Ruprecht-Karls-Universität Heidelberg
Alfred-Weber-Institut für Wirtschaftswissenschaften
M.Sc. Economics

Scaling of Quadratic Voting: Challenges and Opportunities

Cornelius Gaal

Seminar: Blockchain Economics and Radical Markets

Lecturer: Dr. Stefano Balietti

Date of Submission: 31.07.2021

Introduction

Societies use elections to decide on policies, appoint their leaders and to introduce new laws[1]. Since as of 2015, all members of the European Union as well as most other countries in the western world are by constitution some sort of representative democracies, it's really hard for most of us to think about any other kind of legislation. The underlying voting systems for those democracies are in all cases some type of majority voting, where each person is allowed to cast one vote per election or topic. Even though citizens of democracies are, on average, richer, healthier and more well educated than their counterparts in nondemocracies[2], democracies are experiencing a disconnect between the citizens and the government. Between 1987 and 2014 the share of people that reported voting as their civil duty in the UK dropped from 76% to 57%, as well as the percentage that believed that "the government places the needs of the nation above the interests of their own party" more than halved in the same time period. Surprisingly the interest in politics didn't decline at the same time, about two-thirds of the population declared that they follow the politics on a daily basis, as well as one third reported that they have "quite a lot" or "a great deal" of interest, which hasn't changed much since 1986[3]. A major flaw in our voting system is that the intensities of preferences are ignored, which leads minorities to turn their back on voting in elections because of the minimal impact they expect their vote to have on the outcome.

This research paper takes a closer look on another possible voting mechanism, the so called Quadratic Voting (QV), a voting system proposed in 2015 by Eric Posner and Glenn Weyl, where one can indicate the intensity of preferences instead of just being able to cast a single vote. This voting system faces, already by its underlying mechanism, great challenges in its application for larger audiences and has not been tried with audiences even closely resembling a whole nation or even a medium sized district. The paper will further give a quick overview about where QV is applied best and will then discuss solutions for a few of those challenges, namely the initial setup of the whole voting process, different types of methods to prevent collusion and about a possible vote-incentivizing mechanism to provide a very general approach to the scaling of QV.

[1] cf. Faliszewski, 2006, 641.
[2] cf. Rosner, 2012.
[3] cf. Ormston, R. and Curtice, J., 2015, 122.

Quadratic Voting and its current use

In their book “Radical Markets” Eric Posner and Glenn Weyl make the point that the key problem of our current voting system, the so called one-person-one-vote system, which is in use in most of the western democracies nowadays, lies in the scarceness of different preferences that can be indicated; yes, no and indifferent. They argue that opinions about topics cannot be seen in such a one-dimensional way but have to be viewed with respect to the intensity of the different opinions. The main problem arises as soon as the majority doesn’t care about a certain topic or is slightly leaning towards one site, because then they are able to neglect the preference of the minority, no matter how intense it is. This might lead to an inefficient -or better- not welfare optimizing outcome of the election. This flaw in the majority voting system is known as the “tyranny of the majority” and has already been covered in scientific papers and books alike. Posner and Weyl introduce QV to address both this and the welfare-inefficiency problem.

The setup for QV they propose is quite simple. Every participant gets the same amount of so-called voice-credits, which they can use to vote for or against different topics. They are allowed to cast as many votes as they want, but the amount of voice credits they pay for each consecutive vote on one topic increases quadratically. If the marginal cost of casting x votes is m, casting 2x votes will lead to a marginal cost of 2m+1 voting credits. Posner and Weyl argue that a rational voter will vote as many times for a certain topic until their marginal cost equals the marginal utility they gain from an additional vote. By this setup it marginally costs twice as much voice credits to vote for a topic four times than to vote twice for it, and so on. A voter who values a topic twice as much as another will thus buy twice as many votes as the other person will. The robustness of this mechanism has been shown under different conditions as well as the efficiency, which is under most circumstances at least as good as under the one-person-one-vote system.[4]

Number of Votes cast on one topic	Cost in Voice-credits	Marginal Cost
1	1	1
2	4	3
3	9	5
4	16	7
5	25	9
6	36	11

Table 1: (Marginal) cost in voice-credits per votes cast on one topic

[4] cf. Weyl, 2016, 2.

This method of voting can be seen as a compromise between the free rider (which describes people that are not paying for a certain good / are not participating in a vote, but still receive benefits from the good / the outcome of the vote) and the tyranny of the majority problems. Even though they admit that the outcome of votings that are run via QV are only an approximation of the welfare-maximization we talked before, the setup would lead to the optimal outcome under the same conditions as under perfect competition in a market economy.

Currently the application of QV in a real-world setting is mainly restricted to surveys, but in the last few years there have been first trials of the method in various political settings. Among the best known is Colorado's experiment in Spring 2019, where the Democratic Caucus of the Colorado State House of Representatives used QV to prioritize spending bills out of several ones that would have exceeded their budget. The prior employment of traditional methods of prioritization didn't lead to any clear conclusions, which made the Caucus members agree to try QV. According to own statement the trial resulted in a clear prioritization of the budget bills and thus gave the Caucus leaders a better understanding of what the group of senators supported[5]. The second well-known application of the method was during the convention of a pan-European party called Volt in Germany in 2019, where participants were able to choose the agenda for their next convention through QV. The application was done using blockchain technology to which we will get back later. In both examples the number of participants was between 80 and 150, way below the numbers necessary to run e.g., a district wide voting.

Quadratic Voting and arising Problems: A Framework

The framework of QV is not suited for every kind of election process. If we think about an election with only two options, let it be "yes" or "no", we will get the same results for QV and majority voting assuming rational voters. In other words, the optimal setup in which we can use our new mechanism efficiently has to be more dimensional. Particularly we have the option of an election between multiple subjects on which we can weight our voice credits on or a set of "agree" or "disagree" questions. The main difference for those two settings lies in the time dimension, whilst we have to have the first type of question given out and answered at the same time, we would be able to poll for the "agree" or "disagree" questions over a longer period of time. The second case is the more interesting one in the sense of a more direct democracy approach where topics would be discussed and voted for as soon as they come up but requires an underlying storage and spending mechanism for the voice-credits of all participants. For both cases a digital solution would be recommended, since the setup for wide-scaled QV might be very costly considering the amount of voice-credits and logistics that have to be considered.

[5] cf. https://www.radicalxchange.org/media/blog/quadratic-voting-in-colorado-2020/

For the following chapters we will work in a QV setting, in which the participants reveal their preferences on different “agree” or “disagree” questions over a longer period via a digital way of voting. Additionally, we assume the number of participants as too high to have an analogue application of QV as an efficient alternative.

This digital solution instantly raises questions about the principles of democratic voting, especially about the privacy of the turned in votes. One can argue, that as long as QV is only used for the prioritization of budget bills or the importance of addressing topics, privacy issues can be ignored to a certain degree. Nevertheless, in cases like the example that was given by Posner and Weyl in their book to introduce QV, where people had to decide about gun laws or other possible topics where some people might be very passionate about, it is crucial to protect the privacy of voters to at least the same degree as in conventional elections. A possible way to address this issue is the usage of so-called privacy coins on a blockchain, which this paper will go into more depth in the next chapter.

A main difference of QV to traditional voting is the need for an assignment and storage system for the voice-credits. Especially in the case of having multiple votes during a longer period of time it is crucial to have a cost-optimized and secure way of sending out, storing as well as using the voice-credits. There has been some research on the possibility to implement QV in an analogue way by using vote-tokens that could be used to purchase wax chunks, which were then used to vote for the preferred option, which was actually found to be a robust way to adopt QV[6], but the logistics behind a wide-scaled election were neglected in the setting and are assumably connected to high costs and planning. Until now, all of the applications of QV happened in a digital setting, which makes the assignment and storage process cheaper, but introduces QV to new threats like privacy issues as well as the possibility of coercion.

After the initial setup of the process and especially in a digital way of voting it is important to find mechanisms to disincentivize people from colluding. In the currently prevalent one-person-one-vote system the most obvious ways to influence elections are falsifying existent votes or vote buying in the sense of actual vote buying as well as influencing the public opinion on certain topics or candidates. Given that we’ve chosen to run our election in an optimal digital setting we still need to find a way to rule out the possibility of falsifying existent votes. In this setup, just as in the one-person-one-vote system it will be hard to detect cases of vote buying, but there are certain ways to detect participants colluding in a digital setup.

[6] cf. Park, 2017, 7.

Blockchain Voting as a General Solution for Quadratic Voting

In the following chapter digital voting, or more precisely voting by utilizing a blockchain will be presented as a possible solution for the aforementioned challenges and reviewed critically, whilst keeping an eye on the comparison with the traditional one-person-one-voting method.

As mentioned in the introduction the organizers of the voting at the Volt-convention a group called "*Deora*" ran their QV on a blockchain. They reported that most of the participants were first-time users of QV and even new to transaction on a blockchain[7], which makes their case even more interesting in a sense of a possible wide-scaled setup. They gave out QR-Codes to all participants which they could use to access their wallet with voice-credits inside an app. While the participants were choosing their preferences and submitting their votes a balance card which can be seen as non-fungible Token (NFT), kept track on how many votes were subjected to a certain topic and adapted the price for additional votes accordingly. Additionally, this system allowed people to retract their votes after they were submitted to regain the spent voice-credits with the amount of those being tracked on the balance card.

As we've seen in this case it was very possible to setup a system that allowed people to cast their votes on a blockchain with an expense not much higher than it would've been in real-world setting. Even an arbitrary upscaling of the participants would not lift the marginal expenditures over the ones in a majority voting setting, given we choose to give out a random QR-Code or Key to everyone who is eligible to participate in our voting.

Privacy and Technology Mistrust

In the light of privacy issues, which weren't really addressed by "Deora", simply because there was no need for it, it's important to have a look at the key points of criticism against blockchain voting or digital voting in general. A valid critique that can be made is that blockchain technology itself does not provide the right (trust-) properties we are used to have and need to have for an election. Furthermore, the general mistrust in technology must be addressed, as the general perception about technology is that there can and always will be unidentified bugs, which might open backdoors for ill-meaning individuals or just cause the system to not work as designed.

In order to use a blockchain software for voting there are a few properties that it has to fulfil; correct execution of inputs, censorship resistance, privacy and coercion resistance[8]. While the first two properties are given in any working blockchain setup, most of the wide-used

[7] cf. "Quadratic Voting with Deora and Volt Party" w/ S. Weniger, J. Barbie & M. Kuck (RxC Berlin 2019)
[8] cf. Buterin, 2021.

blockchains do not satisfy the privacy conditions that are needed for an election and do not even try to be resistant to coercion.

Nevertheless, there are different options to guarantee privacy. As mentioned before there is the option to work with privacy coins which most of the time make use of the so called “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge” (zk-SNARK). Generally speaking, this type of proof allows one party (the prover) to prove to another entity (the validator) that a made statement is true, without revealing any information about the content of the statement. Additionally, those proofs can, in difference to their predecessors, be verified in very short amounts of time, as well as being proven valid by a single message from the prover to the validator and thus wipes out the need of possibly (time) costly interactions between the entities[9]. To have this technology to work in a voting setting, there has to be a server or optimally several servers to ensure integrity that check for incoming votes, decrypt them and generate a proof for validation which they then give out for everyone to see. Through this mechanism of Zero-Knowledge the correct counting of votes can be guaranteed without having the need of an actual observer counting the votes, but instead having a server do the computing, counting and taking care of the validation process. The second issue that was mentioned before, the requirement of coercion resistance is tackled through the use of multiple server entities ensuring that one server would not be able to falsify votes and therefore the general outcome. This system both works for a majority voting system, as well as for a QV setup.

The next issue that must be considered is the general mistrust in technology, that has to be addressed before being able to convince a majority of people to switch from an analogue way of voting to a digital one. In the last few years there were a lot of high-profile attacks on the data of customers of several big firms, like Canva in 2019 with over 130 Million affected accounts, Zynga in 2019 with over 200 million accounts and Sina Weibo in 2020 with over 500 Million affected accounts [10]. While cyber-security professionals like Gary Golomb, Co-Founder and Chief Research Officer of Awake Security argue, that Cybersecurity is getting better and more effective over the years and that those big breaches mainly show our dependence on the internet and its different applications[11], others could still argue that in the case of implementation of QV on the blockchain not the big firm’s server would be the target of a possible cyber-attack, but the private phones and computers of the participants would be. Tech-giants like HTC or Samsung already started producing so called “blockchain phones” which separate high-security demanding applications from other applications by letting them

[9] cf. https://z.cash/technology/zksnarks/
[10] cf. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
[11] cf. https://www.infosecurity-magazine.com/opinions/cybersecurity-getting-better-worse/

run on a security focused operating system on a trusted hardware chip[12]. But even though those types of security enforcements already exist, it will take time to have this as a standard and freely available to everyone and even then, there will always be security weak points that might be exploited by some for their personal interest. Since this problem is more of a problem for all types of digital processes with a meaningful influence, we can turn away from it for now and focus more on the QV-specific problems the setup will face.

Storage and Assignment of Voice-Credits

Given that the issues around blockchain voting can be put aside, the whole assignment and storage system still needs to be figured out. The solution "*Deora"* chose in their trial at the Volt convention offers a very easily scalable approach to the subject. Sending out QR-Codes by mail to everyone eligible to participate in the election is measured by its cost and effort dimensions not too different than sending out the documents necessary for absentee voting. If the infrastructure for this wasn't laid out before 2020, it certainly had to be improved during the corona pandemic in most parts of the western world, where it wasn't possible or at least not recommended to vote in person without running at risk to contract the virus. For example, in the U.S. the pandemic circumstances led to an unprecedented interest in voting by mail in the 2020 presidential election[13]. But QV, in comparison to the one-person-one-vote system requires an additional application that this QR-Code refers to, which optimally is equipped with an intuitive user-display as well as already the preloaded amount of voice-credits every participant has to their disposal. A key part of this application has to be that every user must verify themselves when first opening the app and are restricted to one account in their lifetime. There are different possibilities to do so and some are already practiced nowadays, for example the identification process when setting up a new bank account.

With a system like this the issue of QR-Code or phone loss arises as well as participants that become eligible to vote in a phase of the voting where the codes have already been sent out and some votes possibly have already been missed. Both problems can be addressed by choosing an interval of sending out new, preloaded wallets, short enough to not drop out of the election circle to miss too many votings but not too short to increase the costs of sending out the codes significantly. Those wallets and QR-codes could possibly work in a way that every half a year new codes with a predetermined amount of voice-credits are sent out, that can be scanned and redeemed upon an existing account to increase the stored credits or for new voters, to open up a new account to participate in the upcoming elections. There may be other

[12] cf. https://www.technologyreview.com/2019/02/28/66000/what-the-hell-is-a-blockchain-phoneand-do-i-need-one/

[13] cf. Yoder, 2020, 2.

ways to constantly upload voice-credits to all existing wallets, probably even paper-less ones, but for the sake of simplicity this paper won't go into detail with those.

This finalizes our general setup, which would be able to produce efficient election outcomes under the assumption of having no maliciously acting participants involved in the voting process as well as all participants being perfectly rational agents.

The Problem of Collusion and Coercion

The focus is now shifted from the technical prerequisites to mechanisms that need to be put in place to control for people either acting malicious or not rational and how to adopt them in a blockchain setting.

The possibility for people to collude has to be taken very serious in a voting setting where the marginal costs for a vote change depending on the number of votes already casted. It has already been recorded at different occasions where the mechanism of Quadratic Funding (QF) was used to support different projects, that this problem actually poses a threat. QF is in its underlying setup very closely related to QV. QF can be described as a democratic and scalable form of matching funding for public goods, where matching funds are optimized by prioritizing projects more on the number of people contributing than on the amount they contributed. Important to understand for the following is, that a project that receives 1$ each from 3 persons will be funded with more money than a project that received 3$ from one person. This results from the setup of QF, where organic donations are matched by an amount that is proportional to the square of the sum of the square roots of the contributions a single project receives[14]. This type of funding has been run several times through a platform called "Gitcoin Grants", where different donors set up a fund to match incoming donations for several public good projects, and then had everyone donate to their favourite projects, so that they received the donations as well as the matchings coming from the fund. Already by default we see that participants are incentivized to split their donations over as many persons as possible to gain maximal value out of the matching process. In our previous example this would mean, that the person that donates 3$ to their designated project would be in total better off to pay someone 2$ of his 3$, so that the other person donates 1$ to the project and keeps 1$ to themselves (of course depending on the amount of money in the matching fund)[15]. Since it's very easy to see why people are encouraged to collude with each other, it's as easy to see why there need to be rules and/or mechanisms in place preventing participants from colluding and even going so far to actually penalize them if they are caught.

[14] cf. https://finematics.com/quadratic-funding-explained/
[15] cf. https://wtfisqf.com/

Before looking into possible solutions, just a quick example to underline why QV actually faces the same problem as QF. Assuming there are two people, where one is really invested in topic A and doesn't care about topic B and the other one exactly vice-versa. Let's roll with an example where both participants have 36 voice-credits at their disposal. The non-colluding outcome would be that both person 1 and 2 spend their voice-credits on topic A or B respectively and both topics receive a total of 6 votes. Now if A and B collude and make a deal that they both will only buy 5 votes for their preferred topic, which ramps up at a cost for 25 voice-credits each, and spend 9 (3 votes) of the remaining 11 credits on the topic the other person cares about, both topics will end up with a total of 8 votes and both persons would still have 2 credits left in their accounts. This obviously violates the idea behind QV, where it is assumed that everyone casts as many votes until marginal utility of another vote equals marginal cost of the next vote and therefore is a problem for the integrity of the whole mechanism. In a setting where vote-credits were actually bought and not assigned, it was concluded, that if the collusion is reasonably anticipated by the rest of the participants and reasonably small in size, they will not be able to make the outcome differ significantly from the efficient one[16].

In our setting, where everyone is endowed with voice-credits we still need to make sure that participants are disincentivized from colluding. A few approaches of "Gitcoin" might be translated into the QV-environment, namely the adoption of a mechanism that is able to detect if larger groups are showing similar voting behaviour and flagging them for further investigation. The way they aimed to prevent people from colluding in the QF setting included discounting the amount of money donated if the donors showed to have similar donating behaviour. This approach has been criticized by a lot of people, since subgroups tend to support each other and thus display comparable donating behaviours[17]. Translating this straight away into QV might raise new problems, because firstly mechanisms like this have to be built into the servers that were introduced in an earlier chapter and thus are not able to be observed and secondly penalizing a person by reducing their influence without being absolutely sure if the person really did try to collude with others or had other reasons for their behaviour cannot be done light-heartedly. Since this way of disincentivizing people from colluding has obvious flaws and can be very easy argued against, the mechanism needs to be made suitable for a QV setting.

A possible solution is to source out the actual decision whether people are colluding from the server and to deal with the issue via the traditional way through a court-system. This would mean that the servers are still checking for entities colluding but aren't discounting their votes on their own. Depending on the severity of the case traditional punishments, like paying fines

[16] cf. Weyl, 2016, 10.
[17] cf. https://gitcoin.co/blog/how-to-attack-and-defend-quadratic-funding/

or being sentenced to prison might be appropriate, but the setup of the QV that is inspected actually allows for another form of punishment, that is the slashing of voice credits, which can be compared to the often-used method of stake slashing, which is mostly used to penalize people for inactivity, dishonest validations and any other malicious behaviour in the blockchain environment[18]. To adapt this into the QV framework, there are two viable alternatives; firstly the possibility to build the app that manages the assignment and storage system in a way that allows legal bodies to decrease the voice credits a person has to their disposal or secondly to exclude persons who were found guilty of collusion from receiving their "recharge" letters for a determined time period. The first option has to be viewed very critically since it runs contrary to the whole point of making a voting secure if certain people have access to the voice credit wallets of everyone. The second option strays a little further from the initial idea of stake slashing, since it denies the colluders the possibility to influence upcoming elections to the potential, they would have had without acting malicious, so it acts more like a long-run penalty than an actual present punishment. This approach suits the long run setting the framework is aiming for, since collusion in our setting can only happen when it's involving more than one vote, so there has been a time dimension to the collusion itself. Nevertheless, this option poses a viable middle path between having secure digital votings and disincentivizing people from acting in an undesired way. Anyhow it has to be carefully determined how people actually react to the delay of the possible punishment to actually ensure the efficiency of this mechanism.

The problem of coercion can be ruled out to a certain degree in a blockchain-voting environment, since some setups allow people to withdraw and recast their votes. Coercion in an election setting describes the activity of some entities that force others to vote in a desired way, let it be through threatening them or by buying their votes. If our setup allows the withdrawal and recasting of votes the adversary has no cost-efficient possibility to check if the influenced participants act in the desired way. Both described methods rely on the possibility for the maliciously acting entity to be able to find out if the influenced voters actually followed their instructions[19]. This possibility can be taken away from them by giving participants a large enough time window to vote and to recast their votes as well as allowing them to change their votes without any repercussions. By taking this possibility from the adversary we impede wide-scaled coercion, since the influencer can never be sure that the "victim" did not change their vote after being forced to vote in a certain way. This can be easily implemented into a blockchain environment as shown by the example of "*Deora*", where the participants were allowed to recast their votes thus simply overwriting the previously cast ones. Therefore, our setup for QV offers a very intuitive and easy way to prevent coercion.

[18] cf. https://novuminsights.com/post/slashing-penalties-the-long-term-evolution-of-proof-of-stake-pos/
[19] cf. Kempka, 2014, V.

Incentivization for people to vote

Similar to the one-person-one-vote system, the QV setup is facing the problem of people deciding not to vote. There are two main reasons for people to refrain from participation in a voting, first assuming their vote is not pivotal in an election and second not caring about the topic the vote is about. There has been a lot of research done about why people are actually participating in elections even though the chance of them being pivotal for an outcome goes to zero and a lot conclude that the voting behaviour of humans is mostly irrational in the sense of their engagement[20]. The second reason is levied by the storage mechanism we have introduced earlier, since it will induce people to be even more hesitant with the spending of their vote-credits on topics they do not care that much or not at all about. It is important to find a way to work around this issue because otherwise the outcome of multiple votings would be dependent on the other topics that are being voted on around the same time.

Before going more into detail with the QV specific problem, it is important to understand why having a low percentage voter turnout is a problem and to look at solutions that the one-person-one-vote system has already produced, since it faces this same general problem as QV. People not voting are a problem as soon as the people that aren't voting are not chosen at random, but have share similar characteristics like income, age or ethnicity[21]. A very intuitive solution to get people to participate in every vote they are eligible to, is to make voting mandatory. There haven't been many countries trying this approach, because forcing citizens to vote can be seen as an in intrusion into the freedom of choice most democratic countries are guaranteeing their citizens. Albeit this criticism Australia adopted this mechanism in the early 20th century and is fining citizens if they choose to not participate in elections they are eligible to vote in without a reason. This led to an increase in participation of around 24% and the public policies resulting from those elections were described as being more in line with the preferences of the citizens than before the compulsory voting[22].

Having the possibility to fine people inside of the voting mechanism as described in the last chapter, might actually be a more harmonic and not too costly way of implementing compulsory voting into our QV framework. We have already talked about pausing the bi-annual sending of the QR codes to participants who acted in an improper way. To adapt this to fit into a compulsory voting system it is possible to reduce the amount of voice credits someone receives in the next period for exactly one voice-credit per missed voting. Since this equals exactly the cost of one vote, the person would, by rational choice theory, disregarding transportation and opportunity costs, be indifferent between not voting on one topic and voting with one vote for the side they prefer. This would incentivize people that are only marginally

[20] cf. Brennan, 1998, 149f.
[21] cf. Fowler, 2013, 161.
[22] cf. Fowler, 2013, 180.

preferring one side over the other to vote and would therefore increase the voter turnout, which can generally be considered as a desired effect, because of its impact on the optimality of the outcome of the vote[23]. In our case this can be done, by letting the servers check each period how often a certain entity did cast a vote in the given time period, and then reduce the balance on the next recharge-QR-Code by the amount of missed elections. There are other possible ways to implement voting-incentivization in a QV setting, especially in the case where voice-credits are bought and not endowed to everyone, but the presented mechanism suits best to the given framework.

A very specific problem: Retroactive Tampering with model rules

This general setup faces a problem in the specific case, when an elected official grants amnesty to people that verifiably misbehaved in his own election to his advantage. Before being able to find a solution it is important to understand the different approaches the illegitimately elected official can take in the QV setup.

The general environment of the blockchain-based voting is the most obvious attacking point; it is very important for the integrity of any blockchain-based voting mechanism to have the blockchain run on different independent servers, so that no entity has the possibility to actively change the information that is being transmitted over the blockchain. Real-World examples like the Russian blockchain-powered voting, which was already rolled out in recent trials, further increase the importance of this aspect. Many people criticise this specific program as it appears to the public as a way to prevent fraud in elections, while in reality it actually allows officials to govern without democratic traditions, simply by the fact that the whole blockchain setup does not run on independent servers, but on standard corporate distributed networks[24], that can be controlled by the government. This would allow the people with access to most of the servers to not only change the rules, like granting amnesty, but to even change the outcome of the votings. As mentioned in the chapter about blockchain-voting it is vital for our setup to be decentralized and independent to prevent the government from influencing elections in this way.

The second approach an official with malicious intentions can take, is much more specific for our QV setting. In our example with the periodical reimbursements of voice-credits, which can be reduced or suspended after verified misbehaviour, it is crucial to provide the model with a mechanism that does not allow any person or group to influence this process. If the government had any influence on the assignment of the voice-credits, there is no way to

[23] cf. Fowler, 2013, 160.
[24] cf. Alper, 2020.

prevent them from just ignoring penalties or in an even worse case, assigning the credits in a way that is favourable to them.

There are a few ways to secure the system against this kind of attack, but just as it is for all democratic voting mechanisms its only possible to a certain degree. A very efficient but probably costly method would be to set up an initial mechanism, that includes and controls all aspects of the QV process, that is the assignment and storage, the reimbursements, the penalties, as well as the public announcement of winners and of the potential occurrence of manipulations but does not allow for any kind of change. This would make the whole setup rigid and vulnerable to a changing environment where it might be important to adapt to certain events. On the other hand, this setup would defy any accusations of fraud since there is no way to tamper with anything system-related after the initial launch, but to delete the system and set up a new one, which can not be done without attracting attention.

A possible “outside” solution would be to protect the penalties for voter-fraud by constitutional law to prevent single entities from being able to grant amnesty in those cases. Even though this might be a viable possibility after the QV has been tested and been found acceptable as the main voting mechanism, this is the utmost point our setup can go to protect its integrity, because both blockchain voting as well as QV are not designed to work under dictatorship and face the same problem as all democratic voting mechanisms in the light of a single entity or group trying to take control over the system.

Selection and Sequence of Topics to vote on

In the traditional voting system, most elections can be seen as stand-alone votings, with -in theory- zero impact on other votings. In the presented setting QV faces the issue of the interdependence between the votes for the topics that are voted for. If voting for two topics that a lot of people have very strong feelings about are taking place at short intervals, participants are forced to decide which topic is more important to them, which might alter the outcome of the election in comparison to a scenario where a longer time interval between the particular votings elapsed. Therefore, it is important to find a way to decide on the topics that should be voted for and preferably publish some sort of voting schedule as far ahead of the elections as possible. This alone already goes against the target of a direct as possible democracy, in which -in a perfect scenario- people are able to vote on topics as soon as they come up. QV in our setting is not suited for a perfect direct democracy because of the issue mentioned above. In the real-world applications that already took place in a more serious setting, the topics that were voted for were predetermined by a certain person or group. An additional problem arises as soon as these entities have an agenda they are pushing for and start to manipulate or set up the voting topics in a way favourable to them. This shows that a profound mechanism of deciding on topics to vote on must be put in place to prevent the general outcomes of votings

from depending on the alternative votings that happen around the same time period. Finding a way to solve this problem might be one of the hardest ones to figure out, since it is closely related to individual thinking and has probably no one-fits-all solution and the adoption of blockchain voting might not even play any part in it at all. Nevertheless, it is a very important topic for further research, since without some sort of protection against this type of manipulation, the whole integrity of QV in general is threatened.

Conclusion

Quadratic voting offers a truly new opportunity to remodel the quite rigid democratic system, we all have accustomed to. In theory QV achieves the ideal balance between the free-rider problem and the tyranny of the majority[25] and might be a viable alternative to the one-person-one-vote mechanism. Since this way of voting faces many challenges, some fundamentally different from those the traditional voting system is facing, this paper tried to offer some ideas and approaches to the most important ones and attempted to set up a framework for an election-series, that might be able to provide a way to scale QV to an arbitrary level without increasing its costs relative to the prevailing way of voting.

An additional positive effect of the framework decision to vote on a blockchain offers a corruption-secure way of voting for countries where this actually poses a threat to democracy itself. Over the last years there have been a few proposals to increase the focus on blockchain voting with the most recent one being the Kenyan electoral commission nominee who stated that the country should consider blockchain-based voting, which he claims will both decrease the estimated costs for elections as well as improve the transparency and security of the election[26].

While it's clear that the technology of today is capable of carrying the theoretical setup of QV via voting on the blockchain by automating the storage process of voice credits as well as supplying mechanisms to detect and penalize malicious behaviour, a very important factor has been neglected in most literature and approaches on QV; the people voting. This stems from the fact, that the topic is still in its early stage and therefore most researchers are focusing on the mechanism itself to further optimization instead of trying to setup an actual wide-scaled implementation. In theory QV works, and it has proven itself very useful in those cases where it has been applicated in a non-survey environment. The next step to be taken now, is to roll out increasingly bigger field experiments with QV to strengthen the trust of the targeted audience in the mechanism as well as gathering information about the actual behaviour of participants in different settings in contrast to the assumed rational voter in all of the literature. Collecting those insights in addition to further research on the mechanism design and finetuning regarding the framework around QV might offer a way to renew the stagnating voting environment in democracies all around the world.

In addition to this, the framework of our scaled QV gives us the opportunity of testing a more direct democracy, both through the digital way of voting which can be repeated in a short

[25] cf. Posner, 2018, 108.

[26] cf. https://cointelegraph.com/news/kenyan-electoral-commission-nominee-clamors-for-blockchain-voting

interval without increasing the costs too much as well as the possibility to capture the intensity of preferences. Increasing direct democracy has been found to be connected to an increase in efficiency as well as utility, proxied by happiness, total factor productivity as well as growth and higher output per capita[27].

Those effects combined with the effects of a higher voter turnout, which were found to be positive on generating optimal outcomes lay a good foundation to justify further research on the topic which is definitely still needed but also strongly recommended to be able to offer a working alternative voting system for democracies to choose from.

[27] cf. Matsusaka, 2005, 201.

Literature

Alper, Tim, 2020, ""Russian Dictators Will Use Blockchain to Rig Elections" says Critic": https://cryptonews.com/news/russian-dictators-will-use-blockchain-to-rig-elections-says-8246.htm 16.08.2020

Avan-Nomayo, Osato, 2021, "Kenyan electoral commission nominee clamors for blockchain voting": https://cointelegraph.com/news/kenyan-electoral-commission-nominee-clamors-for-blockchain-voting 21.07.2021

Brennan, G., Hamlin, A., 1998, "Expressive voting and electoral equilibrium". Public Choice 95, 149–175.

Buterin, Vitalik, 2021, "Blockchain voting is overrated among uninformed people but underrated among informed people": https://vitalik.ca/general/2021/05/25/voting2.html 21.06.2021.

Colomb, Gary, 2017: "Believe It: Cybersecurity is Getting Better, Not Worse": https://www.infosecurity-magazine.com/opinions/cybersecurity-getting-better-worse/ 21.06.2021.

Faliszewski, Piotr, Edith Hemaspaandra, and Lane A. Hemaspaandra, 2006, "The complexity of bribery in elections." In AAAI, vol. 6, pp. 641-646.

Fowler, Anthony, 2013, "Electoral and Policy Consequences of Voter Turnout: Evidence from Compulsory Voting in Australia", Quarterly Journal of Political Science, 2013, 8: 159–182.

Hill, Michael, Dan Swinhoe, 2021, "The 15 biggest data breaches of the 21st century": https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html 21.06.2021.

Jakub, 2020, "How Can $1 Turn Into $27? Quadratic Funding Explained": https://finematics.com/quadratic-funding-explained/ 10.08.2020

Kempka, Carmen, 2014, "Matters of Coercion-Resistance in Cryptographic Voting Schemes".

Matsusaka, John, G. 2005, "Direct Democracy Works." Journal of Economic Perspectives, 19 (2): 185-206.

Novuminsights, 2021, “Slashing Penalties - The Long Term Evolution of Proof of Stake (POS)”: https://novuminsights.com/post/slashing-penalties-the-long-term-evolution-of-proof-of-stake-pos/ 21.06.2021.

Orcutt, Mike, 2019, “What the hell is a blockchain phone and do I need one?”: https://www.technologyreview.com/2019/02/28/66000/what-the-hell-is-a-blockchain-phoneand-do-i-need-one/ 05.05.2021.

Ormston, R. and Curtice, J. (eds.), 2015, British Social Attitudes: the 32nd Report, London: NatCen Social Research.

Park, Sunoo, Ronald L. Rivest, 2017, “Towards secure quadratic voting”, Public Choice 172, 151-175.

Posner, Eric, Glenn Weyl, 2018, “Uprooting Capitalism and Democracy for a Just Society”, Princeton University Press.

RadicalXChange, 2019, "Quadratic Voting with Deora and Volt Party" w/ S. Weniger, J. Barbie & M. Kuck (RxC Berlin). 2019): https://www.youtube.com/watch?v=ajeiN05iab4

Ray, Shaan, 2019, “What is quadratic voting?”: https://towardsdatascience.com/what-is-quadratic-voting-4f81805d5a06 21.06.2021.

Roser, Max, 2013, Democracy. Published online at OurWorldInData.org. Retrieved from: https://ourworldindata.org/democracy.

Vivex, 2021, “How to Attack and Defend Quadratic Funding”: https://gitcoin.co/blog/how-to-attack-and-defend-quadratic-funding/ 21.06.2021.

Weyl, E.G., 2017, “The robustness of Quadratic Voting”, Public Choice 172, 75-107.

Wtfisqf: https://wtfisqf.com/ 21.06.2021

Yoder, Jesse, Cassandra Handan-Nader, Andrew Myers, Tobias Nowacki, Daniel M. Thompson, Jennifer A. Wu, Chenoa Yorgason, and Andrew B. Hall, 2020, “Absentee Voting Is Popular During COVID-19 But Does Not Change Turnout or Partisan Rates of Voting”, 2.

Z.cash, 2021, “What are zk-SNARKs?” https://z.cash/technology/zksnarks/ 21.06.2021.