Lithium Finance
Litepaper v1

April 7th 2021

.

Steve Derezinski, sjd@mit.edu

Lithium Finance uses collective intelligence to price the unpriced.

ABSTRACT

Pricing information for private and pre-IPO companies, while highly valued, is difficult to accurately predict; it is private and infrequently updated. Imagine how powerful it would be if we could access all global analysts and brokers with unique pricing knowledge and incentivize them to provide superior pricing? How can we coordinate and share the best aggregate pricing information and reward all participants? This is the challenge that Lithium Finance solves by combining pricing oracles together with economic incentives to ensure honest information is rewarded and malicious information is punished. The result is accurate, frequent pricing information of virtually all hard to value assets: pre-IPO stocks, private equity, and other illiquid assets -- all accurately priced using Lithium Finance.

INTRODUCTION

Currently DeFi protocols are constrained by lack of pricing of real world illiquid assets. Off-chain collateral requires informed pricing in order to execute corporate actions such as investments, liquidations and mergers and acquisitions. Creating a network of accurate and incentivized pricing experts for these off-chain assets is **the critical missing link** in enabling DeFi's expansion from $77B+ to the real world assets of $100T -- a 1300X increase. At the same time, we aren't able to tokenize assets we can't price.

Lithium Finance's Pricing Oracle is a collective-intelligence version of platforms like PitchBook and Crunchbase, powered by cryptocurrency incentives which leverage the immutability of Ethereum's global asset rails for reliable delivery of quality information. In addition, the participating oracles develop a reputation which enhances their earning potential and rewards increasingly accurate information.

Lithium Finance leverages a convergence of multiple growth areas:

- Globally available asset rails on which any expert anywhere can stake and receive rewards.
- Immutable blockchains store permanent records of previous transactions for reputation.
- Experts can come from anywhere with only a smartphone required.
- Advances in cryptography and information theory that enable sourcing of information with minimal knowledge of its quality, other than the answer itself. i.e. no requirement for expert certification, source verification, etc dramatically reduces cost and opens access. Reputation is additive, not required.
- We attract users by creating market-based incentives to source data for the network and create value: we are fundamentally addressing information asymmetry in the private markets.

STAKEHOLDERS

Wisdom Node (Pricing Providers)

Experts who have knowledge in the latest pricing of private companies - they could be brokers, investors or anyone that is familiar with private market activities. A broker usually has the latest transaction prices of private companies. However, currently they have no incentive to disclose the pricing to industry peers, creating a very opaque market. Investors who have regular touchpoints with their portfolios also have better estimation on changing prices. We will explain the mechanism in detail on how to incentivize these Wisdom Nodes to provide the right data points.

Wisdom Querier (Pricing Seekers)

Crypto projects, investors, private equity firms, merger and acquisition investment banks, wall street analysts -- all of these firms are seeking accurate pricing information to make decisions. Aggregating a global mind-hive of information creates the best pricing available. These players will also provide feedback on the ultimate accuracy of the pricing information, leading to rewards for the most accurate.

PROTOCOL DESIGN

The protocol is designed with several key desired outcomes in mind. 1) Pricing provided by Lithium Finance is fair and not manipulated 2) An incentive mechanism for Wisdom Nodes to participate in the system 3) Privacy of data submission is safeguarded.

Dominate Truthful Peer-Prediction

Recent advances in peer-prediction capabilities allow us to query individuals to provide answers without access to the ***ground truth*** (an external answer with finality, i.e. stock price once IPO, or final score of a match). Previously, aggregating multiple users' opinions has been thought to require access to final answers (ground truth) -- but this is not the case. We can therefore select a set of Wisdom Nodes or aspiring Wisdom Nodes to answer questions in binary fashion (i.e. higher / lower or yes / no) or ternary (i.e. higher / neutral / lower) or categorically (i.e. <$10, $10-$20, >$20). From this set of Wisdom Nodes and their confidence staking, we can mathematically determine the best answer prior to disclosure of the future ground truth, giving us the pricing information we need during illiquidity. The mathematical combination of all answers allows common answers to reinforce each other and off-axis -- or non-correlated answers to cancel each other. This combination allows us to reward those participating in consistent results. In some cases where the eventual ground truth is revealed, the reward will be distributed on disclosure, meaning once an asset is priced in the market.

Modern peer-prediction theory has seen significant technical advances in recent years, starting with the original work of Miller, et. al [9], and more recently advanced to show how peer-prediction can be structured to uncover honest truth and also reward it, Kong, et. al [6]. The latest theories provide the background for a robust algorithm to predict prices from individuals. These innovations provide for a) simple questions and a finite number of samples to create credible, reliable answers to difficult questions. Building on these theoretical frameworks to include a global asset rail on which to build an oracle network is the opportunity Lithium Finance is developing.

The algorithm's core is based on calculating the determinant of answers after randomizing their sequence into a set of matrices. Based on a binary question (i.e. will the price be higher / lower than X), we can create two matrix of answer T_1 and T_2, each containing at least $> 2C$ answers, were C is the number of options (in this case, 2 for higher / lower). These sequences of answers are combined into M_1 and M_2 matrices, and the Payment ($Payment_i$) for the resulting sequence can be calculated as:

$$Payment_i = \sum_j^N \det M_1^{i\,j} \det M_2^{i\,j}$$

This has been proven [6] to simultaneously a) discourage and negatively impact incongruent answers and b) provide a strong reward calculation to encourage honest answers. See *Specific Rewarding Process* section for a visual of how the payments are calculated.

From Kong et. al [6], which states: *Main Theorem: When n ≥ 2 and T ≥ 2C, DMI-Mechanism is detail-free, minimal, individually rational, informed truthful, and dominantly truthful. In the normalized DMI-mechanism, every participant's expected payment is in [0,(1/C)^C].* This means that as long as we have questions with 2 possible answers (high / low, for example) and we have more than 2x those options of people answering the question (>4 in this example), we can calculate an always positive payout which will reward informed truthful answers. Extending this theorem to more optional answers (i.e. 5 or 10 price points, for example) means we'll simply need 2x (10 or 20) Wisdom Nodes to provide answers in order to calculate the correct payouts. These numbers are easily realizable and as the size of the network grows, so does the robustness and quality of results.

PoWS -- Proof of Wisdom Staking

The protocol will include a specific role for Wisdom Nodes to provide their expert information. They will answer a series of questions (e.g. regarding pricing of upcoming private stock) and will stake some of their tokens to signal confidence level. Initially we will airdrop tokens to an invited set of brokers to bootstrap the process. This will allow them to get started with zero crypto experience, creating a simple onboarding experience.

Reputation is an added incentive and enhancement to correctness over time. Initially individuals may have low or no reputation, but as their performance improves they receive a higher reward, all else being equal. The closer a Wisdom Node is to the final ground truth, the higher their compensation. In addition, the more an individual signals their confidence in the results (by staking more tokens) the more they earn, enabling a strong feedback loop to encourage positive, honest behavior.

Of course if a malicious actor decides to provide answers designed to manipulate, they might also decide to add a significant stake to their answer to maximize the impact. In this case, once the consensus answer or ground truth is uncovered, not only will the malicious actor's reputation be slashed, so will all of their stake. In the case of an attempt to collude with a number of malicious actors, the amount of funds required to stake plus the lack of direct influence (due to the random down-selection) means all of these funds will get slashed and the resulting answers will not be impacted. Therefore, the best action is to both answer honestly and stake your confidence.

Wisdom Nodes

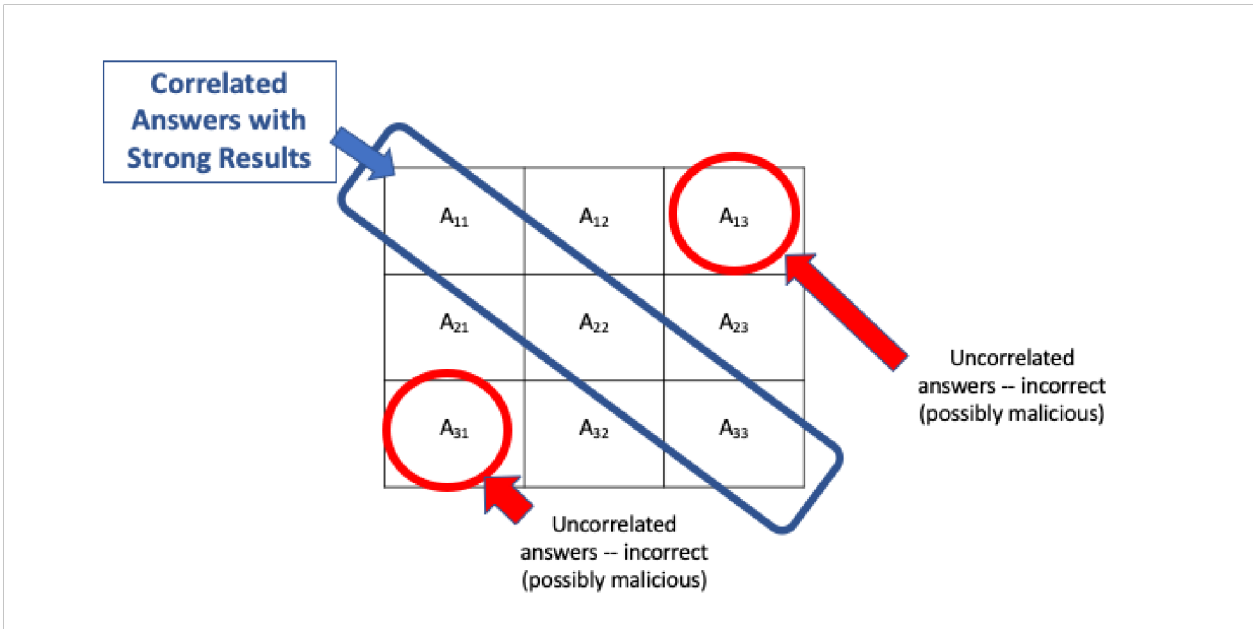
Brokers and analysts from all firms across the globe have access to the public information (reports, studies, analysis, historical performances, etc) on which to form their opinion about the price of an asset. Lithium Finance combines these views into a globally synthesized accurate price oracle. Given each stakeholder will act in their own best interest, we reward the information after the final price is determined (the ground truth) with Lithium tokens. By design, the protocol rewards honest actors and slashes malicious actors by rewarding those closest to the ground truth.

Wisdom Node Reputation

Because the transactions are all on-chain, the immutable record of performance by each actor is available for evaluation as any new answer is put forth. It becomes clear to the protocol that someone is a) stating their answer b) signalling their confidence by staking an amount of tokens and c) providing their reputation (as visible in their historical transactions) as evidence of their credibility.

Specific Rewarding Process

Once either the ground truth is known or the time limit is up, the answering process stops and the answers are aggregated and the solution is calculated using the DMI-Mechanism described above. The answers will be aggregated in a matrix form:



Where answers are in agreement they will provide strong values in A_{11}, A_{22}, A_{33}. These answers will receive the largest percentage of rewards and improvements to their overall reputation. Malicious answers will be

far from the central axis and mostly in the A_{31} and A_{13}, which will be negatively impacted meaning their stake will be slashed (and allocated to the honest pool) and their reputation slashed. Those in-between (minor-subaxis) will receive a smaller percentage of the overall reward pool and no change to their reputation (A_{32} or A_{12}, for example). It is challenging in these areas to delineate between malicious answers and random noise.

Data Privacy During Information Submission

It is important to make clear the data accessibility during the protocol interaction. When a question is posed, from that point on, no one knows the answers being submitted (except the individual submitting them). These are private to everyone except the protocol, which will aggregate results using a multi-party computation (MPC) technique to ensure global privacy. MPC injects randomness into the data flow such that any man-in-the-middle attack will result in zero information gathered. The results of this data will be further down-selected through a private and random selection process. Once all of the data is aggregated, the final price is published, (either via a ground truth revealing event or a timed event). At this point, rewards are sent out and reputations are updated. And finally, to ensure post-event audit confirmations of correctness, the sequence and path for the data will be disclosed. However for every epoch (an epoch starts when a question is posed to final disclosure of pricing information) the specific identity will be hashed to prevent a malicious actor from aggregating reputation information.

Flow of operations

Data Oracle -- Steps to create the pricing information are as follows:

Example 1: Pricing a pre-IPO company

1. A Wisdom Querier wants to know what a pre-IPO company might price on IPO. They pose this question to Lithium Finance and post a bounty, say $100 in Lithium Tokens.

2. Wisdom Nodes (Analysts, investors, others) provide answers and stake their answer to provide a confidence rating in their results.

3. Aggregated answers are pulled together and a subset of answers are selected blindly and randomly by the protocol (i.e. no one knows) to create the final answer. Once the final answer is revealed, the source is also visible to enable verification of valid answers. Final scores are calculated using the DMI-Mechanism algorithms.

4. Final answer is available on a regular basis, enabling frequent pricing of an illiquid asset.

5. Once the *ground truth* is revealed (pricing of IPO, for example) the rewards are paid out to those who were closest, and the reputations of the Wisdom Nodes (experts / oracles) are updated.

Note: this entire sequence from steps 1-5 is considered one epoch of Q-A.

Example 2: Finding the next-round valuation of a private company

1. A Wisdom Querier wants to know what the next private round will be priced at. They pose this question to Lithium Finance and post a bounty, *say $100 in Lithium Tokens*. In addition, a time period is selected for the answer, for example *by the end of next week*.

2. Wisdom Nodes (Analysts, investors, others) provide answers and stake their answer to provide a confidence rating in their results.

3. Aggregated answers are pulled together and a subset of answers are selected blindly and randomly by the protocol (i.e. no one knows). Final scores are calculated using the DMI-Mechanism algorithms.

4. This process runs until the deadline (*end of next week, in this example*) after which the final price is disclosed, the rewards are paid out to those who were closest, and the reputations of the experts (oracles) are updated.

Note: this entire sequence from steps 1-4 is considered one epoch of Q-A.

Example 3: Finding Daily pricing of a private company

1. A Wisdom Querier wants to know what the price per share of a private company is today, they pose this question to Lithium Finance along with a bounty, *say $100 in Lithium Tokens*. Daily time limit.

2. Wisdom Nodes (Analysts, investors, others) provide answers and stake their answer to provide a confidence rating in their results.

3. Aggregated answers are pulled together and a subset of answers are selected blindly and randomly by the protocol. Scores and reputations are updated and final prices are shown daily.

NATIVE TOKEN FOR LITHIUM FINANCE: LITH

Lithium Finance will issue its native digital cryptographically-secured utility token (**LITH**), to be used as a reward mechanism and as a staking token to indicate the user's confidence in questions and answers. During the process of posing a question and answering, each individual will stake a certain amount as either bounty (when asking a question) or confidence (when answering). This combination of staking creates stronger signals towards the best information. LITH is designed to be used solely as an interoperable utility token on the network/protocol.

LITH is a non-refundable functional utility token which will be used as the medium of exchange between participants on Lithium Finance in a decentralised manner. The goal of introducing LITH is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on Lithium Finance, and it is not, and not intended to be, a medium of exchange accepted by the public (or a section of the public) as payment for goods or services or for the discharge of a debt; nor is it designed or intended to be used by any person as payment for any goods or services whatsoever that are not exclusively provided by the issuer. LITH does not in any way represent any shareholding, participation, right, title, or interest in the Company, the Distributor, their respective affiliates, or any other company, enterprise or undertaking, nor will LITH entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. LITH may only be utilised on Lithium Finance, and ownership of LITH carries no rights, express or implied, other than the right to use LITH as a means to enable usage of and interaction within Lithium Finance.

LITH also provides the economic incentives which will be distributed to encourage users to contribute to and participate in the ecosystem on Lithium Finance, thereby creating a win-win system where every participant is fairly compensated for its efforts. LITH is an integral and indispensable part of Lithium Finance, because without LITH, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on Lithium Finance. Given that additional LITH will be awarded to a user based only on its actual usage, activity and contribution on Lithium Finance, users of Lithium Finance and/or holders of LITH which did not actively participate will not receive any LITH incentives.

The specific usage of tokens is set out below:

Bounty Offer from Wisdom Queriers to incentivise Wisdom Node answers

Wisdom Queriers would be able to spend an amount of LITH as a "bounty" to reward Wisdom Nodes for information. The more valuable information is to someone, the more they are willing to pay for an answer. In aggregate with many people wanting access to the same information, the bounty can become substantial.

Staking for Wisdom Nodes to signal confidence level of their answers

When each Wisdom Node provides an answer to the question, they will stake a certain amount of LITH tokens to signal their confidence. This together with their reputation within the sector of answers increase their influence and also entitles them to potential reward of the bounty (for correct responses) plus the stake of other incorrect Wisdom Nodes.

Reward for Wisdom Nodes for correct answers

Once the answers are known, the bounties of LITH and the Wisdom Node stakes are pooled and distributed according to how close their answers came to the ground truth. Conversely, malicious actors will have their stakes slashed.

In particular, it is highlighted that LITH: (a) does not have any tangible or physical manifestation, and does not have any intrinsic value (nor does any person make any representation or give any commitment as to its value); (b) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other digital asset) or any payment obligation by the Company, the Distributor or any of their respective affiliates; (c) does not represent or confer on the token holder any right of any form with respect to the Company, the Distributor (or any of their respective affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to Lithium Finance, the Company, the Distributor and/or their service providers; (d) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss; (e) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument, unit in a collective investment scheme or any other kind of financial instrument or investment; (f) is not a loan to the Company, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Company, the Distributor or any of their respective affiliates, and there is no expectation of profit; and (g) does not provide the token holder with any ownership or other interest in the Company, the Distributor or any of their respective affiliates.

Notwithstanding the LITH distribution, users have no economic or legal right over or beneficial interest in the assets of the Company, the Distributor, or any of their affiliates after the token distribution.

To the extent a secondary market or exchange for trading LITH does develop, it would be run and operated wholly independently of the Company, the Distributor, the distribution of LITH and Lithium Finance. Neither the Company nor the Distributor will create such secondary markets nor will either entity act as an exchange for LITH.

SYNERGIES WITH ALL DEFI PROTOCOLS

As the growth of digital securities and convergence between traditional finance markets and DeFi grows, the demand for pricing information for opaque assets will grow. More and more traditional financial companies are looking to digital assets and Lithium Finance *will operate across all sectors*, providing higher quality information to all traders, brokers, and investment bankers.

All sectors are available to Lithium Finance -- the only tool Wisdom Nodes need is a smartphone and a desire to earn money for their expertise. Wherever there is a market -- there is a need for Lithium Finance.

CONCLUSION

Lithium Finance is uniquely positioned to capitalize on a unique point of convergence between blockchain, distributed wisdom and the economic and technical engine to bring these forces together to pull the worlds of traditional finance and DeFi together, enabling tremendous growth and innovation at the interface. **Crowdsourcing has been a powerful tool for creating datasets that already exist but are distributed throughout the web—Lithium Finance takes this into DeFi by gathering collective intelligence from people who previously wouldn't give their expertise, but now have an incentive, to the benefit of the whole market.**

BIBLIOGRAPHY

1. Buterin, Vitalik. https://ethresearch/t/prediction-markets-for-content-curation-daos/1312.
2. "Forecast: A Community for Crowdsourced Predictions." *Facebook*, https://www.forecastapp.net/. Accessed 9 Mar. 2021.
3. George, William. "Kleros and Augur — Keeping People Honest on the Blockchain through Game Theory." *Medium*, 17 Apr. 2018, https://medium.com/kleros/kleros-and-augur-keeping-people-honest-on-ethereum-through-game-t heory-56210457649c.

4. Hogrefe, Victor. “The Oracle Problem.” *Medium*, 8 Sept. 2018, https://victorhogrefe.medium.com/the-oracle-problem-5611bed763ba.
5. Kong, Yuqing. “Dominantly Truthful Multi-Task Peer Prediction with a Constant Number of Tasks.” *ArXiv:1911.00272 [Cs, Econ]*, Nov. 2019. *arXiv.org*, http://arxiv.org/abs/1911.00272.
6. Lambur, Hart. “UMA’s Data Verification Mechanism.” *Medium*, 9 Aug. 2019, https://medium.com/uma-project/umas-data-verification-mechanism-3c5342759eb8.
7. Mandal, Debmalya, et al. “Peer Prediction with Heterogeneous Tasks.” *ArXiv:1612.00928 [Cs]*, Oct. 2017. *arXiv.org*, http://arxiv.org/abs/1612.00928.
8. Miller, Nolan, et al. “Eliciting Informative Feedback: The Peer-Prediction Method.” *Management Science*, vol. 51, no. 9, Sept. 2005, pp. 1359–73. *pubsonline.informs.org (Atypon)*, doi:10.1287/mnsc.1050.0379.