Token NET

Version 1.0

NEWElements

white paper

Token NET

Unlocking the Future of
Technological Life Healthcare

CONTENT

01 Project Overview

OVERVIEW

1.1 Project Background

A) Current situation and challenges in the global healthcare industry

Globally, the healthcare industry is facing many serious challenges. With the aging of the population, the increasing prevalence of chronic diseases and the rising demand for health, the burden on the healthcare system continues to increase. According to statistics, global healthcare expenditure as a percentage of GDP has been increasing year by year, however, the quality and efficiency of healthcare services have not improved in tandem.

The rapid growth of healthcare data poses storage and management challenges. Medical institutions generate a large amount of patient data every day, including electronic medical records, medical images, test reports, etc., which are dispersed in different systems and departments, forming numerous "data silos". Difficulty in sharing and interoperability of data between different healthcare organizations has resulted in the need for patients to repeat tests during cross-institutional visits, which not only wastes healthcare resources, but also continues to increase patients' financial burden and time costs.

On the other hand, patient privacy and data security issues are becoming increasingly prominent. Under traditional medical data management, patient data is often centrally stored in medical institutions or third-party data centers, and these centralized storage methods have the risk of a single point of failure, which makes it extremely easy for patient data to be leaked in the event of cyber-attacks or irregular operations by internal personnel.

The growing demand for cross-border healthcare has also brought new challenges to the healthcare industry. Due to the uneven distribution of medical resources in different countries and regions, many patients need to travel to other countries to seek better medical services. However, the process of cross-border healthcare faces many obstacles, such as difficulties in currency exchange, cumbersome payment processes, and inconsistent medical standards, which are continuously limiting the rapid development of the cross-border healthcare market.

1.2 The Potential of Blockchain Technology in the Medical Field

Blockchain technology, as a kind of distributed ledger technology, has unique advantages such as decentralization, non-tampering, traceability, etc., which provides new ideas and methods to solve many problems in the medical industry.

Encrypted sharing of medical data

① Blockchain encryption algorithm protects patient data, accessible only to authorized institutions/personnel, enabling precision medicine.

② Distributed storage eliminates single point of failure and enhances data security and reliability.

Collaboration and Sharing of Medical Resources

① Smart contracts build a resource platform, where patients can book global quality resources and institutions can share equipment/medicine.

② Enhance resource utilization, promote healthcare collaboration, and optimize global resource allocation.

Cross-border healthcare payment upgrade

① Decentralized payment network, cryptocurrency fast, low-cost cross-border settlement, handling fee < 1%.

② Real-time clearing improves capital efficiency and optimizes international patient payment experience.

02 Industry Analysis

ANALYSIS

2.1 Healthcare Data Silos and Lack of Interoperability

A) Performance of data silo phenomenon

In the current healthcare system, medical institutions (e.g., hospitals, clinics, laboratories), insurance companies, etc. each use independent database systems, which are often based on different technical architectures and data standards, resulting in data that cannot be effectively shared and interoperated. For example, one hospital's electronic medical record system may not be compatible with another hospital's system, and data such as patients' examination results and diagnostic records cannot flow smoothly between different organizations. The phenomenon of data silos increases the cost and time for patients to seek medical care, making the integration and optimal allocation of medical resources difficult.

B) Impact on medical efficiency and precision medicine

Data silos seriously hinder the improvement of medical efficiency and the development of precision medicine. Without access to patients' complete medical data, doctors may face the problem of incomplete information during diagnosis and treatment, leading to misdiagnosis or imprecise treatment plans. For example, in cancer treatment, information such as a patient's genomic data, medical history, and test results are crucial to the development of a personalized treatment plan, but data silos make it difficult to integrate this information, affecting the effectiveness of precision medicine.

2.2 Patient Privacy and the Data Sovereignty Crisis

A) Data Misuse Phenomenon

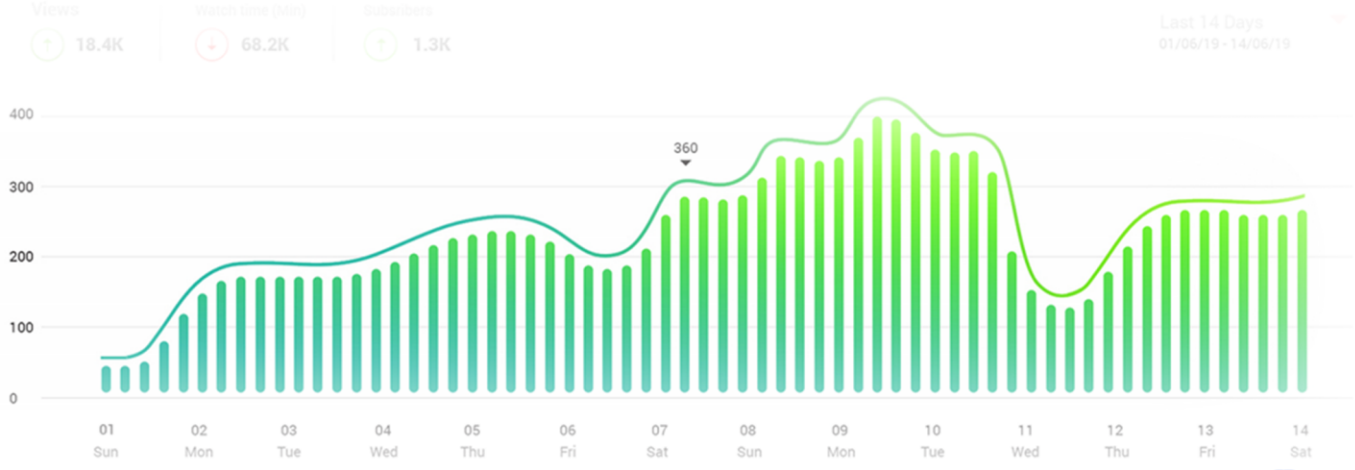
Patient privacy and data sovereignty face a serious crisis in current medical data management. Some medical institutions and third-party data companies collect, use and sell patients' medical data without their consent for commercial interests. For example, in 2022, a genetic testing company sold users' genetic data to a pharmaceutical company for $500 million to be used in the research and development of new drugs without the users' knowledge.

B) Limitations of Traditional Encryption

Traditional encryption has limitations in protecting the privacy of medical data. The encryption technology used by most healthcare organizations relies on third-party trust, such as the encryption standards set forth by HIPAA (Health Insurance Portability and Accountability Act), which have many loopholes in their practical application. For example, insiders can access and leak data with legitimate privileges, and traditional encryption is not effective in preventing this from happening.

C) Data leakage cost data

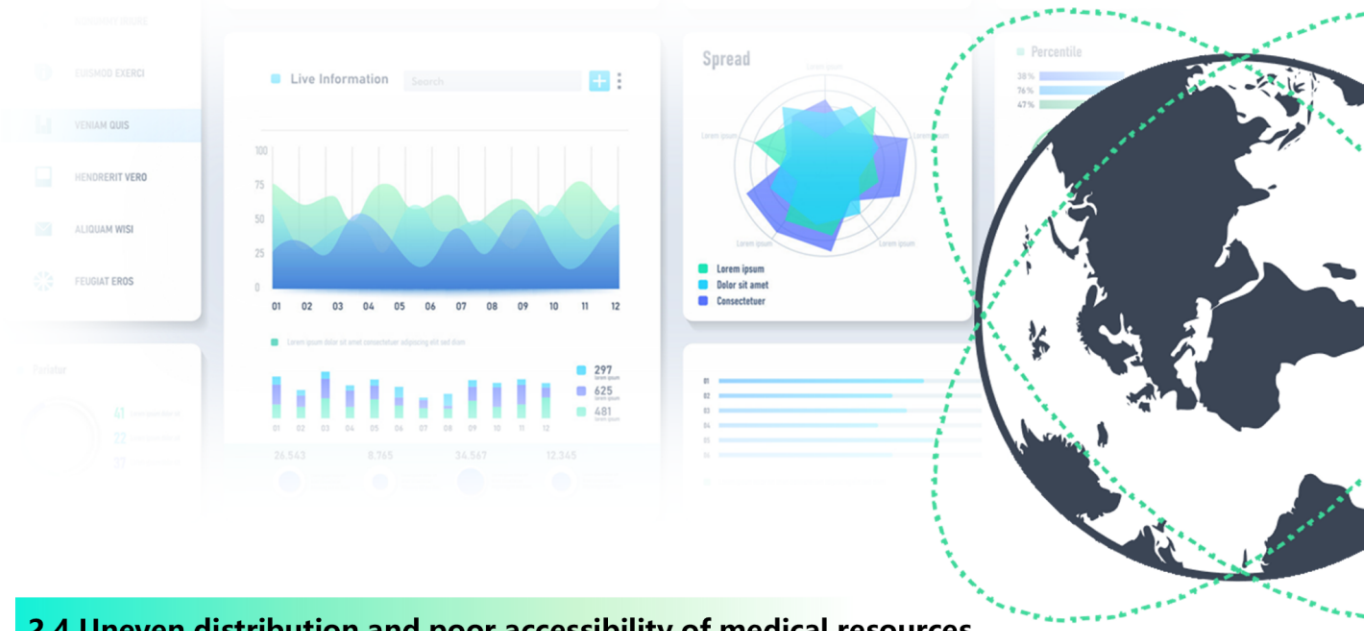
Medical data leakage is costly and brings huge financial losses to healthcare organizations and patients. According to HIMSS (Healthcare Information and Management Systems Society), the average cost of a global healthcare data breach reaches $11 million per breach in 2024, up 12% year-on-year. In the event of a data breach, healthcare organizations will have to bear huge financial losses, as well as face reputational damage, lawsuits and other issues, which will seriously affect the normal operation of healthcare organizations.



2.3 High cost and inefficiency of cross-border medical payments

Traditional cross-border healthcare payments are fraught with difficulties. When international patients use traditional bank remittances to pay for medical expenses, they usually need to wait for 3 - 5 working days, and the handling fee is as high as 5 - 10%. For example, for a $100,000 medical bill, a patient would need to pay $5,000 - $10,000 in fees, which undoubtedly increases the financial burden on the patient.

Patients from emerging market countries also face currency exchange problems in cross-border medical payments. Due to foreign exchange control and other reasons, it is difficult for patients in these countries to obtain enough foreign currency to pay for medical expenses. For example, when patients from some South American countries go to the U.S. for treatment, they may not be able to exchange enough U.S. dollars in a timely manner due to foreign exchange controls, leading to delays in their treatment plans.



2.4 Uneven distribution and poor accessibility of medical resources

The distribution of global medical resources is extremely uneven, and high-quality medical resources are mainly concentrated in developed countries and regions such as North America and Europe. According to statistics, most of the world's top 100 hospitals are located in North America and Europe, while medical resources in developing countries are relatively scarce. For example, many countries in Africa and South America lack advanced medical equipment and technology, and there is a shortage of medical personnel, which makes it difficult for patients to obtain high-quality medical services.

Low-income countries have low coverage of healthcare services, especially high-end healthcare services. According to the World Health Organization 2024, only 24% of the population in low-income countries has access to basic diagnostic imaging services, with less than 1% coverage of high-end services. This means that a large number of patients do not have access to basic medical services, let alone high-end medical technologies and treatments.

2.5 Inefficiency and Data Barriers in Medical R&D

The medical R&D sector faces the challenges of inefficiency and high costs. The R&D cycle for new drugs can take up to 10 - 15 years and cost more than $2.5 billion. Pharmaceutical companies need to manually integrate data from multiple sources during the R&D process, including clinical trial data and real-world data, which is a time-consuming and labor-intensive process of data acquisition and integration. For example, clinical trials require recruiting a large number of patients and collecting and organizing data on patients' medical histories, test results, etc., a process that often takes 6-12 months or more.

Data barriers are one of the main reasons for the inefficiency of medical R&D. Pharmaceutical companies and research organizations face many barriers in accessing real-world data, such as data fragmentation, inconsistent data formats, and data privacy protection. Data barriers make it difficult for researchers to obtain sufficient sample data, leading to sample bias and affecting the accuracy and reliability of R&D results. For example, in Alzheimer's disease drug development, the failure rate of drug development is as high as 99.6% due to sample bias caused by data barriers.

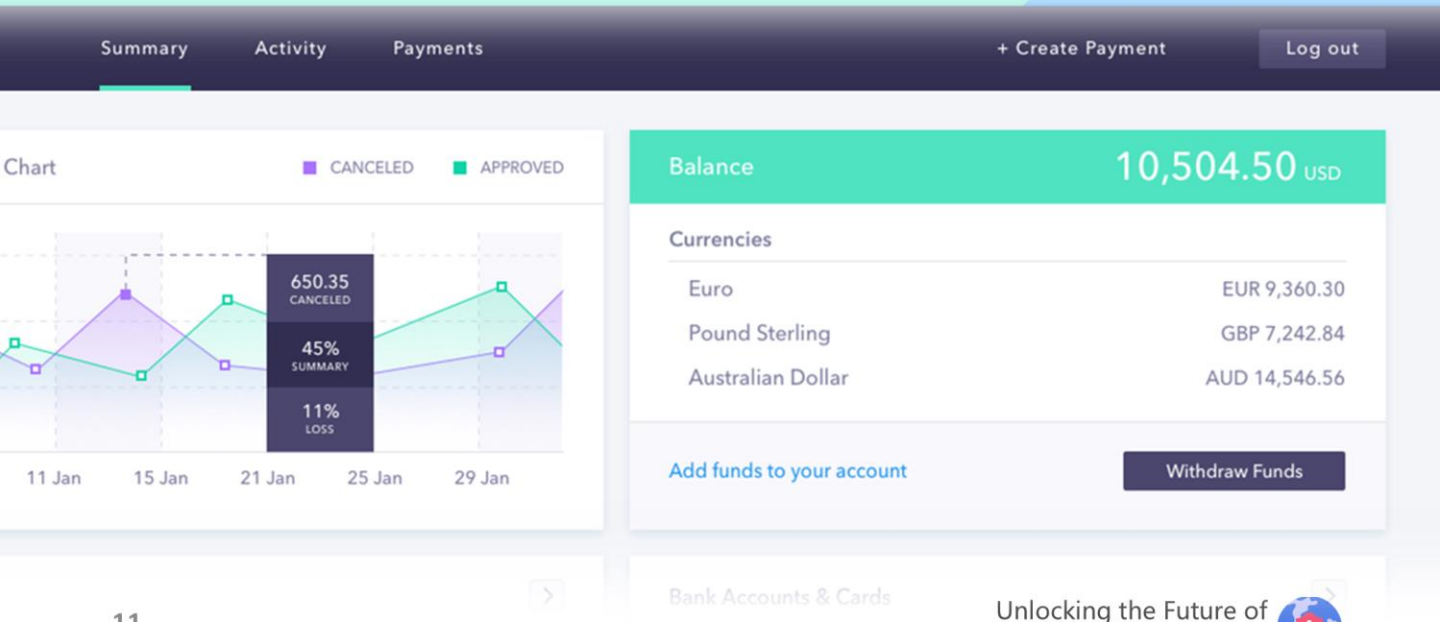
2.6 Insurance Fraud and Claims Disputes

A) Problems in the Insurance Claims Process

There are many problems in the insurance claims process, leading to frequent insurance fraud and claims disputes. Insurance companies often rely on manual review of medical records and other information, which is cumbersome and error-prone. For example, the manual review of medical records may omit important diagnostic information or treatment details, resulting in inaccurate claim amounts. In addition, the insurance claims process is complicated, and patients need to submit a large amount of information and procedures, with a long waiting time, causing great inconvenience to patients.

B) Insurance Fraud Loss Data

Insurance fraud brings huge financial losses to insurance companies and patients. According to the U.S. NHCAA (National Health Care Anti-Fraud Association), the annual loss of medical fraud exceeds $30 billion. Insurance fraud takes various forms, including fictitious medical services, exaggerated medical costs, and fraudulent use of another person's identity. These fraudulent behaviors will harm insurance companies and may result in higher insurance costs for patients, affecting their regular claims. The high incidence of insurance fraud makes insurance companies more cautious in the claims process, further aggravating claims disputes.



03 Project Solution

SOLUTION

3.1 Blockchain Application in Medical Data Management

A) Encryption and Confirmation of Medical Data

In medical data management, data security and privacy protection are crucial. Blockchain technology provides strong security for medical data through its unique encryption mechanism. Specifically, blockchain uses asymmetric encryption technology, where each patient and healthcare organization owns a pair of public and private keys.

Blockchain technology can realize the right of medical data. In traditional medical data management, the ownership and control of data is often unclear, and patients lack control over their medical data. Blockchain, on the other hand, clearly attributes ownership of medical data to patients through its distributed ledger feature. Every data access and usage record of the patient is recorded on the blockchain, creating a tamper-proof audit trail.

Distributed ledger & data authentication

① Decentralized storage: medical data is dispersed across blockchain nodes, preventing single point of failure and providing clear data ownership.

② Non-tamperable records: Data access and usage records are uploaded to the chain, any tampering is easily detected and patient data ownership is guaranteed.

Asymmetric encryption safeguards privacy

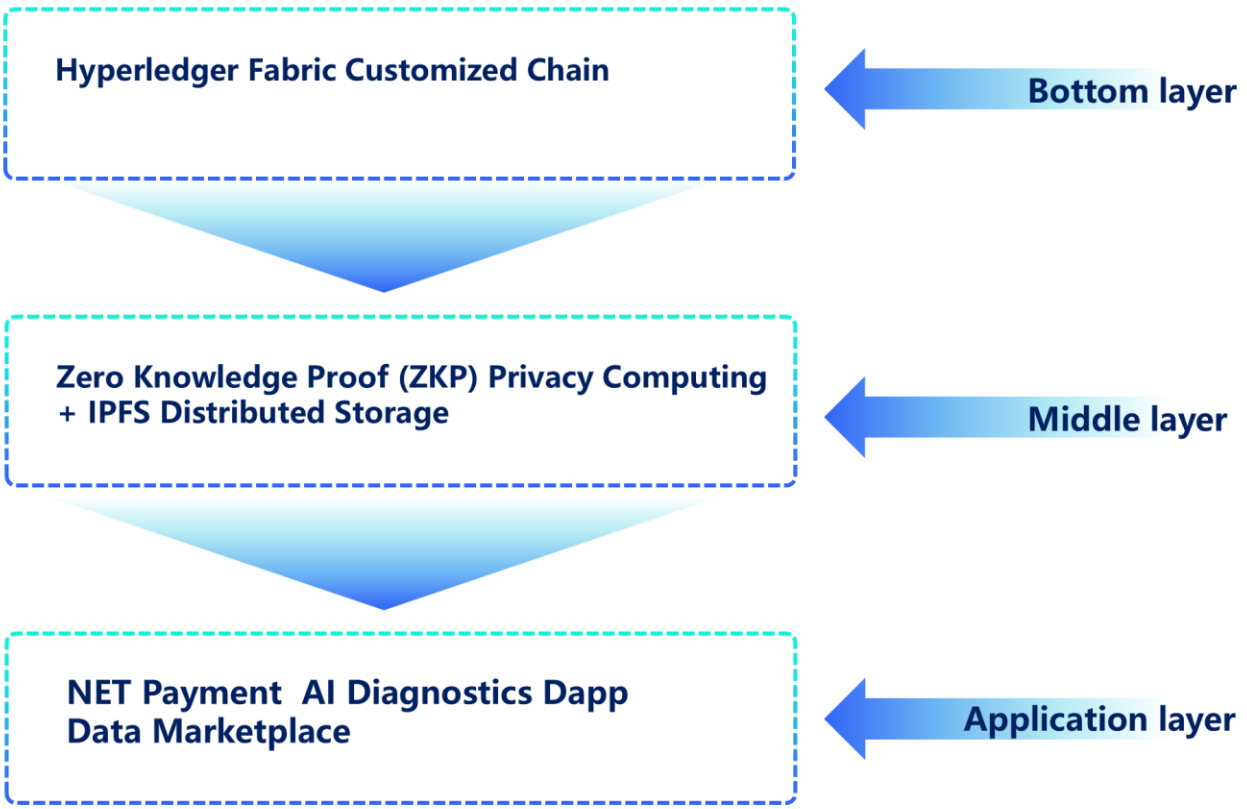
① Public-private key encryption: public key encrypts data, private key decrypts, ensuring secure data transmission and storage and protecting patient privacy.

② Fine-grained permissions: Patients set permissions with private key, medical institutions access according to authorization, enhancing patient data control.

B) Zero-Knowledge Proof (ZKP) Technology

Zero-Knowledge Proof (ZKP) technology is another important application of blockchain technology in healthcare data management.ZKP technology allows one party (the prover) to prove to the other party (the verifier) that it owns certain information without revealing any specific data content. In healthcare data management, ZKP technology can effectively protect patient privacy while ensuring data authenticity and integrity.

Specifically, when a healthcare organization needs to verify certain medical information about a patient (e.g., whether he or she suffers from a certain disease, whether he or she has received a certain treatment, etc.), the patient can use ZKP technology to generate a proof that he or she indeed possesses this information without having to disclose the specific data content to the healthcare organization. Upon receiving this proof, the healthcare organization can verify it via the blockchain network to confirm that the information claimed by the patient is true.



3.2 Cross-border Medical Payment Solutions

A) NET Token Payment System

NET Token Payment System is a cross-border medical payment solution based on blockchain technology.NET Token, as a digital currency, is decentralized, secure and efficient. Through the NET Token Payment System, patients can use NET Tokens to pay for medical expenses, and medical institutions can receive NET Tokens and exchange them for legal tender.NET Token Payment System utilizes the distributed ledger technology of blockchain to ensure the transparency and tamperability of transactions, providing a secure and reliable platform for cross-border medical payments.

B) Advantages of NET Token Payment System

Real-time Settlement

NET Token Payment System uses blockchain technology to realize real-time settlement. After the patient pays the medical expenses, the medical organization can receive the payment immediately without waiting for the processing time of traditional banks. This greatly shortens the payment cycle.

High security

The NET Token Payment System utilizes blockchain encryption technology and distributed ledgers to ensure the security and tamperability of transactions. Every transaction is recorded on the blockchain, creating a tamper-proof audit trail and preventing the risk of transaction fraud and data leakage.

Low Handling Fee

Token payment systems have much lower fees than traditional cross-border payments. While traditional cross-border payments typically have fees as high as 5 - 10%, the NET Token Payment System's fees are less than 1%. This translates into significant savings for both patients and healthcare organizations, reducing the cost of cross-border healthcare.

Easy Exchange

NET Tokens can be exchanged on compliant exchanges worldwide, allowing patients and healthcare organizations to easily convert NET Tokens into legal tender. This solves the problem of difficult currency exchange in emerging markets and facilitates cross-border healthcare payments.

B) Comparison with traditional payment methods

Comparative aspects	Traditional Cross Border Payments	NET Token Payment System
Processing times	3-5 working days	Real-time settlement
Handling fee	High to 5-10%	Less than 1%
Security	High security risk, vulnerability to attacks and data leakage	Utilizes blockchain technology for high security and tamperability
Convenience	Emerging market currency exchange difficulties	Global Compliance Exchange Convertible
Application	No specially optimized cross-border medical payment scenarios	Optimized for international patient care, medical tourism, etc.

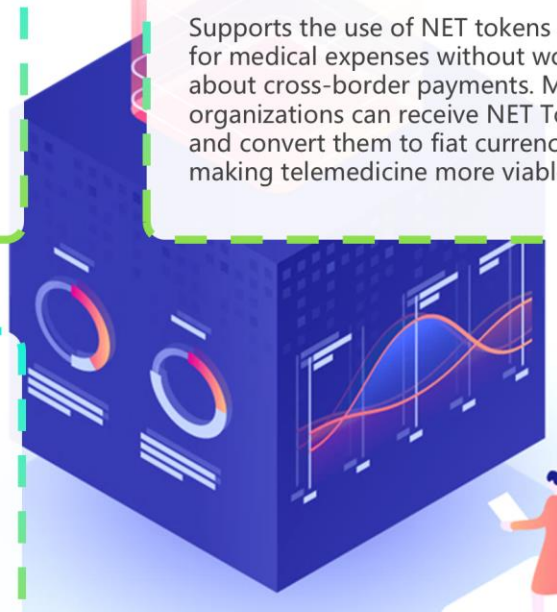
C) Application Scenarios

International Patient Access

Supports the use of NET Tokens to pay for medical expenses without worrying about currency conversion and fees. Healthcare organizations can receive NET Tokens and convert them to legal tender, improving the efficient use of funds.

Telemedicine

Supports the use of NET tokens to pay for medical expenses without worrying about cross-border payments. Medical organizations can receive NET Tokens and convert them to fiat currency, making telemedicine more viable.



Medical Tourism

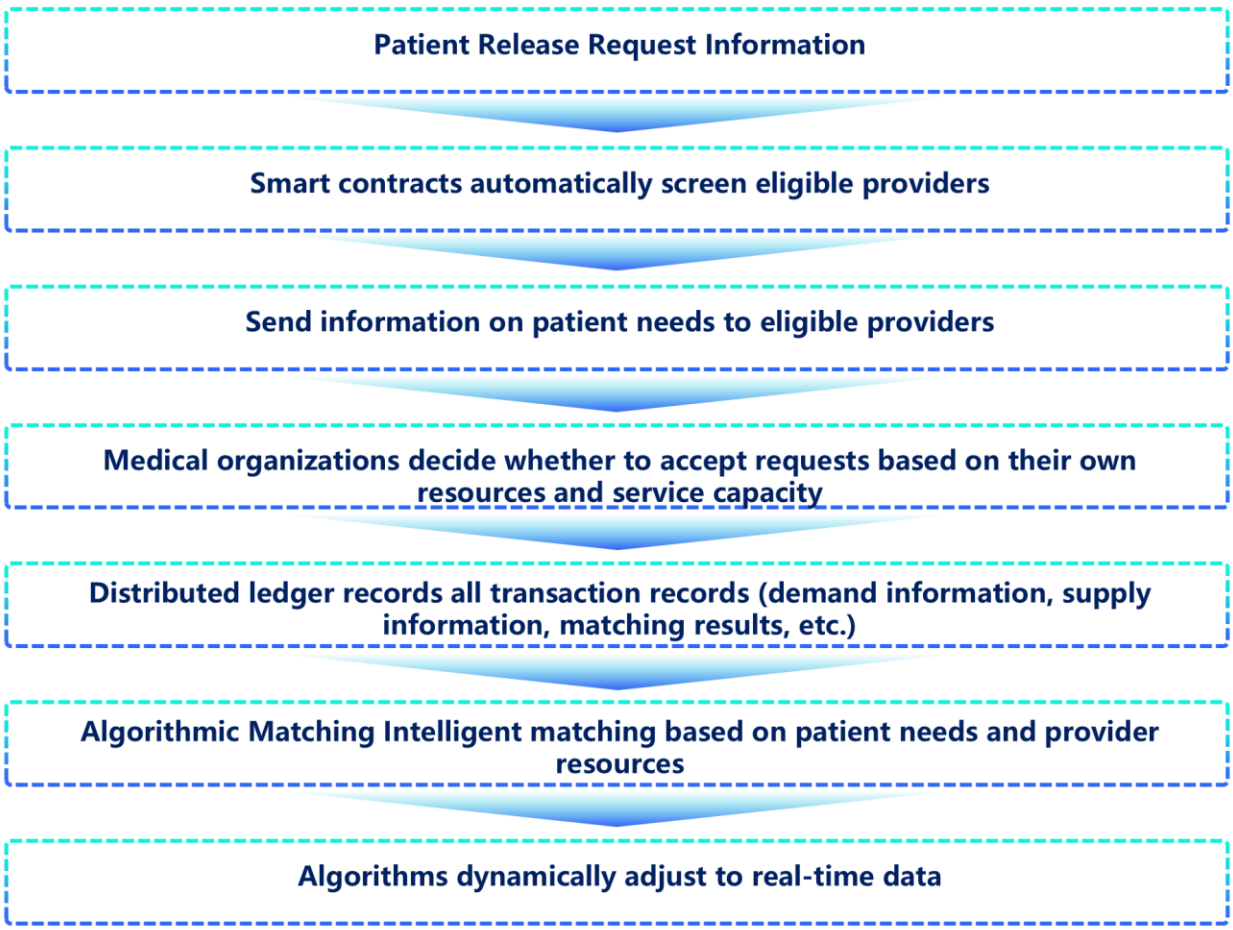
During medical tourism, you can use NET tokens to pay for medical expenses and travel expenses, enjoying a more convenient payment experience. Medical institutions and travel organizations can receive NET Tokens, increasing the competitiveness of their services.

3.3 Optimized allocation of medical resources and DAO matching mechanism

A) Principle of DAO matching mechanism

DAO (Decentralized Autonomous Organization) matching mechanism is a decentralized resource matching system based on blockchain technology. In the optimal allocation of medical resources, DAO matching mechanism realizes efficient matching between patients and medical resources through smart contracts and distributed ledger technology. Patients can release demand information through the DAO platform according to their needs and preferences, and medical institutions can release supply information through the DAO platform according to their own resources and service capabilities.The DAO matching mechanism automatically matches the needs of patients and medical institutions through smart contracts to ensure rational allocation and efficient utilization of resources.

B) Working principle of DAO matching mechanism



C) Advantages of DAO matching mechanism

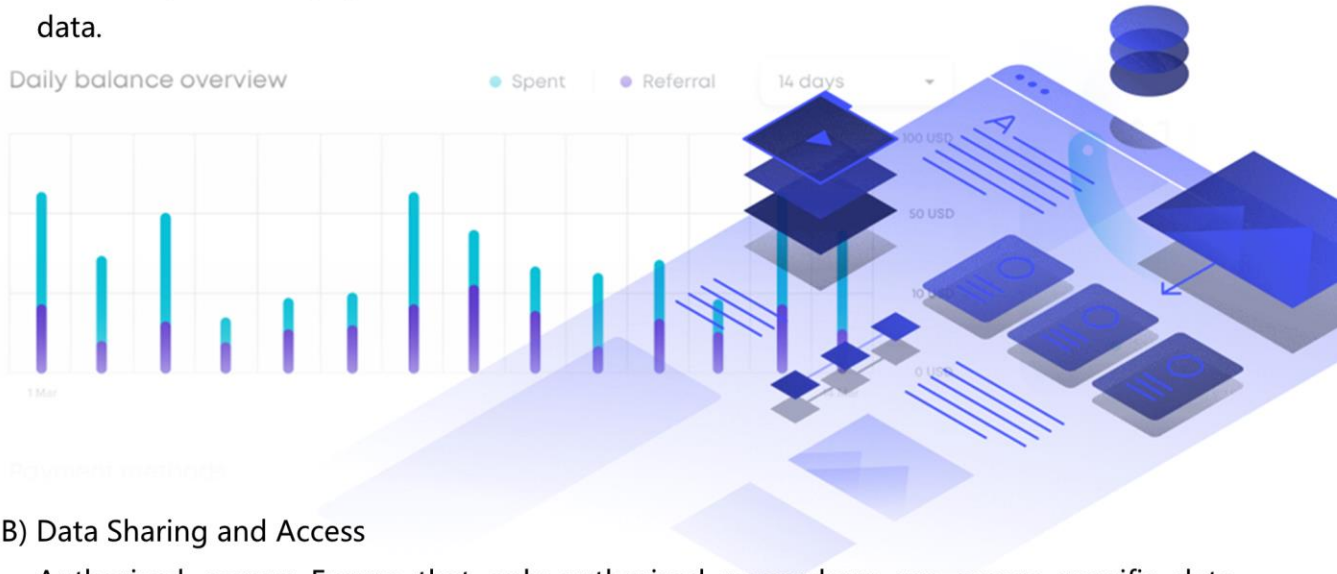
- Reduce the commission ratio: DAO matching mechanism reduces the involvement of intermediaries through decentralization, thus reducing the commission ratio. On the DAO platform, patients and healthcare organizations can conduct transactions directly without the need to go through intermediaries. This reduces the commission rate to 3% or less. For example, on the DAO platform, patients can transact directly with healthcare providers, who pay a small fee for the platform service instead of a high intermediary commission.
- Improved efficiency: The DAO matching mechanism improves the efficiency of resource allocation by automating matching and transactions through smart contracts and distributed ledger technology. Demand and supply information of patients and healthcare organizations can be updated in real time, and matching results can be generated quickly, greatly reducing transaction time.
- Enhanced Transparency: All transaction records are recorded on the blockchain, and patients and healthcare organizations can view the transaction records at any time for detailed information about the transaction. This enhances trust between patients and healthcare organizations and reduces transaction disputes. For example, patients can check the qualifications and service evaluation of medical institutions through the DAO platform, and medical institutions can also check information such as patients' needs and medical history, ensuring fairness and transparency of transactions.

DAO matching mechanism has a broad application prospect. With the continuous development and improvement of blockchain technology, DAO matching mechanism will provide a more efficient, transparent and low-cost solution for the optimal allocation of medical resources. In the future, DAO matching mechanism will cooperate with more medical institutions, patients, insurance companies, etc. to promote the globalization of medical resources allocation and sharing.

3.4 Medical R&D Data Sharing Platform

A) Data Storage and Management

- High-capacity storage: The platform is equipped with massive data storage capacity, capable of accommodating a large amount of medical data from different medical institutions and research institutes, including electronic medical records, image data, gene sequencing data, etc.
- Data Classification and Labeling: The stored data is carefully classified and labeled, making it easy for researchers to quickly locate the data they need. For example, categorize according to dimensions such as disease types, treatment modalities, patient age, etc.
- Data version control: Record the update and modification history of data to ensure the traceability and integrity of data and facilitate researchers to understand the evolution of data.



B) Data Sharing and Access

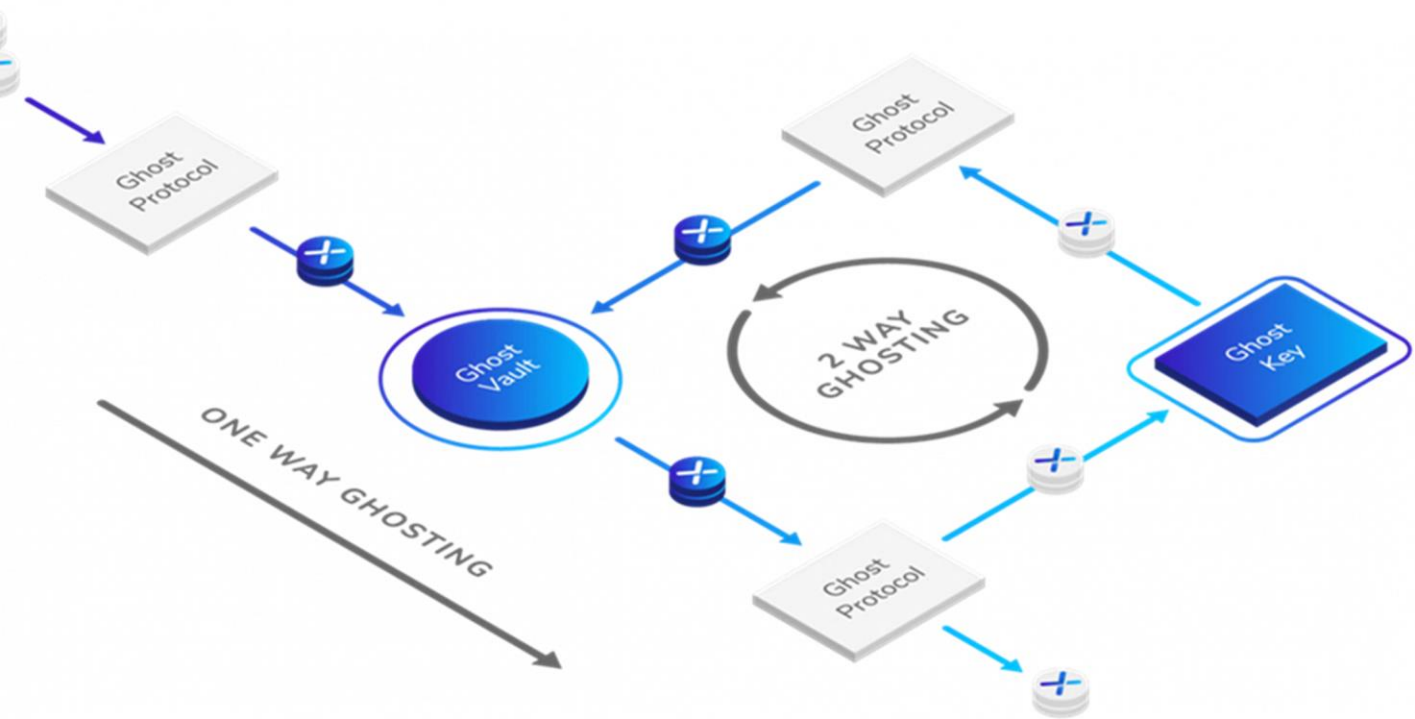
- Authorized access: Ensure that only authorized researchers can access specific data through a strict permission management mechanism. Researchers can apply for different levels of data access rights according to project requirements.
- Data sharing protocols: The platform supports a variety of data sharing protocols to ensure that data is shared under the premise of legal compliance. For example, it supports Data Use Agreement (DUA), etc., which specifies the scope and limitations of data use.
- Data desensitization and anonymization: During data sharing, sensitive information is desensitized and anonymized to protect patient privacy. For example, removing direct identifying information such as patient name and ID number.

C) Data Integration and Standardization

- Data Integration: Integrate medical data from different data sources to break down data silos and form a unified view of the data. For example, integrating data from hospital information systems (HIS) and laboratory information management systems (LIMS).
- Data standardization: Adopt unified data standards and formats to ensure data consistency and comparability. For example, follow international common medical data standards, such as HL7, DICOM, etc., to facilitate data sharing and exchange.

D) Data Security and Compliance

- Data encryption : Encrypt data in storage and transmission to ensure data security. For example, advanced encryption algorithms, such as AES, RSA, etc., are used to encrypt data.
- Access Control : Strictly control data access rights to ensure that only authorized users can access specific data. For example, adopting role-based access control (RBAC) mechanism to assign different data access rights according to user roles.



04 Token Economy

TOKEN

4.1 Token Overview

Token symbol: NET

Total number of tokens: 1,000,000,000 (1 billion)

Payment Functions

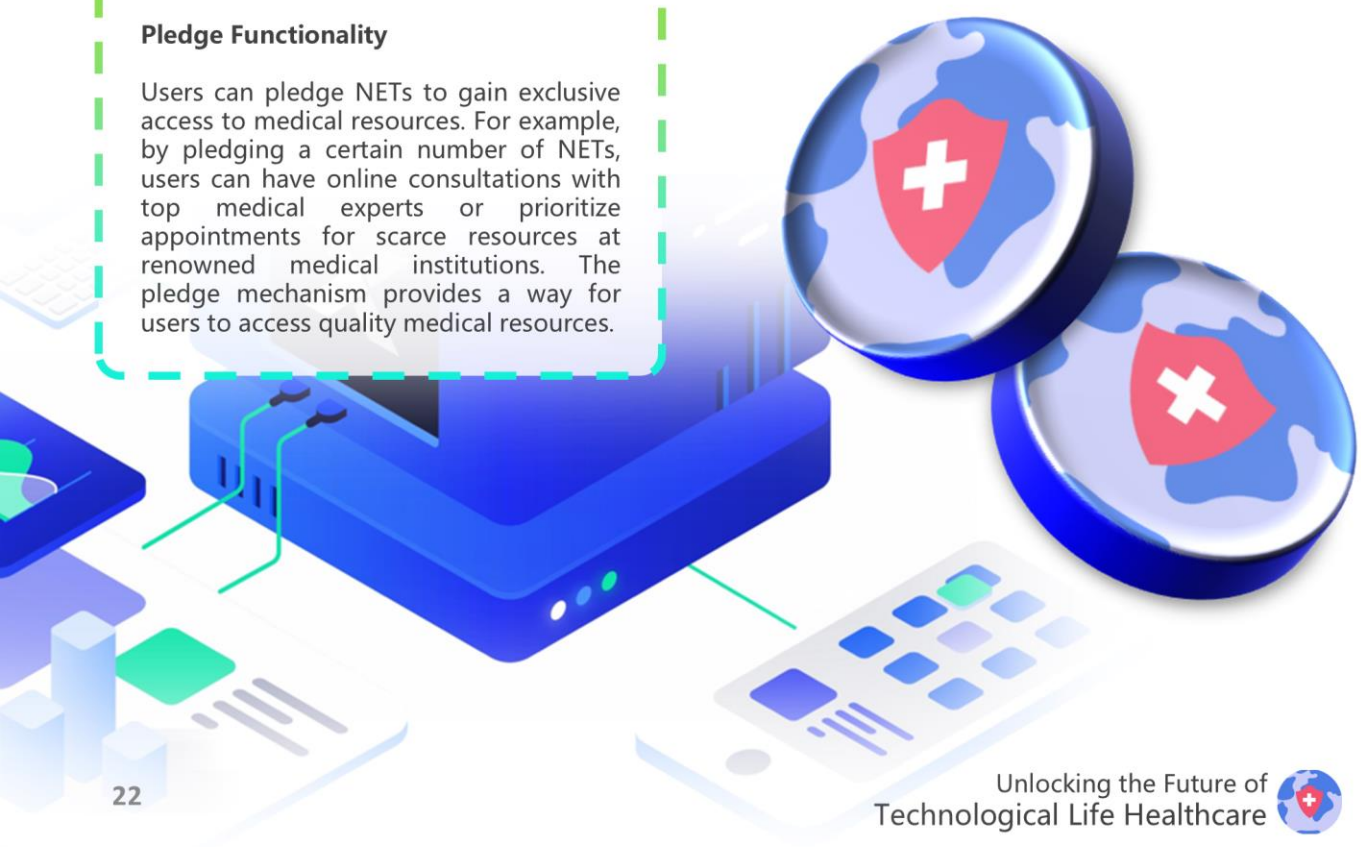
NET is the official payment token of the NEW Elements ecosystem and can be used by patients to pay for high-end medical expenses, such as specialist consultation fees, surgery fees, etc. It supports the purchase of healthcare data and promotes data sharing and industry advancement.

Governance Features

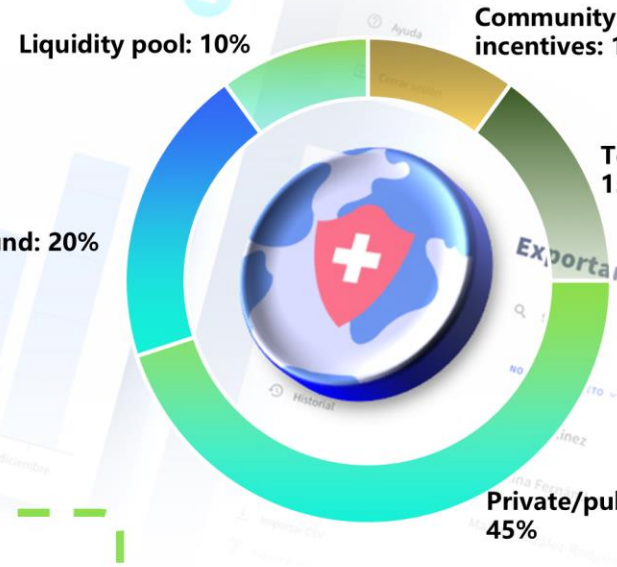
NET holders can participate in ecosystem governance through DAO voting, voting on upgrades and major decisions to ensure that developments are aligned with participant needs, such as voting to express their opinion on the introduction of new healthcare data standards.

Pledge Functionality

Users can pledge NETs to gain exclusive access to medical resources. For example, by pledging a certain number of NETs, users can have online consultations with top medical experts or prioritize appointments for scarce resources at renowned medical institutions. The pledge mechanism provides a way for users to access quality medical resources.



4.2 Token Distribution Program



Community Rewards (10%)

Incentivize community members to participate in ecosystem construction and promotion, e.g. receive NET rewards for participating in activities, promotion, providing constructive feedback, etc., to attract more users and partners and promote ecosystem development.

Team & Consultants (15% Lock-in for 2 years)

Reward core team members and consultants, including development, operations, marketing, and medical specialists, to encourage positive contributions.

Private Placement / Public Placement (45%)

Raise capital through private and public placements to support ecosystem development, operations and promotion for qualified investors and institutions, providing early participation opportunities and potential benefits to help build and promote the ecosystem.

Eco Fund (20%)

Set up an eco-fund to support long-term ecosystem development and innovation projects, investing in R&D and innovation in the fields of medical data security, medical AI, cross-border medical payment, etc., to promote technology upgrading and business expansion.

Liquidity Pool (10%)

Establish a liquidity pool to ensure the liquidity of NETs in the trading market, reduce transaction costs, improve transaction efficiency, support the trading of NETs on decentralized exchanges, and promote market liquidity and value discovery.

05 Team Members

MEMBERS

Jeremy Richardson

D. in Bioinformatics from Johns Hopkins University, former Director of Medical Data Analytics at Mayo Clinic, leading the development of early cancer screening models based on federated learning, published 27 medical AI papers and 5 patents. He is mainly responsible for the design of layered encryption architecture for medical data and leading the development of AI diagnosis module.

Neeraj Murarka

Currently also the Chief Technology Officer (CTO) and co-founder of Bluzelle. He has an extensive background in computer science and mathematics with a focus on decentralized and trustless computing systems.Neeraj has many years of experience in technology development and deep expertise in the blockchain space.

Oliver Peterson

A graduate of Stanford University, Oliver is a veteran full-stack developer specializing in creating high-performance applications using React and Node.js. He has worked at Netflix on the design and implementation of several front-end projects.

Nathan Matthews

Nathan has 20 years of hands-on experience in cybersecurity. He holds a related PhD from MIT and has worked at Palo Alto Networks, specializing in firewalls and intrusion detection systems.

Frank Douglas

Frank is a data researcher with a PhD in Artificial Intelligence from the University of Chicago. He has done excellent research in both natural language processing and machine vision, and has worked at Nvidia, driving several deep learning projects.

Samuel Wright

Samuel is a senior database administrator with deep technical knowledge of MySQL and PostgreSQL. He earned his degree from the University of Florida and worked on Uber's data team, managing large-scale data infrastructure.

Dr. Michael Anderson

D. in biomedical sciences from Stanford University, specializing in cellular aging and regenerative medicine. With more than 15 years of research experience in the life sciences, he has led several groundbreaking programs dedicated to the development of new therapies to slow cellular aging, providing core scientific support for NEW Elements' life science technologies.

Dr. James Thompson

Graduated from Harvard University's PhD program in genetic engineering, he specializes in gene editing and personalized medicine. He has achieved significant results in the application of CRISPR technology to life science research, advancing the use of gene therapy in extending human lifespan, and has become a leading figure in the NEW Elements genetic program.

Dr. Robert Martinez

D. in bioinformatics from MIT, specializing in big data analytics and life science research. He utilizes advanced data analytics to analyze aging-related genes and biomarkers to help develop precise life science strategies and enhance the science and effectiveness of programs.

06 Disclaimer

DISCLAIMER

The purpose of this white paper is to provide detailed information about the NEW Elements platform, including its technical architecture, market positioning, operational strategy and future plans. Before proceeding to read this document, we hope that you will understand and accept the terms and conditions contained in the following disclaimer.

A) Nature of Information

- FORECAST NATURE: The information and forecasts contained in this white paper are based on current market conditions and internal analysis of the NEW Elements platform. Forecasts may be affected by market changes, technological advances, changes in the regulatory environment, and other unforeseen factors and may differ from actual results.
- NON-INVESTMENT ADVICE: The information in this white paper should not be considered investment advice or any form of financial recommendation. Investors should conduct independent research and analysis before making any investment decision.
- Risk Warning: Investing in projects related to digital assets and blockchain technology involves certain risks, including but not limited to market risk, technology risk, operational risk and regulatory risk. Investors should be fully aware of these risks and bear the possible losses arising from the investment on their own.

B) Legal Compliance

- Compliance: The NEW Elements Platform is committed to complying with applicable laws and regulations and works with regulators to ensure compliant operations. However, the regulatory environment is subject to change, which may have an impact on the platform's operations and users' investments.
- Governing Law: The interpretation and application of this White Paper is governed by the laws of the particular jurisdiction. Investors should be aware of the laws and regulations of their location and ensure that their investment behavior complies with local legal requirements.

C) Intellectual Property

- Copyright: All content in this white paper, including but not limited to text, graphics, design and layout, is the intellectual property of the NEW Elements platform and is protected by copyright law.
- Restrictions on Use: No content in this white paper may be reproduced, distributed, transmitted, displayed, performed, modified or otherwise exploited by any person or entity without the prior written permission of the NEW Elements platform.

D) Other Disclaimers

- Accuracy of Information: Whilst every effort has been made to ensure the accuracy and completeness of the information contained in this White Paper, the NEW Elements Platform does not warrant that the information is completely error-free and accepts no liability for any loss arising from reliance on such information.
- Right to Change: The NEW Elements Platform reserves the right to update, modify or change the information contained in this White Paper at any time without prior notice.
- Limitation of Liability: In no event shall the NEW Elements platform be liable for any direct, indirect, incidental, special or consequential damages, including, but not limited to, lost profits, business interruption, loss of data or other commercial damages, arising out of the use of the information contained in this white paper.

The NEW Elements platform appreciates your interest in this whitepaper and hopes that this information will help you better understand our platform and vision. We encourage all potential investors to conduct adequate due diligence and to carefully consider all relevant factors before making an investment decision. NEW Elements Platform looks forward to exploring the future of digital asset trading with you and contributing to a more open, transparent and efficient financial market.

Please note that this disclaimer is not intended to limit or exclude restrictions or exclusions that may not be lawful under applicable law. If you have any questions about any of the terms of this disclaimer or would like more information, please do not hesitate to contact us.