SoK: Market Microstructure for Decentralized Prediction Markets (DePMs)

Nahid Rahman[1], Joseph Al-Chami[2][0009−0001−8381−8080], and Jeremy Clark[1][0000−0002−3533−5965]

[1] Concordia University, Montreal, Canada
nahid.rahman@mail.concordia.ca
j.clark@concordia.ca
[2] Independent Researcher
alchamijoseph@gmail.com

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 include 35+ relevant proposals. Perhaps surprising, modern DePMs like Polymarket deviate materially from earlier designs like Truthcoin and Augur. We use our knowledge to present a modular workflow comprising seven stages: underlying infrastructure, market topic, share structure and pricing, 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 offer open problems for researchers interested in contributing to this ecosystem.

1 Introduction

In late 2024, the United States was in the midst of a presidential election when the decentralized prediction market, Polymarket, broke through mainstream news coverage. 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 effectively a betting market where odds are extrapolated from the prices of trades made in an open market (or somewhat open, as it was banned 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. 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-stated or under-stated, and withdrawing profits if the odds realign with their view.

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 set by many previous attempts (we list 30+ DePMs in Appendix A). DePMs were first given a few paragraphs in the Ethereum vision paper, 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 and an academic paper at WEIS (informally known as the 'Princeton DePM' because of author affiliation). Developed independently,[3] the two papers' designs are vastly different, representing two different goalposts for how a DePM might look.

Early systems, like Augur and Gnosis closely resembled Truthcoin, while modern systems like Polymarket either resemble the Princeton DePM or use new solutions that resemble a hybrid of the two designs. Consider some examples. (1) In Truthcoin, the market creator is active in setting initial prices (*i.e.,* odds) for each option and risks its own money until enough traders balance the book. In the Princeton system, the market creator is passive and only generates complete sets of outcome shares for every option. Polymarket uses the latter. (2) In Truthcoin, outcome shares are created with an early version of an automated market maker (tweaks to this design by Gnosis led to Uniswap years later). In the Princeton DePM, outcome shares are traded with an orderbook. In Polymarket, outcome shares can be traded with either an AMM or an orderbook. (3) In Truthcoin, the blockchain decides event outcomes (*e.g.,* who won the election) through a reputation-based on-chain vote with slashing. In the Princeton paper, they are resolved through trusted arbiters acting as oracles. The Ethereum whitepaper suggests both. In Polymarket, oracles decide outcomes but the specific oracle used, UMA, operates under the hood through on-chain voting with slashing when outcomes are disputed.

Noticing these points of differences inspired us to ask what are all the design decisions involved in creating a DePM? We break the design into a 'modular workflow' with seven stages: underlying infrastructure, market topic, share structure and pricing, trading, market resolution, settlement, and archiving. For each stage, we enumerate the possible designs and discuss competing trade-offs.

2 Preliminaries

2.1 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.[4]. We also searched news sources for opinions and

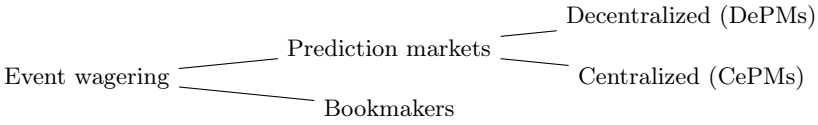
[3] The Princeton paper describes Truthcoin as being released while the paper was under review, and the Truthcoin FAQ mentions hearing about the Princeton paper but not having found the paper itself.

[4] `https://www.zotero.org/groups/5750510/2024_prediction_markets/library`

issues on leading decentralized prediction markets, such as polymarket. Finally, we informally monitored markets on popular markets but we did not conduct a systematic measurements as this paper is more concerned with the underlying mechanics than specific markets.

2.2 Taxonomy

Consider the following taxonomy of 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 bookmaker (or online 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.

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

2.3 Definitions

We define a market within a prediction-market system. In contrast to existing definitions, we abstract away details about how they are implemented. If the

definitions are not clear, we refer the reader to Appendix C where we describe a specific market offered by Polymarket and map each term in the following definitions to this real world example.

Definition 1 (Market). *A (single) market is a tuple $M = (E, \Omega, J, R)$, where E is a well-defined uncertain event, Ω is a nonempty outcome space for E, J is a finite index set of contract labels ("shares"), and $R = (R_j)_{j \in J}$ are nonnegative payoff functions with $R_j : \Omega \to \mathbb{R}_{\geq 0}$. When M resolves to $\omega_M \in \Omega$, one unit of share $j \in J$ pays $R_j(\omega_M)$ (in units of $\mathcal{N}$ defined below).*

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 $\mathsf{Res} = \{\mathrm{res}_M\}_{M \in \mathcal{M}}$ is a family of resolution registers such that, for each M with outcome space Ω_M, we have $\mathrm{res}_M \in \{\bot\} \cup \Omega_M$, res_M is initially $\bot$, and res_M transitions exactly once to some $\omega_M \in \Omega_M$.*

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

System axioms. For every market $M = (E, \Omega, J, R) \in \mathcal{M}$ operating in system $\mathcal{S} = (\mathcal{M}, \mathcal{N}, \mathsf{Res})$:

1. **Issuance.** The system may increase the outstanding supply of any label $j \in J$ by any $q \geq 0$ subject to policy (unspecified here). Let $S_j(M) \geq 0$ denote the total outstanding supply of label j in M.
2. **Transfer.** Holdings of each label $j \in J$ are transferable between accounts; transfers conserve per–label totals $S_j(M)$.
3. **Burn/Cancel.** The system may decrease $S_j(M)$ via explicit burn/cancel operations according to policy (optionally allowed pre–resolution).
4. **Resolution.** The resolution register satisfies $\mathrm{res}_M \in \{\bot\} \cup \Omega$, is initially $\bot$, and transitions exactly once[5] to a realized outcome $\omega_M \in \Omega$.
5. **Settlement.** Once $\mathrm{res}_M = \omega_M \in \Omega$, any holder of q units of label $j \in J$ may redeem for $q \cdot R_j(\omega_M)$ units of the numeraire $\mathcal{N}$; redeemed units are removed from supply (burned).
6. **Conservation of liability.** Let $S_j^{\mathrm{pre}}(M)$ be the outstanding supply of label j immediately before settlement. The total settlement liability is

$$\mathsf{Liability}(M) \;=\; \sum_{j \in J} S_j^{\mathrm{pre}}(M)\, R_j(\omega_M) \;\in\; \mathbb{R}_{\geq 0},$$

which equals the aggregate numeraire paid out if all outstanding units are redeemed.

[5] Real world DePMs like Polymarket might resolve a market, receive a dispute of over the outcome, and resolve it differently after a process (see Section 3.5). In the definition, resolution refers to the final outcome only. An outcome is final when shares can be redeemed for payouts.

Table 1. 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	Partially redacted leaked email from an HBO executive implies Len Sassaman.	Immaterial	Fake
06 Oct	A long-dormant X account belonging to someone who had corrosponded with Sassaman on Twitter posted a new message stating they were interviewed for the documentary.	Immaterial	Fake
07 Oct	Widow of Sassaman states she was not interviewed.	Moderate	Truthful
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, also featured heavily in the trailer	Material	Wrong but factual basis
07 Oct	End credits of documentary leaked 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
08 Oct	Peter Todd confirms being confronted for documentary but unsure if he will be named.	Material	Truthful
08 Oct	Scene with Todd leaked but inconclusive if it is film's thesis.	Material	Truthful
08 Oct	Commenter on Polymarket claims to screen test and names Nick Szabo.	Immaterial	Fake
08 Oct	Fortune publishes movie review disclosing Todd is named	Very Significant	Truthful
08 Oct	Documentary airs and names Todd	Very Significant	Conclusive

7. **No pre–resolution obligation.** While $\mathrm{res}_M = \perp$, the system owes no cash payoff on holdings of (M, j) beyond recording balances and permitting issuance/transfer/burn per policy.

2.4 An Example of a Market

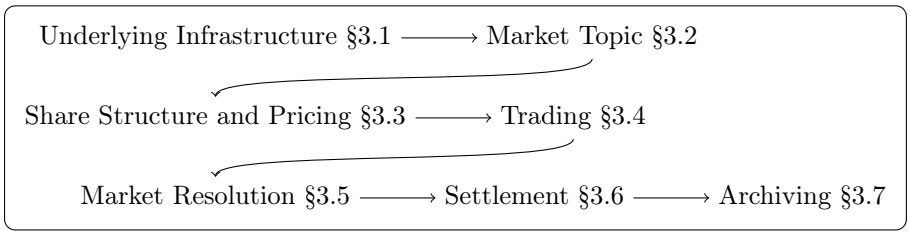
Before diving deep on the mechanics of decentralized prediction markets, we illustrate how markets work and provide value with a lighthearted example. On 3 Oct 2024, a trailer was released with press coverage of a new HBO documentary on Bitcoin to air about a week later on 8 Oct 2024. In an interview, 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.' The

next day, Polymarket setup a market for speculating on who the documentary would name, providing 15 names plus an 'other/multiple' option. 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. 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 1. Further details are provided in Appendix B.

Also of interest is how the prediction market did not seem to extract insider information which is in violation of what the theory would predict. The director did state he did not participate in the market and advised his team working on the film not to either. Friction for novice users is also perhaps high—web3 apps have a learning curve and if insiders were based in the US, access would require circumvention of Polymarket's geofencing. Perhaps these reasons kept insiders out of the market.

3 Modular Workflow



We now turn to the design landscape of DePMs and step through our modular workflow, summarized above. Some design decisions will be common issues for both centralized and decentralized prediction markets. We include these anyways for completeness. However we put the emphasis on discussing design decisions that are pertinent to the decentralization and permissionlessness of prediction markets.

3.1 Underlying Infrastructure

In theory, a decentralized and permissionless system might run on a system other than a blockchain, but blockchain technology underlays all known DePMs. Selecting a blockchain constitutes the initial design decision within our modular workflow. In selecting a blockchain, a set of desirable features include expressive

smart contracts, low transactions fees, fast finality, guaranteed inclusion, and censorship resistance. The earliest research was in agreement that Bitcoin Script was not powerful enough to operate a DePM, and a separate chain (perhaps integrated with Bitcoin as a sidechain) would be required. Later Ethereum was deployed, providing general smart contracts, and most DePM activity moved to it. Much later, high fees on Ethereum caused the diversification of the VM-based blockchain space into numerous competing chains and layer 2 (L2) scalability solutions. As of today, the most active DePMs run on chains built to execute smart contracts (*e.g.,* EVM or WASM). Most no longer run on Ethereum but on either an Ethereum competitor (*e.g.,* Polygon or Solana) or an Ethereum L2 (*e.g.,* Arbitrum or Optimism).

Generally, there are no strong qualitative differences between the named blockchain options—it is a choice driven by fees, user base, and supporting infrastructure. In all cases, the logic of the prediction market operations is placed in smart contracts and the blockchain executes the contracts. A materially different approach is to put the prediction market logic into the blockchain rules themselves, either with a purpose-built blockchain or with a customized layer (called an L3) that uses custom rules but settles on a standard L1 or L2.

3.2 Market Topic

CePMs include the Iowa Electronic Markets, Kalshi, and PredictIt, as well as InTrade historically. 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 [2].

By contrast, DePMs like Augur, Gnosis, and PlotX enable *permissionless* market creation by any user without centralized review. This removes the regulatory hook, enables niche topics that might not attract mainstream interest, 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, and unlawful topics, such as the 'assassination markets' which appeared on Augur in 2018. 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) but this does not prevent users from building an alternative UI or directly transacting with the smart contracts. While DePMs have the option to operate permissionlessly, they may also choose to permission market creation while leaving other aspects permissionless. At the time of writing, Polymarket is considered a DePM and while market topics can be suggested by users, final approval is made by a Market Integrity Committee [3].

A *hybrid model* puts some controls on topic creation without centralizing it fully. For example, proposers may have to stake tokens to propose a market, and while the market is optimistically published, a review (either centralized or

Table 2. Some pitfalls that illustrate the difficulty in properly defining a prediction market topic. [Topic] is an issue with the topic itself and [Def'n] with the way the predicate is defined.

Pitfall	**Description**
Borderline Categories [Def'n]	*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;[6] media equivocated on describing it as a suit.[7]
	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.[8])
Precedence Gaps [Def'n]	*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 [1]. 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.[9]
	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 [Def'n]	*Example*: A market concerning a divorce presumes the couple are married (as opposed to common law) which was unknown.[10]
	Mitigation: Parse the predicate for any presumptive statements and remove/address them.
No Ground Truth [Topic]	*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.[11] A market on whether Baron Trump was 'involved' in the $DJT memecoin lacked an authoritative source.[12] 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.[13]
	Mitigation: Avoid markets without ground truth sources; or include an additional option in the market for unverified.
Platform Coupling [Topic]	*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.* [1]).
	Mitigation: Avoid markets that are self-referential, including topics on the platform itself and its numinaire.

via an on-chain voting mechanism) could remove the market and/or slash the proposer.

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 2 provides several examples of pitfalls. A pitfall in the predicate means the market topic is acceptable but there is an issue with its exact specification (*e.g.,* a market about wearing a suit needs to define a suit). A pitfall in the topic means the topic itself is problematic, even if it is worded impeccably (*e.g.,* a Polymarket market about whether Polymarket will shut down is problematic because winners will not be paid if it does). The first pitfall, borderline categories, is very prominent with many other disputes, including whether enforcement against TikTok in the US constitutes a ban,[14] or if finding debris from the Titan submersible constitutes it being found.[15]

These issues are not limited to DePMs and apply to event wagering in general, however some issues are more pronounced in DePMs. If market creation is permissionless, market creators may be amateurs and error-prone; may draft adversarial markets to trick traders; or duplicate existing markets, thinning out liquidity. CePMs have the latitude to organize, pause, or revise markets or ban users. DePMs may give themselves this latitude at the risk of appearing less permissionless. Further it seems inevitable that some markets will fall into a pitfall and DePMs have to carefully consider how dispute resolution will work while also appealing to blockchain enthusiasts.

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. Future research could develop machine-checkable predicate specifications (precedence rules, ranked sources, time semantics, and default outcomes) and verify they are well-defined with model checking.

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.

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

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). Consider a market with three possible outcomes: $\Omega = \{\mathsf{A}, \mathsf{B}, \mathsf{C}\}$.

The first structure we term *winner-take-all (WTA)* and is prominent on Iowa Electronic Markets and supported by Augur and Gnosis. A WTA market issues a outcome share for each outcome $J = \{j_\mathsf{A}, j_\mathsf{B}, j_\mathsf{C}\}$. If the outcome is B, the share j_B pays \$1 (or one unit of numeraire $\mathcal{N}$) and the other shares pay \$0. For any $k \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}\}$,

$$R_{j_\mathsf{k}}(\omega) = \begin{cases} 1, & \text{if } \omega = \mathsf{k}, \\ 0, & \text{otherwise.} \end{cases}$$

For a WTA market to be well-functioning, conditions must hold on outcome shares. (i) They should be *mutually exclusive* so no more than one share wins: $R_{j_\mathsf{k}}(\omega) R_{j_\ell}(\omega) = 0 \quad \forall \omega \in \Omega, \forall \mathsf{k} \neq \ell$; and (ii) they should be *complete* so at least one share wins: $\sum_{\mathsf{k} \in \Omega} R_{j_\mathsf{k}}(\omega) = 1 \quad \forall \omega \in \Omega$. If they are not mutually exclusive, the operator could be undercollateralized for making all payments. 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 the next section on trading.

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. 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.

The second structure we term a *yes-no bundle (YNB)*. YNB markets were prominent on InTrade and are currently prominent on Polymarket. A YNB market issues two outcome shares for each outcome, a 'yes' and a 'no:' $J = \{j_{\mathsf{A_Y}}, j_{\mathsf{A_N}}, j_{\mathsf{B_Y}}, j_{\mathsf{B_N}}, j_{\mathsf{C_Y}}, j_{\mathsf{C_N}}\}$. For any $k \in \{\mathsf{A}, \mathsf{B}, \mathsf{C}\}$,

$$R_{j_{\mathsf{k_Y}}}(\omega) = \begin{cases} 1, & \text{if } \omega = \mathsf{k}, \\ 0, & \text{otherwise.} \end{cases} \qquad R_{j_{\mathsf{k_N}}}(\omega) = \begin{cases} 1, & \text{if } \omega \neq \mathsf{k}, \\ 0, & \text{otherwise.} \end{cases}$$

Each outcome-specific pair $\{j_{\mathsf{k}_\mathsf{Y}}, j_{\mathsf{k}_\mathsf{N}}\}$ constitutes a two-outcome WTA market (k vs. not-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).[16] Multiple words can resolve to yes (not exclusive) and it is possible he says none of the listed words (not complete). If a YNB market is established and being actively traded, because it is not complete, new outcomes can be added fairly to the market mid-flight.

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 variant as *YNB negative risk (YNB-NR)*, a term introduced by Polymarket. 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 are the same as a WTA share and sum to \$1, while the No shares will sum to $|\Omega| - 1$. The Satoshi/HBO YNB market from Section 2.4 was made exclusive and complete across bundles by including a bundle for the outcome: 'other/multiple.'

Further, in a YNB market, 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):

$$j_{\mathsf{k}_\mathsf{N}} \equiv \sum_{\ell \in \Omega \setminus \{\mathsf{k}\}} j_{\ell_\mathsf{Y}} \quad \text{for any } \mathsf{k} \in \Omega.$$

And multiple No outcome shares can be converted into Yes shares plus cash:

$$\sum_{\ell \in \Omega \setminus \{\mathsf{k}\}} j_{\ell_\mathsf{N}} \equiv j_{\mathsf{k}_\mathsf{Y}} + \$1 \cdot (|\Omega| - 2)$$

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. Termed a *linear* or *scalar* market, there is only one share and its payout is what value the quantity takes on (perhaps 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).

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

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_{lin} pays:

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

While linear markets are supported by DePMs like Augur, Gnosis, and Omen, they are not frequently used. Even though Polymarket uses the Gnosis Conditional Tokens Framework (CTF) which supports linear markets, it instead approximates one by splitting the quantity into 'buckets' and running a YNB market for each bucket. This allows greater code-reuse 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. Generally, an unfortunate cutpoint between boundaries can dilute expected return on capital (as investors buy more than one bucket) and can lead to volatile market jumps when the market forecast switches between buckets.[17]

3.4 Trading

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-1155. By contrast, CePM outcome shares are held in-house by the operator. Withdrawing outcome shares allows traders to exchange tokens outside of the platform and to compose with third party DeFi services (*e.g.,* on-chain trading, lending, leverage, *etc.*). From a software development perspective, it also means that DePMs can be built with external libraries or using outside infrastructure. 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?

The first trade. Probably the greatest evolution in DePMs, from Truthcoin through Augur and Gnosis 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 and was first suggested for DePMs by Truthcoin, which heavily influenced Augur and Gnosis. 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. If Alice is the first trader, she can immediately trade

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

with the operator. The operator is autonomous and sets buy/sell prices algorithmically, originally using Hanson's logarithmic market scoring rule (LMSR). The key point is that the operator is Alice's counterparty; if Alice wins, the operator loses, and vice-versa. The pros are instant liquidity for the first trader and the cons are risk of losing money and the burden of needing to set initial odds (getting them wrong increases the chances it loses). Acute readers might wonder if this is the same as an automated market maker (*e.g.,* Uniswap) discussed below. 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.

The second approach, *splitting*, is used by IEM and was first suggested for DePMs by the Princeton DePM. Augur switched to this approach, Gnosis implemented it in CTF, and Polymarket uses it. 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. Splitting allows any trader to purchase a complete portfolio of shares for \$1 (and generally *merging* is also permitted 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, and the operator is always fully solvent, 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_{kY} and one j_{kN} for the chosen k. Hence, within any bundle $\mathrm{totSupply}(j_{\mathsf{kY}}) = \mathrm{totSupply}(j_{\mathsf{kN}})$. Across outcomes, however, supplies are uncoupled—the total minted for the A bundle need not match that for B or C.

The third approach, *matching*, was used by InTrade and a variant by Fairlay. 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. The pros/cons mirror those of splitting but matching is operationally more complex: the operator needs to run an orderbook and is involved in the trading process.

Trading in established markets. Once outcome shares are in wide 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 bookmarking for prediction markets. They first developed alternatives to the LMSR rule, including the constant product rule. Initially, it was proposed that a trader holding two kinds of tokens could set up an automated market maker using this, or other, rules. This is precisely what the prediction market operator does in automated bookmaking. 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.

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. Adapting AMMs to these constraints is an interesting open problem. Paradigm's pm-AMM tapers liquidity as a scheduled expiry approaches, which helps for events with a known horizon; but many markets jump or resolve unexpectedly, so pre-expiry shocks can still hurt liquidity providers.

When trading on-chain, miners and other users can front-run transactions, an area of study called maximum extracted value (MEV). Although the term MEV did not exist at the time, the Princeton DePM describes the MEV problem extensively and proposes a mitigation now called a frequent batch auction (FBA) (again, the term FBA was not popularized until later) to be conducted at the blockchain-level (adaptable to a layer 3 chain). On-chain FBAs have been studied and while linear time operations in the size of the orderbook are still infeasible for Ethereum or even layer 2 roll-ups, succinct proofs that auctions were closed correctly could be used.

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 presidency) and measures roughly \$40M USD of realized arbitrage profits over the measurement period.

3.5 Market Resolution

It is possible that a market topic can be determined on-chain (*e.g.,* total value locked in a DeFi service) in which case resolution is simple, however typically, prediction market outcomes concern facts that are off-chain. In these cases, resolution is the process of finalizing an off-chain outcome in an on-chain market. The predominate approaches are the following: 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 (while the first two could be considered oracle-less). A DePM may use a hybrid approach. For example, an arbiter might optimistically resolve a market outcome while also allowing disputes. 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.

Oracle-less approaches are largely academic. A *self-settling market* assumes *splitting* and *merging* (see §3.4) of shares and 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 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).

The *designated arbiter* space is evolving, with platforms exploring a shift from centralized human arbiters to AI councils. Kalshi exemplifies centralized resolution: staff settle markets per published rules/sources; as a CFTC-regulated DCM and for platform credibility, team is incentivized to resolve accurately.[1], [2] Chaos Labs' Edge Proofs is a concrete AI-arbiter design where a decentralized network of agents from multiple models gather evidence from predeclared sources and finalize only on a consensus threshold. [3] [4] Because AI is probabilistic and blockchains are deterministic, no-consensus loops can arise; timebox decisions and fall back (relax threshold, resolve Unknown, or escalate, e.g., to UMA). AI oracles also inherit adversarial ML risks [5] such as RAG poisoning [6] Blockchain has seen analogous integrity failures with mutable off-chain references (e.g., Marlinspike's "poop-emoji" NFT [7]). Early empirical results are mixed but promising: a Chainlink study of 1,660 Polymarket questions reports 89.3% accuracy (sports 99.7%, politics 84.3%) with temporal-reasoning challenges.[8]

Reporter networks deliver fast, parameterizable, and auditable resolution for markets tied to structured external data (prices, scores). An aggregation contract (e.g., a Chainlink feed) acts as the definitive on-chain authority. Multiple independent reporters submit signed observations off-chain; an off-chain consensus protocol (OCR) coalesces these into a single report whose value is typically the median (or a mean with outlier filtering) and whose metadata (round ID, timestamp) and quorum signatures are verified on-chain. Updates are emitted when deviation or heartbeat thresholds are met, giving explicit control over latency/recency and bounding staleness under network stress. Median aggregation is resilient to a minority of faulty or adversarial reporters (Byzantine tolerance),

while source and operator diversity mitigate data-correlation risk; compressing n submissions into one update reduces gas and surface area. The result is a deterministic, publicly auditable outcome primitive: DePM contracts read the aggregator at resolution time and settle without discretionary intervention.

Thales and its Overtime on-chain sportsbook instantiate this model end-to-end: market predicates reference Chainlink sports feeds for scores and final results, odds can be parameterized from on-chain feeds, and expiry reads the aggregator's answer to resolve. Augur Turbo similarly relies on reporter-network feeds for schedules, scores and stats, so sports markets settle immediately upon event close. Entropyfi resolves scalar price rounds by sampling Chainlink aggregator contracts at round start/end and uses on-chain automation (Keepers) to trigger settlement, coupling reporter-network data with deterministic payout logic.

In *crowdsource voting* systems, the most common approach is to use staked tokens to determine voting weights. Final authority rests with an on-chain arbitrator whose outcome is chosen by stake-weighted voting; the system finalizes to the majority of stake, which does not guarantee resolution to the real outcome. There are two designs: (i) Schelling/always-vote (e.g., Augur/REP), where token holders stake and vote on every market and repeated disputes can escalate to a fork lasting up to 60 days, effectively pausing other non-finalized markets while REP holders migrate to a "true" universe [1] making this approach slow and operationally heavy, and (ii) optimistic, dispute-driven, where anyone proposes an answer with a bond, the market resolves if unchallenged during liveness, and only disputed cases go to a vote. UMA is the canonical version (on Polymarket: 2-hour challenge window, $750 bond, and a DVM commit–reveal vote if challenged). This optimistic pattern is faster and more cost-effective. [2], [3] A closely related optimistic stack is Reality.eth + Kleros, where disputed questions go to a randomly drawn, staked juror court that uses commit–reveal; jurors in the majority are rewarded while those in the minority are penalized. [4]

Token-voted dispute resolution decentralizes market resolution but inherits governance voting's flaws and adds carrot/stick incentives that reward the eventual majority while penalizing minorities and non-participants. In practice, stake can centralize, enabling whale capture: a coordinated or whale-tilted majority can settle a market incorrectly with no penalty to itself, only the minority is slashed mirroring patterns seen in governance (e.g., Uniswap, where 11 wallets can determine a majority; a16z's influence on a proposal) [5], [6].

A similar concentration risk surfaced on Polymarket/UMA during a governance attack [7].

For UMA specifically, the top five wallets control 45.6% of votes and the top 13 exceed 65%, enough to meet the passing threshold [8] These payoff asymmetries induce "beauty-contest" behavior: because minorities are slashed and majorities paid, rational voters may try to forecast the majority rather than report private information, permitting majority-wrong outcomes when expectations align or large holders coordinate. Finally, bribery and vote-buying (the p+ϵ attack) can flip results whenever an attacker's external payoff from a wrong resolution exceeds the system's economic security [9] Beyond capture and bribery,

token voting can impose real costs when platform policy diverges from oracle outcomes. In June 2024, UMA voters resolved "No" on a high-profile Polymarket market, while Polymarket publicly deemed the opposite "conclusive" and refunded users, an unusual split that highlights governance/interpretation friction between platform administrators and token-vote results [10] As a possible mitigation, platforms like Polymarket that rely on UMA's token-vote oracle could, in theory, replace it with a native dispute token, leveraging their scale to increase economic security and align incentives for truthful voting and platform integrity by directing a share of platform revenues to voters. Kleros addresses several of these challenges by using commit–reveal to prevent mid-round copycatting, an appeal ladder that roughly doubles the jury (+1) and increases fees at each step to make capture and bribery costlier, and topical subcourts so disputes are heard by more knowledgeable jurors.

3.6 Settlement

The slogan 'sweat the game, not the payout' 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.[18] 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 Axioms in Section 2.3).

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. Augur, CTF, and Omen implement such a *pull* mechanism. 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), 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.

3.7 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

[18] 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.

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.

4 Discussion and Research Agenda

Composability. Perhaps the biggest evolution in DePM design is modularity. Early DePMs were monolithic, single-vendor codebases. Modern DePMs are built from existing infrastructure, which glues together nicely because of standardized interfaces. For example, Polymarket's core DePM code is Gnosis' conditional token framework. 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-20 and ERC-1155 tokens. Market outcome disputes are escalated to UMA's DVM oracle. Polymarket also uses third party services for bridging assets, embedded wallets (based on email verification), and EIP-3009 gasless withdrawals. Beyond

Table 3. DePM Design Decisions Across the Modular Workflow.

Platform	Infrastucture (§?.?)	Topic	Share Structure	Initial Issuance	Numeraire	Trading	Resolution	Settle	Archive	Implementation
Augur (v1)	ETH L1	○	WTA	Split	ETH	O-OB	REP	PL	L	P + S
Princeton PM (design)	ETH L1	○	WTA	Split	—	O-OB	C	PL	L	P
Augur (v2)	ETH L1	○	WTA	Split	DAI	X	REP	PL	L	P + S
Gnosis / Omen	ETH L1/L2	◐	CTF	Split + CF: FPMM	DAI, xDAI	A	R/K	RP	L	P + S
Polymarket	Polygon (L2)	● (+ Pilot)	YNB	Split	USDC	X + A	UMA	PL + XG	L	P + S
Hivemind (Truthcoin)	BTC-side	○	Comb.	CF: LSMR	—	A	VTC	PL	S	P
PlotX (v2)	Polygon (L2)	○	B/S	CF: CFMM	USDC	A	Ext.O	PL	P	S
CePM: Kalshi	CEX Deri	● (Rulebook)	Binary	Admin	USD	C	C	PS	C	S
CePM: PredictIt	CEX Retail	● (Operator)	Binary	Admin	USD	C	C	PS	C	S

Legend:
Infrastructure: L1 = Ethereum L1; L2 = optimistic/zk-rollup or sidechain (Polygon); Side = dedicated sidechain; CEX = centralized infra.; Deri = Derivatives
Topic: ○= Permissionless; ◐= Supports permissionless framework; ●= Permissioned.
Share: WTA = Winner-Take-All; CTF = Conditional Tokens; YNB = Yes/No Bundle; Comb. = Combinatorial; B/S = Binary/Scalar.
Initial Issuance: Split = complete-set minting; CF = Cost Function; LSMR = Logarithmic Market Scoring Rule ; FPMM = fixed-product MM; CF: CFMM = constant-function MM; Admin = centralized.
Trading: A = AMM; O-OB = on-chain order book; X = off-chain order book; C = centralized.
Resolution: REP = Augur REP; UMA = UMA optimistic; R/K = Realitio→Kleros; VTC = VoteCoins; Ext.O = external oracle; C = centralized.
Settlement: PL = pull; RP = redeemPositions; PL+XG = pull + gasless; PS = push.
Archive: L = On-chain Logs + IPFS; S = Sidechain; P = On-chain + Proprietary; C = Off-chain.
Implementation: P = Paper; S = System; P+S = Both.

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.

Regulation. The legal and regulatory concerns of CePMs and, to a lesser extent, DePMs are well-covered in the literature. Jurisdictions like the United States tightly control prediction markets. Where do the regulatory concerns show up in our taxonomy? The two paramount issues are: who is operating the market and what is being bet on. A fully autonomous DePM would sidestep enforcement actions and this is, for some, the motivation for a DePM. For a CePM or DePM operated by a registered business, regulations will mostly address consumer protection and money laundering. Market topics will dictate who regulates it (*e.g.,* if limited to sports, it could be regulated at the state level, but expanded to general topics, it would be regulated by the CFTC). Beyond this, the market

microstructure of a prediction market is relevant only to the extent it impacts the integrity of the market.

Research Agenda. The history of DePM shows a convergence toward trading outcome shares, creating by splitting, on CLOBs and AMMs. While many aspects of prediction markets have been studied formally, comparing different market microstructures has not received adequate research; and optimizing AMMs for DePMs is still at the beginning stages. Less convergence exists on how to decide market outcomes, a uniquely DePM problem (since a CePM can arbitrate its own markets). Another way to look for research problems is to pinpoint where faulty behaviour is still occurring: for Polymarket, the biggest sources are poorly defined market topics and the vulnerability of market resolution to manipulation (both discussed extensively already). Analysis of new approaches (formal verification for topics? AI as oracles?) would be welcome research. A lesser known issue is archiving DePM data and tools that could fully 'replay' a market at each timestep could be useful for understanding how markets process news (real and fake) and incorporate knowledge into prices. Finally, the degree to which DePMs can be pushed further toward permissionlessness in all aspects is still largely open, particularly around setting topics for markets.

5 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.

Acknowledgements. We thank the reviewers who helped to improve our paper. J. Clark acknowledges support for this research project from (i) the National Sciences and Engineering Research Council (NSERC), Raymond Chabot Grant Thornton, and Catallaxy Industrial Research Chair in Blockchain Technologies, (ii) the AMF (Autorité des Marchés Financiers), and (iii) NSERC through a Discovery Grant.

References

1. Clark, J., Bonneau, J., Felten, E.W., Kroll, J.A., Miller, A., Narayanan, A.: On decentralizing prediction markets and order books. In: Workshop on the Economics of Information Security, State College, Pennsylvania. vol. 188 (2014)
2. 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)

3. 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)

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.
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. Pivoted to developing underlying infrastructure for DePMs, including the widely used Conditional Tokens Framework (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

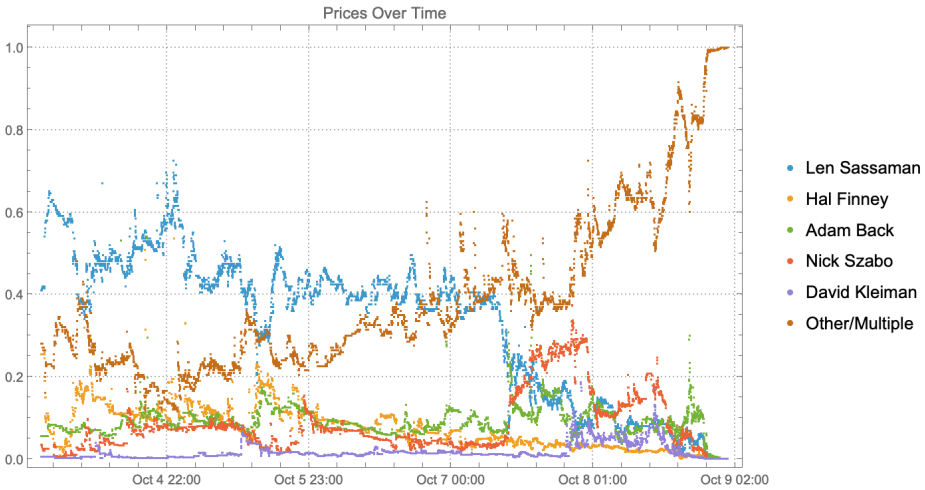


Fig. 1. The price movements for 6 leading candidates in the Polymarket market for who would be named as Satoshi Nakamoto in the HBO documentary 'Money Electric' which aired the evening of October 8.

C Example instantiation of definition

In section 2.4, we discussed an example market concerning who the HBO documentary 'Money Electric' would name as Satoshi Nakamoto. In this section, we will see how this fits the definitions of a market, prediction market system, and the Arrow–Debreau special case. As discussed in Section 3.3, Polymarket employs a market mechanism we call a yes/no bundle (YNB), as opposed to winner-take-all (WTA). YNB requires an extra step in the definitions so we will do a first pass with a simplified WTA submarket, and then add the full YNB market.

C.1 Pass 1: Single WTA Market

Consider a simplified market that questions whether one specific candidate, *e.g.,* Hal Finney, is named as Satoshi: yes or no. If through unforeseen circumstances, who the documentary names is not verifiable by the air date, the market resolves to no.

Recall Definition 1 of a market:

Definition 3 (Market). *A (single) market is a tuple $M = (E, \Omega, J, R)$, where E is a well-defined uncertain event, Ω is a nonempty outcome space for E, J is a finite index set of contract labels ("shares"), and $R = (R_j)_{j \in J}$ are nonnegative payoff functions with $R_j : \Omega \to \mathbb{R}_{\geq 0}$. We assume $|J| \geq |\Omega|$ and we require* outcome distinguishability *on Ω:*

$$\forall\, \omega \neq \omega' \in \Omega \;\; \exists\, j \in J : \;\; R_j(\omega) \neq R_j(\omega').$$

When M resolves to $\omega_M \in \Omega$, one unit of share $j \in J$ pays $R_j(\omega_M)$ (in units of $\mathcal{N}$ defined below).

Event E is whether or not Hal Finney is named as Satoshi in the documentary.

Ω is the set of resolution outcomes the market recognizes for E—the labels the system can publish at settlement. For this Hal-only binary market the outcome space is $\Omega = \{\mathsf{True}, \mathsf{False}\}$. Here True means the documentary (per the market's stated criteria) identifies Hal Finney as Satoshi; False aggregates all other possibilities (Hal not named, someone else named, no one named, the film does not air, or the identification is not verifiable by the resolution deadline).

We require that Ω contain no redundant labels. A label is redundant if it does not change at least one contract's payoff: $\omega \sim \omega' \iff \forall j \in J,\; R_j(\omega) = R_j(\omega')$. For example, "Hal is named and it is raining" and "Hal is named and it is not raining" are distinct real-world states, but they cannot both appear in Ω since they both map to True. The restriction can be written as:

$$\forall\, \omega \neq \omega' \in \Omega \;\; \exists\, j \in J : \;\; R_j(\omega) \neq R_j(\omega').$$

In a prediction market, there are a set of shares. If we label them and add them all to an index set, that set is J. For this example, $J = \{\mathsf{YES}, \mathsf{NO}\}$: Hal

Finney is named (yes) and else (no). This is a normal case where each share in J corresponds to an outcome in Ω but it is possible that the number of shares could exceed the number of outcomes.[19]

J is the index set of contract labels—the names of the tradeable shares. In this binary market we take $J = \{\mathsf{YES}, \mathsf{NO}\}$.

The labels get their meaning from the component payoff functions $R_j : \Omega \to \mathbb{R}_{\geq 0}$. In this example, a payoff of 1 is given for shares that correctly predict the outcome and 0 otherwise. This means $R_{\mathsf{YES}}(\mathsf{True}) = 1$, $R_{\mathsf{YES}}(\mathsf{False}) = 0$, $R_{\mathsf{NO}}(\mathsf{True}) = 0$, $R_{\mathsf{NO}}(\mathsf{False}) = 1$.

Recall Definition 1 of a prediction–market system $\mathcal{S} = (\mathcal{M}, \mathcal{N}, \mathsf{Res})$: $\mathcal{M}$ is the (countable) catalog of markets; $\mathcal{N}$ is the numeraire (unit of account used to price and settle claims); and $\mathsf{Res} = \{\mathrm{res}_M\}_{M \in \mathcal{M}}$ assigns to each market M a resolution register that is initially $\perp$ and flips exactly once to some $\omega_M \in \Omega_M$. When $\mathrm{res}_M \neq \perp$, we set $\omega_M := \mathrm{res}_M$ and each unit of label $j \in J$ settles for $R_j(\omega_M)$ units of $\mathcal{N}$.

The market tuple $M = (E, \Omega, J, R)$ specifies *what* to pay *given* an outcome (via R). The register res_M is the system's single source of truth for *which* outcome actually occurred: before resolution $\mathrm{res}_M = \perp$ (no settlement), after resolution $\mathrm{res}_M = \omega_M \in \Omega_M$ (settlement applies).

Polymarket instantiates $\mathcal{S}$ with $\mathcal{M}$ equal to its live and historical markets, $\mathcal{N}$ the USD–denominated stablecoin USDC, and Res implemented by its on–chain resolution process (e.g., UMA's optimistic oracle) that writes a single outcome to each res_M.

For the Hal–only binary market, the system maintains a resolution register $\mathrm{res}_{M_{\mathrm{Hal}}} \in \{\perp\} \cup \Omega$ with $\Omega = \{\mathsf{True}, \mathsf{False}\}$ (i.e., "yes/no" to the proposition). The register is initially $\perp$ and, after the platform's resolution process completes, the oracle writes a single value $\omega_{M_{\mathrm{Hal}}} \in \Omega$ to the register.

Set $\omega_{M_{\mathrm{Hal}}} = \mathsf{True}$ iff the documentary (per stated criteria) identifies *Hal Finney* as Satoshi; otherwise set $\omega_{M_{\mathrm{Hal}}} = \mathsf{False}$.

Shares are fully collateralized to \$1 in the numeraire $\mathcal{N}$ (USDC): a unit of YES pays 1 USDC at True and 0 USDC at False; a unit of NO pays 1 USDC at False and 0 USDC at True. Formally,

$$R_{\mathsf{YES}}(\mathsf{True}) = 1, \quad R_{\mathsf{YES}}(\mathsf{False}) = 0, \qquad R_{\mathsf{NO}}(\mathsf{True}) = 0, \quad R_{\mathsf{NO}}(\mathsf{False}) = 1.$$

In the aired documentary, *Peter Todd* was named; therefore

$$\mathrm{res}_{M_{\mathrm{Hal}}} = \omega_{M_{\mathrm{Hal}}} = \mathsf{False},$$

and each unit settles as

$$\mathsf{YES} \;\to\; 0 \text{ USDC}, \qquad \mathsf{NO} \;\to\; 1 \text{ USDC}.$$

[19] For example, consider a market of where Newcastle United (NUFC) finishes in the 2024-35 English Premier League season. Since there are 20 teams, the outcome has 20 possible labels: positions 1 to 20. Shares could exist for each of the 20 positions. But the outcome could also settle shares for whether NUFC finishes in the top 5 (which is relevant to champions league admittance), or shares on finishing in the bottom 3 (which is relevant to relegation).

This market is a winner–take–all (Arrow–Debreu) special case: there is a bijection $\iota : J \to \Omega$ and payoffs $R_j(\omega) = \mathbf{1}\{\omega = \iota(j)\}$. Hence, for each $\omega \in \Omega$, exactly one label pays 1 and all others pay 0. In the prediction–market system, the resolution register $\mathrm{res}_M \in \{\perp\} \cup \Omega$ is initially $\perp$ and flips exactly once to $\omega_M \in \Omega$; one unit of label $j \in J$ then settles for $R_j(\omega_M)$ units of the numeraire $\mathcal{N}$.

C.2 Pass 2: YNB Market

Families. Given an index set C, a *family of markets* indexed by C is a map $c \mapsto M_c$; we write $\{M_c\}_{c \in C}$. Each $c \in C$ names one market in the family.

Instantiation for the HBO event. Let C be the set of candidates (e.g., $\{\mathsf{Szabo}, \mathsf{Sassaman}, \mathsf{Back}, \ldots, \mathsf{Other/Multipl}$ Polymarket lists a family $\{M_c\}_{c \in C}$, one binary market per candidate:

$$M_c = (E_c, \Omega_c, J_c, R^{(c)}), \quad E_c = \text{“The documentary identifies } c \text{ as Satoshi”}, \ \Omega_c = \{\mathsf{True}, \mathsf{False}\}, \ J_c = \{\mathsf{YES}, \mathsf{NO}$$

with indicator payoffs

$$R^{(c)}_{\mathsf{YES}}(\mathsf{True}) = 1, \ R^{(c)}_{\mathsf{YES}}(\mathsf{False}) = 0, \qquad R^{(c)}_{\mathsf{NO}}(\mathsf{True}) = 0, \ R^{(c)}_{\mathsf{NO}}(\mathsf{False}) = 1.$$

System-level mapping to Polymarket. Polymarket instantiates the prediction–market system $\mathcal{S} = (\mathcal{M}, \mathcal{N}, \mathsf{Res})$ as follows:

- $\mathcal{M}$ contains all candidate markets $\{M_c\}_{c \in C}$ under the HBO event (plus all other site markets).
- $\mathcal{N}$ is USDC (USD–denominated stablecoin). Each unit share settles to 0 or 1 USDC according to $R^{(c)}$.
- $\mathsf{Res} = \{\mathrm{res}_M\}_{M \in \mathcal{M}}$ gives each M_c a register $\mathrm{res}_{M_c} \in \{\perp\} \cup \Omega_c$, initially $\perp$, that flips exactly once to $\omega_{M_c} \in \Omega_c$ when the platform's oracle process (e.g., UMA's optimistic oracle) writes the outcome on-chain.

Settlement in our notation is $R^{(c)}_j(\omega_{M_c})$ USDC for each unit of label $j \in J_c$.

What resolved in the HBO case. The documentary focused on *Peter Todd*, which Polymarket grouped under $\mathsf{Other/Multiple}$. Hence

$$\omega_{M_{\mathsf{Other/Multiple}}} = \mathsf{True} \quad \text{and} \quad \omega_{M_c} = \mathsf{False} \ \text{ for all named } c \neq \mathsf{Other/Multiple}.$$

Equivalently: $\mathsf{Other/Multiple}$: YES paid 1 USDC; every named candidate's NO paid 1 USDC; the corresponding YES paid 0 USDC.

Relation to Arrow–Debreu (single book) vs. Polymarket (bundle). A single winner–take–all (Arrow–Debreu) market would model the event as one market $M^\star = (E^\star, \Omega^\star, J^\star, R^\star)$ with $\Omega^\star = C$ and $J^\star$ in bijection with $\Omega^\star$, so exactly one label pays 1 at resolution. Polymarket instead uses a *bundle of binaries* $\{M_c\}_{c \in C}$ (one YES/NO pair per candidate). This is a different microstructure: prices live in separate order books, and each market M_c resolves independently via its own register res_{M_c}.

Negative risk (Polymarket's cross-market linkage). When the parent event is configured as *negative risk*, Polymarket enables a conversion that links prices across the family: informally, a NO on candidate i is convertible into the basket of YES on all $j \neq i$. At the price level this couples the binaries so that, up to frictions,

$$\text{price}(\mathsf{NO}_i) \;\approx\; \sum_{j \neq i} \text{price}(\mathsf{YES}_j) \quad\Longrightarrow\quad \sum_{j \in C} \text{price}(\mathsf{YES}_j) \;\approx\; 1,$$

making the bundle trade *as if* it were a single Arrow–Debreu book while remaining, in our abstraction, a family $\{M_c\}$ with distinct $(E_c, \Omega_c, J_c, R^{(c)})$ and registers res_{M_c}.