chain
Deploy contract	0.003927833 FTM ($0.0011)	0.00448948 ETH ($6.67)	0.01120938 BNB ($3.12)
call setContent	0.000247230422 FTM ($0.000066)	0.00022971 ETH ($0.34)	0.00773244 BNB ($2.15)
call setVerifyContent	0.000171262102 FTM ($0.000046)	0.00015912 ETH ($0.24)	0.005584608 BNB ($1.55)

B. Results

Reporters have the role of defining and submitting report content to the YVC system. Since this submission has not yet reached the validation stage on the blockchain, the Reporter will not waste gas reporting content. This is similar to Middleman, Middleman acts as the receiver of the authenticated data on the blockchain and transfers that authenticated data to the database which then reports back to the social media platform. Middleman's authentication and data forwarding does not affect smart contracts on the blockchain platform. Therefore, Middleman will not cost gas on the YVC system.

For Verifier, when the verifier verifies content in the YVC system, they will call two methods, *setContent* and *setVerifyContent*. When these two methods are called, the verifier will incur a gas fee for publishing verification on the blockchain. In Table II, we conduct verification to determine the price of each gas fee on blockchains including the Fantom blockchain platform, Ethereum blockchain platform, and Binance smart chain platform.

VI. Conclusion

This article introduces a content verification system for social media platforms (namely, YouTube) based on blockchain and a smart contract called YVC (YouTube Verify Content). The main aim of this study is to solve the problem of tightening dirty content that is existing on social media platforms. The highlight of the system is the application of blockchain technology to limit the human impact in changing report information. To evaluate the results of the YVC system, we deployed and analyzed it on three popular platforms, including Fantom, BNB Smart Chain, and Ethereum. Based on the evaluation results, we can confirm that Fantom's Gas is one of the lowest of the three. Regarding possible future directions, we aim to expand to apply the system to verify a lot of dirty content on multiple social media platforms. We will set up verification not only for videos but also for other digital content.

References

[1] A. Chu, A. Arunasalam, M. O. Ozmen, and Z. B. Celik, "Behind the tube: Exploitative monetization of content on youtube," in *31st USENIX Security Symposium (USENIX Security 22). Boston, MA: USENIX Association. URL https://www. usenix. org/conference/usenixsecurity22/presentation/chu*, 2022.

[2] H. Green, "Hank green, 35 minutes on youtube demonetization. (2017)," 2017. [Online]. Available: https://www.youtube.com/watch?v=ouMeAaAWUEg

[3] E. Tseng, R. Bellini, N. McDonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart, "The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1893–1909.

[4] R. Bellini, E. Tseng, N. McDonald, R. Greenstadt, D. McCoy, T. Ristenpart, and N. Dell, "" so-called privacy breeds evil" narrative justifications for intimate partner surveillance in online forums," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW3, pp. 1–27, 2021.

[5] D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, G. Stringhini, and A. Vakali, "Measuring# gamergate: A tale of hate, sexism, and bullying," in *Proceedings of the 26th international conference on world wide web companion*, 2017, pp. 1285–1290.

[6] Y. Hua, M. Naaman, and T. Ristenpart, "Characterizing twitter users who engage in adversarial interactions against political candidates," in *Proceedings of the 2020 CHI conference on human factors in computing systems*, 2020, pp. 1–13.

[7] Youtube, "Youtube kid," online; accessed 29 October 2022. [Online]. Available: https://www.youtube.com/intl/ALL_ie/kids/

[8] S. Alghowinem, "A safer youtube kids: An extra layer of content filtering using automated multimodal analysis," in *Proceedings of SAI Intelligent Systems Conference*. Springer, 2018, pp. 294–308.

[9] M. Picha Edwardsson and W. Al-Saqaf, "Drivers and barriers for using blockchain technology to create a global fact-checking database," *Online Journal of Communication and Media Technologies*, vol. 12, no. 4, p. e202228, 2022.

[10] N. Duong-Trung, X. S. Ha, T. T. Phan, P. N. Trieu, Q. N. Nguyen, D. Pham, T. T. Huynh, and H. T. Le, "Multi-sessions mechanism for decentralized cash on delivery system," *Int. J. Adv. Comput. Sci. Appl*, vol. 10, no. 9, 2019.

[11] X. S. Ha, H. T. Le, N. Metoui, and N. Duong-Trung, "Dem-cod: Novel access-control-based cash on delivery mechanism for decentralized marketplace," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 71–78.

[12] N. T. T. Le, Q. N. Nguyen, N. N. Phien, N. Duong-Trung, T. T. Huynh, T. P. Nguyen, and H. X. Son, "Assuring non-fraudulent transactions in cash on delivery by introducing double smart contracts," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 677–684, 2019.

[13] N. Duong-Trung, H. X. Son, H. T. Le, and T. T. Phan, "On components of a patient-centered healthcare system using smart contract," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, 2020, p. 31–35.

[14] ——, "Smart care: Integrating blockchain technology into the design of patient-centered healthcare systems," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, ser. ICCSP 2020, 2020, p. 105–109.

[15] H. X. Son, T. H. Le, N. T. T. Quynh, H. N. D. Huy, N. Duong-Trung, and H. H. Luong, "Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems," in *International Conference on Mobile, Secure, and Programmable Networking*. Springer, 2020, pp. 44–56.

[16] N. H. Tuan Khoi *et al.*, "Vblock - blockchain based traceability in medical products supply chain management: Case study in vietnam," in *International Conference on Artificial Intelligence for Smart Community*, 2020.

[17] H. T. Le, L. N. T. Thanh, H. K. Vo, H. H. Luong, K. N. H. Tuan, T. D. Anh, K. H. N. Vuong, H. X. Son *et al.*, "Patient-chain: Patient-centered healthcare system a blockchain-based technology in dealing with emergencies," in *International Conference on Parallel and Distributed Computing: Applications and Technologies*. Springer, 2022, pp. 576–583.

[18] H. X. Son, M. H. Nguyen, N. N. Phien, H. T. Le, Q. N. Nguyen, V. Dinh, P. Tru, and P. Nguyen, "Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 4, pp. 45–50, 2019.

[19] H. H. Luong, T. K. N. Huynh, A. T. Dao, and H. T. Nguyen, "An approach for project management system based on blockchain," in *International Conference on Future Data and Security Engineering*. Springer, 2021, pp. 310–326.

[20] N. H. Tuan Khoi *et al.*, "Domain name system resolution system with hyperledger fabric blockchain," in *International Conference on Inventive Computation and Information Technologies*, 2022.

[21] X. S. Ha, T. H. Le, T. T. Phan, H. H. D. Nguyen, H. K. Vo, and N. Duong-Trung, "Scrutinizing trust and transparency in cash on delivery systems," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. Springer, 2020, pp. 214–227.

[22] E. Bouma-Sims and B. Reaves, "A first look at scams on youtube," *arXiv preprint arXiv:2104.06515*, 2021.

[23] A. Tripathi, K. K. Bharti, and M. Ghosh, "A study on characterizing the ecosystem of monetizing video spams on youtube platform," in *Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services*, 2019, pp. 222–231.

[24] K. Papadamou, A. Papasavva, S. Zannettou, J. Blackburn, N. Kourtellis, I. Leontiadis, G. Stringhini, and M. Sirivianos, "Disturbed youtube for kids: Characterizing and detecting inappropriate videos targeting young children," in *Proceedings of the international AAAI conference on web and social media*, vol. 14, 2020, pp. 522–533.

[25] T. C. Alberto, J. V. Lochter, and T. A. Almeida, "Tubespam: Comment spam filtering on youtube," in *2015 IEEE 14th international conference on machine learning and applications (ICMLA)*. IEEE, 2015, pp. 138–143.

[26] V. Chaudhary and A. Sureka, "Contextual feature based one-class classifier approach for detecting video response spam on youtube," in *2013 Eleventh Annual Conference on Privacy, Security and Trust*. IEEE, 2013, pp. 195–204.

[27] S. Zannettou, S. Chatzis, K. Papadamou, and M. Sirivianos, "The good, the bad and the bait: Detecting and characterizing clickbait on youtube," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 63–69.

[28] S. Ghimire, J. Y. Choi, and B. Lee, "Using blockchain for improved video integrity verification," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 108–121, 2019.

[29] S. K. Sathish, A. A. Patankar, and H. Khanna, "Aurum: A blockchain based decentralized video streaming platform," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–8.

[30] P. Banerjee, C. Govindarajan, P. Jayachandran, and S. Ruj, "Reliable, fair and decentralized marketplace for content sharing using blockchain," in *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 365–370.

[31] A. Zelensky, V. Voronin, E. Semenishchev, I. Svirin, and A. Alepko, "Video content verification using blockchain technology," in *2018 IEEE International Conference on Smart Cloud (SmartCloud)*. IEEE, 2018, pp. 208–212.