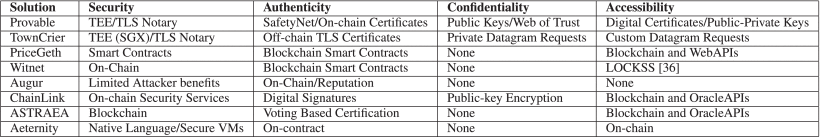
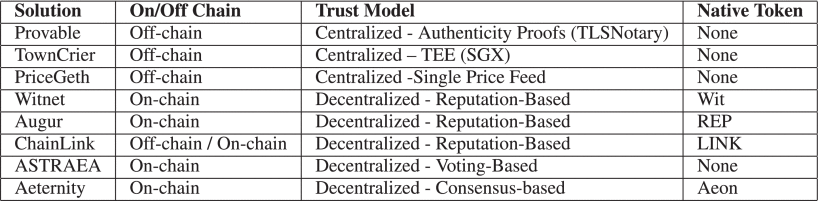
Based on the extensive review, we found that existing blockchain oracle solutions can be differentiated based on different aspects as detailed in Table 1 and Table 2.



The first aspect is related to the deployment of the solution (e.g., whether the solution is deployed on-chain, off-chain, or in both sides). Provable, Town Crier, and PriceGeth provide off-chain solutions that can be connected to a smart contract on-chain to transfer the requested data. Whereas, Witnet, Augur, ASTRAEA, and Aeternity are all on-chain solutions. However, ChainLink provides both on-chain and off-chain components for its solution.

Trust model is the second aspect of analysis. As we discussed in the oracles taxonomy section, the number of nodes used by oracle solution to get data into smart contracts defines the trust model used by oracles, where the single node represents a centralized trust model and multiple nodes represent decentralized models. Three of the above solutions follow a centralized trust model, but each of them is based on a different approach. Provable is an example of a centralized oracle service leveraging a variety of authenticity proofs such as TLSNotary Proof; whereas, TownCrier is another centralized solution that is based on Trusted Execution Environments (TEEs), where it uses Intel’s SGX (Software Guard eXtensions) to ensure that responses from HTTPS queries can be verified as authentic. The third centralized solution is PriceGeth, which relies on a single price feed (PriceFetcher). The remaining five solutions rely on multiple nodes to get external data into smart contracts, where these solutions follow a decentralized trust model with different approaches. Witnet is a decentralized oracle network based on reputation points. Augur is another reputation-based decentralized oracle and platform specifically designed for prediction markets. ChainLink operates as a fully decentralized network that is also based on reputation; whereas, ASTRAEA is a decentralized oracle based on a voting game between voters and certifiers and it detects and penalizes the dishonest voters by enabling sealed voting mechanism as well as the assessment of majority votes.

However, the possibility of adversarial attacks on oracles still exist whereby an oracle can intercept the responses of other oracles and replicate the voting behavior accordingly to benefit from the voting mechanism. Since oracles on ASTREA can participate as submitters, voters, and certifiers, there still exist the risk of Sybil attacks whereby one oracle may observe the behavior of other oracles and then start acting as certifiers as well. Finally, Aeternity uses state-channels (i.e. off-chain transaction processing) to enable communication between peers on the decentralized network. The blockchain, on the Aeternity, plays the role of arbitrator in case of any dispute between two participants. This trust model ensures more privacy due to less exposure to data on the blockchain. In addition, off-chain state-channels ensures speedy, secure, and low-cost blockchain transactions. Finally in the third aspect, Witnet, Augur, ChainLink and Aeternity use their native tokens; whereas the other solutions do not introduce new tokens.

Source: [ieeexplore.ieee.org](https://ieeexplore.ieee.org/abstract/document/9086815)