

Baohua Yang

Principal Architect | Agentic AI, Distributed Systems & Security
Bay Area, CA | yangbaohua@gmail.com | [LinkedIn](#) | [GitHub](#) | [Homepage](#)

PROFILE

- Systems architect and technical leader with nearly 20 years of turning research into production systems, from 10 Gbps network security and enterprise blockchain to agentic AI.
- Designs agentic AI platforms end to end: multi-agent orchestration, MCP tool integration, context management, evaluation, and runtime safety; hands-on in Python and Go.
- Early designer of Hyperledger Fabric; founding contributor to Hyperledger and three-term TSC member; 10 granted patents, 20+ papers, and open-source books with 100M+ reads.

TECHNICAL SKILLS

- **Agentic AI:** multi-agent orchestration (LangGraph, supervisor pattern), MCP, A2A, RAG, NL2SQL, context and memory management, evaluation and telemetry, LLM inference, fine-tuning (LoRA).
- **Security:** prompt-injection and jailbreak defense, NVIDIA NeMo Guardrails, OPA policy-as-code authorization, RAG data protection, PKI and X.509 identity, network security.
- **Systems:** Go, Python, C/C++; Kubernetes operators, multi-tenant control planes, consensus (Raft), high-performance packet processing.

EXPERIENCE

Principal Architect, *Oracle*

Aug 2017 – Present

- Own architecture for Oracle Blockchain Platform and Oracle TSAM, serving Fortune 500 customers (~\$200M ARR, ~50 engineers); partner with the Database AI team on agents.
- Architected and shipped an AI agent for TSAM that answers natural-language questions over monitoring data and diagnoses failures; raised accuracy from ~30% to 90%+ and cut latency 50%.
- Built the agent's safety layer: NeMo Guardrails input, output, retrieval and tool rails against direct and indirect prompt injection, jailbreaks and data leakage; OPA policy for scoped tool permissions.
- Designed a supervisor-based multi-agent architecture on a LangGraph-style framework, replacing fixed call chains with runtime orchestration; drove its adoption by database engineering.
- Influenced the Oracle Select AI Agent roadmap (RAG, context management); selected for Oracle's AI Champion program (~100 company-wide).
- Architected three generations of Oracle Blockchain Platform (VMs, containers, Kubernetes) after winning Group VP buy-in; wrote its operator and cut provisioning from minutes to seconds.
- Scaled the platform to 10,000 TPS and several hundred tenants; made the case for continued fintech investment, which led to a new token service on Hyperledger Besu.
- Led resolution of the hardest production failures, e.g. a Fabric consensus freeze (fail-closed fix shipped upstream) and state-database corruption (10K+ TPS Go ledger parser).

Research Scientist, *IBM Research*

Jan 2013 – Aug 2017

- Early designer and core developer of Hyperledger Fabric, one of the first enterprise blockchain platforms; led the applied research behind it.
- Architected IBM's enterprise blockchain platforms in Go (X.509 identity, CA hierarchy, revocation, endorsement policy), sustaining 1,000+ TPS per cluster across hundreds of production clusters.

OPEN SOURCE & COMMUNITY

Hyperledger Foundation TSC Member (now LF Decentralized Trust) 2017–2019; 2020–2021

- Founding contributor; shaped technical strategy and governance across Hyperledger over three terms and contributed to ISO/TC 307 blockchain standardization.
- Maintainer of Hyperledger projects; community mentor and technical writer.

EDUCATION

Ph.D. in Control Science and Engineering, *Tsinghua University* Sep 2007 – Jan 2013

Research: high-performance networking and security; built a 10 Gbps UTM system.

IBM Ph.D. Fellowship Award (9 winners, 2011).

Visiting Scholar, *EECS, University of California, Berkeley* Sep 2010 – Sep 2011

Research: software-defined and data-center networking.

Bachelor of Science and Engineering, *Tsinghua University* Aug 2003 – Jul 2007

PATENTS

- 10 granted patents in distributed ledgers, cloud, and networking, including [US 11,822,538](#), [US 11,741,075](#), [US 11,546,425](#), and [US 10,983,816](#).
- 3 AI patent filings (2024–2026): long-context management for agentic systems, enhanced NL2SQL querying, and AI knowledge-base protection.

SELECTED PUBLICATIONS

- LazyCtrl: A Scalable Hybrid Network Control Plane Design for Cloud Data Centers. K. Zheng, L. Wang, B. Yang, Y. Sun, S. Uhlig. IEEE Transactions on Parallel and Distributed Systems, 28(1):115–127, 2017.
 - Keep Forwarding: Towards K-link Failure Resilient Routing. B. Yang, J. Liu, S. Shenker, J. Li, K. Zheng. IEEE INFOCOM 2014.
 - Practical Multi-tuple Packet Classification using Dynamic Discrete Bit Selection. B. Yang, J. Fong, W. Jiang, Y. Xue, J. Li. IEEE Transactions on Computers, 63(2):424–434, 2014.
 - Data-Driven Network Connectivity. J. Liu, B. Yang, S. Shenker, M. Schapira. ACM HotNets-X, 2011.
- 20+ peer-reviewed papers in total; full list on [Google Scholar](#).

SELECTED BOOKS AND TECHNICAL GUIDES

- Docker Container Technology in Action (2015, 4 editions); Blockchain: Principle, Design and Applications (2017, 2 editions), China Machine Press.
- Open-source books [Docker Practice](#) (26K+ GitHub stars) and [Blockchain Guide](#) (7K+), 100M+ reads; 4,800+ GitHub followers.
- Open-source AI guides (2026): Agentic AI, Harness Engineering, AI Security, Context Engineering, LLM Internals.