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. Abstract goes here.

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. 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

[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.

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 eight stages: underlying infrastructure, market topic, market mechanism, pricing, trading, market resolution, settling, and archiving. For each stage, we enumerate the possible designs and discuss competing trade-offs.

2 Preliminaries

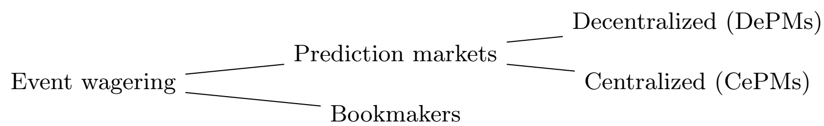
2.1 Methodology

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 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:

[4] `tk`



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 B 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* $\mathrm{res}_M \in \{\perp\} \cup \Omega_M$*,* res_M *is initially* $\perp$*, 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 $\mathrm{res}_M \in \{\perp\} \cup \Omega$, is initially $\perp$, 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.
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

[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

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 A.

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 in Figure **??**. 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 [5].

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 [6].

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 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

[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'

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 [4]. 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.* [4]).
	Mitigation: Avoid markets that are self-referential, including topics on the platform itself and its numinaire.

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.

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

[14] Polymarket: 'TikTok banned in the US before May 2025?'
[15] Polymarket: 'Will the missing submarine be found by June 23?'

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 $\{j_{\mathsf{k_Y}}, j_{\mathsf{k_N}}\}$ 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 and the market does not need to include every possible word (or an 'other' category). Further if the market is already underway with active trades, the word list can be expanded before the speech with a YNB market, whereas a WTA market cannot be fairly altered once the market begins trading.

A variant of the YNB market is one where, even though it is not necessary, the share outcomes are in fact complete and exclusive. For example, 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.' 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

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

(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 $|\Omega| - 1$.

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).

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 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

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

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 $j_{\mathsf{k_Y}}$ and one $j_{\mathsf{k_N}}$ for the chosen k. Hence, within any bundle $\text{totSupply}(j_{\mathsf{k_Y}}) = \text{totSupply}(j_{\mathsf{k_N}})$. 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 to our knowledge is not used in any DePMs. 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

To be finalized

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.

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

[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.

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

Archival, transparency, and metadata persistence within DPMs ensure verifiable and accessible records, directly impacting market integrity and governance processes.

Critical metadata, such as market states, transaction histories, and resolution outcomes, inherently benefit from blockchain immutability and cryptographic verification [5], [6]. Augur v2 stores metadata, including user profit/loss computations, directly on-chain, providing immediate access without external archives. This design increases transparency but also results in higher transaction costs and larger blockchain state size [7].

Off-chain metadata - including market descriptions, resolution criteria, and user-generated content - are typically stored in decentralized storage solutions due to blockchain capacity constraints [3]. IPFS (InterPlanetary File System) employs peer-to-peer, content-addressable storage using cryptographic hashes, verifying content authenticity through immutable identifiers. IPFS's availability depends on node operators maintaining persistent storage through pinning, without central points of failure [12]. Arweave offers an economic incentive structure combined with a "blockweave" architecture for permanent data storage, providing perpetual availability and resistance to censorship [15].

Recent updates to Ethereum, such as proto-danksharding, provide ephemeral "blob" storage. These storage blobs temporarily allow for large metadata availability and cryptographic verification. However, their short-term nature necessitates subsequent migration to persistent storage solutions [7].

The archival model chosen by a DPM influences governance outcomes and resilience against manipulation. Persistent archival supports retrospective audits critical for resolving disputes and maintaining accountability of oracle activities [6]. Decentralized archival mechanisms prevent centralized control from suppressing or altering market data, enabling community-driven governance or protocol forks when required [15].

Table 3 compares archival methods such as blockchain storage, IPFS, Arweave, Ethereum blob storage, and hybrid models. It details each method's durability, authenticity, and accessibility, highlighting their distinct operational trade-offs and cost implications for decentralized prediction markets.

4 Discussion

The design of DPMs involves inherent economic trade-offs affecting platform adoption, integrity, and resilience. This analysis examines these trade-offs across four dimensions: decentralization versus speed, liquidity versus capital efficiency,

Table 3. Comparative Evaluation of Archival Methods for Decentralized Prediction Markets

Archival Method	**Description**	**Durability & Persistence**	**Authenticity & Integrity**	**Accessibility & Discovery**	**Example Platforms**
Blockchain On-chain Storage	Directly store meta-data and outcomes on-chain (e.g., Ethereum).	Extremely high (immutable, perpetual)	High authenticity (cryptographic guarantees)	Excellent (immediate, global nodes)	Augur (partial), Gnosis
IPFS (Inter-Planetary File System)	Decentralized, peer-to-peer, content-addressable storage.	Medium (requires community pinning)	High (content hashes provide tamper-evidence)	Good (distributed nodes, variable retrieval speeds)	Augur, Polymarket
Arweave Permanent Storage	Blockchain-based storage with economic incentives for permanent retention.	Very high (economically incentivized permanence)	Very high (blockchain-backed immutability)	High (permanent, redundant node distribution)	Mirror.xyz, RedStone Oracles (experimental)
Ethereum Blob Storage	Temporary large-data storage via Ethereum blobs (proto-danksharding).	Low (temporary, ephemeral data availability)	High (cryptographic authenticity guaranteed short-term)	Moderate (short-term retrieval from Ethereum nodes)	Ethereum L2s (Optimism, Arbitrum)
Centralized Cloud Storage	Traditional cloud services (AWS, Google Cloud).	Variable (single point of failure risk)	Low–moderate (trust reliant on centralized operator)	High (fast retrieval, easy indexing)	Early centralized prediction platforms
Hybrid Storage Model	Combination: blockchain on-chain pointers plus decentralized or permanent storage.	High (leverages strengths of multiple methods)	High (on-chain hashes guarantee authenticity)	Very high (multiple redundancy points, robust discovery)	Polymarket, UMA

incentive robustness versus usability, and expressiveness versus composability, with agility noted as an additional consideration.

A fundamental trade-off occurs between decentralization and execution speed. Fully decentralized DPMs, such as early Augur versions, achieve censorship resistance but experience latency and high transaction costs due to reliance on Ethereum's mainnet [4] [13]. Hybrid models, including Polymarket, employ off-chain order matching and on-chain settlements or dedicated sidechains to increase throughput and improve usability, albeit with the addition of trust assumptions and centralization risks [6]. Layer-2 technologies like state channels and rollups offer alternative methods to balance decentralization and performance [11].

Liquidity provision versus capital efficiency presents another critical trade-off. Automated market makers (AMMs), such as Hansonian market scoring rules or constant product market makers (CPMM), deliver continuous liquidity by committing substantial collateral, reducing capital efficiency [9] [1]. Conversely, order-book-based models maximize capital efficiency by avoiding idle capital but can encounter liquidity issues and impaired price discovery, as noted in Augur v1 markets [14]. Platforms like Gnosis address some of these challenges through conditional markets that dynamically allocate capital among outcomes [8].

Incentive robustness and usability reflect another key trade-off. Augur's multi-stage dispute mechanisms and token staking enhance manipulation resistance but complicate user experience and slow resolution processes [13] [6]. In contrast, simplified oracle solutions, such as UMA's optimistic oracle, offer streamlined resolution processes but carry greater risks of manipulation. Hierarchical or two-tiered dispute frameworks (e.g., Pisa watchtowers) seek to address these issues by maintaining manipulation resistance while minimizing complexity [11].

Expressiveness versus composability represents an additional design dimension. Highly expressive combinatorial market structures, such as those enabled by Gnosis's Conditional Tokens, allow detailed market configurations but reduce interoperability and composability with other decentralized finance (DeFi) systems due to technical complexity [8]. Simpler binary or categorical markets increase interoperability and composability but sacrifice detailed market structuring capabilities.

5 Conclusion

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. Angeris, G., Chitra, T.: Improved price oracles: Constant function market makers. In: Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. pp. 80–91 (2020)
2. 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
3. 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)
4. 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)
5. 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)
6. Foxley, W.: 5 years after launch, predictions market platform augur releases version 2. https://www.coindesk.com/tech/2020/07/28/5-years-after-launch-predictions-market-platform-augur-releases-version-2 (Jul 2020), updated Dec 10, 2022; Accessed: 2025-06-25
7. Gnosis: Gnosis whitepaper. https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/Gnosis.pdf (2017), accessed: 2025-06-01
8. Hanson, R.: Combinatorial information market design. Information Systems Frontiers **5**, 107–119 (2003)
9. McCorry, P., Bakshi, S., Bentov, I., Meiklejohn, S., Miller, A.: Pisa: Arbitration outsourcing for state channels. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 16–30 (2019)
10. Merlec, M.M., In, H.P.: Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study. MDPI Sustainability **16**(17), 7671 (2024)
11. Peterson, J., Krug, J., Zoltu, M., Williams, A.K., Alexander, S.: Augur: a decentralized oracle and prediction market platform. arXiv preprint arXiv:1501.01042 (2015)
12. Team, O.D., Akhunov, A.: Client optimizations to parity: Openethereum v2.3.0. https://github.com/openethereum/parity-ethereum/releases/tag/v2.3.0 (2020), accessed: 2026-06-01
13. Williams, S., Kedia, A., Berman, L., Campos-Groth, S.: Arweave: The permanent information storage protocol. https://www.arweave.org/files/arweave-lightpaper.pdf (2023)

A Satoshi HBO Market

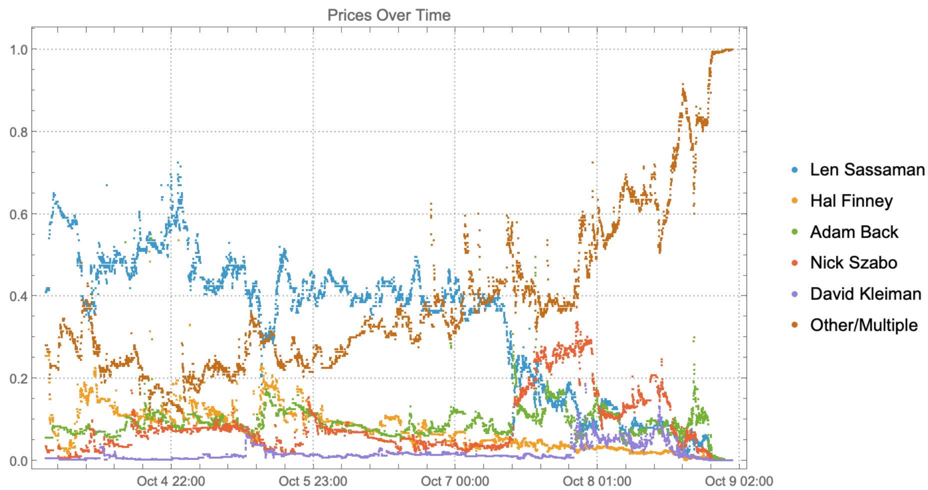


Fig. 1. The price movements for 6 leading candidates in the Polymarket market for who would be named as Satoshi Nakamoto in the HBO documentary 'Money Electric' which aired the evening of October 8.

B Example instantiation of formal definitions

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.

B.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

[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).

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

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

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 $\mathcal{N}$.

B.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 $R_j^{(c)}(\omega_{M_c})$ 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 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: 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,

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

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}.

C Leverage

Edge, capital, and "leverage" in binary prediction shares. Let a YES share pay \$1 if the event occurs and \$0 otherwise. If the market price is $v \in (0,1)$ and your subjective probability is p^*, then the expected profit per share is

$$\mathbb{E}[\pi] = p^* - v.$$

Although the dollar edge per share may look small (e.g., $p^* = 0.60$ vs. $v = 0.48$ gives $\mathbb{E}[\pi] = 0.12$), the capital at risk is only the purchase cost v. The expected *return on capital* for that trade is

$$\mathrm{ROC}_{\mathrm{EV}} = \frac{p^* - v}{v} = \frac{0.12}{0.48} \approx 25\%,$$

which is large. If price moves toward your view before resolution, you can also exit early and realize gains without tying up capital to maturity.

Sizing the position with Kelly (from first principles). Suppose you invest a fraction f of current wealth W into the share at price v. You buy fW/v shares. If the event occurs (probability p^*), post-settlement wealth is

$$W^+ = W - fW + \frac{fW}{v} = W\big[1 + f\,(v^{-1} - 1)\big],$$

and if it does not occur (probability $1 - p^*$), wealth is $W^- = W(1 - f)$. Kelly sizing chooses f to maximize expected log-wealth:

$$\max_{0 \le f < 1} \; p^* \ln\!\big(1 + f(v^{-1} - 1)\big) + (1 - p^*) \ln(1 - f).$$

Differentiating and setting the derivative to zero yields the closed-form optimal fraction

$$f^* \;=\; \frac{p^* - v}{1 - v}.$$

Equivalently, writing the "net odds" on a \$1 stake as $b = (1 - v)/v$, the familiar Kelly form is $f^* = (b\,p^* - (1 - p^*))/b$. For the running example ($p^* = 0.60$, $v = 0.48$), $f^* = (0.60 - 0.48)/0.52 \approx 0.231$, i.e., about 23% of bankroll on the YES side.[20]

Practical notes. Kelly is optimal for log-utility over *repeated, independent* favorable bets with known p^*. In markets, p^* is estimated, bets are correlated, capital is finite, and fees and liquidity matter. Practitioners therefore use fractional Kelly (e.g., $f = \lambda f^*$ with $\lambda \in [0, 1]$, often $\lambda = \frac{1}{2}$) to reduce drawdowns and model-error risk. Time to resolution also matters: tying up v until maturity lowers annualized return unless you recycle capital via interim exits.

[20] For shorting a YES share priced at v (i.e., taking NO), replace v by $1 - v$ and p^* by $1 - p^*$ in the formula, or derive symmetrically.