Paying Salaries to Scientists Using Prediction Markets on Blockchain

Victor Porton – https://orcid.org/0000-0001-7064-7975

Abstract: It's described an applied technology to pay (fair) salaries to scientists and free software authors based on their forecast future "score" (such as the number of direct and indirect citations in a point of time in the future). Forecasting is doing using prediction markets. Prediction markets can be effectively used to transfer money from the future (provided we can predict the future well enough). The technology is being implemented in the Ethereum blockchain. It's considered a market solution of the problem to stimulate search engine owners to invest into scoring scientists. This system can be also used for carbon accounting and other common goods.

Introduction

The ideas first originate from my less formal writing [1].

The problem of scientists and free software authors not receiving the due reward for their work for the common good is well known. Many free software authors also work at a different job just not to die of hunger during creation of common good. Some die.

The problem is worsened by discrimination of various categories of people. One of the discriminations is the system of academic degrees (that is the purchased for money right to be paid for a work) that sometimes qualified well-working persons do not have.

Another problem is that the distribution of the reward inside the categories of scientists and free software authors is not just. Some projects dominate, other projects that could be perspective in the future are in monetary stagnation at the very beginning. That's because the distribution of reward is highly associated with the current success of a project rather than its future perspectives, because such perspectives are hard to value.

The author offers a blockchain-based solution to this problem.

Valuing of the future utility of a project is proposed to be market-based, to bring monetary incentives to many expert to value a project and for the best experts opinion to be weighted more than the opinion of an average person.

Prediction Markets

Prediction Markets can be defined as markets for future events. Such platforms make it possible to obtain, aggregate and process information of dispersed knowledge. Two different contract categories require differentiation: binary (reveal probabilities of occurrence) and indexed (reveal mean values of the underlying index). Both payoff types are present in the analysed dataset of this study. Binary contracts are stocks tied to events that either occur or do not occur at a specific date or time interval. Contracts pay off $1 (or $10, $100, respectively) in case an event happens, zero otherwise. A hypothetical example for a contract is whether or not the United Nations will impose additional sanctions against Iran before 31.12.2010, paying off $1 if the event occurs according to predefined sources within this interval; zero if it does not. A market price of $0.67 suggests that the last trading occurrence between traders implies a 67% probability of occurrence.

Indexed contracts pay out the corresponding value of an underlying indicator (e.g. stock prices, interest rates, exchange rates, GDP, industry-specific data, etc.) at a specific date or the mean over a specific range, respectively. A contract paying off $1 for each rounded thousand-digit of the Dow Jones Industrial Index at 31.12.2010 is an example for an indexedcontract/event. Assuming a value of 12,230 at expiry date this contract would pay off $12. The ex-ante market value (e.g. $8.71) reveals the market's mean value of what the market believes that value will be upon expiry. [2]

In this article I will consider exclusively "quantitative" (rather than yes/no) (for *indexed contracts* above) prediction markets.

"Conditional Tokens are a new, application-agnostic, asset class designed to facilitate the creation of highly liquid prediction markets. They enable combinatorial outcomes for high resolution information discovery through prediction markets." [3] That is conditional tokens is the blockchain way of facilitating prediction markets.

So condition tokens are guaranteed by the cryptographic logic of the blockchain to be exchanged for some other asset (*collateral*) proportional to the index values at the time (to be precise, after the time) of the event.

In fact, there can be multiple collateral currencies, but that does not matter much for our discussion, as in a free stable market they are just different representations of the same measure of value.

Prediction Market as an Estimation of the Future

My (probably original) idea is to associate future indexes (determined by a conditional token) in an indexed contract of a prediction market with users' monetary accounts (for example, with Ethereum addresses) while allocating each registered user (i.e. anybody

on the market) some supply of his (or her or institutional) "own" condition token (that he can later sell).

The simplest way to allocate conditional tokens to a registered user is to give him a fixed amount of tokens (e.g. 1000) once at the time of registration.

Another approach is to give a registered user amount of tokens proportional to the time since registration (or since some fixed moment of time in the past). In this case the amount of allocated tokens per unit of time may be constant or some function of time.

Let $f(u, c, t)$ be the total price (relative the the summary total price of all the conditional tokens in our set of conditional tokens) of the conditional token c at user u account at the time t.

Let $g(c)$ be the amount (relative to the entire market) of the collateral given (in the future) for token c.

The further theorems will assume a free market with gratis transfer of tokens. I don't try to formulate the "theorems" fully formally, but just use the well known facts about markets.

Theorem. If the forecast function g (let's denote it g_*) is the same for every market participant and every market participant buys/sells the conditional tokens in such a way that maximizes his collateral at the time of the event (provided that there are no other incentives or disincentives to transfer conditional tokens except to get the collateral in the future), then $f(u, c, t) = g_*(c, t)$ after a short period of time since the start of the trading. We assume the trade can be done quickly enough.

Proof. Suppose the contrary. Then there is a price discrepancy between the value (the desire to maximize the collateral) of the conditional tokens and the price of the conditional tokens. It causes the traders to compensate this discrepancy. To finish the proof we note that this kind of market is stable and therefore $f(u, c, t)$ quickly becomes equal to $g_*(c)$ (as it requires a finite amount of deals).

Corollary. Under the conditions of the above theorem, if a limit of $f(u, c, t)$ is taken on a set of markets with the "forecast" g_* approaching g then $f(u, c, t) \rightarrow g(c)$, provided that the market participants transfer funds quickly after each change of estimated g_*.

Proof. $f(u, c, t) = g_*(c, t) \rightarrow g(c)$.

Open problem. Prove the generalization of the last corollary if g_* is different for each market participant.

In other words, if the future is known well enough, then the price of conditional tokens is proportional to the future amount of the collateral.

"The **efficient-market hypothesis** (**EMH**) is a hypothesis in financial economics that states that asset prices reflect all available information. A direct implication is that it is impossible to "beat the market" consistently on a risk-adjusted basis since market prices

should only react to new information." [4] The same Wikipedia article states that EMH was widely criticized.

However, from EMH and the above theorem it follows that prediction market is the best mean people have to predict the future. I assume, it is really one of the best means. In any case, it is in a sense the most democratic or liberal mean: we can't easily choose an arbitrary person ("expert") to do predictions for us, because different experts have different criteria of how to choose other experts, but the market chooses experts for us, having it weighted as the most well behaving experts (in fact, traders) bear the most "weight" (money) in the system, instead of the "democratic" vote of average stupids.

Transferring Money from the Future

The above theorems imply that knowing the future well enough, the values of the conditional tokens at present are equal to the values of the collateral in the future (relatively to the sizes of the present and the future markets).

The collateral may be placed into the prediction market in the future, the conditional tokens can be used now. So, provided that somebody placed a collateral in the future, we can withdraw the conditional token in present, that is we have effectively a mean of transferring money from the future.

Give Nobel Prize for invention of time machine :-) Seriously, prediction markets and conditional tokens were well know at the time of this writing, but I am probably the first person who proposed very simple idea to associate them with users' accounts to facilitate transfer of money to these accounts from the future.

Well, there were known methods of putting money in the future and taking it now, e.g. bank loans and angel investment. But they don't provide equality (or approaching of equality) of the future put money to the money withdrawn at present, so they are not really "transferring money from the future". They also have a high threshold to entry.

Loans and investments unlike my method don't integrate a systematic method of estimating a future value, so they are arbitrary and thus inefficient.

Using Prediction Markets for Paying Salaries to Scientists and Free Software Developers

I would like to pay salaries to scientists and free software developers proportional to their future (e.g. after 100, 50, or 20 years) "score" (such as the number of direct and indirect citations of all publications of a scientist in the future). This would stimulate the science development.

We can set a prediction market for 100 years and gather donations of collaterals during 100 years to transfer that money from the future to present scientists.

It looks viable that in 100 years global donations will be enhanced compared to the present fragmented donations landscape. It looks viable that in 100 years we will have a global government that would use taxes or inflation to donate to this prediction market. It also looks viable that during that time the blockchain or blockchains maintainers will agree to allocate a share of miners' profits (effectively, a tax) to support this project.

Some investors may be reluctant to invest into a 100 years future. The reasons are:

- Many people are just not interested in future profits.

- A global disaster may happen, so it may make no sense to invest. (However, on the other hand, investing in the future may help to overcome a global disaster.)

- It is not quite sure that the current markets will survive after 100 years. (However, the planned implementation (using Ethereum blockchain, see below) seems to be so stable that it is likely to be well after 100 years, as the Ethereum network is currently the biggest network of validators of reliable, non-hijackable in very much foreseeable future transactions and is growing.)

- The values of collaterals may diminish or even go to zero. (However, the system allows to use essentially any Ethereum token as a collateral, with the current advent of interchain transfers, effectively any blockchain token can be used as a collateral. In my opinion (provided not complete collapse of the civilization), some of blockchain tokens will be well valued in near hundreds of years; so at least some of the donations will be valued at the time of "scoring".)

But for sure, there are investors wanting to invest into distant future. The value of something is determined by interested people, not by others; so, even if the amount of such investors is small (e.g. 5% of the total market value), the conditional tokens will be indeed valued by the market. 5% of potential of being invested into science is much better than effectively nothing invested at the global level now.

We should not pay the entire scientists' salary in one installment, because many scientists are scattered persons and could probably use the entire sum too quickly, before his token price reaches a reasonable value to sell. So the salaries should be paid in amounts proportional to the time since registration. (We could also choose the start time as the time of the launch of my system, but in this case future scientist would in a sense receive too much. Even better, we would choose the start of the scientific carrier as the point of starting count the salary, but we have no way to reliably check if the information about the time of the scientific carrier start is not fraudulent.)

Recalculation of the Salaries

The first version of my software had this bug:

Suppose a trader buys the salary of a scientist for 10 years. Then it probably makes sense for the trader to kill the scientist for him not to receive his token for the rest of his

or her life to increase the price of the held token. So I have created an incentive to kill scientists.

To overcome the problem, new version of the software has this feature:

Every time when a salary recipient makes an outgoing transfer, my software creates a new token that replaces the old salary token (the old token is then converted to the new one on the salary recipient's account).

This way the scientist does not receive the old token anymore, so its supply does not increase anymore, and thus the trader doesn't have this incentive.

Moreover I added the ability for anyone (including the salary recipient himself, traders, and anybody else) to recreate any salary token (just like the above), that is to effectively inform traders that they may recalculate the salary of this recipient.

Anyone's salary may be recalculated as often as it may happen (for a famous person it may be a few times per minute).

Salary recalculation make sense after a change of somebody's work performance (e.g. retirement or change of the job title). Also effectively stopping paying somebody's salary at his or her death can be done just by the usual salary recalculation procedure. (Previously I was going to give the ability to declare somebody dead to the DAO that is to procedures delegated by voters, what could be a source of a discrimination by declaring an alive person dead, e.g. by an elected dictator.)

It is possible to wrap/lock salary tokens in any time diapason "into" one new token to make outgoing payments convenient. Note that using this mechanism it's possible to recreate the situation with killing a salary recipient incentive, so the salary recipients should be warned not to use token contract in this dangerous way. (Just use my (to be created) contract for this purpose, probably not somebody's other.) It is similar to the common warning of not bequesting your funds to a potential killer.

The Ethereum Implementation

I am not an economist, I am a software developer. My purpose it to implement this plan in a real software.

I have chosen the Ethereum network for this, because it is the biggest platform for DeFi (decentralized finance) now and in the foreseeable future. With coming advent of Ethereum 2.0, it also becomes one of the most non-expensive means of financial transactions. Also, Ethereum 2.0 is going to support WebAssembly [5] for competitive to other platforms speed and energy-efficiency of execution, flexibility of used programming languages. (However, as EWASM is still not released, I use old EVM and Solidity. This system is not extremely computationally intensive, so it's OK.)

Incentivizing Search Engine Owners

The hardest problem (maybe, except of actually receiving donations) is to set up "oracles" that will (in the future) store in the blockchain the scores of the scientists. Designing and running oracles is complex and expensive. This task is comparative (and similar) to creating and running an Internet search engine.

My proposed way to solve this problem is to stimulate the market to pay to search engine owners to do the job for us. To do this, we allocate a portion of the money paid to the scientists to creators or oracles.

So, we are to give a share of the collateral to oracle owners. This can be done by giving them conditional tokens.

But the conditional tokens given to the oracles also require some oracle to asses their amount of the collateral in the future and moreover we need to decide which oracles we will use. I propose to use the weighted average of scientists' scores of the oracles as the amount of the collateral for scientists' tokens. To calculate this weighted average we also need to score the oracles themselves. So we need the oracle for the oracles or ion other words the prediction market of prediction markets. The score of the (first-level) oracles would be used both to distribute the collateral between oracles and for deciding of how much an oracle's weights for the salary of a scientist.

Clever (second-level) oracles are necessary to score every scientist objectively. But to bootstrap the scores of the oracles themselves it's enough to value the oracles in *some* way, as the choosing between several oracles is not a so hard task as scoring many scientists. So scoring oracles can be done just by a (future) voting. (It is an open problem whether current search engine owners will rely on a future voting about their profits.) We can set a voting system now, using for example a DAOstack [6] DAO (DAO basically means a system of voting in a blockchain). The voting could possibly (as the voting algorithm can be change in the future) take arithmetic average of each voter's choice of scores of the oracles as the oracles' scores.

In practice, this can be done by linking several prediction markets of different oracles together, with lower level oracles being "customers" of higher level oracles receiving collaterals from them (in the future). To make this work, we can allow everybody to redeem a collateral for himself or anybody else, so allowing anybody to redeem the collateral for the upper-level oracle before redeeming for a lower level oracle. This "automatically" makes the weighted average of lower-level oracles.

So, to bootstrap the market, it's enough to set one DAO as an oracle (deciding by voting).

Actual Implementation

The system [7] is mostly implemented in software. It remains:

- create a front-end interface for scientists (partly done)
- create the DAO (easy) and deploy the smart contracts
- test and audit the smart contracts for errors

It is implemented as a set of software repositories, most importantly:

- https://github.com/vporton/future-contracts/tree/salary

  - `BaseLock` – A base class to lock collaterals and distribute them proportional to an oracle result.

  - `BaseBidOnAddresses` – the contract that provides general "mechanics" of prediction markets associate with Ethereum accounts and to pay the condition tokens on user registration.

  - `BidOnAddresses` – the contract that specialized `BaseBidOnAddresses` for one-time payments of conditional tokens at user registration (unused by this project but provided for completeness).

  - `Salary` – the contact that specializes `BaseBidOnAddresses` for salaries paid in amounts proportional to the time since registration.

  - `BaseRestorableSalary` – the contract that specializes `Salary` provides means to restore lost accounts by some (settable by the global voting) mean. (Otherwise one error would cause the salary to be lost.)

  - `SalaryWithDAO` – the contract that specializes `BaseRestorableSalary` allowing to restore lost accounts by some (settable by the global voting) mean (DAO) and allows to allocate resources proportional to the salary of all the scientists to the DAO. (Otherwise one error would cause life-time salary to be lost.) Namely this contract is planned to be used.

All these contracts provide ERC-1155 collaterals and accept any ERC-1155 donations and "staking" as collaterals.

Contracts in https://github.com/vporton/wrap-tokens provide several different ways to "transform" between ERC-1155 and ERC-20 and ETH, because ERC-20 is the most popular token format now and needs to be usable with my system.

I am also working on contracts that allow to donate or bequest (to be allowed to be withdrawn in a point of the future) all (or some) funds on a smart wallet. It is to be done by allowing anyone to transfer the funds from this wallet (e.g. after a certain point of time) to our contract. Bequesting a smart wallet is also a way to bequest a DeFi token (e.g. company's shares) together with all its future profits.

So, unless 100 years pass, the tokens bequested to the system could be unable to take back only if the bequeathing person loses the ability to take them back e.g. by death or

by lost of private key (an Ethereum secret code). It is easier to persuade people to bequeath than to donate.

The development of these smart contracts is considered finished (however, the community feedback is welcome), and the only remaining thing is to audit them (carefully check for errors) by a trusted third party auditor. I make the contracts non-replaceable for a greater trust of traders.

The DAO

It is planned to use a DAOstack DAO. It can be easily implemented purchasing reputation for some donated token(s) (e.g. a ERC-1155 equivalent of Ether, the "main" Ethereum payments currency).

So voting weight of somebody depends on his amount of donated tokens and his behavior in the past. (Note that DAOstack allows voting to grant/strip reputation to anybody. It also allows to completely replace the voting algorithm as a result of voting in an old algorithm.)

The only function of the DAO is to nominate "attorneys" or attorney companies that are able to restore funds on lost accounts. (I remind that in a previous version of my software the DAO was also able to declare somebody dead.) I also give the users the option to go out of control of the DAO (in expense of being impossible to restore lost accounts).

Paying Publishers

At first, it seems that paying big salaries to scientists solves the problem of widely publishing important scientific discoveries (and likewise for free software packages), as the scientists would be able to pay for SEO or other kind of publishing, but:

- A scientist may for whatever reason not use his or her salary funds at all.
- He or she may just "live fast" and/or gamble the funds.
- He or she may pay a fraudster for publishing/SEO.
- He or she may deliberately neglect publishing, maybe to harm a science project.

The first solution of this problem that comes to mind is to allocate (by the future global voting) a part of funds to "publishers" (such as SEO companies). Maybe after 100 years there will be a way to value the performance of publishers (how much a publisher has advanced the science), but now apparently there is no: the best thing that comes to my mind is to pay the publisher for increasing currently accounted (as personal token prices) scores of scientists, but it seems this would make no other effect than creating economical bubbles. Even if after 100 years they will be able to calculate, it is useless, because traders need scores predictions now. But after a little more out-of-the-box think-

ing, it's clear that we don't need the silly (a struggle of opposite incentives between search engines and SEO companies) SEO business for this case: We could instead expect the future voting to redeem directly to search engines' "personal" tokens for fair publishing of scientific text: A search engine would acquire a "personal" token, publish its policy on the rating of scientific texts (e.g. by their currently traded "personal" tokens) and get a reward from the market based on such criteria as its fairness and search volume.

However, it requires to amend the proposed use cases: Instead of rating a scientist or an research institute (or free software, etc.) as a whole, we probably need to rate individual publications and individual editions of publications (search engines may use them as a rating criterion). This in turn creates the following problem: There would be both scientists' personal tokens and "personal" tokens of every publication, what: 1. duplicates the market operations; 2. complicates the scientists' tasks of trading away their salaries. So, the "personal" tokens of individual publications should go instead to a centralized fund of scientific publication, that in turn would distribute them to search engines. (So, we don't need to distribute funds directly by global voting to search engines, the fund will do it for us; however the funds can rely on the same DAO as the "main" global voting.)

Note that search engines have (at least) two-fold role in the project: acting as the future oracles and as benefactors of the publication fund.

Other Uses

The same system can be used for carbon accounting in the following way:

A carbon accountant (normally a corporation) can register in the system.

Then they account carbon and mint their own token to carbon reducers. The "personal" conditional token of the carbon accountant may gain value and they make their customers able to exchange their token for real value (or they pay to customers directly in a liquid currency).

Likewise it can be used for other common goods not specifically mentioned in this article.

Note that previously I developed another system for accounting carbon [8]. The system described in this article is more decentralized and therefore is expected to be more reliable to fraud (despite of advanced anti-fraud measured taken in [8]). The system [8] can be used together with this system.

Conclusion

It is created a sophisticated, well-designed, durable, fair global system for scientists' and free software developer's salaries and other common goods. Universities and govern-

ment funding of science, as well as proprietary software and patents are going to the past!

The system needs to be finished, deployed, and advertised. Need to start receive donations.

Donations Accepted

The project accepts donations in Ethereum:

https://gitcoin.co/grants/1591/science-of-the-future

We need about $3000 to audit (check for errors) the smart contracts and some amount of money to deploy it.

Bibliography

1: Victor Porton, Social Crypto Libertarianism (Not Capital), 2020
2: Diemer, Sebastian, Does money matter in predicting future events?, 2013
3: Gnosis Developer Portal, Gnosis Developer Portal Conditional Tokens · Create conditional tokens, a new asset class with richer informational capabilities that makes the outcome of any future event tradable, Retrieved 11 Dec 2020, https://docs.gnosis.io/conditionaltokens/
4: Wikipedia contributors, Efficient-market hypothesis, 5 December 2020 13:15 UTC, https://en.wikipedia.org/w/index.php?title=Efficient-market_hypothesis&oldid=992474133
5: Ethereum WebAssembly authors, Ethereum WebAssembly (ewasm), ,
6: DAOstack, DAOstack, 2019, https://daostack.io
7: Victor Porton, PREDICT PREDICTION MARKETS OR HIRE GOOGLE TO ACCOUNT SALARIES FOR SCIENTISTS AND FREE SOFTWARE DEVELOPERS, , https://reward.portonvictor.org/predict-prediction-markets-or-hire-google-to-account-salaries-for-scientists-and-free-software-developers/
8: Victor Porton, Carbon Flow, , https://github.com/vporton/carbon-flow