Decentralized Oracle Network
Powered by
XinFin Blockchain Network

Build on XinFin (XDC) Blockchain Network as an open source initiative

Table of Contents

1. Disclaimer

The purpose of this document is to present information about the Decentralized Oracle Network Powered by XinFin Blockchain Network. The information set forth above may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information on whether to undertake a thorough analysis of the project to be used for various smart contracts.

Whilst every effort is made to ensure that statements of facts made in this document are accurate, all estimates, projections, forecasts, prospects, expressions of opinion, and other subjective judgments contained in this paper are based on assumptions considered to be reasonable as of the date of the document in which they are contained and must not be construed as a representation that the matters referred to therein will occur. Any plans, projections, or forecasts mentioned in this paper may not be achieved due to multiple risk factors. No information in this Whitepaper should be considered to be business, legal, financial, or tax advice. We suggest that you do your own research and consult your own legal, financial, tax, or other professional advisers about Decentralized Oracle Network respective businesses and operations.

This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or make a binding legal commitment.

No regulatory authority has examined or approved any of the information set out in this Whitepaper. No such action has been or will be taken under the laws, regulatory requirements, or rules of any jurisdiction. The publication, distribution, or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements, or rules have been complied with.
This whitepaper is subject to change as the product progression and development advances. Changes will be reflected in future updated/revised whitepaper versions.

2.   Market Opportunity

Background

Evolution of Decentralized Ledger Technology is disrupting many legacy based businesses and functionalities around the world including finance. The emergence of Blockchain, a form of distributed ledger technology where transactions are duplicated and saved onto a large number of nodes. Transactions are defined as a set of data packages for storing monetary value, parameters, and function call results, and their integrity is ensured by cryptographic techniques. They are collected in the form of blocks where there are immutable records, and each block is linked to the succeeding block through the hash. Blocks are appended to the ledger by means of consensus algorithms such as Proof of Work (PoW). Introduction of smart contracts to the blockchain has further added programmability to the blockchain and revolutionized the software ecosystem leading toward development of decentralized applications (DApps) trustless Applications such as Decentralized lending (DeFi), stable currencies, prediction markets and synthetic assets are being researched and built on top of them.

But in order for DLT applications to work and to provide value to people and organizations around the world, they require a host of information from the non-blockchain data source viz. pricing data for derivatives or weather information for insurance contracts or, really, almost any critical data you can imagine. Without access to such accurate data, these applications would be of little or no use. This is where oracles play a critical role. Oracles primarily work as connective tissue for accessing, processing and transmitting critical data. Being on Blockchain ecosystem not any kind of oracle system will do. To ensure the integrity of the data, they must be fully decentralized.

As per our estimate, the market potential for such a fully decentralized oracle network is very high and it represents approximately USD 100 Billion.

3.   Challenges of Current Centralized System

Centralized Oracles like Decentralized Computing act as a single entity that provides critical data from an external source to a smart contract operating with a set of security features. Due to its architecture, such oracles are controlled by a single source which predominantly works as sole source of information for smart contracts. Since it works similarly to the traditional financial system where a single entity is responsible for everything, it suffers major limitations, or we can say it has a single point of failure. These oracles have a simple architecture with lesser investment in terms of infrastructure and maintenance. Although they provide protection against game theory attacks, these are still prone to vulnerabilities to being corrupted and attacked.

3.1   Data Reliability

Since in a centralized system, single entity is the solely responsible for data feeds, the data reliability will be highly in doubt. Malicious actors can easily login to systems and manipulate data, thus leading to compromised data.

3.2   Cyber Attacks

Malicious players can attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems in a centralized oracle network.

3.3   Blockchain Oracle Problems

The Blockchain Oracle Problems result from the inability of oracles to verify the integrity of their data. Additionally, the likelihood of malfunction and deliberate tampering varies by type. On the other hand, if the information is trusted and verified, the oracle may fail to function properly on the smart contract due to a malfunction or deliberate tampering. From a game-theoretic perspective, it can be demonstrated that the higher the value of the smart contract, the greater the incentive to compromise the system.

4.   What is Decentralized Oracle Network?

Decentralized Oracle Networks eliminate any single point of failure in a smart contract by utilizing multiple data inputs. This enables end-to-end reliability and allows high-value smart contracts in low trust environments to become viable, Decentralized Oracle Networks are designed to enhance and extend the capabilities of smart contracts on a target blockchain or main chain through functions that are not available natively. They do so by providing the three basic resources found in computing systems: networking, storage, and computation. A DON aims to offer these resources with strong confidentiality, integrity, and availability properties, as well as accountability.

DONs are formed by committees of oracle nodes that cooperate to fulfill a specific job or choose to establish a long-lived relationship in order to provide persistent services to clients. DONs are designed in a blockchain-agnostic way. They promise to serve as a powerful and flexible tool for application developers to create off-chain support for their smart contracts on any supported main chain.

Two types of functionalities realize the capabilities of a DON: executables and adapters. Executables are programs that run continuously and in a decentralized manner on the DON. While they do not directly store main-chain assets, they have important benefits, including high performance and the ability to perform confidential computation. Executables run autonomously on a DON and perform deterministic operations. They work in hand with adapters that link the DON to external resources and may be called by executables. Adapters, as we envision them for DONs, are a generalization of the external adapters in PLUGIN today. While existing adapters typically only fetch data from data sources, adapters may operate bidirectionally; in DONs, they may additionally leverage joint computation by DON nodes to achieve additional features, such as encrypting reports for privacy-preserving consumption by an executable.

5. PLUGIN

Decentralized Oracle Platform, provides cost effective solutions to any smart contract which runs on XinFin EcoSystem. PLUGIN is a fork of Chainlink open-source technology that is collectively developed by a large community of developers, researchers, and users who share the goal of building PLUGIN into a public good for the benefit of the XinFin blockchain ecosystem.

Through PLUGIN we enable smart contracts to speak to the outside world easily. Data that gets stored in smart contracts is trustable as we have strong collaboration with Data Feed partners.

PLUGIN is currently committed to DeFi Application which includes:

a. Stable currencies, also known as "Stablecoins"
b. Decentralized Insurance
c. Decentralized Prediction markets
d. Decentralized Synthetic assets
e. Decentralized exchanges and Derivatives Trading Market
f. Decentralized Identity

PLUGIN Decentralised Oracle Network comes with:

a. Highest Level of Security
b. Decentralize Architecture to Prevent Single Point Failure
c. Censorship resistance
d. Prevent Bad action from Performing malicious activities
e. Developer Friendly Interface for Ease of Deployment & Operation

5.1   Core Focus of PLUGIN Platform

Our core focus is to provide the cost effective solutions to the node operators and end users who will require the reliable data onto their blockchain through decentralized oracle service.

5.2   PLUGIN for Node Operators

The PLUGIN network is built on independent node operators, making it decentralized Oracle technology, unlike other Oracle designs that depend on a centralized entity as a gateway. The node operators are rewarded with the PLUGIN tokens for doing high-quality, honest work. PLUGIN nodes have job specifications registered with each node to execute jobs coordinated by the on-chain Oracle contracts.

5.3   PLUGIN for Customers

Majority of PLUGIN users relying on smart contracts make use of data feeds. These are reports on the current value of key pieces of data according to authoritative off-chain sources. For example, price feeds are feeds reporting the prices of assets—crypto-currencies, commodities, forex, indexes, equities, etc.—according to exchanges or data-aggregation services. Such feeds will help secure billions of dollars in on-chain value through their use in DeFi systems such as Aave and Synthetix. Other examples of PLUGIN data feeds include weather data for crop insurance and election data, inflation data, among a number of others.

5.4   PLUGIN Guarantees

- Thoroughly Tested Platform for Quality Assurance
- Dedicated support delivered directly by our engineers
- Enterprise-grade SLA up to 24/7
- Reliable data feed

6.   PLUGIN Features

6.1   Security

Security forms the most important aspect of PLUGIN EcoSystem, We are fully aware that security & system stability is the most important aspect that clients look at and our system is designed to be the equivalent of spreading an encrypted droplet of water in the vast ocean. All our nodes are safeguarded with a strong firewall.

6.2   Reliability

Oracles play an extremely important role in facilitating the full potential of smart contract utility. Without a reliable connection to real-world conditions, smart contracts are unable to effectively serve the real-world.   PLUGIN is a decentralized network of nodes that provide data and information from off-blockchain sources to on-blockchain smart contracts via oracles. This process, along with extra secure hardware, eliminates the reliability issues that might occur if using only a single centralized source.

6.3   Node Operators

Hardware requirements for Node operators are not heavy and they can start operating it with minimal infrastructure. With 2GB RAM & 20 GB storage, nodes can be deployed and they can start providing oracle services.

6.4   PLUGIN Initiators

External initiators allow jobs in a node to be initiated depending on some external condition. The ability to create and add external initiators to PLUGIN nodes enables blockchain agnostic cross-chain compatibility. To utilize this PLUGIN service on any other blockchain than Xinfin, then PLUGIN Initiators comes handy.

6.5   PLUGIN Adapters

Custom computations and complex business logics can be applied using PLUGIN Adapters. Bringing down the value through authorized API's is much easier through PLUGIN adapters.

6.6   Job

Job specifications, or specs, contain the sequential tasks that the node must perform to produce a final result. PLUGIN jobs are divided into 2 segments (PLUGIN Initiators & PLUGIN Adapters). Jobs must contain at least one of each.

7.   PLUGIN EcoSystem

7.1   Users

Users who want to utilize the data feed from our PLUGIN Ecosystem, have to purchase PLUGIN token in exchange of XDC or using FIAT money through the exchanges. Before they request the data or any value of asset from our data feed, the user has to fund the contract using the XinPay wallet.

7.2   Data Feed Providers

Core part of PLUGIN is "Data Feed Providers", PLUGIN strongly encourages the data feed providers to actively participate and constantly share trustable data. Malicious or false data is not entertained and it will be heavily punished through our "Carrot & Stick" approach. For good and trustable data, data feed providers will be consistently rewarded.

7.3   Blockchain

PLUGIN is built on top of Xinfin Blockchain and we continue to evolve and provide the services to other blockchain in future.

8.   PLUGIN Token

8.1   Token Supply

500 Million tokens are our total supply. Dapp's produce so many data requests that it is effectively a limitless amount — and when PLUGIN is the industry-standard oracle service provider; we'll need lots of PLUGIN to fulfill all those contract requests. Additionally, the Proof of Burn mechanic functions to eliminate tokens from the supply, so there needs to be a constant allowance of new PLUGIN being created.

8.2   Tokenomics

On the PLUGIN platform, The PLUGIN token would serve as a part of the payment system, the user requesting data would have to make payments in PLUGIN as fee to the client contract and the farmer hosting node would also receive payments in PLUGIN.

8.3   PLUGIN Token (XRC 20) Economies and Allocation:

- 18% to the promoters and founders (Token under vesting period using smart contract)

- 2% core team members. (Token under vesting period using smart contract)

- 10% Community Placement

- 10% Contingency

- 40% Ecosystems Adoption and Development Rewards

- 5% Technology Ops

- 15% Advisors, Partnership, Market Making & Exchange Listing etc.

9.   Project Milestone

PLUGIN MILESTONE

Business Concept Development	**2021 - Q1**		Use Case Development	**2022 - Q2**
2021 - Q2	Product Development Starts		**2022 - Q1**	Webinars, Promotions, Hackathon & Other Activities
Go - Live in Testnet - Onboard VinterAPI	**PRESENT**		GoLive in Mainnet & Onboard Data Feed Providers	**2021 - Q4**

Product inceptions started in the Quarter 1 - 2021, where we have brainstormed about the pros & cons of different decentralized oracle network in the market and we observed that the "High gas fee", "complex infrastructure" & "unclear reward & punish" model is notable one to improvise

Product Development started in the Quarter 2 - 2021, development team formed and the actual development started, with the help of experts and the architects we were able to successfully build our core product PLUGIN

Go-Live in "Testnet" - Quarter 3 - 2021 (Present), we have gone live in Testnet and onboarded our first data feed provider - VinterAPI. It is our game changing moment and we are glad to operate and provide index value for xdc in USD onto the smart contract.

Mainnet Preparation & Onboarding New Data Feed Providers - Quarter 4 - 2021, we are in initial discussion with various data feed providers and we are aggressively working on to go live in Mainnet.

Promotions & Marketing starts - Quarter 1 - 2022, we are ready with our plan of action to go viral and create a big community of developers, contributors through effective webinars, hackathons & other interactive activities

Use case development - Quarter 2 - 2022, decentralized finance, weather forecasting & insurance domain use cases are in our radar at the present and we are constantly doing research to make a bigger impact in different industry use cases in future

10. References

a. [Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System](#)
b. [Nasdaq.com - build-truly-decentralized-oracles](#)
c. ["Analysis of Centralized and Decentralized Cloud Architectures" by the School of Computing, University of South Alabama (2016)](#)
d. [Chain Link whitepaper-v2.pdf (chain.link)](#)
e. [Whitepaper.pdf (razor.network)](#)
f. [2106.09349.pdf (arxiv.org)](#)