TrustChain: Enabling Consensus-Driven Multitasking AI

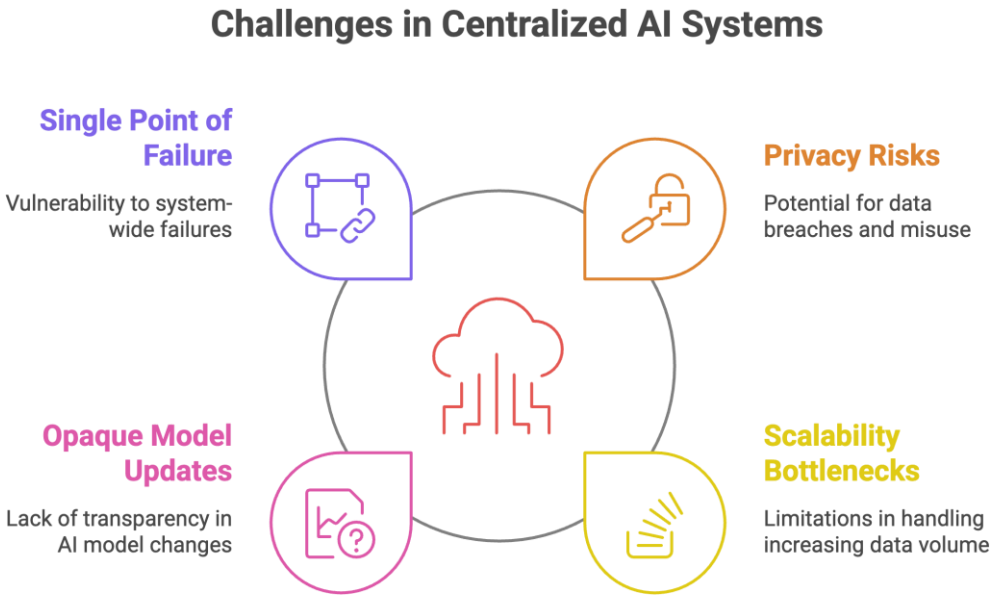
A Decentralized AI Framework for Secure, Multi-Institutional Collaboration

SPONSORED BY CEDA IEEE Council on Electronic Design Automation SIGDA ACM

TrustChain

TrustChain is a research prototype designed to support secure, decentralized AI collaboration across institutions without requiring centralized data pooling.
It leverages Matrix for encrypted communication, IOTA Tangle for immutable logging and consensus, and knowledge distillation to aggregate fine-tuned task-specific models into a unified global model.
Our evaluated setup demonstrates how TrustChain supports multitasking AI — including NER, ICD coding, and QA — while ensuring update transparency and preserving local data privacy.
This research highlights the feasibility of a trust-enhanced, domain-agnostic framework for future scalable AI systems..

Challenges in Current AI Collaboration



- Centralized models lack scalability, are resource-heavy, and prone to single points of failure.
- Privacy concerns with centralized data collection.
- Task-specific models are limited to narrow applications and lack flexibility.
- Existing frameworks suffer from scalability issues, reliance on single points of failure, and lack transparent mechanisms for validating model updates.

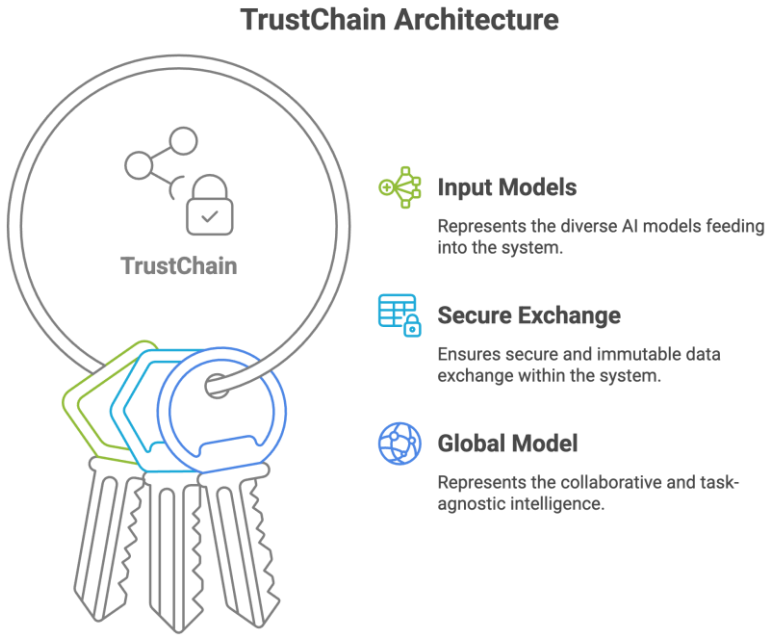
TrustChain: Decentralized AI for Collaborative Multitasking

Proposed Solution: A decentralized AI framework.

Leverages: IOTA Tangle for tamper-proof, immutable update logs and Matrix for secure, encrypted communication.
Multitasking Capability: Unified Global Model via Knowledge Distillation.

Key Opportunities:

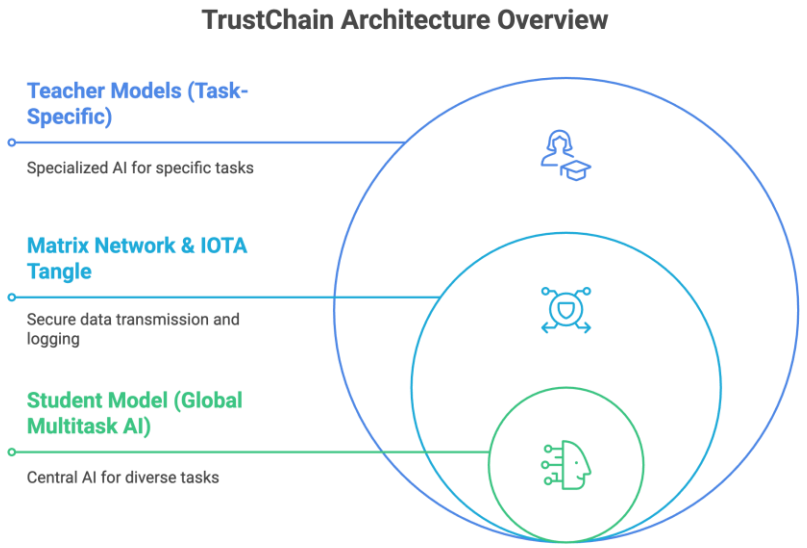
- Democratic Collaboration: Institutions retain data ownership while contributing updates.
- Secure and Transparent: Via Matrix and IOTA.
- Privacy-preserving federated learning with local data ownership.



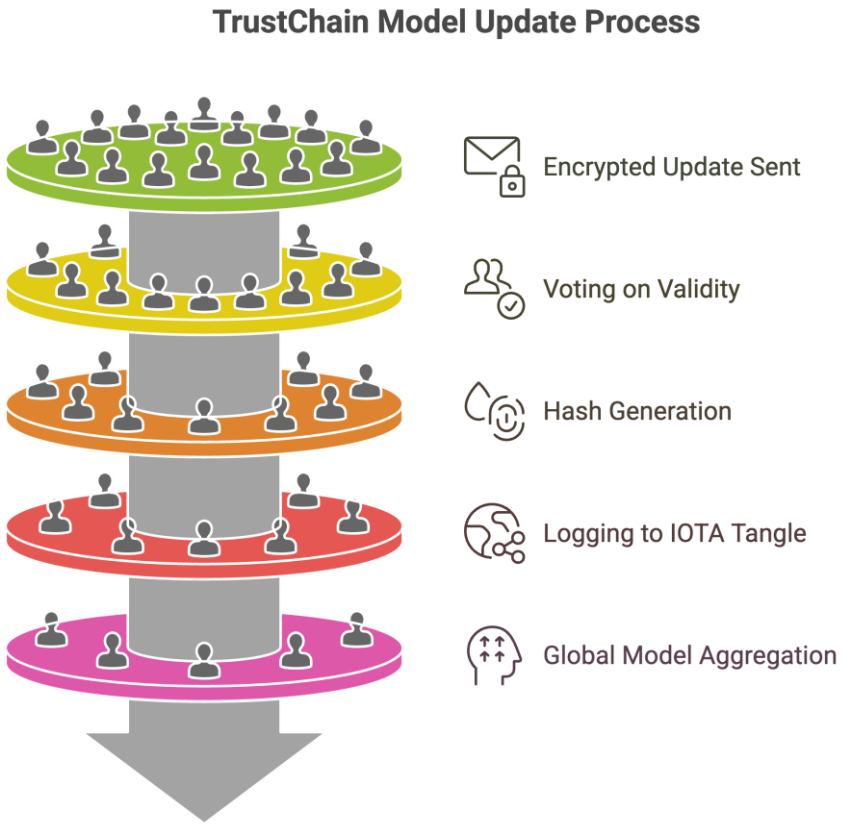
TrustChain: Decentralized AI for Collaborative Multitasking

Key Components :

- **Teacher Models:** Fine-tuned on specific tasks (NER, ICD, QA) using BioBERT, LLAMA, and BioGPT.
- **Global Model (Student Model):** Combines task-specific expertise via Knowledge Distillation to support multitasking.
- **Decentralized Infrastructure:** Secure updates via Matrix Network and transparent logging using IOTA Tangle.

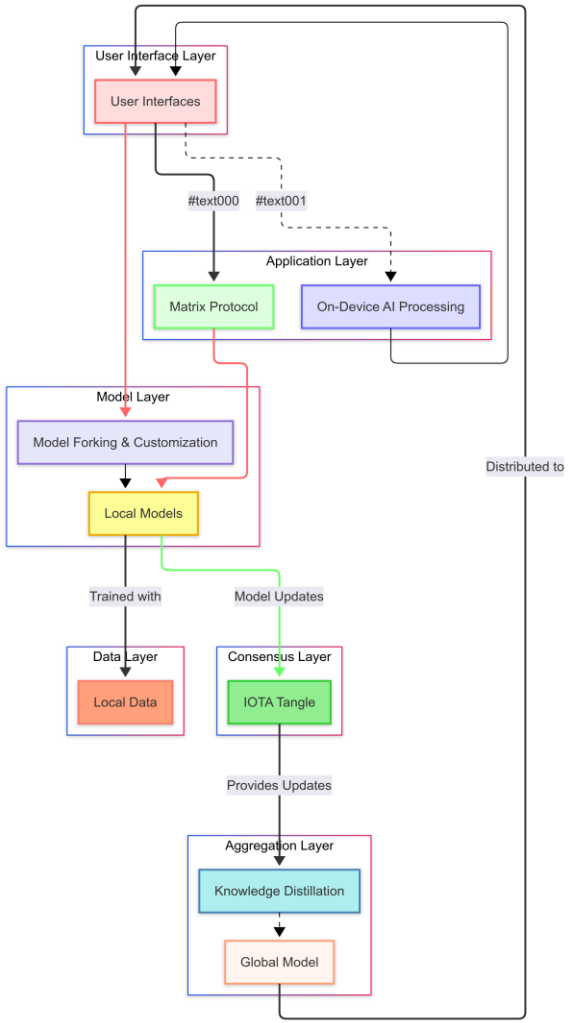


TrustChain Detailed Workflow



- Local fine-tuning of models on respective tasks.
- Decentralized updates via Matrix Network with tamper-proof logging using IOTA Tangle.
- Model aggregation through Knowledge Distillation for a multitasking Global Model.

Methodology & Experimental Setup

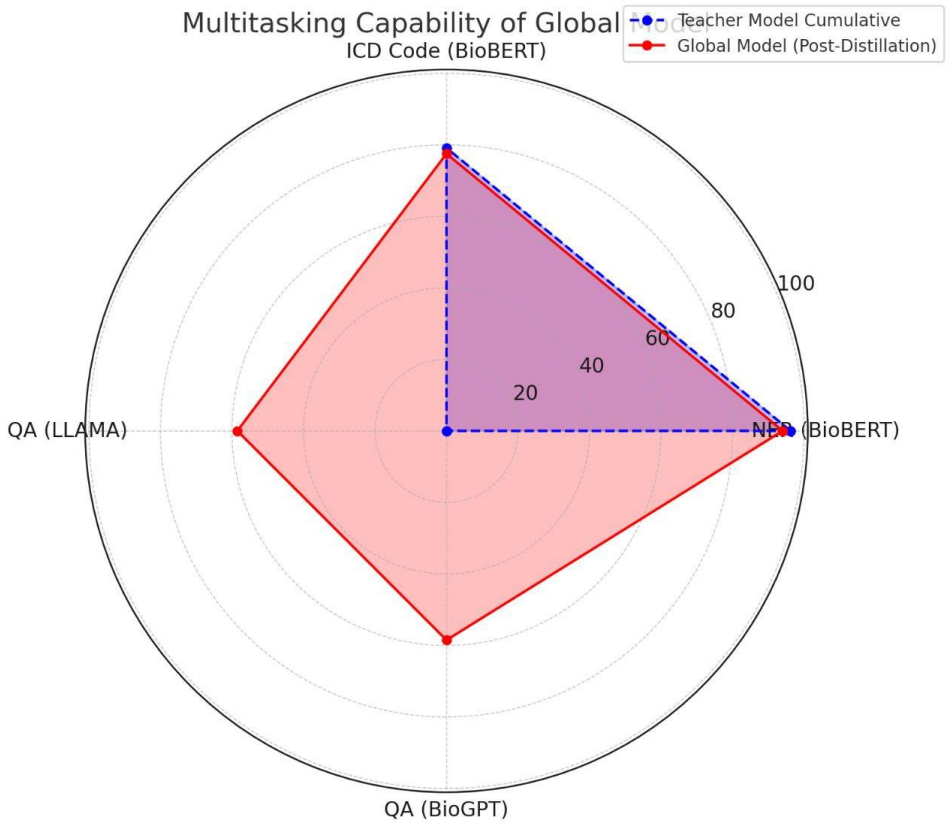


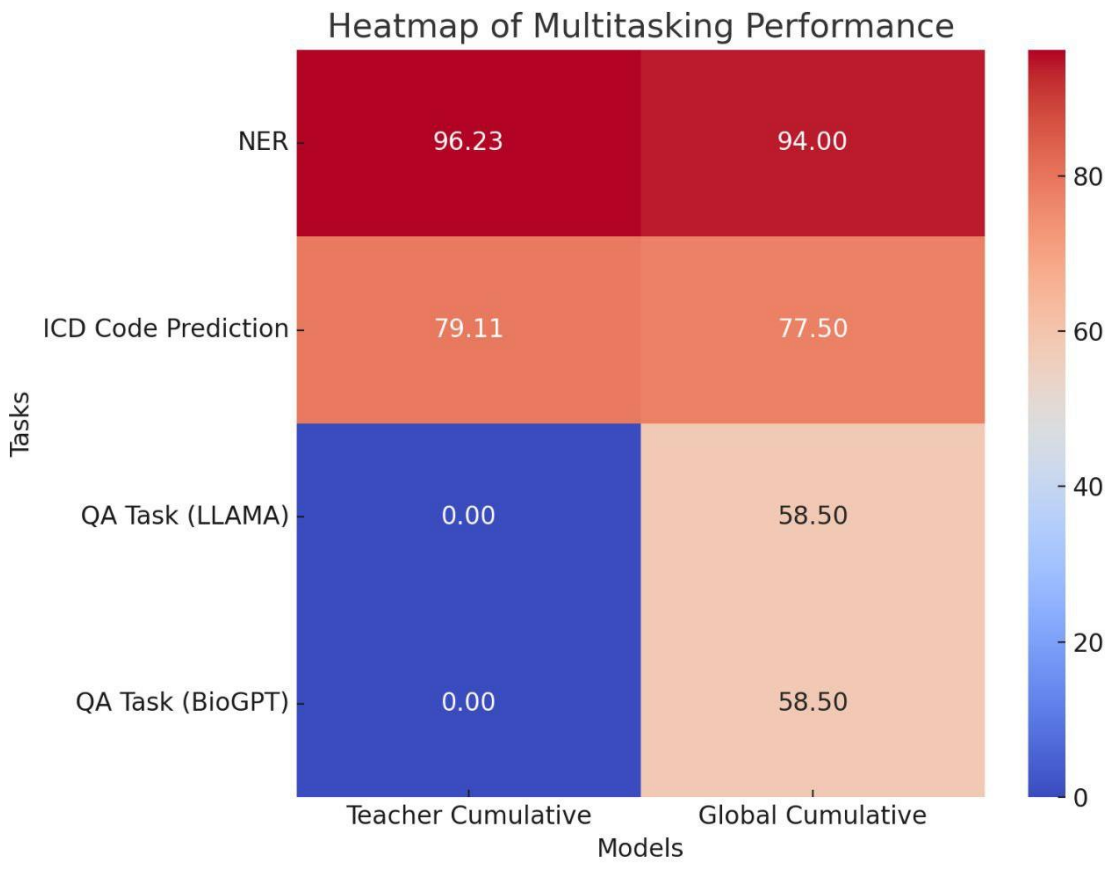
- **Tasks:**
- NER and ICD Code Prediction using BioBERT.
- QA tasks using LLAMA and BioGPT.

Infrastructure: 200 Compute Units with GPU (L4 Colab).
Training Parameters: Batch size: 32, Epochs: 5, Learning Rate: 2e-5.
Evaluation Metrics: NER: Accuracy; ICD: Multi-code classification; QA: BLEU, ROUGE, and Similarity.

Results: Teacher Model Performance

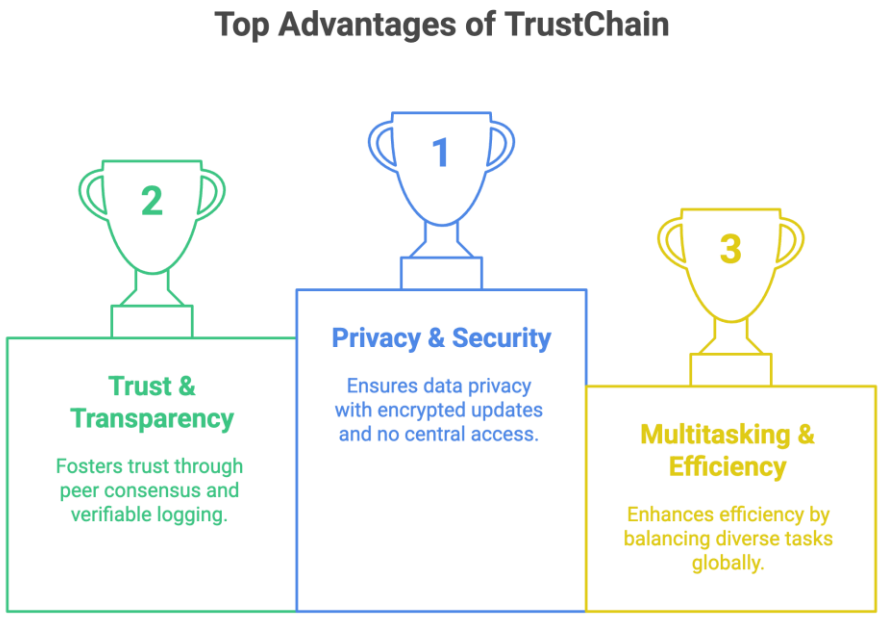
Global Model (Post-Distillation) achieves balanced multitasking:





Key Benefits & Takeaways

- Ensures privacy by keeping data local and sharing only model updates.
- Democratic decision-making through voting and consensus mechanisms.
- Unified AI model capable of handling diverse tasks simultaneously.
- Enables decentralized and democratic collaboration.
- Privacy-preserving federated learning.
- Transparent updates via IOTA Tangle.
- No dependency on centralized resources.
- Combines multiple task-specific models into a single multitasking Global Model (Efficiency).
- Suitable for use across industries, research, and institutions (Adaptability).



Future Enhancements & Conclusion

Transition from Research to Reality: Explore practical applications and commercialization efforts, such as forkit.dev, to bring decentralized, collaborative AI solutions to real-world use cases.

TrustChain offers a robust foundation for secure, multi-institutional AI development by ensuring privacy, adaptability, and decentralized collaboration.

Thank You! Questions?

Arpita Sarker

ICPS, Heilbronn University

HEILBRONN UNIVERSITY
OF APPLIED SCIENCES

AI

Security

Systems

EDA

Design

62 THE CHIPS TO SYSTEMS CONFERENCE

SPONSORED BY CEDA® IEEE Council on Electronic Design Automation

sigda acm