www.platon.network

PlatON

PlatON 2.0:

Decentralized Privacy-Preserving AI Network

LatticeX Foundation /

November 04, 2021

The Nine Chapters on the Computational Art

Abstract

In the past ten years, our society has witnessed the transition from analog to digital, and we are fast forward to a fully digital life. However, the utilization rate of data is very low due to the extreme centralization of artificial intelligence (AI), coupled with data abuse and privacy leakages. The value of data needs to be intellectualized urgently in order to be deposited and utilized, hence the calling for a next-generation intelligent network known as web 3.0 is growing. PlatON brings blockchain, AI and privacy-preserving computation together to create a decentralized collaborative privacy-preserving AI network that takes data utilization to a new level. It also serves as an infrastructure for autonomous AI agents and their collaboration that can facilitate the emergence of advanced AI and explore the path to artificial general intelligence (AGI). Based on an underlying blockchain network, we will first establish a decentralized privacy-preserving computation network that connects data, algorithms, and computing power through privacypreserving computation protocols. Developers can obtain the required resources at low cost, train AI models and publish them to the network, where AI services or agents interact with each other to form a self-organized, collaborative AI network. Anyone can access AI technologies or become a stakeholder in its development on this network, thus achieving AI democratization. The PlatON network creates a new AI fabric that delivers superior practical AI functionality today, while moving toward the fulfillment of PlatON's AGI visions of tomorrow.

Contents

1 / Intelligence and privacy security in the digital age

According to Statista analysis [1], the number of connected devices worldwide is expected to reach 30.9 billion by 2025. Connected devices and services create enormous amounts of data, and IDC [2] predicts that the global data will grow from 33 Zettabytes (ZB, that is a trillion gigabytes) in 2018 to 175 ZB by 2025. All this data will unlock unique user experiences and a new world of business opportunities. Where once data primarily drove successful business operations, today it is a vital element in the smooth operation of all aspects of daily life for consumers, governments, and businesses alike. In the past 10 years, our society has witnessed the transition from analog to digital. What the next decade will bring using the power of data is virtually limitless.

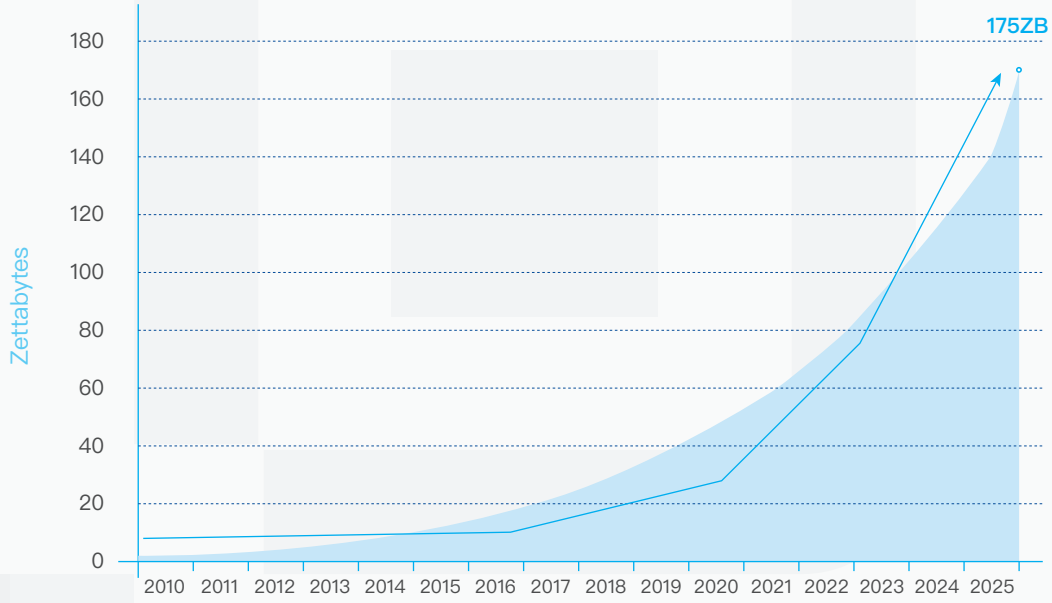


Figure 1: Annual Size of the Global Data [2]

In Data Age 2025 [2] , IDC identified AI and security as critical development trend.

- **AI that change the landscape.** New technologies such as machine learning, natural language processing and AI turn data analysis from an uncommon and retrospective practice into a proactive driver of strategic decision and action. Artificial intelligence can greatly step up the frequency, flexibility, and immediacy of data analysis.
- **Security as a critical foundation.** All this data from new sources open up new vulnerabilities to private and sensitive information. There is a significant gap between the amount of data being produced today that requires security and the amount of data that is actually

being security protected, and this gap will widen. By 2025, almost 90% of global data will require a certain level of security, but less than half will be security protected.

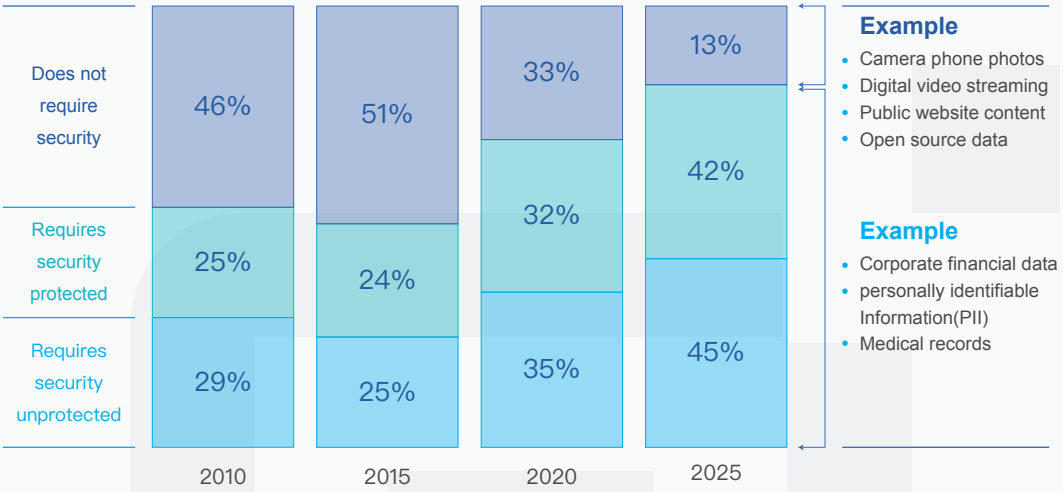


Figure 2: Actual Status of Data Security [2]

2 / The coming "intelligent web"

2.1. From WEB 2.0 to WEB X.0

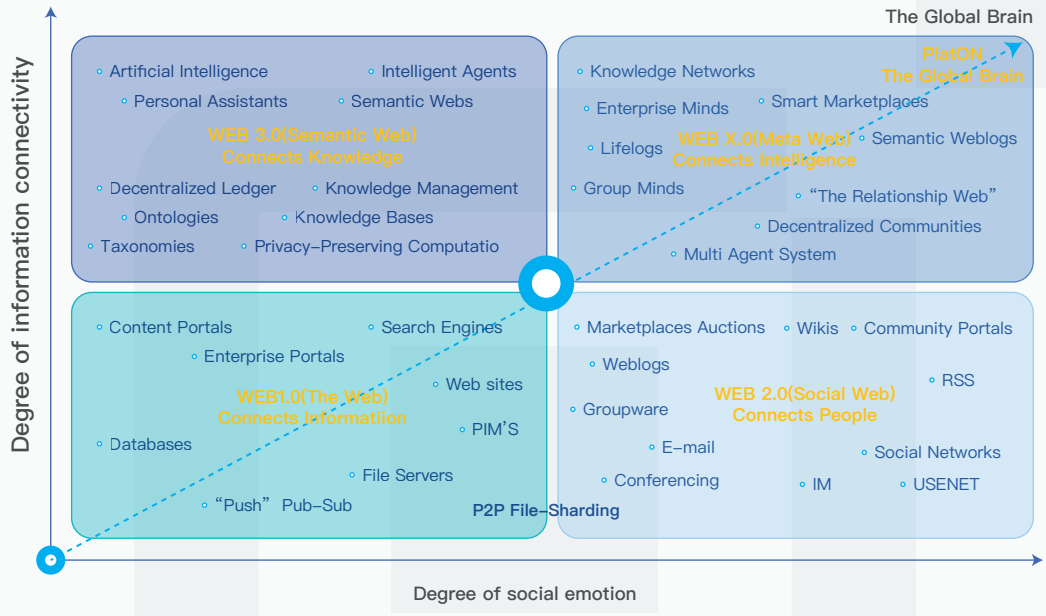


Figure 3: The Evolution of the web [3]

Web 2.0, coined as such by O'Reilly and others between 1999 and 2004, is a platform that reached millions of users and facilitated communication, organization and collaboration. Today, more than a decade later, serious questions are being asked about the centralization, privacy concerns and security of the current Web.

- **Centralization:** Web 2.0 has evolved to a point where large technology and social media companies dominate the market and hold vast amounts of personal data on users.

- **Privacy and security:** With the increasing amount of data being captured, large data center-sact as honeypots for organized crime.

- **Scalability:** With larger datasets from billions of connected devices, there will be increasing-pressure on existing infrastructure. Today's client server model works well, but is not likely toscale for the next generation web.

The next generation of the Web was first named "Web 3.0" by John Markoff of the New York

Times, but there is no definitive definition of Web 3.0. The Semantic Web, as proposed by Berners-Lee, is often used as a synonym for "Web 3.0," which would process content in a human-like manner. Broadly speaking, the characteristics most commonly associated with Web 3.0 include the following.

- **Ubiquitous Connectivity:** Connect anyone, anywhere, anytime to anything that is open, trustless, and permissionless.
- **The Semantic Web:** Web 3.0 will use efficient machine learning algorithms to connect data from individuals, companies and machines in a cryptographic way, and machines will be able to understand and intelligently process the data in a human-like manner.
- **The Intelligent Web:** Web 3.0 is an evolutionary path to AGI that can run intelligent applications, such as natural language processing, machine learning, machine reasoning, and autonomous agents.
- **Self Sovereignty:** Everyone is in control of their own identity and data. No need to rely on third parties, individuals can sell or exchange their data without losing ownership and privacy.

Nova Spivack [3] proposes that in the coming “intelligent web”, web services are connected to autonomous intelligent agents, that roam the network and are able to interact with one another or even people. As the intelligence with which such processes unfold, in atotally decentralized and grassroots manner, vast systems of “hybrid intelligence” (humans + intelligent software) will form, which is the Metaverse. The network becomes increasingly autonomous and self-organizing (the network as a whole is becoming even more "smart"). As structures that provide virtual higher-order cognition and self-awareness to the network emerge, interconnection, and become sophistic, the Global Brain will self-organize into a Global Mind.

2.2. Underlying technologies of the intelligent web

Where Web 2.0 was driven by the advent of mobile internet, social network and cloud computing technology, the intelligent web vision is built upon three new layers of technological innovation: blockchain, AI and the Internet of Things (IoT). Its ubiquitous nature

is underpinned by the growth of the Internet of Things. AI will be a crucial tool used to tag web content, and a truly semantic web will enable AI systems to leverage it in new and novel ways. Distributed ledger technology such as blockchain will underpin an intelligently connected Web 3.0, by facilitating data exchange and transactions between divergent systems, manufacturers and devices.

The key to the leap from Web 2.0 to the intelligent web remains the protection of data privacy and the ownership of data being should be able to be controlled by individuals themselves. Privacy-preserving computation is an emerging solution and technology trend, and is listed in Gartner's 9 key strategic technology trends for 2022 [4]. Privacy-preserving computation makes personal data more secure and private, allowing users to truly take ownership of their data, fundamentally balancing the contradiction between data security and data value fundamentally, and completely resolving the safe and free flow of data.

2.3. Developments and Issues in Artificial Intelligence

2.3.1. Trends in Artificial Intelligence

During the last 5 to 10 years, the rapid growth of the internet, mobile internet and The Internet of Things has generated enormous amounts of data. The increase in chip processing power, the popularity of cloud services and the decline in hardware prices have led to a significant increase in computing power. The broad industry and solution market has enabled the rapid development of AI technology. AI has been everywhere in daily life, and AI has been applied in many industry verticals such as medical, health, finance, education, and security.

A growing number of governments and corporate organizations worldwide are gradually recognizing the economic and strategic importance of AI and are dabbling in AI from national strategies to business activities. A study by PwC on the economic impact of AI [5] on the world economy by 2030 reports that the emergence of AI will bring an additional 14% boost to global GDP by 2030, equivalent to a growth of $15.7 trillion, more than the current GDP of China and India combined. The global AI market will experience phenomenal growth in the coming years. In its 2019 Global AI Development White Paper [6], Deloitte projects the world AI market to exceed $6 trillion by 2025, growing at a CAGR of 30% from 2017-2025.

In the field of mainstream AI, deep learning has made breakthroughs in recent years, rekindling hopes for “human-like” AI. Claims that the “Turing test has been surpassed” and AlphaGo’s victory in the human vs computer Go match have made the discussion of AGI a hot topic in the industry. Technology giants such as Apple, Amazon, Alphabet, Microsoft and Facebook have invested heavily in AGI research and development, with Google spending $540 million to acquire DeepMind in 2014, Microsoft investing $1 billion in Open AI in 2019, and according to a report on general AI by Seattle research firm Mind Commerce [7] , investments related to general AI will reach $50 billion by 2023.

According to Mind Commerce’s AGI report, the global market for general AI for enterprise applications and solutions will reach $3.83 billion by 2025, and the global market for AGI-enabled big data and predictive analytics will reach $1.18 billion by the same year. By 2027, 70% of enterprise and industrial organizations will deploy AI-embedded intelligent machines, more than 8% of global economic activity will be done autonomously by some kind of AI solution, compared to less than 1% today, and more than 35% of enterprise value will be directly or indirectly attributable to AGI solutions.

2.3.2. Challenges of Artificial Intelligence

Data Privacy and Security Regulations

Machine learning technology, mainly deep learning, cannot be learned and inferred without enormous amounts of data, so data becomes one of the most important resources for the development of frontier technology in the field of AI. Technology giants have accumulated huge amounts of data through the internet services, and as the value of data becomes increasingly prominent in the era of AI, this data will gradually evolve into an important asset and essential to the competitiveness of enterprises.

The smarter AI becomes, the more personal data it needs to be acquired, stored and analyzed, which will inevitably involve the important ethical issue of personal privacy protection. Today, all kinds of data and information are collected all the times, everywhere, almost everyone connected to the digital space, personal privacy is easily stored, copied and spread in the form of data, such as personalidentity information data, network behavior trajectory data, as well as data processing and analysis of preference information, prediction information, etc. It is foreseeable that in the near future, more and more AI products will be found in thousands of households, which will bring convenience to

peoples' lives whilst mining their private personal data with ease.

Entering the 21st century, many companies worldwide, including internet giants, have been exposed to data leaks and abuse. Google, Amazon, Facebook, Apple and other U.S. internet companies have been fined by the EU one after another in Europe in the past two years for data privacy, monopoly, taxation and other issues, which has caused widespread concern worldwide and made people gradually aware of the importance of personal privacy protection. Countries around the world have successively introduced bills to further regulate the market. The promulgation of Cybersecurity Law of the People's Republic of China and the National Cyberspace Security Strategy in China, and the General Data Protection Regulation (GDPR) in the EU have had a profound impact on the protection and regulation of personal information.

In the current climate, individuals and organizations are reluctant to share personal and professional data due to data privacy and misuse issues and increased data regulation, AI organizations with limited resources do not have access to larger valid datasets to train better models, and published models can quickly become out of date without effort to acquire more data to re-train them. As a result, the focus of AI has shifted from an orientation centered on AI-based algorithms, to one on big data architectures that guarantee security and privacy. Isolation of data and protection of data privacy is becoming the next challenge in the field of AI.

Expensive Training Costs

While advances in hardware and software have been driving down AI training costs by 37% per year, the size of AI models is growing at a much faster rate of 1000% per year. As a result, total AI training costs continue to climb. ARK[8] believe that state-of-the-art AI training model costs are likely to increase 100-fold, from roughly $1 million today, to more than $100 million by 2025.

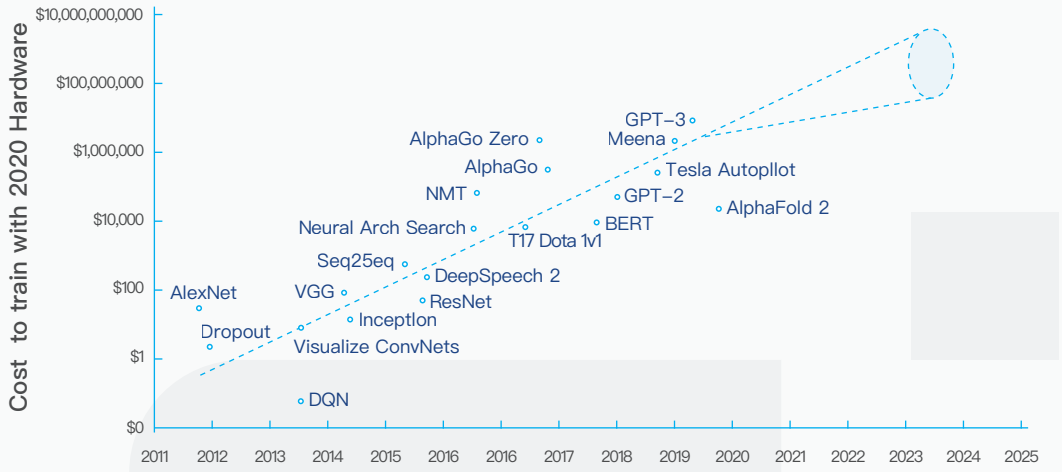


Figure 4: AI training cost [8]

Centralization and De-Democratisation

The democratization of AI means that more people are able to conduct AI research and/or build AI-powered products and services, and democratization is the lowering of barriers to entry in terms of resources and knowledge. This includes:

- The right to use powerful AI models.
- The right to use algorithms and models without advanced mathematical and computational science skills.
- The right to use the computational resources required by the algorithms and models.

While AI has made tremendous progress, the potential benefits of AI are not widely utilised, AI has not yet been democratized, and there is a trend toward increasing centralization.

- Most AI research is controlled by a handful of tech giants. Independent developers of AI have no readily available way to monetize their creations. Usually the most lucrative option is to sell their technology to one of the tech giants, leading to even more concentration of technology control.
- A handful of tech giants have monopolized the upstream of data through the method of providing services to consumers, in return for unprecedented access to their data, then training high-end AI models using said data and incorporating them into their ecosystem,

further increasing the dependence of users and other companies on them. Outside of this data monopoly, other market players such as small and innovative companies find it difficult to collect large-scale data. Even if they manage to obtain data at a significant cost, they lack effective usage scenarios and are unable to exchange them, making it difficult to precisely align with relevant AI learning networks.

- Most organizations are facing a lack of AI skills and AI talent. But tech giants are strategically working to monopolize AI talent at an unprecedented rate and scale, further widening the gap with other companies.

2.3.3. AI needs Blockchain & Privacy-preserving Computation

Blockchain, privacy-preserving computation, and AI affect and utilize data in differing ways. The combination of these technologies can take data utilization to new levels while enhancing blockchain infrastructure and the potential of AI.

- Blockchain consensus algorithms can help subjects in decentralized AI systems collaborate to accomplish tasks. For example, in the field of intelligent transportation, AI is the "brain" behind countless autonomous vehicles, and these autonomous vehicles need to cooperate with each other trustfully to accomplish a common goal. AI systems have no mechanism to ensure that these autonomous vehicles can reach consensus among themselves in a trustworthy manner. Of course, the collaboration of these autonomous vehicles could rely on trusted third parties, but this would expose the public to security and privacy issues.

- AI models require massive amounts of high-quality data for training and optimization, and data privacy and regulation prevent effective data sharing. Blockchain and privacypreserving computation enable the privacy and security controls needed for compliance and facilitate data sharing and value exchange.

- The intersection between AI and cryptography economics is another interesting area where blockchain combined with AI can enable the monetization of data and incentivize the addition of a wider range of data, algorithms and computing power to create more efficient AI models.

- Blockchain can make AI more coherent and easy to understand, and as all data, variables and processes used in AI training decisions will have an untamperable record, they can be tracked and audited.

3 / What is PlatON 2.0

3.1. Vision & Goal

Combining blockchain and privacy-preserving computation technologies, PlatON is building a decentralized and collaborative AI network and global brain to drive the democratization of AI for safe artificial general intelligence.

- To build the infrastructure needed for autonomous AI agents and their collaboration, to facilitate the emergence and evolution of advanced AI, and to explore the path to general AI.

- Extend the power of AI to anyone who requires it through our decentralized network and open-source software tools to make the best AI technology accessible for the masses.

The overall goal is to be achieved in three phases.

- A decentralized privacy-preserving computation network, establishing a decentralized data sharing and privacy-preserving computation infrastructure network that connects data owners, data users, algorithm developers and arithmetic providers.

- A decentralized AI marketplace that enables the common sharing of AI assets, agile smart application development, and provides the whole spectrum of products and services from AI computing power and algorithms, to AI capabilities and their production, deployment, and integration.

- A decentralized AI collaboration network that allows AI to collaborate at scale, bringing together collective intelligence to accomplish complex goals.

3.2. Privacy-preserving Artificial Intelligence Network

3.2.1. Three-Tier AI Network Model

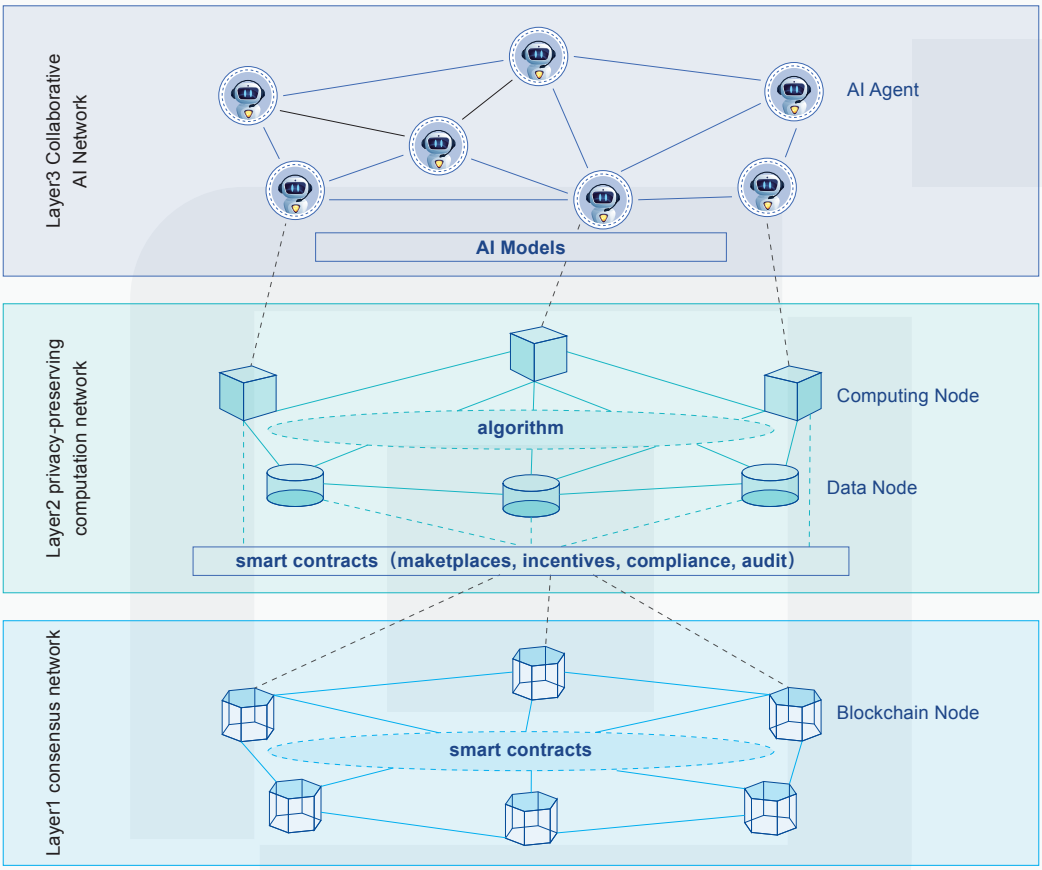


Figure 5: Three-Tier AI Network Model

The entire privacy-preserving AI network is divided into three layers.

Layer1： Consensus Network

Consensus network is a decentralized blockchain network composed of blockchain nodes, which are connected to each other through a P2P protocol and can be consensual through consensus protocol in an trustless environment. On the blockchain network, smart contracts can be executed, but due to performance and transaction cost limitations, smart contracts do not support computational logic of an overly complex nature, and can only access on-chain data with limited storage capabilities.

On the blockchain, anyone can view or obtain a complete copy of the on-chain data and

all transactions are open and transparent, so the blockchain technology itself does not have the ability to protect privacy. By overlaying privacy-preserving computation protocols based on homomorphic encryption, zero-knowledge proof, TEE and other technologies on the consensus network, the privacy of data and computations on-chain can be protected.

Layer2: Privacy-preserving computation network

The basic elements of computing are data, algorithms, and arithmetic power. Data nodes and computing nodes can be connected to the privacy-preserving computation network through P2P protocols to publish data and arithmetic power, and algorithms can be computed using data and computing power. Through smart contracts on the blockchain, a decentralized sharing and trading market for data, algorithms and computing power can be built. Based on the cryptographic economics on the blockchain, data, computing power and algorithms can be monetized, forming an effective incentive mechanism to motivate more data, algorithms and computing power to join the network.

Privacy-preserving computation networks can execute smart contracts of consensus networks privately and also run popular deep learning frameworks.

The data in privacy-preserving computation networks is generally kept locally and are available invisibly through secure multi-party computation, federated learning, and other techniques for collaborative computation. Not only the privacy of the data is protected, but also the privacy of the computation results such as the completed trained AI models.

Layer3: Collaborative AI network

By using the datasets and computing power of privacy-preserving computation networks, AI models can be trained, which can be deployed on the AI network, and served externally through AI agents, forming a marketplace for AI services. Through technologies such as Multi Agent Systems, AI agents can operate independently and communicate and collaborate with each other to create further innovative AI services, enabling AI DAOs and formulation of autonomous AI networks.

3.2.2. Technology Stack

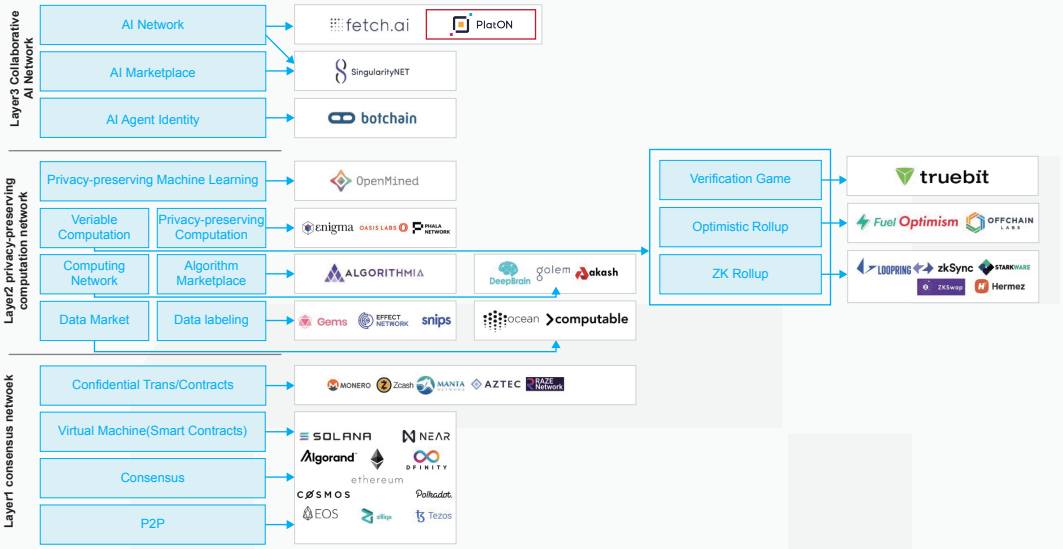


Figure 6: privacy-preserving AI network technology stack

The technology stack of the privacy-preserving AI network is shown in Figure 6, which is generalized based on the resources and technologies that privacy-preserving AI relies on. Some existing blockchain projects can be mapped to this stack, but certain projects may not match so well.

There are projects that try to combine blockchain, privacy-preserving computation and artificial intelligence, some combine privacy-preserving computation and blockchain to enhance blockchain privacy protection and computing capabilities, some combine blockchain and AI to provide a marketplace for AI services, and some use the decentralization of blockchain to build computing power and data market. Although there seem to be many projects, they can all only meet part of the needs of privacy-preserving AI in a fragmented manner and cannot be combined organically, they have not yet formed a mature privacy-preserving AI ecology.

Layer1: Consensus Network

Layer1 is the basic protocol of blockchain, the core is consensus and smart contracts, Layer1 is the basis of decentralized computing, and smart contracts are a simple computing model, which is a kind of Serverless in a sense. There are a lot of blockchain projects to implement Layer1, which are basically Ethereum model and decentralized computing, such as Ethereum, Eos, Cosmos, Polkadot, Algorand, Dfinity, Solana, Near, etc.

On Layer 1, cryptographic technologies such as zero-knowledge proofs and homomorphic

encryption are adopted to encrypt blockchain data to achieve data privacy, including privacy transactions and data privacy in smart contracts, such as Monero, Zcash, Manta, and those based on other Layer1 networks such as Aztec and Raze Framework.

Layer2: Privacy-preserving computation network

As the amount of data that can be stored on Layer1 is limited, the logic of smart contract cannot be too complex and does not have access to off-chain data either, so the training of AI models cannot be done in the smart contract.

Privacy-preserving computation network closely combines data, algorithms and computing power to build a complete computing ecology where all subjects, including individuals and institutions, would be financially incentivized to provide personal and professional data. As data security and privacy are guaranteed through decentralization and secure computation, all subjects are more willing to share sensitive data (consumption and health information). Over time, the market will accumulate more higher quality data. AI experts will be motivated to create and share higher performance AI models.

Here we analyze the three key building blocks of decentralized AI: data, models, and computing power.

- **Data**

Ocean and Computable Labs are working to build data marketplace protocols. Snips is using crypto economics to incentivize a network of workers involved in synthetic data generation. Gems and Effect. AI are also building crowd-sourcing marketplaces, using cryptoeconomics to motivate people to complete data labeling and annotation.

- **Computing power**

A lot of the recent progress in AI has been facilitated by the massive ramp up in computing power, which resulted both from better leveraging of the existing hardware, and also building new high performance hardware specifically for AI (Google TPUs, etc).

DeepBrain aims to share idle computing resources from around the world to enable decentralized arithmetic networks. Its general philosophy is comparable to other projects such as Akash and Golem, but DeepBrain is more specifically focused on the type of computing power needed for AI.

Starkware and zkSync are all zkRollup scaling solutions for scaling payment transactions and smart contract transactions on Ethereum. LoopRing and Hermez are also zkRollup scaling solutions focused on scaling payment transactions and token transfer transactions.

- **Algorithm**

For a decentralized computation networks to work, it is important to guarantee that whatever data is provided by individuals and companies is processed in a completely private manner.

Enigma, Oasis, Phala and OpenMined all provide secure computation solutions, Enigma, Oasis and Phala target general computing, OpenMinded focuses on privacy-preserving machine learning. Enigma, Oasis and Phala use TEE techniques, while OpenMinded primarily uses Federated Learning, championed by Google, and Differential Privacy, championed by Apple. The Algorithmia project enables an interactive machine learning model marketplace with the help of blockchain, which is actually a model transaction enabled by smart contracts.

Layer3: Collaborative AI network

The privacy-preserving computation network provides the three key elements needed for AI: data, models and computing power. A decentralized AI marketplace will help create better AI. People provide their data, developers compete to provide the best machine learning models, and the entire system acts as a self reinforcing network that attracts more and more participants and creates better AI.

AI continues to thrive and accelerate through decentralized AI marketplaces. We will have the ability to create many types of AI for almost every task. These AI robots need an effective organizational model to help them cooperate in a transparent manner. Fetch AI works to build and enable Autonomous Economic Agents (AEAs) to cooperate in an organized manner. An AEA is a software entity that can perform actions without external stimuli, and can intelligently search for and interact with other AEAs. SingularityNET is another very ambitious and complex project that aims to be the leading protocol for networking artificial intelligence and machine learning tools to form efficient applications across vertical markets, ultimately resulting in coordinated AGI. The SingularityNET platform currently focuses on providing a commercial launchpad for developers to launch their AI services on the web where they can interoperate with other AI services and paying subscribers. The Botchain project is a system that provides identity authentication to autonomous AI agents.

A step further than autonomous AI agent cooperation is that the entire network operates completely autonomously, supported by AI. This is the AI DAO, a decentralized autonomous organization supported by AI, which can be a decentralized organization run entirely by AI, with no or limited human intervention. Many companies in this field have ambitious plans, but are currently at the conceptual stage.

3.2.3. Competitive Landscape

	Layer			Technical Features			Application	
	Layer1	Layer2	Layer3	TPS	TTF	Privacy-Preserving Computation	Smart Contract	AI Model
PlatON	✓	✓	✓	10K	3s	Cryptography	EVM、WASM	✓
Ethereum	✓	✓		10	6m	×	EVM、eWSM	
Cosmos	✓			1K	6s	×	×	
EOS	✓			4K	163s	×	WASM	
Solana	✓			50K	1.5s	×	Rust	
Oasis	✓			1K	6s	TEE	EVM、eWSM	
Enigma		✓				TEE		
Phala		✓				TEE		

Table 1: PlatON Competitive Landscape

Firstly, PlatON is an underlying public chain, which is not inferior to any mainstream public chains such as Ethereum, Eos, Cosmos, Polkadot, Algorand, Dfinity, Solana, Near, etc. in terms of decentralization, security, performance, and smart contract development. These public chains mainly aim to build WEB3 network infrastructure and decentralized application platforms, while PlatON is to build a privacy-preserving computation network as well as an collaboration AI network with the main applications being AI training, AI services and autonomous agents.

In comparison to other projects with privacy-preserving computation such as Enigma, Oasis and Phala, PlatON focuses on the combination of privacy-preserving computation and AI.

- PlatON uses a different privacy technology route. PlatON uses secure multi-party computation technology based on cryptography, while Oasis, Enigma and Phala mainly use TEE technology. PlatON is also an independent and complete blockchain network.

- PlatON supports more complex privacy-preserving computations of machine learning, and will also provide specific privacy-preserving computation acceleration hardware for AI.

- PlatON is more focused on privacy-preserving training of AI models and construction of AI agents, as well as interoperability of AI agents, rather than just layer2 computational enhancement of blockchain networks.

3.3. Competitive Advantages

PlatON features the following advantages by integrating blockchain, privacy-preserving computation and AI technology.

Decentralization

Any user and node can connect to the network in a permissionless mananer. Any data, algorithms and computing power can be securely shared, connected and traded. Anyone can develop and use AI service.

Privacy-preserving

Modern cryptography-based privacy-preserving computation techniques provide a new computing paradigm that makes data and models available but not visible, allowing privacy to be fully protected and data rights to be safeguarded.

High-performance

PlatON achieves high-performance asynchronous BFT consensus through pipeline verification, parallel verification, aggregated signatures and other optimizations. Besides, the network adopts a formal verification methods to prove its safety, liveness, and responsiveness.

Low training costs

With blockchain and privacy-preserving computation technologies, anyone can share data and algorithms in a secure and frictionless marketplace, thus drastically reducing marginal costs and drastically reducing training costs.

Low development threshold

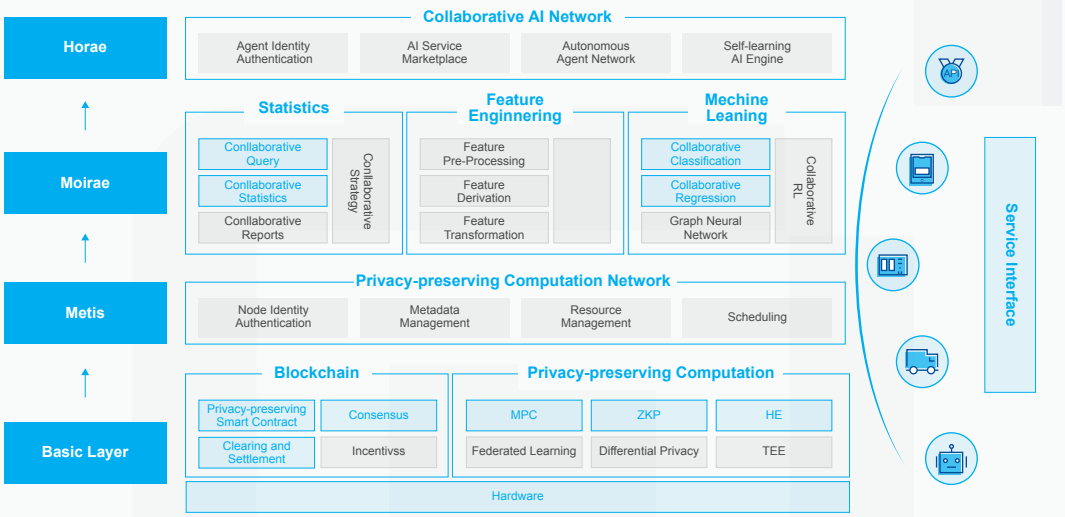
PlatON supports Visualized AI model development and debugging, and automated machine learning(AutoML). It can greatly lower the threshold for AI model development and improved development efficiency by simplifying the entire process management of AI model development, training, and deployment through MLOps.

Regulatory and compliance

All data, variables and processes used in the AI training decision making process have tamper-evident records that can be tracked and audited. Privacy-preserving technologies enable data usage to meet regulatory requirements, such as the right to be forgotten, the right to portability, conditional authorization, and minimum collection.

4 / Technical Architecture

4.1. Overall technical framework



PlatON overvall technical architecture

PlatON does not attempt to implement the entire privacy-preserving AI technology stack, focusing on the combination of privacy-preserving computation and AI. The overall architecture is shown in Figure 7, followed by a detailed description of each module.

4.2. Privacy-preserving AI Framework (Rosetta)

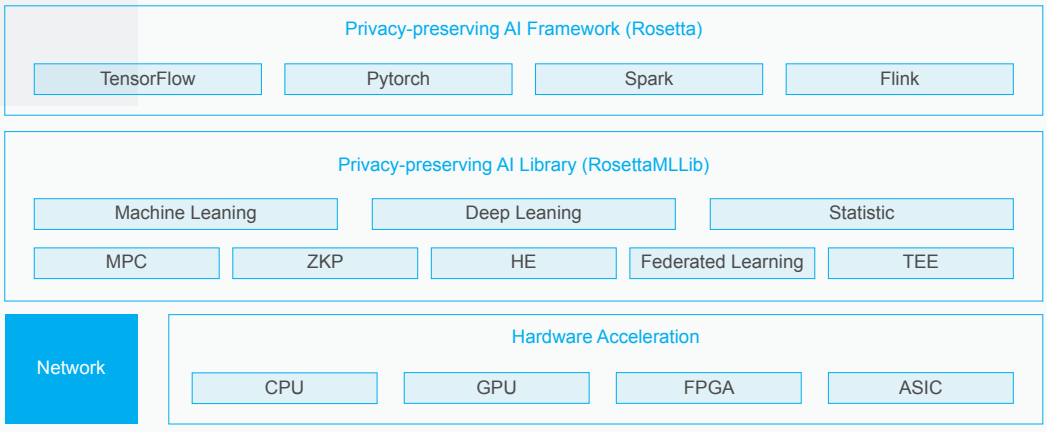


Figure 8: Privacy-preserving AI development Framework

Rosetta aims to provide AI solutions to protect privacy-preserving without requiring expertise in cryptography, federated learning, and trusted execution environments.

- Rosetta integrates mainstream privacy-preserving computation technologies, including cryptography, federated learning, and trusted execution environments. Moreover, it provides privacy-preserving statistical analysis algorithm library, privacy-preserving machine learning algorithm library, such as regression, decision tree, clustering, and privacy-preserving deep learning algorithm library such as CNN and RNN.

- Rosetta can be combined with mainstream machine learning and AI frameworks such as TensorFlow, Pytorch, Spark, Flink, etc. Rosetta currently implements the combination with TensorFlow and reuses the TensorFlow API, allowing the migration of legacy TensorFlow code to a privacy-preserving approach with minimal changes.

4.3. Underlying Protocol and Privacy-preserving Computation Protocol on Layer1

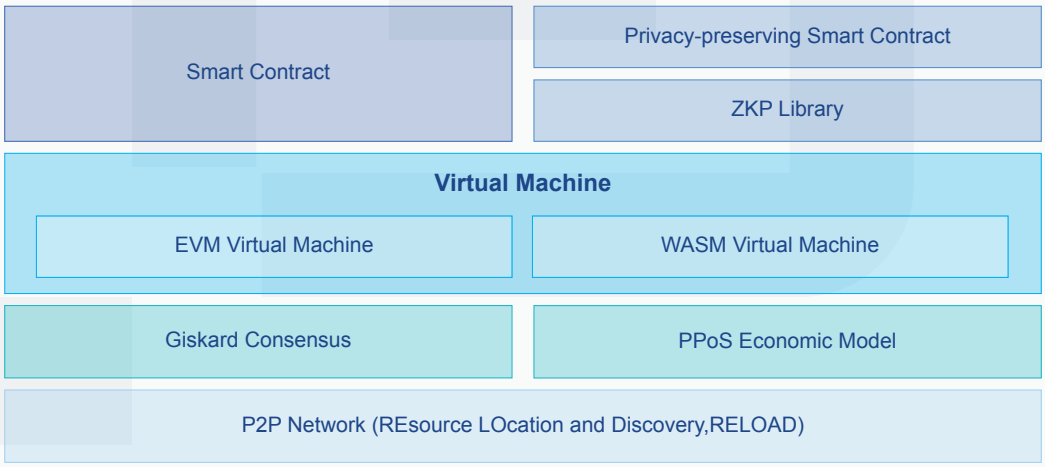


Figure 9: Underlying Protocol and Privacy-preserving Computation Protocol on Layer1

The current public chains cannot well meet the computing needs of privacy-preserving AI. Therfore, it is still necessary for PlatON to implement a complete Layer1 basic protocol to deeply adapted to privacy-preserving computation and privacy-preserving AI.

- **P2P network**

PlatON has implemented the P2P base protocol, which is mainly used for node discovery and connection. As a decentralized computation network, there is also a need for discovery and use of data and computing resources, as well as discovery and transparent invocation of AI model services, all of which will be implemented in PlatON 2.0 through the RELOAD protocol. RELOAD protocol.

- **Giskard consensus**

  Giskard is a consensus of the BFT category, which includes optimization in many aspects. While reducing complexity and further improving throughput through parallelism, it has the advantages of high performance and low latency.

  - Three-stage Pipeline validation: After the previous block completes a round of voting, it can move on to the next block, and the final confirmation of a block requires the completion of the previous three block votes.
  - Concurrent block production and validation: Separate block production and confirmation, concurrently process in Prepare, Pre-Commit and Commit phases.
  - Communication optimization: Adopt aggregated signatures to reduce the communication traffic, and also provide an optimized version based on leader to further reduce the communication complexity.
  - View-change optimization: Integrate the view-change process into the normal process, eliminating the need for a separate view-change process.

- **PPoS economic model**

  PPoS is a staking economic model in which every LAT holder can participate. Any node that locks more than a pre-determined minimum number of LATs becomes an alternative node candidate. Other LAT holders can lock LATs delegated to alternative node candidates, and the top candidates with the highest number of votes become alternative nodes. After being randomly selected from the alternative nodes using VRF, the validators can participate in block producing and validation. The validators can receive block rewards and transaction fees. The validators and the alternative nodes share the staking rewards with their supporters according to the prior agreement.

- **Dual virtual machine support**

  PlatON supports both EVM and WASM virtual machines and is compatible with solidity contracts. Smart contracts on Ethereum can be ported to PlatON with minor modifications.

- **Privacy-preserving smart contract**

  Both the EVM and WASM virtual machines have built-in privacy-preserving algorithms (including homomorphic encryption and zero-knowledge proofs) that developers can use directly in smart contracts to protect the privacy of data within the contract. Based on the privacy-preserving algorithms, PlatON has developed a standard for privacy token contracts that incorporates minting, destruction, and interaction with standard tokens to anonymize them.

4.4. Privacy–preserving Computation Network (Metis)

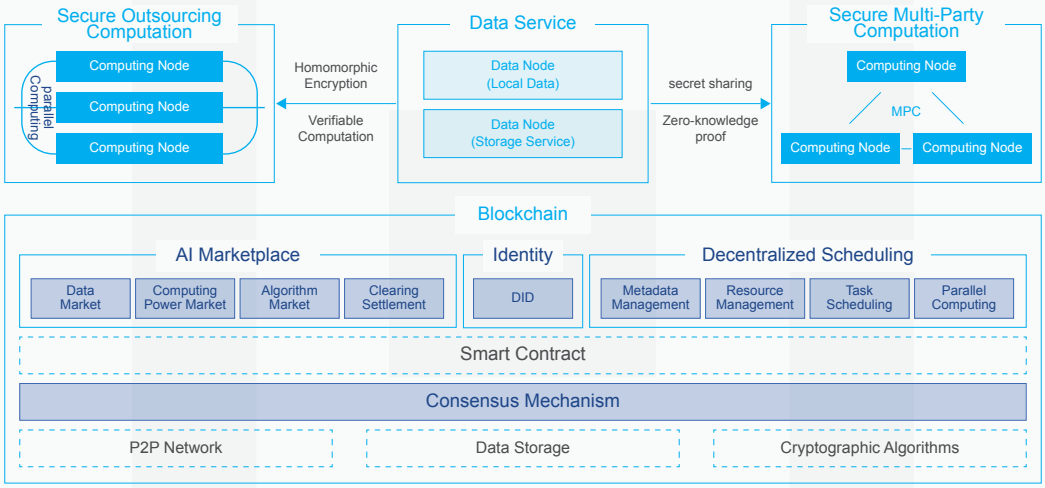


Figure 10: Privacy-preserving computation network Metis

Metis aggregates the data, algorithms, and computing power needed for computing in a decentralized manner to create a secure privacy-preserving computation paradigm.

- **Decentralized scheduling**

  Layer2 underlying network is the RELOAD overlay network, data nodes and computing nodes are connected through P2P protocol, and the RELOAD protocol is used to publish, discover, locate and schedule data and computing resources.

- **Data service**

  The data subject can either start the data node locally or host the data encrypted to the data node. Upon receiving a computation request, the data node uses secret sharing to slice the data and distribute it to randomly selected computing nodes for secure multi-party computation. The computation task and selection of computing nodes need to be confirmed

among multiple data nodes via the consensus protocol. Data nodes can also encrypt the data by homomorphic encryption, distribute it to computing nodes for outsourced computation, and verify the returned computation results and computation proofs using verifiable computation algorithms.

- **Computation service**

Metis supports two different types of privacy-preserving computation protocols and can also be extended with additional privacy-preserving computation protocols.

– secure multi-party computation

The privacy-preserving computation is performed between computation nodes following the secure multi-party computation protocol, and the computation results are returned to the computation result party through blockchain smart contracts. In the case of AI model training, the completed AI model can be deployed to Layer3's AI network and become an AI agent to provide AI services to the outside world.

– secure outsourcing computation

If users have their own data and algorithms, but do not have enough computing power, they can give their data (after homomorphic encryption) and algorithms to third-party computing nodes for outsourced computation. Data and algorithms can be distributed to multiple compute nodes for parallel computation, and the computation task can be decomposed according to the data or model. After the computation completed by the node, it returns the computation result and computation proof to verify the correctness of the computation.

- **Blockchain**

Through the blockchain based economic incentives and smart contracts, a decentralized data, computing power and model trading markets is established on the blockchain network. PlatON realizes privacy-preserving computation economic model, capitalizing and monetizing data and computing resources. In order to ensure the security and validity of data and computation, the economic model contains staking and slash mechanisms. All data, variables and processes used in privacy-preserving computation have tamper-evident records , which can be tracked and audited.

Decentralized identity (DID) schemes are used to enable decentralized authentication and authorization of nodes and resources, including data validation and usage authorization. DID refers to a set of completely decentralized identities that enable individuals or organizations to fully possess their ownership, management, and control of digital identities and data.

4.5. Moirae: Privacy–preserving AI Platform

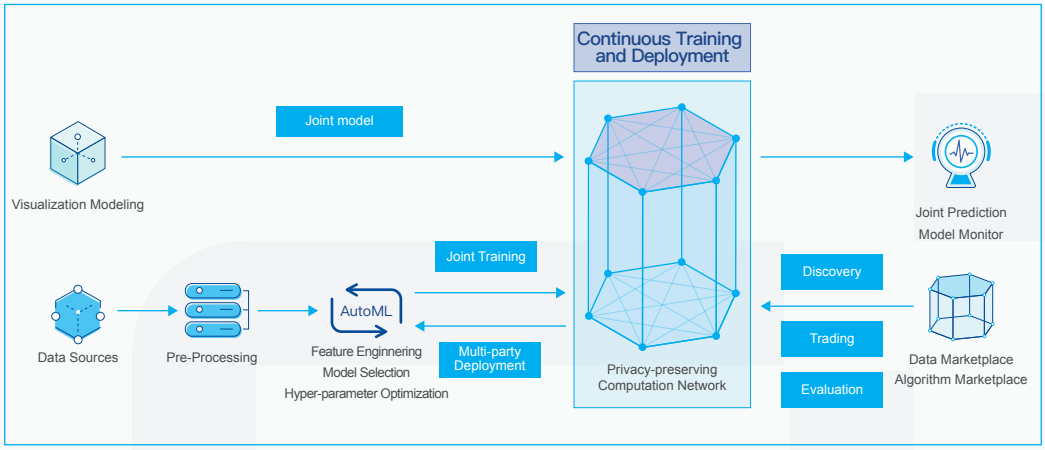


Figure 11: Privacy-preserving AI platform Moirae

Moirae is a decentralized AI *cloud* platform. On the one hand, it provides developers with a one-stop AI development platform as well as a one-stop all-round modeling process to help users quickly create and deploy models, and manage full-cycle AI work. On the other hand, it is also an open AI market. Developers can find training data sets, training models, launch AI models, and interact with other AI models or paying users.

All-in-one AI development platform

- Full range of modeling processes

  Moirae integrates data import, data processing, model development, model training, model evaluation, and service launch to provide a one-stop, all-round machine learning and deep learning modeling process to quickly build intelligent businesses. In addition, it provides visual and low-code development tools, automated model generation, and continuous training and deployment for machine learning and deep learning, lowering the threshold of developers, helping users to quickly create and deploy models and manage full-cycle AI workflow.

- Distributed model training and service hosting

  Metis provides globally distributed computing power and supports multiple chip architectures such as GPU and FPGA at the AI computing level, forming a heterogeneous AI computing platform that allows AI developers to directly submit computation tasks such as

data preprocessing, feature engineering, and model training at low cost, with computing resources automatically scheduled on demand.

Moirae provides service hosting services. A successfully trained model can be deployed directly on the network. The model can be deployed to a single network node or deployed in multiple network nodes in fragments. Multiple nodes is able to make predictions through secure multi-party computation protocol.

Open AI Marketplace

- Data marketplace

Moirae established a data exchange protocol based on zero-knowledge proof and fair exchange protocol. Through this protocol, training datasets can be traded fairly, and no one party can gain an advantage through early withdrawal or other kinds of bad actions. The training data set participates in model training through secure multi-party computation protocol instead of exchanging in plain text.

AI developers can actively search for training datasets in the data market. Besides, they can publish models so that others can provide data to collaborate on training models. In order to protect the privacy and security, the data must be authorized and model training must be conducted through privacy-preserving outsourcing computation or secure multi-party computation protocols.

The data market establishes an incentive mechanism through cryptoeconomics to encourage the submission of data to improve the accuracy of the model. In order to ensure the validity of the data, the data provider are required to stake, they will be punished when their submission verified as bad data.

- AI service marketplace

The successfully trained models can be directly deployed on the network and provide prediction services externally. The prediction service information is registered in the smart contract and can be searched and invoked by paying users.

4.6. Horae: Collaborative AI Network

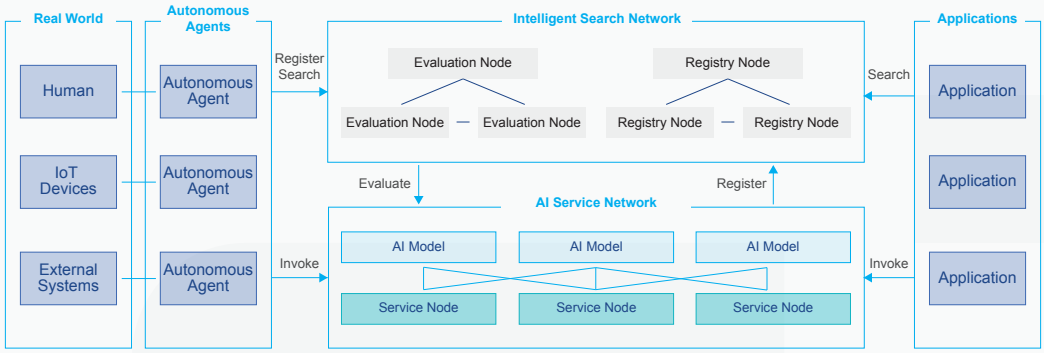


Figure 12: Collaborative AI network Horae

For developers who want to provide AI services over the web, the most critical component is the service node, which is an execution container for an AI model that can host multiple AI models and provide AI services externally. Considering network redundancy and fault tolerance, AI models can generally be hosted to multiple service nodes and can be migrated between service nodes.

The registration node and the evaluation node form an intelligent search network, allowing users to search and interact with AI services and agents. AI services and agents register their text descriptions and labels to registry nodes so that users can discover their services, pricing, addresses, and other information and invoke them. The evaluation node establishes a reputation scoring system through consensus algorithms by conducting service testing, evaluation and rating on AI services and agents. They conduct searches and recommendations based on this scoring system so that other users can quickly and easily query AI services and agents. The effect of evaluation can be improved by machine learning algorithms trained on historical data, such as successful queries and interactions. Users can identify potential AI services and agents by using search based on machine learning.

Horae aims to use self-organizing group intelligence to create a entirety that is greater than the sum of its parts. Autonomous agents do not just exist in the digital world, but can also serve as a bridge between the digital world and the real world, connecting to humans, IoT devices, and external IT systems. Each autonomous agent is an independent daemon process pursuing its own relatively simple goals, but their interaction will produce more complex goals and generate more intelligent higher-order agents.

In order to make AI agents to be truly autonomous, they need to understand how to mcommunicate to each other, not just the corresponding communication protocol. The application of Natural Language Processing (NLP) and Process Mining technologies enables autonomous agents to understand tasks described in natural language and develop true autonomy.

5 / Applications and Ecology

PlatON is working to apply the results of this established research area to new areas such as finance, medicine, smart cities and IoT.

5.1. AI Oracle

Oracles in blockchain are a kind of middleware that connects the blockchain with external resources. The existing blockchain oracles still mainly collect data from other data sources and map them to smart contracts on the chain, or allow smart contracts to call external APIs to provide more functions for the blockchain, but they are still limited to external data acquisition interfaces.

Due to difficulty to obtain deterministic results, such as face recognition, from AI model, and the high algorithm complexity, large data scale, the blockchain smart contract cannot run the AI model internally. Moreover, it is almost impossible to integrate the AI model into smart contracts.

Through the AI oracle, the AI services in the PlatON network can be aggregated and connected to smart contracts. PlatON is easily extended to AI oracle.

- Provides an open AI marketplace where users can have access to, search for and select an ever-increasing AI algorithms and models from different suppliers around the world.
- The test, evaluation, and rating on AI services based on machine learning can ensure the trustworthiness and security of AI services.
- Users can easily implement oracle agents, intelligently search and access AI services in the network by using PlatON's SDKs.

The followings are a few use cases for using AI to make smart contracts smarter.

- Blockchain users can use biometrics based on biometric methods, such as human faces and fingerprints, to control accounts without using the private key.
- The Automatic trading built on price prediction and AI strategies can be optimized based on ROI, risk rating, and price prediction indicators.

- The smart contract can determine the loan scale based on the user's credit scores.
- Check whether the products in the supply chain are fake or not.

5.2. Game

With the development of the game industry, peoples' pursuit of immersive experiences and personalization, more and more games have chosen to adopt open settings, Players have the freedom to create unique content, which are actually the player's private property. Some types of games are also exploring the use of players' private data, such as human body data, geographic location, social relationships, etc. Serious games blur the boundaries between games and general Apps.

The transaction of private virtual works, the training of privacy-preserving-based game agents, the mining of real data, etc., all require a safe and secure technology or mechanism to complete. All these functions require technologies and platforms like PlatON. PlatON can bring more innovative gameplay and effective operation methods to the game.

- In-game or even across games virtual currency unification
- Unique and personalized virtual asset trading
- Distributed game data collection and bot AI training
- Cross-game operation data analysis
- Analysis of Cross-Game Payment Habits

The following shows a specific application case of privacy-preserving AI in games.

A location-based AR game similar to Pokemon, allows players to catch different elves or obtain different items in real places. The difference is that these places can be real businesses shops. For example, an Hunan cuisine restaurants can provide fire elves, the elves in the north-eastern restaurant may have freezing skills. Players can can buy gym sets in sports clothing stores, the daily supermarket can provide some consumable supplies, the playground can provide a copy of the boss, and so on. If users consume in the store by scanning the QR code generated by the merchant, they can increase the probability of catching or the attribute value will be slightly higher or cheaper. Even

merchants in the same block can unite to provide players with a smooth monster-killing upgrade experience, attracting an increasing number of distant players to visit, and merchants also receive more customers and consumption.

In this game, sprites and props can not only be generated by the system, their various attributes can be influenced by the merchants in the real world. For merchants and game manufacturers, they are looking for their own potential customers. Game manufacturers hope to find possible players in the form of the merchants'existing customers. The merchants hope that the game will guide players to consume more in their store. Obviously, both parties want to cooperate but do not wish to expose their customers' information. Meanwhile, privacy-preserving AI comes. Merchants and game manufacturers can jointly train a model, guiding and recommending players based on the model's inference results according to the player's physical distance, freshness, revenue, encountered actors, etc. This model can be updated and upgraded through real feedback from players.

5.3. Biomedicine

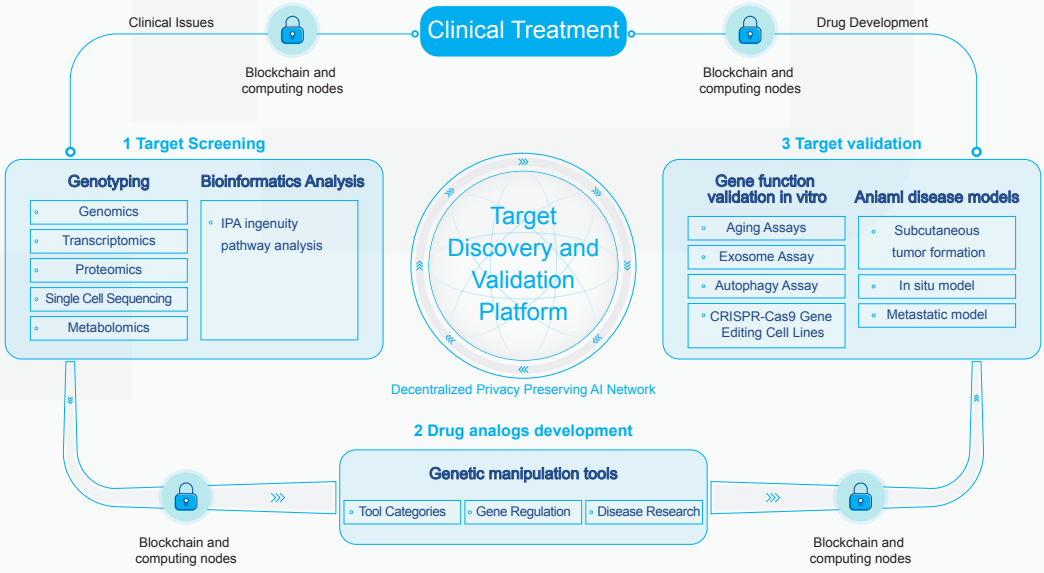
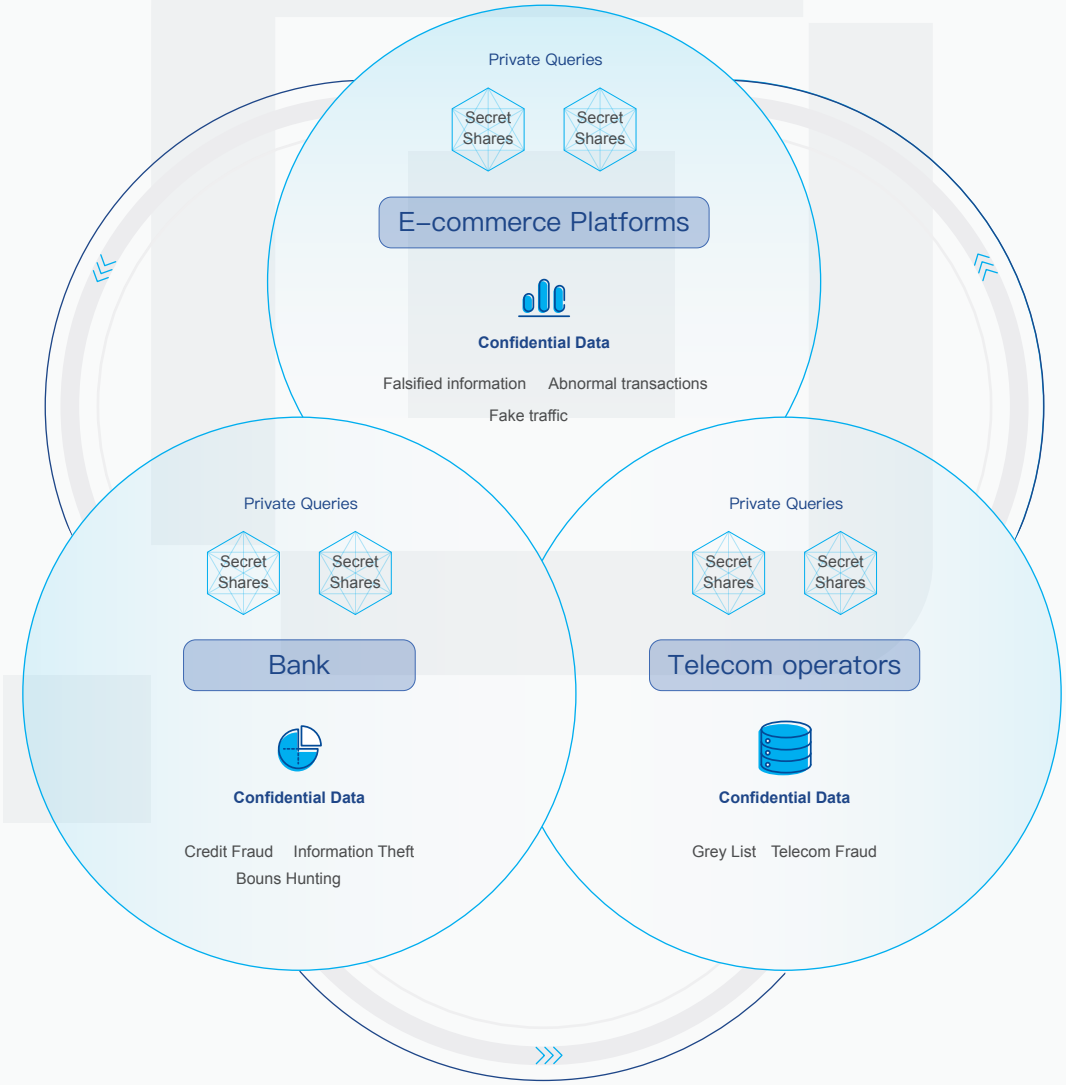


Figure 13: Privacy-preserving AI in Biomedicine

As an AI infrastructure, PlatON provides a credible data collaboration environment for hospitals, pharmaceutical companies, and various scientific research institutions etc. By integrating different types and fields of activities, research fields, operation modes and

data streams, PlatON forms a large-scale data aggregation effect, maximizing the value of pharmaceutical datasets, including clinical trials, medication use, electronic health records and patient genomics data, etc. Hence, it forms a data analysis and mining system for pharmacogenomics, disease genomics, network pharmacology, protein structure simulation and other technical means, thus accelerating the process for new drug discovery and R&D.

5.4. Financial Risk Control



Fgure 14: Privacy-preserving AI in Financial Risk Control

Operators, internet platforms, insurance institutions and other multi-party data institutions can use privacy-preserving computation technology to open more risk control private domain data tags to collaborate with banks in a confidential manner. The collaboration can better support the financial risk control business, realize the whole-process monitoring before, during and after the loan, and improve the timeliness of risk control.

Through the private set intersection (PSI) and privacy-preserving join query, the bank can facilitate the statistics and understanding of the customer's comprehensive credit risk, and does not disclose any party's customer ID and private domain data information, forming a joint risk prevention, joint control and joint ecology.

5.5. Smart City

After more than 50 years of development, the Internet has gradually evolved from a mesh-like structure to a brain-like model. In the 21st century, the intelligence of billions of human groups and the intelligence of tens of billions of machines will form a complex brain-like intelligent giant system of human-machine collaboration through the Internet brain architecture. Based on PlatON's multi-agent-based autonomous collaborative AI network, an intelligent collaborative network is formed with the combination of cloud group intelligence and cloud machine intelligence in the Internet brain architecture [9] in the figure below.

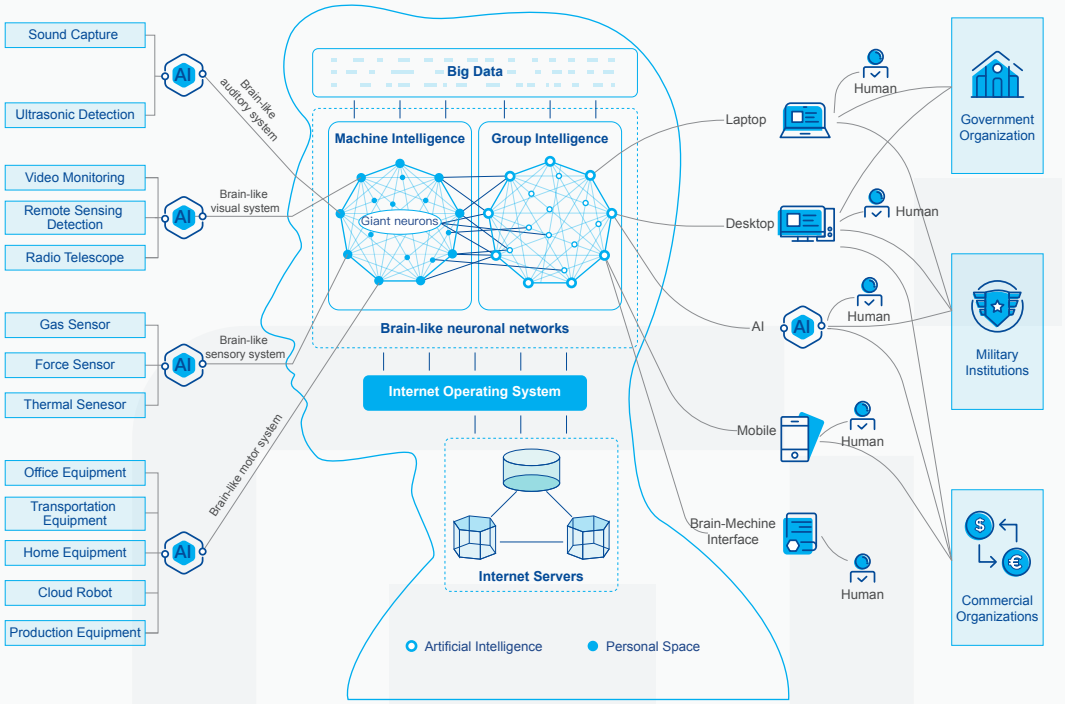


Figure 16: The Internet Brain Architecture [9]

Imagining such a specific scenario, in a smart city, a blockchain-based multi-agent AI digital services can provide smart mobile solutions in commercial real estate in the city center.

Take parking a car as an example. In a smart city, an autonomous agent in your car will search and communicate with a parking agent to find the nearest available parking space to your destination, make a reservation for you, and then guide your parking. When you return to drive away, your car agent automatically handles the departure formalities, calculates the parking fee and pays for you, eliminating the hassle of parking tickets.

AI agents can optimize resource use and reduce a city's carbon footprint, and we predict that largescale implementation of smart city infrastructure will result in a reduction of 34,000 tons of carbon dioxide emissions per year.

6 / LATs in PlatON

LAT is the native utility token which will capture the value around trustless coordination of actors within the PlatON network.

Clearing and settlement

LATs are used as payment and settlement tokens to pay for online economic activities such as service/asset transactions, transfer tokens. Users need to pay and settle transaction fees, service fees, data or computing power and other resource usage fees, and so on.

Network governance

In PlatON, LAT holders have the right to vote on the operation of the network, including the developer's work focus and the implementation time of software upgrades.

Staking service economy

LAT holders can stake their LAT to provide profitable services for the network, including transaction verification, computation, provision of data and algorithms, data annotation, etc. They can get rewards from network or users, such as block rewards, stake rewards, Transaction fees. LAT holders can delegate their LAT to the validator and get a certain reward share.

7 / Related Research and Progress

Since 2016, PlatON has established a research fund for privacy-preserving computation and recruited research teams around the world. Today, it has a large number of top cryptographic talents around the world, including professors and PhDs from major universities in China and the US.

Our research team has been carrying out and publishing exploratory in-depth research in the fields of cryptography, IoT, AI, economics and governance. Besides, the team has published relevant research papers on top journals and results at conferences.

- LEAF: A Faster Secure Search Algorithm via Localization, Extraction, and Reconstruction, In ACM CCS, 2020

We applied the research results to privacy-preserving AI by engineering and open sourced the privacy-preserving AI framework Rosetta. The project introduced secure multi-party computation algorithms into TensorFlow. Under the premise of being compatible with TensorFlow's original development interface, we have realized the data privacy protection in the process of AI model training and prediction.

We regularly fund academic research and conferences on cryptography and privacy-preserving computation, and conduct in-depth cooperation with various projects and research groups.

- The conferences we've sponsored including Crypto, Eurocrypt, Asiacrypt, CCS, AsiaCCS, IDASH, etc.

- We've participate in Ethereum's privacy-preserving computation project, for example, MPC implementation of Proof of Custody in Eth 2.0.

8 / Milestones

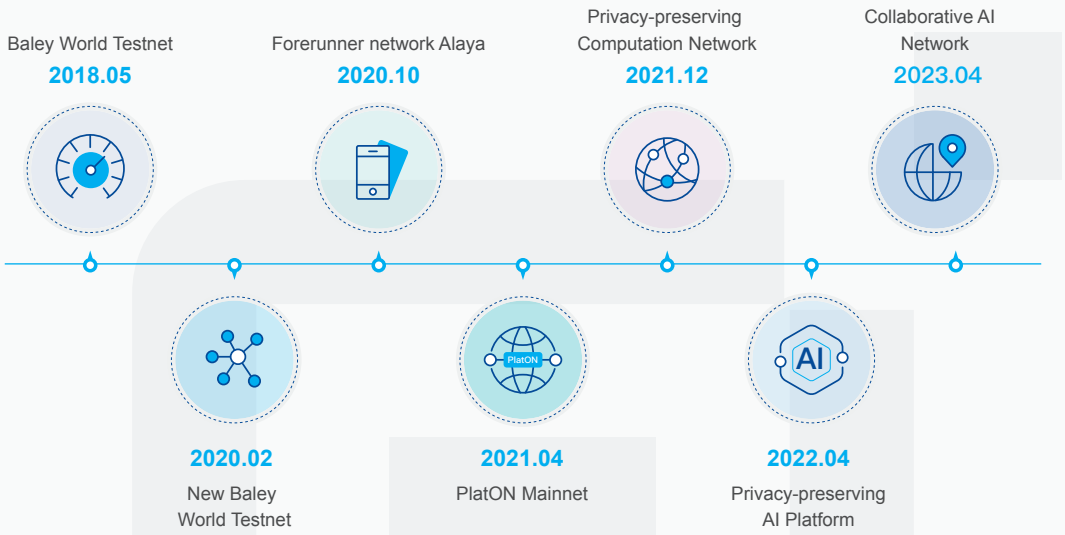


Figure 16: PlatON2.0 milestones

2018.Q4 the Belle World Test Network launch

- Open Source PlatON Belle World

2020.Q4 Alaya forerunner network launch

- High Performance Asynchronous BFT Consensus
- Staking Economic Model
- EVM and WASM dual virtual machine support
- Secure assets across chains
- DeFi platform and portal
- Privacy DeFi Capabilities

2021.Q2 PlatON Mainnet launch

- Increase the number of validators
- Optimized economic model
- Fully compatible with Ethereum

2021.Q4 Privacy-preserving Computation Network (Metis) launch

- Data/computing node networking
- Secure multi-party computation protocol
- Decentralized computation scheduling

2022.Q2 Privacy-preserving AI Platform (Moirae) launch

- Privacy-preserving AI development platform
- Privacy-preserving AI Service Marketplace
- Privacy-preserving AI economic incentive model

2023.Q2 Collaborative AI Network (Horae) launch

- AI agent interoperability protocol
- AI Oracle

References

[1] Data volume of IoT connected devices worldwide 2019 and 2025, Lionel Sujay Vailshery, Statista, Mar 2021.

[2] Data Age 2025, David Reinsel, John Gantz, John Rydning , IDC, April 2017and Nov 2018.

[3] New Version of My "Metaweb" Graph — The Future of the Net, http://www.novaspivack.com/science/new-version-of-my-metaweb-graph-the-future-of-the-net, Nova Spivack, April 2004.

[4] Top Strategic Technology Trends for 2022, Gartner, October 2021, https://www.gartner.com/en/information-technology/insights/top-technology-trends

[5] A PwC study of the economic impact of AI on the world's economy, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

[6] Global Artificial Intelligence Industry Whitepaper, https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-ai-report-en-190927.pdf, Deloitte,2019.09

[7] Artificial General Intelligence 2018–2023, Mind Commerce, 2018.

[8] Big Ideas Report 2021: https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/ARK%E2%80%93Invest_BigIdeas_2021.pdf, ARK INVEST, January 2021.

[9] 2020 City Brain Global Standards Research Report, City Brain Global Standards Research Group, 2020