TrueChain

——Hybrid Consensus Public Chain
with High Performance

Abstract

It is the demand of the times and the dream of TrueChain to create a public chain that will carry the future commercial decentralized applications. Based on the hybrid consensus mechanism, TrueChain aims to provide high-speed point-to-point communication, value transfer and the infrastructures of smart contract for the society.

The ultimate goal of decentralization is to create a free and mutual trust society. Thanks to the efforts of public chain projects like Etherum, public chain has developed significantly, and the commercialization of digital currency and smart contracts has become possible. Prior to this, some private chain and alliance chain have been successfully applied to make people have greater expectations for public chain developers. It is hoped that the arrival of the commercial public chain can solve the practical problems of high cost, such as digital payment, smart contract and so on. However, the core reason why the public chain is different from the private chain and the alliance chain is that the design of the consensus mechanism needs to ensure that the unfamiliar and scale extending nodes can build trust between each other through technical means, accomplish tasks together and ensure the stable and efficient operation of the public chain. Most of the existing consensus mechanism design is difficult to achieve a good balance between security and performance, as the dilemma between decentralized decision-making and administrative efficiency, has plagued the public chain developers.

TrueChain hopes to keep the essence of decentralization while improving efficiency as much as possible simultaneously. The emergence of the hybrid consensus mechanism which combined POW with PBFT brings a ray of dawn to the solution of the problem.

I. Strength

Support entry of infinite nodes

For large-scale commercial applications such as Internet e-commerce, instant messaging software, and bilateral trading platforms, supporting large-scale and increasing number of users is a necessary condition for the public chain to carry them. The communication complexity of PBFT determines that nodes participating in decision making can only be kept in a very limited range. The combination of the characteristics of POW that can accept unlimited nodes can make up for this disadvantage.

Safety

Because there is no guarantee in PBFT mechanism that all nodes participate in decision-making, there are relatively strong moral hazard and security risks. A small number of nodes' inaction or downtime may result in data tampering of other nodes or full chain paralysis. On the basis of POW, a hybrid consensus mechanism for the election of PBFT backbone nodes is designed to ensure timely re-election of the PBFT backbone nodes and monitor the backbone nodes in real time.

High performance

The timely recording of user transactions is a guarantee for the availability and security of the public chain. The communication efficiency of PBFT backbone nodes is sufficient to support 10000-100000 TPS (transactions per second). It is possible to ensure that the whole chain communication is not blocked while multiple smart contracts or commercial applications deal with transactions at the same time, and the ledger accurately records the transactions in chronological order.

Free use

Whether it is the initial test network or the future main network Stellar, TrueChain will remain open to all users free of charge. TrueChain always considers that the public chain is an infrastructure for all users, not a profit making tool. It is not only for TrueChain to find an appropriate source of profit in the future, but also for the development of public chain, or even the whole block chain industry.

II. Technical architecture

The technical framework of TrueChain is divided into three layers from bottom to top: hybrid consensus mechanism, smart contract and contract abstraction. For the specific design, please refer to the yellow book or GitHub open source code: https://github.com/truechain.

Hybrid consensus mechanism

The design of consensus mechanism is the core difference between the public chain and the private chain and the alliance chain. It needs to be decentralized enough to achieve security, and high speed to ensure performance. The industry has basically formed the understanding that it is difficult to balance the essence of decentralization and efficiency only by single consensus mechanism. In order to make up for the shortcomings of the previous two generations of block chain: Bitcoin and Etherum, of which TPS are too low and prevent them from realistic commercial application development, TrueChain selected a hybrid consensus mechanism combining the efficiency of PBFT with the decentralization of POW. On the basis of guaranteeing the essence of decentralization, a public chain with high performance and high reliability can be realized to carry out the target of large-scale commercial Dapp operation.

The solution of distributed protocol is roughly divided into two parts. One kind of POW solution, represented by bitcoin, has been proved to be difficult to go further in the transaction processing speed; one is a PBFT solution represented by a large number of private chains and alliance chains, which can efficiently deal with a large number of transactions. However, the PBFT solution requires that many nodes participating in the bookkeeping trust each other, so the nodes had better know each other before the agreement comes into effect. There is no doubt that when applying backbone nodes which records all transactions to the public chain architecture, a huge moral hazard exists. Establishing a consensus mechanism of efficient mutual trust in the public chain has become a worldwide difficulty.

The solution of TrueChain is taken by the director of the two. Keeping the mechanism of PBFT remained, the selection of backbone nodes is open to the public chain, and the POW protocol is used as the dynamic selection and agreement of the quasi-system to support the backbone nodes. The establishment of the backbone nodes community is converted from the nature of the private chain and the alliance chain to the public chain nature.

Smart contract

Smart contract layer is a key step in the application of consensus mechanism. The operation of smart contracts must rely on the completion of virtual machines to ensure that unified smart contracts can compute the same results in different environments. TrueChain inherited the design idea of EVM, and launched TVM on PBFT. TVM will be implanted into each backbone node, enabling them to invoke requests based on individual requirements.

Contract abstraction

The contract abstraction layer will abstract the basic business logic in the abstract smart contract, and simplify the process of developing complex smart contracts by developers.

III. Applications

Insurance

Insurance is also a field that can be put into force for TrueChain. The integration of block chain and insurance industry can really promote the development of insurance to automatic claims. The intelligent contracts under the block chain can automatically make claims when the triggering conditions happen, avoid cumbersome claims steps and get rid of possible moral hazard. Agricultural insurance has always been a difficult area for insurance to be involved in, because the grain output is affected by many natural and human factors. It is difficult to retain the evidence, so it is difficult for farmers to understand and accept agricultural risks. If the sensor is used to measure the weather conditions such as temperature, humidity, wind speed and so on, the automatic claim is triggered when the condition is reached, and the low cost, rapid and standardized claim will be realized by the characteristics of automatic completion and non-tampering of the smart contract. The same can be applied to aircraft delay risk. By calling the airline or the airport public interface, the smart contract automatically determines whether the flight is delayed and the cause of the delay is determined, thereby automatically triggering the claim. When the flight is delayed, passengers may calm down when seeing their account balance increasing. Large scale of siege around the boarding gate will not break up.

In addition, the traditional insurance industry may be subverted by the new mutual insurance model. Mutual insurance and decentralization trading mechanism are completely interconnected. All users are completely equal, instead of in a weak position compared to the insurance companies. Since the intermediary is no longer required to act as an organizer to establish a pool of funds, users can fully utilize the design of the block chain consensus mechanism and establish insurance on the form of point to point mutual assistance. Each premium payment can be traceable, open, transparent, timely and efficient. Combined with the hybrid consensus mechanism of TrueChain, mutual insurance can also be supervised to ensure the emergence of moral hazard.

Block chain technology enables the insurance industry to return to the main business of matching supply and demand and calculating risks, rather than focusing on asset management capabilities as much as today. This should not be the intention of insurance.

Medical care

In the medical field, the anonymity and decentralization of the block chain can be used

to protect the patient's privacy. Electronic health cases (EHR), DNA purse, and drug anti-counterfeiting are all possible applications of block chain technology.

IBM published a report on health care and block chain in 2017, which specifically explained the potential value of block chain technology in clinical laboratory records, regulatory compliance, and medical / health monitoring records, as well as health management, medical equipment data records, drug treatment, billing and claims, safety of adverse events, medical assets management, medical contract management and other special advantages.

In terms of EHR, an individual's complete health history record contains all the vital signs, high and accurate records of the medicine, the doctor's diagnosis, the patient's disease, and all the information related to the operation. The whole historical data related to the medical staff, the location and the events are valuable for precision treatment and disease prevention. The block chain happens to be the right one. The data of individual and institutional groups are stored and shared in real time.

In the system of TrueChain, every transaction has timestamp, and becomes a part of the permanent record which cannot be tampered with afterwards. All nodes can view all records in a public chain without permission. In a permission-restricted public chain environment, each node can establish a consensus mechanism to determine the node's access to the transaction, thus maintaining privacy and concealment of the real identity of each node when needed. In this way, the block chain realizes the complete record of the asset lifecycle. When assets flow through the entire supply chain, no matter patient health records or a bottle of pills, all records are clearly visible.

IBM investigates the value of medical executives to the block chain, and executives generally believe that block chains can most effectively eliminate medical information friction, including incomplete information, information risk and inability to access information. For example, computer records can ensure the accuracy of information input, and the property of the block chain, such as the selection of the fastest and best information into the database and the high security, will break through the past medical information barriers and maximize its own strength.

The standardization of smart contracts is a key link in the application of block chains, which is of great value in the supervision of medical behavior. When non-compliance events occur, smart contracts will automatically track compliance and send notifications to relevant parties in real time, effectively remove inspection links, simplify the implementation process, and reduce supervision costs.

On the basis of data confidentiality and reliable quality, organizations, institutions and enterprises can join the system and cooperate with data. Using personal health data, medical equipment data, data collected by medical and nursing staff, developing new medical applications or providing services, implementing health management and

creating new data sources, can form a larger block chain ecology and a virtuous cycle.

In terms of billing and claims, block chains can also effectively prevent improper behavior such as fraud, and reduce the waste of medical resources. Enterprise PokitDok, Capital One, and Gem proposed a platform supported by block chains to help patients before receiving treatment, determine the amount of self-payment in advance, provide pre-payment services, avoid the unexpected costs of the patients, and to reduce the amount of unpaid payments by medical institutions.

The traceability of block chain also includes the tracing of medical malpractice and the backtracking and supervision of drugs. For example, the establishment of a consistent drug distribution and management system will be a fatal blow to counterfeit drugs. Because the data of the block chain is updated and widely shared, pharmacies, manufacturers, buyers, regulators and other parties can observe the flow of data in real time, including drug manufacturing and distribution information, so as to strengthen drug regulation and prevent counterfeit drugs from entering the market. It is reported that the UK company, Blockverify, is one of the organizations to carry out drug source pilot projects to help medical staff verify authenticity through scanning drugs.

Block chain can eliminate adverse safety incidents, such as solving the safety problems of medical devices, especially the health devices connected to the network. In 2016, Johnson warned patients that their "OneTouch Ping" insulin pump was easily attacked by hackers, and FDA had reported a network security leak in St. Judah's medical heart equipment. Therefore, the normal operation of medical devices connected to the network is very important. Maintaining network security is also an important application of block chain in medical scenes.

Game

The combination of the block chain and the game refers to the creation of virtual assets for collection on the block chain, which is not like Etherum cat or Etherum Three Kingdoms, in which the players can obtain the false "block chain" game through the contribution of new players and the circulation of the virtual assets, but the use of cross chain technology in the game production which can upgrade the industry.

As far as current development is concerned, the focus of block chain can be applied to the game of virtual asset circulation and gaming platform. For most games, the users are not sticky enough and may lose quickly after playing Company A's game, because its gain in Company A's game can't be transformed into a drive to play other games of Company A. Through applying the block chain technology, the traceability, convenient circulation and low cost of the virtual assets can be ensured, and the loyalty of the old

players can be greatly improved, the ecology between different games of A company and the life cycle of the users can be extended. Small game companies can even unite to trade virtual assets in the same chain, in order to reduce user diversion costs and enhance user dependency.

Large games often hold many friendly matches and league matches. Using block chain smart contract can solve problems such as timely delivery and transparency. When the interface invocation gets the result of the game, the code automatically runs to complete the gambling delivery.

Public welfare

Public welfare is one of the main themes of today's time. By the end of July 2017, among the 70 million poor people in our country, nearly 30 million of the poor were poor. How to make public welfare more efficient, more fair and more transparent is the wish of every public welfare person.

Donors, out of social responsibility or personal love, donate money to charitable organizations to help the trapped groups or improve social problems. Where are these money used in the end? It may be a question mark in the hearts of every donor. The charity department will often be challenged. How can we prove that the money has been sent to the disaster area? How can we prove that hospitals really donate money to patients? The two sides often produce a lot of contradictions, like suspension of the source of denoted money, embezzlement, corruption and so on. It not only reduces the donated money, but also hurts the feelings of the donor.

The application of block chain technology to public charity will change the traditional mode of public charity donation information transmission. As a distributed ledger technology, the information on block chain has the characteristics of non-tampered, transparent and traceable. It can solve the pain point of public welfare charitable cause perfectly. When the user's good money enters the block chain system, it will be automatically recorded on the ledger of block chain and stamped with a timestamp. This record cannot be tampered and every donation and support will be tracked as "express".

Many blocks chain and charity projects have been tried to land.

In July 2016, the Ant charity block chain was officially launched. "Let the deaf children get the new sound" became the small scale test project of the Ant Financial and the Chinese Social Assistance Foundation. The new edition was launched in December 2016, adding the first block chain of the Chinese Red Cross Foundation "Say Goodbye to the Hearing Barrier" and the "Children Illuminating the Stars", realizing the real time

account publicity and helping to solve the "pain point" of public financial transparency. Until March 16, 2017, all the donation project on Alipay has been accessed to the ant block chain platform. Statistics show that, by January 30, 2018, there were 37 public welfare institutions, more than 300 public welfare projects, access to the Ant Block Chain Platform. More than 9.37 million donations have collected a total amount of over 48 million yuan donations.

In December 2016, the network mutual support platform held a "Heart Chain" conference in Shanghai. "Heart Chain" is a product which relies on block chain technology, specially designed for the public welfare industry. Relying on the block chain technology, all donations will be recorded on the "heart chain". Data including the amount of donations, capital flow is open and transparent. It is impossible for the public funds to be misappropriated illegally. This also makes personal kindhearted behaviors an objective "digital asset". As of October 2017, the times of platform donation has exceeded 100 million, and nearly 2 billion of the assets had been issued.

Numerous examples show the future trend of the integration of block chain and charity.

Asset Securitization

The extension of the digital currency lies in the token. Assets can be converted into tokens, and token can be turned into a proof of the assets usage rights. The transformation of assets into currency is a kind of securitization. If a book can be set up between the nodes and all the assets in the asset securitization pool are moved to this book, all the characteristics of the basic assets are marked, the block updates according to the transaction time which means non-tampered, and regular following up is conducted, the effective combination of asset securitization and block chain can be realized.

Digital advertising industry

The digital advertising industry monopolized by Facebook, Alibaba, Google, Baidu and other Internet giants has many industry pain points. Small and medium-sized advertising media, constrained by the size of Internet giants, are forced to form a "flow alliance" with weak bargaining power. For advertisers, the users who can modify the data and the group that is difficult to measure makes the digital advertisers face serious information asymmetry. Advertisers often pay high advertising costs for distorted users' clicks and coverage, but fail to achieve the desired results.

The existence of many advertising trading platforms has provided an alternative solution to advertisers to some extent, but the trust problem between the two sides

has not been eliminated. On one hand, some advertising platforms rely on the development of robots to increase the amount of advertising clicks and cheat for advertising fees; on the other hand, some advertisers refuse to pay advertising costs before the advertising media is released. Therefore, in fact, compared with the Internet advertising platform, the small and medium-sized advertising platform has lower efficiency and less mutual trust.

In the final analysis, the crux of the digital advertising industry lies in the trust mechanism. In the face of the high cost of trusting the Internet giants and the less expensive but fraudulent situations, advertisers are most hopeful of the emergence of a low-cost mutual trust trading platform. The commercial application of block chain technology makes this hope a reality.

Because of the characteristics of de-centralization, anonymity, openness, autonomy and irreversibility of transaction records, block chain technology provides a transparent and mutual trust trading platform for its advertisers. Followings can be mainly realized:
(1) data can be transmitted to the audience and can be counted.
(2) advertisers and advertising media are safe in funding.
(3) translucent transactions of all parties.

By using smart contracts, both parties can establish a safe and reliable trading mechanism, and make the advertising result measurable and reduce transaction costs. Users involved in advertising transactions have also entered the economic ecosystem of TrueChain, which can acquire or create higher added value in TrueChain's ecology.

Micropayments

In many situations, people occupy too much public resources or cause negative externalities but fail to pay the corresponding remuneration. If the rear vehicle exceeds the front vehicle from the left, it actually takes up the road traffic resources of the fast lane. A front car with the right of way has to slow down and yield the rear vehicle. If the times of autopilot is coming, when the rear car has the need to surpass the front car, it can send out a request for transcending from the left side and pays a small fee, and the front car will automatically yield to it after receiving the request. It can not only guarantee the completion of Overtaking Behavior, but also make the front car gain from giving up the right of way, which is safe and fair.

For another example, solve the problem of spam emails and spam messages. Assume every mail and text message is required to pay the counterpart a small fee before sending. For the normal communication, the cost of communication is not significantly improved because they send messages in both directions, but for people who send a

large number of spammers or spam messages, they will face a huge cost which reduces the possibility of sending garbage information in one way greatly.

The realization of small payment must be done by block chain without charge. TrueChain that provides high performance and stable trading environment is just suitable for these scenes.

Value transmission

Although there is a long way for block chaining technology to go, it can be seen that its application in the financial field is inevitable. It is not only currency creation, but the real changes that the block chain can bring to the financial industry lie in the value transmission and the public account. Many institutions both at home and abroad have made active exploration in the aspects of payment and settlement, asset registration and asset transfer. Because the block chain is a public, traceable, and non-tampered distributed general ledger system, it can effectively reduce the error rate of payment, liquidation, settlement steps, and monitor the inflow and outflow of each step of funds simultaneously, promoting the establishment of a faithful society and be conducive to financial supervision. With the development of block chain technology, the authenticity of assets will be further guaranteed.

Digital copyright

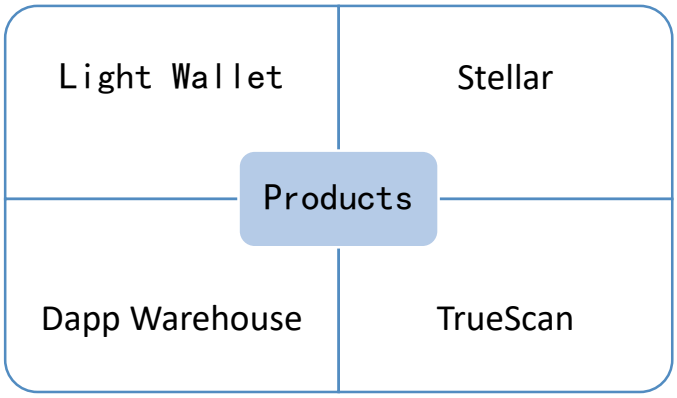
DECENT, a block chain company in Switzerland, hopes to use block chain technology to improve digital rights management. Through the digital video fingerprint identification, the unique "fingerprint" is abstracted from the motion change, color and key frame of the video. This fingerprint is used to track the video content on the protection network. Because of the uniqueness and irreversibility of the hash coding used widely in block chain data storage, the encoding of each file is not the same. Digital fingerprinting technology can systematically use the detailed characteristics of documents to distinguish genuine and pirated content, and trace the source of piracy.

Other application scenarios

Using the extensibility of its nodes and the efficiency and security of the consensus mechanism, TrueChain can be more applied to the fields of financial formats like mobile digital bill of exchange, securities trading, and supply chain management, property right tracking, digital certificate, etc.

IV. Product matrix

The product matrix of TrueChain is as follows:



TrueChain Light Wallet provides nodes with services such as receiving, sending and managing all TrueChain digital assets.

Stellar provides a convenient, stable and efficient smart contract development platform for commercial Dapp developers. Developers can manage the whole life cycle of contracts.

Dapp Warehouse is a user-oriented Dapp downloading platform.

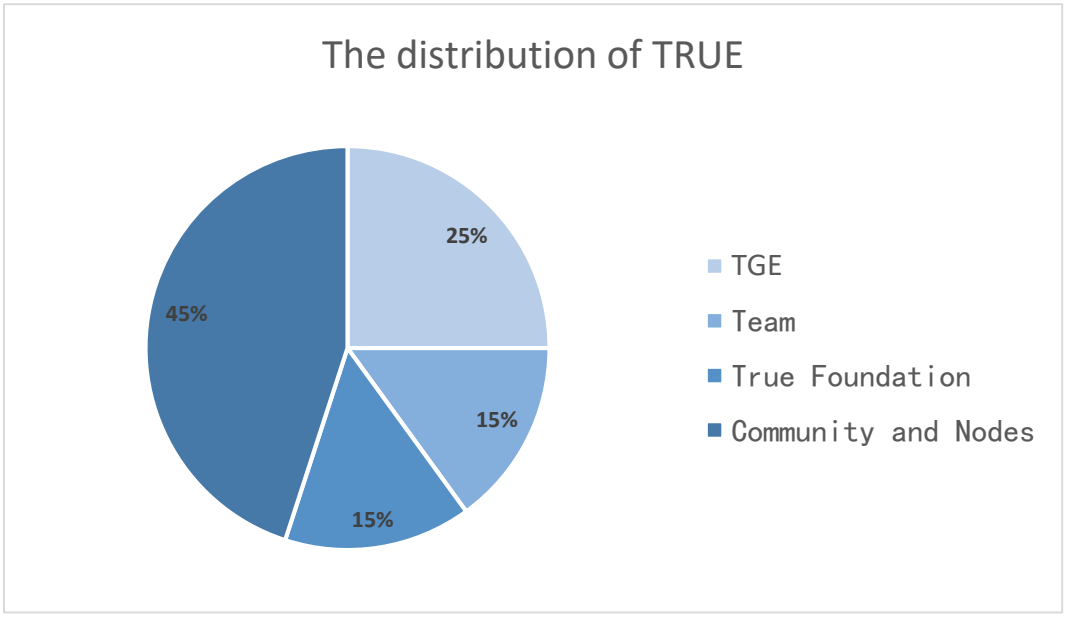
TrueScan, as TrueChain's browser, provides contract monitoring, transaction statistics, book search, privacy protection and other services to nodes.

In the future, TrueChain will continue to improve the smart contract development kit and expand the product richness of the infrastructure to meet the needs of the new generation of public chain users to develop personalized and complex smart contracts.

V. Token Economy

TrueChain uses its own TrueChain Currency (TRUE) as its token, which can realize the functions of value storage, payment means, value scale, etc. The total amount of issuance is 100 million.

The proportion of True distribution is shown as follows:



TRUE allocated to TrueChain's team will be restricted by the long term weighting schedule, and the specific contact rules are as follows:

A. 20%, or 3000000 TrueChain Currency (TRUE), is released after 3 months of token distribution.
B. 25%, or 3750000 TrueChain Currency (TRUE), is released after 12 months of token distribution.
C. 25%, or 3750000 TrueChain Currency (TRUE), is released after 24 months of token distribution.
D. 30%, or 4500000 TrueChain Currency (TRUE), is released after 36 months of token distribution.

At this point, TrueChain Currency allocated to the TrueChain team is lifted.

VI. Team Introduction

Technology, research and products

Archit Sharma (Ren X), an expert at distributed system, operation systems and performance engineering, is responsible for TrueChain engineering and engineering team management. Ren X has worked in Red Hat and CERN, engaged in large-scale cloud service and distributed system design and development. Ren X is a contributor of several important open source projects, as well as several Docker Hackathon champions.

Eric Zhang, is the founder and CEO of TrueChain, also the founder of China's top geek platform “TopHacker Group”, which connects technology geeks with various industries. TopHacker helps multiple block chain enterprises solve the core technical problems at application level.

Felix Cai, the front-end product leader of TrueChain, also a front-end geek, is graduated from Xi'an Jiao Tong University youth class.

Home Chen, the mobile terminal product leader, engaged in IT work for 20 years, has rich experience in Internet product design and development, and software project management. He was a technical partner of “CaiHuohuo”, responsible for the research and development of new products, server cluster and high concurrent processing.

Jesper L, an expert at applied cryptography, cryptographic protocol, distributed system consensus, is responsible for TrueChain’s consensus research. Jepser L is graduated from Tsinghua University.

Richard Wang, the leader of TrueChain’s China technology community, has the resources of 4000+ Internet technology executives nationwide, 300+ author and 400+ frontline developers. Wang has been the CTO and CEO of many Internet companies, and participated in several transformations of traditional Internet enterprises projects. He is also the technical author of Mechanical Industry Press, and have attended several major domestic technical seminars as guests and judges.

Seay (wizard), the security consultant of TrueChain, the author of “Code Audit: Enterprise Edition Web Code Security Architecture”, Seay source code security audit system author, and the blogger of well-known security blog “cnseay.com”. He once served at Alibaba security, and was the leader of Ali attack and defense laboratory, Sobug technology partner. Seay has experiences of more than ten years in security attack and defense and served for several well-known enterprises.

Business and operation

Xiaoyong Cheng, is the founder of TrueChain, Chief Strategic Officer, also the leader of global public relations and institutional investors, an experienced entrepreneur, and the member of Chang'an club. He is also the vice president of the black horse (2015-2016) and the member of the Great Wall Association.

Yan Liu, the operations director, is responsible for TrueChain products and business operations, as well as TrueChain community building and operation.

Larry Lin, as the founder of TrueChain, chief development officer, the expert of Internet marketing and community operation, has been responsible for the operation of "Baidu encyclopedia", which is the largest co-building community in China. Lin has more than 10 years of digital advertising and Internet industry experience, and was the author of several bestsellers in propaganda.

James Cooper, TrueChain's North American investor and media relations leader, is responsible for the global legality. He is also a global intellectual property legal expert, the professor of California Western School of Law, chairman of Proyecto ACCESO foundation project, former United States State Department, American Development Bank, American patent and Trademark Office consultant, United States representative of the world intellectual property organization.

Zhu Yu (binke), is the head of the Block Chain and the New retail Research Institute, the first head of the new retailing (O2O) department of Alibaba Group. He became the vice president of Shopin Enterprise in 2015, taking charge of offline entities and online overall work. He has rich experience in complete digitization and full channel communication, and digital marketing business.

Consultant team

Wei Xianhua, the professor and PhD tutor of Chinese Academy of Sciences, is also the deputy director of the virtual economy and data science research center of Chinese Academy of Sciences, and the executive director of the CAS - Reuters financial risk management joint laboratory.

Zhou Jinglong, the former partner of the Great Wall, which is the world's largest Internet Organization. He has a wide range of connections and resources of Internet industry and governments all over the world.

Zou Jun, the author of best seller "block chain technology guide", is also an expert of Zhongguancun block chain industry alliance. He is a PhD of Service Contract, the former chief software architect of IBM Australian financial industry, and have published more than 200 papers in the International Conference on IEEE, of which block chain related papers were awarded to IEEE ICWS in 2016.

Li Xiong, is the founder of LianXiang Finance and Economics.

Investor