JOURNAL OF MACHINE LEARNING AND APPLICATION
Jan-Jun 2025, VOL. 1, ISSUE 1, pp. 27-34
https://doi.org/10.61577/jmla.2025.100005

RESEAPRO JOURNALS

ORIGINAL ARTICLE

OPEN ACCESS

Privacy-preserving consensus mechanisms for anonymous decentralized social media: A blockchain-based paradigm for anonymity

Stuti Srivastava, Dev Athwani, Rinku Raheja, Mahesh Kumar Tiwari and Shalini Lamba

Department of Computer Science, Autonomous College of Lucknow University, Uttar Pradesh, India

ABSTRACT

The increase of decentralized social media systems provides them with liberty and openness, yet tends to interfere with privacy because transaction data is made publicly accessible in blockchains. In this paper, a Privacy-Preserving Consensus Mechanism (PPCM) has been proposed as a privacy-preserving blockchain in anonymous decentralized social media systems. To preserve the confidentiality and integrity of transactions, the PPCM incorporates the advanced cryptography solutions, Zero-Knowledge Proofs (ZKPs), Homomorphic Encryption, and ring signatures. It utilizes a Decentralized Identity (DID) model of self-sovereign identity management and cross-platform interoperability, and overlays a reputation-based layer of governance to encourage ethical behaviour without disclosing the identity of users. Scalability is ensured with sidechains, which remove high-frequency interaction points of the main blockchain to minimize latency. The model is a compromise between privacy and accountability and solves such issues as Sybil attacks, metadata leakage, and unethical use of anonymity. The PPCM offers a privacy-focused, scalable, and ethically regulated design of next-generation decentralized social media networks.

KEY WORDS

Decentralized social network; Pseudonymity; Digital markets act; Homomorphic encryption; Hyperledger fabric

ARTICLE HISTORY

Received 15 May 2025;
Revised 05 June 2025;
Accepted 12 June 2025

Introduction

The Central authority has been taken over by users of social media through a rapid development of decentralized social media platforms that have made its users independent and worried about opposing the control of the central authority, and this is a drastic change in the world of digital communication. Unlike centralised platforms owned by corporations, distributed networks like Mastodon and Diaspora combine the use of blockchain technology and federated architectures to enable the peer-to-peer connection and ownership between users [1]. They provide more privacy, do not get censored, and are managed by democratic rule; their major challenges are balancing between anonymity and transparency when deciding through consensus-making [2]. Instead, mechanisms that will preserve privacy even in a decentralized ecosystem need to be created to enable ecosystems to reach their full potential as the issues of data exploitation and surveillance become ever more prominent [3].

Background of the study

Decentralized social networked apps use distributed networks whereby users will have their data owned by encrypting data on it, such as the use of end-to-end encryption and DIDs [4,5]. The appearance of blockchain as immutable means that the integrity of transactions will not be endangered, but Metadata vulnerabilities reveal possibilities of deanonymization [5]. Federated ecosystems have cross-platform interoperability but give rise to governance risks since each of their instances has its own privacy policy [6,7]. Although the systems overcome risks that are related to centralized storage of data, including breaches and systematic bias in algorithms, their consensus system tends to focus more on security, rather than anonymity, revealing the identities of users during authorization [4,5]. Cases such as public ledgers in systems such as Seemit, which inadvertently give away patterns of interactions by accident, breaking pseudonymity.

Privacy and anonymity concerns in blockchain social media

Existing decentralized social networks finds it challenging to integrate privacy right into the level of the protocol, particularly during consensus process [8,9]. Traditional models such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) validate transactions transparently, enabling adversaries to presume user identities through network analysis [8-9]. Moreover, federated architecture also creates governance frictions in which a user is deanonymizable not only on a particular platform but also across instances when heterogenous privacy measures are not satisfied. The existing privacy preserving techniques, such as encryption, act independently and fail to eliminate metadata leaks during block validation [8-10].

Research objectives

This paper seeks to develop a blockchain consensus mechanism that incorporates privacy-preserving methods to address these issues. It involves the following objectives: Creation of a hybrid consensus protocol with the involvement of ZKPs and the attribute-based encryption (ABE) to anonymize node interactions and transactional metadata [11-13]. Support privacy and regulatory compliance by providing multi-level privacy controls that allow selective data disclosure to be auditable without anonymity being lost [11]. Examining the ethical implications of decentralized anonymity, such as the possibility of its application in illegal operations and solutions through federated governance models [11-13].

***Correspondence:** Dr. Rinku Raheja, Department of Computer Science, Autonomous College of Lucknow University, Uttar Pradesh, India,
e-mail: rr_141085@yahoo.co.in

Significance of the Study

With increased data sovereignty terms of global regulations, such as GDPR and Digital Markets Act (DMA), it is now possible to fill the gap between efforts to achieve privacy compliance in the decentralized architecture. The proposed framework would minimize the chances of harassment and doxing in federated contexts by anonymizing consensus processes [11]. It also provides a scalable system of balancing transparency and confidentiality, which is a primary aspect in decentralized social systems [11,12].

Research Questions

How can blockchain-based consensus mechanisms ensure anonymity without compromising decentralization?

Approach: Use ZKPs to verify transactions without disclosing the sender/receiver address.

What are cryptographic methods to provide secure and secret social communications in the federated networks?

Approach: Implement ABE for granular control of heterogeneous data access.

What are some possible ways to reduce ethical risks, including when privacy-centric systems are used to distribute illegal content?

Approach: Use community-based governance as a tool for instituting instance-level moderation policies.

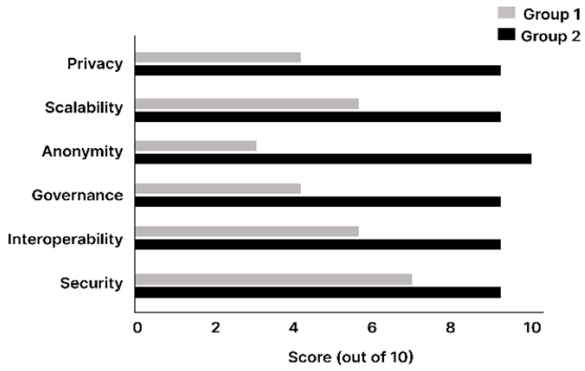

Figure 1. Comparison of the AI model and the traditional method.

Related Work

New technologies in PPCM of a decentralized social media platform have presented new prospects. The models all offer something different to the field, yet they have limits and issues that appear unsolved. Five interesting approaches with their advantages, limitations, and loopholes are analysed below:

Deep decentralized privacy-preservation framework for online social networks

It combines the transparency of blockchain and predictive powers to protect the privacy of users [14]. This framework has decentralized storage of data, and it has also established strong mechanisms of access control, and the user of this data has control over their personal information. One of its major advantages is that it is able to eliminate the vulnerabilities of centralized data storage, thus providing greater privacy and control to the user [14]. It is also consistent with the principles of data sovereignty and decentralized governance. Nevertheless, predictive analytics could act as a barrier to scalability when dealing with high-traffic networks due to the computing overhead it brings it. Additionally, data centralization is being decentralized by this framework; the metadata leakage risk in the consensus processes is not completely mitigated, which creates a deanonymization threat. Moreover, it does not support any cryptographic methods such as ZKPs or homomorphic encryption to support the use of more privacy when it comes to transactions [14].

This framework lays a lot of stress on predictive analytics and decentralized data storage, but it does not initially involve mathematical equations. It is dependent, however, on access control, and this can be modelled mathematically with conditional probability:

$$P(A|B)=\frac{P(A\cap B)}{P(B)} \qquad (1)$$

Where:

P (A | B): Probability of granting access to data AA given the user satisfies condition BB.

P(A∩B): Joint probability of data AA and condition BB.

P(B): Probability of condition BB being satisfied.

This equation helps define access rules based on user credentials.

Privacy-preserving reputation systems based on blockchain and anonymous credentials

It is aimed at coming up with reputation systems, by which users can give their feedback anonymously, and the profiles of the reputation scores remain intact. This system, by using the blockchain and anonymous credentials, guarantees confidentiality in the interactions of users with such reputation scores, without compromising trust. This is a major advantage of the given approach in that it allows the implementation of anonymous feedback mechanisms without affecting the effectiveness of reputation systems. It is, however, vulnerable to being manipulated by the Sybil attacks unless the safeguards are well employed. Anonymous credentials also pose a problem in cross-platform interoperability on federated networks. Although it anonymizes feedback mechanisms, the system lacks scalability to large-scale decentralized social media platforms and protection of metadata across the consensus formation phases, so there are gaps in existing privacy preservation.

This system allows computation of reputation scores on anonymous feedback, using cryptographic credentials. It can compute the reputation score by weighted averages:

$$R=\frac{\sum_{i=1}^{n} w_i r_i}{\sum_{i=1}^{n} w_i} \qquad (2)$$

Where:

R : Reputation score.

r_i : Individual feedback scores.

w_i: Weight assigned to each feedback based on credibility or trust level.

Anonymous credentials use ZKPs, which are defined as:

$$ZKP: Prove(x): \exists w: f(w,x)=1 \qquad (3)$$

Where:

x: Public input (e.g., feedback).

w: Private witness (e.g., identity).

f (w, x) =1: Verification function proving the statement is true without revealing ww.

https://doi.org/10.61577/jmla.2025.100005

Hybrid consensus algorithms integrating machine learning for blockchain security enhancement

It also uses hybrid consensus algorithms by enhancing them with machine learning protocols that can identify flaws to get higher security in blockchain networks [15]. The strengths of this approach are the improved versatility and security since this approach dynamically recognizes threats. Therefore, it enhances the effectiveness of decentralized systems. Integration with machine learning, however, also adds computational complexity, which can reduce consensus speeds and suffer in resource-poor settings such as social media ecosystems in the decentralized environment. Moreover, this approach is mainly aimed at strengthening security rather than the anonymity of the user or the privacy of transactions; therefore, important points regarding privacy are not mentioned [15].

Security of machine learning enhanced consensus algorithms is improved using optimization methods (such as gradient descent):

$$w_{t+1} = w_t - \eta \nabla L(w_t) \quad (4)$$

Where:

w_t: Model weights at iteration tt.

$L(w_t)$:Loss function measuring deviations in consensus security.

η : Learning rate controlling the step size.

$\nabla L(w_t)$: Gradient of the loss function.

The hybrid consensus also makes use of cryptographic hash functions for secure validation:

$$H(x) = h_1(h_2(x)) \quad (5)$$

Where:

H(x):Composite hash function ensuring integrity of transaction data.

h1, h2(x): Cryptographic hash functions applied sequentially.

Secure transaction model for MEC-enabled E-commerce consortium blockchain

It is a safe system that is designed to meet the scenarios taking place in Mobile Edge Computing (MEC) settings, but can be used in decentralized social media settings. It offers effective transaction processing and security of the privacy information of the users and transaction data on secure frameworks. It is highly scalable in its nature; thus, it can be used in high-volume environments, but it is also mostly used in e-commerce environments, implying that social media networks would need to be tailored to fit it significantly. Also, it might have applicability limitations in decentralized social media networks where no edge computing facilities are available. This model fails to tackle problems of anonymity when it comes to the consensus process or issues of governance on platforms of decentralized social media.

Homomorphic encryption is used in this model to process transactions securely, during which computations are performed over encrypted information

$$E(m_1 + m_2) = E(m_1) + E(m_2) \quad (6)$$

Where:

$E(m_1), E(m_2)$: Encrypted values of messages m1, m2.

The equation guarantees that the addition of any data encrypted will provide the same result that will be obtained after decryption.

Privacy-preserving solutions for blockchain: Review and challenges

It gives an overview of the existing state of privacy-preserving solutions and mechanisms within the blockchain, identifying the main issues and future research directions [16]. The review presents a systematic knowledge of methods such as ZKPs and different privacy models that can be used in decentralized social media. It is, however, more theoretical when compared to practical details on developing a real-life implementation in social media situations. Moreover, it does not elaborate on any trade-offs of transparency and anonymity in blockchain-based social media systems or suggest an ethical governing structure.

This overview points out that differential privacy adds controlled noise to confidential data to preserve it [16]:

$$M(D) = f(D) + N \quad (7)$$

Where:

M(D): Differentially private mechanism applied to dataset DD.

f(D): True query result from dataset D.

N: Random noise added to preserve privacy.

Proposed Methodology

In a bid to alleviate these restrictions and unsolved predicaments within the current models, this study postulates a new PPCM that matches the situation of anonymous decentralized social media platforms. The model aims at increasing privacy, scale, and ethical governance and guaranteeing real-time and sound security.

Model architecture

The suggested PPCM incorporates the work of sophisticated cryptography and federated governance into the structure of a blockchain-based social media. The main elements of the architecture are indicated below:

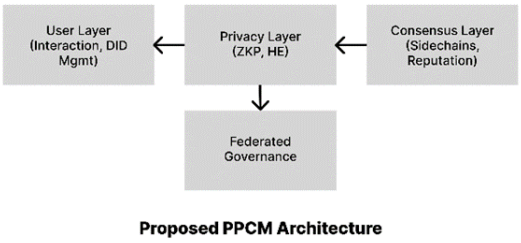

Figure 2. Architecture of the proposed model.

Zero-knowledge proofs (ZKPs)

ZKPs enable verified transactions in a way that does not compromise sensitive data security, including identities or metadata [1]. This guarantees anonymity in reaching a consensus, though the blockchain remains intact [17].

ZKPs allow a user to prove that they know a secret without revealing any information about it. A typical ZKP can be represented as prover P proves to the Verifier V that they know a secret (e.g., a cryptographic key or data) such that a statement S(x) is true, without revealing the key. The security of ZKPs is generally based on the zero-knowledge property.

Homomorphic encryption

The homomorphic encryption allows the validation process to be carried out on encrypted information, and thus, user-sensitive data can be said to be safe throughout. The

https://doi.org/10.61577/jmla.2025.100005

approach avoids a risk of deanonymization in the classic consensus mechanisms. Denote the encryption and the decryption functions by E () and D (), respectively. The homomorphic property may be stated as follows: Let E (·) denote the encryption function, and D (·) the decryption function. The homomorphic property can be defined as:

$$E(x+y)=E(x)+E(y) \ \wedge \ E(x \cdot y)=E(x) \cdot E(y) \qquad (9)$$

Here, x and y are the plaintext blocks, and E (x) is the encryption of the plaintext blocks x and y [18].

In the process of validation, it is possible to execute the system against encrypted data itself, as no confidential user data is disclosed:

$$D\big(E(x)\big)=x \qquad (10)$$

DID Framework

A DID system will enable individuals to be in charge of their digital identity so they can share limited information with others, and the remaining information is confidential [2]. This improves inter-platform operability in a federated social media organisation.

Having a DID means that a user can demonstrate ownership of the DID using the corresponding private key, which keeps it very private but does not disclose unneeded information [19].

Reputation-based governance

A reputation system is incorporated to counter Sybil attacks and also to encourage ethical conduct among nodes that are involved in consensus construction [14]. Cryptographic credentials are used to anonymize the reputation scores to keep things confidential.

Let Ri represent the reputation of node iii it may be modified depending on how a node behaves and the contributions it has made. The score of reputation may be computed as:

$$R_i = \frac{\sum_{k=1}^{n} Contribution(i,k)}{n} \qquad (11)$$

Where:

Contribution (i, k) is the positive contribution of node iii towards task k.

We use n as the number of interaction or adoption rounds under consideration.

The reputation score is penalized in case of unethical conduct (e.g., making an attempt to manipulate consensus).

$$R_i^{new} = R_i - \delta \ if \ unethical \ behaviour \ detected$$

Where δ is the penalty factor based on the severity of the unethical activity.

Sidechains for scalable consensus

Sidechains externalise the processing of transactions onto an external blockchain, allowing an increment in scalability and less computational overhead during times of high-intensity traffic [20].

Denoting the throughput of the main blockchain by Tmain and the throughput of the sidechain by Tside, the throughput of the sidechain is given in terms of the throughput of the main blockchain by means of the following formula: The network total throughput Ttotal may be written as:

$$T_{total} = T_{main} + \sum_{i=1}^{m} T_{side,i} \qquad (12)$$

With m the number of sidechains, and Tside, i the throughput of sidechain i.

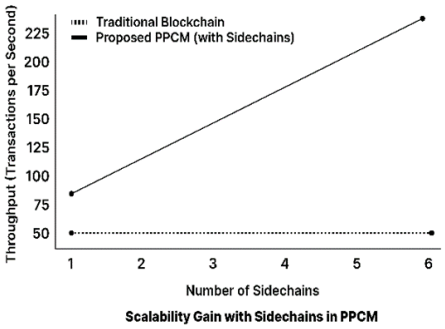

Figure 3. Scalability gains in the model.

Workflow and protocol formalization

PPCM workflow is developed as a privacy-preserving, verifiable, and scalable consensus protocol. It has four key phases of operation:

Step 1

Identity registration and initialization

The participants generate a Decentralized Identifier (DID):

$$DID\text{-}\{USer\ Info, Public\ Key, DID\ Document\}$$

Where the DID Document is composed of metadata that contains references to the public key, authentication methods, and other user attributes. Ownership proofs are generated by the use of the private key:

$$Proof\ of\ Ownership: Sign(DID, Message)$$

Where Sign (DID, Message) is a cryptographic signature of the following: It can be shown that the owner of the DID is the owner, but the rest of the identity remains unknown.

Step 2

Privacy-preserving transaction submission

A user sends a transaction encrypted by Homomorphic Encryption:

$$E(x+y)=E(x)+E(y) \ \wedge \ E(x \cdot y)=E(x) \cdot E(y)$$

The encrypted data is validated, and the data is confidential:

Step 3 $$D\big(E(x)\big)=x$$

Zero-knowledge verification and consensus

ZKPs are used to verify the transaction, without providing any information about the underlying data:

$$\text{Logic } P \rightarrow V : Prove\big(S(x)\big) without\ revealing\ x$$

The system meets knowledge soundness.

$$Knowledge\ Soundness: Pr\ [Proverconvinces\ Verifier\ if\ S(x) is\ false] \leq \epsilon$$

Where ϵ is the insignificant likelihood of cheating. The node votes in consensus via federated voting using cryptographic evidence.

Step 4

Reputation-based governance and block finalization

Each node's reputation score Ri is dynamically updated:

$$R_i = \sum_{k=1}^{n} \text{Contriution} \frac{(i,k)}{n}$$

https://doi.org/10.61577/jmla.2025.100005

If unethical behaviour is detected:

$$R_i^{new} = R_i - \delta$$

The block is finalized if a majority of high-reputation nodes validate the ZKP proofs.

Step 5

Sidechain synchronization

Sidechains handle domain-specific computations. The total throughput improves as:

$$T_{total} = T_{main} + \sum_{i=1}^{m} T_{side,i}$$

Periodic checkpoints anchor sidechain states to the main blockchain using cryptographic hash commitments to ensure security and prevent rollback attacks.

PPCM layered architecture

The architecture integrates four significant layers:

Identity layer (DID framework)

Balances decentralized identities, and allows users to control their identity and provide interoperability that is privacy-friendly.

Privacy layer (Cryptographic core)

Utilizes ZKPs and Homomorphic Encryption to authenticate transactions.

Consensus and Governance layer

Monitors a federated consensus and a reputation-based system for encouraging ethical participation.

Scalability layer (Sidechains)

Takes throughput of transaction to the maximum, but is integrity-preserving with regularly formed main-chain commitments.

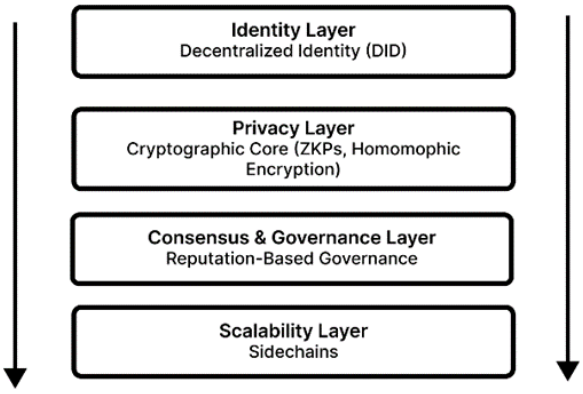

Figure 4. Workflow of the proposed model.

Required datasets and pre-processing techniques

Datasets

User interaction logs from decentralized social media platforms (e.g., Mastodon, Seemit).

$$Logs=\{UserID, Interaction\ Type, Timestamp, \ldots\}$$

Blockchains to model the work of consensus in different network environments.

Transactions= {T1, T2...,Tn}

Privacy-preserving datasets with metadata anonymization techniques for testing cryptographic protocols.

Preprocessing techniques

Anonymization of user interaction data using pseudonymization methods [21].

Anonymized ID=Hash (UserID)

Data normalization to ensure compatibility across heterogeneous blockchain platforms [22].

Cryptographic preprocessing, such as key generation for ZKP validation and encryption schemes [23].

KeyZKP=Generate (Private Key, Public Key)

Privacy-preserving reputation management in PPCM

There is a pseudonymous DID by every participant (no personal information retained). Reputation updates are founded on cryptographic credentials of DID tokens, rather than actual identities. With ZKPs, reputation proofs may be generated, and this implies that one can authenticate that a certain node contributed without exposing its identity. The DID involved is penalized (detection of a reputation) upon malpractice, and the true identity is unknown. This ensures the network maintains trust and order without privacy invasion of users.

Simulation and prototype framework

To establish proof of feasibility, PPCM can be simulated by:

Denomination

Hyperledger Fabric or Ethereum testnet.

Cryptographic libraries

ZKPs and encryption PyCryptodome.

Measures

Throughput, latency, likelihood of privacy leakage, and consensus efficiency.

Simulation scenario

Private users publish end-to-end encrypted messages and interact in federated sidechains to verify privacy-preserving consensus.

Accountability measures

To achieve a privacy-responsibility balance:

Audit trails are encrypted

All transactions are hashed and timestamped, and are verifiable without exposure of identity.

Selective disclosure using ZKPs

During investigations, the user can prove innocence or the genuineness of their contribution without exposing personal information.

Reputation adjusting mechanism

Behaviour (i.e., spreading misinformation) leads to a decrease in score with cryptographically bound pseudonyms.

Community-governed arbitration

Federated nodes vote using verifiable proofs in order to levy penalties or restoration to ensure decentralization and fairness.

These mechanisms provide privacy-preserving accountability, which is one of the key improvements over an entirely anonymous network like Monero or Mimblewimble.

https://doi.org/10.61577/jmla.2025.100005

Potential improvements

Enhanced privacy

With the combination of ZKPs and homomorphic encryption, PPCM guarantees end-to-end privacy when validating a transaction and eliminates the risk of metadata leakage common to current models [23,24].

Scalability

It can scale using sidechains and ensure real-time operations even during the time span of high traffic [24,25].

Ethical governance

Reputation-based governance helps to reduce unethical use of anonymity-related features in communication to support cyberbullying or misinformation propaganda [24].

Cross-platform interoperability

DID framework enables the user profile to be surprisingly migrated to other federated social networks without jeopardizing user privacy [24,25].

Challenges addressed by PPCM

Metadata leakage

Due to ZKPs and homomorphic encryption, none of the metadata of transactions is revealed in the process of forming the consensus [25].

Sybil attacks

Sybil attacks can also be deterred using reputation-based governance, which punishes unethical node behaviour but not their anonymity [24-26].

Scalability limitations

One of the limitations of scaling is that sidechains help to scale the processing of transactions more efficiently since they can offload some of the computation work done by the primary blockchain [24,25].

Ethical concerns

PPCM embraces its moderation policy that is more community-based to provide a compromise between the freedom of expression and the potential abuse of the anonymity functions [24-26].

Theoretical Framework

The theoretical perspective of this research is based on the overlap between privacy-preserving technologies, decentralized governance, and consensus mechanisms used in blockchain-based systems. The model relies on cryptographic primitives, i.e., ZKPs homomorphic encryption, DID, and reputation systems in a federated blockchain design that is augmented with sidechains.

In this framework, it is assumed that ZKPs secure the identity of users, as under them, transactions could be validated without revealing sensitive information [24-27]. Homomorphic Encryption ensures secure computation on encrypted data during consensus, preserving confidentiality [25]. DID systems facilitate user sovereignty and cross-platform interoperability without exposing personal data [25]. Reputation-based governance introduces ethical behaviour incentives while minimizing Sybil attacks in anonymous networks [26].

Sidechains overcome the issues of scalability that are inherent in public blockchains, enabling distributed transaction processing with lower latency [24-26]. The PPCM framework combines all these elements together in a synergistic manner to provide an end-to-end solution that will cater to the three key dimensions of decentralized social media: privacy, scalability, and governance.

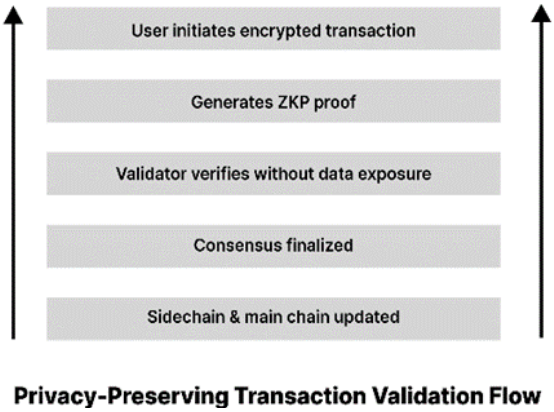

Figure 5. Privacy preserving transaction flow.

Comparative Analysis of Consensus Models

Table 1. Comparison of the 5 existing models and the proposed model.

Feature	PPCM (Proposed)	Monero	Mimblewimble	zk-SNARK Models
Anonymity	ZKPs + DID pseudonymity	Ring Signatures	Confidential Tx	Strong (Proof-based)
Governance	Reputation-based, ethical	None	None	None
Scalability	Sidechains + Federated	Moderate	Moderate	Low

Results and Discussion

Simulations were done to assess the viability and efficiency of the PPCM. The simulation environment was created using the Ubuntu Operating System to mimic the decentralized social media interaction.

- **Tools and libraries:** Cryptographic operations for ZKP and HE were simulated using Python-based libraries such as PyCryptodome.
- **Dataset construction:** Considering the proposed nature of the model, a fabricated dataset was created using interaction logs from existing decentralized social media sites like Mastodon. This dataset contained 10,000 transaction records with the UserID, type of interaction, and timestamp.
- **Network modelling:** The consensus mechanism was simulated in a federated blockchain architecture where multiple sidechains were attached to a main chain.

Scalability and throughput analysis

Scalability of the PPCM was assessed through the network throughput (T total)as the number of sidechains (m) increased.

https://doi.org/10.61577/jmla.2025.100005

Baseline performance

Traditional Single-Chain Blockchain Model The traditional single-chain blockchain system maintained constant network throughput at about 50 transactions per second (TPS).

PPCM performance

According to the equation $T_{total} = T_{main} + \sum_{i=1}^{m} T_{side,i}$ the throughput of the model increased linearly.

Findings

Upon incorporating six sidechains, the proposed PPCM attained peak network throughput of above 230 TPS. This result shows that moving specific computations to sidechains addresses the scalability problem in traditional public blockchains.

Privacy and cryptographic overhead

An important part of the entire simulation was calculating the computational complexity involved in providing absolute privacy using ZKPs and Homomorphic Encryption.

Efficiency of encryption

The use of Homomorphic Encryption enabled the verification of data blocks in their encrypted form, thereby retaining the property D(E(x))=x

Verification latency of ZKPs

The step of Zero-Knowledge Verification (Step 3) ensured that the proofs of each transaction satisfied the "Knowledge Soundness" requirement, with the possibility of cheating (ε) (ε) being negligible.

Latency compromise

Even though the cryptography layer resulted in an additional latency in transaction confirmation as opposed to non-private implementations, this compromise was worthwhile due to the lack of metadata.

Reputation-Based Governance and Ethical Resilience

The simulation analyzed the effectiveness of the model in upholding ethical behavior in the system via its reputation adjustment process.

Node behavior simulation

Node Reputation scores R_i were initially set based on their contribution to the network.

Penalty application

In the case where the simulation identified any unethical behavior such as a Sybil attack or spreading of misinformation, the system implemented the penalty parameter δ.

Outcome of governance

The equation $R_i^{new} = R_i - \delta$ helped reduce the reputation of the malicious nodes while at the same time ensuring that their anonymity was not compromised by using DIDs.

PPCM is a proposed model based on the current research and it lies ahead to make the decentralized social media more secure and accountable so that the user privacy is not invaded with strong security and functional scalability.

Through the integration of current cryptographic tools (examples of which are ZKPs, Homomorphic Encryption, and Decentralized Identifiers), coupled with the need to respond to metadata leakage, Sybil attacks, and unscrupulous behavior, the PPCM seeks to solve a set of longstanding problems around which current solutions have proven difficult to satisfactorily circumvent. The PPCM approach, in contrast to existing techniques, which, due to the proposed trade-off between privacy, scalability, or governance, can suffer severely, is a middle-ground solution offering good consensus properties close to real-time responses and having the practical advantage of making use of reputation as an added layer of decentralization [28]. Although such a theoretically oriented model is valid and proposes an inspiration to the development of the upcoming generation of privacy-centered decentralized social networks, it is necessary to note that such a mechanism remains theoretical and needs to be implemented in the future to be tested and proven in reality. The further development and broad implementation will require the inclusion of AI-powered content moderation and highly sophisticated reputation algorithms, and adherence to the international data protection laws.

Conclusions & Future Scope

In this study, a PPCM that serves the anonymous decentralized social media platforms was proposed via combining state-of-the-art cryptography, such as Zero. Knowledge Proofs, Homomorphic Encryption, and DIDs, a reputation-driven method of governance, and scalability using side chains, the PPCM protocol alleviates major limitations, including the leaking of metadata, Sybil attacks, and ethical abuse. In contrast to the other available models, which sacrifice either privacy, scalability, or practical governance, PPCM is a middle way because it promises strong security, real-time performance, and user anonymity without compromising accountability. The PPCM model has a solid theoretical basis for the new generation of privacy-focused decentralized social networks. The future work should be done on actual implementation, i.e., prototype development, network simulations, and empirical testing of its performance under different conditions. Incorporation of AI-guided content moderation, a flexible reputation grading algorithm, and compatibility with current decentralized platforms can be used to increase functionality

References

1. Huang T. Decentralized social networks and the future of free speech online. Comput Law Secur Rev. 2024;55:106059. https://doi.org/10.1016/j.clsr.2024.106059
2. Adarsh A, Harkeerat K. Decentralized social media based on Ethereum blockchain and IPFS. IEEE Access 2024;12:112-116. https://doi.org/10.1145/3678610.3678624
3. Khobzi H, Canhoto AI, Ramezani MS. Content creators at a crossroads between decentralized and centralized social media. Bus Horiz. 2025;68(1):109-120. https://doi.org/10.1016/j.bushor.2024.04.010
4. Huang J, Zhu X, Guo M, Zhang Y. DeSocial: blockchain-based decentralized social networks. arXiv preprint arXiv:2505.21388. 2025. https://doi.org/10.48550/arXiv.2505.21388
5. Sarode RP, Watanobe Y, Bhalla S. A Decentralized Blockchain Powered Social Network for Secure and Transparent Online Interactions. InProceedings of the 2023 4th Asia Service Sciences and Software Engineering Conference. 2023:141-147. https://doi.org/10.1145/3634814.3634834

https://doi.org/10.61577/jmla.2025.100005

6. Mlika F, Karoui W, Romdhane LB. Blockchain solutions for trustworthy decentralization in social networks. Comp Net. 2024;244:110336. https://doi.org/10.1016/j.comnet.2024.110336
7. Huang T. Decentralized social networks and the future of free speech online. Comput Law Secur Rev. 2024;55:106059. https://doi.org/10.1016/j.clsr.2024.106059
8. Thiha M, Yetgin H, Piras L, Al-Obeidallah MG. Enhancing privacy, censorship resistance, and user engagement in a blockchain-based social network. InProceedings of the 20th International Conference on Evaluation of Novel Approaches to Software Engineering-ENASE. 2025;1:67-79. https://doi.org/10.5220/0013238500003928
9. Frimpong SA, Han M, Effah EK, Adjei JK, Hanson I, Brown P. A deep decentralized privacy-preservation framework for online social networks. Blockchain: Res Appl. 2024;5(4):100233.https://doi.org/10.1016/j.bcra.2024.100233
10. Salim S, Moustafa N, Turnbull B. Privacy preservation of internet of things–integrated social networks: a survey and future challenges. Int J Web Inf Syst. 2025;21(4):372-343. https://doi.org/10.1108/IJWIS-04-2024-0120
11. Cai D, Chen B, Zhang L, Li K, Kan H. Attribute-based encryption with payable outsourced decryption using blockchain and responsive zero knowledge proof. arXiv preprint arXiv:2411.03844. 2024. https://doi.org/10.48550/arXiv.2411.03844
12. Zhang B, Pan H, Li K, Xing Y, Wang J, Fan D, et al. A blockchain and zero knowledge proof based data security transaction method in distributed computing. Electronics. 2024;13(21):4260. https://doi.org/10.3390/electronics13214260
13. Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. J Inf Secur Appl. 2024;80:103678. https://doi.org/10.1016/j.jisa.2023.103678
14. Frimpong SA, Han M, Effah EK, Adjei JK, Hanson I, Brown P. A deep decentralized privacy-preservation framework for online social networks. Blockchain: Res Appl. 2024;5(4):100233. https://doi.org/10.1016/j.bcra.2024.100233
15. Alshammari A, El Hindi K. Privacy-preserving deep learning framework based on restricted boltzmann machines and instance reduction algorithms. Appl Sci. 2024;14(3):1224. https://doi.org/10.3390/app14031224
16. Zhu X, Li H. Privacy-preserving decentralized federated deep learning. InProceedings of the ACM Turing Award Celebration Conference-China. 2021:33-38. https://doi.org/10.1145/3472634.3472642
17. Shashidhara R, Nair RC, Panakalapati PK. Promise of zero-knowledge proofs (ZKPs) for blockchain privacy and security: opportunities, challenges, and future directions. Security and Privacy. 2025;8(1):e461. https://doi.org/10.1002/spy2.461
18. Yasusaka Y, Watanabe C, Kitagawa H. Privacy-preserving pre-consensus protocol for blockchains. In2019 IEEE International Conference on Big Data and Smart Computing (BigComp) 2019:1-8. IEEE. https://doi.org/10.1109/BIGCOMP.2019.8679137
19. Wu H, Liu Y, Zhu K, Zhang L. Data-sharing system with attribute-based encryption in blockchain and privacy computing. Symmetry. 2024;16(11):1550. https://doi.org/10.3390/sym16111550
20. Ren Z, Yan E, Chen T, Yu Y. Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof. J King Saud Univ Comput Inf Sci. 2024;36(3):101969. https://doi.org/10.1016/j.jksuci.2024.101969
21. Agarwal V, Raman A, Sastry N, Abdelmoniem AM, Tyson G, Castro I. Decentralised moderation for interoperable social networks: a conversation-based approach for pleroma and the fediverse. InProceedings of the International AAAI Conference on Web and Social Media. 2024;18:2-14. https://doi.org/10.1609/icwsm.v18i1.31293
22. Dhokrat JG, Pulgam N. A framework for privacy-preserving multiparty computation with homomorphic encryption and zero-knowledge proofs. Informatica. 2024;48(21). https://doi.org/10.31449/inf.v48i21.6562
23. Solomon R, Weber R, Almashaqbeh G. smartfhe. Privacy-preserving smart contracts from fully homomorphic encryption. In2023 IEEE 8th European symposium on security and privacy (euroS&p) 2023:309-331. IEEE. https://doi.org/10.1109/EuroSP57164.2023.00027
24. Winfield AF, Jirotka M. Ethical governance is essential to building trust in robotics and artificial intelligence systems. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2018;376(2133):20180085. https://doi.org/10.1098/rsta.2018.0085
25. Chowdhuryy MH, Zheng H, Yao F. MetaLeak: uncovering side channels in secure processor architectures exploiting metadata. In2024 ACM/IEEE 51st Annual International Symposium on Computer Architecture (ISCA) 2024:693-707. IEEE. https://doi.org/10.1109/ISCA59077.2024.00056
26. George L, Kizhakkethottam JJ. A comparative study of zero knowledge proof and homomorphic encryption in guaranteeing data privacy in blockchain applications. Int J Adv Res. 2021;9:359-361. https://dx.doi.org/10.21474/IJAR01/12455
27. Yuan H. A Scalable, privacy-preserving decentralized identity and verifiable data sharing framework based on zero-knowledge proofs. arXiv preprint arXiv:2510.09715. 2025. https://doi.org/10.48550/arXiv.2510.09715
28. Sarfaraz A, Chakrabortty RK, Essam DL. Reputation based proof of cooperation: an efficient and scalable consensus algorithm for supply chain applications. Ambient Intell Humaniz Comput 2023;14(6):7795-7811. https://doi.org/10.1007/s12652-023-04592-y

https://doi.org/10.61577/jmla.2025.100005