

Building Trusted Agentic AI

User Intent-driven & Decentralized Mechanism

Li Li (aka. Thomas), Huawei Technologies Düsseldorf GmbH

Workshop: Designing Trust Management for Agentic AI, Geneva Switzerland

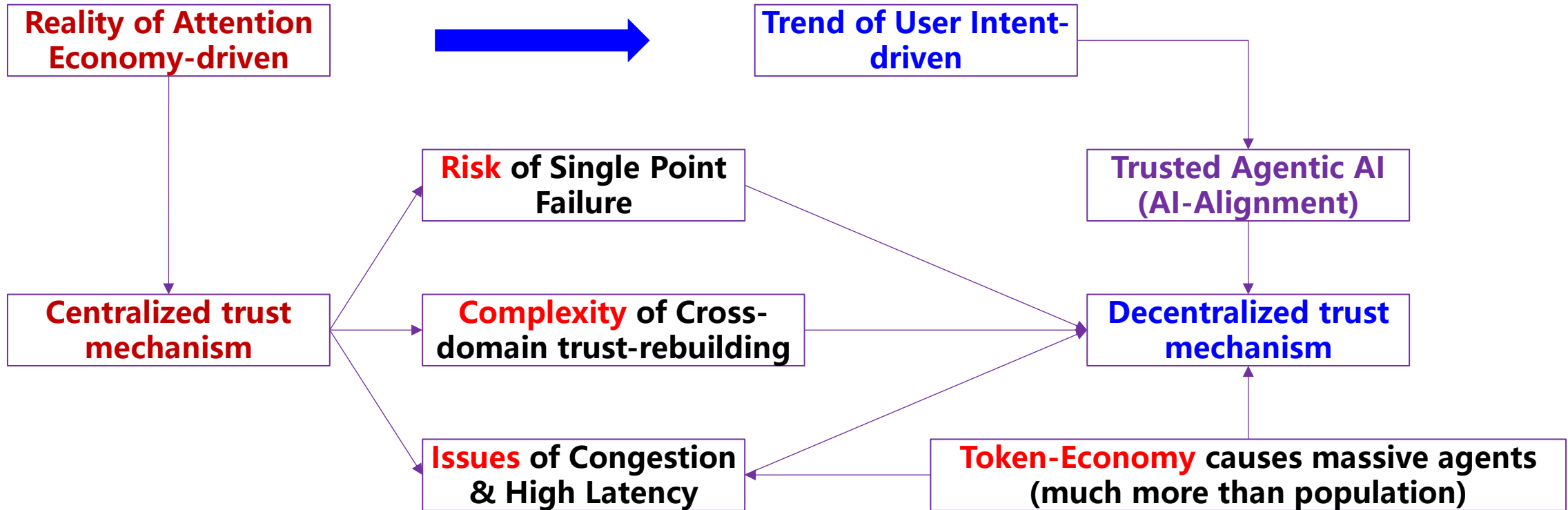
AI for Good Summit, 7-10 July 2026

Web access is evolving to User Intent-driven

User perception	Attention Economy-driven	User Intent-driven
Free of charge	Access Web through Platform	Access Web through User Agent
Pay for	Applications on platform & some platform functions (in few cases)	Resources consumed by user agents: Token, computing power, storage, 3 rd party tool/data/agent, etc.
User input	Simple intents : make friends, get information, buy goods, publish self-media, etc.	Simple intents + Complex intents : Plan action, do professional job, design solutions, code, etc.
Pros	Platform free (paid by Ad customers)	Generate income , protect autonomy
Cons	Risk of privacy leaking , risk of algorithm manipulation (lose autonomy)	Cost could be out of control, strong and clear user intent required
Fitted scenario	Cost center mode : Convenient for living, tolerant on part of personal data being controlled by others	Profit center mode : Convenient for working, zero tolerant on user data & user agents being controlled by others

- ◆ **Coexisting & Evolving**: Technically Attention Economy-driven and User Intent-driven can coexist, but AI-replacing effect will facilitate evolving to User Intent-driven Web with dramatic speed.
- ◆ **Advantage**: Comparing platform, User Agent has more powerful function, more personalized service, no ad interruptions, better privacy protection, and could generate income. It's the better entrance of Web in AI time.
- ◆ **Challenge**: **Trusted Agentic AI (AI-Alignment)** is crucial for achieving **User Intent-driven**.

Trust mechanism is moving to Decentralized



- ◆ **Centralized mechanism:** Platform control user' s identity, data, credentials, applications, tools, LLMs, AI agents, publications, everything. **Zero-Trust framework** protects platform, platform "protect" user.
- ◆ **Decentralized mechanism:** User control its own identity, data, credentials, applications, tools, LLMs, AI agents, publications, everything. **MAX-Trust framework** protects all users and agents.

Goal: Build a Multi-party, Agentic, and eXtensible next-generation Trust Framework

Multi-party Trust

M-Address the Delay and Single Point of Failure Issue

Single Point -» Multiple Points
Centralized -» Distributed

Agentic Trust

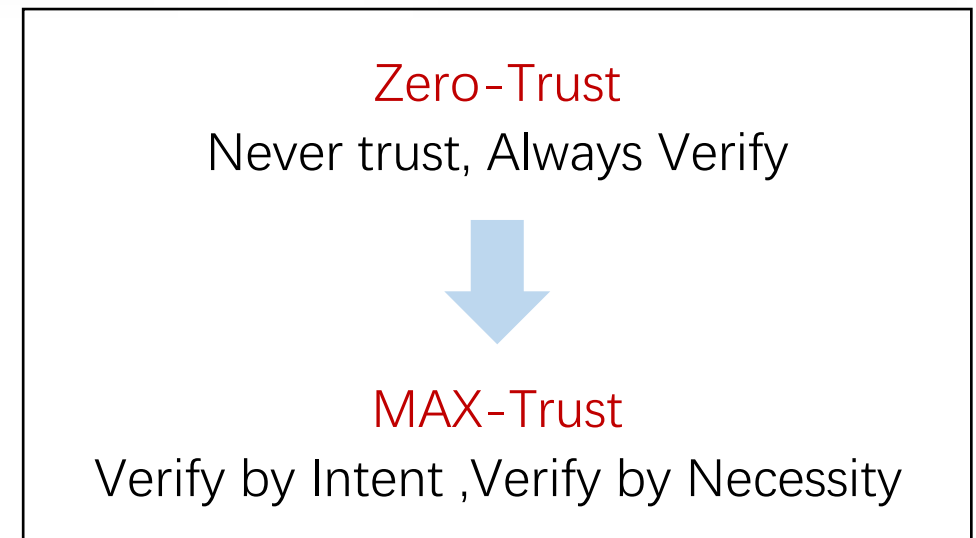
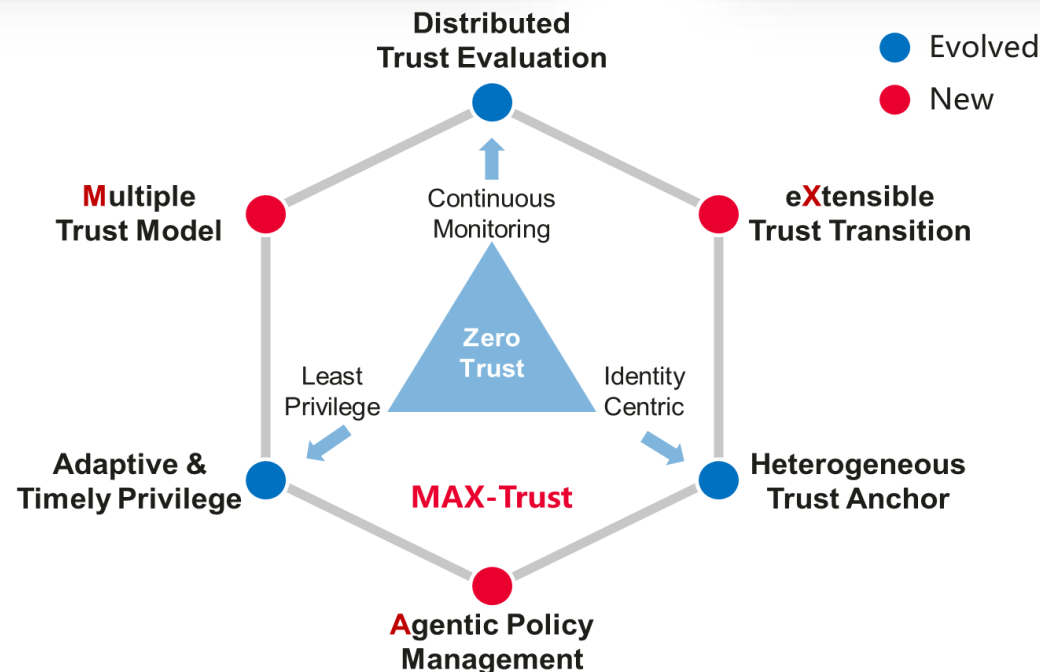
A-Address the Efficiency and Uncertainty Issue

Identity -» Intent
Fixed -» Flexible

eXtensible Trust

X-Address the Breadth and Compatibility Issue

Single-Domain -» Multi-Domain
Singularity -» Diversity



Slogan: Building Maximal Trust for Users

Thank you !