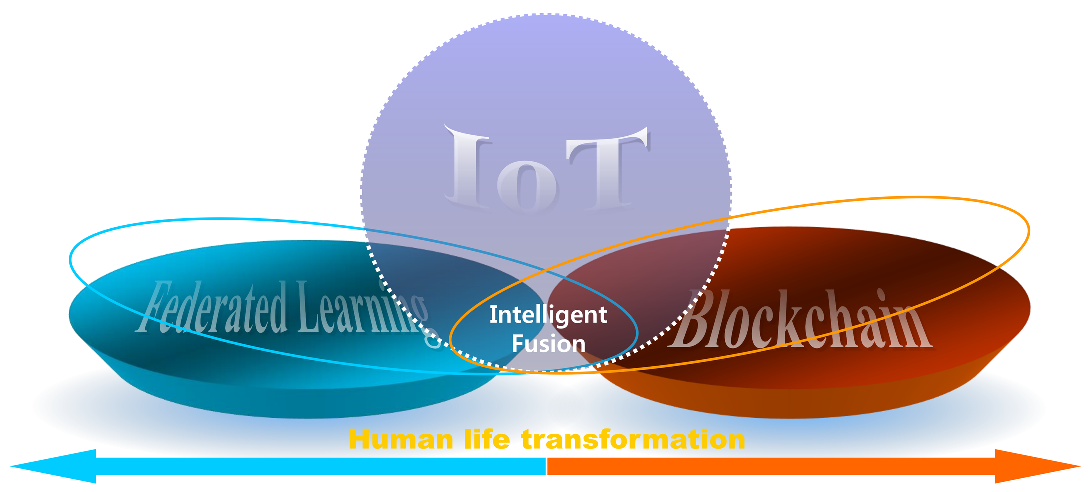
MicroFL: A Lightweight, Secure-by-Design Edge Network Fabric for Decentralized IoT Systems

Ronghua Xu, Yu Chen, Jian Li
Binghamton University, SUNY, Binghamton, NY 13902, USA

NDSS 2020

Introduction



- Distributed Internet-of-Thing (IoT) systems generate a large amount of data for Machine Learning (ML)
- Federated Learning (FL) facilitates large-scale collaborative learning of a global ML model with privacy preservation
- Blockchain brings decentralization, security and privacy enforcement into distributed cross-devices FL scenarios
- Intelligent Fusion based on IoT, FL and Blockchain needs a secure-by-design, self-adaptive, and totally decentralized network architecture

Key Challenges

IoT
- Constrained computation and storage resource
- Energy efficiency and heterogeneous network
- Data security and privacy concerns

FL
- Privacy-preserving in learning and aggregation
- Robust to adversarial attacks and failures
- Complex incentive mechanism

Blockchain
- The trade-off between scalability and efficiency
- The computation cost for consensus algorithm
- The ledger data storage overhead on host

Main Objectives

- Design a secure, self-adaptive, and totally decentralized network architecture
- Enable an efficient, privacy-preserving and secure cooperative training framework on top of distributed IoT hierarchies, consisting of the cloud, the fog and edge devices
- Integrate an optimized and lightweight blockchain fabric to enhance privacy, security and incentive compatible guarantees for FL
- Build an organic system in which FL and blockchain have a mutual reinforced relationship

Contact Information

Web : https://www.binghamton.edu/ece
Email : rxu22@Binghamton.edu
Phone : +1 (607) 338-8444

System Architecture

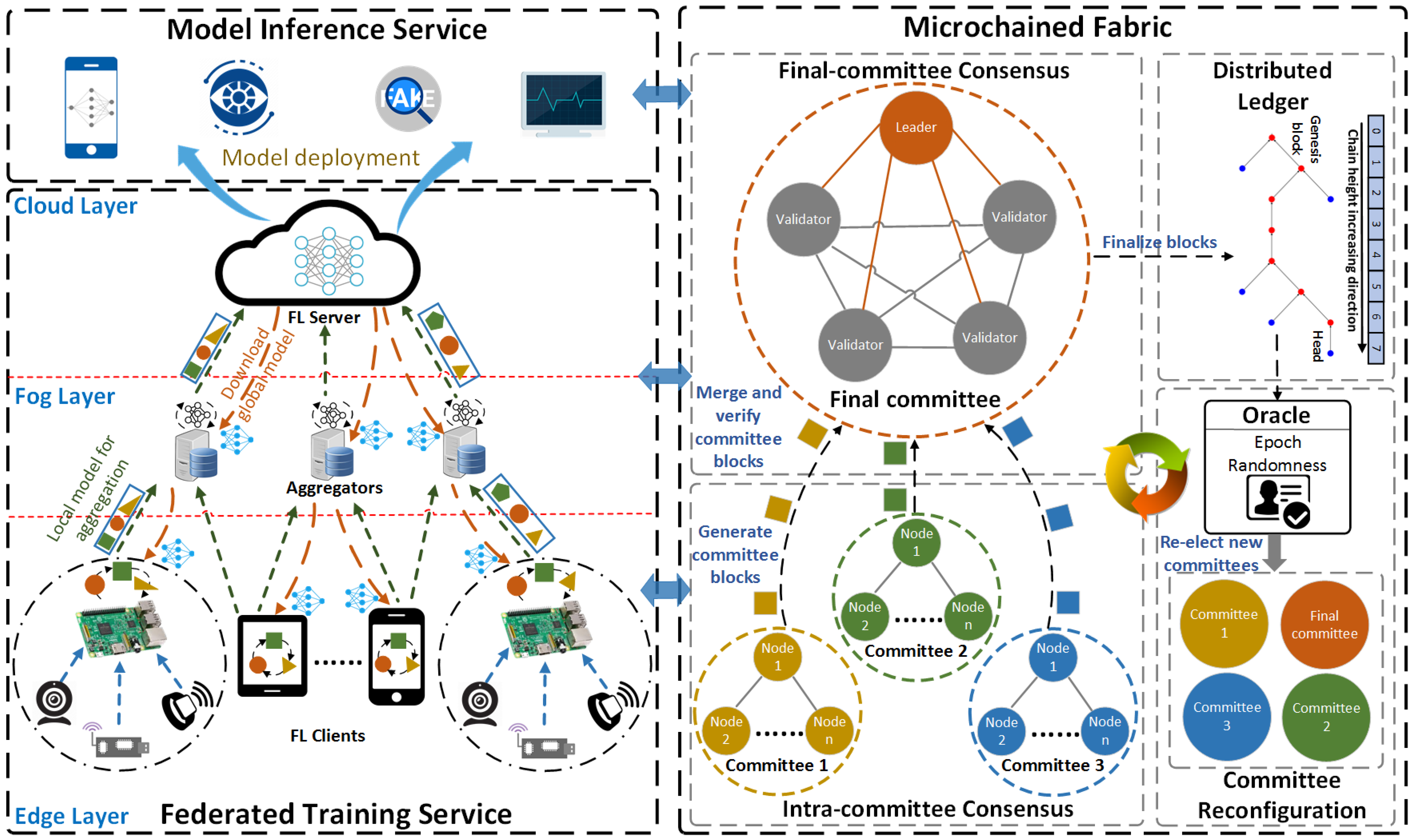


Figure 1 : System Architecture of MicroFL.

Hierarchical FL Framework

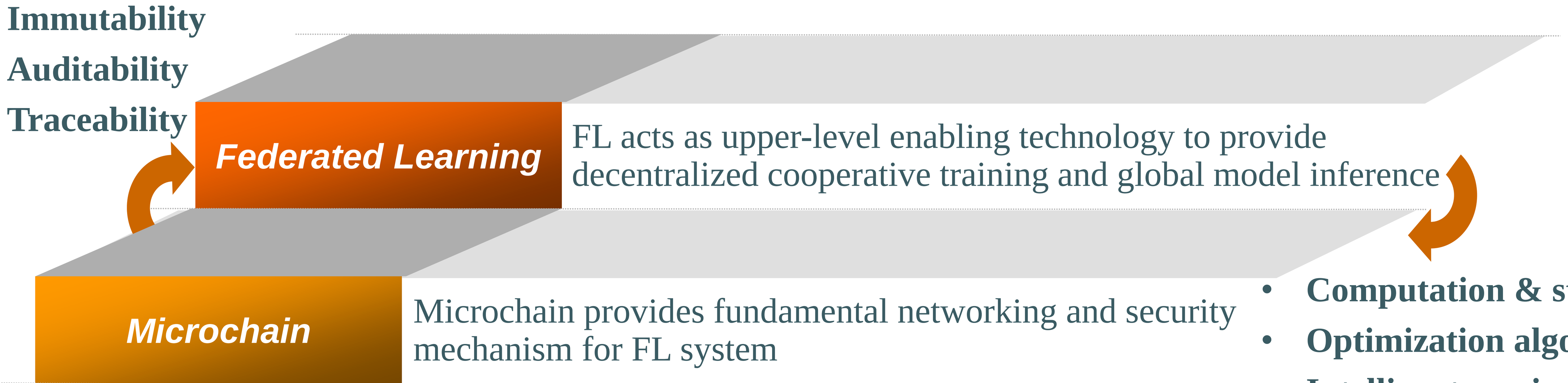
- Hierarchical cloud-fog-edge computing architecture
- Players: FL clients, aggregators and FL server
- Main workflows: Global model propagation (down-stream) and local model aggregation (up-stream)
- Support scalability, flexible management and coordinated central and local decisions for distributed FL service under heterogeneous network and IoT devices

Hybrid Microchained Fabric

- Interconnect key players in FL to enhance user data & model updates protection and multi-party computing security
- Two-level committee consensus protocols offer an efficient, scalable and privacy-preserving distributed ledgers for hierarchical FL framework
- A bias-resistant public randomness mechanism ensures unpredictable and statistical representative committee formation

Design Rationale

- Immutability
- Auditability
- Traceability



- Computation & storage
- Optimization algorithm
- Intelligent services

Microchain Summary

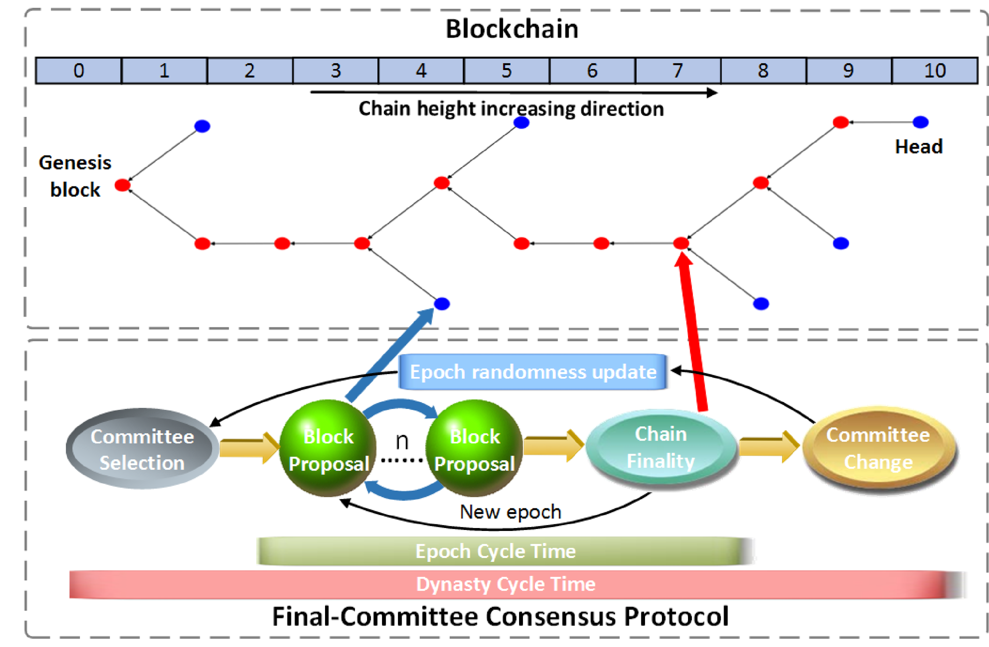


Figure 2: Key Components and Workflows in Microchain [1].

The features of Microchain

Permissioned Network
- Provide basic security primitives, such as public key infrastructure (PKI) and access control
- Handle heterogeneous networks with varying security requirements

Random Committee Election
- Unpredictable committee selection based on unbiased randomness protocol
- Lower communication cost and high throughput for IoT

Efficient Virtual Mining
- A computational efficient virtual mining manner for probabilistic block generation
- Limited computation and storage overhead as executing on IoT devices

Incentive Capability
- Adopt incentive compatibility based on rewarding and punishment strategies
- Helpful to address incentive issues in FL system

References:

[1] R. Xu, Y. Chen, E. Blasch, and G. Chen, “Microchain: A hybrid consensus mechanism for lightweight distributed ledger for iot,” *arXivpreprint arXiv:1909.10948*, 2019.

Ongoing Efforts and Future Directions

Table 1: Configuration of Experimental Nodes.

Device	Dell Optiplex 760	Raspberry Pi 3 Model B+
CPU	3 GHz Intel Core TM (2 cores)	Broadcom ARM Cortex A53 (ARMv8), 1.4GHz
Memory	4GB DDR3	1GB SDRAM
Storage	250G HHD	32GB (microSD card)
OS	Ubuntu 16.04	Raspbian GNU/Linux (Jessie)

Table 2: Network latency for one round of Microchain (In seconds; computed over 50 runs; Setting I:4 nodes; Setting II: 16 nodes)

Operations	Setting I	Setting II
Commit Transaction	0.16	0.25
Block Proposal	0.5	1.7
Chain Finality	1.4	21.5

Table 3: Throughput based on average transactions rate (in M/h: Mbytes per hour)

Block size	Transactions rate
512 K	202
1 M	293
2 M	405
4 M	263

Table 4: Average processing time of running each Microchain operations with 1 M block size (In milliseconds, computed over 50 runs; Setting I: Desktop; Setting II: Raspberry Pi)

Operations	Setting I	Setting II
Verify Transaction	47	179
Mining Block	27	147
Validate Block	358	492
Verify Vote	303	436

	CPU usage (%)
Setting I	10
Setting II	15

Our future work includes but not limited to:

1) Integrating MicroFL with our current smart surveillance research to enable anomalous behavior detection based on Multi-view cameras;

2) Investigating impacts of executing MicroFL in terms of detection accuracy of training algorithm, networking efficiency, data security and privacy protection.