STUDY OF NASH EQUILIBRIA IN BLOCKCHAIN VOTING SYSTEMS

Alon Benhaim

A DISSERTATION

in

Mathematics

Presented to the Faculties of the University of Pennsylvania

in

Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

2022

Supervisor of Dissertation

Brett Falk, Research Assistant Professor of Computer and Information Science

Graduate Group Chairperson

Ron Donagi, Professor of Mathematics

Dissertation Committee

Brett Falk, Research Assistant Professor of Computer and Information Science
Gerry Tsoukalas, Associate Professor of Information Systems, Boston University
David Harbater, Professor of Mathematics
James Haglund, Professor of Mathematics

STUDY OF NASH EQUILIBRIA IN BLOCKCHAIN VOTING SYSTEMS

This thesis work is dedicated to my wife, Margalit, whose constant support made this thesis paper possible. I am truly thankful for having you in my life. This work is also dedicated to my sons, Daniel and Itai, who have always inspired me and loved me unconditionally.

ACKNOWLEDGEMENT

I would like to thank my advisor Brett Falk for his continuous support throughout my years at Penn. On top of patiently holding many discussions on probability and game theory, he also introduced me to the subject of cryptography and blockchains, the latter becoming the main focus of my thesis.

I would also like to thank my unofficial co-advisor Gerry Tsoukalas for many helpful suggestions on my thesis, and also giving possible directions of research related to my work. I also extend my thanks to the faculty members, especially David Harbater and Julia Hartmann, for the many interesting conversations, both mathematical and nonmathematical, during my doctoral studies.

I am grateful to my friends at Penn for their help in mathematics and otherwise. My graduate life would not have been so much fun without the company of Gunnar Arvid Sveinsson, Sammy Sbiti, Artur Bicalho Saturnino, Ellen Urheim, Yao-Rui Yeo, George Wang and many more.

Last but not least, I own a big thanks to my family for always being there.

ABSTRACT

STUDY OF NASH EQUILIBRIA IN BLOCKCHAIN VOTING SYSTEMS

Alon Benhaim

Brett Falk

In the first part of this thesis we analyze the three most common blockchain committees selection strategies: lottery, single-vote and approval voting, where voters can "approve" of any number of candidates. We first show that all these mechanisms converge to optimality exponentially quickly as the size of the committee grows. Approval-voting requires that even honest voters act strategically, we characterize different approval voting strategies and we show that although finding the optimal approval voting strategy is extremely complex, almost any approval voting strategy outperforms the single-vote mechanism enforced on the majority of blockchains. In the second part, we investigate a blockchain governance model where a group of n voters must choose between two collective alternatives. As opposed to the usual voting system (one person – one vote), we propose a voting system where each agent buys votes in favor of their preferred alternative, paying the m-th root of the number of votes purchased. Its novelty relies on allowing voters to express the intensity of their preferences in a simple manner. We provide a rigorous comparison of the utilitarian welfare between Regular Voting ($m = 1$) and Quadratic Voting ($m = 2$). We present closed form equilibrium solutions to the 2 voters and 3 voters games. In addition to characterizing the nature of equilibria, one of our main result demonstrates that the normalized utilitarian welfare of the mechanisms tends to one as the population size becomes large.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

PREFACE

This thesis is divided into two parts, the unifying theme being the analysis of optimal strategies in voting games. Theorems from game theory and probability theory like Chernoff bound are used throughout, and each part is intended to be self-contained. In particular, each part has its own introduction. In the first part (Chapter 1), we analyze the three most common committees selection strategies: lottery, single-vote and approval voting and show they are converge to optimality exponentially quickly as the size of the committee grows. We provide an expression for the probability of selecting an honest committee in the approval voting setting. We then continue to characterize the different approval voting strategies and compare them with respect the probability of selecting an honest committee.

In the second part (Chapter 2), we characterize the nature of Nash equilibria of a blockchain governance model where a group of n individuals must make a binary choice. We compare the mechanisms of RV and QV where agents buy votes (in favor of their preferred binary choice), paying the exact and square of the number of votes purchased, respectively. We demonstrate that the utilitarian efficency of the mechanisms tends to the same value as the population size becomes large. The results obtained in this thesis naturally lead us to a few questions. One is, how to relate the quadratic voting in the committee selection setting. The other is extending our model to the multi-choice setting and allowing non-discrete votes. All of the work is joint with my advisor Brett Falk and his colleague Gerry Tsoukalas, Sections 1.4 to 1.6 and 2.3 to 2.5 are my main contribution.

CHAPTER 1

Committee-based consensus in blockchain systems

ABSTRACT

In the high-stakes race to develop more scalable blockchains, some platforms (BSC, Cosmos, EOS, TRON, etc.) have adopted committee-based consensus protocols, whereby the blockchain's record-keeping rights are entrusted to a committee of elected block producers. In theory, the smaller the committee, the faster the blockchain can reach consensus and the more it can scale. What's less clear, is whether this mechanism ensures that honest committees can be consistently elected, given voters typically have limited information. Different voting blockchains use different mechanisms for selecting committees, and in this work we analyze the three most common selection strategies: lottery, single-vote and approval voting, where voters can "approve" of any number of candidates. We first show that all these mechanisms converge to optimality exponentially quickly as the size of the committee grows. Approval-voting requires that even honest voters act strategically, we characterize different approval voting strategies and we show that although finding the optimal approval voting strategy is extremely complex, almost any approval voting strategy outperforms the single-vote mechanism enforced on the majority of blockchains.

Keywords: Approval Voting, Blockchain Consensus Protocols, Blockchain Economics, Token Voting, Committee-Based Consensus, Delegated Proof of Stake, DPoS, Stake-Weighted Voting.

1.1. Introduction

Permissionless blockchains face a challenging problem: How can anonymous/untrusted decentralized agents all agree on a sequence of events, e.g., transactions, or more general state updates? The Bitcoin Whitepaper (Nakamoto, 2008) introduced "Nakamoto Consensus", a novel consensus protocol that allowed participants to reach agreement on the state of a distributed database in the absence of trust and stable identities, paving the way to a new form of decentralized money. Once Bitcoin's success highlighted the value of blockchain technology, a high-stakes race ensued to build improved consensus mechanisms that could shore-up Bitcoin's flaws – most notably low throughput/scalability, high economic and environmental costs, and delayed finality of records (we expand on these in §1.2).

One suggested alternative with the potential to address all of the above is "Committee-based consensus", whereby participants delegate the chain's record-keeping rights to a relatively small committee. The core idea is that smaller committees can reach consensus more efficiently (albeit, at the cost of less decentralization). Currently, several prominent blockchains including the Binance Smart Chain (BSC), Cosmos-based chains[1], Algorand, EOS, and TRON use this approach,[2] though, importantly, they differ in *how* the committee members are chosen.

Despite the prevalence of committee-based consensus protocols in practice, they have received relatively little attention in the academic literature so far. In particular, the question of how participants of blockchain systems, who typically have limited and dispersed information, can optimally choose/elect effective and trustworthy committees to maintain the state of the chain is of critical importance, and is not well understood. This work seeks to help bridge this gap.

Before diving into further details, we first provide a brief overview of some common consensus protocols.

Leader-based vs. committee-based consensus protocols

Bitcoin's implementation of Nakamoto consensus relies on leader-based consensus protocol termed "Proof of Work" (PoW). In PoW, blockchain users can compete with each other by engaging in "wasteful" computations, for the chance of being selected "block leader." If selected, they have the (exclusive) right to append a block of transactions to the blockchain, and reap any rewards that come with it. The more computing (hash) power participants have, the higher their odds of selection. This incentive structure, in turn, has lead to an arms race to invest in specialized computing hardware (ASIC), beyond traditional chips.

[1]Including the Cosmos Hub, crypto.org, Terra, Osmosis and Secret among many others.

[2]Note, blockchains like EOS, WHO raised a record-breaking $4 billion in its Initial Coin Offering, in 2017, and Tron, define themselves as "Delegated Proof of Stake" systems, but this branding has become tarnished by the criticisms of their technical design (The Interchain Foundation, 2017; Xu et al., 2018) and some of their business behavior (Copeland, 2020; Rubin, 2021; Hui, 2020). It is important to note that these criticisms do *not* undermine the core ideas of committee-based consensus, as evidenced by the fact that more prominent blockchains (like Cosmos) rely on it as well.

One desirable feature of PoW's wasteful computation is that it affords Sybil resistance[3] by imposing a cost to enter the block-producer "lottery." However, less wasteful alternatives exist: Nakamoto consensus can also be implemented using Proof-of-Stake (PoS), and early PoS protocols like Nxt (Nxt Community, 2016) were essentially PoS-based versions of Nakamoto consensus, where the chance of being selected as block leader is proportional to one's token stake, rather than one's computing power.

Blockchain platforms are increasingly gravitating towards PoS consensus as this mechanism is generally believed to be more scalable and less wasteful than PoW (John et al., 2020). Nonetheless, both PoW and PoS suffer from lack of "instant finality": records aren't considered "final" until several successive blocks have been appended to the chain, meaning, their internal states can only reach eventual consistency. In practice, these chains can and do "fork" unpredictably, creating conflicting versions of message history, for instance, when two producers independently produce blocks at around the same time, or when a malicious producer actively purposely produces multiple conflicting blocks.[4]

Committee-based consensus protocols attempt to address this issue (and others) by replacing the "single-block-producer" leader model of PoW and PoS, with one that relies on the formation of dynamic committees.[5] As such, they can be built on top of existing PoW and PoS systems.

At its core, (elected) committee-based consensus is rather simple: users continuously vote to elect their preferred block producers to the committee. Keeping the committee size small improves efficiency: increasing throughput, decreasing latency and allowing for member specialization. Unfortunately, a small number of malicious committee members can also undermine the security of the entire blockchain, thus there is a fundamental tension be-

[3] A Sybil attack involves creating a large number of pseudonymous accounts in an attempt to seize control of the network.

[4] It should be noted that forking frequency on PoW and PoS can be quite different in practice. For instance, Ethereum (PoS) sees hundreds of (short-term) forks every day (Etherscan, 2022). By contrast, Bitcoin (PoW) sees fewer than one fork per month (Lovejoy, 2020).

[5] When the committee is static, the blockchain is said to be "permissioned." In this work, we focus solely on the permissionless setting, where the committee changes dynamically.

tween performance and robustness – a small committee is extremely efficient but is more centralized, and may compromise security.

Despite their simplicity, there is considerable variation in the design of committee-based consensus protocols in practice, and in particular, on the question of how committee members should be optimally chosen. We outline below three of the most popular implemented designs:

- **Lottery:** Algorand committees are elected by a (stake-weighted) lottery.
- **Single-vote election:** Most Cosmos-based chains (including the Cosmos Hub, Terra, Crypto.org, Osmosis and Secret) use single-vote elections to elect a committee, as does Tron and the Binance Smart Chain.
- **Approval voting:** EOS (which raised a record breaking $4 Billion in its ICO in 2017) as well as its forks like Telos use "approval voting" where voters can approve of a collection of candidates rather than focusing their voting power on a single one.

Although these blockchains (Algorand, BSC, Cosmos, EOS, Tron etc) differ widely in their features – they have different tokenomics, different virtual machines and their committees run different consensus algorithms – the method for *selecting* committees can be largely divorced from the other features of the system, making it amenable to independent study.

Research Questions

Several interrelated questions follow: First, how should agents vote for their preferred candidates given they only have partial information? Second: How small can the committee be without undermining security? Third: How does committee-based consensus with approval voting compare to other PoS protocols?

Summary of Model

To answer these questions, we develop a simple voting model using EOS' Delegated Proof of Stake (DPoS) protocol as a backdrop. Block producers have two types, either "honest" or

"dishonest," and the vote succeeds if a $(1-p)$ fraction of the elected committee is honest.

This mimics the analysis of most consensus protocols (like those used in Cosmos, Algorand and EOS) where participants are either honest or "byzantine," and the consensus protocol exhibits a strict phase transition when the number of byzantine participants exceeds a given threshold (usually 2/3rds).

Token holders elect block producers into a committee, but the voters have limited information about the candidates: they receive private signals about the type of each candidate block producer and vote strategically to try and maximize the probability of electing an honest committee. The election process is based on a variation of approval voting, whereby voters approve of a collection of candidates, and the candidates with the most approvals are elected to the committee (Brams and Fishburn, 2007). As we will discuss later, this is fundamentally different from traditional voting schemes, where voting for more than one candidate means splitting your vote.

Assuming the block producer committee uses a traditional consensus protocol to certify blocks, such as Practical Byzantine Fault Tolerance (Castro and Liskov, 1999), this imposes a strict threshold effect on the committee: if fewer than 1/3rd of the committee members are dishonest, they cannot disrupt the consensus protocol, but once more than 1/3rd of the committee members are dishonest, they can completely subvert the committee (which can result in halting transactions, or executing double-spend attacks).

We seek to characterize agent optimal voting strategies under these conditions. Further, guided by some stylized facts emerging from our basic empirical observations, we also consider a restriction of the voting strategy space to two simple and intuitive classes: "threshold voting," where voters vote for all candidates whose (conditional) probability of being honest is above a certain threshold (Definition 5), and "cardinal voting," where voters vote for their top k candidates (Definition 6).

Summary of Results

Even with this relatively simply model, computing the probability of electing an honest committee turns out to be extremely challenging. In Theorem 1, we derive this probability in the most general terms, allowing for specialization to various voting strategy classes. We then proceed to examine the outcomes success probabilities for the two, intuitive, voting strategy classes we consider.

We first analyze a special case where there is only a single voter, and show that it is (mathematically) equivalent to a setting in which all voters can credibly (and costlessly) pool their information. Pooling of information is often regarded as a pure hypothetical exercise, but it is worth studying in our setting because voter incentives are aligned, and there is no obvious downside to sharing one's information with others. Under these conditions, we show that the cardinal voting strategy *is* in fact the optimal strategy (Proposition 2). But this result breaks down when there is more than one voter, if signals cannot be shared (Proposition 5).

Proposition 1 gives a closed-form solution for the the probability of electing an honest committee when voters follow the threshold strategy. But threshold voting can be suboptimal even when there is just a single voter (Proposition 3).

Despite the general suboptimality of these simple strategies (other than in the special pooling case), we show that the system is asymptotically stable. More specifically, regardless of the strategy considered, and under very weak assumptions, the probability of electing an honest committee tends to one, *exponentially fast,* as the number of voters increases (Theorem 3). Thus, although the *optimal* voting strategy may be too complex to be realistically achievable in practice, simple, intuitive voting strategies, that token holders tend to use in practice, exhibit very strong robustness.

Finally, we compare the approval-voting mechanism for committee selection to another popular mechanism used by many PoS blockchains: the random assignments protocol. We find that approval voting typically requires much smaller committee sizes (1 to 2 orders of

magnitude) to attain the same levels of failure tolerance.

Overall, our results suggest that for most practical purposes, committee-based consensus, of the type implemented in DPoS blockchains, is theoretically efficient and robust to the complexity it introduces on the agent strategy space (some limitations are discussed in Section 1.9).

Below, in Section 1.2, we discuss some of the basics of blockchain consensus protocols and the approval voting mechanism that we model. Readers already familiar with these concepts can skip the section, or its relevant parts, without loss.

1.2. A Primer on Blockchain Consensus Protocols & Committee Elections

Herein we provide a primer on single-leader and committee-based consensus protocols. Readers familiar with their basic operational features can skip this section without loss.

As mentioned in the introduction, the core problem facing all cryptocurrencies (and decentralized databases of all kinds), is how to provide a single, universally accepted *ordering* of transactions (or state updates). Most modern cryptocurrencies are based on the notion of a *hash chain*, where blocks of data are chained together using cryptographic hash functions. Hash chains are an append-only data structure, meaning that new blocks (containing transactions) can be appended to the end of the chain, while internal blocks of the chain cannot be modified or re-ordered (without modifying all subsequent blocks). Since anyone can easily append new blocks to the end of a hash chain, decentralized systems need a method for deciding how and when new blocks can be added to the chain.

Most cryptocurrencies use a form of leader election, where a leader is elected at regular intervals. This leader, or "block producer," is given the right to produce a single block. There is an inherent value in becoming a block producer, as block producers have the power to insert, re-order and censor transactions (Daian et al., 2020).[6] In addition, most

[6]The value that can be extracted by inserting, re-ordering and censoring transactions is termed "Maximum Extractable Value" (MEV), and is worth hundreds of millions of dollars on blockchains like Ethereum (Flashbots, 2021).

cryptocurrencies provide direct incentives for block production in the form of transaction fees and block rewards. Transaction fees are paid by the users to incentivize the block producer to include specific transactions in a block. Block rewards are new coins that are minted and paid directly to block producers. For example, in Bitcoin, block rewards are currently set to 6.25 BTC. In many cryptocurrencies, block rewards are the *only* mechanism by which new coins are generated. For reference, in July 2021, Ethereum miners received about 18% of their direct compensation from transaction fees and 82% from block rewards (The Block, 2021).

Block producers also have the ability to harm the platform itself. Block producers can censor transactions *within the block they produce*. Lazy or inept block producers can reduce the total transaction throughput of the system by failing to include enough transactions in a block or failing to produce a block altogether. Malicious block producers can "fork" the chain by appending two blocks at the same block height. This type of behavior can lead to "double-spending attacks" and can destabilize the entire blockchain.

Block producers' power to harm the ecosystem, means that the selection mechanism must ensure that only "honest" producers are elected. When block producer candidates have stable identities, classical consensus protocols (e.g. Lamport et al. (1982); Castro and Liskov (1999)) provide efficient and robust mechanisms for leader election. In a permissionless setting, however, where the set of block producer candidates is anonymous and dynamic, classical consensus protocols fail, and other leader-election methods must be devised.

Proof of Work (PoW)

As mentioned earlier, the Bitcoin whitepaper Nakamoto (2008) introduced a novel leader-election protocol whereby block-producing candidates ("miners") expend effort in the form of computing cryptographic hashes on random values, and their chance of becoming block leader is proportional to the amount of effort they exert. This Proof of Work consensus, is used by many of the leading cryptocurrencies (by market cap), including Bitcoin, Ethereum, Dogecoin and Litecoin.

Although PoW-based consensus has proven stable and secure, it has several drawbacks, most notably its societal cost, and its low transaction throughput. Currently, block producer candidates on Bitcoin expend about as much electricity as the country of Finland in an effort to be chosen as block producers (Cambridge University, 2021).

Proof-of-Work based consensus, also has limitations on how frequently block producers can be chosen, and this directly affects the blockchain's transaction throughput. Currently, the leading PoW-based blockchains, Bitcoin and Ethereum, can handle less than tens of transactions per second. By contrast Visa handles thousands of transactions per second (Binance Academy, 2021).

Proof of Stake (PoS)

The aforementioned drawbacks of PoW have pushed the blockchain community to explore alternatives, and in this quest, Proof of Stake (PoS) has aruably emerged as the current frontrunner. The Ethereum blockchain, for instance, which supports the world's second largest cryptocurrency ETH, originally launched with a PoW protocol but has been gradually trying to transition to a form of PoS for several years (InsideTheSimulation, 2021).

In PoS, block producers are elected in proportion to their token balance ("stake") on the blockchain, rather than their computational effort. Similar to PoW systems, where candidates signal their support of the platform by expending computing resources, in PoS systems, candidates signal their support of the system by acquiring and holding native tokens on the blockchain.

There are many variants of the PoS protocol, but a common feature of almost all PoS systems is that block producers are elected with probability proportional to their "staked" tokens (as in Ethereum 2.0) or their passive token balances (as in Algorand).

Committee-based Consensus

Although under PoS, block producers can earn significant returns, being an efficient block producer usually requires powerful computing equipment, a dedicated internet connection,

and a robust software configuration. In some blockchains, a nontrivial minimum amount of tokens is also required to be eligible to participate. Many regular token holders are thus ineligible (or simply unwilling) to take on this type of role. To address this problem, most PoS systems support some type of delegation mechanism, whereby token holders can delegate their stake to professional block producers (usually in exchange for some sort of profit sharing).

Committee-based consensus takes this separation between token holders and block producers to the extreme. In most traditional PoW systems, block producers are selected in a lottery-like procedure according to their (proportional) hash power. Several PoS systems (e.g. Tezos, Algorand, Cardano) adapted this idea to elect leaders randomly with probability equal to their proportional token stake.[7] As an alternative to this lottery-based leader election, several blockchains allow users to cast (stake-weighted) votes for block producers and the ones with the highest number of votes become producers for some fixed duration of time.

In platforms using committee-based consensus, a small committee ($k = 150$ in the Cosmos Hub, $k = 21$ in EOS or 27 in TRON) of block producers is elected by a stake-weighted vote, and is responsible for producing and validating blocks.[8]

In committee-based consensus, the elected committee typically runs a traditional consensus algorithm — Practical Byzantine Fault Tolerance Castro and Liskov (1999), Proof-of-Authority Angelis et al. (2018) or Tendermint (Buchman, 2016) — to certify the next block.

Some Advantages of Committee-based Consensus

Committee-based consensus has several perceived advantages over other commonly used consensus protocols. First, the committee can check each other's actions, and prevent ma-

[7] In fact, the core technical contribution in systems like Algorand and Cardano is a decentralized, verifiable lottery mechanism.

[8] Although almost all PoS systems support some form of delegation, the term "Delegated Proof of Stake" is usually reserved for the specific type of committee-based consensus protocols used by systems like EOS and TRON.

licious behavior. For example, in most classical consensus protocols a p-fraction[9] of the participants can behave maliciously without adversely affecting the system.

Second, the voting process takes a nonzero amount of time, so electing a batch of producers at once increases efficiency in contrast two Nakamoto consensus, where a single block producer is selected at each step.

Third, it allows the chain to achieve instant finality – when the committee certifies a block, that block is immediately finalized. This is in contrast to PoW blockchains that only achieve eventual finality. Bitcoin wallets, for instance, typically wait until a transaction is buried 6 blocks deep in the chain before considering it "finalized" (Bitcoin Wiki, 2021). Blockchains that rely on committee-based-consensus can achieve instant finality in the following sense. If the system *never* elects a committee with more than a p-fraction of malicious members, then as soon as a committee certifies a block, that block can be considered final, and will never be forked away. Thus committee-based consensus protocols need to ensure that the probability a malicious committee is elected is so small, that even if the chain runs for years, there will *never* be a committee with more than a p-fraction of malicious members.

Fourth, it can eliminate the need for "slashing" penalties. In many traditional PoS systems (e.g. Ethereum 2.0), block producer candidates need to stake their tokens by locking them in a smart contract, and this stake is held as a bond against misbehavior. If a block producer engages in (provable) misbehavior, their stake can be confiscated ("slashed"). In committee-based consensus, if a small minority of the committee misbehaves, they cannot adversely affect the system, and voters (having noticed this misbehavior) will not elect them again. For this reason, some systems (like Algorand, EOS and Tron) do not have slashing penalties. On the other hand, Cosmos, which uses committee-based consensus *does* include slashing penalties.

Finally, having a distinct separation between stakeholders and block producers allows specialization, and thus block producers in systems using committee-based consensus, may have

[9]Most consensus protocols can tolerate $p = 1/3$.

better hardware and software infrastructure which would lead to lower latency and faster block times.

Of course, these advantages hinge on the system's ability to consistently elect an honest majority of committee members. This then raises the need to dive into the committee election mechanism.

Approval Voting

Committee-based consensus protocols can vary on several dimensions, but we focus on *how* the committee is selected. The selection process is independent of many other features of the blockchain, e.g. the actual consensus protocol employed by the elected committee, or how data is stored and processed on the blockchain. In this work, we focus on *approval voting*, which is the selection mechanism employed by EOS and Telos.

In approval voting, voters "approve" of a collection of candidates, and the candidates with the most approvals are elected to the committee (Brams and Fishburn, 2007). This is fundamentally different from traditional voting schemes, where voting for two candidates means splitting your vote. In approval voting, if a voter votes for two (or more) candidates, each receives the same "approval" as if the voter only voted for one candidate.

For example, the Cosmos blockchain uses a traditional (single-vote) mechanism to elect a committee of 150 block producers[10]. By contrast, EOS uses approval voting to elect a committee of 21 block producers. Although Cosmos and EOS vary on several other dimensions (The Interchain Foundation, 2017), the committee selection mechanism is essentially independent of all these other variables. Since Cosmos could be modified to use approval voting, and EOS could be modified to use a single-vote mechanism, designing the most efficient committee-based consensus protocols requires analyzing the characteristics of these mechanisms in the blockchain setting.

[10]The documentation suggests 125, (Cosmos, 2021), but this seems to have been increased to 150

1.3. Literature Review

Committee-based consensus is widely used in the blockchain space (Kogias et al., 2016; Meng et al., 2018; Gleehokie et al., 2018; TRON, 2018; Cosmos, 2021), but the academic literature is arguably still lagging behind. Of the few studies we could find, Meng et al. (2018), Yang et al. (2019), Hu et al. (2021) examine related topics, but they focus mostly on hypothetical tweaks that could be added to improve existing systems. In contrast, we seek to formally analyze and understand whether the existing systems themselves are robust and efficient, given voters have limited information.

Approval voting was introduced into the blockchain space in Delegated Proof of Stake (DPoS), and the first literature on DPoS started with practitioners, where it was often asserted that DPoS consensus is a more efficient and democratic version of the standard PoS mechanism (Binance, 2020; Cryptopedia, 2021). The approval voting mechanism underlying DPoS is described in the original whitepaper, Bitshares (2021), but there is little attempt to assess potential agent voting behavior and what could go wrong with it.

Approval voting has been widely studied in the context of political elections
(Brams and Fishburn, 2007), and we highlight here some facts about the known dynamics of approval voting in general. In a k-winner election system, it is desirable to have the property that if a candidate is ranked first by at least n/k of the voters, then that candidate should be elected to the committee. Unfortunately, this property does *not* hold under approval voting (Elkind et al., 2017).

Similarly, an approval voting scheme can end up electing candidates that would lose a majority of pairwise contests against the other candidates, i.e., an approval voting scheme may elect a "Condorcet loser" (Niemi, 1984).

One of the most interesting features of approval voting schemes is that voters typically have multiple honest strategies (Niemi, 1984). For example, consider an up-to-2, 2-winner system with two voters ($n = 2$), and four candidates ($m = 4$), $\mathcal{C} = \{c_1, c_2, c_3, c_4\}$. If the two

voters' preference orders are $(c_2; c_3; c_4; c_1)$ for voter 1 and $(c_1; c_3; c_4; c_2)$ for voter 2 then the candidate c_3 will be in the elected committee for any $t \geq 2$, so both c_1 and c_2 cannot be in the elected committee. Should voter 1 vote for c_2 only, or c_2 and c_3? These are both honest strategies, and thus even honest players must think strategically. This feature makes the analysis of approval voting systems complex.

DPoS consensus, being based on approval voting, inherits these aforementioned properties, but it differs from traditional approval voting in several ways that we describe in the model section. The most significant departure is perhaps that extant studies (outside of the blockchain literature) assume voters have competing interests, and usually have perfect information about the candidates themselves. By contrast, in the DPoS setting, most voters' interests are aligned. All voters wish to elect an honest committee, but they have limited information about the candidates. This completely changes the nature of the analysis.

Though we are not aware of any studies considering strategic agent voting behavior in committee-based protocols, numerous studies have looked at strategic agent behavior in other Blockchain protocols. Saleh (2021); Roşu and Saleh (2021); Fanti et al. (2019) are some of the first studies looking at the economics of PoS systems. Leonardos et al. (2020) study weighted voting in validator committees in PoS protocols. There is also a relatively large computer science literature blending strategic considerations and technical design elements of PoS, such as Gaži et al. (2019); Chen and Micali (2016); Bentov et al. (2016); Kiayias et al. (2017).

Beyond PoS, Alsabah and Capponi (2020); Biais et al. (2019); Cong et al. (2021)
Garratt and van Oordt (2020) focus on the economics of PoW, and the underlying mining mechanism. Several other studies focus more specifically on Bitcoin, such as Nakamoto (2008); Easley et al. (2019); Huberman et al. (2021); Pagnotta (2021); Prat and Walter (2021).

Other works have considered consensus in the presence of three types of participants byzantine, altruistic and rational Aiyer et al. (2005), or just byzantine and rational

Amoussou-Guenou et al. (2020). In the byzantine-rational model of consensus Amoussou-Guenou et al. (2020), there are still two types of participants, and there is still a phase transition when the number of byzantine participants exceeds a certain threshold, thus our analyses applies almost equally in this setting as well.

Finally, on a broader note, our work is related to the literature studying security guarantees for different types of blockchain protocols, e.g., Lewis-Pye and Roughgarden (2020, 2021), though we are not aware of any prior work focused specifically on committee-based consensus. More generally, our work also has implications for the literature studying the economics of token systems, see e.g., Cong et al. (2021); Tsoukalas and Falk (2020); Gan et al. (2021a,b).

To the best of our knowledge, ours is the first paper to analyze the efficiency of committee elections in committee-based consensus protocols, with private information and strategic agents.

1.4. Preliminaries and Empirical Observations

1.4.1. Definitions

Approval voting is a system where each voter may select ("approve") any number of candidates, and the winners are the candidates approved by the largest number of voters (see Kilgour (2010) for a survey on approval voting). Formally:

Definition 1 (k-winner Approval Voting)**.** *A set of voters $\mathcal{V}$ votes on a set of candidates, $\mathcal{C}$. Let $n \stackrel{\text{def}}{=} |\mathcal{V}|$, and $m \stackrel{\text{def}}{=} |\mathcal{C}|$. Voter v chooses a subset of candidates $\mathcal{C}_v \subseteq \mathcal{C}$ they wish to vote for. For each candidate $c \in \mathcal{C}$, the* score *of candidate c, that is, the number of votes the candidate receives, is defined to be*

$$\mathsf{score}(c) \stackrel{\text{def}}{=} |\{v \mid c \in \mathcal{C}_v\}| \,. \tag{1.1}$$

The elected committee is determined to be the k candidates with the highest scores.

In DPoS protocols, stake-holders vote for a set of "block-producers" modifying the *k-winner*

Approval Voting system to include a cap on the number of candidates. Formally:

Definition 2 (up-to-t-vote, k-winner Approval Voting)**.** *With notation as in definition 1, we limit the maximum number of candidates t each voter can vote for, so that voter v chooses a subset of candidates $\mathcal{C}_v \subseteq \mathcal{C}$ restricted to $|\mathcal{C}_v| \leq t(\leq m)$. As before, the elected committee is determined to be the k candidates with the highest scores.*

We will assume throughout that there are at least k candidates, $m \geq k$. In general, there may be less than k candidates in the elected committee if less than k candidates received any votes. Alternatively, there may be more than k candidates if there are ties. We specify how we handle these cases in Definition 3.

1.4.2. Empirical Observations: Approval Voting on EOS

Block Producers on EOS are elected by token holders according to a up-to-30-vote, 21-winner approval voting system (see Definition 2, with $t = 30$ and $k = 21$). The 21 winning candidates form the block producer committee. Elections are held continuously, and each committee of block producers remains in control of the chain for 126 seconds (EOS, 2018).

EOS voters are not directly rewarded for staking (although this has been proposed as in NY (2019)), instead voters are assumed to benefit indirectly from the stability and performance of the platform. In EOS and other DPoS systems, votes are weighted by stake, and voters are allowed to "proxy" their votes, i.e., delegate their voting power to a different voter.

To understand real-world voting strategies, we gathered voting data from EOS. As the EOS blockchain is extremely large (over 8TB) and the majority of transactions are unrelated to voting, we gathered daily voting snapshots from EOS Authority (a block producer) and we used these to analyze voter behavior during the period 2021-08-20 - 2022-02-09. Each snapshot contained the current votes of the nearly 1 million accounts that have ever voted.

Figure 1.1 shows the number of votes cast by individual voters (left panel), and stake-weighted votes (right panel), on a typical day. Although EOS votes are stake-weighted, and the unweighted votes do not directly affect the elected committee, we include them in our

data be cause they illustrate the strategy pursued by the majority of voters.

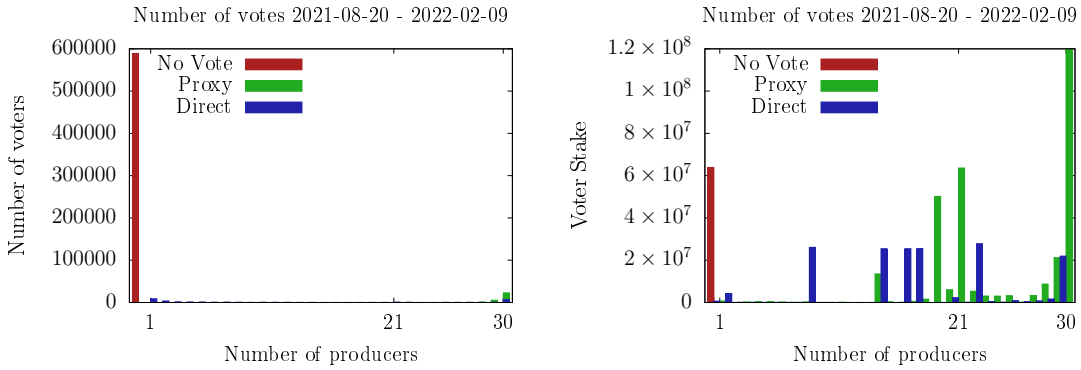

Figure 1.1: The number of producers that each token holder voted for, during the period 2021-08-20 - 2022-02-09. Left panel: unweighted voting. Right panel: stake-weighted voting. *Key Takeaway:* most voters follow a "cardinal voting" strategy.

As can be seen from Figure 1.1, when votes are weighted by stake, most stake is proxied, and most voters vote for either 21 or 30 producers.

Figure 1.2 shows a different view of the same data: the left panel shows the breakdown (in %) of unweighted voting and the right panel shows the breakdown (in %) for stake-weighted voting.

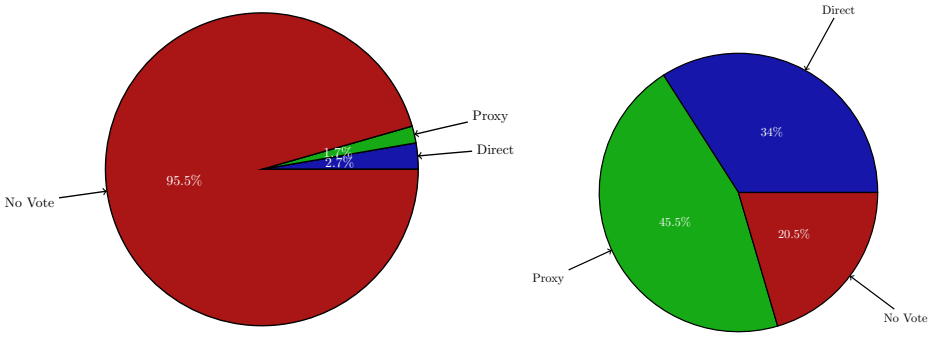

Figure 1.2: The percentage breakdown of votes during the period 2021-08-20 - 2022-02-09. The left-hand plot shows unweighted voting. The right-hand plot shows stake-weighted votes.

Note, both figures represent a week's worth of voting data on EOS, but these patterns are consistent and exhibit relatively little variability, over different/longer time windows.

The key observation is that most voters follow a "cardinal voting strategy" where they vote for a fixed number of block producers. A formal definition is given in Definition 6.

We rely on these basic empirical observations to inform our model in Section 1.5. In Section 1.6, we explore how optimal these types of voting strategies can be.

1.5. Model

1.5.1. Voting with Limited Information

We lay out a simple model, where the blockchain's token holders vote according to an up-to-t, k-winner approval voting system, to elect a committee of block producers. There is a pool of m producers to choose from, $c_1, \ldots, c_m$, and n strategic voters on the platform, $v_1, \ldots, v_n$. Every producer has an unknown type, either "honest", H, or "malicious", M. The goal of each voter is to maximize the probability that a supermajority (e.g. a $(1-p)$-majority) of the elected committee is honest. We discuss some possible alternative objectives in Appendix A.4.

Definition 3 (Honest Committee)**.** *Suppose the k producers with highest number of votes are elected to be on the block-producer committee, $\mathbb{T}$. If there are less than k candidates with non-zero score, then the committee is filled adversarially (i.e., in a worst-case fashion), and if there are ties between the candidates such that there are more than k producers with highest score, then they are broken adversarially (between the ones with least score). Since most Byzantine Agreement protocols require at least $\lceil (1-p)\cdot k \rceil$ honest members, we say the committee $\mathbb{T}$ is* honest*, $\mathbb{T} = H$, if at least $\lceil (1-p)\cdot k \rceil$ of the elected block producers are honest.*

Suppose the *a priori* probability that producer j is honest is $\Pr[c_j = H] = p_j$. Also, suppose voter v_i receives a private noisy signal vector, $\mathbf{s}_i^* = (s_{ij}^*)_{j=1}^m$ about producer's c_j honesty,

$$s_{ij}^* = \begin{cases} p_h + \epsilon_{ij} \text{ if Producer } j \text{ is honest} \\ p_m + \epsilon_{ij} \text{ if Producer } j \text{ is malicious,} \end{cases} \tag{1.2}$$

where ϵ_{ij} is a normally distributed noise term with $\mathbb{E}[\epsilon_{ij}] = 0$ and $\text{Var}[\epsilon_{ij}] = \sigma_{ij}^2$, i.e., $\epsilon_{ij} \sim \mathcal{N}(0, \sigma_{ij}^2), \forall j \in \{1, \ldots, m\}$. It follows that signals are normally distributed with $s_{ij}^* \sim \mathcal{N}(p_h, \sigma_{ij}^2)$ if producer j is honest, and $s_{ij}^* \sim \mathcal{N}(p_m, \sigma_{ij}^2)$ if producer j is malicious.

When voter i receives a signal, s_{ij}^*, regarding producer j, the voter can compute the *posterior* probability that producer j is honest *conditioned on* s_{ij}^*. We call this conditional probability s_{ij}:

$$s_{ij} \stackrel{\text{def}}{=} \Pr\left[\text{ producer } j \text{ is honest } \;\middle|\; s_{ij}^* \right]. \tag{1.3}$$

The map $s_{ij} \leftrightarrow s_{ij}^*$ is a bijective function, and we calculate it explicitly in Lemma 2 in Appendix A.1.1. The result is given below in (1.4).

$$s_{ij} = \frac{1}{1 + \frac{1-p_j}{p_j} e^{\frac{(s_{ij}^* - p_h)^2 - (s_{ij}^* - p_m)^2}{2{\sigma_{ij}}^2}}} \tag{1.4}$$

Our core model assumes all voters are strategic (fully rational), and we seek to characterize the pure-strategy Bayesian Nash equilibria of the game.

Note, we also assume all voters in our model have equal weight. Although essentially all real-world platforms rely on stake-weighted voting where voters can have different stakes, our model still applies since we can view each voter as encompassing the voting power of a single unit stake.

Voter i's payoff is given by u_i if the elected committee is honest ($\mathbb{T} = H$) and 0 otherwise. We assume voting has some unit cost, c (the opportunity cost of staking one unit of capital).

Thus voter i's goal is to optimize the rewards

$$u_i \Pr[\mathbb{T} = H] - c. \tag{1.5}$$

This means that voter i's goal is to maximize the success probability — the probability that the elected committee $\mathbb{T}$ is honest, conditioned on the private signal vector they receive, $\mathbf{s}_i$, given the platform voting system in Definition 2.

$$\max_{\mathcal{C}_{v_i} \subseteq \mathcal{C}} \Pr\left[\mathbb{T} = H \mid \{\mathbf{s}_i\}_{i=1}^{n}\right]. \tag{1.6}$$

We assume that $(p_j)_{1 \leq j \leq m}, (\sigma_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}, p_h, p_m$, are publicly visible, but voters cannot observe others' private signals.

Definition 4 (Voting Strategy)**.** *A voting strategy is an algorithm A (in the class $\mathbb{S}$) used by all voters, that takes as input the parameters the voter has access to $\mathbf{s}_i = (s_{ij})_{j=1}^{m}, (p_j)_{j=1}^{m}, (\sigma_{ij})_{j=1}^{m}, p_h, p_m$ and outputs a subset of candidates the voter wishes to vote for $\mathcal{C}_v \subseteq \mathcal{C}$. We denote the committee elected by exerting algorithm A as $\mathbb{T}_A$.*

After observing their private signal, voters simultaneously submit their "votes" $\mathcal{C}_{v_i} = \mathcal{C}_{v_i}(\mathbf{s}_i)$; we consider any voting strategy in the class of voting strategies, represented by the letter $\mathbb{S}$. With Definition 4, we can interchangeably talk about the voters maximizing the success probability by exerting a voting algorithm $A \in \mathbb{S}$ and rewrite Equation 1.6 as:

$$\max_{A \in \mathbb{S}} \Pr\left[\mathbb{T}_A = H\right]. \tag{1.7}$$

We say that a strategy is optimal if it maximizes the success probability - the probability of electing an honest committee, Equation 1.6 or 1.7. Table 1.1 summarizes the notation.

m	Number of (candidate) block producers
n	Number of voters
p_j	*A priori* probability block producer candidate j is honest
p_m	The base signal for a malicious candidate producer
p_h	The base signal for an honest candidate producer
σ_{ij}	Standard deviation of the noise, ϵ_{ij} for voter i, and producer j
k	Elected Committee size
s^*_{ij}	Voter i's raw signal about producer j
s_{ij}	Producer j's posterior probability of being honest, conditioned on s^*_{ij}.

Table 1.1: Notation

While voters' optimization problem is well-defined, computing the objective function $\Pr[\mathbb{T}_A = H]$ is challenging. As a first step, we need to define the types of voting strategies that are accessible to agents. This is the goal of the next section.

1.5.2. Class of Voting Strategies

In principle, any function $f : [0,1]^m \to \{0,1\}^m$ is a possible voting strategy. It seems clear, however, that any reasonable strategy should be coordinate-wise non-decreasing, i.e., if $s'_j > s_j$ and $f(s_1, \ldots, s_m) = (y_1, \ldots, y_m) \subset \{0,1\}^m$, and if $f(s_1, \ldots, s_{j-1}, s'_j, s_{j+1}, \ldots, s_m) = (y'_1, \ldots, y'_m)$ then $y'_j \geq y_j$. In other words, if one candidate's signal increases (while the other signals remain the same) this *cannot* cause the voter to switch their vote away from the candidate. If we also assume that, aside from the signals, the candidates are otherwise indistinguishable to each voter, then a class of reasonable voting strategies would be to sort the candidates by their signal and vote for the top t candidates. With this intuition we will now consider the reasonable strategies described above as the class $\mathbb{S}$.

Within this broad class, we also single out two particularly simple and intuitive strategies related to our empirical observations, that users could follow: *threshold voting* (Definition 5) and *cardinal voting* (Definition 6).

Definition 5 (Threshold Voting)**.** *Voter v_i is said to follow the* threshold voting strategy *if (prior to seeing the realization his or her signals), voter v_i chooses a threshold $z_i \in [0,1]$ and voter v_i votes for all producers c_j, with probability of being honest higher than the threshold*

$s_{ij} = \Pr\left[c_j = H \;\middle|\; s^*_{ij}\right] > z_i$.

If we define $p_{ij} \stackrel{\text{def}}{=} \Pr\left[s_{ij} > z_i\right]$, then p_{ij} is the probability that voter i votes for producer j (assuming voter i is following the threshold voting strategy). Summing over all n voters, the number of votes received by producer j is distributed as the sum of n Bernoulli random variables with parameters $p_{1j}, \ldots, p_{nj}$. If $p_{1j} = \cdots = p_{nj}$, then the number of votes received by producer j is a binomial random variable. When the p_{ij} are distinct, then the number of votes received by producer j is a *Poisson Binomial Random Variable*. See Appendix A.2 for a review of known facts about the Poisson Binomial Distribution.

This characterization of the distribution of votes when voters follow the *threshold voting strategy* will be important as we study the dynamics of this strategy in Section 1.6.

Definition 6 (Cardinal Voting)**.** *Voter v_i is said to follow the* cardinal voting strategy *if (prior to seeing the realization his or her signals), voter v_i creates a strategy $z_i \in \{1, \ldots, t\}$, then voter v_i orders producers according to their probability of being honest $s_{ij} = \Pr\left[c_j = H \;\middle|\; s^*_{ij}\right]$ and votes for the top z_i producers in the list.*

When voters follow the *cardinal voting strategy*, the number of votes received by each producer is still distributed as a Poisson Binomial random variable, but now the parameters p_{ij} (the probability that voter i votes for candidate j) are much more difficult to compute.

Connecting this back to the empirical voting strategies discussed in Section 1.4.2, Figure 1.1 shows that EOS voters tend to follow the cardinal voting strategy with $z = 1, 21$ or 30.

1.6. Analysis

We begin our analysis by characterizing the probability of electing an honest committee in the most general terms possible (Section 1.6.1) and unveiling some associated complexities (Section 1.6.2). We then examine outcomes in a special single-voter/signal pooling case which helps build intuition (Section 1.6.3), before looking at the general multi-voter case (Section 1.6.4). The results obtained raise additional questions about asymptotic optimality

(Section 1.6.5). We then compare DPoS to other PoS-based mechanisms (Section 1.7).

1.6.1. The Probability of Electing an Honest Committee

The first step in the analysis is to determine the objective function of the optimization, which is the probability that an elected committee is honest.

Theorem 1 (Success Probability)**.** *Suppose there are m producers, and each producer is honest independently with probability p. If the number of votes received by each candidate are independent random variables then the probability that there are at least $\lceil (1-p)\cdot k \rceil$ honest producers in a committee of size k, is given by:*

$$\begin{aligned}\Pr\left[\mathbb{T}=H\right] = &\sum_{a=m-\lceil p\cdot k\rceil+1}^{m}\binom{m}{a}p^a(1-p)^{m-a} + \sum_{a=\lceil (1-p)\cdot k\rceil}^{m-\lceil p\cdot k\rceil}\binom{m}{a}p^a(1-p)^{m-a}\sum_{x=0}^{n}\Bigg[\\ &\left(\sum_{j=0}^{\lceil (1-p)\cdot k\rceil-1}\binom{a}{j}\left(\left(1-F^h(x)\right)^j\left(F^h(x)\right)^{a-j} - \right.\right.\\ &\left.\left.\left(1-F^h(x)+f^h(x)\right)^j\left(F^h(x)-f^h(x)\right)^{a-j}\right)\right)\\ &\left(\sum_{j=0}^{\lceil p\cdot k\rceil-1}\binom{b}{j}\left(1-F^m(x)+f^m(x)\right)^j\left(F^m(x)-f^m(x)\right)^{b-j}\right)\Bigg],\end{aligned} \tag{1.8}$$

where f^h, F^h are the PDF and CDF of the number of votes received by an honest producer, and f^m, F^m are the PDF and CDF of the number of votes received by a dishonest producer.

All proofs are in the Appendix. Theorem 1 is very general, in the sense that it gives the expression for the probability of electing an honest committee under *any* type of voting strategy – provided that the distribution of votes (f^h, f^m) can be computed.

Note, in Theorem 1 and for the rest of this section, we assume that producers are indistinguishable except for their type, meaning, the variance of the noise $\sigma_{ij} = \sigma_i$, for $1 \leq j \leq m$ in Equation 1.2. This implies there is a single pdf, $f^h(x)$ that denotes the probability an honest producer receives x votes. This simplification is done purely for expositional purposes; to obtain the result for the more general case, one would need to replace Theorem 9 (used in

the proof of Theorem 1) by the more general Bapat-Beg Theorem (Bapat and Beg, 1989). The resulting expression remains closed-form, but is too cumbersome for display.

Theorem 2 gives the general form of the distribution of votes (f^h, f^m) received by honest and dishonest producers given the probability that voter i casts a vote for producer j.

Theorem 2 (Distribution of Votes)**.** *For a producer, j, let p_i^h (resp. p_i^m) denote the probability that voter i casts a vote for producer j conditioned on producer j being honest (resp. dishonest). Then the probability distribution of the number of votes received for honest and dishonest producers is given by*

$$f^h(x) = \sum_{A \in F_x} \prod_{i_1 \in A} p_{i_1}^h \prod_{i_2 \in A^c} 1 - p_{i_2}^h \tag{1.9}$$

$$f^m(x) = \sum_{A \in F_x} \prod_{i_1 \in A} p_{i_1}^m \prod_{i_2 \in A^c} 1 - p_{i_2}^m, \tag{1.10}$$

where F_x is the set of all subsets of x integers that can be selected from $\{1, 2, 3, ..., n\}$.

Combining Theorems 1 and 2 gives a closed-form expression for the success probability whenever p_i^h and p_i^m can be calculated. In Propositions 1 we show how to calculate these probabilities for the threshold-voting strategy.

Proposition 1 (Threshold voting)**.** *For a producer j, let p_i^h (resp. p_i^m) denote the probability that voter i casts a vote for producer j conditioned on producer j being honest (resp. dishonest).*

When voters follow the threshold strategy (Definition 5) with threshold, z_i,

$$p_i^h = 1 - \Phi\left(\frac{h^{-1}(z_i) - p_h}{\sigma_i}\right), \quad p_i^m = 1 - \Phi\left(\frac{h^{-1}(z_i) - p_m}{\sigma_i}\right), \tag{1.11}$$

where Φ is the density function of the standard normal distribution, and

$$h^{-1}(q) \stackrel{\text{def}}{=} \frac{p_h^2 - p_m^2 - 2\sigma^2 \log\left(\frac{p(1-q)}{(1-p)q}\right)}{2(p_h - p_m)} \tag{1.12}$$

is derived in Lemma 2.

In 12 in Appendix A.6 we show how to calculate those probabilities for the cardinal-voting strategy. Unfortunately, for cardinal voting, we cannot apply Theorem 1 because the number of votes received by each candidate are not independent.

1.6.2. The Complexity of Approval Voting

Combining Theorems 1 and 2 with Propositions 1, gives concrete formulas for the probability of electing an honest committee when voters follow either the threshold voting strategy. When voters follow the Cardinal strategy, Theorem 1 does not apply (see Appendix A.6).

Unfortunately, these objective functions are extremely complex, and this makes the voters' general optimization problem in (1.7) challenging. To understand the origin of this complexity, we visualize below the objective function, that is, the probability of electing an honest committee, focusing on the case where voters follow a simple threshold voting strategy (the more tractable of the two voting strategy classes).

As a first step, we imagine that *all* voters follow a threshold voting strategy, with some common threshold, z. In this setting, Proposition 1, into Theorems 1 and 2, allow us to calculate the *exact* probability of success as a function of the threshold chosen. Figure 1.3 shows the success probability under threshold voting, for *small* numbers of voters ($n = 1$ to $n = 4$). Although, in practice, systems have many more voters, these graphs highlight the complex dynamics of approval voting.

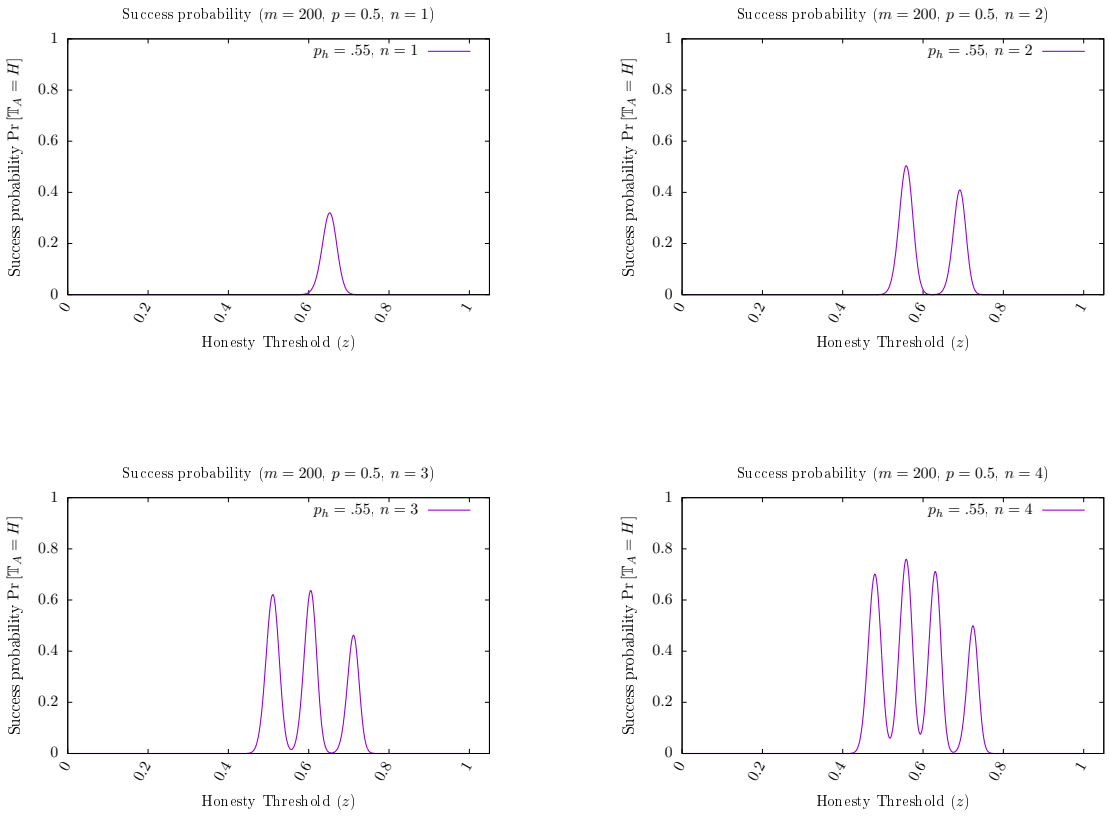

Figure 1.3: Success probability as a function of threshold chosen, assuming small number of voters ($n \in \{1, 2, 3, 4\}$), and all voters use the same threshold. *Key Takeway:* The number of local optima increases with n.

The optimal thresholds tend to hover around $0.5 - 0.7$, meaning that with these parameters, voters should vote for any candidate, j, whose posterior probability, s_{ij}, is above this threshold and not vote for any candidate below this threshold. The thinness of the peaks, however, indicates that even small deviations from the optimal strategy can drastically reduce the success probability. In addition, the number of local optima increases with n. These properties can make the optimization problem intractable at relatively low or medium values of n (with the exception of $n = 1$, for which the objective is unimodal).

Next, we examine the situation for a large number of voters $n = 100$, in Figure 1.4.

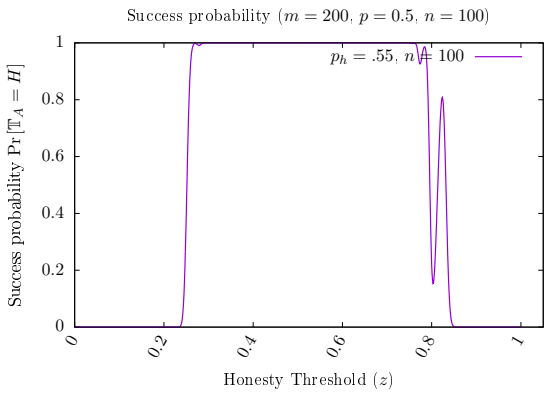

Figure 1.4: Success probability as a function of threshold chosen, assuming large number of voters ($n = 100$). *Key Takeway:* For large n, the probability of success goes to 100% across a wide range of thresholds, and thus a wide range of voting strategies yields nearly optimal results.

Figure 1.4 shows that for large n, the previous issues fade: the local optima tend to merge, and almost any reasonable threshold has an almost 100% probability of success.

Combining insights from Figures 1.3 and 1.4, we conclude that the voters' problem behaves drastically differently depending on low vs. high-number of voters, and hints that asymptotic analysis may offer more tractable results.

Next, we analytically characterize (to the extent possible) the optimality of voting strategies, separating the $n = 1$ case from the general $n > 1$ case.

1.6.3. Special Cases: Single-Voter & Signal Pooling

In this section we consider the special case of a single voter ($n = 1$). Beyond letting us build intuition, we show that the general $n > 1$ case, collapses to $n = 1$ when voters are allowed to credibly (and costlessly) share their signals. This is more than a mere hypothetical exercise. Signal pooling has no obvious downside in our setting given voter incentives are aligned, and thus could be plausible in practice.

Single Voter

Before presenting the result, we introduce one intermediate technical lemma that will be useful throughout the analysis.

Lemma 1. *Suppose X is a Poisson Binomial random variable with k trials and let X_P with $P = \{p_{j_1}, \ldots, p_{j_k}\}$ denote the Poisson Binomial with parameters $(p_{j_1}, \ldots, p_{j_k})$. Let $m \geq k$, and x be positive integers, $\{p_1, \ldots, p_m\} \subseteq [0,1]^m$ such that $p_1 \geq \cdots \geq p_m$ then* $\underset{P \subseteq \{p_1, \ldots, p_m\}}{\operatorname{argmax}} \Pr[X_P > x] = \{p_1, \ldots, p_k\}$.

To understand the implication of Lemma 1, consider a k-winner approval voting system in which candidates have posterior probabilities of being honest $s_1, \ldots, s_m$. Suppose the subset of candidates elected to the committee is $\mathbb{T} = \{c_{j_1}, \ldots, c_{j_k}\}$ so that their posterior probabilities are $\{s_{j_1}, \ldots, s_{j_k}\}$. If we think about the realization of honesty of each candidate as a trial l with probability s_{j_l} then the number of honest candidates on the committee X is a Poisson Binomial with parameters $(s_{j_1}, \ldots, s_{j_k})$. The success probability, e.g. the probability of an honest committee is the probability that the number of honest candidates on the committee is at least $\lceil (1-p) \cdot k \rceil$. Lemma 1 implies that the success probability is maximized when each of the posterior probabilities of the different candidates is as high as it can be.

Proposition 2 (Optimality of Cardinal voting when $n = 1$)**.** *Consider a k-winner approval voting system with $n = 1$ voter and $m \geq k$ candidates, then the globally optimal strategy is the cardinal strategy with $z = k$.*

Proposition 2 follows from the fact that if there is only a single voter, that voter possesses *all* relevant information about each producer's type, and the voter can unilaterally decide the committee. Thus the optimal strategy is to form the committee from the candidates that have the highest (posterior) probability of being honest. In other words, the voter should vote for the top k candidates (when sorted accorded to their posterior probability of being honest), and this strategy is optimal across *all* possible strategies, not just cardinal

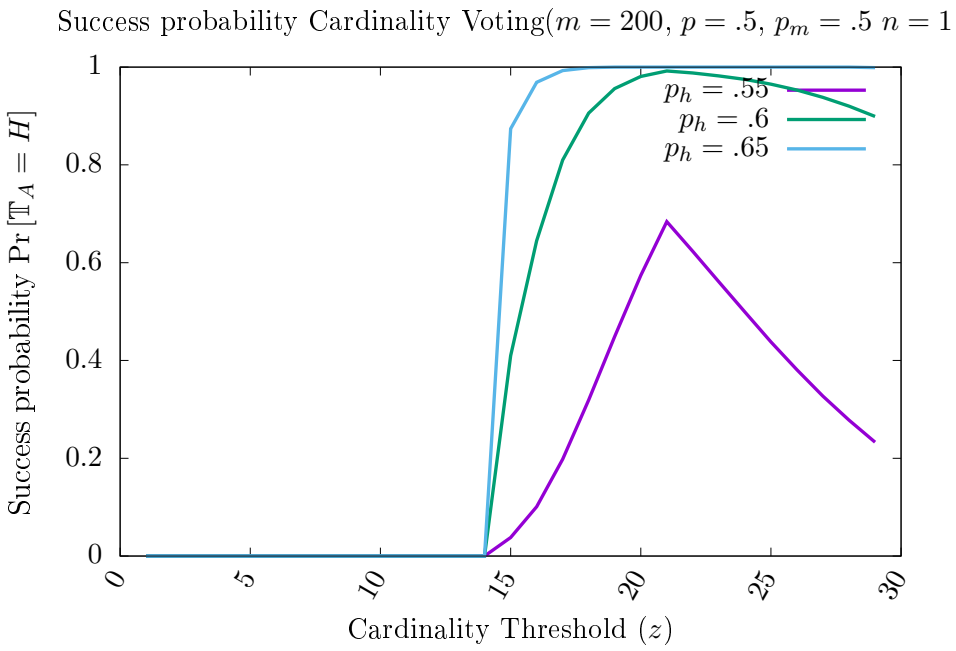

Figure 1.5: The success probability when there is a single voter who follows the cardinal voting strategy. In this figure, the committee size, $k = 21$. The optimal success probability occurs when the threshold $z = k$, even as the accuracy of the voter changes.

or threshold voting.

Proposition 3 (Suboptimality of Threshold voting when $n = 1$)**.** *Consider a k-winner approval voting system with $n = 1$ voter and $m \geq k$ candidates, then any threshold strategy is* **not** *optimal.*

More specifically, when we say a strategy $A \in \mathbb{S}$ is not optimal we mean that there is a non-zero probability event (realization of signals) in which the non-optimal strategy achieves a success probability that is strictly smaller than would be achieved using a different strategy $B \in \mathbb{S}$.

$$\Pr\left[\mathbb{T}_A = H \mid (\mathbf{s}_i)_{i=1}^n\right] < \Pr\left[\mathbb{T}_B = H \mid (\mathbf{s}_i)_{i=1}^n\right], \text{ for } \Pr[(\mathbf{s}_i)_{i=1}^n] > 0. \tag{1.13}$$

In particular, in the proof of Proposition 3 we show Equation (1.13) is true for $n = 1$ and $A = \text{Threshold}, B = \text{Cardinal}$. In other words, we show that for $n = 1$ the threshold strategy gives a strictly lower success probability than the cardinal strategy.

Signal Sharing/Pooling

If voters could credibly (and costlessly) share their private signals, then it is straightforward to show that they effectively act as a single voter.

As in the private signal setting, each voter can calculate the probability that a given producer is honest, conditioned on the received signals. But now, we assume voters can condition on *all* the signals. We calculate the resulting posterior probability in Lemma 3 in Appendix A.1.1.

Proposition 4 shows that when voters share their signal, the optimal strategy (out of *all* possible strategies) is to follow the cardinal voting strategy with threshold $z = k$.

Proposition 4 (Optimality of Cardinal Voting with Shared Signals)**.** *Consider a k-winner approval voting system with $n > 0$ voters, $m \geq k$ candidates and such that voters' private signals are credibly shared. Then the globally optimal strategy is the cardinal strategy with $z = k$ where each voter v_i is ranking based on the shared s_j instead of their private s_{ij}.*

A natural question that follows is, whether cardinal voting persists to be the optimal strategy in the general multi-voter case. We examine this in the next section.

1.6.4. General Case: Multiple Voters

Given we show in the previous Section 1.6.3 that the threshold strategy is already suboptimal for $n = 1$, while the cardinal strategy is in fact optimal for $n = 1$, we focus our attention here on the latter.

In the multi-voter setting ($n > 1$), the optimal cardinal strategy becomes extremely complex and even computing the exact success probability for a fixed strategy is difficult. Despite this, we can formally show that the cardinal strategy that was always optimal with $n = 1$ may become suboptimal with $n > 1$.

Proposition 5 (Suboptimality of Cardinal voting when $n > 1$)**.** *Consider a k-winner Approval Voting system with $n > 1$ voter and $m \geq k$ candidates, then the cardinal strategy can be suboptimal.*

Intuitively, this result occurs because a vote for a candidate can actually *bump* other candidates out of the committee. To dig deeper, consider a situation with two voters (voter 0 and voter 1), where voter 0 has better information than voter 1, (i.e., $\sigma_{0j} \ll \sigma_{1j}$ for all $j \in [m]$). Even if σ_{1j} is large, voter 1's signals convey information (a single voter who had access to the signals $(s_{01}, \ldots, s_{0m})$ *and* $(s_{11}, \ldots, s_{1m})$ would do better than one with access to $(s_{01}, \ldots, s_{0m})$ alone). The problem is that voter 1 can only convey information about their signal through *discrete* votes, and a vote for candidate j may be too strong an endorsement for that candidate given that the signal s_{1j} is only weakly informative.

As an extreme case, consider a situation where voter 0 is perfectly informed (i.e., voter 0 can differentiate between honest and dishonest producers with probability 1), and voter 1 is perfectly uninformed (i.e., from voter 1's perspective, each candidate is honest independently with probability p, in other words $s_{1j} = p$ for all $j \in [m]$). In this case, it should be clear that voter 1 should *not* cast any votes, while voter 0 should cast k votes.

The suboptimality of the cardinal voting strategy persists even if both voters have the same information (i.e., $\epsilon_{0j} = \epsilon_{1j}$ for $j \in [m]$). This is because the *realized* signals can convey different amounts of information. For example, suppose voter 0's sorted signals are $s_{0j_1^0} \geq s_{0j_2^0} \geq \cdots \geq s_{0j_m^0}$ and voter 1's sorted signals are $s_{1j_1^1} \geq \cdots \geq s_{1j_m^1}$. Suppose as well that $s_{0j_k^0} \gg s_{0j_{k+1}^0}$, but $s_{1j_{k-1}^1} \approx s_{1j_k^1} \approx s_{1j_{k+1}^1}$. In this case, voter 0 has high confidence that the committee should consist of the candidates $\left\{j_1^0, \ldots, j_k^0\right\}$, but voter 1 is essentially indifferent between candidates $j_{k-1}^1, j_k^1, j_{k+1}^1$. The cardinality strategy with threshold k would force voter 1 to vote for j_{k-1}^1 and j_k^1, but not j_{k+1}^1, and this vote (based on little information) could displace committee members who would have been elected by voter 0 (whose signals were very informative).

1.6.5. Asymptotic Optimality

So far, we have established via Proposition 3, that the threshold strategy is suboptimal, and via Proposition 5, that the cardinality strategy may be suboptimal. However, our basic numerical study in Section 1.6.2 suggests that as the number of voters increases, this

optimality gap becomes less important.

Theorem 3 (Exponential Convergence)**.** *Let $\mathcal{M}$ denote the set of dishonest producers, and suppose there exists a set of honest producers, $\mathcal{H}$, with $|\mathcal{H}| \geq (1-p)\cdot k$, and a $\delta > 0$ such that $\min_{i\in[n],j\in\mathcal{H}} p_{ij} \geq \max_{i\in[n],j\in\mathcal{M}} p_{ij} + \delta$, where p_{ij} denotes the probability that voter i votes for producer j. Then*

$$\Pr\left[\mathbb{T} = H\right] \geq 1 - 2m^2 e^{-\delta^2 n/2}. \tag{1.14}$$

Theorem 3 shows that as the number of voters, n, tends to infinity, almost *any* reasonable strategy has a very high chance of electing an honest committee. In particular, as long as signals are not completely uninformative, that is, as long as there exists a $\delta > 0$ gap $p_{ij} > p_{ij'} + \delta$ when j is honest and j' is dishonest, the probability of an honest committee tends to one exponentially in the number of voters n (assuming there are enough honest producers to fill the committee). The lower bound on the success probability *decreases* quadratically in the number of block producer candidates m, because if there are too many block producers relative to the number of voters, no single block producer can amass enough votes to make it onto the committee with high probability. As long as there are not too many candidates, however, the exponential dependence on the number of voters dominates the quadratic dependence on the number of producer candidates. Importantly, this result holds across all voting strategy classes, and this leads to the following two corollaries.

Corollary 1. *If $p_h > p_m$, and $m \cdot p \gg k$, then the probability of an honest committee when all voters follow the Threshold strategy converges to 1 as $m, n \to \infty$ (assuming $n \gg m$).*

Corollary 2. *If $p_h > p_m$, and $m \cdot p \gg k$, then the probability of an honest committee when all voters follow the Cardinality strategy converges to 1 as $m, n \to \infty$ (assuming $n \gg m$).*

Remark 1. *Since m is the number of producers, and p is the a priori probability a candidate is honest, the number of honest candidates is distributed as $\mathrm{Bin}(p, m)$, and the expected number of honest candidates is $m \cdot p$. If the number of honest candidates is less than k, then*

there is no way to elect k honest producers. The assumption that $m \cdot p \gg k$ ensures that the probability there are fewer than k honest candidates is small.

Figure 1.6 illustrates the exponential convergence result, assuming each voter follows a (generally suboptimal) Threshold Voting strategy (Definition 5) with $z = p$. The figure shows that as long as the signals are not completely uninformative ($p_h \neq 0.5$), the probability of success rapidly converges to 100%.

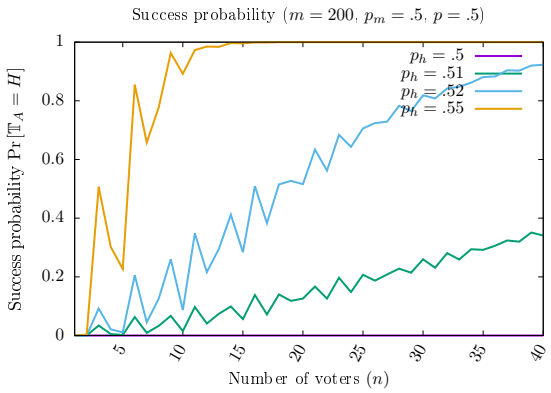

Figure 1.6: Rate of Convergence to Optimality under a suboptimal threshold voting strategy. Note that these are *exact* probabilities, and the jaggedness of the plot comes about from the combinatorial nature of the problem, which depends on the number of voters (which only takes integral values). **Key Takeaway:** The success probability quickly goes to one, as n increases.

Note, convergence to optimality also holds (more trivially) for other asymptotics of interest, such as if the signal informativeness $\frac{p_h - p_m}{\sigma} \to \infty$ or if the prior $p \to 1$. See Appendix A.5 for an illustration.

1.7. Alternatives to approval voting

Since most Proof of Stake systems support delegation, the main difference between Proof of Stake and *Delegated* Proof of Stake comes down to how the block producers are elected.

Although DPoS systems like EOS and TRON elect committees using approval voting, other blockchains that make use of committee-based consensus use alternative methods for electing committees.

This feature is not restricted to DPoS, and PoS systems also use committees to run classical consensus mechanisms.

1.8. Single-vote elections

Most blockchains built using the Cosmos SDK[11]also employ committee-based consensus, where a committee is elected by single-choice voting (not approval voting), and the elected committee runs the Tendermint consensus protocol (which requires a 1/3 fraction of honest participants). This is the voting mechanism used by the Cosmos Hub, Terra, crypto.org, Osmosis, Secret, Oasis, Binance Chain etc. It is also the mechanism used by Tron and the Binance Smart Chain.

In this setting, in stark contrast to approval voting, each voter's optimal strategy is simple: vote for the candidate that is most likely to be honest, *i.e.*, voter i votes for candidate j where s_{ij} is maximized.

Unfortunately, in this setting, we cannot apply Theorem 1, because when voters follow a cardinal-voting strategy the number of votes received by each candidate are *not* independent variables. See Appendix A.6 for a more detailed discussion of the problem.

In this setting, we resort to *simulations* to analyze the effectiveness of different cardinal-voting strategies. The strategy $z = 1$, where voters vote for a single producer, is of particular interest because that is the only strategy available on most chains that use elected committee-based consensus.

Figure 1.7 show how the probability of electing an honest committee differs when voters follow a cardinal voting strategies with different thresholds, z. The key observation is that when voters vote for only a single voter, $z = 1$, the success probability is minimized. In single-vote systems (e.g. Cosmos chains and Tron) voters are forced to follow the cardinal voting with threshold $z = 1$, and this essentially forces them to follow the *worst* cardinal voting strategy.

[11]In addition to the Cosmos Hub, this includes several other popular chains including, Terra, Secret, Osmosis, Binance Chain, Thorchain, crypto.org, axelar and many others.

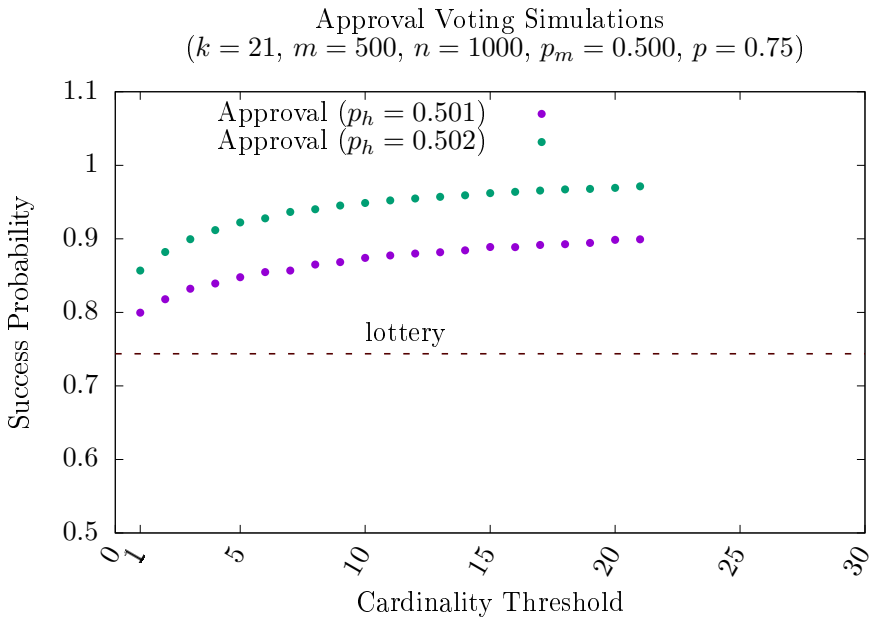

Figure 1.7: Success probabilities with cardinal voting strategies. The key observations is that when the threshold is one (i.e., single-vote elections) the success probability is at its lowest. Voting for a single candidate (which is the only possible strategy on most platforms) is essentially the *worst* strategy.

By contrast, in approval voting systems (e.g. EOS, Telos), even if voters choose their threshold suboptimally, they are essentially guaranteed to have higher success probabilities than in the single-vote setting.

The dashed line shows the probability of electing an honest committee by lottery, when $p = .75$ (i.e., each candidate has a 75% chance of being honest) and the committee size is 21. The line is flat because it does not depend on voters' strategy – the committee is selected at random with no voting at all.

1.8.1. Electing committees by lottery

Algorand employs committee-based consensus, but uses a randomly selected committee to certify each block. In order to ensure that the Algorand protocol never forks, the protocol must *never* elect a dishonest committee.

The analysis of the Algorand protocol proceeds as follows. Suppose some fraction, $p > 2/3$,

of the tokens are held by honest participants (*i.e.*, , an elected committee member is honest with probability p) then if a committee of size k is randomly selected, then the probability the committee is at least 2/3rds honest is

$$\Pr\left[\text{Bin}\, k, p \geq \frac{2}{3}k\right] \tag{1.15}$$

A Chernoff bound (e.g. Dubhashi and Panconesi (2009)[Exercise 1.2]) then shows

$$\Pr\left[\text{Bin}\, k, p \geq \frac{2}{3}k\right] > 1 - e^{-\frac{\left(1-\frac{2}{3p}\right)^2 pk}{2}} \tag{1.16}$$

which decays exponentially as the committee size, k, increases (as long as $p > \frac{2}{3}$). In particular, we can make the failure probability arbitrarily small by choosing the committee size to be large enough.

Remark 2. *A key drawback of the lottery-based election method is that the success probability only converges to 1* as the committee size (k) increases. *By contrast, Theorem 3 shows that for approval voting, the success probability converges to 1* as the number of voters increases. *This is the key reason why voting-based systems can have much smaller committee sizes than lottery-based systems.*

For example, Algorand suggests a target committee size of about 1500, instead of 21 for EOS (Chen and Micali, 2016)[Section 5.1]. If we assume that (at most) 20% of the tokens are ever held by malicious participants, a Chernoff bound gives that the probability of electing a dishonest committee (*i.e.*, a committee with more than 1/3 dishonest members), is bounded by 10^{-12}.

The probability that a dishonest committee is *ever* elected can then be bounded by taking a union bound over all potential elections (e.g. if there is an election every four seconds for the next twenty five years, there will be approximately 200 million elections). Taking a

union bound over the $2 \cdot 10^8$ elections held in the text 25 years, we have the probability of a fork in the next 25 years is at most .5%.

In Algorand, it is very easy to calculate the probability of a dishonest committee, for a given fraction of honest candidates (p), and a given committee size (k).

Intuitively speaking, allowing users to vote, should increase the probability of electing an honest committee, and thus reduce the size of the committee needed to ensure that it reaches the critical (2/3rd) threshold of honest members.

In Figure 1.8, we plot the minimum committee size necessary to achieve a desired failure probability, when the committee is chosen randomly (as in Algorand) or according to an approval vote (as in DPoS). Even when the voters have only minimal information ($p_m = .5, p_h = .51$ and $\sigma = .1$), allowing users to vote for candidates *drastically* reduces the size of the committee necessary to achieve a specific failure bound. Since the committee executes a Byzantine Agreement protocol with communication cost that is quadratic in the committee size, k, minimizing the committee size is critical for performance.

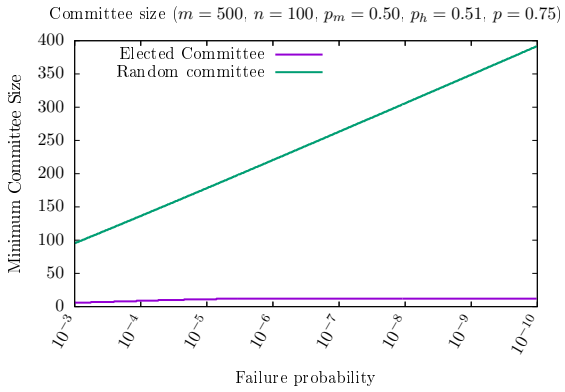

Figure 1.8: The minimum committee size required (y axis) to achieve a failure probability of $10^{-x}, x \in [3, 10]$, when the committee is chosen at random (as in Algorand) vs. when the committee is elected by voters (as in DPoS). **Key takeaway:** DPoS consensus requires much smaller committee sizes for the same level of security.

Note, Figure 1.8 was generated assuming the voters follow the threshold voting strategy with $z = p$. Since we know this strategy is suboptimal, the figure can be viewed as a conservative

estimate. In other words, plotting a similar figure for the optimal election strategy would further reinforce our key insight.

1.9. Discussion

Different objectives: Our results suggest that while voters in committee-based consensus seem to be following intuitive, yet suboptimal strategies, these systems are nonetheless asymptotically robust and efficient from an election perspective. Beyond optimizing to reduce failure rates, however, our model does not deal with other features that voters may care about (a discussion can be found in Appendix A.4). These are outside the scope of this work, but could be of interest for future work.

For instance, one drawback of electing committees as opposed to selecting random committees is that elections seems to lead to stagnation, especially early on in the blockchain life-cycle. EOS represents a rather extreme example: The first 89 million EOS blocks were mined by only 63 distinct producers Zheng et al. (2020b). By comparison, the first 655,000 Bitcoin blocks were mined by more than 275,000 distinct addresses, and the first 8 million Ethereum blocks were mined by over 5000 distinct addresses Zheng et al. (2020a).

A small, static set of block producers reduces decentralization – a core tenet of almost all cryptocurrencies. The idea that there should be a diversity of block producers is core to the open, democratic ideals that spawned much of the blockchain ecosystem, and the idea that there should be turnover in the set of block producers has been formalized in the notion of *chain quality* which is a measure of fairness. Chain quality is a measure of whether (in sufficiently long time windows) the fraction of blocks contributed by each participant is proportional to their hash power or stake Garay et al. (2015).

Chain quality is a different metric by which we could measure different election mechanisms, and this could be an interesting direction for future research.

Different voting schemes: In this work, we focused on lottery-based selection, single-vote mechanisms and approval voting because these are the systems that have currently

been deployed for committee selection.

Many alternative voting systems exist, e.g. ranked-choice voting Nurmi and Palha (2021), and it is an interesting question whether these can outperform approval voting in settings where voter incentives are aligned, but voters are (on the whole) poorly informed.

A separate question is vote-weighting. All current Proof-of-Stake blockchains weight stake *linearly*, but there are alternative weighting mechanisms, the most common being *Quadratic Voting* Posner and Weyl (2014); Lalley and Weyl (2018a). In Quadratic Voting, a voter's vote weight is proportional the *square-root* of their stake, rather than being proportional to the stake itself. Quadratic Voting has been used in the blockchain context (e.g. Gitcoin Grants), but has *not* been used as a method for electing a consensus committee.

It is worth noting that the quadratic weighting mechanism is compatible with many different types of vote-aggregation mechanisms (e.g. single-vote, approval voting, or ranked-choice voting). One problem with quadratic voting mechanisms is that voters are incentivized to split their stake, and so systems that employ quadratic voting need some mechanism to prevent a single voter from splitting their stake, and such a mechanism is difficult to implement in permissionless blockchains.

CHAPTER 2

Nash equilibria for quadratic voting in blockchain governance

ABSTRACT

We investigate a blockchain governance model where a group of n voters must choose between two collective alternatives. As opposed to the usual voting system (one person – one vote), we propose a voting system where each agent buys votes in favor of their preferred alternative, paying the m-th root of the number of votes purchased. Its novelty relies on allowing voters to express the intensity of their preferences in a simple manner. We provide a rigorous comparison of the utilitarian welfare between Regular Voting ($m = 1$) and Quadratic Voting ($m = 2$). We present closed form equilibrium solutions to the 2 voters and 3 voters games. In addition to characterizing the nature of equilibria, one of our main results demonstrates that the normalized utilitarian welfare of the mechanisms tends to one as the population size becomes large.

Keywords: Quadratic Voting, Collective Decisions, Blockchain Governance, Blockchain Economics, Bayes-Nash equilibrium.

2.1. Introduction

Decentralized blockchain projects require decentralized governance, and most projects have incorporated some form of stake-weighted governance. Layer-1 blockchains, like Tezos Tezos (2021), which use stake-weighted voting to determine system upgrades. DeFi projects like Curve Curve (2021), Uniswap Uniswap (2021) and Maker MakerDao (2021a) use stake-weighted voting to determine system parameters. Votes can be binary (e.g. should a token like WBTC be allowed as a collateral type for minting DAI tokens? MakerDao (2021c)) or multiple choice (e.g. should the system surplus buffer be increased? With 5 possible options for the amount and speed of increase MakerDao (2021b)). In these situations, voter interests are aligned – all voters are incentivized to set the surplus buffer to the size that maximizes the stability of the system. The issue is that voters have limited information about which option will actually provide the most benefit to the system.

This scenario – where voters' have common interest but imperfect information – differs significantly from most models in the voting literature, where voters have heterogeneous

incentives, but perfect information about their payouts.

Our model is more akin to the crowdsourcing literature, where votes are used to capture "the wisdom of the crowd." In the blockchain setting, essentially every governance system requires voters to stake tokens as a form of sybil resistance. It is an open question, however, how to design a mechanism to aggregate these votes in order to maximize the utilitarian welfare. The simplest mechanism aggregates user votes and weights them according to each user's stake. One widely-studied alternative mechanism is *quadratic voting* Lalley and Weyl (2018a,b); Posner and Weyl (2014, 2015); Quarfoot et al. (2017), where user votes are weighted according to the square-root of their stake. When voters have perfect information (but diverse incentives), quadratic voting has been shown to be optimal Lalley and Weyl (2018a). In this work, we introduce the study of quadratic voting in the situation where voters have imperfect information, but aligned incentives.

2.2. Related Work

One of the known drawbacks of traditional one-person-one-vote (1p1v) or approval voting mechanisms is that they do not allow voters to signal the *strength* of their preference. Qualitative Voting Hortala-Vallve (2012) considers a setting where voters are choosing between N alternatives, and they have a fixed voting budget of V that can be allocated between the N alternatives. Voters are heterogeneous, but have *perfect* information about their own payoffs.

An alternative method for allowing voters to express the strength of their preference by "storing" their votes on issues for which they have weak preferences, and then using those votes later on issues where their preferences are stronger Casella (2005). Storable voting only makes sense when voters are asked to vote on a sequence of propositions, whereas our model focuses on a single-shot vote. Like most of the voting literature the Storable votes model assumes that voters know their current preferences at the time they cast a vote. Their model does implicitly incorporate imperfect information, because a voter who stores a vote during round i does not (yet) know their preferences over the issues in round $j > i$.

Other models have incorporated a cost to voting Matveenko et al. (2021), but these works also assume that voters have *perfect* information about their own preferences at the time they choose to participate.

2.3. Model

2.3.1. Motivation

Consider a binary (± 1) collective-decision problem with n voters. Each voter has a value $u_i > 0$ that determines their utility towards the decision and $s_i = \pm 1$ that determines their preference, i.e., $s_i = 1$ indicates affinity towards outcome $+1$ and $s_i = -1$ towards outcome -1.

In tradition one-person-one-vote (1p1v) systems, the outcome will be $\operatorname{sgn}\left(\sum_i s_i\right)$, and the overall welfare of the system will be $\sum_i r_i$, where

$$r_i = \begin{cases} u_i \text{ if } \operatorname{sgn}(s_i) = \operatorname{sgn}\left(\sum_i s_i\right) \\ 0 \text{ otherwise} \end{cases} \tag{2.1}$$

Although the one-person-one-vote mechanism is widely used, it cannot maximize aggregate welfare since voters have no way of signaling the magnitude of their preference (u_i).

To allow voters to signal the magnitude of their preference, we can allow voters to purchase a number of votes $v_i \in \mathbb{R}_{\geq 0}$, at a cost of $c(v_i)$. If the revenue from the sale of these votes is redistributed to the voters, the *aggregate* utility is independent of the redistribution mechanism, and the aggregate utility is $\sum_i r_i$

$$r_i = \begin{cases} u_i \text{ if } \operatorname{sgn}(s_i) = \operatorname{sgn}\left(\sum_i s_i v_i\right) \\ 0 \text{ otherwise} \end{cases} \tag{2.2}$$

When $c(v) \stackrel{\text{def}}{=} v^2$, we obtain *Quadratic Voting*, which can be shown to be the unique mechanism for optimizing aggregate welfare in this model Lalley and Weyl (2018a).

Quadratic voting can be optimal for funding public goods Buterin et al. (2019). In this model, citizens, with perfect information, but heterogenous preferences contribute money towards in the Quadratic Funding mechanism, proposition p receives a funding level $\left(\sum_i \sqrt{c_i^p}\right)^2$, where c_i^p is the amount of funding contributed towards proposition p. One issue with this mechanism is that it may incur a budget deficit (i.e., $\sum_p \left(\sqrt{c_i^p}\right)^2 > \sum_p \sum_i c_i^p$). In this case the deficit needs to be filled through some other mechanism (e.g. taxation or charitable donation). This quadratic funding mechanism is currently implemented in the Gitcoin Grants program Gitcoin (2021a), where individual users' contributions to public goods are matched quadratically by philanthropic donors. As of Q4 2021, Gitcoin Grants has distributed over $40M USD in funding to community projects Gitcoin (2021b).

Quadratic voting has also been implemented in blockchain governance, e.g. in the Panther protocol Panther.io (2021).

2.3.2. Voting with Imperfect Information

Voters are asked to make a choice between two alternatives, one of which is "good" while the other is "bad". The voters, however, have imperfect information, and voter i can identify the good option with probability p_i. If the good option is chosen, voter i receives a payout of $u_i > 0$, and if the bad option is chosen, all voters receive payout of 0. In case of a tie the bad option is chosen. We assume that the p_i and u_i are publicly known.

Concretely, assume that voter i receives a signal $p_i \in [0, 1]$ (see Appendix B.2 for the distribution). Now, suppose each voter is allowed to *buy* votes. Each voter i chooses a number of votes $v_i \in \mathbb{Z}_{\geq 1}$ to buy, and pays $f(v_i)$ for these where $f(x) = x^m$ for $m \in \mathbb{Z}_{\geq 1}$ and $f(x) = 0$ for $m = 0$. Each voter receives $\frac{1}{n-1}$ of the revenues paid in by all other voters and none of the revenue collected directly from him
Summary of the game environment:

- Voters $i = 1, \ldots, n$.
- Binary decision with a good option and a bad option. Voters are aligned in their

preference with respect to the binary decision.

- Voter i has probability p_i of choosing the good option. His reward is $u_i > 0$ if the good option is chosen and 0 if the "bad" is chosen.
- Tie break rule: in case of a tie the bad option is chosen.
- The voters' probabilities $p_1, \ldots, p_n$ are independent.
- p_i, u_i are publicly known.
- Voters are asked to submit votes $v_1, \ldots, v_n$ with strategy space $v_i \in \{1, 2, \ldots\}$ - no abstaining. Each voter pays $f(v_i)$ where $f(x) = x^m$ $(m \geq 1)$.

For each voter i, we define $s_i \in \{\pm 1\}$ to be the realization of the direction of voting. For good; $s_i = 1$, and for bad; $s_i = -1$.

Notation: We will denote the strategy (votes) vector as $\vec{v} = (v_1, \ldots, v_n), v_i \in \mathbb{Z}_{\geq 1}$, the signals vector as $\vec{p} = (p_1, \ldots, p_n), p_i \in [0, 1]$ and the votes directions vector as $\vec{s} = (s_1, \ldots, s_n), s_i \in \{\pm 1\}$. Also $\vec{1}_n \in \mathbb{Z}^n$ will denote the 1-vector of size n.

Definition 7. *With the above notation, the* ***probability of winning the game*** *or the* ***winning probability*** *is*

$$p\left(\vec{v}\right) \stackrel{\text{def}}{=} \Pr\left[\sum_{i=1}^{n} s_i v_i > 0\right] \tag{2.3}$$

The expected payoff to voter i is:

$$U_i = u_i \cdot p\left(\vec{v}\right) - f(v_i) + \frac{1}{n-1} \sum_{j \neq i} f(v_j) \tag{2.4}$$

The last term in Equation 2.4 represents a redistribution transfer in which each voter receives $n-1$ of the revenues paid in by all other voters and none of the revenue collected directly from him; however, none of the results below depend on this particular redistributive scheme.[1]

[1] Any rule in which all revenues are redistributed and each voter receives the same share of the revenues

Remark 3. *Note that this scheme is budget balanced as*

$$\sum_{i=1}^{n}\left(f(v_i)-\frac{1}{n-1}\sum_{j\neq i}f(v_j)\right)=\sum_{i=1}^{n}f(v_i)-\frac{n-1}{n-1}\sum_{j=1}^{n}f(v_j)=0$$

Voters are expected payoff maximizers and thus voter i chooses his v_i to maximize

$$u_i\cdot p\left(\vec{v}\right)-f(v_i) \tag{2.5}$$

Let $U=\sum_{i=1}^{n}u_i$, the expected welfare of the mechanism is

$$W\left(\vec{v}\right)=\sum_{i=1}^{n}U_i=U\cdot p(\vec{v}) \tag{2.6}$$

Definition 8. *A voting mechanism is a choice of $m\geq 1$ that determines the vote cost function $f(v_i)$. We give names to the following values of $m=1,2$:*

- *Regular Voting (RV): $m=1,\ f(v)=v$*
- *Quadratic Voting (QV): $m=2,\ f(v)=v^2$*

We wish to compare the different voting mechanisms in terms of the overall net utility for all voters and find the one that maximizes it. This is the same as asking which voting mechanism maximizes the probability of winning the game.

Question 1. *For what value of $m\geq 0$ is $p\left(\vec{v}\right)$ maximized?*

Each game might have multiple Nash Equilibria. The problem with phrasing the question this way, is that we might get a different value of this probability for different Nash Equilibrium of the game. Moreover, since this probability is dependent on u_i, p_i. It might be the case that for different values of u_i, p_i this probability is maximized for different values of m. This leads us to the following definition:

he pays suffices to establish essentially all results that follow.

Definition 9. *Denote* $\left\{NE_1^{(1)}, \ldots, NE_k^{(1)}\right\}$ *the set of Nash equilibrium strategies of the game under voting mechanism* m_1 *and* $\left\{NE_1^{(2)}, \ldots, NE_l^{(2)}\right\}$ *under voting mechanism* m_2 *(*k, l *non-negative integers). We say that a voting mechanism* m_1 *is* ***better*** *than* m_2 *if for every* u_i, p_i*, it holds that either* $\left\{W\left(NE_i^{(1)}\right)\right\}_i = \left\{W\left(NE_j^{(2)}\right)\right\}_j$ *or* $\min_{NE_i^{(1)}} W\left(NE_i^{(1)}\right) \geq \max_{NE_j^{(2)}} W\left(NE_j^{(2)}\right)$ *and if for a range of values* u_i, p_i *it holds that the equilibria are not identical and the above inequality is strict.*

2.4. Analysis

2.4.1. Preliminaries

Even the $n = 3$ case is harder to solve than the simple $n = 2$ case and requires some key observations. We start from analyzing the one-person-one-vote strategy $v_i = 1$. The probability of winning in this game will turn out to have great importance in our results.

Proposition 6. *In a one-person-one-vote game (1p1v)* $v_i \in \{1\}$*, the probability of winning is*

$$p\left(\vec{1}_n\right) = \Pr\left[\sum_{i=1}^{n} s_i \cdot 1 > 0\right] = \Pr\left[X > \frac{n}{2}\right], \tag{2.7}$$

where $X \sim \text{PoiBin}(p_1, \ldots, p_n)$*.*

All proofs are in the appendix B.1. We will now provide the preliminary definitions needed to prove the main tool for analyzing the game.

Definition 10. *We define* $F_{\vec{v}}$ *to be the set of all subsets of* $[n]$ *such that the sum of votes of voters indexed by it, is strictly larger than the sum of votes of voters indexed by the complement set:*

$$F_{\vec{v}} \stackrel{\text{def}}{=} \left\{A \subseteq [n] \;\middle|\; \sum_{i \in A} v_i > \sum_{i \in A^c} v_i\right\} \tag{2.8}$$

This definition is motivated by the following observation:

Proposition 7 (Success probability)**.**

$$\begin{aligned}\Pr\left[\sum_{i=1}^{n} s_i v_i > 0\right] &= \Pr\left[\{i \mid s_i = 1\} \in F_{\vec{v}}\right] \\ &= \sum_{A \in F_{\vec{v}}} \prod_{i \in A} p_i \prod_{j \in A^c} (1 - p_j),\end{aligned} \tag{2.9}$$

Remark 4. *Note the similarity of the expression of Equation 2.9 to that of the probability of a Poisson Binomial with k trials. Let* $X \sim \text{PoiBin}(p_1, \ldots, p_n)$ *then*

$$\Pr[X = k] = \sum_{A \in F_k} \prod_{i \in A} p_i \prod_{j \in A^c} (1 - p_j), \tag{2.10}$$

where F_k *is the set of all subsets of k integers that can be selected from* $[n]$*.*
In this analysis, we are required to deal with a more general ***weighted Poisson binomial random variable*** *since it can be viewed as if each* s_i *is weighted with weight* v_i*. Let's see this in practice, Proposition 7 generalizes the result of Proposition 6 to any integral strategy space* $\vec{v} \in \mathbb{Z}_{\geq 0}$ *and thus gives a different proof to Proposition 6 in Appendix B.1.1.*

Proposition 7 tells us that voter i's goal is to maximize:

$$\max_{v_i} u_i \sum_{A \in F_{\vec{v}}} \prod_{i \in A} p_i \prod_{j \in A^c} (1 - p_j) - f(v_i) \tag{2.11}$$

The key observation here is that the success probability depends on $F_{\vec{v}}$ and many different voting strategies $\vec{v}$ yield the same $F_{\vec{v}}$. In fact, when the number of voters is small, we can enumerate all possible realizations of $F_{\vec{v}}$.

Let $\mathcal{F}_n$ denote the set $F_{\vec{v}}$ for all possible (sorted) realizations of the vote-weights $\vec{v}$. In other words

$$\mathcal{F}_n \stackrel{\text{def}}{=} \{F_{\vec{v}} \mid \vec{v} \in (\mathbb{Z}_{\geq 1})^n \text{ and } v_1 \geq v_2 \geq \cdot \geq v_n\} \tag{2.12}$$

Example 1.

$$\mathcal{F}_3 = \{\{\{1,2,3\},\{1,2\},\{1,3\}\},$$
$$\{\{1,2,3\},\{1,2\},\{1,3\},\{2,3\}\},$$
$$\{\{1,2,3\},\{1,2\},\{1,3\},\{1\}\}\}$$

We can use $\mathcal{F}_3$ to calculate all possible success probabilities in the 3 players game. By abuse of notation we denote $F_{\vec{v}}^{-1}$ to be the set of strategy vectors $\vec{v}$ that result in the set $F_{\vec{v}}$.

Example 2. *Assume* $v_1 \geq v_2 \geq \cdot \geq v_n$.

$F_{\vec{v}}$	$p(\vec{v})$	$F_{\vec{v}}^{-1} \subseteq (\mathbb{Z}_{\geq 1})^n$
{{1, 2, 3}, {1, 2}, {1, 3}}	$p_1p_2 + p_1p_3 - p_1p_2p_3$	$v_1 = v_2 + v_3$
{{1, 2, 3}, {1, 2}, {1, 3}, {2, 3} }	$p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3$	$v_j < v_{j+1} + v_{j+2} \forall j$
{{1, 2, 3}, {1, 2}, {1, 3}, {1}}	p_1	$v_1 > v_2 + v_3$

Table 2.1: 3 Players game variables summary

Permuting the indices $\{1,2,3\}$ gives the variables for all other assortments of the v_i. From here on we will assume that $\forall i : u_i = u$. It facilitates the analysis and doesn't change any of the key insights. We may also assume that $p_1 > p_2 > \cdots > p_n \geq 0.5$ since if a voter receives a signal $p_i < 0.5$ he votes for the other option with probability $1 - p_i \geq 0.5$ and we order the voters by the signals.

2.4.2. Two Players Game

We start by analyzing the simple case of only two voters.

2 Player game presentation:

v_1 / v_2	**1**	**2**
1	$up_1p_2 - 1, up_1p_2 - 1$	$up_2 - 1, up_2 - 2^m$
2	$up_1 - 2^m, up_1 - 1$	$up_1p_2 - 2^m, up_1p_2 - 2^m$

Table 2.2: 2 Player game normal form for $v_1, v_2 \leq 2$

Proposition 8. *Assume that $n = 2$, then the following is an exhaustive list of the possible Nash Equilibria of the game:*

Nash Equilibrium	Welfare	Necessary and Sufficient Condition
$(1,1)$	Up_1p_2	$c_1 \leq 2^m - 1$ and $c_2 \leq 2^m - 1$
$(2,1)$	Up_1	$c_1 \geq 2^m - 1$
$(1,2)$	Up_2	$c_2 \geq 2^m - 1$

where $c_1 = up_1(1 - p_2)$ and $c_2 = up_2(1 - p_1)$ and it holds that $c_1 \geq c_2$.

Corollary 3. *For $n = 2$, neither RV or QV is better.*

For $n = 2$ it is not true that RV is better than QV. It is only true in the region $c_1 < 3$ or $[c_1 \geq 3$ and $(c_2 < 1$ or $c_2 > 3)]$. Figure 2.1 captures the voting mechanism RV and QV welfare as function of c_1, c_2 and comparing them by regions.

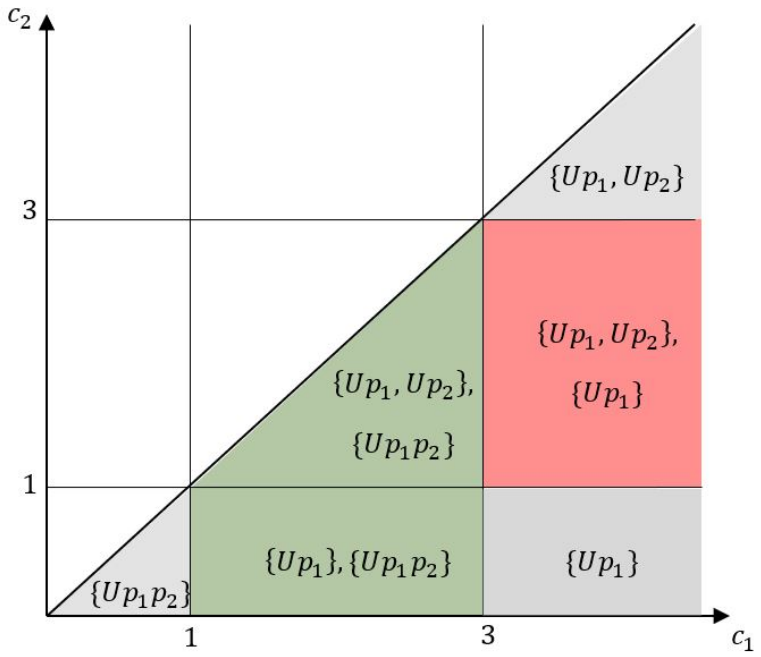

Figure 2.1: 2 players game welfare for RV and QV. Green region is RV better than QV with strict inequality, Red is where it fails. Grey is where the mechanisms have the same N.E. set. The terms for each region are $\left\{W\left(\mathrm{NE}_i^{(\mathrm{RV})}\right)\right\}_i, \left\{W\left(\mathrm{NE}_j^{(\mathrm{QV})}\right)\right\}_j$.

2.4.3. Three Players Game

Denote $P_{\bar{1}23} \stackrel{\text{def}}{=} p_2 p_3 (1-p_1), P_{1\bar{2}3} \stackrel{\text{def}}{=} p_1 p_3 (1-p_2), P_{12\bar{3}} \stackrel{\text{def}}{=} p_1 p_2 (1-p_3)$,$P_3 \stackrel{\text{def}}{=} p(\vec{1}_3)$.

Using Table 2.1 we can present the 3 Players Game Normal Form:

v_2 / v_3	**1**	**2**
1	$uP_3 - 1, uP_3 - 1, uP_3 - 1$	$u\left(P_3 - P_{12\bar{3}}\right) - 1, u\left(P_3 - P_{12\bar{3}}\right) - 1, u\left(P_3 - P_{12\bar{3}}\right) - 2^m$
2	$u\left(P_3 - P_{1\bar{2}3}\right) - 1, u\left(P_3 - P_{1\bar{2}3}\right) - 2^m, u\left(P_3 - P_{1\bar{2}3}\right) - 1$	$uP_3 - 1, uP_3 - 2^m, uP_3 - 2^m$

Table 2.3: 3 Player game normal form for $v_2, v_3 \leq 2, v_1 = 1$

v_2 / v_3	**1**	**2**
1	$u\left(P_3 - P_{\bar{1}23}\right) - 2^m, u\left(P_3 - P_{\bar{1}23}\right) - 1, u\left(P_3 - P_{\bar{1}23}\right) - 1$	$uP_3 - 2^m, uP_3 - 1, uP_3 - 2^m$
2	$uP_3 - 2^m, uP_3 - 2^m, uP_3 - 1$	$uP_3 - 2^m, uP_3 - 2^m, uP_3 - 2^m$

Table 2.4: 3 Player game normal form for $v_2, v_3 \leq 2, v_1 = 2$

Proposition 9. *Assume that $n = 3$, then the following describes all possible options of Nash Equilibria of the game:*

Nash Equilibrium	Net Utility	Necessary and Sufficient Condition
$(1,1,1)$	UP_3	$c_4 \leq 3^m - 1$
$(3,1,1)$	Up_1	$c_4 \geq 3^m - 1$
$(1,2,2)$	UP_3	$c_4 \leq 5^m - 1, c_2 \geq 2^m - 1, c_3 \geq 2^m - 1$
$(2,2,1)$	UP_3	$c_4 \leq 4^m - 2^m, c_1 \geq 2^m - 1, c_2 \geq 2^m - 1$
$(2,1,2)$	UP_3	$c_4 \leq 4^m - 2^m, c_1 \geq 2^m - 1, c_3 \geq 2^m - 1$

where $c_1 = uP_{\bar{1}23}, c_2 = uP_{1\bar{2}3}, c_3 = uP_{12\bar{3}}, c_4 = u(p_1 - P_3)$

Corollary 4. *For $n = 3$, only if $p_1 > P_3$ then RV is better than QV. Otherwise, they always yield the same unique welfare UP_3.*

2.4.4. General Case

Proposition 10. *Let $1 > p_1 > p_2 > \cdots > p_n \geq 0.5$ then*

$$\lim_{n\to\infty} p(\vec{1}_n) = 1$$

Since $p(\vec{v}) \leq 1$ always then when n is large, all voting mechanisms are essentially the same. This subsection is dedicated to making this statement precise.

Proposition 11. *Let v satisfy $v = \arg\max_{1<v\leq n} \left[up_{(v,1,\ldots,1)} - v^m\right]$. The strategy $\vec{v} = \vec{1}_n$ is a N.E. if and only if*

$$u(p_{(v,1,\ldots,1)} - p_{\vec{1}_n}) \leq v^m - 1 \tag{2.13}$$

Theorem 4. *Let $\bar{p} = \frac{1}{n}\sum_i^n p_i$ and assume that $u(p_{(v,1,\ldots,1)} - p_{\vec{1}_n}) \leq v^m - 1$ with $v = \arg\max_{1<v\leq n} \left[up_{(v,1,\ldots,1)} - v^m\right]$, then*

$$\max_{\vec{v}} p_{\vec{v}} \geq 1 - e^{-2(\bar{p}-1/2)^2 n} \tag{2.14}$$

Corollary 5. *When $n \to \infty$, RV and QV yield the same probability of winning in the u, p_i, n dimensional space defined by*

$$u(p_{(v,1,\ldots,1)} - p_{\vec{1}_n}) \leq v^2 - 1 \tag{2.15}$$

where $v = \underset{1<v\leq n}{\arg\max} \left[up_{(v,1,\ldots,1)} - v^2 \right]$.

2.5. Discussion

Our results suggest that while voters reach a different set of Nash Equilibria in RV versus QV, these systems are nonetheless asymptotically the same with respect to the utilitarian objective. However, for small committees RV is better than QV. This follows from the fact that QV does not allow a single knowledgeable user to express their dominance. For larger committees, the wisdom of the crowd is so strong that no individual is more knowledgeable than the crowd.

Extant literature says the QV is better when all voters have equal information. However, our work shows that when voters are not perfectly informed, QV can actually be worse.

In chapter 1 we discussed different voting mechanisms and in this chapter we discussed voting weighting mechanisms. As a future direction, it would be interesting to combine the two and analyze a model where both weighting and the mechanism are not traditional, e.g. approval-quadratic voting.

APPENDIX A

Chapter 1 Appendix

A.1. Proofs

A.1.1. Posterior probabilities

Lemma 2. *Let c be a producer with a priori probability to be honest p, suppose a voter receives a signal*

$$s^* = \begin{cases} p_h + \epsilon \text{ if Producer } j \text{ is honest} \\ p_m + \epsilon \text{ if Producer } j \text{ is malicious} \end{cases}$$

with $\epsilon \sim \mathcal{N}(0, \sigma^2)$, then

(i) $$\Pr\left[c = H \mid s^*\right] = \frac{1}{1 + \frac{1-p}{p} e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}}}$$

(ii) $$f_{s|H}(x) = \frac{\sigma}{\sqrt{2\pi}x(1-x)(p_h - p_m)} \cdot e^{-\left(\frac{(p_h-p_m)^2+2\sigma^2 \log\left(\frac{p(1-x)}{(1-p)x}\right)}{2\sqrt{2}\sigma(p_h-p_m)}\right)^2}$$

One useful implication of Lemma 2 is that we can interchangeably talk about the voters considering the probabilities of producers to be honest conditioned on their signals instead of the original signals. Meaning, the model facilitates comparisons with Bayesian posteriors. In particular conditioned on s^*_{ij}, Lemma 2 shows that the probability that producer c_j is honest is

$$s_{ij} \stackrel{\text{def}}{=} \Pr[c_j = H | s^*_{ij}] = \frac{1}{1 + \frac{1-p_j}{p_j} e^{\frac{(s^*_{ij}-p_h)^2-(s^*_{ij}-p_m)^2}{2{\sigma_{ij}}^2}}}. \tag{A.1}$$

Proof of Lemma 2. Part (i): Let $f_\epsilon(x)$ denote the PDF of ϵ. Bayes' Theorem says

$$\begin{aligned}
\Pr[c = H \mid s^*] &= \frac{\Pr[c = H]\Pr[s^* \mid c = H]}{\Pr[s^*]} && \text{(A.2)}\\
&= \frac{\Pr[c = H]\Pr[s^* \mid c = H]}{(\Pr[c = H]\Pr[s^* \mid c = H] + \Pr[c = M]\Pr[s^* \mid c = M])} && \text{(A.3)}\\
&= \frac{1}{1 + \frac{\Pr[c=M]}{\Pr[c=H]}\frac{\Pr[s^* \mid c=M]}{\Pr[s^* \mid c=H]}} && \text{(A.4)}\\
&= \frac{1}{1 + \frac{1-p}{p}\frac{f_\epsilon(s^*-p_m)}{f_\epsilon(s^*-p_h)}} && \text{(A.5)}\\
& && \text{(A.6)}
\end{aligned}$$

Now,

$$f_\epsilon(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}. \tag{A.7}$$

Thus

$$\Pr[c = H \mid s^*] = \frac{1}{1 + \frac{1-p}{p} e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}}} \tag{A.8}$$

Part (ii): Let

$$h(s^*) \stackrel{\text{def}}{=} \frac{1}{1 + \frac{1-p}{p} e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}}} \tag{A.9}$$

then $s = h(s^*)$, by Lemma 2.

Since $h(\cdot)$ is strictly increasing, the cumulative density function satisfies

$$F_s(x) = F_{s^*}\left(h^{-1}(x)\right) \tag{A.10}$$

and the conditional cumulative distribution function satisfies

$$F_{s|H}(x) = F_{s^*|H}\left(h^{-1}(x)\right) \tag{A.11}$$

Thus it suffices to calculate $h^{-1}(\cdot)$.

$$
\begin{aligned}
q &= \frac{1}{1+\frac{1-p}{p}e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}}} \\
&\Updownarrow \\
\frac{1}{q} &= 1+\frac{1-p}{p}e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}} \\
&\Updownarrow \\
\frac{p}{1-p}\left(\frac{1}{q}-1\right) &= e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}} \\
&\Updownarrow \\
\frac{p(1-q)}{(1-p)q} &= e^{\frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2}} \\
&\Updownarrow \\
\log\left(\frac{p(1-q)}{(1-p)q}\right) &= \frac{(s^*-p_h)^2-(s^*-p_m)^2}{2\sigma^2} \\
&\Updownarrow \\
2\sigma^2\log\left(\frac{p(1-q)}{(1-p)q}\right) &= (s^*-p_h)^2-(s^*-p_m)^2 \\
&\Updownarrow \\
2\sigma^2\log\left(\frac{p(1-q)}{(1-p)q}\right) &= 2(p_m-p_h)s^*+p_h^2-p_m^2 \\
&\Updownarrow \\
s^* &= \frac{p_h^2-p_m^2-2\sigma^2\log\left(\frac{p(1-q)}{(1-p)q}\right)}{2(p_h-p_m)}
\end{aligned}
$$

Thus

$$
h^{-1}(q) = \frac{p_h^2-p_m^2-2\sigma^2\log\left(\frac{p(1-q)}{(1-p)q}\right)}{2(p_h-p_m)} \tag{A.12}
$$

Since $F_{s^*|H}(x) = F_\epsilon(s^* - p_h)$, and

$$f_\epsilon(x) \stackrel{\text{def}}{=} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}, \tag{A.13}$$

We have

$$\begin{aligned} f_{s|H}(x) &= \frac{df}{dx} F_{s^*|H}(h^{-1}(x) - p_h) \\ &= f_{s^*|H}(h^{-1}(x) - p_h) \cdot \frac{df}{dx} h^{-1}(x) \end{aligned} \tag{A.14}$$

Now

$$\begin{aligned} f_{s^*|H}(h^{-1}(x)) &= f_\epsilon\left(h^{-1}(x) - p_h\right) \\ &= \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(h^{-1}(x) - p_h\right)^2}{2\sigma^2}} \\ &= \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(\frac{-(p_h - p_m)^2 - 2\sigma^2 \log\left(\frac{p(1-x)}{(1-p)x}\right)}{2(p_h - p_m)}\right)^2}{2\sigma^2}} \\ &= \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{(p_h - p_m)^2 + 2\sigma^2 \log\left(\frac{p(1-x)}{(1-p)x}\right)}{2\sqrt{2}\sigma(p_h - p_m)}\right)^2} \end{aligned} \tag{A.15}$$

and

$$\begin{aligned} \frac{d}{dx} h^{-1}(x) &= \frac{d}{dx} \frac{p_h^2 - p_m^2 - 2\sigma^2 \log\left(\frac{p(1-x)}{(1-p)x}\right)}{2(p_h - p_m)} \\ &= -\frac{\sigma^2}{p_h - p_m} \frac{d}{dx} \log\left(\frac{p(1-x)}{(1-p)x}\right) \\ &= \frac{\sigma^2}{p_h - p_m} \frac{1}{x(1-x)} \end{aligned} \tag{A.16}$$

Thus by Equations A.14, A.15 and A.16

$$f_{s|H}(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{(p_h-p_m)^2+2\sigma^2\log\left(\frac{p(1-x)}{(1-p)x}\right)}{2\sqrt{2}\sigma(p_h-p_m)}\right)^2} \cdot \frac{-\sigma^2}{x(x-1)(p_h-p_m)}$$
$$= \frac{\sigma}{\sqrt{2\pi}x(1-x)(p_h-p_m)} \cdot e^{-\left(\frac{(p_h-p_m)^2+2\sigma^2\log\left(\frac{p(1-x)}{(1-p)x}\right)}{2\sqrt{2}\sigma(p_h-p_m)}\right)^2} \tag{A.17}$$

Similarly

$$f_{s|M}(x) = \frac{\sigma}{\sqrt{2\pi}x(1-x)(p_h-p_m)} \cdot e^{-\left(\frac{(p_h-p_m)^2-2\sigma^2\log\left(\frac{p(1-x)}{(1-p)x}\right)}{2\sqrt{2}\sigma(p_h-p_m)}\right)^2} \tag{A.18}$$

□

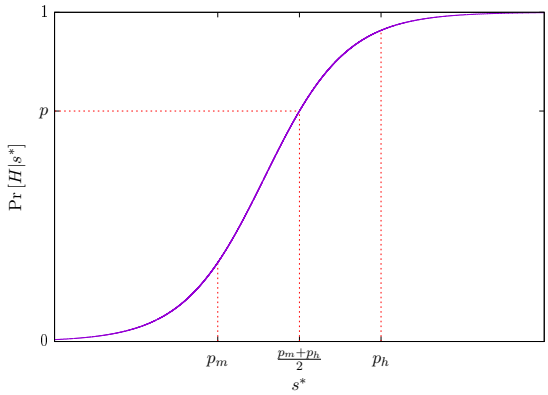

Figure A.1: The probability a producer is honest, conditioned on a single voter's received signal, s^*

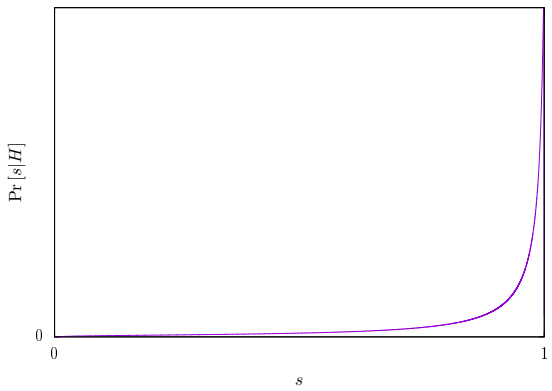

Figure A.2: The distribution of the posterior probability, s, conditioned for an honest producer.

Lemma 3. *Let c_j be a producer with a priori probability to be honest p_j, suppose voter v_i receives a signal (s^*_{ij}) about producers c_j honesty as in equation (1.2).*

$$s^*_{ij} = \begin{cases} p_h + \epsilon_{ij} \text{ if Producer } j \text{ is honest} \\ p_m + \epsilon_{ij} \text{ if Producer } j \text{ is malicious} \end{cases}$$

with $\epsilon_{ij} \sim \mathcal{N}(0, \sigma^2_{ij})$, then

$$\Pr\left[c_j = H \mid s^*_{1j}, \ldots, s^*_{nj}\right] = \frac{1}{1 + \frac{1-p_j}{p_j} e^{\frac{\sum_{i=1}^{n}\left[(s^*_{ij}-p_h)^2-(s^*_{ij}-p_m)^2\right]}{2\sigma^2_{ij}}}}.$$

Proof of Lemma 3.

$$\begin{aligned}
\Pr\left[c_j = H \;\middle|\; s^*_{1j}, \ldots, s^*_{nj}\right] &= \frac{\Pr\left[c_j = H\right] \Pr\left[s^*_{1j}, \ldots, s^*_{nj} \;\middle|\; c_j = H\right]}{\Pr\left[s^*_{1j}, \ldots, s^*_{nj}\right]} \\
&= \frac{\Pr\left[c_j=H\right] \Pr\left[s^*_{1j},\ldots,s^*_{nj} \;\middle|\; c_j=H\right]}{\left(\Pr\left[c_j=H\right] \Pr\left[s^*_{1j},\ldots,s^*_{nj} \;\middle|\; c_j=H\right] + \Pr\left[c_j=M\right] \Pr\left[s^*_{1j},\ldots,s^*_{nj} \;\middle|\; c_j=M\right]\right)} \\
&= \frac{1}{1 + \frac{\Pr[c_j=M]}{\Pr[c_j=H]} \frac{\Pr\left[\{s^*_{1j},\ldots,s^*_{nj} \;\middle|\; c_j=M\right]}{\Pr\left[\{s^*_{1j},\ldots,s^*_{nj} \;\middle|\; c_j=H\right]}} \qquad \text{(A.19)} \\
&= \frac{1}{1 + \frac{\Pr[c_j=M]}{\Pr[c_j=H]} \frac{\prod_{i=1}^n \Pr\left[s^*_{ij} \;\middle|\; c_j=M\right]}{\prod_{i=1}^n \Pr\left[s^*_{ij} \;\middle|\; c_j=H\right]}} \\
&= \frac{1}{1 + \frac{1-p_j}{p_j} \frac{\prod_{i=1}^n f_{\epsilon_{ij}}(s^*_{ij}-p_m)}{\prod_{i=1}^n f_{\epsilon_{ij}}(s^*_{ij}-p_h)}}
\end{aligned}$$

Now,

$$f_{\epsilon_{ij}}(x) = \frac{1}{\sigma_{ij}\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2_{ij}}}. \qquad \text{(A.20)}$$

Thus

$$\Pr\left[c_j = H \;\middle|\; s^*_{1j}, \ldots, s^*_{nj}\right] = \frac{1}{1 + \frac{1-p_j}{p_j} e^{\frac{\sum_{i=1}^n (s^*_{ij}-p_m)-(s^*_{ij}-p_h)}{2\sigma^2_{ij}}}}. \qquad \text{(A.21)}$$

□

A.1.2. Proofs for Section 1.6

Proof of Theorem 1. We condition on the number of honest and dishonest producers. There are m producers, and each is honest with probability p. Suppose there are a honest producers and $b \stackrel{\text{def}}{=} m - a$ dishonest producers. (Note that $a \sim \text{Bin}(m, p)$).

The committee is *honest* if at least $\lceil (1-p) \cdot k \rceil$ of the elected block producers are honest.

Claim 1. *The committee is honest if and only if the $\lceil (1-p) \cdot k \rceil$-st top-ranked honest producer has more votes than the $\lceil p \cdot k \rceil$-th ranked dishonest producer*

Let $X_1^h, \ldots, X_a^h$ denote the number of votes received by an honest producer j and $X_{a,1}^h, \ldots, X_{a,a}^h$ their order statistics. Similarly, let $X_1^m, \ldots, X_b^m$ denote the number of votes received by a malicious producer j and $X_{b,1}^m, \ldots, X_{b,b}^m$ their order statistics. With this notation Claim 1 becomes:

$$X^h{}_{a,a-\lceil(1-p)\cdot k\rceil+1} > X^m{}_{b,b-\lceil p\cdot k\rceil+1} \tag{A.22}$$

We define $X \stackrel{\text{def}}{=} X^h{}_{a,a-\lceil(1-p)\cdot k\rceil+1}$ and $Y \stackrel{\text{def}}{=} X^m{}_{b,b-\lceil p\cdot k\rceil+1}$.

If $a < \lceil(1-p)\cdot k\rceil$ then the success probability is zero. Also if $a > m-\lceil p\cdot k\rceil$ then $b < \lceil p\cdot k\rceil$ so the success probability is 1 hence:

$$\Pr[\mathbb{T} = H] = \sum_{a=m-\lceil p\cdot k\rceil+1}^{m} 1\cdot\Pr[a=a] + \sum_{a=\lceil(1-p)\cdot k\rceil}^{m-\lceil p\cdot k\rceil} \Pr[X > Y | a=a]\Pr[a=a] \tag{A.23}$$

We have:

$$\Pr[a=a] \sim \text{Bin}(m,p) = \binom{m}{a} p^a (1-p)^{m-a} \tag{A.24}$$

For any discrete, independent random variables, X and Y

$$\Pr[X > Y] = \sum_x \Pr[X=x]\Pr[Y<x] \tag{A.25}$$

so together with Theorems 9,10 we have:

$$\begin{aligned}
\Pr[X>Y] &= \sum_{x=0}^{n} \Pr[X=x]\Pr[Y<x] \\
&= \sum_{x=0}^{n} f_X(x)(F_Y(x) - f_Y(x)) \\
&= \textstyle\sum_{x=0}^{n} \Bigg[\Big(\sum_{j=0}^{\lceil(1-p)\cdot k\rceil-1} \binom{a}{j} \Big(\big(1-F^h(x)\big)^j \big(F^h(x)\big)^{a-j} - \big(1-F^h(x)+f^h(x)\big)^j \big(F^h(x)-f^h(x)\big)^{a-j} \Big) \Big) \\
&\quad \Big(\sum_{j=0}^{\lceil p\cdot k\rceil-1} \binom{b}{j} (1-F^m(x)+f^m(x))^j \big(F^M(x)-f^m(x)\big)^{b-j} \Big) \Bigg]
\end{aligned} \tag{A.26}$$

Plugging the last equation and Equation A.24 to Equation A.23 gives the result. □

Proof of Theorem 2. If the probability that voter i votes for candidate j when candidate j is honest (resp. dishonest) is p_i^h (resp. p_i^m), then the total number of votes for candidate j is distributed as a Poisson Binomial with parameters $p_1^h, \ldots, p_n^h$ (resp. $p_1^m, \ldots, p_n^m$).

Then applying Equation A.54 in Definition 11 gives the result. □

Proof of Proposition 1. The number of votes received by an honest producer is distributed according to a Poisson random variable with parameters $p_1^h, \ldots, p_n^h$, where

$$p_i^h = 1 - F_{s|H}(z_i) = 1 - \Phi\left(\frac{h^{-1}(z_i) - p_h}{\sigma_i}\right) \tag{A.27}$$

where Φ is the CDF of the standard normal distribution and $h^{-1}(\cdot)$ is defined in Equation A.12. Similarly, the number of of votes received by a dishonest producer is distributed according to a Poisson random variable with $p_1^m, \ldots, p_n^m$, where

$$p_i^m = 1 - F_{s|M}(z_i) = 1 - \Phi\left(\frac{h^{-1}(z_i) - p_m}{\sigma_i}\right) \tag{A.28}$$

□

Proof of Proposition 12. When voters follow the cardinal strategy, for voter i to vote for candidate j, its signal needs to be among the top z_i signals, meaning:

$$p_i = \Pr\left[s_{ij} \text{ is in the top } z_i \text{ signals}\right] \tag{A.29}$$

Let $S_{m,1}^i, \ldots, S_{m,m}^i$ denote that order statistics of $s_{i1}, \ldots, s_{im}$. Then for candidate j to be chosen by voter i it needs to hold that $s_{ij} \geq S_{m,z_i}^i$ so:

$$p_i = \Pr\left[s_{ij} \geq S_{m,z_i}^i\right] = \Pr\left[s_i \geq S_{m,z_i}^i\right] \tag{A.30}$$

with the last equality since we assumed $\sigma_{ij} = \sigma_i$. Let $X_i = s_i$ and $Y_i = S_{m,z_i}^i$ then

equation A.30 becomes:

$$p_i = \Pr[X_i \geq Y_i] = \int_{-\infty}^{\infty} \Pr[Y_i \leq x] \Pr[X_i = x]\, dx = \int_{-\infty}^{\infty} F_{Y_i}(x) f_{X_i}(x)\, dx \tag{A.31}$$

As in the Proof of Theorem 1, we condition on the number of honest producers: a. $a \sim \mathrm{Bin}(m, p)$ where p is the probability of a producer to be honest. The real valued random variables $(s_{ij})_{1 \leq j \leq m}$ are drawn from two populations. Lemma 2 provides the PDF and CDF of honest producers $f_{s_i|H}, F_{s_i|H}$ and malicious producers $f_{s_i|M}, F_{s_i|M}$. W.L.O.G, suppose that $F_{s_{ij}} = F_{s_i|H}$ for all $1 \leq j \leq a$ and $F_{s_{ij}} = F_{s_i|M}$ for all $a+1 \leq j \leq m$. By Theorem 12 we have that

$$F_{Y_i}(x) = \sum_{l=z_i}^{m} \frac{(a!(m-a)!)^2}{z_i!(m-z_i)!} \sum_{\substack{0 \leq \lambda_1 \leq z_i \\ 0 \leq \lambda_2 \leq m - z_i \\ \lambda_1 + \lambda_2 = a}} \left[\binom{z_i}{\lambda_1} \left(F_{s_i|H}\right)^{\lambda_1} \left(F_{s_i|M}\right)^{z_i - \lambda_1} \binom{m - z_i}{\lambda_2} \left(1 - F_{s_i|H}\right)^{\lambda_2} \left(1 - F_{s_i|M}\right)^{m - z_i - \lambda_2} \right] \tag{A.32}$$

So finally Equation A.31 becomes:

$$p_i = \sum_{a=0}^{m} p^a (1-p)^{m-a} \int_{-\infty}^{\infty} F_{Y_i(x)} f_{s_i}(x)\, dx, \tag{A.33}$$

where F_{Y_i} is given by Equation A.32. If the candidate is honest then p_i^h is given by Equation A.33 with $f_{s_i} = f_{s_i|H}$ derived in Lemma 2. Similarly, if the candidate is malicious then p_i^m is given by Equation A.33 with $f_{s_i} = f_{s_i|M}$. □

Proof of Lemma 1. Follows immediately from Lemma 4,5 and stochastic order definition 13. □

Proof of Proposition 2. Suppose that voter v_1 receives conditioned signals s_j on candidate c_j and they are sorted so that $s_1 \geq \cdots \geq s_m$. Let $\mathcal{C}_{v_1} = \{c_{j_1}, \ldots, c_{j_z}\}$ be voter v_1 strategy then the candidates on the chosen committee are $\mathbb{T} = \{c_{j_1}, \ldots, c_{j_z}, c_{j_{z+1}}, \ldots, c_{j_k}\}$ where $c_{j_{z+1}}, \ldots, c_{j_k}$ are filled adversarially. Let X be the random variable that is the number of

honest producers on the chosen committee. Then X is a Poisson Binomial with probabilities $(s_{j_1}, \ldots, s_{j_z}, s_{j_{z+1}}, \ldots, s_{j_k})$ and so $\Pr[\mathbb{T} = H] = \Pr[X > (1-p) \cdot k]$. Define X_P with $P = \{s_{j_1}, \ldots, s_{j_l}\} \subseteq \{s_1, \ldots, s_m\}$ to be the Poisson Binomial with parameters $(s_{j_1}, \ldots, s_{j_l})$ then by Lemma 1 we have (with $x = (1-p) \cdot k$) that

$$\underset{P \subseteq \{s_1, \ldots, s_m\}}{\operatorname{argmax}} \Pr[X_P > (1-p) \cdot k] = \{s_1, \ldots, s_k\} \tag{A.34}$$

So by definition the optimal strategy for v_1 is achieved by setting $z = k$ and $\mathcal{C}_{v_1} = \{c_1, \ldots, c_k\}$. That is, choosing the top $z = k$ candidates which is the Cardinal strategy with $z = k$. □

Proof of Proposition 3. It suffices to consider the single voter case. Let $z \in (0, 1)$ and suppose voter v_1 receives ordered, conditioned signals s_j, follows the threshold strategy and votes for all candidates $s_j > z$. Let $m_z \in [0, \ldots, m]$ denote the number of candidates that receive a vote.

If $m_z \neq k$ then this strategy is not optimal by equation A.34. To show that the Threshold strategy is not optimal, it remains to show that $\Pr[m_z \neq k] > 0$.

Since m_z is distributed as a Poisson Binomial with parameters $p_1, \ldots, p_m$ with $p_j \overset{\text{def}}{=} \Pr[s_j > z]$ and $p_j > 0, \forall j \in [1, \ldots, m]$, we have that $\Pr[m_z = i] > 0$ for all $i \in [0, \ldots, m]$, which means that $\Pr[m_z = k] < 1$. □

Proof of Proposition 4. Suppose that the resulting posterior probabilities of honesty for the candidates using Lemma 3 are s_j and they are sorted so that $s_1 \geq \cdots \geq s_m$. Let the elected candidates on the committee be $\mathbb{T} = \{c_{j_1}, \ldots, , c_{j_k}\}$. Let X be the random variable that is the number of honest producers on the chosen committee. Then X is a Poisson Binomial with probabilities $(s_{j_1}, \ldots, s_{j_k})$ and so $\Pr[\mathbb{T} = H | \mathbf{s}_i] = \Pr[X > (1-p) \cdot k]$. Define X_P with $P = \{s_{j_1}, \ldots, s_{j_l}\} \subseteq \{s_1, \ldots, s_m\}$ to be the Poisson Binomial with parameters

$(s_{j_1}, \ldots, s_{j_l})$ then by Lemma 1 we have (with $x = (1-p)\cdot k$) that

$$\underset{P \subseteq \{s_1,\ldots,s_m\}}{\operatorname{argmax}} \Pr[X_P > (1-p)\cdot k] = \{s_1, \ldots, s_k\} \tag{A.35}$$

If we set $z = k$ and $\mathcal{C}_{v_i} = \{c_1, \ldots, c_k\}$. That is, choosing the top $z = k$ candidates based on the posteriors s_j we achieve the maximum on the RHS of equation (A.35). □

Proof of Proposition 5. Proposition 2 shows that for $z \neq k$ the Cardinal strategy may be suboptimal.

Consider a setting with two voters, where $p_m = p_h$. When $p_m = p_h$, all the signals are uninformative, i.e., $s_{ij} = p$ for all $i \in [n]$, $j \in [m]$.

Now, suppose both voters follow the cardinal strategy with thresholds z_0, z_1. In this case, voter i will vote (randomly) for z_i candidates.

Since there are only two voters, every candidate receives $0, 1$ or 2 votes. Let X_0, X_1, X_2 denote the subsets producers that receive $0, 1$ and 2 votes respectively. Let $\mathcal{H}$ and $\mathcal{M}$ denote the set of honest and dishonest producers.

Thus $X_0 \dot{\bigcup} X_1 \dot{\bigcup} X_2 = [m] = \mathcal{H} \dot{\bigcup} \mathcal{M}$, where $\dot{\bigcup}$ denotes the disjoint union of sets.

First, note that since there are two voters,

$$|X_1| + 2\,|X_2| = z_0 + z_1 \tag{A.36}$$

Since $|X_2| \leq \min(z_0, z_1)$, we have $|X_1 \cup X_2| \geq \max(z_0, z_1)$, which means that when $\max(z_0, z_1) \geq k$ (i.e., either voter votes for k candidates) no candidates from X_0 will ever make it to the committee.

To show that the threshold $z_i = k$ strategy is suboptimal, it suffices to consider strategies

with $\max(z_0, z_1) \geq k$.

Since we assume that ties are broken in a worst-case fashion, the committee will be dishonest if and only if there are x dishonest candidates in X_2 and there are at least $t+1-x$ dishonest candidates in X_1 and $|X_2| \leq k-(t+1-x)$. because in this case, the adversary can choose $k-(t+1-x)$ dishonest candidates from X_1 to fill the committee.

In other words, the committee will be dishonest with probability

$$\Pr[\mathbb{T} \neq H] = \sum_{a=0}^{\min(z_0,z_1)} \Pr[|X_2| = a] \sum_{x=0}^{a} \Pr[|X_2 \cap \mathcal{M}| = x \mid |X_2| = a] \Pr[|X_1 \cap \mathcal{M}| \geq t+1-x] \tag{A.37}$$

Note that if we did *not* assume $\min(z_0, z_1) \geq k$, some candidates from X_0 could make it onto the committee, and Equation A.37 would have extra terms.

Now $|X_2|$ is distributed as a hypergeometric random variable with parameters (z_0, z_1, m) (i.e., z_1 draws from a population of size m with z_0 "distinguished" items), and $|X_1|$ is distributed as a $z_0 + z_1 - 2|X_2|$.

Thus we have

$$\Pr[|X_2| = a] = \frac{\binom{z_0}{a}\binom{m-z_0}{z_1-a}}{\binom{m}{z_1}} \tag{A.38}$$

Since each producer is dishonest independently with probability p, the number of dishonest producers in X_2 is binomial random variable with parameters a, p.

$$\Pr[|X_2 \cap \mathcal{M}| = x \mid |X_2| = a] = \Pr[\mathrm{Bin}(a, p) = x] \tag{A.39}$$

$$\tag{A.40}$$

and

$$\Pr\left[|X_1 \cap \mathcal{M}| = x \mid |X_2| = a\right] = \Pr\left[|X_1 \cap \mathcal{M}| = x \mid |X_1| = z_0 + z_1 - 2a\right] \tag{A.41}$$

$$= \Pr\left[\mathrm{Bin}(z_0 + z_1 - 2a, p) = x\right] \tag{A.42}$$

$$\tag{A.43}$$

Equation A.37 becomes

$$\Pr\left[\mathbb{T} \neq H\right] =$$

$$\sum_{a=0}^{\min(z_0,z_1)} \Pr\left[|X_2| = a\right] \cdot \sum_{x=0}^{a} \Pr\left[\mathrm{Bin}(a,p) = x\right] \cdot \Pr\left[\mathrm{Bin}(z_0 + z_1 - 2a, p) \geq t + 1 - x\right] \tag{A.44}$$

$$= \sum_{a=0}^{\min(z_0,z_1)} \Pr\left[|X_2| = a\right] \cdot \Pr\left[\mathrm{Bin}(z_0 + z_1 - a, p) \geq t + 1\right]$$

$$\geq \sum_{a=0}^{\min(z_0,z_1)} \Pr\left[|X_2| = a\right] \cdot \Pr\left[\mathrm{Bin}(\max(z_0, z_1), p) \geq t + 1\right]$$

$$= \Pr\left[\mathrm{Bin}(\max(z_0, z_1), p) \geq t + 1\right]$$

When $z_0 = z_1 = k$ (both voters vote for k producers) Equation A.44 becomes

$$\sum_{a=0}^{k} \Pr\left[|X_2| = a\right] \cdot \sum_{x=0}^{a} \Pr\left[\mathrm{Bin}(a,p) = x\right] \cdot \Pr\left[\mathrm{Bin}(2(k-a), p) \geq t + 1 - x\right]$$

$$= \sum_{a=0}^{k} \Pr\left[|X_2| = a\right] \cdot \Pr\left[\mathrm{Bin}(2k - a, p) \geq t + 1\right] \tag{A.45}$$

$$> \sum_{a=0}^{k} \Pr\left[|X_2| = a\right] \cdot \Pr\left[\mathrm{Bin}(k, p) \geq t + 1\right]$$

$$= \Pr\left[\mathrm{Bin}(k, p) \geq t + 1\right]$$

When $z_0 = k$, and $z_1 = 0$ (voter 1 abstains) Equation A.44 becomes

$$\Pr\left[\text{Bin}(k,p) \geq t+1\right] = \sum_{b=t+1}^{k} \binom{k}{b} (1-p)^b p^{k-b} \tag{A.46}$$

Here, we see that Equation A.45 is strictly greater than Equation A.46, so voter 1 is strictly better off setting $z_1 = 0$ (voting for no producers) than voting for k producers. □

Proof of Theorem 3. First, note that since $|\mathcal{H}| \geq (1-p) \cdot k$, then if *all* members of $\mathcal{H}$ receive more votes than all dishonest producers, then the committee will be honest. Thus it suffices to show that all members of $\mathcal{H}$ will receive more votes than all members of $\mathcal{M}$ with high probability.

Let X_j denote the number of votes received by producer j. Then X_j is a Poisson Binomial with parameters $p_{1j}, \ldots, p_{nj}$.

Fix $j_h \in \mathcal{H}$, and $j_m \in \mathcal{M}$. Then, by assumption

$$\sum_{i=1}^{n} p_{ij_h} \geq n\delta + \sum_{i=1}^{n} p_{ij_m} \tag{A.47}$$

The Chernoff bound for Poisson Binomials (Theorem 7) shows that for all $t > 0$

$$\Pr\left[X_{j_h} < \sum_{i=1}^{n} p_{ij_h} - t\right] \leq e^{-\frac{2t^2}{n}} \tag{A.48}$$

and similarly

$$\Pr\left[X_{j_m} > \sum_{i=1}^{n} p_{ij_m} + t\right] \leq e^{-\frac{2t^2}{n}} \tag{A.49}$$

If $X_{j_h} \leq X_{j_m}$, then either

$$X_{j_h} < \sum_{i=1}^{n} p_{ij_h} - \frac{n\delta}{2} \tag{A.50}$$

or

$$X_{j_m} > \sum_{i=1}^{n} p_{ij_m} + \frac{n\delta}{2}. \tag{A.51}$$

By a union bound, the probability that either of these events happens is bounded by

$$2e^{-\delta^2 n/2}. \tag{A.52}$$

Taking a union bound over all pairs $j_h \in \mathcal{H}$, and $j_m \in \mathcal{M}$, we have the probability that *all* $j_h \in \mathcal{H}$ receive more votes than *all* $j_m \in \mathcal{M}$, is at least

$$1 - 2m^2 e^{-\delta^2 n/2}. \tag{A.53}$$

□

A.2. Poisson Binomial Distributions

A.2.1. Definitions

Definition 11 (Poisson Binomial Distribution)**.** *If* $\{X_i\}$ *are independent Bernoulli random variables, and* $\Pr[X_i = 1] = p_i$*, then the distribution of* $X \stackrel{\text{def}}{=} \sum_i X_i$ *is called the* Poisson Binomial Distribution *with parameters* $(p_1, \ldots, p_n)$*.*

A simple counting argument shows that if X has a Poisson Binomial distribution with parameters $p_1, \ldots, p_n$, then for any $\ell \in 0, \ldots, n$

$$\Pr[X = \ell] = \sum_{A \in F_\ell} \prod_{i \in A} p_i \prod_{j \in A^c} 1 - p_j \tag{A.54}$$

where F_ℓ is the set of all subsets of ℓ integers that can be selected from $\{1, \ldots, n\}$.

Lemma 4 (Symmetry of Poisson Binomial Distributions)**.** *Suppose* $\sigma : [n] \to [n]$ *is a permutation, and let* X *be a Poisson Binomial random variable with parameters* $p_1, \ldots, p_n$*,*

and X' be a Poisson Binomial random variable with parameters $\sigma(p_1), \ldots, \sigma(p_n)$, then for all $\ell \in 0, \ldots, n$,

$$\Pr[X = \ell] = \Pr[X' = \ell]$$

Lemma 5 (Monotonicity)**.** *Suppose X is a Poisson Binomial random variable with parameters $p_1, \ldots, p_n$, and X' is a Poisson Binomial random variable with parameters $p'_1, \ldots, p'_n$, satisfying $p_i \leq p'_i$ for $i = 1, \ldots, n$, then*

$$X \leq_{\text{st}} X'.$$

Proof. The proof follows immediately from Lemma 6 since a Bernoulli random variable with parameter p'_i stochastically dominates a Bernoulli random variable with parameter $p_i \leq p'_i$. □

A.2.2. Alternative characterizations of Poisson Binomial Distribution

Theorem 5 (Alternative characterization of a PDF of a Poisson Binomial Fernández and Williams (2010))**.** *If X has a Poisson Binomial Distribution with parameters $(p_1, \ldots, p_n)$, then*

$$\Pr[X = t] = \frac{1}{n+1} \sum_{j=0}^{n} \left(e^{-2\pi i \frac{jt}{n+1}} \prod_{k=1}^{n} \left(p_k e^{2\pi i \frac{j}{n+1}} + (1 - p_k) \right) \right) \tag{A.55}$$

We use $f^{(PB)}_{p_1,\ldots,p_n}(x)$ to denote the PDF of a Poisson Binomial random variable with parameters $p_1, \ldots, p_n$.

Theorem 6 (CDF of a Poisson Binomial Fernández and Williams (2010))**.** *If X has a Poisson Binomial Distribution with parameters $(p_1, \ldots, p_n)$, then*

$$\Pr[X \geq t] = 1 - \frac{1}{n+1} \sum_{j=0}^{n} \left(\left(\sum_{k=0}^{t-1} e^{-2\pi i \frac{jk}{n+1}} \right) \prod_{\ell=1}^{n} p_\ell e^{2\pi i \frac{j}{N+1}} + (1 - p_\ell) \right) \tag{A.56}$$

We use $F^{(PB)}_{p_1,\ldots,p_n}(x)$ to denote the CDF of a Poisson Binomial random variable with parameters $p_1, \ldots, p_n$.

A.2.3. Concentration bounds

Theorem 7 (Chernoff-Hoeffding (Dubhashi and Panconesi, 2009, Theorem 1.1))**.** *Let $X = \sum_{i=1}^{n} X_i$ is a Poisson Binomial with parameters $\{p_i\}$, and define $\bar{p} \stackrel{\text{def}}{=} \frac{1}{n}\sum_{i=1}^{n} p_i$, then*

$$\Pr\left[X > n\bar{p} + t\right] \leq e^{-2t^2/n} \tag{A.57}$$

$$\Pr\left[X < n\bar{p} - t\right] \leq e^{-2t^2/n} \tag{A.58}$$

Linear combinations of order statistics of Poisson Binomial RVs also satisfy a central limit theorem Pham and Tran (1982).

A.3. Order Statistics

Definition 12 (Order statistics)**.** *Let $X_1, \ldots, X_n$ be random variables. Define $X_{n,1}, \ldots X_{n,n}$ to be the* order statistics *of $X_1, \ldots, X_n$, to $X_1, \ldots, X_n$ in sorted order.*

Remark 5. *The random variables $X_{n,1}, \ldots, X_{n,n}$ are* dependent *even if the underlying $\{X_i\}$ are independent, and they satisfy*

$$X_{n,1} \leq \cdots \leq X_{n,n}. \tag{A.59}$$

Theorem 8. *If $\{X_i\}$ are* continuous *IID random variables, with absolutely continuous PDF $f(x)$ and CDF, $F(x)$, then the CDF of the kth order statistic from a sample of size n is*

$$\Pr\left[X_{n,k} \leq x\right] = F_{(k,n)}(x) = \sum_{j=k}^{n} \binom{n}{j} \left(F(x)\right)^j \left(1 - F(x)\right)^{n-j} \tag{A.60}$$

Theorem 9. *If $\{X_i\}$ are* discrete *IID random variables, with PDF $f(x)$ and CDF, $F(x)$,*

then the PDF of the kth order statistic from a sample of size n is

$$\Pr\big[X_{n,k}{=}x\big]{=}f_{(k,n)}(x){=}\textstyle\sum_{j=0}^{n-k}\binom{n}{j}\big((1{-}F(x))^j(F(x))^{n-j}{-}(1{-}F(x){+}f(x))^j(F(x){-}f(x))^{n-j}\big) \tag{A.61}$$

Theorem 10. *If* $\{X_i\}$ *are* discrete *IID random variables, with PDF* $f(x)$ *and CDF,* $F(x)$*, then the CDF of the kth order statistic from a sample of size n is*

$$\Pr\left[X_{n,k} \leq x\right] = F_{(k,n)}(x) = \sum_{j=0}^{n-k} \binom{n}{j} \left(1 - F(x)\right)^j \left(F(x)\right)^{n-j} \tag{A.62}$$

Theorem 11 (Bapat-Beg Theorem (Glueck et al., 2008, Theorem 3.1))**.** *Let* X_i*,* $i = 1, \ldots, m$ *independent, real-valued random variables with cdf* $F_i(x)$ *respectively.* Y_i *the order statistics defined by sorting the values of* X_i*. Let* $n, 1 \leq n_1 < n_2 < \cdots < n_k \leq m$ *and* $y_1 \leq y_2 \leq \cdots \leq y_k$ *the values of the arguments of the joint cdf of* $\{Y_{n_1}, Y_{n_2}, \ldots, Y_{n_k}\}$*. Define the index vector* $\mathbf{i} = (i_0, i_1, \ldots, i_{k+1})$ *and the summation index set* $\mathcal{I} = \{\mathbf{i} : 0 = i_0 \leq i_1 \leq \cdots \leq i_k \leq i_{k+1} = m,$ *and* $i_j \geq n_j$ *for all* $1 \leq j \leq k\}$*. The joint cdf of the order statistics satisfies:*

$$F_{Y_{n_1},\ldots,Y_{n_k}}(y_1, \ldots, y_k) = \sum_{\mathbf{i}\in\mathcal{I}} \frac{P_{i_1,\ldots,i_k}(y_1, \ldots, y_k)}{(i_1 - i_0)!(i_2 - i_1)! \cdots (i_{k+1} - i_k)!}, \tag{A.63}$$

where $P_{i_1,\ldots,i_k}(y_1, \ldots, y_k)$ *are permanents of block matrices*

$$P_{i_1,\ldots,i_k}(y_1, \ldots, y_k) = \operatorname{per}\left[\left[F_i(y_j) - F_i(y_{j-1})\right]_{(i_j - i_{j-1})\times 1}\right]_{j=1,i=1}^{j=k,i=m}, \tag{A.64}$$

with the subscripts indicating the dimensions of blocks created by the repetition of the term in the brackets, and $F_i(y_0) = 0, F_i(y_{k+1}) = 1$*.*

Theorem 12 ((Glueck et al., 2008, Theorem 3.2))**.** *With notation as in Theorem 11, suppose that* $F_i(x) = F(x)$ *for all* $1 \leq i \leq n$*, and* $F_i(x) = G(x)$ *for all* $n + 1 \leq i \leq m$*.*

Then:

$$F_{Y_{n_1},\ldots,Y_{n_k}}(y_1,\ldots,y_k)=\sum_{\mathbf{i}\in\mathcal{I}}\sum_{\boldsymbol{\lambda}}\prod_{j=1}^{k+1}\frac{n!(m-n)!}{\lambda_j!(i_j-i_{j-1}-\lambda_j)!}[F(y_j)-F(y_{j-1})]^{\lambda_j}[G(y_j)-G(y_{j-1})]^{i_j-i_{j-1}-\lambda_j}, \tag{A.65}$$

where $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\ldots,\lambda_{k+1})$ *ranges over all integer vectors such that*

$$\lambda_1+\lambda_2+\cdots+\lambda_{k+1}=n,\ 0\le\lambda_j\le i_j-i_{j-1}, \tag{A.66}$$

and $F(y_0)=G(y_0)=0, F(y_{k+1})=G(y_{k+1})=1$.

Definition 13 (Orderings)**.** *Let* X *and* Y *be random variables with PDFs* f_X*,* f_Y *and CDFs* F_X*,* F_Y*.*

- ***Stochastic Order:***

$$X\le_{\text{st}}Y\Leftrightarrow F_Y(x)\le F_X(x)\ \textit{for all}\ x\ , \tag{A.67}$$

- ***Hazard-rate Order:***

$$X\le_{\text{hr}}Y\Leftrightarrow(1-F_Y(x))/(1-F_X(x))\ \textit{is increasing in}\ x\ , \tag{A.68}$$

- ***Likelihood-ratio Order:***

$$X\le_{\text{lr}}Y\Leftrightarrow f_Y(x)/f_X(x)\ \textit{is increasing in}\ x\ , \tag{A.69}$$

Lemma 6 (Summations)**.** *If* $X_1\ge_{\text{st}}Y_1$*, and* $X_2\ge_{\text{st}}Y_2$*, then*

$$X_1+X_2\ge_{\text{st}}Y_1+Y_2$$

Proof.

$$
\begin{aligned}
\Pr\left[X_1 + X_2 \geq t\right] &= \sum_{x_1=0}^{n} \sum_{x_2=t-x_1}^{n} \Pr\left[X_1 = x_1\right] \Pr\left[X_2 = x_2\right] \\
&= \sum_{x_1=0}^{n} \left(\sum_{x_2=t-x_1}^{n} \Pr\left[X_2 = x_2\right] \right) \Pr\left[X_1 = x_1\right] \\
&= \sum_{x_1=0}^{n} \Pr\left[X_2 \geq t - x_1\right] \Pr\left[X_1 = x_1\right] \\
&\geq \sum_{x_1=0}^{n} \Pr\left[Y_2 \geq t - x_1\right] \Pr\left[X_1 = x_1\right] \\
&= \sum_{x_1=0}^{n} \left(\sum_{x_2=t-x_1}^{n} \Pr\left[Y_2 = x_2\right] \right) \Pr\left[X_1 = x_1\right] \\
&= \sum_{x_2=0}^{n} \left(\sum_{x_1=t-x_2}^{n} \Pr\left[X_1 = x_1\right] \right) \Pr\left[Y_2 = x_2\right] \\
&= \sum_{x_2=0}^{n} \Pr\left[X_1 \geq t - x_2\right] \Pr\left[Y_2 = x_2\right] \\
&\geq \sum_{x_2=0}^{n} \Pr\left[Y_1 \geq t - x_2\right] \Pr\left[Y_2 = x_2\right] \\
&= \sum_{x_2=0}^{n} \left(\sum_{x_1=t-x_2}^{n} \Pr\left[Y_1 = x_1\right] \right) \Pr\left[Y_2 = x_2\right] \\
&= \Pr\left[Y_1 + Y_2 \geq t\right]
\end{aligned}
$$

□

Corollary 6. *If X is a Poisson Binomial with parameters $p_1, \ldots, p_t, p_{t+1}$, and Y is a Poisson Binomial with parameters $p_1, \ldots, p_t$, then*

$$X \geq_{\text{st}} Y \tag{A.70}$$

A.4. Alternative Objective Function: Quality Model

Our main model considers discrete types of producers ("honest" and "dishonest"). In addition to selecting honest producers, voters may be interested in electing block producers who will

offer the highest *performance* (e.g. transaction throughput). In this section, we outline an alternative model where producers vary continuously based on their "quality" (e.g. a metric of their computing performance, uptime and network latency). As before, voters receive a noisy signal about each producer's quality, and the voters use approval voting to elect a committee.

Definition 14 (Continuous quality model)**.** *Producer j has an (unknown) quality, $q_j \sim \mathcal{Q}$ for some (known) quality distribution $\mathcal{Q}$. As before, suppose voter i receives a quality estimate $\hat{q}_{ij} = q_j + \epsilon_{ij}$, where $\epsilon_{ij} \sim N(0, \sigma_i)$.*

As above, voter i will rank the block producers in order of of the signals $\{q_{ij}\}_j$, and may employ a *Threshold* or *Cardinality* voting strategy to determine how many block producers they choose to elect.

When focusing on honesty, we considered a one-shot game, since a single dishonest committee can potentially wreak havoc on the system, whereas a single low performing committee may only have a small effect on the overall popularity and utility of the system as a whole.

Thus in the quality model, it would make more sense to consider a *multi-round* game where voters earn *rewards* and receive *feedback* at each round. When a set of block producers is elected, the voters can observe their throughput and latency, and thus get feedback about the quality of the committee. We can consider different levels of granularity regarding the feedback received by the voters:

- **Individual feedback:** The quality of *each* of the c block producers that were elected to the committee
- **Average feedback:** The *average* quality of the c block producers that were elected to the committee

We can also consider different types of voter rewards, which model the benefit they receive from higher throughput and and lower latency among the block-producer committee.

- **Average rewards:** The *average* quality of the c block producers that were elected to the committee

- **Weakest-link rewards:** The *minimum* quality of the c block producers that were elected to the committee

Once we specify the exact type of feedback and rewards, we can ask how should voters behave in order to maximize their rewards. If a single voter could unilaterally specify the entire committee, the problem would fall in the class of *combinatorial* multi-armed bandit problems (CMAB) (Cesa-Bianchi and Lugosi, 2012).

Combinatorial bandit problems have been reasonably well studied Cesa-Bianchi and Lugosi (2012); Chen et al. (2013); Combes et al. (2015); Chen et al. (2016); Agarwal and Aggarwal (2018); Rejwan and Mansour (2020) under two different feedback models (i) semi-bandit feedback, where the voters learn the quality of each individual producer in the committee and (ii) (full) bandit feedback, where the voters learn the average quality of the committee. There would be two main differences between our own model and traditional combinatorial multi-armed bandit problems:

First, most CMAB papers assume there is a single player who unilaterally selects which bandits to play (i.e., which candidates to elect). In our setting, we have multiple voters, who vote independently, and the committee is chosen based on the outcome of this vote.

Second, most CMAB papers assume the player starts with no information about the underlying bandits (i.e., the voters receive no signals). If voters start with no information about the committee (and all committee feedback is public), then for practical purposes, there is essentially only one voter, and the problem completely becomes a CMAB problem.

Given the difficulty of finding the optimal voting strategy in the static model, it will like be intractable to find the voting strategy that optimally combines with the CMAB exploration-exploitation strategy. But this could nonetheless be an interesting direction for future work.

A.5. Other Asymptotic Results

Figure A.3 shows that when the signal informativeness is high, that is, $p_h \gg p_m$, the success probability rapidly approaches 1 (even for a small number of voters), but if the threshold is too high ($z \approx 1$), then the success probability drops to zero as all candidates receive 0 votes.

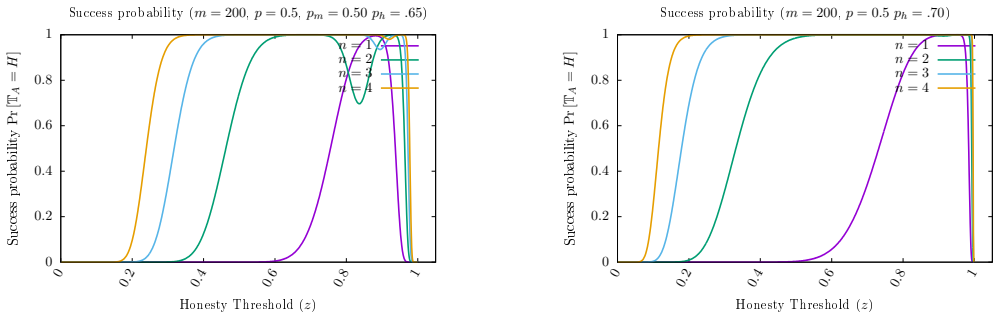

Figure A.3: Success probability as a function of voting threshold when signal informativeness is high.

Figure A.4 shows that when the signal informativeness is high, as the *a priori* probability that a producer is honest increases, then almost any threshold yields a nearly 100% chance of electing an honest committee.

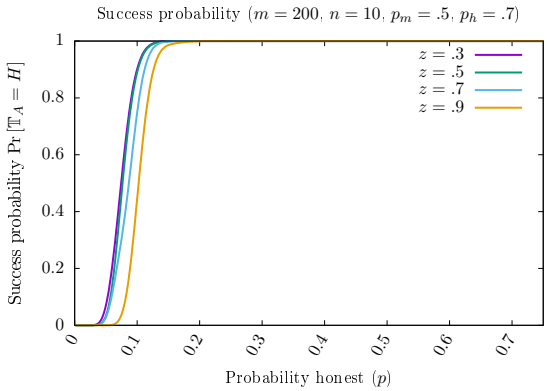

Figure A.4: Success probability as a function of the prior.

A.6. Dependencies in Cardinal Voting

When voters follow a cardinal voting strategy, i.e., they vote for the z candidates with the highest posterior probability of being honest, the analysis is Theorem 1 no longer applies because the probabilities that each candidate receives a vote are no longer independent. If you vote for candidate j_1, you are less likely to vote for candidate j_2, since you are only going to cast z votes. By contrast, when voters follow the threshold-voting strategy, the votes for different candidates *are* independent.

Nevertheless, in the cardinal-voting setting, we can calculate the probabilities p_i^h (resp. p_i^m) denote the probability that voter i votes for producer j conditioned on j being honest (resp. dishonest).

Proposition 12 (Cardinal voting)**.** *With notation as in Proposition 1, when voters follow the cardinal strategy (Definition 6) with cardinal, z_i, then*

$$p_i^h = \sum_{a=0}^{m} p^a (1-p)^{m-a} \int_{-\infty}^{\infty} F_{Y_i(x)} f_{s_i|H}(x)\, dx, \tag{A.71}$$

$$p_i^m = \sum_{a=0}^{m} p^a (1-p)^{m-a} \int_{-\infty}^{\infty} F_{Y_i(x)} f_{s_i|M}(x)\, dx, \tag{A.72}$$

where

$$F_{Y_i}(x) = \sum_{l=z_i}^{m} \frac{(a!(m-a)!)^2}{z_i!(m-z_i)!} \sum_{\substack{0\le\lambda_1\le z_i \\ 0\le\lambda_2\le m-z_i}} \left[\binom{z_i}{\lambda_1} \left(F_{s_i|H}\right)^{\lambda_1} \left(F_{s_i|M}\right)^{z_i-\lambda_1} \binom{m-z_i}{\lambda_2} \left(1-F_{s_i|H}\right)^{\lambda_2} \left(1-F_{s_i|M}\right)^{m-z_i-\lambda_2} \right] \tag{A.73}$$

and $f_{s_i|H}, F_{s_i|H}, f_{s_i|M}, F_{s_i|M}$ are derived in Lemma 2.

Now, voter i will vote for an honest candidate if the top-ranked honest candidate is higher than the top-ranked dishonest candidate. Let $f_{s|H}$ (resp. $f_{s|M}$) denote the cdf of the signal, s, conditioned on a candidate being honest (resp. dishonest). These cdfs are calculated

explicitly in Equations A.17 & A.18.

Suppose there are a honest candidates and b dishonest candidates, in this setting, the CDF and pdf of the highest ranked honest candidate are

$$F_{H_{(a)}}(x) = F_{s|H}^{a} \tag{A.74}$$

$$f_{H_{(a)}}(x) = a\left(F_{s|H}(x)\right)^{a-1} \cdot f_{s|H}(x) \tag{A.75}$$

Similarly, the CDF and PDF of the highest ranked dishonest candidate are

$$F_{M_{(b)}}(x) = F_{s|M}^{b} \tag{A.76}$$

$$f_{M_{(b)}}(x) = b\left(F_{s|M}(x)\right)^{b-1} \cdot f_{s|M}(x) \tag{A.77}$$

Thus the probability that voter i votes for an honest candidate is

$$\int_0^1 F_{M_{(b)}}(x) f_{H_{(a)}}(x)dx = a\int_0^1 F_{s|M}^{b} \cdot \left(f_{s|H}\right)^{a-1} \cdot f_{s|H}(x)dx \tag{A.78}$$

Thus

$$p_i^h = \sum_{a=1}^{m} \binom{n}{a} p^a (1-p)^{m-a} \left[\int_0^1 F_{s|M}^{m-a} \cdot \left(f_{s|H}\right)^{a-1} \cdot f_{s|H}(x)dx\right] \tag{A.79}$$

$$p_i^m = \sum_{a=1}^{m} \binom{n}{a} p^a (1-p)^{m-a} \left[\int_0^1 F_{s|H}^{a} \cdot \left(f_{s|M}\right)^{b-1} \cdot f_{s|M}(x)dx\right] \tag{A.80}$$

APPENDIX B

Chapter 2 Appendix

B.1. Proofs

B.1.1. Proofs for Section 2.4

Proof of Proposition 6.

$$\Pr\left[\sum_{i=1}^{n} s_i > 0\right] = \Pr\left[\frac{n + \sum_{i=1}^{n} s_i}{2} > \frac{n}{2}\right] = \Pr\left[\sum_{i=1}^{n} \frac{s_i + 1}{2} > \frac{n}{2}\right]$$

Let $X = \sum_{i=1}^{n} \frac{s_i+1}{2}$ random variable. Since $\frac{s_i+1}{2} = 1$ for $s_i = 1$ with probability p_i and $\frac{s_i+1}{2} = 0$ for $s_i = -1$ with probability $(1 - p_i)$, then $X \sim \text{PoiBin}(p_1, \ldots, p_n)$ and we are done. □

Proof of Proposition 7. We use a simple counting argument. Let $\vec{v}, \vec{s}$ be some realization of the votes and their direction respectively and let $A = \{i \in [n] \mid s_i = 1\}$ be the set of indices of all successful voters. If $\sum_{i=1}^{n} s_i v_i > 0$ then

$$0 < \sum_{i=1}^{n} s_i v_i = \sum_{i \in A} v_i - \sum_{i \in A^c} v_i \tag{B.1}$$

and so $\sum_{i \in A} v_i > \sum_{i \in A^c} v_i$ meaning $A \in F_{\vec{v}}$. Hence

$$\Pr\left[\sum_{i=1}^{n} s_i v_i > 0\right] = \sum_{A \in F_{\vec{v}}} \Pr(A) \tag{B.2}$$

Now,

$$\Pr(A) = \prod_{i \in A} \Pr(s_i = 1) \prod_{j \in A^c} \Pr(s_j = -1) \tag{B.3}$$

And we are done since $\Pr(s_i = 1) = p_i$ and $\Pr(s_j = -1) = 1 - p_j$. □

Another proof of Proposition 6. If $v_i = 1$ for all i then

$$\begin{aligned} F_{\vec{v}} &= \left\{ A \subseteq [n] \;\middle|\; \sum_{i \in A} v_i > \sum_{i \in A^c} v_i \right\} \\ &= \{A \subseteq [n] \mid |A| > |A^c|\} = \left\{ A \subseteq [n] \;\middle|\; |A| > \frac{n}{2} \right\} = \dot{\bigcup_{k>n/2}} F_k \end{aligned} \tag{B.4}$$

Plugging into Proposition 7 we get

$$\begin{aligned} \Pr\left[\sum_{i=1}^{n} s_i v_i > 0\right] &= \sum_{A \in \dot{\bigcup}_{k>n/2} F_k} \prod_{i \in A} p_i \prod_{j \in A^c} (1 - p_j) = \sum_{k>n/2} \sum_{A \in F_k} \prod_{i \in A} p_i \prod_{j \in A^c} (1 - p_j) \\ &= \sum_{k>n/2} \Pr[X = k] = \Pr\left[X > \frac{n}{2}\right] \end{aligned} \tag{B.5}$$

□

Proof of Proposition 9.

This is an easy to check fact about real numbers.

Claim 2. *Let $x, y \in \mathbb{R}$. If $1 > x > y > 0.5$ then $x + 2y - 2xy > 1$.*

As an immediate result we get (for $x = p_1, y = p_3$):

Corollary 7. $P_3 > p_2, p_3$

Proof. $P_3 = p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3 > p_1p_2 + p_2p_3 + p_2p_3 - 2p_1p_2p_3 = p_2(p_1 + 2p_3 - 2p_1p_3) > p_2 > p_3$ □

We can use the winning probabilities calculated in Table 2.1. We use iterated dominance, that is, for N.E. strategy it suffices to show that $v_i = BR_i(v_{-i})$ for $i = 1, 2, 3$.

$\vec{v} = (1, 1, 1)$:

v_1	$(v_2, v_3) = (1, 1)$
1	$uP_3 - 1$
2	$u\left(P_3 - P_{\bar{1}23}\right) - 2^m$
≥ 3	$up_1 - v_1^m$

(a) Voter 1 payoffs

v_2	$(v_1, v_3) = (1, 1)$
1	$uP_3 - 1$
2	$u\left(P_3 - P_{1\bar{2}3}\right) - 2^m$
≥ 3	$up_2 - v_2^m$

(b) Voter 2 payoffs

v_3	$(v_1, v_2) = (1, 1)$
1	$uP_3 - 1$
2	$u\left(P_3 - P_{12\bar{3}}\right) - 2^m$
≥ 3	$uP_3 - v_3^m$

(c) Voter 3 payoffs

Table B.1: Strategy space for $n = 3$ for the cell $\vec{v} = (1, 1, 1)$. The values in the table represent the voter i's payoff

Starting from v_1: Table B.1(b), we see that $v_1 = 2$ decreases the winning probability and increases the payment so this strategy is dominated. Also, the strategies $v_1 > 3$ are dominated by $v_1 = 3$ since the winning probability stays the same while the payment increases. So we are left with comparing the payoff from $v_1 = 1$ to $v_1 = 3$. The condition for when $v_1 = 1$ is a better response is

$$u\left(p_1 - P_3\right) \leq 3^m - 1 \tag{B.6}$$

For v_2: Table B.1(a), we see that $v_2 = 2$ decreases the winning probability and increases the payment so this strategy is dominated. Also, the strategies $v_2 > 3$ are dominated by $v_2 = 3$ since the winning probability stays the same while the payment increases. So we are left with comparing the payoff from $v_2 = 1$ to $v_2 = 3$. Since $P_3 > p_2$ then $v_2 = 1$ is the dominant strategy.

The case of v_3 is proved similarly to v_2. The above calculation can be made to show the rest of the N.E. in the table.

We will now show that this list is exhaustive. Assume by contradiction there exists another N.E. strategy $\vec{v}$.

If $p(\vec{v}) \neq p(\vec{1}_n)$: then the only other option is $p(\vec{v}) = p_1$ since any other winning probability is strictly smaller than $p(\vec{1}_n)$ and costs more. The calculation from Table 2.1 shows that this is only possible in the case $v_1 > v_2 + v_3$. So assume $v_1 > v_2 + v_3$, if $v_2 \neq 1$ or $v_3 \neq 1$

than these voters are paying higher cost for the same winning probability, so $v_2 = v_3 = 1$. And then if $v_3 > 3$ then voter 1 is paying higher cost for the same winning probability so $\vec{v} = (3, 1, 1)$ which is already on our list.

If $p(\vec{v}) = p(\vec{1}_n)$: then we know that $v_j < v_{j+1} + v_{j+2} \forall j$. Assume W.L.O.G that $v_1 \geq v_2 \geq v_3$ then v_1 can vote v_2 amount, the probability of winning will stay the same while the cost for him will decrease. Then v_2 can vote v_3 amount and the probability of winning stay the same. And then v_1 can vote v_3 amount. For any value of $t \geq 2$ the strategy (t, t, t) will be decreased by each voter using $t \to t - 1$ sequentially until $t = 2$. And we saw before this decreases to either $(2, 2, 1), (2, 1, 2)$ or $(1, 2, 2)$. □

Proof of Corollary 4. This follows from the fact that if Up_1 is the maximum welfare for QV then it must be the maximum welfare for RV (since $c_4 \geq 3^m - 1$ for $m = 2 \Rightarrow c_4 \geq 3^m - 1$ for $m = 1$).

If $c_4 < 2$ then the only possible welfare for both games is UP_3.

If $2 \leq c_4 < 8$ then the strategy $(3, 1, 1)$ becomes a N.E. for $m = 1$ but not $m = 2$ so in any case the RHS of the inequality is UP_3 and the LHS is $\geq Up(\vec{1}_3)$. If we restrict $4 < c_4 < 8$ then it is guaranteed the RV has Up_1 with $(3, 1, 1)$ as a unique N.E. so since $p_1 > p(\vec{1}_3)$ we get a strictly larger welfare for RV in this region. If $c_4 > 8$ then RV only gets $(3, 1, 1)$ as N.E. and so the unique welfare for it is Up_1 so we are done. □

Proof of Proposition 10.

Lemma 7. *Let* $1 > p_1 > p_2 > \cdots > p_n \geq 0.5$ *then*

$$\Pr\left[X = \frac{n}{2}\right] \underset{n\to\infty}{\to} 0$$

Let $\bar{p} = \frac{1}{n}\sum_i^n p_i$ we have using the Chernoff bound (Theorem 7) that for any $t > 0$

$$\Pr\left[X < n\bar{p} - t\right] \leq e^{-2t^2/n} \tag{B.7}$$

Let $t = n\bar{p} - \frac{n}{2} > 0$ then $\Pr\left[X < \frac{n}{2}\right] \leq e^{-2(\bar{p}-1/2)^2 n}$

Now, by Lemma 7,

$$p_{\vec{1}_n} = \Pr\left[X > \frac{n}{2}\right] = 1 - \Pr\left[X < \frac{n}{2}\right] - \Pr\left[X = \frac{n}{2}\right] \geq 1 - \Pr\left[X = \frac{n}{2}\right] - e^{-2(\bar{p}-1/2)^2 n} \underset{n\to\infty}{\to} 1 \tag{B.8}$$

□

Proof of Proposition 11.

Lemma 8. *For all* $1 < i \leq n$*:* $u_{(v_1,1,\ldots,1)} - v_1^m \geq up_{(1,\ldots,v_i,\ldots,1)} - v_i^m$ *for all* $v_i > 1$

If $\vec{v} = \vec{1}_n$ is a N.E. then $1 \in BR_i(v_{-i})$ for all i. Meaning that for all i:

$$up_{\vec{1}_n} - 1 \geq up_{(1,\ldots,v_i,\ldots,1)} - v_i^m \text{ for all } v_i > 1 \tag{B.9}$$

Letting $i = 1$ and rearranging the last equation, we have:

$$u(p_{(v_1,\ldots,,1)} - p_{\vec{1}_n}) \leq v_1^m - 1 \text{ for all } v_1 > 1 \tag{B.10}$$

which gives the forward direction. Conversely, assume by contradiction that $\vec{v} = \vec{1}_n$ is not a N.E. then there exists an i for which

$$up_{(1,\ldots,v_i,\ldots,1)} - v_i^m > up_{\vec{1}_n} - 1 \text{ for some } v_i > 1 \tag{B.11}$$

By lemma 8 we know that

$$up_{(v_i,\ldots 1)} - v_i^m > up_{\vec{1}_n} - 1 \text{ for some } v_i > 1 \tag{B.12}$$

If we take the maximum of the LHS over all $v_i > 1$ then we obviously get something bigger, that yields:

$$up_{(v,\ldots 1)} - v^m > up_{\vec{1}_n} - 1 \tag{B.13}$$

where $v = \arg\max_{1<v\leq n} \left[up_{(v,1,\ldots,1)} - v^m\right]$, which is a contradiction to Equation 2.13. □

B.2. Underlying signals

There are two options, one "good" and one "bad." A priori, each voter gets a signal for each alternative

$$s_{ib} \sim \begin{cases} N(\mu_g, \sigma_i) \text{ if option } b \text{ is "good."} \\ N(\mu_b, \sigma_i) \text{ if option } b \text{ is "bad."} \end{cases} \tag{B.14}$$

where σ_i is a measure of voter i's information, and $\mu_g > \mu_b$ are the means of the good and bad options.

Since (by assumption) $\mu_g > \mu_b$, then $s_{ib} > s_{i(1-b)}$ if and only if $\Pr[\text{ option } b \text{ is good }] > \frac{1}{2}$. Thus voter i will vote for option b if and only if $s_{ib} > s_{i(1-b)}$.

Thus voter i's probability of voting for the good option is

$$\Pr[\text{ Voter } i \text{ votes for the good option }] = \Pr\left[N\left(\mu_g, \sigma_i^2\right) > N\left(\mu_b, \sigma_i^2\right)\right] \tag{B.15}$$

Thus we define

$$p_i \stackrel{\text{def}}{=} \Pr\left[N\left(\mu_g, \sigma_i^2\right) > N\left(\mu_b, \sigma_i^2\right)\right] \tag{B.16}$$

Since the signals are independent,

$$p_i = \Pr\left[N(\mu_g - \mu_b, 2\sigma_i^2)\right] > 0 \tag{B.17}$$

This means

$$p_i = \Pr\left[N(0,1) > \frac{\mu_b - \mu_g}{\sqrt{2}\sigma_i}\right] \tag{B.18}$$

$$= \frac{1 - \operatorname{erf}\left(\frac{\mu_b - \mu_g}{2\sigma_i}\right)}{2} \tag{B.19}$$

For most of the analysis, we will focus on the probability p_i rather than the underlying signals s_{i0}, s_{i1}.

BIBLIOGRAPHY

Mridul Agarwal and Vaneet Aggarwal. Regret bounds for stochastic combinatorial multi-armed bandits with linear space complexity. arXiv preprint arXiv:1811.11925, 2018.

Amitanand S Aiyer, Lorenzo Alvisi, Allen Clement, Mike Dahlin, Jean-Philippe Martin, and Carl Porth. BAR fault tolerance for cooperative services. In *Proceedings of the twentieth ACM symposium on Operating systems principles*, pages 45–58, 2005.

Humoud Alsabah and Agostino Capponi. Pitfalls of bitcoin's proof-of-work: R&d arms race and mining centralization. *Available at SSRN 3273982*, 2020.

Yackolley Amoussou-Guenou, Bruno Biais, Maria Potop-Butucaru, and Sara Tucci Piergiovanni. Rational vs byzantine players in consensus-based blockchains. In *AAMAS*, pages 43–51, 2020.

Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain. In *Italian Conference on Cyber Security (06/02/18)*, January 2018. URL https://eprints.soton.ac.uk/415083/.

RB Bapat and MI Beg. Order statistics for nonidentically distributed variables and permanents. *Sankhyā: The Indian Journal of Statistics, Series A*, pages 79–93, 1989.

Iddo Bentov, Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. *IACR Cryptol. ePrint Arch.*, 2016(919), 2016.

Bruno Biais, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta. The blockchain folk theorem. *The Review of Financial Studies*, 32(5):1662–1715, 2019.

Binance. Delegated proof of stake explained, 2020. URL https://academy.binance.com/en/articles/delegated-proof-of-stake-explained.

Binance Academy. https://academy.binance.com/en/glossary/transactions-per-second-tps, 2021.

Bitcoin Wiki. https://en.bitcoin.it/wiki/Confirmation, 2021.

Bitshares. Delegated proof of stake (dpos), 2021. URL https://how.bitshares.works/en/master/technology/dpos.html.

Steven Brams and Peter C. Fishburn. *Approval Voting*. Springer, 2007. doi: 10.1007/978-0-387-49896-6.

Ethan Buchman. Tendermint: Byzantine fault tolerance in the age of blockchains, 2016.

Vitalik Buterin, Zoë Hitzig, and E Glen Weyl. A flexible design for funding public goods. *Management Science*, 65(11):5171–5187, 2019.

Cambridge University. Cambridge bitcoin electricty consumption index, 2021. URL https://cbeci.org/.

Alessandra Casella. Storable votes. *Games and Economic Behavior*, 51(2):391–419, 2005.

Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, page 173–186. USENIX Association, 1999.

Nicolo Cesa-Bianchi and Gábor Lugosi. Combinatorial bandits. *Journal of Computer and System Sciences*, 78(5):1404–1422, 2012.

J. Chen and S. Micali. Algorand. ArXiv: abs/1607.01341, 2016.

Wei Chen, Yajun Wang, and Yang Yuan. Combinatorial multi-armed bandit: General framework and applications. In *International Conference on Machine Learning*, pages 151–159. PMLR, 2013.

Wei Chen, Wei Hu, Fu Li, Jian Li, Yu Liu, and Pinyan Lu. Combinatorial multi-armed bandit with general reward functions. In *Proceedings of the 30th International Conference on Neural Information Processing Systems*, pages 1659–1667, 2016.

Richard Combes, M Sadegh Talebi, Alexandre Proutiere, and Marc Lelarge. Combinatorial bandits revisited. *arXiv preprint arXiv:1502.03475*, 2015.

Lin William Cong, Zhiguo He, and Jiasun Li. Decentralized mining in centralized pools. *The Review of Financial Studies*, 34(3):1191–1235, 2021.

Tim Copeland. Steem vs tron: The rebellion against a cryptocurrency empire. *Decrypt*, 2020.

Cosmos. Validator FAQ. https://hub.cosmos.network/main/validators/validator-faq.html, 2021.

Cryptopedia. What are proof of stake (PoS) and delegated proof of stake (DPoS)?, 2021. URL https://www.gemini.com/cryptopedia/proof-of-stake-delegated-pos-dpos#section-delegated-proof-of-stake.

Curve. Understanding voting. https://resources.curve.fi/base-features/understanding-voting, 2021.

Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz

Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. IEEE, 2020.

Devdatt P. Dubhashi and Alessandro Panconesi. *Concentration of measure for the analysis of randomized algorithms*. Cambridge University Press, 2009.

David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109, 2019.

Edith Elkind, Piotr Faliszewski, Piotr Skowron, and Arkadii Slinko. Properties of multiwinner voting rules. *Social Choice and Welfare*, 48(3):599–632, 2017.

Aurora EOS. EOS voting guide. https://medium.com/@auroraeos/eos-voting-guide-3bf4e0be251b, September 2018.

Etherscan. Ethereum uncle count and rewards chart. https://etherscan.io/chart/uncles, 2022.

Giulia Fanti, Leonid Kogan, and Pramod Viswanath. Economics of proof-of-stake payment systems. Technical report, Working paper, 2019.

Manuel Fernández and Stuart Williams. Closed-form expression for the poisson-binomial probability density function. *IEEE Transactions on Aerospace and Electronic Systems*, 46 (2):803–817, 2010.

Flashbots. https://explore.flashbots.net/, 2021.

Jingxing Gan, Gerry Tsoukalas, and Serguei Netessine. Initial coin offerings, speculation, and asset tokenization. *Management Science*, 67(2):914–931, 2021a.

Rowena Gan, Gerry Tsoukalas, and Serguei Netessine. To infinity and beyond: Financing platforms with uncapped crypto tokens. *Available at SSRN 3776411*, 2021b.

Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The Bitcoin backbone protocol: Analysis and applications. In *EUROCRYPT*, pages 281–310. Springer, 2015.

Rodney Garratt and Maarten RC van Oordt. Why fixed costs matter for proof-of-work based cryptocurrencies. *Available at SSRN 3572400*, 2020.

Peter Gaži, Aggelos Kiayias, and Dionysis Zindros. Proof-of-stake sidechains. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 139–156. IEEE, 2019.

Gitcoin. Discover and fund extraordinary public goods. https://gitcoin.co, 2021a.

Gitcoin. Gitcoin results. https://gitcoin.co/results, 2021b.

Gleehokie, 1337micro, Chanryma, testzcrypto, hkshwa, bytemaster, and nathanhourt. EOS.IO technical white paper v2, 2018. URL https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

D. H. Glueck, A. Karimpour-Fard, J. Mandel, L. Hunter, and K. E. Muller. Fast computation by block permanents of cumulative distribution functions of order statistics from several populations. *Communications in Statistics - Theory and Methods*, 37(18):2815–2824, 2008.

Rafael Hortala-Vallve. Qualitative voting. *Journal of theoretical politics*, 24(4):526–554, 2012.

Qian Hu, Biwei Yan, Yubing Han, and Jiguo Yu. An improved delegated proof of stake consensus algorithm. *Procedia Computer Science*, 187:341–346, 2021.

Gur Huberman, Jacob D Leshno, and Ciamac Moallemi. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *The Review of Economic Studies*, 03 2021. ISSN 0034-6527. doi: 10.1093/restud/rdab014. URL https://doi.org/10.1093/restud/rdab014. rdab014.

Ada Hui. Arbitration challenged in hostile work environment lawsuit. https://www.coindesk.com/markets/2020/07/09/tron-arbitration-challenged-in-hostile-work-environment-lawsuit/, July 2020.

InsideTheSimulation. https://ethmerge.com/, 2021.

Kose John, Thomas J Rivera, and Fahad Saleh. Economic implications of scaling blockchains: Why the consensus protocol matters. *Available at SSRN*, 2020.

Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.

D.M. Kilgour. Approval balloting for multi-winner elections. In *Handbook on Approval Voting*. Springer, Berlin, Heidelberg, 2010.

Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing Bitcoin security and performance with strong consistency via collective signing. In *USENIX*, pages 279–296, 2016.

Steven P Lalley and E Glen Weyl. Quadratic voting: How mechanism design can radicalize democracy. In *AEA Papers and Proceedings*, volume 108, pages 33–37, 2018a.

Steven P. Lalley and E. Glen Weyl. Nash equilibria for quadratic voting. *Microeconomics:*

Welfare Economics & Collective Decision-Making eJournal, 2018b.

Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

Stefanos Leonardos, Daniël Reijsbergen, and Georgios Piliouras. Weighted voting on the blockchain: Improving consensus in proof of stake protocols. *International Journal of Network Management*, 30(5):e2093, 2020.

Andrew Lewis-Pye and Tim Roughgarden. A general framework for the security analysis of blockchain protocols. *arXiv preprint arXiv:2009.09480*, 2020.

Andrew Lewis-Pye and Tim Roughgarden. How does blockchain security dictate blockchain implementation? *arXiv preprint arXiv:2109.04848*, 2021.

James Peter Thomas Lovejoy. An empirical analysis of chain reorganizations and double-spend attacks on proof-of-work cryptocurrencies. Master's thesis, Massachusetts Institute of Technology, 2020.

MakerDao. Mkr governance 101. https://makerdao.com/en/governance/, 2021a.

MakerDao. https://vote.makerdao.com/polling/QmUqfZRv?network=mainnet#poll-detail, 11 2021b.

MakerDao. Add wbtc-c as a new vault type. https://vote.makerdao.com/polling/QmdVYMRo?network=mainnet#poll-detail, 11 2021c.

Andrei Matveenko, Azamat Valei, and Dmitriy Vorobyev. Participation quorum when voting is costly. *European Journal of Political Economy*, page 102126, 2021.

Yuli Meng, Zhao Cao, and Dacheng Qu. A committee-based byzantine consensus protocol for blockchain. In *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, pages 1–6. IEEE, 2018.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

Richard G. Niemi. The problem of strategic behavior under approval voting. *The American Political Science Review*, 78(4):952–958, 1984. ISSN 00030554, 15375943. URL http://www.jstor.org/stable/1955800.

Hannu Nurmi and Rachel Perez Palha. A theoretical examination of the ranked choice voting procedure. In *Transactions on Computational Collective Intelligence XXXVI*, pages 1–16. Springer, 2021.

Nxt Community. Nxt whitepaper. https://nxtdocs.jelurida.com/Nxt_Whitepaper, 2016.

EOS NY. The missing piece to the EOS incentive model: Part 1. https://medium.com/eos-new-york/the-missing-piece-to-the-eos-incentive-model-bd39977d243f, May 2019.

Emiliano S Pagnotta. Decentralizing money: Bitcoin prices and blockchain security. *The Review of Financial Studies*, 01 2021. ISSN 0893-9454. doi: 10.1093/rfs/hhaa149. URL https://doi.org/10.1093/rfs/hhaa149. hhaa149.

Panther.io. Privacy preserving protocol for digital assets. https://www.pantherprotocol.io/resources/panther-protocol-v-1-0-1.pdf, 07 2021.

Tuan D. Pham and Lanh T. Tran. On functions of order statistics in the non IID case. *Sankhyā: The Indian Journal of Statistics, Series A*, pages 251–261, 1982.

Eric A Posner and E Glen Weyl. Quadratic voting as efficient corporate governance. *The University of Chicago Law Review*, 81(1):251–272, 2014.

Eric A Posner and E Glen Weyl. Voting squared: Quadratic voting in democratic politics. *Vand. L. Rev.*, 68:441, 2015.

Julien Prat and Benjamin Walter. An equilibrium model of the market for bitcoin mining. *Journal of Political Economy*, 129(8):000–000, 2021.

David Quarfoot, Douglas von Kohorn, Kevin Slavin, Rory Sutherland, David Goldstein, and Ellen Konar. Quadratic voting in the wild: real people, real votes. *Public Choice*, 172(1): 283–303, 2017.

Idan Rejwan and Yishay Mansour. Top-k combinatorial bandits with full-bandit feedback. In *Algorithmic Learning Theory*, pages 752–776. PMLR, 2020.

Ioanid Roşu and Fahad Saleh. Evolution of shares in a proof-of-stake cryptocurrency. *Management Science*, 67(2):661–672, 2021.

James Rubin. Block.one pays $27.5m to settle class-action lawsuit. *Coindesk*, June 2021.

Fahad Saleh. Blockchain without waste: Proof-of-stake. *The Review of financial studies*, 34 (3):1156–1190, 2021.

Tezos. Tezos governance. https://wiki.tezosagora.org/learn/governance, 2021.

The Block. https://www.theblockcrypto.com/data/on-chain-metrics/ethereum, 2021.

The Interchain Foundation. https://blog.cosmos.network/consensus-compare-tendermint-bft-vs-eos-dpos-46c5bca7204b, September 2017.

TRON. TRON whitepaper version 2.0. https://tron.network/static/doc/white_paper_v_2_0.pdf, December 2018.

Gerry Tsoukalas and Brett Hemenway Falk. Token-weighted crowdsourcing. *Management Science*, 66(9):3843–3859, 2020.

Uniswap. Uniswap governance. https://gov.uniswap.org, 2021.

Brent Xu, Dhruv Luthra, Zak Cole, and Nate Blakely. EOS: An architectural, performance, and economic analysis. *Retrieved June*, 11:2019, 2018.

Fan Yang, Wei Zhou, QingQing Wu, Rui Long, Neal N Xiong, and Meiqi Zhou. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 7:118541–118555, 2019.

Peilin Zheng, Zibin Zheng, Jiajing Wu, and Hong-Ning Dai. Xblock-ETH: Extracting and exploring blockchain data from Ethereum. *IEEE Open Journal of the Computer Society*, 1:95–106, 2020a.

Weilin Zheng, Zibin Zheng, Hong-Ning Dai, Xu Chen, and Peilin Zheng. Xblock-EOS: Extracting and exploring blockchain data from EOSIO. arXiv preprint arXiv:2003.11967, 2020b.