Amulet: The Decentralized Reputation Ledger

Andrey Lukatsky
Bachelor's in Computer Science
University of California, Berkeley
Berkeley, CA 94720
andrey@amuletplatform.com

Alex Lukatsky, PhD
Ph.D. in Theory of Functions
and Functional Analysis
Lomonosov Moscow State University
Moscow, RU 119991
alex@amuletplatform.com

Horia Margarit, MS
Master's in Statistics
Stanford University
Stanford, CA 94305
horia@amuletplatform.com

Adam Hooker
Bachelor's in Software Engineering
University of Advancing Technology
Tempe, AZ 85283
adam@amuletplatform.com

Abstract

The status quo for how financial market experts achieve compensation is fundamentally structured to produce low-quality, misguided advice. Many experts earn income by posting eye-catching content on websites that pay per one thousand impressions, like Seeking Alpha. In this model, entertainment-value outweighs accuracy and actionability of advice. Others receive affiliate compensation for promoting dubious investment opportunities that have no legitimate prospect of generating revenue. Low quality, misleading advice has been proliferated by individuals seeking to capitalize on these incentive models and this has gone unchecked by any significant negative consequences. Furthermore, in the status quo, experts in exclusive possession of a useful insight hoard their insight to avoid diluting their own ability to profit. The net effect, is that valuable advice is extremely scarce and impossible to tell apart from the noise.

Amulet solves this problem with the first of its kind Decentralized Reputation Ledger. Amulet incentivizes qualified experts to contribute verifiable predictions to the ledger, so that investors can observe how accurate they are over time. Investors can begin to filter out advice from experts who aren't right often enough for their liking. The incentive for market experts to participate is a large payout for the expert who correctly predicts an event contrary to the predictions of other experts on the Amulet marketplace. Experts are also able to tout their superior accuracy (verifiable by anyone via the blockchain) as a reason why their advice should command a higher premium from advice-seekers who subscribe to them via the Amulet Marketplace.

1 Introduction: Why The Market For Financial Experts Is Broken

When evaluating which cryptocurrencies to buy, hold, or sell, you're making a prediction about what will happen to the price of this coin in the future. You would benefit from a detailed prediction from a qualified expert to gut check your own, but where would you go for reliable predictions from verifiable market experts?

Currently, there is no service available for investors to audit a third-party market expert's track record. This leaves many investors in a catch-22: they need advice from individuals with different expertise than themselves, but they lack the expertise to validate the quality of these individuals. Even investors who are equipped to do this well, lack the bandwidth to do it repeatedly.

Now suppose you are on the other end - you are are a highly skilled financial market expert, and you want to profit from correctly predicting market outcomes. You look for services that will pay you fairly for your content, and discover that they all pay you based on how many impressions you generate.

You need a large following but what strategies will you employ to win over followers against the backdrop of dump scams, shilling, FUD and infeasible technology pitches being hawked by established, celebrity personalities? Unfortunately, the answer is to create sensational content to generate louder noise than your competitors. There is no financial incentive for you to publish accurate predictions, there are only incentives for winning over a large audience. This renders all current domains and services for market advice useless.

Amulet solves both the problem of verifiable expert predictions, and of discovering experts based on the quality of their expertise rather than their social popularity. The Amulet platform enables market experts to grow their reputation through a first-of-its-kind Decentralized Reputation Ledger. The Amulet Reputation Ledger will help investors discover the most objectively-qualified Crypto investment experts to follow based on the metric that matters most: how often they've been right.

We believe that blockchain technology is critical for the task of tracking reputations because trusted third-parties can be corrupted or biased by the very people it purports to rate. Only a trustless record of reputation like the Amulet Decentralized Reputation Ledger fits the bill.

So how does Amulet use blockchain technology to establish an objective record for experts? Amulet accomplishes this by treating financial market predictions in a similar way that Bitcoin treats hashing. Every prediction an expert makes costs the expert money before it can be published. This is like the investment a Bitcoin miner must make in hardware and electricity and time. But only the winning prediction will earn the payout from the pot. This is like the Bitcoin miner who only wins the block reward after successfully mining a valid block.

This is implemented through a smart contract which defines the Amulet token. The smart contract enables an expert to submit a cryptographic hash of their predictions once they pay a submission fee. This data gets immutably written to the blockchain along with a timestamp. The smart contract waits a predetermined amount of time until the prediction can be verified. After the time has expired and the prediction has been verified, market experts submit the plaintext version of their prediction to the smart contract and the hash is checked. The smart contract permanently records which experts were correct in their prediction on the blockchain, and rewards them.

Amulet therefore relies on blockchain in three crucial ways. First, it is built on the philosophy of economic disincentive from cheating, as famously pioneered by Bitcoin. Second, it implements the smart contract for the handling of prediction pay outs in a public, permissionless, and fully auditable blockchain. Third, it leverages crypto tokens to become the universal transaction medium for financial predictions, completely unrestrained from border controls, fiat currency exchanges, and manipulation from traditional corporate finance players.

We are envisioning a world in which investors begin to view an auditable history on the blockchain as a minimum requirement for experts. Many unqualified commentators have been getting a free pass, but Amulet is putting them on notice. If you can't stand behind your record of predicting crypto markets, then you will be disqualified from giving advice. Lenders don't extend credit to entities without a credit history, and we believe investors will stop listening to experts who don't have an Amulet reputation rank.

For real experts, this presents a massive new opportunity. They can finally prove their value - objectively - by displaying how often they beat the market through their skilled predictions. They can change the conversation from "I'm popular", to "I'm usually right", and this will help them both grow their following and justify greater compensation. They also gain access to an audience via the Amulet platform, and can publish their accuracy wherever they want.

1.1 Amulet Token and Amulet Platform

Our product offering consists of two products, broadly speaking. The first is the Amulet Token, which is an on-chain decentralized reputation management system. The second is the Amulet Platform, which hosts off-chain tools for advanced financial market predictions.

Amulet's token fully utilizes smart contract technology to become the universal medium for transacting financial predictions. It accomplishes this by requiring market experts to pay before they can respond to a request for a financial prediction (RFP), and similarly by requiring an investor to pay before they can receive the responses to an RFP. The details of the token and its implementation can be found in chapter 2.

The plaform provides more value to traders and experts beyond the token and Decentralized Reputation Ledger. This suite of best-in-class machine learning-powered data tools, provides real-time Market Sentiment Analysis and other crucial trading signals that have been promised by many, but delivered by few.

Amulet Platform is one of many future services leveraging the Amulet Token. The separation between token and platform is necessary to empower a booming economy for both market experts and for investors. This economy and its ecosystem is detailed in chapter 4.

Our platform provides a suite of market insight tools to enable market experts to formulate the best responses to any request for prediction (RFP), and to enable the receiving investors to validate the assumptions made by said market experts. Our platform also empowers investors to form syndicates to keep the cost per person low while enabling large payouts for correct predictions from market experts. Amulet Platfom and its implementation is detailed in chapter 3.

2 Amulet Token: A Cryptoeconomic Solution To This Trust Problem

2.1 Amulet Token: The Universal Medium For Transacting Financial Predictions

At a high level, this is how the Decentralized Reputation Ledger will work:

- Investors solicit time-boxed requests for prediction (RFPs) from participating experts.
- Experts pay with XAM to offer their predictions which are recorded with a timestamp on the blockchain.
- Investors pay with equal increments of XAM to receive exclusive access to the predictions experts submit pertaining to the RFP.
- All paying investors will get to see all of the experts submissions, and any investor who wishes to receive an expert's prediction without other investor interest can repeatedly buy in multiple times.
- After the timing specified in the RFP has transpired, a software oracle introduces data from real-world events pertaining to the experts' predictions so that a recording can be made of whether each predictions has come to fruition.
- Experts who made accurate predictions are rewarded in XAM tokens per the execution of smart contracts.
- When fewer experts are correct for a given RFP, the pool of XAM contributed by highest bidding investor and by all experts who answered the RFP is divided up between fewer winners yielding a larger payout.
- After an expert has answered many RFPs a picture emerges of how accurate they tend to be, in the form of their Amulet reputation rank.
- This rank takes into account: the recency of predictions made, the difficulty of predictions made and other factors.

- Experts who have recently started can choose when they wish to associate their account with their public-facing identity to showcase their Amulet reputation rank as a measure of their accuracy to their followers.

The Amulet reputation rank gives investors an objective basis to evaluate the merit of an expert and the advice they offer. The computation of this score is detailed in section 2.2.1. We envision that the market will eventually dictate that experts must participate in this objective scoring in the same way that creditors demand that lenders build up their reputability via a credit score. Both traders and market experts will benefit in this system. The following sections go over in detail the mechanics of how this Decentralized Reputation and its participants will operate.

See figure 1 for a high-level overview of the end-to-end process.

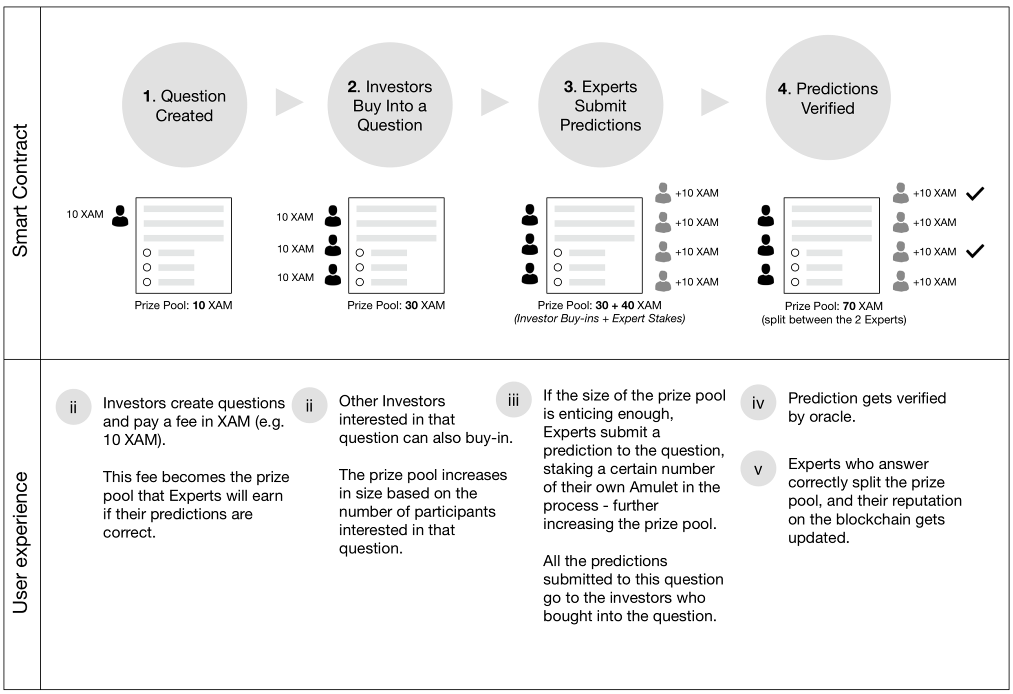


Figure 1: High-level overview of the end-to-end process for Expert Reputation Management

2.1.1 Users Deposit Amulet Into Reputation Smart Contract

All users (investors and experts) will first need to deposit Amulet Tokens into the Reputation Contract wallet. The Reputation Contract keeps a mapping of user addresses and balances. When a user wants to use a feature of the Reputation Contract, tokens are deducted from this balance.

2.1.2 Creating Requests For Prediction

Investors create requests for predictions (RFPs) related to specific topics in which they're interested. Creating an RFP costs a nominal fee in Amulet Tokens to disincentivize spam.

All RfPs will require buy-in by investors who wish to receive a response. This buy-in will be in equally spaced increments of Amulet tokens (eg., 10 XAM). After RFP creation, all the investors who wish to view the responses from market experts must pay some integer multiple of the equally spaced increment. This payment will get deducted from their token balance.

In order to ensure that the RFPs are measurable, Investors will be provided with templates that they can use. When the RFP is submitted to the Reputation Smart Contract, the RFP will also be verified off-chain (to ensure it's valid and measurable), and a "verified" flag will be set on the RFP within the Smart Contract.

Fields Within An RFP A request for prediction will have the following fields upon creation:

- Body - RFP text describing the outcome to be predicted
- Options - List of possible outcomes that may occur
- Buy-In Period - Date range where investors buy-in to receive the experts' predictions in the form of responses to a particular RFP.
- Prediction Period - Date range where experts can contribute their predictions as a response to a particular RFP.
- Event Date - Date when the outcome being predicted occurs and will be verified by an oracle.
- Buy-In Increment - The equally space increments of Amulet tokens (XAM) will vary in spacing from one RFP to the next based on the supply and circulation volume of XAM (eg., low circulation volume may yield buy-in increments of 1 XAM whereas high circulation volumens may yield buy-in increments of 10 XAM).
- Verified Status - Whether this RFP has been verified to ensure that it is measurable

2.1.3 Buy-In Process For A Request For Prediction

Once the RFP is verified, investors buy into the RFP during the Buy-In Period. When an investor pays with an integer multiple of the buy-in increment, the XAM is deducted from their token balance.

Investors send the following information to the Smart Contract when they buy into a response:

- Unique ID of the RFP - There could be hundreds of requests for predictions so investors must explicitly specify for which RPFs they're paying for a response.
- Integer multiple of the Buy-In increment - This quantity of the XAM will get deduced from their Amulet token wallet.
- Public Key - If this RFP receives responses from market experts, the public keys of all bought-in investors will be used by the experts to encrypt their responses so that only the paying investors will be able to view the predictions.

2.1.4 Experts Submit Predictions

After the buy-in period is over, Experts can choose to respond to an RFP by submitting a prediction. Experts are incentivized to participate based on the size of pooled buy-in increments from all the investors who purchased a response. This pool will get rewarded to the experts if their predictions turn out to be correct. If no market experts respond with predictions, then the investor buy-in amounts are all returned to the respective investors.

If Experts decide to submit a prediction, they send the following data to the Reputation Smart Contract:

- Hash of prediction concatenated with a 64-character random string (this secret ensures that adversaries can't determine the expert's predictions by hashing all the possible event outcomes).
- Encrypted prediction and the secret (same random string as above) using the public keys of all bought-in investors.
- Hash of explanatory text that describes how experts arrived at their answer (optional)
- URL of the text file containing the encrypted explanatory text using the public keys of all bought-in investors (optional)

The Investors who bought into receiving a response for this particular RFP are able to access all the predictions submitted by Experts in response to the RFP. Said investors can view the historical performance of each expert who offered a prediction, which will provide useful context if there is disagreement in the predictions. The Investor uses their Private Key (that corresponds to the Public Key that they submitted when they bought into this RFP) to decrypt each Expert's prediction (figure 2).

At first, only these Investor are able to view the predictions with which the Experts respond to the RFP - no one else, not even the Smart Contract, can view their predictions at first. After the Event Date occurs, Experts are required to submit their plaintext predictions to the Smart Contract for verification as described below.

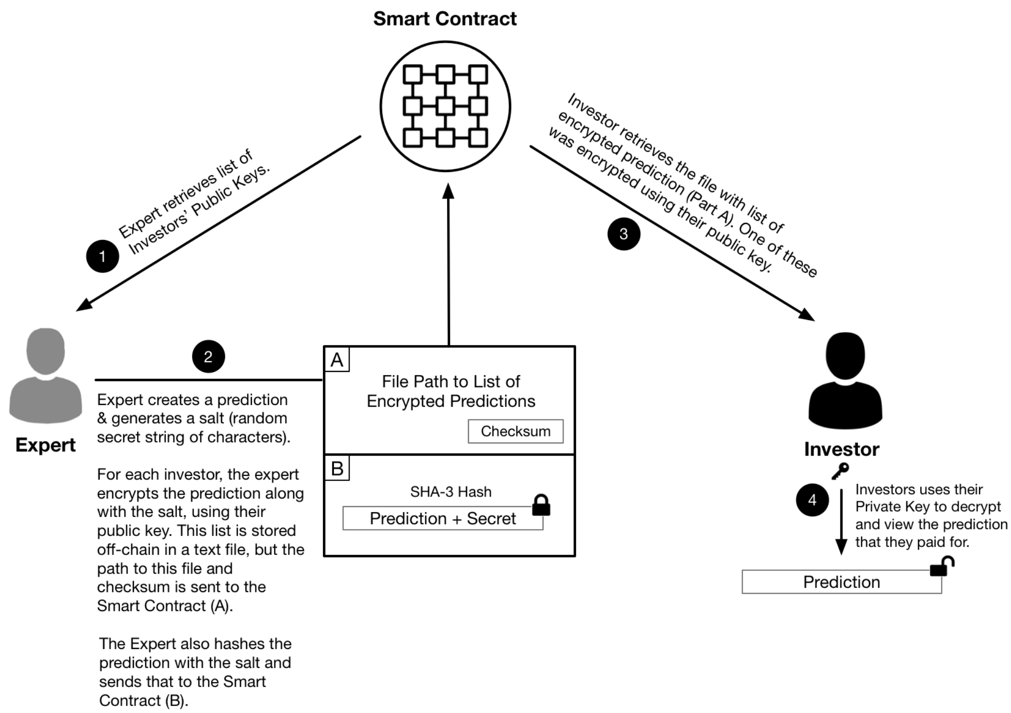


Figure 2: Experts submit predictions to the blockchain through the Smart Contract and anyone of the bought-in Investors reads them.

2.1.5 Expert Prediction Verification

After the Event Date occurs, Experts have 72 hours to submit their plaintext predictions along with the secret used during the hashing process to the Smart Contract, and a URL to text file containing their analysis (unencrypted; and optional).

72 hours after the Event Date, an Oracle performs the following actions (see figure 3):

- Using each Expert's plaintext prediction and secret, computes the hash and compares it to what the Expert submitted to the Smart Contract during the Prediction Period. If this doesn't match, the prediction is considered incorrect. The purpose is to ensure the Expert accurately reports the prediction she originally provided.
- Using each Expert's plaintext prediction and secret, along with the Public Key of anyone of the bought-in Investors, encrypts the prediction and compares it to what the Expert submitted during the Prediction Period. If this doesn't match, the prediction is considered incorrect. The purpose is to disincentivize Experts from predicting one outcome, but giving the bought-in Investors another.
- Verifies the actual outcome of the event using a Web API (e.g. Gemini API) and writes the result to the blockchain via the Smart Contract. If an Expert fails one of the 2 checks above, the Oracle will notify the Smart Contract and that Expert's answer will be marked incorrect.

After receiving the actual event outcome from the Oracle, the Smart Contract awards the Experts who predicted correctly with the prize pool as detailed in section 2.5, and the reputation of all participating Experts gets updated as detailed in section 2.2.1.

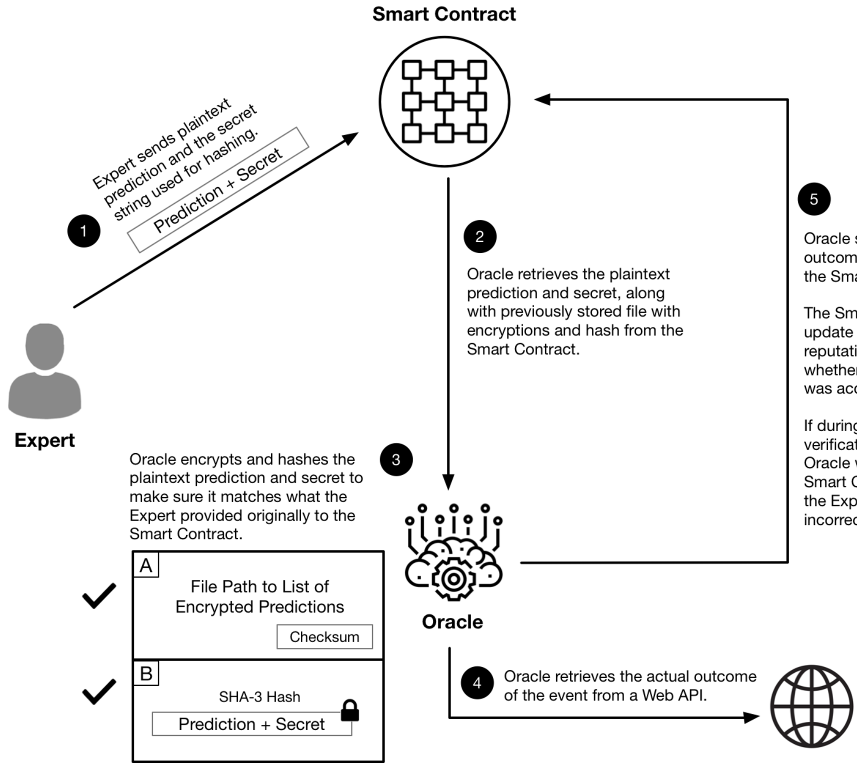
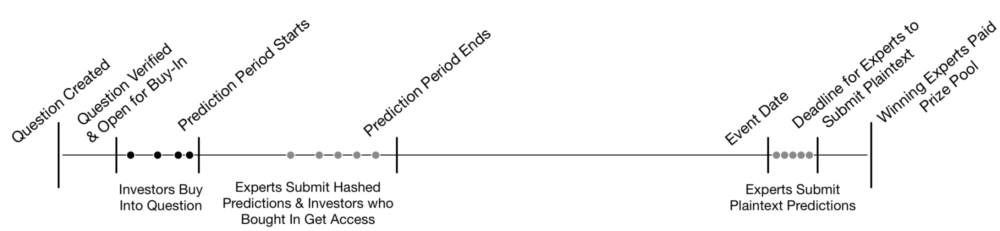


Figure 3: After the event occurs, Experts submit their plaintext predictions to the Smart Contract. An Oracle ensures that the plaintext prediction matches what the Expert previously reported, and records the actual outcome on the blockchain through the Smart Contract.

2.1.6 Order of Operations Recap



2.1.7 Scenarios

Common Case Investor Alice creates a question related to which cryptocurrency out of a list of 10 will appreciate the most in the next 2 weeks. She pays a nominal fee of 1 XAM to write this question to the blockchain. She buys in with 10 XAM. Alice's 10 XAM are held in escrow. An Oracle checks that her question is measurable and marks it as Verified.

Investor Bob sees her question and decides that he too would like to see the answer, so he buys-in with 15 XAM. Bob's 15 XAM are held in escrow, raising the value of the pot for a request to this RFP to 25 XAM. The buy-in period ends.

The Prediction Period begins. Expert Charlie sees this question and decides that the prize pool (25 XAM) is worth his time. He performs some analysis and comes up with a prediction. He also generates a 64-character random string (the secret in figures 2 and 3). Using the Public Keys of both bought-in investors (Alice and Bob), expert Charlie encrypts his plaintext prediction + the secret. Separately, expert Charlie hashes his plaintext prediction + the secret. He submits the encrypted prediction and the hashed prediction to the Smart Contract, along with the 5 XAM required to submit an answer. The prize pool thereby grows to 30 XAM. Another Expert Dave sees this question, comes up with a prediction, and performs the same steps, increasing the prize pool to 35 XAM.

Alice queries the Smart Contract to see that her question has 2 predictions. She retrieves the 2 encrypted predictions from the Smart Contract and decrypts them using her Private Key. Only Alice and Bob know their respective Private Keys, so only they can read the responses encrypted with their public keys. While reading Charlie and Dave's predictions, Alice uses the Amulet Platform to see how accurate Charlie and Dave have been in the past (as detailed in chapters 3 and 4). She realizes that although Dave has accurately predicted more events, Charlie has performed better with her type of question.

The Prediction Period ends, and everyone waits for the actual event to occur. For this specific question, the wait time is 2 weeks. After the Event Date occurs, Experts Charlie and Dave submit their predictions in plaintext to the Smart Contract.

An Oracle encrypts and hashes the plaintext to ensure it matches what the Experts submitted during the Prediction Period. If a mismatch is found, the Expert's prediction is considered incorrect. Charlie and Dave are honest and the check succeeds. The Oracle reports the actual outcome of the event after consulting a Web API to the Smart Contract (which of those 10 coins grew the most in 2 weeks).

The Smart Contract determines that Charlie was correct, while Dave was not. Charlie earns a reward as detailed in section 2.5. Charlie receives 35λ XAM where 1-λ represents the commission rate taken out by Amulet platform, and where the 35 XAM come from the 10 XAM in Alice's buy-in for the RFP plus 15 XAM in Bob's buy-in from the RFP plus the 5 XAM staked for each of the two responses to the RFP.

(Alice and Bob can either represent individuals or syndicates pooling money together)

Investor Submits An Invalid Request For Prediction Investor Alice creates an RFP that is not specific or measurable, "What crytocurrency is better?" She pays the 1 XAM fee and attempts to buy-in with 10 XAM, which gets held in escrow. An Oracle parses this RFP and compares it against a list of known templates. It determines that this RFP is invalid. The RFP gets locked and Alice's buy-in of 10 XAM gets returned to her. However, she forfeits the 1 XAM fee.

Investor Doesn't Receive Any Predictions Investor Alice creates an RFP and no Experts submit predictions. The likely cause is that the prize pool was too small (an insufficient amount of XAM was bought-in to entice any Experts). When the Prediction Period ends, any outstanding buy-ins are returned to the Investors.

Investor Doesn't Receive Quality Predictions Investor Alice creates an RFP that gets successfully verified. She buys-in to receive a response from the Experts, as do other Investors. Experts Charlie and Dave submit predictions that are of low quality. Alice and the other bought-in investors check the reputations of Charlie and Dave on the blockchain and know not to act on their predictions. Unfortunately, no other Expert responds to the RFP with a submitted prediction of acceptable quality.

When the Oracle submits the actual outcomes of the event to the Smart Contract, it turns out that both Charlie and Dave were wrong. Because no Experts predicted correctly, all of the bought-in investors XAM are returned, except for Alice's stake of 1 XAM for creating the RFP in the first place. The Experts do not receive any refund for their own XAM which they staked to submit a prediction.

Expert Doesn't Submit their Valid Plaintext Prediction After the Event occurs, Experts have 72 hours to submit their plaintext prediction. Experts Charlie and Dave realize that they predicted incorrectly. Charlie decides not to submit his plaintext prediction altogether, and Dave decides to submit a different plaintext prediction than the one he originally chose.

72 hours after the Event, the Oracle checks the blockchain for the plaintext predictions from the Experts. Because Charlie didn't submit any plaintext, the Oracle skips verifying his previously submitted encrypted string and hash. The Oracle knows that the Smart Contract will mark his prediction as incorrect because it is missing. For Dave, the Oracle attempts to compute the encrypted string and hash using the submitted plaintext. It doesn't match what Dave previously submitted during the Prediction Period, so the Oracle instructs the Smart Contract to mark Dave's prediction as incorrect.

In summary, the Smart Contract will mark both Charlie's and Dave's predictions as inaccurate, adversely impacting their reputation and returning the bought-in XAM to the investors but keeping the stake posted by the experts to respond to the RFP.

Expert Submits Their Own Request For Prediction Expert Charlie is very good at responding to RFPs related to the future of Litecoin. However, he doesn't see any RFPs related to Litecoin being posted by Investors. So he creates an RFP about it and posts it to the blockchain with a nominal buy-in amount of 5 XAM. Investor Alice sees this RFP, becomes interested, and buys-in for 10 XAM. At this time, the total prize pool for a response with a correct prediction is 15 XAM. At the end of the Buy-In Period, Charlie is satisfied with the potential prize pool and stakes 5 XAM to submit his prediction. If no other Experts submit a response, and if Charlie's prediction is correct, then he would earn 20 λ XAM. Where 1-λ is the commission of the Amulet platform.

Unexpected Event Occurs Between the time an RFP has been verified by the Oracle and the prize pool paid out, an unexpected event occurs that renders the RFP invalid. For example, the RFP is about a certain cryptocurrency and that coin ceases to exist. Another example is if an RFP asked to predict which of a set of 3 coins would growth the most, but they all grew the same. Well defined RFPs will ensure that these types of scenarios are rare, but they may occur. In these cases, the bought-in XAM will be returned to all bought-in Investors and all XAM staked by Experts to respond with a prediction will also be refunded to all responding Experts.

Expert Loses The Secret Used To Encrypt Their Submitted Prediction Expert Charlie decides to respond to a particular request for prediction (RFP). To submit his prediction, he generates a random secret string, concatenates it to his prediction, and encrypts and hashes it before sending to the Smart Contract. Unfortunately, Charlie forgets to save this secret. After the Event occurs and it's time to submit his plaintext prediction along with the secret, he's unable to do so. The most likely scenario is that the Expert's prediction will be marked as incorrect. However, there is some hope for Charlie. The bought-in Investors will have access to the secret key that Charlie used. If they cooperates with Charlie and send it to him, Charlie will be able to successfully submit his plaintext prediction and secret.

2.2 Ranking Reputation

Disincentivizing cheating the reputation system requires devaluing being correct on predictions on which many other experts are also correct. This devaluation is to prevent collusion, where two or more market experts jointly respond to the same request for prediction (RFP) in the same way. Sybil attacks are a special case of collusion, where a market expert colludes with one or more clones of herself.

Amulet platform therefore ranks the reputation of market experts as a percentile rank of their probabilities of correctly responding to an RFP. If you collude by giving good predictions to others (or to clones of yourself) then you're increasing the ratio of market experts who are scoring at least as high as you. By definition, a smaller ratio of participants scored strictly lower than you. Colluding has therefore decreased your percentile rank.

Percentile rank also ensures the Amulet platform is welcoming to market experts at all stages throughout the platform's life. This is because experts are not penalized for the number of incorrect predictions. Rather they are penalized for being outperformed by other experts.

Amulet token ensures that this percentile rank reflects the global participation of market experts. If a market expert responds to an RFP which was posted by another platform, she should be rewarded if few other experts responded correctly to that prediction. It would not be fair to only consider her responses to an RFP from a single platform.

2.2.1 Defining Reputation Rank With Fair Utility Estimates

Suppose we want a mathematically reusable representation of the performance of a market expert. One attempt at implementing this would be to estimate the probability that expert ℓ will yield a correct prediction on the j+N attempt, given their performance on the previous N prediction attempts for $j \in \{0, 1, 2, 3, 4, \ldots\}$. Formally,

$$\begin{aligned}
Pr\{\text{correct prediction}_{\ell,j+N} \mid \text{previous } N \text{ outcomes}\} &= \mathsf{E}\Big(\mathbb{1}\{\text{correct prediction}_{\ell}\} \mid \text{previous } N \text{ outcomes}\Big) \\
& \quad \frac{1}{N} \sum_{n=j}^{j+N-1} \mathbb{1}\{\text{correct prediction}_{\ell,n}\} \\
&= \rho_{\ell,j+N}
\end{aligned}$$

where you need to compute $\rho_{\ell,j+N}$ as a simple or exponential moving average to guarantee that high values remain high only if active participation and correct predictions are sustained. This is fair, because we want high ranking market experts who become lazy to lose their rank to hard working but relatively new market experts. The simple moving average is defined in 3.3.1 but is reproduced here for convenience

$$\begin{aligned}
\rho_{\ell,j+N+1} &= \frac{1}{N}\Big(\mathbb{1}\{\text{correct prediction}_{\ell,j+N}\} + N\rho_{\ell,j+N} - \mathbb{1}\{\text{correct prediction}_{\ell,j}\}\Big) \\
&= \frac{1}{N}\Big(\mathbb{1}\{\text{correct prediction}_{\ell,j+N}\} - \mathbb{1}\{\text{correct prediction}_{\ell,j}\}\Big) + \rho_{\ell,j+N}
\end{aligned} \tag{1}$$

Which yields the intuitive result that your $\rho_{\ell,N+1}$ decreases for every new wrong prediction if you used to make correct predictions. Similarly your $\rho_{\ell,N+1}$ increases for every new correct prediction if you used to make wrong predictions. But this probability is not the best score to use when ranking market experts because it does not account for the difficulty of an RFP.

Amulet assumes that the free market will price the RFPs based on difficulty. In other words, it assumes that a difficult RFP will provide enough value to the investors that they will bid higher and higher to have it answered by market experts. Therefore we can leverage the $\rho_{\ell,N+1}$ to define the expected monetary return of having a particular expert respond to a sequence of the M most recent requests for prediction. Formally, the expected monetary return for expert ℓ responding to the M most recent RFPs is defined as

$$\begin{aligned}
\mu_{\ell,j+M} &= \mathsf{E}_{\rho_\ell}\big(\boldsymbol{\theta}\big) \\
& \quad \frac{1}{M} \sum_{m=j}^{j+M-1} \frac{\theta_{m+1}}{N} \sum_{n=m-N+1}^{m} \mathbb{1}\{\text{correct prediction}_{\ell,n}\} \\
&= \frac{1}{M} \sum_{m=j}^{j+M-1} \theta_{m+1}\, \rho_{\ell,m+1}
\end{aligned}$$

where $N \quad M$ and where $j \in \{0, 1, 2, 3, 4, \ldots\}$ as before and where θ_{m+1} is the total amount of Amulet tokens available to be won if you correctly respond to the m+1$^{\text{th}}$ RFP and where the probability of market expert ℓ correctly responding is computed as before using a simple moving average of the previous N results. Factoring this to substitute the computed values $\rho_{\ell,m+1}$ is trivial and yields the simple moving average of the utility function over a window of the M most recent RFPs.

$$\begin{aligned}
\mu_{\ell,j+M+1} &= \frac{1}{M}\Big(\theta_{j+M+1}\, \rho_{\ell,j+M+1} + M\mu_{\ell,j+M} - \theta_{j+1}\, \rho_{\ell,j+1}\Big) \\
&= \frac{1}{M}\Big(\theta_{j+M+1}\, \rho_{\ell,j+M+1} - \theta_{j+1}\, \rho_{\ell,j+1}\Big) + \mu_{\ell,j+M}
\end{aligned} \tag{2}$$

Amulet then sorts the vector $\boldsymbol{\mu}$ containing the utilities for every market expert ℓ and reports their percentile rank. Meaning their reputation score will be the percentage of market experts who have a strictly smaller μ.

The percentile rank ensures fairness throughout the entire lifecycle of Amulet, because market experts will not be penalized if their raw number of correct predictions is low. Rather they will be penalized if other market experts are outperforming them.

2.3 Benefits to Experts

Participating in Amulet Predictor Scoring will: level the playing field for Crypto experts, simplify the task of marketing their services across the internet, and will help them achieve a fair market compensation from traders seeking their insights. Participating in this process also leads to direct compensation for each accurate prediction that comes true.

As the ecosystem of experts with Amulet Predictor Scores grows, the value of a given experts' advice will become quantifiable and directly comparable against other participating experts. This will allow the most accurate amongst them to monetize their insights more effectively than ever before. Market experts who establish a "winning-record" will be able to tout this objectively-measured credential internally, within the Amulet Marketplace to acquire paying subscribers. The most accurate experts will be discovered more often and will be able to charge more for their insights.

Experts who begin making predictions to the Decentralized Reputation Ledger will have their identity masked by default. This provides a riskless means to begin experimenting with the system. Over time if an expert chooses to link their performance to their public-facing persona. We enable this process via an irreversible unmasking.

The Expert signs with their private key to associate their public key and public facing Amulet username (and the prediction score attributed to this persona).

After this unmasking process, these experts will also be able to publish their score externally, to aid their efforts in acquiring an audience on any number of other platforms. We're building an embeddable widget functionality that can act as a trust stamp on forum posts, similar to VeriSign security trust stamps on e-commerce websites. These stamps will refer back to the Amulet website where an observer can verify their veracity.

The market is hungry for a way of comparing credibility of voices in public forums and so it is plausible that the presence of this widget (as part of a digital signature) will become expected and required to have your views treated seriously.

Standing out amongst other crypto market experts will no longer require competing for virality or popularity and will instead become as simple as publishing a favorable predictor score wherever you advertise your services.

In addition to these core benefits, experts will also reap the immediate benefit by receiving amulet token rewards when predictions they write to the blockchain come to fruition.

2.4 Economic Disincentives From Cheating Your Reputation

Amulet token requires market experts to pay before responding to a request for a prediction (RFP). This ensures that collusion (or Sybil) attacks become as expensive as the number of participating addresses in the attack. Payouts for correctly responding to an RFP decrease with the number of correct responses. Collusion or Sybil attacks therefore result in the same payout being distributed among more correct market experts, each one who had to pay to submit their prediction.

Case Study Eleanor clones her identity on the blockchain N-1 times to all respond to the same RFP with the same prediction (thereby launchin a Sybil attack). If her prediction is correct and there are M additional correct responses from identities not associated with her, then the total reward is split N+M ways but she also staked N times as many Amulet tokens to submit the N predictions. Therefore she would have earned a higher reward if she only submitted her prediction through one identity. That would have split the reward only M+1 times and she would have only staked Amulet once.

A market expert could also attempt to cheat their reputation, and win a payout without earning it, is to randomly guess at predictions when responding to an RFP. This might work if the payout on the rare occasion they guess correctly is high enough to exceed the costs of all the lost stake when they guessed wrong. Amulet's reward function as defined in equation 4 section 2.5 is proved to guarantee that the expected net payout from random guesses never exceeds the lost stake from the previous wrong guesses.

2.4.1 Amulet Platform's Net Payout Function Disincentivizes Random Guessing

Selecting predictions uniformly at random will cause the probability of correct predictions to suffer, as defined in equation 1 section 2.2.1. This will in turn cause the expected payout to be reduced as the payout is defined in equation 4 section 2.5.

The fact that investor and market expert identities are represented as public addresses to the Amulet token creates the attack vector for an individual to create many short lived identities and to have each one of them select predictions uniformly at random. Any short lived identity which randomly guesses responses to RFPs will have a poor probability of correctly responding, as it is defined in equation 1 section 2.2.1, because that probability is defined as a moving average of recent responses. However, this attack vector opens up the blockchain implementing the Amulet token to Denial of Service attacks.

It is therefore critical that the expected net payout from selecting predictions uniformly at random is strictly negative and decreasing. Such a property would ensure that a malicious market expert will eventually bankrupt herself by randomly guessing in response to a sequence of RFPs.

2.4.2 Proof: Expected Net Payout Of Random Guesses Is Always Negative And Decreasing

Let W_n be the net payout from selecting predictions uniformly at random for n consecutive RFPs. Then we desire a net payout function ψ such that the supermartingale property [4] strictly holds true $8n\ 2\ f1, 2, 3, \ldots g$ which implies that the expected net payout from selecting predictions uniformly at random decreases as the numbers of such responses increases.

$$\begin{aligned} \mathsf{E}\Big(W_{n+1}\ j\ W_1, W_2, \ldots, W_n\Big) &< W_n \\ &+ \\ \mathsf{E}\Big(W_{n+1}\Big) &< \mathsf{E}\Big(W_n\Big) \end{aligned}$$

Let the net payout function ψ for each response to an RFP be the stake posted by market expert ℓ to respond to the n^{th} RFP, subtracted from the reward function defined in equation 4 section 2.5. Formally, $\psi\big(\ell, n\big)$ is the net payout received by market expert ℓ upon responding to the n^{th} RFP after her reward was reduced by the stake she put up to respond. Observe that, for any ℓ and any n

$$\begin{aligned} W_{n+1} &= \psi\big(\ell, n\big) + W_n \\ \mathsf{E}\Big(W_{n+1}\ j\ W_1, W_2, \ldots, W_n\Big) &= \mathsf{E}\Big(\psi\big(\ell, n\big) + W_n\ j\ W_1, W_2, \ldots, W_n\Big) \\ &= \frac{1}{j\ \boldsymbol{c}_n\ j}\psi\big(\ell, n\big) + W_n \\ &= \frac{1}{j\ \boldsymbol{c}_n\ j}\left(0\ \lambda\left(b_n + \sum_{\ell} s_{\ell,n}\right) \quad s_{\ell,n}\right) + W_n \\ &= W_n \quad s_{\ell,n}\frac{1}{j\ \boldsymbol{c}_n\ j} \\ &< W_n \end{aligned} \tag{3}$$

because $\alpha_{\ell,n} = 0$ when the prior probability $\rho_{\ell,n}$ of a correct prediction by expert ℓ is no better than a random guess. A sequence of consecutive random guesses will result in $\rho_{\ell,n}$ being no better than a random guess, by definition, since $\rho_{\ell,n}$ is computed as a moving average as in equation 1 section 2.2.1

This strict supermartingale guarantees that the expected net payout from guessing randomly is negative and strictly decreasing. Put simply, a sequence of consecutive random guesses will bankrupt such a market expert.

2.5 Market Expert Reward Function Implementation

Amulet platform wants to strongly incentivize market experts who outperform uniform random selection of responses to a request for prediction (RFP). Highly skilled market experts will be incentivized to apply their skills to the most difficult RFPs through this weighting.

Given a bid from an investor b_n tethered to the n^{th} RFP and a stake $s_{\ell,n}$ posted by the market expert ℓ to respond to the same RFP, their reward is determined as

$$\alpha_{\ell,n}\,\lambda\left(b_n + \sum_{\ell} s_{\ell,n}\right) \tag{4}$$

where $\lambda \in (0,1)$ such that 1-λ is the percentage of the correct respondent's reward which the Amulet platform keeps for revenue and where $\alpha_{\ell,n}$ is the ratio of the investor pool plus staked predictions to pay out to the correct respondent based on how likely she was *a priori* assumed to correctly respond to this RFP.

The $\alpha_{\ell,n}$ are computed using the set of possible choices $\boldsymbol{c}_n$ for the n^{th} RFP and using the $\rho_{\ell,n}$ as defined using the moving average in equation 1 section 2.2.1

$$\alpha_{\ell,n} = \frac{\max\left(0,\phi_{\ell,n}\right)}{\sum_{\ell}\max\left(0,\phi_{\ell,n}\right)} \qquad\qquad \phi_{\ell,n} = \left(\rho_{\ell,n} - \frac{1}{|\boldsymbol{c}_n|}\right)\mathbb{1}\{\text{correct prediction}_{\ell,n}\}$$

Wrong answers cost the market experts their entire stake, which is redistributed to the experts with the correct predictions. Market experts with a recent record which is no better than random guessing are treated as having made incorrect predictions. This ensures that the expected payout from random guessing is negative and strictly decreasing as detailed in equation 3 section 2.4.2

Without the interplay of equations 3 and 4 in sections 2.4.2 and 2.5, respectively, a malicious market expert would have a chance at being profitable by merely random guessing in response to RFPs.

2.6 Proving Identity To Monetize High Ranking Reputation

Market experts who are highly ranked will benefit from unmasking their identity to enable monetizing their reputation through paid presentations and other means outlined in chapter 4. Amulet platform defines a market expert's rank as the percentile rank of their expected monetary return after responding to the M most recent RFPs, as defined in equation 2 section 2.2.1.

The unmasking of a market expert's identity is easily accomplished, should she choose to unmask herself. All she has to do is digitally sign content such as her website, podcasts, et cetera with the same private key she uses to sign her predictions + the secret when submitting responses to RFPs. Then when she wishes to prove her real life identity is the same as the market expert with the high reputation, all she has to do is provide the world with the public key which matches her private key. This public key will work in verifying the digital signatures of her content as well as of her predictions + the secret . . . thereby proving one and the same identity.

3 Amulet Platform: Transparent Syndication, And Evaluation Of Predictions

3.1 Amulet Platform's Suite Of Market Insight Tools

Empowering market experts to make verifiable predictions, with measurable financial value requires building a suite of market insight tools which is unparalleled in current offerings. Experts should have access to a custom search engine, tailored to their needs to segment the financial market by asset type, geography, and market signals such as momentum indicators and sentiment from reputable social media and finance discussion forums.

This same suite of market insight tools should be available to investors, so that they can verify the assumptions which underlie predictions they've purchased from market experts. The remainder of this chapter details the custom search engine, the momentum indicators, and the sentiment indicators.

3.2 Crypto Search Engine

Amulet team is building the world's first search engine dedicated to cryptocurrencies. Amulet team has built a distributed crawling infrastructure that monitors various crypto communities in real-time. It ranks the content based on the author's post history to determine its quality and likelihood of spam.

Investors and experts alike are able to stay up to date with all the latest social discussions that could have an influence on price.

3.2.1 Problems With Using Standard Search Technology For Crypto

The Amulet platform search engine is built on top of the open-source search library, Apache Lucene. The majority of enterprise level search appliances, including ones built on top of Lucene, score documents using TF-IDF weighting [6] to assign a weight to each term in a query.

Given a collection of documents D and a vocabulary V common across all documents in D, the TF-IDF weighting scheme [6] is defined as the number of times a vocabulary item $v \in V$ occurs in a particular document $d \in D$, divided by the number of documents which contain that same vocabulary item at least once. Formally

$$
\begin{aligned}
TF_{v,d} &= \text{sum}\big(1 \text{ for } w \text{ in } d \text{ if } w == v\big) \ / \ \text{len}\big(d\big) \\
DF_v &= \text{sum}\big(1 \text{ for } d \text{ in } D \text{ if } d \text{ contains } v\big) \\
TF\text{-}IDF_{v,d} &= TF_{v,d} \ / \ DF_v
\end{aligned}
$$

The intuition behind this weighting scheme is that words which are commonly used in all documents are not informative in distinguishing documents from one another. At the same time, words that occur only in a limited set of documents, but occur very frequently within those particular documents are likely indicative of the subject matter of those documents. Unfortunately, using only term statistics to identify relevant documents has major limitations due to the following reasons:

- Many cryptocurrency tokens designations are common abbreviations or acronyms in the English language such REP (Augur), GAS, SALT, and ICON. Achieving even moderate precision for these types of names is difficult using naive term frequency measures.
- Many ICOs have so-called "bounty programs" that financially incentivize users to post content about the particular coin. This artificially inflates the $TF\text{-}IDF_{v,d}$ because the participants of the bounty program publish meaningless content in specialized domains. The number of documents containing a mention to a cryptocoin will remain small while the number of mentions of that coin within the meaningless posts will be large.
- Social conversations on-line consist of a tree like structure where users reply to posts that occurred elsewhere on the page (or in the case of traditional forums, on a different page entirely). The context and meaning of the post changes substantially based on which post a user is replying to.

3.2.2 Improving Relevancy Through Social Signals

The Amulet platform search engine is designed specifically for social discussions and news articles about crypto. By tailoring ranking scores to this domain, Amulet is able to surface hyper relevant information about all major coins.

The search engine uses the following signals to rank relevant results:

- Posters history
- Freshness of content
- Likelihood of shilling

3.2.3 Enriching Data using Domain-Specific Models

The detection of named entities, such as financial ticker symbols, has the highest precision with a rules based approach (eg., regex). This approach also has the lowest coverage. Any misspellings or overloaded ticker symbols, such as REP, GAS, SALT and ICON, will be incorrectly ingested by the pattern match.

Low coverage results in missed market data and impoverished market forecasts. A better alternative is to train a machine learning model to predict the presence of a named entity of interest, simply by inspective the surrounding context of any given word position. Such a model is known as a named entity recognizer (NER) and it is a crucial component in the implementation of the Amulet platform crypto search engine.

NER enables the search engine to index all relevant market data. But providing rich market forecasts additionally requires identifying the sentiment of a post or a comment regarding a particular crypto asset. Amulet team has therefore built several machine learning models to classify the sentiment of a particular post or comment as negative, neutral / undetermined, or positive. These classifications of these multiple sentiment models are ensembled to provided the best mix of precision and coverage.

Ensembled sentiment classification is provided as a searchable index, and it is used as input to the price forecasting model which is custom and specific to Amulet platform, as described in section 3.4.

3.3 Momentum Indicators

Market experts often use the momentum of the price of an asset to filter out noise from short term market influences, and to infer the true market value of the asset. Investors should be able to compare the momentum of an asset's predicted price with any prediction from a market expert. If the momentum does not support the prediction, the investor should have additional tools to verify the claim of the market expert. Such a tool is the reputation rank of the expert as detailed in section 2.2.1. If the momentum does not support the prediction, and the reputation rank of the market expert is low, then the investor would be ill-advised to adhere to that particular prediction.

Amulet platform enables this level of objective verification of predictions submitted by market experts through a suite of market insight tools, which include the simple and exponential moving averages, the on-balance volume, the moving average convergence-divergence indicators and the relative strength index. The remainder of section 3.3 outlines how these quantities are computed and the intuition behind their definitions.

This entire section denotes a sequence of historical prices as $\{y_t\}_{t=1}^{\tau}$ and denotes the volume of transactions at those same times as $\{v_t\}_{t=1}^{\tau}$ up to and including time τ. It is also helpful to define a sequence of price differences as $\{z_t\}_{t=1}^{\tau}$ where $z_t = \frac{y_{t+1} - y_t}{y_t}$ for all t.

3.3.1 Moving Averages

Intended to be indicators of momentum, simple and exponential moving averages are the most fundamental of market insight tools built into the Amulet platform. They smooth out noise to give a clearer picture of the trend, eg., in an asset's price. The formulas which Amulet platform uses to compute these two are

$$SMA_\tau = \frac{y_\tau - y_0}{\tau} + SMA_{\tau\text{-}1} \qquad\qquad EMA_\tau = (1 - \lambda)\, y_\tau + \lambda\, EMA_{\tau\text{-}1} \qquad \lambda \in (0,1)$$

Where Amulet platform implements the industry gold standard of a burn-in period for the exponentially weighted moving average by defining

$$EMA_0 = SMA_T$$

and lets the investor, or market expert select their own $\lambda \in (0,1)$ and $T \in \{0,1,2,\ldots,30\}$ during their use of the Amulet platform market insight tools.

3.3.2 On-balance Volume

Intended to be an indicator of institutional money (sometimes called smart money), the on-balance volume is simply tracking the volume with a negative multiplier if the current asset price is lower than the previous asset price. When institutional investors sell (or dump) a large quantity of their holdings, the OBV takes a large dip, signaling a price drop. It is formally defined as

$$OBV_\tau = \begin{cases} OBV_{\tau\text{-}1} - v_\tau & \text{if } y_\tau < y_{\tau-1} \\ OBV_{\tau\text{-}1} + v_\tau & \text{if } y_\tau > y_{\tau-1} \\ OBV_{\tau\text{-}1} & \text{otherwise} \end{cases}$$

Where the fundamental assumption is that price is always determined solely by the order book supply and demand. This assumption leads to the conclusion that a flood of sell orders will always drive down price. OBV is therefore decreased if we see a price decrease, to reflect our belief that the price decrease was due to a flood of sell orders.

3.3.3 Moving Average Convergence Divergence

Arguably the simplest of technical analysis tools, the moving average convergence divergence is simply defined as the difference of a short term and a long term moving average. It is built in such a way as to indicate if the short term trend in an asset price is higher or lower than the long term trend in the same asset price. For example,

$$MACD_{\tau_1,\tau_0} = EMA_{\tau_1} - EMA_{\tau_0} \tag{5}$$

where the investor or the market expert decides on the size of the short term time window τ_1, and of the long term time window τ_0. The use of a moving average smooths out the noise of ephemeral spikes and troughs, giving you a clearer picture as to whether the recent price is indeed higher (or lower) than the historical trend.

The industry gold standard is to plot the $MACD$ with the short term moving average of the $MACD$ itself. This momentum of momentums is called the signal line, because a $MACD$ which is approaching its own short term moving average from above signals an opportunity to sell. It signals the short term moving average of price is decreasing below recently earned gains.

3.3.4 Relative Strength Index

Oscillators are also very important in determining the market value of an asset. They provide a bounded metric which can be universally applied to different assets such that a high value indicates an overbought asset while a low value indicates an oversold asset.

One of the most fundamental oscillators based on the momentum of an asset's price is the relative strength index. There are two parts to computing it. The first requires partitioning the sequence of price differences $\{z_t\}_{t=1}^{\tau}$ into a set S_- of only negative price differences, and into a set S_+ of only positive price differences.

Computing either the simple or the exponential moving average of the absolute values of each of these two partitions yields the relative strength for a particular time window. For example,

$$RS = \frac{EMA_\tau(|S_+|)}{EMA_\tau(|S_-|)}$$

Then finally computing the second part of the relative strength index requires bounding it between 0 and 100 by setting it to

$$RSI = 100 - \frac{100}{1 + RS} \tag{6}$$

And noting that, as the gains greatly outpace the losses in a specified time interval, the RS becomes ∞ which means that the RSI becomes 100. Similarly, if the losses greatly outpace the gains in a specified time interval, the RS becomes 0 which means that the RSI becomes 0.

3.3.5 Common Use Of The Momentum Indicators And Oscillators

Suppose Alice is a market expert responding to a request for predicting which of three crypto assets will be sold off (or dumped) within the next week. She might first look at the RSI of the first crypto asset and notice that it is squarely at 50, indicating neither overbought nor oversold. She might then check the SMA and the EMA for this particular asset and notice these momentum trend lines have been stable for a couple of weeks. Therefore Alice does not predict this particular asset as being dumped in the near future.

Now suppose Alice looks at the second crypto asset and sees it has an RSI of 90. This makes her suspect it will be sold off soon because the oscillator is indicating it is overbought. She checks the OBV and notices a cliff, indicating a large volume sell-off by an institutional player. Alice immediately flags this crypto asset as being dumped because she predicts the institutional sell off reflected in the OBV will trigger market panic, and others will follow in the sell-off.

Finally Alice looks at the third crypto asset and sees it also has an RSI of 90, but the OBV is seemingly stable. To double check, she looks at the SMA of the OBV itself and indeed it is stable. This indicates that, despite this third crypto asset being overbought, no institutional player is dumping the asset. Alice, being a seasoned market expert, then checks the $MACD$ and observes that it is approaching its own signal line from above. She immediately realizes what is going on: a very savvy institutional investor is avoiding market panic by quietly selling parcels of its holdings. Rather than causing a cliff drop in the OBV, this parceled sell off is slowly reducing the asset's price and gradually eroding the short term gains which originally placed the $MACD$ above its signal line. Alice anticipates that once the $MACD$ breaks down the signal line, the broader market will be tipped off and at that point panic will strike - inducing a sell off.

3.4 Forecasting Asset Prices From Descriptive Models Of Asset Returns

What if the request for prediction is not as simple as which of three particular crypto assets will be dumped within a week? What if the RFP asks which of five particular crypto assets will grow the most after two weeks (highest ROI in two weeks)? Then momentum indicators and oscillators are insufficient. What is required is a forecasting model which is interpretable and customizable by market experts.

Amulet platform provides such a forecasting model, where the rate of return of an asset at time t is defined as $r_t = \frac{y_t}{y_{t\text{-}1}}$ the ratio of its current price versus its previous price. Amulet platform follows the industry gold standard in assuming that r_t is Log-Normal distributed [5] with mean 0 and unknown standard deviation σ_t. Formally, let $z_t = \log\left(r_t\right)$ then

$$z_t \mid X_t \sim \mathcal{N}\left(0, \sigma_t^2\right) = \sigma_t \, \mathcal{N}\left(0, 1\right) \tag{7}$$

where X_t are the observations which are input to Amulet's forecasting model at time t. Knowing the price of an asset at time t, Amulet platform can forecast the price of the same asset at time τ by multiplying the consecutive returns of the asset with the initial price, and taking the $\log$ of the entire product to yield the identity

$$\begin{aligned} \log\left(y_\tau\right) &= \log\left(y_t\right) + \sum_{s=t+1}^{\tau} \log\left(r_s\right) \\ &= \log\left(y_t\right) + \sum_{s=t+1}^{\tau} z_s \end{aligned} \tag{8}$$

But the z_s in equation 8 are Gaussian random variables parametrized as in equation 7, therefore the forecast of the $\log$ of the asset price at time τ is a random variable sampled from a Gaussian distribution parametrized by

$$\log\left(y_\tau\right) \mid X_{t+1}, \ldots, X_\tau \sim \mathcal{N}\left(\log\left(y_t\right), \left(\sum_{s=t+1}^{\tau} \sigma_s\right)^2\right)$$

This makes sense because the model's uncertainty is expressed as its variance, which increases quadratically as the length of time of the forecast increases. Roughly speaking, doubling the time horizon of the forecast quadruples the uncertainty of the forecast.

A market expert's first choice might therefore be for how far into the future to consider the forecast reliable. Such an expert may wish to quantify a maximum error tolerance on the forecast and only forecast as far into the future as this tolerance enables. Such a strategy can even be incorporated by the market expert before deciding whether or not to stake her Amulet in response to an RFP.

3.4.1 Describing Asset Returns Using Only Observations X_t

Price ticker data may not be granular enough to obtain reliable estimates of the variance σ_t for small time windows. Or the price ticker data may not be available in overlapping periods of time with another ticker. Therefore a market expert may be unable to estimate σ_t for two different tickers during the same window of time.

Amulet platform leverages its niche crypto search engine, as detailed in section 3.2, to overcome these difficulties. It concatenates word embeddings, sentiment classification, named entity recognition, and other textually mined information into a row $\boldsymbol{x}_d^\top$ of numerical data representing some particular document $d \in \mathcal{D}$ indexed by Amulet platform's niche crypto search engine. It then groups all of the rows of numerical representations by time windows, such that X_t is a matrix of such rows for documents published within time window t. Each matrix X_t is assumed *a priori* to be the driver of the σ_t through the multi-linear mapping

$$\sigma_t = \left| \boldsymbol{\alpha}^\top X_t \, \boldsymbol{\omega} \right|$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$ are model parameters shared across all time windows. This implies the additional assumption of conditional independence $\sigma_r \perp \sigma_s \mid \boldsymbol{\alpha}, \boldsymbol{\omega}$ whenever $r \neq s$. Amulet platform fits the model parameters $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$ by maximizing the joint probability of the $\log$ of observed asset returns. This joint probability is concisely expressed as

$$\begin{aligned}
\prod_{i=1}^{n} \mathcal{N}\left(0, \sigma_i^2\right) &= \prod_{i=1}^{n} \sigma_i \, \mathcal{N}\left(0, 1\right) \\
&= \exp\left(-\frac{1}{2} \sum_{i=1}^{n} z_i^2 \right) \left(\prod_{i=1}^{n} \sigma_i \right) \left(\prod_{i=1}^{n} \frac{1}{\sqrt{2\pi}} \right) \\
&\propto \exp\left(-\frac{1}{2} \sum_{i=1}^{n} z_i^2 \right) \prod_{i=1}^{n} \sigma_i
\end{aligned}$$

Taking the natural logarithm and multiplying by -1 yields the negative log-likelihood function which results in the simpler and more numerically tractable objective which will be minimized by Amulet platform using an alternating least squares (ALS) algorithm

$$\begin{aligned}
\mathcal{L}\left(\{z_i\}_{i=1}^{n};\ \boldsymbol{\alpha}, \boldsymbol{\omega}\right) &= \frac{1}{2} \sum_{i=1}^{n} z_i^2 - \sum_{i=1}^{n} \log\left(\sigma_i\right) \\
&= \frac{1}{2} \sum_{i=1}^{n} z_i^2 - \sum_{i=1}^{n} \log\left(\left| \boldsymbol{\alpha}^\top X_i \, \boldsymbol{\omega} \right| \right)
\end{aligned} \tag{9}$$

where the z_t are the $\log$ of the observed asset returns for time window t with Gaussian distribution, as detailed in equation 7 from section 3.4. The optimization problem detailed in equation 9 yields reusable $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$ which Amulet platform can then apply to forecast the prices of a particular crypto asset using the random walk defined in 8 from section 3.4

The problems of lacking granular data or lacking data for two tickers in overlapping time windows are resolved using the time invariant (time independent) $\boldsymbol{\alpha}$ and $\boldsymbol{\omega}$ because Amulet platform's crypto asset forecasting model can now reuse those optimally fitted parameters on textually mined data from forums and discussion boards, even if it lacks granular and regular price ticker data.

4 Amulet Ecosystem

4.1 Amulet Integration Transforms Financial Expertise Into A Tradeable Commodity

Amulet aims to work with and enhance all systems that service the needs of Market Experts: tools for analyzing data, platforms to distribute content, and different ways for them to monetize. Third party systems have a strong incentive to accept Amulet tokens: reputation is ephemeral.

If a third party system uses Amulet tokens to seed the most reputable market experts, then pays them through a mechanism outside of our token, those market experts are no longer accountable. Without the ability to verify their reputation, the experts will find it financially lucrative to avoid the work that goes into making valid predictions and to instead cash out on their past reputation.

In a sense, the Amulet token is like open source software. The whole community benefits from contributing back to the token.

4.1.1 Market Insight Tools Empower Market Experts To Monetize Skill Not Popularity

Market insight tools are essential for market experts to create predictions. These tools allow experts to incorporate historical price information, sentiment, real-time news, social data and more into their analyses.

The same tools are also essential for investors, because they can leverage them to double check the assumptions behind any market expert's predictions. And who wouldn't want to reassure themselves before investing their hard earned money?

Today, there is no unifying platform for these market insight tools because there is no platform which rewards market experts based on verifiable predictions.

Amulet token enables this payment model, but it requires an ecosystem of platforms to integrate with the token. Amulet platform will be the first one-stop-shop integrating the Amulet token. It will therefore be the first comprehensive platform for market experts to monetize their skills instead of their popularity, and for investors to invest their money based on the expert predictions with confidence.

4.1.2 Integration Provides Transferability Of Reputation And Enables Network Effects

Amulet token is a globally open reputation management system. This is by virtue of it being an auditable smart contract on a public, permissionless blockchain. The benefit to integrating with it is therefore attribution.

Any platform which integrates with the Amulet token can attribute a market expert's predictions to their particular reputation. Regardless of what forum or other platform that expert used to monetize their reputation. This is beneficial to market experts, because their reputation is not dependent on the predictions they've submitted through just one medium, but rather it is based on all the predictions they've ever submitted anywhere. Amulet token integration enables market experts to freely transact their expertise on any platform at any time.

What prevents a platform from mining an expert's reputation from the blockchain without continually updating said expert's reputation by integrating with the token? Such a platform would be unable to monetize that expert's predictions based on accuracy. Market experts will prefer to retain the network effect and scale that Amulet token provides them. If they transact their predictions on a platform which doesn't integrate with the token, the market experts cannot transfer their reputation and work with other platforms. Investors will flock to other platforms which continually reassure them that their experts' reputations are being held to the standard of accurate predictions.

4.1.3 Monetizing A Global Marketplace Of Financial Expertise

Market experts can monetize their reputation of accurate predictions beyond the payout model of Amulet token. They can additionally publish content to a paying subscriber base, receive bids for paid public speaking opportunities, or form partnerships with other market experts.

Investors can also monetize the requests for predictions (RFPs) by forming syndicates (either with active investments, or passive investment counseling).

Any platform which integrates with the Amulet token can monetize the decentralized reputation ledger by fostering the monetization opportunities for market experts and for investors. Such a platform could sell the services necessary to form investor syndicates, or it could broker partnerships between market experts. Such a platform could also provide the hosting and publishing tools for podcasts by top ranked marked experts.

4.2 Open Platforms For Open Markets Of Financial Expertise

Enabling the rich ecosystem described in section 4.1 can only be accomplished by adhering to the quality and values of open-source software.

Amulet token embodies all of the core values of open source technology. The Decentralized Reputation Ledger and all its data is freely accessible to all. The value of Amulet increases as more people contribute to it (creating questions and predictions).

We are releasing an open source SDK to seed the Amulet ecosystem and enable it to become as robust as possible.

4.2.1 Amulet SDK

The Amulet SDK allows any third-party website, company, or user to leverage the Reputation Ledger to provide visibility into Experts on their platforms. This free and open source SDK allows any third-party to enable the following functionality on their website:

- Display any Expert's reputation score
- Allow Investors to create their own questions, browse existing questions, and bid on questions
- Allow Experts to submit predictions to questions
- Drill down into any Expert's prediction history
- Verify the identity of an Expert

The Amulet SDK allows anyone to use every aspect of Amulet in their own applications. In fact, the SDK powers all the functionality on AmuletPlatform.com.

4.2.2 Use Cases

Financial Blogs Any content platform that provides financial advice can use the Amulet SDK to display each author's prediction history and historical accuracy. Readers will have more confidence in the author's advice if the author is transparent.

Custom Reputation Ranking There are an infinite number of ways to rank Experts. The approach the Amulet Platform employs (and described above) is one of many ways to do it. The SDK allows custom ranking functions to be developed using the Reputation Ledger data. We envision a new industry being created with companies selling custom Expert ranking, so people can find the best Experts for their needs.

Trustless Verification If a user wants to see for themselves the track record of Expert (without trusting any intermediaries), they can use the SDK directly to query the blockchain and get all the information about any Expert.

Corporate Back Office Integration Companies who provide investment advice by employing a workforce of financial experts can integrate Amulet into their internal tools. For example, a company could require that each of its employees submit at least one prediction a week. The company could use the Amulet SDK to track which employees submitted predictions and offer them bonuses for being correct.

Investor Pools / Syndicates The SDK allows the creation of automated services to let Investors pool their tokens together and collectively bid on questions that the majority agree on. For example, a Web application could be built with the SDK that allows Investors to vote on questions to bid on and on some regularly scheduled interval, the app would tally the votes and submit a bid.

Desktop & Mobile Applications A third-party developer can leverage the SDK to create apps on any platform, allowing the growth of the platform to not be limited by the core Amulet Team.

References

[1] Hastie, Trevor & Tibshirani, Robert & Friedman, Jerome (2016) *The Elements Of Statistical Learning: Second Edition*. Springer. Stanford University.

[2] Bishop, Christopher M. (2011) *Pattern Recognition And Machine Learning*. Springer. University of Edinburgh

[3] Russell, Stuart & Norvig, Peter (2009) *Artificial Intelligence A Modern Approach: Third Edition*. Pearson Publishing. University of California, Berkeley.

[4] Ross, Sheldon M. (1995) *Stochastic Processes: Second Edition*. Wiley Publications. University of California, Berkeley.

[5] Rice, John A. (2006) *Mathematical Statistics and Data Analysis: Third Edition*. Cengage Learning. University of California, Berkeley.

[6] Witten, Ian H. & Frank, Eibe & Hall, Mark A. (2016) *Data Mining Practical Machine Learning Tools And Techniques: Fourth Edition*. Morgan Kaufmann Press.