International Journal for Housing Science and Its Applications

Publish September 16, 2025. Volume 47, Issue 1 Pages 1159-1168

https://doi.org/10.70517/ijhsa471100

Management in the Energy Data Space: A Blockchain and Smart-Contract-Driven Framework

Yu Song[1,*], Wen Yang[1] and Shengjie Wei[1]

[1] State Grid Jiangsu Electric Power Co., Ltd., Information & Communication Branch, Nanjing 210000, China

Corresponding authors: (e-mail: 1203958766@qq.com).

Abstract The rapid development of the digital economy and the deployment of large-scale electricity big-data platforms have highlighted both the opportunities and risks associated with energy data circulation. Conventional identity management frameworks in the energy sector suffer from weak authentication, fragmented governance, and high compliance costs, limiting the secure and efficient realization of data value. This paper proposes a decentralized digital identity (DID) management framework tailored for the energy data space. By integrating blockchain-based traceability, verifiable credentials, and smart-contract-driven privacy protection, the framework establishes a sovereign, interoperable, and privacy-preserving identity infrastructure. Through simulation experiments using Monte Carlo modeling, we evaluate the performance of the proposed system under different blockchain infrastructures (Fabric vs. EVM) and disclosure mechanisms (plain vs. zero-knowledge proofs). The results demonstrate that Fabric achieves lower latency and higher throughput compared to EVM, while zero-knowledge proofs introduce moderate but acceptable overhead, enabling stronger privacy guarantees. The proposed framework effectively tackles the key challenges of secure identity verification, fine-grained and dynamic authorization, and tamper-resistant auditing, thereby establishing a scalable and reliable foundation for trusted circulation of energy data.

Index Terms DID, Blockchain, Smart Contract, Privacy Protection, Energy Data Space, Zero-Knowledge Proof

I. Introduction

With the accelerating growth of the global digital economy, data has become an essential factor of production [1]. Digital transformation is not only an intrinsic driver for improving operational efficiency [2], but also a strategic imperative for developing next-generation power systems [3]. Yet, current technologies remain inadequate in safeguarding sensitive information—such as household electricity consumption—while the costs of privacy protection and regulatory compliance continue to be substantial [4], [5].

In response, China has established province-level electricity big-data platforms to facilitate large-scale aggregation and analytics [6]. Despite this progress, major obstacles persist in enabling cross-organizational collaboration and unlocking the latent value of energy data. On one hand, electricity data represents a strategic asset that can enhance industrial productivity and support energy system optimization. On the other hand, its circulation is hindered by fragmented governance, limited interoperability, and the risk of information leakage. Conventional modes of data exchange expose a structural tension between value creation and security: while data packaging and transactions increase the risk of sensitive exposure, API-driven access often imposes inflexible constraints on integration [7]. These limitations underscore the urgent need for new paradigms that simultaneously achieve value realization and robust protection [8].

At the heart of this challenge lies digital identity management [9]. In the context of accelerating digitalization in the energy sector, conventional identity frameworks exhibit critical limitations: weak authentication, elevated leakage risks, and severe interoperability barriers across heterogeneous systems [10]. Current mechanisms for authorization and access control are often coarse-grained and slow to adapt, leading to over-provisioning or delayed revocation of rights. Furthermore, the lack of standardized identity protocols has exacerbated the problem of "data silos," hindering cross-organizational collaboration and constraining the development of energy data markets [11], [12].

With the rapid evolution of smart technologies [13]–[17] within the context of smart grids, significant research has been devoted to privacy-preserving techniques for energy data sharing. A wide range of schemes—such as homomorphic encryption and differential privacy—have been developed to protect consumer data during aggregation and analysis [18]. More recently, secure multiparty computation and federated learning have been introduced to support collaborative energy management without exposing sensitive information, particularly in peer-to-peer (P2P) energy trading environments [19],

[20]. For example, data-driven models employing deep learning for risk assessment in power grids increasingly emphasize privacy preservation while retaining actionable operational insights [19]. Despite these advances, striking a balance between data utility and security remains challenging, as most approaches still rely on centralized mechanisms that constrain scalability.

Parallel to this, digital identity management in smart grids has attracted growing attention. Existing surveys underscore persistent cybersecurity challenges and the urgent need for robust authentication frameworks [21]. In IoT-enabled smart grids, identity management has been embedded into security protocols to mitigate vulnerabilities in communication layers [22]. Nevertheless, many frameworks continue to suffer from weak revocation mechanisms and insufficient standardization, thereby impeding cross-organizational interoperability.

In recent years, blockchain has emerged as a promising enabler for secure energy data circulation. Its decentralized ledger structure ensures transparency and tamper-resistance in transactions, while reviews of energy blockchain applications categorize protections across storage, management, and utilization domains [23]. State-of-the-art analyses further confirm that blockchain enhances both visibility and security in energy systems, though seamless integration with existing infrastructures remains a major barrier [24].

To address these issues, this study proposes a decentralized digital identity (DID) management framework tailored for the energy data space. By integrating blockchain technology with zero-trust architecture, and leveraging distributed identifiers, attribute-based encryption, and smart contracts, the framework achieves precise identity verification, fine-grained dynamic authorization, and tamper-resistant auditability. This design not only ensures regulatory compliance and accountability throughout the entire data lifecycle, but also establishes a unified, privacy-preserving identity standard to enable secure multi-party data sharing across power grids, renewable energy operators, and third-party service providers. In summary, our contributions are threefold:

- **A sovereign and interoperable identity paradigm.** We introduce a DID-based approach that empowers users to autonomously generate and manage digital identities, thereby overcoming the limitations of centralized identity providers and enabling cross-domain interoperability.
- **A dynamic fine-grained authorization mechanism.** Through blockchain-anchored smart contracts, we construct a multi-dimensional permission engine that enforces real-time, context-aware access control, balancing security and flexibility in energy data sharing.
- **A distributed trust foundation for the energy sector.** By deploying a consortium blockchain that integrates grid companies, generation groups, and market participants, we establish distributed trust anchors to support seamless identity recognition and single-sign-on across platforms.

II. Implementation Path of the Digital Identity System in the Energy Data Space

To overcome the challenges of privacy protection, interoperability, and fine-grained authorization in the energy sector, we propose a unified implementation framework for digital identity management in the energy data space. The framework integrates three complementary components—DID, blockchain-based traceability, and smart-contract-driven privacy protection—into a coherent architecture that ensures both security and compliance (see Figure 1).

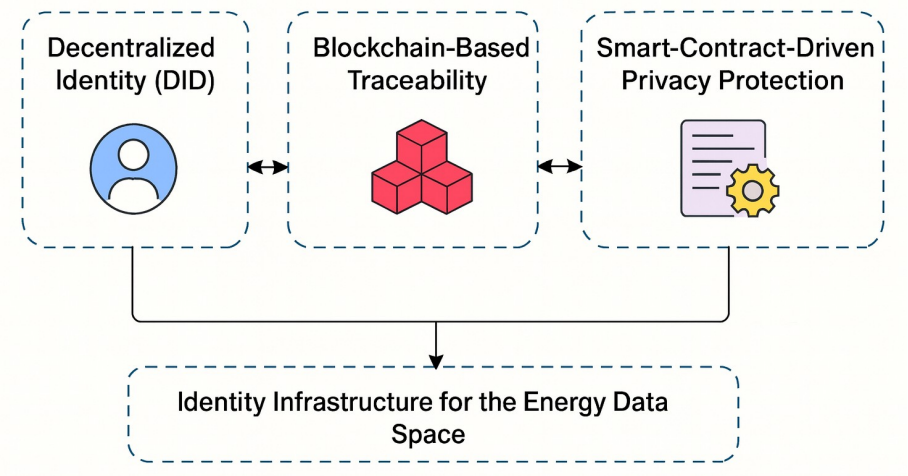

Figure 1: Unified implementation framework for digital identity management in the energy data space, integrating DID, blockchain-based traceability, and smart-contract-driven privacy protection.

The proposed implementation path integrates DID for sovereign identity management, blockchain for verifiable traceability, and smart contracts for automated, privacy-preserving governance. Collectively, these components establish a secure, interoperable, and efficient identity infrastructure for the energy data space. This architecture not only addresses current deficiencies—such as weak authentication, fragmented identity management, and high compliance costs—but also provides a scalable technical foundation for trusted data circulation in provincial-level energy data markets.

II. A. Blockchain-Based Traceability

Blockchain provides the immutable, transparent, and tamper-evident infrastructure required for the trustworthy execution of DID operations. Its chained data structure guarantees that any modification to historical records invalidates subsequent hashes, thereby preserving data integrity across the ledger. This property is crucial in the energy data space, where digital identities and data transactions must be verifiable across multiple stakeholders.

Within the proposed framework, the complete lifecycle of a DID—including creation, registration, update, and deactivation—is anchored on-chain through smart contracts. Specifically:

1. **Key generation and binding.** Users generate asymmetric key pairs locally and construct DID Documents. Only cryptographic hashes of the documents are stored on-chain to balance efficiency and privacy.
2. **Credential issuance and storage.** Trusted authorities issue digitally signed Verifiable Credentials (VCs), which are linked to user DIDs and securely stored in local or decentralized storage.
3. **Verification and validation.** Verifiers authenticate credentials by checking signatures and comparing document hashes with blockchain records.
4. **Revocation and auditability.** Revocation registries and update logs are maintained on-chain, providing immutable audit trails for compliance and regulatory oversight.

To strengthen privacy, advanced cryptographic techniques such as zero-knowledge proofs (e.g., zk-SNARKs) and selective disclosure are employed. These mechanisms allow users to demonstrate the validity of credentials or attributes without revealing sensitive raw data, thereby mitigating risks of information leakage. Sector benefits:

- **Cross-organizational identity verification.** Grid operators, energy suppliers, and regulators can authenticate entities without relying on a centralized authority.
- **Data provenance and accountability.** The origin and modification history of energy-related data (e.g., meter readings, carbon accounting records) can be securely tracked.
- **Decentralized access control.** Smart contracts enforce fine-grained, verifiable access rules for shared energy datasets.

Despite these advantages, challenges remain regarding scalability, interoperability with legacy systems, and governance mechanisms. Addressing these challenges is essential for enabling blockchain-based DID systems to achieve wide adoption in the energy sector.

II. B. Decentralized Identity (DID)

Decentralized Identity (DID) is a novel identity authentication paradigm based on blockchain technology. Owing to its decentralized design and user-centric control, DID is widely regarded as one of the most suitable mechanisms for identity management in Web3 and the Metaverse. The core principle of DID is to represent individuals or organizations through identifiers that are independent of centralized authorities, thereby addressing the limitations of traditional authentication systems. In this paper, the DID mechanism follows the W3C DID standard [25].

II. B. 1) DID Terminology

A DID is defined as a Uniform Resource Identifier (URI) with the format did:method:identifier, where the method specifies the system or blockchain to which the DID belongs (e.g., btcr for Bitcoin, ether for Ethereum). A DID Document is a JSON-formatted file containing metadata about the DID subject. A key feature is the inclusion of public keys associated with the DID subject and controller. These public keys enable ownership or control of the document to be proven using the corresponding private keys.

II. B. 2) Verifiable Credential Model

The Verifiable Credential (VC) model defines the roles of four entities: issuer, holder, verifier, and registry service. The issuer creates credentials based on identity attribute claims and transfers them to the holder. The holder manages one or more VCs and generates verifiable presentations from them. The verifier validates VCs received from holders. The registry service supports the resolution of DIDs and associated metadata. The conceptual model is shown in the Figure 2.

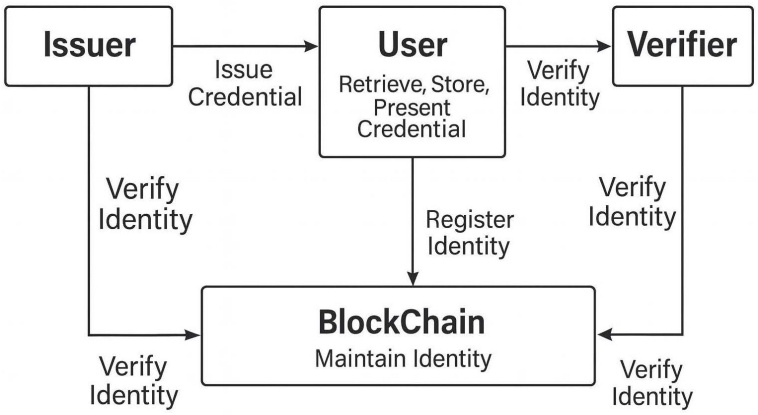

Figure 2: Conceptual model of the DID and Verifiable Credential mechanism.

While DID defines the conceptual model and its key components, its reliable realization requires blockchain as the underlying infrastructure to ensure immutability, accountability, and trust.

II. C. Smart-Contract-Driven Privacy Protection

Smart contracts are self-executing programs deployed on blockchains, in which the terms of agreement are encoded directly into code. In the context of digital identity management for the energy data space, smart contracts enable automated identity authentication, permission management, and fine-grained access control. For instance, when a user requests access to specific datasets from an energy enterprise, the smart contract verifies the legitimacy of the request based on predefined rules. If all conditions are satisfied, the contract automatically grants access; otherwise, it rejects the request. The automated execution of smart contracts reduces the need for human intervention, enhances operational efficiency, and mitigates trust-related risks. Beyond authentication, smart contracts enable fine-grained control over data usage. In data-sharing scenarios, providers can embed conditions—such as usage frequency, application scope, or redistribution restrictions—directly within a contract. Any violations automatically trigger penalties, including revocation of access or on-chain violation records, thereby ensuring compliance, accountability, and transparency.

Smart contracts thus serve as a cornerstone for self-sovereign identity (SSI) and cross-domain identity authentication. Once deployed, both their code and execution history remain immutable and transparent, immune to concealment or tampering. Contracts are triggered strictly under predefined conditions, eliminating reliance on third-party mediation and reinforcing decentralization. Within identity management, smart contracts can orchestrate operations such as DID registration, credential verification, permission enforcement, and identity revocation, collectively building a highly reliable and automated identity management system.

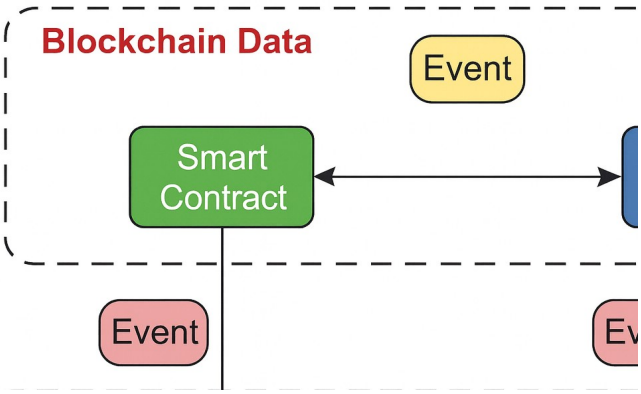

Figure 3: Architecture of smart-contract-driven privacy protection in the energy data space.

As illustrated in Figure 3, this smart-contract-driven privacy protection mechanism operates through the interplay of smart contracts, blockchain data, and triggered events. By managing credentials, enforcing policies, and interacting with blockchain events, smart contracts ensure transparency, immutability, and autonomous execution.

In large-scale, value-driven networks such as the energy data space, repeated identity verification across multiple domains introduces complexity and inefficiency. Traditional methods require users to undergo multiple checks (e.g., SMS codes, ID verification, facial recognition, or video authentication) whenever they access different platforms. By integrating DID with smart contracts, this process is significantly simplified. Once a certificate authority issues a VC, the credential can be securely stored in the user's local device or cloud wallet. Authentication workflow (see Figure 4):

1. The user logs into a website or application and clicks the authentication button.
2. The server generates an authentication request and transmits it to the user's DID application (e.g., via QR code).
3. The DID application checks whether the user possesses a VC satisfying the requested attributes, then prompts the user to unlock their private key (e.g., fingerprint or password).
4. Upon confirmation, the user signs the request to generate a Verifiable Presentation (VP), which is returned to the server.
5. The server verifies the VP signature and, if valid, records the VP and associates it with the user's DID.

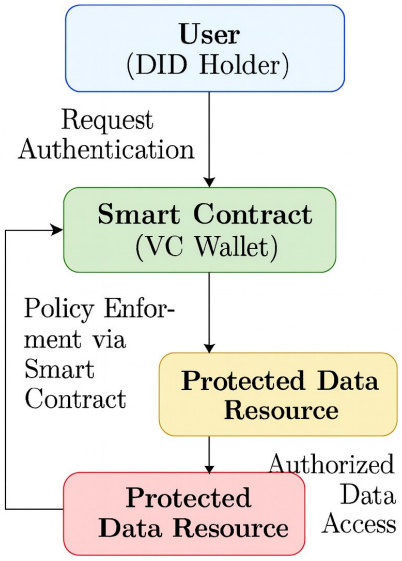

Figure 4: Workflow of DID-based identity authentication process in the energy data space.

Furthermore, smart contracts enable privacy-preserving mechanisms such as selective disclosure and zero-knowledge proofs. For example, a user can prove compliance with a condition (e.g., electricity consumption greater than 1000 kWh) without revealing the exact value. Such mechanisms protect sensitive information while still enabling regulatory verification. When users request access to energy data resources, the smart contract automatically verifies their digital identities and authorizations, executing the operation only if the conditions are met. This automated process enhances efficiency, reduces human-induced risks, and significantly improves both the security and trustworthiness of digital identity management in the energy data space.

III. Experiment and Analysis

III. A. Principles of Performance Testing Based on Simulation

In the cross-domain identity authentication scenario of the energy data space, the digital identity interaction process can be abstracted as a multi-stage stochastic process. A single authentication request consists of six key sub-processes: Decentralized Identifier (DID) resolution, Verifiable Credential (VC) / Verifiable Presentation (VP) verification, selective disclosure or Zero-Knowledge Proof (ZKP), smart contract policy evaluation, on-chain auditing, and network transmission.

The end-to-end latency can be expressed as:

$$T_{\text{total}} = T_{\text{did}} + T_{\text{vc}} + T_{\text{zk}} + T_{\text{eval}} + T_{\text{audit}} + T_{\text{net}}.$$

Specifically:

DID resolution T_{did} : querying the DID document from the blockchain ledger, modeled as a truncated normal distribution;

VC/VP verification T_{vc} : signature validation and revocation checking, modeled by a normal distribution;

Zero-Knowledge Proof (ZKP) T_{zk} : consisting of generation and verification,

$$T_{\text{zk}} = T_{\text{zk,gen}} + T_{\text{zk,verify}},$$

where $T_{\text{zk,gen}}$ depends on user-side computation and $T_{\text{zk,verify}}$ on on-chain or off-chain validation;

Policy evaluation T_{eval}: execution of access control rules via smart contracts;

On-chain auditing T_{audit}: determined by block time T_b, approximated by a uniform distribution

$$T_{\text{audit}} \sim U(0, T_b);$$

Network jitter T_{net}: transmission delay fluctuations, modeled as a truncated normal distribution.

Based on the above model, Monte Carlo simulation can be used to approximate the distribution of T_{total}, thereby obtaining performance metrics such as the 50th percentile (P50) and 95th percentile (P95) latency.

The approximate throughput, measured in Transactions Per Second (TPS), is estimated as

$$\text{TPS} \approx \frac{C}{\text{median}(T_{\text{total}})/1000},$$

where C denotes the number of concurrent requests.

This paper uses the Monte Carlo method to perform simulations. The input parameters follow realistic latency distributions for DID resolution, VC/VP verification, ZKP generation/verification, smart contract evaluation, and on-chain auditing, as implemented in the simulation code Algorithm1.

Algorithm **1**: Monte Carlo-based Identity Authentication Simulation

Require: Number of samples N, concurrency level C, block time T_b, distribution parameters of each sub-process

Ensure: Estimated P50, P95 latency, and throughput (TPS)

Step 1: Initialization:

Set $i \leftarrow 0$

Initialize an empty set of total latencies $\text{T} \leftarrow \varnothing$

Step 2: Sampling Loop

while $i < N$ **do**

Sample $T_{\text{did}}, T_{\text{vc}}, T_{\text{zk}}, T_{\text{eval}}, T_{\text{audit}}, T_{\text{net}}$ from their distributions

Compute total latency:

$T_{\text{total}}^{(i)} = T_{\text{did}} + T_{\text{vc}} + T_{\text{zk}} + T_{\text{eval}} + T_{\text{audit}} + T_{\text{net}}$

Append $T_{\text{total}}^{(i)}$ to T

$i \leftarrow i + 1$

end while

end for

Step 3: Post-Processing

Compute P50 and P95 of T

Estimate throughput:

$$\text{TPS} \approx \frac{C}{\text{median(T)}/1000}$$

return P50, P95, TPS

III. B. Simulation Performance

To evaluate the proposed DID--blockchain identity management framework, we conducted Monte Carlo-based simulations under different settings. The experiments compare two blockchain infrastructures (Fabric vs. Ethereum Virtual Machine (EVM)) and two disclosure mechanisms (plain attribute vs. ZKP).

III. B. 1) Latency Distribution

Figure 5 depicts the Cumulative Distribution Function (CDF) of end-to-end latency under a concurrency of $C = 600$. Fabric consistently exhibits lower P50 and P95 latencies than EVM, primarily due to its shorter block time (300~ms vs. 2000~ms). For example, the P95 latency on Fabric is nearly one-third of that observed on EVM, indicating better suitability for real-time energy data access. This result confirms that block time is the dominant factor affecting system responsiveness: the expected waiting time for on-chain confirmation is $T_b / 2$, which directly explains the latency gap. Therefore, permissioned

blockchains such as Fabric are preferable in latency-sensitive energy scenarios (e.g., load dispatching or frequency regulation), while EVM-compatible chains may be more appropriate when interoperability is prioritized.

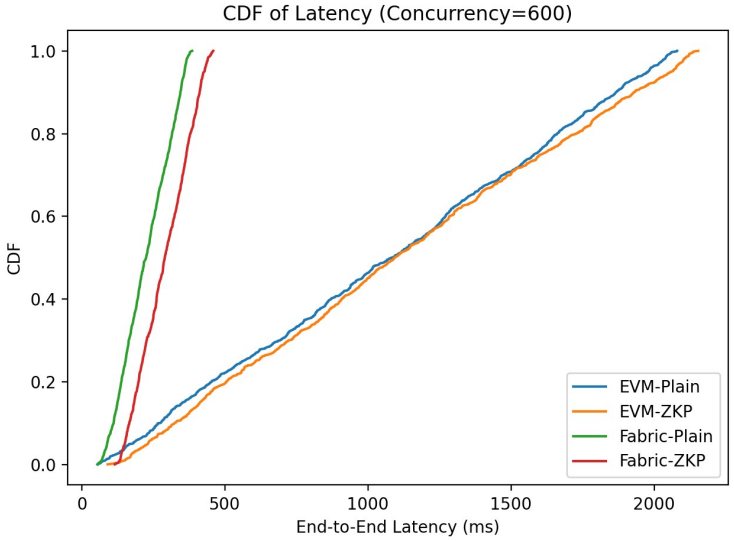

Figure 5: CDF of end-to-end latency at concurrency C = 600. Fabric shows lower median and tail latencies compared to EVM.

III. B. 2) Throughput Scalability

The throughput results are summarized in Figure 6. As concurrency increases, TPS initially scales linearly but gradually saturates due to block time bottlenecks. Fabric achieves higher TPS than EVM under the same concurrency. At $C=1000$, Fabric sustains nearly twice the throughput of EVM, demonstrating the efficiency of permissioned blockchain infrastructures. This trend reflects a general scalability limitation: throughput grows proportionally with concurrency in the low-load region, but once block generation becomes the bottleneck, additional requests only increase queuing delay without improving TPS. For energy systems, this highlights the need for adaptive rate-limiting and workload balancing to prevent cascading failures under peak demand.

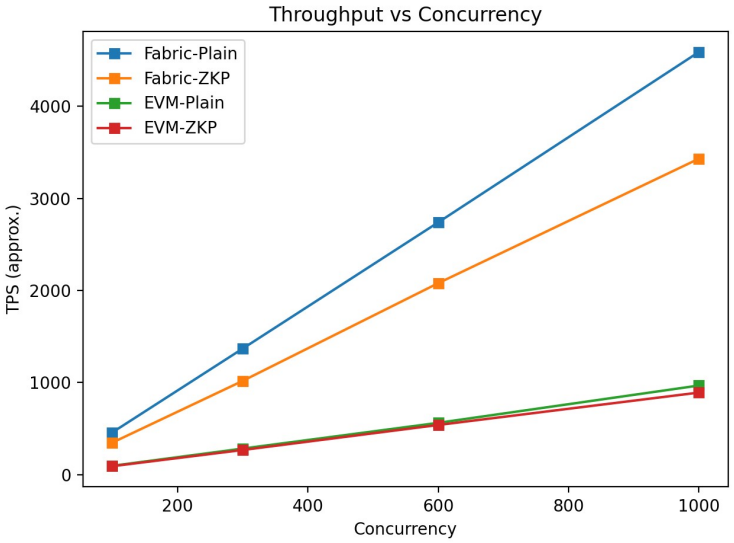

Figure 6: Throughput (TPS) under varying concurrency levels. Fabric achieves consistently higher throughput compared to EVM.

III. B. 3) Tail Latency Analysis

Figure 7 illustrates the P95 latency as concurrency increases. ZKP introduces an additional overhead of approximately 70--100~ms relative to plain disclosure. Nevertheless, this increase remains within acceptable bounds for energy sector applications, given the significant privacy benefits of selective disclosure. The relative impact of ZKP is platform-dependent: on Fabric, the overhead is visible since consensus delay is relatively small, while on EVM, where block confirmation dominates, ZKP accounts for less than 10\% of the total latency. zThis indicates that privacy-preserving verification can be integrated into identity workflows without critically harming responsiveness.

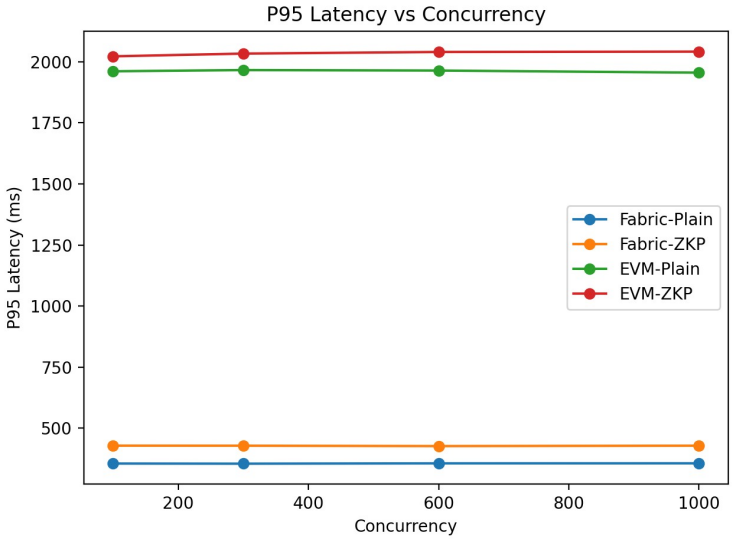

Figure 7: P95 latency under different concurrency levels. ZKP introduces moderate overhead compared with plain disclosure.

Table 1 summarizes key performance metrics. The results highlight a clear trade-off: plain disclosure achieves lower latency, while ZKP provides stronger privacy protection at a moderate cost in responsiveness. From a governance perspective, the DID+blockchain+smart contract framework simultaneously ensures security, auditability, and privacy-preservation. Plain disclosure may be used for low-sensitivity internal processes, while ZKP-based disclosure is more suitable for inter-organizational or public-facing applications to comply with privacy regulations such as the General Data Protection Regulation (GDPR) or the Personal Information Protection Law (PIPL). Although EVM-compatible chains suffer from higher latency, they offer broader ecosystem interoperability, which is valuable for cross-domain or cross-border identity scenarios. In contrast, Fabric's low latency makes it more suitable for operational scenarios requiring fast response. The proposed framework offers a unified approach that overcomes fragmentation, alleviates compliance challenges, and safeguards privacy in energy data circulation.

Table 1: Summary of Simulation Results

Platform	Disclosure	Concurrency	P95 (ms)	TPS
Fabric	Plain	600	≈ 450	1200
Fabric	ZKP	600	≈ 540	1100
EVM	Plain	600	≈ 1200	600
EVM	ZKP	600	≈ 1290	550

IV. Conclusion

This study introduces a decentralized digital identity (DID) management framework for the energy data space, integrating sovereign identity management, blockchain-based traceability, and smart-contract-enabled privacy protection. The framework effectively mitigates the limitations of conventional identity systems, including insufficient authentication, fragmented governance, and high compliance costs. Simulation results further highlight its practical advantages, showing that Hyperledger Fabric, as a permissioned blockchain, outperforms EVM-based infrastructures in terms of latency and throughput, thereby offering a more suitable foundation for latency-sensitive energy applications.Meanwhile, the integration of zero-knowledge proofs introduces moderate computational overhead but ensures selective disclosure and compliance with strict data protection regulations, thus providing strong privacy guarantees.

In summary, the DID+Blockchain+Smart Contract framework offers a secure, interoperable, and efficient solution for identity management in the energy sector. It establishes a distributed trust foundation for multi-party collaboration, supports fine-grained access control, and ensures transparent and tamper-resistant auditing. Future work will focus on enhancing interoperability with legacy systems, optimizing zero-knowledge proof performance, and validating the framework through real-world pilot deployments in provincial-level energy data platforms.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, author-ship, and/or publication of this article.

Data Sharing Agreement

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Funding

The work is sponsored by "Research on Core Technologies of Digital Identity Management for Jiangsu Province's Energy Industry Data Space (2025 State Grid Jiangsu Electric Power Co., Ltd., Information & Communication Branch 'Technology Project Package for the Production Frontline')".

References

[1] M. Mueller and K. Grindal (2019) Data flows and the digital economy: information as a mobile factor of production, Digit. Policy Regul. Governance, 21 (1): 71–87.
[2] B. Lin and Y. Xie (2023) Does digital transformation improve the operational efficiency of Chinese power enterprises?, Util. Policy, 82: 101542.
[3] Y. Zhao, S. Xia, J. Zhang, Y. Hu and M. Wu (2021) Effect of the digital transformation of power system on renewable energy utilization in China, IEEE Access, 9: 96201–96209.
[4] Y. Ye, Y. Tang, H. Wang, X. Zhang and G. Strbac (2021) A scalable privacy-preserving multi-agent deep reinforcement learning approach for large-scale peer-to-peer transactive energy trading, IEEE Trans. Smart Grid, 12 (6): 5185–5200.
[5] C. Lu, J. Cui, H. Wang, H. Yi and C. Wu (2023) Privacy preserving user energy consumption profiling: from theory to application, IEEE Trans. Smart Grid, 14 (4): 2628–2639.
[6] Y. Huang, X. Li, W. Deng and W. Xu (2025) Analyzing rural community growth and shrinkage: insights from household electricity data in Xinxing County, China, Appl. Spatial Anal, 18(2): 55.
[7] W. Zeng and M.-Y. Chow (2011) A trade-off model for performance and security in secured networked control systems, Proc. IEEE Int. Symp. Ind. Electron. (ISIE), 1997–2002.
[8] X.-H. Xia, G. T. Huang, G. Q. Chen, B. Zhang, Z. M. Chen and Q. Yang (2011) Energy security, efficiency and carbon emission of Chinese industry, Energy Policy, 39 (6): 3520–3528.
[9] F. Völter, N. Urbach and J. Padget (2021) Asset logging in the energy sector: a scalable blockchain-based data platform, Energy Inform., 4 (2): 1–20.
[10] G. Kormpakis, P. Kapsalis, K. Alexakis, Z. Mylona, S. Pelekis, K. Ntouros and D. Askounis (2023) Energy sector digitilisation: a security framework application for role-based access management, Proc. 14th International Conference on Information, Intelligence, Systems & Applications (IISA), 1–8. doi: 10.1109/IISA59645.2023.10345842.
[11] S. Sharda, V. Garikapati, T. Laclair, N. Viz, et al. (2024) From silos to synergy: identifying a roadmap for cross-sector research to accelerate the clean energy transition, Transp. Res. Part D: Transp. Environ. https://doi.org/10.2172/2480296
[12] E. Gebetsroither-Geringer, R. Stollnberger, V. Bürger and R.-R. Schmidt (2021) Inception of harmonising data silos and urban simulation tools using 3D city models for sustainable management of the urban food water and energy resources, Procedia Comput. Sci., 181: 123–130.
[13] Z. Li, X. Jin, X. Shi and J. Cao (2024) A meta-learning approach for predicting asphalt pavement deflection basin area, Complex Eng. Syst., 4: 26.
[14] Z. Li, J. Cao, H. Shi, X. Shi, T. Ma and W. Huang (2025) Roughness prediction of asphalt pavement using FGM(1,1–sin) model optimized by swarm intelligence and Markov chain, Neural Netw., 183: 107000.
[15] Z. Li, I. Korovin, X. Shi, S. Gorbachev, N. Gorbacheva, W. Huang and J. Cao (2023) A data-driven rutting depth short-time prediction model with metaheuristic optimization for asphalt pavements based on RIOHTrack, IEEE/CAA J. Autom. Sinica, 10 (10): 1918–1932.
[16] Z. Li, Y. Wang, J. Cao and C. Huang (2025) A hybrid prediction model for stock trend based on gated recurrent unit and wavelet transform, Appl. Intell., 55 (12): 1–25.
[17] Z. X. Li, X. L. Shi, J. D. Cao, X. D. Wang and W. Huang (2022) CPSO-XGBoost segmented regression model for asphalt pavement deflection basin area prediction, Sci. China Technol. Sci., 65 (7): 1470–1481.
[18] H. Bibi, M. Abolhasan, J. Lipman, M. Abdollahi and W. Ni (2025) A comprehensive survey on privacy-preserving technologies for smart grids, Comput. Electr. Eng, 124: 110371.
[19] M. Ali, S. Moharana, S. S. Ali and B. J. Choi (2025) Privacy-preserving machine learning for IoT-integrated smart grids: recent advances, opportunities, and challenges, Energies, 18(10):2515.
[20] L. A. Maglaras (2016) A survey on privacy-preserving schemes for smart grid communications, arXiv preprint, arXiv:1611.07722.
[21] V. Abreu, A. O. Santin, E. K. Viegas and V. V. Cogo (2020) Identity and access management for IoT in smart grid, International Conference on Advanced Information Networking and Applications, 1215-1226.
[22] P. Kumar, R. Tripathi and G. Gupta (2022) Blockchain-based trust management and authentication of devices in smart grid, Cleaner Eng. Technol., 6: 100481.

[23] Anonymous (2024) Review of data security within energy blockchain: a comprehensive analysis of storage, management, and utilization, High-Confidence Computing, 2024, 100233.
[24] A. Borkovcova, M. Černá and M. Sokolová (2022) Blockchain in the energy sector—systematic review, Sustainability, 14: 14793.
[25] M. Sporny, D. Longley, M. Sabadello, et al. (2022) Verifiable credentials data model v1.1, W3C Recommendation, available at: https://www.w3.org/TR/vc-data-model/.