MetaMesh

WHITE PAPER

MetaMesh

MetaMesh is an all-encompassing platform supported by blockchain technology

Goal

MetaMesh is an all-encompassing platform supported by blockchain technology, covering distributed supercomputing public chains, distributed storage systems, and scientific computing knowledge management tools.

Our vision is to eliminate trust barriers in the exchange of scientific research information and enhance the productivity of scientific research through the widespread use of MetaMesh, and in doing so, drive the pace of scientific research and technological progress.

We are committed to scientific research, especially around scientific computing in the process of scientific research.MetaMesh is designed to support and protect the computational instances carried out in the process of scientific computing, validate the process of computation, archive the results of computation, provide evidence of the results of scientific research, and provide traceability of scientific and technological achievements (including theses, patented technologies, etc.).

MetaMesh hopes to be a catalyst for the creation of a more adaptive and future-oriented scientific research ecosystem in the Internet era, disrupting the scientific research system that has been in place today for over 500 years. We firmly believe that there is a lot that can be done to improve and enhance the scientific research methodology, and MetaMesh is our bold attempt to do so.

For the future, we hope MetaMesh can strike a good balance between public participation and centralized management.

postscript

Digress

In modern technological society, Artificial Intelligence (AI) has become a key driver for the development of many fields, including economy, scientific research, and society. However, the development and application of AI faces a number of challenges, including the shortage of computing resources, data security and privacy issues, as well as the development and optimization of AI algorithms, etc. The goal of MetaMesh public chain is to solve these challenges by enabling all kinds of participants to obtain the required AI arithmetic on the public chain through distributed technology.

MetaMesh has an ambitious vision, but we understand it won't happen overnight. Every great journey has a starting point. In the development of MetaMesh, we have always adhered to the principle of "think big, start small" and have been steadfast in advancing our goals.

Roadmap (also fig.)

December 2019: The Birth of MetaMesh, the Beginning of a Great Journey

January 2020: MetaMesh initiators published a paper in the top international journal Science, introducing the idea of MetaMesh and winning wide attention and recognition from academia

March 2020: First version of distributed supercomputing network prototype released, attracting industry attention

May 2020: Received first round of venture capital to accelerate technology development and team expansion

September 2020: Establishment of partnerships with world-renowned research institutions such as Stanford University's Department of Computer Science and the European Center for Nuclear Research (CERN) to promote innovation and development of distributed supercomputing networks

December 2020: release of MetaMesh arithmetic storage tools

Release of MetaMesh Knowledge Graph Tool Chain, April 2021

Release of MetaMesh Public Research Indexing Toolkit, June 2021

September 2021: Completion of MetaMesh public chain 1.0 testing

February 2022: Successful deployment of a new generation of supercomputing nodes to enhance computational performance and data processing capabilities

Jun 2022: Launch of MetaMesh supercomputing cloud service to provide high-performance computing power cloud solutions to research organizations and enterprises

July 2022: Collaboration with Johns HopkinsUniversitySchoolofMedicine to crack medical problems using distributed supercomputing networks

September 2022: Start of MetaMesh public chain 2.0 testing

December 2022: Start the global expansion of the supercomputing network, with the goal of covering major cities and research centers around the world and providing efficient, high-performance computing support for global scientific research

2023-Future: To become the world's leading high-performance distributed supercomputing network, providing innovative solutions and excellent services for global scientific computing and artificial intelligence applications, leading the future of computational science, and contributing to the leap of civilization of mankind

Status and challenges of scientific computing

Scientific computing is an important engine for driving scientific research and technological progress. However, the field currently faces several important challenges:

1. Algorithm

Open-source software has now become the mainstay of scientific computing, with a large number of applications but a relatively high barrier to adoption. In contrast, commercial software often derives from open source software, which provides a better user experience but is expensive. Moreover, the development of open source software often relies on community support, which limits its speed and breadth of development to some extent.

2. Arithmetic

Currently, local workstations are widely used in scientific computing, but their software adaptation is difficult, their stability is insufficient, and their operation and maintenance are difficult. Although supercomputing platforms or service providers provide a large amount of arithmetic resources, they are expensive and inconvenient to operate and interact with.

3. Arithmetic examples

The modeling threshold for scientific computing is very high and the number of models is huge. Users need to learn complex command line submissions to load computational tasks, and the amount of computation is generally large. In addition, the threshold for calibration and value assessment of computational results is also very high.

MetaMesh: solving the challenges of scientific computing

To address the above challenges, we designed MetaMesh, a high-performance distributed supercomputing public chain. Our goal is to provide easier-to-use, more stable, and more optimized scientific computing solutions by using and popularizing MetaMesh.

Optimize algorithmic application experience:

MetaMesh aims to integrate and optimize open-source and commercial software to lower the threshold of scientific computing, while establishing a robust community ecosystem to drive algorithm development and optimization through blockchain technology.

Provide stable and efficient arithmetic resources:

MetaMesh solves the problem of obtaining arithmetic resources through a distributed supercomputing network. Our network not only provides stable and efficient arithmetic resources, but also reduces the difficulty of operation and maintenance and provides a better operation experience.

Solving the Calculation Instance Conundrum:

MetaMesh lowers the threshold for modeling and evaluation through blockchain technology, which enables the traceability and fairness of calculation instances.

Blockchain technology

What is blockchain? From a scientific and technological perspective, blockchain involves many scientific and technological issues such as mathematics, cryptography, the Internet and computer programming. From the application perspective, simply put, blockchain is a distributed shared ledger and database, with the characteristics of decentralization, tampering, traceability, traceability, collective maintenance, openness and transparency. These features ensure the "honesty" and "transparency" of blockchain, and lay the foundation for blockchain to create trust. The rich application scenarios of blockchain are basically based on the ability of blockchain to solve the problem of information asymmetry, and to realize collaborative trust and concerted action between multiple subjects.

Blockchain is a new application model of computer technology such as distributed data storage, peer-to-peer transmission, consensus mechanism, and cryptographic algorithms. Blockchain, a key concept of Bitcoin, is essentially a decentralized data

The library, which also serves as the underlying technology for Bitcoin, is a string of data blocks generated using cryptographic methods associated with each block containing information about a batch of Bitcoin network transactions used to validate the validity of their information (anti-forgery) and to generate the next block.

Blockchain technology features

In a typical blockchain system, data is generated and stored in blocks and linked into a chained data structure in chronological order. All nodes are involved in data validation, storage and maintenance of the blockchain system. The creation of a new block is usually confirmed by a majority (the number depends on different consensus mechanisms) of nodes across the network, and broadcasted to each node to achieve network-wide synchronization, after which it cannot be changed or deleted.

Externally, a blockchain system should have the following characteristics.

·Multiple writers, joint maintenance

Multiple parties in this context refer only to bookkeeping participants and do not include clients using the blockchain. The bookkeeping participants of a blockchain should consist of multiple entities with incomplete alignment of interests, and different participants will take the lead in initiating bookkeeping in different bookkeeping cycles (the rotation will depend on different consensus mechanisms), while the other participants will co-verify the bookkeeping information initiated by the lead party.

·open book

The ledger recorded by the blockchain system should be in a state where all participants are allowed to access it, and in order to verify the validity of the information recorded by the blockchain, the bookkeeping participants must have the ability to access the information content and the history of the ledger. However, public ledger refers to the openness of accessibility and does not mean the openness of the information itself. Therefore, the industry expects to apply many privacy-preserving techniques, such as zero-knowledge proof, homomorphic encryption, and threshold encryption, to the blockchain field in order to solve the problem of verifying the validity of the information by means of ciphertext operation.

·decentralization

The blockchain should be a system that does not rely on a single trust center, and the blockchain itself is capable of creating trust between participants when dealing with data that only involves a closed system within the chain. However, in some cases, such as identity management and other scenarios, external data will inevitably be introduced, and these data require trust endorsement from a trusted third party, at this time, for different types of data, the trust should come from different trusted third parties, rather than relying on a single trust center. In this case, blockchain itself does not create trust, but acts as a carrier of trust.

·Not be tampered with

As the most significant feature of blockchain, tamperability is a necessary but not a sufficient condition for blockchain system, and there are many hardware-based technologies that can also realize that data can be written once, read many times and cannot be tampered with, such as the one-time burning of compact disks (CD-R), as a typical example. Blockchain is tamper-proof based on cryptographic hashing algorithms, as well as multi-party co-maintenance features, but at the same time, due to this feature, blockchain tamper-proof is not strictly speaking, it is more appropriate to call it difficult to tamper with.

MetaMesh Technology Solutions

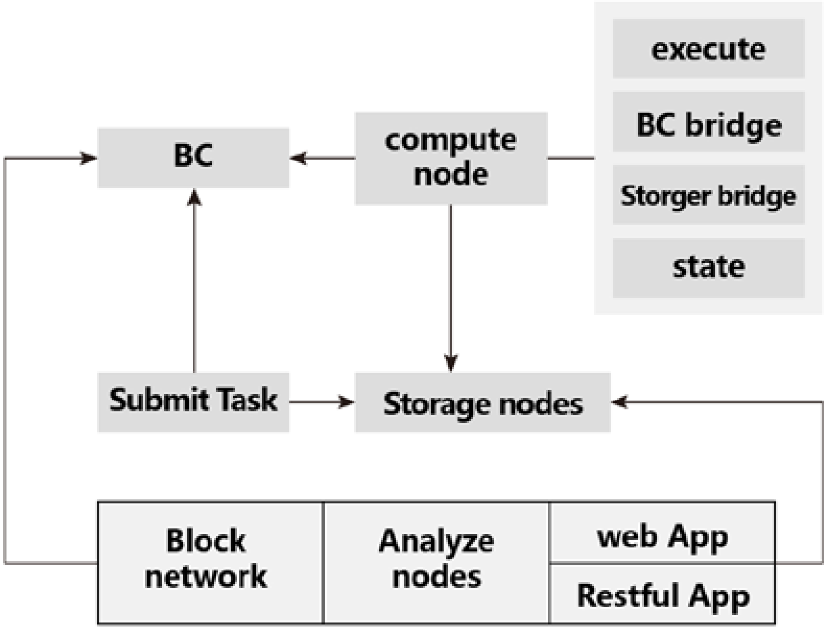
MetaMesh is not just a single blockchain, but a holistic platform that includes a blockchain public chain, a distributed storage system, and scientific computing knowledge management tools.

Technical architecture

MetaMesh nodes include three types: ledger nodes, storage nodes, and computation nodes.

For blockchain, ledger nodes are relatively easy to understand, that is, nodes that are capable of distributed bookkeeping. Storage nodes, which are still blockchain nodes, do not participate in bookkeeping, but perform data storage, data storage

The types of scientific computing are diverse and continue to develop, so the computing nodes need to effectively balance the cost investment and adaptability, MetaMesh will be effective incentive mechanism, incentives for computing nodes to continue to improve the processing capacity, through the governance and incentives to gradually realize the balance, is the basic principle of the construction of the MetaMesh.



MetaMesh public chain

The MetaMesh public chain is a core part of the technology solution, which provides a decentralized collaboration platform for storage and compute nodes while underpinning the operation of a global distributed supercomputing network.

The design principle of MetaMesh public chain is to build a high-performance distributed supercomputing network that is open, transparent, safe and reliable by using the distributed, decentralized and trustworthy characteristics of blockchain technology. Our vision is to reduce the trust barriers in scientific research information exchange and improve the efficiency of scientific research production conversion through the wide application of public chain, which in turn can influence the speed of scientific research and technological progress.

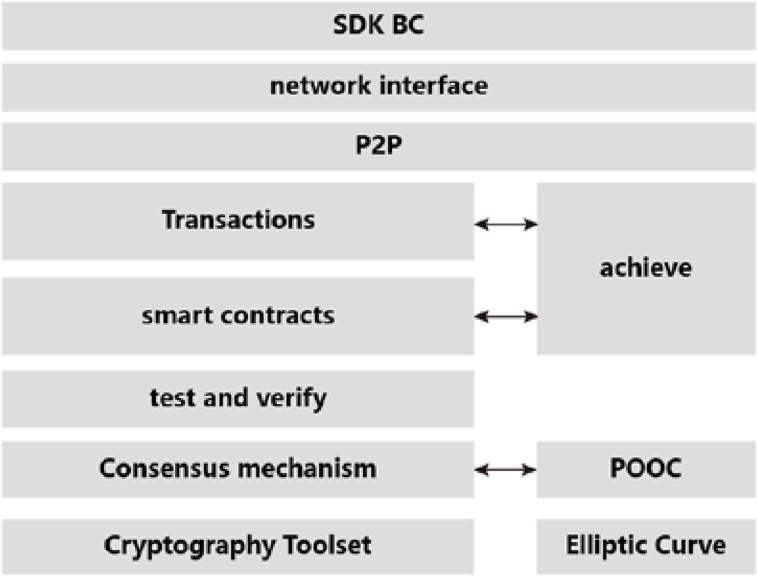
Fabric

The MetaMesh public chain consists of several important parts:

Blockchain Network : A blockchain network consists of multiple bookkeeping nodes that are responsible for performing distributed bookkeeping on the network. These nodes use a consensus mechanism to validate and record all transactions in the network.

Storage Nodes: storage nodes are another important component of the MetaMesh public chain and they are responsible for storing data in the network. Although these nodes are not involved in bookkeeping, they provide key functionality in terms of data storage and access.

Computing Nodes: Computing nodes are the part of the MetaMesh public chain that performs scientific computing tasks. These nodes need to handle diverse and continuously evolving scientific computing tasks, so MetaMesh needs to continuously incentivize these computing nodes to improve their processing capabilities through effective incentives and governance strategies, and gradually achieve a balance between cost investment and adaptability.



Based on POA consensus

1. Characteristics of PoA

· PoA relies on predefined authorized nodes (signers), which are responsible for generating blocks.New signers can be added by election (voting more than 50%) of the authorized signers.

· Even if there is a malicious signer, he can only attack at most 1 of the consecutive blocks (the number is (SIGNER_COUNT/2)+1), during which other signers can vote to kick out the malicious signer.

· The time at which the block is generated can be specified.

2.PoA algorithm flow

Specify a group of initially authorized signers in the genesis block, all addresses are stored in the genesis block Extra field to start mining, the group of signers start signing and broadcasting the generated blocks.Specify a group of initially authorized signers in the genesis block, all addresses are stored in the genesis block Extra field to start mining, the group of signers start signing and broadcasting the generated blocks.

The signature result is stored in the Extra field of the block header, which is updated with the addresses of all authorized signers at the current height as new signers are added or kicked out. one signer at each height is in the IN-TURN state, and the others are in the OUT-OF-TURN state, and the block signed by the IN-TURN signer is broadcast immediately, while the block signed by the OUT-OF-TURN signer is delayed for a random period of time before broadcasting, ensuring that the IN-TURN signer has the right to broadcast. The block signed by the IN-TURN signer will be broadcast immediately, and the block signed by the OUT-OF-TURN signer will be delayed for a little bit of random time before broadcasting, so as to ensure that the block signed by the IN-TURN signer will have a higher priority to be uploaded to the chain. If there is a need to add a new signer, the signer initiates a proposal through the API interface, and the proposal is sent to the signer by multiplexing the block header Coinbase (the address of the new signer) and Nonce("0x⊠⊠⊠ a⊠⊠ect") fields are broadcast to other nodes. All the authorized signers vote for the new signer to "join", if the affirmative vote is more than 50% of the total number of signers, they agree to join. If an old signer needs to be kicked out, all authorized signers vote "kick out" on the old signer, if the yes vote is more than 50% of the total number of signers, it means yes to kick out.

3. PoA block header signature algorithm

- Signing of BlockHeader by Signer
- Extra is at least 65 bytes long (signature results in 65 bytes, i.e. R,S,V,V is 0 or 1)
- RLP encoding of all fields in the BlockHeader except the 65 bytes of Extra
- Keccak256hash on the encoded data
- The signed data (65 bytes) is saved into the last 65 bytes of the Extra

4. PoA authorization strategy

The following recommended strategies will reduce network traffic and forking:

- If the signer is allowed to sign a block (in the authorization list, but not recently signed).
- Calculate the optimal signature time for the next block (parent block time + BLOCK_PERIOD).
- If the signer is in-turn, sign and broadcast block immediately.
- If signer is out-of-turn, delay rand(SIGNER_COUNT*500ms) before signing and broadcasting

5. PoA voting strategy

Because blockchains may reorganize in smallreorgs, regular voting mechanisms (cast-and-forget) may not be optimal, as blocks containing individual votes may not be on the final chain, because the most up-to-date block is already on the chain.

block and be discarded.

A simple but effective way is to configure signers with a "proposal". For example, "add0x..." , "drop0x..." , when there are multiple concurrent proposals, the signing code "randomly" selects a proposal to be injected into the block signed by the signer, so that multiple concurrent proposals and reorgs can be kept in the chain. The list may expire after a certain number of blocks/epoch, and just because a proposal passes doesn't mean it won't be re-invoked, so it shouldn't be discarded as soon as it passes.

- Votes to add and kick out new signers are immediate and participate in the next vote count.

☒Both joining and kicking out require a vote of more than 50% of the total number of current signers

- Can kick yourself out (also requires more than 50% vote)
- Parallel voting is possible (A,B cross vote C,D), as long as the final vote count operates at 50%.
- Entering a new epoch, all previous pending votes are nullified, and the vote counting starts again.

6.Attacks and defenses in PoA

· Malicioussigner

A malicious user is added to the signer list or the signer key/machine is compromised. The solution is a list of N authorized signers, any one signer can only sign 1 of them for every K blocks. This minimizes damage and the rest of the miners can vote to kick out the malicious user.

· Censoringsigner

If a signer (or a group of signers) tries to check the offers of other signers in the block (in particular to vote to kick them out), to solve this problem we limit the allowed mining frequency of a signer to 1/(N/2). If he doesn't want to be kicked out, he has to control more than 50% of the signers.

· Spammingsigner

These signers injec[illegible] new vote proposal into each block they sign [illegible]e the nodes need to count all the votes [illegible] a list of authorized signers, over tim[illegible] number of spammy and useless votes w[illegible]ated, causing the system [illegible] Through the mechanism of epoch, each time [illegible]h is entered, th[illegible]cks are discarded. If the number of authorized sign[illegible] allow e[illegible] to [illegible]

Then at any given [illegible] block ca[illegible]sfully signed by [illegible] N-K signers.To avoid these blocks comp[illegible]g), each [illegible]erates a ne[illegible] with a little random delay. This ensures [illegible]icult for [illegible]r.

MPT Tree Based Ledger Implementation

MerklePatriciaTree (also known as MerklePatriciaTrie) is a modified data structure that combines the advantages of both Merkletree and PrefixTree tree structures, and is used to organize and manage account data and to generate important data structures for the hashing of transaction collections.

1. Concept:

State of the world: the state data of all accounts (including contract accounts and ordinary accounts) are collectively referred to as the state of the world; Light node: refers to a blockchain node that only stores block header data;

Blockchain forks: a situation where 2 blocks pointing to the same parent block are generated simultaneously, with some portion of miners seeing one of the blocks and others seeing the other. This results in 2 blockchains growing at the same time;

Block header: refers to a part of the block structure, used to store the block's header information, such as the parent block hash, the world state hash, the transaction receipt collection hash, and so on. The block header only stores some "fixed" length hash fields;

2. the role of the MPT tree:

- Stores key-value key-value pair data of arbitrary length, conforming to the state model;
- Provides a mechanism to quickly compute hash identifiers for maintained datasets;
- Provides a mechanism for fast state rollback;
- A proof method called Merkle's proof is provided to perform light node extensions for simple payment verification;
- MPT combines the features and advantages of both Radixtrie and Merkle tree structures.

3. Structure of the MPT:

Leaf nodes and branch nodes can hold value, extension nodes hold key;

No common key becomes 2 leaf nodes; key1=[1,2,3] key2=[2,2,3];

There are common keys that need to be extracted as an extended node; key1=[1,2,3]key2=[1,3,3]=>ex-node=[1], the next level supports the key of the node;

If the common key is also a complete key, the data is saved to the next level branch node; key1=[1,2]key2=[1,2,3]=>ex-node=[1,2],the key of the next level branch node; the next level branch=[3],the value corresponding to the previous level key.

Distributed storage

MetaMesh hopes to strike a good balance between public participation and centralized management. Scientific research results and processes generate a large amount of data, the ownership of which rightfully belongs to its creators and not to any intermediary/commissioning agency. In the past, entrusted organizations have been taking the initiative in the distribution of the value created by scientific research data by taking advantage of the traffic portal entrance, which is unavoidable at this stage.MetaMesh hopes to enable a more equitable distribution of benefits from scientific research data (including the results), and needs to be more skillful in its ownership. Therefore, the basic idea of MetaMesh design is to store the encrypted research data in a distributed storage network, which should be efficient and continuously scalable.

IPFS

IPFS, InterPlanetary File System IPFS (InterPlanetaryFileSystem, is a peer-to-peer distributed file system.

(1) IPFS is a distributed, decentralized storage and single bittorrent cluster using git.

(2) IPFS generates addresses based on content and thus provides a high-throughput content-addressed storage model.

(3) IPFS is mainly built as a versioning file system through the Merkle tree data structure.

(4) IPFS does not have a separate point of failure, and the nodes are not required to trust each other.

IPFS is a globally distributed, peer-to-peer version of a file system that connects all computing devices with the same file system, with the primary goal of complementing (or even "replacing") the Hypertext Transfer Protocol (a.k.a. HTTP), which we currently use to dominate the Internet.

IPFS utilizes content-based addresses to replace domain-based addresses, and users looking for content stored somewhere, rather than an address, will only need to confirm the hash that verifies the content, so they can over get faster, secure, robust, and persistent web pages.

The IPFS architecture can be categorized into the following 8 layers:

(1) Network: for better decentralized computing.

(2) Identity layer (Identity): manages node identity generation and authentication.

(3) Exchange layer (Exchange): a new block swap protocol (BitSwap) that supports efficient block allocation, simulates a trusted market, weakens data replication, and prevents cheating.

(4) Routing: maintains information to locate specific peers and objects. Responds to local and remote queries. Defaults to DHT, but can be replaced.

(5) File: A Git-inspired hierarchy of versioned file systems.

(6) Naming: a self-authenticating variable name system.

(7) Application layer (Application): applications running on IPFS.

(8) Objects: MerkleDAGs with linked content-addressable immutable objects for representing arbitrary data structures, such as file hierarchies and communication systems.

IPFS-based research data storage

MetaMesh supports IPFS-based research data storage. With the toolkit provided by MetaMesh, research data can be encrypted and stored on the IPFS network, and MetaMesh will also provide support for IPFS to ensure that IPFS can meet the storage performance requirements of the scientific computing chain.

MetaMesh Knowledge Management Tool

Focusing on the specific needs of scientific computing, MetaMesh's knowledge management tools provide a range of tools with a high degree of specialization, including knowledge graphs and knowledge bases.

Knowledge map

The concept of knowledge graph was proposed by google in 2012, when it was designed to upgrade the traditional keyword-base search model to semantic-based search. Knowledge graph can be used to better query complex associated information, understand user intent at a semantic level and improve search quality.

In the field of scientific computing, knowledge graphs are regarded as a powerful tool that can graphically represent complex associative information, providing deep understanding and accurate querying of large-scale scientific computing data. The power of knowledge graphs lies in its ability to visually describe and understand data, while at the same time, it can well compensate for the lack of descriptive ability of machine learning algorithms.

Repository

MetaMesh's knowledge bases are divided into two types: CuratedKBs and ExtractedKBs. CuratedKBs carefully filters and organizes a large number of entities and their relationships extracted from various knowledge bases such as Wikipedia and WordNet. ExtractedKBs, on the other hand, extracts entity-relationship triples from web pages through big data techniques to provide a richer knowledge background for scientific computing.

ExtractedKBs: mainly represented by OpenInformationExtraction(OpenIE), Never-Ending Language Learning(NELL), they directly extract entity-relationship triples from hundreds of millions of web pages. Compared with freebase, the entity knowledge thus obtained is more diversified, while their entity relations and entities are more in the form of natural language, such as "Yao Ming was born in Shanghai." can be represented as ("YaoMing", "wasalsoborn-in", "Shanghai"). Knowledge extracted directly from web pages will also have some noise and its accuracy is lower than CuratedKBs.

CuratedKBs: represented by yago2 and freebase, they extract a large number of entities and entity relationships from knowledge bases such as Wikipedia and WordNet, which can be understood as a kind of structured Wikipedia in the city.

MetaMesh Knowledge Toolset

To enable researchers and software technology developers to better utilize this knowledge, MetaMesh offers a range of tool sets, including:

1. Knowledge Encryption Toolkit: Safeguard the security of knowledge data and prevent data leakage during transmission and storage.

2. Zero-knowledge proofing toolkit: provides a guarantee of data integrity and correctness, ensuring that the authenticity of the data is verified without revealing specific information.

specific information.

3. Storage Toolkit: Provides efficient solutions for storing and managing data, supporting fast access to large-scale data.
4. Knowledge Graph Toolkit: Provides tools for creating and querying knowledge graphs to support in-depth understanding and accurate querying of scientific computing data.
5. Machine Learning Toolkit for Scientific Computing: Provides a range of machine learning algorithms and models to support the optimization and automation of scientific computing.

These tools not only help researchers and software technology developers to better utilize MetaMesh's data resources, but also provide strong support for them to further develop more interactive tools or systems that are more suitable for specific research areas.

Technical Highlights of MetaMesh

Generation and validation of data records based on State secrets

One of the main challenges to be solved in blockchain systems is known as the "double-spendattack": what happens if there are two transactions in the network, both trying to spend all the money in the same account (so-called conflicts)? Do the transactions conflict with each other?

The simple answer is that you don't have to care. The network automatically selects a sequence of transactions for you and packages them into so-called "blocks", which are then executed and distributed among all participating nodes. If two transactions contradict each other, the one that is eventually recognized as having occurred later will be rejected and will not be included in the block.

These blocks form a linear sequence over time, which is where the term "blockchain" comes from. Blocks are added to the chain at regular intervals.

As part of the "sequential selection mechanism" (also known as "mining"), there may be times when blocks are rolled back, but only at the "end" of the chain. "The more blocks are added to the end of the chain, the more blocks are rolled back. The more blocks that are

State secret-based block record signatures and verification

The process of signing a MetaMesh is as follows.

Signature operation.

1. Calculate the Hash value of the original data;

2. Use the Hash value as input to compute the output of the signature function. It is not a direct signature on the original data, but a signature on the Hash value.

The following actions should be performed when verifying signatures:

1. Calculate the Hash value of the original data;
2. Hash value and signature value as input, calculate the output of the signature check function, according to the output to determine the signature is "valid" or "invalid".

According to the domestic industry standard, the SM2 signature algorithm is to be used in conjunction with the SM3Hash algorithm, and the input to the computation of the SM2 signature is the output of a preprocessing stage.

The preprocessing is divided into two steps:

1. define a cascade-generated byte stream T1=ENTL||ID||a||b||x_G||y_G||x_A||y_A, where || denotes the splicing of the byte stream.

ENTL is the bit length (note that it is not a byte length) of the signer's ID expressed in two bytes, with the ID being the identifier of the signer.

a,b,x_G,y_G are the values given in the standard and x_A and y_A are the public key of the signer.The SM3 hash value is computed for the byte stream T1 and the output obtained is Z=SM3(T1).

This step does not use the data to be signed.

2. denote the data to be signed by M, and cascade Z with the data to be signed to obtain T2 = Z||M.

Compute the hash value of T2, i.e., SM3(T2), which is the real input to the SM2 signature function.

When verifying a signature, it goes through the same preprocessing process, using the output of the preprocessing stage, the signature value, as input to the signature checking function.

Zero-knowledge proofs for MetaMesh

The domains involved in scientific computing are so diverse that there is no possibility of realizing non-interactive zero-knowledge proofs of computational processes and computational results in each domain in a single way.

The MetaMesh design scheme is based on zkSnark, using libSnark as an implementation with a scalable and selectable processing engine for zero-knowledge proof support by supporting different R1CS for different computations.

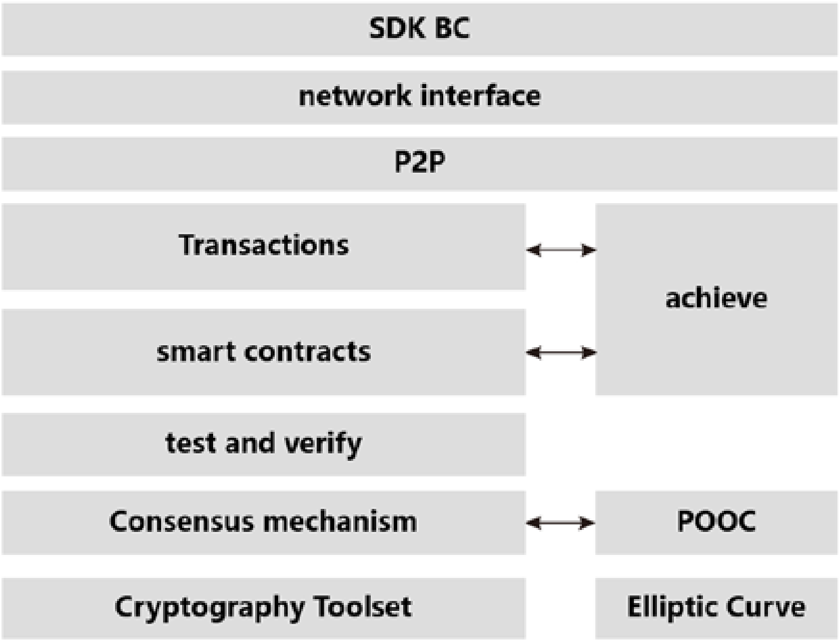
Proof of Zero Knowledge: Proof of Zero Knowledge is a cryptographic technique that enables a party to prove to another party that it knows or possesses certain information without having to tell the other party that information directly. This technique has important applications in protecting user privacy and enhancing system security.

zk-SNARKs: zk-SNARKs are a special type of zero-knowledge proofs that are both non-interactive (i.e., a single message transfer is sufficient for the prover to prove his knowledge or possession of certain information) and concise (the size of the proof itself and the computational effort to verify the proof are small). This property makes zk-SNARKs ideal for blockchains and other distributed systems.

libSNARK: libSNARK is a C++ library that provides tools and functionality for building zk-SNARK proofs. libSNARK has the advantage that it can be used to implement a wide variety of different zero-knowledge proof schemes, and it provides a rich library of interfaces and functions that enable developers to customize the proof system to meet specific needs.

In MetaMesh, we use libSNARK to build an extensible and selectable processing engine that is capable of supporting different Rank-1 Constraint Systems (R1CS) for zero-knowledge proof support.R1CS is a constraint system for describing complex computations, which reduces a complex computational problem to a set of linear relations, which allows computational problems to be more easily adapted to zk-SNARKs proof systems.

For different scientific computing tasks, the MetaMesh system is able to select suitable R1CSs for the generation and validation of zero-knowledge proofs. This flexibility and scalability enables the MetaMesh system to efficiently support a wide range of different scientific computing tasks and provide strong support in protecting the privacy of computational data and ensuring the correctness of computational results.



SDK BC

network interface

P2P

Transactions

smart contracts

achieve

test and verify

Consensus mechanism

POOC

Cryptography Toolset

Elliptic Curve

MetaMesh Blockchain-based Arithmetic Network for Artificial Intelligence

The operating model of the MetaMesh network allows for the presence of AI arithmetic service providers.AI arithmetic service providers can build their own AI arithmetic centers by leasing an IDC room.Through the MetaMesh blockchain, they can fairly authenticate the type, arithmetic size, and online status of the AI training and inference chips, thereby confirming their total arithmetic on the MetaMesh network.The AI arithmetic service providers are also allowed to use the MetaMesh blockchain as a tool to provide AI training and inference services. power on the MetaMesh network.

However, AI Computing Power ≠ AI Computing Power Services. What the buyer of an order of computing power needs is a high-quality AI computing power service for AI model training and deployment. The online AI computing power is only one of the production factors of AI computing power service. In order to provide AI computing power services, service providers also need to purchase CPU servers, hard disks, rent network bandwidth, ensure a stable power supply for AI servers, and other production factors.

So, how do you measure and ensure the quality of AI arithmetic services? This is an important question. We have designed an efficient off-chain AI arithmetic network solution for MetaMesh blockchain to efficiently connect arithmetic service providers' AI arithmetic centers around the world to achieve efficient sharing and circulation of multiple elements such as data, arithmetic, algorithms, models, and services.

And, we also designed a quality scoring mechanism for AI arithmetic services based on MetaMesh blockchain. The chain can track and publicize the transactions between buyers and sellers of arithmetic services. The on-chain provides public verification capability and the off-chain provides efficient productivity in the age of intelligence. The combination of on-chain and off-chain can maximize incentives for AI computing power service providers to join the MetaMesh network, reduce the cost of computing power usage, promote the unified settlement of heterogeneous computing power in different places, make the production, distribution, circulation and consumption of AI computing power more smooth, and improve the efficiency of market operation. Our goal is to build a worldwide AI computing power infrastructure with easy access to computing power resources, efficient and unified task scheduling, convenient and inexpensive use by users, and a sustainable operation model and mechanism.

In the platform layer of MetaMesh smart computing network, we designed four sub-platforms: a one-stop platform for debugging and training deployment of smart computing centers, a platform for unified scheduling and management of smart computing network tasks, a platform for unified storage and management of smart computing network data, and a marketplace for smart computing network data.

· Smart Computing Network Task Unified Scheduling and Management Platform:

The Unified Scheduling and Management Platform for Artificial Intelligence Tasks will effectively schedule and manage different types of online resources in different IQ centers to improve the utilization and efficiency of the entire IQ network. Function:

Collecting resource information:

Arithmetic resources include not only TPUs, but also CPUs, GPUs, NPUs, GPGPUs, FPGAs, and so on. Network resources include Internet with dedicated lines, public network, supercomputing intranet under controlled management, smart computing intranet under controlled management, etc. Data resources include public datasets of various AIs, private datasets of users, etc. Each resource on the network has its unique advantages and applicable scenarios.

Integration of resources:

According to the different minimum granularity of each heterogeneous resource, AI tasks are often required to combine a single type of arithmetic resource with different types of heterogeneous resources to form a resource package, which is assigned to the most suitable task requirements to optimize the task completion efficiency and resource utilization.

Managing jobs:

each AI job often contains multiple nested tasks, called subtasks, and individual subtasks can be dispatched to different smart computing centers in a distributed manner, and successful job scheduling will constitute a network of subtasks required for the job. In due course, it is necessary to monitor and manage the operation status and performance of jobs and subtasks, so that problems can be detected and dealt with in a timely manner.

Scheduling jobs:

The platform schedules the jobs submitted by users, and schedules the various sub-tasks included in the job to run in the appropriate IQC based on the load of the IQCs, data location, arithmetic price factors, communication efficiency, and the demand for job resources in order to maximize the efficiency of the task completion and the utilization of resources.

Scheduling strategy:

a number of scheduling factors will be used as inputs to process the candidate IQCs that meet the job resource requirements using certain processing logic, and output a normalized score for each IQC. The output of each scheduling polylog will be used as the input model of the scheduling evaluation model for further comprehensive decision making. The scheduling strategies are determined according to the actual scenario requirements, and the optional scheduling strategies are load-minimum priority, resource-idle priority, data affinity, arithmetic-price-minimum priority, arithmetic-performance-maximum priority, network-performance priority, and so on.

Scheduling factors:

scheduling factors are selected according to actual scenario requirements, and scheduling factors can also be customized. Optional scheduling factors include: job requirements, resource requirement specifications, data location, arithmetic price arithmetic performance, and load of intelligent computing centers.

Scheduling Evaluation Model:

The outputs of multiple scheduling policies will be used as inputs to the evaluation model, which calculates the optimal ICC to obtain the final scheduling result. The following evaluation model is used: for a job waiting to be scheduled, the scheduling policy S1 is used

· Smart Computing Network Data Unified Storage and Management Platform:

This is a platform for unified management and storage of all IQN data. Regardless of which IQC generates the data or which user uploads it, it will be managed and stored uniformly on this platform. This will make the data more secure and easier to manage and use.

·Smart Computing Network Data Market:

Smart Computing Network Data Marketplace is a platform for trading data. Users can buy or sell the data they need or have on this platform. The existence of this platform makes it easier for data to be traded between different users, thus increasing the operational efficiency of the entire Wisdom Computing Network.

Algorithmic Model Library for MetaMesh

In order to enable users to quickly start AI projects on MetaMesh, we have built a rich library of algorithmic models. This library integrates a variety of pre-trained models, providing users with models for a wide range of AI application scenarios, from image classification and speech recognition to natural language processing and deep learning.

·Pre-trained models

Our algorithmic model library integrates a large number of pre-trained models, such as ResNet, BERT, GPT, DNN and so on. These models can help users start quickly in various AI projects and lower the threshold of AI.

·Model sharing and reuse

On MetaMesh, users can upload their trained models to the algorithmic model repository for other users. This not only promotes model sharing and reuse, but also helps users earn additional revenue.

·Model Evaluation and Optimization

We have set up a set of evaluation mechanisms for each model, which allows users to evaluate the models based on their accuracy, complexity, applicability scenarios, and other factors. In this way, other users can refer to this evaluation information when choosing a model and select the most suitable model for themselves.

·Model Protection and Privacy

To protect users' model rights, we copyright every model uploaded to the model library. Also, to protect users' privacy, we encrypt the models to ensure

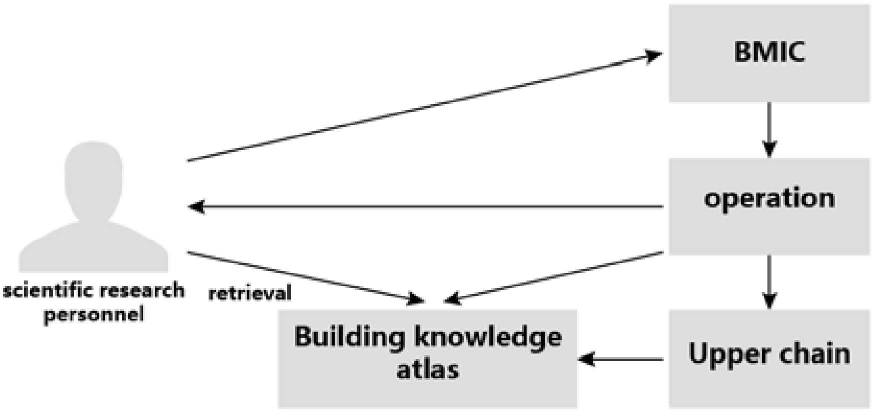
MetaMesh Application Scenarios

·Search for Specific Compound Research Results

BMCI (BoronMaterialComputingIndex), a Boron Scientific Computing Index database system, is currently under construction.

Through BMCI, researchers working on boron compounds can search all the open literature, information, scientific computing programs and scientific computing results related to boron and boron compounds, and through BMCI, they can submit their cases to BMCI after authorization. At the same time, through BMCI, boron researchers can submit their algorithms to BMCI after authorization, and BMCI will submit the corresponding data to MetaMesh public chain, and BMCI can also make use of the computing resources of the scientific computing chain, so if researchers are willing to wait for the scheduling of the algorithms, they can submit their algorithms to BMCI, and the corresponding algorithms can be computed when there are computational resources available, and the results are automatically archived, documented, and verified. And the calculation results are automatically archived, documented and organized, and directly entered into BMCI's boron knowledge graph.

BMCI Operations Process:



BMCI is operated and maintained entirely by volunteers on a public interest basis, and BMCI's depository function ensures that the pre-eminence of scientific research results is effectively proven.

·Drug research and development

In the field of drug research and development, MetaMesh can serve as an important tool. Through this platform, researchers can retrieve relevant literature, data, and computational results to assist them in multiple phases of research, including new drug discovery, efficacy prediction, and drug design. Similarly, researchers can utilize MetaMesh's computational resources to perform complex simulations and predictions, thereby accelerating the drug development process.

·Climate change research

MetaMesh can be used for global climate change research. Scientists can retrieve and analyze various climate data on MetaMesh to draw scientific conclusions about climate change. In addition, MetaMesh can utilize its vast computational resources to model and predict climate change trends and impacts.

·Artificial Intelligence Research

Artificial Intelligence (AI) researchers can use MetaMesh to obtain training data for algorithm development and model training. In addition, AI researchers can use MetaMesh's computational resources for large-scale model training and optimization to accelerate the development of AI technologies.

·bioinformatics

In the field of bioinformatics, MetaMesh can provide massive gene sequence data and protein structure data, providing powerful support for gene research, protein design, and so on. At the same time, MetaMesh's computational resources can also help bioinformaticians perform complex simulations and predictions to accelerate the development of biotechnology.

·Education

Educational institutions can utilize the resources provided by MetaMesh to provide a hands-on learning platform for their students. For example, students can run their science experiments on MetaMesh, get the results, and archive and deposit them, which will greatly improve the quality of teaching and learning.

·Energy Research

MetaMesh can be used for research and development of new energy materials, such as solar cells, fuel cells and energy storage systems. Researchers can utilize MetaMesh's computational resources to perform simulations and predictions, thereby accelerating the research and development process of new energy technologies.

MetaMesh Economic Modeling

In MetaMesh's economic model, we aim to build a fair, sustainable, and thriving ecosystem that provides attractive incentives for users and participants. Below is an overview of the MMT tokens:

Total MMT supply: 2.3 billion

Token distribution:

30% of the token supply is allocated to the MetaMesh founding team and advisors for program development, operations and long-term growth.

25% of the token supply is allocated to community building to reward community contributors, developers and promoters.

20% of the token supply is allocated to the Ecosystem Development Fund to support the network's infrastructure, technology development and ecosystem expansion.

15% of the token supply is distributed through airdrops and social media campaigns to attract more users to participate and promote MetaMesh.

10% of the token supply is used for private placements and initial investors to support the launch and initial development of the program.

Incentives for MMT tokens:

User Participation Rewards: MetaMesh has designed a set of token incentives to reward users for contributing computational resources, participating in network governance, engaging in consensus mechanisms, and promoting the MetaMesh ecosystem.

Developer Incentives: MetaMesh offers a developer incentive program that encourages developers to build MetaMesh-based apps, tools, and smart contracts that contribute to the growth and innovation of the ecosystem.

Community Contribution Rewards: MetaMesh will establish a Community Contribution Rewards Fund to reward community members for active participation, content creation and contributions on social media, forums and other channels.

Output mechanism of MMT tokens

MMT tokens are native to the MetaMesh network, and their output mechanism is designed to encourage various positive behaviors in the network to maintain the healthy operation of the whole network.

Scientific Computing Reward: For nodes participating in scientific computing (also known as computing nodes), according to the computing power they provide and the number of tasks they have completed, they will be rewarded with a corresponding number of MMT tokens as a reward. The specific number of rewards will be dynamically adjusted according to the actual network conditions and the complexity of the computing tasks.

Block Verification Reward: In order to ensure the security of the MetaMesh network, nodes (also known as miners or verifying nodes) that successfully create a new block and have it verified by the network are rewarded with MMT tokens as a reward for contributing to the security of the network.

Storage and Transmission Reward: nodes that provide data storage and transmission services (also known as storage nodes) will be rewarded with a corresponding number of MMT tokens as a reward based on the amount of storage space, transmission volume, and quality of service they provide.

Network Governance Reward: In MetaMesh networks, MMT tokens are also used to participate in network governance, including voting on network parameters, upgrading suggestions, etc. MMT holders who actively participate in network governance may also receive certain MMT rewards.

Pulsar Foundation

The Pulsar Foundation is a non-profit organization dedicated to advancing and expanding the impact of the MetaMesh project. The Foundation's work centers on providing support to scientific researchers, advancing the use of blockchain technology, and further developing the field of scientific computing. Below are the main areas of work and responsibilities of the Foundation:

PROJECT PROGRESS AND COORDINATION

The Foundation is committed to ensuring the progress of the MetaMesh project by managing the project's R&D roadmap and coordinating the various participants. This includes, but is not limited to, assessing project needs, monitoring project milestones, and addressing any issues and challenges that may arise.

Community Building and Management

The Foundation plays the role of managing and maintaining the MetaMesh community by organizing a variety of online and offline activities, including workshops, research competitions, and web forums. In addition, the Foundation is committed to improving the transparency of the community by regularly releasing project progress and financial reports to maintain the trust and participation of community members.

Legal and Compliance

The Pulsar Foundation will ensure that the MetaMesh program strictly adheres to the legal and regulatory requirements of each country, including, but not limited to, the areas of intellectual property, data privacy and security. The Foundation has a team of legal advisors to provide consulting services and conduct compliance audits.

Education and training

The Foundation is concerned with the public's understanding and mastery of scientific computing and blockchain technology. To this end, the Pulsar Foundation will invest in a variety of education and training programs, such as public courses, workshops, and online teaching resources.

Funds Management

The Pulsar Foundation is responsible for raising and managing funds for the program, which includes accepting donations, administering the fund, auditing financials, etc.

Partnership building

The Foundation will actively seek out partners and establish good partnerships, including but not limited to research institutions, universities, government departments, corporations and other non-profit organizations.

Pulsar Foundation

The Pulsar Foundation is a non-profit organization dedicated to advancing and expanding the impact of the MetaMesh project. The Foundation's work centers on providing support to scientific researchers, advancing the use of blockchain technology, and further developing the field of scientific computing. Below are the main areas of work and responsibilities of the Foundation:

PROJECT PROGRESS AND COORDINATION

The Foundation is committed to ensuring the progress of the MetaMesh project by managing the project's R&D roadmap and coordinating the various participants. This includes, but is not limited to, assessing project needs, monitoring project milestones, and addressing any issues and challenges that may arise.

Community Building and Management

The Foundation plays the role of managing and maintaining the MetaMesh community by organizing a variety of online and offline activities, including workshops, research competitions, and web forums. In addition, the Foundation is committed to improving the transparency of the community by regularly releasing project progress and financial reports to maintain the trust and participation of community members.

Legal and Compliance

The Pulsar Foundation will ensure that the MetaMesh program strictly adheres to the legal and regulatory requirements of each country, including, but not limited to, the areas of intellectual property, data privacy and security. The Foundation has a team of legal advisors to provide consulting services and conduct compliance audits.

Postscript

We stand at the forefront of science and technology, face the future, and embark on this challenging journey in the name of science and technology with a lot of passion. We are witnessing and participating in the creation of this new era of science and technology, this revolution of science and technology.

The challenge now is to build a distributed computing network that is both open and transparent, secure and efficient, and MetaMesh, whose name is derived from the Hawaiian word for "endless sky," is the sky of infinite possibilities we've been waiting for.

We imagine a future where all researchers have easy access to and utilize the world's computing resources, and where all research results can be fairly assessed and respected. We imagine a future where our technology can be a powerful force for scientific development and social progress.

This is our mission, our vision. We need your talent, your passion, your determination. Let's join together and work together for this goal. This is not just a technical challenge, it is a sign of our endeavor for the fairness of research, for the progress of society, and for the future of mankind.

We believe that through our joint efforts, MetaMesh will be able to open up new possibilities and usher in a new era in research. Together we will create unprecedented value, and together we will achieve a better world.

Join us to build the future, meet new challenges and realize our vision. Wherever you are, whoever you are, as long as you have ideas, passion and talent, MetaMesh welcomes you.

Together, with the spirit of innovation and the power of science and technology, let's create a future that belongs to all of us.

Bibliography

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

2. Buterin, V. et al. (2014). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform.

3. ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2014). SNARKs for C: Verifying Program Executions SucciMMTly and in Zero Knowledge. in Proceedings of the 33rd Annual Cryptology Conference.

4. poon, j., & dryja, t. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.

5. bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptography and Cryptographic Protocols. in Proceedings of the 36th Annual International Cryptology Conference.

6. National Cryptography Development Strategy Outline, China. (2016).

7.Gao, S., Ma, Q., Zhang, W., & Liu, L. (2018). Performance Analysis of SM2 Digital Signature Algorithm.

8.Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin.

9.Lipmaa, H. (2012). Progression-Free Sets and Sublinear Pairing-Based Non-Interactive Zero-Knowledge Arguments.

10. "IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End -Use Applications and Loads," in IEEE Std 2030-2011, pp. 1-126, Sept. 2011, doi: 10.1109/IEEESTD.2011.6015835.

11.S. King and S. Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper.pdf

12. chaum, David. "Blind signatures for untraceable payments." advances in cryptology.

13.Chiesa, A., Tromer, E., & Virza, M. (2015). Cluster computing in zero knowledge. in Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques .

14.Akavia, A., Ben-Sasson, E., & Kopparty, S. (2018). Noninteractive Proofs of Proximity. in Proceedings of the 59th Annual IEEE Symposium on Foundations of Computer Science.

15.Arora, S., & Barak, B. (2009). Computational Complexity: a Modern Approach. Cambridge University Press.

16.Karp, R. M. (1972). Reducibility among combinatorial problems. in Complexity of Computer Computations.

17.Vasco, D. A., Oliveira, H. C. B., DeRose, L. F. W., & Navaux, P. O. A. (2002). Performance evaluation of parallel strategies in public key cryptography. in Proceedings of the 16th International Symposium on Parallel and Distributed Processing.

18.Hu, Y., Liu, J., Ma, W., & Zhang, W. (2018). The Research and Application of Boron-Containing Materials in Biomedicine. journal of Inorganic Materials.

19. Liang, J., Zhang, Z., & Chen, N. (2016). Recent Progress in Engineering Materials for Sodium Ion Batteries. materials.

20. Emsley, J. (2001). Nature's Building Blocks: An A-Z Guide to the Elements. Oxford University Press.

21.Shen, B., Chen, M., Yao, Y., & Li, M. (2017). Boron-Based Hydrogen Storage Materials: research and application. journal of Materials Science & Technology.

22.Zheng, J. Q., Wang, P., Li, H., & Du, M. H. (2015). Boron-Based Anode Materials for Lithium Ion Batteries: the State of the Art and Perspectives. advanced energy materials.