# SoK: Market Microstructure for Decentralized Prediction Markets (DePMs)

No Author Given

No Institute Given

**Abstract.** Decentralized prediction markets (DePMs) allow open participation in event-based wagering without fully relying on centralized intermediaries. We review the history of DePMs which date back to 2011 and includes hundreds of proposals. Perhaps surprising, modern DePMs like Polymarket deviate materially from earlier designs like Truthcoin and Augur v1. We use our review to present a modular workflow comprising eight stages: underlying infrastructure, market topic, share structure and pricing, initialization, trading, market resolution, settlement, and archiving. For each module, we enumerate the design variants, analyzing trade-offs around decentralization, expressiveness, and manipulation resistance. We also identify open problems for researchers interested in this ecosystem.

## 1 Introduction

In late 2024, the United States was in the midst of a presidential election when the decentralized prediction market, Polymarket [66], broke through mainstream news coverage [17,85]. Stories focused, in particular, on the fact that it offered odds more favourable to eventual winner Donald Trump than those reflected in conventional polls and forecasts. Polymarket's odds are not set by experts or pundits, instead it is a specific type of betting market where odds are extrapolated from the prices of trades made in an open market (or somewhat open, as Polymarket was banned at the time in many countries including the US).

As with traditional betting, whether online or through a bookie, prediction markets allow speculators to profit from correct forecasts [3,84]. However the structure of a prediction market is different than traditional betting. One key difference is that prediction markets ease the process of moving in and out of bets before the event resolves, encouraging traders to place bets if they think the odds are over- or under-stated, and withdrawing profits if the odds realign.

It would be easy to think that Polymarket's design is the most obvious, straight-forward way to deploy a decentralized prediction market (DePM) on a blockchain. However the central thesis of this systemization of knowledge (SoK) paper is that Polymarket found success in bucking the trend. DePMs were first given a few paragraphs in the Ethereum vision paper [14], released in late 2013 for the blockchain that would be deployed in 2015. Then two 2014 papers presented flushed out systems: a whitepaper called Truthcoin [77] and an academic

paper at WEIS 2014 [19] (informally known as the 'Princeton DePM' because of author affiliation). Developed independently,[1] the two papers' designs are vastly different, representing two different goalposts for how a DePM might look.

Early systems, like Augur [63] and Gnosis [34] closely resembled Truthcoin [77], while modern systems like Polymarket [66] either resemble the Princeton DePM [19] or use new solutions that resemble a hybrid of the two designs. Consider some examples:

1. From §3.3, in Truthcoin, the market creator is active in setting initial prices (*i.e.,* odds) for each option and risks its own money (bounded) [77]. In the Princeton system, the market creator is passive, not setting prices or risking any money [19]. Polymarket uses the latter [66].
2. From §3.5, in Truthcoin, outcome shares are created with predecessor to an automated market maker [77]. In the Princeton DePM, outcome shares are traded with an orderbook [19]. In Polymarket, outcome shares can be traded with either an AMM or an orderbook [66].
3. From §3.6, in Truthcoin, the blockchain decides event outcomes (*e.g.,* who won the election) through a reputation-based on-chain vote with slashing [77]. In the Princeton paper, they are resolved through trusted arbiters acting as oracles [19]. The Ethereum whitepaper suggests both [14]. In Polymarket, the third party oracle, UMA, operates under the hood through on-chain voting with slashing, but only when outcomes are disputed [66,81].

*Research Questions.* Noticing these points of differences inspired us to enumerate all of the design decisions involved in creating a DePM. What are the core modules that appear across DePM designs? How do DePMs differ in how they implement each module (creation, trading, resolution, settlement)? Which early design choices shaped later DePM architectures? Which design choices create recurring failure modes or operational problems? What trade-offs do DePMs make between decentralization, usability, and correctness of resolution? We also ask what open design gaps remain for building robust DePMs (these are marked as 'research gaps' in the paper).

*Systemization of Knowledge (SoK).* Within the blockchain literature, a variety of SoKs have been published with a variety of methodologies and deliverables, making it difficult to establish what constitutes an SoK paper. We review several SoKs from *FC* and *AFT* that, like us, consider a blockchain technology: oracles [27], stablecoins [59], DeFi services [82], light clients [16], layer 2s [36], privacy technologies [8], and MEV mitigations [41]. Like us, every one of these papers compares/contrasts a set of technologies [27,59,82,36] or theoretical models [16,8,41] from academia and industry. Like us, the main deliverable is decomposing designs into a taxonomy or classification system for comparison and

---

[1] The Princeton paper describes Truthcoin as being released while the paper was under review [19], and the Truthcoin FAQ [76] mentions hearing about the Princeton paper but not having found the paper itself.

evaluation [27,59,82,36,16,8,41]. Like us, some distill the technology into a single model into layers or abstractions before classifying [27], others offer definitions [16,82]. Only one of these papers does quantitative experiments [82], a welcome but unnecessary requirement for SoKs. Unlike a literature review—which primarily summarizes prior work paper-by-paper—an SoK imposes a common set of concepts, abstractions, and evaluation criteria so that disparate systems can be compared on a level playing field rather than merely described.
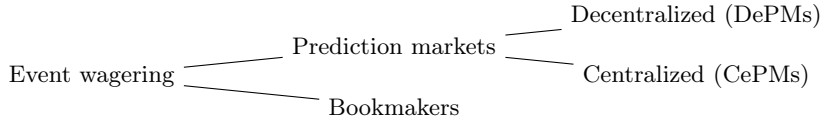
*Methodology.* We obtained a collection of academic works on decentralized prediction markets, as well as various intersecting topics including (centralized) prediction markets, oracles, DeFi, and AMMs. We used our knowledge of the field, Google Scholar (search and cited by features), and citations within papers. Our library is available, sorted by topic, on Zotero.[2] We also identified projects without white-papers or academic papers, reviewing the 97 current projects listed on a recently released online dashboard [73] and by studying 20+ historical systems that are no longer active. We also searched news sources for opinions and issues on leading decentralized prediction markets, such as Polymarket. We applied the following exclusion criteria to remove from consideration designs that are: fully permissioned CePMs, alternative wager structures beyond the first notable design we saw (*e.g.,* parimutuel betting [78,49,80], back/lay exchanges [20] and cash for difference contracts [26]), supporting/adjacent infrastructure, and insufficiently documented or scams. We reviewed over a hundred projects, distilled into the 35+ notable DePMs listed in Appendix A.

A modular workflow (*cf.* [27]) is an abstraction that breaks competing designs into the same common set of steps and parts, enabling side-by-side comparison. We used multiple rounds of affinity diagramming to cluster DePM subcomponents from our corpus into eight stages: underlying infrastructure, market topic, share structure and pricing, trading, market resolution, settlement, and archiving. Relevant artifacts and data are available on GitHub.[3]

## 2   Preliminaries

### 2.1   Wagering Systems

Consider the following taxonomy of a few wagering systems:



*Bookmakers versus prediction markets.* A wager is a two-party contract with payouts based on the outcome of a future event. Consider Alice and Bob who wager on the same outcome of an event. With a fixed-odds bookmaker (or online

---

[2] Zotero: Link withheld for anonymity.

[3] GitHub: Link withheld for anonymity.

betting), Alice's contract is different from Bob's contract in at least two regards: (i) it specifically names Alice as the counterparty and (ii) the payouts could be different if the odds changed between Alice's wager and Bob's. By contrast, in a prediction market contract (called a outcome share), Alice and Bob hold identical contracts: (i) all contracts are between the market operator and whoever redeems the contract, and (ii) the payout is exactly the same (typically \$0 if incorrect and \$1 if correct). Odds are reflected in the price paid for a prediction market contract (*i.e.,* variable cost and fixed payout), while a bookmaker contract has a fixed cost and variable payout. Thus the key distinction is that prediction market outcome shares are *fungible* and can be freely traded between participants, enabling a free market that communicates information to the public through outcome share prices, trading volume, market depth, and other financial market metrics. Operating a prediction market also differs from operating a bookmaker in a very important way:

> **Insight 1.** Bookmakers quote odds without needing to hold sufficient funds in the event of a payout. It is merely a promise to pay. By contrast, a prediction market is structured with sufficient collateral for all outcomes at all times (including the very first trade! See §3.4). Every dollar paid to a winning trader is a dollar from either (a) a losing trader or (b) bounded within a special loss fund setup before the market opens.

*CePM versus DePM.* The term *decentralized prediction market* originates from the Ethereum whitepaper [14] and we abbreviate it DePM to match terms like DeFi (decentralized finance) [82] and DePIN (decentralized physical infrastructure networks) [51,56]. The term *decentralized* [62] in each of these is actually shorthand for both *decentralized* and *permissionless*, where permissionlessness is generally the more important way DePMs distinguish themselves from centralized prediction markets (CePMs). Permissionlessness could extend itself to the market topic, the trading of outcome shares, the closing of the market, and the withdrawing of rewards, but not all systems will open up each of these operations (as we will explain in §3). We say a system is DePM if at least one is permissionless.

## 2.2   Definitions

We start with an abstract definition of a prediction market. Our definition generalizes on recent computer science-based definitions [11,30,72] which each presume specific sub-types of a prediction market (*e.g.,* [11,72] use *merging/splitting* while [30] presumes *automated bookmaking* from §3.5).

**Definition 1 (Market).** *A (single) market is a tuple $M = (\Omega, J, R)$, where $\Omega$ is a nonempty outcome space, $J$ is a finite index set of contract labels ("shares"), and $R : \Omega \to \mathbb{R}_{\geq 0}^{J}$ is a nonnegative payoff map. Intuitively, $M$ is associated with an underlying uncertain event, whose possible resolutions are represented by $\Omega$. When $M$ resolves to $\omega \in \Omega$, one unit of share $j \in J$ pays $R(\omega)_j$ units of the numeraire $\mathcal{N}$ (Def. 2).*

*Remark: WTA special-case.* For a market $M = (\Omega, J, R)$, suppose there exists a bijection $\iota : J \to \Omega$ and $R(\omega)_j \in \{0, 1\}$ with $\sum_{j \in J} R(\omega)_j = 1$ for all $\omega \in \Omega$. Then $M$ is a winner-take-all (WTA) or Arrow–Debreu market: a unit claim of label $j$ pays 1 iff the realized outcome equals $\iota(j)$, and 0 otherwise.

**Definition 2 (Prediction Market System).** *A prediction–market system is a tuple $\mathcal{S} = (\mathcal{M}, \mathcal{N}, \mathsf{res})$, where $\mathcal{M}$ is a countable set of markets, $\mathcal{N}$ is a numeraire (unit of account), and $\mathsf{res}$ is a resolution function such that, for each $M = (\Omega, J, R) \in \mathcal{M}$, we have $\mathsf{res}(M) \in \{\bot\} \cup \Omega$, $\mathsf{res}(M)$ is initially $\bot$, and $\mathsf{res}(M)$ transitions exactly once to some $\omega \in \Omega$.*

**Definition 3 (System Axioms).** *For every market $M = (\Omega, J, R) \in \mathcal{M}$ operating in system $\mathcal{S} = (\mathcal{M}, \mathcal{N}, \mathsf{res})$, the following axioms hold. In what follows, all quantities are for this fixed market $M$, and we write $\mathsf{Treas} := \mathsf{Treas}_M$ and $L := L_M$.*

1. ***Issuance and Solvency.*** *Let $S = (S_j)_{j \in J} \in \mathbb{R}^J_{\geq 0}$ be the outstanding supply vector, and let $\mathsf{Treas} \geq 0$ be the market's treasury (in the numeraire $\mathcal{N}$). Define the worst-case liability*

$$L(S) := \sup_{\omega \in \Omega} \sum_{j \in J} S_j \, R(\omega)_j. \qquad (1)$$

   *The system maintains, at all times,*

$$\mathsf{Treas} \geq L(S). \qquad (2)$$

   *Any operation that changes supplies (including issuance) must preserve solvency. In particular, if issuance changes supplies from $S$ to $S'$, then treasury increases sufficiently:*

$$\Delta\mathsf{Treas} \geq L(S') - L(S). \qquad (3)$$

2. ***Transfer and Fungibility.*** *Holdings are transferable between accounts and transfers conserve per–label totals $S_j$. Shares are fungible within each label: for all $j \in J$, any $\omega \in \Omega$, and any $q \geq 0$, redeeming $q$ units pays $q \, R(\omega)_j$ units of $\mathcal{N}$.*
3. ***Settlement and redemption.*** *If $\mathsf{res}(M) = \omega \in \Omega$, then any holder may redeem: for all $j \in J$ and $q \geq 0$, redeeming $q$ units of label $j$ pays $q \, R(\omega)_j$ units of $\mathcal{N}$. Redemption burns the redeemed shares and debits the treasury by the corresponding payout, preserving the solvency invariant above.*

## 3   Modular Workflow

We now turn to the design landscape of DePMs and step through our modular workflow (*cf.* [27]) of eight stages: underlying infrastructure, market topic, share structure and pricing, trading, market resolution, settlement, and archiving. For

**Table 1.** Classification of selected (for significance or novelty) DePMs using our modular workflow. Keywords used in the table are defined in referenced section, while ●, ◐, ○ respectively infer that the related property is fully, partially or not supported.

| Year | System | Infrastructure (§3.1) | Permissionless Topic (§3.2) | Share Structure (§3.3) | Numeraire (§3.3) | Initial Issuance (§3.4) | Permissionless Trading (§3.5) | Resolution (§3.6) | Settlement (§3.7) | On-Chain Archiving (§3.8) |
|---|---|---|---|---|---|---|---|---|---|---|
| 2014 | Truthcoin [77] | Sidechain | ● | WTA | Pegged BTC | Auto Bookmaking | ● | Vote | Pull | ● |
| 2014 | Princeton [19] | Sidechain | ● | WTA | Pegged BTC | Splitting | ● | Arbiter | Push | ● |
| 2015 | Augur [63] | Smart Contract | ● | WTA | ETH | Auto Bookmaking | ● | Vote | Pull | ● |
| 2019 | Gnosis Sight [7] | Smart Contract | ● | WTA | DAI | Splitting | ● | Arbiter | Pull | ◐ |
| 2019 | Augur [64] | Smart Contract | ● | WTA | DAI | Splitting | ◐, ● | Vote | Pull | ◐ |
| 2020 | Polymarket [66] | Smart Contract | ○ | YNB(-NR) | USDC | Splitting | ◐, ● | Optimistic, Vote | Gasless Pull | ◐ |
| 2020 | Omen [25] | Smart Contract | ◐ | YNB | DAI | Splitting | ● | Optimistic, Vote | Push | ◐ |
| 2021 | Kalshi [46] | Centralized | ○ | YNB | USD | Matching | ○ | Arbiter | Push | ○ |
| 2022 | Zeitgeist [87] | App-chain | ◐ | WTA | Multi | Auto Bookmaking | ○ | Optimistic, Vote | Pull | ◐ |

each stage, we enumerate the possible designs and discuss competing trade-offs, summarized as the columns of Table 1.

> **Research Gap 1.** Can accuracy metrics [33] be used to compare various CePM and DePM platforms? Are there meaningful correlations between accuracy and the market microstructure options in Table 1?

### 3.1   Underlying Infrastructure

Due to page restrictions, we relegate the designs for the underlying infrastructure to Appendix C. It describes various blockchain options and notes that the transparency of a blockchain can lead to copy-trading, posing a research gap related to that.

### 3.2   Market Topic

Due to page restrictions, we relegate the designs for the market topic to Appendix D. It describes the differences between permissioned and permissionless systems for setting up what the market is about. Permissioned topic selection requires a central party, while permissionless designs can have problems with unethical markets (*e.g.,* assassination markets), spam, fragmentation, and poorly defined topics. The appendix also provides important real-world examples of ill-defined market topics that have proven to be problematic. It provides an insight and a research gap related to these points.

### 3.3   Share Structure and Pricing

The core requirement of a prediction market is that wagers are represented by fungible outcome shares. The structure of outcome shares typically falls into one of three categories and two variants (although more exotic structures are possible and explored in research).

**WTA.** The first structure we term *winner-take-all (WTA)* (*a.k.a. categorical*) and was popularized by Iowa Electronic Markets [42]. Consider a market with three possible outcomes: $\Omega = \{\mathsf{A}, \mathsf{B}, \mathsf{C}\}$. A WTA market issues an outcome share for each outcome $J = \{j_\mathsf{A}, j_\mathsf{B}, j_\mathsf{C}\}$. If there are only two outcomes, it is called a *binary market*. If the outcome $\omega$ is $\mathsf{B}$, the share $j_\mathsf{B}$ pays \$1 (or one unit of numeraire $\mathcal{N}$) and the other shares pay \$0. For any $k \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}\}$,

$$R(\omega)_{j_k} = \begin{cases} 1, & \text{if } \omega = \mathsf{k}, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

For a WTA market to be well-functioning, two conditions must hold on outcome shares. (i) They should be *mutually exclusive* so no more than one share wins: $R(\omega)_{j_k} R(\omega)_{j_\ell} = 0 \quad \forall \omega \in \Omega, \forall \mathsf{k} \neq \ell$; and (ii) they should be *complete* so at least one share wins: $\sum_{\mathsf{k} \in \Omega} R(\omega)_{j_k} = 1 \quad \forall \omega \in \Omega$. If they are not mutually exclusive, the operator could be under-collateralized for making all payments (in violation of solvency in Definition 3). If they are incomplete, a deficient market might end with all participants receiving \$0. A consequence is that holding one share for each outcome is equivalent to holding \$1, a fact we will return to in §3.5.

In a WTA market, the price of a outcome share (*e.g.,* $p(j_\mathsf{A}) = \$0.54$) is a proxy for the probability that the outcome will occur (*e.g.,* $\Pr[\omega = \mathsf{A}] = 54\%$). A common adage is the prices of each share sum to \$1.00 ignoring fees and discounting (*e.g.,* $p(j_\mathsf{A}) = \$0.54$, $p(j_\mathsf{B}) = \$0.23$, $p(j_\mathsf{C}) = \$0.23$) but this is imprecise [19]. Outcome shares (like anything) have two prices: a bid price (what a trader is willing to buy for) and an ask price (willing to sell for). If the sum of the bid prices exceeds \$1.00 or if the sum of ask prices are below \$1.00, arbitrageurs have an opportunity to secure risk-free profit through a trade that will erase the condition when fully extracted. This means the sum of bids and sum of asks should result in the bid-ask spread straddling \$1.00 but the amount of the spread could be arbitrarily large. So in user interfaces that display a single 'price' (*e.g.,* the last sale price or the midpoint between the best bid and the best ask), prices may indeed not sum to \$1.00—this is not a market failure, just a misunderstanding.

**YNB.** The second structure we term a *yes-no bundle (YNB)*. YNB markets were popularized by InTrade [43]. A YNB market issues two share labels for each outcome, a 'yes' and a 'no:' $J = \{j_{\mathsf{A}_\mathsf{Y}}, j_{\mathsf{A}_\mathsf{N}}, j_{\mathsf{B}_\mathsf{Y}}, j_{\mathsf{B}_\mathsf{N}}, j_{\mathsf{C}_\mathsf{Y}}, j_{\mathsf{C}_\mathsf{N}}\}$. For any $k \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}\}$,

$$R(\omega)_{j_{k_\mathsf{Y}}} = \begin{cases} 1, & \text{if } \omega = \mathsf{k}, \\ 0, & \text{otherwise.} \end{cases} \qquad R(\omega)_{j_{k_\mathsf{N}}} = \begin{cases} 1, & \text{if } \omega \neq \mathsf{k}, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

Each outcome-specific pair $\{j_{k_\mathsf{Y}}, j_{k_\mathsf{N}}\}$ constitutes a binary WTA market ($\mathsf{k}$ vs. not-$\mathsf{k}$). A YNB market is the union of these pairs, so the WTA exclusivity and completeness properties hold per pair. However exclusivity and completeness do not necessarily hold across all bundles, allowing more flexible markets. For

example, a market on what words Trump will say in a congressional address included Bitcoin (no), beautiful at least 10 times (yes), and Canada (yes).[4] Multiple words can resolve to yes (not exclusive) and it is possible he says none of the listed words (not complete). An established YNB market that is being actively traded, because it is not complete, can have new outcomes added to it fairly, whereas WTA markets must account for every possible outcome at the start of the market (perhaps utilizing an 'other' outcome).

**YNB-NR.** A variant of the YNB market is one where, even though it is not necessary, the yes share outcomes are in fact complete and exclusive. In other words, each yes/no bundle is a WTA market and the set of all yes shares is also a WTA market. We term this YNB variant as *negative risk* (YNB-NR), a term introduced by Polymarket [66]. Recall that in a WTA market, roughly speaking, the share prices sum to \$1 (modulo the fine print about bid/ask spreads above). For a YNB-NR market, the Yes shares sum to \$1, while the No shares will sum to $|\Omega| - 1$.

$$\sum_{\mathsf{k}\in\Omega} R(\omega)_{j_{\mathsf{k}_\mathsf{Y}}} = 1 \quad \text{and} \quad \sum_{\mathsf{k}\in\Omega} R(\omega)_{j_{\mathsf{k}_\mathsf{N}}} = |\Omega| - 1 \quad \text{for all } \omega \in \Omega. \tag{6}$$

The HBO documentary market from Section B is an example of a YNB-NR market (Polymarket markets are either YNB or YNB-NR[5]). This market was intended to be exclusive and complete across bundles by including a bundle for the outcome: 'other/multiple.' Holding a No outcome share for Hal Finney has the same payoff as holding a Yes share for every other candidate. Polymarket introduced a *negRisk* gadget that allows a trader to convert any No share into a portfolio of Yes shares for every other outcome. This enables traders to adjust their positions with less buying/selling on the markets, and also aligns prices between Yes and No markets with low friction arbitrage opportunities. Formally, a single No share has the equivalence (*i.e.,* same payoff ignoring fees and discounting):

$$R(\omega)_{j_{\mathsf{k}_\mathsf{N}}} = \sum_{\ell \in \Omega \backslash \{\mathsf{k}\}} R(\omega)_{j_{\ell_Y}} \quad \text{for all } \omega \in \Omega \text{ and any } \mathsf{k} \in \Omega. \tag{7}$$

While Yes has equivalence to:

$$R(\omega)_{j_{k_Y}} = \sum_{\ell \in \Omega \backslash \{k\}} R(\omega)_{j_{\ell_N}} - (|\Omega| - 2) \tag{8}$$

**Scalar.** A third structure is provided in Appendix E. It is not frequently used.

---

[4] Polymarket: 'What will Trump say during address to Congress?'

[5] Dune Analytics: 'Polymarket - Activity and Volume' compares YNB (called CTF there) and YNB-NR (called negrisk there) statistics.

> **Research Gap 2.** How does a *negRisk* gadget encourage price parity between equivalent positions? Can we quantify its improvements for price execution and trade execution costs? Does a reverse gadget, for converting a single yes share, offer similar benefits?

> **Research Gap 3.** The academic literature has explored advanced market types, including combinatorial markets and establishing conditional probabilities from markets. Implementing and experimenting with these designs for DePMs is open. In sports-betting, chaining together multiple outcomes in an all-or-nothing bet (parlay) is popular but a treatment for DePMs is lacking.

### 3.4   Market Initialization

Options for trading outcome shares can be broken into two steps: (i) how does the first outcome share come into existence and how does the first trader trade, and (ii) how do traders trade once a market has been established? Probably the greatest evolution in DePMs, from Truthcoin to Polymarket, concerns how the first trade happens. There are three options: *automated bookmaking*, *splitting*, and *matching*.

*Automated bookmaking* was popularized through the academic work of Robin Hanson [38,40], researched for Intrade [55], and first suggested for DePMs by Truthcoin [77], which heavily influenced Augur v1 [63].

**Definition 4 (Automated bookmaking).** *Fix a market $M = (\Omega, J, R)$. An automated bookmaker posts (i) a loss fund $\mathsf{Treas} \in \mathbb{R}_{\geq 0}$ in the numeraire $\mathcal{N}$ and (ii) a pricing rule (odds) for labels $j \in J$. It accepts deposits in $\mathcal{N}$ and issues shares, updating the supply vector $S$, and must always satisfy solvency (Definition 3).*

In this model, the operator sets initial prices for each outcome share (equivalent to setting market odds) and collateralizes enough payout money to cover a worst-case loss in its treasury. If Alice is the first trader, she can immediately trade with the operator. The operator is autonomous and sets buy/sell prices algorithmically, originally using Hanson's logarithmic market scoring rule (LMSR) [40]. The key point is that the operator's fund is Alice's counterparty; if Alice wins, the fund loses, and vice-versa. The pros are instant liquidity for the first trader and the cons are the risk to the operator of losing money and the burden of needing to set initial odds (getting them wrong increases the chances it loses).

Acute readers might wonder the relationship between automated bookmaking and an automated market makers (*e.g.,* Uniswap), which are discussed in the next section. Roughly speaking, a WTA market run by automated bookmaking is termed a cost-function prediction market (CFPM) and a CFPM is equivalent in pricing (and trade costs) to an AMM (defined by a set of axioms) with the right invariant [30].

The second approach, *splitting*, was first suggested for DePMs by the Princeton DePM [19] based on the Iowa Electronic Market [42]. Augur switched from

automated book making to splitting in v2 [64], Gnosis implemented splitting in CTF [22], and DePMs built on CTF, including Polymarket [66] and Omen [25], use it.

**Definition 5 (Splitting and merging).** *Fix a market $M = (\Omega, J, R)$ in numeraire $\mathcal{N}$. A* splitting/merging *mechanism provides counterparty-free state transitions for a fixed* unit bundle $B$ *of WTA share labels such that*

$$\sum_{j \in B} R(\omega)_j = 1 \quad \text{for all } \omega \in \Omega.$$

Splitting *maps $1 \cdot \mathcal{N} \mapsto \sum_{j \in B} j$ (minting one unit of each $j \in B$), and* merging *maps $\sum_{j \in B} j \mapsto 1 \cdot \mathcal{N}$ (burning them), typically before resolution. Repeating the operation yields multiple bundles.*

Recall that in a WTA market, exactly one share in a set of shares will payout $1. This means that holding a complete portfolio of every share is equivalent (in payoff, ignoring fees and discounting) to holding $1. A splitting gadget allows a trader to input $1 and receive a portfolio contain 1 share of each outcome. Generally, a *merging* gadget is also available where a complete set can be redeemed for $1 at any time before the market closes. Alice can obtain a set of shares and list asking prices (through a limit order book or by being the first liquidity provider in an AMM) for some or all of the shares, and if Bob is willing to buy a share from Alice, the first trade occurs. The pros to splitting is that the operator has zero exposure to the market, while the con is that Alice must wait for a second trader, Bob, before she can trade.

In YNB markets, each outcome's YES/NO pair is its own two-outcome WTA market. Splitting is per outcome: converting $1 of collateral mints one $j_{k_Y}$ and one $j_{k_N}$ for the chosen k. Across outcomes, supplies are uncoupled—the total minted for the outcome A's bundle need not match that for outcomes B or C.

---

**Insight 2.** If the first trader makes one dollar, someone must lose a dollar. It either needs to be the operator or a second trader. This forces DePMs to choose between needing a loss fund or having no instant liquidity for the first trader.

---

The third approach, *matching*, was used by InTrade [43] and a variant by Fairlay [28], and is used today by Kalshi. We provide a description and research insight in Appendix F.

### 3.5   Trading

Once outcome shares are in circulation, they can be traded any way fungible blockchain tokens can be traded. This includes *centralized exchanges* that custody the tokens and use central order book (CLOBs); *partially decentralized exchanges* where CLOB matching is done off-chain and settlement is done on-chain; or *fully on-chain exchanges*, of which automated market makers (AMMs) are the most common.

Of interest, AMMs were born out of Gnosis' research into automated book-marking for prediction markets. They first developed alternatives to the LMSR rule, including the constant product rule [53]. In parallel, Bancor worked on exchanges where multiple traders could contribute tokens to a common liquidity pool. Uniswap v1 merged these two ideas to create the basic template of an AMM that is common today.

Circling back to automated bookmaking, splitting can be used in conjunction with AMMs to realize automated booking, as first used in Gnosis' closed beta Sight [7]. An operator begins with $2n$ units of the numeraire, $e.g.,$ $2n$ USDC. It takes half of the money, $n$ USDC, and uses the splitting gadget to obtain $n$ shares in each outcome. For each outcome share, it estimates the outcome probability as $p_i$ and starts an AMM with initial liquidity of $n$ outcome shares and $p_i \cdot n$ USDC. It repeats for each outcome. Thus assuming the probabilities sum to 1, the operator has split its remaining $n$ USDC across the AMMs. The operator can lose up to $2n$ USDC in divergence loss, assuming traders can split as well (and thus create the shares necessary to drain the AMM of its USDC), in addition to failing (through stale prices) to realize profits ($i.e.,$ LVR [57]). The important point is that the operator is still solvent per Definition 3 as the $2n$ USDC is either locked in the splitting gadget or locked in the AMM.

Despite the direct lineage between prediction markets and AMMs, AMMs are problematic for prediction market trading. DePM outcome shares behave in specific ways that differ from typical crypto-assets and tokens. The price is strictly bounded between \$0 and \$1, the value of a share can jump to \$0 or \$1 near-instantly when an event outcome is finalized, and once finalized, the price is permanent. When real world events occur, AMMs can be drained faster than liquidity providers can withdraw liquidity.

---

**Research Gap 4.** Adapting AMMs to the unique constraints of predictions markets is at an early stage. Paradigm's pm-AMM tapers liquidity as a scheduled expiry approaches, which helps for events that crystallize over a fixed time horizon [58]; but many markets jump or resolve unexpectedly, falling outside of the model used for the results.

---

When trading on-chain, miners and other users can front-run transactions, an area of study called maximum extracted value (MEV) [23]. Although the term MEV did not exist at the time, the Princeton DePM describes the MEV problem extensively [19] and proposes a mitigation now called a frequent batch auction (FBA) (again, the term FBA was not popularized until later [13]).

---

**Research Gap 5.** Can we measurement MEV extraction for on-chain DePMs? What mechanisms for order-flow privacy apply to on-chain DePMs?

---

A final trading-relevant subject for prediction markets is arbitrage. Arbitrageurs ensure market prices are consistent, for example across all shares in a WTA market or between Yes/No bundles in a YNB market. A recent paper studies combinatorial arbitrage on Polymarket between markets with logically related predicates ($e.g.,$ Republicans win the presidency; Trump wins the pres-

idency) and measures roughly $40M USD of realized arbitrage profits over the measurement period [72].

### 3.6   Market Resolution

Market resolution approaches specify how a DePM determines and finalizes the winning outcome and triggers settlement. Designs vary in where the ground truth comes from (market prices, external sources, or participants), who can influence the decision, and what incentives/penalties secure it. In this section we review: oracle-less designs (on-chain truth, self-settling markets, auto-resolve rules), using a designated arbiter, using a network of reporters, and crowdsourcing a vote. The term *oracle* is commonly used for any of the latter three approaches.

**Oracle-less.** A market topic might reference *on-chain truth* (*e.g.,* total value locked in a DeFi service at the end of the year) in which case resolution can be made directly. A *self-settling market* [11] works with *splitting* and *merging* (see §3.5) of shares; it relies on participants with winning shares to purchase the losing shares (for close to $0) and redeem $1 by merging them. If losing shares do not trade near $0 or become illiquid, the broader market might accept winning shares as a substitute for dollars. If a market outcome is contentious with no recognized winner (*e.g.,* a poorly defined market in §3.2), the market will not settle. An *auto-resolve rule* could also be used such that outcomes are finalized when, say, their token trades above $0.99 for at least $t$ time. Auto-resolve rules are subject to market manipulation (losing shares are wash traded near $1 long enough to finalize, in which case they are worth $1) or griefing attacks (yes shares are traded below $0.99 to prevent finalization). While an auto-resolve rule is too fragile to rely on solely, it could be used optimistically to provide an initial settlement; only disputed cases would be escalated to an oracle [4].

**Designated arbiters.** Typically a CePM will decide events within the platform [45]. A DePM might outsource decisions to a trusted organization, such as the Associate Press (AP) which experimented with writing US election results into Ethereum.[6] From a trust perspective, this is equivalent to using an AP CePM, but from a logistics perspective, it is simpler to AP to be an oracle than to run an entire CePM. Further, it allows *trust agility* where AP can be replaced by a competing source with minimal disruption [19]. A DePM might also used a designated party only as a last resort if other methods lead to a contentious result [71].

Recently interest is in evaluating arbitration through an AI system [15]. A 2025 Chainlink study poses 1,660 Polymarket questions to LLMs and reports 89.3% accuracy (sports 99.7%, politics 84.3%) with temporal-reasoning challenges [88]. AI can also be used in agent-mode, tasked with actively gathering

---

[6] Etherscan: `https://etherscan.io/address/0x0792724900B551d200D954a5Ed709d9514d73A9F`

evidence and reporting if resolution can be reached [15]. AI oracles are potentially vulnerable to adversarial manipulation and poisoning attacks [89], and may recall incorrect facts that are incorrectly stated in the training data. An over-reliance on AI systems in generating news, trading in markets based on news, and settling markets based on news could result in bad interactions or negative feedback loops.

**Reporter networks.** Some oracle systems focus on quickly reporting on updating values [12], such as an asset price or a sports score which could naturally settle some types of prediction markets, such as rapid markets from Augur Turbo [5] and Polymarket [67]. Generally a set (or network) of arbiters (or reporters) will report the value and an aggregation method (*e.g.,* median value or a mean value after outlier filtering for quantitative data, mode for qualitative) will update the value on-chain [27]. Updates are emitted when deviation or heartbeat thresholds are met, giving explicit control over latency/recency and bounding staleness under network stress. A DePM can read the aggregator at a fixed resolution time and settle without discretionary intervention [5,79].

**Crowdsourced vote.** A final mechanism is to determine off-chain facts by polling a set of willing participants [14,77,63,64,81,50]. This procedure is defined by four design choices:

1. *Electorate*: participants stake governance tokens to enrol and votes are either held with all participants, or with a randomly selected subset of all participants.
2. *Ballots:* may be visible to other participants or may be hidden until voting closes (typically with a two-round commit-reveal protocol but more sophisticated methods could be used [32]).
3. *Aggregation:* votes are weighed by the amount of staked tokens, categorical questions are decided by plurality (perhaps with minimum quorum) while quantities with a median or smoothed mean.
4. *Incentives:* participants who affirmed the final result in their individual votes receive rewards, while those who did not will at least forgo rewards, but might also have their participation tokens slashed.

The precise parameters of these systems vary significantly across many different designs, while deployed systems like UMA's data verification mechanism (DMV) [81] and Kleros [50] have settled billions of dollars. Topics like fee mechanisms and proof of stake consensus protocols have received much academic attention, but incentive-compatible designs and formal proofs for oracles is largely under-explored. By contrast, a growing theoretical line proposes truth-elicitation schemes with formal guarantees [69,74]. However in practice, uptake is absent, in part because these designs are complex to run, sensitive to Sybil attacks, and can fail if voters rely on a common source of information.

Token votes for DePMs are hostile environments where an attacker's external payoff from a wrong resolution exceeds the system's economic security,

which can lead to failure [29]. Rational voters are incentivized to agree with the majority, rather than necessarily reporting the ground truth (a situation colloquially known among economists as a Keynesian beauty contest). The system often works because the ground truth is an obvious point where participants will coordinate (known as a Schelling point), however voters might fear voting for truth if large token holders (whales) visibly stake on a wrong outcome early in the vote. An example[7] occurred on Polymarket [70], leading to concerns of token concentration within the UMA token. At the time of writing, the top five UMA wallets UMA control  45.6% of votes and the top 13 exceed 65%, enough to meet the passing threshold.[8] If successful attacks depress token prices, the attacks become cheaper, potentially creating a spiral (*cf.* [48]).

These concerns affirm design decisions like a secret ballot, using subsets of participants in a vote (potentially split by subject expertise), and redrawing larger panels on appeal with higher bonds/fees to raise capture costs only when disputes persist.

---

**Research Gap 6.** Deciding market outcomes is a uniquely DePM problem (since a CePM can arbitrate its own markets). Can we bring a theoretical lens to deployed oracle voting systems and understand what formal guarantees about incentives and safety can be made?

---

A DePM will probably use a *hybrid* or *chained approach* that does not rely on a single method. For example, an arbiter from an allowlist might be able to propose a market outcome while also allowing disputes from anyone. If an outcome is disputed, it is escalated to a crowdsourced vote. If the vote is considered defective, a further escalation could allow an Admin account to overrule the decision. The ultimate backstop is the law which would not stop a wrong outcome but could be used to remunerate parties damaged by it.

### 3.7   Settlement

Once the market is resolved, a DePM will enable each winning share to be converted into 1 unit of the numeraire (*e.g.,* 1 USD in a stablecoin) and transferred into the user's self-custody. While a DePM in theory could *push* payouts to users, it is common to wait for the user to initiate the redemption—a *pull* mechanism [22]. In this case, users pay the gas cost of the redemption which requires users to hold the native currency of the underlying blockchain. Polymarket offers gasless withdrawals (using OpenGSN relayers [35]), however users can bypass this at their choice. In a pull model, some users may not redeem their shares in a timely manner—a DePM may opt to sweep this surplus into its own capital or burn it, but DePMs generally hold it on-chain in perpetuity. As with any smart contract allowing withdraws based account balances, hardening against reentrancy attacks is critical.

---

[7] Polymarket: 'Ukraine agrees to Trump mineral deal before April?'
[8] Dune Analytics: $UMA Voting Participation

The slogan 'sweat the game, not the payout [31]' is used to differentiate regulated sportsbook operators from 'neighbourhood bookies,' however even legitimate operators in the US have allegedly denied payouts using a legal loophole.[9] The advantage of a DePM in this context is two-fold: (i) payouts are fully (or largely) autonomous, not subject to human discretion, and (ii) the share structure ensures the operator has zero risk (or predetermined bounded risk, in the case of automated bookmaking) and is therefore financially indifferent to making any fair payout (see the solvency axiom in Definition 3).

---

**Insight 3.** A prediction market has no need to fight against paying out a bet the way bookmakers have in practice [31]. When operations are on-chain, solvency can be demonstrated directly from blockchain data.

---

### 3.8   Archiving

Due to page restrictions, we relegate the designs for archiving markets to Appendix G. It describes how a market can be reconstructed after the fact, through a mix of on-chain data and off-chain data collected by the operator and possibly offered through APIs. It also presents a research gap related to this.

## 4   Conclusion

Researchers and builders have used a set of shifting designs, definitions, and vocabulary for DePMs. We aim to provide a modular framework that is useful for careful comparison between systems with different design choices, showcasing the full set of choices available, uncovering unsolved research problems, understanding the history of DePM ideas, and providing a learning resource for those wanting to catch up on DePMs. Our taxonomy does not identify a single best design but helps illustrate the trade-offs between them.

## References

1. Adelman, J.: A disputed election would mean long delays in betting market payouts. here's how the winner gets decided. Barron's (31 Oct 2024)
2. Almeida, L.: Gambling platform polymarket not paying bets on us invasion of venezuela. The Guardian (January 2026)
3. Arrow, K.J., Forsythe, R., Gorham, M., Hahn, R., Hanson, R., Ledyard, J.O., Levmore, S., Litan, R., Milgrom, P., Nelson, F.D., Neumann, G.R., Ottaviani, M., Schelling, T.C., Shiller, R.J., Smith, V.L., Snowberg, E., Sunstein, C.R., Tetlock, P.C., Tetlock, P.E., Varian, H.R., Wolfers, J., Zitzewitz, E.: The promise of prediction markets. Science **320**(5878) (2008)

---

[9] A law protects sports books from obvious errors, like a 'fat finger' when setting odds, but can be misused to claim long-shot bets were 'obvious mistakes' after the fact [31].

4. Scaling augur part 2, a roadmap (2015), `https://augur.mystrikingly.com/blog/scaling-augur-part-2-a-roadmap`
5. Augur turbo, `https://github.com/AugurProject/turbo`
6. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains. Tech. rep., Blockstream (2014)
7. Barnes, G.: Gnosis: How to build a regulated prediction market (talk). In: DeFi Summit London (2019)
8. Baum, C., Chiang, J.H.y., David, B., Frederiksen, T.K.: SoK: Privacy-Enhancing Technologies in Finance. In: 5th Conference on Advances in Financial Technologies (AFT 2023). Leibniz International Proceedings in Informatics (LIPIcs), vol. 282, pp. 12:1–12:30. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2023). `https://doi.org/10.4230/LIPIcs.AFT.2023.12`, `https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.AFT.2023.12`
9. Becker, S.: Hbo bitcoin doc 'money electric' hunts for satoshi nakamoto— see a first look at the trailer. Fast Company (3 Oct 2024)
10. Beganski, A.: Crypto betting has turned hbo's satoshi nakamoto reveal into a 'sporting event': Director. decrypt.co (7 Oct 2024)
11. Bentov, I., Mizrahi, A., Rosenfeld, M.: Decentralized prediction market without arbiters. In: Financial Cryptography and Data Security: FC 2017 International Workshops. pp. 199–217 (2017)
12. Breidenbach, L., Cachin, C., Coventry, A., Juels, A., Miller, A.: Chainlink off-chain reporting protocol. `https://blog.chain.link/off-chain-reporting-live-on-mainnet/` (2021), accessed: 2025-06-24
13. Budish, E., Cramton, P., Shim, J.: The high-frequency trading arms race: Frequent batch auctions as a market design response. The Quarterly Journal of Economics **130**(4), 1547–1621 (2015)
14. Buterin, V.: Ethereum: A next-generation smart contract and decentralized application platform. Tech. rep., Ethereum Foundation (2013), `https://ethereum.org/whitepaper/`
15. How chaos labs built a multi-agent system for resolution in prediction markets. LangChain Blog (2024), `https://blog.langchain.com/how-chaos-labs-built-a-multi-agent-system-for-resolution-in-prediction-markets/`
16. Chatzigiannis, P., Baldimtsi, F., Chalkias, K.: Sok: Blockchain light clients. In: International Conference on Financial Cryptography and Data Security. pp. 615–641. Springer (2022)
17. Chayka, K.: The crypto betting platform predicting a trump win. The New Yorker (23 Oct 2024)
18. Clack, C.D.: Languages for smart and computable contracts. Tech. rep., Centre for Blockchain Technologies, UCL (2021)
19. Clark, J., Bonneau, J., Felten, E.W., Kroll, J.A., Miller, A., Narayanan, A.: On decentralizing prediction markets and order books. In: WEIS. vol. 188 (2014)
20. Cliff, D., Hawkins, J., Keen, J.E., Lau-Soto, R.: Implementing the BBE agent-based model of a sports-betting exchange. In: Proceedings of the 33rd European Modeling & Simulation Symposium (EMSS 2021) (2021)
21. Crawford, V.P., Sobel, J.: Strategic information transmission. Econometrica: Journal of the Econometric Society pp. 1431–1451 (1982)
22. Conditional tokens contracts, `https://conditional-tokens.readthedocs.io/en/latest/index.html#`

23. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In: 2020 IEEE Symposium on Security and Privacy (SP) (2020)
24. Dubin, J.D.: Blockchain prediction markets: Where they came from, why they matter & how to regulate those involved. Washington University Law Review **97**, 575 (2019)
25. dxDAO: Omen prediction market documentation. `https://dxdocs.eth.limo/docs/Products/omen/` (unknown), accessed: 2025-09-07
26. Eskandari, S., Clark, J., Sundaresan, V., Adham, M.: On the feasibility of decentralized derivatives markets. In: Financial Cryptography and Data Security: FC 2017 International Workshops. pp. 553–567 (2017)
27. Eskandari, S., Salehi, M., Gu, W.C., Clark, J.: Sok: Oracles from the ground truth to market manipulation. In: Proceedings of the 3rd ACM Conference on Advances in Financial Technologies. pp. 127–141 (2021)
28. Fairlay prediction market, `https://github.com/fairlay`
29. Ford, B., Böhme, R.: Rationality is self-defeating in permissionless systems (2019)
30. Frongillo, R., Papireddygari, M., Waggoner, B.: An axiomatic characterization of cfmms and equivalence to prediction markets. Innovations in Theoretical Computer Science Conference (ITCS) (2024)
31. Funt, D.: He hit three monster bets — and then the sportsbook wouldn't pay. The Washington Post (2024)
32. Glaeser, N., Seres, I.A., Zhu, M., Bonneau, J.: Cicada: A framework for private non-interactive on-chain auctions and voting. Cryptology ePrint Archive (2023)
33. Gneiting, T., Raftery, A.E.: Strictly proper scoring rules, prediction, and estimation. Journal of the American statistical Association **102**(477), 359–378 (2007)
34. Gnosis: Gnosis whitepaper. `https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/Gnosis.pdf` (2017), accessed: 2025-06-01
35. The ethereum gas stations network, `https://github.com/opengsn/gsn`
36. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: Sok: Layer-two blockchain protocols. In: Financial Cryptography (2020)
37. Gunter, J.: Post from @jillrgunter. X.com (2024), `https://x.com/jillrgunter/status/1854083649031086147`
38. Hanson, R.: Combinatorial information market design. Information Systems Frontiers **5**, 107–119 (2003)
39. Hanson, R.: Insider trading and prediction markets. JL Econ. & Pol'y **4**, 449 (2007)
40. Hanson, R.: Logarithmic markets coring rules for modular combinatorial information aggregation. The Journal of Prediction Markets **1**(1), 3–15 (2007)
41. Heimbach, L., Wattenhofer, R.: Sok: Preventing transaction reordering manipulations in decentralized finance. In: Proceedings of the 4th ACM Conference on Advances in Financial Technologies. pp. 47–60 (2022)
42. Iowa electronic markets, `https://iemweb.biz.uiowa.edu/about-iem/`
43. Intrade: How does it work?, `https://web.archive.org/web/20100502022133/http://www.intrade.com/jsp/intrade/help/howitworks.html`
44. Kalodner, H., Goldfeder, S., Chen, X., Weinberg, S.M., Felten, E.W.: Arbitrum: Scalable, private smart contracts. In: USENIX Security (2018)
45. Kalshi: Market rules, `https://help.kalshi.com/markets/markets-101/market-rules`
46. Kalshi: Kalshi api documentation. `https://docs.kalshi.com/welcome` (unknown), accessed: 2025-09-08

47. Kanani, J., Nailwal, S., Arjun, A.: Matic whitepaper. Tech. rep., Polygon Technology (2021)
48. Klages-Mundt, A., Minca, A.: (in) stability for the blockchain: Deleveraging spirals and stablecoin attacks. Cryptoeconomic Systems (2021)
49. Koessler, F., Noussair, C., Ziegelmeyer, A.: Parimutuel betting under asymmetric information. Journal of mathematical Economics **44**(7-8), 733–744 (2008)
50. Lesaege, C., George, W., Ast, F.: Kleros: Long paper (v2.0.2). Tech. rep., Self-published (2021)
51. Lin, Z., Wang, T., Shi, L., Zhang, S., Cao, B.: Decentralized physical infrastructure networks (depin): Challenges and opportunities. IEEE Network (2024)
52. Loporchio, M., Di Francesco Maesa, D., Bernasconi, A., Ricci, L.: Analyzing erc-1155 adoption: A study of the multi-token ecosystem. In: International Conference on Complex Networks and Their Applications. pp. 385–397. Springer (2024)
53. Lu, A.: Building a decentralized exchange in ethereum (2017)
54. Mattmuller, K.: Decentralized prediction markets. Georgetown Law Technology Review **8**, 384 (2024)
55. McClusky, P.: Automated market maker for certain intrade contracts (2008), `https://www.bayesianinvestor.com/amm/`
56. Milionis, J., Ernstberger, J., Bonneau, J., Kominers, S.D., Roughgarden, T.: Incentive-compatible recovery from manipulated signals, with applications to decentralized physical infrastructure. arXiv preprint arXiv:2503.07558 (2025)
57. Milionis, J., Moallemi, C.C., Roughgarden, T., Zhang, A.L.: Quantifying loss in automated market makers. In: Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security. pp. 71–74 (2022)
58. Moallemi, C., Robinson, D.: pm-amm: A uniform amm for prediction markets (2024), `pm-AMM:AUniformAMMforPredictionMarkets`
59. Moin, A., Sekniqi, K., Sirer, E.G.: Sok: A classification framework for stablecoin designs. In: Financial Cryptography (2020)
60. Moosavi, M., Clark, J.: Lissy: Experimenting with on-chain order books. In: FC Workshops (WTSC) (2023)
61. Optimisim docs, `https://docs.optimism.io`
62. Ovezik, C., Karakostas, D., Kiayias, A.: Sok: A stratified approach to blockchain decentralization. In: International Conference on Financial Cryptography and Data Security. pp. 128–155. Springer (2024)
63. Peterson, J., Krug, J.: Augur: a decentralized, open-source platform for prediction markets. Tech. rep., Self-published (2015), `www.augur.net`
64. Peterson, J., Krug, J., Zoltu, M., Williams, A.K., Alexander, S.: Augur: a decentralized oracle and prediction market platform (v2. 0). Whitepaper, https://augur. net/whitepaper. pdf (2019)
65. plotx: Github profile: plotx. `https://github.com/plotx` (unknown), accessed: 2025-09-08
66. Polymarket documentation, `https://docs.polymarket.com`
67. Polymarket partners with chainlink to enhance accuracy of prediction market resolutions. PR Newswire (2025)
68. PredictIt FAQ: Predictit frequently asked questions. `https://www.predictit.org/support/faq` (unknown), accessed: 2025-09-08
69. Prelec, D.: A bayesian truth serum for subjective data. science **306**(5695), 462–466 (2004)
70. Reynolds, S.: A contentious ukraine bet leads to clash between polymarket, uma communities. CoinDesk (2025)

71. Reynolds, S.: Update: Polymarket says it's 'conclusive' barron trump was involved in $djt. CoinDesk (27 Jun 2024)
72. Saguillo, O., Ghafouri, V., Kiffer, L., Suarez-Tangil, G.: Unravelling the probabilistic forest: Arbitrage in prediction markets. Adavances in Financial Technology (2025)
73. Saleh, F.: Prediction markets directory, `https://frontseat.co/prediction-markets`
74. Srinivasan, S., Karger, E., Chen, Y.: Self-resolving prediction markets for unverifiable outcomes. In: Proceedings of the 26th ACM Conference on Economics and Computation. pp. 547–573 (2025)
75. Sx network docs, `https://docs.sx.technology`
76. Sztorc, P.: Truthcoin: Faq (2014), `http://truthcoin.info/faq/`
77. Sztorc, P.: Truthcoin: Trustless, decentralized, censorship-proof, incentive-compatible, scalable bitcoin prediction marketplace (v1.1). Tech. rep., Self-published (2015)
78. Thaler, R.H., Ziemba, W.T.: Anomalies: Parimutuel betting markets: Racetracks and lotteries. Journal of Economic perspectives **2**(2), 161–174 (1988)
79. Thales markets documentation, `https://docs.thalesmarket.io/`
80. Uedan, H., Li, Y., Sakiyama, K., Miyahara, D.: Parimutuel betting on blockchain: A case study on horse racing. In: International Conference on Advanced Information Networking and Applications. pp. 177–187. Springer (2025)
81. Uma data verification mechanism: Adding economic guarantees to blockchain oracles (2020), `https://github.com/UMAprotocol/whitepaper/blob/master/UMA-DVM-oracle-whitepaper.pdf`
82. Werner, S., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.: Sok: Decentralized finance (defi). In: Proceedings of the 4th ACM Conference on Advances in Financial Technologies. pp. 30–46 (2022)
83. Whitaker, N., Mazlish, J.Z.: Why prediction markets aren't popular. Works in Progress **15** (2024)
84. Wolfers, J., Zitzewitz, E.: Interpreting prediction market prices as probabilities. Tech. rep., National Bureau of Economic Research (2006)
85. Yaffe-Bellany, D., Griffith, E.: Betting on the election and on the economy. New York Times (26 Oct 2024)
86. Yakovenko, A.: Solana: A new architecture for a high performance blockchain v0. 8.13. Tech. rep., Self-published (2018)
87. Zeitgeist documentation, `https://docs.zeitgeist.pm`
88. Zintus-art, K., Vass, B., Ward, J.: Empirical evidence in ai oracle development. Tech. rep., Chainlink (2025)
89. Zou, W., Geng, R., Wang, B., Jia, J.: {PoisonedRAG}: Knowledge corruption attacks to {Retrieval-Augmented} generation of large language models. In: 34th USENIX Security Symposium (USENIX Security 25). pp. 3827–3844 (2025)

## A   List of DePMs

1. **Bets of Bitcoin** (2011–2014): Centralized event wagering system with BTC as numeraire. Promoted as a prediction market but mechanically it used parimutuel betting. Went offline unannounced with some user funds stuck.
2. **BitBet** (2012–2020): Centralized event wagering system with BTC as numeraire. Promoted as a prediction market but mechanically it used parimutuel betting. Disruption in 2016 and winddown in 2020.
3. **Predictious** (2013–?): Centralized prediction market and CLOB with BTC as numeraire. Promoted as InTrade successor. Appears abandoned in late 2010s.
4. **Fairlay** (2014–present): Centralized prediction market with BTC as numeraire. Traders were matched on a CLOB (back/lay mechanism). After ownership changes, still operating as Bitcoin Betting.
5. **BetMoose** (2014–present) Centralized event wagering system with BTC as numeraire. Promoted as a prediction market but mechanically it used parimutuel betting or back/lay. Still active.
6. **Truthcoin / Bitcoin Hivemind** (2014): Decentralized prediction market (DePM) design with follow-up refinements with some code artifacts. Inspired other DePMs (particularly around automated book making and token vote market resolution) and sidechain technologies.
7. **'Princeton' DePM** (2014): Decentralized prediction market (DePM) design as an academic paper only. Inspired other DePMs (particularly around share splitting/merging), on-chain CLOBs (frequent batch auctions) and the concept of MEV.
8. **Augur** (2015–present): DePM whitepaper design, later deployed on Ethereum (live in 2018) and Polygon (2021). Numeraire is DAI and later USDC. Native token (REP) used in market resolution was one of Ethereum's first ICOs (2015). Still active. Front-ends for Augur include **Predictions.Global**, **Veil**, **Gueser**, and **Helena Network**.
9. **BitShares Prediction Markets** (2015–present): DePM functionality was added to the BitShares 2.0 blockchain to support WTA markets and hybrid on/off-chain CLOBs. DePM functionality dormant. BitShares itself is still active but usage has heavily declined.
10. **Gnosis** (2015–present): DePM whitepaper design for Ethereum. Ran closed beta (sight.pm). Pivoted to developing underlying infrastructure for DePMs, including the widely used Conditional Tokens Framework (CTF). Co-built Omen based on CTF. Also known for self-custody wallets (Gnosis Safe) and AMM-relevant research (proposing the constant product market maker). Still active.
11. **Stox** (2017–2018): Centralized prediction market and CLOB with custom ERC20 token STX as numeraire. Known for celebrity promotions. Abandoned around 2018 after legal issues.
12. **Delphy** (2017–?): Prediction aggregator deployed on Ethereum for mobile devices based on points/leaderboard ('play money') rather than money. Appears to have been abandoned within 2-3 years.

13. **Bodhi** (2017–?): DePM deployed on Qtum blockchain and later Ethereum. Appears to have been abandoned within 2-3 years.
14. **BlitzPredict** (2018–2019): Prediction aggregator on Ethereum that appears to have been abandoned before being developed into a full DePM.
15. **SportX** (2018–): Sports-centric DePM deployed on Ethereum, Polygon, and later its own EVM chain (SX Network). Still active.
16. **BetProtocol** (2018): Toolkit for DePM infrastructure using custom ERC20 token BEPRO. Bepro Network pivoted in 2021 and no active development on toolkit since.
17. **Sharpe Capital** (2017–2019): Prediction aggregator on Ethereum that appears to have been abandoned before being developed into a full DePM.
18. **Amoveo** (*ca.* 2018–?): DePM functionality into state-channels on a custom PoW L1 chain. Sporadic ongoing development.
19. **SEER** (2018–?): DePM deployed on custom Graphene-based DPoS L1 chain with custom SEER token as numeraire. Appear abandoned as of 2020.
20. **Veil** (2019): DePM front-end built on Augur and 0x. Launched and shut down within 2019.
21. **PredIQt** (2019–?): DePM deployed on EOSIO with IQ/EOS as numeraire. Project pivoted to encyclopedia IQ.wiki and PredIQt appears inactive.
22. **Catnip.exchange** (2019): DePM front-end for Augur v1 that composed with Balancer AMMs for trading outcome shares. Discontinued after 2020 US presidential election.
23. **Flux Protocol** (2019–2022): DePM deployed on Ethereum and later NEAR. Appears dormant after 2022.
24. **Thales** (2019–2022): Event wagering system deployed on Ethereum and later NEAR. Market resolution with Chainlink. Largely dormant after 2022.
25. **Omen** (2020–present): DePM built with Gnosis CTF, deployed on Ethereum and later Gnosis Chain (xDai) and Polygon with any ERC20 as numeraire. Market resolution with Reality.eth and Kleros. Still active.
26. **Polymarket** (2020–present): DePM built with Gnosis CTF, deployed on Polygon with USDC as numeraire. First DePM to receive wide mainstream coverage in the media. Market resolution with UMA. Still active but restricted in some jurisdictions (including the US).
27. **PlotX v1** (2020–2022): DePM deployed on Ethereum and later Polygon. Specialized for crypto price predictions. PlotX still active but 2022 pivot left DePM functionality dormant.
28. **Reality Cards** (2020–2022): DePM deployed on Ethereum and later Gnosis and Polygon. Outcomes shares are NFTs that can be rented with payouts based on how long a user held the winning NFT (time-weighted to compensate early traders more). Appears abandoned in 2022.
29. **Prosper** (2021–present): DePM deployed on Avalanche and BSC. Still active.
30. **Zeitgeist** (2021–present): DePM deployed into the logic of a parachain (custom L1) in the Polkadot/Kusama ecosystem (L0). Still active.
31. **Polkamarkets** (2021–present): DePM toolkit for EVM chains like Polygon and Moonriver with any ERC-20 as numeraire (and custom ERC20 POLK for governance). Still maintained.

32. **Hedgehog Markets** (2021–?): Event wagering platform deployed on Solana with USDC as numeraire. Supports both no-loss contests and prediction markets. Appears dormant after 2022.
33. **Unihedge** (2021): DePM design for EVM with an experimental prototype. Outcomes shares are structured different than a typical prediction market (lots implementing what is known as a Harberger-tax).
34. **Mojito Markets** (2022–present): DePM designed for Aptos but not yet deployed.
35. **Insight Prediction** (2024–present): CePM with blockchain-based payments in various stablecoins, including USDC. Still active.
36. **Moonopol** (2024–present): DePM deployed on Solana with USDC as numeraire. Still active.
37. **Miscellaneous**: There are decentralized event wagering systems (or toolkits) that deploy betting structures different from prediction markets. For the earliest systems using such an adjacent approach, we have included them above. However we do not expand on every follow-up project. These include: **Wagerr**, **BetDEX**, **Monaco Protocol**, **Peerplays**, **DexWin**, **DuelDuck**, **BetterFan**, **Oriole Insights**, **BetSwag.gg** and **Azuro**. We also note here the most prominent CePMs: **Kalshi**, **PredictIt**, **Futuur**, and **Manifold**.

## B    Satoshi HBO Market

Before diving deep on the mechanics of decentralized prediction markets, we illustrate how markets work with a lighthearted example. On 3 Oct 2024, a trailer was released with press coverage of a new HBO documentary on Bitcoin to air about a week later on 8 Oct 2024. In an interview, the director stated, the film would question Satoshi's anonymous identity and, 'who we land on is unexpected and is going to result in a fair amount of controversy. [9]' The next day, Polymarket setup a market for speculating on who the documentary would name, providing 15 names plus an 'other/multiple' option.[10] A benefit of a decentralized prediction market is allowing niche topics for markets, unlikely to attract mainstream betting websites—in this case, attracting \$44M USD in trading volume. Having an 'other' option is also critical after many markets have failed to fully articulate every eventuality and in this case, the winner, was not one of the original 15 names (see Section 3.2).

In game theory, *cheap talk* describes strategic misinformation or signalling aimed at shaping beliefs or prices, provided the cost of deception is outweighed by the potential payoff [21]. This is well illustrated by what followed in the HBO Satoshi market as new pieces of evidence emerged, some real and some fake, with some fakes relatively elaborate (professional appearing end-credits or hijacking a target's X.com account) as summarized in Table 2. Further details are provided in Appendix 7.

---

[10] Polymarket: 'Who will HBO doc identify as Satoshi?'

**Table 2.** Over a few days, truthful and untruthful ('cheap talk') evidence was presented to traders. The market reacted to correct signals and effectively filtered out fake signals, demonstrating a beneficial feature of prediction markets.

| Date | Information | Market Impact | Hindsight Verdict |
|---|---|---|---|
| 05 Oct | A long-dormant X account belonging to someone who had corresponded with Sassaman on Twitter posts a new message stating they were interviewed for the documentary. | Immaterial | Fake |
| 05 Oct | Partially redacted leaked email from an HBO executive implies Len Sassaman. | Immaterial | Fake |
| 07 Oct | CNN piece states director 'confronts' Satoshi suspect 'face-to-face' ruling out Sassaman, David Klieman, and Hal Finney. | Material | Truthful |
| 07 Oct | Samson Mow, featured in the trailer, speculates it will name Adam Back. | Material | Wrong but factual basis |
| 07 Oct | End credits of documentary leak featuring a tribute to Klieman. | Immaterial | Fake |
| 07 Oct | Mow states Nick Szabo refused to discuss with director implying he was not 'confronted'. | Material | Truthful |
| 07 Oct | Widow of Sassaman states she was not interviewed. | Moderate | Truthful |
| 08 Oct | A scene with Todd leaked but inconclusive if it is film's thesis. | Material | Truthful |
| 08 Oct | Peter Todd confirms being confronted for documentary but unsure if he will be named. | Material | Truthful |
| 08 Oct | Polymarket commenter claims screen test names Nick Szabo. | Immaterial | Fake |
| 08 Oct | Fortune movie review discloses Todd is named | Very Significant | Truthful |
| 08 Oct | Documentary airs and names Todd | Very Significant | Conclusive |

Also of interest is how the prediction market did not obviously extract *insider information* which is in violation of what theory would predict [39]. The director did state he did not participate in the market and advised his team working on the film not to either [10]. Friction for novice users is also high: web3 apps have a learning curve and if insiders were based at HBO in the US, access would require circumvention of Polymarket's geofencing. Perhaps these reasons kept insiders out of the market for the 5 days it ran. By contrast, allegations of insider trading have be levelled in other markets, including the removal of Nicolas Maduro from power immediately before his seizure by the United States military [2].

**Research Gap 7.** Can insider trades be classified from blockchain data with reasonable percision? Are occurrences higher on unregulated markets? Are markets with insider trading more accurate? What correlations exist between insider trading activity and market metrics (price, liquidity, *etc.*)?
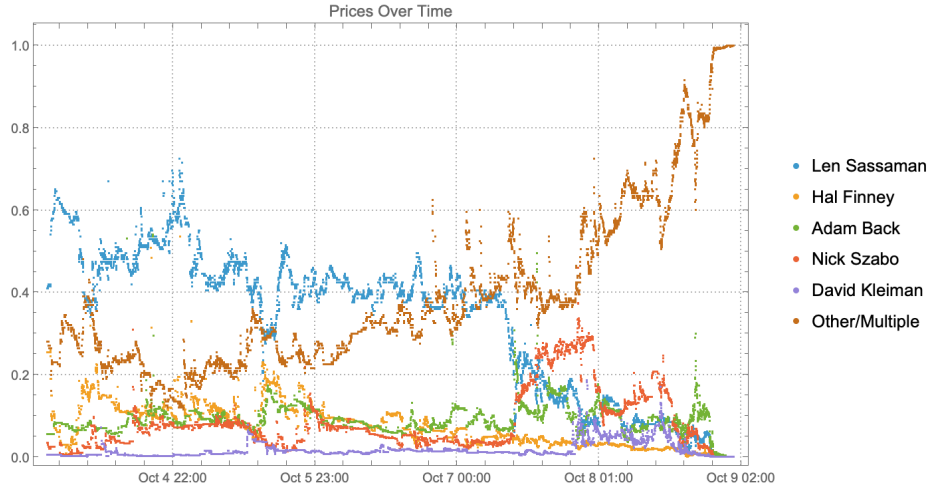


**Fig. 1.** The price movements for 6 leading candidates in the Polymarket market for who would be named as Satoshi Nakamoto in the HBO documentary 'Money Electric' which aired the evening of October 8.

## C    Underlying Infrastructure

In theory, a decentralized and permissionless system might run on something other than a blockchain, but blockchain technology underlays all known DePMs. The earliest (pre-Ethereum) research was in agreement that Bitcoin Script was not powerful enough to operate a DePM, and a *sidechain* [6] would be required [77,19]. Today, projects tend to run as *smart contracts* on an Ethereum competitor (*e.g.,* Polygon [47] or Solana [86]) or an Ethereum L2 (*e.g.,* Arbitrum [44] or Optimism [61]). There are no strong qualitative differences between the underlying blockchain—it is a choice driven by fees, user base, and supporting infrastructure. One other approach (*e.g.,* Zeitgeist [87] or SX Network [75]) is to put the prediction market logic into the blockchain rules themselves on a custom *app-chain*.

A near universal difference between any CePM and DePM is that a DePM allows outcome shares to be withdrawn from the platform, typically in a form compliant with a token standard such as ERC-20 or the more efficient ERC-1155 [52]. Withdrawing outcome shares allows traders to exchange tokens outside
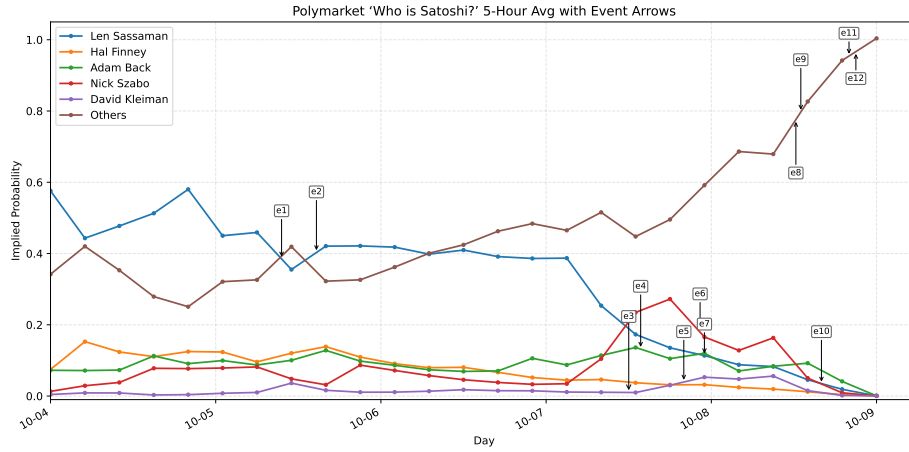
**Fig. 2.** A variation of Figure 1 with smoothing and super-imposed with the events (e1–e12) listed in Table 2.

of the platform and to compose with third party DeFi services, including on-chain trading, lending, and leverage [82].

Perhaps the biggest evolution in DePM design is infrastructure [37]. Early DePMs were monolithic, single-vendor codebases. Modern DePMs are built from existing infrastructure, which composes through highly standardized interfaces. For example, Polymarket's core DePM code is Gnosis' conditional token framework [22]. The numeraire is Circle's USDC stablecoin, which can be bought with a credit card through MoonPay. Trading outcome shares and USDC works out-of-the-box on any platform (on- or off-chain) that supports ERC-1155 tokens. Market outcome disputes are escalated to UMA's DVM oracle [81]. Polymarket also uses third party services for bridging assets, embedded wallets (based on email verification), and EIP-3009 gasless withdrawals. Beyond software engineering benefits, building a service by composing modules can enhance trust agility, which is the ability to quickly swap out modules that are faulty or malicious. For example, Polymarket could switch from UMA to say Chainlink or Kleros, with less effort than if the oracle service was vertically integrated.

---

**Research Gap 8.** On-chain markets provide open information about the trading strategies of other traders who do not deliberately and successfully obfuscate their trades and identities. Can we classify copy traders and measure occurrences? Is copy trading profitable? Under what conditions? Is there a negative impact on market accuracy due to cascading/herding effects?

**Table 3.** Some pitfalls that illustrate the difficulty in properly defining a prediction market topic, collected through our literature review and manual observation of top markets on Polymarket over 2024–2025.

| Pitfall | Description |
|---|---|
| Borderline Categories | *Example*: A market on whether Zelensky would wear a *suit* was contested when he wore a single-breasted jacket with patch chest pockets and matching trousers;[11] media equivocated on describing it as a suit.[12] Other ambiguities include whether enforcement against TikTok in the US constitutes a *ban*,[13] or if finding debris from the Titan submersible constitutes it being *found*.[14] |
| | *Mitigation*: Clearly state inclusion/exclusion criteria (*e.g.,* a subsequent market on a potential hug between Trump and Putin spent a paragraph defining a hug.[15]) |
| Precedence Gaps | *Example*: A proposition bet on the colour of the 2014 Super Bowl 'Gatorade shower' was contested when the coach was showered twice with different colours [19]. A market on whether Zelensky would be 'the' 2022 TIME Person of the Year was contested when both Zelensky and the Spirit of Ukraine were named.[16] |
| | *Mitigation*: Parse the predicate for any statements needing explicit precedence (*e.g.,* first, majority, primary); or establish a payout rule for ties; or include an outcome for 'multiple.' |
| Hidden Presumptions | *Example*: A market concerning a divorce presumes the couple are married (as opposed to common law) which was unknown.[17] |
| | *Mitigation*: Parse the predicate for any presumptive statements and remove/address them. |
| No Ground Truth | *Example*: A market on whether a US strike destroyed an Iranian nuclear facility was contested when each country reported different outcomes and no neutral third party was granted access to the site.[18] A market on whether Baron Trump was 'involved' in the $DJT memecoin lacked an authoritative source.[19] An election market on Venezuela's president was contested when the government declared Maduro won, while international media and democracy watchdogs declared Gonzalez received more votes.[20] |
| | *Mitigation*: Avoid markets without ground truth sources; or include an additional option in the market for unverified. |
| Platform Coupling | *Example*: Hypothetically, traders who correctly predict USDC will completely de-peg on a platform that pays out in USDC will receive a payout but it will be worthless (*cf.* [19]). |
| | *Mitigation*: Avoid markets that are self-referential, including topics on the platform itself and its numeraire. |

## D    Market Topic

CePMs include the Iowa Electronic Markets [42], Kalshi [46], and PredictIt [68], as well as InTrade historically [43]. These systems exercise control over what topics may form a market and thus are *permissioned* with respect to market topics. They also operate under regulations that may restrict markets to certain topics or fully ban operations in regulated jurisdictions [24,54].

By contrast, DePMs like Augur [63,64], the original Gnosis [34], and PlotX [65] enable *permissionless* market creation by any user without centralized review. This removes the regulatory hook, enables niche topics that might not attract mainstream interest [83], and allows markets to be created without delay after real world events. However it can also lead to a greater incidence of malformed (or even malicious) market definitions, spam duplicates of existing markets, and unlawful topics, such as the 'assassination markets' which appeared on Augur in 2018 [24]. DePMs are generally web3 applications which means that a web-based user interface mediates transactions between the user and the underlying smart contracts. Market topic moderation could be implemented at the web3 layer (*e.g.,* Predictions.Global unlisted assignations markets from Augur's smart contracts [24]) but this does not prevent users from building an alternative UI or directly transacting with the smart contracts.

These systems are not all purely permissionless. A *hybrid model* puts some controls on topic creation without centralizing it fully [64]. For example, proposers may have to stake tokens to propose a market, and while the market is optimistically published, a review (either centralized or via an on-chain voting mechanism) could remove the market and/or slash the proposer.

If issues in a market's topic or definition are uncovered while the market is still active, DePMs like Polymarket allow 'additional context' notes to be added. However these clarifications could alter the market ex post and also disadvantage traders who do not see the note. The latter can be mitigated by advertising that a note will be published, always publishing at the same time (*e.g.,* 5pm ET), and clearing standing limit orders from an orderbook before posting [66].

---

[11]  Polymarket: 'Will Zelenskyy wear a suit before July?'
[12]  Google Docs: Did President Zelenskyy wear a suit before July 2025?.
[13]  Polymarket: 'TikTok banned in the US before May 2025?'
[14]  Polymarket: 'Will the missing submarine be found by June 23?'
[15]  Polymarket: 'Will Trump and Putin hug on Friday?'
[16]  Polymarket: 'Will Volodymyr Zelenskyy be the 2022 TIME Person of the Year?'
[17]  Polymarket: 'Astronomer Divorce Parlay'
[18]  Polymarket: 'Fordow nuclear facility destroyed before July?'
[19]  Polymarket: 'Was Barron involved in $DJT?'
[20]  Polymarket: 'Venezuela Presidential Election Winner'

---

**Insight 4.** Careful attention must be paid to both the general topic of the market and the 'fine-print' or exact predicate that decides the market. Table 3 provides several examples of pitfalls. Dealing with definitional pitfalls has been, to date, a trial and error process where market creators learn from past mistakes and ad hoc 'legalese' (e.g., a 'consensus of credible reporting' may be used to resolve markets) is copied from market to market [1].

---

**Research Gap 9.** Can market topics be written with machine-checkable predicate specifications (precedence rules, ranked sources, time semantics, and default outcomes), where model checking (*cf.* [18]) could eliminate ambiguities, corner cases, and loopholes? What would real world case studies of markets with additional context tell us?

---

## E   Scalar Markets

The third structure is a market where the outcome is a quantity of interest (*e.g.,* popular vote, temperature, price level, *etc.*) observed at a cutoff time with a strict lower bound and upper bound. Termed a *linear* or *scalar* market, there is only one share and its payout is what value the quantity takes on (typically normalized to the range $[0, 1]$ with rounding). As an example, in a market on Trump's popular vote, if the quantity is 49.8%, the share will pay \$0.498. Shares can also be sold in bundles with 'long' receiving \$0.498 and 'short' receiving (\$1-\$0.498).

Formally, if we let $X : \Omega \to \mathbb{R}$ be the observed quantity, and $[a, b]$ be an interval of values, then the linear outcome share $j_{\text{lin}}$ pays:

$$R(\omega)_{j_{\text{lin}}} = \begin{cases} 0, & X(\omega) \leq a, \\ \dfrac{X(\omega) - a}{b - a}, & a < X(\omega) < b, \\ 1, & X(\omega) \geq b. \end{cases} \tag{9}$$

While scalar markets are supported by DePMs like Augur [63,64] or those based on Gnosis' Conditional Tokens Framework (CTF) [22], including Polymarket [66] and Omen [25], they are not frequently used. For Polymarket, markets instead cheat, approximating a scalar market by splitting the quantity into 'buckets' and running a YNB market for each bucket. This avoids a less-vetted codebase within CTF, unifies the user interface across market types, and possibly avoids small edge cases over the exact resolution of the quantity (*e.g.,* off by 0.1 percentage disputes). However a problem with buckets is as follows: Alice estimates correctly that Trump will win the election with 49–51% of the popular vote. If there is a bucket for 45–49.9% and a bucket for 50–54.9%, Alice's forecast does not fit into a single bucket. Alice buys both buckets, knowing only one will win, diluting her expected return on capital. A second consequence of bucketization is volatile market jumps when the market consensus crosses from one expected bucket into a neighbouring bucket.[21]

---

[21] Polymarket: 'April 2025 Temperature Increase (ºC)'

## F   Matching

In the market initialization component of the modular workflow, a third approach, *matching*, was used by InTrade [43] and a variant by Fairlay [28], and is used today by Kalshi.

**Definition 6 (Matching).** *Fix a market $M = (\Omega, J, R)$ in numeraire $\mathcal{N}$. For each label $j \in J$, define its per-unit worst-case payoff*

$$c_j \ := \ \sup_{\omega \in \Omega} R(\omega)_j,$$

*and define the complementary label $\bar{j}$ with payoff*

$$R(\omega)_{\bar{j}} \ := \ c_j - R(\omega)_j.$$

*A* matching *mechanism accepts orders of the form $(j, q, p)$, meaning "trade $q \geq 0$ units of label $j$ at price $p$ (in $\mathcal{N}$) per unit," and executes a trade only when a buy order and a sell order coincide on $(j, q, p)$. Upon such a match, the mechanism: (i) transfers $qp$ units of $\mathcal{N}$ from the buyer and $q(c_j - p)$ units of $\mathcal{N}$ from the seller into escrow; (ii) mints $q$ units of label $j$ to the buyer and $q$ units of label $\bar{j}$ to the seller. At resolution $\omega \in \Omega$, the two positions pay $qR(\omega)_j$ and $qR(\omega)_{\bar{j}}$, which sum to $qc_j$, exactly covered by the escrow; hence the operator is riskless.*

Briefly, it mirrors a futures market, where Alice posts a desired short/long position at a chosen price on an orderbook with a margin account holding enough cash to cover her maximum loss if she obtains the position. If Bob is willing to take the other side, also with sufficient margin for his maximum loss, the operator matches them, creates two shares and gives them to Alice and Bob. Alice and Bob are not counterparties, both settle with the operator once the shares are created, however their coincidence of wants (COW) is necessary for the operator to create shares at no risk to itself.

---

**Insight 5.** A DePM operated through smart contracts should use automated bookmaking or splitting/merging. Matching effectively requires a central limit order book, which is too expensive to run on-chain at scale [60].

---

## G   Archiving

Publicly accessible DePM data provides society with a useful forecasting tool, and archival datasets enable calibration, insight into historical events, and replication of findings. On-chain records (state, logs, and calldata) inherit strong archival and verification properties so long as the chain persists. These records can be replayed and exposed via deterministic chain indexers (*e.g.,* The Graph, SubQuery) or managed subgraph hosting (*e.g.,* Goldsky). Human-readable materials can be stored in content-addressed, peer-to-peer systems (*e.g.,* IPFS) and mirrored to permanence layers with economic durability (*e.g.,* Arweave,

Filecoin), with their content identifiers anchored on-chain. Privately held operational data can be released as signed public snapshots or made queryable via open APIs.

Two kinds of artifacts matter most. First, the market semantics: the market topic, resolution rules, and any clarifications. Platforms such as Augur and Polymarket record stable on-chain identifiers (e.g., market/condition and token IDs) and keep the human-readable documents in content-addressed storage, with their content hashes/CIDs referenced on-chain. Second is the market data, including trading data (time, volume, price), outcome share supply and redemption totals, and timestamps for the status of the market (*e.g.,* opened, resolved, finalized). In practice, settlements and token movements are emitted on-chain, then replayed by deterministic chain indexers into queryable tables for research and UX. The same applies to the resolution process, its dispute trail and finalized outcome. If trading is off-chain (fully or partially), DePMs will need to expose application indexes/APIs for fast access and publish signed public snapshots for reproducibility. This missing data includes detailed trading, order-book depth, and liquidity metrics.

For example, Polymarket settles markets on the canonical ledger using the UMA Optimistic Oracle (the dispute game) and writes the final payout vector into the Gnosis Conditional Tokens Framework (CTF) (the settlement contract); outcome shares are ERC-1155 tokens (a multi-token standard), so transfers, mints, and redemptions are visible in logs. Trades are matched off-chain on a central limit order book (CLOB) but settle on-chain, while detailed order-book depth, quotes, and liquidity metrics are exposed via Polymarket's API (called Gamma). For reproducible research, the same on-chain events are also mirrored by deterministic chain indexers (subgraphs run by services such as Goldsky/The Graph), and API time series can be cross-checked against transaction hashes on the ledger.

---

**Research Gap 10.** A useful tool that does not exist yet could use on-chain data, API data, and external data (news, social media, *etc.*) to replay a past market, allowing researchers to step forward and backward at each timestamp. It was onerous for us to manually study how how markets incorporate news (real and fake) into prices in §7 without such a tool. It would also make it possible to backtest and train trading strategies using strictly point-in-time information, avoiding hindsight bias from revised data or retrospectively curated search results.

---