Elections, civic trust, and digital literacy:

The promise of blockchain as a basis for common knowledge

**Author:** Mark Alfano, Macquarie University

**Keywords:** elections, civic trust, digital literacy, blockchain, common knowledge

**Abstract:** Few recent developments in information technology have been as hyped as blockchain, the first implementation of which was the cryptocurrency Bitcoin. Such hype furnishes ample reason to be skeptical about the promise of blockchain implementations, but I contend that there’s something to the hype. In particular, I think that certain blockchain implementations, in the right material, social, and political conditions, constitute excellent bases for common knowledge. As a case study, I focus on trust in election outcomes, where the ledger records not financial transactions but vote tallies. I argue that blockchain implementations could foster warranted trust in vote tallies and thereby trust in the democratic process. Finally, I argue that if the promise of blockchain implementations as democratic infrastructure is to be realized, then democracies first need to ensure that these material, social, and political conditions obtain.

Elections, civic trust, and digital literacy:

The promise of blockchain as a basis for common knowledge

**1 Introduction**

Few recent developments in information technology have been as hyped as blockchain, the first implementation of which was the cryptocurrency Bitcoin (Nakamoto 2008). Such hype furnishes ample reason to be skeptical about the promise of blockchain implementations, but when something provokes so much fascination and excitement, we should also ask whether the smoke means that there’s fire. My contention is that there is. In particular, I think that certain blockchain implementations, in the right material, social, and political conditions, constitute excellent bases for common knowledge, which in turn should function to promote public goods such as civic trust in the outcomes of elections and referenda. If this is right, then philosophers should take note, as they are among best-prepared to think through the normative questions that such a development raises. In particular, I contend that philosophers in the fields of social epistemology and political philosophy should pay more attention to blockchain implementations.

Which features of blockchains are most epistemically important? I am not here interested in the identity-verifying use of private keys. Nor do I have anything to say about cryptocurrencies such as Bitcoin and Ethereum. What I want to focus on instead are the features of blockchains from which they draw their names. A blockchain is a persistent, transparent, distributed, append-only ledger that records a sequence of events. The events could be financial transactions, but they could just as easily be records of supply chain handoffs or vote tallies. What’s recorded in the ledger can never be deleted or changed unless a single actor manages to acquire more than half of the computing power in the network. However, new information can be added to the ledger, and every addition to one copy of the ledger is automatically and verifiably added to every other copy of the ledger. As a case study, I focus on trust in election tallies, where the ledger records votes at the precinct, city, regional, and national level. I argue that blockchain implementations could foster trust in election tallies and thereby trust in the democratic process.

Here is the plan for this paper: in section 2, I recount the essentials of a recent case in which trust in the official outcome of a hotly-contested presidential election was augmented by a digital open governance initiative. In section 3, I employ the concept of common knowledge to show that, in such contexts, warranted trust is associated with there being bases for common knowledge. I argue that certain blockchain implementations, in the right material, social, and political conditions, constitute excellent bases for common knowledge among voters and other citizens and denizens. I conclude in section 4 by arguing that, if the promise of blockchain implementations as democratic infrastructure is to be realized, then democracies need to ensure that these material, social, and political conditions obtain — a much more challenging task than building and maintaining the technological infrastructure itself.

**2 A case study in digital open governance**

Consider the following scenario: in the second decade of the twenty-first century, a diverse country with a population of hundreds of millions is holding an election. The citizenry is highly polarized around just two candidates, both of whom enjoy support from over 40% of voters. On both sides, there are hints and allegations of tampering and fraud. The tallies at local voting precincts are to be aggregated at multiple levels through a byzantine process that many are loath to trust. As the official tally is assembled, both campaigns indicate that they may be willing to contest the outcome in the courts and even in the streets. Ominous messages spread online, some of them from legitimate accounts but others seemingly from pseudonymous sock-puppets and anonymous trolls. Foreign interference cannot be ruled out. There is a genuine prospect of online rancor spilling over into the real world in the form of targeted harassment and violence.

No, I’m not talking about the 2016 or 2020 US Presidential election, though what I am talking about has implications for American and other elections that I will discuss in section 4. I refer to the 2014 Indonesian Presidential election and, to a lesser extent, the 2019 Indonesian Presidential election. In 2014, Probow Subainto and Joko Widodo vied for the highest office in the nation. Voting was conducted with hand-marked paper ballots at over 470,000 local polling stations across the Indonesian archipelago. Vote tallies at each polling station were recorded on hand-marked paper sheets (known as C1 forms) and aggregated at the level of the subdistrict, the district, the city regency, the province, and the whole nation.[[1]](#footnote-1) The potential for fraud in such a system is apparent, and the fact that Indonesia had a poor reputation when it came to corruption led many to be wary of the final official tally.

However, three years prior to the election, Indonesia had joined the Open Government Partnership, a multilateral initiative among dozens of countries and sub-national entities that seeks to promote open government and fight corruption through concrete commitments and the use of new technologies. As part of its commitment to open government, Indonesia’s Elections General Commission (KPU) shared election data, in the form of digital scans of the C1 forms and aggregate forms at the five higher levels, on its official website ([www.kpu.go.id](http://www.kpu.go.id)). This made it possible — at least in principle — to verify that aggregation from polling station to subdistrict, from subdistrict to district, from district to city regency, from city regency to province, and from province to the whole nation was done correctly. However, with nearly half a million C1 forms to verify, citizens could be forgiven for continuing to distrust the process. On the assumption that it would take ten seconds to verify a single C1 form, any given individual would need to do over 13,000 hours of work to verify all C1 forms. Verifiability in principle is valuable, but public verifiability presumably sets a higher bar.

Enter Ainun Najib, an Indonesian technology expert. Like many others, Najib was concerned *both* that the official tally be *trustworthy* and that it be *trusted*, especially by supporters of the losing candidate. Immediately after the election, Najib, together with Andrian Kurniady and several others, co-founded Kawal Pemilu ([kawalpemilu.org](https://kawalpemilu.org)), which is Indonesian for “guard the election.” Rather than relying on sometimes-buggy optical character recognition (OCR) to automatically extract tallies from the digitized C1 forms, this citizen-led open government initiative recruited approximately 7000 volunteers from Indonesia and the global Indonesian diaspora to manually examine every single scanned C1 form made available on the KPU website and extract vote tallies at the level of the polling station. Those tallies were then entered into a secure back-end website, aggregated at the five higher levels, and outputted to a public-facing website that compared the government’s official tallies with those as determined by Kawal Pemilu. The public-facing site made visible both the scanned C1 forms (but not individual ballots) and the extracted tally data, and it made available an online form that enabled users to report errors. This herculean effort was completed in less than half a week with a start-up cost of just $54.

Lo and behold, the official tally and the tally as established by Kawal Pemilu were remarkably similar at all levels of aggregation, with Joko Widodo edging out Prabowo Subianto by just over six percentage points. The Prabowo camp was at the time contesting the election in the courts. During court hearings, members of Kawal Pemilu testified alongside KPU officials and expert witnesses, leading the court to decide in favor of Joko Widodo. Furthermore, because of the remarkable transparency displayed both by KPU and by Kawal Pemilu, supporters of the losing candidate, while no doubt disappointed, largely accepted the result as legitimate.

Five years later, the same two candidates again vied for the Indonesian Presidency. This time Kawal Pemilu replicated its efforts and was joined by other open government efforts such as Selamatkan-Jaga Demokrasi (<https://indonesia2019.ballotbox.eu/>), which uses blockchain technology to ensure that, once uploaded, the digitized C1 forms and other data are immutable. This new twist on transparency adds valuable reliability to the endeavor because it ensures that, once a vote tally is uploaded to the ledger, it cannot be modified accidentally or by malign actors unless someone manages to take control of more than fifty percent of the computing power associated with the blockchain — a feat that, while technologically possible, would be virtually impossible to keep a secret. Both Kawal Pemilu (55.29% for Joko Widodo, 44.71% for Prabowo Subianto) and Selamatkan-Jaga Demokrasi (51.35% for Joko Widodo, 46.69% for Prabowo Subianto) corroborated the headline result of the official vote tally (55.50% for Joko Widodo, 44.50% for Prabowo Subianto). Indonesia (along, I should add, with Estonia) is fast emerging as a global forerunner in election security, open governance, and citizen oversight. In the next section, I explore in more technical and philosophical detail how blockchain helps to ensure election security.

**3 Common knowledge and trust in election tallies**

In this section, I explain in more depth how a modern election system is organized, with emphasis on the trustworthiness of election systems. A normatively acceptable election system must be *both* *trustworthy* and *trusted*, especially by supporters of the losing candidate. For this to be the case, the system must be contestable and strongly defensible, as these technical terms are defined in the literature. I then argue that what makes an election system contestable and strongly defensible is its containing or constituting a basis for common knowledge of the election outcome.

**3.1 Defensibility and contestability of election systems**

To better understand how and to what extent a blockchain implementation such as Selamatkan-Jaga Demokrasi may help ensure the trustworthiness of an election, let’s break down the pipeline from voter intention to electoral outcome. The purpose of an election or referendum is to determine the will of the people. The process by which the will of the people is measured is illustrated in a somewhat stylized fashion in Figure 1.



**Figure 1: the electoral pipeline and threats to election security.**

 Moving from top to bottom, we begin with each individual voter’s intention, which is an internal mental state. That mental state is *expressed* by marking a paper ballot by hand. Next, at the precinct level, each ballot is recorded via *manual addition* by election officials (with witnesses present) on a paper form (e.g., the C1 form) until all ballots have been counted. The paper ballots are then securely stored to ensure that chain of custody is maintained (this will be important later). Next, the precinct tally is *digitized* as an image file (again with witnesses present) and the physical C1 form is, like the individual paper ballots, securely stored to preserve chain of custody. Meanwhile, the digitized tally is uploaded to a secure server where all other digitized tallies from other precincts are also uploaded. It would be possible to upload both the image file and the number of votes for each candidate at the same time, but in the Indonesian case, only the image is uploaded. However, as mentioned above, KPU makes all digitized C1 forms freely available via its website. The next steps occur in parallel. On the official side, the tallies of the C1 forms are aggregated by hand with witnesses present at the city, regional, and national levels, as described above, until the national tally is determined. On the citizen audit side, volunteers for Kawal Pemilu and Selamatkan-Jaga Demokrasi examine the digitized C1 forms and *extract* numeric representations of the tallies, which they then upload to their own secure servers. It is then trivially easy to *digitally add up* all the votes that each candidate received and then *compare* the vote totals to determine the electoral outcome. It is also trivially easy to compare the official national tallies and outcome with the citizen-audited tallies and outcome.

In the event of either large discrepancies between the official result and the open governance audit or allegations of mistakes or vote fraud, it is then vitally important for the whole process to be verified and, if needed, corrected. People need to be able to trust that the official outcome accurately reflects the will of the people. And that means that each step in the process just described needs to be publicly and independently verifiable. It is for this reason that election experts have long held that voting systems should be “software independent,” in the sense that “an undetected change or error in its software cannot cause an undetectable change or error in an election outcome” (Rivest 2008). As Appel et al. (forthcoming) point out, “Software independence is similar to tamper-evident packaging: if somebody opens the container and disturbs the contents, it will leave a trace.” This leads Appel and colleagues to argue for the desirability of voting systems that are both (strongly) *defensible* and *contestable*.

These notions refer to two counterfactual conditionals. First, consider the counterfactual, “If the electoral outcome were trustworthy, then the system would produce public evidence that the electoral outcome was trustworthy.” When this counterfactual holds, the system is defensible. Defensibility is important because it makes the system immune to “crying wolf” by the losing candidate and their supporters. There’s little point in claiming that you were robbed of electoral victory if it is publicly demonstrable that you lost fair and square. Next, consider the counterfactual, “If the electoral outcome were not trustworthy, then the system would produce public evidence that the electoral outcome was not trustworthy.” When this counterfactual holds, the system is contestable.[[2]](#footnote-2) Contestability is important because it documents errors. However, simply being able to verify that errors or tampering occurred is not as desirable as having a guaranteed way to also *correct* errors and tampering that have been detected. This leads Appel and colleagues to define “strong defensibility” as defensibility *plus* the ability to reconstruct, with convincing *public* evidence, the correct result “using only the ballots and ballot records of the current election.”

Thus conceptualized, (strong) defensibility and contestability are what Philip Pettit (2015) calls *modally robust goods*. A defensible election system isn’t simply one that produces public evidence of trustworthiness in the actual world, but also one that would provide certain kinds of public evidence in nearby possible worlds in which the electoral outcome was trustworthy. A contestable election system isn’t simply one that produces public evidence of untrustworthiness in the actual world, but also one that would provide certain kinds of public evidence in nearby possible worlds in which the electoral outcome was not trustworthy. Likewise, a strongly defensible election system is one that, were the contestability condition to trigger a public indication that the official outcome was not trustworthy, would make it possible to reconstruct the correct outcome using pre-existing, publicly available evidence.[[3]](#footnote-3)

Relatedly, (strongly) defensible and contestable election systems *reliably signal*, via publicly accessible evidence, that the electoral infrastructure is trustworthy, which means that they ensure what Jones (2012) calls “rich trustworthiness.” Jones’s account of rich trustworthiness is formulated for the dyadic interpersonal context, but Alfano & Huijts (2020) show that it can be extended to larger contexts, including institutions and governance. In line with the arguments provided by Alfano & Huijts, the envisaged blockchain implementation for election infrastructure minimizes the length of epistemic geodesics (because citizens can directly access digitized C1 forms), enables citizens to express their voice in a meaningful way (because they can report errors online via the Kawal Pemilu website), and promotes diversity (because any citizen with an internet connection can participate, which is much less demanding than, for instance, requiring in-person attendance at town halls or court hearings).

**3.2 Bases for common knowledge ensure (strong) defensibility and contestability**

To ensure the strong defensibility and contestability of a voting system, it is essential that each step in the process depicted in Figure 1 be publicly verifiable and reconstructable. Beginning with *expression*, Appel et al. (forthcoming) argue that the “only known practical technology for contestable, strongly defensible voting is a system of hand-marked paper ballots, kept demonstrably physically secure, counted by machine, audited manually, and recountable by hand.” This leads them to argue against the use of so-called electronic “ballot-marking devices” (BMDs) and all-in-one “direct-recording electronic voting machines with a voter-verifiable paper audit trail” (DRE+VVPATs), as such devices can be hacked if they are connected to a network, hacked even if air-gapped using USB plug-ins, or pre-hacked during manufacture at the level of either firmware or hardware. The *expression* and *manual addition* steps thus crucially rely on hand-marked paper ballots and precinct-level tallies (e.g., C1 forms) that are securely stored to preserve chain of custody and can be recounted with witnesses present as part of either a full recount or a risk-limiting post-election audit (Stark 2008, 2009).[[4]](#footnote-4)

Supposing that each C1 form or a large enough representative, random sample of C1 forms is publicly verified as accurate(-enough), a suitably-implemented blockchain could handle the remaining stages (*digitization* through *comparison*). This is because *digitization* could be done before witnesses just like the manual recount, ensuring that scanned precinct-level tallies correspond to the paper copies they purportedly represent. Next, because a blockchain is append-only, all interested parties could be sure that the digitized precinct-level tallies had not been modified, either by malign actors or by bugs in the electoral software. Next, *manual data extraction* from the digitized copies could be publicly verified via the reporting mechanism enabled by Kawal Pemilu, as described above. Finally, *computerized addition* and *comparison* could be publicly verified by any interested party using simple arithmetic.

If this is right, then an election system (1) based on hand-marked paper ballots and precinct-level tallies that (2) preserves chain of custody and (3) allows for partial and full manual recounts with witnesses present can reasonably be conjoined with a blockchain implementation in which (4) scans of precinct-level tallies are uploaded before witnesses, (5) errors can be reported by interested parties, and (6) national-level summation and comparison can be performed by anyone with a calculator or even just paper and pencil. In other words, it should be possible to build an election system that combines paper records as its ground truth with an append-only digital ledger to make publicly verifiable each step of the process that translates voters’ intentions into the outcome of the election.

Such a hybrid election system seems to satisfy Lewis’s (1969, p. 56) definition of common knowledge:

Let us say that it is *common knowledge* in a population P that B if and only if some state of affairs A holds such that:

1. Everyone in P has reason to believe that A holds.
2. A indicates to everyone in P that everyone in P has reason to believe that A holds.
3. A indicates to everyone in P that B.

We can call any such state of affairs A a *basis* for common knowledge in P that B.

In the envisioned system, P refers to the citizenry or possibly even the whole world (given that other nations and anyone with an interest in global democracy has reason to care about the integrity of elections not only at home but also abroad). Next, B refers to the proposition that states who won the election or referendum (e.g., Joko Widodo in Indonesia in 2014 and 2019). Finally, A refers to the hybrid election system that involves paper records, witnesses, and a secure blockchain implementation.

As Lewis points out, the fact that there exists a basis for common knowledge does not guarantee that every member of the population actually acquires one or more levels of mutual knowledge. That further step depends on the inductive standards of the population, their background information, their rational capacities, and so on. Without a basis for common knowledge, though, arriving at higher-order mutual knowledge would be extremely difficult, which would in turn undercut both contestability and (strong) defensibility. In the final section of this paper, I address the material, social, and political conditions that must be met for a hybrid paper-witness-blockchain election system to actually contain or constitute a basis for common knowledge of election outcomes in a population.

**4 Material, social, and political conditions for common knowledge via blockchain**

In order to reap the benefits of coordination, cooperation, and civic trust made possible by common knowledge, we humans have developed a variety of technologies that constitute bases for common knowledge. Their usefulness in this regard depends on how effectively and how reliably they do the job of *indicating* for members of the population. As Lewis (1969, p. 57) notes, these technologies and cultural forms include explicit agreements, such as promises and other contractual commitments. They also include salience markers afforded by or built into the environment. For example, church-bells pealing the time every hour helps ensure that everyone in town knows what time it is, and that everyone knows that everyone knows what time it is — but only if they peal reliably enough for long enough and everyone has sufficient reason to trust that the operators of the bells will continue to prove reliable. Likewise, mosques sounding the call to prayer helps ensure that practicing Muslims know that it is time to face Mecca, and that all other practicing Muslims in the area know likewise — but only if the call is sounded reliably enough for long enough and everyone has sufficient reason to trust that the operator of the call will continue to prove reliable. A further basis for common knowledge is precedent. For example, the fact that everyone in my community demonstrably drives on the right rather than the left side of the road strongly indicates that everyone in this community knows that everyone drives on the right, and that everyone knows that every knows this, and so on.

More recently, Michael Chwe (2001) has argued that the cultural form of sitting in inward-facing circles is a basis for common knowledge because such a circle is geometrically ideal for ensuring simultaneous joint attention and the possibility of making eye contact with any other particular participant. Indeed, anthropologists now speculate, based on evidence from contemporary small-band hunter-gatherers such as the Ju/’hoansi Bushmen, that human language evolved in part to make possible communal discussions around the campfire at night, using public announcements to the inward-facing circle that naturally forms around the fire as a basis for common knowledge (Wiessner 2014).

These examples share an important feature: a unique copy of the basis for common knowledge is simultaneously accessible to all members of the relevant population. Only when all parties to a contract have verified that an agreement has been made does it go into effect. Church bells and the call to prayer are audible to everyone in town or the neighbrhood. Everyone around the inward-facing circle is present for announcements. Blockchain implementations break this pattern. Instead of handling version control by having a unique item or event that serves as a basis for common knowledge, a blockchain implementation distributes a copy of the basis for common knowledge to every member of the population and ensures algorithmically that every copy is identical. In the envisioned election system, this could be handled in at least three ways. First, a centralized, permissioned blockchain run by the government could be set up, for example, by KPU. Second, a centralized, permissioned blockchain run by trusted citizen-auditors could be set up, for example, by Kawal Pemilu or Selamatkan-Jaga Demokrasi.[[5]](#footnote-5) Third, a permissioned blockchain run by all voters could be set up. Indeed, all three systems could in principle operate in parallel and keep tabs on each other. What this in turn means is that everything one voter can see in or infer from their copy of the shared blockchain is also something that they can expect each other voter to see in or infer from your copy.

From this perspective, the hype surrounding blockchain starts to make some sense. Blockchain is just the next step in a long human tradition of fostering coordination, cooperation, and trust with technologies, artifacts, and cultural forms that serve as bases for common knowledge. A blockchain could be used to establish a basis of common knowledge for vote tallies (alongside hand-marked paper ballots and witnesses). However, this promise will only be fulfilled if the polity has secure digital infrastructure, public access to online resources, and public computing, and only if citizens possess sufficient numeracy and digital literacy and higher-order knowledge of their compatriots’ secure digital infrastructure, public access to online resources, and public computing. In other words, blockchain is a promising basis for common knowledge in democratic societies, but only if they also invest in cyber-security, digital literacy, access (e.g., smartphones or laptops for all, free and fast Internet), public computing infrastructure, civic trust, and numeracy.

However, this optimistic perspective assumes that all citizens’ background knowledge, inductive standards, and rational capacities are sufficiently similar. Alas, in many contemporary self-styled democracies, this is far from certain. While the Indonesian and Estonian cases are encouraging, other countries should make us less sanguine. For example, in 2016, Donald Trump notoriously indicated before the US Presidential election that he would accept the result only if it indicated that he won. Then, even when he won the election in the Electoral College despite losing the popular vote, he alleged that three million ballots had been illegally cast for his opponent — an unsubstantiated allegation that many of his supports (claim to) accept. This paper was written during the summer of 2020, and when it was submitted for peer-review, Trump was again indicating that he would accept the result of the 2020 US Presidential election if he won.

Can a hybrid paper-witness-blockchain do anything to ensure common knowledge of the election outcome in a largely-failed democracy such as the contemporary United States?[[6]](#footnote-6) I confess to being pessimistic on this count. If that pessimism is warranted, then we should recognize that the technological infrastructure we build for election systems is only as valuable as its weakest link. If a large proportion of the voting public cannot be expected to understand the infrastructure (a question of digital literacy) or the paper ballots and witnesses essential to that infrastructure (a question of civic trust), then no blockchain implementation — no matter how snazzy — will help ensure that election outcomes are trusted when and only when they are (strongly) defensible and contestable.

**References**

Alfano, M. & Huijts, N. (2020). Trust and distrust in institutions and governance. In J. Simon (ed.), *Handbook of Trust and Philosophy*. Routledge.

Appel, A., De Millo, R., & Stark, P. (forthcoming). Ballot-marking devices (BMDs) cannot assure the will of the voters. *Election Law Journal*.

Chwe, M. (2001). *Rational Ritual: Culture, Coordination, and Common Knowledge*. Princeton University Press.

Jones, K. (2012). Trustworthiness. *Ethics*, 123(1): 61-85.

Lewis, D. (1969 / 2002). *Convention*. Blackwell.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Pettit, P. (2015). *The Robust Demands of the Good: Ethics with Attachment, Virtue, and Respect*. Oxford University Press.

Purwanto, A., Zuiderwijk-van Eijk, A., & Janssen, M. (2018). Group Development Stages in Open Government Data Engagement Initiatives: A Comparative Case Studies Analysis. In E. Kalampokis, S. Virkar, P. Parycek, O. Glassey, M. Janssen, H. J. Scholl, & E. Tambouris (Eds.), *Proceedings of 17th IFIP WG 8.5 International Conference, EGOV 2018* (pp. 48-59). Springer. https://doi.org/10.1007/978-3-319- 98690-6\_5.

Rivest, R. (2008). On the notion of ‘software independence’ in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881): 3759-67.

Stark, P. B. (2008). Conservative statistical post-election audits. *Annals of Applied Statistics*, 2: 550-81.

Stark, P. B. (2009). Risk-limiting post-election audits: *p*-values from common probability inequalities. *IEEE Transactions on Information Forensics and Security*, 4:1005-19.

Venkatasubramanian, S. & Alfano, M. (2020). The philosophical basis for algorithmic recourse. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM FAT\*)*.

Wiessner, P. (2014). Embers of society: Firelight talk among the Ju/’hoansi Bushmen. *Proceedings of the National Academy of Sciences*, 111(39): 14027-35.

1. For more details, see url = < <https://odimpact.org/files/case-study-indonesia.pdf> >, accessed 27 August 2020. For a scholarly assessment of the case by an Indonesian expert, see Purwanto et al. 2018). [↑](#footnote-ref-1)
2. Formally, these counterfactuals can be represented as follows: Let *t* be the proposition “the electoral outcome is trustworthy” and  be the operator “the system produces public evidence that….” Then a system is defensible if and only if *t* 🡪 *t* and contestable if and only ~*t* 🡪 *~t*. [↑](#footnote-ref-2)
3. Pettit primarily focuses on robust goods that attach to individuals, such as character virtues. For an example of an analysis of a robust good at the institutional level involving a socio-technical system, see Venkatasubramanian & Alfano (2020). [↑](#footnote-ref-3)
4. A risk-limiting audit uses a representative, random sample of the full population of ballots to enable a null hypothesis significance test of whether the margin of the sample differs significantly from the margin of the official vote count, i.e., whether the difference between the margin in the sample and the margin in the official tally could be expected to occur simply due to sampling error with probability less than *p* for some value of *p* such as .01. [↑](#footnote-ref-4)
5. As an outsider, I should admit that I am not sure how trusted Selamatkan-Jaga Demokrasi is by the Indonesian citizenry. If it lacks trust, then this detail should be read as hypothetical. [↑](#footnote-ref-5)
6. I should also note that the discussion in this paper in no way addresses problem with election systems beyond the scope of enumerating vote tallies. For instance, gerrymandering, disenfranchisement efforts, voter intimidation, and a wide variety of other problems occur before people even make it to the polling station or manage (or at least try) to vote by mail. A comprehensive account of what makes an election system trustworthy in this wider sense is far beyond the scope of this paper. [↑](#footnote-ref-6)