Fiducia - Distributed Blockchain Data Oracle Network

Steve Chen*
Fiducia Network Project
Berkeley, California, USA
contact@fiducia.network

August 18, 2019

Abstract

Fiducia Network is a distributed network of data oracle nodes providing off-chain data to blockchain applications. Fiducia node acts as a proxy server at its core. The Fiducia node software takes user request, retrieves data off blockchain, and generate an intermediate response. In order to ensure data veracity, security, and confidentiality, a peer-to-peer network consensus mechanism is applied to process and generate a final response to the requesting party. The Fiducia node software operates within industry-standard secure computing environment to ensure that data are not tampered by the node operator.

Fiducia Network operates as a peer-to-peer network with nodes participating and leaving the network in a permission-less fashion. In order for the network to function effectively and efficiently, node operators are incentivized to participate by fees made by the requesting party.

Data source providers may make data available through well-known API endpoints. The node software may access data through well-known API endpoints. Alternatively, data providers may operate the node software and participate in the Fiducia Network directly.

Data requesting party, blockchain application (Dapp) developers, may utilize data provided by the node software by including Fiducia Data Provision SDK in the blockchain Dapps.

Figure 1: Fiducia - trust, faith, confidence

*corresponding author

Contents

List of Figures

1 Introduction

Blockchains like those of Bitcoin and Ethereum, do not have ready access to information outside of the chain. Smart contracts have no direct access data necessary for conditional verification processes. Data processing and verification are an essential part of smart contract functionality. And yet, currently, smart contracts are severely limited in their capabilities due to such lack of direct data access. An blockchain data oracle is, simply put, a conduit for information provided by an outside platform.

1.1 Blockchain Applications and Data Access

The central benefit of blockchain to businesses and developers is its ability to present data in a trusted manner. The immutability and time-stamp features of blockchain are central to distill trust in applications. Through properly designed infrastructure, data that are locked up in business vaults and that are currently not easily accessible can be brought the public in a trusted and trustworthy manner. All of this can be done at a lower cost than current non-blockchain system.

Businesses, organizations, and various agencies around the world possesses a tremendous amount of data. A lot of these data are meant to be used by the public. What prevents many such public data from being utilized by the public is the high cost of providing such a service. Centralized applications require large staff to set up and maintain. Distributed blockchain applications, on the other hand, requires dramatically less resources to maintain. The built-in economic system associated with blockchain applications offers a way to properly incentivize stakeholders, which dramatically reduces the on-going cost of maintaining a public access system. Through properly designed blockchain applications, deep web or deep data applications become feasible and cost-effective. A whole new category of deep data and deep web application could be effectively and efficiently built and deployed using blockchain technology.

Most of blockchain applications in the present time centers around financial payments. This is understandable given that the first successful and practical embodiment is Bitcoin, a peer-to-peer digital cash payment system. Various other blockchain payment systems followed Bitcoin into wide acceptance. Financial service is the first sector that blockchain technology has been successfully applied. It is by no means the only sector that could be disrupted in a positive way by blockchain technology.

We believe the immediate next sector that blockchain could prove disruptive is deep web and data associated with deep web. Modern day search engines crawl the web for surface data. Surface data are content that could be index by search engines. Prime examples of surface data are public web pages. Businesses and organizations also possesses a tremendous amount of data and content that are not in the form of web pages. They include presentations, pdf files, and other data stored in databases.

In many situations, deep web data are public information meant to be consumed by the general public. Deep web data are different from proprietary and private data. Through properly designed blockchain solutions, deep web data could be brought to the public in an efficient and cost-effective manner. One of the primary aim of the Fiducia Blockchain Platform is to make access to deep web data possible. In order to bring such deep data available, it requires an active effort on the part of data owners. One major problem that prevents data owners to make deep data available is the tremendous amount of resources required.

We believe data driven applications built on blockchain technology could open up a whole new format of search applications. Data driven blockchain application would be the next disruptive category of blockchain application in addition to financial payment solutions.

In the case of Deep Web Search: According to Popular Science: "[Deep web] is a place where online information is password protected, trapped behind paywalls, or requires special software to access—and it's massive. By some estimates, it is 500 times larger than the surface Web that most people search every day. Yet it's almost completely out of sight. According to a study published in Nature, Google indexes no more than 16 percent of the surface Web and misses all of the Deep Web. Any given search turns up just 0.03 percent of the information that exists online (one in 3,000 pages). It's like fishing in the top two feet of the ocean—you miss the virtual Mariana Trench below."

1.2 Inaccessibility Problem

Given the benefits of blockchain technology, what is preventing the wider adoption of blockchain and quicker deployment of blockchain applications?

The simple answer is that there is virtually no easy connection between blockchain and the existing IT data infrastructure. There is a "misconception" that blockchain applications can access all the data on the web and existing IT infrastructure, and vice versa.

Additionally, in order to develop blockchain applications, developers need to deal with the low-level blockchain interfaces directly. As there are many competing blockchain platforms in the market, dealing with low-level blockchain intricacies has become an arduous task for developers.

Furthermore, current blockchain technology does not support the scale and performance requirements of large scale business applications. The time required to process transactions on existing blockchains does not meet the needs of business grade applications. New methods of taking advantage of blockchain's unique characteristics while making sure blockchain applications can meet the expectations of businesses and users are necessary.

2 Distributed Data Oracle Network for Blockchain

Oracles provide the necessary data to smart contracts to process and verify. These operations are the core functionality of smart contracts. Off-chain data form the basis for smart contract to make conditional decisions. These conditions could be anything associated with the smart contract - prices, payment completion, proprietary corporate data, etc. These oracles are the only way for smart contracts to interact with data outside of the Blockchain environment.

Blockchain oracles can be categorized into centralized and decentralized types. Centralized oracles operate within a traditional corporate computing environment by an authority. Centralized oracles may be proprietary or open source. One defining feature of the centralized oracle system is that the system is closed to outsiders. We have to place faith into the integrity of the system and its operators to ensure data veracity, security, and fairness.

Distributed blockchain oracle operates as a p2p network of data provision nodes. It addresses the shortcomings of the centralized oracles. Our team believes that given the open nature of blockchain, a permission-less, p2p network based blockchain oracle system is necessary for the further development of the blockchain industry. Thus, Fiducia Blockchain Platform is born.

3 Our Solution - Fiducia Data Oracle Network

Fiducia Blockchain Platform strives to offer fast development and deployment of blockchain based data driven applications, thus enabling wider and quicker adoption of blockchain technology in every segment of the economy. Our ultimate goal is to enable the building of a high-trust economic system through blockchain technology.

With Fiducia Network, developers may take advantage of all the benefits of being able to access data from any source while not being entangled by the low level issues associated with data provisioning.

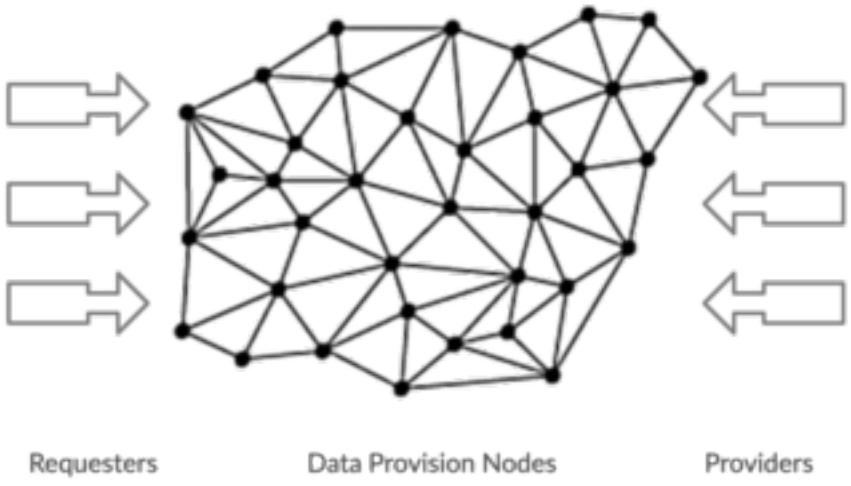

Figure 2: Fiducia Network

3.1 Components of Fiducia Network

Fiducia Data Provision Node Data Provision Node forms the center piece of Fiducia ecosystem. The node software forms a peer-to-peer network. The network collectively processes user requests, assign tasks to nodes, retrieves data from various sources, processes data, generates response to requesting parties.

Fiducia Developer SDK Blockchain application developers imports the Fiducia Developer SDK into their development environment. Inside smart contracts, developers may call functions associated with the SDK and use them to retrieve data necessary for the functioning of the smart contracts. The SDK is tailored toward different blockchains, such as Ethereum, Cosmos, Parity, or EOS. The SDK connects to the Fiducia Data Provision Node through a peer-to-peer fashion. Data requests are submitted and collected by the data request cache. Requests are processed based on a ranking and incentive scheme.

Random nodes are chosen to process the data retrieval requests. Retrieved data are further verified, combined and processed to form a finalized response to the requester.

Fiducia Data Provider SDK Data source owners may choose to become an active provider to the Fiducia Network. The Data Provider SDK can be used by data source owners to submit their data to the data provision cache. The list maintained by the data provision cache is available to the public. It serves as a list of available data types and sources currently accessible through the Fiducia Network.

Parties that are not data source owners may also use the Data Provision SDK to access publicly available data through public API end points. For some reason, if a data source owner does not want to actively participate in the Fiducia Network, but provides data publicly through open API endpoints, any third-party developer may use the Data Provision Node to connect to the public data API endpoints and participate in the Fiducia Network.

Fiducia Peer-to-Peer Network Consensus Mechanism Central to the peer-to-peer data provision node network is the randomness beacon used to select random active nodes to process a certain data request. Several randomness generator and beacon may be used independently or collectively to generate network randomness. Nodes will be chosen based on the network randomness, and perform tasks. For a single data request, several nodes are randomly selected to retrieve data. The retrieved data are compared, combined, and otherwise processed to generate a finalized version of the response. This ensures that no single node can be manipulated to generate false or inaccurate response. The node software works through the list of requests based on a ranking mechanism. Data requesting parties may define the level of urgency, data type, source, and other parameters for their intended results.

3.2 Trusted Execution Environment for Fiducia Network

Fiducia Data Provision Node is designed to work inside Trusted Execution Environment. A trusted execution environment (TEE) is a secure area of a main processor. It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. TEE further prevents the node operators from tampering with data processed inside the nodes.

Several open and propriety Trusted Execution Environments are currently available with varying degree of maturity:

- Intel SGX
- ARM TrustZone
- IBM Secure Service Container
- RISC V MultiZone

3.3 Operations of Fiducia Network

Fiducia Network operates as a matching service and marketplace between data requester and providers. The data provision nodes forms the foundation of the Fiducia Network when they establish a peer-to-peer network. Data requester and provider participate in the marketplace through their respective SDKs. The request cache and the provision cache serve as the order-book for the marketplace. Ranking and matching of the requests and provisions take place collectively on the peer-to-peer network of data provision nodes.

Very importantly, the Fiducia Network operates on a transaction fee based economic system. Requesters pay to use the service in the form of a network token, Fiducia Data Oracle (FDO) Token. Data providers and the node operators are compensated for their services by the fees paid by the requesters.

Fiducia Network provides the following unique attributes:

- Distributed and peer-to-peer network of data provision nodes
- Permission-less and open to participate
- Data veracity and security through randomness

4 Conclusion

Fiducia Network provides an open, distributed, secure, and robust solution to the data availability issue affecting blockchain projects. As blockchain and blockchain applications are still in their infancy, we believe Fiducia Network would be an important enabling technology driving towards wider and speedier adoption of blockchain technology.

4.1 Future Work

We plan to release updates and details on Fiducia Network on a regular basis or as new versions become available.

4.2 Acknowledgements

We would like to acknowledge several industry veterans for advising our project.

4.3 Versions and Revisions to this position paper

- v. 1.0 – August 2019, initial release