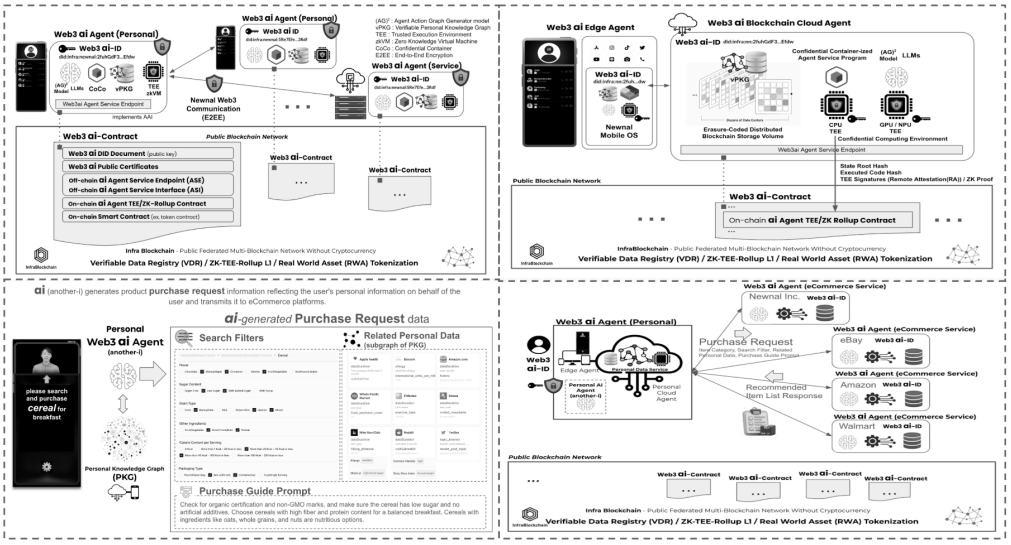
Web3 ai **Newnal** - Technology 2

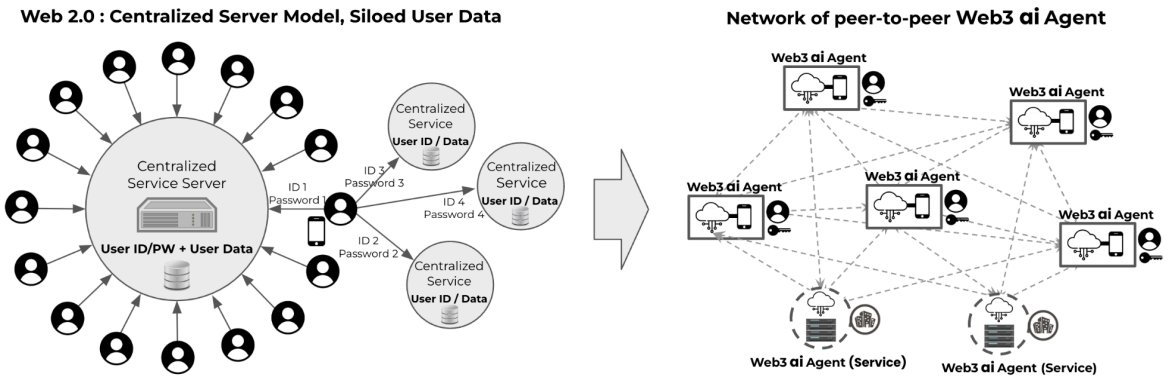
Web3 ai OS

Appless OS that removes the need to manually run apps



What is Web3 ai Agent and Newnal ai OS?

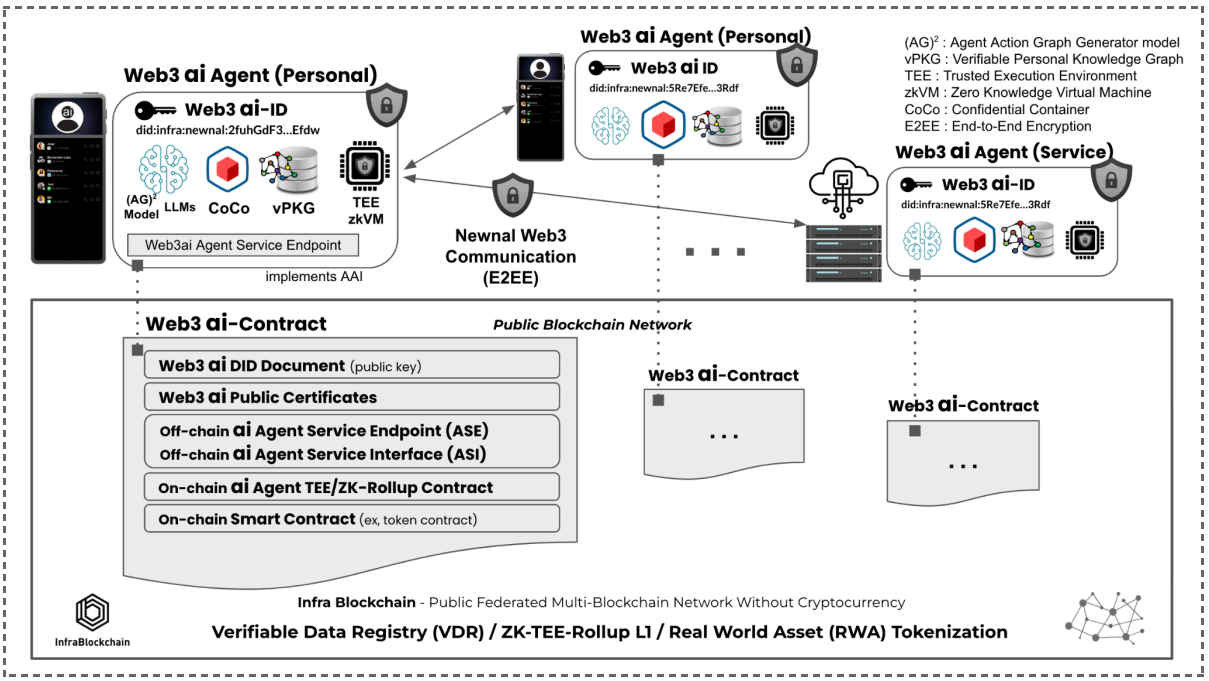
Software in the AI era will shift away from the existing “central server <-> client application”-oriented Web 2.0 IT system architecture and change to a way in which all software exists in the form of decentralized AI agents. All individual users, as well as existing web service providers, will own their AI agents, each operating autonomously. The existing cloud SaaS paradigm gradually disappears and changes to the *Decentralized Autonomous AI Agent Network* paradigm. Individual users can store all their personal data and operate their own AI agents in their mobile devices and a private cloud space supporting confidential computing only accessible through the user’s blockchain ID. These personal AI agents can perform creative activities based on personal data, search for personalized information, perform tasks (shopping, scheduling, taxi calling, remittance, etc.) on behalf of individual users. The AI exists as "another-i" (ai) of the user in the information space.



These individuals' *Web3 ai agents* can provide services for other people or other *Web3 ai agents* not only for the user who owns the ai, and can autonomously use services provided by other *Web3 ai agents*. People can talk to the other people's ai, and companies can deliver advertisements and information to an individual's Web3 ai, not an actual user, and the Web3 ai can filter and refine the information for the real user who owns Web3 ai. Famous artists can service their Web3 ai based on their data so that fans can communicate with their Web3 ai. Companies will move away from providing *app-oriented* information services designed to be used directly by real people, not by personal ai, and build their Web3 ai agent back-end services that interact with people's Web3 ai. In the Web 2.0 paradigm, individuals installed countless apps and used the apps directly by humans. But, In the Web3 ai paradigm, users communicate with their Web3 ai agents, and the Web3 ai communicates with numerous Web3 ai agent services that exist on the Internet on behalf of the user to achieve the best user experience.

iOS and Android mobile OS, which were at the center of the Web 2.0 mobile IT revolution, were operating system software for running mobile applications of Web 2.0 paradigm on user mobile devices. **Newnal ai OS** is the **blockchain-based network protocol and system software in the Web3 ai paradigm** that enables decentralized AI agents of individual users and service providers to be implemented on mobile devices and cloud servers, and to be securely connected and interoperable with each other.

Decentralized Newnal Web3 ai Agent Network Built Upon Blockchain-based Web3 ai-ID and Web3 ai-Contract



Web3 ai-ID

Web3 ai agents do not exist alone, but must communicate and collaborate with numerous public and private Web3 ai agents on the Internet. Web3 ai agents must have an ID system that can securely identify and authenticate each other. Web3 ai agents cannot use ID systems of Web 2.0 paradigm such as ID/Password system and OAuth-based SSO(Single-Sign-On), where authentication information and sensitive personal data are stored and managed on central servers of big tech companies. If the Web 2.0 ID system is applied to ai agents, it will hand over ownership and control of Web3 ai agents from individuals and companies who own the ai agents to the centralized platforms owned by for-profit big tech companies such as Google, Apple, Meta, and OpenAI, and it will have serious consequences that sensitive personal data and corporate data can be leaked from the central servers of big tech companies. Web3 ai's ID system should adopt blockchain-based *Decentralized Identifiers (DID)* web standard technology so that the owners of Web3 ais can have sovereignty over the IDs and data of Web3 ai by using blockchain ID (asymmetric cryptographic key) generated from users' devices without relying on central server systems. Through the blockchain ID, users and Web3 ai agents can create cryptographic signatures to authenticate their ownership of the ID themselves, and

communicate with other users and Web3 ai agents in a way that ensures complete security by not leaking personal information to central servers or network equipment. When personal data of Web3 ai agents are created and stored in the form of VC (Verifiable Credentials), a DID-based web standard technology, the data source (creator) information and Web3 ai's DID are cryptographically bound to the data itself, so the data processed by Web3 ai agents cannot be forged and altered and the source of the data can be verified through the blockchain. The more personal data in VC format issued by trusted institutions (government agencies, companies, medical institutions, etc.), the more reliable a Web3 ai's ID becomes. By creating a Zero-Knowledge Proof that a number of trusted organizations cryptographically signed user's data in VC format without exposing sensitive personal data, the Web3 ai agent can prove the reliability of its DID. In the process of connecting and interacting with a Web3 ai agent the identity of the currently connected Web3 ai agent can be immediately authenticated through the blockchain by using DID/VC technology, thereby safely protecting users from deep-fake, spam, and voice phishing. The public identity of an ai agent who registered their public identity certificates in *Web3 ai-Contract* on blockchain can be immediately verifiable, or when an ai agent is accessed, by inquiring private identity certificate (VC) in peer-to-peer connection context, the peer agent's identity can be verified through blockchain in real time.

Web3 ai-Contract

Owners of Web3 ai-ID can register Web3 **ai-Contract** on the public blockchain to disclose the existence of their Web3 ai agents. Traditional smart contract technology is limited to deploy and execute smart contract codes on blockchain, but Web3 ai-Contract expands existing smart contract technology to register Web3 ai's DID information and public certificate information, and register information about Web3 ai agent services operating off-chain, and enable the ai agent service operation to be verifiable through the blockchain.

By exposing the Web3 ai agent's DID information and public identity information on ai-Contract on-blockchain, anyone can search for public ai agents. With access rights, anyone can use the published ai agent service features and communicate with the ai agent. By disclosing where one's Web3 ai agent service is being serviced (**Web3 ai Agent Service Endpoint**, ASE) and what service functions are implemented on agent (**Web3 ai Agent Service Interface**, ASI) registered on ai-Contract, other ai agents can implement useful ai agent services for their users by orchestrating open ai agent services. In addition, proof data verifying that an Web3 ai agent service implementation running off-chain is performing the open source AI agent operations without leaking personal information on

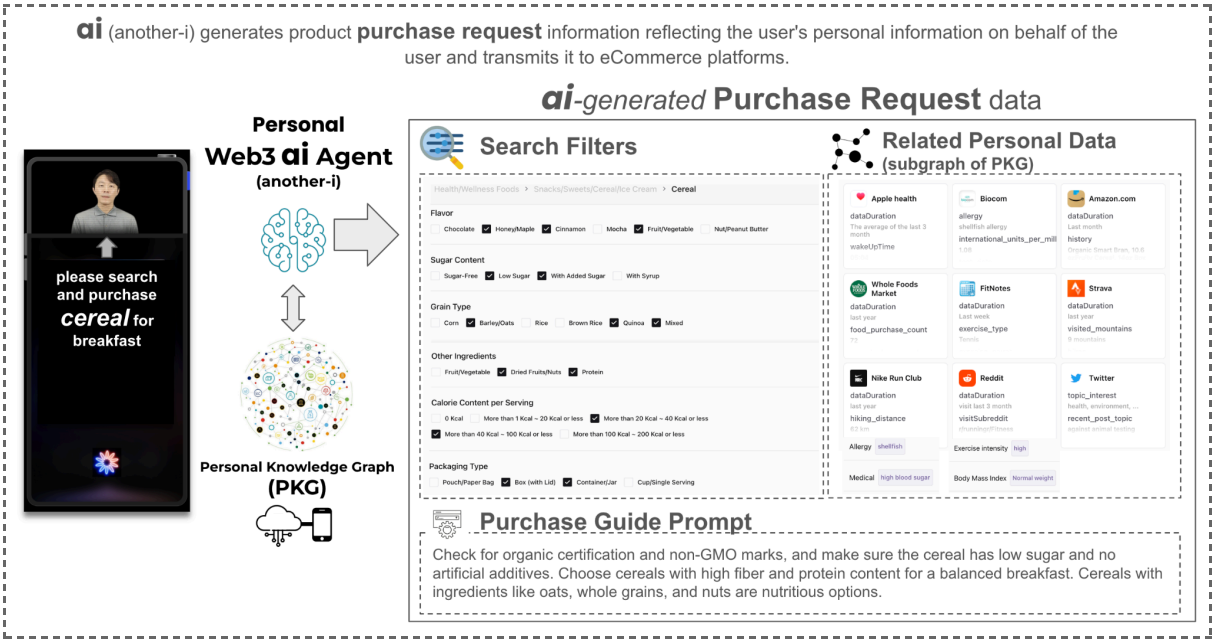
server-side are continuously registered on the **TEE/ZK Rollup Contract**. This ensures that the ai agent is running in a *verifiable confidential computing environment* that does not leak sensitive personal information. Web3 ai-Contract supports traditional smart contract features, allowing Web3 ai-ID owners to deploy token contracts that manage ownership of the Web3 ai agent and equity in the revenue of the Web3 ai agent service. The Web3 ai agent service may be set as a paid model, and agent service usage fees may be settled through tokens on the blockchain.

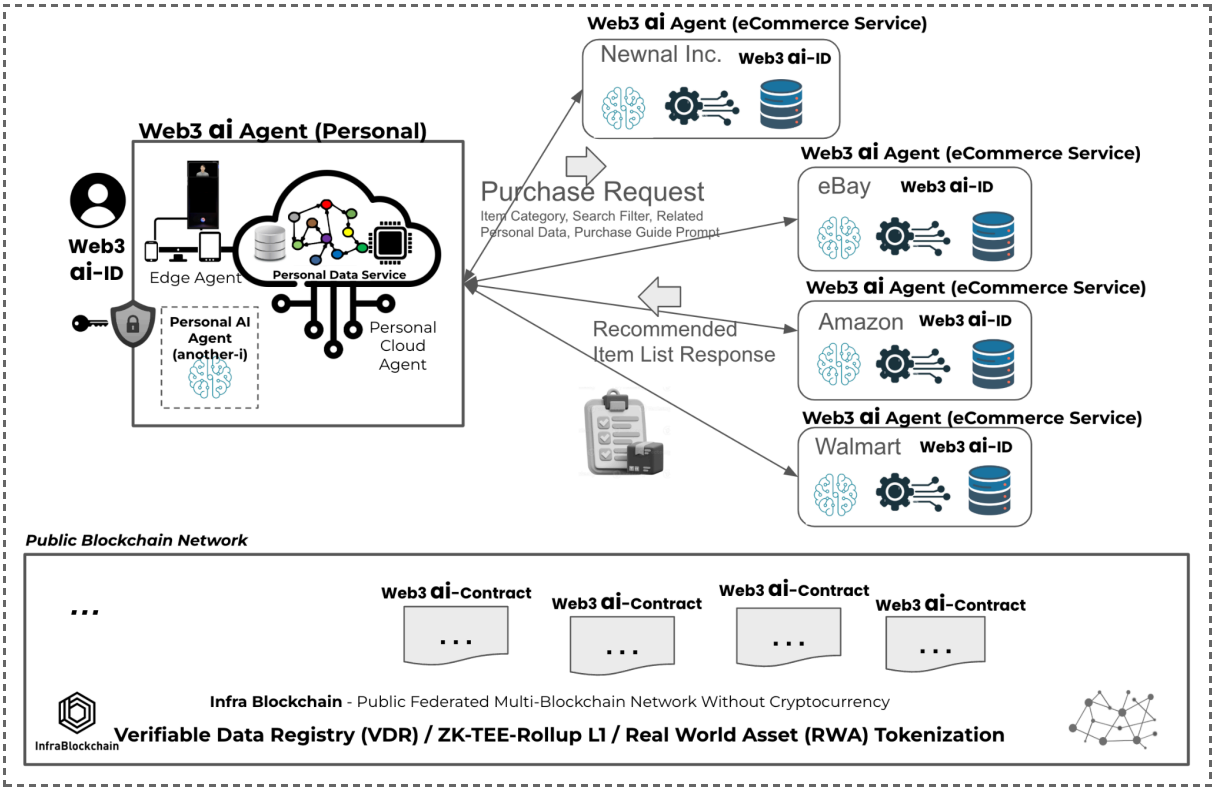
Blockchain-based Newnal **Web3 ai-ID** and **Web3 ai-Contract** technology enable the establishment of an open AI agent ecosystem that makes AI agents running in a decentralized and verifiable confidential computing environment interoperate with each other.

Web3 ai-Contract component		*Features*
Web3 ai DID Document		• Verifiable DID Data Registry containing public keys controlled by ai-ID owner
Web3 ai Public Certificates		• List of public certificates in VC formats issued by trusted entities that contain public information about Web3 ai • If an ai agent owner wants to disclose the identity of the agent (e.g., the ai agent of a company, public institution, or public figure), public identification VCs issued by trust organizations selectively registered on blockchain
Web3 ai Agent Service	**Off-chain Web3 ai Agent Service Endpoint (ASE)**	• URL of mobile devices or cloud server that provide ai agent service implementing the specified ai Agent Service Interface (ASI)
	Off-chain Web3 ai Agent Service Interface (ASI)	• Service interface specification of Web3 ai Agent Service being serviced off-chain • ai Agent Service Interface Types ○ Natural Language Chat Interface ○ Audio/Video Call Interface ○ RPC(Remote Procedure Call) Interface ○ Publish-Subscribe-Notify Interface • It's possible to Import and reuse the same ASI specification already published in other ai-Contract
		• Register TEE's RA(Remote Attestation) hardware

	On-chain Web3 ai Agent TEE/ZK-Rollup Contract	cryptographic signatures to verify that the ai agent system operating off-chain has run the Confidential Contained Program on the TEE hardware • Register ZK proofs about whether the ai agent system has run the open source agent service implementation code on zkVM
On-chain Smart Contract		• Support for traditional blockchain-based Smart Contract technologies enabling the deployed contract codes to be executed on blockchain implementing functions such as issuing tokens or trading tokens (DEXs) on-chain • Web3 ai-ID owners can deploy token contracts responsible for ownership and profit management of the Web3 ai agent

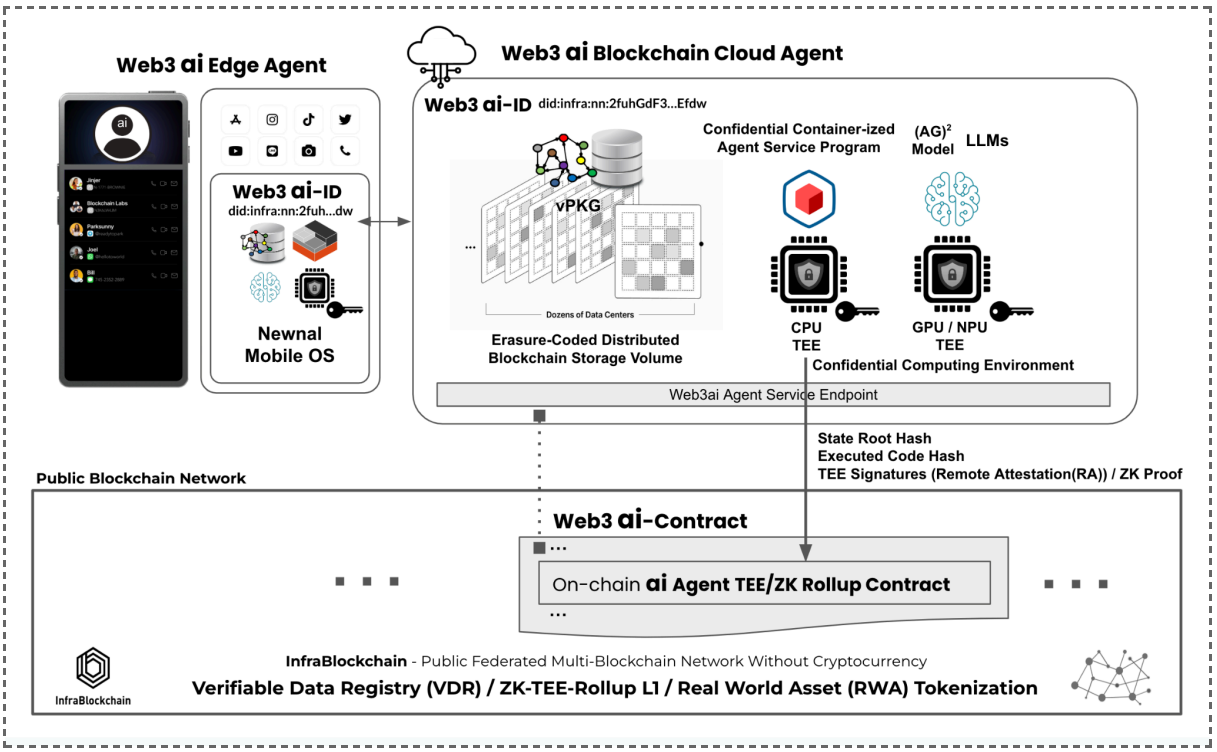
Appless eCommerce : Inter-Web3 ai Agent Service Orchestration Example





Above is an example of an Apples eCommerce service implementation in which a user does not directly search for and purchase a product using eCommerce apps, instead an personal Web3 ai agent autonomously processes a product purchase on behalf of the user. The personal Web3 ai agent searches for eCommerce AI agents published on the blockchain, identifies the *product-search* and *product-purchase* Agent Service Interface (ASI) served through the Web3 ai-Contracts, and then automatically searches, compares, recommends, and purchases products. The user's Web3 ai Agent can automatically set a product search filter suitable for the user based on the user's personal data stored in the PKG(Personal Knowledge Graph) database on the ai agent, and extracts anonymized personal information that can help purchase the item and delivers it to external eCommerce Web3 ai agents through a publicly specified agent service interface (ASI). eCommerce ai agents provide recommended items to the user's ai agent by executing their AI-based recommendation system that matches the most suitable item based on personal data provided by the user's ai agent. In this way, through the blockchain-based Web3 ai-ID and Web3 ai-Contract protocols, Web3 ai agents can automatically purchase very suitable products through autonomous interaction among the Web3 ai agents without the user using the app directly.

Verifiable Confidential Cloud Computing Technology for Newnal Web3 ai Agent



A Newnal Web3 ai agent consists of an *Edge Agent* that operates on a user's mobile device and a *Cloud Agent* that operates on a cloud server that can be accessed only through the user's blockchain ID(Web3 ai-ID). Edge Agent alone cannot store and manage all large amounts of user data. Entire personal data is backed up to the Cloud Agent, and the Edge Agent manages only frequently used data to be cached on devices to prepare for loss or damage to the user's mobile devices. Cloud Agent is required to execute AI models such as LLMs that require high-performance computing resources (GPU/NPU/HBM) that are difficult to process with only on-device AI computing resources. In addition, there must be a Cloud Agent in order to provide ai agent services to other users or other Web3 ai agents not only to the user who owns Web3 ai-ID. Newnal Web3 ai OS technology provides mobile OS-level system software for Web3ai Edge Agent to operate in conjunction with blockchain networks and Web3 ai Cloud Agent, and provides server-side system software for implementing Web3 ai Cloud Agent.

User's personal data collected in various ways and integrated/stored in verifiable PKG(Personal Knowledge Graph) databases are encrypted by Web3 ai-ID, and data is encrypted and stored in a fragmented form in a number of distributed cloud servers that doesn't belong to a single cloud infrastructure service through blockchain cloud storage technology. The stored personal data is encrypted using a blockchain ID (Web3 ai-ID), so that only the owner of the ai-ID can access the data, and personal information leakage

cannot occur while the data is stored. However, if the stored personal data is decrypted and processed by the cloud server, personal data is exposed to the server's memory, so there is a possibility that personal data may be leaked to cloud infrastructure providers such as AWS, GCP, and Azure. Confidential Computing technology utilizing TEE (Trusted Execution Environment), a hardware security module mounted on CPU/GPU processors, is the technology that can solve this problem. The code and data executed in the TEE mode of the CPU/GPU are encrypted on the memory by the key generated by the TEE hardware, so even the OS that can access the memory of the hardware cannot access the personal data processed by the TEE. TEE generates cryptographic signatures (RA, Remote Attestation) from the hardware itself that public codes identified by code hash are executed on the hardware in such a way that the user's data is not exposed. The TEE Signatures generated by hardware for the state root value of modified personal data and hash value of the personal information processing program code executed by TEE are continuously registered in the ***TEE Rollup Contract*** of Web3 ai Contract and verified on blockchain. This allows the Web3 ai agent service system to be publicly verified that its service implementation code (code hash shows what public code is executed) is executed on TEE hardware securely without personal data leakage even if it was executed on a public cloud server environment. The open-source, personal-data-leak-free ai agent service program executables are virtualized through Confidential Container (CoCo) technology and privately executed on the CPU's TEE, and the open source AI models are executed on the GPU's TEE in such a way that the TEE hardware provided by the GPU removes the possibility of leakage of personal data used for AI model learning and inference.

The Web3 ai Agent service may be implemented as a Layer 2 blockchain. In this case, the operation of the ai agent service is implemented on a zkEVM (zero-knowledge virtual machine) or a RISC-V instruction set-based zkVM (zero-knowledge virtual machine), and Zero-Knowledge proofs are created that publicly certified open source code has been executed securely without exposing processed data. ZK proofs are continuously registered in the **ZK-Rollup contract** on the Web3 ai-contract of the Layer 1 blockchain, and verified on the blockchain.

Through Web3 ai Contact's TEE/ZK Rollup Contract, TEE-supporting hardware, and ZK-based VMs, the ai Agent services can be guaranteed to be operated without personal information leakage.

Patents

[USPTO] US-20240414014-A1
DEVICE FOR PROVIDING BLOCKCHAIN DID-BASED MULTI CLOUD SERVICE AND ITS OPERATING METHOD

[USPTO] US-19/038309

A DEVICE AND METHOD FOR OWNING AND TRADING VERIFIABLE PERSONAL DATA THROUGH BLOCKCHAIN BASED PERSONAL WEB NODES

[USPTO] US-63/764594

DECENTRALIZED AI AGENT NETWORK SYSTEM BUILT UPON BLOCKCHAIN-BASED WEB3 AI-ID AND WEB3 AI-CONTRACT FOR VERIFIABLE CONFIDENTIAL AI AGENT COMPUTING