IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 25, 2022, accepted May 24, 2022, date of publication May 30, 2022, date of current version June 13, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3179374

Toward Trustworthy DeFi Oracles: Past, Present, and Future

YINJIE ZHAO, (Student Member, IEEE), XIN KANG, (Senior Member, IEEE), TIEYAN LI, (Member, IEEE), CHENG-KANG CHU, (Member, IEEE), AND HAIGUANG WANG, (Senior Member, IEEE)

Digital Identity and Trustworthiness Laboratory, Huawei Singapore Research Center, Singapore 138588

Corresponding author: Xin Kang (kang.xin@huawei.com)

ABSTRACT With the rapid development of blockchain technology in recent years, all kinds of blockchain-based applications have emerged. Among them, the decentralized finance (DeFi) is one of the most successful applications, which is regarded as the future of finance. The great success of DeFi relies on the real-world data which is not directly available on the blockchain. However, due to the deterministic nature of blockchain, the blockchain cannot directly obtain indeterministic data from the outside world (off-chain). Thus, oracles have appeared as a viable solution to feed off-chain data to blockchain applications. In this paper, we carry out a comprehensive study on oracles, especially on DeFi oracles. We first briefly introduce the application scenarios of DeFi oracles, and then we talk about the past of DeFi oracles by categorizing them into several types based on their design features. After that, we introduce five popular DeFi oracles currently in use (such as Chainlink and Band Protocol), with the focus on their system architecture, data validation process, and their incentive mechanisms. Then, we compare these present DeFi oracles from their data trustworthiness, data source trustworthiness and their overall trust models. Finally, we propose a set of metrics for designing trustworthiness DeFi oracles, and propose a potential trust architecture and a few promising techniques for building future trustworthiness oracles.

INDEX TERMS DeFi, oracles, blockchain, trustworthiness.

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION

Over the past decades, blockchain has attracted great attention from both the industry and academia, due to its immutable and decentralized features. Blockchain has been widely used in many fields, such as decentralized digital identity and decentralized finance (DeFi). However, the blockchain system is in-nature a closed-system, which cannot retrieve off-chain data from the outside world directly. This is acceptable for the first generation blockchain, such as bitcoin, due to its simple application scenarios. However, for the second generation blockchain, such as Ethereum, due to the adoption of smart contract, this becomes a severe issue. This is due to the fact that in order to execute the smart contract, certain pre-defined conditions must be met, which usually depend on off-train information. As a key application of the second generation blockchain, DeFi also suffers from this issue, since DeFi highly relies on smart contracts.

To solve this issue, oracles, which are able to collect off-chain information data and feed desired data to on-chain smart contracts, have been proposed as a promising technology. Due to their importance, oracles gradually became the key components of DeFi as data providers and as an interconnection between the blockchain and the off-chain world. Oracles are now playing significant roles in many aspects of DeFi, such as decentralized coin exchange, DeFi lending, synthetic assets, decentralized insurance, and digital payment. Currently, there are many different types oracles in use, focusing on different functionalities. However, the trustworthiness of these oracles has not been investigated and discussed in existing literature. On the other hand, the trustworthiness of oracles is very important and directly affects the trustworthiness of the related DeFi projects. Guaranteeing the trustworthiness of oracles is of great importance to the success of DeFi projects. Thus, motivated by this, we are

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

going to investigate and provide a comprehensive analysis of the trustworthiness issues of DeFi oracles in this paper.

B. RELATED WORKS

Most existing works focused on categorization of blockchain oracles. These works categorized oracles by the data sources, transmission approaches, and transmission directions. By data sources, they are categorized mainly into software-sourced and hardware-sourced oracles in [1] and [2], as well as human-sourced oracles in [3] and [4]. By data transmission directions, they are categorized into inbound and outbound oracles [1], [3]–[5]. Inbound oracles transmit data from the off-chain side to on-chain side, and vice versa for outbound oracles. By data transmission approach, oracles can be categorized into pulling-based and pushing-based in [6] and [5]. Pulling-based oracles are executed on the data requester side while pushing oracles are executed on the data provider side. Reference [7] gave the categorization of centralized and consensus oracles by their degree of centralization of data feeds. These categorization works provided a detailed description of oracles. However, narrowing the scope to the DeFi industry, data transmission is mostly restricted to the method of inbound and software-sourced oracles, and current categorization criteria are too broad to provide an effective analysis on the trustworthiness of DeFi oracles.

Some research work also categorized oracles by their data validation mechanism. Reference [8] categorizes the oracles into voting-based and reputation-based ones together with the respective detailed variations. Reference [9] categorizes them into prediction markets, centralized data feeds, and oracle networks. Reference [6] specifies voting-based oracles as one of the data validation approaches. Reference [1] categorizes them into majority voting, weighted voting, trusted third party and self-verification, and so on. Reference [10] divides data on-chaining into TLS-based, enclave-based, and voting-based types. Reference [2] categorizes them into reputation systems, automated oracles, and human oracles. From the literature mentioned above, it can be told that ''voting-based'' data validation shows up as a high-frequency category. Indeed, as a data-validation approach, voting-based mechanisms contribute to the trustworthiness of oracles, but we would like to point out that there could be a more comprehensive and more essential way to analyze the trustworthiness of the oracles.

There are also some other works focusing on the criteria and challenges of oracles. Reference [11] suggests that oracles should have more transparency, accountability, and operational robustness; Reference [8] proposes that lower cost and higher speed, decentralization and security, and chain agnosticism are the future directions of research; Reference [4] proposes witness mechanism or reputation algorithms, security and privacy; Reference [9] suggests oracles emphasize on data authenticity, integrity, confidentiality, and availability. Most of the criteria for oracles proposed above focus on the functionality of oracles while neglecting the trustworthiness of the oracles.

C. CONTRIBUTION AND NOVELTY

The existing works neglected the trustworthiness of data source and the trustworthiness of data itself. Thus, it is necessary and important to have further up-to-date research to study the data feeding and validation from the perspective of trustworthiness. To fulfill the gap in the field, in this paper we contribute in the following ways:

1) We provide a comprehensive overview of the existing oracles, categorize these oracles by their data processing and validation process methods and provide visions and analyses of them from a trustworthiness point of view.

2) We provide a detailed analysis of existing popular DeFi oracles, such as Chainlink and Band Protocol. We investigate their design criteria, system architecture, data validation process, incentive mechanisms, as well as applications and ecosystem. We analyze their trust models and make a detailed comparison of the similarity and differences among them.

3) We summarize and propose a set of design metrics for trustworthy DeFi oracles. We propose a potential trust architecture for DeFi oracles. Besides, we propose several viable technical suggestions on enabling the trustworthiness of the data source and the trustworthiness of the data itself.

The rest of the paper are organized as follows. In Section II, we demonstrate applications of oracles in DeFi projects. In Section III, we analyze and give a categorization of DeFi oracles. In Section IV, we give a detailed analysis of current popular DeFi oracles and their design mechanisms. In Section V, we give our point of view on the future design of trustworthy DeFi oracles.

II. APPLICATION OF ORACLES IN DeFi

Oracles in DeFi mainly serve as price data providers. They are widely applied in decentralized exchange, DeFi lending, synthetic assets (such as stable coins), insurance, digital payment (such as cross-border payment), etc. In this section, we introduce the application of oracles to DeFi, including decentralized exchange, synthetic assets and DeFi lending.

A. DeFi LENDING

In a DeFi lending platform, price data is fed from oracles to miscellaneous procedures (Flowchart shown in Figure 1). Similar to lending in the traditional finance market, borrowers need to collateralize some assets of certain value in case users do not return the borrowed assets. Price data as an important input parameter determines the collateral rate and amount of deposit tokens issued.

An example of DeFi lending is Compound. In Compound, to borrow an asset, users need to collateralize DeFi assets at a certain rate against the borrowed assets. Users operate on an asset with a function *supportMarket*, which is validated and enabled by a smart contract *Comptroller*. Comptroller checks collateral rate with price data fed from Compound's own price oracle and makes sure actions are only validated

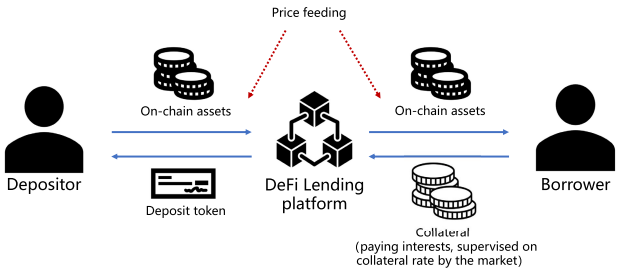


FIGURE 1. DeFi lending.

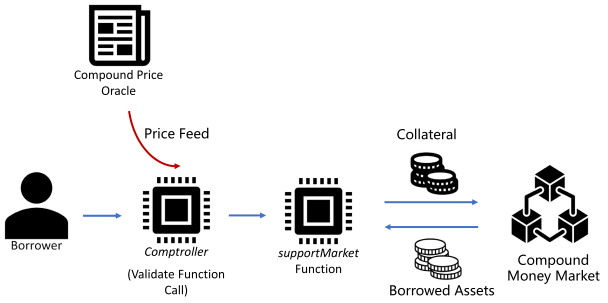


FIGURE 2. Compound lending.

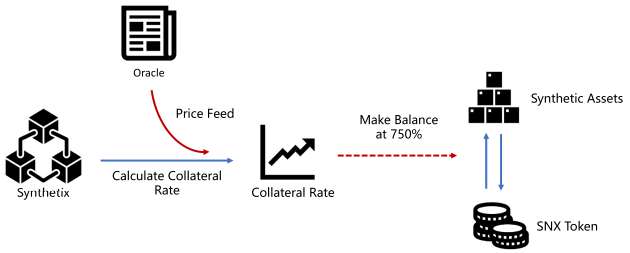


FIGURE 3. Synthetix flowchart.

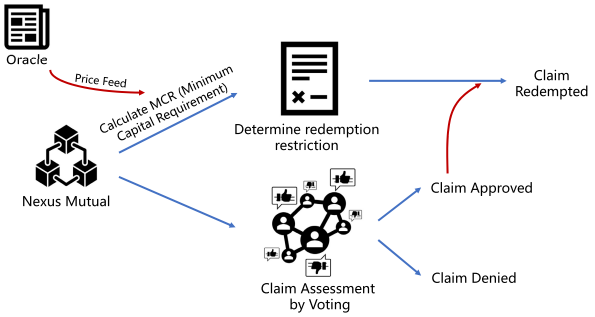


FIGURE 4. Nexus mutual insurance claiming flowchart.

with proper collaterals. With a valid collateral rate, a lending process is enabled. Oracle, in this circumstance, enables the core functionality of the lending platform. The flowchart is shown in Figure 2.

B. SYNTHETIC ASSETS

Synthetic assets are created by tracking the value of certain original assets and minting them into new assets against collaterals, similar to derivatives in traditional finance. Oracles provide price data to calculate the value of DeFi assets and decide the collateral amount on certain assets so that users can mint new assets by following the amount. The collateral rate and amount, as a key component of the system operation, are decided by the oracles.

An example is Synthetix, a synthetic asset platform. In Synthetix, users have to collateralize SNX token (the native token of the platform) to Synthetix Exchange to obtain synthetic assets, and a collateral rate of 750% is required, namely, the value of the collaterals should be 7.5 times that of mint assets. Such a proportional relationship is regulated by referring to the assets price data obtained from oracles [12]. For example, if a user mints 10 units of synthetic asset *A* worth 100 USD (10 USD per unit of A), and 250 SNX worth 750 USD (assuming 3 USD per SNX) need to be collateralized, then when SNX experiences a depreciation, with its price droped to 2 USD per SNX, then the value of total collateral (250 SNX) decreases to 500 USD, lower than the required 750 USD. Oracles feed the price data to the system. In this case, the user will be required to increase the SNX collateralized or burn out a certain amount of asset A to rematch the collateral rate, otherwise not being able to liquify the SNX collateralized (liquify, meaning the user exchange A back into SNX). As shown in Figure 3, oracles (mainly Chainlink for Synthetix) play an important part in DeFi synthetic assets.

C. INSURANCE

Due to the high volatility of DeFi asset value, users holding on DeFi assets face a high risk of incurring a loss. Therefore, DeFi insurance projects come to demand. Similar to insurance in the traditional finance world, users anticipate the risk of high value with relatively small cost.

An example is Nexus Mutual, a DeFi insurance project. To be covered by the insurance, clients need to collateralize a certain amount of assets to reach the Minimum Capital Requirement (MCR), the value and amount of which are determined by price data provided by oracles. In addition, a claim assessment process is conducted via voting to determine whether to approve the claim of insurance. If the claim is approved, the claim will be executed within a redemption restriction. The flowchart is shown in Figure 4.

III. PAST OF DeFi ORACLES

In this section, we compare the difference between centralized and decentralized oracles and their respective advantages over each other. We categorize decentralized oracles into four categories, based on their data validation process (i.e. source of data validity).

A. PIONEER: CENTRALIZED ORACLES

Centralized oracles are usually trusted third-party data providers backed by authorities or trustworthy parties

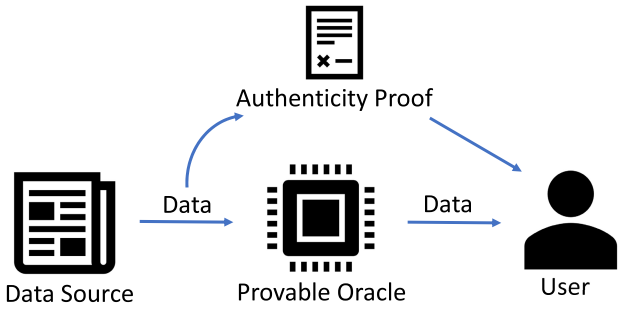


FIGURE 5. Flowchart of provable oracle data processing.

(e.g. government authorities, large companies with benign reputations, etc.), and usually have a single data source. In centralized data providing, data are validated from both the level of software and hardware. The data acquired from local storage of data providers are secured by trusted execution environments (TEEs), which isolate data from the operating system of the untrusted local devices, and the data transmitted online are secured by data transmission protocols to ensure that the data is not tampered or lost.

Provable is an example of centralized oracles, providing users with authenticity proof of the data along with the data fed. As introduced by its whitepaper, the authenticity proof mainly includes 3 types: the TLSNotary Proof, Android Proof and Ledger Proof. These proofs enable users to audit untampered processes of data transmission and are supported by software and HTTP protocols and hardware (namely TEEs) (Flowchart shown in Figure 5). Provable claims that with authenticity proof users can receive data from Provable without trust. Despite the claim given by the whitepaper above, users still withstand the probability of Provable's protocols not being reliable or failing at data feeding, for example, encountering system failure or being attacked. Such risks are taken by Provable users and backed by the company's credit [13]. Provable now has partnerships with IT research companies (Gartner etc.), banking companies (Intesa Sanpaolo, EY, etc.), blockchain venture companies (Coinsilium, etc.), and so on.

B. DEVELOPMENT: FROM CENTRALIZED TO DECENTRALIZED ORACLES

With the development of DeFi oracles, decentralized oracles began to show their advantage, with increasing application in DeFi. Decentralized oracles obtain data from multiple data sources with certain decentralized validation mechanisms to prevent or reduce the impact of malicious data, which will be introduced in detail in later parts of this paper.

In comparison, centralized oracles usually have an advantage in data processing speed than decentralized ones and are easier to construct and realize, while decentralized oracles have better scalabilities and lower failure risks due to the fact of having multiple data sources and decentralized data processing mechanism. Therefore, centralized oracles are more applicable to circumstances with high time-effectiveness requirements than decentralized ones, while decentralized oracles are more applicable to higher adversarial risks situations but with lower time-efficiency requirements. Furthermore, decentralized oracles fit better with the ideology and development trend of scalability and decentralization of DeFi. The comparison is summarized in Table 1.

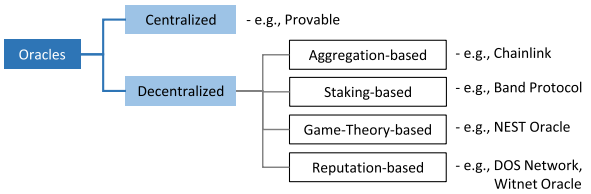


FIGURE 6. Categorization of DeFi oracles.

C. DECENTRALIZED ORACLES: DATA VALIDATION MECHANISMS

Decentralized oracles have miscellaneous methods of processing and integrating data obtained from providers. In this paper, we categorize the data validation methods into 4 main categories: aggregation-based processing, staking-based processing, game-theory-based processing, and reputation-based processing (as shown in Figure 6). Meanwhile, it should be noticed that an oracle may use a combination of multiple mechanisms mentioned above.

1) AGGREGATION-BASED PROCESSING

Aggregation-based data processing use predefined logic and mechanisms to obtain a deterministic result from multiple data sources, regardless of individual data source quality or performance. It aims at canceling out the impact of malicious data and other adversarial actions by aggregation.

Data aggregation may take miscellaneous methods, including taking the medians, mean value, or mode value of the data. One of the commonly used methods is taking the median to aggregate the data. It can be done along with additional validation methods including adding a maximum tolerance of price variance so that the price cannot change at an abnormally large rate (e.g., the Compound), or adding a time limitation of data validation so that too newly added data or obsolete data is not used for the price reporting (e.g., the AmpleForth) and so on.

2) STAKING-BASED PROCESSING

Staking-based data processing ensures the trustworthiness of data by requiring participants to stake a certain amount of assets as collateral against malicious actions, namely economical penalties. For example, Band Protocol has a data validation mechanism of selecting validators with the most staking to conduct data feeding, and users conducting adversarial actions will be slashed (meaning their staking is reduced by a certain amount). The more staking a validator has, the more likely he will be selected for the data feeding job since it is

TABLE 1. Comparison between centralized and decentralized oracles.

Criteria	Centralized Oracles	Decentralized Oracles
Data Feeding Mechanism	Single trusted third party	Multiple decentralized data sources
Feasibility	Relatively higher	Relatively lower
Performance	Higher time efficiency and data throughput	Lower time efficiency and data throughput
Risks	Low scalability; single node failure risk	Strong scalability; resistant to single node failure risk
Examples	Provable, etc.	Chainlink, Band Protocol, NEST Protocol, etc.
Applicable conditions	Fast response requirement; lower risk-tolerance	Slow response requirement; higher risk-tolerance

less likely that he behaves dishonestly against his staking. On Tellor [14], miners of a new block have certain stake requirements and will be slashed if the data determined by the block he mined is successfully overthrown by a later disputation process.

3) GAME-THEORY-BASED PROCESSING

Game-theory-based data processing provides users and data providers with economic incentives to act in non-adversarial ways even though they have no assets as regular collaterals. In such systems, users have an overall higher mathematical expectation for benefit from conducting non-adversarial actions than adversarial ones, or a lower expectation for the cost of non-adversarial ones than adversarial ones. An example is the NEST Protocol, which constructs a price-chain mechanism. In the system, any user is able to raise a new price of an asset and claim it as a new block on the price chain. To ensure the uploaded price is accurate, the new price raiser has to collateralize a certain proportion of assets at the moment he raises the price. He have to wait for a time period before his collaterals are returned. During this time period, anyone is able to liquify collateral. This means if the price is not accurate for the market within the period, the collateral can be bought/sold by arbitragers at the real market price. Therefore, providing inaccurate price data causes a loss when the collaterals are liquified. Meanwhile, arbitragers need to raise another price and put new collaterals to continue the self-correcting mechanism [15].

4) REPUTATION-BASED PROCESSING

Reputation-based data processing aims at filtering data providers with a reputation evaluation on data providers, punishing the adversarial nodes by reducing their reputation and therefore restricting their chance of data feeding. *DOS Network* (Decentralized Oracle Service Network) is an example of reputation-based data processing. The system provides a service of calculating the *QoS score (Quality of Service)* of data providers and reduces the score of low-quality nodes while it removes certain nodes with abnormal scores [16]. Witnet is another example, giving nodes reputation scores, and incrementing or decreasing the score according to their performance [17].

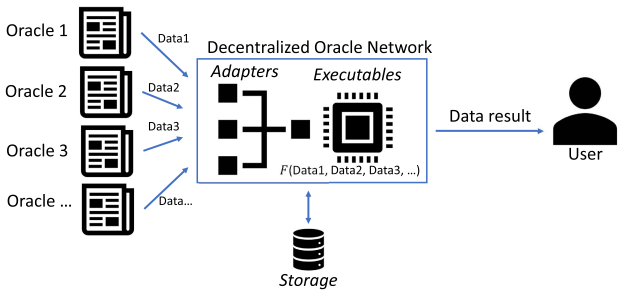


FIGURE 7. Flowchart of chainlink oracle data processing.

IV. PRESENT OF DeFi ORACLES

In this section, we introduce and analyze five currently active oracles mechanisms, including Chainlink oracle (aggregating-based), Band Protocol oracle (staking-based), NEST Protocol (game-theory-based), DOS Network (reputation-based) and Witnet oracle (reputation-based), and give a brief comparison among them.

A. CHAINLINK ORACLES

Chainlink oracle is an aggregation-based oracle with a*Decentralized Oracle Network* (DON) aggregating data from different data providers and is one the most popular decentralized oracles in DeFi.

1) DESIGN CRITERIA

According to the Whitepaper of Chainlink [18], the main goals of Chainlink include *hybrid smart contracts* (being a framework integrating the computational power both on-chain and off-chain, realizing the full potential of smart contracts), *abstracting away complexity* (simplifying user experience), *scaling* (meeting the demand of growing scales of the system), *confidentiality* (protecting the privacy of users while maintaining the transparency of the system), etc. Among these goals above, the main goal is the first one, constructing a hybrid smart contract.

2) SYSTEM ARCHITECTURE

a: DECENTRALIZED ORACLE NETWORK (DON)

DON is the core framework of Chainlink as a decentralized oracle. As the name of it indicates, DON is a network of oracles, receiving data from an open network of data providers, aggregating the data into a relatively trustworthy result, and returning them to the users. Furthermore, DON also functions as a key component of the transaction execution mechanism (TEF) mentioned later.

DON mainly consists of executables, adaptors, and storage. Executables are algorithms that run predetermined algorithms including data aggregation. An executable consists of*logic* and *initiator*.*Logic* is the deterministic algorithm that executes data aggregation, (for example, calculating the median of a given set of data received), while *initiator* triggers the logic under certain determined circumstances. Meanwhile, adaptors define methods and APIs transiting data from outside data providers such as web servers or external storage to the DON. Storage of DON keeps data in the network, and it could be an external cloud or decentralized storage [18].

b: TRANSACTION EXECUTION FRAMEWORK (TEF)

Chainlink not only aims at providing trustworthy data but also proposes its own vision on the architecture for on-chain transactions, *hybrid smart contracts*, by converting a smart contract into a *Hybrid Contract* with a DON logic off the main chain and an anchor contract on the main chain. The DON logic receives the transactions of users and executes them in the DON. Such an approach is designed to be faster than a pure main-chain transaction execution since it natively accesses oracle data in the DON. The transaction executed by it will be periodically updated to the main chain. Meanwhile, the anchor contract has higher trustworthiness than the DON logic since it is immutable on the main chain. Therefore, the anchor point contract is used for asset custody, syncing verification, and as a guard rail of the DON logic [18].

Furthermore, Chainlink proposed *Fair Sequencing Services* (FSS) to cooperate with its TEF, which aims at achieving the goal of*order-fairness for transactions*. With FSS, the sequence of transactions put on-chain will no longer be determined by economic incentives, for example, gas fees for the miners, but by pre-designed deterministic algorithms designed to maximize the system efficiency. It is believed via this design Miner Extractable Value (MEV) can be reduced and a more effective transaction processing mechanism can be achieved.

3) DATA VALIDATION PROCESS

In DON, data is mainly validated and processed by *executables*' core component, *logic*, which is programable to integrate data obtained in data-requester-desired ways. For example, with data sent from multiple nodes (namely individual oracles) to the DON, the logic of the executable can take the median of the data obtained to cancel out the overly high or low data, which is likely to be malicious, and return the relatively accurate final result (the median) to users. The flowchart of Chainlink data processing is shown in Figure 7.

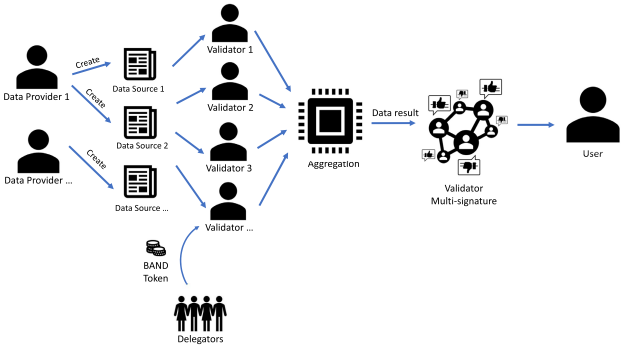


FIGURE 8. Flowchart of band protocol data processing.

4) INCENTIVIZATION MECHANISM

If data is requested from a DON node, the data-providing nodes can charge a certain amount of LINK token as the gas fee. Therefore, for data requesters, the more nodes used as data providers, the more costly it is to aggregate the data due to the gas fee but the higher the reliability of the data received. Furthermore, Chainlink oracle rates the performance of data providers with a quality evaluation (namely the nodes of DON), which can be regarded as a reputation system with evaluation criteria including *Total Transactions*, *Total Link Earned*, *Response Ratio*, *All Time Average Response (Blocks)* and so on [19]. The higher the reputation ranking of a node is, the more likely users to request data from it, which therefore motivates data-providing nodes to act honestly and efficiently.

However, the system merely provides users with quantified performance indexes of data providers (as mentioned in the previous paragraph) and gives no further restriction to filter or distinguish among data providers by different performances. Such filtering can only rely on the judgment of data requesters based on reading the performance indexes. Therefore, although with reputation ranking among data providers, in this paper, Chainlink is not regarded as a typical reputation-based data processing oracle but an aggregating-based data processing oracle.

5) APPLICATIONS AND ECOSYSTEM

Currently, Chainlink is one of the largest decentralized oracles with applications in DeFi projects including lending (such as Aave and dYdX), synthetic assets (Synthetix), and decentralized exchange (Pancakeswap), etc. as introduced on its official website. The market capitalization of LINK tokens reached more than 12 billion USD by the time of writing.

B. BAND PROTOCOL ORACLES [20]

Band protocol oracle is a staking-based decentralized oracle. It has certain similarities with Chainlink oracle on data

aggregation procedure but also differences in the incentivization mechanism (namely the staking-based data processing).

1) DESIGN CRITERIA

According to the whitepaper of Band protocol [20], the goals of Band protocol includes *speed and scalability* (being able to process large amount and high throughput data), *cross-chain compatibility* (achieving a blockchain-agnostic system with zero-trust and high-efficiency data verification) and *data flexibility* (building a permissionless and open system that is compatible with future changes and new data aggregation methods).

2) SYSTEM ARCHITECTURE

Users can participate in the network in 3 roles: data providers, validators, and delegators. A data provider can be any user that creates a "data source" (a data fetching script from a predetermined source) on the BandChain. A validator mainly contributes by proposing and putting new blocks onto the chain and responding to data requests from oracle clients by obtaining data from data sources. A delegator does not commit to data on chaining but stakes their tokens to the validators to receive commissions from them. With this delegation mechanism, BAND Protocol is a Delegation Proof-of-Stake system (DPoS).

Band protocol allows users to interact with the oracle through a Cosmos' *Inter-Blockchain-Communication* (IBC) protocol, therefore enabling other IBC-compatible blockchains for the oracle.

3) DATA VALIDATION PROCESS

In a data feeding process, after the clients request data, validators obtain data from data sources and on-chain the data to the system for aggregation. The data from data sources is therefore aggregated by the system.

After the aggregation result is obtained, it will be verified by validators on new blocks. Like most Cosmos blockchains, a new block is validated through multi-signature, and therefore new price data is produced. The flowchart of Band Protocol is shown in Figure 8.

4) INCENTIVIZATION MECHANISM

Band Protocol has its native token, BAND token, with a 7% - 20% inflation rate each year, allowing the users to participate in governance and to obtain reward fees for processing transactions.

In order to become validators, users need to stake their BAND at the oracle, and the probability of being selected as validators is proportional to the amount of BAND staked. A validator gets rewards in BAND for performing tasks including provisioning data for new blocks of the chain and processing transactions. Validators may be slashed (meaning stake being fined by the system) due to adversarial actions including participating in too few block proposals and commits, double signing, or unresponsiveness for data requests. For delegators, they are incentivized to stake BAND tokens to obtain rewards. For data providers, they are able to participate as *Premium Data Provider* to receive rewards for creating data sources.

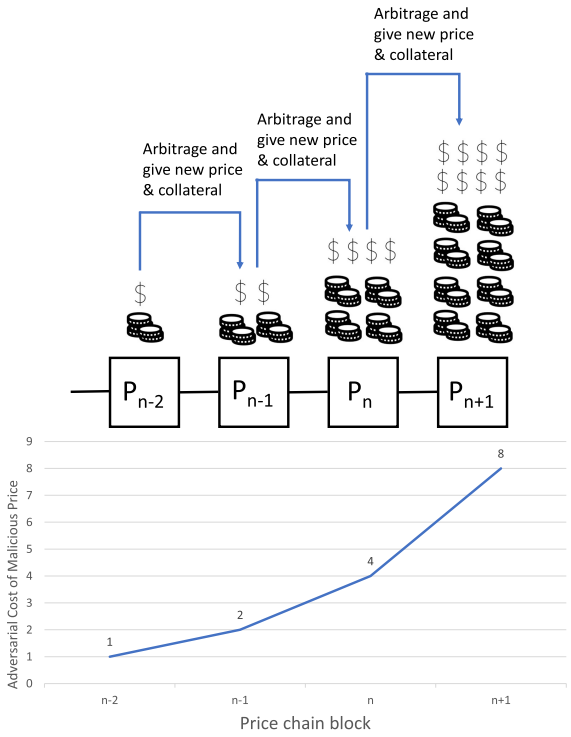


FIGURE 9. Price chain and collateral of NEST protocol.

5) APPLICATIONS AND ECOSYSTEM

According to the official website of Band Protocol, it has been partnered with DeFi projects including Terra, Mirror Protocol, etc. It also supports various DeFi exchanges, including Binance, Uniswap, Coinbase, etc. The native BAND token of the oracle has reached a market capitalization of 340 million USD by the time of writing.

C. NEST PROTOCOL

NEST Protocol is a game-theory-based data processing oracle, which aims at economically disincentivizing users from malicious behavior. Compared to staking-based processing, its incentivization process only exists during the process of data providing and does not require pre-existing regular staking from participants in the system or slashing after data is provided, and any user can join the process without prerequisites.

1) DESIGN CRITERIA

NEST Protocol points out in its whitepaper [21] 5 key criteria to judge oracle data quality, which are accuracy, price sensitivity (following changing data on time), attack resistance (high attacking cost), direct verification (data verifiable by any third party) and distributed quotation system (no requirement on the user side and users are free to join and leave without malicious impact to the system).

2) SYSTEM ARCHITECTURE & DATA VALIDATION PROCESS

NEST Protocol has a core mechanism of*Quote Mining Process*, a decentralized incentive solution for price reporting.

The quote mining process of the Oracle Quote mechanism enables users to report new exchange prices between 2 DeFi tokens and correct unreasonable prices (as shown in Figure 9). The process has the following steps:

1. Any participant can pass an exchange price between 2 assets to the quotation contract, meanwhile collateralizing a certain amount of both the 2 assets to the system at the same proportion as the exchange price just reported.

2. After step 1., the system will observe the price for T0 time, which is 25 blocks (around 5 minutes). During this period, anyone is able to liquify a part or all the collateralized assets at the reported price if it is believed that arbitrage is possible compared to the market price. This means any unreasonable price can be arbitraged by later upcoming users. If during the T0 period, all of the collaterals are liquified by other users, and the total collateral left untouched is zero, the price will be considered invalid; and vice versa if some transactions happen and part or none of the assets collateralized are liquified, the price is considered valid and the amount of collateral is remaining value left not liquified during T0 period.

3. The users who arbitrage at the price during T0 have to report a new price to the system and stake collateralized assets, which have to be beta times the amount they traded in order to arbitrage. Currently, beta is at the value of 2, which means the adversarial cost doubles at each new price and increases geometrically.

4. The new price is reported, and new assets are collateralized. Such processes form a chain, namely the price chain.

3) INCENTIVIZATION MECHANISM

For a miner (namely who proposes new blocks in the price chain), the cost of mining a price block on the chain is 1% of the quoted ETH scale and the gas fee as a reward NEST token will be issued to miners who successfully on-chains a price chain block. The total amount of NEST tokens released has an upper bound of 10 billion, which will be 400 NEST per block at the beginning and decrease to 80% of the last period every 2.4 million blocks (around 1 year), and after the block reward is reduced to 40 NEST per block, it will no longer decrease.

4) APPLICATIONS AND ECOSYSTEM

NEST Protocol currently has partnerships with exchanges including CoFix, crypto.com, iNFT, etc. according to its official website. The market capitalization of its native token NEST has reached 25 million USD by the time of writing.

D. DOS NETWORK

DOS Network is a reputation-based oracle, which decides the chance of participation of a user with a reputation score mechanism. Different from Nest Protocol mentioned above, reputation-based oracle does not only give an immediate penalty to malicious users (collateral liquified) but also a long-term penalty of having less chances of participation in the system.

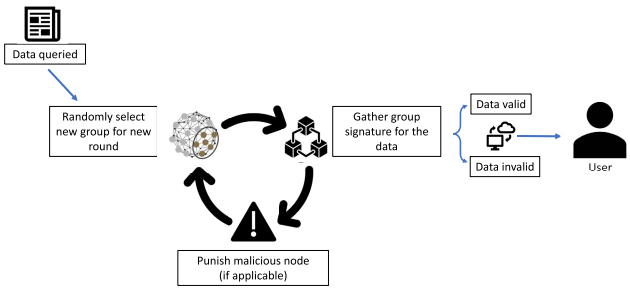


FIGURE 10. DOS network working flowchart.

1) DESIGN CRITERIA

According to the Whitepaper, DOS Network offers mainly 2 aspects of service, which are decentralized data feeding (by providing connection among on-chain and off-chain data) and decentralized verifiable computation (by providing computation power to blockchains). Based on these services, DOS Network enables chain-agnostic oracle and DApp construction.

2) SYSTEM ARCHITECTURE

The Decentralized Oracle Service (DOS) Network is a reputation-based network based on layer-2 protocols, providing services including decentralized data feeding and decentralized verifiable computation oracles.

Its design mainly consists of 2 parts, the on-chain part, and the off-chain part of the oracle. The on-chain part of the oracle includes a proxy system and on-chain governance system (consisting of subsystems of monitoring, registration, and payment). The proxy system is an interface for the user to interact with on-chain user contracts, and the governance system mainly provides services including recording the Quality of Service (QoS) of DOS nodes (namely monitoring), registering new joining DOS nodes, and processing payment rewarded to the DOS Network nodes runners.

The off-chain part of its design mainly guarantees the validity of the data provided by the network nodes, which is based on 2 techniques, the Verifiable Random Function (VRF) and the threshold signature scheme, and together they support a Byzantine Fault Tolerance (BFT) data feeding system of DOS Network.

3) DATA VALIDATION PROCESS

DOS nodes need to deposit certain *security reserves* as collaterals in the system, and during data feeding, they are randomly divided into groups by the VRF, and a group is randomly selected to perform computation or to execute a configured script such as responding to data requests. Within

the group, nodes can reach an in-group BFT consensus as long as the number of non-adversarial nodes is above a threshold (i.e. "t-out-of-n"). The malicious nodes, if not responding or providing invalid data, will be excluded from future runs of the protocol, and their security reserve will be slashed.

Each group has a quality score as a measure of their Quality of Service (in the terms of criteria such as correctness and responsiveness), and for non-responding groups, their negative score will be incremented until their score is abnormal enough to be banished from the protocol. Furthermore, for a node with overly low QoS, it will be excluded from the off-chain protocol and payment process. The flowchart of the DOS Network is shown in Figure 10.

Therefore, a reputation-based data validation process is constructed with this QoS system.

4) INCENTIVIZATION MECHANISM

DOS Network has its native token, DOS Tokens, used to incentivize participants of the system, including DApp developers (for submitting development proposals), mining node runners, and premium data providers (those who monetize data feeding in the system). Nodes who on-chain a new block obtain rewards, while users can also obtain rewards from staking. If the user conducts adversarial actions, the penalty is being excluded from future participation in the system. Such a mechanism incentivizes honest actions.

5) APPLICATIONS AND ECOSYSTEM

DOS Network currently has strategic partners including mining pools (Huobi Pool), lending platform (ForTube), blockchain infrastructure (Meter), etc. according to its official website. The market capitalization of its native token DOS has reached 40 million USD by the time of writing.

E. WITNET ORACLE

Witnet Oracle is a reputation-based oracle. Compared to DOS Network, its difference lies in the reputation score system that the total reputation score of the system is constant, and the increase in the reputation score of some users can only mean a decrease in reputation score of others.

1) DESIGN CRITERIA

Witnet Oracle gives data reporters reputation points based on their performance of data provision. The system was designed to conduct tasks of *Retrieve-Attest-Deliver*, to provide trustworthy data to clients.

2) SYSTEM ARCHITECTURE

In Witnet Oracle, users are divided into 3 types: clients, witnesses, and bridges. Clients are users who request certain data provisions, witnesses work as data reporters, and bridges work as interconnections between the Witnet oracles and other public smart contract platforms. Witnet's data processing system is based on its *Decentralized Oracle Network* (DON).

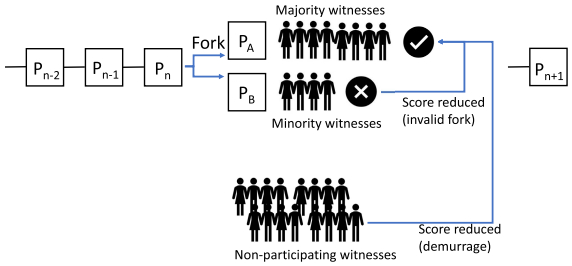


FIGURE 11. Witnet oracle working flowchart.

In Witnet, prices are produced in the form of giving mining blocks on the price chain. If at a block there exist dispute among witnesses, the price chain will fork and proceed to the dispute solving by choosing the fork with majority reputation support as the valid result.

3) DATA VALIDATION PROCESS & INCENTIVIZATION MECHANISM

Witnet incentivizes users with reputation scores and its native token Wit. Miner publishing a new block can obtain block reward in the form of Wit token, which is inflationary to provide long-run incentive. Meanwhile, the likelihood of successfully mining a new block is related to the reputation score he gets. Namely the higher the reputation score he gets, the more likely he is to get tasks, where such task returns payoffs to the witnesses.

Each witness (represented by a public key in the system) has a minimum reputation score, and at checkpoint 0 (the genesis block) of the ledger, the minimum score is set to be 1. Considering that the public key has a length of 256 bits, there exist 2^{256} initial scores to be distributed among the witness identities (public keys). In addition to the basic 1 point, another x times 2^{256} points are used for further re-distribution among the witnesses. Namely, a witness starts with a reputation score of x+1 [22]. If a witness loses all of his re-distributable points, he still has the minimum 1 score which is never reduced from him. In the system, reputation flows from witnesses with worse reputations to those with higher reputations. Therefore, the gain in the reputation score of a witness only comes from the reduction of the scores of other witnesses.

If a controversy on data happened among witnesses, forking will happen on the price chain (meaning the chain grow into more than one branch temporarily), and witnesses anchor their reputation onto different forks of the chain. Under this situation, the reputation score is directly deciding the voting power of a witness. Eventually, the data fork receiving the support of the majority of voting power eventually becomes valid and survives as the final result, while other forks became invalid and are discarded. For a witness who supports an invalid fork, his reputation score will be reduced. The reputation scores reduced will transfer from dishonest witnesses to honest ones, with total reputation score amount to be constant. The flowchart of Witnet oracle is shown in Figure 11.

In addition, for a witness that does not participate in the data validation process (namely not anchoring his score to any of the data outcomes), his score will still be reduced by a demurrage process, and the more scores he has the faster his score reduces due to absence from responsiveness. Therefore, a witness is incentivized to join the price reporting process.

Furthermore, Witnet system gives a so-called ''Double-agent Incentive'' to the witnesses, meaning in the system witnesses do not reveal which claim of data they support. This means that even though potential bribers may provide economic incentives to witnesses, the witnesses can still choose to behave honestly to the DON and obtain both the reward from the system and the bribers.

In this case, it is important to find the optimized balance between the dishonesty penalty and the demurrage. If the former is too low, the quality of data provided cannot be guaranteed due to low adversarial cost; if the latter is too low, the witnesses may tend to not participate in the price reporting process to avoid the risk of supporting the wrong forks, causing the operation of the system inefficient. Therefore, a balance is required so that the witnesses are incentivized to report data to the client honestly under such mechanisms.

4) APPLICATIONS AND ECOSYSTEM

According to its official website, Witnet's ecosystem mainly includes other related infrastructure developed by Witnet, including wallet (Sheikah wallet) and block explorer (witnet.network). Currently, the native token of Witnet, WIT, is not active in DeFi market.

F. COMPARISONS: SIMILARITIES AND DIFFERENCES

In previous sections of this paper, decentralized oracle designs are categorized into 4 types by data validation mechanisms and their active cases are studied. It can be concluded that the generation trustworthiness is based on 2 basic conditions: Con.1) non-adversarial majority; Con.2) benefit of adversarial acts smaller than the that of honest acts.

The aggregation-based data processing mainly relies on Con.1 and barely relies on Con.2, since it merely aggregates the data received in a node- and data-quality-agnostic way with pre-determined algorithms.

The staking-based processing also mainly relies on Con.1 but compared to the aggregation-based ones it has a higher reliance on Con.2 since it provides an economic incentive to voters by staking, rewarding, and slashing. The higher the staking, the less likely the malicious action.

The game-theory-based processing mainly relies on Con.2 rather than Con.1. It barely relies on a higher proportion of non-adversarial users against adversarial ones. Thus, it is able to work in environments with more malicious users.

Reputation-based processing relies on both Con.1 and Con.2 since a reputation system incentives honest users with future participation opportunities and meanwhile decides the reputation of a user with a judgment based on the majority users' performance.

For various oracle designs, their suitable circumstances of applications depend on the feature of their condition of trustworthiness. We can also draw a conclusion that, Chainlink mainly relies on Con.1, NEST Protocol mainly relies on Con.2, and Band Protocol, DOS Network and Witnet rely on both Con.1 and Con.2.

With respect to the scalability of the data processing nodes, current active oracles have different characteristics. For Chainlink, users need to use adaptors of Chainlink and fulfill hardware requirements to become a data feeding node. For Band Protocol, to become a data provider, a Data Provider's Account and a ''gateway server'' are required to be set up. To become a validator, staking is required on the system. For DOS Network, users are also required to stake to become data validators, while for NEST and Witnet, any user is able to join the data validation process as long as they are in the network. The comparison above is summarized to Table 2.

Furthermore, it cannot be ignored that a new data validation mechanism may show up in the future. For example, Uniswap, as a decentralized exchange, has the potential of being converted into an oracle with its current infrastructure, according to Vitalik Buterin [23]. With the advantage of large market capitalization, Uniswap has the potential to increase the adversarial cost of attackers.

Although with the data processing and validation mechanism mentioned above, current oracles are not solving the oracle problem perfectly and are experiencing some shortcomings. For example, inaccuracy of price data feeding may cause huge loss for DeFi platforms and users; data feeding may not be on time; data type requested by users may not be accessible by the oracle or the platform due to compatibility issues; DeFi attacks by manipulating oracles are frequently heard, etc. The problems DeFi oracles are facing give us insight into their potential development of them in the future, which is going to be mentioned in the next section.

V. FUTURE OF DeFi ORACLES

With past and present DeFi oracles analyzed and compared, in this section, we give out our view on the future of trustworthy DeFi oracles, including the metrics of DeFi oracles and the potential trustworthiness mechanism for data feeding and data providers.

A. METRICS FOR BUILDING TRUSTWORTHY DeFi ORACLES

Current DeFi oracles have disadvantages in the application to the industry, as [7] pointed out, oracle problems may encounter malfunctions, biased data, and lack of timeliness of data feeding, which points to some possible future direction of improvement. In this paper, we propose some possible improvement metrics or criteria of oracles, which include accuracy, time-efficiency, scalability, and adversarial cost (risks). (shown in Figure 12)

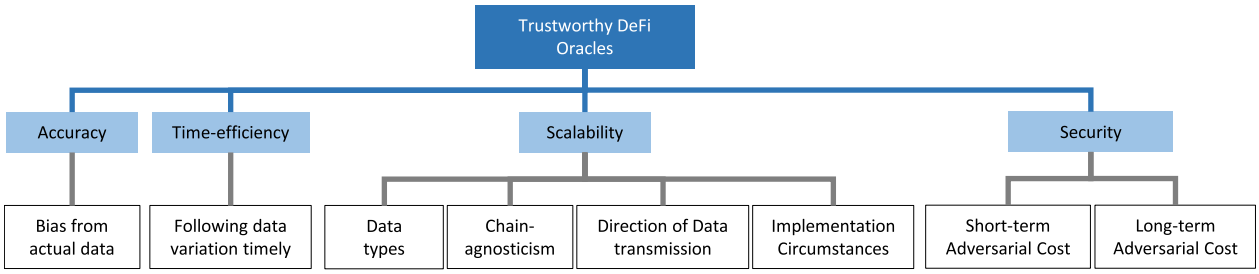


FIGURE 12. Design metrics for DeFi oracles.

TABLE 2. Comparison between real examples of decentralized oracles.

	Trust model	Trustworthiness Source	Data Provider Scalability	Native Token
Chainlink	Aggregation	Non-adversarial majority	Adaptor & Hardware requirement	LINK
Band Protocol	Staking & Aggregation	Non-adversarial majority & high adversarial cost	Data Provider: data source account and infrastructure setup; Validator: staking	BAND
Nest Protocol	Game-theory	High adversarial cost	Any user can participate with low barrier	NEST
DOS Network	Reputation	Non-adversarial majority & high adversarial cost	Staking	DOS
Witnet	Reputation	Non-adversarial majority & high adversarial cost	Any user can join as a witness	WIT

1) ACCURACY

Accuracy means that the variance between data fed by the oracle and actual data is held within an acceptable threshold. The variance may be caused by the fluctuation of price or the difference among various data sources or trading platforms. In the highly volatile DeFi market, a small proportion of price change may cause a relatively large fluctuation of DeFi asset value.

Currently, DeFi oracles have limited accuracy. For example, Chainlink updates the price when a deviation threshold of the price is surpassed. Within the deviation threshold, the price with certain inaccuracy may still cause loss of the users. Therefore, oracles have to take accuracy as one important criterion.

2) TIME EFFICIENCY

Time efficiency measures the timeliness of data fed to users when receiving data requests. With changing data sources, whether oracles can update the data on time is an important factor of data feeding quality in a fast-fluctuating DeFi market.

Furthermore, in the future, the balance between accuracy and time-efficiency of oracles will be given higher importance. Currently, higher accuracy usually requires more time spent on data validation, and less data processed in a limited time period, while in contrast time efficiency may require less data validation time.

3) SCALABILITY

Scalability means that oracles are able to integrate and adapt to more data types and chains and has more flexibility in service functionalities. With a higher scalability, users may receive and transmit data in more circumstances and environments, expanding the market and user groups of DeFi.

Currently, we can see such a trend in the 3rd generation blockchains such as the Polkadot chain, which enables chain-agnostic data transmission [24]. It is seen that emerging outbound oracles (also known as reverse oracles) are bringing new applications of data transmission in the direction of on-chain to off-chain, in contrast to traditional oracles. For example, Parsiq [25] is nowadays one of the examples of applications of outbound oracles, providing services including on-chain wallet supervision and management. With these trends, DeFi oracles are being applied to more circumstances, with more types of DeFi projects and ecosystems, and even an integration with traditional centralized finance.

4) SECURITY

For an oracle, the degree of security is reflected by the cost of adversarial users conducting malicious actions and attacks, which is an important factor to improve the reliability of oracles since it is directly related to the probability of attacks.

Adversarial costs can be divided into short-term and long-term ones. Although now traditional oracles including Chainlink and Band Protocol are dominating the market with short-term cost mechanisms (such as the cost of 51% attack

and stake slashing), we can see new designs coming up with a more long-term way to raise adversarial costs. For example, reputation-based oracles have outstanding potential from this aspect by depriving the long-term/future chance of participation of malicious users on the reputation system.

B. PROPOSED TRUST ARCHITECTURE FOR FUTURE TRUSTWORTHY DeFi ORACLES

With potential improvement on the metrics of DeFi oracles mentioned above, oracles will not only generate trustworthiness more efficiently but also make trust evaluation more universal and general in DeFi industry. It is possible for a user to possess certain universal reputation proof among different blockchains and DeFi platforms, supported by a general trust evaluation system. (flowchart for demonstration as shown in Figure 13)

1) ON THE TRUSTWORTHINESS OF DATA FEEDING

With metrics mentioned above for DeFi oracles, data feeding is challenged with higher standards. Currently, DeFi oracles mainly rely on user groups' general behavior to decide the trustworthiness of data, which may not be an optimal approach with respect to time efficiency and operational cost. To make sure user groups act honestly rather than adversarial, economic incentives need to be provided. Therefore, it is natural to think of a potential trust model, where trust evaluation is not based on human judgment but automatically.

a: AUTOMATED TRUST MODELLING

An automated algorithm for trustworthiness is one of the possible future development directions, where trust modeling based on algorithms is the key factor for trustworthiness evaluation. In [26], Lim et al categorized trust models into 4 basic categories, including basic models, graph methods, Bayesian methods, machine learning methods, etc. If applied to DeFi, such trust modeling is automatable by algorithms (with smart contracts in DeFi), therefore automating the trust evaluation on data feeding, rather than evaluating the reputation of users based on the judgment of the majority users.

b: MACHINE LEARNING IN DATA VALIDATION

Data validation is the process of determining the trustworthiness of data and one of the promising approaches of automated trust modeling is the machine learning approach. Such machine learning models can be trained by historical data from DeFi trading platforms, etc. Compared to the approach supported by user group behavior, the machine learning approach is able to process a much larger amount of data than user committees do. Furthermore, the machine learning trust model is relatively more scalable and migratable to other systems with data set or environment fed to the model. In contrast, human users conventionally tend to process certain data types or certain platforms. With respect to user cost, a machine-based trust model does not require an economic incentive to make a non-adversarial decision which lowers the system operating cost and makes the system less corruptible.

The data used for the machine learning trust model is accessible through DeFi transaction records. Such records contain information including user addresses, transaction platforms, and transaction amounts, which are completely traceable due to the nature of blockchain. The information can be used as input data for trustworthiness classification.

Furthermore, trust modeling can be regarded as a prediction problem on a social network, which is represented by a graph consisting of nodes (users) and edges (trust value). On such a graph, transactions are information that propagating along the graph edges. Therefore, a graphical neural network model has the potential of conducting trust modeling among users.

2) ON TRUSTWORTHINESS OF DATA PROVIDERS

In addition to the trustworthiness of data itself mentioned in the previous section, the trust modeling of data providers is also of importance. Reputation-based oracle has a certain advantage over other oracles in this aspect. It is a more direct and essential solution to the problem and will be further discussed in this session.

a: REPUTATION-BASED ORACLES: LIMITATION AND ADVANTAGE

On one hand, current reputation-based oracles have certain limitations. As section E-1 of [2] pointed out, a reputation-based data validation system may be less cost-effective due to the fact that users experience the opportunity cost of not obtaining benefits from adversarial behavior. Therefore, they need extra incentives in order to overcome the opportunity cost, which makes the system less cost-effective.

On the other hand, reputation-based oracles' advantages include but are not limited to i) High barrier for an adversarial user to participate in the system. A reputation system usually limits the chance for low-reputation users to participate in the data feeding process. Furthermore, it requires much more effort to gain more reputation than losing it, which is also known as a property of trust, *easier to lose than to gain*. ii) Filtering out malicious data from the system. By rejecting data provided from low-reputation users, malicious data cannot enter the data set provided. In contrast, in oracles based on other data validation mechanisms, adversarial users can still participate in data processing but only with their impact restricted or disincentivized, leaving higher potential threats to the system. iii) Introducing reputation and trust into the system is likely to meet future trends of development. With more integration with traditional finance and the physical world, more stable investment and trading environment is demanded, especially with concepts introduced from CeFi, including KYC (Know Your Costumer), AML (Anti-Money Laundering), CFT (Combatting Financial Terrorism), etc. A reputation and trust system is able to fill the gap between the traditional centralized and on-chain world.

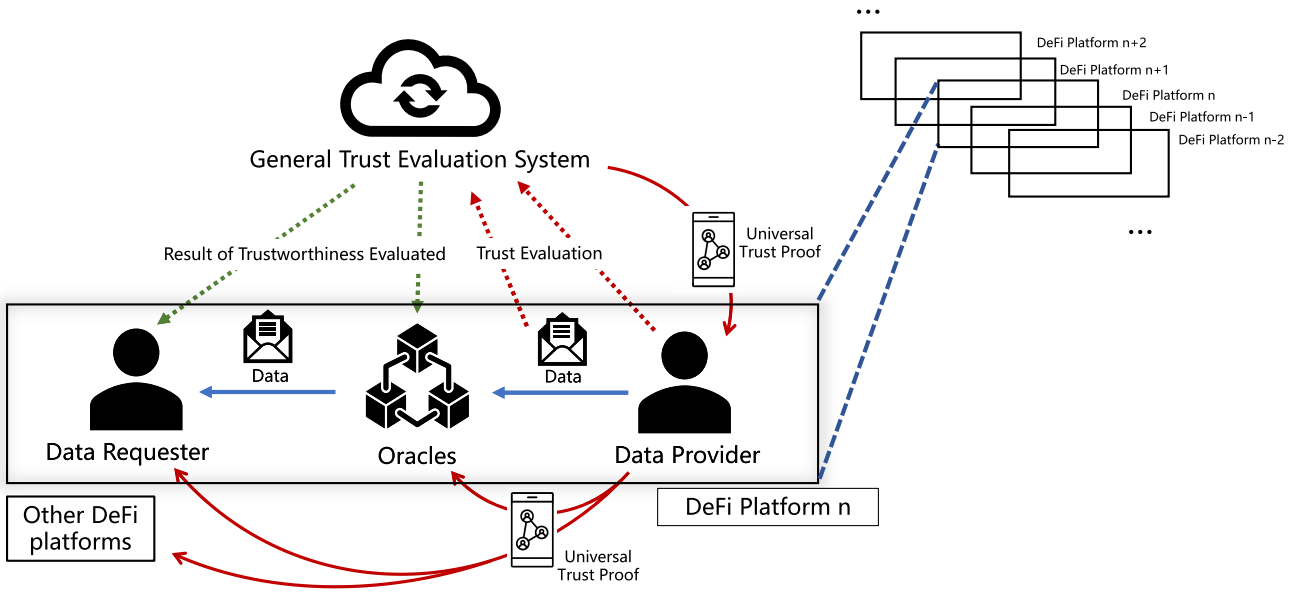


FIGURE 13. Blueprint for future DeFi oracles.

b: LESS HUMAN EFFORT IN REPUTATION EVALUATION

As mentioned in previous sections of trust on data feeding, one direction of future development is conducting user reputation evaluation with fewer human factors and a higher degree of automation. Currently, the trust in data by reputation-based oracles is based-on its provider's reputation, which is evaluated by the general behavior of a user group, for example, Witnet choose the data chain fork with the majority witnesses' voting power's support as the valid data and DOS gives negative QoS score if the data provided deviates from the majorities'.

Such reputation evaluation mentioned above a process has limited effectiveness. On one hand, it always has basic condition requirements on the general user group, for example, that the proportion of adversarial users does not exceed a certain threshold (50% in the case of Witnet) so that the system can always return valid answers. On the other hand, the quality of data does not fully depend only on the reputation of its provider. Therefore, it is reasonable to reduce the reliance on human behavior and introduce more factors that can be observed by automated algorithms to determine the trustworthiness of data, for example, the time distance of the data being published from the present time, the response speed, and rate of the user, etc.

3) GENERAL TRUST EVALUATION SYSTEM

In this paper, we predict that in the future trust evaluation has the potential for universal generalization. It may no more be limited to one specific chain or DeFi project due to the demand for transactions and user migration among different chains and platforms. Such an evaluation system may be supported by specialized oracles and smart contracts obtaining related data so that trust evaluation can be conducted by automated trust models.

Trustworthiness can be evaluated during the transmission from data providers (including APIs, humans, smart contracts, etc.) to requesters (smart contracts, human users, etc.) on both the data itself and the provider of it.

4) UNIVERSAL REPUTATION PROOF

With a generalized trust evaluation system mentioned above, it is likely that users or other data sources may possess a certain universal proof of their reputation. Such proof may help data receivers validate the data fed to them, especially for DeFi projects without a trust evaluation system of their own. Such universal proof is able to prevent users from conducting malicious actions as a "new user" in a different DeFi platform without receiving a penalty. For example, it is possible to represent the reputation of a user with an NFT (non-fungible token), which is unique as a single proof among the users, enabling reputation evaluation universally.

It is possible that such reputation proof is not limited to the DeFi world. For a DeFi project that is related to real-world assets, for example, synthetic assets or housing, reputation proof may be linked to the real-world identity with no requirement for knowledge publicized to the blockchain network. Such features may contribute to the combination between DeFi and traditional centralized finance.

VI. CONCLUSION

In recent years, decentralized finance (DeFi) has appeared as a rapidly developing field, where oracles provided viable solutions and promising applications. In this paper, the applications of oracles in DeFi have been introduced, including

DeFi lending, synthetic assets, and insurance. The past development of DeFi oracles has been introduced by categorizing them into aggregation-based, staking-based, game-theory-based, and reputation-based based on their data processing features. Furthermore, five current active oracles have been introduced with respect to their system architecture, data validation process and incentive mechanisms. A detailed comparison has been conducted among them according to the trust mechanism of the data and trustworthiness conditions. Lastly, metrics and possible future techniques development have been proposed, including the application of automation and machine learning, and a potential overall trust architecture has been given.

REFERENCES

[1] K. Mammadzada, "Blockchain oracles systematic literature review master thesis (20 ECTS)," Inst. Comput. Sci., Innov. Technol. Manage. Curriculum, Univ. Tartu, Tartu, Estonia, Tech. Rep., 2019. [Online]. Available: https://comserv.cs.ut.ee/home/files/Mammadzada_MasterThesis_ITM.pdf?study=ATILoputoo&reference=B913660BDAEE6C01D5D887A09A79331E898F990F and https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=67343&year=2019

[2] A. Egberts, "The oracle problem—An analysis of how blockchain oracles undermine the advantages of decentralized ledger systems," EBS Univ. Wirtschaft und Recht, Oestrich-Winkel, Germany, Tech. Rep., 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3382343

[3] A. Beniiche, "A study of blockchain oracles," 2020, *arXiv:2004.07140*.

[4] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy blockchain oracles: Review, comparison, and open research challenges," *IEEE Access*, vol. 8, pp. 85675–85685, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9086815

[5] R. Mhlberger, S. Bachhofner, E. C. Ferrer, C. D. Ciccio, I. Weber, M. Wöhrer, and U. Zdun, "Foundational oracle patterns: Connecting blockchain to the off-chain world," 2020, *arXiv:2007.14946*.

[6] J. Heiss, J. Eberhardt, and S. Tai, "From oracles to trustworthy data on-chaining systems," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 496–503. [Online]. Available: https://ieeexplore.ieee.org/document/8946220

[7] G. Caldarelli and J. Ellul, "The blockchain oracle problem in decentralized finance—A multivocal approach," *Appl. Sci.*, vol. 11, no. 16, p. 7572, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/16/7572/htm

[8] A. Pasdar, Z. Dong, and Y. C. Lee, "Blockchain oracle design patterns," 2021, *arXiv:2106.09349*.

[9] I. Homoliak, S. Venugopalan, Q. Hum, D. Reijsbergen, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Towards a standardized model for studying vulnerabilities, threats, and defenses," 2019, *arXiv:1910.09775*.

[10] M. Kumar, N. Nikhil, and R. Singh, "Decentralising finance using decentralised blockchain oracles," in *Proc. Int. Conf. Emerg. Technol. (INCET)*, 2020, pp. 1–4, doi: 10.1109/INCET49848.2020.9154123.

[11] B. Liu, P. Szalachowski, and J. Zhou, "A first look into DeFi oracles," 2020, *arXiv:2005.04377*.

[12] Synthetix. (2020). *Synthetix System Documentation, Litepaper*. [Online]. Available: https://docs.synthetix.io/litepaper

[13] Provable. *Documentation of Provable, Official Website of Provable*. Accessed: Dec. 15, 2021. [Online]. Available: https://docs.provable.xyz/

[14] Tellor. *Whitepaper, How Tellor Works*. Accessed: Dec. 15, 2021. [Online]. Available: https://docs.tellor.io/tellor/whitepaper/tellor-oracle-overview/overview

[15] NEST Protocol. *Nest Protocol: A Distributed Price Oracle Network*. Accessed: Dec. 15, 2021. [Online]. Available: https://docs.tellor.io/tellor/whitepaper/tellor-oracle-overview/overview

[16] DOS Network. (2019). *A Decentralized Oracle Service Boosting Blockchain Usability With Off-Chain Data & Verifiable Computing Power*. [Online]. Available: https://s3.amazonaws.com/whitepaper.dos/DOS+Network+Technical+Whitepaper.pdf

[17] A. S. de Pedro, D. Levi, and L. I. Cuende. (2017). *Witnet: A Decentralized Oracle Network Protocol*. [Online]. Available: https://neironix.io/documents/whitepaper/5141/witnet-whitepaper.pdf

[18] L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfara, A. Miller, B. Magauran, D. Moroz, S. Nazarov, A. Topliceanu, F. Tramèr, and F. Zhang. (2021). *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks*. [Online]. Available: https://research.chain.link/whitepaper-v2.pdf

[19] Chainlink Oracle Reputation. *Oracle Reputation*. Accessed: Dec. 15, 2021. [Online]. Available: https://reputation.link/

[20] Band Protocol. *Bandchain Whitepaper*. Accessed: Dec. 15, 2021. [Online]. Available: https://docs.bandchain.org/whitepaper/

[21] Nest Protocol. *Overview of Nest: Decentralized Price Oracle*. Accessed: Dec. 15, 2021. [Online]. Available: https://docs.nestprotocol.org/

[22] Witnet Verified GitHub Page. *Reputation Initialization in Witnet*. Accessed: Dec. 15, 2021. [Online]. Available: https://github.com/witnet/research/blob/master/reputation/docs/initialization.md#reputation-initialization-in-witnet

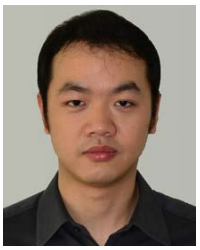
[23] Y. Khatri. (2021). *Uniswap's Uni Should Become an Oracle Token, Says Vitalik Buterin*. [Online]. Available: https://www.theblockcrypto.com/post/104597/uniswap-uni-oracle-token-vitalik-buterin

[24] G. Wood. *Polkadot: Vision for a Heterogeneous Multi-Chain Framework Draft 1*. Accessed: Dec. 15, 2021. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf

[25] Parsiq. *PARSIQ Official Website*. Accessed: Dec. 15, 2021. [Online]. Available: https://www.parsiq.net/en/

[26] H. L. J. Ting, X. Kang, T. Li, H. Wang, and C.-K. Chu, "On the trust and trust modeling for the future fully-connected digital world: A comprehensive study," *IEEE Access*, vol. 9, pp. 106743–106783, 2021.

YINJIE ZHAO (Student Member, IEEE) is currently pursuing the bachelor's degree in electrical and electronic engineering from Nanyang Technological University. He has interned at the Digital Identity and Trustworthiness Laboratory, Huawei Singapore for eight months, and studied on decentralized finance and trustworthy oracles. The paper was completed during the period of his internship at the Laboratory. His research interests include artificial intelligence and data science and intends to pursue further studies in this area.



XIN KANG (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from Xi'an Jiaotong University, China, in 2005, and the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2011. He was a Research Scientist at the Institute for Infocomm Research, A*STAR, Singapore, from 2011 to 2014. He joined as a Senior Researcher with the Shield Laboratory, Huawei Singapore Research Center, where he is the Principal Researcher with the Digital Identity and Trustworthiness Laboratory. He has published more than 40 journal articles on IEEE top journals, and more than ten of them are listed as SCI highly cited research papers. He has also published more than 30 conference papers on first-tier IEEE conferences. He received the Best 50 Papers Award from IEEE Global Communications Conference (GlobeCom), in 2014, and the Best Paper Award from IEEE International Conference on Communications (ICC), in 2017. After joining Huawei, he has filed 50+ patents on security and communication networks. He is also very active in standardization. He has contributed more than 30 technical proposals to 3GPP SA3 and 17 of his proposals have been accepted by 3GPP SA3. He is one of key contributors to the newly published ITU-T standard X.1365, and the Lead Editor for newly established work item X.ztd-iot. He is also one of the key contributors to Huawei 5G security white paper series. He has more than ten years of research experience and his research interests include trust modeling, machine learning, digital identity, blockchain, wireless communication, network security, and security protocol design.

TIEYAN LI (Member, IEEE) received the Ph.D. degree in computer science from National the University of Singapore.

He has more than 20 years experiences and is proficient in security design, architect, innovation and practical development. He was also active in academic security fields with tens of publications and patents. He is the Expert of security and applied cryptography, and a Technology Generalist of applications, systems and networks. He is currently the Leader of the Digital Trust Research with the Shield Laboratory, Singapore Research Center, Huawei Technologies, where he works on building the trust infrastructure for future digital world, and previously on mobile security, IoT security, and AI security. He is the Director of Trustworthy AI C-TMG and the Vice-Chairperson of ETSI ISG SAI. He has served as the PC members for many security conferences, and is an influential speaker in industrial security forums. His current research interests include trustworthy AI, trustworthy computing, trustworthy identity and future network infrastructure.

CHENG-KANG CHU (Member, IEEE) received the Ph.D. degree in computer science from National Chiao Tung University, Taiwan. He was a Research Scientist at the Cryptography and Security Department, Institute for Infocomm Research (I2R), Singapore. He is a Senior Researcher with Huawei International, Singapore. He had a long-term interest in the development of new technologies in applied cryptography, cloud computing security, and IoT security. His current research interests include mobile security, IoT security, and decentralized digital identity. He has published many research papers in major conferences and journals like PKC, CT-RSA, AsiaCCS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS (TPDS), and IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (TIFS). He received the Best Student Paper Award in ISC 2007. He was the Vice Chair of IEEE Consumer Communications and Networking Conference (CCNC), in 2012, and on the program committee of many international conferences.

HAIGUANG WANG (Senior Member, IEEE) received the bachelor's degree from Peking University, in 1996, and the Ph.D. degree in computer engineering from the National University of Singapore, in 2009. He was a Research Engineer/Scientist at the Institute for Infocomm Research, from 2001 to 2013, I2R Singapore, and doing research on communication and network protocol design, innovation and practical development. In 2013, he joined Huawei International, where he is doing research on security area. He is an Expert of communication network security and identity management and access control, and a Technology Generalist of systems, communications, and networks. He has published/filed more than 60 research papers and patents together. He is actively contributed to various standard including, IEEE 802.11, 3GPP SA3 and ITU-T SG-17, and IETF. He is currently doing research on digital identity and trust management, security automation, and network infrastructure security for future digital world, and previously on 5G communication network security.