# Digital Acta4 Solution

**Solution for voting audit improvement task using FreeTON technology**

by Laugan

Solution for **Proposal #83 Crowdsource Voting Audit Solutions for Latin American Elections**

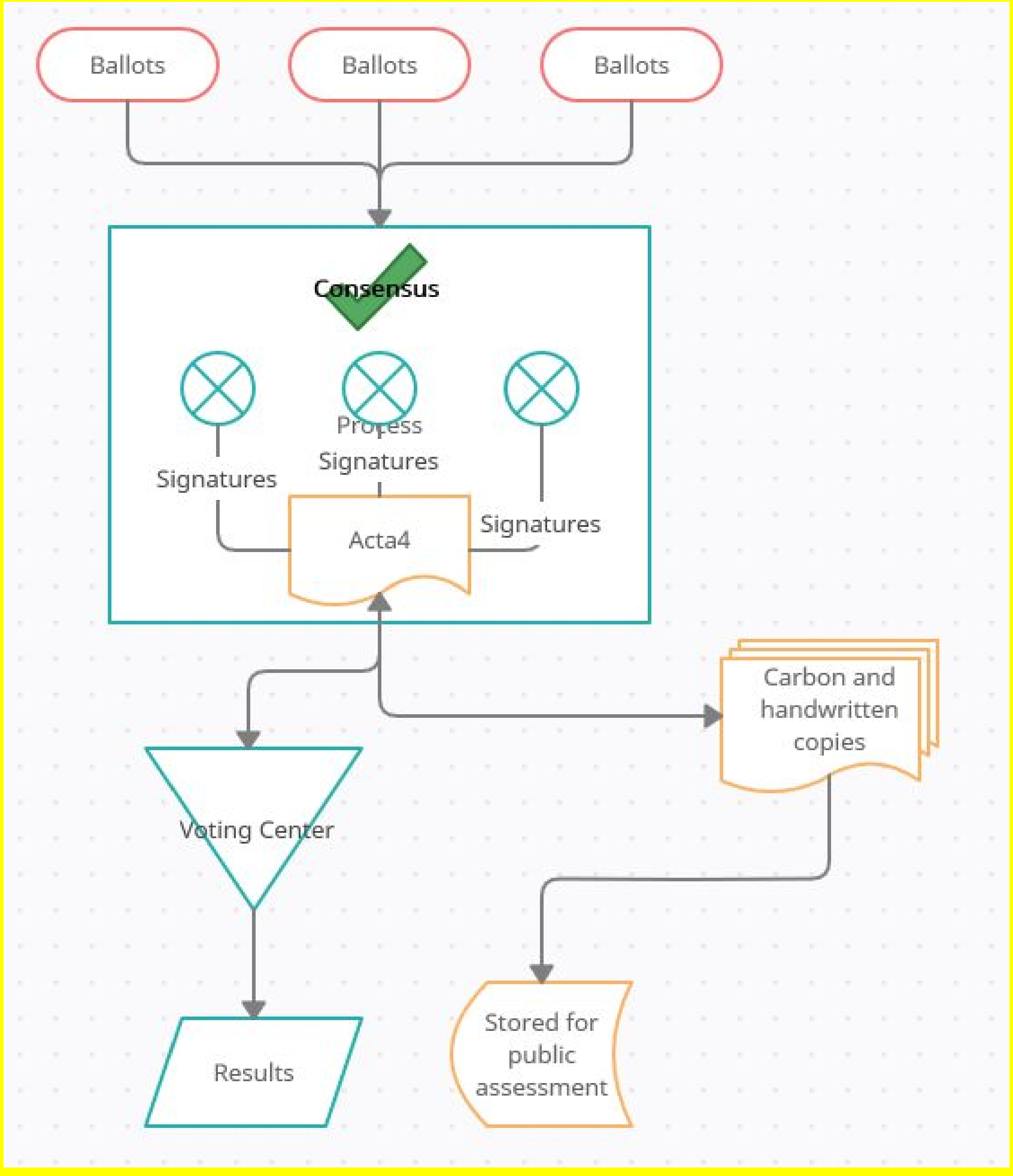
## Short Task Description

*Provide a solution using FreeTON blockchain technology and community to solve any possible vote count inconsistencies and remove the possibility of manipulation of the vote counting and auditing process. Make vote counting and auditing infallible and to accelerate reporting of voting results information with keeping in mind that no laws or actual voting processes can be easily changed.*

### Current election process details (as stated in Case Study [4])

- 20000+ Voting Tables -> 1000+ Voting Centers (for 340 municipal subjects at 23 regions)
- Every voting table is ran by 3-5 volunteers. They manage the voting process
- A certain number of **Fiscals** (observers/witnesses from different parties) controls the voting process at each Voting Table
- Ballots are counted after the end of voting period. All calculations are made in presence of Fiscals.
- Voting Totals are written to "*summary table document*" (**Acta#4**) with 1 primary paper and 1 carbon copy paper
- This document is signed when a "**physical consensus**" is reached between Voting Table volunteer staff and fiscals
- All volunteers and witnesses that desire a paper copy of the results must create a certified copy, by hand, that is signed by all volunteers with 4 carbon copies created during each new, hand-written, certification.
- Individual ballots are never recounted
- Stored **Acta#4** can be recounted if needed

Current election process is shown on image below.



## Potential and current problems and flaws of current process

- A LOT of paper
- Any additional paper copies are prone to intentional errors or non-intentional typos
- Paper Acta4 information can be changed
- There is no simple process to make independent count of results
- Paper carbon-copies should be accessible to public, but they are not (due to bureaucratic obstacles)

To sum it up, a process makes audit and independent vote count very hard. All voting results copies are prone to errors and hardly accessible to make independent count.

## Overview of #Fiscal_Digital Solution to audit

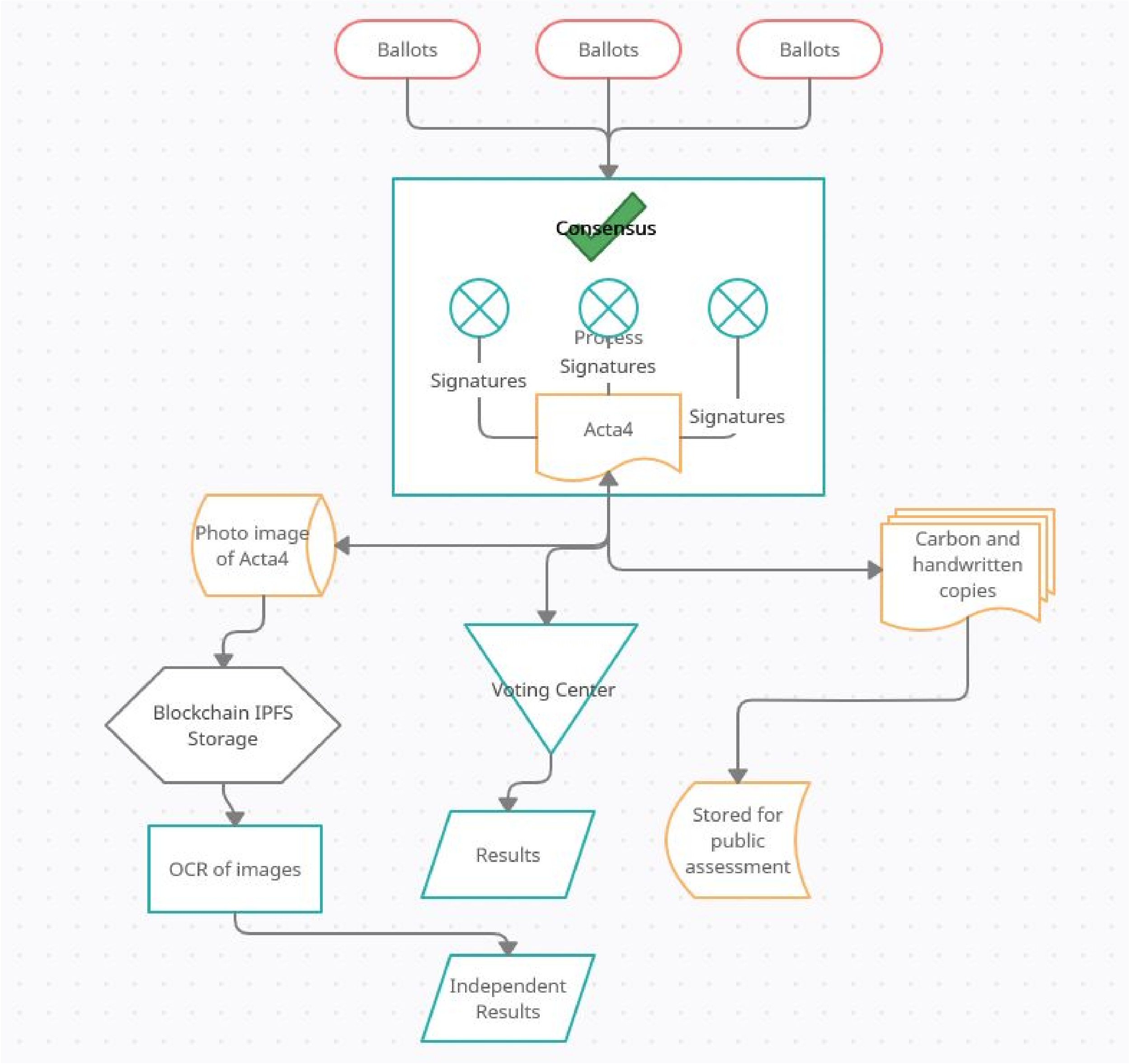
As stated in Case Study [4] #Fiscal_Digital proposes to:

- *Include a purpose built IOS or Android device at each voting table to photograph ORIGINAL* ***summary table documents*** *(Acta#4) as soon as they are created by the voting table volunteers themselves. The local app on the device will upload the JPGs to as many blockchains as possible, including the hash of a JSON that includes geolocation, timestamp, table ID and unique device ID (IMEI), thereby replacing dozens of handwritten, carbon paper certifications with a single digital blockchain certification.*

- *Redesign voting table results documents (Acta#4) for optimal OCR performance via automatic systems as well as crowdsourced efforts. Ensuring that machine OCR is able to produce preliminary results eliminates the need for human-generated results for informative purposes with no legal impact on official results. Machines generate the public preliminary results, human volunteers check their work via #Fiscal_Digital and other similar civilian audits.*

- *Redefine IT department's role as the implementer of blockchain certifications and OCR technology as efficiently and transparently as possible instead of contracting thousands of temporary workers and other third parties.*

#Fiscal_Digital process is shown on image below:



## Potential problems and flaws of #Fiscal_Digital solution

Despite obvious improvements of Voting audit that is proposed, #Fiscal_Digital solutions have some flaws that will be addressed in this solution:

1. The description states that *"The local app on the device will upload the JPGs to as many blockchains as possible, including the hash of a JSON that includes geolocation, timestamp, table ID and unique device ID (IMEI)"*, but all of this info still can be compromised before going on-chain
2. There is no guarantee that Fiscal uploaded this image. Election frauders can upload such image too (with predefined wrong results). It seems that #Fiscal_Digital does not provide (or doesn't state clearly) any defense against adding images from fake app (thus ignoring KYC principle [5])
3. Even if all images on blockchain are correct and trusted, it's still a lot of manual or machine (OCR) work to make independent count
4. OCR is not a precise tool. There is no guarantee that court officials will accept results of such machine count. Even if fraud is obvious, there is a possibility that only manual recount can be legally trusted as precise (and we still end in counting papers)

5. Even if machines are counting Acta4 forms via OCR from a blockchain source, it is still possible to temporary replace preliminary results with fake results or make results inaccessible (because OCR scans and a counting process are executed off-chain).

## Proposed changes to voting audit process

Let's return to the main steps of Voting Results process:

1. Votes are counted
2. Physical consensus is made (between volunteers and witnesses)
3. All involved are signing Acta4 summary paper form with Voting Results
4. All current and proposed defense solutions are applied (carbon copies, images, hashes and so on)

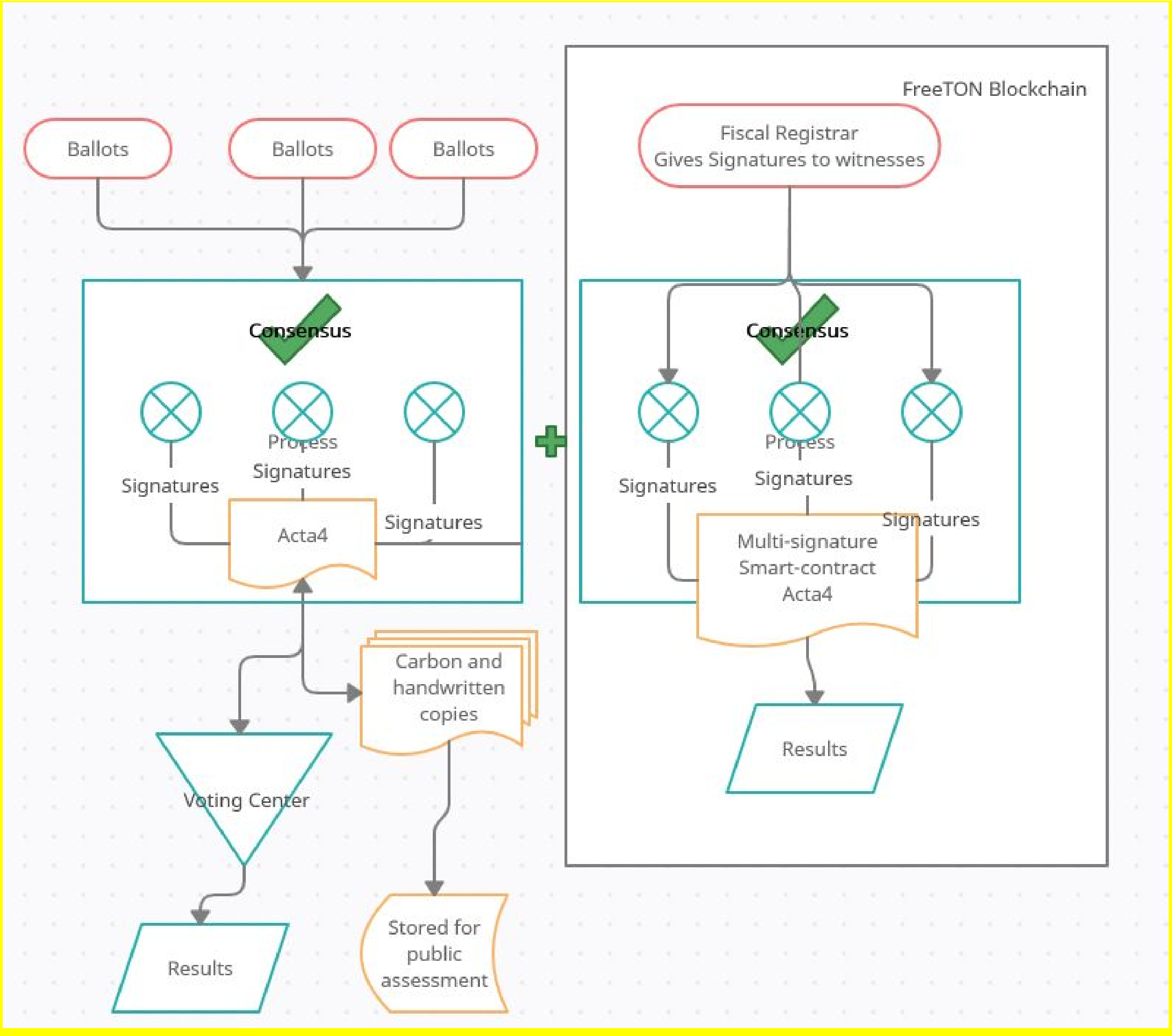
To cope with aforementioned flaws we propose alternate solution methodology that needs to get rid (or make it unimportant) of step #4 (physical copying of the results) and apply blockchain solution right on steps #2-3 (signing the consensus).

This step is a strong (trusted) moment in a process of voting. Everyone made a consensus about voting results. This fact is accepted by a needed number of volunteers and witnesses. **So it is trusted**. To preserve this trust we do not need to copy this fact (and lose legitimacy of these copies in the process) many times. We need to make this "physical consensus" as a digital on-chain fact.

**Consensus should be signed one more time in digital, on-chain way by multi-sign a summary form in mobile app with digital signatures.**

To do this, #Fiscal_Digital can use technologies of FreeTON blockchain – multi-signature wallets. FreeTON is perfectly fit to execute multi-signature transactions.

Below is the flowchart of proposed process:



## Physical multi-signature consensus -> Digital multi-signature consensus

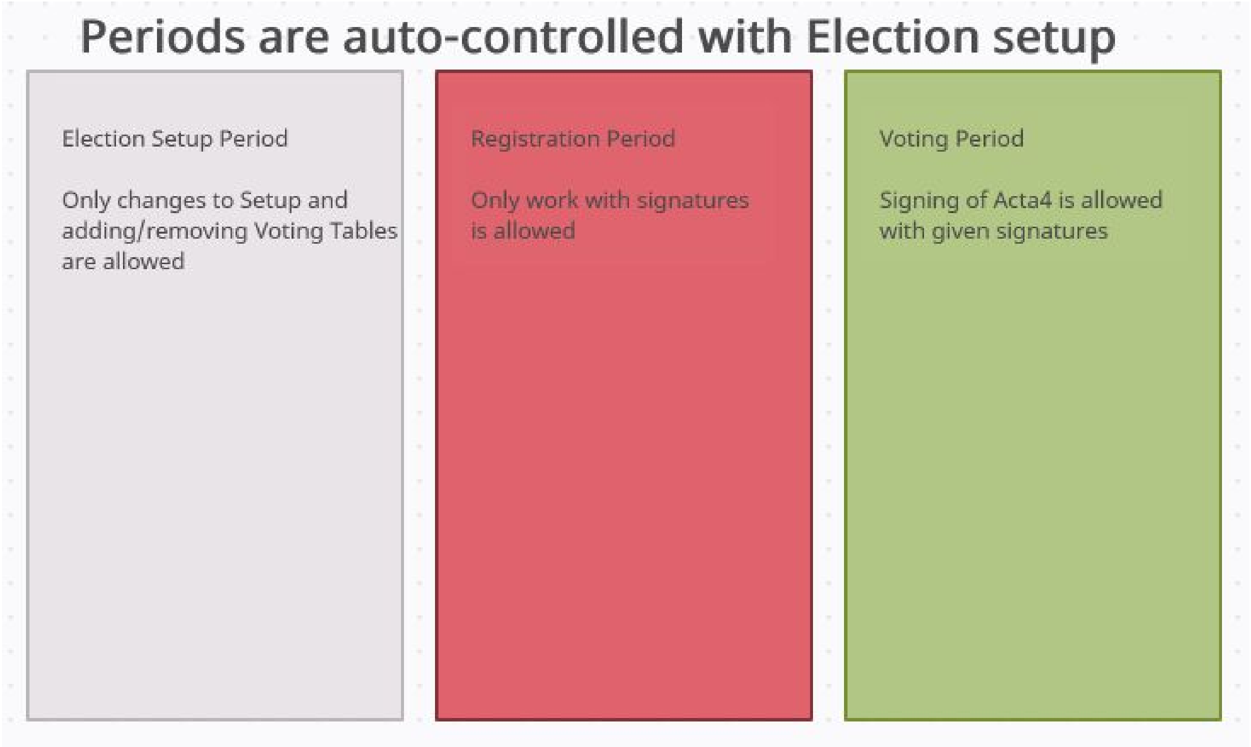
If we made a consensus between everyone involved and store it as an on-chain fact in FreeTON blockchain, there is no need to control further paperwork, copies, OCR and results count. All correct **results are already on-chain with signatures of everyone involved**. More to say, they are ready for counting. All we need is to get preliminary results right from the blockchain.

These changes will require the presence of digital signatures for all involved staff (volunteers and witnesses). These signatures will be prepared and given by witness authority (Fiscal Registrar). All signatures, election periods, limits and settings of multi-signature consensus will be realized as an on-chain (fully blockchain) solution.

The signature process on Voting Table will be implemented with a mobile decentralized app (DApp) that will control voting results (with additional checks) and confirm them only when consensus is reached (via digital signatures).

Overall voting process is described in steps below.

## New voting process steps



Periods are auto-controlled with Election setup

Election Setup Period

Only changes to Setup and adding/removing Voting Tables are allowed

Registration Period

Only work with signatures is allowed

Voting Period

Signing of Acta4 is allowed with given signatures

### Election Setup Step

Ruled by witnessing organisation (#Fiscal_Digital for example). This step is needed to create all election settings and dates.

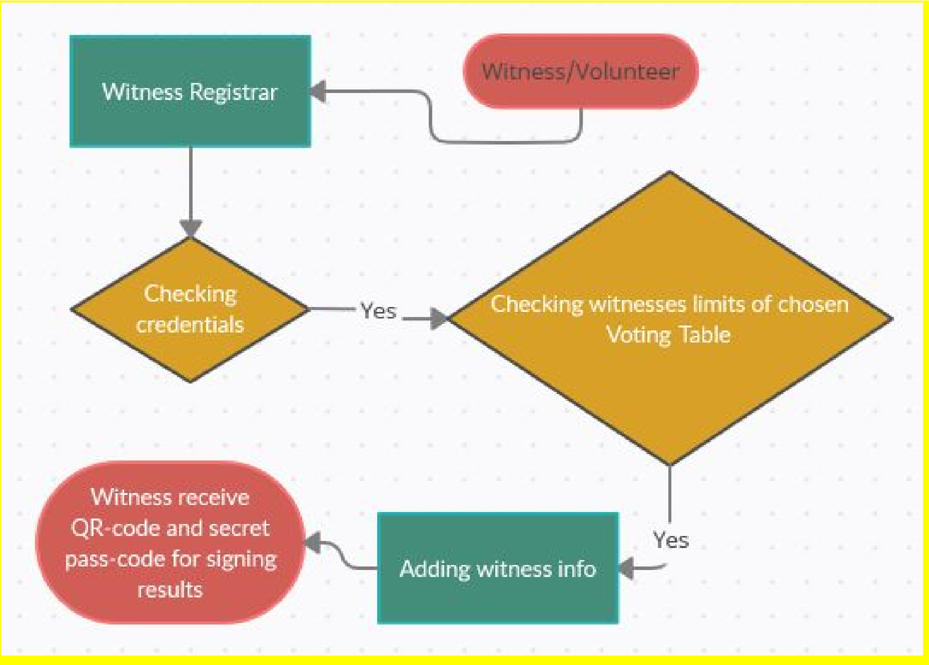
1. Witness organization official sets up new election parameters (periods, consensus parameters (minimal amount of signatures for consensus, maximum limit of personnel and so on, election candidates) This configuration will be used for all contests
2. Witness organization official adds Voting Tables list for this election

### Witnesses and Volunteers Registration Step

Ruled by witnessing organisation (#Fiscal_Digital for example). This step is needed to provide volunteers and witnesses with their signatures.

1. #Fiscal_Digital (or other witnessing orgs that have signature to rule this created election) can register witnesses and volunteers
2. Every witness and volunteer registered is given a QR-code and unique signature. It can either be a printed secret code (cheaper) or FreeTON Security card (harder to lose/copy). In FreeTON blockchain every such signature is a separate wallet.

Additional chart of this step:


Witness Registrar
Witness/Volunteer
Checking credentials
Yes
Checking witnesses limits of chosen Voting Table
Yes
Witness receive QR-code and secret pass-code for signing results
Adding witness info

### Signing Voting results on Voting Table Step

1. Volunteers open phone/tablet device and enter Voting Totals for election candidate in a Digital Acta4 DApp GUI interface (GUI design can replicate current Acta4 form)
2. All participants reach consensus and authorize on their apps (or on the same device) with their signatures to sign these results.
3. If consensus is reached . For example, ¾ volunteer signatures and ⅔ of witness signatures or something like this have signed (will depend on Election setup)– then **Voting Results are submitted, trusted and already on-chain**.
4. All results can be publicly viewed from now on via ton.live (speed of FreeTON transactions is very high)

## Possible Questions

### *What is a signature?*

QR-code + (Pass-code, Key phrases, FreeTON Security Card or any other form of signatures that will be best to fit witnessing process needs) to identify the correct owner of the wallet

### *How can I be sure that Digital_Acta4 is signed by the people presented on an election table?*

No one else has signatures. Blockchain tracks all signatures for a current address and we can limit the amount of signatures given for each Voting Table, so even if an additional signature is somehow issued, it will not be enough for reaching fake consensus.

## Technical details on each part of implementation

### Witness Organisation Administration GUI Client

**Tasks:**

- GUI for Election setup.
- GUI for adding/removing Voting Tables.
- GUI for adding signatures to the Voting Table.

**Frontend:**

Can be written on any language or framework for web using current TON SDK bindings

Screen forms:

- New Election form
- Adjust Election form
- Add Voting Table
- Adjust Voting Table
- Add Signer for Voting Table
- Remove Signer from Voting Table

**Backend:**

Smart-contract Election should be implemented for controlling election periods (it is very similar with Contest smart-contract, shouldn't be much work). A smart-contract Voting Table is needed for storing results of a certain election and accepting multi-signature.

No additional software or hardware is needed.

If a process of receiving a signature will be made through the app then additional GUI will be needed.

If a process of receiving a signature will be made through printing QR-codes and secret pass then some printing methods should be added to

## Digital_Acta4 Mobile DApp

**Tasks:**

- GUI for filling form with Voting Table Summary Results (Acta4).
- GUI for multi-signing results by all involved.

**Frontend:**

Can be written on JS or Java/Kotlin (using TON SDK Bindings). It may have design similar to paper form to reduce additional teaching of involved personnel. Also, it will reduce amount of errors.

**Backend:**

Working with Voting Table smart-contract and wallets, making additional checks (Voting Total = sum of candidate votes and so on).

## Smart Contracts

To fit all possible requirements of the legal process, it seems that additional smart-contracts should be written.

**Election:**

Smart-contract to check election dates and overall settings.

Proposed inputs:

- name
- type
- register period
- active voting period

- vote counting period
- results period
- consensus rules

**Voting Table:**
Smart-contract to store votes for every candidate (submission in Contest terms).

Proposed inputs:

- name
- address
- table ID
- results (array of vote results, vote total)

Methods:

- update results (voteAll)
- confirm results (for each signature, until consensus)

## Disclaimer

Described solution doesn't solve all election problems like:

1. Fake ballots
2. Repeated voting
3. Forbidding candidates from elections

This solution follows task description and works only with votes counting, audit and fast showing of results (without serious improvements of election laws). There is a possibility that it will not be enough to defend against all election fraud strategies.

## Recommended Implementation Stages

1. Contest for implementing this solution via FreeTON Contests (creation of mobile DApp and GUI for Fiscal Registrar)
2. Choosing the best technical implementation and working with winner team
3. Presentation of Digital Acta4 UI/UX and multi-signature process to officials/observers
4. An acceptance of both witnessing and volunteers organisations about registering and getting their signatures and mobile DApps
5. Using "Digital Acta4" at local elections to produce digital multi-signed "carbon-copy" of Acta4.
6. After gaining trust, Digital Acta4 can be used as a primary document. After that, paper Acta4 can act as a "carbon copy" itself

I hope that #Fiscal_Digital initiative will succeed in transforming outdated election systems to be more modern and transparent. Thanks for reading!

## Contacts

- **Telegram:** https://t.me/laugan
- **FreeTON Forum:** https://forum.freeton.org/u/laugan

## Links

1. Proposal #83 Crowdsource Voting Audit Solutions for Latin American Elections (https://gov.freeton.org/proposal?proposalAddress=0:e4cdeb29d95d940ead30fd7ce93db4c6f6397c4ae1bd6ee6814b5c07612839ec )
2. Proposal Discussion Thread (https://forum.freeton.org/t/crowdsource-voting-audit-solutions-for-latin-american-elections/4571 )
3. Contest: Crowdsource Voting Audit Solutions for Latin American Elections ( https://firebasestorage.googleapis.com/v0/b/ton-labs.appspot.com/o/documents%2Fapplication%2Fpdf%2Fzf7e37wnlajkhcap0m8-Contest_Crowdsource_Voting_Audit_Solutions_for_Latin_American_Elections%20(2).pdf?alt=media&token=302942c4-5aba-46c7-8a24-26bfa11b0a9c )
4. Case study in Guatemala for post-election audit of paper ballot election results documents in real-time (https://www.gbaglobal.org/fiscal_digital_2020 )
5. Wikipedia ( https://en.wikipedia.org/wiki/Know_your_customer )