QED ORACLE PROTOCOL MODEL

SEPTEMBER 2021

QED.NETWORK

IMPORTANT NOTICE

Nothing contained in this announcement constitutes or shall be deemed to constitute financial, legal, tax or other advice of any kind. Do not trade or invest in any tokens, companies or entities based solely upon this document. Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. This paper is published solely for informational purposes and has no regard to the specific objectives, financial situation or particular needs of any person.

Information contained herein is believed to be reliable, but no warranty is given as to its accuracy or completeness and views and opinions are subject to change without notice.

Specifically, the information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. No representations or warranties are made as to the accuracy of such forward-looking statements. Any projections, forecasts and estimates contained in this document are necessarily speculative in nature and are based upon certain assumptions. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond control. It can be expected that some or all such forward-looking assumptions will not materialise or will vary significantly from actual results.

Information contained in this announcement in respect of any digital assets should not be considered an offer to sell or a solicitation of an offer to buy or subscribe for an interest in any investment vehicle or any other securities.

This paper is not directed to any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where the content of this paper would be contrary to law or regulation, or which would subject us to any registration or licensing requirement within such jurisdiction. You expressly acknowledge that you are, as the case may be, an individual who is legally or authorized to seek information about the matters referred to or described on the paper.

ORIGIN VENTURES LIMITED, INCLUDING ITS DIRECTORS, AGENTS, EMPLOYEES, CONTRACTORS AND PARTNERS (TOGETHER, THE "ORIGIN PARTIES") DISCLAIM, IN ACCORDANCE WITH APPLICABLE LAW, ANY LIABILITY FOR LOSSES OR DAMAGE OF ANY KIND ARISING DIRECTLY OR INDIRECTLY AS A RESULT OF: (1) THE CONTENT OF THE PAPER, IN PARTICULAR ITS UP-TO-DATE NATURE, ACCURACY AND COMPLETENESS (2) ERRORS OR OMISSIONS IN THE PAPER; (3) USE OF OR ACCESS TO THE PAPER; (4) INABILITY TO ACCESS OR USE THE PAPER FOR ANY REASON.

THE ORIGIN PARTIES, IN ACCORDANCE WITH APPLICABLE LAW, DISCLAIM ANY LIABILITY FOR: (1) LOSS OF PROFITS, REVENUE, SAVINGS OR OTHER ECONOMIC LOSS; (2) LOSSES INCURRED DURING BUSINESS TRANSACTIONS OR OTHER LOSSES PERTAINING TO BUSINESS ACTIVITIES OR GOODWILL; (3) LOSS OF OR DAMAGE TO DATA; (4) INCIDENTAL OR SPECIAL DAMAGE; (5) WASTED OR LOST MANAGEMENT TIME; OR (6) INDIRECT OR CONSEQUENTIAL DAMAGE ARISING FROM THE USE OF OR ACCESS TO THE PAPER, EVEN IF A PRIOR WARNING WAS GIVEN ABOUT SUCH LOSS OR DAMAGE, OR IF SUCH LOSS OR DAMAGE WAS FORESEEABLE.

Introduction

Smart contracts resident on blockchains or other decentralised platforms offer the prospect of huge efficiency increases in the management of commercial and legal transactions both in the conventional person-centered economy, and in the emerging machine-to-machine economy. Through their automatic operation, smart contracts hold out the crucial benefit of absolute certainty about execution, so that the threat of non-compliance is made, in effect, mathematically impossible.

This major benefit has led to intense interest in smart contracts in a whole range of areas, from the financial economy to smart supply chains to the Internet of Things. However, there is one potential weakness which has so far held up the practical deployment of smart contracts. The triggers of such contracts must ultimately depend on factors outside the contract itself, outside the blockchain or platform it sits on and in the real world. For smart contracts to work, it is necessary for real-world information to be brought into them in order to meet the execution criterion. This crucial function is performed by oracles, protocol-based methods for transferring information from the external world into the blockchain/platform-based smart contract.

The major problem facing the development of smart contracts is that up to now customers have had simply to rely on the good faith and accuracy of the relevant oracle or oracles, with no means either of verifying their reliability or of securing recourse in the event that they prove unreliable.

All this is now changing as smart contracts enter a second generation with the revolutionary introduction of decentralised oracle reliability verification in the form of the QED Oracle protocol.

QED Oracle Protocol

QED is an Oracle protocol and utility token model that is designed to ultimately interface with any blockchain or smart contract platform. The initial QED platform is comprised of performance scaling components built on UX Network, as well as treasury and funding components built on Ethereum for secure settlement at the value layer

The initial version manages Oracles delivering data to smart contracts that typically reside on DeFi platforms. Further rollouts will include other services or work that Oracles need to provide that create the foundations for decentralised protocols and economies.

Differentiation

In general, Oracles provide external data to a smart contract that triggers an action. Smart contracts currently have no choice but to accept that Oracles will act in good faith. There are no recourse or recovery mechanisms in place for inaccurate results or malicious attacks. The QED model takes the technical delivery of data a step further and deals with veracity of data provided and recovery of potential loss.

QED embeds financial recourse in a codified and trustless smart contract environment with no loss of execution experience.

Decentralised protocols are now able to receive and pass data whilst maintaining security and decentralisation itself. This removes a key friction point for dApps and unlocks capital seeking a rational commercial experience.

The crucial advantage of QED is that the reliability ranking of oracles is itself performed by a completely decentralised and automatic procedure not requiring the intervention of an adjudicating third-party. This both preserves the decentralised nature of the entire smart contract and also ensures that no additional negotiation or arrangement is required of the parties beyond that of simply setting the fee for the overall performance of the contract (which must in any case always be determined).

The QED Model

- Oracles bond collateral that is defined by the smart contract risk exposure. Collateral is external to the QED system and not an internal economic token.
- Oracles are subject to dynamic accuracy scoring that determines their capital efficiency and creates a macro survival bias.
- Customers can use a post-execution collateral claim process that includes the most accurate Oracles to participate in resolution. Restitution of loss is drawn from the collateral posted by erroneous Oracles.

The QED model rebalances the risk profile to a level playing field that is now commercially viable and allows markets to find fair pricing levels. This is particularly relevant to DeFi protocols who are vulnerable financially to malicious Oracle behaviour.

With QED, smart contracts can access data at a frictional cost that does not disrupt their business case and Oracles can deliver data at scale to a much larger customer base.

In effect, this removes from the smart contract the need to confront the dilemma of either simply accepting the good faith and reliability of a given oracle or set of oracles or of engaging in extensive examination and assessment, a process that would severely offset the efficiency gains offered by the use of a smart contract in the first place.

QED Version 1.0

This paper is a high-level description of the principles and process that underly the initial version of the QED Model. More technical resources and underlying mathematical processes are not presented in detail at this point in favour of the reader gaining a more intuitive understanding of the system. For Version 1.0, we refer to price data as being provided by Oracles as we see this as a common use case, especially in the DeFi universe, However the model extends to other data feeds and utility.

QED is designed to be a decentralised model. Model parameters and calculations may be amended over time through system evolution and governance.

The Oracle dilemma

Once a truly trustless smart contract has released value, errors are irrecoverable through code.

This basically means that smart contracts not protected by oracle ranking have no solution to the problem of garbage-in-garbage-out. If erroneous data is entered in such naive smart contracts, then there is no mechanism intrinsic to the contract itself by which restitution can be achieved. The aggrieved party will be forced to have recourse to conventional recovery methods, thereby again eroding any value that he might have derived from the use of a smart contract.

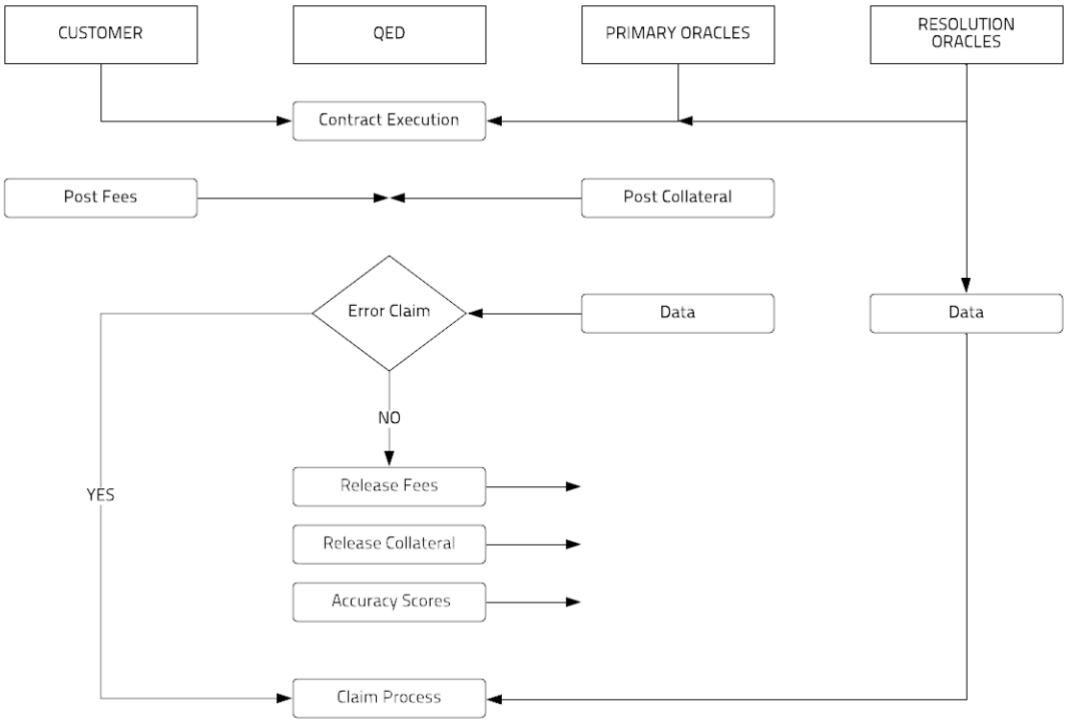
QED inverts the problem whereby Oracles bond collateral upfront and a claims process can be implemented post-execution.

The posting of collateral by oracles ensures that the means of restitution are built into the contract itself. Restitution becomes as automatic (and invisible) as the execution of a completely claim-free and successful contract.

Initial Process

An Oracle contract contains Primary and Resolution Oracles. Primary Oracles arrange the initial fees and collateral and provide data accordingly. Resolution Oracles also provide data, but this is not revealed unless there is a collateral claim. The combination of the two data sets determines the outcome of the claim.

The introduction of the resolution oracle layer provides a new and independent platform for the rapid and painless remediation of contractual malfunctions. However, crucially, it does not involve a new layer of contractual structure from the perspective of the customer. The resolution tier of oracles emerges naturally from the existing activities of the primary oracles.



Pre-Execution

The QED Oracle contract is configured and agreed by its users, that is Oracles and their customer. Whilst initially these will be bespoke, we expect standardised contracts to appear as there are in traditional financial markets (for example, the ISDA Master Agreement in OTC derivatives).

This will be the case in particular in the machine-to-machine economy, where the micro nature of the transactions will make the use of bespoke contracts (even smart contracts) economically non-viable.

Customers and Oracles publish on chain their contractual requirements and terms of service, which are then matched to ensure both parties agree on commercial terms for an oracle feed contract. Terms of service may include multiple requirements with some examples highlighted below.

These further requirements are intended to secure the quality level of the primary oracles, ideally rendering the involvement of the resolution oracles unnecessary. However, it is a key feature of QED that the system does not depend critically on the right choice of such further requirements, which has been the industry standard approach up to now.

Specific Source	Oracles do not act as aggregators of data inputs but provide specific source points.
Time Shard	The length of window for data observations
Minimum Nodes	Customers may set the minimum number of Oracles required to participate
Minimum Accuracy	Customers may set a standard for accuracy ratings
Consensus	Version 1 is set at a modal average, 75% threshold
Proposed Fee Rates	Customer can set fee limits
Contract Loss	The Collateral requirement from the Oracles in total
Collateral Form	e.g., BTC / ETH / USDC

Primary Oracle Collateral

The collateral quantity and form are defined in the Oracle contract from the "Loss" component and formally calculated (C) as follows:

L: Specified Collateral Loss
N: Number of Oracles
T: Threshold for consensus

Where $C = \frac{L}{T.n}$

In Version 1.0, the consensus threshold is set at 75% and therefore Oracles in aggregate post 133% of Loss. This means that in the event of a proven collateral claim, a minimum of 100% collateral is available from those who created the error. If more than 75% of Oracles were proven to be erroneous, there will be excess collateral.

The actual loss experience may be less than the defined Loss depending on the contract. For example, a perpetual swap smart contract will have a variable payment obligation capped by the margin component as the maximum loss.

These two factors effectively ensure that there is a margin on the margin. It is in practice impossible that a situation could arise in which there is insufficient collateral available to cover any proven claim under the contract.

Collateral can be in any form as long as it can bond to the QED smart contract. Where Oracles are providing support for interoperability or cross-protocol data, we would expect collateral to be in protocol native tokens. As risks become more linked to external enterprise, we see collateral as digital fiat currencies.

Fees

Primary Oracles provide fee quotations through an auction system and a price is established for execution. Fees are weighted by accuracy scores. Two oracles contracting at the same price may receive different fee allocations depending on their historic performance.

This provides a strong incentive for oracles to achieve a record of accuracy and reliability. Oracles that fail to do this can be expected gradually to disappear from the platform.

Oracle return on capital is proportionate to Accuracy.

Identity

Oracles are by definition unique accounts since they rely on their accuracy score for pricing and fees. Specific contracts may rely on further identity requirements which can be established by QED from identity protocols.

Accuracy Rating

For the purposes of this paper and a high-level view of the QED principles, we look at accuracy as a binary outcome of Accurate or Inaccurate per data point. However, various statistical methods will be implemented to manage Accuracy depending on the specific contracts.

As an example, Oracles providing price data for a ten second window may return a range of prices that are all fundamentally Accurate but numerically different. In this case, a mean price and standard deviation approach may be taken to define both the range for Accuracy and a non-binary accuracy score for that operation.

Such non-binary accuracy scores will also evolve to cover non-financial smart contracts, for example through agreed service performance quality determinations.

Price Data Oracles

In the example where 10 Oracles are publishing a price:

Oracle Node	1	2	3	4	5	6	7	8	9	10
Price	8.00	8.00	8.00	8.00	8.00	8.00	8.00	8.00	14.00	20.00

80% of Oracles are supplying the modal price of 8 which exceeds the 75% threshold requirement.

Assuming there is no claim from the customer, the model divides the Oracles into two cohorts as simply "Accurate" and "Inaccurate"

Oracles 1 – 8 are Accurate and Oracles 7 – 10 are Inaccurate.

All fees are paid to Accurate Oracles in proportion to their accuracy scores. Accurate Oracles receive a fee benefit from the Inaccurate group who receive nothing.

Again, this simplified binary picture can be appropriately adjusted for non-binary real-world use cases.

Rating Process

The Oracle rating ranges from 0 to 1 and reflects the probability of accuracy.

- Accuracy is measured on a fixed time period with a set number of data points required per period generating the initial and dynamic score.
- The period resets at the earlier of the number of data points has been reached or the time period ends.
- The ratings per period are averaged with a time weighting towards more recent data.
- A collateral weighting is applied to scores to generate Collateral Weighted Accuracy Rating.
- New Oracles start at 0.50 and Oracles receive 0.50 for missing data points in their period.

Each Oracle has an Accuracy Rating and a Collateral Weighted Accuracy Rating – both of which are useful for customers depending on the type of contract they wish to employ. For both ratings, number of data points provided, and standard deviation metrics are attached to provide a fuller picture of Oracle accuracy.

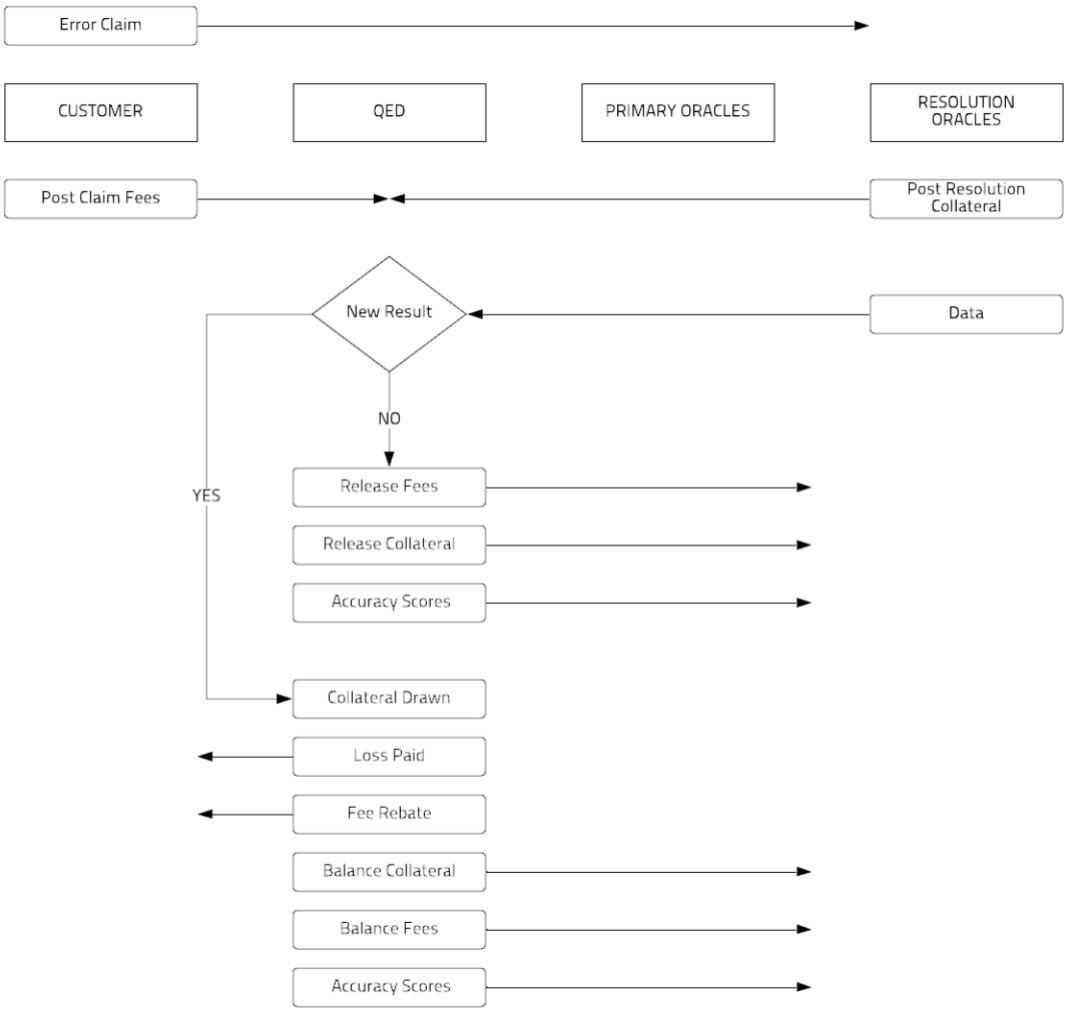
In some contracts, the simple Accuracy Rating will be more important for the customer and in others the Collateral Weighted Accuracy Rating. However, from the perspective of the oracle itself it is sustaining the level of the latter which will guarantee its long-term profitability.

Since Oracle return on capital is directly affected by accuracy, Oracles are incentivised to improve performance and poorly performing Oracles will not be able to compete on pricing.

Claim Process

A claim process from a customer freezes the collateral and fees. In order to commence the process a claim fee is paid by the Customer which is set at 50% of the initial fee which is recovered in the event of a successful claim.

This brings the Resolution Oracles into play who now reveal their data to determine the final outcome.



Resolution Oracles

Only Oracles with a Collateral Weighted Accuracy Rating minimum of 0.95 and a standard deviation of less than 0.01 can operate as a Resolution Oracle. (These are initial settings to be calibrated).

This means that it is not necessary to select resolution oracles by some further process. Rather, the selection of resolution oracles will emerge naturally from the operation of the primary oracles themselves

Positive Accuracy Scores are not gained from Resolution activity therefore Oracles must participate and maintain a position as Primary Oracles to qualify for Resolution positions

Resolution Oracles provide data points for every Oracle contract they are attached to, but their data is not required nor revealed unless there is a collateral claim.

Resolution Oracle Collateral

At the point of a claim, Resolution Oracles provide additional collateral to the contract as a proportion of existing collateral. Inaccurate Resolution Oracles will share secondary collateral losses as described below but they have a distinct economic advantage over the Primary Oracles. Resolution collateral is determined by:

C: defined above as Collateral provided by Primary Oracles
F: the proportion of the Initial Fee charged for a Claim Fee set at 0.50
S: the proportion of QED tokens staked in the system.
C_r: Collateral provided by the Resolution Oracles

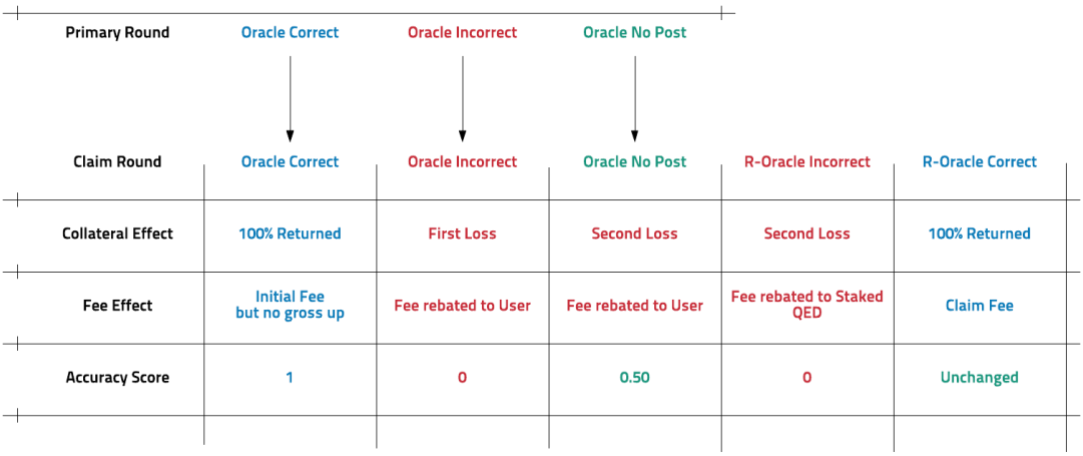
$$C_r = C \times (1 - S) \times F$$

Unless there are zero QED staked, Resolution Oracles post less collateral than Primary Oracles generating a better return on collateral.

Successful Collateral Claim

The customer receives 100% of contract Loss drawn from Oracle collateral and a fee rebate from Inaccurate Oracles. This results in a minimum 75% rebate in the current version and a lower net fee overall post claim.

The customer is thus given double protection. 100% of the actual contract loss is covered and at the same time a reduction in fee compensates for the nuisance of having to lodge a claim.



Oracles that were "Correct" through both rounds as to the final result, receive the initial fee charged (but no extra for inaccuracies since this is rebated to Users).

Oracles that end up as "Incorrect" take the first loss of Collateral loss. The excess loss remaining depends on the excess to the consensus threshold in the primary round.

Oracles that do not post a data point receive a 0.50 score for their Accuracy Rating.

Excess loss is shared pari-passu between Oracles that did not post a data point and Inaccurate Resolution Oracles.

Resolution Oracles that were Correct receive their claim fee. No positive accuracy scores are given to Correct Resolution Oracles, but Inaccurate Resolution Oracles are marked at zero accordingly.

Excess Resolution Oracle fees from Incorrect data are paid to QED token holders that are staked.

This ensures that all parties, customer, primary oracle and resolution oracle, are appropriately remunerated for their participation and penalised for any inaccuracies.

Credit and Syndication

It may not be practical for Oracles commercially to post 100% collateral once the system becomes larger and faster. A collateral market will develop for Oracles from external collateral providers akin to the performance bond market provided by insurance companies.

QED Token

Initial Circulation	400 Million
Adoption Issuance	600 Million
Cap	1 Billion

Quantity	Use	Circulation	Total Issue
250 M	Origin Treasury	62.5%	25%
150 M	Distribution	37.5%	15%

The QED token in version 1 uses Ethereum and other chains as settlement layers with UX Network as its scaling chain hub. Here, computation can be carried out with minimal resource costs.

Staking

The collateral requirement for Resolution Oracles is determined by the amount of QED that are staked.

Staking is done on a rolling 28-day basis and surplus fees from Inaccurate Resolution Oracle failings are paid to staked QED.

Critically, QED are not required to be staked as collateral as this allows "Death spiral" risk.

Fee Payments

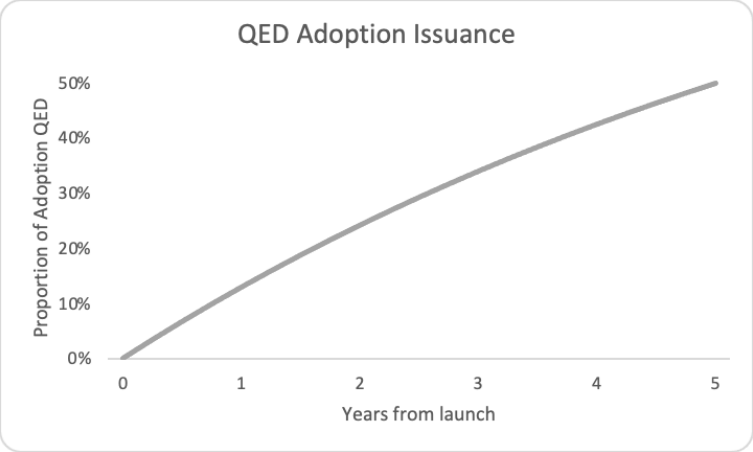
All fees are paid and settled in a mixture of QED and the currency specific to the contract. The proportion of QED is determined by (1-S) from the QED Staking amount. In extremis, at 100% QED Staked, fees are settled with no QED included.

Governance

As the system develops and matures, QED stakeholders, those bearing the risk of the model, should be responsible for its evolution and a voting structure will be implemented for QED token holders to make amendments to the model as they see fit.

QED Adoption Issuance

The residual 600 million QED are distributed following a negative exponential curve whereby 50% of these tokens are issued by the 5th anniversary of the token launch.



These tokens are shared equally between:

(1) QED Staked
(2) Oracles participating

- Distribution amongst Oracles is a function of their activity and respective Accuracy Scorings.
- QED Fees from inaccurate Resolution Oracles are distributed in the same way.

Since over time we envisage QED tokens to pass into the hands of Oracles since it is their collateral lever, the most accurate oracles will take ownership of the protocol over time.

Technology

The execution of the QED model is not blockchain specific but is designed to be flexible and fit for purpose. By being a multi-blockchain, it can avoid recursive congestion, seek the optimal venue for execution, and efficiently connect Oracles to smart contracts within a risk framework that has financial and commercial logic.

Furthermore, the QED model is designed to cater for customers that have generally selected the chain upon which they wish to operate. That decision is specific to their business model and their enterprise requirements.

Oracle Software: DelphiOracle

QED has been built as a successor to DelphiOracle, a DPOS-aligned oracle framework developed by Origin Ventures' principals. It currently powers algorithmic stablecoins, prediction markets and other applications on EOS Mainnet.

The QED protocol employs a Commit Reveal mechanism, where Oracles first during the Commit phase, publish a hash of the observed value together with a random nonce. During the Reveal phase, Oracles publish their actual value and nonce. This value and concatenated nonce must successfully hash into the previously submitted commit hash, in order to be accepted by the smart contract.

Customers of Oracle data should also run their own feeds as a verification mechanism to allow them to initiate claims against primary oracles should there be a discrepancy between the customer and the oracle feeds.

Resolution oracles also submit their commit hash during the Commit phase, but do not reveal their data unless a claim is made by the Customer.

Oracles' collateral remains locked until the end of the claim period, preventing multiple concurrent claims to the same capital. After the claim period is over (assuming no claim took place), collateral is unlocked and can be pledged again.

Token Form: ERC-20 Ether to UX Network Bi-Directional Bridge

The QED token is a dual ERC-20 / UX Network token, initially to be issued on Ethereum liquidity pools such as Uniswap. The token can be staked (locked) and unstaked (unlocked) via a trustless, permissionless bridge that connects Ethereum and UX Network.

By staking the token, the owner gains access to functionality on UX Network. By unstaking the token, the owner gets the ability to sell or transfer it on Ethereum.

The ETH / UX bridge works as a Simple Payment Verification ("SPV") client to both chains, where headers and schedule changes can be pushed by anyone wishing to perform interchain transfers. Bi-directional transfers of wrapped tokens are supported here.

To perform locking and unlocking actions, the smart contracts require the data of the specific transaction, minimal valid merkle proof paths, as well as cryptographically correct linkage of block headers to prove transactions on the correspondent chain. In addition, additional confirmation block headers must be submitted to provide sufficient guarantees of irreversibility to complete the proof.

The ETH / UX bridge is not limited to the QED token.

It allows for any ERC-20 or ERC-721 tokens, as well as for ETH itself, to be transferred between Ethereum (native token) and UX Network (under the form of a wrapped token), and vice-versa (native UX tokens to be represented as wrapped tokens on Ethereum.

Scaling Chain – UX Network

Launched in August 2020, UX Network is a high-performance, highly scalable, permissionless blockchain and smart contract platform. It has an advanced resource model and market facilities that provide long-term predictable resource costs (instead of relying on unpredictable gas prices).

It can also be used to support the execution of EVM-compatible smart contracts (such as those written in Solidity), as well as web3.js-compatible view functions queries.

In addition to providing sidechain scaling capabilities to Ethereum 1.0, 2.0 and other chains, UX Network supports smart contracts written in C++ and Rust, as well as a native WebAssembly runtime for maximum transactional throughput.

Oracle operations on UX Network can be performed directly by interfacing with the chain, or automatically via the oracle plug-in available to users of the UX Wallet.

https://uxnetwork.io/

Summary

QED creates a balanced commercial environment for Oracles and users to operate within decentralised protocols.

- The use of bonded external capital avoids systemic risk to Oracle customers.
- The model incentivises Oracle accuracy with dynamic incentives and capital efficiency maximising the system efficiency and performance.
- The QED token staking action correlates the utility value of the token to return on Oracle collateral.

QED employs a self-propagating credit rating for Oracles with dynamic internal reinforcement and no third-party subjectivity.