

XOR Protocol

Version 0.3

Abstract

The XOR Protocol is a financial system built on a public blockchain¹ that supports a unique class of markets and securities, which are more transparent, decentralized, democratic, and general than current systems. Examples include simple loans, mortgage bonds, and derivative markets such as Collateral Debt Obligations (CDO). XOR uses smart contracts to model any type of loan. Many markets can be modeled as debt contracts thus enabling a universe of potential XOR markets with the aforementioned benefits over their current analogs. All market transactions are recorded on the blockchain to ensure end-to-end transparency. An additional benefit of XOR's decentralized approach is the elimination of parasitic fees such as fees from third party credit ratings agencies, insurance providers, and centralized banks. Borrowers receive superior borrowing rates and lenders receive higher Return on Investment (ROI). Another important aspect of XOR is self governance and modularity. Actors in the system will be able to choose their own credit score implementations, insurance rates, risk models, and any other market variables. We can assume that any given model will not stay relevant for infinite time. XOR aims to rectify this by allowing democratized modularity in the creation and evolution of markets over time, since we can be sure that in the future at least one type of basic functioning model will exist. This flexibility is important in order to ensure that the XOR Protocol can adapt to future changes in market and real-life circumstances. In addition, the potential applications of the XOR Protocol are far-reaching, such as third-world microloans and startup fundraising for example. XOR will open doors to fair loans and credit access to people across the world by providing an accessible platform through which anyone in the world can create a market or invest in markets in a way that is transparent, distributed, fair, and flexible.

I. Introduction

1. Background

The 2008 Housing Crisis is well known to have triggered a global financial meltdown. Many factors contributed to the crisis, but two major causes were excessive risk-taking by large centralized financial institutions, and a lack of transparency on the part of these institutions. For the purposes of maximizing profit lenders, primarily large financial institutions, were incentivized to enter into mortgage contracts with borrowers who could not actually afford the mortgage rates over time, creating a market of immense risk. This was compounded by additional liquidity and market exposure from securitization derivative instruments such as mortgage-backed securities (MBS) and collateralized debt obligations (CDO). Under a system where issuers of CDO's and MBS's pay ratings agencies to rate the strength and weaknesses of the securities they offer, ratings agencies are incentivized to underrate the riskiness of securities, creating an opaque system where investors are unaware of the true riskiness of investments. Such securities were widely held by financial firms across the globe as they offered better returns than government securities,

¹ While XOR is currently based on Ethereum, the framework aims to be blockchain and DLT agnostic once other technologies mature and become interoperable with one another. In this context, "distributed ledger" is interchangeable with "blockchain".

but they also held attractive risk ratings. When US home prices declined sharply beginning in 2006, mortgage delinquencies soared causing a widespread devaluation of said securities triggering a full-blown international banking and financial crisis.

2. Solution

XOR solves the lack of transparency and the issues with the centralization of the financial system by employing a distributed and self-governed financial system. All transactions are stored on a public blockchain. This makes it impossible to misrepresent the riskiness of contracts because there is no one central party to determine and rate such loans. Anyone can check the ledger and verify the contents of a contract. This automatically allows for a more fair contract system for individual users. Moreover, it becomes possible to create derivative markets (and thus provide important liquidity to markets) in a transparent and scalable way that circumvents the issues faced in 2008. As XOR is decentralized, anyone in the world can make any market or derivative market. With additional governance structures participants can democratically achieve maximum system efficiency.

Another issue with modern financial systems is that once elements become entrenched in the system it becomes hard to improve upon them, even if such elements are harmful. For example, the mechanisms for calculating credit scores are entirely opaque, meaning that no credit borrower understands the process of calculating their own credit score. Additionally, credit scores reward some unspecified amount of debt exposure, and penalize having zero debt exposure. A system that encourages paying off debts rather than obtaining them would create a healthier financial society. However, it is possible that a future financial system could require a different approach to personal ratings. In this paper, we propose models that are transparent and scaleable. In spite of that, the core premise of XOR is the acknowledgement that no matter how good a model may be, it could become obsolete in the future. Keeping this in mind, our implementation is modular and thus future-proof.

XOR aims to provide a general financial framework that can encompass any market type. Examples include standard cryptocurrencies, stablecoins, physical commodities such as gold (eg. Digix), mortgages, car loans, etc. Ultimately, we wish to create a general and open protocol that will stand the test of time and last for as long as the concept of finance itself.

II. XOR Loans Overview

A loan on the XOR Protocol is different in that it utilizes decentralized approaches to centralized systems. This creates a fee-free structure, enabling better rates for borrowers and higher ROI for lenders by eliminating trickle-down costs found within traditional loans (eg. loan application fee, underwriting fee etc.). The two primary types of lending markets currently on XOR are Syndicated Loan Markets and Peer-to-Peer Loan Markets. With the ability to program a customized risk mitigation model as a Risk Mitigation **Instance Component (IC)** that can interface with a market, XOR allows for the possibility of integrating more sophisticated risk mitigation models as time goes on. Additionally, another key focus for the XOR Protocol is to enable stablecoin-denominated loans which does away with the consequences of taking or giving out a loan in a highly volatile cryptoasset.

1. Syndicated Loans

With the ability for a lender to distribute their capital over various different borrowers, Syndicated Loans form an important part of the XOR Protocol. Here an initial borrow request is split amongst

multiple lenders, and each lender separately earns interest on their lending amount. In a risk mitigated market loan, all lenders share responsibilities for loan defaults. Through the creation of a many-to-many relationship between lenders and borrowers in each market the default exposure for each lender is greatly reduced. Within Syndicated Loan Markets borrowers also have better chances of fulfilling their loan applications as long as they satisfy the necessary qualifying requirements and parameters of the market.

2. Peer-to-Peer Loans

Borrowers and lenders on the XOR Protocol also have the option to engage in one-on-one, peer-to-peer loan markets. Though these types of loans/markets lack the same degree of default risk mitigation as in Syndicated Loan Markets, it may be a good option for lenders who wish to take a more hands-on and personal approach to vetting borrowers (since it is much simpler to vet one borrower as compared to many in a Syndicated Market). It can also be a good alternative for borrowers who may be in search of an unusually large loan, extended lending periods, or other uncommon lending parameters.

3. Stablecoin Loans

Price fluctuations can be extreme in cryptocurrencies. In the context of loans such volatility can have far-reaching implications. For example, over the duration of the loan period, if the cryptoasset in which the loan is denominated has increased significantly in relation to fiat, the fiat value of the amount that the borrower must repay also increases at the same rate. This can put extensive strain on borrowers who choose to convert the cryptoasset in their loan to fiat near the beginning of the lending period. On the contrary, given a large dip in the cryptoasset's relative value to fiat, the fiat value of the repayment amount lenders collect is significantly lower. One way to mitigate this is to have loan markets based on stablecoin-denominated loans. Stablecoins are price stable cryptocurrencies that are pegged to some stable asset. For example, MakerDAO's stablecoin DAI is pegged against the USD at a rate of 1:1. Stablecoin-specific loan markets are important in XOR because they provide certainty and stability to a loan.

III. Markets

Markets within the XOR market were designed with the principles of generality, modularity, upgradability, and openness in mind. With the goal of fostering a vibrant development community surrounding the XOR Protocol, the process of market creation and the modularization of markets facilitates an open framework that invites developers to create their own markets, instance components, and integrations within the Protocol.

1. Market Creation

XOR is designed to provide a general and open financial framework and protocol layer that can encompass any market type. A market can be initialized by anyone with access to the XOR Protocol. Because XOR utilizes a smart contract architecture markets can be based on any asset that can be modeled as a type of monetary debt contract. Any of a market's parameters and components can be adjusted modularly enabling a range of different market architectures developed by third parties and the

open-source XOR development community. This allows for borrowers and lenders to experiment with a growing number of diverse market architectures thus allowing well-constructed markets to propagate and stand the test of time.

2. Market Components

The XOR Protocol is highly **modular** and **upgradable** by design. Every XOR market is made of small building blocks called market components such as identity, social staking, risk mitigation, trust score, interest and insurance rate calculations that can be added, edited/upgraded, and removed through market-level voting/governance. Each of these components takes the form of a delegate proxy smart contract that interfaces with **Instance Component (IC)** contracts programmed by third-parties and the XOR development community.

Markets are associated with a particular set of instance components at creation time. This modularity becomes a point of efficiency in that these instance component contracts need only be referred to by their contract address (both at market creation and in proposals to change/upgrade instance components). These contracts can be reused, and need not be redeployed onto the blockchain saving both storage and deployment costs. With an increasing number of these building block IC's available in the development community, the development of sophisticated markets will become easier over time. Writing entire markets from scratch while also taking security into consideration is impractical. However, on XOR, each instance component contract is expected to receive a greater amount of individual security and vetting thereby facilitating ease of development.

Actors are incentivized to participate in markets that use high-accuracy/effective instance components; those that consistently output proper identity verification, effective social staking, risk mitigation, trust score, and interest rates that justly reflect the underlying risk of the loan. This is accomplished by rewarding instance component creators based on the throughput² of markets utilizing said instance component. Having programmable components ensures that the XOR Protocol will never become stale as more intelligent implementations are discovered or the attitudes/needs of market participants change. Rather than accept permanence within a financial market, the XOR Protocol encourages healthy competition in order to find the most intelligence components that fit the needs of participants.

3. List of Customizable Market Parameters & Components

1. Underlying Crypto Asset - The cryptoasset with which the loans are conducted (eg. ETH, DAI, other ERC20 Tokens).
2. Duration of Request/Loan/Settlement/Collection Periods
3. Risk Coefficient - Parameter used alongside Trust Score IC to calculate interest rates for each borrower in market
4. Identity Component - Proof of unique identity for users within the protocol ensuring each user is accountable for their actions (More details below in Identity (V) section)
5. Trust Score/Social Staking Component - Trust Score is a representation of the trustworthiness of a borrower. It is used in the calculation of interest rates. Social Staking is a process through which a borrower can increase their Trust Score by having other users stake their Trust Score on them. (More details below in Trust Score (VI) section)
6. Interest Calculation Component - Used to calculate borrower-specific interest on their principal. Based on Trust Score.

² To be precise, throughput of markets will be measured as the total volume of repayments.

7. Governance Component - Dictates process in which decisions over direction of market is made (More details below in Governance (VIII) section)
8. Risk Mitigation Component - As discussed earlier, markets can decide how funds are distributed between lenders and borrowers. Examples include syndicated loans (many-to-many relationship between borrowers and lenders), simple peer-to-peer loans etc.

IV. Loan Procedure

Within a given market, we have designed a procedure for processing loan contracts. It is important to remember that loans are just a model for generic financial contracts. The loan procedure is processed within a round. Information for both stages are processed from individual and market level risk profiles. Investors may also process bids with Loan Intents which are contracts of automated contract selection logic.

1. Rounds

All markets operate in rounds which are composed of a request period followed by settlement. During the request period borrowers are able to request funds with a certain maturity date and maximum interest rate they are willing to pay. Lenders are also able to file loan intents during this period which contain a single vote for the risk coefficient used to calculate interest rates in the market (described in more detail below). Lenders and borrowers select markets which best fit their needs by looking at the market parameters. Market creators are rewarded for the success of their markets in the form of an XOR Value Token (XVT) reward, as mentioned below in the Cryptoeconomics section.

2. Loan Intents

To supply funds to a certain market an investor creates a Loan Intent with the specific amount of funds to be supplied, and the risk coefficient that the investor believes characterizes the current risk-reward profile in the market. The Loan Intent is essentially a pre-programmed instruction to automatically invest in a contract that meets certain programmed parameters.

If the investor is selected in the round they are issued a Debt Obligation Token (DOT) that represents the claim on the principal plus interest accrued at the end of the round.

If the investor is not selected to participate in the round (i.e. since the supply of credit exceeds the demand for credit, or all contracts are fulfilled), the funds are added to a queue within the market, and in the case that a lender inside the market decides to exit their position by selling their DOT's, the next lender request in the queue is accepted, and they become the new owner of the DOT and the loan itself.

3. Voting

An important element within each market round is voting by lenders and/or borrowers at the end of the collection period. During this period market participants have the opportunity to vote on active proposals (as outlined in the Governance section) for various components. The method in which voting is done is dependent on the Governance IC chosen by the specific market. This allows full democracy on all components within markets.

4. Insurance

In order to hedge against defaults the token mechanics within XOR ensure that lenders incur minimal losses depending on the risk of the market. By minting tokens to cover loans defaults in low risk markets with less minting for high risk markets, lenders are able to hedge their risk within markets ensuring limited risk.

5. Loan Market Exchange

XOR Loan Market Exchange is a decentralized exchange built on top of OX³ which allows lenders to exchange DOT's. This will consist of an order book of individuals offering to become lenders that will be ready to take over existing loans due to favourable market conditions for investment. This is essential for enabling flexibility for lenders and enabling them to exit a loan market early.

6. Portfolios

Portfolios in XOR, in a manner analogous to mutual funds in the traditional financial system, allow investors to organize their investments. Just as markets aggregate borrower requests, portfolios aggregate a user's loan intents. This additional layer of abstraction allows XOR to natively support investment diversification (since each market represents a relatively consistent risk profile) so holding a portfolio with many different markets constitutes diversification.

Just like a mutual fund it is possible for many lenders to invest in a single portfolio which simply means that each investor creates loan intents in the same markets and supplies funds to each market in the same proportions. This allows layman investors who are not capable of analyzing the individual risk-reward profiles of individual markets, as well as investors who do not have the time to construct their own portfolio, to choose a suitable portfolio to invest in out of the current well-performing portfolios. As with everything in XOR, the performance of a portfolio is completely transparent; statistics on past returns and losses can be computed by any user since historical information on the underlying markets is freely available. Finally, as portfolios represent a group of investments in different markets, it follows naturally that portfolios can be combined with other portfolios. This allows portfolios to be iterated upon seamlessly

V. Identity

In order to be able to use the protocol, it is necessary to implement a robust Proof of Identity system. Without Proof of Identity, a financial system is vulnerable to attacks where one user can create multiple identities and increase his borrowing power by gaming the Trust Score system.

Proof of Identity is a complicated problem that many blockchain companies are attempting to solve. Bloom ID is tackling this problem by allowing individuals to verify their identity using ID Government Document, Sanction Screening⁴ as well as PEP screening⁵. This provides a robust verification to ensure the legitimacy of individuals. Other companies such as Cambridge Blockchain LLC and Civic also have variations on Proof of Identity. For customers in countries which heavily document their citizens such as the US, simply uploading a government ID would potentially suffice as Proof of Identification.

It is again important to note that because XOR is designed to be modular, any identity system can be swapped in or out simply by changing the Identity IC used within the market. For example, in the future,

³ OX is an Open Protocol For Decentralized Exchange On The Ethereum Blockchain.

⁴ Sanctions Screening is the process of reviewing sanctions lists to check if any investor is involved in financing crime or terrorism, so that you can take the appropriate action.

⁵ PEP (Politically Exposed Person) screening refers to reviewing individuals with higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

perhaps biometric identifiers will become the new bank-grade standard. XOR is designed to be flexible enough to handle these types of situations.

VI. Trust Scoring

Borrower trust scores are used to allow lenders to assess the trustworthiness of borrowers without a third party rating agency or black-box credit scoring algorithms. As with other components/delegate proxies in XOR, Trust Scoring is modular such that it differs upon the instance component used within each market, and can be updated over time. The two situations that are possible are that a borrower has a Trust Score on the system, and the borrower does not have a Trust Score. In the event that the borrower does not have a Trust Score, the system has to initialize a score. Depending on the Trust Score IC used in a given market, a Trust Score can be initialized for a borrower based on user-specific data or parameters in their identity (which is once again dependent on the Identity IC used within the market) and a process called Social Staking. Through Social Staking borrowers are encouraged to verify other borrowers. In addition, a given market's Trust Scoring procedure, as shown through its Trust Score IC code, is fully transparent creating for a more fair system than the lack of transparency that FICO scores offer. Depending upon the various IC's used within a given market a higher Trust Score will likely translate to increased borrowing power and lower interest rates from having a better/safer risk profile.

1. Trust Score

The Trust Score is the decentralized and transparent XOR analog to a credit score. A borrower's Trust Score can be determined by a combination of the borrower's history of repayments and defaults on the XOR Protocol, and user-specific data or parameters in their identity (for instance existing FICO scores, evidence of education, country of residence etc.). In addition, a Trust Score can be supplemented by Social Stakers. A high Trust Score indicates that a borrower is trustworthy on the network, and likely to repay their debt. Depending on the Trust Score/Social Staking IC used in the market this can also mean that the borrower's opinion on vetting low/no credit customers (in the process of social staking) is highly valuable. As a reward for having high Trust, the borrower may also have access to more capital and better interest rates from lenders. Borrowers can increase their Trust Score by paying back loans and by correctly verifying other borrowers through the Social Staking system.

2. Social Staking

Social Staking is a process through which a borrower can increase his Trust Score (and thus obtain the various benefits associated with a higher Trust Score as outlined above) by having other borrowers stake their own Trust Score. In the event that the original borrower pays the loan back, the Trust Score increases for the borrower and all participating Stakers, and if a borrower defaults, the Trust Score decreases for each party. This creates a system where Stakers are incentivized to accurately assess fellow borrowers who utilize the Social Staking mechanism. The limit to which Stakers can stake their own Trust Score and increase the Trust Score of the borrower in question is determined by the Staker's Trust Score. For example, a borrower that has previously built up their Trust Score on the protocol, could choose to stake ten percent of their score on another borrower, enabling their trust score to increase by that amount. If the borrower repays the loan, both of their trust score increases. In the case that they default both of their trust scores would decrease. The Social Staking mechanism has large implications for new and first-time borrowers who might lack both a history on the XOR Protocol and favourable user-specific

data/parameters in their identity. It also opens the door for individuals in underdeveloped nations and regions to have access to credit at reasonable interest rates.

VII. Cryptoeconomics

We introduce the XOR Value Token (XVT) as the representation of the XOR Protocol's value, through the inflation and deflation of the token supply based on the health of markets.

1. XOR Value Token (XVT)

XVT is a governance token within the XOR Protocol in which token holders are entitled to make decisions within the protocol (this is discussed further in the governance section). Additionally, through the use of inflation and deflation of the currency, XVT is a direct representation of the health of markets. This is done by minting tokens in the event of defaults, and burning tokens in the event of healthy markets.

2. Token Acquisition and Usage

XVT will be used as the functional currency on XOR. There are several examples of uses of XVT that provide value to XVT. It is important to note that this list does not encompass all use cases for XVT.

1. When creating a market, the market creator must pay a fee in XVT which will be burned. The market creator will then receive a percentage of the throughput of a market (which is defined as the amount of the original loans in a loan market that are actually repaid) by minting XVT tokens relative to the amount repaid. This percentage will be determined by XVT token holders by voting.
2. Similar to the rewards the market creators receive from successful markets component creators also receive a percentage of the throughput of a market by minting XVT tokens. This incentivizes the creation of market components that reduce the number of defaults within markets.
3. XVT tokens are minted in the event of defaults within markets as a form of compensation for lenders. The amount of tokens minted per market is dependent on the history of that market, specifically the history of defaults. Since this acts to inflate XVT supply, and hence lower the value of each token, this mechanism is designed to incentivize XVT token holders to make decisions which result in healthy markets.
4. Borrowers can lock XVT into the market or a contract as collateral. This essentially allows for the possibility of secured loans versus unsecured loans as described in this paper above. In certain markets borrowers can also have voting rights.
5. XVT can be staked to boost the rank of a governance proposal in the queue (as mentioned below in the governance section).

VIII. Governance

Within the protocol, there are two types of governance, one at the global protocol level and the other at the market level. Global governance is done using DAOstack's proposal voting system, while market-level governance is dictated by the Governance IC used by that particular market. In the event that a Governance IC is not referenced, market-level governance would default to the DAOstack system as well.

1. Global Governance

In addition to payment of the Market Creation Fee the XVT token plays an important role in the governance of the XOR Protocol on a global level.

Global governance is primarily concerned with the mechanisms of minting and burning of the XVT Token. Since the minting and burning (inflation and deflation) of XVT is designed to correspond with the health and risk of the markets on the XOR Protocol a corollary of performing governance over the minting and burning mechanism would be performing governance over the mechanism by which the health of XOR markets is assessed. This Health Assessment Mechanism can be based on parameters such as the throughput and default rate of each market. We call the minting/burning/health assessment mechanisms collectively the Global Governance Mechanisms (GGM's).

The process of global governance will be centered around a democratic voting system based on DAOstack⁶. The governance process allows every XVT holder the ability to submit proposals to make changes to the GGM's. These proposals will then be voted upon with a *Yes* or *No*, and be subject to a time limit after which they will be closed and their acceptance or rejection decided based on the number of votes. To avoid finalization attacks, we implement DAOstack's *Quiet Ending* mechanism, which will automatically extend the closing time of proposals if significant changes are made to votes just before the proposal closes. With the anticipation that there will be a relatively high volume of proposals open at any given time, we implement DAOstack's concept of an *Opening Stack* in order to keep the proposal voting system organized and safe from overloading while also reducing voter apathy. In our case the opening stack will have only one proposal under consideration (eg. 2 choices: *Yes* to choose new proposal, *No* to stay the course). Meanwhile, all other proposals reside in a queue ordered by a *Ranking System*. Once a proposal in the opening stack becomes finalized, the highest ranking proposal in the queue enters the opening stack as the proposal under consideration. Proposals in the queue are ranked according to the number of XVT tokens staked on a given proposal. The stake must remain locked for a minimum of 3 months. If the proposal is successfully voted in, the stakers receive their XVT back, otherwise, they are burned.

2. Market-Level Governance

Governance at the market level is performed by the participants in a market. Depending on the Governance IC used for the market, either both lenders and borrowers can partake in governance, or only one of the two parties can. Examples of market-level governance systems include unweighted voting, weighted voting, sortition systems (where delegates with voting powers are randomly chosen from a pool of candidates), representative democracy with delegates (where eligible voting market participants elect delegates who have voting powers over the direction of the market), and many other structures. In the event that a Governance IC is not referenced at the creation of a market, the governance mechanism will default to a DAOstack-like mechanism as described above, except that proposals to change IC's would be submitted, ranked, and voted upon for each component of the market.

IX. Legal Consideration

⁶ DAOstack. (2017). *DAOstack: The Operating System for DAOs* [White paper]. Retrieved April 20, 2018, from <https://daostack.io/wp/DAOstack-White-Paper-en.pdf>

Contracts have to be legally reconcilable in order for lenders and borrowers to be able to safely participate. For example, in the event that a borrower borrows money and tries to disappear, it has to be possible for lenders to pursue legal action. This requires Proof of Identity as well as a strong legal protocol.

XOR currently plans to use the OpenLaw protocol to handle automation and reconciliation of legal contracts. OpenLaw allows for the decentralized and autonomous generation of legal contracts. It has flexible functionality, including cross-border functionality where lenders and borrowers from different countries can select the appropriate jurisdiction. Combined with blockchain notarizing and Proof of Identity, XOR will be able to provide a framework for customers to assess and reconcile legal issues. The OpenLaw contract can be encapsulated within the lending/borrowing contract itself.

X. Applications

In this section, we briefly discuss several examples of potential XOR Protocol applications. The first two examples are examples of loans while the rest of the examples are examples of derivative markets.

1. XOR College Loans

Typical college loans currently have high interest rates and default rates. The 2017-2018 student loan rates are 4.45 percent for undergraduates, 6 percent for graduate Direct Subsidized Loans, and 7 percent for graduate Direct Plus Loans. As of 2018, the total exposure is 1.48 trillion USD at a default rate of 11.2 percent. The primary issue with high exposure and default rates with college loan borrowers is not necessarily the loans themselves, but the rapidly rising cost of college itself.

An XOR college loan could potentially alleviate part of the problem by attempting to drop interest rates and thus provide cheaper loans. This would be possible with the removal of third party fees. In addition this would essentially enable a market where lenders can invest in potential college students' futures.

2. XOR Third World Borrowing Access

A goal for XOR is to enable members of third world countries to participate in the modern financial system. XOR can help with this because of its decentralized and fee-free design. Since anyone can participate in an XOR market provided they meet the preconditions (proof of identity, proper trust score through social staking or other means, etc.) the XOR Protocol is far more accessible as a financial system than traditional banking.

However it is important to note that Proof of Identity is difficult in countries which do not have strong documentation procedures because government identities may not exist for everyone.

3. Startup Fundraising

An interesting use case for XOR would be as a startup fundraising platform. A traditional ICO involves trading some value of tokens (representing equity in the system) for cash. The company running the ICO then uses that cash to further develop their system.

An XOR loan round would be fundamentally different in that instead of trading cash for equity in the startup, the startup would instead provide a contract with a repayment protocol. This contract can be

programmed with complex logic to dictate the repayment. A simple example would be to simply pay the cash back with interest. A more complicated example could be to pay the investor back a discounted percentage of the company's valuation at the time of the settlement date. This type of fundraising round could be used in conjunction with traditional fundraising (i.e. angel investments, venture capital, etc.) and cryptocurrency-specific fundraising styles (public token pre-sales, ICOs, etc.)

4. Creation of Prediction Markets

An especially unique facet of the XOR Protocol is that it enables anyone to create any type of market. As explained previously a debt obligation contract can be used to generally model a myriad of economic systems. Because of this, the XOR Protocol system allows for the creation of markets by anyone within the framework of fairness, accessibility, and trustworthiness. One example is the creation of prediction markets on top of Loan Markets based on the riskiness of that specific market. For instance, individuals may place bets on metrics such as the default/repayment rate of the market, the throughput of the market etc. These prediction markets would not require complex reporting and dispute resolution mechanisms since the specifications for the outcome will come from data on chain, such as profitability or percentage of defaults.