

Practical Networking & Blockchain Lab (PRANET) at IIT Hyderabad

Kotaro Kataoka (kotaro@cse.iith.ac.in)
Department of Computer Science and Engineering
Indian Institute of Technology Hyderabad

Indian Institute of Technology Hyderabad

- Founded in 2008
- Ranked 8th (Engineering) in India (NIRF 2023)
- Faculties: 299
- Students: 4242
- Departments: 18+1



Practical Networking and Blockchain Lab

- Covering various aspects of Networking and Blockchain from the view points of theory and practice
- Interacting with people inside and outside the institute to collaborate through R&D and consultancy services to address the real world problems
- Quick History
 - “Practical Networking Lab” was originally launched in 2015
 - “Chainers Lab” was launched to work on Blockchain having Chaintope Inc. as a founding sponsor in 2019
 - These two labs were integrated to Practical Networking and Blockchain Lab in 2020

People (Faculty)



Kotaro Kataoka
Associate Professor
Internet, and Blockchain



Maria Francis
Assistant Professor
Computational Algebra,
Symbolic Computation,
Lattice Cryptography



Praveen Tammana
Assistant Professor
Systems and Networking,
Network Security, Software-
Defined Networking, ML for
Networks

People (Students)

- 10+ from Ph.D., M.Tech TA/RA (Masters), B.Tech (Bachelors)
- Free to join and collaborate

Past and Present Industry Collaborations



ALL INDIA DISASTER MITIGATION INSTITUTE
...risk reduction for the poor



NEDO New Energy and Industrial Technology
Development Organization



chaintope



DRIVING WIRELESS CONVERGENCE®

DENSO



I'm beside you 

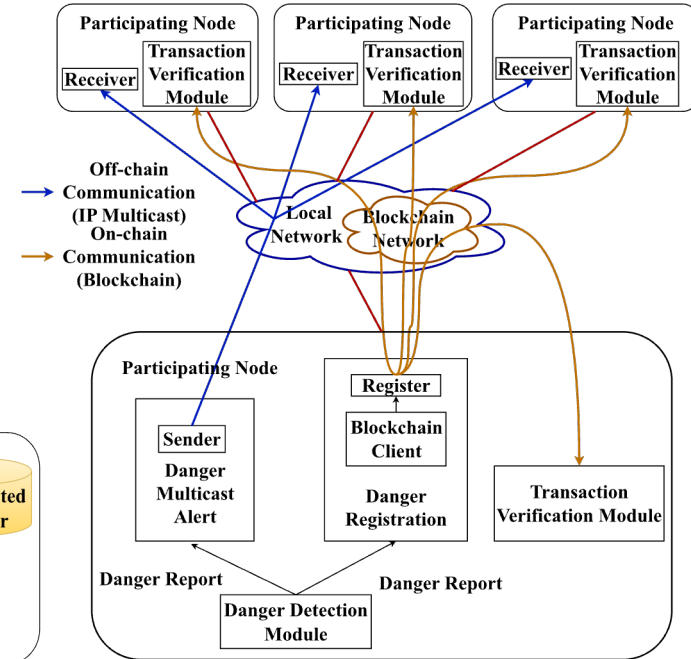
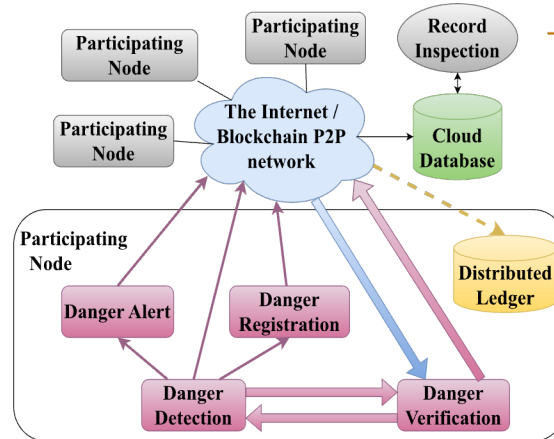
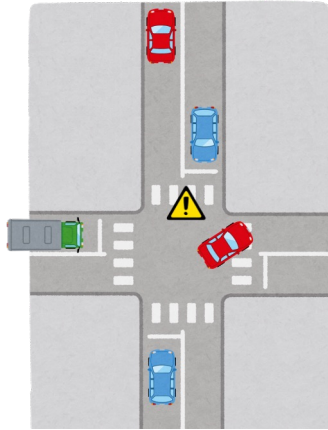


Recent Works

- D. R. R. RAJ, T. A. Shaik, A. Hirwe, **P. Tammana** and **Kotaro Kataoka**, "Building a Digital Twin Network of SDN Using Knowledge Graphs," in IEEE Access, vol. 11, pp. 63092-63106, 2023.
- Adeeba Naaz, T. V. Pavan Kumar B, **Maria Francis**, and **Kotaro Kataoka**, "Integrating Threshold Opening with Threshold Issuance of Anonymous Credentials over Blockchains for a Multi-certifier Communication Model", IEEE Access, Vol.10, pp.128697-128720, 2022.
- Reshu Verma, Vishnu V. S., **Kotaro Kataoka**, "Verifiable and Robust Monitoring and Alerting System for Road Safety by AI based Consensus Development on Blockchain", 2023 IEEE Intelligent Vehicles Symposium (IV), pp.1-8, 2023.
- Harish S A, Suvrima Datta, Hemanth Kothapalli, **Praveen Tammana**, Achmad Basuki, **Kotaro Kataoka**, Selvakumar Manickam, Venkanna U., Yung-Wey Chong, "Scaling IoT MUD Enforcement using Programmable Data Planes", NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, pp.1-9, 2023.
- Harish S. A., Hemanth Kothapalli, Shubham Lahoti, **Kotaro Kataoka**, **Praveen Tammana**, "IoT MUD Enforcement in the Edge Cloud Using Programmable Switch", The ACM SIGCOMM 2022 Workshop on Formal Foundations and Security of Programmable Network Infrastructures (FFSPIN '22), pp.1-7, 2022.

Verifiable and Robust Monitoring and Alerting System for Road Safety on Blockchain

- Enabling collective intelligence to cooperatively cross-check and alert dangerous situation
 - Archiving context of danger with the recorded evidence and verifiability
 - Verifying the contextual of dangerous situation with Multi-AI based PBFT consensus development



A Decentralized Threshold Revocable Anonymous Credential (DTRAC) Scheme over Blockchains

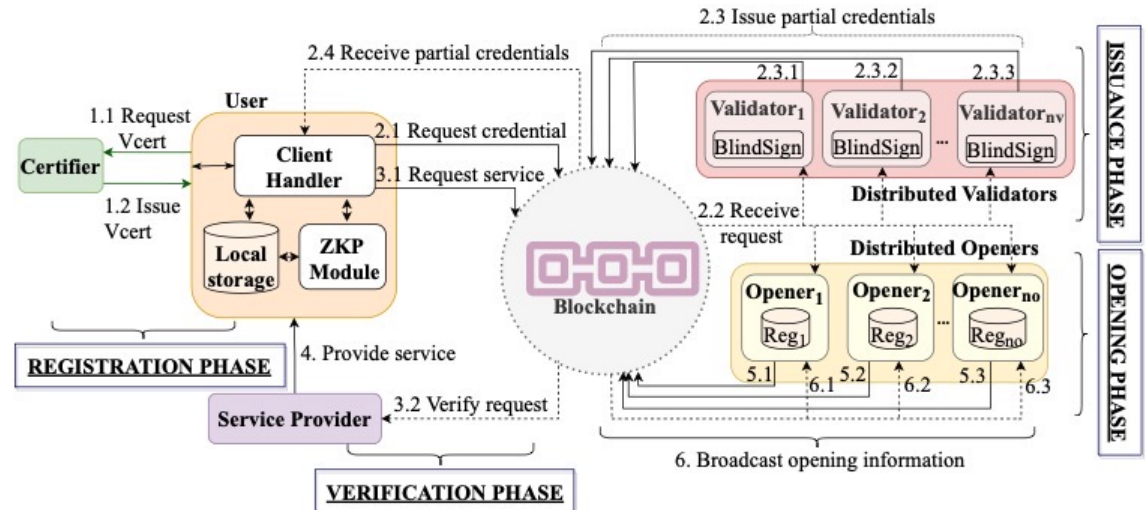
- Privacy and Selective Disclosure on Credential Management

- Verifiable certificates
- Multi-certifier model
- Threshold issuance
- Opening schemes

- Enabler Concepts

- Pairings-based cryptographic primitives
- Publicly Verifiable Secret Sharing Scheme (PVSS)
- Threshold PS Signatures
- Pedersen Commitments
- Zero-Knowledge Proofs of Knowledge (Non-interactive)

- PoE: DTRAC over Ethereum

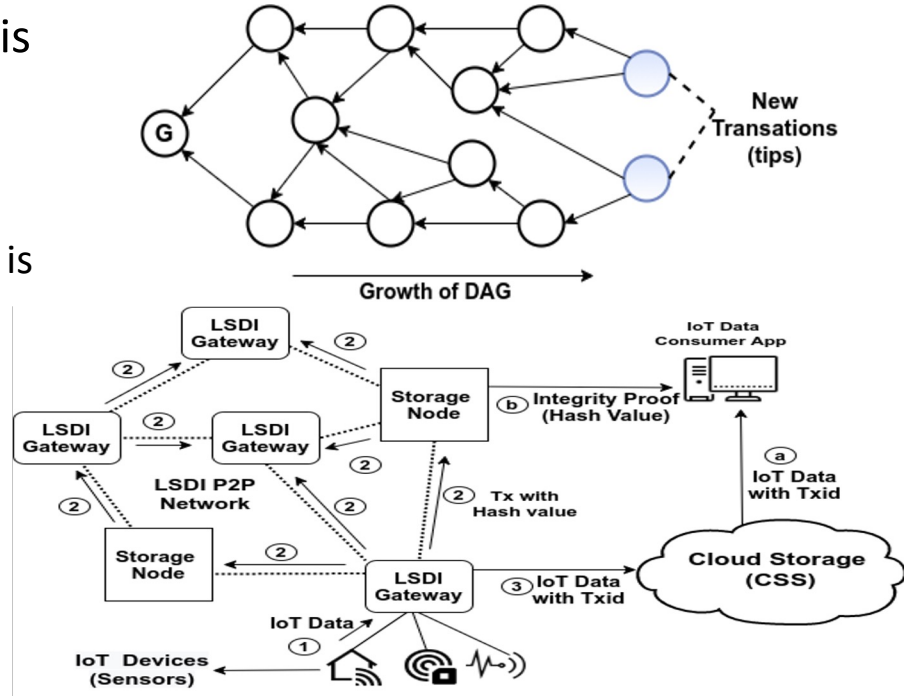


Method Name	Gas consumption	Smart Contract	Executed by	Frequency
RequestCred	6,089,587	Request	User	once for every credential request
VerifyCred	1,099,204	Verify	User	once for every service request
SendBlindSign	32,445	Issue	Validator	once for every credential request
SendOpeningInfo	41,599	Opening	Opener	once for every opening of a credential

Gas consumption for execution of smart contract methods.

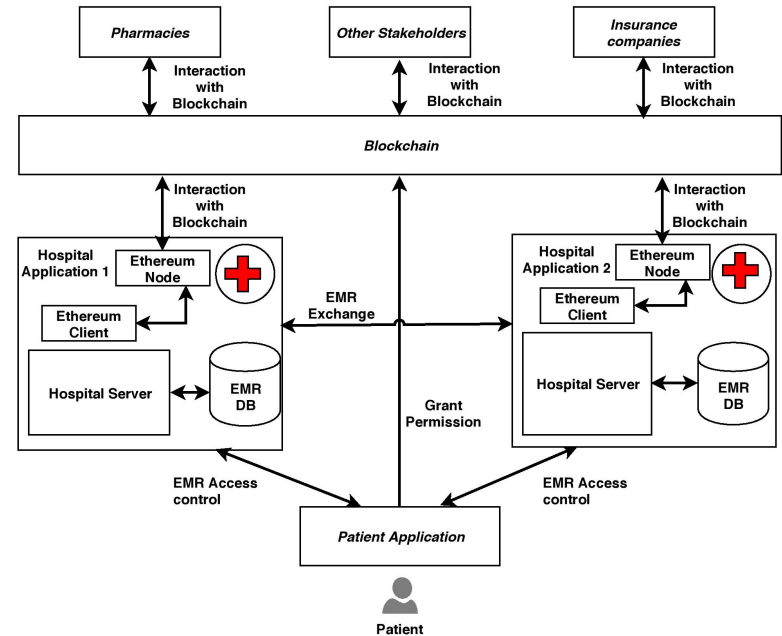
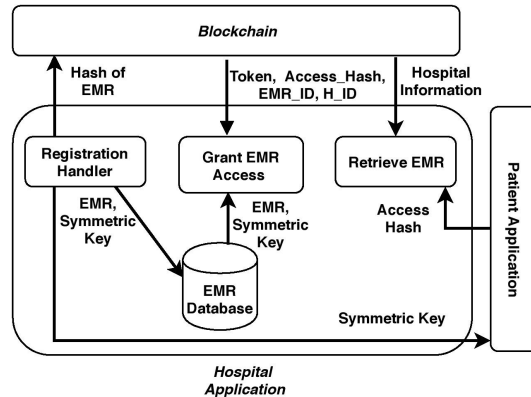
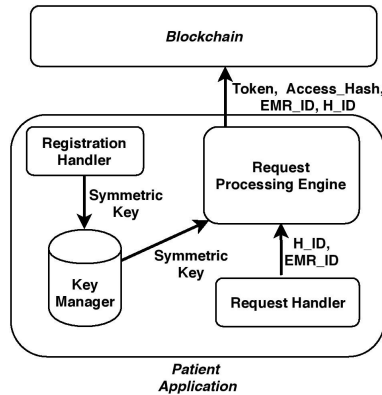
Lightweight and Scalable DAG based Distributed Ledger for IoT data integrity

- Check with Blockchain whether IoT Data is trustworthy and good to use
- Trustworthiness
 - IoT Data kept somewhere (ex. cloud storage) is NOT tampered
 - Separate the integrity check information and the IoT data from each other
- DAG based Distributed Ledger
 - More transaction throughput
 - PoW to regulate transaction generation



PACEX: PATient-Centric EMR eXchange in Healthcare Systems using Blockchain

- Patient-Centric Access Control among Healthcare Stakeholders
 - Can have full authority over EMR
 - Can easily track the history of EMR movements and use
 - Blockchain-based interplay
- PoC Implementation using Ethereum



Funding & Collaboration Schemes (We used)

- Industry Collaboration
 - Sponsored Research & Consultancy Services
- Government Schemes
 - ASEAN-India Science, Technology & Innovation Cooperation
 - IIT Hyderabad, Brawijaya University, University of Science Malaysia
 - Sakura Science Program, Japan
 - Sending students to Japan for 1 to 3 weeks

THANK YOU. Q&A?