



The Denver Mobile Voting Pilot: A Report

This report describes the following: the post-election audit process of the Denver Municipal election mobile voting pilots conducted by the National Cybersecurity Center. An overview of how uniformed military voters, their families and civilians residing overseas received, marked and returned their ballots from their iOS and Android smartphones from 36 countries. It outlines the challenges facing remote voters and the issues with online voting. It reviews the technology partner selection process, the capabilities of the technology partner, and a description of the audit process. We conclude with the results of the pilot election, audit and recommendations for the future.



**NATIONAL
CYBERSECURITY
CENTER**

© 2019, The National Cybersecurity Center

<https://cyber-center.org/>

Published August 1st, 2019

Author: Forrest Senti, Director of Government Affairs

Contact Information:

Email: forrest.senti@cyber-center.org

Phone: 719-255-5225

Contents

Denver Mobile Voting Pilot Report	3
Background	3
Partners	3
Purpose	3
UOCAVA Voting	4
Issues with Online Voting.....	5
Technology Partner Selection Process	5
Capabilities of the Voatz System to Address the Security Issues with Online Voting.....	6
Description of the Voatz System as used in the Denver Municipal Pilot	7
Results of the Pilot Elections.....	8
Results of the Audit.....	8
Conclusions and Recommendations for the Future.....	9
About the Collaborators	10
Denver Elections Division.....	10
National Cybersecurity Center.....	10
Tusk Philanthropies.....	10
Voatz, Inc.	10
Appendix 1: Mobile Voting Application - Minimum Pilot Requirements	11
Appendix 2: Blockchain Standards and Election Observer of Blockchain Standards.....	12
Appendix 3: Third Party Election Audit of the May 7 Municipal Election and the June 4 Runoff	13
Appendix 4: Election Observer of Blockchain Standards.....	14
Appendix 5: Auditors' Critique, Observations and Questions	15
Appendix 6: The Voatz Audit Workflow (Diagram)	17
Appendix 7: The Voatz Blockchain and Independent Audit Architecture (Diagram).....	18

Denver Mobile Voting Pilot Report

Background

In early 2018, the National Cybersecurity Center (NCC) was approached by the City/County of Denver (then Director of Elections, Amber McReynolds) and the Colorado Secretary of State's (Former Secretary of State Wayne Williams) office with a proposal. They wanted to collaborate on a pilot program for the April/May 2019 municipal elections to improve voting for UOCAVA¹ voters. They sought a solution that could deliver blank ballots faster and more reliably to *eligible registered* voters; that enabled their diverse set of voters to, privately and independently, make and review their selections; that provided a secure, tamper proof, method of returning and safely storing the voted ballots; and that would allow for a rigorous and independent post-election audit.

In addition, the solution had to have the capability of integrating into the established procedures of the county, which included the return of a signed voter affidavit in which the voter acknowledged that their ballot was not secret. Since Colorado allows same-day registration, the system had to ensure that, as registrations were coming in during the early voting period, only eligible registered voters could vote.

Partners

Groups that were involved in the creation and operation of this pilot project were:

- City and County of Denver, Jocelyn Bucaro, Director of Elections.
- National Cybersecurity Center, Forrest Senti, Director of Business and Government Initiatives.
- Tusk Philanthropies, Sheila Nix, President. Tusk acted as a funding catalyst to enable Denver City/County to finance the pilot outside of the normal (and lengthy) budget process, and, once selected, to fund the technology partner.
- Amber McReynolds, former Director of Elections for the City/County of Denver and currently serving as the Executive Director of the National Vote at Home Institute and Coalition.
- Voatz, Inc., Nimit Sawhney, CEO, and Larry Moore, Senior Vice President.

Purpose

This report describes the Denver pilot. It outlines the problems facing UOCAVA voters and the issues with online voting; it reviews the technology partner selection process, the capabilities of the recommended partner, and a description of the audit process. We conclude with the results of the pilot and audit, as well as recommendations for the future.

¹ Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)

UOCAVA Voting

In federal elections, the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) protects the rights of military personnel deployed outside of their county of residence, their voting-age family members, and citizens residing abroad. The Military and Overseas Voter Empowerment (MOVE) Act, further protects UOCAVA voters by requiring that ballots be sent to UOCAVA voters no less than 45 days before Election Day to ensure adequate time for postal mail delivery and return.

In Colorado, UOCAVA voters receive their ballot by postal mail or, unlike most other states, via a web-based portal. Those receiving their ballot by postal mail, make their selections and return their ballot just like all other voters in Colorado – a vote-at-home state.

The reliance on postal delivery and return – especially for overseas voters – poses challenges to voters and election administrators, including:

- Timely delivery and return of ballots.
- Postal costs for delivery of blank ballots and the return of marked ballots.
- An unreliable post office cancellation policy that is routinely used to determine when voter mailed their ballot and, accordingly, whether it should be counted.
- The potential for the U.S. to withdraw from the Universal Postal Union treatyⁱ in October 2019

Moreover, voters face a variety of hurdles to sending their ballot back to their county of residence. For civilians living overseas, the hurdles in the current system lead to a 7% voter turnout versus a 72% domestic turnout in 2016.ⁱⁱ

Our study reveals that the voting rate of Americans living abroad would have increased from 7 percent to 37.5 percent, if overseas obstacles to voting were removed."

**David Beirne
Director, Federal Voting Assistance Program**

Issues with Online Voting

Since the introduction of the Australian ballot in 1888², voting in the United States has evolved from in-person voting at precincts, to in-person voting centers, to vote-by-mail and absentee voting, to remote electronic voting via email. With every change there has been an increase in voter access and convenience and a decrease in the cost of election administration. Today, in addition to the pressures to make voting more accessible and election administration less costly, the need to increase election security has emerged as nation-state enemies have attempted to undermine confidence in U.S. electionsⁱⁱⁱ. Broadly speaking, there is agreement on four areas of concern with mobile voting as shown below.

Security Concern	Questions
1. Device security	Can we tell if the voter's device been compromised?
2. Voter identity proofing and authentication	Are we reasonably confident that the remote voter has presented valid credentials to prove they are who they say they are, and at the time of voting, is the eligible voter the same person whose credentials were validated?
3. Protection of the aggregate vote	Since the place where voted ballots are stored is a natural target of attack, how can we be confident that there has been no tampering with voted ballots?
4. Election audits	Can the voter verify their own selections? Do the tallies of ballots cast remotely match the tallies reported by the federally certified primary voting system?

Table 1: Common security concerns for mobile voting

The specific issue examined by this pilot is to determine if the technology helps UOCAVA voters address difficulties in voting without sacrificing their confidence in the security of their ballot.

Technology Partner Selection Process

In order to meet the needs of the City/County of Denver, a commercial vendor, non-profit, or open source application was needed that had working technology, experienced leadership, a proven track record with positive results, and a technical approach and auditing tool to addressing the issues raised in Table 1 above. Two companies were identified that fit the description of what was needed to accomplish these requirements, Voatz and Votem. These companies were invited to participate in a process that involved three components: a private demonstration to election staff and their partners, a technical review by the City/County of Denver Technology Services Team, and a public demonstration.

Voatz was selected for the Denver pilot through this review process, which also included a recommendation from the West Virginia pilot team. As part of their acceptance as the vendor for the pilot, Voatz received a letter that outlined the minimum requirements that Voatz had to meet for the pilot to commence (see Appendix 1). In addition, NCC submitted two documents to Denver City/County, “Blockchain Standards” (see Appendix 2 for an excerpt from the letter) and “Election Observer of Blockchain Standards” (see Appendix 3).

² The Australian ballot, also called the secret ballot, is the system of voting in which voters mark their choices privately on uniform ballots printed and distributed by the government.

Capabilities of the Voatz System to Address the Security Issues with Online Voting

The Voatz system was built by engineers who had extensive experience in designing applications for mobile payments and people with deep practical knowledge of voting systems architecture and the process of regulatory certification. Below is a brief description of how the Voatz system addresses the security concerns outlined in Table 1 above.

Security Concern	Voatz Approach to Mitigating Security Concerns
1. Device security	Voatz has integrated sophisticated in-house and third party “mobile threat defense” systems that, upon application launch, quickly performs dozens of tests to detect if the smartphone has been compromised. The app may not be used for voting if any of the critical tests fail (e.g. a jailbroken phone or the presence of malware or applications lacking the proper certificate from Apple or Google).
2. Voter identity proofing and authentication	Voatz also integrates proven third-party “remote identity proofing” services in addition to its in-house proofing services that 1) enable fraud detection of government-issued IDs, and 2) detect whether the person presenting the credential is alive and registered to vote,
3. Protection of the aggregate vote	A 32 node blockchain infrastructure divided equally between the two leading cloud service providers - Amazon AWS and Microsoft Azure. Each service provider further split their 16 nodes equally across two U.S. sites. Distributed denial of service attacks on the DNS servers has been mitigated by Cloudflare. Man-in-the-middle (MITM) attacks are prevented by certificate pinning, end-to-end encryption, strong passwords and system-wide certificates.
4. Election audits	The programmable smartphone, which obviates the need for the voter to record or the voting system to print their anonymous voter ID, and immutable blockchain enables an independent, end-to-end voter verified election.

Table 2: The Voatz approach to mitigating security concerns for mobile voting

Description of the Voatz System as used in the Denver Municipal Pilot

This section outlines the processes that were followed by Denver, Voatz, and the National Cybersecurity Center. See Appendix 6 for a supporting diagram of the workflow and Appendix 7 for how the blockchain infrastructure secures the aggregate vote and enables end-to-end voter verified elections.

1. Administrative processes (Denver)
 - a. Creation of the election definition; proofing smartphone-formatted ballots
 - b. Manual import from the voter registration system (VRS)
 - c. Invitation to vote sent to UOCAVA registered voters
2. Voter identity proofing (Voatz)
 - a. Voter installs application from approved application stores from around the world, provides proof of identity including: Credential validation (i.e. test for counterfeit credential), remote identity proofing, and authentication by the voter based on NIST guidelines.
 - b. Client-side security provisions (automatically create certificate for each smartphone, exchange public keys between the smartphone and the voting infrastructure)
3. Voting process (Voatz smartphone application)
 - a. Blank ballot delivery (voter authentication required to open the ballot)
 - b. Ballot marking and review, voter signs affidavit
 - c. Ballot submission (biometric voter authentication required to submit the ballot)
4. Processing the vote (automated processes)
 - a. An anonymized ballot receipt and signed affidavit is sent to the voter. Identical copies are sent to the jurisdiction. Note: Ordinarily the voter would be able to spoil their ballot, but this feature was disabled in the Denver pilot.
 - b. Votes encrypted and delivered to the blockchain infrastructure
 - c. Consensus process adds blocks containing encrypted, anonymous votes to the blockchain
 - d. The anonymous IDs are posted on the bulletin board
 - e. Ballot receipts automatically converted to ballots tabulated by federally certified primary voting system
5. Independent Audit (National Cybersecurity Center)
 - a. Audit infrastructure
 - i. Read-only blockchain node
 - ii. Audit portal and blockchain viewer
 - b. Independent auditors (See Appendix 5)
 - c. The audit
 - i. Ballot accounting
 - ii. Ballot comparison audit
 - iii. Comparison of the tallies as reported by the primary voting system and the independent audit system

To learn more about Voatz and their product, visit their website at voatz.com.

Results of the Pilot Elections

Three key metrics were of keen interest to the collaborators in the two pilots:

1. The percentage of people who downloaded the application and successfully completed the identity proofing steps: 94% (146/156) of people downloading the app completed this task successfully³.
2. The percentage of people receiving ballots who submitted them for return. 82% (120/146). This statistic compares very favorably with the average return rate of 54% (15,247/28,929) for Colorado and 52% (338,271/655,409) nationally^{iv}.
3. The number of originating countries: 36. This is an indication of degree of connectivity.

	Denver Municipal Election May 7, 2019	Denver Municipal Run-off June 4, 2019
# Smartphone application downloads by eligible voters	156	22 New
# Ballots delivered upon completing identity proofing process	146	18 New
# Ballots returned	120	112
Minus: # Ballots initially rejected due to signature mismatch	2	0
Plus: # Ballots cured by voter	1	0
Equals: # Ballots returned & counted	119	112
# Originating countries	36	34

Table 3: Results of the Denver Pilot Elections

Finally, the feedback from the Denver voters was overwhelmingly positive as evidenced in survey responses.^v

Results of the Audit

The purpose of any pilot is to obtain feedback from the participants. We were gratified by the quality and amount of the feedback we received from the volunteer auditors. There were 18 comments/questions raised in the first audit and 79 in the second audit. We divided the comments/questions into two categories: substantive and procedural. A substantive issue pertained to aesthetics or suggested features. A procedural issue indicated a misunderstanding with how the program operated.

NCC believes that its third-party audit pilot was a success. There were no issues with the tabulation and recording of the ballots, and the auditors were pleased with the results overall.

“I reviewed the ballot receipts from about 60 [anonymous voters’] IDs and compared them the scanned ballots - all were perfect aligned. Regarding the blockchain, I only checked three of them due to the complexity of toggling back and forth. All three that I reviewed were perfect.”

Conny McCormack, volunteer auditor, former Clerk/Recorder, Los Angeles County

³ Arguably, remote identity proofing is the most challenging part of the Voatz system. That’s because it requires scanning both sides of a driver’s license and making a “video selfie”. Fortunately, it is not done again until the credential expires or is re-requested for some reason.

After each pilot, NCC made recommendations to improve the audit process. Almost all suggestions in the first audit were incorporated in the second. The consolidated commendations and the Voatz response are summarized at Appendix 5.

Conclusions and Recommendations for the Future

Ballot delivery and return introduce substantial obstacles to UOCAVA voters. Those hurdles significantly reduce their participation. The collaborators on these pilots – Denver, NCC, Tusk Philanthropy and Voatz – believe this pilot clearly demonstrated the effectiveness and convenience of secure ballot delivery and return for eligible UOCAVA voters. In a survey conducted by Denver that had an exceptionally high response rate of 35%, every respondent said that of all the methods of voting, they preferred voting on their smartphone.

The two pilots also directly addressed the four major concerns that have stymied progress in remote voting for over a decade: Device security, voter identity, secure ballot storage, and end-to-end voter verifiable elections.

We believe that additional pilots will show rapid progress towards the introduction of a new voting method. Designed to address the requirements for security, accessibility, and convenience, this new, mobile voting method will take its place among the nation's other voting options, including in-person precinct and vote center and vote-at-home. A mobile voting channel will allow eligible voters to securely receive, mark, verify, and submit their ballot from virtually anywhere in the world.

We have the following specific recommendations going forward:

- Broaden the UOCAVA audience to include voters with disabilities.
- Engage formally with the Department of Homeland Security to conduct rigorous audits of the platform.
- Continue to develop the audit tools in ways that build trust through visualization. (It is powerful when a voter can *visually compare* their ballot receipt to the ballot that will be tabulated.)
- Add mobile voting as a topic to the agenda of every election conference; invite the vendor practitioners to participate on panel discussions – not just members of the academic community.
- Seek opportunities for NCC to speak on their experience in post-election audits.

About the Collaborators

Denver Elections Division

The Denver Elections Division's mission is to conduct Denver's elections in a fair, accurate, accessible, secure transparent and efficient manner; to educate and encourage the public to participate in voting process; and to maintain accurate voter registration and election records. Denver Elections has won multiple national and international awards for use of technology in elections administration including awards for the first-in-the-nation ballot tracking system BallotTRACE which allows voters to track the status of their mail ballot the same way they track a package and eSign, which lets candidates and issue campaigns gather petitions on tablets instead of paper.

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, Colorado, 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.

Tusk Philanthropies

Tusk Philanthropies was created by Bradley Tusk, Founder and CEO of Tusk Holdings, for the purpose of working on reducing hunger throughout the United States by providing greater access to programs like school breakfast. The Philanthropy also seeks to dramatically increase voter turnout and participation in U.S. elections through mobile voting, beginning with qualified military service members. The [Mobile Voting Project](#) is a non-partisan initiative designed to not favor any one candidate or party, but to expand voting options to increase participation in our electoral process. None of the Tusk entities has a financial interest in Voatz or any other voting technology company.

Voatz, Inc.

Voatz is a mobile elections platform that is attempting to change the way the world votes. Backed by military-grade security and cutting-edge technology (including biometrics and blockchain infrastructure), Voatz enables smartphone and tablet voting to increase accessibility and security in elections. Since 2016, Voatz has run 40 elections with towns, cities, states, both major state political parties, colleges and universities, and unions. More recently, Voatz ran the first mobile blockchain vote in US Federal Election history. Specifically, Voatz partnered with the State of West Virginia to empower deployed military and overseas citizens to vote in the 2018 Primary Elections (2 counties) and the 2018 Mid-Term Elections (24 counties). In March 2019, Voatz was selected by the City/County of Denver CO for its 2019 Municipal General & Run-off Elections where its use led to a more than 2x increase in voter participation amongst deployed military and overseas citizen voters. Learn more [here](#).

Appendix 1: Mobile Voting Application - Minimum Pilot Requirements

Following the public demonstration on February 11, 2019, Denver County issued the following requirements to Voatz as conditions that must be met to proceed to a live pilot.

Cost

- Voatz must provide a detailed and satisfactory quote of the cost to run the pilot
- Denver Elections will supply any needed information to ensure an accurate quote

Administrative Interface:

- Voatz must conduct a detailed demonstration of the election setup process with key members of the Denver Elections team. The demonstration must include:
 - Election creation
 - Integration with SCORE through FTP site for real-time voter registration updates
 - Import from Democracy Suite and SCORE
 - Data mapping
 - Creation of ballot content
 - Proofing of ballot styles
- Voatz must conduct a second demonstration of the voted ballot extraction process, to ensure that Denver Elections can perform the following requirements:
 - Must be able to bulk print affidavits and ballots
 - Must be able to segregate printed affidavits and ballots from unprinted affidavits and ballots
 - Must be able to reprint (with proper security, such as an administrative password) in the event of print errors
 - Must be able to view audit logs of all processes in the admin interface, including printing of ballots and user log-in/access
- User Interface:
 - Voatz must either provide wireframes or otherwise demonstrate the new user interface expected to be released before our pilot
 - The new user interface must contain the following features:
 - Either clear instructions or a more intuitive user guide through the initial verification to accessing and casting the ballots
 - A help button in the app to assist the user, including frequently asked questions and contact information
 - A language preference option to view all content in English or Spanish (in place of the current format that includes both languages)
 - Contrast options for low-vision voters
 - A clearer method of voting, including either an ability for the voter to view previous selections while progressing through the ballot or a single screen/page per race with easy navigation through ballot
 - A write-in candidate feature, to be demonstrated to Denver Elections
- Additional Requirements:
 - Voatz must meet standards for Blockchain security and auditability as proposed by the National Cyber Security Center (see Appendix 2)
 - Voatz must offer access to the Block Explorer for election observers to audit the election in the Blockchain

Appendix 2: Blockchain Standards and Election Observer of Blockchain Standards

The following requirements were generated by NCC and were incorporated into the list of mandatory requirements (see Appendix 1).

- Voatz will provide a multi-node Hyperledger based permissioned blockchain network that is geographically diversified across the United States
- Voatz will provide a web-based blockchain viewer and optional additional tools to enable independent tallying and end-to-end auditing of cast UOCAVA ballots
 - Community Viewing Options
 - Fully Public (Anyone with an internet connect web browser may view) or
 - Partially public to select individuals (Whitelist IP addresses for people to view)
- Voatz will ensure that the blockchain will anonymize or remove any personal identifying information (P.I.I.) about the voter
 - Note: the Voatz implementation does not store any voter information on the blockchain.
- Voatz will ensure that all cast UOCAVA ballots will be recorded onto the blockchain
 - This information will be anonymized and secured using standard National Institute of Standards and Technology (NIST) approved encryption algorithms [AES 256].
- Voatz will ensure that only the City of Denver Elections staff can provision eligible UOCAVA voters into the platform and that no ghost or unauthorized voters are given access to the live ballots.
- Voatz will ensure that no monetary compensation or cryptocurrency is provided to any individual or entity operating the Validator nodes
- Voatz will comply with standard security procedures and best practices for operating cloud-based networks
- Voatz will optionally provide a supply chain-like visualization of a UOCAVA voters anonymized activity from the point of requesting an absentee ballot to the eventual production of a paper ballot for tabulation on election day.

Appendix 3: Third Party Election Audit of the May 7 Municipal Election and the June 4 Runoff

Description of the Audit

The purpose was for members of the public to conduct an independent, third-party audit of the Voatz election results by a web-based tool that can view the voter-verified receipt, the tabulated ballot image and the blockchain transaction. Volunteers from diverse backgrounds used their expertise and knowledge to verify the election and offer feedback for this new technology. The first audit ran from May 9-16, 2019 and had a public demonstration by the NCC of how to use the technology (watch the video [here](#)). The second audit ran from June 7th to July 8th. This audit was the first 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.

Who Participated?

The participating volunteers are shown below. Participants who did not expressly give their consent to have their name given to the public were redacted from this table. All other participants have consented to being contacted at their email address.

Timestamp	First Name	Last Name	What is your email address?
5/8/2019 11:35:30	Forrest	Senti	forrest.senti@cyber-center.org
5/8/2019 11:42:31	Harvie	Branscomb	harvie@electionquality.com
5/8/2019 12:37:55	Steven	Rosenfeld	steven@ind.media
5/8/2019 12:52:17	Aaron	Wilson	aaron.wilson@cisecurity.org
5/8/2019 12:58:53	Neal	McBurnett	nealmcb@gmail.com
5/8/2019 13:10:03	Conny	McCormack	connymccormack@gmail.com
5/8/2019 13:25:27	Ray	Lutz	raylutz@citizenoversight.org
	John		
5/8/2019 21:44:41	Susan	Pynchon	susanpynchon@gmail.com
5/9/2019 5:32:10	Rokey	Suleman	rokeysuleman@gmail.com
5/9/2019 8:00:46	Hannah	Parsons	hannah@exponentialimpact.com
5/10/2019 9:45:12	Jana	Persky	janapersky15@gmail.com
5/13/2019 9:59:08	Orlando	Aloma	oaloma2017@student.hult.edu
	Benjamin		
5/13/2019 16:43:08	Yugma	Patel	yugmaa@icloud.com
	Bill		
	Aileen		
	Analiene		
6/7/2019 13:53:48	Neal	McBurnett	nealmcb@gmail.com
6/8/2019 8:28:18	Keo	Frazier	keof@keosmarketing.com
6/9/2019 13:31:07	Rokey	Suleman	rokeysuleman@gmail.com
6/11/2019 0:09:55	Harvie	Branscomb	harvie@electionquality.com
	Aileen		
	Analiene		
6/14/2019 17:04:30	Harve	Branscomb	harvie@electionquality.com
6/14/2019 22:44:46	Steven	Rosenfeld	steven@ind.media
6/21/2019 12:50:33	Dale	Hetke	dale.hetke@cyber-center.org

Appendix 4: Election Observer of Blockchain Standards

- Voatz, the National Cybersecurity Center, and the City/County of Denver will work together to lay the groundwork for setting up public election observer framework and governance infrastructure for this blockchain network.
 - This would include:
 - Establishing vetting standards and security protocols for entities and individuals who may be eligible to become independent auditors.
 - Establishing a governance mechanism for this to be managed independently by a reputable non-partisan third party.
 - Providing access to signed Voatz Hyperledger binary builds for the approved entities to run independent nodes.

Appendix 5: Auditors' Critique, Observations and Questions

The volunteer auditors provided excellent feedback on their experience. Shown below are the consolidated comments/questions and the responses by the Voatz team (*in italics*).

Substantive

- There is no feature to keep track of what ballots have been audited and the ones that haven't been verified.
Done. A feature was added to the Audit Portal that shows the audit activity across all auditors.
- It's hard to distinguish between Capital I (i) and regular I (L). This problem happens when verifying the Anonymous ID's from the Voter Verified Receipt VVR and the Tabulated Ballot.
Done by changing the font.
- There is nothing to address the transactions that take you to a "redacted per CO State Law" message.
Under review
- A ballot may have the write-in option chosen, yet it is not calculated on the Cast Vote Record CVR file under "write-in" row.
If you look a little closer at the CVR file, the write-ins are in there. If you look at Mayor, for example, column L simply states "Write-In", followed by qualified write-ins. Qualified write-ins are a pre-approved list of write-in possibilities which are the only ones tabulated. Not all races had qualified write-ins. If the race did have qualified write-ins, and a voter put one in their ballot, it would show up in the CVR. If a voter voted for a write-in that was not on the qualified list, or if the contest didn't have a qualified list, then they were rejected during adjudication.

Procedural

- The vote for the Major race is recoded in the Ballot, VVR, Blockchain view, and CVR. However, when looking in the Ballot Mapper using the Choice ID it does not show.
See next answer
- When looking for the Choice ID number in the Ballot Mapping Table there appear to be many duplicates.
Since different ballot styles can have the same candidate/choice on them (e.g. YES/FOR), what appear to be duplicate-looking entries are possible. In other words, in the case of the ballot mapping table listing multiple entries of the same candidate choice (i.e. "Timothy O'Brien"), this is because this choice shows up on multiple ballot styles (i.e. a different ballot style per precinct), which all have that same contest on them.
In the case of a choice being the same between contests (i.e. YES/FOR), if you'd like to differentiate which contest the choice is for, you can use the second tab in the mapping table which has the contest names included.

- Provide additional information on how the blockchain viewer pulls the voter-verified receipt, the tabulated ballot, and the blockchain transaction.

Partially done. Voatz has initiated a project to make the blockchain viewer more intuitive and visual.

- Provide an independent, read-only node for a third party to review.

The node provided for both Denver audits was instantiated by Voatz on the Amazon AWS portion of the Voatz blockchain. Voatz agrees that NCC should be able to provision its own “bare metal” server, install both the open source distribution of the Hyperledger blockchain node and the credentials that are necessary to communicate with the blockchain network in read-only node.

- How can I compare the hashes of the blocks correctly?

Looking inside the structure of a block

```

header: {
  number: {},
  previous_hash: "e4617a6446d30628b723206d3f0a0e61308e08dc5eef502bb4c87d228c1c4d10",
  data_hash: "38afae3941a400149c8508f7d0e4a26bf938cf60dd3a6f4be602ec829f7115fd"
},
data: {
  data: []
},
metadata: {
  metadata: []
}

```

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 in the next block.

More info: https://fabric-sdk-node.github.io/global.html#BlockchainInfo_anchor

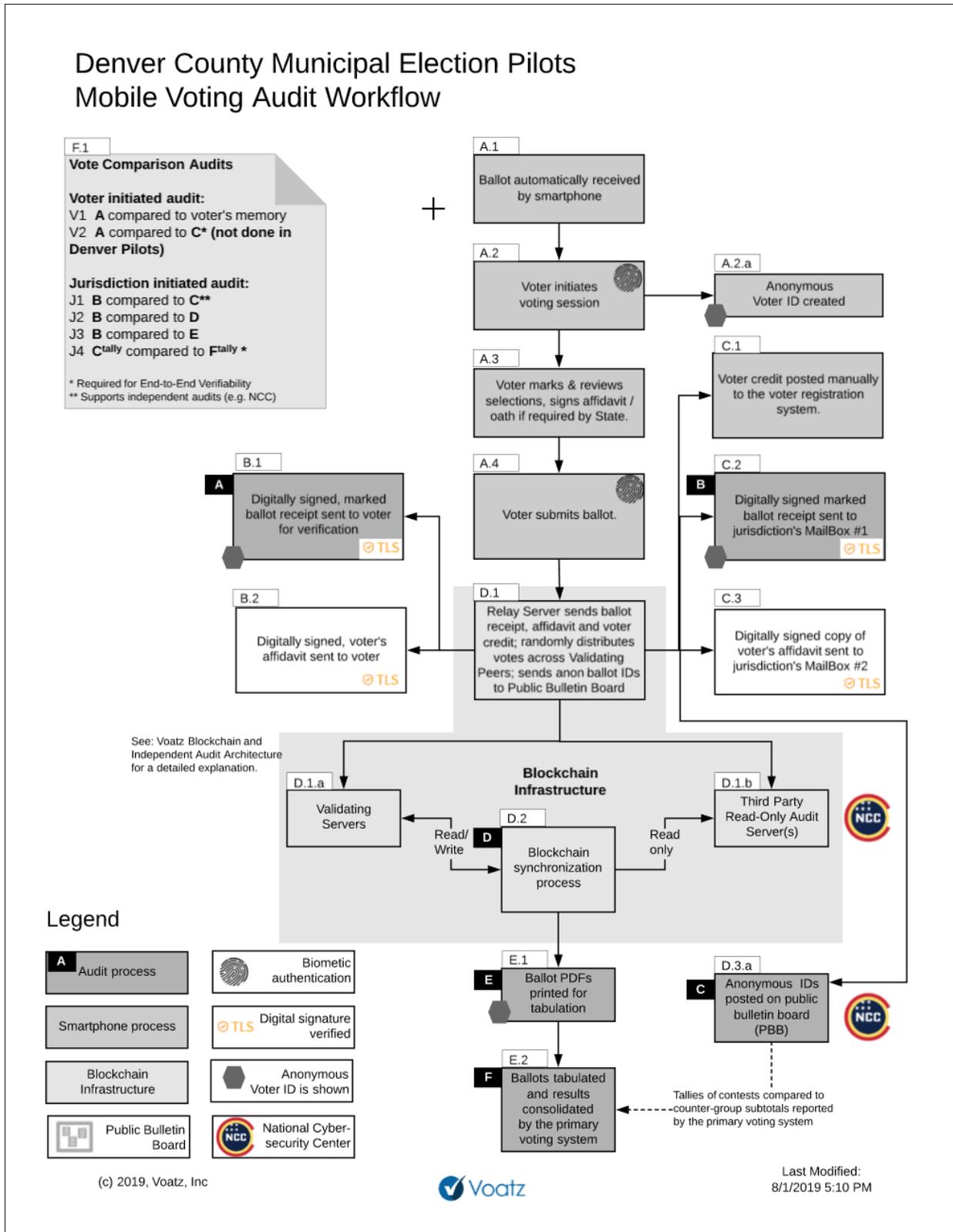
- Provide an independent, read-only node for a third party to review.

The node provided for both Denver audits was instantiated by Voatz on the Amazon AWS portion of the Voatz blockchain (see Appendix 7). Voatz agrees that NCC, and any other independent auditor, should be able to provision its own “bare metal” server, install both the open source distribution of the Hyperledger blockchain node and the credentials that are necessary to communicate with the blockchain network in read-only node.

- We also recommend reviewing the paper^{vi}, “Denver Voatz on cell phones – initial review” from Harvie Branscomb.

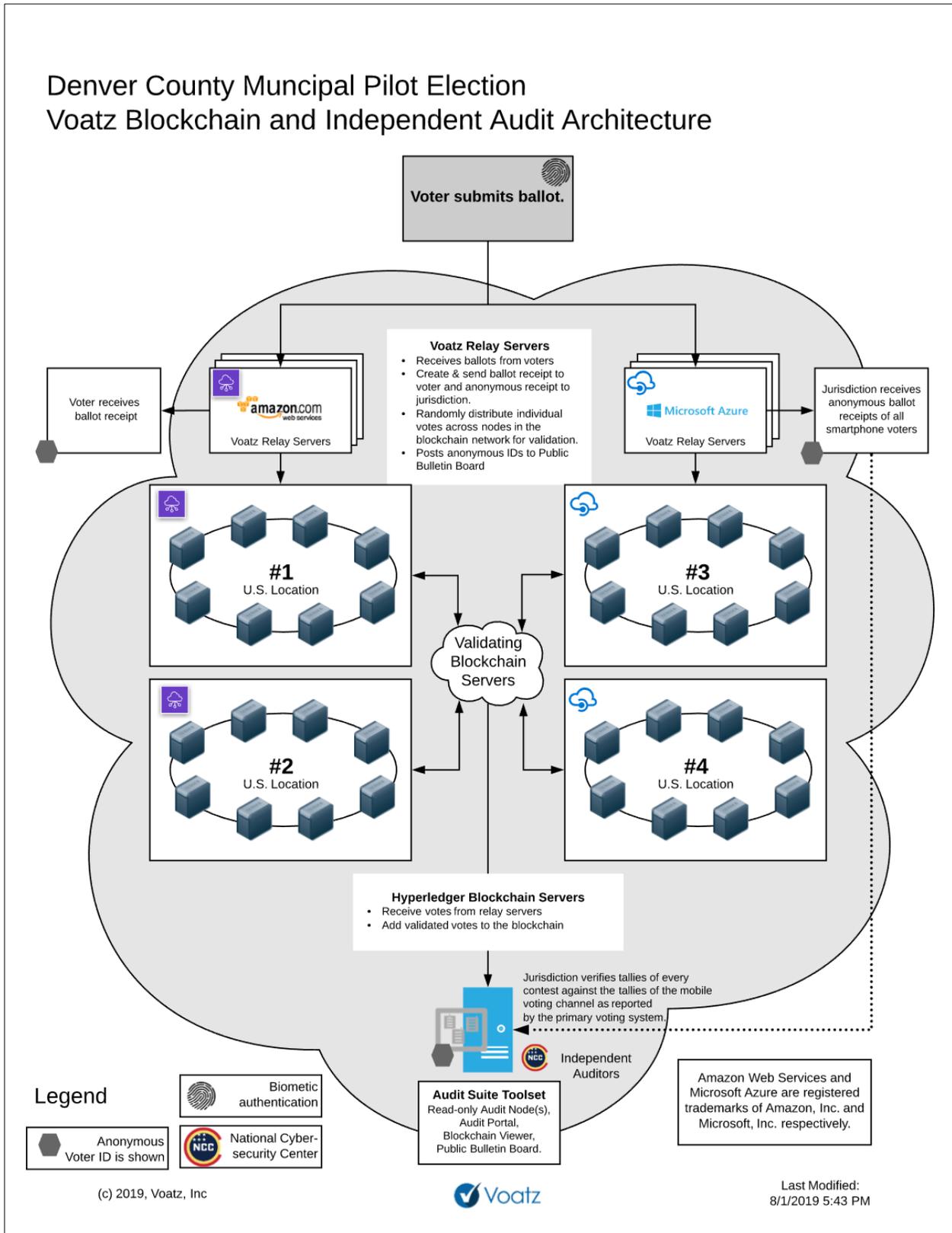
Appendix 6: The Voatz Audit Workflow (Diagram)

This diagram is taken from a forthcoming document on the architecture of the Voatz Mobile Voting Platform.



Appendix 7: The Voatz Blockchain and Independent Audit Architecture (Diagram)

This diagram is taken from a forthcoming document on the architecture of the Voatz Mobile Voting Platform.



Endnotes:

ⁱ See Kim, Eliot in Lawfare, July 26, 2019 “[Withdrawal from the Universal Postal Union: A Guide for the Perplexed](#)”

ⁱⁱ See, “DoD Releases Study of U.S. Voters Abroad” at <https://www.fvap.gov/info/news/2018/9/12/dod-releases-biennial-study-of-us-voters-abroad>

ⁱⁱⁱ See, The Muller Report, Volume 1 “[Report On The Investigation Into Russian Interference In The 2016 Presidential Election](#)”

^{iv} See, page 110 of “Election Administration and Voting Survey: 2018 Comprehensive Report” at https://www.eac.gov/assets/1/6/2018_EAVS_Report.pdf

^v See, Jocelyn Bucaro’s interview with Fox News at <http://bit.ly/2I4PlkP>

^{vi} See, Branscomb, Harvie “Denver Voatz on cell phones – initial review” at <http://electionquality.com/2019/05/denver-voatz-1/>