National Cybersecurity Center Audit Summary

What was the Audit?

The purpose this effort was to enable public citizens to conduct an independent, third-party audit of the Voatz application with a web-based blockchain viewer tool developed by Voatz. With this tool, auditors were able to view and verify the security of the Voatz mobile voting technology by comparing the anonymized voter-verified receipt, the tabulated paper ballot image and the blockchain transaction. This audit hosted 10 volunteers from diverse backgrounds (7 are listed below, other auditors chose not to publicly list their identity) that were willing to use their expertise and knowledge to verify the election and offer feedback for this technology used in the Utah County Primary Elections. The audit showed that there were no problems with the election and that all comments related to the audit were on the tool itself or the information provided. This audit was another step in the eventual goal of being able to conduct an end-to-end verified election which can be routinely and quickly audited by independent organizations.

What were the standards for the audit?

The NCC advises the following standards as best practices for utilizing such an auditing tool. These standards were used in the 2019 City/County of Denver pilot with great success.

- Provide a web-based blockchain viewer (and optionally additional tools) to enable independent tallying and end-to-end auditing of submitted UOCAVA ballots
- Enable one of two community viewing options:
    - Fully public (anyone with an internet connected web browser may access)
    - Partially public to select individuals (whitelist IP addresses for people to view)
- Ensure that the blockchain will anonymize or remove any personal identifying information (P.I.I.) about the voter. **Note**: It is an established best practice not to store any voter information on the blockchain.
- Set-up a public election observer framework and governance infrastructure for this blockchain network:
    - Establish vetting standards and security protocols for entities and individuals who may be eligible to become independent auditors.
    - Establish a governance mechanism for this to be managed independently by a reputable, non-partisan third party.
    - (optional) Provide access to signed binary builds for the approved entities to run independent nodes.

Who Participated?

Damon Townsend
Harvie Branscomb
Mike Quigley
Tyler Dergen
Julianne Blaney
Keo Frazier
Chris Null

What was the outcome?

Ten auditors registered to audit the election using the web-based tool. After the audit concluded, four of the ten auditors submitted notes, and of the four notes submitted, three deemed the election a success. The fourth gave feedback that not enough information was given to complete the audit successfully. This feedback is listed in its entirety under the procedural section for transparency. The feedback was not related to the integrity of the system or the ballots but is related to the information given to complete the audit.

This audit process leveraged used new, innovative technology. With new, innovative technology, there are course corrections to be made in order to improve the process for the next implementation. All submitted issues are listed below, categorized between two categories: substantive and procedural. A substantive issue addresses aesthetics, usability of the tool and missing or suggested features. A procedural issue addresses an issue or a misunderstanding with how the program operated. All feedback submitted was around the audit tool. No feedback was received that flagged the integrity of the election, nor suggested any errors in the submitted ballots or tabulation data.

All feedback has been anonymized.

Substantive

- The body of the email is fine, clear and to the point. The links below were not intuitive, nor in order. I suggest changing the order - Video, Presentation, Portal, Notes, then a sub section for "Data for this audit", followed by the links to the CVR and BMT
- The procedure on how to compare the CVR is not clear at all in the presentation. The video's explanation of both the process and the execution of testing that are much clearer. Email has an attachment with that slide in the presentation entitled: this is more clearly explained in the video
- Process is very painful to perform and takes more than basic computer skill for the common election worker/official/interested party. The video has a much clearer explanation of the process.
- Suggest adding a check for oval count on VVDR and corresponding number of UUIDs in all included blocks. Election officials like to make sure the sum is correct as well, so if they see three ovals on the picture, they want to see three transactions before they delve into each individual one. This will also help explain to them that the blockchain is like a train, and some of the ovals will all be in one car, or they might be split up on different cars. But either way they all were on the train, no one fell off on the way.
- The need to copy and paste data into an outside vendor has a fishy feel to it. It would be nice to have the decoder built into the tool somewhere, poach the code if it is open source, license if needed.
- Some users will struggle with identifying the needed portion of the decoded payload (the 500... part), and to copy, switch over to another program, and search for the copied number. If possible create a macro enabled template in excel or google sheets that allows them to copy the entire payload (and if it could incorporate the decoder as well that eliminates a step) into a input box/field. Parse it down to the 500... choice ID and search/highlight the vote.
- I tested a large number of the payloads, but in a large election this process would be very tedious. It illustrates the futility of trying to hack the chain, it takes a lot of effort to garner one portion of the entirety. It may help to suggest a proposed

strategy to test this, like a entire blockchain audit of a percentage of the whole ballots. Folks want a goal for a task, leaving it open ended makes them either think that it is optional, or they need to do a super large number to satisfy the sample. In Washington the required audit was 4% when we used DRE equipment (this feels like a DRE-like product, you select votes on a machine, it produces a voter receipt and sends the results to the tabulator).

- Please consider adding a base64 decoder into the audit portal itself so users don't have to go to an external site (this is not a biggie but a nice to have).

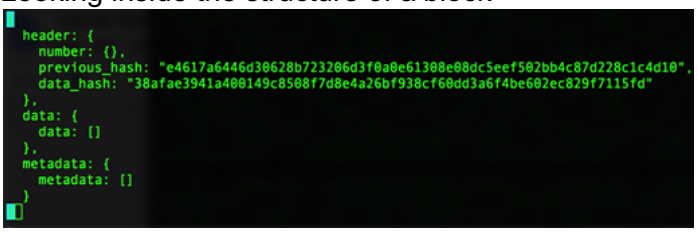
- The jurisdiction should include the ballot anonymous IDs in the CVR file so that auditors can do 1-to-1 matching. Right now you can kind of do it as the number of ballots is small but if that grows, that part will be problematic. I believe it should be possible for the jurisdiction to add the anonymous IDs as they are the ones scanning the paper ballots (I categorize this as a must have for the future).

Procedural

- The '20190830 Voatz CVR.csv' file does not appear to contain the necessary information to complete the first half of the audit, as described by the instruction video that was provided ('20190607_VoatzAuditVideo_vF.mp4'). According to the video, the first column of the CSV file should contain anonymous IDs to match up with the ones seen on the voter-verified receipt and the digital ballot. (The 'Overview-MobileVotingAuditProcess-Demo_v7.3.pdf ' that was provided also describes the same procedure.) However, the first column of the CSV that was made available to us has a different identifier, 'Cast Vote Record' in the first column, and it does not appear to have the anonymous ID in it at all.

F.A.Q.

- How can I compare the hashes of the blocks correctly?
    - Looking inside the structure of a block



    - **data_hash** is calculated only with the data object of the current block and written at its header. Must not be confused with the currentBlockHash.
    - **currentBlockHash** A block hash is calculated by hashing over the concatenated ASN.1 encoded bytes of: the block number, previous block hash, and current
    - **block data hash** The chain of the block hashes is what guarantees the immutability of the ledger.
        - The currentBlockHash will be the previousBlockHash at the next block.
        - More info: https://fabric-sdk-node.github.io/global.html#BlockchainInfo anchor

One auditor commented: “The audit tool performed well and was easy to use. No issues encountered.”

Recommendations and Next Steps

We can conclude that the Utah public audit was a success. Of the ten auditors we did not receive a report that would give us the conclusion that there was any tampering with the results that were audited.

Our recommendations for the tool and Utah County moving forward are:

- All auditors’ comments that have not been addressed in this report are addressed by Voatz before the next audit
- Address the educational materials sent to all auditors
- Add a feature that not only tracks which ballots have been audited but also include a submit button
- Provide additional information and resources for auditors to discuss results
- Provide additional information on how the blockchain viewer pulls the voter-verified receipt, the tabulated ballot and the blockchain transaction.
- An independent node for a third party to review
- Larger window for registration

About the National Cybersecurity Center

The National Cybersecurity Center exists to help secure the world using knowledge, connections and resources to solve global cybersecurity challenges and develop a protected cyber ecosystem. An independent and non-profit think tank based in Colorado Springs, Colo., the NCC provides cybersecurity leadership, services, training and a cybersecurity community for public officials, business executives and the workforce. Discover the NCC at cyber-center.org.