Project Staghunt

A Six Pager on Coordination Markets / hashdag

---

1. Azazel

Every generation a new social theory offers a fresh "solution" to "society", galvanizing our freshmen and the existentially unmoored. Workers of the world unite, tax the rich, check your privilege. But before we Greta ourselves into the abyss, we should less enthusiastically analyze when and how our current system - capitalism - fails or underperforms: What specifically fails when you give agents the autonomy to gather information, make judgment calls, choose actions, bear consequences?

Oh! you cry, The Prisoner's Dilemma! Aha The Moloch!!

But the games we actually play suggest a different response, one that promises less than social-welfare optimization, but also demands less than rewiring our selfish instincts and slaying the Moloch. Namely, mechanisms for committable and actionable coordination.

Consider Rousseau's stag hunt: Two hunters can collaborate on a stag and eat well, or each hunt a hare and eat for a few hours. Both are better off coordinating on a stag – wherein neither is incentivized to defect! – but moving from hare to stag alone makes you worse off. If they are stuck in a (hare,hare) equilibrium, the challenge is not defection from cooperation rather failure to reach coordination (stag,stag).

	Cooperate	Defect
Cooperate	$10, 10$	$0, 13$
Defect	$13, 0$	$3, 3$

Fig. 1: Prisoner's Dilemma

	Stag	Hare
Stag	$10, 10$	$-2, 3$
Hare	$3, -2$	$3, 3$

Fig. 2: Stag Hunt

If Moloch is the demon of defection, this is a different demon. I call it Azazel - the deity of the wilderness, pre civilization, where humans wander alone and no associations form.

The distinction between Moloch and Azazel matters because these two demons require very different remedies. If you believe society is trapped mostly by Moloch, the natural response is to build central institutions that restrain selfish behavior. Central planning, regulation, social-justice activism, superintelligence singletons. But if the problem is mainly Azazel, the remedy changes, people's behaviour doesn't need to be corrected or coerced, they already want to collaborate. What we lack, in the Azazel-Staghunt framework, is "merely" mechanisms to communicate and bind shared actions.

In short, we need Coordination Markets.

2. Why Cheap Talk Is Not Enough

Coordination Markets (CMs) are a category of markets built around binding primitives for coordinated action. These primitives compose, condition on external state, respond dynamically to market activity, and settle atomically.

Improving the internet through better communication channels does not suffice, since cheap talk is non-binding. In many scenarios, moving alone is risky: hunting a stag alone risks hunger and injury, rioting alone against a despot risks death, bootstrapping a liquidity pool alone risks getting eaten alive by arbitrageurs.

The missing layer, therefore, is not communication but binding intents, otherwise known as assurance contracts (Bagnoli and Lipman 1989). An assurance contract is a primitive allowing one to express and enforce conditional commitments of the form “I will do X if N others do X.” In our stack, these conditional commitments will be called *intendos*.

None of this is fundamentally new. PledgeBank ran conditional commitments from 2005, but the binding there was enforced by social pressure in small groups. The Point built assurance contracts in 2007, then pivoted to Groupon, more demand aggregation than assurance contracts. Kickstarter owned assurance contracts for creative projects, but remained niche. Each of these attempts either collapsed into a single vertical or was heavily biased toward petitions and activism, which is an esoteric death sentence.

Instead, we should take a market approach to coordination. A market framing has many implications; three immediate ones: First, endogenous incentives. Participants communicate their intents and commit not (merely) because they believe in the cause, but (also) because the mechanism makes commitment individually rational.

Second, a market approach is unopinionated, it should engineer for no specific agenda or world order (e/acc, radical markets). Market rails should remain open to whatever coordination problems and causes users initiate. In fact, if CMs are to unlock even a fraction of their potential, the rails should be optimized for unopinionatedness–-design for hard resilience to pressure, extortion, manipulation. This also means the mechanism should support heterogeneous preferences and risk thresholds, rather than hard-code a single safety threshold. A tenured professor might come out of the closet provided 5 colleagues do so; an assistant

professor might require 50; one LP is comfortable with a liquidity bootstrap floor of $1M; another is risk-averse and demands $10M.

Third, the mechanism should be able to condition on external state. Conditions should be able to reference on-chain data, real-world events, and other facts verifiable on the web. Intendos should also be able to condition on other intendos, chaining coordination markets into multi-stage sequences.

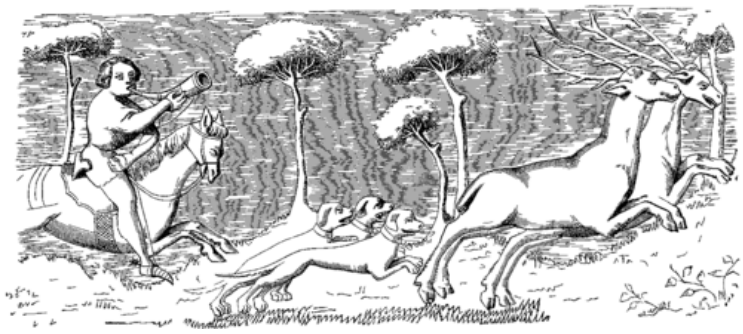
–

But before any of that, CMs must allow shielding one's intendo. Even before the move-alone risk, being the first to signal willingness is itself a primary source of risk: revealing one's political preferences in a hostile environment, disclosing one's financial intention in the face of arb bots, exposing a social cause when it is still small and can be killed. Allowing for confidential intents should receive axiomatic treatment.

On the other hand, collaborating in a dead dark forest is unlikely to catch momentum. Our attention is scarce, and the design should therefore borrow from and interleave with attention markets. It must foster some social p2p dynamic and/or incentive structures that outweigh the mental load of considering one's stance and opportunities.

3. The Mechanism

A social or financial entrepreneur believes she spotted a Stag - a certain opportunity that increases the payoff of its rational (selfish) participants. She posts a Hunt, and individual users or agents discover it and contemplate. An agent deciding to join signs cryptographically an intent to join - an intendo - conditioned on a sufficient number of others joining too. The signed intendos accumulate and Pack, in an opaque process, during which more agents opt in but also may opt out at will. Once some subset of agents crosses the threshold, satisfying internally the threshold conditions of all of its members, the Hunt snaps and executes together.



Glossary.

- **Stag** - coordination market instance; defines target outcome, execution logic, and community eligibility.
- **Pack** - accumulation phase; intendos cluster around a Stag, aggregate state is opaque.
- **Hunt** - resolution, the pack hunts: a qualifying subset is found and execution triggers atomically; remaining intendos persist for future resolution.

Hunts can compose (through expressive intendos) - users switch platforms and LP positions migrate to the same venue; public endorsements commit and capital deploys to the endorsed cause - all in one atomic event.

--

Four properties are axiomatic for the core primitive of CMs:

i. **Coordinated Atomicity**. The commitments of the qualifiying subset - the participants whose thresholds are met together - execute simultaneously across all participants; no partial execution no gradual commit, as this would undermine the assurance.

ii. **Accumulation Opacity**. No-one - neither participants nor operators - can determine how close the initiative is to activation. The threshold crosses or it does not.

iii. **Capital Multiplexing**. Users can co-commit the same capital across different markets (eg user backing a liquidity bootstrap and a supply lock with the same 1000$); whatever commitment activates first applies. - Crucial for capital efficiency, UX scalability, and participation in overlapping markets.

iv. **Composability**. The output of one market is a valid input to another, and can compose with other shared state contracts. Coordination markets as lego blocks.

Both composability and capital multiplexing are unique to crypto rails. Traditional payment services operate behind isolated APIs, you can't lego box API calls, and you can't pre-authorize

PULL based payments ("IF THIS THEN act on my behalf and charge my account) without statically delegating your funds to the service provider.

Any mechanism satisfying these four properties can facilitate large-scale coordination between people and agents who share similar preferences but couldn't, so far, safely and practically express actionable coordination. It can compose populations with different resources and risk profiles, allow them to feed each other's assurance thresholds, and trigger downstream execution that neither population could bootstrap alone.

4. Stags in the Wild

A broad category where CMs have particular utility is escaping network effect traps. Apps that "suck but everyone's using it", or the media platform that's blatantly lying but everyone's watching it. CMs allow the public's true preference to materialize as concrete switching plans, in formal terms, it allows to aggregate demand and to alter the focality.

Example 1: Liquidity migration. Superior DeFi machinery exists but liquidity is stuck on legacy tech, 5.7B$ on BNB for instance. LPs don't move because moving alone means providing liquidity to an empty pool. Utilizing CMs, each LP can set a threshold for migrating to kaspa - 5M$, 50M, 500M - whatever they need to feel comfortable. Their capital stays productive on BNB until a subset's thresholds are met and resolved. The same capital can back multiple campaigns to exit BNB to different platforms, solana kaspa tempo. Individual intendos can double-sign conflicting intendos (!) and whatever triggers first applies.

Example 2: Content platform bootstrap. Netflix and Disney+ push woke agenda, and large segments of the user base - parents - resent it (and many others like it; see below). Sure HBO and Amazon exist, but not huge for family content. As a concerned parent you need to know the other people ranting on the internet are willing to actually act, not just complain. Entrepreneurs face the same obscurity from the other side: If I launch a streaming service with neutral or conservative agenda, how many of those ranting parents will actually subscribe. This pure coordination failure is solvable by CMs: Users can intendo-commit subscription fees to a new platform, and provided a sufficient Instmental overhead as costly, DAC renders joining the stag hunt a dominant strategy -- hence its name.

The rewards for the DAC mechanism originate from a social/political/financial entrepreneur willing to fund the fail rewards. This mechanism induces novel dynamics. Instead of capital buying attention and shaping opinion, influencing public opinion becomes costly only if you fail to shape it. The asymmetry significantly weakens the advantage of capital: a billionaire funding a fringe cause pays when the public doesn't follow, whereas a correct minority rallies the public resource-free.

--

Attention markets are designed to amplify organic propagation dynamics of some underlying social network. Ideally, we would wish for coordination initiatives to propagate spontaneously,

via group chats, community forums, DMs. Albeit whenever we enforce Opaque Accumulation (Axiom 2) we are shielding participants' intendos from their peers, which goes against organic social discoverability.

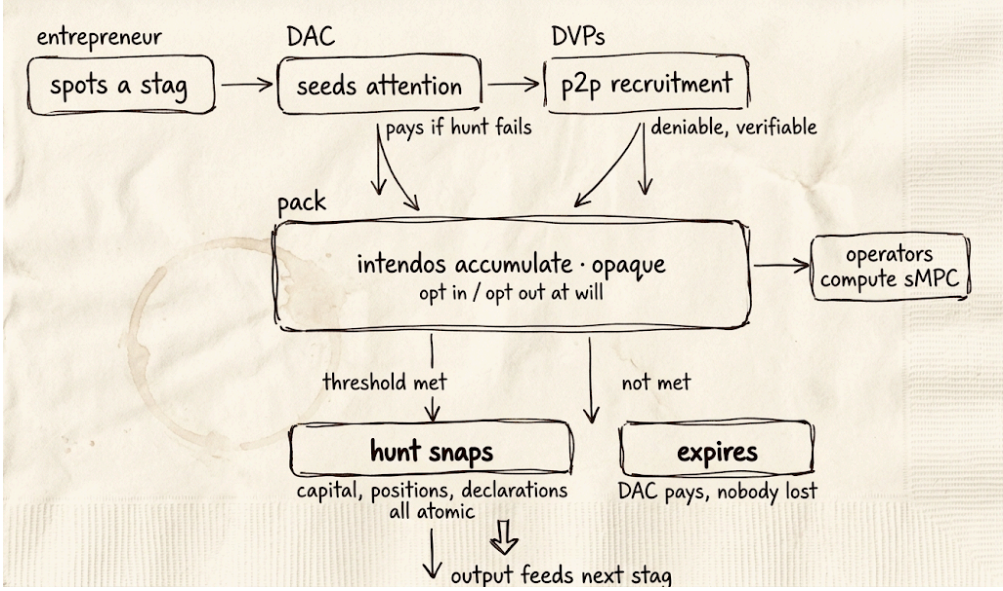
Can we preserve p2p propagation while maintaining privacy and deniability? Designated Verifiable Proofs (DVPs) to the rescue. DVPs enable off-the-record messaging: they allow a prover to convince a peer, or a set of peers (Multi-DVP / MDVS), that a certain statement is correct whilst maintaining full deniability in case the proof is leaked. In practice this looks like group chat messages that are internally verifiable yet practically unleakable. See: https://eprint.iacr.org/2019/1153.pdf.

--

Besides attention dynamics, initiators of stags should fund the continuous computation of the state of the pack. The CM stack requires a layer of operators/searchers/solvers continuously checking for subsets of intendos that can be co-satisfied. I will touch on the architecture shortly, but regardless of the details we obviously need some form of pay-for-compute. The funding for this computation can start with the stag entrepreneur -- and migrate to a fee model sustained by the pack once it reaches scale.

--

Revisiting the full lifecycle in one schematic:



Entrepreneur spots a Stag → seeds a Hunt, DAC-backed → intendos accumulate (paid if it fails) → signals propagate p2p via DVPs → Pack grows opaque → compute scans for satisfiable subset → threshold hits → Hunt snaps, atomic execution.

6. The Stack

Beyond generic support for market mechanics, the stack of coordination markets requires a few new components:

i. Intendos, the layer aggregating persistent intents of users; limited implementation of persistent intents have been implemented before, eg in CowSwap (whereas Near's intents are real-time only), but far from the flexibility required for CMs' composability and multiplexing.

ii. An efficient data structure and incremental algorithmic framework to solve Pack states, namely, "what is the current maximum subset with internally-satisfying thresholds?" Briefly, for a large set of intendos - including thresholds defined in number of participants or amount of capital - resolving the state belongs to the class of monotone fixed-point computation, which admits incremental algorithms of time complexity O(polylog) or O(1) amortized. The same properties extend to other more expressive monotone intendos, but we can't guarantee sublinear costs for the entire category; still the state is resolvable in polynomial time in the worst case. Outside this category - ie non-monotone intendos - eg ones which condition on the Pack not exceeding a certain amount - the problem becomes NP-hard in the general case. Supporting such intendos should therefore remain outside what our CM rails aspire to support.

iii. A computation fee mechanism appropriate for the algorithmic framework mentioned. This component includes both metering the cost ("computation gas") per signed intendo, as well as dictating the payment mechanism, potentially distributing it across the set. As mentioned in the previous section, the cost can potentially be absorbed by the Stag entrepreneur, especially if they wish to ensure participation is a dominant strategy.

iv. A cryptographic protocol that can support opaque accumulation of the pack. While not all use-cases require opacity, the ones that do anchor the trust in the system's neutrality and minimized pressure surface. The broad family here is secure multi-party computation (sMPC), but standard interactive sMPC is incompatible with continuous evaluation over an open permissionless validator set -- round complexity is prohibitive. The mostly-noninteractive alternative is threshold FHE (thFHE), which distributes a shared public key at the outset (DKG) and runs a lightweight sMPC for the decryption phase (ie when a maximal pack subset with satisfied thresholds is found). Still, the compute overhead is asymptotically O(poly(\lambda)) in the FHE security parameter \lambda, practically 5 or 6 orders of magnitudes (\lambda=128 bits). Feasibility requires deploying mixed-mode, hiding only essential parts of the computation. Typically, less than 5% of a program's logic needs to run in encrypted mode (aka the sensitive "leaf state"); the rest can be computed transparently without revealing useful information.

--

When discussing the actual rails - fundamentally the sequencing layer - one would typically recite the crypto liturgy: decentralized, permissionless, censorship-resistant, credibly neutral, link to purchase my governance token. This is all nice and true - these properties are the correct

new standard for open market infra. I do wish to highlight however the overlooked submetric of "time to achieve property XYZ", at what timeframes can a system guarantee XYZ.

Censorship resistance, for instance, is useful for several use cases (payments, SoV), but for many others - for financial and big market moves, timeframes of minutes are irrelevant: a system that guarantees that all financial txns will be sequenced within an hour (eg bitcoin with ~15% non-censoring hashrate) - or even within a minute and a half (ethereum for same params) - is censorship-fragile still for all things finance.

Coordination by definition leads to large market moves and cascading effects. Any gap between pack formation and execution increases the manipulation surface and multiplies pressure points. The gap lies between Axiom 1 and Axiom 2 -- a coordination threshold has been crossed but not yet sequenced. To eliminate or minimize this gap, CMs must run on infra that satisfies the hard properties we listed -- censorship resistance, permissionlessness, fairness -- in real time. I use real-time decentralization (RTD) as a codename for this metaproperty.

More details on the architecture will follow in longer versions of this doc.

7. The Consistent Individualist

In democratic ages, the bonds of human affection are extended, but relaxed (de Tocqueville).

The internet, the ultimate egalitarian project, allowed us to connect with complete anons and discover shared ideas and interests. But it did not offer ways to move together and act on common interests. It is missing an association layer which grants dynamic, ephemeral, or context-specific communities ‘write’ permissions to the shared state of the digital space.

Project Staghunt aims to build it.