Vote Count and Auditing Solution For Latin America Using Blockchain

Part I
The Static Problems

Since the current state of affairs regarding Guatemalan (and their neighboring nations') voting procedure has already been defined in the documentation attached to the contest one will now take the proverbial jump to directly address the problems found therein. In trying to tackle the issue of eliminating vote tampering and manipulation it became clear just how easy it is to do so under current conditions. The 'paper trail' that was supposed to bring transparency to elections in Latin America is today a cloud of confusion to concerned voters and adding to their sense of alienation and unwillingness to participate in the democratic process.[1] It is a victim of its time, sure (as it is easier for any interested party to doctor voting documents at will with modern technology than it was before, especially considering the vast and growing number of documents in play), but also of it's design: a system that, in order to function properly, relies on a limited amount of votes to be cast (the higher the numbers, the more vulnerable it is). If we are to create a solution for vote counting and auditing, we must be sure that said solution will be flexible and adaptable to generations wielding technology superior to our own. This will likewise have to coexist with government institutions who, as has been well documented, are resistant to change. In Guatemala the paper trail and the Preliminary Results (also notoriously issue laden) are in the purview of the Supreme Electoral Tribunal (TSE). The goal here is to work with them.

[1] Barriers to Electoral Participation in Guatemala: Diagnostic of 4 Municipalities

Part II
'Fiscal Digital'

The work that #Fiscal_Digital has been doing to address the aforementioned issues is a perfect illustration of citizens engaged in meaningful action as enshrined in the principles of democracy's hallowed name. The point here is therefore to refine their work with our technology, and some creative thinking. The main area for improvement which stands out in the current audit and vote count procedure is it's sheer randomness and inexactitude. The conundrum could be laid out as such:

- How to avoid mistakes in, or tampering with, Acta#4 data once it is written on paper. Even if every Acta#4 is miraculously handed over to #Fiscal_Digital for audit after every election it is still quite inexact given that the TSE has already proven to be a central and subservient party in the existing power structures which are responsible for the growing concerns about vote manipulation.
- So how do we avoid relying on central authorities for information for future vote audits. We should create a system wherein auditing can occur immediately, transparently, and in concert with the current process.
- How do we implement such a system without the need to change legislation or without the need for large scale government investment, as we see from past efforts that such principles are doomed to fail, and our goal here is to save money (and, as will be explained later on, perhaps create money too). Of course authenticated e-voting or blockchain based voting are solutions to voter fraud, and encryption of the Acta#4's as soon as they enter the digital database from the voting center is a solution to the faulty

preliminary results, but these are large-scale and expensive projects often requiring a change in legislation.

Part III
The Solutions

What we therefore propose is a simple grassroots solution which Free TON and #Fiscal_Digital can implement when needed.

When looking to Free TON for a solution to the concerns posed by #Fiscal_Digital it is logical to assume that it is not only our technology which can play a role, but also some (admittedly rough) version of our principles of governance, and even labour, as organized by a financial model based on the one currently working on Free TON. In short, as the problem is trust, one proposes a financial incentive for honesty. Together with blockchain encryption technology and organization, open democratic values, and reach, I propose we issue a token, let's call it the 'Democracy Token,' minted only during an election, which can be issued for any election around the globe. The total number of minted tokens will depend on the number of documents. *The essential work of getting people to participate in this token will be the job of #Fiscal_Digital and Free TON on their respective ends*. It goes without saying that what we are proposing is not to eliminate the current system, seeing as that is unrealistic, but to create a new set of checks and balances to make sure the current system isn't being gamed, while hopefully also creating monetary value in the process. The token will work in the following way (the example given is based on Guatemala's vote count system, though, with edits, it can be applied anywhere):

People who participate in the vote count and audit will be divided into two groups respectively, ‘Collators’ and ‘Validators.’ The Collators will first upload copies of the Acta#4 onto *a Free TON blockchain smart contract specially created for releasing Preliminary Results*. The Validators will then confirm these results. The token will be minted by this process: you upload, you validate, you mint tokens. However, these minted tokens will be locked and will only be accessible once it is confirmed that the results are correct. Let’s go into more detail, step by step.

The Collators

The Collators will be people on the ground in Guatemala, at voting centers; volunteers, temporary workers, and witnesses. It goes without saying that Collators will have to create their digital wallet beforehand. With this set in place, a Collator will upload a JPEG of an Acta#4 using an app on their phone to the Free TON blockchain. The JPEGs will be accepted by the smart contract only through the period of Acta#4 creation. At this point they mint X amount of locked tokens per Acta#4, to be distributed if said Acta#4 is accurate. Whoever sends the *first copy* of an Acta#4 will get the most tokens, then progressively less, divided by 2 for every upload of *the same* Acta#4, up until the time is up. This achieves two things: first, it prevents people from sharing their documentation and thereby fosters honesty, second, it prevents a free-for-all overloading the system. The more Collators are participating, the more documents are submitted up until the end of the process, the more tokens will be minted for all. This is obvious, yet in this system we will have another reward mechanism: If 50% of all the documents are submitted the total number of minted tokens will be X, at every additional 10% the total number of minted tokens will double for everyone. If we want to further reduce the possibility of spamming on the Collator mechanism we can introduce a

verifiable delay function which will only make possible submissions from the same device after a certain delay. Those who will verify the Collators will be the Validators.

The Validators

Once the copies of the Acta#4 documents will be uploaded to the blockchain, an anonymous and randomly selected group of Validators, can be people or AI (more on that later) operating anywhere in the world, will compare and verify that the numbers that have been input are correct. How will this work?

- First off, we will have to establish the honesty of a Validator (a process which will simultaneously, indirectly, determine the honesty of the Collators).
- The Validators will be shown photos of both the Government and Collator uploaded Acta#4 documents, Validators have to put in the correct numbers into a blockchain digital Acta#4 of sorts, the correct number for every political party, this will verify the numbers. For every validated document set and number inputs, Validators will mint tokens, locked until the numbers are probabilistically validated.
- If the numbers are correct, the Validators' own input numbers will be put into the pool of ballots and shown to the Validators again later.
- We will also show them fake computer generated Acta#4 documents, if the Validators validate the fake documents their stake will be slashed in a progressive function, meaning that each mistake will be more costly than the last. The Validators will have no way of knowing which documents are real or fake.

- The numbers will be cycled over and over so they will constantly be validating the vote counters, the collators, and themselves.
- By this process of Acta#4 verification, we will be getting an ever-more-exact set of mathematical probabilities as to which documents are correct and which aren't, the more the Validators validate the correct documents the more tokens they mint.
- The way we quantify reputation will be reward-based, much like the system used in AI Neural Networks; on the back end, the validators have a set number of tokens they get per validated document, for every correct pair they get more, for every incorrect pair their tokens will be slashed. This is why the idea of AI Validators could actually work well, we will include AI in this stage to validate the same Acta#4s alongside the humans, the AI creators will also make money.
- In the mechanics of the Validators' process the Byzantine Fault Tolerance algorithm will be used, *for a document to be validated, it must have 66% consensus of the locked Validator tokens, on every round*. So, for example, if there are 10 Validators, 66% will *not* be 7; it will be 66% of the total share of tokens of those 10 Validators, it could mean 5 Validators with an excellent reputation could verify a pair.
- We will have sets of Validators selected randomly for each document, how many per document will be decided based on the total number of registered Validators and the total amount of documents. These are the 'consensus settings' which can be tuned for each election separately.
- One Acta#4 document will pass through multiple rounds. Every round which every document passes will be counted at 66%, every time the same document gets 66% consensus from a set of Validators it gets '1 Round Up'. This will help us select which documents will

need to be validated next by showing Validators documents with less Rounds.

- The system will run on with every document getting multiple Rounds. The documents will be mashed randomly between each other to create pairs of the same Acta#4s. If 66% of a set of the Validators' stake approves a document then every future round dramatically decreases the probability that that document is forged.
- Validators will continue to work until the entire national total is counted for safety.
- Over weeks of Validating and getting the document 'Round Ups' we will decrease the probability of forged documents to virtually zero.
- We will know which copies are forged because we will know who is honest from both groups.
- Once a sufficient number of Rounds for all the documents is reached, the locked tokens for both Collators and Validators will be unlocked.
- With each round of all documents reached the total amount of tokens will double again. This by itself introduces an interesting social mechanism by setting a goal which all the Collators and Validators can strive for.

Part IV
What You Can Do With The Token

Once the correct results have been verified by honest participants the Democracy Tokens will be unlocked, to be collected by those participants. But what next? In order for this token to be a feasible monetary incentive it must have value. The value I propose it has is twofold.

Ancient Greek Democracy had a peculiar and (to our modern senses) quite undemocratic rule: nobody who “worked for bread” could participate. The idea being that someone who is bound to someone else for sustenance cannot be called free. Today the multiplicity of an expanded world renders this logic more complex, yet somewhere it still rings true.

Yet here we propose to create a token as a way of quantifying an involved interest and honest reputation in the democratic process. In a sense, bread earned by and for democracy. The perfect platform around which a democratic community can be formed.

Today’s politics is a dishonest contract: that those who participate in it work for the people, and are supposed to have no direct monetary benefit from that work, while the people know very well that that is a lie but most choose to block their ears and ignore it out of a feeling of impotence in the face of the massive institutional weight. Here we have an idea which challenges this contract, in a grassroots way.

I propose that those who hold these tokens, citizens from around the globe, who are responsible in making sure that the government is indeed chosen by the people, can create a digital Governance. This digital Governance will work as a forum not unlike a sub-governance, running as an allied parallel to Free TON. The difference being that only holders of the Democracy Token will be admitted and that its functions will be more specialized.

Those functions will, over time, be refined and redefined and expanded on by the participants. At the beginning, however, the forum should work as a monitor on existing democratic institutions and free space in which citizens can converse. This Governance can now introduce contests for

TON Crystals for democratic initiatives, which can be judged by people with proven merit in the democratic process. They can also participate in the machinations of Free TON, with their tokens acting as tender.

The second way in which this token can have value is for those who do not wish to hold on to their tokens. Since the basis of the token's value is the reputation of it's holder, then exchanging the token for money would dilute its original value. It goes, therefore, to say that this token should only be held by those who earned it and not to be transferable. I propose that if the holders wish to get rid of it they can turn it, through a special smart contract, to Free TON Crystals from a referral giver allocated by Free TON community, at which point the tokens will be burned.

This offers Free TON the added bonus of enlarging its user base with new members of a proven reputation and interest. By introducing new and engaged voices we can not only benefit, but benefit those that wish to use our technology and participate with us in the future, as we are doing here with #Fiscal_Digital.

Part V
UI/UX, Backend, and Tech Specs

The 'Democracy Token'
The governance token will be based on TIP-3 design and they will be non transferable tokens with a lock functionality. It will be completely decentralised.

Acta#4 (or other such documents or ballots)
Every official Acta#4 document (or other such documents or ballots) will have hashes, so that we can safely say that the document will be treated

like a block on a blockchain. The documents will be decentralised based on smart contracts. There will be a node software which will generate the fake ballots and populate the system during the time of the acta#4 uploads, it will download acta#4s and create fakes with fake numbers and upload them back to the blockchain, this way nobody (but the nodes) will be able to distinguish between the fake and original ballots, fake ballots will include random salt generated from the private key of the server, this way, knowing this private key *the node* will be able to distinguish between the real and the fake ballots, at the end of each validation round, the node will release a private key to the smart contract for this document, subsequent calculation will take place on smart contract which will determine whether tokens should be added or slashed, from each validator that participated in a round.

UI/UX (Collators)

Collators will use the existing Surf app, where they will sign up. There will be a special DeBot for Collators created for this precise job, which they will have to install, which will notify them as to when the time they have to upload the JPEGs of the Acta#4s will start and end, all they will need to do will be to hit one button to upload Acta#4.

UI/UX (Validators)

Validators, just like collators, will also use Surf. They will sign up and install their special DeBot for Validators. Surf will periodically send them a link asking whether they validate the document and ask them to fill in the numbers they see in the photo into a digital form.

Sybil Attacks

The prevention against the sybil attacks is inherent to the system, it works on two levels.

In the case of Collators the sybil attack will be cancelled out because only the correct version of the document will be validated, the incorrect Acta#4s will be nullified (if the government provides wrong copies, it will not be verified either). We assume that either the government document will be correct and at least one Collator copy, or a majority of the Collator copies will be correct. This allows Validators to verify the Acta#4. If the Government copy is incorrect and the majority of the Collator copies are incorrect the whole county election results won't be validated at all. Still, in order to validate wrong results, both the Government copy as well as at least one Collator copy should be wrong in exactly the same way.

In the case of Validators, we assume that 66% of validators are honest in every round, seeing as we have multiple rounds we reduce the need for honest validators, especially as seeing as we introduce wrong data, we will know based on probability, as long as we have a minimum of honest validators they will cancel out the rest. On top of that, because the validators are entering numbers, and because we will know which numbers are correct, *the entire election could be recounted on the blockchain, if needed.*

Part VI
The Conclusion

What we hope to achieve with this proposal is to create a secure vote counting and audit mechanism so dearly needed, especially in developing countries, while fostering an international spirit of participation in the democratic process. The example used in this text is Guatemala. It, like it's Latin American neighbors, has a very distinct voting system. Yet the mechanism outlined herein works as a foundation for vote counting in any

nation, with only some basic adjustment required. Through it we can encourage transparency and inclusion in systems so far defined by trying to keep people out. I know that the job of conclusions is to pack as many adverbs into a sentence as possible for fluff, so I'll just conclude by saying that while there are many solutions possible for applying the blockchain to questions such as voting and vote counting, most of them require institutions to move, as they control the fields. However, when you go from the bottom up, with the participation of citizens, as in this case, you can get a lot of progress done.