SEBA BANK

February 2021

Oracles
The Internet of Blockchains

The Bridge

Redefining Finance for the New Economy

Table of Contents

Authors

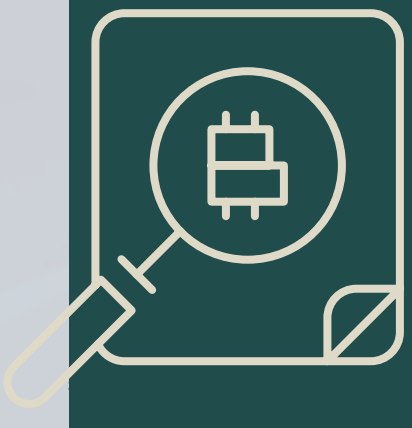
Yves Longchamp
Head of Research
SEBA Bank AG

Saurabh Deshpande
Research Analyst
B&B Analytics Private Limited

Kunal Goel
Research Analyst
B&B Analytics Private Limited

Contact

research@seba.swiss



Executive summary

Just “knowing thyself” is not sufficient for a smart platform blockchain. Oracles are critical middleware that connect blockchains to the real world unlocking the full potential of platforms chains.

Their use is ubiquitous across decentralised applications in all new themes such as decentralised finance, interoperability and supply chain, and their use will grow as these themes play out.

In this issue of the Bridge, we discuss how blockchains' inherent inability to connect to the real world limits their use and how oracles provide the solution by acting as middleware to their connection to the world. We discuss "the oracle problem" and why it is imperative that oracles follow a decentralised model.

1. Introduction

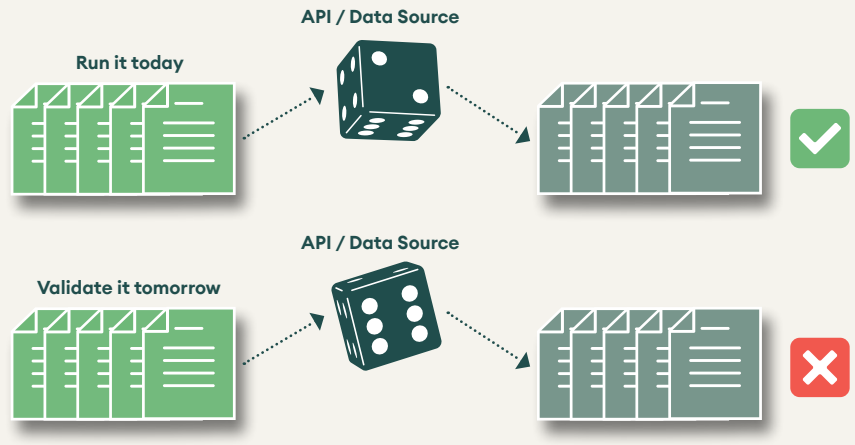
We find that oracles are pervasive in their use across decentralised applications and find use throughout all key themes and implementations of blockchain technology such as decentralised finance, interoperability and supply chain. We also cover key oracle projects that are enabling the growing ecosystem of decentralised applications today.

2. Blockchains are a black box

A blockchain can only read the information that is present on itself. It is unable to access any information outside of it or any metadata about itself. Blockchains function like a computer that is not connected to the internet and can only read the data available on it. This closed architecture minimises vulnerabilities and ensures the blockchain's security, but it also limits its use.

For blockchains used only to settle value like Bitcoin, Litecoin, Ripple, this limitation is not an issue. For blockchains designed to run smart contracts and applications like Cardano, Ethereum, Polkadot, to name three, this is a severe limitation. The ability to interact with the outside world and to use information is key to unleashing the full power of decentralised applications. Without it, any decentralised applications (dapps) built on these platforms will be limited to only information available on the blockchain. For example, consider the case of a prediction market for whether the price for ETH will exceed, say, USDk 5 at any point in 2021 or not. No information on the Ethereum blockchain records ETH price in USD so the prediction market would not be able to resolve whether the condition has been met or not. Similarly, since smart contracts are executed separately and independently at every node, for an application that leverages random numbers, every node may resolve a different random number and achieve a different result (see figure 1). Multiple results would stop the block from achieving finality as consensus would not be achieved. Further, it breaks down the deterministic quality of blockchains – the ability to rerun all the transactions and get to the same result.

Figure 1: Different Ethereum nodes resolving different random numbers



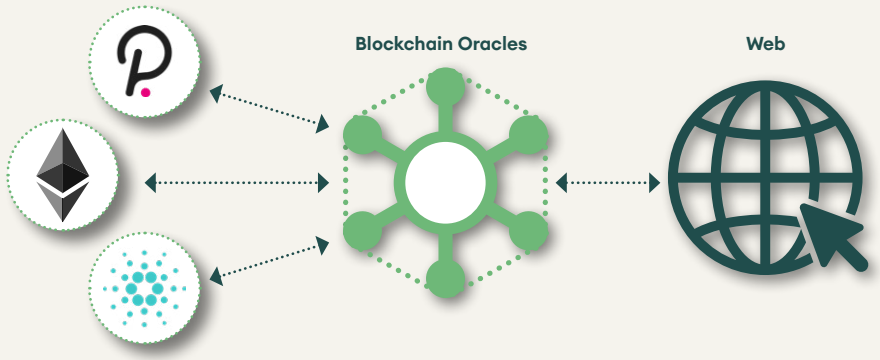
Source: SEBA Bank, Chainlink Blog

3.
What is an Oracle?

Oracles provide solutions to the problems mentioned above. They bring off-chain (outside the blockchain) data, to the blockchain so various applications and smart contracts may access it. Oracles connect blockchains to the real world, the internet, and each other.

In a multiple platform blockchain world, one or many decentralised oracle solutions will connect them to the internet and each other allowing information to be shared and accessed by the multitude of applications built on these blockchains. If blockchains were computers, oracles would be the modems, allowing them to interact with the internet and with each other (see figure 2). Oracles also help resolve problems like the random number problem suggested above. Instead of the computing nodes separately generating random numbers, the oracle runs the random number simulation and publishes it on the blockchain. The computing nodes will use this published number to achieve the same result. In this way, block finality is achieved, and the deterministic nature of the blockchain is preserved.

Figure 2: An oracle connecting blockchains to the web and each other



Source: SEBA Bank

There are two broad types of oracle blockchains:

- **On-chain oracles** act as bridges between blockchains, allowing blockchain information to be read and used by other blockchains. For example, a multi-chain decentralised exchange (DEX) aggregator will need price feeds from the decentralised exchanges running on Ethereum, Cardano and other blockchains to fetch the best price available. For this purpose, an on-chain oracle may run through the DEXes on Ethereum, Cardano and others to fetch the best price for the aggregator. An on-chain oracle may also be one dapp providing oracle services to another dapp. For example, Uniswap (a decentralised protocol for automated market making) natively knows the price between any two assets listed on the platform through its liquidity pool. Any dapps that need the price relationship between the two assets can use this data.
- **Off-chain oracles** act as middleware connecting blockchains to the non-blockchain world. For example, suppose the shipping journey of a product is being recorded on a blockchain. Here, the off-chain protocol will connect to the sensors reading the NFC (Near Field Communication) tag of the product through its various hops and communicate it to the blockchain where it is recorded.

They may also be classified in other ways :

- **Inbound** vs **outbound** oracle – Inbound oracles transfer information from outside the blockchain to the blockchain. An outbound oracle will do the opposite, moving data from the blockchain to outside it.
- **Software** vs **hardware** vs **human** – Software oracles will pull data from the internet, other blockchains and dapps, APIs and so on. A hardware oracle may connect an Internet of Things (IoT) device reporting real-world data to the blockchain. A human may also act as an oracle as in the case of Augur's prediction market where a user may vote that a particular outcome has occurred by staking their asset on it.

4.
The Oracle Problem

Public blockchains are designed with decentralisation as one its central philosophies, and they are not subject to a single point of attack risk. Using a centralised oracle to feed data defeats the purpose of a decentralised blockchain. A malicious actor need not attack the nodes of a blockchain if it can compromise the oracle it uses to input incorrect data onto the blockchain. Continuing from the previous example, if a malicious actor in control of the oracle has made a bet that the price of ETH will remain below USDk 5 for 2021, it will never allow the oracle to send a price higher than USDk 5 to the blockchain for the smart contract to resolve correctly.

A malicious actor is not necessary for centralised oracles to fail to do their job correctly. We have seen that price data from one source may get affected by a flash crash (see article) leading to a cascading effect if more applications trust it.

Therefore, to mitigate this problem, decentralised oracles solutions aggregate data from multiple sources and use a consensus mechanism to minimise the risk of misreporting. The operators that feed the data to the aggregating algorithm are incentivised to report correct information and punished for incorrect information. For every correct piece of data reported, the contract, or user requesting the data, transfers some value to the protocol that splits it among the operators that provided it. Operators lock certain value on the protocol; if consensus is reached for which an operator's data is rejected, some pre-decided value is slashed from the operator's stake. As with blockchain consensus, as long as 51% of the participants are reporting correctly, the oracle reports the correct data.

5.
Applications of oracles

To understand the ubiquitous use of oracles, we explore a few blockchain use-cases.

Decentralised Finance

DeFi applications have extensive data needs to be able to deliver financial solutions efficiently. For example, Maker Protocol that lends out collateralised DAI relies on price data from oracles to determine how much DAI to issue per unit of cryptocurrency collateral. It also uses oracles to ensure that the DAI already issue is always sufficiently collateralised.

Interoperability

Interoperability protocols may have their own oracle solutions or may rely on existing oracles to allow free flow of information between different blockchain protocols to ensure coordination. For a multi-chain decentralised exchange (DEX) aggregator, information must flow freely to provide its users with the best price.

Supply chain

One of the applications of blockchain technology is to record the full history of a product to be verified independently by its consumer. For example, this may be used to independently ensure that a product's origin is from a particular country or to ascertain its carbon footprint. To achieve this in a fully automated manner and to ensure no conflicts, an oracle needs to be used in conjunction with a reporting mechanism like Near Field Communication (NFC) tags to feed a product's journey through its supply chain onto the blockchain. Any interested party can later independently verify it and be confident of its accuracy.

Prediction markets

Prediction markets allow users to make bets on the outcome of an event. For example, the result of a football or cricket game or the winner of an election. An oracle is required to report an event's outcome, so the winning bettors may be paid as the blockchain independently cannot know what real-world event has occurred.

Gaming / Gambling

Gaming relies on randomness to provide a level of luck and excitement to the players. Games may use randomness provided by oracles to resolve the chances for loot drop rate, miss and hit rate, and critical hit rate and other similar game mechanics. For unique drops, oracles can also verify the number of items in existence using NFT (non-fungible tokens) and confirm their historical drop rate. For gambling, players can individually verify that the deck of cards, dice roll, spin or any other mechanic used is verifiably random and how it has behaved historically.

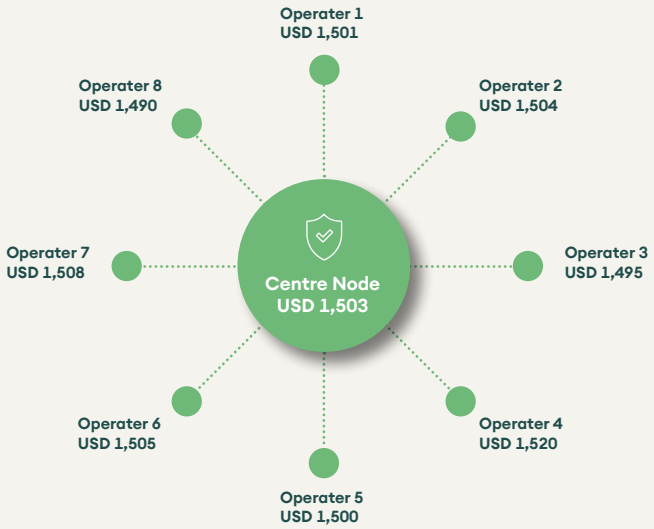
6.
Oracle Networks

In this section, we present a few oracle projects to understand how they work and the scope of their functionalities.

ChainLink Network (LINK)

Chainlink is the leading decentralised oracle solution with almost all large DeFi projects relying on its data feeds. It is an off-chain oracle with a network of independent node operators that gathers and delivers data to its middleware application. The middleware application aggregates and combines it into single data output and delivers it to the blockchain to be read by smart contracts relying on it.

Figure 3: Chainlink software aggregates inputs from all operators



Source: SEBA Bank, Chainlink Blog

Chainlink network is blockchain agnostic, and developers can modify the core software to connect to any blockchain. It is currently widely used for Ethereum-based dapps, and the LINK token on Ethereum platform is used for payment of services by the users and will be used to bond by the operators. As more smart-contract based blockchain platforms grow operational, the LINK token may be added to other platforms to provide oracle and cross-platform services.

For a more detailed analysis of the Chainlink project and the LINK token economics, please follow the link (no pun intended) to the Digital Investor's February edition – Chainlink Investment Thesis.

Band Protocol

Band Protocol is an on-chain oracle that runs on an independent Cosmos-based blockchain called BandChain and runs through smart platform blockchains. It allows for developers to write custom oracle scripts to fetch data to use in their dapps. BandChain uses a Delegated Proof of Stake consensus mechanism, and its 100+ validators fetch the queried data which is first published on BandChain and then on the requesting platform chain. Similar to Chainlink, validators are paid in the native BAND token for delivering data, and they have to stake these tokens so the any misreporting may be penalised. The turnaround time for a data request to be delivered is about 6 seconds as the block time for BandChain is only 2 seconds. Since BandChain is an independent chain, it does not suffer from network issues on the requesting chain like slow block time or high network fees.

The Graph

The Graph is an outbound oracle that indexes and collects blockchain data to be read and displayed in a user-friendly manner. It aggregates and indexes blockchain data by processing all the blocks. This allows it to deliver data through APIs which otherwise would not be easily accessed.

Developers or "curators" create applications that query the blockchain for specific data that may be of interest to the user. The node operators or "indexers" collect this data from every blockchain block and index it to be delivered to the user. For this service, they are paid by the developers of the app. The users of the application have to pay the "indexer" and "curator" to use their app and data. Typically, the developer for the application on the Graph is pulling information from their own dapp on the blockchain and presenting it to their users so that they may be able to make the best decision for themselves.

Simply speaking, it acts as an open-source search engine for blockchain data, with incentivised operators providing indexing and storage services. Applications built on it can visualise blockchain data for the user to understand and make a more informed decision.

For example, Uniswap's information page (see here) uses The Graph to pull pair analytics, top pairs, transaction data, most liquid pairs, etc. It provides an intuitive front-end for the users to analyse and transact.

Other Oracles

Other than the projects covered above, any data generated by one app may be used by another. For example, Uniswap (a decentralised protocol for automated market making) natively knows the price between any two assets listed on the platform through its liquidity pool. This data can be used by any dapps that require price data between the two assets. A lending dapp may use price data to ensure that it has sufficient outstanding collateral against all loans.

7.
Conclusion

We find that oracles are pervasive in their use across decentralised applications and find use throughout all key themes and implementations of blockchain technology like decentralised finance, interoperability, supply chain, and so on. We also cover the basics of crucial Oracle projects that enable the growing ecosystem of decentralised applications today.

Disclaimer

This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head once and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial investment or to participate in any particular investment. strategy. This document is for distribution only under such circumstances as may be permitted by applicable law. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction.

No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document, except with respect to information concerning SEBA. The information is not intended to be a complete statement or summary of the financial investments, markets or developments referred to in the document. SEBA does not undertake to update or keep current the information. Any statements contained in this document attributed to a third party represent SEBA's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Any prices stated in this document are for information purposes only and do not represent valuations for individual investments. There is no representation that any transaction can or could have been elected at those prices, and any prices do not necessarily reflect SEBA's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by SEBA or any other source may yield substantially different results.

Nothing in this document constitutes a representation that any investment strategy or investment is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgment in making their investment decisions. Financial investments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Certain services and products are subject to legal restrictions and cannot be offered on an unrestricted basis to certain investors. Recipients are therefore asked to consult the restrictions relating to investments, products or services for further information. Furthermore, recipients may consult their legal/tax advisors should they require any clarifcations. SEBA and any of its directors or employees may be entitled at any time to hold long or short positions in investments, carry out transactions involving relevant investments in the capacity of principal or agent, or provide any other services or have offcers, who serve as directors, either to/for the issuer, the investment itself or to/for any company commercially or financially affliated to such investment.

At any time, investment decisions (including whether to buy, sell or hold investments) made by SEBA and its employees may differ from or be contrary to the opinions expressed in SEBA research publications.

Some investments may not be readily realizable since the market is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be diffcult to quantify. Investing in digital assets including cryptocurrencies as well as in futures and options is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may under certain circumstances occur. The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. Tax treatment depends on the individual circumstances and may be subject to change in the future.

SEBA does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specifc investor's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of individual investors and we would recommend that you take financial and/or tax advice as to the implications (including tax) prior to investing. Neither SEBA nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information provided in the document.

This document may not be reproduced or copies circulated without prior authority of SEBA. Unless otherwise agreed in writing SEBA expressly prohibits the distribution and transfer of this document to third parties for any reason. SEBA accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this document.

Research will initiate, update and cease coverage solely at the discretion of SEBA. The information contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. SEBA may use research input provided by analysts employed by its affliate B&B Analytics Private Limited, Mumbai. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information The compensation of the analyst who prepared this document is determined exclusively by SEBA.

Austria: SEBA is not licensed to conduct banking andfinancial activities in Austria nor is SEBA supervised by the Austrian Financial Market Authority (Finanzmarktaufsicht), to which this document has not been submitted for approval. France: SEBA is not licensed to conduct banking and financial activities in France nor is SEBA supervised by French banking and financial authorities. Italy: SEBA is not licensed to conduct banking and financial activities in Italy nor is SEBA supervised by the Bank of Italy (Banca d'Italia) and the Italian Financial Markets Supervisory Authority (CONSOB - Commissione Nazionale per le Società e la Borsa), to which this document has not been submitted for approval. Germany: SEBA is not licensed to conduct banking and financial activities in Germany nor is SEBA supervised by the German Federal Financial Services Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht), to which this document has not been submitted for approval. Hong-Kong: SEBA is not licensed to conduct banking and financial activities in Hong-Kong nor is SEBA supervised by banking and financial authorities in Hong-Kong, to which this document has not been submitted for approval. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Hong-Kong where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not "professional investors" within the meaning of the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong) and any rules made thereunder (the "SFO"). Netherlands: This publication has been produced by SEBA, which is not authorised to provide regulated services in the Netherlands. Portugal: SEBA is not licensed to conduct banking and financial activities in Portugal nor is SEBA supervised by the Portuguese regulators Bank of Portugal "Banco de Portugal" and Portuguese Securities Exchange Commission "Comissao do Mercado de Valores Mobiliarios". Singapore: SEBA is not licensed to conduct banking and financial activities in Singapore nor is SEBA supervised by banking and financial authorities in Singapore, to which this document has not been submitted for approval. This document was provided to you as a result of a request received by SEBA from you and/or persons entitled to make the request on your behalf. Should you have received the document erroneously, SEBA asks that you kindly destroy/delete it and inform SEBA immediately. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in Singapore where such distribution, publication, availability or use would be contrary to law or regulation or would subject SEBA to any registration or licensing requirement within such jurisdiction. This document is under no circumstances directed to, or intended for distribution, publication to or use by, persons who are not accredited investors, expert investors or institutional investors as declned in section 4A of the Securities and Futures Act (Cap. 289 of Singapore) ("SFA"). UK: This document has been prepared by SEBA Bank AG ("SEBA") in Switzerland. SEBA is a Swiss bank and securities dealer with its head offce and legal domicile in Switzerland. It is authorized and regulated by the Swiss Financial Market Supervisory Authority (FINMA). This document is for your information only and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product.

SEBA is not an authorised person for purposes of the Financial Services and Markets Act (FSMA), and accordingly, any information if deemed a financial promotion is provided only to persons in the UK reasonably believed to be of a kind to whom promotions may be communicated by an unauthorised person pursuant to an exemption under the FSMA (Financial Promotion) Order 2005 (the "FPO"). Such persons include: (a) persons having professional experience in matters relating to investments ("Investment Professionals") and (b) high net worth bodies corporate, partnerships, unincorporated associations, trusts, etc. falling within Article 49 of the FPO ("High Net Worth Businesses"). High Net Worth Businesses include: (i) a corporation which has called-up share capital or net assets of at least GBP 5 million or is a member of a group in which includes a company with called-up share capital or net assets of at least GBP 5 million (but where the corporation has more than 20 shareholders or it is a subsidiary of a company with more than 20 shareholders, the GBP 5 million share capital / net assets requirement is reduced to GBP 500,000); (ii) a partnership or unincorporated association with net assets of at least GBP 5 million and (iii) a trustee of a trust which has had gross assets (i.e. total assets held before deduction of any liabilities) of at least GBP 10 million at any time within the year preceding the promotion. Any financial promotion information is available only to such persons, and persons of any other description in the UK may not rely on the information in it. Most of the protections provided by the UK regulatory system, and compensation under the UK Financial Services Compensation Scheme, will not be available.

SEBA BANK

SEBA Bank AG
Kolinplatz 15 • 6300 Zug • Switzerland • www.seba.swiss • info@seba.swiss