OSET INSTITUTE

TRUST THE VOTE PROJECT

Security Innovation in Voter Registration Management

Vanadium™

Overview

Project Vanadium ("veh-nay-dee-um") is a timely, if not imperative software development effort for Pilot deployments in 2023 to demonstrate how the use of digital ledger technology (Blockchain-like) can revolutionize the security and integrity of voter rolls, while ***not*** requiring any change to existing practices of voter registration processing and voter list management. Success of pilots will serve as reference for production deployments. The Institute has several States and/or their counties interested; and seeks to launch with a consortium of at least five.

> Vanadium addresses a clear and present elector and voter registration database security issue: how does one verify the integrity of the voter roll against allegations of unauthorized poking, prodding, or penetration of the registration system?

In the spirit of developing technology with horizontal applicability where appropriate, lessons learned from Vanadium can be equally applicable to many kinds of government IT processing practices that have similar requirements and current challenges: systems that require *irreversible* transactions and *tamper-proof* transaction records, but are beset by IT privilege abuse threats and limited security of legacy database management systems (DBMSs). However, for purposes of the OSET Institute, the imperative application is for the *integrity of voter registration databases*.

For the U.S., this project has enormous importance and timeliness in light of the upcoming 2024 U.S. General Election (for which we anticipate learning from observation during the midterms of this year). Voter registration systems continue to represent a clear and present cyber-attack target and risk. Vanadium was originally a collaborative project with **Accenture Labs**, **AWS**, and **DXC Technology**. Today, we continue to work closely with AWS and Google Cloud.

The Challenge

Today, nearly everywhere—in the U.S. and abroad—we find that voter rolls (lists) are stored in traditional relational database management systems, with no practical controls on data integrity. Ideally, the Elector/Voter Records Database (VRDB) would be modified only by a voter records management application, used by an authorized election official. In practice, the database is accessible to a variety of IT administrator and database administrator staff. The data is vulnerable not only to abuse of this privilege, but theft of this privilege and use by adversaries. As usually deployed in a typical datacenter environment, the data in a VRDB is vulnerable to attacks via privilege abuse or theft of privilege of any of a large number of IT staff and elections staff.

Given these basic vulnerabilities, the threat surface is broad, including the home-based, or mobile personal computers used for remote access by IT staff or election administration staff, to phishing for election staff access credentials to the VR system, to the gateway routers in regional office environments and staff's home routers.

This high-risk operation is the result of one major mismatch between a system objective and a design flaw.

- The objective: elector and voter records transactions need to be *immutable*;
- The design flaw: rather than being the primary data, the transactions are not stored in the DBMS, but rather used to drive the transaction's changes to a voter record.

As a result of the design flaw, the transactions are *not* immutable, and records can be modified out-of-band of legitimate transactions.

For example, once an authorized election official completes a transaction, such as re-activating an inactive voter's record as a result of their voting, that transaction should not be reversed, ever. It may be superseded by another transaction, such as in the U.S. another election official deactivating the voter record due to a felon match with States' Department of Corrections data, but the previous reactivation should *never* be reversed.

Another example: after a transaction creates a new voter record, a later transaction can change the voter's name, but there is no transaction to change a voter's data of birth; yet DOB is just as easily modifiable in the VRDB as the voter's name.

In reality, any actor that has obtained access to the DBMS can freely modify the content of the database. The choice of mutable data in a DBMS as the basis for voter records is a choice that makes it impractical to meet the data integrity requirements.

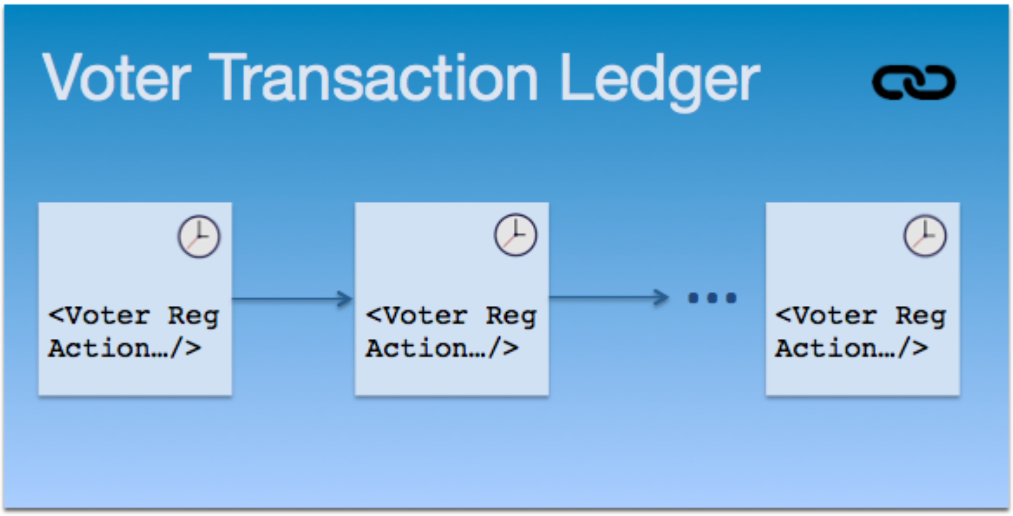

Figure 1. A Digital Ledger of Voter Records Transactions

The Vanadium Approach

Today, the voter registration DBMS is the mechanism for storing the data-of-record for a voter list. The Vanadium technical approach in the near term is to augment the DBMS by adding a digital ledger that immutably records each voter record transaction.

If any actor in a voter registration system needs to ensure the integrity of a voter list, that voter list can be reconstructed by replaying all the transactions (*add, update, and delete records*) up to the desired date. Even completely removed voter records have an immutable history in the ledger, from the transaction that created the record to the transaction that deleted it.

For purposes of this type of records keeping, "immutability" can be explained as follows. The primary data object is the voter records transaction. Each transaction, stored as a ledger item, is tamper-evident to all viewers, and tampering will only be possible with collusion among the multiple parties each of which operates a node in the distributed data-store that redundantly stores each transaction.

Instead of making changes to a specific voter record, the Vanadium data layer stores every transaction on a voter record including those that modify it. Instead of DBMS queries on a voter record, Vanadium enables a scan of the entire ledger for relevant transactions to replay, in order to determine the current state of a voter record.

Whereas current systems rely on DBMS capabilities for reporting, in the future Vanadium will provide a capability to replay the entire ledger into a transient DBMS that can be used for query-based processing.

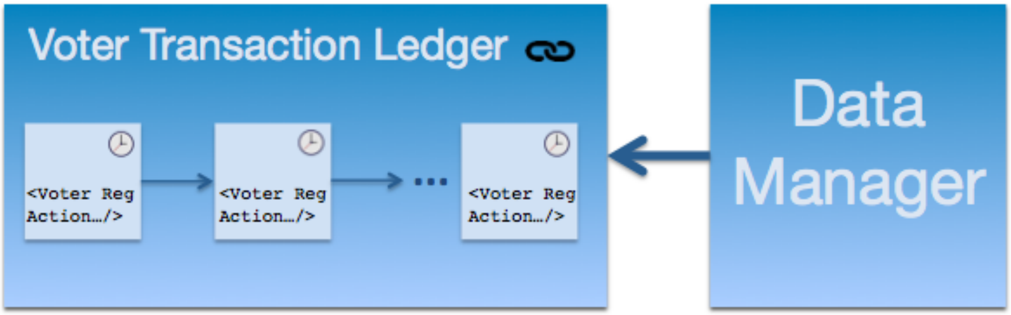

Figure 2. Vanadium Data Manager Controls Appends to the Ledger

The Vanadium Pilot and Related Tasks

Today's voter databases are a highly scalable threat. In 2016 in the U.S. over two-dozen voter registration systems were poked, prodded, and in several cases penetrated. However, it was difficult, and in some cases, impossible to determine if the voter roll had been tampered, or even if it were possible, proving such including the use of rollbacks was difficult and inconclusive. There is a need for a verification service that can layer on to the legacy voter registration database without requiring alterations to the existing production system.

Vanadium can address this by providing a Blockchain-like ledger as the definitive repository of all voter registration transactions (create, update, suspend, etc.) for each voter registration record contained in the legacy DBMS that provides strong data security, redundancy, and accountability.[1] In practice, if anything untoward is alleged to have happened to that voter registration database during an election cycle, the voter records can be recovered from the Vanadium ledger.

When the time comes to produce a list of qualified voters for a given election, both the existing legacy voter registration DBMS method and the ledger-based method can be exercised, so that any variance would be an immediate way to detect possible issues with the voter registration database.

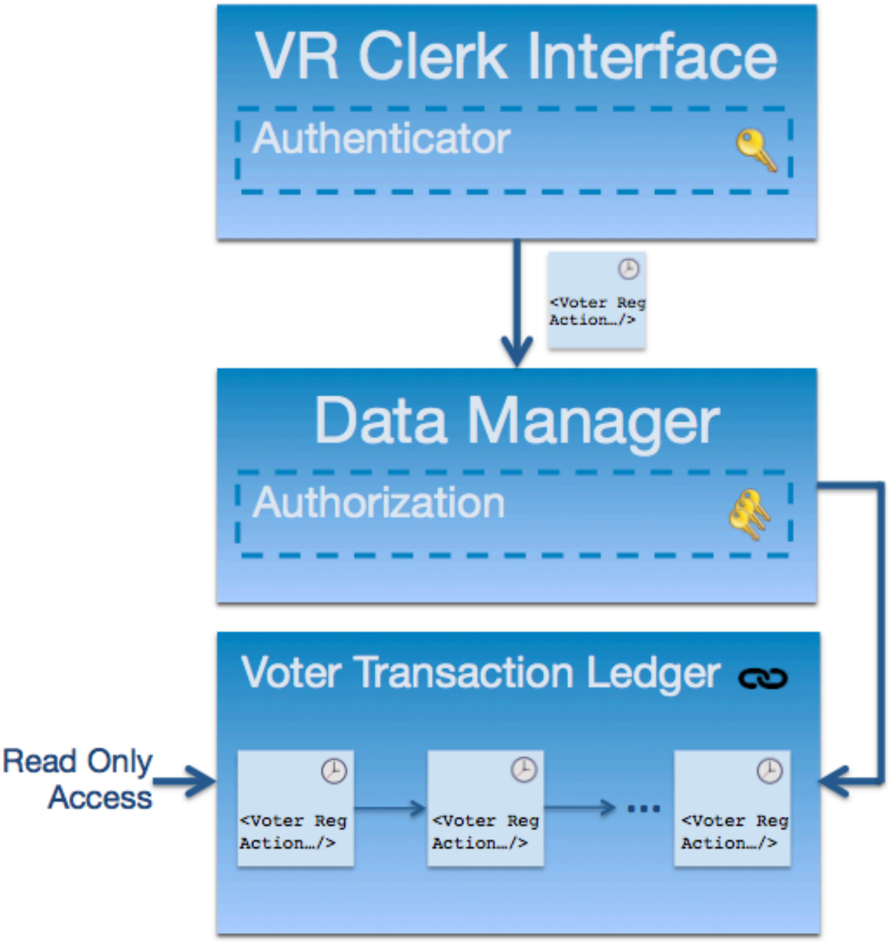

Figure 3. Voter Registration Clerks Submit Authorized Transactions to the Data Manager

It's worth noting to drive home the intent of the Pilots (*five contemplated so far*), the ledger will be a cryptographically protected *append-only* audit log of actions that change the existing Elector/Voter Registration Database (VRDB). It will be used to re-compute

[1] The OSET Institute has an innovation agenda to demonstrate responsible uses of Blockchain-class technology outside of ballot casting and counting. Immutable ledgers are a key opportunity to do so.

the voter list at any time, in order to either verify that the current VRDB is valid, or identify potential issues.[2]

The Vanadium Pilot will include:

- A complete data layer centered on the ledger;
- A subset of the voter registration data schema (*based on existing national data standards from the National Institute for Standards and Technology* (*"NIST"*));[3]
- A complete *but scaled-back* authorization layer, including data authentication; and
- A *demonstration application* that implements the user interface and business logic of common, essential voter registration system functions.

The central task is the construction of the ledger itself, using software building blocks provided by the Linux Foundation's HyperLedger Project.[4] Use of HyperLedger both reduces the development level of effort and ensures proper implementation of the cryptographic primitives by re-use of established and tested software. Deployment of the ledger will include four (4) nodes to implement the synchronization protocols, and act as local data stores for each of four (4) participants (*in the manner that each county would be a player in a state's distributed database of VR transactions*).

The POC system itself will be a privileged client of the ledger servers, with permission to append transactions to the ledger. The system will be implemented as a simple web application with the user interface and business logic for recordation of common voter records transactions.

The ledger servers and the POC system will be initially deployed as AWS virtual servers, using machine images pre-configured for appropriate server security practices (**Note**: Amazon AWS is a significant annual supporter of the OSET Institute's work).

Based on this work the first "deployment opportunity" (starting as a Pilot with a few state or county election jurisdiction partners) includes building:

- The Data Manager;
- The authentication and authorization subsystem; and
- The Clerks' Client App.

We intend these Pilots will include all of the necessary documentation, visual explanatory aides, user interface work for the demonstration system; a white paper, and

[2] We should note that over time, the situation will likely reverse, with the ledger becoming the data of record, and the legacy VRDB being used as a transient copy that's convenient for standard SQL-based legacy components such as reporting.

[3] While Vanadium has an initial U.S. perspective, the OSET Institute has been approached by two other countries interested in the potential of this technology for their own elector and voter registration systems. The U.S. NIST Standard is: NIST 1500-103. A good portion of this data standard was authored by OSET Institute's CTO, John Sebes. See: https://pages.nist.gov/VoterRecordsInterchange/

[4] https://www.hyperledger.org/

with approval of Pilot participants, public demonstrations at major election official events (conferences) in 2023.

We anticipate applying formal methods for development of elements of Vanadium in order to facilitate a fully transparent peer-reviewed system given it national security interest (the initial pilot of this was demonstrated to DHS/CISA in October 2019 prior to the emergence of the global COVID-19 pandemic).

If successful as anticipated, opportunities to deploy production versions of Vanadium could present themselves in time for the 2024 Presidential election cycle.

For more information contact:

For technical questions: John Sebes, CTO, OSET Institute | jsebes@osetinstitute.org

For Pilot information: Gregory Miller, COO, OSET Institute | gmiller@osetinstitute.org