ORACLE CHAIN

欧链技术白皮书

ORACLECHAIN TECHNICAL WHITE PAPER

ORACLECHAIN TECHNICAL WHITE PAPER

Contents

Abstract

As the world’s first application built on an EOS ecosphere, OracleChain needs to meet the demands of the Oracle (oracle machine) ecosystem by efficiently linking blockchain technology services with various real-life scenarios, thereby delving into this immense multibillion dollar valuation market. As a decentralized Oracle technology platform based on the EOS platform, the autonomous Proof-of-Reputation & Deposit mechanism is adopted and used as a fundamental service for other blockchain applications. In addition to Oracle services that provide real-world data to the blockchain, Oracle services that provide cross-chain data are also offered. Given that OracleChain can accomplish the functions of several prediction market applications, such as Augur and Gnosis, it can also support smart contract businesses that require high-frequency access to outside data in certain scenarios, such as Robo-Advisor. OracleChain will nurture and serve those blockchain applications that change the real world. Our mission is to “Link Data Link World,” with the aim of becoming the infrastructure linking the real world with the blockchain world. By achieving intra-chain and extra-chain data connectivities, we aspire to create a service provisioning platform that can most efficiently gain access to extra-chain data in the future blockchain world.

Keywords

blockchain, crypto-currency

Chapter 1 Design Concept

1.1 Industry Background

According to whether an interaction exists between intra-chain and extra-chain information, the application scenarios of blockchain can be approximately categorized into two types.

The first type is similar to Bitcoin, a single currency system, which mainly supports the circulation of currency within a chain. Thus, the entire business process exists only within a blockchain, and the interaction with extra-chain information is not needed. Currently, the majority of public chain projects fall into this type. Confined in its system, participants generate and consume data within this blockchain only.

However, in the process of blockchain technology development, particularly the development of smart contract technology, the interaction of intra-chain and extra-chain data is required in many application scenarios. This interaction forms the second type of application scenarios that require extra-chain data.

For example, in the financial sector, the realization of financial contracts as smart contracts on the blockchain inevitably requires the use of information stored in external financial systems to determine the status of contracts. This model of integrating extra-chain business processes and intra-chain smart contracts requires a channel where intra-chain and extra-chain data can be connected. For those blockchain applications that aim to serve the real world, obtaining external data to trigger the logical judgment of smart contracts is necessary. Applications such as decentralized trading market systems, decentralized insurance systems, various prediction market systems, and instant compensation systems for flight delays fall into this type. These applications require an oracle machine to obtain real-world data to perform smart contracts.

If the EOS platform opens the possibility for an efficient blockchain, then OracleChain further strengthens it by providing extra-chain data for blockchain applications to bridge the data chasm separating the real world and the blockchain world and to break down data barriers among different blockchain applications. OracleChain will invigorate the blockchain community, thereby generating more possibilities.

1.2 Innovation

A. Based on EOS Blockchain Platform

The EOS blockchain platform is designed based on a concept that has been universally verified and experimentally tested for a long time, representing the fundamental advancements of blockchain technology. The goals of the EOS blockchain platform are to support millions of users; to achieve free usage, easy upgrades, bug recovery, and low latency; and to integrate serial and parallel performances. With the excellent features of EOS, OracleChain can achieve a high throughput, efficiently provide Oracle data service, and ensure high processing capacity and low latency data services for blockchain applications, which make financial applications such as Robo-Advisor possible.

B. Participant Motivation and the Closed Loop of OCT

OracleChain will use an effective reward and penalty mechanism with the aim of stimulating data feeders to provide effective data feed service. All the data feeders, which regularly participate in data feed, will attain a high reputation and be rewarded with OracleChain Tokens (OCT). Conversely, irregular or fraudulent data feeders will have a low reputation and lose the OCT risk fund they deposited in the OracleChain platform. Through this double-effect mechanism, which we refer to as Proof-of-Reputation & Deposit (PoRD), OracleChain will effectively defend against hostile data feeders, which could affect the actual results of Oracle through malicious data feeds. Clients need to pay in OCT to have access to services, thereby achieving the closed-loop circulation of OCT within OracleChain.

C. Bridging the World

OracleChain will use data as a tool to connect the world and bridge the data chasm separating the real-world and blockchain applications, which will ensure connectivity between data in the real world and data in the blockchain world to promote the overall prosperity of the blockchain ecosystem.

D. A More Scientific Outlook on Data

OracleChain proposes the concept of “value of data” in blockchain. OracleChain also provides data service for blockchain applications and charges data consumers, thereby reflecting the value of data.

1.3 Mission

Our mission is to “Link Data Link World.” In view of the superior performance of the EOS blockchain platform, OracleChain positions itself as a service platform that connects intra-chain and extra-chain data, and provides public data services for large-scale commercial blockchain applications. Although the EOS project is still at its initial stage, it has already attracted considerable attention in the blockchain industry. OracleChain plans to take an active part in the establishment of the ecosphere, provide public oracle machine services, promote the landing of more applications, and ensure the common prosperity of the ecosphere.

The core objective of OracleChain is to become the infrastructure that links the real world and the blockchain world by introducing extra-chain data into blockchain to achieve data connectivity inside and outside the chain, and to build a service provisioning platform that can most efficiently gain access to extra-chain data in the future blockchain world.

Chapter 2 Technology Architecture

2.1 Platform Model

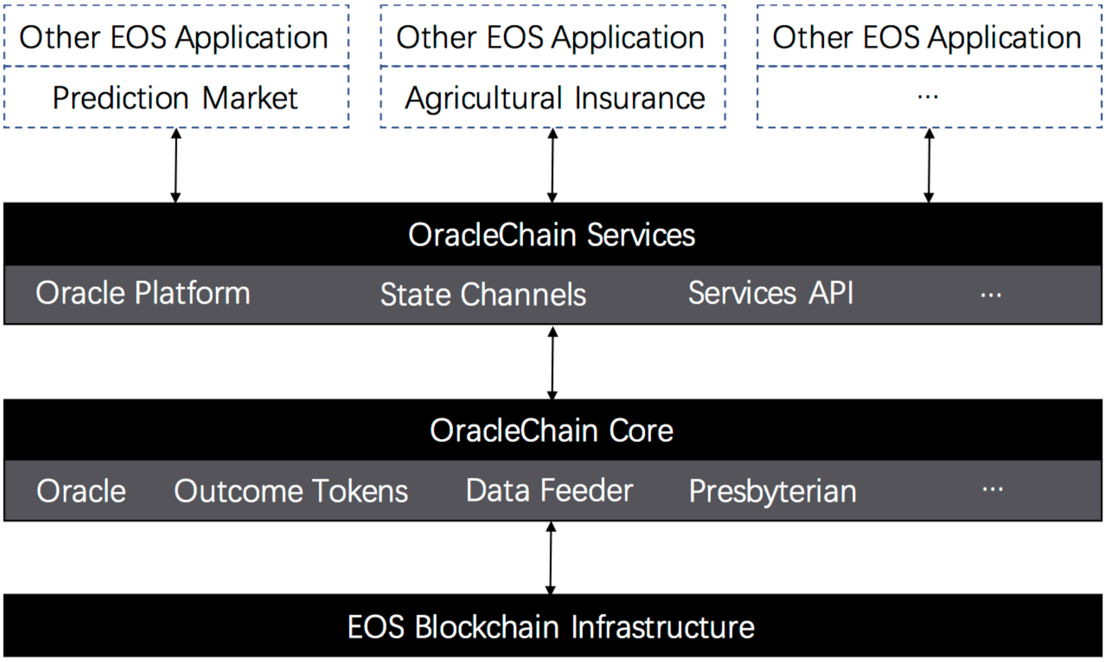

Figure 2.1 OracleChain Platform Model

The OracleChain platform consists of two levels, namely, core and services. On the basis of the EOS blockchain infrastructure, the OracleChain core builds on the basic service and operation mechanism. The services level on top of the core transforms the Oracle platform into an application programming interface (API) to provide Oracle services.

OracleChain Core

OracleChain Core provides Oracle, Outcome Tokens, and Data Feeder management and other basic services. OracleChain accomplishes the management of

Oracle and Data Feeder on this level. Data Feeders read the data based on the requirements of Oracle and work with other Data Feeders to complete the Oracle answer. In particular, OracleChain introduces the reward and penalty mechanism "Reputation," the penalty mechanism "Deposit," and the reward mechanism "Oracle fees" to complete the data feed process and finally provide an answer to Oracle.

Data Feeders work together to complete an Oracle and share its benefit. Data Feeders can also discover abnormal Data Feeders and trigger the penalty mechanism through self-organizing methods. Meanwhile, a whistleblower can report any dishonest yet not easily detected behavior of Data Feeders.

OracleChain deliberately sets up a Presbyterian mechanism, which consists of the most prestigious Data Feeders in the network to form a final group of judges who adjudicate the malicious data feeds and reporting behavior, and trigger the penalty mechanism to prevent malicious Data Feeder organizations (which do not self-punish members of the organization) and malicious whistleblowers.

OracleChain Services

OracleChain Services provide external services, such as Oracle Platform, State Channels, and Services API. OracleChain implements the matching and billing of Oracle services in this layer, which establishes the infrastructure capability of OracleChain.

The Oracle platform will match Oracle demanders and Data Feeder organizations. Data Feeder organizations may be unconsolidated temporary organizations or organizations that provide professional services. Each Oracle will state the cost, required organization mode, and participation thresholds of Data Feeders. For example, a total of 100 highly prestigious Data Feeders will be needed, among which 80 feeders have to reach an agreement to complete a data feed. The Services API will be designed to be more generic, in line with the design concept of the EOS cross-chain and the need for easy and convenient development.

Oracle services can be used for any EOS application on the OracleChain Platform model. Whether for a high-frequency prediction market or low-frequency agricultural insurance, OracleChain services can be used to truly serve the blockchain technology in real life.

2.2 Data Feed Mechanism

In a traditional centralized system, data are usually obtained directly from a data source in the form of data input. This data source could be within the centralized system or from a third party where the operation trusts and depends on the data entered by the data source. The data source acts as an upright, unbiased judge because it could be a tightly controlled module within the system or is performed by an absolutely trusted third party, where the system works efficiently under the drive of the data source.

We consider the decentralized blockchain situation in depth. This simple question becomes complicated and will lead to various questions, such as “Who qualifies for the trust of all subjects on the blockchain and can function as the data source?” or “Who is qualified to determine the credibility of the participants?” The sustainability of credibility is also subject to doubt. However, after attaining higher authority, a participant who consistently followed the rules and gradually accumulated credit has the potential to do evil.

OracleChain proposes a data feed mechanism to assist the data collection and trust gaining processes of blockchain under the background of decentralization. OracleChain will use an effective reward and penalty mechanism with the aim of stimulating data feeders to provide effective data feed service. All the data feeders, which regularly participate in data feed, will attain a high reputation and be rewarded with OCT. Conversely, irregular data feeders will have a low reputation and lose the OCT risk fund they deposited in the OracleChain platform. Through this double-effect mechanism, which we refer to as PoRD, OracleChain will effectively defend against hostile data feeders, thereby affecting the actual results of Oracle through malicious data feeds. Clients need to pay in OCT to have access to services, thereby achieving the closed-loop circulation of OCT within OracleChain.

In the PoRD mechanism, each Oracle corresponds to a smart contract. Each Oracle will have a threshold for its Reputation and Deposit. Active feeders of the blockchain network can participate in the data feed service of the Oracle only if its Reputation and Deposit exceed its threshold. When specified conditions trigger an Oracle to enter the settlement phase, the smart contract that corresponds to the Oracle will determine well-intentioned data feeds and malicious data feeds by using its processing logic and parameter settings. Well-intentioned data feeds will be rewarded with increased reputation and OCT deposit, whereas malicious data feeds will be punished with a deduction from its reputation and OTC deposit. Thus, the double-effect mechanism can ensure that the data feed service of the entire system works properly.

2.3 Technological Advantages

The four technological advantages of the OracleChain Platform are efficiency, compatibility, participation, and convenience.

Efficiency

Fine-grained control of block data and good parallel processing optimization are achieved by the basic blockchain infrastructure. The architecture of OracleChain can support second-level validation time and powerful transaction throughput.

Compatibility

OracleChain can provide data services to the entire EOS ecosphere and ensure data transfer and connectivity of intra-chain and extra-chain data through the cross-chain mechanism of the basic blockchain infrastructure.

Participation

Users can participate in the global Oracle consensus system and OCT ecological operation through data feeds. Unique governance strategies will encourage feeders to comply with community rules and use the PoRD double-effect mechanism to ensure the normal operation of OracleChain.

Convenience

OracleChain can provide a more efficient and practical Services API for other blockchain applications to use Oracle services.

Chapter 3 Governance Architecture

Governance based on blockchain systems has always been a difficult issue. Whenever an upgrade is needed, a hard fork should be implemented, which usually leads to many arguments and discussions between all blockchain stakeholders. Even a simple approach like modifying any set of variables in the source code could become complicated, such as the debate over the size of the block and the Segregated Witness mechanism in the Bitcoin community, because no clear upgrade path exists. Achieving such an agreement becomes more difficult when the interests of end users and decision makers are inconsistent. In fact, some complicated governance decisions, such as fixing a single smart contract error in “The DAO,” could lead to complex problems, resulting in community fragmentation.

The most significant cause of these problems is the lack of clarity and transparency in the definition of the decision process for protocol upgrade or modification. To address this problem, OracleChain takes its own management as part of its community consensus. The Oracle mechanism provided by OracleChain is used to make the negotiation process as effective and transparent as possible. Moreover, the consensus mechanism could be defined by multiple variables, which determine the function of the system or the modification of a certain parameter of the system, such as the basic cost of using Oracle services.

The basic understanding of community governance is that the governance strategy is to hand over authority to the highly prestigious feeders (users) on the OracleChain network. That is, different levels of governance activities require feeders to reach different levels of reputation to participate such that users will have different effects on the OracleChain based on different reputation levels. Feeders on the higest level can be granted limited and supervised permissions to freeze accounts, update defective applications, and even propose changes to underlying protocols.

OracleChain users can learn how to improve the protocol effectively by setting the to-be-negotiated variables as Oracle and by voting at all levels in the entire community. The governance strategy of OracleChain can prompt feeders to abide by the data feed rules in the community and maintain a high reputation to have a powerful voice in community governance. By building an Oracle for potential problems, we can help the community agree on which version of code to use. Each user will select the optimization measures, but a simple default strategy will maximize its value. By virtue of the rational decision of each user, many users will provide the correct direction for the entire OracleChain community.

Chapter 4 Implementation and Iteration

4.1 Development Roadmap

OracleChain officially launched its roadshow in China in June 2017. The first demo system is expected to start at the end of the year. The official system will be launched in July 2018. During the entire R&D process, the OracleChain team will closely track the development progress of the EOS project and advance the project synchronously.

4.2 Ecosphere Establishment

OracleChain positions itself as an essential link that connects intra-chain and extra-chain data in the EOS ecosystem and cultivates more advance applications based on it. The prosperity of an ecosystem depends on more active participation from many talents. Therefore, 10% of the OCT allocation scheme is the community promotion fund. The fund will be used to support several community activities, such as hackathons, to foster more developers. By organizing these activities, we also hope to find excellent ideas and teams, develop more blockchain applications around the database services of OracleChain, and promote the overall prosperity of the ecosystem actively.

Chapter 5 Application

5.1 Prediction Market

OracleChain can be applied in the prediction market. Prediction market applications based on OracleChain basic services will provide unique value discovery for local and global economies. In terms of blockchain, two projects, namely, Augur and Gnosis, connect intra-chain and extra-chain data. These projects use the prediction market structure, which indicates that a series of processes, such as community votes, can be used to generate fair data on the blockchain to import an extra-chain data into a chain. The prediction market structure can fully support scenarios that are low in interaction with extra-chain data, such as a smart contract on betting on the outcome of a football match. However, for scenarios where the frequencies are high, high requirements are proposed for the real-time performances of intra-chain and extra-chain data channels. OracleChain can support not only the low-frequency prediction market operation in the traditional manner but also the offline capturing of extra-chain data in real-time by multiple feeders and selecting an outcome from the feeding data provided by feeders and synchronizing it to the blockchain. In an EOS blockchain ecosphere with various application scenarios, an efficient strategy is needed to replace the inefficient offline supervision. To solve this problem, OracleChain will ensure a real-time and accurate service of the connectivity of intra-chain and extra-chain data through the self-governing structure of the PoRD mechanism.

5.2 Insurance Market

OracleChain can be used to organize the price and income of agricultural products of decentralized insurance markets in response to the national call to serve agriculture-related issues.

In the traditional insurance industry, insurance companies assume the intermediary status of absorbing and consuming risks. The emergence of blockchain has made large-scale mutual insurances possible. However, such self-organizing insurance schemes are beset by efficiency and risk levels, and they are difficult to generalize. OracleChain provides an alternative, particularly with respect to the prices of and income from agricultural products.

On June 1, 2017, the General Office of the Central Committee of the Communist Party of China and the General Office of the State Council issued “the suggestions on accelerating the establishment of the policy system to promote new agricultural business entities” (hereinafter referred to as “the suggestions”). The suggestions propose that we should actively conduct pilot projects, such as weather index insurance, agricultural product prices and income insurance, “insurance + futures,” farmland water conservancy facilities insurance, and loan guarantee insurance. In terms of agricultural product prices, which are a type of concentrated risk, insurance companies cannot easily use the traditional “space + time” risk-sharing model to reduce their own risks. Insurance companies can only use the “time” risk-sharing model. However, finding a corresponding risk distribution agency is difficult.

OracleChain can develop various types of smart insurances designated for agricultural product prices, which directly connect insurers and the insured. The purchase and compensation method based on smart contracts will significantly reduce the cost of insurance and directly apportion the concentrated risk of insurance companies to the individual risk takers.

5.3 Robo-Advisor

A blockchain machine has many application scenarios. Before smart contracts can truly automatically execute business logic in real life, its primary job is to access external data and use the automatic function of smart contracts based on the blockchain to execute business logic in place of traditional methods of human involvement. Robo-Advisor refers to a virtual robot that is based on the financial needs of customers, algorithms, and products, and performs the financial advisor services previously provided by human beings. In the blockchain, the functions of Robo-Advisor are accomplished mainly through smart contracts. Through the Oracle smart contract mechanism, OracleChain can be used to detect and process the price of intra-chain and extra-chain investment objectives, which can be used to establish the decentralized Robo-Advisor. Investment objectives can be either traditional financial targets or blockchain assets.

5.4 Sports Bidding

OracleChain can provide a decentralized data organization and processing scheme for sports bidding. Gnosis reports that the online global sports bidding market is large. The amount of gambling fees in regulated markets is at least billions of US dollars, whereas some estimates indicate that unregulated markets are 10 times larger than regulated markets. Despite considerable opportunities, companies and governments have been slow to innovate under existing models. Existing applications running in isolated data and pools of liquidity have limited accessibility and take a long time to promote new products to the market. Moreover, with the centralization of services, users will encounter additional risks, such as theft or other failures, and unexpected problems in payment.

The main obstacles to this centralized sports bidding service are data isolation and poor accessibility. Without an open, fair, and transparent access mechanism for the markets, products cannot provide a platform model that promotes innovation, yet it can be undermined.

OracleChain operates on an open platform, and the organization of all the bidding results is decentralized, fair, unbiased, and transparent. In this manner, old and new participants can safely obtain operational returns on the same platform, such as increasing liquidity, which translates to better odds.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[2] block.one,“EOS.IO Technical White Paper”, 2017.
[3] block.one(赵微、谭智勇、宋承根@OracleChain，梓岑@YOYOW 译),“EOS.IO Technical White Paper(EOS 白皮书-中文版)”, 2017.
[4] V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform,” 2014.
[5] Consensys, A Visit to the Oracle, 2016.
[6] J. Peterson and J. Krug, “Augur: A decentralized, open-source platform for prediction markets,” 2014.

First published in Chinese on June 22, 2017

Translated into English on Nov 7, 2017