SoK: Decentralized Prediction Markets

Jeremy Clark[1][0000−0002−3533−5965] (✉) and Nahid Rahman[1][0000−000x−xxxx−xxxx]

Concordia University, Montreal, Canada
j.clark@concordia.ca, nahid.rahman@mail.concordia.ca

Abstract. Abstract goes here.

Keywords: security · cryptography

1 Introduction

2 Background and Motivation

3 Methodology

4 Modular Workflow

The modular workflow for DPMs, detailed in sub-sections 4.1 through 4.8 , outlines key components and decision pathways involved in platform development and operation. Initially, designers select an appropriate blockchain infrastructure, evaluating trade-offs between Layer-1 mainnet's decentralization and security versus Layer-2's cost and throughput efficiencies, considering bridging delays and associated security risks (Section 4.1). Following this, market creation is structured by deciding on permissioned or permissionless market listing models (Section 4.2). Next, the workflow addresses the tokenization of market outcomes (Section 4.3) and implements suitable trading mechanisms such as automated market makers (AMMs), limit order books, or a hybrid combination of both (Section 4.4). After market closure, the platform utilizes either centralized or decentralized oracle systems, including potential dispute resolution processes for contested outcomes (Section 4.5). Subsequent stages involve selection of payout methods (automatic push or claim-based pull) and managing remaining funds or platform fees (Sections 4.6). The market metadata archival is preserved on-chain logs or decentralized storage services such as IPFS and Arweave (Section 4.7). Finally, economic trade-offs affect the popularity usability and adoption of the market (Section 4.8). This modular workflow is visualized in Figure 1 below.

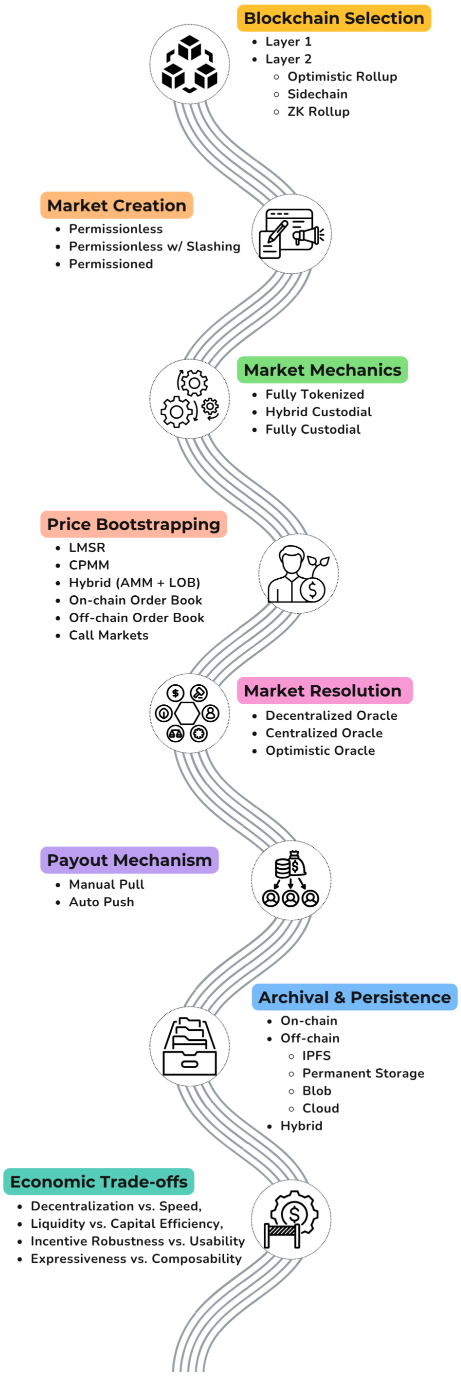

Fig. 1. Modular Workflow for Decentralized Prediction Market Platforms.

4.1 Underlying Blockchain Infrastructure

The base blockchain layer (Layer-1 vs. Layer-2) impacts transaction fees, finality guarantees, throughput, and censorship resistance for DPMs, influencing the efficiency and reliability of each stage within the DPM modular workflow. Selecting the underlying blockchain infrastructure constitutes the initial design decision within the modular workflow for DPMs.

Ethereum Layer-1 (L1) mainnet uses proof-of-stake consensus with explicit finality at approximately 13-minute intervals post-Merge, incurring transaction fees typically between $1 and $20 and supporting throughput of around 15–30 transactions per second (TPS) [12]. The relatively higher fees and limited throughput can restrict frequent trading activities and real-time market responsiveness within the DPM modular workflow.

Bitcoin's proof-of-work consensus results in probabilistic finality, generally confirmed after around 60 minutes, with throughput around 7 TPS and fees from $1 to $5, impacting the settlement timing and reliability of outcome reporting and payouts in DPMs [8]. Ethereum's implementation of proposer/builder separation (PBS) and fair-ordering protocols addresses maximal extractable value (MEV) risks, mitigating transaction front-running and block reordering threats that could compromise fairness within market trading and resolution stages [9].

Layer-2 (L2) solutions, including optimistic and Zero Knowledge (ZK) rollups, reduce fees to few cents per transaction and improve throughput to thousands of TPS, facilitating high-frequency trading and timely market resolution. Optimistic rollups introduce withdrawal delays of around 7 days due to fraud-proof verification, complicating liquidity management and affecting timely payouts in the market settlement stage. ZK rollups, using validity proofs, offer quicker withdrawal options, beneficial for improving liquidity availability in the workflow [18]. However, the centralization of sequencers in some L2 platforms like Arbitrum introduces potential censorship issues, partially mitigated by reducing forced-inclusion delays from 24 to 4 hours, thereby influencing market openness and fairness during trading and settlement phases [3].

Bitcoin's simpler architecture provides resistance to blockchain reorganizations but lacks detailed MEV mitigation, potentially exposing prediction markets to transaction ordering vulnerabilities. Bridging infrastructure connecting L1 and L2 platforms introduces additional latency, complexity, and security risks, potentially disrupting seamless market transitions between layers. Multisig custodians and relay validators involved in bridging have historically been susceptible to financial exploits, highlighting critical risks to asset safety and liquidity flow within the modular workflow of DPMs.

Table 1 below summarizes the performance and decentralization characteristics of blockchain infrastructures relevant to the DPM modular workflow. These infrastructure characteristics shape the feasibility of subsequent market design elements, including market setup and initialization.

Explicit finality mechanisms, such as Ethereum's proof-of-stake consensus, provide certainty regarding transaction irreversibility after a specific period, enabling precise timing for market settlements and payouts [12]. In contrast, prob-

Table 1. Comparative Attributes of Blockchain Infra for DPM Platforms

Attribute	**Ethereum Mainnet**	**Polygon**	**Bitcoin**
Transaction Latency	∼12–15 sec/block; ∼13 min finality	∼2–5 sec/block	∼10 min/block; ∼60 min finality
Bridging Delays	∼7 days (Optimistic Rollups)	∼30 min–3 hrs (Checkpointing)	∼60 min (Sidechains)
Transaction Costs	High ($1–20+ per tx)	Very low ($0.01–0.05 per tx)	Moderate-high ($1–5+ per tx)
Throughput (TPS)	∼15–30 TPS	∼7,000 TPS (peak)	∼7 TPS
Validator Decentralization	High (∼600,000 validators)	Moderate (∼100–150 validators)	High (large miner base)
Censorship Resistance	High (MEV risk present)	Moderate (checkpoint risk)	High (minimal MEV risk)

abilistic finality, characteristic of Bitcoin's proof-of-work, introduces uncertainty, requiring multiple block confirmations, thereby delaying final market outcomes and associated payout distributions [8].

4.2 Market Setup and Initialization

Market setup and initialization choices influence censorship resistance, regulatory compliance, and operational effectiveness of DPMs.

Permissionless Models: In permissionless setups, such as Augur, any user can initiate markets without centralized oversight, enabling maximum censorship resistance and innovation [10]. This openness creates potential regulatory challenges, illustrated by Augur's "assassination markets" controversy, where third-party moderation efforts (e.g., Predictions.Global) were limited in effectiveness. Economic penalties like validity and no-show reporter bonds address malicious or ambiguous market creation. Permissionless setups typically encourage standardized event templates to minimize ambiguity, though custom markets remain allowed. Collateral selection often involves endogenous (native) tokens (e.g., ETH for Augur), introducing volatility risk and regulatory complexity, balanced by potential hedging benefits when outcomes correlate with token value [25] [26].

Hybrid Governance Models (Permissionless with Centralized Slashing): Hybrid models allow permissionless market creation combined with centralized oversight mechanisms. Platforms like Polymarket use entities such as a Market Integrity Committee to enforce compliance and penalize markets violating rules [12] [10]. This partially decentralizes market listing but maintains centralized control, creating regulatory accountability and single points of control. Hybrid platforms also leverage standardized event templates to maintain clarity and reduce dispute risk, supplemented by custom market oversight. Collateral choices generally include stablecoins, reducing volatility exposure and regulatory uncertainty compared to endogenous tokens.

Permissioned Models: Fully permissioned setups, including Kalshi and PredictIt, require internal or regulatory reviews before listing markets, significantly reducing regulatory and operational risks by limiting ambiguous or unlawful markets [8]. Market proposals typically use standardized event templates to ensure unambiguous resolution, supported by rigorous internal review. Collateral is generally stablecoins or fiat currency, minimizing volatility and simplifying regulatory compliance. Strict implementation of KYC/AML protocols further reduces regulatory exposure, though it introduces operational overhead and restricts market diversity [10].

Table 2 summarizes operational implications for each market setup, guiding stakeholders in selecting appropriate governance models based on desired censorship resistance, compliance requirements, and collateral management.

Table 2. Comparative Evaluation of Market Creation and Permission Models

Market Setup	**Benefits**	**Drawbacks**	**Platforms**
Permissionless	Open participation, censorship resistance, flexible collateral (endogenous tokens)	Regulatory risks, potential misuse, collateral volatility exposure	Augur, PlotX, Gnosis
Permissionless with Slashing	Openness balanced by centralized enforcement, stable collateral (stablecoins)	Centralized oversight, regulatory accountability	Polymarket, UMA*
Permissioned	Compliance, controlled market environment, stable collateral (stablecoins, fiat)	Limited diversity, lower censorship resistance, operational overhead	Kalshi, PredictIt, Stox

*UMA is not a DPM in the traditional sense; it is mentioned here due to its Permissionless with Slashing model usage.

4.3 Market Mechanics and Share Custodianship

Market mechanics and share custodianship directly influence the operational efficiency, liquidity, and decentralization of DPMs.

Binary markets offer intuitive simplicity and consolidated liquidity, facilitating hedging via straightforward YES/NO token pairs, as exemplified by Polymarket's ERC-1155 tokens redeemable for $1 upon outcome resolution [25] [17] This binary structure enables users to hedge risks akin to insurance instruments, although extensive hedging activities by risk-averse participants can temporarily distort prices, potentially diverging from true event probabilities until arbitraged by informed traders [16].

In contrast, combinatorial markets, which enable complex bets on interdependent outcomes, significantly enhance theoretical information aggregation by capturing correlations and conditional probabilities but impose exponential computational complexity (#P-hard for LMSR market makers) and cognitive burdens on users [6] [7]. Thus, combinatorial markets have remained largely experimental, given the difficulty in matching trades efficiently without algorithmic support and substantial fragmentation of liquidity (Pennock & Sami, 2007).

Markets inherently start with zero traders, necessitating careful liquidity bootstrapping to avoid under-collateralization and price manipulation. Safe market initialization requires at least two traders with opposing views (or one trader matched by an automated market maker) to create balanced, fully collateralized initial positions. This balanced issuance is critical to avoid under-collateralization and ensure meaningful initial price discovery; for instance, Polymarket only mints YES and NO shares simultaneously upon matched buyer-seller orders that sum exactly to $1 collateral [8]. Similarly, Augur mandates traders to initially collateralize all outcomes fully, thus guaranteeing solvent market conditions from inception [25].

Custodianship models significantly affect decentralization, regulatory visibility, and systemic trust. Fully tokenized on-chain shares (ERC-20/ERC-1155) maximize decentralization and composability within broader DeFi ecosystems. Conversely, centralized custodial models, though enabling simpler KYC/AML integration, inherently risk censorship and unilateral asset control, undermining core decentralized principles [10]. Polymarket notably adopted more centralized custodianship following regulatory enforcement by the CFTC, underscoring the practical impacts of regulatory pressures on market design [20]. Table 3 below summarizes custodianship models, highlighting their implications for composability, decentralization, and systemic trust.

Table 3. Comparative Analysis of Custody Models for Outcome Tokenization

Custody Model	**Composability**	**Regulatory Visibility**	**Systemic Trust & Risk**	**Decentralization**	**Examples**
Fully Tokenized (ERC-20 / ERC-1155)	High (DeFi interoperability)	High (public)	Smart-contract reliant	High	Augur, Gnosis
Hybrid Custodial	Moderate	Moderate-high (KYC/AML)	Partial central reliance	Moderate	Polymarket, UMA
Fully Centralized	Low (none)	Low visibility, high control	Centralized, censorship risk	Low	Kalshi, PredictIt

4.4 Price Bootstrapping and Liquidity Mechanisms

Price bootstrapping and liquidity provision enable initial price formation and continuous trading in DPMs. Automated Market Makers (AMMs) address the bootstrapping challenge by providing immediate liquidity and initial price setting without requiring initial trading counterparties. The Logarithmic Market Scoring Rule (LMSR), introduced by [16], utilizes a convex cost function: FORMULA REMOVED where b>0 defines liquidity depth [23]. LMSR adjusts instantaneous outcome prices using a softmax function to maintain valid probability distributions. LMSR limits liquidity provider losses to a maximum of $b \ln N$ for a market with N outcomes, providing a known loss boundary [7]. Selecting the liquidity parameter b presents practical challenges; inappropriate values can result in either excessive price sensitivity or limited market responsiveness [16]. Constant Product Market Makers (CPMM), such as those based on the invariant:

$$x \cdot y = k$$

manage liquidity by holding two token reserves, with outcome prices determined by the ratio of these reserves [1]. Arbitrage ensures prices generally sum to a valid probability distribution. However, CPMMs expose liquidity providers to divergence loss (impermanent loss), where large shifts in outcome probabilities leave providers holding primarily the less valuable tokens at resolution [5]. Unlike LMSR, CPMM does not limit potential losses, thus introducing additional financial risk despite operational simplicity and compatibility with decentralized finance (DeFi) protocols. Hybrid models integrating AMMs with limit order books (LOBs), as implemented by platforms like Polymarket, combine continuous liquidity provided by AMMs with liquidity precision offered by order books [12]. These hybrid systems facilitate arbitrage-driven adjustments that stabilize market prices and maintain accurate probability reflections, balancing AMM simplicity with order book responsiveness.

Alternative liquidity mechanisms, including pure on-chain order books and periodic call markets, introduce distinct trade-offs, which are detailed in Table 1. Pure on-chain order books offer precise pricing but encounter issues related to transaction latency and high gas fees, whereas off-chain order books mitigate these problems at the expense of decentralization [8]. Call markets aggregate trades at regular intervals to improve liquidity but face latency issues and potential arbitrage vulnerabilities due to delayed execution [11].

Table 4 contrasts liquidity mechanisms used in decentralized prediction markets by evaluating their risk characteristics, price formation methods, and operational attributes. Each mechanism presents unique trade-offs, balancing liquidity provider risks, system complexity, arbitrage vulnerabilities, and operational efficiency.

4.5 Market Resolution and Dispute Models

Market resolution and dispute models are essential for accurate and fair settlement in DPMs, directly affecting market credibility and operational continuity. Single-trusted entity models utilize a single oracle, such as the Associated Press, enabling efficient and rapid finalization. However, reliance on a single entity introduces centralization risks, including vulnerability to bribery and biased reporting [12]. Economic deterrents like escrow bonds may not prevent manipulation if potential gains surpass the penalties.

Decentralized oracle collectives distribute decision-making across multiple oracles. Chainlink aggregates data from independent nodes using median or majority votes, with nodes required to stake tokens, incentivizing accuracy and

Table 4. Comparative Analysis of Liquidity Mechanisms

Liquidity Mechanism	**Loss Limitation**	**Price Formation**	**Complexity**	**Arbitrage Exposure**	**Operational Latency**
LMSR	Yes	Softmax pricing	Moderate	Moderate	Low
CPMM	No	Reserve ratios	Low	High	Low
Hybrid (AMM + LOB)	Partial	Mixed	High	Moderate	Low to Moderate
On-chain Order Book	No	Order matching	High	Moderate	High
Off-chain Order Book	No	Order matching	Moderate	Moderate	Low
Call Markets	No	Batch matching	Moderate	High	Moderate to High

penalizing errors. MakerDAO uses governance-based collectives, electing trusted data feeders through community governance to enhance transparency and reduce individual collusion risks [12]. These collectives, however, experience higher latency and complexity and remain susceptible to coordinated manipulation and governance capture. UMA's Data Verification Mechanism (DVM) dynamically calculates stakes based on the Cost of Corruption versus Profit from Corruption, aiming to ensure corruption costs always exceed potential profits [19]. Realitio employs a tiered dispute escalation process, resolving uncontested outcomes swiftly while disputed cases escalate to external arbitrators like Kleros, balancing speed and decentralization.

Self-settling models depend entirely on internal incentives to align reporter behaviour around Schelling points. Augur exemplifies this, with REP tokens staked to encourage reporting consistent with the majority's expectations. Disputes trigger increased staking requirements and potentially protocol forks, reinforcing truthful reporting through economic incentives [25]. Yet, these mechanisms are vulnerable to coordinated bribery and external manipulation, especially when attackers exploit side-bet strategies [13]. An attacker-defender payoff matrix clearly illustrates these economic vulnerabilities, highlighting equilibrium conditions shaped by manipulation costs and incentives.

Table 5 provides a comparative evaluation of oracle types, outlining operational characteristics, specific risks, and representative examples. It succinctly differentiates between single trusted entities, decentralized oracle collectives, and self-settling oracles by highlighting advantages such as decentralization levels and inherent vulnerabilities like susceptibility to bribery.

Table 6 presents a detailed incentive compatibility payoff matrix for Augur's REP staking mechanism. It describes four distinct situations with different combinations of attacker and honest stakes, and potential rewards if an attacker succeeds versus consequences if defenders successfully prevent the attack. The first scenario shows stability when no attack occurs and reporting remains honest, generating standard rewards. In the second scenario, a small attacker stake versus a larger honest stake renders attacks unlikely due to limited attacker profitability. However, in scenarios with higher attacker stakes or significant external

Table 5. Comparative Evaluation of Market Resolution Types

Oracle Type	**Pros**	**Cons**	**Examples**
Single Trusted Entity	Fast resolution; clear accountability	Single failure point; high censorship risk	Associated Press, Chainlink
Decentralized Oracle Collective	Distributed trust; censorship resistance	Higher complexity; risk of collusion	UMA, Realitio, MakerDAO
Self-Settling (Schelling-Point)	No external trust; economic incentives	Vulnerable to bribery; fork complexity	Augur, Truthcoin, Kleros

bets, the table demonstrates potential attacker profitability, making bribery economically viable and possibly leading to the breakdown of the Schelling point equilibrium.

Table 6. Oracle Incentive Compatibility Payoff Matrix (Example: Augur REP Game)

Scenario	**Attacker Stake (A)**	**Honest Stake (H)**	**Attacker Reward if Successful**	**Defender Reward if Successful**	**Equilibrium Result**
No Attack, Honest Majority	$0	$1,000,000	$0	$0 (normal fees)	Honest Reporting Stable
Attack, Low Attacker Stake	$500,000	$1,000,000	$10,000,000	Attacker's stake (slashed)	Honest Reporting Stable (Attack Unlikely)
Attack, High Attacker Stake	$1,500,000	$1,000,000	$10,000,000	Attacker's stake (slashed)	Attacker Profitable (Bribe Possible)
Coordinated Side-Bet Bribery	$2,000,000	$1,000,000	$20,000,000 (external bets)	Attacker's stake (slashed)	Attack Profitable (Schelling Point Fails)

To mitigate vulnerabilities identified in Table 6, designers can implement thresholds for stake escalation and require proportionally larger attacker stakes relative to honest stakes to disrupt equilibrium [25]. Additionally, periodic audits or community-based moderation processes may deter coordinated attacks, reinforcing equilibrium stability [12].

4.6 Payout and Redemption Mechanisms

DPMs commonly implement push or pull payout mechanisms, each presenting distinct trade-offs. Push payout models automatically distribute winnings once market outcomes are resolved, reducing user interaction requirements. However, they face scalability and cost constraints due to increased gas usage, especially in scenarios involving numerous recipients [12]. Polymarket uses a hybrid model on the Polygon network with USDC that mimics push mechanisms via meta-transactions, effectively removing direct user gas fee payments [20] Castle Capital, 2024). Conversely, Augur utilizes a pull mechanism, requiring users to manually redeem tokens to collect payouts. This approach prioritizes decentralization but increases the complexity and cost associated with claiming rewards [24].

Gasless redemption mechanisms aim to improve usability by eliminating user gas fees, typically relying on third-party relayers to cover transaction costs. Such mechanisms enhance accessibility but introduce dependencies on centralized components, creating potential points of failure or censorship (Castle Capital, 2024).

Time-bounded redemption windows set deadlines for payout claims, aiming to reduce inefficiencies caused by permanently locked collateral. These mechanisms can enhance capital utilization but raise ethical and regulatory concerns, including issues related to unclaimed property regulations and user fairness [12]. Major platforms like Augur and Polymarket generally favor open-ended claims to uphold continuous user rights.

Surplus management deals with residual funds from unclaimed or locked winnings. Permanent locking maintains explicit user ownership at the expense of economic efficiency over time, exemplified by Augur's approach [12]. Redistribution methods periodically allocate surplus to liquidity providers or active users, increasing capital efficiency but potentially creating incentives to abandon minor balances intentionally. Governance-controlled treasuries allow directed surplus management, balancing efficiency against the risk of centralized governance influence and regulatory attention [2].

Table 7 compares surplus management methods in decentralized prediction markets, evaluating their economic efficiency, ethical considerations, and regulatory implications. It identifies trade-offs between preserving explicit user ownership and maximizing capital efficiency, highlighting potential governance risks and compliance requirements for different mechanisms.

4.7 Archival, Transparency, and Meta-Data Persistence

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 [10], [12]. 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 [14].

Off-chain metadata - including market descriptions, resolution criteria, and user-generated content - are typically stored in decentralized storage solutions due to blockchain capacity constraints [4]. 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 [22]. Arweave offers an economic incentive structure

Table 7. Comparative Evaluation of Surplus Management Mechanisms

Mechanism	**Description**	**Economic Efficiency**	**Ethical Considerations**	**Regulatory Implications**	**Example Platforms**
Permanent Locking	Surplus funds locked indefinitely post-resolution	Low	Maintains explicit user ownership	Low regulatory risk	Augur, Gnosis
Redistribution to LPs/Stakers	Surplus periodically redistributed to liquidity providers	High	May incentivize intentional abandonment	Moderate, potential property concerns	UMA, Realitio
Governance-controlled Treasury	Surplus directed by governance structures	Moderate–High	Potential governance influence risk	Moderate–High, regulatory attention	Polymarket, SX Network
Burning Tokens	Surplus tokens destroyed to reduce supply	Moderate–High	Minimal ethical concerns	Moderate, regulatory stance uncertain	Truthcoin (theoretical)
Returning to Original Funders	Surplus returned to initial market creators	Moderate	Risks manipulation incentives	High, KYC and AML compliance concerns	Kalshi

combined with a "blockweave" architecture for permanent data storage, providing perpetual availability and resistance to censorship [28].

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 [14].

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 [12]. Decentralized archival mechanisms prevent centralized control from suppressing or altering market data, enabling community-driven governance or protocol forks when required [28].

Table 8 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.

4.8 Economic Trade-Offs in DPM Design

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, 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 re-

Table 8. 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 metadata and outcomes on-chain (e.g., Ethereum).	Extremely high (immutable, perpetual)	High authenticity (cryptographic guarantees)	Excellent (immediate, global nodes)	Augur (partial), Gnosis
IPFS (InterPlanetary 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

sistance but experience latency and high transaction costs due to reliance on Ethereum's mainnet [8] [24]. 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 [12]. Layer-2 technologies like state channels and rollups offer alternative methods to balance decentralization and performance [21].

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 [16] [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 [27]. Platforms like Gnosis address some of these challenges through conditional markets that dynamically allocate capital among outcomes [15].

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 [24] [12]. 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 [21].

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 [15]. Simpler binary or categorical markets increase interoperability and composability but sacrifice detailed market structuring capabilities.

5 Security and Adversarial Considerations

6 Regulatory and Ethical Considerations

7 Case Studies

8 Future Directions and Open Challenges

9 Conclusion

Scope. Blah blah blah.

Contributions. Our primary contributions are as follows.

1. Blah blah blah.
2. Blah blah blah.
3. Blah blah blah.

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. Bentov, I., Mizrahi, A., Rosenfeld, M.: Decentralized prediction market without arbiters. In: Financial Cryptography and Data Security: FC 2017 International Workshops. pp. 199–217 (2017)
3. Bjelic, M., Nailwal, S., Chaudhary, A., Deng, W.: Pol: one token for all polygon chains (2017)
4. 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
5. Cartea, Á., Drissi, F., Monga, M.: Predictable losses of liquidity provision in constant function markets and concentrated liquidity markets. Applied Mathematical Finance **30**(2), 69–93 (2023)
6. Chen, Y., Fortnow, L., Lambert, N., Pennock, D.M., Wortman, J.: Complexity of combinatorial market makers. In: Proceedings of the 9th ACM Conference on Electronic Commerce. pp. 190–199 (2008)
7. Chen, Y., Pennock, D.M.: Designing markets for prediction. AI Magazine **31**(4), 42–52 (2010)
8. 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)
9. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. arXiv preprint arXiv:1904.05234 (2019)
10. 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)
11. Eskandari, S., Clark, J., Sundaresan, V., Adham, M.: On the feasibility of decentralized derivatives markets. In: Financial Cryptography and Data Security: FC 2017 International Workshops. pp. 553–567 (2017)
12. 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)
13. Ford, B., Böhme, R.: Rationality is self-defeating in permissionless systems. arXiv preprint arXiv:1910.08820 (2019)
14. 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

15. Gnosis: Gnosis whitepaper. https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/Gnosis.pdf (2017), accessed: 2025-06-01
16. Hanson, R.: Combinatorial information market design. Information Systems Frontiers **5**, 107–119 (2003)
17. IOSG Ventures: Prediction market – a deep dive. https://medium.com/iosg-ventures/prediction-market-a-deep-dive-fbd2ee5b951c (2020), accessed: 2025-06-01
18. Kanani, J., Nailwal, S., Arjun, A.: Matic whitepaper. Polygon Technology (2021)
19. Lambur, H., Lu, A., Cai, R.: Uma's data verification mechanism. https://medium.com/uma-project/umas-data-verification-mechanism-3c5342759eb8 (Aug 2019), accessed: 2025-06-25
20. Mattmuller, K.: Decentralized prediction markets. Georgetown Law Technology Review **8**, 384 (2024)
21. 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)
22. 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)
23. Othman, A., Pennock, D.M., Reeves, D.M., Sandholm, T.: A practical liquidity-sensitive automated market maker. ACM Transactions on Economics and Computation (TEAC) **1**(3), 1–25 (2013)
24. 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)
25. Peterson, J., Krug, J., Zoltu, M., Williams, A.K., Alexander, S.: Augur: a decentralized oracle and prediction market platform (v2. 0). Whitepaper, https://augur.net/whitepaper. pdf (2019)
26. Sztorc, P.: Truthcoin: Peer-to-peer oracle system and prediction marketplace. https://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf (2015), accessed: 2025-06-01
27. 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
28. Williams, S., Kedia, A., Berman, L., Campos-Groth, S.: Arweave: The permanent information storage protocol. https://www.arweave.org/files/arweave-lightpaper.pdf (2023)