A Preliminary Research of Prediction Markets Based on Blockchain Powered Smart Contracts

Shuai Wang\textsuperscript{1,2}, Xiaochun Ni\textsuperscript{1,3}, Yong Yuan\textsuperscript{6,1,3} (Corresponding author, Senior Member, IEEE), Xiao Wang\textsuperscript{1,3}, Liwei Ouyang\textsuperscript{1,2}, Fei-Yue Wang\textsuperscript{1,3,4} (Fellow, IEEE)

\textsuperscript{1}The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China
\textsuperscript{2}University of Chinese Academy of Sciences, Beijing 100049, China
\textsuperscript{3}Qingdao Academy of Intelligent Industries, Qingdao 266109, China
\textsuperscript{4}Research Center of Military Computational Experiments and Parallel Systems, National University of Defense Technology, Changsha 410073, China

\{wangshuai2015, xiaochun.ni, yong.yuan, x.wang, ouyangliwei2018, feiyue.wang\}@ia.ac.cn

Abstract—Prediction markets are markets where participants trade contracts whose payoffs are tied to a future event, thereby yielding prices that can be interpreted as market aggregated forecasts. Past studies have shown that the prediction markets can provide accurate forecasts, sometimes better than sophisticated statistical tools. Due to their advantages, prediction markets have been widely used in the prediction of elections, project management, product quality, and impact of events. However, prediction markets also have some limitations, e.g., poor anonymity and limited market liquidity. In this paper, we propose to apply blockchain powered smart contracts to the prediction markets. First, we give a comprehensive overview on the prediction markets, including their theoretical basis, classification and applications. Second, we present how to design prediction markets based on smart contracts. Then, the algorithm of contracts implementation is proposed. Finally, in order to verify the effectiveness of the algorithm, an intra-enterprise prediction market is built based on a private blockchain. The experimental results show that the market can make accurate prediction for a particular event. In addition, the autonomy, self-sufficiency, and decentralization characteristics of blockchain make the prediction markets more efficient and robust.

Keywords—prediction markets; blockchain; smart contracts

I. INTRODUCTION

Prediction markets, sometimes referred to as “information markets”, “event futures” or “decision markets”, are markets that are designed and run for the primary purpose of mining and aggregating information scattered among traders, and subsequently using the information in the form of market prices in order to make predictions about the future events [1].

The prediction markets are somewhat similar to the stock markets: when the masses predict a company’s poor prospects, they scramble to offload this company’s shares and vice versa. However, prediction markets are more flexible than stock markets and their information gathering ability is more accurate and timely. This is because prediction markets have an incentive mechanism for traders to reveal and gather information, and traders can also express the strength of their beliefs for a specific event through the quantity of trading. In addition, there is a continuous, rather than passivated belief revealing mechanism in prediction markets that can react quickly to the external information through price changes.

To date, some academic institutions have established their own internal prediction markets, such as Vcon Lab at the University of Virginia, MIT Center for Collective Intelligence, Laboratory for Economics Management and Auction at the Pennsylvania State University, etc. Researches on emerging prediction markets indicate that they are the most efficient financial markets for predicting many types of events such as elections, movie revenues, corporate sales, project completion, economic indicators, even bin Laden’s demise. For example, compared with current major opinion polls on U.S. presidential elections, the prediction result of the famous Iowa Electronic Markets (IEM) is more accurate 451 out of 596 times [2]; When compared with the official prediction for HP printer sales, HP’s intra-enterprise prediction markets are more accurate 6 out of 8 times, even though the official prediction were made after the markets are closed and with knowledge of the market prices [3]. Thus, predict markets are expected to help governments, enterprises and other organizations to make effective decisions, allocate resources and hedge risks [4].

However, there still exist some problems in prediction markets nowadays, e.g., market manipulation, poor anonymity, low participation, etc. Aiming at these problems, in this paper, we propose to using blockchain powered smart contracts in the implementation of prediction markets. On one hand, given that prediction markets are markets where participants trading in contracts, they are very suitable for combination with blockchains, especially in the form of smart contracts (smart contracts are program code that self-execute complex instructions on blockchains). This is because the verification and clearing of market transactions can be automatically enforced by smart contracts. One the other hand, the decentralization, tamper resistance and anonymity characteristics of blockchain ensure that the prediction markets can operate in a transparent, conflict-free manner while avoiding the intervention of a central agency. At last, a
The prototype system of prediction market is established within a Chinese company to verify its effectiveness.

The rest of this paper is organized as follows. Section II gives an overview of the prediction markets, including their theoretical basis, classification, and applications. Section III describes the design of prediction markets based on smart contracts. Section IV presents the algorithm of the contracts implementation. Section V conducts experiments to validate the efficiency of the prediction market we constructed, then gives analysis of the experimental results. Section VI concludes the paper.

II. AN OVERVIEW OF PREDICTION MARKETS

In this section, we first discuss the theoretical basis of prediction markets. Next, we introduce the classification and applications of the emerging prediction markets.

A. Theoretical Basis

The theoretical basis of prediction markets is the information aggregation convergence and equilibrium mechanism, which mainly includes Hayek hypothesis, rational expectations theory, and effective market hypothesis.

- **Hayek hypothesis.** Hayek argued that the absence of complete information is a departure from the classic treatment of market efficiency. His fundamental argument was that no single authority could collect the requisite information to effectively manage society’s resources. However, the price mechanism, by creating signals that reward individuals who make the “right” decisions, is capable of doing so [5]. Wolters & Zitzewitz provided sufficient conditions under which prediction market prices coincide with average beliefs among traders [6]. They consider a trader with log utility and initial wealth , who must choose how many prediction market securities to buy at a price , given that the trader believes that the probability of winning his/her bet is , and this belief is drawn from a distribution . Thus, in deciding how many securities to buy, the trader solves the following problem:

\[
\max_{q \in \mathbb{R}} \quad q \cdot \log [y + x \cdot (1 - \pi)] + (1 - q) \cdot \log [y - x \cdot \pi]
\]

yielding:

\[
x^* = y \cdot \frac{q \cdot \pi}{\pi(1 - \pi)}
\]

The prediction market is in equilibrium when supply equals demand:

\[
\int_{-\infty}^{\infty} y \cdot \frac{q - \pi}{\pi(1 - \pi)} f(q) dq = \int_{-\infty}^{\infty} y \cdot \frac{\pi - q}{\pi(1 - \pi)} f(q) dq
\]

If beliefs and wealth are independent, then it implies:

\[
\frac{y}{\pi(1 - \pi)} \int_{-\infty}^{\infty} (q - \pi) f(q) dq = \frac{y}{\pi(1 - \pi)} \int_{-\infty}^{\infty} (\pi - q) f(q) dq
\]

Hence:

\[
\pi = \int_{-\infty}^{\infty} q f(q) dq = \bar{q}
\]

Equations (1) – (5) show that under log utility, the prediction market price equals the mean belief among traders. If wealth is correlated with beliefs, then the prediction market price is equal to a wealth-weighted average belief. In sum, market prices work as a quick and efficient means to aggregate information that are diversely held by individual market participants.

- **Rational expectations theory.** The rational expectations theory was first proposed by John F. Muth [7]. It is an economic idea that the people make choices based on their rational outlook, available information and past experiences. The theory suggests that the current expectations in the economy are equivalent to what people think the future state of the economy will become. To assume rational expectations is to assume that the agents’ expectations may be wrong, but can be considered as correct on average over time. In other words, although the future is not fully predictable, the agents’ expectations about the future are assumed not to be systematically biased. Then, Robert E. Lucas [8] further proposed the rational expectation equilibrium, in which the markets not only have the ability to gather information, but also can transfer information through the prices and quantity of the transactions. A person’s trading behavior in the market already contains his/her rational expectations of the future and of the others. Therefore, the equilibrium prices of the markets not only include information about the past, but also include the rational expectations of all traders for the future.

- **Efficient market hypothesis (EMH).** Efficient market hypothesis is a theory in financial economics which states that the asset prices fully reflect all available information. The EMH was developed by Eugene Fama [9] who argued that stocks always trade at their fair value, making it impossible for investors to either purchase undervalued stocks or sell stocks for inflated price. There are three common forms in which the efficient market hypothesis is commonly stated: weak-form efficiency, semi-strong-form efficiency and strong-form efficiency, each of which has different implications for how the market works. In weak-form efficiency, future prices cannot be predicted by analyzing prices from the past. Excess returns cannot be earned in the long run by using investment strategies based on historical share prices or other historical data. In semi-strong-form efficiency, it is implied that share prices adjust to publicly available new information very rapidly and in an unbiased fashion, thus no excess returns can be earned by trading on that information. In strong-form efficiency, share prices reflect all
information, public and private, and no one can earn excess returns [9], [10].

Beyond that, in Surowiecki’s best-selling book The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations, he pointed out that a diverse collection of independently deciding individuals is likely to make certain types of decisions and predictions better than individuals or even experts, which also provides a theoretical basis for prediction markets [11].

B. Types of Prediction Markets and Applications

Currently, there exists a numbers of prediction markets. In general, they can be divided into two categories: open markets and intra-enterprise markets.

- **Open markets.** Iowa Electronic Markets (IEM) and Hollywood Stock Exchange (HSX) are two typical examples of open markets. IEM is the longest running prediction market operated by the University of Iowa. IEM allows users to invest real money ($5 - $500) and trade in a variety of contracts whose eventual payoff depends on a future event such as political campaign, economic indicator or a company’s quarterly earnings. As shown in Fig. 1, over the 13 candidacies from 1988-2004, the average absolute error of the market-based forecasts was 1.6 percentage points, while the corresponding number for the Gallup Poll was 1.9 percentage points [12]. HSX is an entertainment market where users join for free and get two million Hollywood Dollars (HS, a virtual currency) when they first log in. Users buy and sell shares in their favorite movies and celebrities stocks with HS (they can trade with any information they find). Prices soar with a blockbuster opening at the box office and plummet with a bomb no one went to see. Leading traders are positioned on leader boards so that other traders are aware of what the market capabilities are and to give “publicity” to leading traders [4].

- **Intra-enterprise markets.** In the past years, Google has experimented with prediction markets in order to study information flows. Employees in Google bet on different issues, including how much demand there will be for a particular product or even how the company will do during a future time period. The study suggests that the trading is made among employees who sit very close or with social or work relationships. In addition, optimism is more prominent in the trading of newly hired employees [13]. Microsoft has utilized prediction markets to predict a number of issues, such as “will the company meet their schedule?” or “how many bugs will be in the new software?” [4], [14]. There are some novel applications of prediction markets in other corporations, e.g., GE elicit and evaluate new ideas in which is known as Idea Markets; British Petroleum (BP) turned to an Internet-based electronic market to aggregate decentralized knowledge, and trade emission rights internally to efficiently find the best ways to lower emissions [15], [16], [17].

III. THE DESIGN OF PREDICTION MARKETS BASED ON SMART CONTRACTS

In recent years, the development of blockchain technology has enabled customizable programming logic to be stored in a decentralized way. This has revived the notion and facilitated the creation of smart contracts. Smart contracts can be considered as the computer protocols that digitally facilitate, verify and enforce the contracts made between two or more parties on blockchains. Smart contracts can help users exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the service of a third party. Thus, prediction markets are particularly suitable for using smart contracts to construct. In this section, we first briefly introduce the smart contracts, then present the contracts design method of prediction markets.

A. Smart Contracts

Smart contracts were first proposed in 1994 by Nick Szabo who is a computer scientist, legal scholar and cryptographer. Szabo defined smart contracts as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises” [18]. Szabo’s original vision was to extend the functionality of electronic transaction methods, such as POS (point of sale), to the digital realm. Nowadays, with the emergence of digital cryptocurrencies based on blockchain technology such as Bitcoin and Ethereum, Szabo’s vision has come true.

Smart contracts are self-verifying and self-executing digital contracts with the terms of the agreements written in code. The code exist across a distributed, decentralized blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for central authorities [19].

Typical blockchain platforms such as Ethereum and Hyperledger Fabric embrace the idea of running user-defined
programs on a blockchain, thus creating an expressive customized contracts with the help of Turing-complete programming language. Smart contracts are expected to be widely used in many fields in the near future, including financial assets exchange, digital rights management, distributed file storage, Internet of Thing(IoT) [20], etc.

B. Contracts Design of Prediction Markets

The success of prediction markets, like any other markets, depend on their design and implementation. Three key design issues include contract types, trading mechanisms, and incentive mechanisms. We consider these issues as follows.

1) Contract types. There are three types of contracts, as shown in Table I [21].

   a) Winner-take-all contract: Such contract costs some amount $p and pays off, say, $1 if and only if a specific event occurs. The price represents the market’s expectation of the occurrence probability of an event.

   b) Index contract: The amount that the contract pays varies in a continuous way based on a number that rises or falls, like the percentage of the vote received by a candidate. The price of the contract represents the mean value that the market assigns to the outcome.

   c) Spread betting contract: In spread betting, traders differentiate themselves by bidding on the cutoff that determines whether an event will occur, like whether a candidate receives more than a certain percentage of the popular vote. The transaction price represents the median of the market’s expectation.

<table>
<thead>
<tr>
<th>Contract</th>
<th>Example</th>
<th>Details</th>
<th>Reveals market expectation of...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winner-take-all</td>
<td>Event $y$: Barack Obama wins the popular vote</td>
<td>Contract costs $p. Pays $1 if and only if the event occurs, otherwise pays $0</td>
<td>Probability that event occurs: $p(y)$</td>
</tr>
<tr>
<td>Index</td>
<td>Contract pays $y$ for every percentage point of the popular vote won by Barack Obama</td>
<td>Contract pays $y$</td>
<td>Mean value of outcome: $E(y)$</td>
</tr>
<tr>
<td>Spread betting</td>
<td>Contract pays even money if Barack Obama wins more than $y*%$ of the popular vote</td>
<td>Contract costs $1$. Pays $y$ if $y &gt; y^*$. Pays $0$ otherwise</td>
<td>Median value of $y$</td>
</tr>
</tbody>
</table>

2) Trading mechanisms.

   a) How to match buyers and sellers: The most common mechanism that matches buyers to sellers is continuous double auction, with buyers submitting bids and sellers submitting asking prices, then a trade is executed whenever the two sides reach a mutually agreeable price. In addition, there are some other mechanisms, e.g., parimutuel pools, bookmaker mediated betting markets, or implemented as market-scoring rules.

   b) How to state a contract: Contracts must be clear, easily understood and easily adjudicated. For example, the contract like “Whether there is extraterrestrial life?” is not appropriate. Instead, contract must specify whether such an event will occur by a certain date, like “Whether aliens can be discovered by 2030?”.

3) Incentive mechanisms. In a prediction market, it is essential to provide traders with sufficient incentives, in purpose of making them willing to using the private information they possess to participate in the trading activities. In some markets, traders get direct profit from the transactions, while others give bonus to those who perform well (Research shows that the enterprises’ prediction markets can be effective whether using real money or virtual money as a reward [22]). Moreover, monetary rewards are not an essential part of stimulating traders’ participation. For example, in Google markets, participants do not seem to quite care about cash prizes, but more on the reputational prizes (e.g., a Google T-shirt). Some research points out that just by showing the traders’ ranking in the system, the markets can have a good performance [23].

IV. THE ALGORITHM OF SMART CONTRACTS IMPLEMENTATION

In order to verify the effectiveness of the combination of the smart contracts and prediction markets, we build a prediction market within a Chinese company. The market is “Can Project A be finished before December 31, 2017? YES - NO”. For the purpose of facilitating the implementation, we take winner-take-all as the contract type, that is, the settlement price is ¥100 or ¥0, representing whether the users make the correct prediction. In this section, we will focus on the key algorithm such as contracts purchasing, contracts transactions, and contracts settlements [24], [25], etc. In the next section, we will analyze the experimental results.

A. Contracts Purchasing Algorithm

The set $\text{FurEvent} = \{f_1, f_2, f_3, \ldots, f_n\}$ is the event contracts released by the prediction markets. The contracts set $\text{UserEvent} = \{u_1, u_2, u_3, \ldots, u_k\}$ that the user purchased is a subset of $\text{FurEvent}$ ($0 < k \leq n$), namely, $\text{UserEvent} \subseteq \text{FurEvent}$. The algorithm sets a price fluctuation range price interval for each contract in order to verify that whether the bid exceeds the limit to avoid significant price fluctuation of the markets. The contracts purchasing algorithm is shown in Fig. 2.

---


1290
The algorithm first traverses the \textit{ListPurchase} which are sorted by \texttt{SortAsc()} function to get the highest price. If the number of a particular contract for selling is greater than or equal to the required number in \textit{ListPurchase}, then the transaction is facilitated and the purchase request in the \textit{ListPurchase} is deleted; otherwise, the \textit{ListPurchase} is updated according to the remaining contract number after the matching is accomplished. Finally, system updates the market prices, enter the next traversal.

2) \textit{Price matching}. The matching algorithm traverses the \textit{ListSale} which are sorted by \texttt{SortDes()} to get the lowest price. After the traversal is completed, if the number of trading contracts can not match exactly, the remaining purchase request is stored in the \textit{ListPurchase} that waiting to be transacted, as shown in Fig. 4.

\begin{algorithm}[h]
\caption{Contracts purchasing.}
\begin{algorithmic}[1]
\State \textbf{Inputs:} Event contract \texttt{f}, Price \texttt{p}, Purchase quantity \texttt{m}.
\State \textbf{Outputs:} Whether the purchasing is successful.
\State 1. \textit{BEGIN}.
\State 2. If \texttt{f} \in \textit{UserEvent}, then.
\State 3. Check whether \texttt{p} \in \textit{price interval};
\State 4. Compute the costs of the contracts: \texttt{cos} $\leftarrow$ \texttt{p} \* \texttt{m};
\State 5. If user account \texttt{acc} $\geq$ \texttt{cos}, then.
\State 6. Deduct \texttt{cos} from user account: \texttt{acc} $\leftarrow$ \texttt{acc} - \texttt{cos};
\State 7. Output True as successful purchasing;
\State 8. Else.
\State 9. Output Error since lack of money;
\State 10. Update prices of \textit{UserEvent} \texttt{f};
\State 11. \textit{END}.
\end{algorithmic}
\end{algorithm}

Fig. 3. The contract publishing algorithm.

\begin{algorithm}[h]
\caption{Price matching.}
\begin{algorithmic}[1]
\State \textbf{Inputs:} Contract sets \textit{ListSale} in the contracts trading center, the purchase price \texttt{p} and quantity \texttt{m}' of contract \texttt{e},
\State \textbf{Outputs:} Whether the matching is successful.
\State 1. \textit{BEGIN}.
\State 2. For each \texttt{ue} \in \textit{ListSale} that has been sorted by \texttt{SortDes();}
\State 3. If \texttt{m}' $\leq$ \texttt{ue.m}, then.
\State 4. Compute the costs of transaction: \texttt{cos}.
\State 5. If buyer's account \texttt{acc} $\geq$ \texttt{cos}, then.
\State 6. \texttt{m}' $\leftarrow$ 0;
\State 7. Deduct \texttt{cos} from buyer's account: \texttt{acc} $\leftarrow$ \texttt{acc} - \texttt{cos};
\State 8. Add \texttt{cos} to seller's account: \texttt{acc} $\leftarrow$ \texttt{acc} + \texttt{cos};
\State 9. Else.
\State 10. Compute the costs of transaction: \texttt{cos}'
\State 11. If buyer's account \texttt{acc} $\geq$ \texttt{cos'}, then.
\State 12. \texttt{m}' $\leftarrow$ \texttt{m}' - \texttt{ue.m};
\State 13. Deduct \texttt{cos}' from buyer's account: \texttt{acc} $\leftarrow$ \texttt{acc} - \texttt{cos'};
\State 14. Add \texttt{cos}' to seller's account: \texttt{acc} $\leftarrow$ \texttt{acc} + \texttt{cos'};
\State 15. Update prices of \texttt{ue};
\State 16. Output True as successful matching.
\end{algorithmic}
\end{algorithm}

Fig. 4. The price matching algorithm.
C. Contracts Settlement Algorithm

When the outcome of the contract event occurs, the system conducts the funds settlement. The winner will get ¥100 for each share due to his/her correct prediction, the loser get ¥0. The settlement algorithm is shown in Fig. 5.

Algorithm 4 Contracts settlement.

Inputs: Contract events results

Outputs: Whether the settlement is successful.

1. BEGIN
2. If a certain time is reached, then
3. Input contract results res ← {true, false};
4. Set SettlementPrice as SettlementPrice;
5. For each event r in ListEvent:
6. If r does not happen, then
7. Continue;
8. Else:
9. gains = SettlementPrice * ConNum;
10. User’s account: acc ← acc + gains;
11. Output True as successful settlement;
12. END.

Fig. 5. The contracts settlement algorithm.

V. EXPERIMENTS

We build a private blockchain based on Geth (Geth is a client software written in Go language that implements the Ethereum protocols) within one Chinese company, which supports the distributed transactions and information storage. The cryptocurrencies (tokens) are issued on blockchain. Each participant got some initial tokens that are the medium for making real-time pricing, trading, matching and clearing. The immutability and tamper resistance of blockchain ensure that the prediction results can not be manipulated and the anonymity of the transactions.

As mentioned before, the prediction market we construct is “Can Project A be finished before December 31, 2017? YES - NO”. The payoff rule was a simple winner-take-all type. One YES share is paid ¥100 if the project can be finished in time and ¥0 if not. Correspondingly, the No share is paid ¥0 or ¥100.

The market was started on November 1st and ended on December 31st, 2017. 50 traders joined the market and 42 became active traders. Trading hours are from 1 p.m. to 6 p.m. on weekdays. Fig. 6 shows the daily average contract prices and quantities traded in the market.

We can observe that the price has some fluctuation in the first month. However, since December 5th, there was a bullish trend for contract “NO”. In contrast, the price of contract “YES” had been declining ever since. This is because employees get some information that is not good for the project to be completed on time, such as lacking of funds and manpower. The final settlement price of the “NO” contract is 81 (representing traders think there is 81% probability that project A can not be completed on time) and the final settlement price of the “YES” contract is 39 (representing traders think there is 39% probability that project A can be completed on time). The end result is that the project A did not finish on time, which confirms the effectiveness of our prediction market.

After the experiment was finished, an exit poll was made among the participants. We found that more than half of the traders answered that they made overall profits in the market. It’s important to note that when asked “Will you participate in similar markets in the future again?” 82% answered they will. Hence it seems that motivation among market participants was quite high, although some of them lost some money.

VI. CONCLUSION

Prediction markets are forums for trading contracts that yield payments based on the outcome of uncertain future events. The markets have shown amazing prediction accuracy since they are first introduced in the 1980s, so they attract many researchers from economics, finance, political science, psychology and computer science. In this paper, we propose the combination of prediction market and blockchain powered smart contracts. We also deploy a private blockchain within a Chinese company and establish a prediction market on it to forecast whether a project will be completed in a timely manner. It turns out that the market accurately predicted the actual result. In addition, the decentralization, tamper resistance and anonymity of blockchain make the prediction markets more trustable, efficient and robust. In the future, we plan to conduct further investigations on the applications of prediction markets based on smart contracts, e.g., generate and evaluate new ideas in order to facilitate the information flows within the company. On that basis, we will further build various types of decentralized autonomous organization (DAO), decentralized autonomous corporation (DAC), and decentralized autonomous society (DAS) [26], [27], [28].
ACKNOWLEDGMENT
This work was supported by National Natural Science Foundation of China (71472174, 61533019, 71232006, 61233001, 61702519), Qingdao Think-Tank Foundation on Intelligent Industries.

REFERENCES