ELECTION AUDITS VIA BLOCKCHAIN

VOATZ, INC.
voatz.com

1 INTRODUCTION

Our Summer 2023 NASS white paper, “Take Me Out to the Blockchain,” explained blockchain technology using the analogy of a baseball game. [1] That paper is the keystone in an arc we are developing to elucidate this technology and show how it would apply to various operations and policies in a practical and efficient way. It explains that blockchains were developed as a means to establish trust between two or more groups that may be distrustful of each other. In particular, it proposed applications to voting and voter registration as a way to increase election security.

One question that paper posed was the following. If marked ballot data is recorded on a blockchain, how do you prevent the release of intermediate election results before an election closes? Our Summer 2024 NASS white paper, “*¡Olé!* Insights from Remote Voting in the 2024 Mexican Federal Election” described, at a relatively nontechnical level, how we solved that problem for the 2024 Mexican federal election. [2] A peer-reviewed article on the technical details, i.e., the cryptographic technology we used to encrypt ballots and tally these encrypted ballots, was recently published by the IEEE. [3]

We also posed a question about how to maintain a paper trail for auditing. Two possible solutions are covered in our Winter 2022 NASS white paper, “Parallel Internet and Paper Elections: A Practical PIPEline to Secure and Accessible Elections.” [4]

This paper will expand upon the summer 2023 paper by proposing the use of a blockchain to facilitate election audits. We note, however, that we currently do perform election audits using blockchain data [5], so the hypothetical language we use throughout this paper is intended for policy makers to envision how such audits could be conducted more broadly, even to election audits being open to the general public.

2 END-TO-END VERIFIABILITY

An effective election audit relies on a property of a voting system called **end-to-end verifiability**, particularly when ballots are cast digitally and there is no traditional paper audit trail. An end-to-end verifiable election is one in which any voter can verify that his or her ballot has been correctly recorded and anyone can verify that the ballots have been tallied correctly.

This catchy, 3-part definition is often used. In an end-to-end verifiable election, ballots are:

1 cast as intended,

2 recorded as cast, and

3 tallied as recorded.

A vaild audit relies upon an election canvass that assesses the eligibility of every ballot cast and counted, establishing a **one-to-one correspondence** between voters and ballots. [6]

The analogy in the next section is merely an illustration that describes an end-to-end voting protocol using paper ballots, giving the physical equivalent of a digital process.

3 PAPER BALLOT ANALOGY

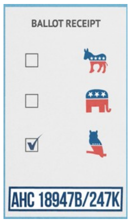
How would an end-to-end verifiable election work using hand-marked paper ballots?

First, how would an auditor, or any member of the public, check for a one-to-one correspondence of voters to ballots?

We would need a public record of the eligible voters, updated after the election with a record of who voted. Each member of the public would therefore verify their registration and voting status. We would also need a public record of the ballots, shuffled and enumerated so as to not compromise voters' privacy.

In this scenario, a voter posts his or her marked ballot in a public location with all other ballots. Tacking ballots to a large bulletin board would work.

You would want to distinguish your ballot from others so that you could pick it out at any time to verify that it is still present for tallying and that it has not been altered. How is that possible in a way that protects the privacy of the voters?



Each ballot would be printed with a unique, random ballot ID number that the voter would record. Then each voter could verify that his or her ballot has not been altered, duplicated, or removed.

So how do we prevent ballots from getting removed or counterfeit ballots from being posted on the bulletin board in the first place?

The one-to-one correspondence property and the use of ballot IDs allow for a valid post-election check. But a preventative measure would be to create a chain of ballots. Tack a blank 0th ballot to the bulletin board. The first marked ballot is appended to the 0th ballot, the second marked ballot is appended to the first, and so on.

This approach, however, might compromise a voter's privacy to several subsequent voters. Could the ballots be posted out of a strict chronological order?

Suppose instead of posting ballots directly, voters put their ballots in a box and mix it with other ballots. Periodically, an election official empties the box in full view of the public, shuffles the ballots into a random order, groups the ballots together, and appends that to the end of the current chain of ballots (or the blank 0th ballot). Then there is no longer a strict chronological ordering of the ballots.

With this approach, any member of the public, including auditors, could find a ballot by its ballot ID, tally the votes in any contest, compare the ballot count to the number of voters, and verify the integrity of the eligible voter list.

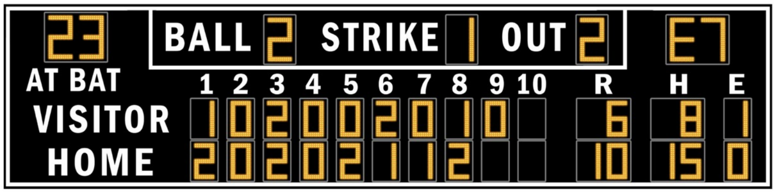
4 BLOCKCHAINS FOR AUDITING

The analogy in the previous section would be rather unwieldy in practice, but it is the essence of how a digital system records ballot data on a blockchain.

Numerous scholars have recognized blockchain technology as a means to achieve end-to-end verifiability in elections. See [7] for one reference.

In the digital example, the random and unique ballot ID would typically be created on a server when the ballot is cast. This ballot ID would be sent to the voter, election officials, and auditors. See [5] for an example for how we audit ballots on a blockchain, given this anonymous ballot ID.

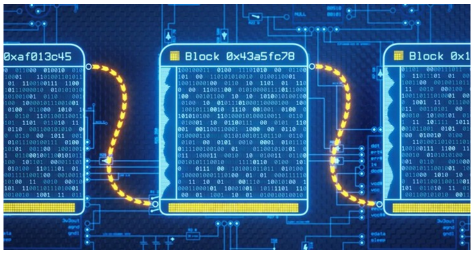
In the “Take Me Out to the Blockchain” article, a baseball scoreboard recorded the number of runs each team scored in each inning. Score data was chronological, verified, and immutable. Each half of an inning represented a **block** of data.



23 AT BAT · BALL 2 · STRIKE 1 · OUT 2 · E7

	1	2	3	4	5	6	7	8	9	10	R	H	E
VISITOR	1	0	2	0	0	2	0	1	0		6	8	1
HOME	2	0	2	0	2	1	1	2			10	15	0

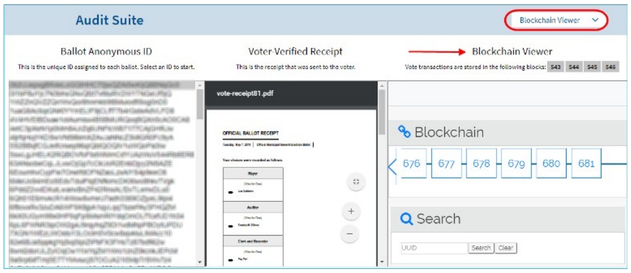
In our analogy in Section 3, the 0th (blank) ballot represents the **genesis block** of a blockchain that initiates the election. A set of ballots that is periodically mixed and posted represents a block of data that establishes a link of a blockchain. In the digital scenario, ballot data is ordered in a random order within the block.



In a blockchain, blocks of data are cryptographically linked so that past data cannot be erased or modified. In the analogy, this cryptographic link is the means of appending one set of ballots to the previous set.

If election data is recorded on a blockchain like this, what might an election audit look like?

At the close of the election, an audit portal would list the ballot IDs from ballots cast in the election. For each ballot ID, such a portal would display the printable marked ballot PDF, and the block(s) in which the corresponding ballot choices are recorded. A scan of the blockchain would check for a one-to-one correspondence of voters to ballot IDs and ballot IDs to ballots on the blockchain.



Audit Suite

Blockchain Viewer

Ballot Anonymous ID

This is the unique ID assigned to each ballot. Select an ID to start.

Voter-Verified Receipt

This is the receipt that was sent to the voter.

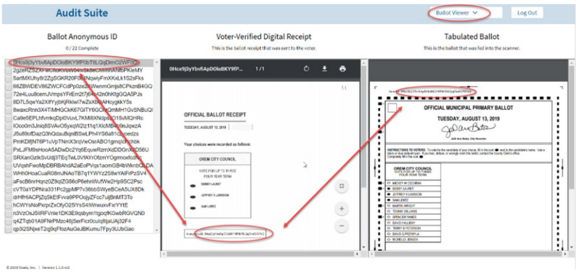
vote-receipt81.pdf

OFFICIAL BALLOT RECEIPT

Your choices were recorded as follows:

Blockchain Viewer

Vote transactions are stored in the following blocks: 543 544 545 546



Audit Suite

Ballot Viewer

Log Out

Ballot Anonymous ID

0 / 22 Complete

0Hcs9j3yYbvfiApDOloBKY9fP0bTtLQqDimO2WFnO
2gzeRZSZXFWCftoKVbW04vSk8eCMimhANfbPKieMY
5artMXUhy8r2ZgSGKR20F0d4NqwlyFmXKxLk1S2sFks
68ZBWDEV86ZWCFCdPp0ze2AWwnmGmjs8CPkznB4GQ
72e4Luu8cemJVmpsYFrEm2t7j64e42n0hKfgGQA5PJs
8D7L5qwYa2XlfYyjbKjRklwI7wZsXb0AHcygkkY5s
8waxcRnn3X4TIMHGCkK67GiTY6GCreQmMH1GvSNBuQ
Ca9e5EPLhfvmkqDpl0VuvL7KMi8XNdps2O15vMQHRc
lOco0m3Jniq8SVAvO5yxqW2lz11q1XlcMB4c9nJqwzA
J5u89ofDazQ3hQdauBqnlBSwLPh4YS6a81c2oedzs
PmKDlfjNT6P1uVpTNmX3rqVwOsrABO1gmqlcRchbk
PxLJFM9sHooA5ADwDc2Yq6EquwRzmXdDDGnX8D56U
SRXanGzlkSvUdj3TEqTwL0VfAYrOfzmYOgmoxfcdNc
UVqshFwoMpDBRBAhdA2aEoPVqs1aomGB4bWknbQLDA
WHh0HoaCuaR08mJNAoTB7q1YWYz2S8wYAlFrPzSV4
aFscB6nrHqnz0Z9qlZG56cP6ehnWufWw2Hp9SC2Psc
cVT0aYDPNra331Pc2gpMP7v36bbSWyeBCeA5UX8Dk
drHfHlACPjZqSkEtFvva9PPOojyZFcc7uijBnMT3To
hCWYsNoPxrprZxOfyO25lYsS4lWnwuxvFxrYYtE
n3VzOsJ5lIRFVnle1DK3E9qsbym1tgoqfKGwbRGVQN0
q4ZTqb01A9FNrPMzc46jSerFicr0culq8ljaUAj32F4
qp3i2SNjxeT2qj9qFtozAuGeJBKumu7Fpy3UJbGao

Voter-Verified Digital Receipt

This is the ballot receipt that was sent to the voter.

0Hcs9j3yYbvfiApDOloBKY9fP... 1 / 1

OFFICIAL BALLOT RECEIPT

TUESDAY, AUGUST 13, 2019

Your choices were recorded as follows:

OREM CITY COUNCIL

VOTE FOR UP TO THREE FOUR YEAR TERM

BOBBY LAURET

JEFFREY K LARSSON

SAM LENTZ

Tabulated Ballot

This is the ballot that was fed into the scanner.

OFFICIAL MUNICIPAL PRIMARY BALLOT

TUESDAY, AUGUST 13, 2019

INSTRUCTIONS TO VOTERS:

OREM CITY COUNCIL

VOTE FOR UP TO THREE FOUR YEAR TERM

○ MICKEY W COCHRAN
● BOBBY LAURET
● JEFFREY K LARSSON
● SAM LENTZ
○ MARTIN WRIGHT
○ TOMMY WILLIAMS
○ SPENCER RANDS
○ DAVID HALLIDAY
○ TERRY D PETERSON
○ DAVID G PRZYBYLA
○ MICHELLE JENSEN

© 2019 Voatz, Inc. | Version 1.1.0-rc2

A common auditing method is a “risk-limiting audit” of random subsets of ballots. One benefit of using a blockchain is that statistically significant random samples can be retrieved almost instantly using programmatic techniques, thus saving auditors a significant amount of time.

5 CONCLUSIONS

This exploration of blockchain technology is intended to help policy and decision makers understand the properties of this technology, the motivations behind its initial development, and its potential applications. Its application to elections is natural. Our various white papers have elucidated numerous aspects of its benefits: for voter registration, for election security, election integrity, and here for auditing.

Further benefits follow. Many of the operations of an election can be automated, including tallying and auditing. If such is the case, then how much would we save in election costs by moving elections to a digital or hybrid digital and paper format? This question will be explored in a future paper.

6 REFERENCES

1. Voatz, Inc. “Take Me Out to the Blockchain.” NASS 2023 Summer Conference. https://www.nass.org/sites/default/files/2023-07/issue-paper-Voatz-NASS-summer23.pdf

2. Voatz, Inc. “¡Olé! Insights from Remote Voting in the 2024 Mexican Federal Election.” NASS 2024 Summer Conference. https://www.nass.org/sites/default/files/2024-06/Voatz-Issue-Paper-NASS-Summer24.pdf

3. E. Landquist, N. Sawhney, and S. Sawhney. “Overcoming Bottlenecks in Homomorphic Encryption for the 2024 Mexican Federal Election,” 2024. https://blockchain.ieee.org/images/files/pdf/techbriefs/tb-2024/TB-2024-3_VoatzMexicoRevised.pdf

4. Voatz, Inc. “Parallel Internet and Paper Elections: A Practical PIPEline to Secure and Accessible Elections.” NASS 2022 Winter Conference. https://www.nass.org/sites/default/files/2022-02/Voatz-white-paper-nass-winter-2022.pdf

5. Voatz, Inc. “How to Audit Your Vote with Voatz.” https://vimeo.com/431781714/e419d0be7a

6. EAC, “Guide to the Canvass,” 2022. https://www.eac.gov/sites/default/files/electionofficials/post-election/Guide_to_the_Canvass_EAC.pdf

7. A. J. Perez and E. N. Ceesay, “Improving end-to-end verifiable voting systems with blockchain technologies,” 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1108–1115, 2018. https://ieeexplore.ieee.org/document/8726502

QR Codes for References: