Written by Benjamin Funk

Our brains, books, and databases serve as both the recipients and creators of humans' ever-increasing propensity to produce data

. The latest in this long lineation—the internet—generates and stores about 2.5 quintillion bytes of data per day. While it's easy to look at this number in awe, data points in and of themselves offer little value. They are akin to scattered pieces of vast puzzles that require careful gathering, processing, and contextual integration for them to become valuable

information

.

Many of today's internet giants have centered their entire business models around doing exactly that, and few companies have done so more successfully than Google

. Their process is as follows: extract massive deposits of invaluable raw materials—billions of peoples' "digital exhaust" in the form of private data—and feed them through pipelines of proprietary algorithms to predict the choices individuals are likely to make. The more data Google extracts and processes into information about us, the better the insights they can give to advertisers, and the more those advertisers bid in Google's ad auctions in an attempt to convert us into customers.

As a result of these processes, Google generates$240B of advertising revenue per year.

While Google intentionally removes human beings from this process, there is another way to produce and monetize valuable information that may be even more powerful—by engaging humans as players in games centered around our inherent desire to create, search for, and speculate on information.

From sports betting to MEV to social deduction games like Among Us, we are already naturally drawn to "information games" that center on competition and coordination, requiring us to skillfully hide and uncover information.

Some information games are just that—games. But as we'll see, others can be used to generate and monetize new, valuable information and serve as the backbone of a new generation of products and business models.

However, information games have always had an Achilles heel: trust

. Specifically, players need to trust that other players can't share or act on information in such a way that violates the rules of the game. If a player of Among Us can switch from a crewmate to an imposter mid-game, or a block builder can calculate bad state roots and still be accepted by validators, no one will want to play the game anymore. To solve this trust problem, we turn to trusted third parties to create and mediate information games for us.

That's fine for games with low stakes like Among Us, but restricting game creation and mediation to a centralized party limits the trust in and experimentation around the types of information games we play, and consequently the types of information we can collect, leverage, and monetize.

Simply put, there are many information games that haven't even been attempted because we haven't found a way to keep them fair and trustworthy in a decentralized context.

Programmable blockchains and new cryptographic primitives are fixing this by allowing us permissionlessly create and coordinate information games at scale, without having to trust third parties or each other.

In turn, crypto-powered information games can rapidly accelerate the quantity and quality of information available to the world, increasing our collective decision making-abilities and unlocking efficiency gains on the scale of global GDP. Imagine prediction markets accessible across the globe, serving as a tool to allocate capital for internet-native megafunds. Or a game that allows individuals to pool their private health data and be rewarded for any new discoveries that result from its use, all while preserving their privacy.

As this piece will show, though, crypto-centric information games may not be ready for these high-stakes use cases just yet. But by experimenting with smaller, entertaining information games today, teams can focus on attracting players and building trust before potentially scaling to create and monetize more lucrative information markets tomorrow.

From prediction markets

to game-theoretic oracles

and TEE networks

, this piece will cover the design space for creating these crypto-powered information games, and the infrastructure critical in bringing them to their full potential.

Permissionless Markets: A Prerequisite for Information Games

From futarchy to information marketplaces, blockchains allow developers to create customizable, automated financial devices that underpin permissionless, unstoppable markets. As a result, anyone can now create mechanisms for incentivizing, coordinating, and settling the exchange of value and information. This underscores blockchains' critical role in enabling us to rapidly experiment on how we can best configure games that maximize value for everyone involved.

It's very difficult to convince centralized intermediaries to adapt at this pace or allow their users to participate in these experiments. For that reason, permissionless markets will serve as the medium through which fringe theories and cutting-edge research papers will come to life

. We've already seen this happen in the context of prediction markets, wheretheoretical automated market-making strategies conceptualized to deal with prediction markets' low-liquidity have been implemented asCPMMs on crypto-rails, and tested with real money.

Permissionless markets serve as a vital enabler of tools to better produce new information and monetize its value.

Information Games for Information Production

Many information games produce new information to be used by players to make better decisions.

These information games create incentive mechanisms to extract raw materials (public and private data

) from people, databases, and other sources, and then aggregate that data through the best information-producing machines (markets and algorithms

). Ideally, in aggregating this information, new information is produced and monetized by helping another player make a good decision. For example, an investment DAO using the outcome of a prediction market to determine whether or not to invest in a new startup.

The games and tools leveraged by designers of information games vary depending on the type of information they may produce, and we have a vast design space of different challenges and opportunities to explore.

But let's start with the most actively developed and discussed information game today–prediction markets

.

Game #1: Prediction Markets as Tools for Generating Information

One of the most popular information games we've seen in crypto (and beyond) is the prediction market

. Polymarket

is the world's leading prediction market, and is leveraging crypto rails to facilitate over$400M in cumulative trading volume (and growing fast).

Prediction markets operate by incentivizing players to wager on the outcomes of various events using their own capital (or play money). This requirement of a personal financial stake, or "skin in the game," helps to guarantee that participants are genuinely committed to their predictions. As traders act on their insights, by buying shares in undervalued outcomes and selling shares in overvalued ones, the market dynamically adjusts. These adjustments in market prices reflect a more accurate collective estimation of event probabilities, effectively correcting any initial mispricings.

The more people with disparate but relevant pieces of public and private knowledge who place bets in the market, the more closely the price will reflect the truth. Ultimately, prediction markets harness the "wisdom of the crowds" by leveraging financial stakes to drive the accurate aggregation of information.

Unfortunately, prediction markets suffer from a few critical challenges, many of which come down to various scalability problems.

Truth Bottlenecks

Keynesian beauty contests—contests where judges aim to select the option they think other judges will also select—are not unique to prediction markets. However, their negative impacts here are more pronounced than in traditional markets, as the very goal of prediction markets is to create accurate

information. Moreover, unlike traditional financial markets where profit maximization predominantly drives participant behavior, bettors in a prediction market are more likely to be influenced by personal convictions, political leanings, or vested interests in certain outcomes. As a result, they are more willing to incur financial losses in the markets themselves if their bets resonate with their personal values or expectations of profit derived from actions outside those markets.

In addition, the more people look at any market or algorithm as a source of truth, the higher the incentive becomes to manipulate that market

. This isn't too dissimilar to the problems social media experiences. The more people trust the information goods produced by our social media platforms, the higher the incentive becomes to manipulate them for profit or sociopolitical gain.

Some players might even leverage the signals and incentives created by prediction markets to reprice collective beliefs and encourage collective action. For instance, imagine a government using a form of "quantitative easing" to influence prediction markets on critical issues like climate change or war. By purchasing large volumes of shares in a relevant prediction market, they could shift financial incentives towards desired outcomes. Perhaps they have determined that the systemic risk of climate change is undervalued, so they buy a significant number of "No" shares in a market predicting climate improvement by 2028. This action could encourage more climate startups to develop technology that gives them an information edge in betting on "Yes" shares, thereby accelerating efforts to find solutions.

While the factors above have been shown to negatively affect thequality of information produced, it has also been shown that instances of manipulation actually increase the accuracy of the market, because market manipulators are noise traders that informed market participants can make money by trading against.

As a result, we can deduce that the problems above are a result of an insufficient amount of well-capitalized, informed traders to help correct markets.

Allowing these informed traders to borrow and short could be a critical means to making these markets more efficient.

Moreover, in markets with longer timelines, it's more difficult for informed traders to counteract manipulation, as manipulators have more time to reflexively influence both market sentiment and the actual outcomes through their trades. Implementing markets with shorter, renewing resolution dates could improve people's trust in the game (and hence the quality of its information), but also make for more attention grabbing gameplay.

We're also seeing early signs that, in some contexts, players enjoy information games where the resolution of the markets is manipulable. Perl

, the #1 account on Farcaster at the time of writing, has leaned into this model and created an in-app platform to speculate on user engagement. Prediction markets like "Will @ace or @dwr.eth (co-founders of Perl and Farcaster respectively) get MORE likes tomorrow?" are initiated, and the trolling one can expect from football teams and their fans begins. Only here, the game happens asynchronously and is measured in likes instead of touchdowns. While Perl's game intentionally subverts the information-producing quality of prediction markets, a fun meta-game emerges from coordinating to resolve the oracle in one's favor.

Prediction-based games can reduce manipulation and boredom by using shorter, potentially renewing rounds. However, in low-stakes games, allowing player manipulation can add to the fun and become an integral part of the gameplay.

Finding the Right Judges & Oracles

Another challenge of prediction markets can be found in adjudication

—how do you resolve the market correctly? In many cases, we can rely on oracles secured by reputation and collateral that can plug into offchain data feeds. To solve this, prediction market designers can lean on game-theoretic and cryptographic oracles

to plug into a wider set of topics, including players' private information.

Game-theoretic oracles, or schelling-point oracles

, assume that in the absence of direct communication, participants (or nodes) in the network will independently converge on a single answer or outcome that they believe others will also choose

. These oracles, pioneered by the likes ofAugur

and later on by UMA

, encourage honest reporting and deter collusion by rewarding participants according to their degree of proximity from the "consensus" answer.

Still, there are many challenges in making these oracles reliable in adjudicating bets across a small number of players, where identifying and communicating with each other to collude becomes a potential threat. While encryption is touted as a critical tool to avoid

collusion between voters, it can also be wielded as a tool to enable collusion

and prevent prediction markets from resolving correctly. We can see this through the potential forDarkDAOs leveraging trusted execution environments (TEEs)

to engage in programmatic bribery and coordinated price manipulation. One of the teams working on balancing these incentives is Blocksense

, which uses secret committee selection and encrypted votes to prevent collusion and bribery.

Source: Hacking Distributed

It's also possible to tackle the oracle challenge by leveraging onchain data. InMetaDAO

, players are rewarded if they correctly predict how a specific proposal would impact the price of its native token. This price is served by the UniswapV3 position, serving as an oracle for the token's value.

Even then, these oracles are limited in resolving markets based on publicly available data. If we can resolve markets based on private data, we can unlock entirely new types of prediction markets.

One of the ways we can resolve markets based on private information is by using the outcomes of information games themselves as oracles. One such example is the Bayesian Market, which leans on the principles ofBayesian reasoning to derive bettors' own beliefs about their private information by getting them to bet on others' beliefs. For example, setting up a market where people are betting on "how many people are satisfied with their lives" reveals the bettor's own beliefs about others' life satisfaction. As a result, we can come to accurate conclusions about a player's private information, which would otherwise be an unverifiable truth.

Another solution we can lean into is to leverage oracles that leverage clever cryptography to "import" data from private web2 APIs. Some of these existing oracles are showcased in the "Oracles for Public & Private Information" section of the market map. Using these oracles, it's possible to create prediction markets around some players' private information, incentivizing the holder of private information to verifiably resolve specific prediction markets in return for claiming trading fees from people betting on it. More generally, the ability to securely access a richer set of people's offchain data onchain can serve as an identity primitive that helps us better identify, incentivize, and match players across information games much more efficiently, helping us bootstrap the necessary information to make information games relevant to players.

Innovations in oracle design will increase the scope of data we can use to resolve prediction-markets, expanding the design space for information games around private information.

Liquidity Bottlenecks

Attracting liquidity to prediction markets is hard. First, these markets are binomial markets, where players bet "Yes" or "No" on a particular topic and either receive a fixed monetary amount or nothing at all. As a result, the value of these shares can shift drastically with small changes in the underlying asset's price, especially close to their expiration. This makes predicting their short-term price movements very important, but challenging. To handle the significant risk of these sudden changes, traders must use advanced and constantly adjusting strategies to protect against unexpected market movements.

More importantly, it becomes even more difficult for prediction markets to attract liquidity as they expand the scope of their markets to more topics and increase their time frames. The higher the variety of markets beyond politics and sports, and the longer their duration, the less people feel they have a perceived edge in betting on them.

As a result, less people bet, and the quality of the produced information degrades.

Prediction markets inherently face these liquidity issues because forming prices requires uncovering private information and

making bets based on that information, both of which are costly activities. Participants need compensation for their efforts and the risks they take, including the cost of gathering information and locking up capital. This compensation typically comes from others willing to accept worse odds for reasons like entertainment (i.e., sports betting) or hedging risk (i.e., oil futures) which help drive significant liquidity and volume. However, prediction market topics with narrower interests have less commercial appeal to players, leading to less liquidity and volume.

Economic Improvements: Overlays & Diversification

We can work towards solving these problems by recycling ideas from traditional finance and other existing information games.

Notably, we could make use of the overlay

which Hasu covers in "The problem with prediction markets." In gambling tournaments, the concept of an overlay—additional value added to the pot by the house to encourage participation—serves a similar purpose to the subsidy proposed for prediction markets. The overlay effectively reduces the cost of entry for players, making the tournament more attractive and thereby increasing participation from both novices and seasoned players.

Just as an overlay in a gambling tournament acts as a catalyst for player engagement by enhancing the potential return on investment, a subsidy

in prediction markets incentivizes participants by lowering the barriers to entry and making participation more financially appealing. The subsidy also serves as a beacon, drawing in a multitude of perspectives and insights from both uninformed and informed traders who stand to profit from correcting them. Teams operationalizing this strategy will have to systematically identify and engage with potential subsidy providers and create markets around their needs, as they are the ones willing to provide the necessary liquidity.

In a similar vein, it's possible that a fund-like structure

could be implemented to achieve time and sector diversification, and increase the liquidity in prediction markets across a broader set of questions and time horizons. For example, many companies might find value in markets centered around how particular lawsuits might resolve. These companies could lower costs for legal experts to participate by lending them capital, allowing them to diversify across a wide set of markets, and then rewarding them according to their performance over time.

In this setup, traders would be able to borrow money to make markets, the amount which could be parameterized according to demand for the information that would be produced and the trader's reputation on the subject. This could be combined with management fees that serve as an additional overlay across each of the markets.

On the side of liquidity providers, they would receive exposure to traders incentivized to bet on these markets correctly, diversified across a large basket of uncorrelated assets with different durations. While the principal-agent problem would have to be considered, this system could increase the magnitude of liquidity provided in these markets and the variety of pools across which they are allocated. As a bonus, the quality and variety of information goods could be increased while creating new information about trader's skills and knowledge across different markets, accelerating returns for liquidity providers through reputational byproducts.

When the value of the information that players could produce is large, integrating composable financial markets like lending and liquidity mining into gameplay can serve as critical tools to lower barriers to entry.

UX Improvements: Simpler Interfaces & Flexible Incentives

The default, exchange-centric UX and limited reward types across today's prediction markets can push out those who are motivated by other types of interfaces and incentives, further limiting liquidity. On the side of bettors, there are many interesting ways to improve the quality of prediction markets, all of which center around increasing reach and accessibility to different types of players.

First, we can improve prediction market UX by integrating them within larger social platforms.Perl and Swaye have demonstrated how, by plugging into Farcaster's data, users are spared the cognitive load of opening up a separate app, and information game designers can identify and direct players to markets they are uniquely situated to play (i.e., top participants in the channel for /nyc-politics).

Source: Perl on Farcaster

There is also opportunity for experimentation around increasing the scope of the rewards distributed to bettors and creating looser requirements for the capital they put at stake. This could look like rewarding individuals with attestations, or increasing the scope of financial rewards to "in-app utility" or equity represented through points or tokens.

While monetary incentives are important to make prediction markets work, some literature indicates thatplay money can create prediction markets with equivalent quality. Practically speaking, this tells us that we can be flexible in our assumptions about the types of "skin in the game" bettors would put at risk and be compelled to gain.

Moreover, there are different types of market mechanisms that can be used to make the UX more poll-based

, which would further minimize friction and lower barriers to entry.A study by Cambridge evaluated this hypothesis and found that polling mechanisms led to more accurate outcomes compared to prediction markets during periods of low trading activity, wide bid-ask spreads, and in markets that resolve quickly. The study also found that combining poll-based prediction games with the monetary incentives of prediction markets yielded significantly more accuracy than prediction market prices alone. Additionally, to solve the potential challenge of stagnant information, polls could "renew" periodically according to some push or pull-based system, incentivizing the dynamic reproduction of information based on new information.

Crypto information games used to deter all but the most dedicated power users. Now, with lower costs, improved usability, and richer data, there's an opportunity to develop more varied and accessible games that target specific audiences.

Game #2: Privacy-Preserving Computation to Produce Information

Imagine a game played by solidity devs, where players leverage multi-party computation (MPC)

to reveal their salaries and compute the average, all while preserving confidentiality of their individual salaries. This would be a valuable way for crypto professionals to negotiate with their respective employers, while also serving as a source of entertainment.

More broadly, information games can leverage privacy-preserving technology to broaden the range of raw materials—specifically private

data and information—that can be analyzed to generate new insights. By ensuring privacy, these tools can increase the variety and propensity for people to share data and information, as well as compensate those data providers for the value derived as a result.

While this isn’t all encompassing, a few of the tools information producers use to do this are zero knowledge (ZK), multi-party computation (MPC), fully homomorphic encryption (FHE), and trusted execution environments (TEES)

. These technologies differ in their core mechanics, but they all arrive at a similar place—enabling individuals to provide sensitive information in a privacy preserving way.

Still, there are many serious challenges to using both software and hardware-based cryptographic primitives for use cases that require strong confidentiality guarantees, which we’ll discuss later.

Privacy-preserving cryptography significantly widens the design space for new information games that couldn’t have existed before.

Game #3: Competition Between Models to Improve Information Production

Imagine a game where data scientists compete against each other by developing and betting on trading models for a decentralized hedge fund. Blockchains then come to consensus on the scores of particular models, and reward or slash participants depending on the correctness of their model’s predictions and their impact on the fund’s returns. This is the approach taken by one of the earliest information games on Ethereum, Numerai. In this game, Ethereum’s consensus is leveraged by global competitions between different models and their creators, effectively incentivizing AI to play information games that result in the production of valuable returns.

Taking this a step further, we could also incentivize AI to play information games for us much more directly, leveraging their encyclopedic knowledge to compete with each other in making predictions. While they might not necessarily be having fun playing these games, using intelligent machines instead of humans would significantly decrease the cost of labor needed to produce information. As a result, these AI models could increase the amount of liquidity in much more niche prediction markets where humans would otherwise be unwilling to play. As Vitalik put it:

“If you make a market, and put up a liquidity subsidy of $50, humans will not care enough to bid, but thousands of AIs will easily swarm all over the question and make the best guess they can. The incentive to do a good job on any one question may be tiny, but the incentive to make an AI that makes good predictions in general may be in the millions.”

Alternatively, we can leverage consensus between ML models to create competition between them around the value of the information they create. Teams like Allora and Bittensor TAO are working on coordinating models and agents to broadcast their predictions to others in the network, who, in turn, are responsible for evaluating, scoring, and broadcasting their performance back to the network. At each epoch, the collective assessments between models are used to distribute rewards and/or power to the different models according to the quality of their predictions. As a result, entrepreneurs can leverage self-improving networks of models to improve the quality of the information flowing through their marketplace.

It’s entirely possible that there are information markets for which the use of models leads to a quality of information goods that information games amongst humans simply cannot match.

Monetizing Information Games

Some information games can sustain themselves purely from the fun that users derive from it. But for those who want to monetize the value of the information they produce, things require a little more thought. Unfortunately, the qualities of information as a good

lead to critical market failures that prevent their seamless monetization:

- Information can be valued only after its consumption, making it hard for buyers to assess whether a seller’s price accurately reflects the value of their information.
- Information is non-rivalrous—its consumption doesn't reduce its availability, meaning it doesn’t have the scarce properties that make it interesting to buyers.
- Information’s non-excludable nature, coupled with low reproduction costs, makes it hard for sellers to prevent unauthorized access, despite high initial production costs.

Information can be valued only after its consumption, making it hard for buyers to assess whether a seller’s price accurately reflects the value of their information.

Information is non-rivalrous—its consumption doesn't reduce its availability, meaning it doesn’t have the scarce properties that make it interesting to buyers.

Information’s non-excludable nature, coupled with low reproduction costs, makes it hard for sellers to prevent unauthorized access, despite high initial production costs.

These economic characteristics create challenges for both buyers and sellers in profiting from information, potentially leading to its underproduction. If information is quickly known by everyone who can exploit it at the same time, then the opportunity for an information buyer to exploit an information asymmetry shrinks due to increased competition or a collapse of the scheme they were going to use. Thankfully, there are a couple of crypto-tools that can be used to solve these problems, and already are.

Game #4: Exchanges—Monetization Through Speculation on Information

One way to monetize information production without keeping said information confidential or limiting the set of actions that can be taken on it is to simply keep that information public, but create a vehicle for people to bet on how it will change – also known as derivatives.

One company actively doing this is Parcl

*, whose exchange enables users to speculate on rising and falling real estate markets. Parcl's markets are powered by real-time price information that Parcl Labs sources from vast real estate data reservoirs and feeds through proprietary algorithms to produce fine-grained, accurate information that surpasses the quality of traditional indexes of real estate prices.

While Parcl does monetize this information more directly through an API, they've created an additional monetization layer by allowing traders to bet on how that information will change over time. Other projects, such as those mentioned in the "alternative information markets" section of the market map like IKB and Fantasy, focus on monetizing through speculation or hedging on how existing public information will change

, from an athlete's performance to a creator's social engagement.

If you can sell the right to speculate on the information you produce, you can monetize it without keeping it confidential or restricting what buyers can use the information for.

Game #5: Marketplaces for Discovering Confidential Information

Picture a game that lets you discover curated alpha on the latest onchain activity and brand new crypto startups before they become known by the whole world. For this to work, information would need to remain confidential in order to solve for the issues of non-rivalrousness and excludability that come with public information. For this reason, the next-generation of information markets are facilitating the exchange of confidential

information

, while leveraging blockchains to discover and regulate access to all the players that could pay to access it.

Freatic's

- decentralized marketplace for confidential information, Murmur

, exemplifies this approach by gating exclusive access to information through NFTs and a queue system. Information buyers first subscribe to a particular topic by buying an NFT represented as a coupon. This then grants them a slot in the queue to redeem confidential information from publishers and, for an additional price, allows them to pay to slow down its rate of dissemination. Buyers can also vote on the quality of that information afterwards. Through this process, Murmur ensures information remains confidential and valuable without having to limit its sale to one entity.

In contrast, Friend.tech

uses keys and bonding curves

to manage access to confidential information in group chats, making entry more expensive as demand increases. As a result, one can think of a Friend.tech key as a proxy for the average value of information from a person (assuming the market for keys is efficient). However, players have always "priced in" some notion of the person's "value" when trading keys, making it difficult for buyers to price the information's

worth. Maybe this serves as another datapoint to support the claim that the most valuable "information markets" to date have actually been the markets for memecoins, serving as prediction markets around the symbolic value of particular trends or people if you squint hard enough.

Memecoins aside, one direction that teams gating information access could pursue is to allow information sellers to design bonding curves that better correlate the access price with the information's value.

For example, pricing for information that quickly loses value as it becomes known could be determined by a bonding curve that reflects the rapid depreciation of the information's value over time.

Decentralized money exchange is challenging due to trust issues and finding double coincidences of wants. Blockchains have resolved this for money (Bitcoin) and are set to do the same for information, catalyzed by fun games centered around seeking hidden information.

Game #6: Futarchy—Monetizing Prediction Markets

One major way of monetizing information without keeping it explicitly confidential is to produce and sell the information that only one organization can and will make use of. This playbook isn't new, as many companies already monetize information by limiting access to particular buyers through auctions or confidentiality agreements. However, we're seeing a new business model for selling information goods—producing public information that's only relevant and valuable to organizations making specific decisions.

In fact, we're just now seeing prediction markets being built on crypto rails in order to experiment withFutarchy

as an alternative mechanism to monetize the information they produce.

Futarchy offers a novel approach to improve decision-making, centered around harnessing the information created by prediction markets. The information produced by the prediction market is used to make decisions, and when prediction markets are resolved, the players with the best predictions get rewarded.

On their own, prediction markets are zero-sum games for players, limiting incentives for informed traders to participate in them and worsening their existing liquidity bottlenecks. Futarchy can solve this, as the wealth created by better decisions can be redistributed back to traders.

Crypto-native entities like MetaDAO

are already experimenting with Futarchy. When a proposal is made, such asPantera's proposal to purchase MetaDAO governance tokens, two prediction markets are created: "pass" for support and "fail" for opposition. Participants trade conditional tokens within these markets, speculating on the proposal's influence on the DAO's value. The resolution hinges on the Time-Weighted Average Price (TWAP)

comparison of the "pass" and "fail" tokens after a designated period. Should the "pass" market's TWAP surpass the "fail" market's by a set margin, the proposal is approved, leading to the execution of the proposal's terms and the annulment of transactions in the losing market. This system employs market dynamics to drive governance decisions, aligning them with the collective projection of the proposal's effect on enhancing or reducing the DAO's value.

There are still some cases where Futarchy must be designed around confidentiality. For example, if prediction markets are used to determine hiring decisions around a specific person, that information would become publicly available and turn into an information hazard

—a competitor might be interested in poaching the hire based on the market's prediction.

Another reason to keep information confidential is its impact on motivation and organizational culture. As Robin Hanson notes in his Future of Prediction Markets speech, Google's own internal experiments met resistance due to executives' fears that public performance indicators could demotivate employees. Naturally, managers aren't inclined to implement something that might reveal the emperor has no clothes, and we're seeing this in practice today. According to MetaDAO's founder, @metaproph3t, some people decide not to submit proposals because they don't want to be evaluated by a market.

Both of these issues could be solved by limiting the availability of prediction-market information to specific decision-makers. However, by empowering these decision-makers with autonomy over their actions based on this information, bettors will incorporate these biases into their bets, reducing the quality of the information generated.

In other cases, Futarchy may just be better applied in specific industries where its advantages outweigh cultural impacts, like Bridgewater's hedge fund. Integrating blockchain could further enhance Futarchy's integrity toprevent manipulation (looking at you, Ray Dalio).

So far, prediction markets have been limited to monetizing by allowing for speculation or hedging. In being used to help organizations make better decisions, prediction markets can unlock an entirely new market, though open questions remain around the role of confidential information.

Game #7: Credible Commitments for Programmable Information Games

As mentioned at the beginning of this piece, Google monetizes information by leasing its use to advertisers while limiting their use of this information to Google's ad auctions. Similarly, credible commitments help information sellers monetize by restricting the actions that buyers can take based on said information.

Cryptographic methods like MPC, TEEs, and FHE can be used by information sellers to secure credible commitments about the computation buyers will take on top of private data. As a result, sellers can delegate their information to buyers, giving them specific control over future actions around their private information without revealing the information itself.

This primitive unlocks all kinds of information games. Imagine enabling traders (information sellers) to sell the right to order their transaction to information buyers (searchers) only if

the buyers commit to simulating the order of their transactions a capped number of times. Taking things a step further, imagine allowing Netflix users to delegate the right for others to watch Netflix movies from their account, allowing them to “yield farm” rewards from their account without leaking its login details. In turn, buyers can unlock value from sellers’ private information, without sellers having to deal with the challenges of selling the information itself (information is a non-rivalrous, non-excludable, experience good).

Unlocking Google-Scale Monetization for Information Game Designers Today

TEEs

present a practical choice for implementing such controls today, albeit withlimited confidentiality guarantees. While not fit for securing large assets or sensitive data, TEEs are suitable for use cases that require more time-limited access to confidential information, such as front-running protection. SUAVE

, a project created by the Flashbots

team, is building a network of TEEs that developers can already use today, with the long-term vision of enabling app developers to find new ways to better monetize the value of their and their customer’s information.

In SUAVE's design, integrating blockchains with TEEs addresses three critical TEE limitations essential for advancing information games. First, blockchains eliminate the need for trust in communication between hosts and players, who could censor or behave maliciously. Second, blockchains provide a secure mechanism for state maintenance, protecting against the rollback attacks that TEEs are prone to. Lastly, blockchains are critical to ensuring the permissionless, censorship-resistant creation of TEE-based information games (SUAPPs), whose smart contracts, inputs, outputs can be trusted by all players.

While many early information games using SUAVE will clearly center around MEV, they have the opportunity to be used in information games that extend far beyond trading.

Game #8: Reputation & Zero-Knowledge to Facilitate In-Game Marketplaces

A key challenge to monetizing information is the inherent nature of information as an "experience good." The value of an experience good is only recognized upon use, complicating the seller’s ability to set a price for it beforehand.

In creating mechanisms to solve for this, we can also create fun gameplay for users. Some games center heavily around enabling players to build a reputation that distinguishes them from other players, like WoW, which can be a source of fun but also a critical way for players to decide who to coordinate with. Other games might want a seller to commit to a price for some intelligence (i.e., enemy locations, secret plans) without requiring them to reveal the information beforehand.

To overcome this, designers of information games can leverage cryptographic solutions like Zero-Knowledge Proofs (ZKPs)

to verify the characteristics of computational information goods—such as the efficacy of a trading algorithm—without disclosing the actual data or code. This can be achieved by creating a cryptographic commitment, timestamping it on a blockchain, and providing a ZKP of the algorithm's performance. However, this method is only effective for information goods whose value derives from the properties of its computation and can be tested on verifiable inputs.

For other types of information goods, reputation and identity become crucial. It’s possible to leverage consensus mechanisms between information buyers to create reputation around the value of the information that sellers are trying to sell.

Systems like Murmur's

leverage subscriber voting within exclusive windows to establish a publisher's reputation, elevating them from unverified to verified status based on community feedback. This process creates a transparent and immutable record of interactions, building a trusted reputation for sellers that gets created with a tight feedback loop.

Alternatively, the **Erasure Bay** protocol requires sellers to stake money as well as their reputation as a signal for their information's reliability. The protocol determines a "griefing factor" that allows buyers to destroy a certain portion of the seller’s stake if the information proves to be of low quality, thereby ensuring sellers are incentivized to offer high-quality information.

To avoid market failures and maximize volume, game designers need to give sellers cryptographic-tools to prove their information’s worth, or credible, quick mechanisms for building reputation around what they’ve sold before.

Conclusion

Information games aren’t new. However, until programmable blockchains, game designers were limited to asking centralized intermediaries for permission, and players were limited to games that could be mediated by trusted third parties.

Now more than ever, the dramatic reduction in the cost for blockspace means that anyone can create a futarchy-inspired DAO or a protocol for confidential information, and plug into an endless amount of tools for verification, adjudication, monetization, and more. The games we’ll see unlocked by low barriers to participation and open innovation on permissionless financial rails are unimaginable.

This piece showcases the early signs and challenges in implementing this new wave of information games, and the potential of using crypto-tools to solve these problems. With these tools in hand, some game designers will improve information games we already play, like trading and MEV, while others create games that simply couldn’t have existed before.

Still, each of these crypto-powered information games represent mini-games that need to be composed with each other to form a complete game. The joy and thrill players gain from building reputation, collaborating with a team, and vying for influence within an organization all act as components of a larger whole.

If you’re creating a fun, crypto-powered information game, please reach out to chat. I’d love to try it, learn more, add your project to the market map, and brainstorm ideas!

*denotes an Archetype portfolio company

Special thanks to all the people in the arena for the thoughtful conversations & feedback that all went into putting this piece together: Arthur Roing Baer, Soumya Basu, sxysun, Tyler Gehringer, Katie Chiou, Dmitriy Berenzon, Quintus, Harry Jones, Alex Kwon, Spenser Huang, E.S, Proph3t, Trace, Hactar, and Connor McCormick.

Disclaimer:

This post is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. You should consult your own advisers as to legal, business, tax, and other related matters concerning any investment or legal matters. Certain information contained in here has been obtained from third-party sources, including from portfolio companies of funds managed by Archetype. This post reflects the current opinions of the authors and is not made on behalf of Archetype or its affiliates and does not necessarily reflect the opinions of Archetype, its affiliates or individuals associated with Archetype. The opinions reflected herein are subject to change without being updated.