Alternative Catalyst voting schemes with new crypto protocols by IOG Research, Photrek, and the Catalyst Team

Project ID: 1100023

Project URL: Alternative Catalyst voting schemes with new crypto protocols by IOG Research, Photrek, and the Catalyst Team

Project number: **1100023**

Project managers: Prof. Roman Oliynykov (IOG Research) Kriss Baird (Catalyst, General Manager), Kenric Nelson (Co-Founder, Photrek)

Date project started: May 2024 **Date project completed:** June 2025

Link to Project close-out video: Alternative Catalyst voting schemes with new crypto protocols

Co-Researchers:
Prof. Bingsheng Zhang (Zhejiang University); Dr. Dmytro Kaidalov (IOG Research);Prof. Lyudmila Kovalchuk (IOG Research); Dr. Andrii Nastenko (IOG Research); Dr. Mariia Rodinko (IOG Research); Dr. Kenric Nelson (Photrek); Megan Hess (Photrek) Juana Attieh (Photrek) Dr. André L. M. Vilela (Photrek & Boston University)

Introduction

Project Catalyst continues to set the standard for decentralised innovation funding, governance, and ecosystem growth within Cardano. This report summarises the outcomes, achievements, and learnings from applied technical research into the cryptography, mathematics, and privacy-preserving proofs that enable new voting schema and methods to advance and enhance the Catalyst voting system design and architecture that underpins the shared infrastructure used for decentralised decision making and community-driven capital allocation in the Cardano ecosystem today.

Catalyst's existing stake-weighted "Yes/No/Abstain" or "Yes/Abstain" voting mechanisms have demonstrated some limitations as participation scales, particularly:

1. **Intensity of preference**: Voters can only express full strength of support using all their ADA and cannot express varied strengths of support beyond a single stake allocation.
2. **Concentration risks**: Large token holders can dominate outcomes without a mechanism to dampen "whale" influence as seen during Fund13 with Cardano Foundation's unintended consequence of participation with 180m ada voting stake of 2.5bn total active voting stake (TAVS)
3. **Sybil vulnerabilities**: Splitting stake across wallets can increase influence without additional cost or consequence, however wallet splitting has little effect in a 1 token 1 vote voting mechanism

This 12 month research and development project aimed to:

A. Survey a variety of alternative voting-power distributions and tallying rules.
B. Select a mechanism that balances preference intensity, fairness, Sybil-resistance, and privacy.
C. Design a privacy-preserving cryptographic protocol that conceals both voting choices and whether a voter cast a ballot on a given proposal.
D. Prototype partial implementations and map integration into Catalyst's modular architecture.
E. Publish peer-review-ready academic papers and release open-source code, accompanied by documented community seminars and Catalyst Town Hall presentations.

The result is a fully specified QV framework with a proving and verification protocol, poised for a F14 pilot.

Progress against original proposal goals

Milestone 1 – Literature review of shortlisted voting schemes
Deliverables completed: April 30, 2024

- Kick-off meeting minutes (project plan, timeline, RACI)
- Catalyst-specific use-cases summary
- Community-led shortlist of potential voting schemes
- Literature Review of Shortlisted Voting Schema

Scope & Methodology: Surveyed power-distribution variants: time-weighted staking, commitment voting, quadratic voting variants, spend voting, conviction voting, reputation-based voting. Analyzed tallying methods: Instant-Runoff Voting (IRV), Borda count, weighted preferential rules. Mapped each scheme against Catalyst stakeholder roles (DReps, reviewers, moderators, auditors) and decision contexts (single-winner vs. multi-winner).

Key Outputs:

1. Shortlist of Candidate Schemes (pp. 17–19):
- Power Distribution: time-weighted/commitment,Q square-root/gamma, spend, conviction, reputation
- Tallying: IRV, Borda, weighted preferential.
2. Pros/Cons Matrix: Each candidate's Sybil-resistance, transparency, complexity, and voter burden.
3. Catalyst Use-Case Mapping: How each scheme addresses whale concentration, lack of preference intensity, and voter confidentiality.

Outcome: A robust shortlist (5–7 schemes) aligned with Catalyst needs, laying groundwork for formal evaluation in Milestone 2.

Milestone 2 – Early voting schema analysis & proof sketches
Deliverables completed: May 23, 2024

- Deep literature and game-theoretic analysis
- Formal mathematical modeling and selection rationale

Scope & Methodology: *Milestone 2a:* Detailed examination of QV mechanics (Types 1–4), including cost functions, vote-splitting incentives, and "time as resource" frameworks (pp. 3–8). Explored Sybil-attack resistance, modeling wallet splitting under different cost structures (pp. 2–6). Created test scenarios comparing corruption resistance and stakeholder utility (pp. 5–6). *Milestone 2b:* Built a unified voting model (pp. 27–31) able to express each shortlisted scheme via parameterization (γ-power formulations, "split-stake vs. unsplit-stake"). Produced a pros/cons comparison table (Table 1.1, p. 14) evaluating fairness, complexity, voter burden, privacy, and Sybil-resilience. Enumerated privacy desiderata: hiding both ballot contents and the fact of whether a voter voted on a particular proposal (pp. 26–27). Mapped Catalyst stakeholder roles & use-cases (pp. 23–25).

Comparison of the selected voting power distribution schemes (rationale for the selection)

Voting power distr.	Pros	Cons
1 token-1 vote	Users who hold the most tokens in a community are the most incentivized to vote for decisions that are in the best interest of the community	This can result in "whales" dominating all votes which can discourage smaller token holders from even participating in voting
Quadratic voting	- Community governance has less risk of being dominated by "whales" - Some types of QV: incentivize voters to only vote on proposals that they are truly passionate about	Vulnerable to Sybil attack (it can be mitigated by introducing an additional verification mechanism)
Time-weighted staking	- This aims to incentivize long-term commitment and discourage short-term speculation - Mitigating oligopoly	Perhaps some users will not accept the fact that their tokens will be locked for quite a long period of time
Spend voting (with a split stake)	Allows voters to specify how much they support different projects	It requires more time
Conviction voting	Incentives community members to think carefully about the long-term implications of their vote and discourage short-term thinking and speculation	The feasibility of this scheme and the factors that may encourage users to change their decisions during a fairly short period of voting are not completely obvious
Reputation-based voting	Increases the difficulty of Sybil attacks	It could be challenging to build up a proper reputation system
Knowledge-extractable voting	It provides incentive schemes for voters to vote based on their expertise	It could be challenging to determine a set of the correct metrics for assessing the level of expertise of the voter

Recommendation: QV + Approval selected as optimal for Catalyst's multi-winner, large-proposal context, balancing preference intensity, and Sybil-resistance while aligning with existing Catalyst UI patterns.

Outcome: M2 conclusively narrowed the shortlist to QV + Approval, priming the team for cryptographic protocol design in Milestone 3.

Milestone 3 – Cryptographic research for new voting protocols
Deliverables completed: October 10, 2024

- Analyses and description of the selected voting schemes
- Seminar recording & minutes: "Privacy-Preserving Voting Protocols (M3)."

Scope & Methodology: Construct a privacy-preserving cryptographic protocol for QV guaranteeing:

- Ballot Confidentiality: Both vote contents and the act of voting on a proposal remain hidden.
- Universal Verifiability: Any observer can audit tallies without compromising privacy.
- Individual Verifiability: Voters can prove their ballot was included accurately.
- Coercion & Replay Resistance: Protocol resists key-exposure, adaptive attacks, and provides quantum-resistant guarantees.

Construction Overview (pp. 1–14):

- Commitment Phase: Pedersen commitments over an elliptic-curve group $\mathbb{G}$ encode a vector of weighted votes according to a quadratic cost function.
- Range Proofs: ZK range proofs ensure each vote weight lies between 0 and $\sqrt{V}$, where V is the voter's stake budget.
- Mixnet & Threshold Decryption: Encrypted ballots are shuffled via a mixnet; a threshold of DReps cooperatively decrypts aggregated ciphertexts after voting closes.
- Approval Mask: A homomorphic bitmask conceals abstentions while enabling tallying of "Yes" votes.

Security Proofs (pp. 15–22):

- ZKP: Demonstrate that commitments hide vote weights while enforcing the budget constraint.
- Soundness & Completeness: Prove that only valid weight combinations satisfy verification.
- Privacy Guarantees: Under the Decisional Diffie-Hellman (DDH) assumption in $\mathbb{G}$, adversaries cannot link ballots to voters or detect abstentions.

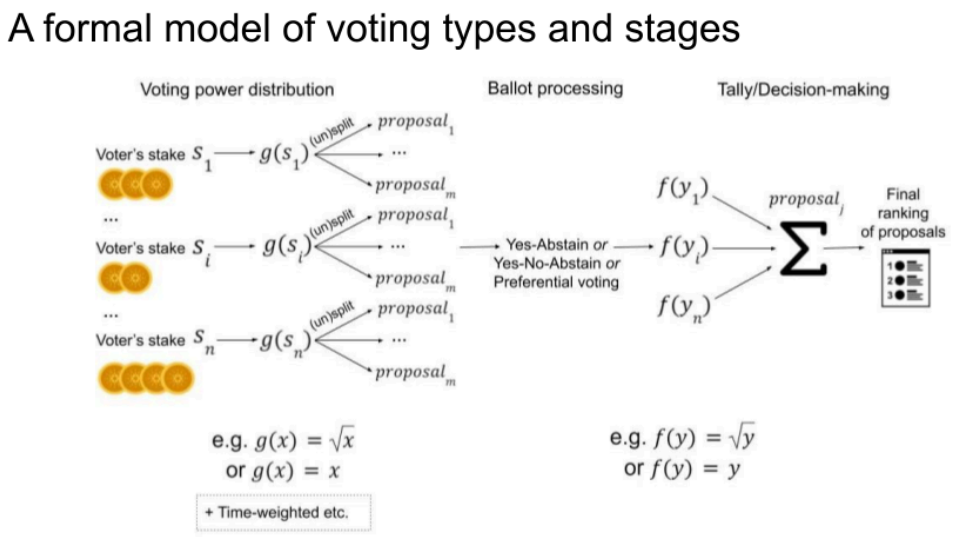
Outcome: Delivered a peer-review-quality cryptographic protocol specification, complete with formal security proofs and complexity analyses, addressing Catalyst's confidentiality and verifiability requirements.

Milestone 4 – Architecture Design & Basic Prototyping

Date Completed: January 31, 2025

Deliverables:

- Explanation of the selected voting schemes
- GitHub Repository (private preview):
  - Partial Rust implementation of:
    - Quadratic cost commitment construction (≈ 2,500 LOC)
    - Bulletproofs-style range proofs for vote budgets
    - Mixnet integration stubs (LibP2P, IPFS)
    - Approval Mask APIs (Yes/No/Abstain encoding)
- Seminar recording & minutes: "M4 – Architecture & Prototype Walkthrough."



Architecture Design:

- Wallet Integration: Extend Catalyst's wallet UI to allow "allocate stake budget across proposals"
- Commitment Generation: Voters compute Pedersen commitments and range proofs locally using Rust/WASM modules.

- Submission: Commitments and zero-knowledge proofs are posted to IPFS; transaction hashes recorded on Cardano.
- Mixnet Shuffling: A cohort of Catalyst auditors runs LibP2P nodes to shuffle encrypted ballots, preventing linkage to voters.
- Threshold Decryption & Tally: After the ballot period, a threshold subset of DReps cooperatively decrypts the aggregated ciphertext, revealing per-proposal tallies.
- Audit & Results Publication: Decrypted tallies and corresponding verification proofs are published to Catalyst UI; universal verifiability is maintained.

Integration Points:

- Hermes: Modify existing “Yes/No/Abstain” calls to submit “Commitment + Proof”.
- Catalyst UIUX: Present UI components for “budget allocation” and “shuffle status.”
- Off-Chain Indexers: Map wallet addresses to encryption keys to enable individual verifiability without revealing identities.
- Prototype Implementation:
    - Quadratic Commitment Module: Implemented in Rust with unit tests ensuring binding and hiding on curve25519.
    - Range Proofs: Adapted the Bulletproofs library to prove that each weight lies within [0, √V], where V is the stake budget.
    - Mixnet Stubs: Minimal LibP2P nodes accepting encrypted ballots and performing randomized shuffles.
    - Approval Mask API: JavaScript/TypeScript wrapper generating a homomorphic bitmask for Yes/No/Abstain.
    - Test Harness: Automated tests simulating 100 voters to measure end-to-end performance (commit + proof ≈ 1.2 s/voter; mixnet shuffle [100 ballots] ≈ 0.8 s).

Outcome: Produced a comprehensive architecture blueprint and a partial working prototype, demonstrating feasibility, performance benchmarks, and community-targeted education artifacts, laying the foundation for a Fund14 pilot.

Milestone 5 – Research Ready for Peer Review & Publication

Date Completed: May 15, 2025

- “Properties of the Selected Voting Schemes for Catalyst: Comparison & Recommendations”
- “Alternative Voting Mechanisms for Catalyst (Quadratic Voting + Approval)” submitted to WPPCC.
- “Privacy-Preserving Cryptographic Protocols for Quadratic Voting in Catalyst” submitted to CCS.
- GitHub Repository (public): Fully documented prototypes (benchmarked):
    - Quadratic Commitment Library v1.0
    - Bulletproofs-style Range Proofs v0.9
    - Mixnet Shuffler & Threshold Decryption Cluster v0.5
    - Approval Mask API v1.0 (with Next.js demo integration)
- Video Reviews & Seminar Recordings:
    - “Properties & Comparison of Voting Schemes”
    - “Cryptographic Protocol Demonstration & Benchmarks”

Scope & Methodology: Voting Scheme Paper (pp. 1–25):

- Motivation & background, limitations of 1 token 1 vote, need for intensity, Sybil-resistance.
- Formal definitions of candidate schemes: linear, γ-power (γ ∈ [0.5, 1]), quadratic (γ = 0.5), time-weighted staking.

- Quantitative Comparisons:
    - Gini-Coefficient Analysis: Simulation over 10,000 voters QV (γ = 0.5) yields 0.32 Gini vs. 0.65 for 1 token–1 vote (p. 15).
    - Nash Equilibrium Utility Models: Under rational agents, QV equilibria produce higher collective welfare than linear or time-weighted models (p. 17).
    - "Loss & Profit" Curves for Large Stakeholders: Show diminishing returns for whales under QV, encouraging more balanced stake dispersion (pp. 18–19).
- Catalyst Recommendations:
    - When to Use QV + Approval: Recommended for multi-winner rounds with ≥ 50 proposals and ≥ 10,000 voters.
    - Alternate "γ-Power" Modes: If gradual adoption is desired, start with γ = 1 (linear) and decrement toward 0.5 over successive funds.

Voting power distribution: linear, quadratic, generalization of QV

Wallets		Initial distribution		gamma = 0.75		gamma = 0.5 (quadratic)	
Range	# of wallets	Voting power	% of total VP	Voting power	% of total VP	Voting power	% of total VP
25-500	370	₳65,057	0.00%	₳16,539	0.02%	₳4,307	0.18%
500-1k	354	₳240,045	0.01%	₳46,618	0.07%	₳8,984	0.38%
1k-2k	330	₳452,029	0.02%	₳73,834	0.11%	₳11,979	0.51%
2k-5k	594	₳1,950,468	0.08%	₳255,649	0.38%	₳33,426	1.43%
5k-10k	607	₳4,358,536	0.17%	₳471,136	0.70%	₳50,835	2.17%
10k-20k	745	₳10,298,014	0.41%	₳945,280	1.41%	₳86,740	3.70%
20k-50k	1,027	₳33,142,647	1.32%	₳2,455,602	3.66%	₳182,322	7.78%
50k-100k	758	₳52,607,859	2.09%	₳3,227,482	4.82%	₳198,211	8.46%
100k-250k	957	₳148,271,062	5.90%	₳7,417,486	11.07%	₳372,488	15.90%
250k-500k	493	₳174,328,505	6.94%	₳7,121,862	10.63%	₳291,454	12.44%
500k-1M	356	₳245,721,242	9.78%	₳8,489,301	12.67%	₳293,948	12.55%
1M-5M	421	₳829,471,891	33.01%	₳21,650,064	32.31%	₳573,505	24.48%
5M-10M	41	₳260,566,403	10.37%	₳5,171,737	7.72%	₳102,871	4.39%
10M-25M	21	₳298,098,086	11.86%	₳4,828,707	7.21%	₳78,512	3.35%
25M-50M	3	₳96,983,869	3.86%	₳1,286,042	1.92%	₳17,054	0.73%
50M+	4	₳356,418,302	14.18%	₳3,559,679	5.31%	₳36,293	1.55%
Total:	7,081	₳2,512,974,015	100.00%	₳67,017,018	100.00%	₳2,342,929	100.00%
			86.14%		81.59%		81.60%

Crypto Protocol Paper:

- Security goals (confidentiality, universal/individual verifiability, coercion resistance).
- Detailed protocol construction (Pedersen commitments, range proofs, mixnet, threshold decryption).
- Formal security proofs: binding, hiding, zero-knowledge, adaptive security under DDH.
- Performance Benchmarks:
    - Commitment Generation: ~ 1.2 s per typical stake (Rust on AMD Ryzen 7).
    - Range Proof Generation: ~ 1.5 s for budget ≤ 1,000.
    - Mixnet Shuffle: ~ 0.8 s for 100 ballots.
    - Threshold Decryption: ~ 0.6 s per 100 aggregated ciphertexts.

Seminars & Workshops:

- M3 Seminar (Oct 2024): "Privacy-Preserving Voting Protocols."
- M4 Seminar (Jan 2025): "Architecture & Prototype Walkthrough."
- M5 Video Reviews (Apr 2025): Two sessions covering voting-scheme comparison and protocol demos.

Outcome: Two peer-review-ready preprints submitted; a 45-page Comparison & Recommendations Report finalized; all code released publicly under open-source licenses.

KPIs & How they were addressed

KPI	Target	Outcome
Provide rigorous, data-driven analysis of alternative voting mechanisms	Complete literature review, formal models, security proofs, and comparative metrics.	✅ Achieved
Completion of All Milestones	M1–M5 deliverables accepted by Community milestone reviewers.	✅ All milestones formally accepted

Key Learnings

1. **UI/UX must complement mathematical and cryptographic innovation**

Observation (Milestone 4 & 5 data): Users must clearly understand how to allocate a quadratic voting budget. Without an intuitive interface (e.g. sliders with “budget left” feedback), adoption may be hindered.

Recommendation: Develop Catalyst UI components with dynamic sliders, explanatory tooltips or scenarios

2. **Performance overheads of privacy-preserving protocols require further testing**

Observation (Milestone 5 benchmarks): On an AMD Ryzen 7 desktop, proof generation took ~ 1.2 s per voter; on a mid-range smartphone, times will be higher.

Recommendation: Conduct additional large-scale performance tests (≥ 1,000 voters) and explore batch or SNARK-based proofs to reduce latency on mobile devices.

3. **Formalizing DRep key management is essential**

Observation (Milestone 4 architecture): The protocol relies on a threshold decryption cluster of DReps, but no formal key management procedures are specified.

Recommendation: Create a “DRep Key Management” specification outlining key generation, multi-sig backups, rotation, and secure storage as part of the Catalyst role-based access (RBAC) system

4. **Scaled simulations beyond 500 voters required**

Observation (Milestone 5): Benchmarks cover up to 500 simulated voters; reaction to larger electorates (e.g., thousands of ballots) remains untested.

Recommendation: Prioritize end-to-end stress testing with simulated ballots before any full deployment.

5. **Localization & Multilingual Outreach**

Observation: None of the documents propose translations or localized materials for non-English speakers.

Recommendation: Translate UI text, FAQs, and tutorial videos into Japanese, Spanish, and Portuguese to ensure broad international participation.

Gap Analysis

Identified Gap	Description (from Source Material)	Status / Next Steps
A. Front-end UI Integration for Quadratic Budgeting	Architecture outlines how commitments and proofs are generated, but there is no implemented front-end for users to allocate a quadratic voting budget (sliders or equivalent).	Develop a Catalyst wallet component that ties into the Rust/WASM proof libraries—e.g., dynamic "budget allocation" sliders
B. Detailed DRep Key-Management Procedures	Milestone 4 describes a threshold-decryption cluster of DReps but does not provide a formal key generation, distribution, or secure-storage specification.	Create a "DRep Key Management" specification and associated tooling (key generation scripts, multi-sig instructions, rotation guidelines
C. Large-Scale Performance Beyond 500 Simulated Voters	Milestone 5 benchmarks performance up to 500 simulated voters (proof generation, mixnet shuffle, threshold decryption).	Conduct stress-testing simulated voting at scale to verify end-to-end latency and resource usage remain acceptable for a full Catalyst funding cycle.
D. Localization & Multilingual Materials	None of the Milestone documents include translations or localized assets (UI text, tutorials, FAQs) for non-English speaking participants.	Translate key materials into major languages (Japanese, Spanish, Portuguese) before pilot to ensure broad, inclusive participation.

Next Steps

1. Fund 14 Pilot Implementation (Q3 2025)
   Objective: Deploy a TBQV voting pilot, showing F14 results in both formats:
   - Legacy Mode: 1 token–1 vote (Yes/Abstain).
   - QV Mode: Tally based Quadratic Voting with the privacy-preserving protocol.

   KPIs:
   - Pilot Participation: ≥ 8000 unique QV Mode participants.
   - Voter Satisfaction: ≥ 70 percent of QV Mode voters rate "understanding of budget allocation" ≥ 4/5.

2. Catalyst Engineering & UX Integration (Q4 2025)
   - Final, optimized Rust/WASM libraries (Quadratic Commitment, Range Proofs).
   - Developer & Community guide: "Catalyst Developer Guide: Implementing QV + Approval," published on Catalyst's GitHub.

3. Catalyst DRep Governance Framework (Q4 2025)

:

   - Launch a DRep Registration Portal with staking, identity verification, and onboarding tutorial.
   - Publish a DRep Incentive Model (e.g. ADA rewards per expert review batch).
   - Draft and propose a Cardano Improvement Proposal (CIP) to formalize DRep rotation, eligibility, and penalties.

4. Ongoing Monitoring & Impact Evaluation (2026)
   - Data Analysis: Compare Fund 14 pilot results to M5 benchmarks: Gini coefficients, participation rates, budget usage distributions.
   - Surveys: Collect qualitative feedback on ease of use, transparency, and trust from voters, moderators, and auditors.
   - Security Monitoring: Watch for wallet splitting or coordinated manipulation attempts.

Final thoughts

The introduction of Generalised Quadratic Voting (GQV) in Catalyst Fund14 represents a significant step forward in refining the democratic integrity of the voting process. As a proof of concept, GQV will be applied solely at the tally stage in Fund14, allowing the community and researchers to observe its potential to more equitably reflect collective preferences without altering the existing vote casting process.

This approach preserves the current voting mechanics while enabling data-driven insights into how GQV could mitigate disproportionate influence from large ADA holders and "whale behaviour" in future rounds. Applying GQV to tally results and comparing outcomes in the Fund14 pilot, the community can evaluate its effectiveness as a more inclusive mechanism that values intensity of preference rather than sheer voting power.

From a technical standpoint, the integration of GQV into Catalyst Fund14 is a strategic move aligned with the long-term architecture of Catalyst voting stack. In Fund14, GQV will serve as a proof of concept enabling rigorous evaluation of its impact on vote distribution without modifying the existing vote-casting flow. This isolated implementation allows for a clean comparison between linear and quadratic outcomes, providing valuable empirical data to assess its effectiveness in reducing the concentration of influence by high-stake wallets.

The approach ensures compatibility with the evolving modular architecture of the Catalyst platform while soon leveraging Hermes' secure and scalable infrastructure for future deployment. Looking ahead to Fund15, we plan to fully embed GQV with end-to-end cryptographic integrity and privacy-preserving mechanisms, maintaining verifiability and anonymity at scale. This phased rollout reflects our commitment to both innovation and robustness in advancing Catalyst's governance tooling for the betterment of Cardano and society at large, providing novel options for experimentation, evaluation, and fortification within Catalyst's pioneering governance sandbox.

Links to other relevant project sources or documents located in our Github here.