Quadratic Voting Assessment for Echelon

Table of Contents

Summary

The central ideas behind quadratic voting emerged in a 2012 paper by Glen Weyl and Steven Lalley, in the context of a desire to address perceived weaknesses in existing democratic systems and, amongst other goals, to reduce concerns about 'the tyranny of the majority' effectively silencing minority views and voices.[1] A core argument was that giving voice to minorities would increase the range of ideas and perspectives within democratic systems, and encourage overall participation. The central method behind quadratic voting (QV) is allocating each voter an equal budget, with which votes can be purchased at exponentially increasing prices, a method giving voters the option of concentrating their votes, but at the expense of broadly weighing in on a range of issues. Despite limited adoption in traditional electoral systems, QV found an enthusiastic audience in the cryptocurrency space. Now, after several years and a number of experiments, many have noted reservations with the actual application of QV systems in the crypto space. These reservations are at least partially related to the reality that the actual implementations of QV systems in the cryptocurrency and web3 spaces generally deviate in important ways from broader theoretical approaches to QV systems.

This overview of Quadratic Voting approaches is relevant in the context of emerging questions about the most appropriate voting approaches for the Echelon community as the community grows and the Echelon ecosystem evolves. As a reminder, the earliest Echelon votes were conducted via the PRIME keys, a structure that by definition meant that only the earliest and most committed of stakeholders were voting. While the interests of this group included a healthy range of views on many subjects, there was little concern about potential nefarious interests or manipulation of the ecosystem due to the lack of transferability of voting power. In early 2023, as the PRIME token was launched and then became transferable, a wider population was able to participate in the governance process. This expansion of the voting community led to questions about whether quadratic approaches to voting were most appropriate for overall system stability and resilience, particularly given the lack of Sybil resistance as the ecosystem is currently structured. While QV approaches were retained for the 2023 Emissary Prime (EP) election, given that the presence of many early backers reduced any potential manipulation risks, conversations about the appropriateness of QV approaches have continued. Now, looking ahead to 2024's planned EP election, a systematic evaluation of QV approaches for the Echelon ecosystem is needed.

This note explores some of the context and initial thinking around issues as they relate to the Echelon ecosystem, including both theoretical and practical concerns –in particular questions about the susceptibility of Echelon's current implementation of QV voting and the potential for manipulation of 2024's planned Emissary Prime election– and outlines several directions for future research that hold promise in allowing the Echelon ecosystem to develop a novel implementation of a QV system. Modifying Echelon's existing approach to QV-based governance holds the potential of retaining much of the core appeal and promise behind QV while also potentially addressing some weaknesses common to most implementations of QV, and in doing so making the Echelon ecosystem more secure and resilient against potential manipulation attempts. Finally, improving Echelon's implementation of QV may also present to the cryptocurrency, web3, and gaming spaces an innovative example of how the challenges of

[1] Lalley and Weyl, "Quadratic Voting."

implementing effective QV approaches can be addressed in one particular context. From a practical standpoint, however, it would be prudent to develop an interim solution that can be deployed in advance of the March 2024 Emissary Prime election process.

Quadratic Voting and its Implementation within the Cryptocurrency and Web3 Spaces

As noted, the central ideas behind quadratic voting emerged in Weyl and Lalley's 2012 paper arguing that thoughtful mechanism design holds promise in addressing a number of perceived deficiencies in democratic systems. Particularly troubling for the authors were concerns about 'the tyranny of the majority' effectively silencing minority views and voices, leading to reduced engagement and participation, and ultimately weaker democratic systems. A remedy was proposed in developing a novel system allocating all voters an equal annual voting budget with which votes would be purchased according to each voter's sentiments, in a system with each successive vote increasing in price. This was imagined as a system that would encourage participation and create spaces for engaged minorities to focus on issues most important to them, while also inspiring voters to more carefully allocate their votes amongst the issues they consider the most pressing.

Despite considerable enthusiasm for the concept, quadratic voting has struggled to find acceptance in real world settings. For instance, while Colorado has experimented with quadratic voting in its state legislature, with a generally positive reception and some amount of success, there have been few examples of quadratic voting within established democratic systems.[2] This muted reception notwithstanding, the cryptocurrency and blockchain space has shown considerable interest in quadratic voting. This is perhaps unsurprising given the stated 'radical' intentions behind quadratic voting, as well as Vitalik Buterin's strong support of quadratic voting.[3]

Relative to the adoption of QV approaches within the cryptocurrency and blockchain space, it is important to note several core assumptions that underpin 'standard' or theoretical approaches to quadratic voting. Doing so also highlights key differences, several of which are significant, with the ways QV has been implemented in the crypto space. The reality, as quickly becomes clear, is that QV systems adapted within the crypto space are generally somewhat far from the broader theoretical conception of quadratic voting, in some cases with important implications.

One of these central assumptions behind theoretical QV systems is the idea of QV beginning from a neutral starting point, with each voter receiving an identical voting budget. This assumption, that individuals should receive equal vote allocations, is at the core of the principle of allowing voters to direct their voting weights to those issues most important to them. If some voters begin with larger budgets, and have the ability to spread more votes across the various issues of importance to them, they do not face the same constraints, and the fundamental concept of fairness and equal representation is immediately lost. A related assumption is how

---

[2] See, for instance, "Quadratic Voting in Colorado."
[3] See, for instance, "On Collusion," and Buterin, Hitzig, and Weyl, "Liberal Radicalism", amongst many others.

this neutral starting point effectively presupposes that individuals are uniquely identified, enabling confident assumptions that in practice all voters receive equal allocations. Finally, allocating a budget under the assumption that individuals can apportion their voting interests between available choices and opportunities implies an underlying assumption that the schedule of elections, and range of choices and candidates with which individuals will be confronted during the period for which they have a voting budget, is known, for this enables voters to make decisions about which of the issues before them are the most important.

While the above assumptions are effectively foundational for a ‘true’ QV system, the reality is that none of these reliably exist in the crypto space. For example, while QV rests upon assumptions of known identities, these are generally absent in the crypto space. This lack of verifiable identity in turn undermines, as noted, important theoretical assumptions for QV, particularly in regards to equal starting points and voting allocations for all participants. Yet, in practice QV in the crypto space almost exclusively begins from a position of each wallet being entitled to vote the tokens it possesses. This is in some cases described as being generally fair, represented as individuals having the ability to acquire tokens in proportion to their interest in a project or ecosystem’s governance, but this argument overlooks the material realities actually constraining the ability of most individuals to acquire tokens in proportion to their actual desires.[4] Further, given the well-known tendency for token holdings to skew to extremes in the crypto space, the issues are immediately apparent. Finally, given the general absence of a scheduled slate of elections with known issues or candidates in the crypto space – votes more commonly are based around the irregular nature of the submission of governance proposals from the general community – it is effectively impossible to imagine stakeholders being granted a voting budget to be apportioned across a fixed time period when an unknown number of votes might occur during that period.

The Realities of ‘Quadratic Voting’ Approaches Within the Cryptocurrency Space

In practice, what passes for QV within the crypto space – given the lack of known identities, the practice of voting the tokens one already holds, and the lack of an established set of votes or issues – is best described as what is merely ‘square root voting.’[5] In this approach, individual wallets see the entirety of their token holdings eligible to be voted in each election, with quadratic principles applied – meaning a wallet receives an effective voting power representing the square root of the tokens it holds. In this approach, a wallet holding 100 tokens receives 10 votes, for instance, while a wallet holding 25 tokens receives five votes and a wallet holding nine votes receives three votes. Importantly, while this is not a technically ‘quadratic’ system as it was first imagined, this nevertheless retains some utility in ensuring the largest token holders are not able to entirely disregard the voting preferences of smaller holders. While a wallet holding 5 million tokens will only receive 2,236 effective votes, for instance, this remains an amount that a dedicated community of smaller token holders could realistically outvote should they be sufficiently motivated. In this sense, while these voting systems as implemented in

[4] Illustrations of this view can be found, for example, in Grace, “DAO Voting Mechanisms Explained - LimeChain.”
[5] See, for example, “Rename ‘Quadratic Voting’ Vote Type as Sybil-Protection Isn’t Implemented · Issue #951 · Snapshot-Labs/Snapshot,” or “Square Root Voting.”

crypto clearly fall short of the full theoretical articulation of QV systems, they nevertheless retain a certain effectiveness in arriving at a system that is functionally a more equitable one.[6]

Significantly, however, it must also be recognized that a fundamental element of the appeal of these square root voting systems is that they are most effective in creating a more level playing field in an ecosystem of honest actors. This becomes clear when considering the example cited above of a ‘whale’ holding 5 million tokens from a particular project. For an honest whale who respects the intent of the QV approach and accepts that seeing the voting power of their holding of 5 million tokens reduced to a voting weight of 2,236 votes helps to ensure a wide range of voices contribute to the evolution of their protocol, they can easily operate within the spirit of the QV approach. The problem, however, is that for another whale who does not accept the premise of QV and splits their holdings into 50 wallets of 100,000 tokens, they would secure for themselves a voting power 15,800 votes, a significantly higher number than the honest whale, and an amount that becomes much more difficult for a community of smaller holders to overcome, even in a situation of smaller holders being largely united in their views. The reality, however, is that lacking effective identity features and Sybil resistance, it becomes virtually impossible to identify whether a series of smaller wallets belong to a single individual looking to game a system intended to equalize voting impacts, or whether this represents an uptick in participation by unique individuals holding smaller token balances.

It is also important to recognize that many of the above observations are not new. From the initial suggestions that QV systems could be useful within the crypto space it has been observed that some form of defense against Sybil attacks–where a single user controls multiple wallets, effectively a defense against the whale cited above holding 5 million tokens who intends to distribute their holdings amongst multiple wallets–has been required.[7] Yet despite the longstanding awareness of this problem, little progress has been made in finding effective solutions. To date, research on Sybil defenses has taken three primary forms, identity-based, friction-based, and challenge based. Each of these three have sought to identify effective ways of constraining any single individual's voting power to a single wallet, yet despite these efforts, no satisfactory, universally applicable solution has emerged.

That no generalized solution has emerged against the Sybil risk in the governance of pseudonymous, tokenized projects speaks to the difficulty of the challenge at hand. That said, given the importance of this challenge, a consideration of the three approaches can shed light on the nature of the difficulties, and suggest future avenues for consideration of potential solutions. Briefly, identity-based approaches attempt to link each wallet to an individual. While KYC using official documents is arguably a straightforward approach, other attempts have sought merely to establish that each wallet belongs to a unique individual.[8] Other, more crypto-native approaches to this challenge have argued for the use of decentralized identifiers

---

[6] In its commentary on this approach, Jump Crypto reached a similar conclusion about this approach, however imperfect it might be, nevertheless representing a generally positive contribution. See also “What Is Quadratic Voting and Why Don’t More Projects Use It?”
[7] See, amongst numerous others, “Quadratic Voting,” and O’Leary, “Experimental Voting Effort Aims to Break Ethereum Governance Gridlock.”
[8] For a view of how even KYC using state-issued documents is potentially problematic at scale, see “On Collusion.”

(DiDs) as potential solutions to this challenge.[9] While it has equally been proposed that protocols might modify voting weights by the degree of verification of individual identities, the seemingly promising approach has seen few actual implementations.[10] Friction-based solutions attempt to introduce measures that make a Sybil attack too costly or logistically difficult to execute, an approach likely better suited to chains or ecosystems with elevated gas or transaction costs, and unlikely to be useful for Echelon. Finally, challenge solutions have sought to develop ways for individual stakeholders to police the ecosystem. While none have emerged as definitive or foolproof approaches, this largely speaks to the nature of the challenge in establishing effective Sybil resistant methods, and not necessarily to the general effectiveness of the approach when used in the appropriate context.

While none of these approaches to establishing reliable methods of Sybil resistance have yielded concrete results to date, this effort unquestionably remains a worthy pursuit, for QV approaches, even in modified ‘square root voting’ forms, nevertheless retain considerable value, both theoretically and in practice, in establishing more equitable, and more decentralized, governance structures. That said, and as the following section exploring the quantitative elements of actual and hypothetical Echelon votes makes clear, the need for meaningful ways to limit Sybil attacks is critical, given the nature of the attack surfaces and the potential for abuse.

Voting Analysis

Developing an appreciation of the potential of quadratic voting systems to be attacked by hostile actors is a challenging but useful undertaking. Doing so provides insights into the nature of the risks, and potential economic logics attached to attack surfaces, related to QV election structures. This section explores the economic logics and range of outcomes in a simulated multi-candidate governance election that employs a structure similar to that of Echelon’s voting structures. What emerges is an image of the uncertain economic logics of attacking a governance system, with outcomes dependent upon a range of factors including the price of the governance token that must be acquired to participate in and manipulate an election, the amount of treasury assets potentially available to a successful attacker, and estimates of an attackers likely ability in liquidating the assets at a price near the pre-election price.

Review of Voting Tabulation Methodology

Votes are calculated using an adaptation of traditional QV, or what has been termed ‘square root voting,’ as noted above; in the case of the our sample election from earlier in 2023, each voter was able to vote the square root of their total tokens in favor of as many candidates as they saw fit. The impact on each candidate for which a voter places votes is not a function of the number of total candidates selected by the voter, but rather, is simply the square root of its total token holdings regardless of the number of candidates selected. The inability for voters to allocate their votes more dramatically to any single candidate is likely a constructive feature, in that it tends to make voting outcomes less volatile.

[9] See, for example, Hajjar, “Decentralized Identity Use Cases.”
[10] See Ehrsam, “Blockchain Governance.”

Voters can vote for an arbitrary number of candidates; some could select their single favorite candidate, others could select the five that they believe should be elected, and others could select the sixteen most qualified (and everything in between). Since our sample election was structured around five candidate slots to fill, the vast majority of voters selected a total of five different candidates, although some selected fewer and some selected more. Given that most voters selected five distinct candidates, it is instructive to consider that behavior as a baseline, although it should be noted that a much wider array of voting selection outcomes is possible.

Conditions Similar to that of the Actual 2023 Election

As a starting point, it is useful to consider the stability (and voting control requirements) of a situation similar to the 2023 election whereby any additional votes are assumed to have originated from wallets with holdings that are emblematic of those that actually voted. Under those assumptions, the following summary applies:

Sample Election Results

Candidate	Gross Token Votes	% of Total
Winner1	5,410,246	19.2%
Winner2	3,706,766	13.2%
Winner3	3,696,170	13.1%
Winner4	3,089,633	11.0%
Winner5	3,004,764	10.7%
Others	9,262,696	32.9%
Total Token Vote (~5x weighting)	28,170,274	
Implied Tokens Voted (if everyone votes 5 candidates)	5,634,055	
Actual Tokens Voted (some only vote one or two candidates)	6,153,512	
Voter Turnout (% of Then-Current Circ Supply)	34.7%	
Percent of Tokens Voted Needed to Control Top 5	67.1%	
Translation to Number of Tokens Needed to Control Top 5	4,130,170	
Percent of Then-Current Circulating Supply Needed to Control Top 5	23.3%	

Tokens representing 67.1% of the total that were used for voting were associated with the candidates receiving the top 5 highest number of votes. As one would expect, it would take a similar amount of tokens to displace these top 5 and replace them with hypothetical candidates that had earned no other organic votes. This 67.1% corresponds to 4.13 million tokens in the context of the 6.15 million tokens voted in aggregate.

To illustrate this, let us imagine a token, X, with similar supply dynamics to the above. Assuming a price deviation from as low as 50 cents to as high as $10 in the near term, the attack cost in this case would range from $2.07 million to $41.3 million, respectively. Adjusting these figures to account for increased circulating supply over time (28 million units as a rough proxy), and assuming similar voter turnout of 34.7%, **the attack costs scale up to $3.26 million and $65.2 million, again assuming a low and high token price of $0.50 and $10, respectively**. These attack costs should be compared to the expected attack proceeds, calculated below:

Total USD Value of Treasury	$	100,000,000
% in Native Tokens		80%
USD Value of Liquid Assets	$	20,000,000
USD Value of Native Assets	$	80,000,000
Liquidation Value Factor, Native Assets		10%
Gross Attack Proceeds	**$**	**28,000,000**

Note: It is assumed that liquidation of the ~$80 million worth of native assets held in the treasury would result in a 90% haircut, thus resulting in $8 million in proceeds. Ultimately, the liquidation value is extremely hard to predict given the amount sold vastly exceeds daily trading volumes, and since the fire sale nature of the liquidation would certainly give would-be buyers pause. The above table assumes current native token price levels and a Liquidation Value Factor of 10%. Liquidation factors act as multipliers to arrive at assumed liquidation proceeds.

Net Attack Proceed Decomposition

		Token Price							
		$ 0.50	$ 1.00	$ 2.00	$ 3.00	$ 4.00	$ 5.00	$ 7.50	$ 10.00
Gross Native Assets Accessed (USD)		13,333,333	26,666,667	53,333,333	80,000,000	106,666,667	133,333,333	200,000,000	266,666,667
Net Native Asset Value Post Liquidation (USD)	Liquidation Factor								
	25%	3,333,333	6,666,667	13,333,333	20,000,000	26,666,667	33,333,333	50,000,000	66,666,667
	22.5%	3,000,000	6,000,000	12,000,000	18,000,000	24,000,000	30,000,000	45,000,000	60,000,000
	20.0%	2,666,667	5,333,333	10,666,667	16,000,000	21,333,333	26,666,667	40,000,000	53,333,333
	17.5%	2,333,333	4,666,667	9,333,333	14,000,000	18,666,667	23,333,333	35,000,000	46,666,667
	15.0%	2,000,000	4,000,000	8,000,000	12,000,000	16,000,000	20,000,000	30,000,000	40,000,000
	12.5%	1,666,667	3,333,333	6,666,667	10,000,000	13,333,333	16,666,667	25,000,000	33,333,333
	10.0%	1,333,333	2,666,667	5,333,333	8,000,000	10,666,667	13,333,333	20,000,000	26,666,667
	7.5%	1,000,000	2,000,000	4,000,000	6,000,000	8,000,000	10,000,000	15,000,000	20,000,000
	5.0%	666,667	1,333,333	2,666,667	4,000,000	5,333,333	6,666,667	10,000,000	13,333,333
	2.5%	333,333	666,667	1,333,333	2,000,000	2,666,667	3,333,333	5,000,000	6,666,667
Non-Native Assets (Liquid, USD)		20,000,000	20,000,000	20,000,000	20,000,000	20,000,000	20,000,000	20,000,000	20,000,000
Gross Realized Attack Proceeds (USD)	Liquidation Factor								
	25%	23,333,333	26,666,667	33,333,333	40,000,000	46,666,667	53,333,333	70,000,000	86,666,667
	22.5%	23,000,000	26,000,000	32,000,000	38,000,000	44,000,000	50,000,000	65,000,000	80,000,000
	20.0%	22,666,667	25,333,333	30,666,667	36,000,000	41,333,333	46,666,667	60,000,000	73,333,333
	17.5%	22,333,333	24,666,667	29,333,333	34,000,000	38,666,667	43,333,333	55,000,000	66,666,667
	15.0%	22,000,000	24,000,000	28,000,000	32,000,000	36,000,000	40,000,000	50,000,000	60,000,000
	12.5%	21,666,667	23,333,333	26,666,667	30,000,000	33,333,333	36,666,667	45,000,000	53,333,333
	10.0%	21,333,333	22,666,667	25,333,333	28,000,000	30,666,667	33,333,333	40,000,000	46,666,667
	7.5%	21,000,000	22,000,000	24,000,000	26,000,000	28,000,000	30,000,000	35,000,000	40,000,000
	5.0%	20,666,667	21,333,333	22,666,667	24,000,000	25,333,333	26,666,667	30,000,000	33,333,333
	2.5%	20,333,333	20,666,667	21,333,333	22,000,000	22,666,667	23,333,333	25,000,000	26,666,667
Control Cost (USD)		3,259,939	6,519,878	13,039,756	19,559,633	26,079,511	32,599,389	48,899,084	65,198,778
Net Attack Proceeds (USD)	Liquidation Factor								
	25%	20,073,394	20,146,789	20,293,578	20,440,367	20,587,155	20,733,944	21,100,916	21,467,889
	22.5%	19,740,061	19,480,122	18,960,244	18,440,367	17,920,489	17,400,611	16,100,916	14,801,222
	20.0%	19,406,728	18,813,456	17,626,911	16,440,367	15,253,822	14,067,278	11,100,916	8,134,555
	17.5%	19,073,394	18,146,789	16,293,578	14,440,367	12,587,155	10,733,944	6,100,916	1,467,889
	15.0%	18,740,061	17,480,122	14,960,244	12,440,367	9,920,489	7,400,611	1,100,916	(5,198,778)
	12.5%	18,406,728	16,813,456	13,626,911	10,440,367	7,253,822	4,067,278	(3,899,084)	(11,865,445)
	10.0%	18,073,394	16,146,789	12,293,578	8,440,367	4,587,155	733,944	(8,899,084)	(18,532,111)
	7.5%	17,740,061	15,480,122	10,960,244	6,440,367	1,920,489	(2,599,389)	(13,899,084)	(25,198,778)
	5.0%	17,406,728	14,813,456	9,626,911	4,440,367	(746,178)	(5,932,722)	(18,899,084)	(31,865,445)
	2.5%	17,073,394	14,146,789	8,293,578	2,440,367	(3,412,845)	(9,266,056)	(23,899,084)	(38,532,111)

Given that the attack proceeds exceed the attack costs in all scenarios except for those demarcated in the lower right side of the above Net Attack Proceeds table, attacks should be a concern even without assuming overly strategic wallet funding processes (whereby attackers deploy thousands of wallets with ~1 token in each wallet). As one would expect, the implications become dramatically more problematic if attackers are assumed to instead deploy miniscule amounts of native assets across thousands of discrete wallets.

What this analysis suggests is that, merely on this relatively simple basis, the economic attack surface for QV voting systems is a real concern. The section below suggests several ways Echelon might consider altering or reinforcing its governance mechanisms to increase the ecosystem's resilience against such an attack.

Looking Forward

Given the theoretical and practical concerns outlined above regarding the shortcomings of standard implementations of QV within the cryptocurrency and Web3 spaces, several courses of action are potentially immediately available to the Echelon community. The first is to allocate resources to continue to explore broader, theoretical approaches to QV as it applies to the cryptocurrency space, and to supplement this research with closer study of examples of how QV has actually unfolded in practice. These efforts will support the primary goal, that of establishing for the Echelon community a sustainable long-term solution that strengthens the governance process and better secures the community's interests. While the Echelon community is of course not obligated to develop a broader theoretical contribution to the challenges of QV as applied to web3 ecosystems, it is likely that doing so will prove valuable in informing Echelon's own efforts to develop a workable solution tailored to its own circumstances. This will, in turn, represent a positive theoretical contribution to the broader space which can be expected to be broadly beneficial while also reinforcing the thoughtful and innovative nature of the Echelon community in a way that may likely prove beneficial in encouraging other groups to consider developing within the Echelon ecosystem.

Second, given that a clear weakness of QV as it has been applied in the cryptocurrency and Web3 spaces is the lack of Sybil resistance (something that was also confirmed as a risk via the voting analysis performed in this initial study, even in cases where attackers do minimal Sybil-style allocations), a particular effort should be made to consider ways that robust Sybil resistance could be effectively developed in Echelon's own ecosystem. Whether through the development of bespoke identity solutions, perhaps a solution in which identity is verified but only stored temporarily, or through the introduction of frictions that reduce the ability of the quadratic approach to be easily gamed, Echelon's structure and unique community likely lend themselves to developing unique solutions to these questions, solutions that may prove innovative across the space and ultimately helping blockchain ecosystems to grow. If these opportunities can be capitalized upon this would further strengthen both Echelon's own community and security, as well as Echelon's reputation across the larger space.

Third, Echelon may also consider a number of interim but potentially significant modifications to its current governance structures and practices. These could include establishing concrete temporal limitations on treasury spending– that would serve to reduce the attack surface for nefarious actors and make Echelon a less appealing target. Another option could be to temporarily suspend quadratic voting approaches in favor of a 'one-token, one-vote' approach that, while likely not an ideal long-term solution, could be useful while work continues to develop more effective Sybil resistant approaches to quadratic voting systems.

Finally, the Echelon community should consider these recommendations not as binary paths, but as an array of options that can be combined to develop the most effective approach to the community's concerns. These could include, for instance, temporary modifications to voting structures along with a longer-term focus on establishing a workable approach to QV approaches and a concerted effort to increase community participation in community elections, which is, as is often noted, likely the best defense against manipulative efforts by potential attackers.

Select Readings

Buterin, Vitalik, Zoë Hitzig, and E. Glen Weyl. “Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds.” SSRN Scholarly Paper. Rochester, NY, December 1, 2018. https://doi.org/10.2139/ssrn.3243656.

CoinCentral. “Quadratic Voting: Rethinking the Future of Governance,” April 21, 2019. https://coincentral.com/quadratic-voting-rethinking-the-future-of-governance/.

Cowen, Tyler. “My Thoughts on Quadratic Voting and Politics as Education.” Marginal REVOLUTION, January 3, 2015. https://marginalrevolution.com/marginalrevolution/2015/01/my-thoughts-on-quadratic-voting-and-politics-as-education.html.

Daubenschütz, Tim, and Tim Daubenschütz. “The User Experience Problems Of Quadratic Voting.” Tim’s website, March 27, 2022. https://timdaub.github.io/2022/03/27/the-user-experience-problems-of-quadratic-voting/index.html.

Ehrsam, Fred. “Blockchain Governance: Programming Our Future.” *Medium* (blog), November 29, 2017. https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74.

GitHub. “Rename ‘Quadratic Voting’ Vote Type as Sybil-Protection Isn’t Implemented · Issue #951 · Snapshot-Labs/Snapshot.” Accessed November 1, 2023. https://github.com/snapshot-labs/snapshot/issues/951.

Hajjar, Alamira Jouman. “Decentralized Identity Use Cases: DIDs For Sybil-Resistant Quadratic Voting.” *Fractal ID* (blog), October 31, 2023. https://medium.com/frctls/decentralized-identity-use-cases-dids-for-Sybil-resistant-quadratic-voting-13970ab3ba50.

Jump Crypto. “Square Root Voting,” January 28, 2022. https://jumpcrypto.com/writing/square-root-voting/.

Lalley, Steven P., and E. Glen Weyl. “Quadratic Voting: How Mechanism Design Can Radicalize Democracy.” *AEA Papers and Proceedings* 108 (May 1, 2018): 33–37. https://doi.org/10.1257/pandp.20181002.

O’Leary, Rachel-Rose. “Experimental Voting Effort Aims to Break Ethereum Governance Gridlock,” May 23, 2018. https://www.coindesk.com/markets/2018/05/23/experimental-voting-effort-aims-to-break-ethereum-governance-gridlock/.

“On Collusion.” Accessed October 31, 2023. https://vitalik.ca/general/2019/04/03/collusion.html.

Posner, Eric, and Glen Weyl. *Radical Markets*. Princeton University Press, 2018.

RadicalxChange. “Quadratic Voting in Colorado: 2020,” January 4, 2021. https://www.radicalxchange.org/media/blog/quadratic-voting-in-colorado-2020/.

RadicalxChange. “QV Polling Method Gains Steam in Colorado State Legislature,” May 24, 2021. https://www.radicalxchange.org/media/blog/qv-polling-method-gains-steam-in-colorado-state-legislature/.

Siddarth, Divya, Sergey Ivliev, Santiago Siri, and Paula Berman. “Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-Resistance in Proof of Personhood Protocols.” arXiv, October 13, 2020. http://arxiv.org/abs/2008.05300.

Vanderbilt Law Review. “Voting Squared: Quadratic Voting in Democratic Politics,” March 19, 2015.

“Voting Types.” Accessed November 1, 2023. https://docs.snapshot.org/user-guides/proposals/voting-types.