Evolving to User Intent-driven Web

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

W3C 2026 AC, Hangzhou, China & Hybrid

April 20-22 2026

Evolving to User Intent-driven

User perception	Attention Economy-driven	User Intent-driven
Free of charge	Use **platform** to access Web	Use **personal agent** to access Web
Pay for	**Applications** on platform & some platform functions (in some cases)	**Resources** consumed by personal agents: Token, computing power, storage, 3rd 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 personal data & personal agent 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.
- **Web entrance**: Comparing platform, personal 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.

Physical Identity Authentication

Physical Identity

Fingerprint
Palmprint

Finger vein
Palm vein

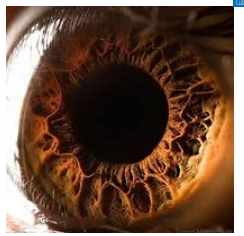
EU DI Wallet

3D Face
Live Face

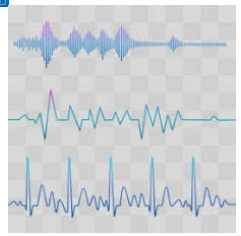
Web Protocol

Linkage

China Net-ID



Iris



Voiceprint

Combined Biometric Recognitions

Official Digital Identities

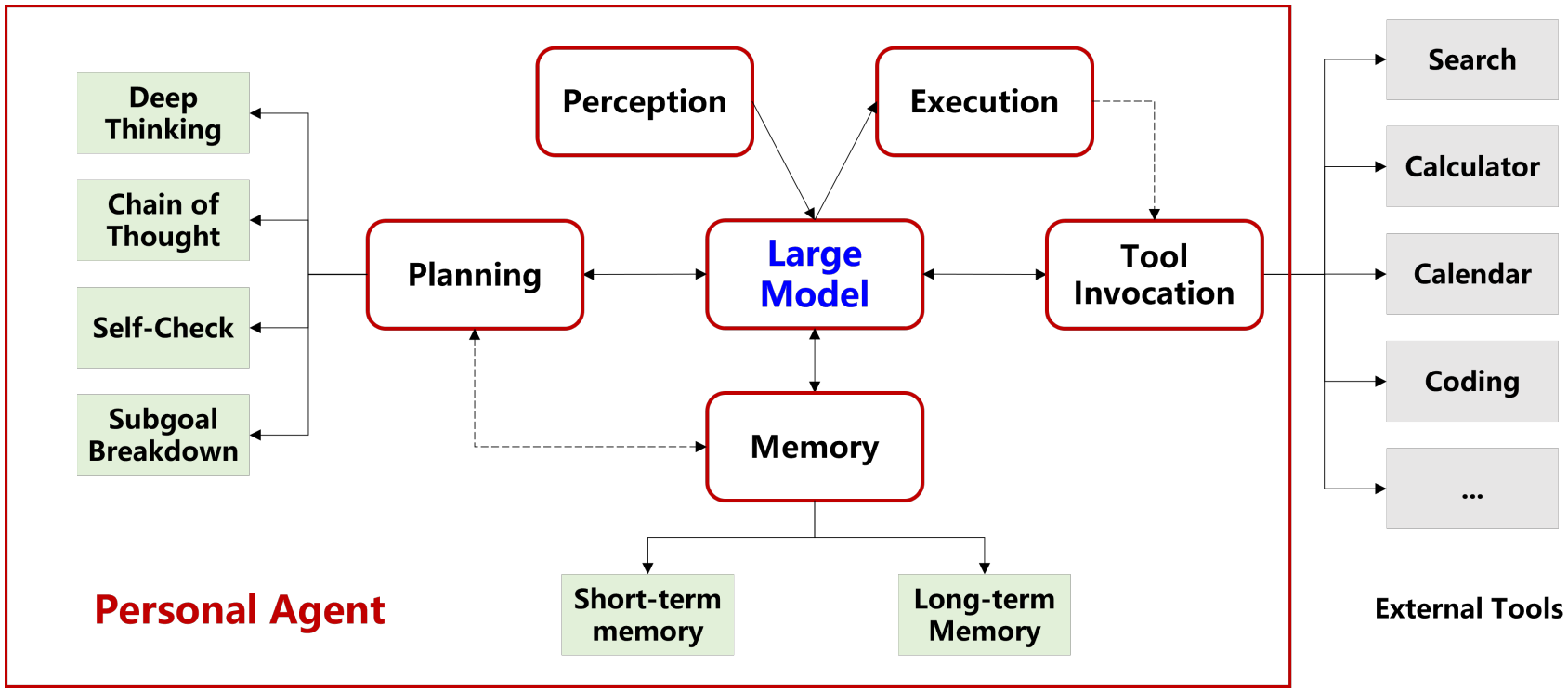
- **Biometric Recognition** (AI-enabled) is the most convenient way to authenticate **Physical Identity** of users and already very secured with technical improvement and combined usage.
- **Web protocol** linking **Official Digital Identity** (e.g. EUDIW, China Net-ID, Crypto-enabled) with biometric recognition will be a necessity. The protocol **security design** is challenging when using **Public Devices**.

Personal Agent as Internet Entrance

EU DI Wallet

Web Protocol

Bi-Auth.



- **Personal Agent** can be powerful enough to integrate all Web Entrance functions: Browser, Search Engine, Chatbots, Social Networking, Self Media, Email, Messaging, Relationship Management, UGC, etc.
- **Web protocol** linking User's **Official Digital Identity** with the **Personal Agent** is important to lock unique and legal access to Internet. **Bilateral authentication** is needed.

Human evolving along with AI

EU DI Wallet

Web Protocol

Intent

Personal Working Agent

Personal Living Agent

Web Protocol

Digital World

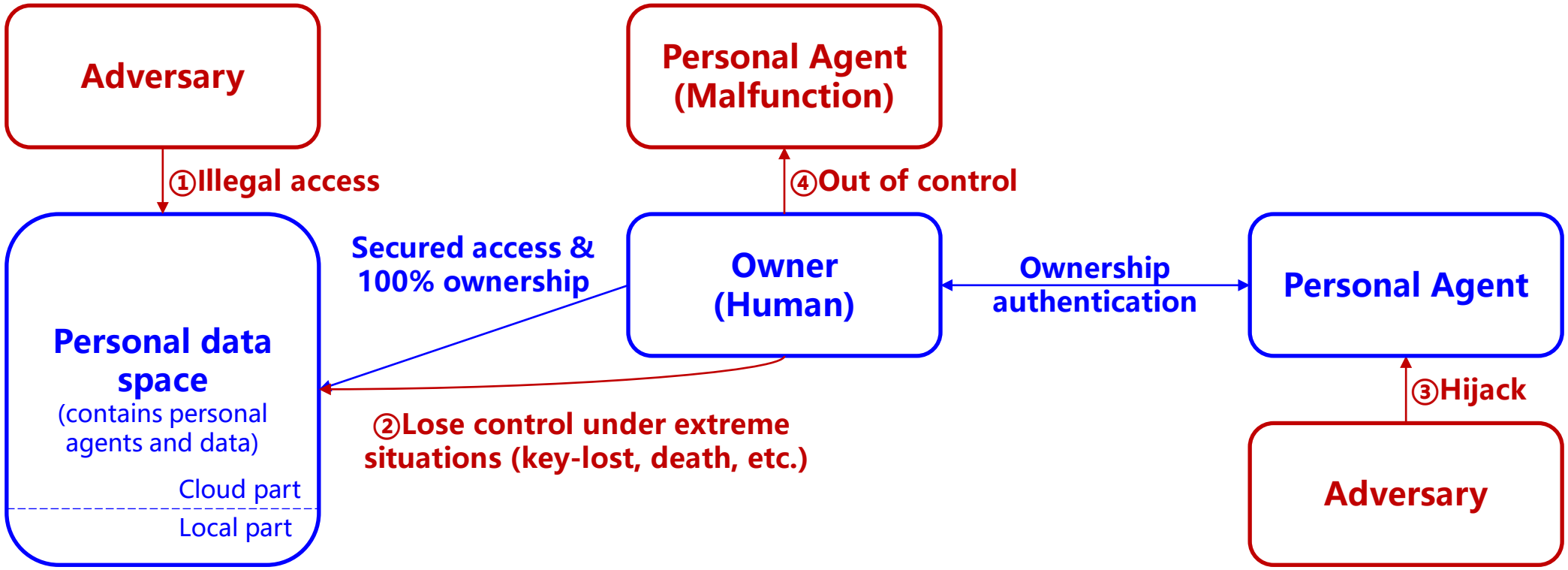
Personal Entertaining Agent

Personal Health Agent

Physical World

- **Personal Agent** will cover all aspects of human life (Working, Living, Entertaining, Healthcare, etc.) and replace almost all repetitive physical & mental activities from human. **AI-Alignment** is essential.
- **Human being** will be free from repetitive activities and can focus on Innovation, Decision-making, Trust-building and Emotional-connecting activities which are difficult or even impossible to be replaced by AI.

Security requirements in Agent Plebification

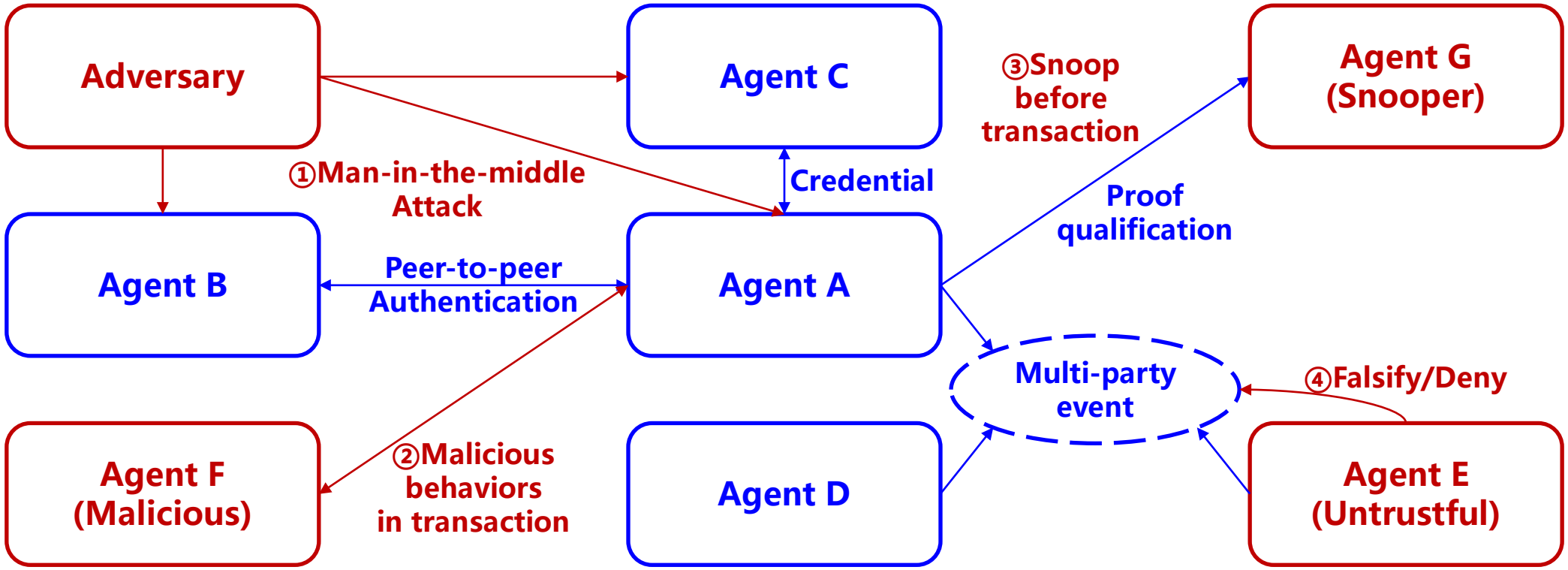


①Highly secured personal data space
②Data protection under extreme situations

③Agent ownership authentication
④Frozen agent behavior boundary

④Agent right administration
……

Security requirements in Agent Decentralization

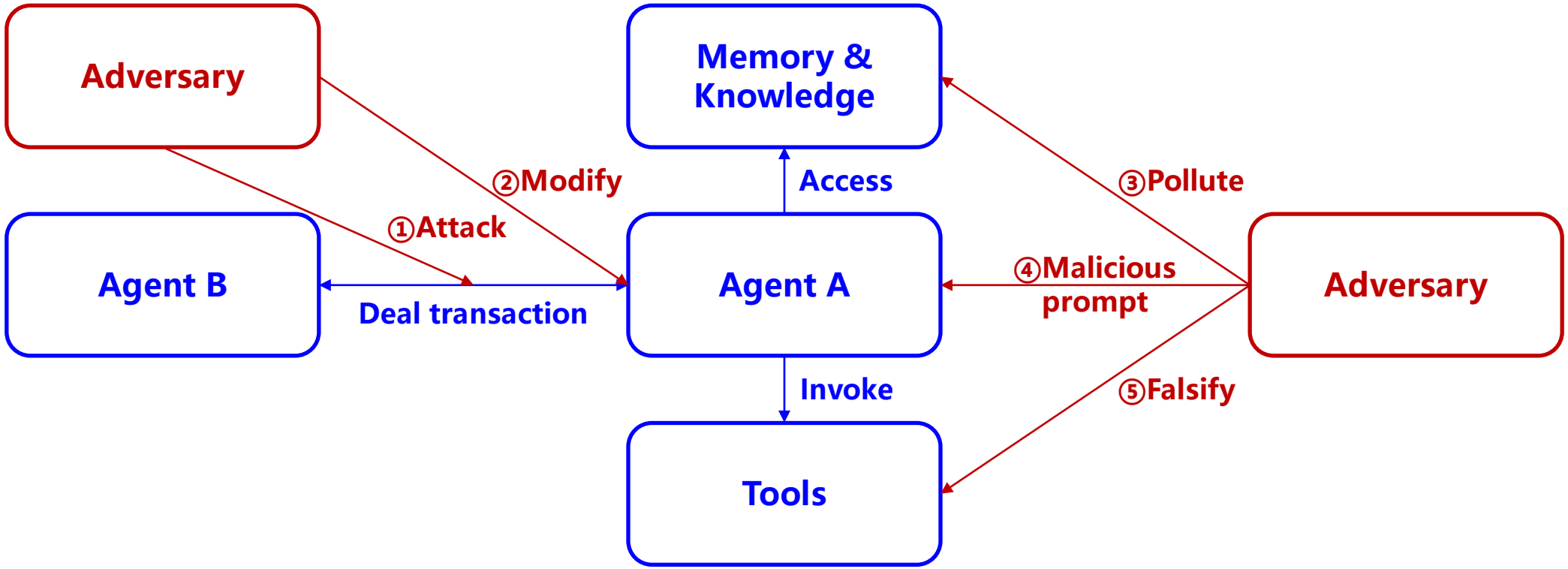


①Decentralized identity authentication
①Credential verification & delivery

②Accountability on malicious behaviors
③Zero knowledge proof

④Multi-party computing
④Un-falsified consensus building & retrieving
……

Security requirements in Agent Networking



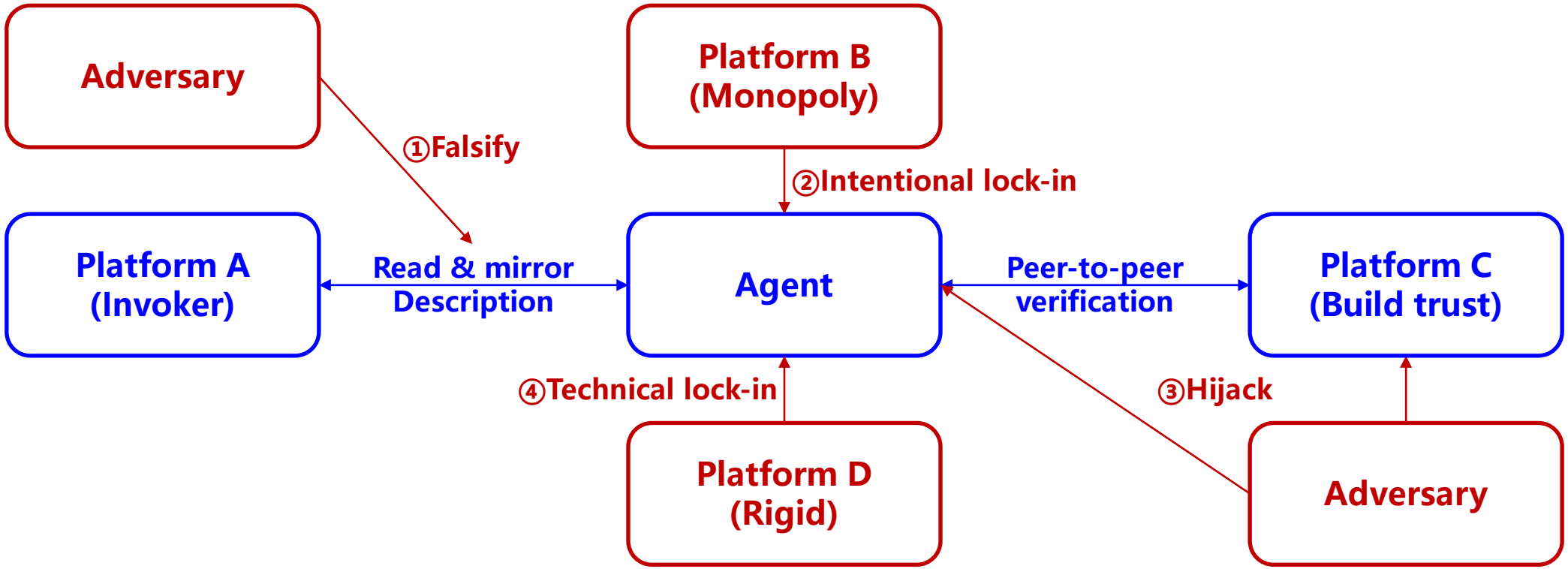
①Protect transaction
②Prohibit illegal modification
④Defend prompt injection attack

④Prevent logic malfunction
⑤Identify fake tools

③Isolate pollution on memory & knowledge
④Avoid privacy leaking
……

Note: Green characters means new requirements could not be fulfilled by existing cybersecurity solutions.

Security requirements in Agent Decoupling



①Anti-falsify of agent description
②Avoid platform lock-in

③Heterogeneous trust root
③Peer-to-peer trust verification

④Intelligent policy configuration
……

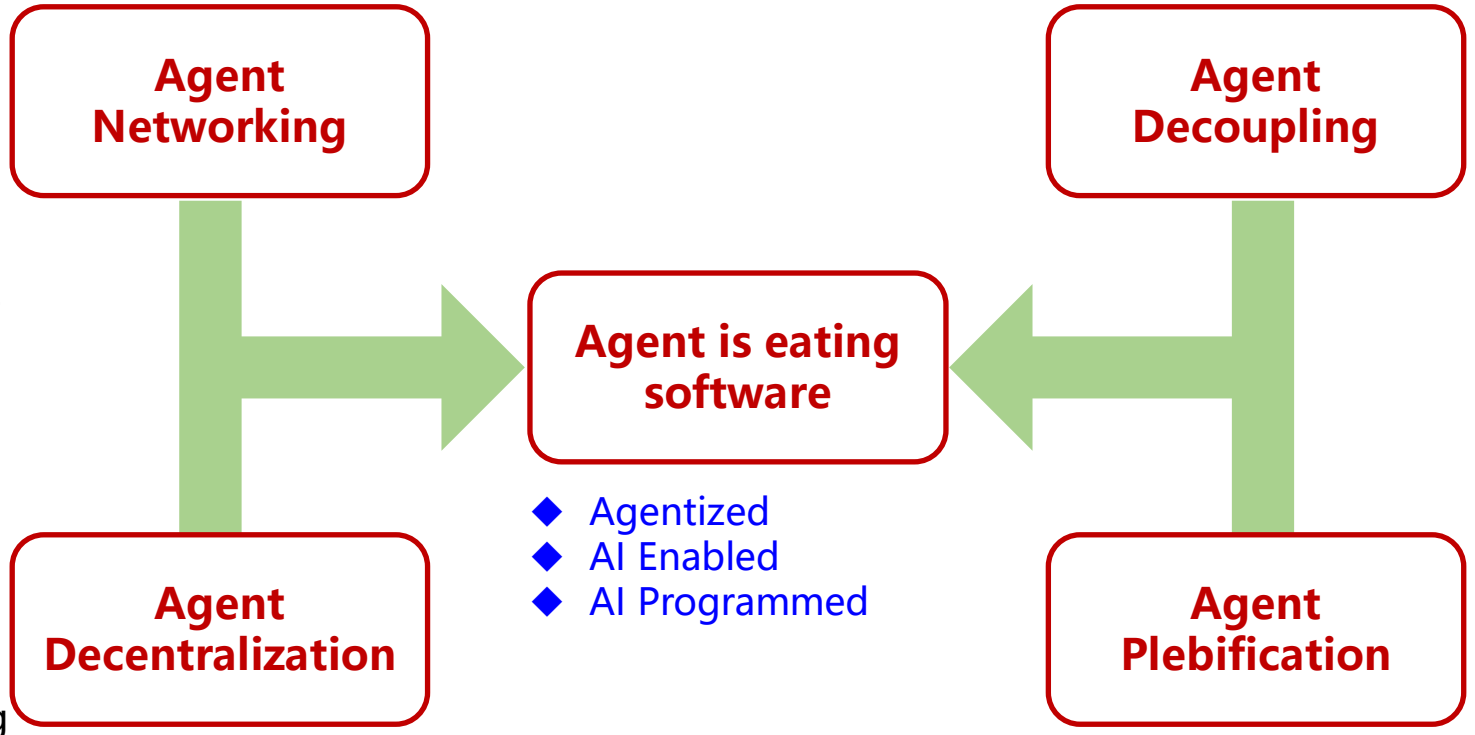
Panorama of security requirements

- Protect transaction
- Prohibit illegal modification
- Defend prompt injection attack
- Prevent logic malfunction
- Identify fake tools
- Isolate pollution on memory & knowledge
- Avoid privacy leaking

……

- Decentralized identity authentication
- Credential verification & delivery
- Accountability on malicious behaviors
- Multi-party computing
- Un-falsified consensus building & retrieving
- Zero knowledge proof

……



- Anti-falsify of agent description
- Avoid platform lock-in
- Heterogeneous trust root
- Peer-to-peer trust verification
- Intelligent policy configuration

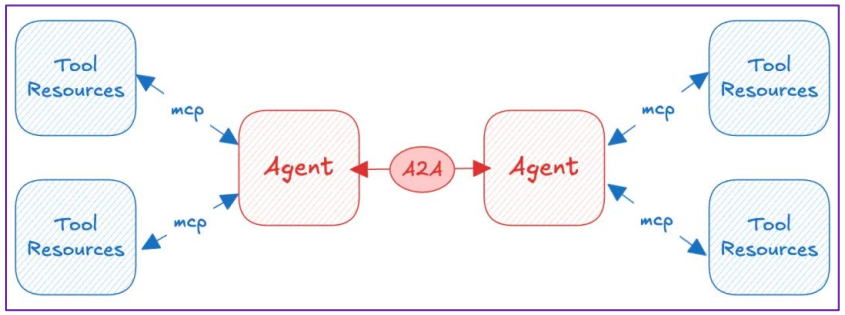
……

- Highly secured personal data space
- Data protection under extreme situations
- Agent ownership authentication
- Frozen agent behavior boundary
- Agent right administration

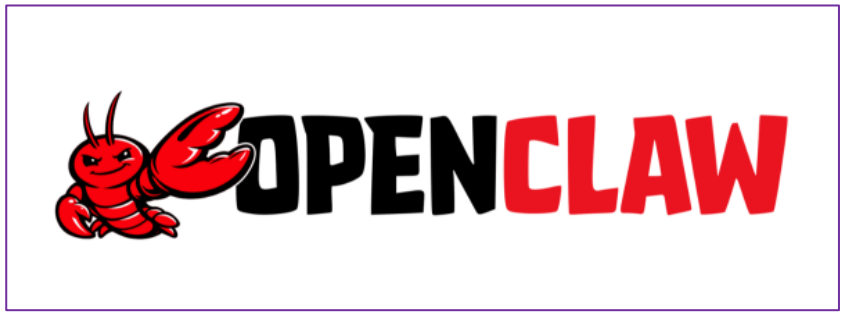
……

Cryptographic algorithm (including PQC) is the last defense line facing adversaries enhanced by AI and quantum computing.
Chip-level key-management is important for Agent security.

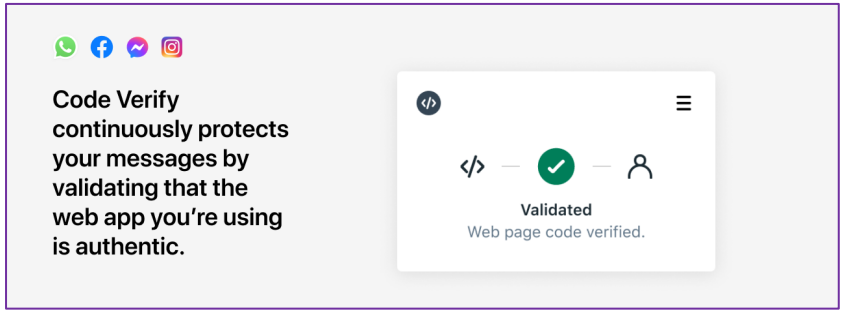
Testing & Verification are crucial



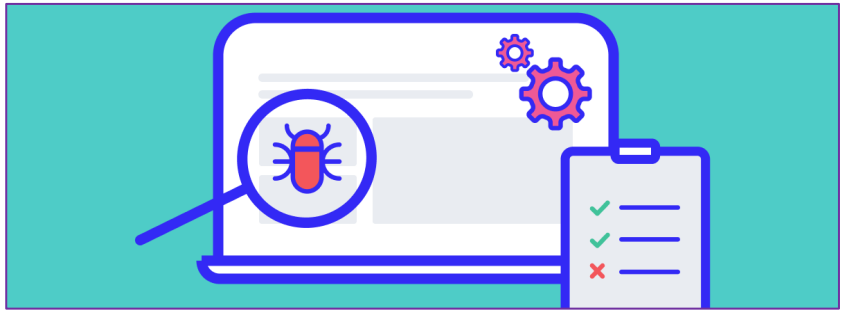
Developing: From signaling to Intent-based, much more simplified



Programming: From hand-made to AI-generated, much more efficient



Verification: On-the-fly continuous protocol-code authentication



Testing: Last chance before uploading, much more careful than ever

Take-aways

- **Trend:** User Intent-driven Web using personal agent as the entrance is better than Attention Economy-driven Web using platform as the entrance, especially in AI time.
- **Challenge:** Evolving to User Intent-driven Web needs to develop a lot of new protocols. The challenges and gaps are huge.
- **Cybersecurity:** When ordinary users facing Internet through personal agent without supporting of platform, the cybersecurity design of protocols is crucial. Keeping AI-Alignment with user intent is the core target of Web agent security.
- **Cryptography:** Whatever the solutions would be, cryptographic algorithms will be the bottom-line because in theory the algorithm would be the only thing that AI can not break. Chip-level key-management is a necessity for Agent security.
- **W3C:** AI-coding will make zero distance from protocol to code, very soon no traditional open source society is needed. Besides developing new protocols, W3C may need to put more effort on testing and verification of protocol-codes.

Thank you !