Blockchain medical systems

Contents

01 Abstract

BMS is a **Blockchain medical systems** based on blockchain technology. It is comprised of three modules: Olife builds a self-perfecting profile of individual's health data, Olivia acts as an artificial intelligent general doctor, and Oleaf creates a comprehensive healthcare service system. In BMS, users have complete control over their own health data, which can be analyzed by the AI doctor to create personalized, full-process healthcare management. Meanwhile, the BMS token economy can also incentivize all participants to contribute to the healthcare ecosystem in their own way, thus truly achieving precise equilibrium of supply and demand of medical resources in a decentralized, immutable, and AI medical ecosystem on the blockchain.

02 Forward-Looking Statements

This white-paper contains certain forward-looking statements. A forward-looking statement is a statement that does not relate to historical facts and events except in using them to predict future behavior and occurrences. The forward-looking statements are based on analyses and forecasts of future results and estimates of amounts not yet concretely determined.

Such forward-looking statements are identified by the use of terms and phrases such as “aim,” “anticipate,” “believe,” “could,” “estimate,” “expect,” “intend,” “plan ,” “ predict,” “project,” “will,” and similar terms, including references and assumptions.

Forward-looking statements are based on current estimates and assumptions that the developer makes to the best of their current knowledge. Such forward-looking statements are predictions, and thus subject to circumstances, uncertainties and other factors which could cause actual developments to differ materially from projections described in these forward-looking statements. In summation, future events described in this white paper are educated estimations only, and thus may not occur.

03 Terms

- BMS

BMS is the primary token within BMS. It is used for on-chain asset transfer, issuing digital asset, facilitating data storage, and executing transaction. It can also be traded f or fiat currency and other cryptocurrencies.

Derivative Token

Derivative Token is the digital asset designed and issued by the DAPPs in BMS. It can be traded for goods and services in the DAPP. Users obtain derivative tokens by trading with BMS, or by contributing to BMS and its DAPP's to earn rewards.

DAPP

Decentralized applications within BMS, which will cover all aspects of healthcare services, including but not limited to chronic disease management, medical technology, medical services, drug traceability, insurance processing, payment and settlement, and medical financial services. They will leverage BMS's blockchain network to create high-quality comprehensive healthcare experience.

Olife

Olife is the decentralized, self-perfecting, and comprehensive profile of individual's health data in BMS. Users' health data in each DAPP will be linked to the profile, which updates with each use. Through such integration of data in a decentralized and encrypted fashion, BMS breaks the data silos while maintaining health data privacy and control, effectively transforming the evidence- based and centralized healthcare system into a personalized, precise, and omnipresent lifestyle. In addition, the data upload process is completely private, decentralized, and encrypted. No one will be able to access or make profits without data owner's consent.

Olivia

Olivia is a super AI doctor of over 3 years' R&D. The AI medical inquiry system is made possible by formulating a medical knowledge map with machine learning algorithms through the combination of digital technology and medical databanks. Olivia produces more than simplified and standardized reports, but will be able to provide personalized healthcare plans by analyzing user health profile and leveraging the vast data resources on BMS.

Oleaf

Oleaf is a turn-key solution for DAPPs to connect onto BMS. It helps BMS to integrate full- process healthcare services and complete a closed loop of healthy

lifestyle that covers general health management, doctor's appointment, prescription filling, insurance processing, etc.

PoS

Proof of Stake (PoS) is a mechanism designed for public chain consensus where the producer of the next block is selected based one's ownership stake of the network as a method of interest alignment.

PoA

Proof of Authority is a mechanism for consensus first introduced by the Ethereum community which usesblockvalidator's authoritywithinthenetworkas astake. It hasimprovedonscalabilitybutisstill susceptible to a potential threat of supernode collusion.

VBFT

VBFT is a consensus algorithm that combines PoS, VRF (Verifiable Random Function), and BFT. Based on key factors of a network, VBFT can support scalability of consensus groups, guarantee the randomness and fairness of the consensus population generation through VRF, and ensure that state finality can be reached quickly.

PoNA

BMS balanced blockchain issues of common concern and adopted PoNA consensus mechanism to improve processing power, fault tolerance, flexibility, and network security.

04 Background

Healthcare data has been widely collected by individuals and institutions in various formats, but its practical applications have been limited due to stagnant data flow and lack of data right enforcement. As blockchain and AI

technologies gradually become available, a great opportunity to extract health data value presented itself.

Healthcare is a promising market worldwide. The percentage of medical expenditure over GDP has been increasing, reaching approximately 16% in 2014 (USD 12 trillion).

Data Source: World Health Organizatio, Global Health Expenditure Database

Of the 12 trillion dollars, health management has made up an important part. For instance, China now has approximately 200 million chronic disease patients and 500 million potential ones, growing 9% annually. The Internet-based healthcare market is about CNY 15 billion, and the general healthcare market is estimate to be CNY 9.65 trillion. As people grow more aware of comprehensive health, they become more willing to invest in healthy lifestyle and routine health management. It is expected that the Internet-based healthcare market will reach CNY 33 billion by 2020, and the general health management market will be CNY 13 trillion.

Data Sources: Frost Sullivan Report, Ping An Good Doctor Prospectus

Meanwhile, health data has been digitized rapidly along with the widespread of electronic devices. In developed countries, the number of consumers with electronic medical record (EMR) has nearly tripled in the past decade, reaching 16%; while in China, as a developing country, only 0.6% of hospitals has reached level 5 or higher in terms of medical data digitization - developing countries still has a long way to go.

Level	DESCRIPTION	2011 (N=178)	2012 (N=905)	2013 (N=2414)	2014 (N=2622)
7	Complete EMR system with regional info sharing capability	0%	0%	0.04% (1)	0.038% (1)
6	Closed-loop and full-process medical data management to support high-level medical decision making	0.56%	0.11%	0.16%	0.19% (5)
5	Unified data management and system data integration of all departments	0.56%	0.66%	0.21%	0.38% (10)
4	Information sharing within entire hospital and support for mid-level medical decision making	6.74%	2.65%	3.89%	5.61% (147)
3	Data exchange between departments and support for elementary-level medical decision making	43.82%	22.21%	13.05%	15.25% (400)
2	Data exchange within department	24.16%	31.16%	22.33%	21.78% (571)
1	Preliminarydatacollection withindepartment	9.55%	11.93%	11.1%	10.41% (273)
0	Absence of EMR	14.61%	31.27%	49.21%	46.38% (1216)

Data Source: Statistical Report of CHINC

However, the cost for comprehensive health data digitization is almost too high. Take China for an example, the average cost for establishing a level-5 EMR system is CNY 10million;bringingallcity-levelhospitalstolevel5 wouldcost CNY 20 billion;bringing 70% of all hospitals to level 5 would cost CNY 200 billion. Counting in 900,000+ community medical institutions would drive the cost to over CNY 500 billion.

In all age groups, the number of consumers with electronic health record in America has been doubled in the past 5 years, raising from 8% to 16%.

Data Resource: Analysis Report on China's Medical Information Industry Market Prospects and Investment Strategic Planning from 2018 to 2023

Due to the complicated nature of the healthcare industry, only building a unified data system seems a logical answer. However, the industry faces the following challenges:

- Health data ownership is difficult authenticate and enforce, causing data silos.

While they should, most individuals have little control over their own health data since it is stored in medical institutions such as hospitals, far beyond their reach. Such centralized storage cannot provide enough data security and privacy for data right enforcement.

Insufficiently clarified data ownership, compiled with the competing nature among medical institutions, seriously impedes inter-agency data flow, retarding the development of many life-saving research projects that require massive data input, such as genetic disease prevention and management.

On the other hand, health data vary in type and format, further increasing the difficulty ofdata standardization. Even in developedcountries, the actual application of medical data protocol such as FHIR is far insufficient for comprehensive health status evaluation to a practical degree.

- Medical resources mismatch the demand.

High concentration of quality medical resources has made major healthcare institutions overcrowded and smaller ones empty. Furthermore, the lack of reliable and convenient initial diagnosis creates a bottleneck where the majority of patients will have to go to a general physician or a major hospital for a trusted opinion before continuing on. Under such circumstances, hospitals are burdened with treatment and forced to overlook quality services.

Meanwhile, as the standard of living improves, healthcare demand has expanded from mere treatment of illness to comprehensive health management, which has become a clear direction in which the healthcare industry has to evolve.

- Fragmented medical services create poor user experience.

Medical services in various fields have continued to improve, but the lack of inter- agency linkage causes great waste of data. Inconvenient non-medical services (lengthy insurance processing, untraceable counterfeit drugs, etc.) also adversely affect user experience. The call for a one-stop solution becomes louder by the day.

05 BMS

BMS is an AI medical ecosystem based on blockchain technology, aimed at creating a decentralized platform for comprehensive and personalized healthcare.

BMS Modules

Data Right + Data Flow

- The current evidence-based healthcare relies on empirical clinical data for the universality of treatment processes. However, the movement to precision healthcare, represented by genetics and 4P medicine (Predictive, Preventative, Personalized, and Participatory), focuses on the individuality of each person’s healthcare strategy, which require massive amount of medical data. BMS powers such transition by creating

a data platform that offers data encryption and data right enforcement in a distribution system, with the assistance from a closed-loop token system and smart contracts.

- Resource Allocation + Artificial Intelligence

In BMS, users can find doctors that best fit their condition with the help of their digitized medical profile, without going to the hospital every time they need one. In particular, BMS can help patients with rare diseases to connect directly with medical resourcesaroundtheglobe. Inaddition, the AIdoctor Oliviacanofferinitialdiagnosis based on user health profile (passive) and direct communication (active), breaking the bottleneck effect.

- Full Range + Full Process

BMS completes a closed loop of healthy lifestyle by integrating full-process healthcare services through modular interfaces, covering general health management, doctor's appointment, prescription filling, insurance processing, etc.

Personalized and self-perfecting health profile

BMS creates an on-chain identification profile Olife for each user, which gathers data from all DAPPs in BMS and continues to self-perfect.

Olife allows transactions in different DAPPs within one token system and facilitates data integration. The value created by user contribution in one DAPP can be transferred to another within BMS.

User has complete control over when and how Olife is used within BMS and achieve any healthcare goal without compromising data security and privacy.

- Health Data On-Chain Storage

  Each Olife is asymmetrically encrypted and stored in BMS nodes through IPFS protocol to ensure information security and data privacy. Only authenticated user consent through smart contract grants controlled data access.

- Data Capitalization

  BMS enforces personal health data rights through its distributed network and takes back data control from centralized organizations. Users can also contribute to BMS by granting data access to medical researchers in exchange for BMS.

- Olife Nexus

  Standardized smart contracts enable health data exchange in BMS by managing access to Olife. Users define Olife access permission protocol through Nexus, and research institutions obtain appropriate health data by providing certain reward through Nexus, thus ensuring data flow, value flow, and privacy protection.

AI health manager

Olivia is a super AI doctor of over 3 years' R&D. This AI medical inquiry system is made possible by formulating a medical knowledge map with machine learning algorithms through the combination of digital technology and medical databanks. Olivia produces more than simplified and standardized reports, but will also be able to provide personalized healthcare plans by analyzing user health profile and leveraging the vast resources on BMS.

- Healthcare at Home

Users can access professional healthcare advice through Olivia without going to a hospital by connecting wearable devices and other health data sources to Olivia, thus greatly reducing hospital burdens and improving user experience for all.

Personalized Healthcare

Olivia monitors user Olife for daily health data fluctuation, and provides alert, advice, as well as healthcare strategies accordingly.

Technical Framework

Olivia is a self-perfecting AI algorithm model. The underlying database is a medical knowledge map that searches, reasons, extracts feature vectors to learn massive volumes of medical cases through deep learning technique with NLP, thus effectively combining medical literature with actual cases to improve its clinical decision-making ability.

Closed Loop of Healthy Lifestyle

BMS builds a foundation platform for healthcare DAPPs through modularized basic services. Oleaf is the modular API interface with SDKs, compatible with smart contracts with plug-and-play expansion capacity.

API and Service Expansion

BMS provides decentralized on-chain hosting services for DAPPs with computing resources, bandwidth, decentralized file storage, big data analysis, and artificial intelligence technology, building a sustainable and resilient network.

Closed Loop for Comprehensive Health

Through Oleaf, BMS integrates healthcare service providers, medical service providers, wearable devices, medical R&D institutions, medical financial services, as well as support groups to create comprehensive, seamless user experience for all healthcare needs.

BMS enables all DAPPs to establish their own token systems through blockchain technology, allowing smart contract collaboration through BMS across the whole network, uniting traditionally fragmented services by simplifying the value flow for the entire ecosystem.

06 Technology

Positioning

CAP Theorem

Blockchain technology's practical application has been one of the core pursuits of many entrepreneurs and developers. The past decade has seen a few mainstream types of consensus mechanism, each trying to balance among the degree of distribution, transaction verification speed, and fork prevention.

Eric Brewer proposed a hypothesis at the Symposium on Principles of Distributed Computing in 2000, and it was later proved to be the CAP Theorem by Seth Gilbert and Nancy Lynch from MIT. It points out that it is impossible for any distributed data store to simultaneously guarantee consistency, availability, and partition tolerance. In terms of blockchain application, the three qualities correspond to security, scalability, and decentralization, among which tradeoffs have to be made.

Healthcare Blockchain Requirements

Data Credibility

Inthe traditional medical system, each institution builds its own independent database with no inter-agency data flow channels, partially due to the sensible nature of medical data. A decentralized clearing system is in need to validate data flow and transactions.

Reasonable Cost

It costs almost 2 dollars per transaction record on mainstream public chains, and Bitcoin transaction costs almost ten times as much. Such high operating cost is unreasonable for any global application, for users as well as service providers. A cost-effective mechanism for

transaction processing is in need to support the large quantity of transactions in a comprehensive healthcare ecosystem.

Upgrading and Debugging

Medical technology never stops evolving, so should the underlying blockchain network to support smart contract updates and DAPPs. In addition, debugging mechanism is also necessary for when bugs occur.

❶ Seth Gilbert Nancy Lynch, Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web ervices, 2002

Low Latency

Prompt feedback is the basis for excellent user experience. Transactions that take more than a few seconds seriously undermine the competitiveness of an application. To meet the commercial use standards, the transaction confirmation time should be under 3 seconds.

Concurrent Computing

Blockchain consensus comes from deterministic (reproducible) behaviors. It means that all concurrent executions have to work normally without using mutex or other locking primitives. Healthcare applications often need to handle a large number of concurrent operation requests, some of which must be sequential, therefore powerful concurrent computing capacity is a must.

Storage

Normal nodes are becoming overburdened by mainstream blockchains such as Bitcoin and Ethereum as their data accumulate over time. The expected amount of healthcare transaction data is far beyond current scale, which requires much more storage space from its nodes.

Privacy

Medical data is private information with great value, which requires strict encryption and desensitization. However, the user name system (hash address) of mainstream public blockchains is cumbersome and inconvenient for commercial use, which calls for a secure yet user-friendly identity verification system.

BMS Solution

BMS is building a global blockchain network for the healthcare industry, which offersanopportunitytotransitionpainlesslyfromtraditional Internet-basedcentralized model to blockchain-based AI medical ecosystem through the loose- coupling multi-level structure of modular design. Individuals and institutions can store and share medical data in BMS, and can create data flow through BMS. In addition to data integration, a healthcare ecosystem also ensures the credibility of medical service providers, maintains lightweight end user nodes, supports massive concurrent transactions, and prevents forks before scaling up. Therefore, for the initial phase, BMS utilizes a decentralized system as an stepping stone from the existing centralized system to the future of completely distributedsystem.

Data Credibility Maintenance

Public blockchains allows anyone to participate, which cannot prevent anonymous users from uploading malicious or forged data. Therefore, BMS only admits healthcare institutions of certain qualification to join and maintain the network. Only strict admission rules can ensure that all parties involved in the blockchain consensus are responsible and accountable, thus ensuring the credibility of data before uploading onto the blockchain.

Zero Transaction Cost to End User

BMS by design does not reward block validators in the traditional sense since the gas fee is zero. Therefore, users can enjoy quality services without excessive cost. The zero fee model is expected to attract more users, and DAPPs can employ profit models upon critical user mass.

Plug-and-Play Modules for Upgrades and Debugging

BMS blockchain contains plug-and-play module design, which allows quick and easy upgrade of the underlying smart contract design as well as the DAPPs.

Admission Control to Guarantees Low Latency

BMS Branch Nodes need to be tested off-chain for its computing capacity before being issued the certificate, thus ensuring the processing capacity of the whole network.

Powerful Concurrent Computing Capacity

BMS can expand its processing capacity infinitely based on the task scheduling pattern. Large-scale computing workload can be divided across multiple independent

computers, balance workloads of multiple CPUs, memories, or disks. It supports million-level concurrent computing and can fully support 100-million-level active users.

Expansion Capacity

BMS nodes confirm transaction data among each other on-chain and broadcasting to the blockchain only when clearing processes or conflict resolution occur, thus obtaining theoretically infinite expansion capacity for commercial application in the healthcare industry.

Privacy and Private Key Retrieval

BMS adopts multi-signature and role-based multi-level access management system to assign different identities and permissions to individual and institutional users. In addition, the multi-signature system provides an opportunity for asset recovery, allowing users to cure the loss caused by misplaced of private keys, making the blockchain truly viable for commercial use.

Quantum Resistance

Considering quantum computing technology that may appear in the future, BMS adopts a signature abstraction method to ensure future scalability and quantum resistance. DAPPs will also arm against collision attack.

Consensus Mechanism

- Consensus Foundation

Proof of Stake

Proof of Stake (PoS) is a consensus algorithm for public blockchain networks. The probability to produce a block is related to one's collateralized asset. PoS assumes that a series of peer nodes in the system are static and stable over a long period of time. However, it is unrealistic in a global blockchain environment.

PoS does have many advantages over traditional PoW consensus algorithms. PoS voting weights are calculated by collateralized equity rather than computing power, which does not require excessive electric power to prove the work. If one wants to attack the PoS network, it needs to own most of the equity tokens in the network, which is a very high cost.

In a PoS network without penalty measures, validators can effectively compromise the network by voting for multiple conflicting blocks at a given height without incurring any cost. Since oligopoly is the norm in many real markets - coordination among a few relatively wealthy validators is much easier than that among most relatively poor verifiers. Under PoS consensus, a cartel with enough interests may control the system, making the rich richer and the poor poorer.

Proof of Authority[2]

Compared to PoW and PoS, PoA consensus algorithm has made improvements in terms of performance and scalability. PoA is similar to PoS, but POS is based on equity ownership, which could lead to oligopoly collusion. In PoA, validators do not need to hold shares in the network, but must have some sort of credibility within the network, which grows or collapses based on their behavior. The higher the credibility, the greater the voting weight, which motivates the validators to act in the best interest of the whole network.

However, all validating nodes of PoA need identity authentication, trading the degree of node distribution for the security and scalability of the entire network. On the other hand, most PoA networks measure the authority of validator nodes through an in- network rating system, of which the algorithm design is difficult to maintain fairness. In addition, new node's reputation rating usually starts low, making the network hard to evolve.

VBFT

VBFT is a consensus algorithm that combines PoS, VRF (Verifiable Random Function), and BFT. The key difference between VBFT and other algorithms is that it is closed based on the network governance model of BMS. VBFT can support scalability of consensus groups, guarantee the randomness and

fairness of the consensus population generation through VRF, and ensure that state finality can be reached quickly.

Nodes apply to participate in the consensus with collateralized shares of the network, and are selected through VRF into groups, in charge of proposing, verifying, and confirming new blocks. VBFT combines the randomness of node selection in VRF, the ~~attack tolerance in PoS, and~~ speed to state finality of BFT, offering scalability for the BMS blockchain.

❷ PoA 权职证明最早由以太坊提出，旨在以权威积分的方式让区块链网络更加安全节能。

Considering the unique nature of healthcare data, BMS adopts a public blockchain model based on VBFT and other auxiliary methods to maintain fairness at the beginning stage of the project, and introduces PoNA (Proof of Network Alliance) consensus mechanism for the credibility of healthcare services as well as the processing capacity of the network.

PoNA

Bridging the current healthcare industry and blockchain, BMS offers a complete set of solutions. Learning from PoS and PoA algorithms as well as VBFT from Ontology, BMS introduces Proof of Network Alliance (PoNA) consensus mechanism. PoNA meets the security and privacy requirements of the healthcare industry through qualification review, authority certification, proof of stake, VRF, and BFT, while staying decentralized.

Qualification Review

Taking into account the healthcare industry's need for risk control, BMS has designed a complete identity verification mechanism and qualification review system for any candidate for Root Node with block-

producing function. Every Root Node candidate is reviewed off-chain to determine their capacity for attack resistance and data credibility.

Proof of Authority and Stake

BMS nodes with different functions need to prove different levels of authority and stake to increase the cost malicious behavior. On one hand, organizations and their administrators of a Root Node need to pass off-chain ID verification. On the other hand, the authority score will decrease significantly after any dishonesty of a Root Node, preventing it from participating in the proposal, verification, and confirmation of new blocks.

Votes

Each BMS block is produced through VBFT voting by Root Nodes. Nodes are selected through VRF to propose, verify, and confirm new blocks. Due to the randomness of the selection process, the consensus algorithm gains additional fault tolerance, and effectively avoid malicious forks.

PoNA Nodes

PoNA consensus mechanism consists of Root Nodes and Branch Nodes.

Root Node

Root Nodes are responsible for producing new blocks and broadcasting them to the rest of the network.

Branch Node

Branch Nodes are also the maintainers of BMS. They synchronize with Root Nodes, store full blockchain data, and assist in network monitoring. Qualified Branch Nodes can also upgrade to Root Nodes.

BMS Blockchain Network Structure

From the very beginning, BMS blockchain is designed as a commercially applicable blockchain ecosystem for the healthcare industry.

- Application Layer

It contains DAPPs to which end users directly access, including wallets, blockchain browsers, mobile applications, websites, etc.

- API and Service Extension Layer

It contains a variety of APIs for accessing the network. BMS will also provide extension SDKs for running logic code on nodes, including identity authorization, smart contracts, and concurrent blockchain services.

- Blockchain Network Layer

It includes DAPP servers, Root Node network, and Branch Node network, responsible for smart contract execution, ledger data storage, etc. Root Node network verifies and confirms transactions, and Branch Node network monitors the BMS blockchain consensus.

- Data and Ledger Layer

It stores the core data of the ledger, including block data, status data, and historical data. This layer provides a world state server with query services in the form of a rich text database. Blocks record transactions and health data for all BMS participants.

- Block Structure

Block Head

Block height, timestamp, transaction hash, etc.

Block Data

Information related to healthcare data and transaction:

- **Transaction Proposal**

  Smart contract ID and version, transaction timestamp, smart contract trigger, timeout, signature of the transaction originator, etc;

- **Transaction Endorsement**

  Signatures of endorsement for the transaction from other nodes;

- **Transaction Feedback**

  proposal hash, smart contract trigger event, status, healthcare data status change, world state change, etc;

Block Metadata

Root Node signature, Branch Node signature, transaction originator signature, etc.

On-Chain HealthData

Identity Trust

Olife ID is a decentralized identity protocol within Olife and is linked to a description subject. It records property data of the Olife subject, including the public key. Identity trust is maintained through mutual verification between Olife subjects. In BMS, users can extend trust relationships through trust anchors, and can also establish such relationships through mutual authentication. Only when the trust score remains above a certain level can the subject's Olife be uploaded to the blockchain and traded freely.

Health Data

Health data includes but is not limited to:

Data Category	Data Description	Note
Medical Examination Data	Medical Examination Report Medical Imaging	Unstructured Data (Text Data) Unstructured Data (Image Data)
Lifestyle Behavior Data	Daily Effective Exercise Time Dietary Status Timely Medication Record Sensor Monitoring Data	Structural Data Unstructured Data (Text and Image Data) Unstructured Data (Text Data) Unstructured Data (Text Data)
Electronic-Prescription		Unstructured Data (Text Data)

Health data is mostly unstructured and large in volume, and yet on-chain data definition is limited by typology and storage. BMS employs 'on-chain-off-chain fusion' structure to store and manage health data. The on-chain data includes a hash index of the user health data, and the complete set of health data is stored in the distributed storage network off-chain. A DHT records the mapping relations between on-chain and off-chain data to assist data retrieval.

Data Tampering Prevention

Each block contains the hash of the previous block, and any change of information at any point will collapse the entire blockchain. However, the data structure alone cannot prevent data tampering. Another key factor is the consensus mechanism.

PoNA uses an endorsement mechanism to force both parties to abide by the contract. In PoNA, an organization first initiates a smart contract that requires a few nodes to participate. Each node validates the contract locally and signs the feedback. Root Nodes, selected through VRF, then independently verify the results and send them to other Root Nodes for final confirmation before broadcasting to the rest of the network.

Due to the mutual independence of each node, no party can control all the Root Nodes to tamper with the transaction process. After the transaction results are confirmed by multiple parties, no one has the opportunity to alter the transaction results, thus preventing data tampering.

Smart contract

Smart contracts are triggered by transactions to read, write, and compute relevant data to support various commercial applications.

Smart ContractDesign

BMS provides general and custom smart contract modules. The general module, which is written natively on the blockchain to reduce block load, includes basic functions such as identity authentication and peer-to-peer transactions. Customized smart contract functions are open for edits. Separate smart contract function modules can be written to handle unique functionalities.

General Module

A number of general modules for core ledger, standardization of medical data, and healthcareapplicationsaredesignednativetotheblockchainforthemostconvenient use and minimal resource consumption. DAPPs on BMS can quickly implement commercial applications with the general module, for the purposes of low system cost, data standardization, and wide compatibility of data connection. Design principles include compatibility with current data standards and provision of application framework standards.

Customized Module

BMS allows DAPPs to customize the design of smart contracts. It can be quickly customized for the specific needs of different commercial scenarios, and can provide flexible support for different services. BMS's underlying protocol is highly flexible, highly adaptive, and highly expandable, meeting almost all healthcare service needs.

Multi-Language Developing

BMS smart contract is a multi-functional, lightweight, concurrent, multi-language, and Turing-complete system. Developers do not need to learn new languages to develop smart contracts in BMS. At the beginning stage, BMS supports Go and Python, and will support other languages such as Java, C++, Rust, JavaScript.

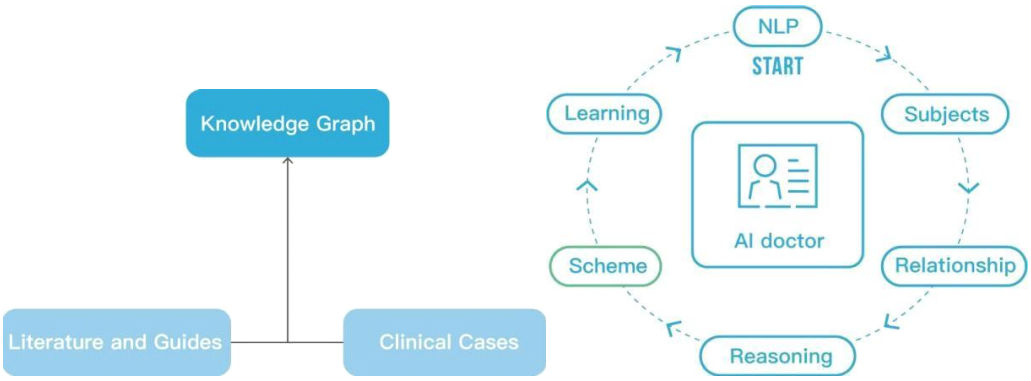
Future development

In the future, BMS will integrate third-party identification system, such as SIM, to further enhance user ID experience. As the ecosystem grows

with larger number of participating nodes and better structure of distributed system, when the storage and computing capabilities of mobile terminals are greatly augmented, BMS intends to upgrade all nodes in the ecosystem to Root Nodes, and develop a new consensus mechanism based on the Algorand algorithm to achieve complete community autonomy, fully evolving from a decentralized system into a distributed blockchain network.

AI Diagnostic Technology

Olivia is a major-hospital-qualified AI doctor, made possible by formulating a medical knowledge map with machine learning algorithms through the combination of digital technology and medical databanks.



Knowledge Map of Unprecedented Volume

Olivia's knowledge map is constructed and trained through RPM model with medical semantic databanks. It consists of millions of category/relation triads and tens of millions of indirect triads. Combined with logic algorithms and search engines, Olivia is able to provide optimal solutions and corresponding evidence in diagnostic scenarios.

Medical NLPAlgorithm

Olivia's natural language processing (NLP) technology for the medical field includes lexical analysis, syntactic analysis and semantic analysis. Semantic analysis is carried out for sentences in each iteration of the algorithm by adopting EM algorithm and using entity/relation names in the knowledge base, and the sentences with high confidence are selected with their semantic analysis results to find specific sets of objects and relations, so as to automatically extract medical entity relations.

Neural Net Deep Learning

Olivia uses the medical semantic network of its knowledge map to search, reason, extract feature vectors, and learn massive volumes of medical cases through deep learning technique, thus effectively combining medical literature with actual cases to improve its clinical decision-making ability.

A neural net is a set of algorithms designed to mimic the structure of the human brain to recognize patterns. The neural net interprets data through a machine sensor system to mark or cluster the original inputs. The patterns that a neural net can recognize are numerical forms contained in vectors, so all real-world data, such as images, sounds, texts, time series, etc., must be converted to numeric values.

Neural net is capable of clustering and classification. It can be understood as clustering and classification on top of stored and managed data. Neural net can group the untagged data according to the similarities of the input samples; if trained with the tagged data set, the neural net can systematically categorize the data.

Each tier of deep learning system consists of nodes. The operation is performed in a node whose mode of operation is roughly similar to that of a human neuron, and activates and releases a signal when there is sufficient stimulus information. The node combines input data with a set of coefficients (or weights) and specifies its importance in the algorithm learning task by amplifying or suppressing the input. The sum of the product of the input data and the weight shall enter the activation function of the node, determine whether the signal continues to be transmitted in the network, and the distance passed, thereby determine how the signal affects the end result of the network, such as the classification action.

……

.....

The node tier is a row of neuron-like switches that turn on or off as input data passes through the network. Starting with the first input layer that originally receives data, the output of each layer is also the input to the next layer.

Matching the input features to the adjustable weights specifies the importance of these features, as in how much they affect the input classification and clustering of the network.

07 Application Scenarios

Everyone's daily health data are of great value. BMS, through the combination of blockchain technology and AI technology, allows health data analysis through AI for comprehensive healthcare without compromising data privacy. In addition, health data is of high research value and can greatly help the development of medical technology. Users can tag part or all of their health data as 'available for anonymous sale' on BMS blockchain. BMS will provide such data to research institutions after desensitization. The process is powered by smart contracts, and the resulting revenue shall be transferred to the customer's wallet in the form of BMS. Through BMS, users can enjoy comprehensive healthcare services while contributing to the development of medical technology.

Healthcare Service

Health Monitoring

Bob's wearable devices constantly collect his physical data into Bob's Olife. Olivia analyzes and compares the data with medical literature records, found that Bob's health was deteriorating, which was manifested by weight gain, poor sleep quality, and high blood glucose. Olivia believes that if things continue this way, Bob would gradually develop chronic diseases such as diabetes. Olivia reports the possibility to Bob. Bob began to actively adjust his lifestyle to address.

Diet and Exercise Guidance

Jenny hopes to improve her health with diet and exercise, but a nutritionist and a fitness instructor would cost a lot of money. So Jenny uploaded her physical data and diet habits to BMS. After Jenny's consent, Olivia also read other data of Jenny on BMS, such as genetic data, sleep data, etc., and then offers a detailed meal plan and exercise program for Jenny. Olivia dynamically adjusts the recipe and fitness program as Jenny goes, and urges Jenny to complete daily tasks for the best results.

Customized Service for Chronic Disease Management

CBMSin is currently troubled by chronic hypertension caused by obesity. CBMSin has tried different antihypertensive drugs and various weight loss methods. Unscientific methods not only failed to control his weight, but also raised other health concerns. By analyzing CBMSin's physical condition, Olivia customized a set of high-BMI blood pressure management programs for CBMSin, including medication supervision, diet, exercise, and work schedule adjustment. As CBMSin make progress, Olivia continues to adjust the program as long-term health management.

Medical Service

Intelligent Diagnosis andReferral

William has been feeling under the weather, but there were no obvious symptoms, so William consulted Olivia. Olivia analyzed William's Olife and found that William's physical condition was sound. After in-depth dialogs with William, Olivia found that William may be suffering from depression, so William was referred to a licensed psychiatrist for more detailed diagnosis. After consulting the psychiatrist, William confirmed the mild depression. His condition was quickly relieved with medication.

Global Medical Referral

David had a rare blood disease, and few doctors in his country have treatment experience in the matter. Through BMS database, Olivia helps David find three cases of the same condition cured in a private hospital in the United States. David reached out to the doctors through BMS and consulted treatment details. In the end, David decided to go overseas for treatment, and paid his medical bill through BMS.

Course Tracking and Postoperative Rehab

Javier is a cancer survivor and he is completing his postoperative chemotherapy, physiotherapy, and nutritional supplements at home. Javier's family is more involved in his recovery process. Through Olivia, they get to understand everything that is happening to Javier. When he has any questions regarding the exclusive care process, Javier asks Olivia for prompt and professional response.

Clinical Trial

John was just diagnosed with a rare cancer. Olivia informs him about an ongoing clinical trial for his cancer. After consideration, John decided to participate in the trial. In the course of the trial, Olivia helped John to customize and manage life routines according to the test requirements uploaded by the testing institution. Olivia tracks John's data to provide better support for the clinical trial. While gaining a fighting chance for his illness, John is also able to receive a certain amount rewards through BMS.

Gene Sequencing and Interpretation

After her mother was diagnosed with breast cancer, Mary worries about her own health. Because Mary is busy with work, she had little time for a genetic test at the hospital. She told Olivia about this concern, and Olivia orders a saliva sampler for gene sequencing. After sampling according to the instructions, she sent the sample back to the testing center. Mary then receives her own genetic test report, which shows that she carried the same breast cancer gene as her mother. During every annual physical, Olivia will remind Mary to focus on breast health, such as mammography and ultrasound, to monitor and record changes in Mary's mammary gland conditions. If any possible anomalies are found during the process, Olivia will remind Mary to conduct further exams.

Drug R&D and Traceability

Pharmacy and R&D

MediResearch is an alliance of pharmaceutical companies, data analytics companies, and genetic engineering non-profit organizations that focuses developing new drugs based on a large number of patient biomarkers and genetic data. Through Olife Nexus, MediResearch can obtain a large

amount of desensitization information in a legalandcost-effectivefashion. Thisinformationcaneffectivelypromotetheresearch progress. MediResearch has already gained preliminary research success on developing gene-target drugs for specific groups of patients.

Drug Traceability - Supply Chain

Carol is running a fever of 104 Fahrenheit, and is suffering from headaches and muscle soreness. After checking Carol's Olife, Olivia orders prescription drugs for Carol. Uponarrival, thedrugs' authenticity isverifiedbytraceablesupplychaindata on theblockchain.

Medical Insurance and Insurance Circle

Medical Insurance

Alice wants to buy a medical insurance policy for herself. She no longer needs to prepare complicated documents. Insurance company can check her Olife with her consent for qualification review and determination of insurance terms. Payments and pricing are made in the form of derivative tokens. The process of insurance reimbursement will also be simplified. When a medical expenditure meeting the insurance clause occurs, the default smart contract will be triggered automatically, and the amount covered by insurance compensation will be automatically transferred to Alice's BMS wallet.

Insurance Circle

Tony is a gout patient who started a gout insurance circle program in the Gout Patient Support Group in BMS. Other users can put tokens in an

escrow smart contract for anyone qualified in the circle. All users who purchase insurance can check the amount of this mutual insurance at any time. The entire process is transparent, open, and automated.

08 BMS Tokens

Two-tier Token System

BMS has introduced a two-tier token system to facilitate normal operation and interaction of various roles in BMS. BMS is the primary token of the BMS, the vessel of the internal rights of BMS, and the means of value circulation between the BMS network and other cryptocurrencies as well as fiat currencies. The derivative token is the pricing measurement of each DAPP. DAPPs can issue the derivative tokens through the BMS.

Primary Token

- A
  M
  B

  N

The primary token BMS is the decentralized crypto token of the BMS, the minimum unit of which is 0.00000001 (decimals: 8). BMS will be first issued as ONT based tokens on Ontology, mapped at a 1:1 ratio upon mainnet launch.

- Function

BMS is the value carrier of BMS, whose functions include but not limited to on- chain asset transfer, data storage and computing, transaction

execution, etc.. Developers can also deposit BMS and deploy smart contracts to issue DAPP-level derivative tokens. Research institutions can obtain desensitized data buy paying BMS. BMS is also the value conversion carrier among DAPPs on the BMS blockchain.

- Acquisition

Users can obtain BMS in a variety of ways, including but not limited to exchanging with fiat currency as well as other cryptocurrencies, contributing to BMS community and earning BMS rewards, converting from derivative tokens, and P2P on- chain transfers.

- DerivativeToken

Derivative Token

Derivative token is the payment method and value scale in BMS at the application-

level, which is designed by different DAPPs. Developers can use BMS to deploy smart

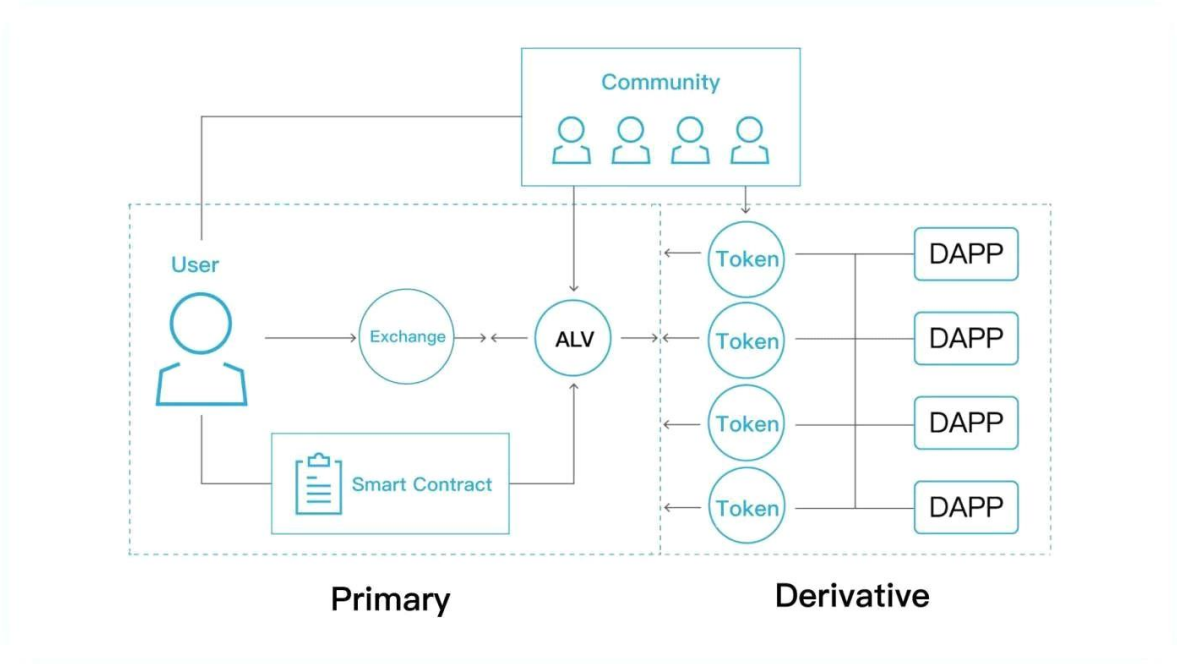
contracts on the BMS blockchain to issue derivative tokens.

- Function

Derivative tokens can be used in the corresponding DAPPs in exchange for goods, services, and/or other privileges.

Acquisition

DAPPs issue their own derivative tokens by deploying smart contracts. Users can use BMS or fiat currency to exchange derivative tokens in the corresponding DAPPs, and canalsoobtaincorrespondingderivativetokenrewardsbycontributingtoeach DAPP’s community. Different derivative tokens cannot exchange among each other without taking BMS as a value medium.



Staking

Under PoNA Consensus mechanism, node institutions have to not only pass qualification review but also lock down certain amount of BMS tokens as proof of stake before executing their duties. DAPPs, upon issuing secondary tokens for their own transaction settlement, also need to lock down BMS tokens depending on amounts of token issuance and fundraising, to ensure healthy circulation of said secondary token. Should node institutions or DAPPs experience failure, active or passive, staked BMS is released as insurance reimbursement.

ALL, IN BMS