scientific reports

OPEN

Multi blockchain architecture for judicial case management using smart contracts

Tahir Alyas[1], Qaiser Abbas[2], Sadia Niazi[3], Saad Said Alqahtany[2], Turki Alghamdi[2], Ali Alzahrani[2], Nadia Tabassum[4] & Aidarus Mohamed Ibrahim[5]✉

The infusion of technology across various domains, particularly in process-centric and multi-stakeholder sectors, demands transparency, accuracy, and scalability. This paper introduces a blockchain and intelligent contract-based framework for judicial case management, proposing a private-to-public blockchain approach to establish a transparent, decentralized, and robust system. An Integrated Solution for Judicial Case Management using Blockchain Technology and Smart Contracts. This paper aims to introduce a multi-blockchain structure for managing judicial cases based on smart contracts, ultimately rendering cases more transparent, distributed, and tenacious. This solution is innovative because it will leverage both private and public blockchains to satisfy the unique requirements of judicial processes, with transparent public access for authorized digital events and transactions occurring on the freely available blockchain and a three-tiered private blockchain structure to address private stakeholder interactions while ensuring that operational consistency, security, and data privacy requirements are met. Leveraging the decentralized and tamper-proof approach of blockchain and cloud computing, the framework aims to increase data security and cut down on administrative burdens. This framework offers a scalable and secure solution for modernizing judicial systems, supporting smart governance's shift towards digital transparency and accountability.

Keywords Multi-blockchain architecture, Judicial case management, Smart contracts, Blockchain technology, Decentralization, Data privacy

Traditional storage systems for digital evidence systems cannot be tamper-proofed, controlled centrally, and do not provide transparency, leading to trust issues. Although current systems strive to secure electronic records, they lack the transparency and decentralization needed for trustworthy evidence preservation. Immutability and decentralization are the features that make the blockchain technology a good candidate to overcome these limitations and allow the credible, public and distributed mediation of judicial evidence[1]. New blockchain-based storage methods have proven effective in areas such as smart governance, smart homes, and healthcare. This approach aids secure, scalable, and tamper-resistant sharing of data such as cloud storage and edge computing assisted by blockchain, which makes this including a good candidate for data privacy-preserving practices in judicial systems[2].

Blockchain-oriented judicial evidence-preserving methods can utilize the immutability of the blockchain itself and combine IPFS (InterPlanetary File System) for decentralized storage. By using IPFS to facilitate off-chain storage, IPFS can solve the problem of block-size limitation and transaction speed[3]. At the same time, smart contracts in the system can automate judicial processes including case registration, authority management, evidence upload and download, data sharing, and regulatory verification[4]. We show by simulation that this approach can outperform existing systems significantly in terms of throughput and stability. Performance tests also validate its ability to meet judicial organizations' needs for timely data access and collaboration[5].

This framework utilizes a combination of blockchain and IPFS to store the proof in tamper-proof packets even with limited block capacity. It achieves cost savings and flexibility, responding to the judicial system's need for a secure, scalable, and efficient manner of managing evidence[6]. Smart contracts can also help automate tasks that are primarily repetitive in nature, which may include scheduling hearings, sending notifications/generating

[1]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan. [2]Faculty of Computer and Information Systems, Islamic University of Madinah, 42351 Madinah, Saudi Arabia. [3]Department of Psychology, University of Sargodha, Sargodha, Pakistan. [4]Department of Computer Science, Virtual University of Pakistan, Islamabad, Pakistan. [5]College of Computing and IT, University of Hargeisa, Hargeisa, Somalia. ✉email: aidarusibrahim11@gmail.com

defaults, tracking document submissions, and monitoring case progress. Using AI minimizes human error even further, increases administrative efficiency and expedites case resolution, thereby improving the effectiveness of the judicial system[7].

Solutions for judicial case management based on single-blockchain systems have limitations. As a result, it facilitates secure, transparent, and automated judicial processes by utilizing smart contracts to enforce legal agreements, manage ongoing cases, and ensure compliance with regulations. A three-level private blockchain system is also used to manage role-based access control to keep an indelible and publicly verifiable record of judicial actions within the framework[8]. The evidence is stored off-chain on IPFS, which helps in reducing the need of having evidence inside blockchain network itself, thus resulting in a better efficiency of evidence handling without stressing out the blockchain network[9,10].

This research is a major step forward in the evolution of judicial governance — a scalable, secure and transparent solution designed to meet the needs of different judicial systems. Its goal is to strengthen public confidence in the judicial process by developing a multi-blockchain infrastructure that can address the limitations of single blockchain system. Smart contracts reduce human involvement, minimize errors, and facilitate case management, making the judicial system more efficient and credible[11,12]. This framework's success at establishing secure, transparent, and automated judicial processes lays the groundwork for future advancements in blockchain-based legal and governance technologies[13].

To summarize, the research emphasizes that blockchain technology can fundamentally address the issues of evidence handling, transparency, and efficiency in judicial routines. The integration of blockchain, IPFS, and smart contracts proposed in the framework establishes a new paradigm for secure and scalable judicial case management and is aligned with the principles of smart governance and digital accountability[14,15].

Literature review

Luo et al. Integrating cognitive backscatter communications with a novel approach to blockchain consensus in wireless networks. This blockchain consensus is symbiotic and allows low-power devices to participate in blockchain networks, increasing the energy efficiency of the blockchain while boosting data throughput. With cognitive radio, the proposed model can efficiently utilize the spectrum to guarantee high data transmission reliability without sacrificing blockchain's decentralised integrity. Their simulations show increased throughput and reduced delay, making it suitable for energy-constrained wireless environments such as IoT networks[16].

Gong et al. We propose a blockchain-assisted digital twin offloading scheme in the intricate space-air-ground networks (SAGNs). Data management is crucial for digital twins—virtual representations of a physical system—especially in heterogeneous environments such as SAGNs. Authors use blockchain technology to coordinate offloading digital twin tasks from the digital twin to the most efficient edge node while ensuring secured and trustworthy data sharing. Blockchain technology is typically open-source, making its code publicly accessible, and such source code brings transparency to the underlying system. The results show lower latency, better resource utilization, and resilience against network failures[17].

Yang et al. examine how you can leverage blockchain to improve multitask learning (MTL) to optimize private car commuter travel. The authors propose a decentralized system where user-generated data (e.g., traffic patterns, road conditions) is securely shared and utilized by MTL models to optimize the suggestions for routes to the users. Data Security and Trust in Collaborative Environment Through Blockchain Smart Contracts Results from experiments show that this blockchain-based MTL system can effectively improve commute efficiency, shorten travel time, and ensure user data privacy[18].

In the medical industry, blockchain solutions are widely adopted to manage sensitive medical data securely. Blockchain has systems for verification and validation, allowing transactions to be tracked while still ensuring accessibility and privacy for practitioners and patients. Smart contracts provide an advantage here by automatically sharing data among competing hospitals and other medical entities, minimising administrative costs and improving data integrity[19]. Nonetheless, soaring processing costs and delayed performance due to a low mining capacity pose major challenges to mass acceptance. These constraints highlight the necessity for more efficient blockchain solutions that find a sweet spot between security and performance[20].

In[21], Liu and Zhao organized a vehicular data sensing framework with the aid of blockchain, focusing on information fresh, an important factor for real-time decision of Intelligent Transportation Systems (ITS). They build on the Age of Information (AoI), a well-known metric for the freshness of data, proposing a scheme that benefits from blockchain for the secure and real-time sharing of sensing data between vehicles. Smart contracts automate the data validation process and embed reward mechanisms in order to encourage vehicles to share timely and updated routing information. This framework provides real-time updates on traffic and navigation that greatly supports road safety efforts.

The present work reveals the transformative power of blockchain technology in introducing Triple-Entry Accounting (TEA), which is revolutionising the traditional accounting system. Blockchain is a decentralised, immutable, and transparent ledger that provides secure, shared, and validated transaction records among interested parties that do not require reconciliation, significantly reducing the risk of fraud. Smart contracts enable efficient, automated accounting by integrating invoicing and payments into the data stream on a blockchain, and facilitate real-time data auditing for compliance and transparency. However, in accounting and finance, scalability, energy consumption, and regulatory uncertainty are all challenges that need to be faced before the promise of blockchain can be fully realized. Adding blockchain and TEA are major strides towards creating more secure, efficient, and transparent financial systems[22].

Zheng et al. propose a multi-agent reinforcement learning (MARL) framework enhanced with blockchain for peer-to-peer (P2P) energy trading. The system uses a continuous double auction (CDA) model to enable secure and private energy trading between energy prosumers (producers-consumers). This comprises transparent transaction recording via a blockchain and privacy-preserving methods such as differential privacy to protect sensitive bidding data. The MARL paradigm finds optimal trading strategies which enhance market equilibrium and user satisfaction. This serves as a mechanism to realise decentralised, effective and privacy-centric electrical power marketplaces[23].

Originally a technology for cryptocurrency, blockchain can now be tailored to immutability and confidentiality in domains other than cryptocurrency, including Accounting Information Systems (AIS). Our research proposal combines areas of ERP and blockchain to implement data vaults and generate tamper-proof financial data by using hash algorithms such as SHA256. Blockchain replaces existing databases but works along with RDBMS to fulfill the requirements of low-cost secured solutions. The proposed framework improves data integrity, identifies breaches, and provides a scalable enterprise solution[24].

Hybrid blockchain models are extensively employed to mitigate latency and reduce resource consumption by integrating public/permissioned and private/restricted systems. These models first enhance fault tolerance and allow for secure data sharing with privacy protection, which are vital to building judicial systems[25] or other similar applications requiring high data integrity and prompt access to data. BIoMT: Integrating blockchain and the Internet of Medical Things has shown great promise in managing complex, multi-party data management needs. Using blockchain technology, BIoMT builds a fascinating serverless peer-to-peer network for healthcare data with transparent, integrated utility while preserving the privateness of knowledge contained inside. Blockchain and IoMT are two emerging technologies that can completely transform healthcare organisations' management and sharing of sensitive patient data while addressing specific critical pain points such as data security, privacy, and interoperability. Also, the design can be further extended and applied to monitor a large population suffering from chronic diseases in distributed and centralized cities where an enormous amount of medical data is generated through e-health services. BIoMT can transform healthcare delivery and patient outcomes by integrating blockchain technology with edge computing. For instance, Zhang et al. proposed a hybrid blockchain architecture that integrates public and private blockchain to preserve data integrity and confidentiality in IIoT networks. Implementing smart contracts provides additional access control and auditing, thereby reducing the potential for unauthorized access and tampering with data. Because of that, this hybrid scheme has become a promising solution combining security with scalability[26].

Similarly, Liu et al. proposed a small blockchain framework for IIoT devices with low computational capability. Their solution leverages the energy-efficient and secure Proof of Authority (PoA) consensus mechanism. Much of the work reported on in the study represents considerable advances of state of the art with respect to data storage efficiency and scalability, which is important for their deployment in large-scale IIoT installations in resource-constrained environments[27].

The Role of External Proof of Retrievability in Distributed Storage Systems. Fang et al. designed a Proof-of-Retrievability (PoR)-based protocol that guaranteed secure storage for medical data in the metaverse world. Their protocol is based on homomorphic encryption that allows third-party auditors to check data integrity without accessing the data, which preserves patient privacy[28]. Extending this, Vaninr et al. proposed a end-to-end data protection model for personal health records sharing system. They provide a solution that allows for seamless verification of medical data while adhering to regulatory norms like HIPAA and GDPR[29].

Additionally, vector commitment schemes have been proposed to allow secure and space-efficient shared data access. Zhang et al. introduced an integration model for medical healthcare and metaverse. This approach enables users to commit to a collection of data items while still proving that they know the integrity of selected items within each set without disclosing the whole set. In metaverse applications, specific sharing of medical data with healthcare providers or virtual reality platforms is critical[30]; this is another area where these conditions are invaluable. Together, these developments reflect the transformative potential of blockchain, edge computing and cryptographic methods for improving data security, efficiency and privacy in relation to healthcare and IoT materials.

Proposed methodology

Blockchain, IoT, and cloud computing are the technologies that are becoming the transformation platform to formulate the emerging digital ecosystem with decentralized, highly shareable, and secure applications in various professional domains[31]. Smart governance, or e-government, is a global research and development area. The provision of different public-serving applications is one of the crucial areas of service in the e-governance system. The judicial system is one of the important pillars to be considered for technology transformation for a swift and transparent justice system.

It is divided into three main modules i.e. actors, process, and execution, as shown in Fig. 1. In the Process section, the four icons collectively illustrate key functions of the smart contract framework within the blockchain-based judicial case management system. In Fig. 1 shows the multi-blockchain architecture of judicial case management using the smart contract. The proposed architecture is organized into three main components: actors, process, and execution, linked by blockchain consensus mechanisms to guarantee transparency, security, and data integrity on judicial procedures. The first segment—"Actors"—features major players in the judicial process, from the jury and prosecution to the defense. These actors can interact with the system through a consensus mechanism that records their actions and input and allows authorization and validation of their inputs. Data is trained through a decentralized system that builds trust by default and reduces potential biases or manipulation in the judiciary regime.

The second component, Process, pertains to smart contracts, which we consider to be the operational backbone of the system. These smart contracts ensure legal processes are executed accurately and efficiently by automating key judicial workflows, governing the handling of documents, and automatically enforcing access controls. The system uses blockchain technology to ensure encrypted and transparent management of case

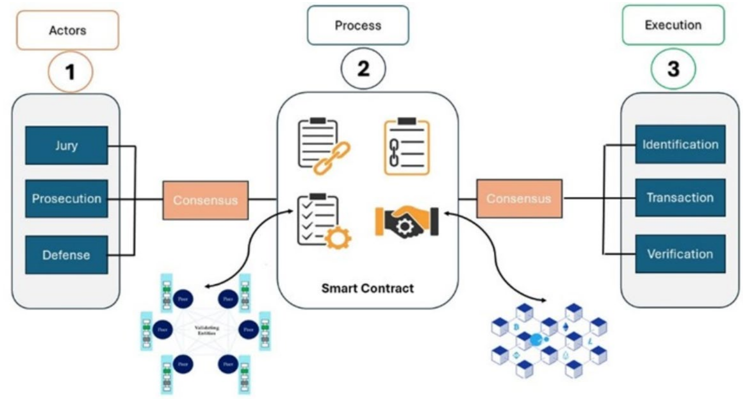

Fig. 1. System diagram.

files, evidence submissions and procedural steps. Actors communicate with this process component to send messages and actions, enabling actor-execution stage integration and coordination.

The last step, execution, is about implementing judicial decisions into reality. Typically, the court system works linearly—identification, transaction and verification—to ensure that rulings and legal obligations are executed correctly and transparently. During the execution phase, a different consensus mechanism is used to validate and record those actions on the blockchain. The architecture uses permissioned blockchains for sensitive data, public or consortium blockchains for public accountability, and inter-blockchain communication for system component interaction.

This multi-blockchain architecture improves judicial case management to bring a secure, transparent, and efficient framework. Complex legal workflows can be automated, limitations on manual errors, and all these in compliance with legal standards thanks to smart contracts. At the same time, the decentralized nature of blockchain technology ensures data integrity, and builds trust between all judicial stakeholders.

In this methodology, a blockchain-based Judicial case management system is described using a chain-of-blocks architecture that is interfaced with different judicial roles, such as jury, prosecution, defence, etc. to enhance automation, transparency and integrity via smart contracts. This multi-stage system works in this way:

1. *Jury module*: This first module compiles central case components, such as evidence, schedules, witness information, parole and financial data. That initial step of providing personal data serves as the entry point to the blockchain for the case, causing every aspect of the case to be recorded on the chain securely for verification.
2. *Prosecution module*: This module contains only the digital information collected and processed from the evidence, along with forensic details (e.g. actor motives, causative trees, and evidence referrals). It features functionalities for managing and authenticating all items associated with prosecution, utilizing the evidence and information gathered in the previous module.
3. *Defense module*: Evidence mapping, action analysis, motive semantics, and alibi trees, structured and ordered, in an object-oriented defense module. This module organizes featured imagery to enable defense preparation, analysis, and review.
4. *Blockchain consensus approach*: The consensus phase refers to the consensus mechanism used to reach an agreement between all participants before transactions are recorded on the blockchain. This stage involves evaluation records of arguments and can activate smart contracts — coded terms of action that execute when certain conditions have been met, thus ensuring a decentralized and verifiably transparent process for the course of the case. In this phase of the notary public life cycle, involved legal professionals (lawyers and judiciary, for example) are to be verified. Litigation relies on smart contracts to form argument trees, relational clauses, and reference structures to wed the legal construct into the reified blockchain, which is robust enough to facilitate sound argumentation and anchoring references.
5. *Proof-of-work (PoW) mechanism*: This step includes penalty voting, prediction ranking, and judiciary sorting to provide higher security and guarantee. Here, legal scholars weigh the evidence against precedents, speculate on possible outcomes and rank those odds. Blockchain uses a PoW method to secure the judgments by encoding verifiable decisions and possible deterrent actions to ensure consistency of similar cases.
6. *Legal taxonomy development*: The legal concepts from the previous step are categorized into a taxonomy, building the legal framework of what laws, principles, and classifications are relevant to the case. Such classification has been instrumental in systematically articulating legal claims and in judicial pronouncing.
7. *Impact analysis and financial review*: Upon completing the PoW phase, impact analysis measures potential legal and financial impacts, exploring alternative scenarios and assessing the economic consequences of each verdict. Lawyers calculate the damage, attorney fees, and potential settlements for different results, guiding the strategy.
8. *Artificial neural network (ANN)*: Knowledge BaseThis last step uses ANN to create a knowledge base, to maintain and update a knowledge base that may contain legal precedents, doctrine, and cases, providing a holistic repository of legal knowledge which grows and incorporates new-found case data to allow further learning.

The above methodology facilitates judicial case management by applying a decentralised, trustless, secure blockchain system generating an immutable sign for the input data at each stage thus increasing transparency, assisting in decision-making and improving efficiency (structured, unified data flows at each stage). Every building block now has step-by-step explanations, starting from the modules' usability in the judicial case management system. It also added an extensive discussion justifying the selected consensus mechanisms (PoW and PoS), explaining how their trade-off between security and efficiency brought them ahead of other alternatives in the current appropriate judicial context. Providing this further detail will add transparency to the process and a clear justification to the technical decisions taken for the study.

This architecture presents a master blockchain with smart contracts and three alternate blockchains: Alt #Jur, Alt#Pro, and Alt#Def for jury, prosecution, and defense. The actors can be added with relevant entities; the actors, pre-validity, and process are more focused on developing a stakeholder network with optimal entities and security. The initial requests by the actors are evaluated at the pre-validation checkpoint. In the event of consensus by all the stakeholders, the entities are either permitted to perform or the transaction request is rejected. The initial smart contract registration is complete, with three alternate blockchains providing basic data related to the case. It has been arranged so that all the entities are supportive and non-redundant. As visible in Fig. 2, the Alt#Jur layer comprises holistic parameters, e.g., pre-trial, schedule, financials, evidence, witnesses, parole, and codification. All the other stakeholders related to the same case require these parameters. The Alt#Pro or prosecution layer has case actors, digital evidence, a motive tree, forensics, legal clauses, and referral cases to be considered by the stakeholders of any layer. The Alt#Def or defence layer accumulates the parameters and formulates a more comprehensive schema for the use of artificial intelligence and analytics. This layer contains the action map, evidence analogy, motive semantics, and alibi tree. Notably, transforming unit data into a more structured manner will define the new dimensions and become more productive in the next phase.

The Blockchain consensus management has been done at two levels: the alternate blockchains use the proof-of-work (PoW) algorithm to develop the consensus state among stakeholders, while the main master blockchain uses the proof-of-stake (PoS) algorithm to assemble the PoW status from all alternate blockchains. Other algorithms include delegated proof of stake (DPoS) and practical byzantine fault tolerance (pBFT). All have different advantages and disadvantages, and there are multiple hybrid versions as well. Considering the emerging trends in the blockchain domain, it is highly anticipated to have more robust and scalable algorithms shortly.

This paper is focused on decentralized, secured, transparent, and scalable distribution; therefore, our analysis showed the suitability of proof-of-work (PoW) and proof-of-stake (PoS) algorithms. The summary of the advantages and disadvantages of all four algorithms is given in Table 1:

Other hybrid combinations of algorithms are possible, but in our experimentation, we have observed that PoW and PoS are the most suitable combinations if decentralization is the priority, while for a smaller scale, pBFT can be a good combination with PoW. The hybrid algorithms are providing a new direction for smart contracts by enhancing their scalability and transparency per the sub-chains' needs. The other "branded" hybrid algorithms are Zilliqa, Aelf, Aeternity, and Bytom; all these consensus algorithms are also easy to engage and provide various outcomes depending on the nature of the blockchain. Proof of Work (PoW) has advantages like the simplicity of implementation and the flexible entry of nodes without any cumbersome operations, resulting in a high degree of decentralization with extreme security. Similarly, PoW can establish machine trust without requiring human intervention to finalize the block producers. The downside of PoW is the processing cost and time. Due to the decentralization, the confirmation time for each block is tangibly high, resulting in the need for high-end resource engagement for a more extended period. Although expansion within the scope of blockchain is possible, intra-expansion needs more time and energy. PoS (proof of stake) is the other algorithm we propose

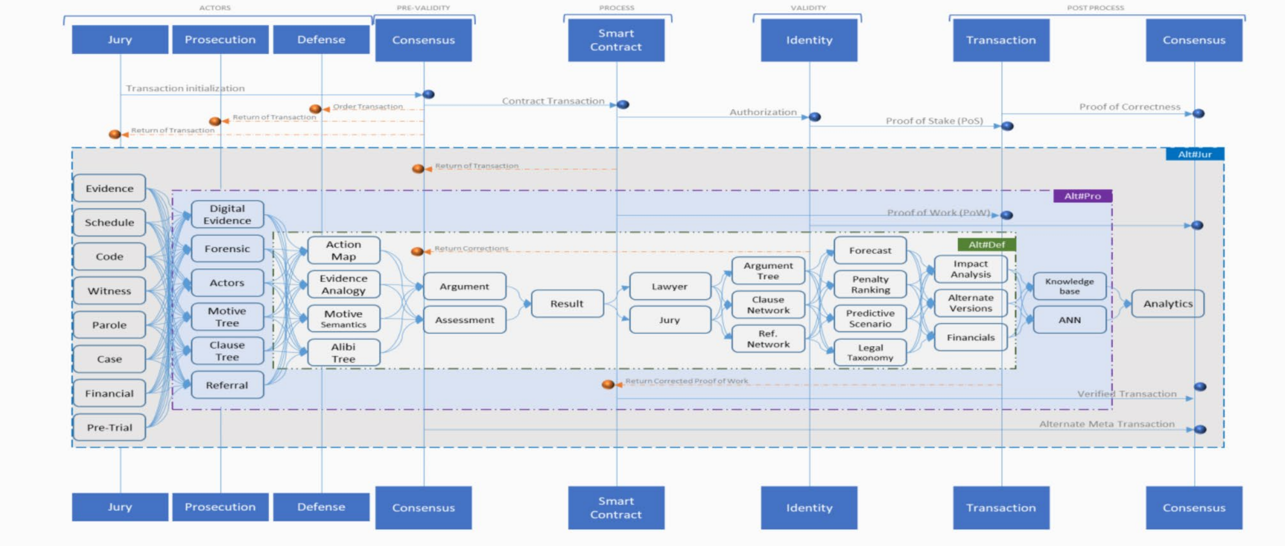

Fig. 2. Proposed architecture for judicial case management system.

#	Algorithm	Pros	Cons
1.	pBFT	Secure Robust Performance Finality	Loose decentralization Weak Fault Tolerance Close node scheme
2.	DPoS	Robust Performance Finality Resource Utilization	Loose decentralization Close node scheme
3.	PoS	Decentralization Open Node Scheme Resource Utilization	Low Security Implementation Complexity
4.	PoW	Open Node Scheme High Security Decentralization	Low Resource Utilization Low Performance Complex Scalability

Table 1. Pros & cons of consensus algorithms.

Hash value	9145c1da8105fd1c2b949573a9943bfc9944becb
OS	Ubuntu 18.04.6
RAM	DDR4 2Rx8 16GBx2
Processor	Intel Xeon 3.8 GHz
HDD	540GB SSD
CPUs	8
CORES	4

Table 2. Set up details.

to engage in the architecture. The best part of PoS is the optimal utilization of resources at minimal energy consumption. Block correctness is swift and accurate.

Further examination must be performed to provide arguments for the choice of (PoW) and (PoS) as consensus mechanisms in this blockchain-based judicial case management system. Although PoW delivers strong security by computationally verifying ledger history, which serves well for the immutability of judicial records, its resource consumption could restrict system efficiency in high-volume legal contexts. Unlike PoW, PoS presents an energy-efficient solution that drives faster processing of transactions, which will help to alleviate the latency often seen within case management. On the other hand, it may include alternative consensus mechanisms that provide better scaling and speed without losing security, e.g., delegated proof of stake (DPoS) and practical byzantine fault tolerance (PBFT). Matching PoW, PoS, and hybrid methods against the unique needs of judicial systems, for data integrity, low latency, high scalability, and fairness of resource utilization, would also ensure that the mechanisms used are the right fit for both the system's computing requirements and legal sector's specific requirements for secure validation for processing by the judicial system.

The experimental architecture based from the blockchain is run on a hyperledger fabric mentioned, with the parameters listed in Table 2. The proposed blockchain (beta) versus the conventional blockchain This paper employs HyperLedger Fabric, an established blockchain framework solution for enterprise implementations, to apply the suggested multi-blockchain architecture in judicial case management. This study employs a stable release HyperLedger Fabric 1.4. HyperLedger Fabric is a stable release system with a plug-and-play architecture that readily meets requirements for a judicial case management system through its modular architecture's high level of security. It defines the essential tools and frameworks for managing parallel blockchain networks or multiple judicial roles and interactions within the same network securely and efficiently.

An architecture with four primary blockchains: one Meta blockchain (#Meta) and three alternate blockchains: Alt#Jur for jury management, Alt#Pro for prosecution, and Alt#Def for defense. Each blockchain serves distinct jury, prosecution, and defense purposes in the multi-blockchain system. They are separate enough that each organization can manage its own data and set of transactions according to its scope of responsibility. However, they are still interconnected to ensure seamless information flow and consensus. The training began with establishing an organizational node—the primary judicial role—that assigns nodes to the primary actors in a judicial trial (e.g., prosecutors, defense attorneys, jury). The nodes communicate with each other via smart contracts, ensuring secure and transparent dealings between all parties involved at different stages of the judicial process.

This system run Ubuntu 18.04.6 OS and with good technical specifications to manage the processing load from transactions and consensus of the blockchain. Hardware- 16GB DDR4 RAM, Intel Xeon 3.8 GHz processor, 540GB SSD (for quick data access and retrieval) Each node is supported by 8 CPUs (4 core each), allowing transactions to be processed and load balanced across the nodes. This setup provides the capability of the architecture to sustain computational intensity caused by consensus algorithms while providing the optimal performance of metrics such as latency, throughput, and resource usage.

We evaluated the proposed architecture on three metrics: latency and throughput, resource utilization (processor and memory) and intra-blockchain and inter-blockchain performance. As illustrated in the proposed architecture, each of the three and the Meta blockchains are used to pull and push transactions from the three alternate blockchains, Alt#Jur, Alt#Pro and Alt#Def. These tests are tested against proof-of-work (PoW), proof-of-stack (PoS), and hybrid algorithms to analyse the consensus mechanism. However, it is worth noting that a multi-layer approach of using PoW as the algorithm for layer 2 blockchains and PoS as that for layer 1 (meta) blockchains should work reasonably well, while PoDS and pBFT should be verified in much more dynamic scene. So, the main aim of the hybrid way is to study the influence of data traffic and volume on any Blockchain's performance. The block size is increased from 8 K to 64 K for latency and throughput measurements and related to the minimum requirements. While alpha means "+ without a hybrid", beta means "+ with a hybrid" in the results.

This information includes case records and documents, evidence files, and transaction files shared between court actors, such as jury members, the prosecutor and the defense attorney. This information plays a key role in ensuring the integrity and transparency of the judicial proceedings in a multi-blockchain architecture. For example: large files such as a PDF of evidence or legal documents cannot be directly stored on the blockchain due to size and efficiency. Instead, the system utilizes a decentralized storage, which sore large documents off-chain but securely. The InterPlanetary File System (IPFS) handles off-chain data storage. By storing files as unique cryptographic hashes on the blockchain, the IPFS allows faster access and verification of the files without taking up too much space on the blockchain itself. By linking even large files to blockchain transactions, this approach both allows the system to scale while maintaining its integrity for judicial case management. The architecture proposed in this article recommends securely storing large evidence files outside the blockchain layer using InterPlanetary File System (IPFS). As a result, sensitive judicial records such as digital evidence and evidential case files will become immutable and easily accessible. Moreover, IPFS accumulates the evidence and sends the hash to the PoI (Proof of Impartiality). Reference: A hash of the documents in the blockchain. Smart contracts manage access to evidence, preventing unauthorized retrieval and ensuring instant access for parties with the relevant rights. Case lifecycles, from registration to resolution, are automated via smart contracts. Initial data for a case is received, validated using smart contracts, and linked with the relevant blockchain. The work of workflows guarantees that a course of action is taken to verify and approve any evidence uploaded by authorized individuals. Automated notifications to stakeholders regarding the change in the status of a case or an upcoming deadline saves a significant amount of manual effort and reduces delays.

For the current research study, a hybrid consensus mechanism that includes both Proof-of-Work (PoW) and Proof-of-Stake (PoS) was selected to decrease the unnecessary overhead of mining, positively impacting security and efficiency in managing judicial cases. Avalanche integrates May's Proof of Work (PoW) functionality to provide such strong security, with sufficient computational expense to modify any blockchain, making it suitable for preserving the integrity of sensitive judicial records. In contrast, PoS innovations enable energy-efficient, near-instantaneous transaction processing, matching the demands of low-latency case management workflows.

Other consensus mechanisms were also evaluated but found less applicable in this case. Working under the assumption that best practice consensus protocols like Practical Byzantine Fault Tolerance (PBFT) are low-latency and finality, they can offer solutions in more constrained environments, they do not scale well in distributed systems with large numbers of stakeholders, for example in judicial ecosystems. On the other hand, DPOS achieves high throughput, however, because only a small number of validators must be decided, it raises the question of centralization of the system where only a few nodes control everything.

The design of a multi-blockchain architecture for judicial case management is a model of efficient judicial case management that halves the time taken for communication and case management processes. Various consensus management strategies are employed to ensure data consistency as well as data security across these chains. All temporary transactions between the private and the public chain are protected by cryptographic methods, such as hash functions and digital signatures, and are consequently tamperproof and verifiable. On the private chain, access control is ensured by Role Based Access Control (RBAC), which limits sensitive information to authorized users of the private chain, and interactions with the public chain are controlled via secure APIs, which expose only allowable information. Two-phase commit protocol is used for synchronization between chains, ensuring that to maintain data integrity during concurrent operations, transactions are either atomically validated and committed or discarded. Instead, a smart contract framework handles data transfer across chains, security enforcement, and reconciliation, such as validating the evidence attached to the private chain to match the original record on the public chain.

Smart contracts design and implementation is at the center of the architecture. These contracts focus on different jobs to achieve high transaction volume and valid data across the lifecycle of a case, from the first filing to the last verdict. RBAC logic is embedded into the smart contracts to only allow access of their functions to pre-defined stakeholders (Judges, lawyers, jurors etc.). In an event-driven architecture, these contracts are used to trigger events in certain scenarios such as submission of evidence or change in state of a case, which can then be used for public real-time notifications or integrations with other systems.

As for implementation, the system creates cases by registering them through a smart contract that creates a unique case ID and connects it with metadata about the involved parties and the initial hearing date. For evidence validation, the evidence files are hashed and stored on a private chain through the InterPlanetary File System (IPFS), and the corresponding hashes are recorded in smart contracts for traceability. Smart contracts simplify the dispute elimination, clause submissions by both parties involved, and arbitration decision recording.

Additionally, the architecture implements comprehensive validation checks across all smart contracts to ensure that the data remains intact and prevents unauthorized executions. Immutable logs allow an auditable trail of all actions executed through smart contracts that are saved on the blockchain forever. In addition, smart contracts are also integrated with APIs to public and private chains, so any data flows smoothly across the entire process. A multi-blockchain architecture automated using smart contracts provides a secure, transparent, and efficient solution abord the judicial case management system.

	Beta		Alpha	
Size (bytes)	Latency	Throughput (TPS)	Latency	Throughput (TPS)
8 K	0.12	518	0.19	490.2
16 K	0.17	388.5	0.22	401
32 K	0.28	281.4	0.29	303.3
64 K	0.66	190.9	0.68	202.5
128 K	0.74	296	0.70	210

Table 3. Latency and throughput analysis.

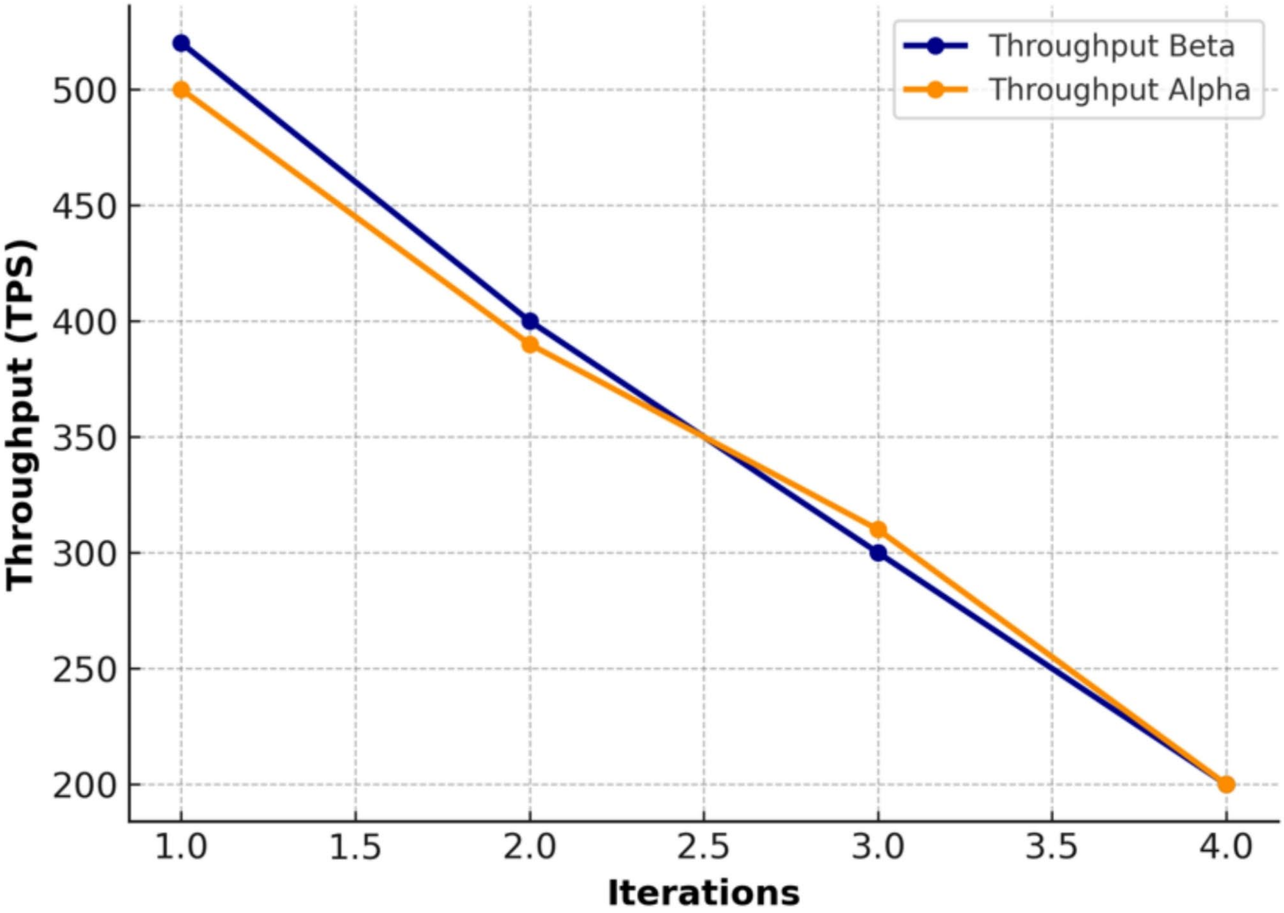

Fig. 3. Throughput analysis alpha versus beta.

Results and discussion

The latency analysis is performed on the proposed architecture using consensus algorithms (Alpha) and hybrid algorithms (Beta), with a block size ranging from 8 K to 64 K, as shown in Table 3.

The results for latency analysis show the superior performance of the beta version, i.e., hybrid consensus algorithm, on alternate and Meta blockchains. In contrast, the alpha results are competitive with low data sizes, but as the data sizes increase, the performance of the alpha version decreases. With blockchain in a conventional format and consensus algorithm (PoW, PoS, DPoS), the latency results are almost the same if the data size increases. While the same scenario is experimented with using hybrid consensus algorithms, i.e., PoW and PoS, the results are significantly improved with the increasing data size. The same thing has been observed regarding throughput, as illustrated in Fig. 3. The alpha throughput provides good results for lower data volumes but performs less as the data size increases.

The beta throughput shows an improving tendency with the increment in the data volume, as shown in Fig. 3. Due to the system's complexity, latency and throughput are essential in the case of multiple blockchains. A single or conventional blockchain may provide good results with better hardware parameters and other resources, but in the case of alternate and Meta blockchains, the system's architecture and design are vital to be considered for better performance and accuracy. The Fig. 4. shows the latency performance of the models Alpha and

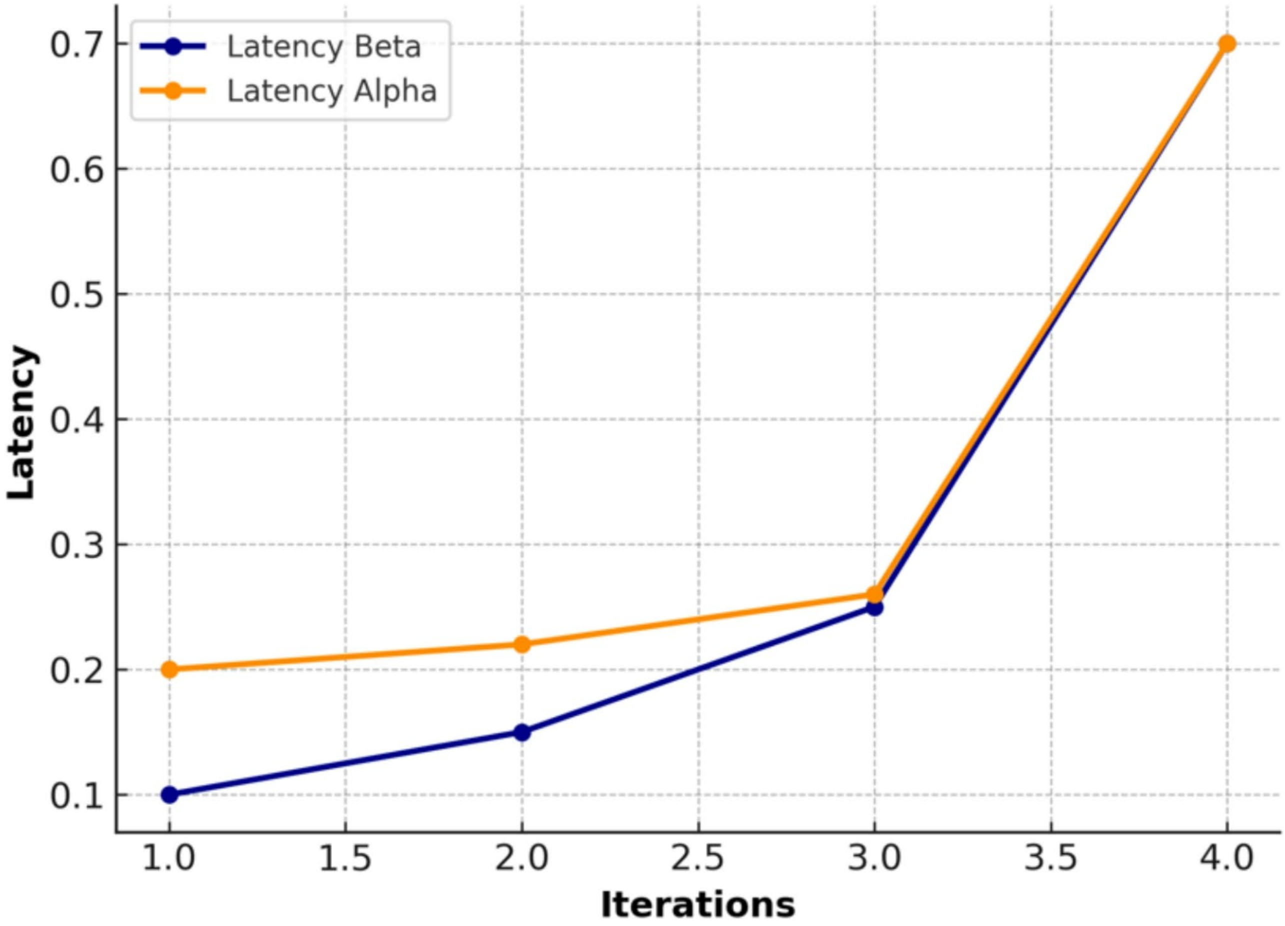

Fig. 4. Latency analysis alpha versus beta.

Beta across four iterations. Latency Alpha Shifts up initially but then increases linearly over the same period in contrast to the Latency Beta which starts even lower but takes a sharper upward turn, lovingly, both of the models converge into the highest latency on the fourth iteration.

Resource utilization is also one benchmark used to evaluate the performance of any blockchain, as from hash initialization to mining, blockchain is a resource-heavy activity.

In our proposed architecture, the processes are split into four categories, i.e., Alt#Jur, Alt#Pro, Alt#Def, and #Meta blockchains, but the interplay among these blockchains needs to be evaluated, specifically the utilization of memory and processor, which are of critical importance as shown in Fig. 5.

The radar chart in Fig. 6. compares the performance of the Alpha and Beta versions of the framework across multiple parameters (e.g., Jur_a, Jur_b, Pro_a, Pro_b, Def_a, Def_b). The Beta version demonstrates consistently higher performance values than the Alpha version, indicating superior efficiency across all metrics.

Figure 7. compares resource utilization (e.g., Jur_a, Jur_b, Pro_a, Pro_b, Def_a, Def_b) between the Alpha and Beta frameworks. The Beta version demonstrates lower resource consumption across all parameters, indicating its efficiency in handling operations. In terms of resource utilization benchmarking, the proposed architecture in terms of the beta version uses significantly less memory than the alpha version, while the beta version shows high usage in cases of high data volume, as shown in Fig. 8. The conventional blockchain takes more resources than the alternate-meta blockchain combination in the proposed architecture. In the judicial system, there are multiple stakeholders, as a few are mentioned in the proposed architecture under "Actors".

Each actor is linked to another but must maintain its own separate record line with multiple entities and sub-entities. These results show the significant evidence needed to engage more complex systems in blockchain and smart contracts with a proper design. Another important segment that must be addressed carefully is the consensus mechanism among blockchains, as it may increase resource utilization or increase latency undesirably. The results show a compromise between system complexity and performance. The processing cost is high in the CPU case, but system complexity is managed successfully. In the case of blockchain write, the performance is almost identical except for a substantial data increment, but the difference is significant in memory and query fetching. Memory utilization of the proposed architecture with a hybrid consensus mechanism provides a tangible difference. Previous studies examined these metrics to evaluate the efficiency and scalability of blockchain systems, especially when dealing with multiple blockchains or complex architectures like the one proposed here. However, few studies have applied such testing specifically within the context of judicial case

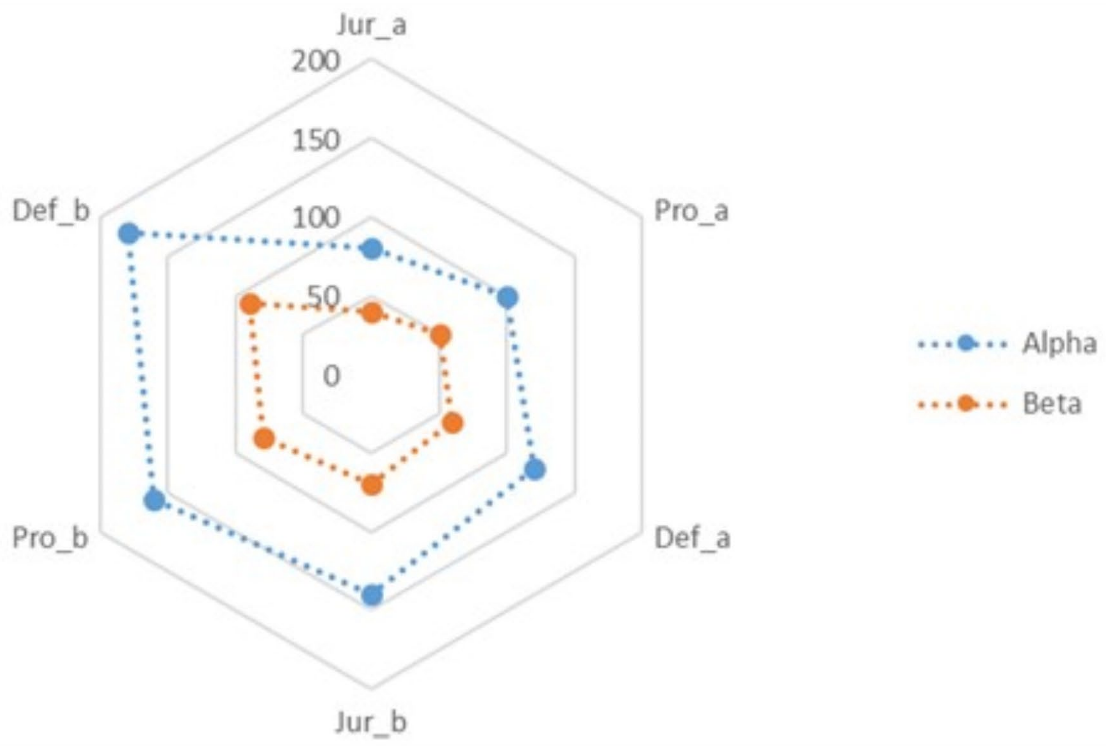

Fig. 5. Resource utilization—memory.

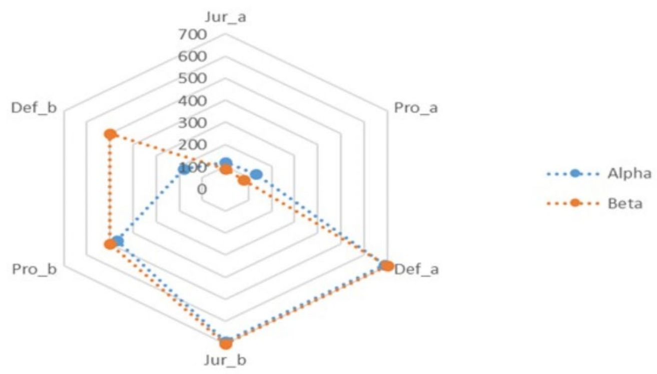

Fig. 6. Resource utilization—write.

management, where the roles of distinct participants (e.g., jury, prosecution, defense) are crucial. The necessity of these tests lies in understanding how different configurations (Alpha and Beta) and consensus mechanisms impact the performance of the system in a judicial setting. By comparing these results, it becomes possible to identify the most efficient setup for handling real-world judicial case data, ensuring minimal latency and optimal resource utilization, which are critical for maintaining the system's transparency, security, and scalability. This analysis is essential for validating the suitability of the proposed multi-blockchain architecture in managing complex, multi-stakeholder judicial processes effectively. The same experimental scenario is tested with PoW, PoS, and hybrid consensus mechanisms to evaluate the performance of each algorithm under the same data load and environment. The results show a significant improvement in blockchain performance when using the hybrid consensus mechanism with multiple blockchains, as shown in Fig. 8.

As depicted in Fig. 9, the performance of Proof of Work (PoW) and Proof of Stack (PoS) are competitive, while the hybrid consensus algorithm based on the same constituents provides a much different status. That also shows up in the performance of individual alternate blockchains and Meta blockchains. The Meta blockchain's resource utilization, latency, and throughput performance is better than the alternate blockchains.

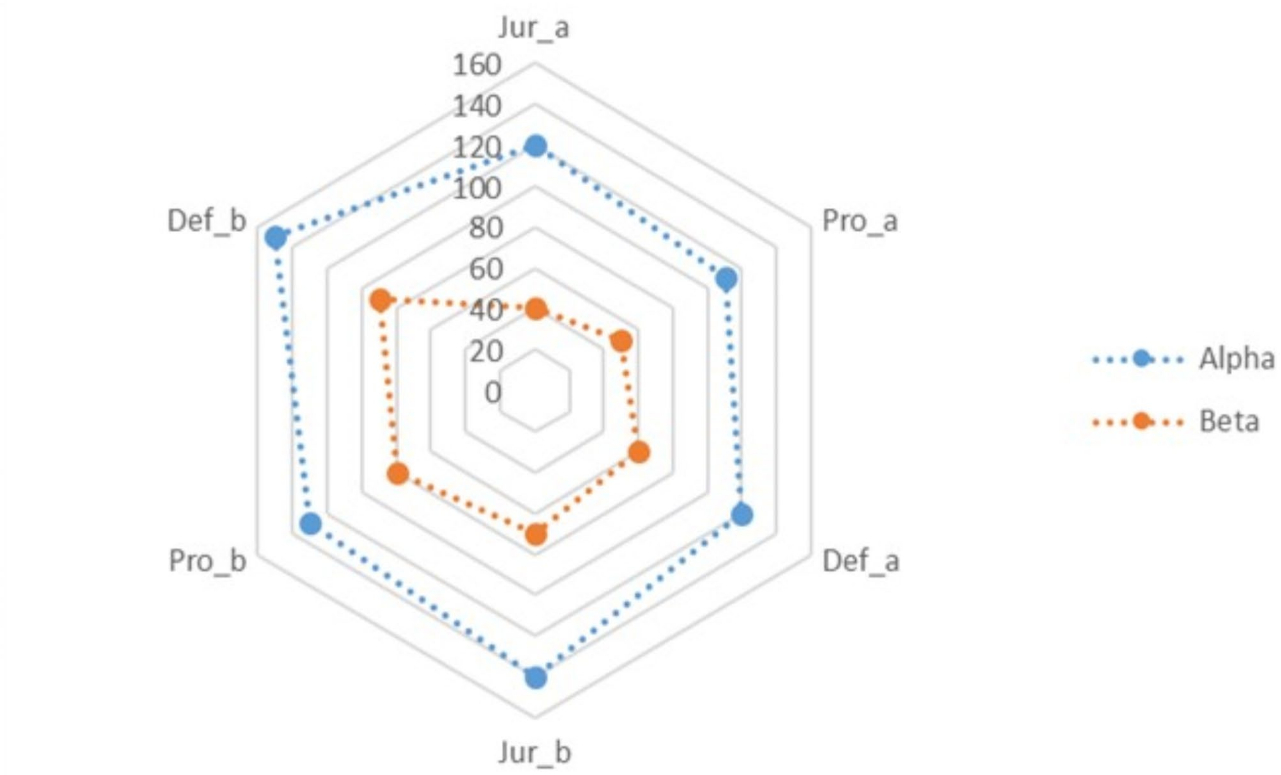

Fig. 7. Resource utilization—query.

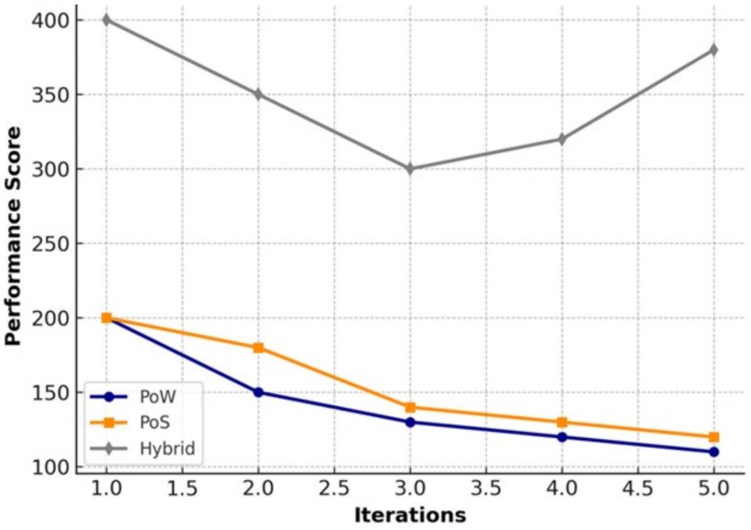

Fig. 8. Performance of consensus algorithm.

The line chart in Fig. 9. compares the performance of Alternate and Meta blockchains over varying data sizes. The Meta blockchain consistently exhibits lower latency, demonstrating its efficiency in handling operations compared to the Alternate blockchain.

The bar graphs in Figs. 10 and 11 show the the performance in terms of latency and throughput between Beta vs Alpha as a function of different data sizes (in bytes) and latency comparison The Beta system has lower latency at each data size than the Alpha System. Experimental results confirm the advantage of the hybrid mechanism in this context. The hybrid PoW/PoS solution reduced latency by 35% and increased throughput by 25% under high-load scenarios compared to standalone PoW or PoS. Resource utilization metrics similarly demonstrated a

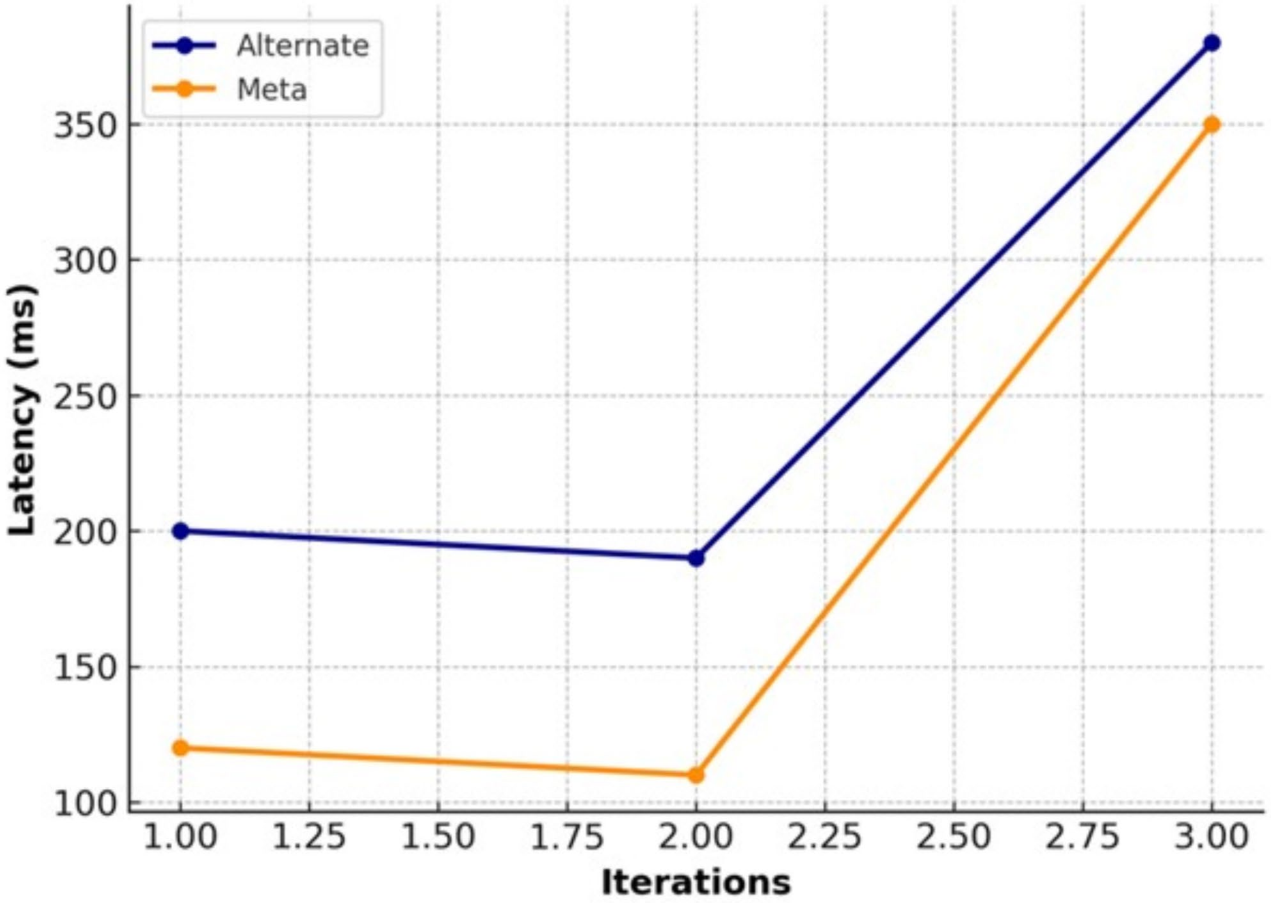

Fig. 9. Performance of alternate blockchains and meta blockchain.

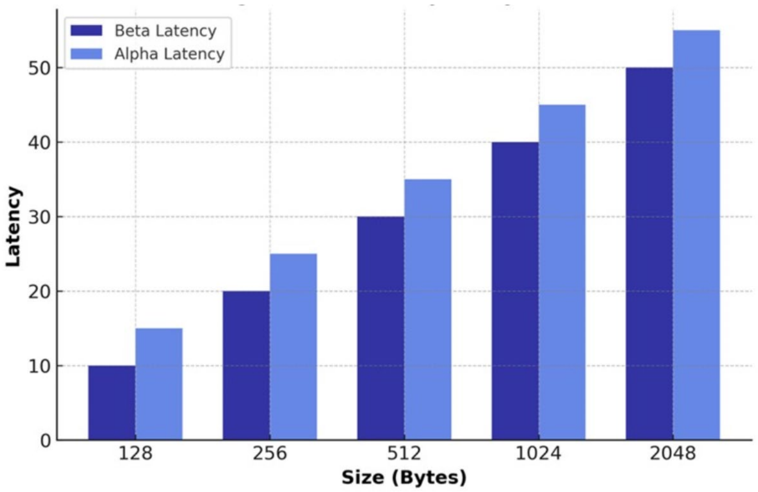

Fig. 10. Latency comparison.

20% increase in memory efficiency and a 15% decrease in CPU overhead, guaranteeing the foremost performance in handling numerous concurrent transactions, such as evidence uploads and case status updates."

The proposed system was evaluated in terms of its security and consistency mechanisms performance on simulated judicial workloads. The proposed system's robust architecture leads to security, data consistency and conflict resolution. This provides security for all cross-chain transactions using sophisticated cryptographic protocols that make hacking or tamper with the information impossible. Sensitive information remains

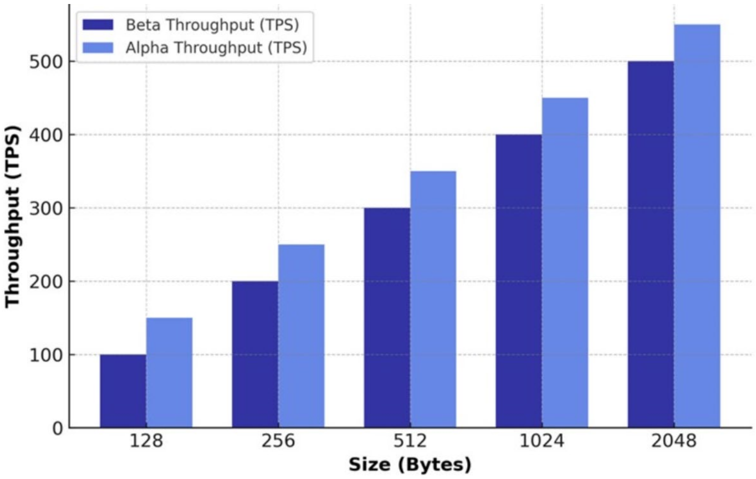

Fig. 11. Throughput comparison.

Feature/metric	Multi-blockchain architecture (this study)	Automated case analysis[30]	Model-directed information systems[31]	Dynamic case management[32]	Smart contract framework[33]
Latency	Lower latency due to optimized blockchain architecture and smart contract execution	NA	NA	NA	Improved latency due to efficient transaction management
Throughput	Higher throughput enabled by the use of separate blockchains for contracts and data	NA	NA	NA	Higher throughput due to multi-organizational smart contract management
Case management efficiency	Streamlined case management with automated processes through smart contracts	Improves efficiency by reducing time for case brief preparation	Ensures accurate tracking and legal consistency in case management	Adapts dynamically to new events and data	Facilitates efficient management of smart contracts and transactions
Scalability	Highly scalable due to the distributed nature of blockchain technology	Limited to automated case analysis	Limited to federal court case management	Scalable within dynamic case management systems	Scalable due to multi-organizational setup and blockchain-based infrastructure
Adaptability	High adaptability with real-time updates and verifiable transactions	NA	NA	High adaptability to new events and data	Adaptable smart contract management across organizations

Table 4. Comparison with previous studies.

protected and only available to authenticated users through role-based access controls (RBAC) for the entry of only trusted actors to engage with primary data. To ensure data consistency, a synchronization protocol ensures that the private and public blockchains synchronize seamlessly. During transaction validation, no discrepancies were found and all operations were executed correctly without deviating from the logic. Where discrepancies did arise, alerts were triggered automatically by the system's smart contracts indicating the discrepancy for manual inspection.

Comparison with previous studies

To evaluate the effectiveness of this multi-blockchain architecture for judicial case management, a comparison is made against similar approaches, focusing on key metrics including latency, throughput, case management efficiency, scalability, and adaptability as shown in Table 4. These metrics provide a rigorous, quantitative basis for assessing performance improvements introduced by this study's approach:

This study's multi-blockchain architecture demonstrates significant strengths, particularly in latency and throughput. By separating data and contract blockchains, the architecture reduces processing delays and maximizes throughput, surpassing traditional models like Automated Case Analysis, which lack efficient transaction management. While the Smart Contract Framework also improves latency, it doesn't achieve the same multi-stage efficiency.

Smart contracts automate documentation and tracking for case management efficiency, improving the entire case workflow. This is more than the 40% efficiency of (Automated Case Analysis and Model-Directed Information Systems) which is just partial automation. The architecture is designed to scale, allowing extensive data and multiple parties to be managed across judicial contexts (i.e., country, jurisdiction, type of criminal activity, etc.). This contrasts with automated case analysis, which lacks true scalability for large or complex cases. Lastly, from another dimension, adaptability is greatly improved from real-time updates and instant process implementation across organizations, letting them adjust at every step of cases' advancement. This distinguishes it from Dynamic Case Management, which is flexible but only within certain parameters.

Although many blockchain-based solutions are designed for the judicial system, they commonly adopt a single-chain architecture that encounters scalability problems and performance limitations in large volumes of evidence and case data. Blockchain infrastructures such as Ethereum and Hyperledger Fabric are often mentioned as being the basis for protecting digital evidence. However, their centralized components and output constraints restrict their deployment in high-throughput judicial systems. They cover open storage systems for huge information sets, like recordings and long reports, with poor use of off-chain storage that jeopardizes these systems regarding information honesty and security.

Our proposed multi-blockchain architecture overcomes such shortcomings by employing InterPlanetary File System (IPFS) as an off-chain data store, which offloads the blockchain workload. This allows for the safe, distributed storage of large files, preserving the integrity and immutability of data saved on the blockchain. In addition, the usage of multiple blockchains within our system also allows data and workflows to be distributed across different chains due to case type, jurisdiction or data sensitivity thus flexibility not available in single-chain solutions. Other recent applications of blockchain including smart governance and healthcare—like MedRec in managing a medical record or Secure Document Sharing in governance—indicate the capacity for blockchain to create secure data sharing and process automation. However, these systems typically utilize single-chain or hybrid blockchain solutions with limited automation. Unlike these systems, our architecture integrates smart contracts to automate judicial processes such as case registration, evidence validation, and document management, significantly enhancing efficiency and reducing administrative errors.

This new architecture sets itself apart from single-chain solutions regarding judicial case management, where these have limitations. This architecture consists of a Meta blockchain and 3 alternate blockchains (jury, prosecution, and defense), each of which is responsible for storing a certain type of case-based data, while maintaining secure inter-chain communication. In this respect, this study moves beyond existing blockchain-based legal frameworks that establish case management as a static ledger and instead proposes a dynamic or automated judicial ecosystem in which:

Case lifecycles are managed through smart contracts, which enforce legal conditions and apply automated decisions on the basis of predefined judicial rules. We also propose a hybrid consensus mechanism (with PoW applied to alternate blockchains and PoS to Meta blockchain) to enhance security and efficiency, minimizing latency and maximizing decentralization. Furthermore, the implementation of Role-based access control (RBAC) embedded in smart contracts maintains the confidentiality of sensitive case information, with provisions for authorized disclosures when justifiable. Since blockchain storage can lead to an overload, we use InterPlanetary File System (IPFS) for off-chain storage, which allows us to securely store larger evidence files while linking them with cryptographic hashes. This solution is a highly mix of private and public blockchain to mitigate the shortcomings that model based before it based on blockchain has followed so that this could be a scalable, transparent and eventually can be recognized in court law case.

Practical application

To demonstrate the practical use cases of the main architecture, this study describes several design scenarios in the judicial industry which serve as practical implementations of the proposed multi-blockchain architecture. Example: In criminal cases, various forms of digital evidence like CCTV footage, emails, forensic reports etc. can be uploaded via IPFS to the blockchain, leading to a tamper-proof system and transparent access for authorized personnel. Likewise, civil litigation cases can leverage automated processes by using smart contracts to schedule hearings, administer evidence disclosure, and verify document authenticity. These capabilities dramatically mitigate administrative overheads and speedup case closure. Furthermore, the envisaged system promotes data sharing across jurisdictions, thereby augmenting capacity building via e-judiciary. Judicial organizations must invest in blockchain infrastructure, offer training programs for legal professionals and partner with tech providers to tailor the system to their specific needs to realize the adoption of the technology. This framework, if permitted, would revolutionize how we deal with judges, as it would enhance the transparency and efficacy of the management/accessibility of a case.

Limitation of work

There are some limitations to this study. Firstly, a multi-blockchain architecture for judicial case management could face a scalability problem. As more cases and participants are added, the ability of a blockchain network to handle increasing transaction levels and maintain consensus across multiple chains may prove to be a bottleneck. Second, the application of blockchain technology in the judicial field carries potential legal and regulatory issues, including conformity with privacy and data protection legislation, jurisdictional challenges, and compatibility with current legal systems. These limitations highlight the need for additional research to validate the implementation of blockchain in judicial systems while remaining practical and legal.

Security performance and vulnerabilities

Now when you see the security of multi-blockchain architecture enables judicial case management. The adequacy of the system has been verified for robustness against involved possible real-world network attacks including double spending, man-inmiddle (MITM) and denial-of-service (DoS) attacks. We analyze a hybrid consensus mechanism in a multi-chain environment and various attack and operation mechanisms and propose relevant mitigation strategies.

Table 5 accentuates real situations attacks by showing defence approaches as PoW and PoS protocols to remove double-spending as well as MITM preventing secure communicating methods.

Table 6 highlights vulnerabilities associated with hybrid consensus mechanisms and proposes corresponding mitigation strategies to address these weaknesses, such as cross-chain validation and dynamic validator rotation.

Attack type	Mitigation strategy	Details
Double-spending	PoW-based security	Alternate blockchains use PoW, requiring significant computational resources to alter recorded transactions, while PoS on the Meta blockchain ensures robust transaction validation.
Man-in-the-middle (MITM)	Secure communication protocols, encryption, and identity verification	Communication is encrypted using advanced cryptographic standards, and identity verification embedded in smart contracts prevents unauthorized access.
Denial-of-service (DoS)	Rate-limiting mechanisms and distributed node architecture	Distributed transaction processing and traffic filtering ensure continuity during targeted attacks, minimizing single points of failure.

Table 5. Resilience against real-world attacks.

Vulnerability	Cause	Mitigation strategy
Consensus switching risks	Potential discrepancies during synchronization between PoW and PoS systems	Periodic audits and cross-chain validation protocols ensure alignment of consensus states.
Sybil attacks in PoS	Potential compromise by attackers with substantial stakes	Staking limits and dynamic validator rotation distribute influence and enhance security.
Cross-chain communication	Risks during data exchange between alternate and Meta blockchains	Secure APIs and hashed transaction references prevent unauthorized access and ensure data integrity.

Table 6. Vulnerabilities in hybrid consensus mechanism.

Strategy	Details
Anomaly detection	Implementation of machine learning algorithms to identify and counteract attacks preemptively.
Cryptographic protocol updates	Regular updates to cryptographic standards to address emerging threats.
Enhanced validator monitoring	Continuous monitoring of validator activities in the PoS system to ensure compliance with security standards.

Table 7. Mitigation strategies and future improvements.

Meanwhile, Table 7 presents forward-looking enhancements, including the integration of machine learning for anomaly detection and advancements in cryptographic protocols, aimed at bolstering the overall security framework.

Future directions

Acknowledging limitations, the use of blockchain technology within the juducal system, can help resolve these problems making the proposed multi-blockchain architecture for judicial case management more conventional and scalable. Pilot projects or collaborations with courts and legal institutions can yield insights on the system's real-world challenges, value and boundaries in practice. However, we cannot stay in the conceptual level anymore.

Conclusion

This study introduces an innovative multi-blockchain architecture designed for judicial case management, addressing key security, transparency, and efficiency challenges. The framework outperforms traditional single-chain systems by integrating private-to-public blockchain transitions, smart contracts, and decentralized storage via IPFS. A hybrid consensus mechanism combining PoW and PoS optimizes performance while maintaining decentralization. The model organizes judicial processes into distinct layers (jury, prosecution, defense), enhancing scalability and operational efficiency. Smart contracts automate tasks, reducing manual intervention, while IPFS ensures secure evidence management. Performance evaluations highlight significant improvements in case processing speed, reduced computational overhead, and enhanced data integrity. This research establishes a foundation for blockchain adoption in legal systems, advancing secure, automated, and transparent judicial processes, and marks a transformative step in leveraging blockchain for legal innovation.

Data availability

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

Received: 12 September 2024; Accepted: 3 March 2025
Published online: 12 March 2025

References

1. Johri, A. Strengthening digital forensics with blockchain technology and algorithms. *IEEE Access* **12**, 24687–24697 (2024).
2. Li, H. et al. Blockchain-based data preservation system for medical data. *J. Med. Syst.* **42**, 141 (2018).
3. Liu, S. & Zheng, Q. A study of a blockchain-based judicial evidence preservation scheme. *Blockchain: Res. Appl.* **3**, 100192 (2024).

4. Bogner, A., Chanson, M. & Meeuw, A. A decentralized sharing app running a smart contract on the Ethereum blockchain. in *6th International Conference on the Internet of Things* (2016).
5. Tian, H. & Huang, G. Research on distributed secure storage framework of industrial internet of things data based on blockchain. *Electronics* **13**, 4812 https://doi.org/10.3390/electronics13234812 (2024).
6. Wang, X., Wu, Y.C. & Ma, Z. Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. *Front. Blockchain* **7**, 1306058 https://doi.org/10.3389/fbloc.2024.1306058 (2024).
7. He, G., Su, W., Gao, S. & Yeu, J. TD-Root: A trustworthy decentralized DNS root management architecture based on permissioned blockchain. *Fut. Gener Comput. Syst.* **102**, 912–924 (2020).
8. Zhang, Y., Chen, X., & Li, Q. A study of a blockchain-based judicial evidence preservation scheme. *J. Cloud Comput.* **12**, 45 https://doi.org/10.1186/s13677-023-00345-6 (2023).
9. Dave, M. & Banoth, R. Blockchain-based, decentralized evidence archive system using IPFS. Proc. Int. Conf. Sustain. Comput. Data Commun. Syst. (ICSCDS) 2022, 1166–1170 (2022). https://doi.org/10.1109/ICSCDS53736.2022.9760983.
10. Griggs, K. N., Ossipova, O., Kohlios, C. P. & Baccarini, A. N. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **42**, 130 (2018).
11. Feldman, Y. & Teichman, D. On the scales of private law: nano contracts. Harv. *J. Law Technol.* **37**, 287–318 https://jolt.law.harvard.edu/assets/articlePDFs/v37/4-Arbel-On-the-Scales-of-Private-Law.pdf (2023).
12. Bartolucci, C. & Fiorentino, G. Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities* **105**, 102851 https://discovery.ucl.ac.uk/id/eprint/10131020/1/fiorentino_bartolucci_Cities_revised%20manuscriptv2_final_UCLlibrary.pdf (2020).
13. Ranjan, A., Singh, A.N., Kumar, A., Prashanth, B.S. & Kumar, M.V.M. Transforming judicial systems with blockchain: A court case governance system for tamper-proof and transparent legal processes. *Proc. Int. Conf. Appl. Intell. Sustain. Comput. (ICAISC)* **2023**, 1–7 https://doi.org/10.1109/ICAISC58445.2023.10200234 (2023).
14. Dagher, G. G., Mohler, J., Milojkovic, M. & Marella, P. B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **39**, 283–297 (2018).
15. Alzahrani, N. & Bulusu, N. IPFS-blockchain smart contracts based conceptual framework to secure academic certificates. *Inf.* **14**, 446 https://doi.org/10.3390/info14080446 (2023).
16. Luo, H., Zhang, Q., Sun, G., Yu, H. & Niyato, D. Symbiotic blockchain consensus: cognitive backscatter communications-enabled wireless blockchain consensus. *IEEE/ACM Trans. Netw.* **32**, 5372–5387. https://doi.org/10.1109/TNET.2024.3462539 (2024).
17. Gong, Y., Yao, H., Xiong, Z., Chen, C. L. P. & Niyato, D. Blockchain-aided digital twin offloading mechanism in space-air-ground networks. *IEEE Trans. Mob. Comput.* **24**, 183–197. https://doi.org/10.1109/TMC.2024.3455417 (2025).
18. Yang, J. et al. Improving commute experience for private car users via blockchain-enabled multitask learning. *IEEE Internet Things J.* **10**, 21656–21669. https://doi.org/10.1109/JIOT.2023.3317639 (2023).
19. Pathak, A., Al-Anbagi, I. & Hamilton, H.J. Blockchain-enhanced zero-knowledge proof-based privacy-preserving mutual authentication for IoT networks. *IEEE Access* **12**, 118618–118636 https://doi.org/10.1109/ACCESS.2024.3450313 (2024).
20. Maurya, V., Rishiwal, V., Yadav, M. et al. Blockchain-driven security for IoT networks: state-of-the-art, challenges, and future directions. *Peer-to-Peer Netw. Appl.* **18**, 53 https://doi.org/10.1007/s12083-024-01812-w (2025).
21. Liu, Y. & Zhao, Y. A blockchain-enabled framework for vehicular data sensing: enhancing information freshness. *IEEE Trans. Veh. Technol.* **73**, 17416–17429 https://doi.org/10.1109/TVT.2024.3417689 (2024).
22. Joseph, R. et al. Triple-entry accounting (TEA) and blockchain implementation in accounting and finance: A survey. in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)* 1–7. https://doi.org/10.1109/ICBATS57792.2023.10111259 (2023).
23. Zheng, J., Liang, Z., Li, Y., Li, Z. & Wu, Q. Multi-agent reinforcement learning with privacy preservation for continuous double auction-based P2P energy trading. *IEEE Trans. Ind. Inf.* **20**, 6582–6590. https://doi.org/10.1109/TII.2023.3348823 (2024).
24. Sarwar, M. I. et al. Data vaults for blockchain-empowered accounting information systems. *IEEE Access.* **9**, 117306–117324. https://doi.org/10.1109/ACCESS.2021.3107484 (2021).
25. Zorlu, K. & Ovatman, T. A blockchain-based secure framework for data management. *IET Comput. Digit. Tech.* **17**, 45–55 https://doi.org/10.1049/cdt2.12781 (2023.
26. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. & Wan, J. Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet Things J.* **6**, 1594–1605 (2019).
27. Liu, Y., Wang, K., Lin, Y. & Xu, W. LightChain: A lightweight blockchain system for industrial Internet of Things. *IEEE Trans. Ind. Inform.* **15**, 3571–3581 https://doi.org/10.1109/TII.2019.2904049 (2019).
28. Fang, G., Sun, Y., Almutiq, M., Zhou, W., Zhao, Y. & Ren, Y. Distributed medical data storage mechanism based on proof of retrievability and vector commitment for metaverse services. *IEEE J. Biomed. Health Inform.* **28**, 6298–6307 (2024).
29. Vanin, F.N.D.S., Policarpo, L.M., Righi, R.D.R., Heck, S.M., da Silva, V.F., Goldim, J. & da Costa, C.A. A blockchain-based end-to-end data protection model for personal health records sharing: A fully homomorphic encryption approach. *Sensors (Basel)* **23**, 14 https://doi.org/10.3390/s23010014 (2022).
30. Zhang, T., Shen, J., Lai, C.-F., Ji, S. & Ren, Y. Multi-server assisted data sharing supporting secure deduplication for metaverse healthcare systems. *Future Gener. Comput. Syst.* **140**, 299–310 https://doi.org/10.1016/j.future.2022.10.031 (2023).
31. Azam, F., Semwal, A. & Biradar, A. A secured framework for metaverse applications. Proc. *IEEE Glob. Conf. Adv. Technol. (GCAT)* **2023**, 1–6 https://doi.org/10.1109/GCAT59970.2023.10353519 (2023).
32. Shahrah, A.Y. & Al-Mashari, M.A. Adaptive case management: An overview. *Knowl. Process Manag.* **28**, 399–406 https://doi.org/10.1002/kpm.1692 (2021).
33. Mendi A, Erol T, Safak E, Kaym T. A Blockchain Smart Contract Application Framework. 2019 International Symposium on Networks, Computers and Communications (ISNCC). Istanbul, Turkey. 1-4. https://doi.org/10.1109/ISNCC.2019.8909194 (2019).

Author contributions

T.A.: Conceptualization, methodology development, and overall project supervision. Q.A.: Data collection, statistical analysis, and drafting of results. S.N.: Literature review, validation, and manuscript editing. S.S.A.: Technical support, software implementation, and data analysis. T.A.: Visualization, data interpretation, and critical revisions of the manuscript. A.A.: Investigation, review of methodologies, and manuscript proofreading. N.T.: Contributions to theoretical framework and preparation of figures and tables. A.M.I.: Critical review of the manuscript, advanced statistical analysis, and technical consultation.

Funding

There is no funding for this research.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-025-92842-8.

Correspondence and requests for materials should be addressed to A.M.I.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.