Int. j. inf. tecnol. (February 2024) 16(2):1095–1109
https://doi.org/10.1007/s41870-023-01619-7

ORIGINAL RESEARCH

Ensuring transparency, confidentiality, and deterrence of political influence in journalism using IPFS, private, public, and semi-public blockchains

Shahoriar Azad Niloy[1] · **Indra Ghosh**[1] · **Saha Reno**[1] · **Asnuka Rahman**[1] · **Sanobar Rahaman**[1] · **Md. Shajjed Hossan**[1]

Received: 13 June 2023 / Accepted: 22 September 2023 / Published online: 21 November 2023

Abstract One of a journalist's most essential rights is the right to free speech. But this can expose them to abuse and other violence. In some cases, journalists may have trouble protecting sensitive or contentious data as they may be threatened to remove it. Also, due to political influences, a news reporting organization might be asked and even threatened to take their published news down. In this paper, we suggest a journalism strategy based on Blockchain and the InterPlanetary File System (IPFS) to preserve journalists' privacy, secure the news, and protect data resources. The immutability of the transactions in blockchain prevents the removal of important news and consensus makes sure that the news going to be published is verified and authenticated. Hyperledger Fabric is used for creating private ledgers, where only the members of privileged media organizations have access to the ledger. To store media data securely, the IPFS, a peer-to-peer (P2P) based decentralized storage where a small change in data drastically changes the hash, is considered the suitable platform for our system. Our proposed system can ensure that a news organization can maintain the security of its journalists and the organization itself by sending the confidential contents to an Ethereum-based semi-public blockchain and a group of intermediate trustees; using only the public key without revealing the identity.

Keywords Blockchain · Hyperledger · Ethereum · IPFS · Journalism

1 Introduction

Journalists have the responsibility to deliver reports on various national or international topics by compiling information from a variety of sources and basing them on observations and facts. They frequently deal with a variety of contentious topics that might be detrimental to a person or group of individuals. This could mislead the situation against journalists and cause them to face numerous threats and acts of violence, including murder, torture, hostage-taking, intimidation, and forced abduction. According to UNESCO's data on journalist killings from 1995 to 2022, the number of journalists killed has fluctuated over the years. In 1995, 33 journalists were killed, which decreased to 10 in 2000. However, by 2005, the number increased to 42, and in 2010, it further rose to 65. The year 2015 saw a substantial spike with 116 journalists killed, but in 2020, the number decreased to 62. Alarmingly, in 2022, there was a notable increase to 88 journalists killed, marking the highest toll since 2015 [1]. Blockchain has the feature where the transactions on the blockchain cannot be altered or changed [2]. Once the news has been tampered with, nodes on the propagation path will modify themselves accordingly, also it is impossible to alter the entire system

✉ Saha Reno
reno.saha39@gmail.com

Shahoriar Azad Niloy
niloyshahoriar@gmail.com

Indra Ghosh
indraghosh0802@gmail.com

Asnuka Rahman
asnukalamia@gmail.com

Sanobar Rahaman
sanobar256@gmail.com

Md. Shajjed Hossan
sshajjedhussain@gmail.com

[1] Department of CSE, Bangladesh Army International University of Science and Technology, Cumilla 3501, Bangladesh

without high computational power [3]. Hyperledger Fabric, a private-permissioned blockchain, offers an identity control service and access control lists through private channels so users can manage and restrict access to their shared information in the network, giving blockchain networks privacy control [4]. As a result, network participants are aware of one another through their public identities but are not required to be aware of the shared information [5]. A thorough analysis of the current state-of-the-art privacy-preserving research methodologies and blockchain-based solutions, as well as the primary privacy issues that surround this innovative and disruptive technology, was also conducted in another study [6]. They developed the performance of zero-knowledge methods suitable to blockchains and constructed quantum-resistant ledgers using effective crypto-privacy algorithms. The method will enhance the privacy-preserving capabilities of blockchain in difficult situations like IoT [7].

Newspapers had a significant part in British political, economic, and cultural life, according to Bingham, who noted in his study [8] that these archives are now a valuable source for historians. This feature of the press is shared by many other nations. In a study [9], a personalized proof-of-Authority consensus method was used along with a weighted-ranking algorithm, as a preventive strategy against fake news propaganda. The solution focuses on a wide variety of media, including any text, image, video, or audio file hash, which may be stored and utilized for transactions during the validation process. But the proposed network excludes end users who are the intended audience for the news being published and only includes news organizations. A method based on blockchain technology and using a specific smart contract capability was proposed in another study [10] to provide reliable sources of information and prevent fake news. But users are not allowed to directly verify the authenticity and veracity of each published story without the help of a third party.

In our proposed system, journalism organizations will be able to publish controversial news that could get them into unwanted situations without disclosing their identities. For the system, the organization will employ Hyperledger Fabric-based private blockchain for all internal operations. To store sensitive information, each company will use an IPFS network. For every piece of stored data, IPFS creates a distinct hash and data stored on IPFS cannot be updated without changing the data hash [11]. There will be two semi-public blockchains available for the publication of news; one for non-controversial news that poses no threat and the other for contentious news that poses a risk. There will be some predetermined endorsing peers for verifying if the news submitted by a publication is valid or not. This will stop any fake news from being published.

2 Literature review

Numerous researchers have ventured into the exploration of blockchain technology and related solutions as a means to address pressing issues in journalism. While these pioneering efforts have brought forth innovative approaches and valuable insights, they are not without their limitations and gaps. This literature review delves into these seminal works, shedding light on their methodologies, findings, and the constraints they faced. The objective is to place our study within the broad canvas of existing research, highlighting the unique contributions of our work and the potential avenues for future exploration it uncovers. Detailed reviews of the existing methodologies to strengthen the security in journalism are provided in Table 1.

The proposed journalism strategy based on blockchain and IPFS stands out in its novelty compared to existing comparable works. While some prior studies have explored blockchain applications in journalism, they often focus on financial aspects, fake news detection, or data validation without explicitly addressing journalists' privacy and data protection. In contrast, our work offers a comprehensive solution that integrates blockchain and IPFS to create a secure environment where journalists can maintain their privacy, authenticate news, and protect data resources. Unlike Agrawal et al.'s system [3], our proposal does more than secure data-it ensures the safety of journalists by allowing them to publish without revealing their identities. Contrary to Bernabe et al.'s work [6], we provide practical implementations of privacy-preserving blockchain-based solutions, specifically designed for journalism. In contrast with Chen et al.'s study [9], our approach involves both news organizations and end-users, providing a more comprehensive defense against fake news. Lastly, unlike the system proposed by Christodoulou and Christodoulou [10], our solution allows users to directly verify the authenticity of each published story, promoting transparency and trust in the news distribution process. Overall, our novel system offers a more robust, all-encompassing approach to ensuring security, privacy, and truth in journalism.

3 Methodology

The proposed framework initiates with two essential procedures. Firstly, maintaining the internal operations of a

Table 1 Reviews of the existing approaches to secure journalism

Authors	Contribution and methodology	Results	Limitations
Dwivedi et al. [12]	- Traced the source of fake news using a scalable blockchain distributed network - Deployed blockchain to trace the source of fake news	Showed effective results in tracing and mitigating the spread of fake news	Lacks adequate scalability and efficiency for real-time use
Hao et al. [13]	- Analyzed performance of consensus algorithm in private blockchain - Studied performance aspects using a practical approach	Established the efficiency and reliability of the consensus algorithms	Focused only on the technical aspect, not the user-centric aspects
Ivancsics [14]	- Discussed blockchain's role in journalism - Analysis of practical and theoretical blockchain applications in journalism	Outlined potential advantages of blockchain in journalism	The theoretical discussion, lack of implementation and evaluation
Kim and Yoon [15]	- Proposed journalism model based on blockchain with sharing space - Used blockchain technology to propose a new model for journalism	Presented a promising model for secure journalism	The proposed model was not tested in a real-world scenario
Kim and Kim [16]	- Analyzed AI news and robot journalism trends - Conducted big data analysis on AI news trends	Identified key trends and the potential impact of AI in journalism	Focused solely on AI, ignoring other potential technologies like blockchain
Chuen and Deng [17]	- Compiled comprehensive information about blockchain and digital finance - Through extensive research and compilation	Offered a strong base for researchers in blockchain technology	Not specific to journalism, wider focus on blockchain applications
Le and Loebbecke [18]	- Discussed deploying blockchain technology for monetizing political journalism - Provided theoretical analysis and potential strategies	Provided new insights on monetization strategies for journalism	Lack of empirical evidence and practical applications
Martin et al. [19]	- Reviewed legal aspects of anonymous speakers and confidential sources - Analyzed various shield laws and their implications	Provided an in-depth legal analysis on anonymity in journalism	Did not consider technological solutions, such as blockchain, for preserving anonymity
Pongnumkul et al. [20]	- Analyzed the performance of private blockchain platforms in varying workloads - Performed practical tests on different workloads	Provided insights on the scalability and performance of private blockchains	Did not specifically address the needs of journalism industry
Saad et al. [21]	- Proposed a blockchain-based solution to combat fake news - Used blockchain technology to trace and authenticate news	Presented a promising model for fighting fake news	The proposed solution was not tested in a real-world scenario
Shae and Tsai [22]	- Proposed an AI blockchain platform for trusting news - Combined AI and blockchain to authenticate news	Outlined a novel approach for news authentication	Limited by the potential biases and errors of AI algorithms
Shang et al. [23]	- Proposed a method for tracing the source of news based on blockchain - Implemented a blockchain-based system for tracing news source	Offered a potential solution to check the authenticity of news	Limited real-world testing, no consideration of anonymity

Table 1 (continued)

Authors	Contribution and methodology	Results	Limitations
Teixeira et al. [24]	- Discussed a new approach to crowd journalism using a blockchain-based infrastructure - Proposed a theoretical model for crowd journalism	Provided fresh insights on the potential of blockchain in crowd journalism	Theoretical discussion, lack of implementation and evaluation
Thakkar et al. [25]	- Performed performance benchmarking and optimizing Hyperledger Fabric blockchain platform - Conducted practical tests on the Hyperledger Fabric blockchain	Provided useful insights on the performance and optimization of blockchain	Specific to Hyperledger Fabric, not generalizable to other blockchain platforms
Vujičić et al. [26]	- Provided a brief overview of blockchain technology, Bitcoin, and Ethereum - Theoretical analysis and compilation of existing work	Offered a good base for understanding the technologies	Not specific to journalism, lack of practical applications
Waisbord [27]	- Reviewed the concept of 'post-truth' in relation to journalism and fake news - Theoretical analysis and review	Offered insightful understanding of the challenges in modern journalism	Does not offer technological solutions
Abdelmohdy Abdelmoaty [28]	- Discussed the uses of blockchain in the field of journalism - Reviewed the potential and realized uses of blockchain in journalism	Outlined the transformative potential of blockchain in journalism	More of an overview, lacks in-depth analysis of specific applications

journalism organization, and secondly, publishing news of those organizations on two distinct blockchain platforms based on the news type (Controversial and Noncontroversial). Every news agency employs a Hyperledger to oversee its internal operations, and the news is published on two different blockchain platforms. The overall methodology covers information flow within the organization Hyperledger, information flow from Hyperledger to two different blockchain platforms, and the mechanism to regulate the disclosure of the organization's identity.

3.1 Transaction flow within journalism organization

The process within a journalism organization starts with participant registration with the client. Subsequently, the system administrator assigns certificates to the participants. The number of participants can differ according to the organization. For example, it is up to the organization how many editors are going to be there. Each reporter has a reporter ID using which they can submit the report to the client. The client, a web application in this context, acts as the medium through which the organization's members communicate both with the blockchain and each another. The process continues with the editor, serving as an endorsing peer, receiving the submitted report. The editor then verifies the report's legitimacy and authenticity based on endorsement policies, which refer to the rules and regulations of a particular news reporting organization. The rules for a news organization include restrictions on using vulgar content, sensitive words, etc. Based on that determination, an endorsement response is created. The endorsement response is sent back to the client. The client sends the transaction (report) along with the endorsement response to the orderers. The valid transactions are compiled into a block by the orderers and delivered to the anchor peer. The anchor peer, the organization's sub-editor collects the transaction block and filters out the invalid transactions based on the endorsement response. The anchor peer then finalizes the block and sends it to the peers, who add the legitimate transactions to Hyperledger, creating the final news report. Anchor peer utilizes a public-private key pair for publishing the news. No other participants need to know the key pair. Figure 1 shows the information flow among participants and Fig. 2 shows the information flow between peers in greater detail and defines the parts of different participants of the organization. The algorithm to forward a transaction among the participants in Hyperledger is provided in Algorithm 1.

3.2 Generating key pairs (public-private)

Key pairs are required in blockchain technology to ensure the ownership of an asset, but it has more significance than that in our system. The public key, along with the organization's identity, is provided to the public in case of publishing non-controversial news, but in case of controversial news, the public key is provided without the organization's identity. Using the same public key for publishing news of both types may jeopardize privacy. Hence, in our system, two pairs of public-private keys are required, one for publishing non-controversial news and another for publishing controversial news. These key pairs are generated using the SECP256K1 cryptographic algorithm SECP256K1 algorithm is commonly known for being used in Bitcoin and Ethereum. We considered using this algorithm because it provides smaller key sizes than other cryptographic algorithms, hence the verification is faster. Furthermore, a 3072-bit RS public key's security is comparable to that of a 256-bit SECP256K1 RSA public key. All the points that satisfy the Eq. (1) form a SECP256K1 elliptic curve:

$$y^2 = x^3 + ax + b \tag{1}$$

where x is the public key on the elliptic curve, y is the private key on the elliptic curve, a & b is the constants that represent the limited field across which the curve is generated.

3.3 Signature generation

Digital signature is used to validate the identity of the transaction sender. The ECDSA algorithm is utilized to create and validate the signature. To create and validate the signature, we utilized the ECDSA algorithm. In comparison to other signature generation and verification algorithms like RSA, the ECDSA key is harder to crack since the Elliptic Curve Discrete Logarithm Problem (ECDLP) must be solved first. It is generated using a message and a private key. The $F_{SHA-256}$ hashing algorithm is first used to create a 256-bit

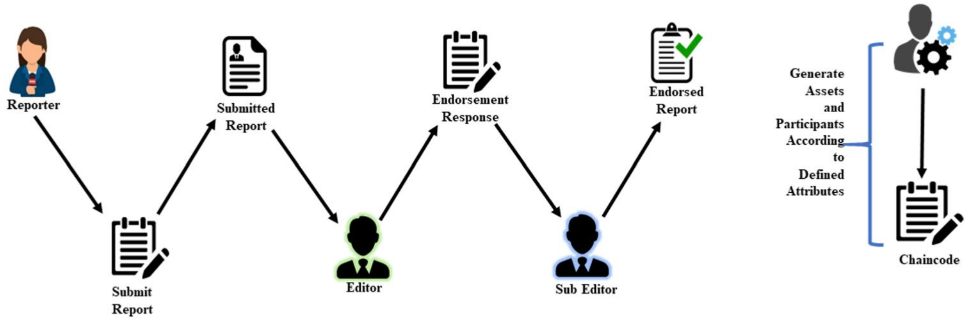


Fig. 1 Utilization of smart contract and defining assets and participants

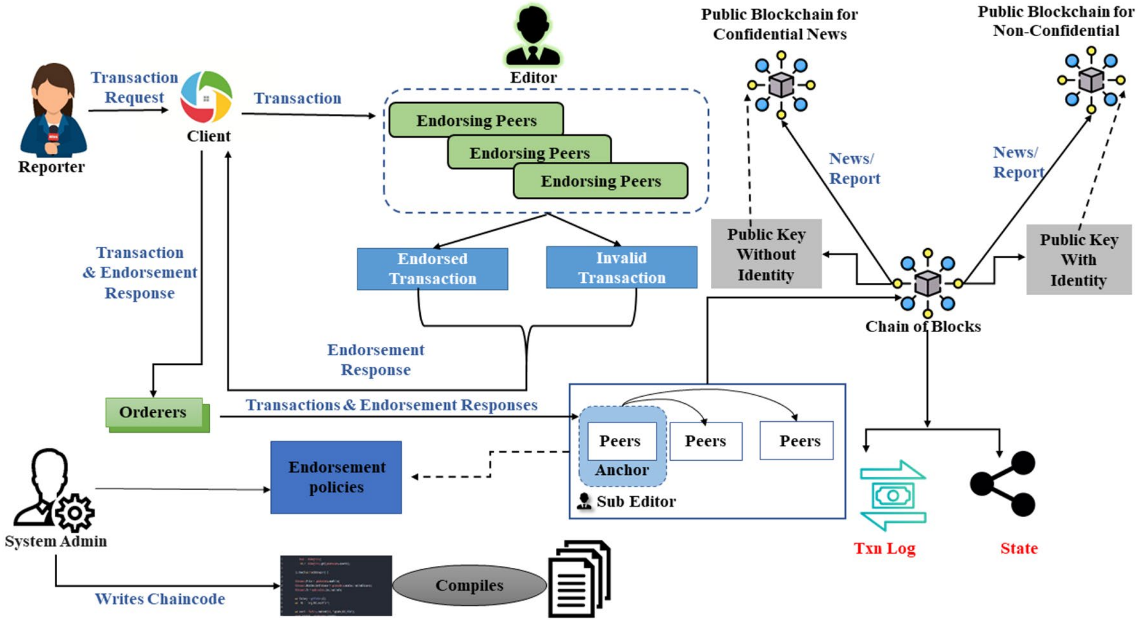
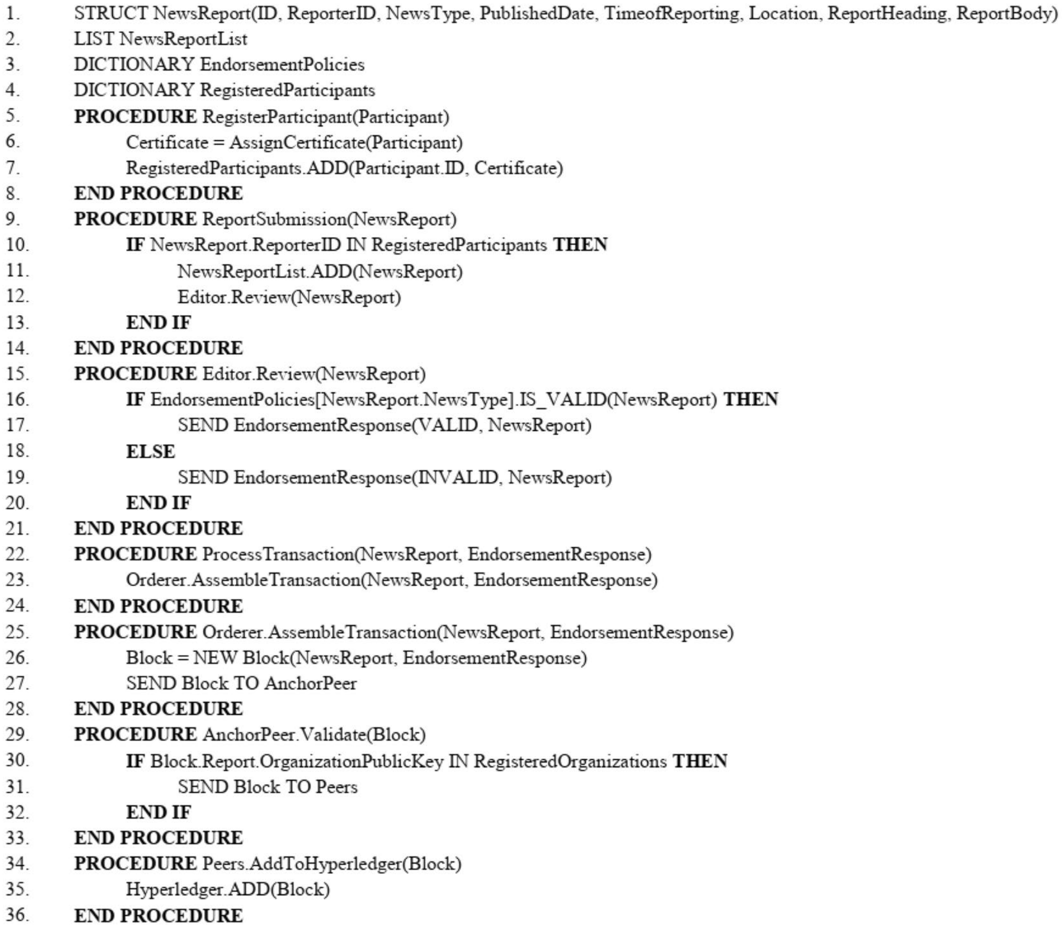


Fig. 2 Information flow among the peers and interaction with the ledger participants



```
STRUCT NewsReport(ID, ReporterID, NewsType, PublishedDate, TimeofReporting, Location, ReportHeading, ReportBody)
LIST NewsReportList
DICTIONARY EndorsementPolicies
DICTIONARY RegisteredParticipants
PROCEDURE RegisterParticipant(Participant)
    Certificate = AssignCertificate(Participant)
    RegisteredParticipants.ADD(Participant.ID, Certificate)
END PROCEDURE
PROCEDURE ReportSubmission(NewsReport)
    IF NewsReport.ReporterID IN RegisteredParticipants THEN
        NewsReportList.ADD(NewsReport)
        Editor.Review(NewsReport)
    END IF
END PROCEDURE
PROCEDURE Editor.Review(NewsReport)
    IF EndorsementPolicies[NewsReport.NewsType].IS_VALID(NewsReport) THEN
        SEND EndorsementResponse(VALID, NewsReport)
    ELSE
        SEND EndorsementResponse(INVALID, NewsReport)
    END IF
END PROCEDURE
PROCEDURE ProcessTransaction(NewsReport, EndorsementResponse)
    Orderer.AssembleTransaction(NewsReport, EndorsementResponse)
END PROCEDURE
PROCEDURE Orderer.AssembleTransaction(NewsReport, EndorsementResponse)
    Block = NEW Block(NewsReport, EndorsementResponse)
    SEND Block TO AnchorPeer
END PROCEDURE
PROCEDURE AnchorPeer.Validate(Block)
    IF Block.Report.OrganizationPublicKey IN RegisteredOrganizations THEN
        SEND Block TO Peers
    END IF
END PROCEDURE
PROCEDURE Peers.AddToHyperledger(Block)
    Hyperledger.ADD(Block)
END PROCEDURE
```

Algorithm 1 Flow of transactions within organization

hash from the message. After that, the hash is encrypted using the sender's private key to create the signature. The signature generation process can be represented by the Eq. (2):

$$Signature = F_{private-key}(F_{SHA-256}(message)). \quad (2)$$

3.4 Publishing news of the organizations to a common platform

The organization decides whether to publish a news report along with or without the identity of the organization. The organization has two pairs of private keys and public keys: one pair for publishing controversial news, and another pair for publishing non-controversial news. There are two platforms for publishing news: a semipublic blockchain platform for publishing controversial news and an Ethereum platform for publishing noncontroversial news. The process of transferring a journalism organization's news-type assets from Hyperledger to an Ethereum-based blockchain platform is facilitated by Interledger or Cosmos. In order to transfer assets of news reports from Hyperledger to Ethereum using Interledger, a user initiates a transaction on the Hyperledger network by sending a request to a Hyperledger node. The Hyperledger node processes the transaction, which involves validating the authenticity and integrity of the news assets. Once verified, the node sends a message to an Interledger connector, indicating that the news assets need to be transferred to the Ethere-um network. The Interledger connector converts the transfer trans-action request into a format that is compatible with the Ethereum network and sends it to an Ethereum node. The Ethereum node processes the transaction on the Ethereum network, updating rele-vant accounts and smart contracts associated with the assets of news reports. This process may involve updating the ownership, licensing, or access rights to the news assets in question. Once the transaction is confirmed on the Ethereum network, the Interledger connector sends a message back to the Hyperledger node indicating that the assets of news reports have been successfully transferred. The Hyperledger node can then update its own records to reflect the successful completion of the transaction which has been used for interledger transfer of report-type assets.

3.5 Publishing controversial news

Publishing contentious news without disclosing the name of the reporter or the reporting organization is one of our system's key characteristics. For publishing contentious news, the news report is encrypted using the organization's private key, which may then be decrypted using the corresponding public key of that specific key pair. The encrypted news report is delivered to a trusted third party. An anchor peer will be randomly chosen as a trustee to carry out the validation by comparing the public key obtained with the news report and the public keys of previously registered organizations. The random anchor peer is selected from the set of Sub-Editors assigned for each organization. A minimum of three anchor peers (minimum requirement of Hyperledger Fabric) selected from every organization on mutual agreement. The random selection is done by using the 'secrets' module of Python where the anchor peer IDs will be given as parameters and the module returns a randomly chosen anchor peer ID which performs the validation process for a particular period. The report is published only if both the public keys match. While publishing the news to the semipublic blockchain for common interest, only the report along with the public key is sent without mentioning which organization it belongs to, keeping the identity secret. To prevent the organization publishing the news from being traced, the trustees will share the keys with the audience instead of the organization. A trusted third party will be responsible for verifying that the news is authentic and is coming from a trusted organization. Selected anchor peers will do this task, who will be known as trustees. To keep the identities of the organizations hidden from the audiences, Identity Mixer technology is used in our systems. One anchor peer from each organization will be assigned as a certificate authority. In Identity Mixer, a certificate authority is a trusted entity that issues digital certificates to users. These certificates contain information about the user's identity and are signed by the CA using its private key. In our system, news received by the trustee module is issued a digital certificate by the selected endorsing peer of that organization who is already assigned as a CA. When a user wants to authenticate to a third party, they present their certificate as proof of their identity. Certificate Authorities (CA) make the public key available to the blockchain participants. The participants will not be allowed to see the logical level, they will only see the public keys without knowing which public key belongs to which CA. Finally, the user or common people have access to read the news from the semipublic blockchain platform. The pictorial representation of this process is illustrated using Fig. 3.

3.6 Publishing noncontroversial news

To publish non-controversial news, the news report is encrypted using the other keypair's private key, which is only constructed for non-controversial news, and then published on the Ethereum-based blockchain. The encrypted news report can then be decoded using the keypair's corresponding public key. The organization uploads the encrypted report to Ethereum, a public blockchain, along with its public key and identity. Since there is no need to conceal the identity, there won't be any intermediate trustee in between. So, organizations can send the encrypted news report along with its public key and identity. The published news report can be viewed by the general public and they are able to identify the news organization. Figure 4 portrays the information flow from a news organization to blockchain platforms for publishing news. The algorithms for publishing both controversial and non-controversial news are represented using Algorithm 3.

3.7 Securing organization resources using IPFS

Every organization utilizes an IPFS network to store necessary data, including media files related to news reports which they want to be secured or not to be altered with. As block-chain can only store textual data, we need a secure data storage platform to securely store media files related to news reports. IPFS is decentralized and P2P-based storage which is similar to the cloud but operates almost exactly like the blockchain algorithm. After the media data is stored on the IPFS, the media data is split into multiple chunks of 256 KB in size. The chunks are distributed across a number of network users. A distributed hash table stores the locations of the chunks and the paths to each peer. There is a unique hash generated for every chunk. The SHA-256 algorithm is used to generate a Content Identifier that combines all the chunk hashes of a particular media data. This Content Identifier is used to retrieve the data from the IPFS. If a chunk gets modified or tampered with, the hash for that chunk will also change, hence the Content Identifier of that media data also changes. All the chunks of media data are checked with the checksum verification algorithm, so any changes in the data can be easily traced.

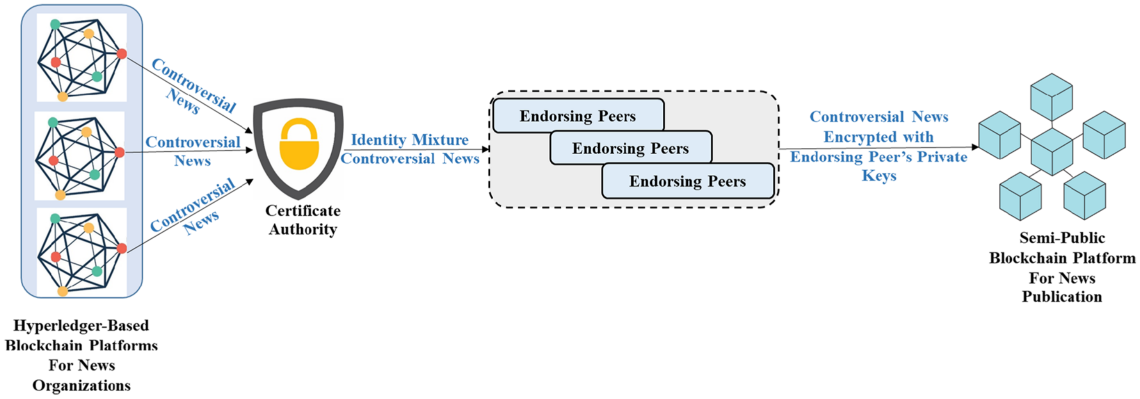

Controversial News
Controversial News
Controversial News
Certificate Authority
Identity Mixture Controversial News
Endorsing Peers
Endorsing Peers
Endorsing Peers
Controversial News Encrypted with Endorsing Peer's Private Keys
Semi-Public Blockchain Platform For News Publication
Hyperledger-Based Blockchain Platforms For News Organizations

Fig. 3 Publishing controversial news to semi-public blockchain platform using certificate authority

3.8 Interaction with asset and historian registry

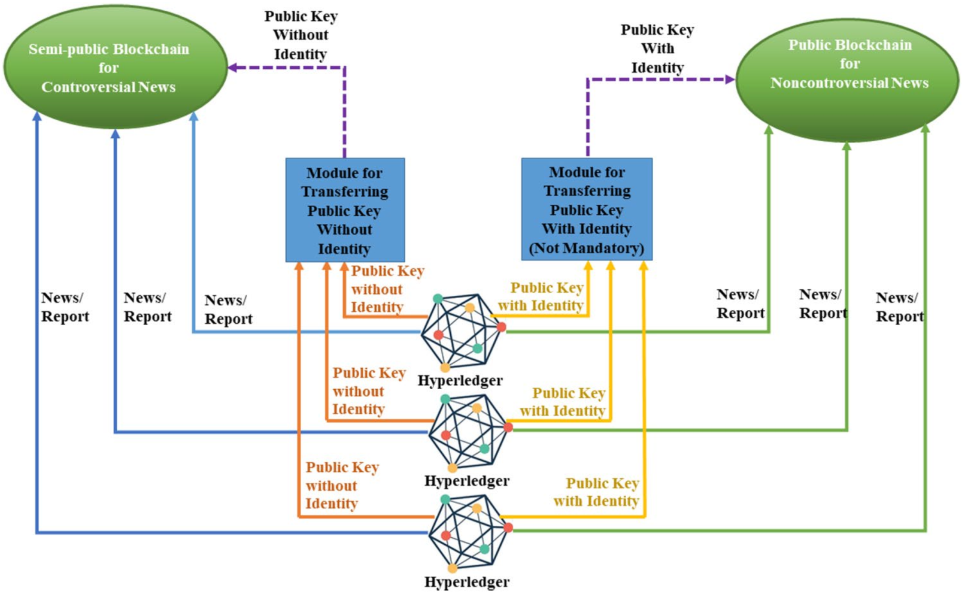
Asset registry and historical registry are the two different types of registries available in Hyperledger. News reports are eventually recorded on the asset registry, and the history of the transactions that were carried out to produce them is kept on the historian registry. Interaction with the asset registry and historian registry for executing a transaction is an integral part of the process. The news report may be stored, read, and updated, but previous versions cannot be deleted. The transactions in the historical registry can be stored and viewed but cannot be updated or deleted [29]. Interaction with the asset registry and historian registry for executing a transaction is shown in Fig. 5. Also, the algorithm for utilizing asset and historian registries to process the transactions can be found in Algorithm 3.

4 Result analysis

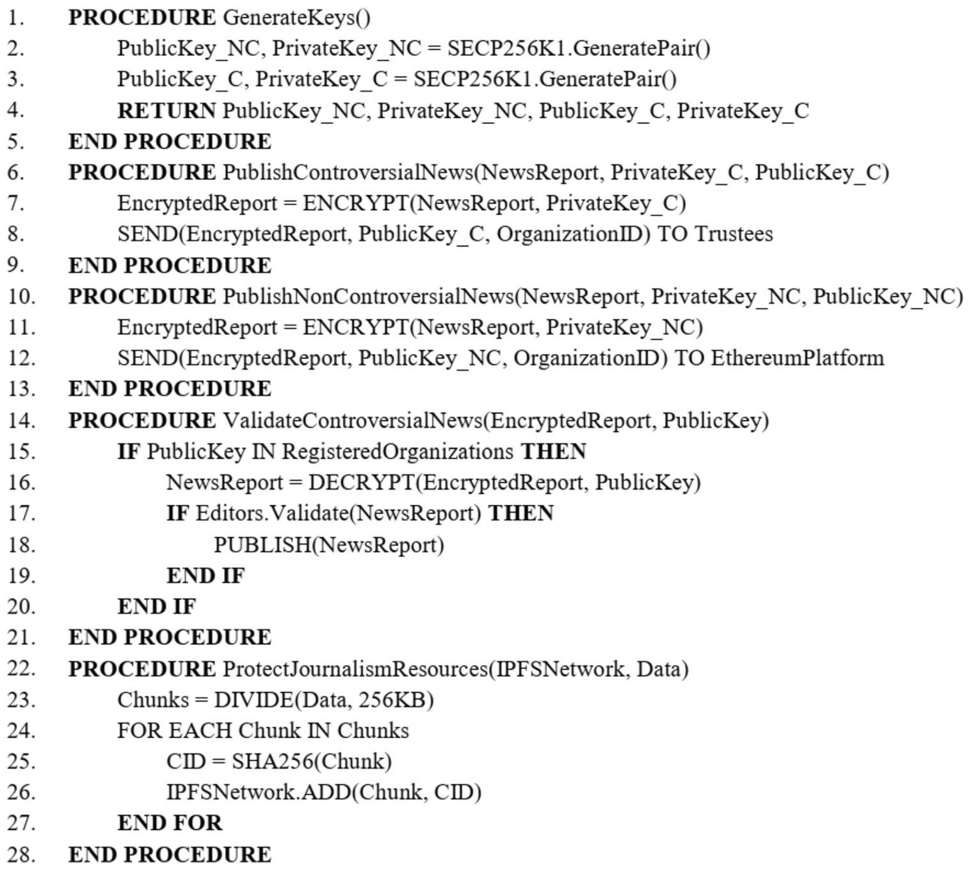
This section evaluates the performance of blockchain platforms used in our proposed system based on average execution time, latency, and throughput. Hyperledger Fabric consistently performs better than Ethereum in all scenarios.

In Fig. 6, we examine the differences in execution time for various numbers of transactions across different platforms and functions. As the number of transactions increases, so does the execution time. Hyperledger consistently outperforms Ethereum with lower execution times across all data sets. Additionally, the difference in execution time between Hyperledger and Ethereum grows larger as the number of transactions increases. For a high volume of transactions, Ethereum provides better performance for GetNews

Fig. 4 Information flow from hyperledger to blockchain-based publication platforms


Semi-public Blockchain for Controversial News
Public Key Without Identity
Public Key With Identity
Public Blockchain for Noncontroversial News
Module for Transferring Public Key Without Identity
Module for Transferring Public Key With Identity (Not Mandatory)
News/ Report
News/ Report
News/ Report
News/ Report
News/ Report
News/ Report
Public Key without Identity
Public Key with Identity
Hyperledger
Public Key without Identity
Public Key with Identity
Hyperledger
Public Key without Identity
Public Key with Identity
Hyperledger

Algorithm 2 Publishing controversial and non-controversial news on shared platforms



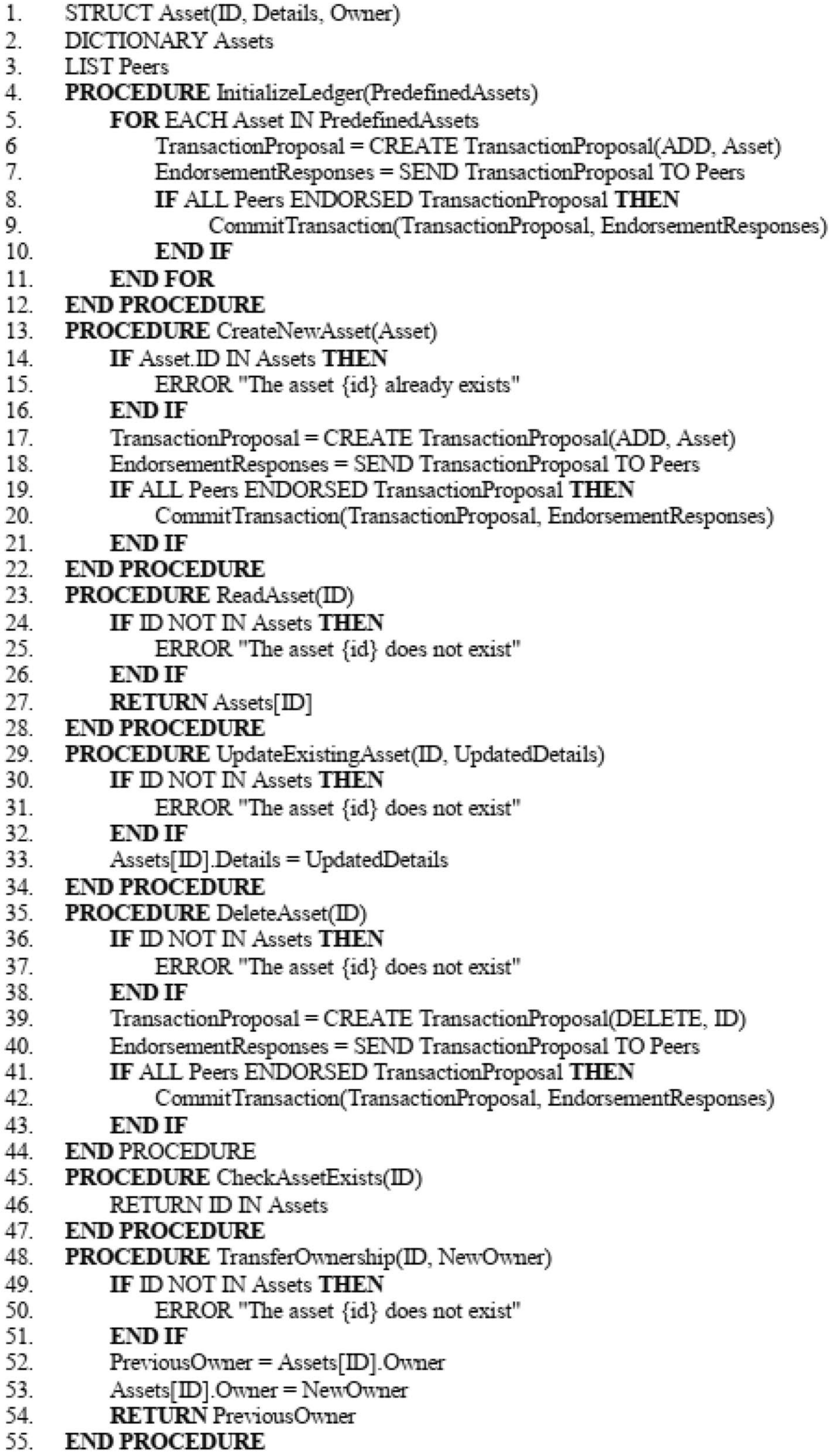
```
PROCEDURE GenerateKeys()
    PublicKey_NC, PrivateKey_NC = SECP256K1.GeneratePair()
    PublicKey_C, PrivateKey_C = SECP256K1.GeneratePair()
    RETURN PublicKey_NC, PrivateKey_NC, PublicKey_C, PrivateKey_C
END PROCEDURE
PROCEDURE PublishControversialNews(NewsReport, PrivateKey_C, PublicKey_C)
    EncryptedReport = ENCRYPT(NewsReport, PrivateKey_C)
    SEND(EncryptedReport, PublicKey_C, OrganizationID) TO Trustees
END PROCEDURE
PROCEDURE PublishNonControversialNews(NewsReport, PrivateKey_NC, PublicKey_NC)
    EncryptedReport = ENCRYPT(NewsReport, PrivateKey_NC)
    SEND(EncryptedReport, PublicKey_NC, OrganizationID) TO EthereumPlatform
END PROCEDURE
PROCEDURE ValidateControversialNews(EncryptedReport, PublicKey)
    IF PublicKey IN RegisteredOrganizations THEN
        NewsReport = DECRYPT(EncryptedReport, PublicKey)
        IF Editors.Validate(NewsReport) THEN
            PUBLISH(NewsReport)
        END IF
    END IF
END PROCEDURE
PROCEDURE ProtectJournalismResources(IPFSNetwork, Data)
    Chunks = DIVIDE(Data, 256KB)
    FOR EACH Chunk IN Chunks
        CID = SHA256(Chunk)
        IPFSNetwork.ADD(Chunk, CID)
    END FOR
END PROCEDURE
```

(133.55 s) as compared to UpdateNews (477.69 s) and CreateNews (485.43 s). This is due to the fact that GetNews transactions do not bring any modifications to the assets and only fetch the existing assets by executing SQL queries. While Create-News creates news assets with every attribute defined in the asset definition, UpdateNews does not usually update all of the attribute values of a particular 'news' asset, thus requiring less amount of time. Therefore, the workload for UpdateNews is around half that of CreateNews. For a batch of 10,000 news items, UpdateNews and CreateNews take 41.13 and 62.58 s, respectively, when executed on Hyperledger. Conversely, they take 477.69 and 485.43 s, respectively, when executed on Ethereum. These results demonstrate noteworthy variations in data management and access between the two platforms.

Figure 7 illustrates a log-log graph that compares the average latency of CreateNews transactions in five separate experiments for both Hyperledger and Ethereum. For a single transaction, Hyperledger has an average latency of 0.11 s, whereas Ethereum has an average latency of 0.23 s. In the case of 10,000 transactions, the Hyperledger's execution time remains below 100 s but Ethereum requires almost 1000 s. Although Ethereum's latency is initially twice as high as Hyperledger's, as the number of transactions increases, Ethereum's latency deteriorates considerably compared to Hyperledger's.

Figure 8 displays a comparison of the average throughput for Hyperledger and Ethereum in five experiments. In the case of executing small amounts of transactions, the difference between Hyperledger and Ethereum is comparatively low. For example, in the case of only 1 and 10 transactions, Ethereum delivers a TPS rate of 4.69 and 27.49 while Hyperledger achieves almost double the TPS rate of Ethereum (10.51 and 68.02 txns/s). For 100, 1000, and 10,000 transactions, the difference is intensely significant and Hyperledger demonstrates almost 8 times more TPS rate than Ethereum. The data also shows that as the number of transactions varies, the change in average throughput for Hyperledger is relatively larger than that of Ethereum.

Algorithm 3 Processing organizational transactions (reports) via hyperledger's registries



```
STRUCT Asset(ID, Details, Owner)
DICTIONARY Assets
LIST Peers
PROCEDURE InitializeLedger(PredefinedAssets)
    FOR EACH Asset IN PredefinedAssets
        TransactionProposal = CREATE TransactionProposal(ADD, Asset)
        EndorsementResponses = SEND TransactionProposal TO Peers
        IF ALL Peers ENDORSED TransactionProposal THEN
            CommitTransaction(TransactionProposal, EndorsementResponses)
        END IF
    END FOR
END PROCEDURE
PROCEDURE CreateNewAsset(Asset)
    IF Asset.ID IN Assets THEN
        ERROR "The asset {id} already exists"
    END IF
    TransactionProposal = CREATE TransactionProposal(ADD, Asset)
    EndorsementResponses = SEND TransactionProposal TO Peers
    IF ALL Peers ENDORSED TransactionProposal THEN
        CommitTransaction(TransactionProposal, EndorsementResponses)
    END IF
END PROCEDURE
PROCEDURE ReadAsset(ID)
    IF ID NOT IN Assets THEN
        ERROR "The asset {id} does not exist"
    END IF
    RETURN Assets[ID]
END PROCEDURE
PROCEDURE UpdateExistingAsset(ID, UpdatedDetails)
    IF ID NOT IN Assets THEN
        ERROR "The asset {id} does not exist"
    END IF
    Assets[ID].Details = UpdatedDetails
END PROCEDURE
PROCEDURE DeleteAsset(ID)
    IF ID NOT IN Assets THEN
        ERROR "The asset {id} does not exist"
    END IF
    TransactionProposal = CREATE TransactionProposal(DELETE, ID)
    EndorsementResponses = SEND TransactionProposal TO Peers
    IF ALL Peers ENDORSED TransactionProposal THEN
        CommitTransaction(TransactionProposal, EndorsementResponses)
    END IF
END PROCEDURE
PROCEDURE CheckAssetExists(ID)
    RETURN ID IN Assets
END PROCEDURE
PROCEDURE TransferOwnership(ID, NewOwner)
    IF ID NOT IN Assets THEN
        ERROR "The asset {id} does not exist"
    END IF
    PreviousOwner = Assets[ID].Owner
    Assets[ID].Owner = NewOwner
    RETURN PreviousOwner
END PROCEDURE
```

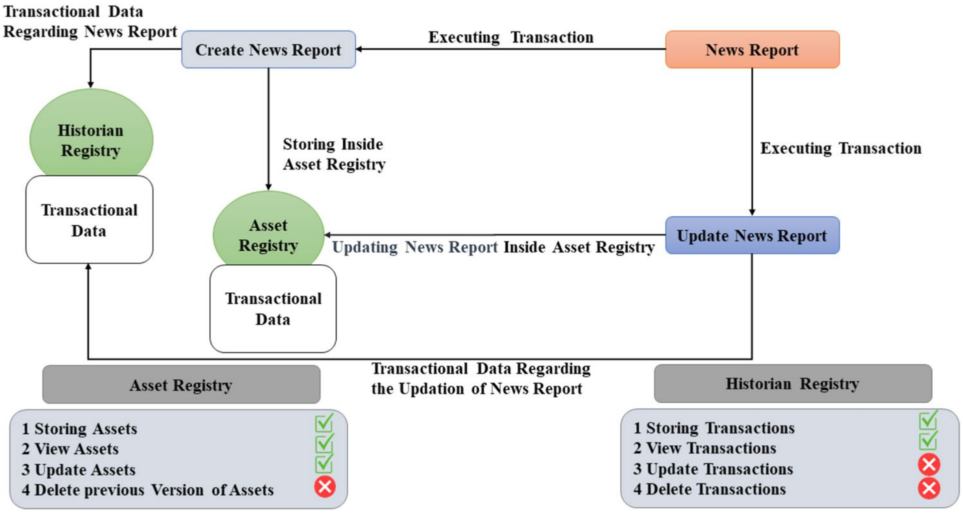


Fig. 5 Interaction with asset and historian for successful processing of transactions

Figure 9 illustrates the mean memory consumption, measured in megabytes (MB), for various Blockchain platforms when performing Identity Issuance, Query, and CreateNews operations. A substantial disparity is evident between Ethereum and Hyperledger Fabric's memory usage, with Ethereum requiring nearly 20 times more memory than all Hyperledger Fabric versions. This finding indicates that Ethereum demands considerable memory resources during benchmark testing. Regarding the Hyperledger Fabric platforms, memory consumption escalates as the Fabric version advances up to 2.2.3, at which point a decrease in memory usage is observed. This reduction may be attributed to the latest Fabric version incorporating enhanced hardware optimization capabilities.

Figure 10 depicts the mean CPU consumption in percentages for each Blockchain framework during the execution of IdentityIssuance, Query, and CreateNews operations. Similar to the experimental results of the memory usage, Ethereum requires greater CPU re-sources in comparison to all Hyperledger Fabric variants. While the difference between Ethereum 2.0 and Fabric 1.2.13 in the IdentityIssuance operation is relatively small, Ethereum demonstrates a substantial CPU utilization for both the Query and CreateNews processes.

To evaluate our system, we collected sample news from different sources and created an instance based on that which is shown in Table 2.

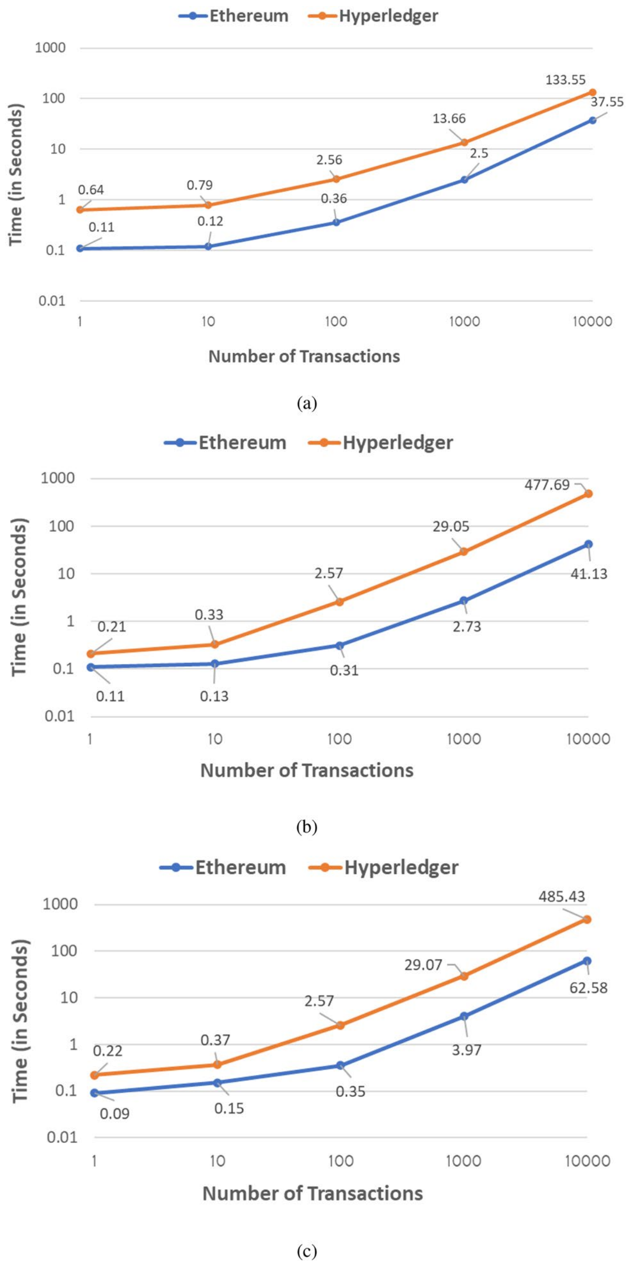
To estimate the costs associated with running a Hyperledger Fabric-based blockchain for a news reporting organization, we conducted a cost analysis considering the hourly cost of each node type, hard-ware, and infrastructure costs shown in Table 3.

Our analysis assumes that the organization has the following nodes: one System Admin, one Network Admin, five Endorsers (Editor), one Orderer, one Anchor Peer (Sub-Editor), and five Normal Peers. Based on an average salary for each role in the Unit-ed States, we estimated the hourly cost for each node type and calculated the total monthly and yearly costs. Additionally, we considered hardware and infrastructure costs, including the cost of servers, storage, and network equipment. Our analysis shows that the total monthly cost for running the Hyperledger Fabric network for a news reporting organization with the given nodes is approxi-mately $3,28,500 including both personnel and hardware costs. The total yearly cost for running the network is estimated to be $30,03,000 It's important to note that these estimates are approxi-mate and may vary depending on various factors such as location, vendor, and specific hardware requirements.

5 Conclusion and future scope

In conclusion, our paper presents a novel journalism strategy based on blockchain and the IPFS to preserve journalists' privacy, secure news data, and protect data resources. This approach can revolutionize journalism, ensuring that journalists can report the news without fear of reprisal, censorship, or data theft. It can also increase trust and transparency in media organizations by providing a verifiable and tamper-proof record of news content.

The current system employs Hyperledger for internal operations and utilizes Ethereum and semi-public blockchain for publishing non-controversial and controversial news respectively. Extending this system to include other blockchain platforms could enhance its applicability and



(a)

(b)

(c)

Fig. 6 The execution time of Ethereum and Hyperledger as the number of transactions increases (1, 10, 100, 1000, 10,000 transactions) in logarithmic scales. The sub-plots present the outcomes of three distinct functions: **a** GetNews, **b** Update-News and **c** CreateNews, respectively

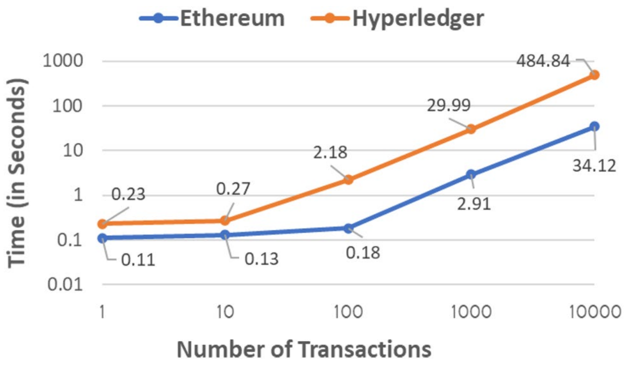


Fig. 7 The average latency of the CreateNews function evaluated for Ethereum and Hyperledger with varying numbers of transactions

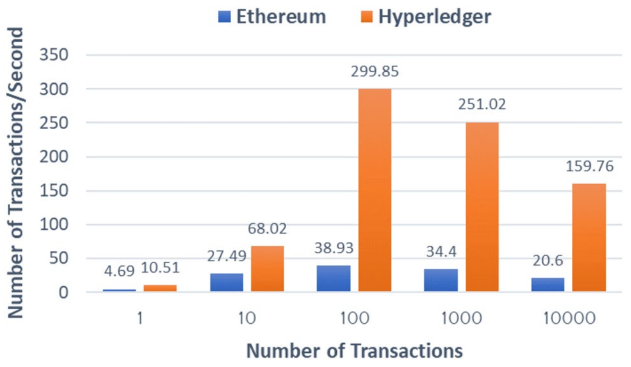


Fig. 8 Comparison of average throughput between Ethereum and Hyperledger

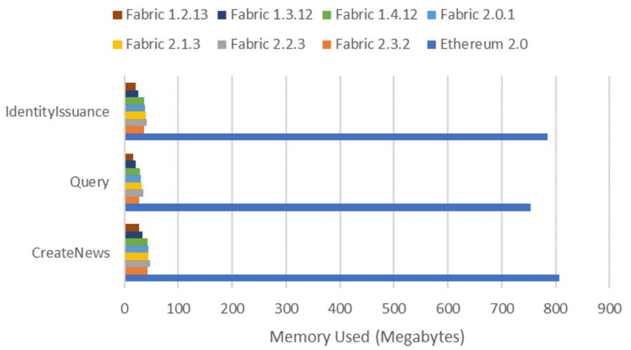


Fig. 9 Average memory consumption of Hyperledger Fabric and Ethereum

interoperability. As the system expands to accommodate more organizations and larger volumes of news data, potential performance and scalability issues will need to be addressed. Future studies could focus on optimizing blockchain's performance, increasing transaction speed, and ensuring the system can scale effectively. Additionally, exploring advanced algorithms to verify content authenticity, integrating AI and NLP technologies, and addressing regulatory implications will enhance the system's scalability, security, and user experience. Last but not the least, the system's effectiveness hinges on the selection of reliable trustees. Future research could explore more sophisticated trustee selection algorithms or mechanisms, ensuring a high level of system integrity. Further studies can focus on real-world applications, conducting case studies with news organizations to validate its effectiveness. By exploring these areas, we can continue to evolve and improve the system, ensuring it remains effective, robust, and relevant in the changing landscape of digital journalism.

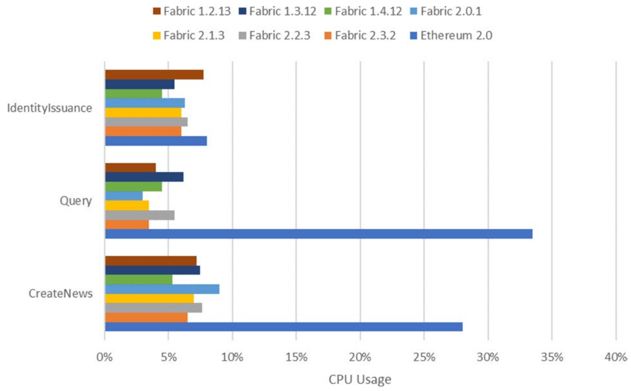


Fig. 10 Average CPU usage of Hyperledger Fabric and Ethereum

Table 2 Various news report collected from different news report organizations in Bangladesh

Asset	Reporter ID	News type	Published date	Time of reporting	Location	Report heading	Report body
1	180,253	Political event	17.10.2022	03.07.30	Uttar Pradesh, India	Police Dog Helps Solve "Blind Murder Mystery"	A 15-year-old boy was murdered and his body was..
2	310,945	Sports	05.10.2022	09.20.00	Dhaka, Bangladesh	Replacement of Sakib: New Captain Selected	During Bangladesh's recent home series against..
3	471,252	Weather & Forecast	20.09.2022	10.44.02	Bhutan	The Earth Shook More Severely	On 19th September 2022, at about..
4	209,042	Opinion	2022-09-16	15:45:00	London, UK	The Importance of Space Exploration	In a world facing numerous challenges..
5	507,031	Political event	2022-09-14	08:20:00	Beijing, China	Trade Deal Signed Between China and Australia	China and Australia signed a landmark..
6	603,015	Political event	2022-09-11	14:30:00	Moscow, Russia	Russia-Ukraine Peace Talks Show Progress	Peace talks between Russia and Ukraine..
7	409,021	Opinion	2022-09-09	16:20:00	Sydney, Australia	The Power of Social Media in Shaping Public Opinion	Social media platforms have become powerful..
8	205,072	Political event	2022-09-10	11:00:00	Paris, France	G7 Summit Concludes with Climate Agreement	The G7 Summit concluded today with a historic..
9	209,042	Political event	2022-09-07	17:50:00	Odesa, Ukraine	Overnight Russian strikes on Odesa caused significant structural damage, destroyed church	Russian strikes on Odesa overnight damaged..
10	105,023	Opinion	2022-09-12	09:55:00	New York City, USA	The Role of Artificial Intelligence in Modern Society	AI continues to shape various aspects..

Table 3 Estimated cost-analysis of proposed system

Node type	Hourly cost (USD)	Monthly cost (USD)	Yearly cost (USD)	Server cost (USD)	Storage cost (USD)	Network cost (USD)	Total monthly cost (USD)	Total yearly cost (USD)
System admin	$75	$15,000	$180,000	$8,000	$1,000	$500	$24,500	$294,000
Network admin	$50	$10,000	$120,000	$8,000	$1,000	$500	$19,500	$234,000
Endorser (5 persons)	$125	$31,250	$3,75,000	$20,000	$5,000	$2,500	$58,750	$705,000
Orderer	$50	$10,000	$120,000	$8,000	$1,000	$500	$19,500	$234,000
Anchor peer (5 persons)	$125	$31,250	$3,75,000	$20,000	$5000	$2500	$58,750	$705,000
Normal peer (5 persons)	$50	$1,00,000	$12,00,000	$40,000	$5,000	$2500	$1,47,500	$17,70,000
Total monthly cost							$3,28,500	$30,03,000

Data Availability The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Conflict of 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. There was no sponsorship or funding agency involved in this study. The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agencies of the authors. This research was conducted independently and did not involve any scenarios that could give rise to a conflict of interest.

References

1. [Online]. Available: https://www.unesco.org/en/safety-journalists/observatory/statistics?fbclid=IwAR2jOH597mlHgUhpSouOM_m9Ts-cbJFJen2DFpHs0p3ZLtM9dn68Jnii69E
2. Hossain CA, Mohamed MA, Zishan MSR, Ahasan R, Sharun SM (2022) Enhancing the security of e-health services in Bangladesh using blockchain technology. Int J Inf Technol 14(3):1179–1185
3. Agrawal V, Agarwal A, Shah S, Parmar D, Rao UP (2020) Decentralised ecosystem for journalism based on blockchain. In: ICBCT 2019: Proceedings of the International Conference on Blockchain Technology. Springer, pp 7–19
4. Quamara S, Singh AK (2022) Schain: towards the quest for redesigning supply-chain by augmenting blockchain for end-to-end management. Int J Inf Technol 14(5):2343–2354
5. Pabitha P, Priya JC, Praveen R, Jagatheswari S (2023) Modchain: a hybridized secure and scaling blockchain framework for IoT environment. Int J Inf Technol 15(3):1741–1754
6. Bernabe JB, Canovas JL, Hernandez-Ramos JL, Moreno RT, Skarmeta A (2019) Privacy-preserving solutions for blockchain: review and challenges. IEEE Access 7:164908–164940
7. Balamurugan S, Ayyasamy A, Joseph KS (2021) Iot-blockchain driven traceability techniques for improved safety measures in food supply chain. Int J Inf Technol 1–12
8. Bingham A (2010) The digitization of newspaper archives: opportunities and challenges for historians. Twentieth Century Br History 21(2):225–231
9. Chen Q, Srivastava G, Parizi RM, Aloqaily M, Al Ridhawi I (2020) An incentive-aware blockchain-based solution for internet of fake media things. Inf Process Manage 57(6):102370
10. Christodoulou P, Christodoulou K (2020) Developing more reliable news sources by utilizing the blockchain technology to combat fake news. In: (2020) second international conference on Blockchain computing and applications (BCCA). IEEE, pp 135–139
11. Tiwari A, Batra U (2021) Ipfs enabled blockchain for smart cities. Int J Inf Technol 13(1):201–211
12. Dwivedi AD, Singh R, Dhall S, Srivastava G, Pal SK (2020) Tracing the source of fake news using a scalable blockchain distributed network. In: (2020) IEEE 17th international conference on mobile ad hoc and sensor systems (MASS). IEEE. pp 38–43
13. Hao Y, Li Y, Dong X, Fang L, Chen P (2018) Performance analysis of consensus algorithm in private blockchain. In: (2018) IEEE Intelligent Vehicles Symposium (IV). IEEE. pp 280–285
14. Ivancsics B (2020) Blockchain in journalism. Columbia Journalism Review, 2019, accessed: May 31
15. Kim B, Yoon Y (2018) Journalism model based on blockchain with sharing space. Symmetry 11(1):19
16. Kim SY, Kim BY (2020) Big data analysis of AI news and robot journalism trends. Technology (Elmsford, NY) 11(10):1395–1402
17. Chuen DLK, Deng RH (2017) Handbook of blockchain, digital finance, and inclusion, volume 1: cryptocurrency, FinTech, InsurTech, and regulation. Academic Press
18. Le HA, Loebbecke C (2020) Deploying blockchain technology for monetizing political journalism
19. Martin JA, Caramanica MR, Fargo AL (2011) Anonymous speakers and confidential sources: using shield laws when they overlap online. Comm Law Policy 16(1):89–125
20. 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
21. Saad M, Ahmad A, Mohaisen A (2019) Fighting fake news propagation with blockchains. In: 2019 IEEE Conference on Communications and Network Security (CNS). IEEE
22. Shae Z, Tsai J (2019) Ai blockchain platform for trusting news. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE
23. Shang W, Liu M, Lin W, Jia M (2018) Tracing the source of news based on blockchain. In: 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS). IEEE, pp 377–381
24. Teixeira L, Amorim I, Silva AU, Lopes JC, Filipe V (2020) A new approach to crowd journalism using a blockchain-based

infrastructure. In: Proceedings of the 18th International Conference on Advances in Mobile Computing & Multimedia, pp 170–178

25. Thakkar P, Nathan S, Viswanathan B (2018) Performance benchmarking and optimizing hyperledger fabric blockchain platform. In: 2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS). IEEE
26. Vujičić D, Jagodić D, Ranić S (2018) Blockchain technology, bitcoin, and Ethereum: a brief overview. In: 2018 17th international symposium Infoteh-Jahorina (Infoteh). IEEE
27. Waisbord S (2018) Truth is what happens to news: on journalism, fake news, and post-truth. J Stud 19(13):1866–1878
28. Abdelmohdy Abdelmoaty HY (2021) Uses of blockchain in the field of journalism. Arab J Media Commun Res (AJMCR) 2021(33):162–216
29. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y et al (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference, pp 1–15