# SOVRINTown- Evoting System Module Story

**Problem Statement**

voter fraud in existing blackbox voting systems where the vote outcome/result is completely controlled by 3rd parties, not the voting populus.

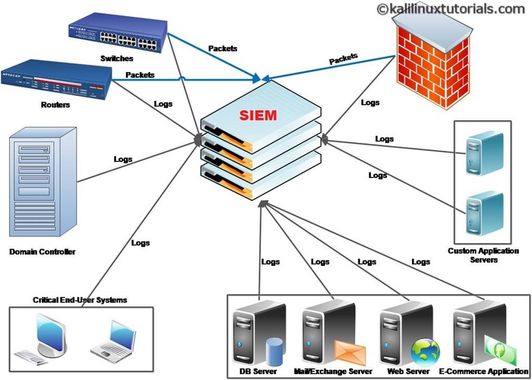
**Solution Goal:** Re-develop Voting Systems in Open Source using existing proven Distributed Ledgers and New security models operating on low cost, fast, low latency simplified networking technologies with built in data flow and C2 log transparency.

**Voting System Security Model: Layered**



**Primary Goal of Security Model : Reduce the Number of Attack Surfaces First.**

**Reference Model : Existing C2 "Common Criteria Logging" SIEM**



In the banking world, SIEM is the order of the day. Say What?

"Secure Information and Event Management", SIEM is a mandatory requirement in most countries, enforced under regulatory statutes or law, that say the bank must track and accurately report what they are doing with your money, often and accurately to keep their bank license.

**SIEM Applicability to Evoting Systems: Partial.** While the SIEM system model is good enough for financial systems, is it good enough to protect evoting systems?SIEM is a partial baseline reference model architecture for trusted voting systems, which can help to secure and support online, in person and even manual voting processes. SIEM is good at the preservation of log data “chain of custody”. Additional references is the C2 "Common Criteria" milspec l[ogging system](https://sourceforge.net/projects/sherlock/) on SF.Net, cited in google patents by many vendors of SIEM and, used today by companies like IBM and HP, way back in 2002.

"Chain of custody" in the C2 "milspec" world gets used by the military and, Telecoms as well as Power Management Systems, to ensure these market players know what happened.

SIEM is largely reactive , not so much dynamically prescriptive, and is used to support a court order as evidence needed to enforce the law when it's broken in the world of Cyber hacks altering or stealing data, like what happened the US 2020 election.

Does SIEM stop cyber vandalism or theft of data? Definitely Not. Does SIEM help in identifying the vandalism and theft activity? Partially, provided the activity is stored in HA SAN Storage protected the C2 Logs.

**EVoting Systems Visibility- In Real Time during the Vote, to Protect Vote Integrity**

Network Sniffers should be employed to watch evoting system network data flows between URIs within and between the precincts or regions, and also watch and capture DNTP protocol time stamped data flows occurring between the states/provinces evoting system backplane networks , where each control, monitoring and data plane set of flows are sniff copied with a sampling rate at minimum to allow the election management team to in real time monitor the health of these flows and also in real time and post election, analyse those flows, so that their behavior can be cross referenced what you see with the evoting system actual C2 logs collected by the system nodes and stored on a HA availability SAN Storage array managed by the state or province election management team, so the election observers can see whether or not the systems behaved as advertised and/or if that advertised behavior was subverted in anyway.



Sniffing made possible the DoD event which raided a server farm in Germany in November of 2020 shortly after the US Election being operated by subverting forces. REcent news of this event has come to light, where the US Cyber Security elements of the DoD apparently setup a "Sting" surveillance through sniffing TCP/IP traffic to that site, that is they sniffed/copied the data flows (without detection) to ID the destination, located the German US Base Data Centre or Colo running the Vote Manipulation Server (virtual most likely operating as a VM operating the containerized, subverting "vote manipulation" code which was creating all the US voter fraud occurring inside the remote Dominion Voting machines, where the sniff of the data flow source address tells where the data comes from, and where the data flow answers and commands were returned from the Remote US Base Server in Germany, which means the code at the source had a backdoor "daemon" chunk of redirection code (usually a copy of "contents addressable memory' CAM in the router/switch is copied to do the sniff in the router itself, or the cable, wireless channel or fiber is tapped/monitored/sniffed by an external "Sniffer" and, on the source address server itself, a 'masquerading chunk of code' (replacement with same name and even size but with backdoor copy write subroutine, periodically sending out data flows to the external destination address (then routed elsewhere by the router/switch through, or around a firewall (adjacent wireless listening router masquerading as a legit Border Router for example), etc.., which does the data register copy from the stack address, for example)

**Additional “Security Layers” for EVoting Systems**

In building up the NextGen Voting System- One Layer of the Security Onion at a Time...

Much has been written about the Security Onion as it applies to protecting Software, all of it applies to voting systems, in today's modern age of Open Source. What I will say is that honest voting starts with the voter themselves, That means the voting system must have accurate validation of the Voter, before they are added to the Voter Registration List.

**SecureID- IOTA example**

SEcureID Software, such as the same named code which works with IOTA's Distributed permissionless Ledger technology, the #TANGLE, needs some additional data input from different ID equipment to be properly employed as part of an Open Source, Transparent Voting System, SOVRINTown. Such equipment enable accurate Bio-metrics validation of the Voter in multiple ways , ie : scanning eye balls, thumbs, recording voices and a picture of the voters face, all in private. The voting system must have the artifacts encrypted and only accessible to the voter to ensure a 100% trusted and transparent form of voting able to match/check the voter applying for voter registration from anywhere to the same data on the voter registration list operating as part of the Voting Epoch Smart Contract running the state , local or even national election in your locale. No people are required in the middle, nor wanted to verify the voter’s right to vote and thus allow the voter to exercise their voting right in complete privacy, at home, in their car or at the polling station. IN this configuration, No one can possibly alter voter data, as only the voter controls the public and private keys via a one time use voting wallet with the colored coins used to place the voter selections on the unique ID voter ballot., as issued by that same Voting Epoch Smart Contract. Validating the Voting Epoch Smart Contract code with trusted , bonded, third party experts is mandatory.

**Smart Contracts- Vote Epoch SC as a Layer 1 SC please, IOTA UTXO Example**

Qualifier: [IOTA's SC](https://blog.iota.org/an-introduction-to-iota-smart-contracts-16ea6f247936/) technology is still in alpha mode with three PoC contracts out "in the wild" to show how their Layer 1 system works, using BTC style UTXO accounting methods, to record transaction data on the #TANGLE DAG "Direct Acyclic Graph". That said the direction IOTA are heading suits the SOVRINTown Project software and solution architecture needs. The existing IOTA SC capabilities enable the ability to design and create a Voting Epoch Smart Contract which issues unique Ballot/wallet/colored coin 'VoterPak' sent securely to the verified voter to run in any browser (possibly as a Browser add-in Extension)on any popular smartphone, table, desktop or tower systems out there running IOS, Android, Windows or Linux. Portability of the extension as assigned to the Voter’s browser is possible, but only after the vote, so the voter can check the status of the Voting Epoch and the status of the voter’s own vote (Posted, consensus validated, added to the vote total, with a Distributed Ledger address accessible only by the voter)

**ZeroProofs- Protecting Voter Privacy**

ZeroProofs (ie- Zcash and others) are one of the best ways to protect voter privacy, the root code is open source, so security can be mathematically proven. “ZPs” as they can be called, means the voter using ZP can get validated as a voter and, at anytime go to a voter precinct, flash the VoterPak (Browser DApp) produced QR Code and the precinct will accept it based on the previous Registration effort , checking the Registration List automatically, WITHOUT A HUMAN REQUIRED acting as gatekeeper. The next step thereafter is the election staff simply make a station available to the voter, at the voter’s option (if the voter is interned and can't get around then the voter can vote remotely). The Station checks the voter provided ZP data in privacy via ZP challenge again, meaning a few key ID artifacts under only the voter control are mathematically verified as voter owned by the voting station, ie- the voter is who who they say they are, then the voting station system allows the voter to place the vote, right from their own device, or directly from the voting station. If the voter is not on the list, then the VoterPak Dapp operating in the Browser found on the voter’s device records that fact to the voting Systems Distributed private Ledger DPL node instance of IOTA responding first (and likely nearest and least busy)to backplane/network connected vote station, where the said DpL node requests a cross-state/province check consensus that will add the voter add request to the voter role/list once it is proved indeed unique (the voter is NOT registered anywhere else within the voting jurisdiction of multiple state.provinces to vote). This ‘cross-check’ must take only a few seconds, so the voter registering for the first time at the polling station quickly gets the "green light" indicator in the VoterPak Dapp and now the voter is registered and ready to place their selections using colored coins on the VoterPak Dapp attached unique voter Ballot record.

**DPLs "Distributed Public Ledgers"**- A Network of Voter Consensus/Settlement Nodes

DPL Nodes connect on the Backplane nd between Backplanes to create the voting system secured set of Distributed Secured Vote Settlement, Reporting & Logging Nodes collectively delivering the TRansactios Per Second computing throughput needed “TPS” to process the vote volume in sufficient time to make the voting experience adequate. In this story we use a private “forked” instance IOTA’s TANGLE DPL with mandatory security audit completed on the open source code. Use of the IOTA TANGLE requires the “Community of Interest”, a set of Nodes , are organized for Consensus of the Votes places between nodes

Are “geo-fence” organized within the state/province on their own unique Backplane/network, where the federal authorities must provide the interstate connectivity with URL to IP NAT Network Address Translation SCION Border Router services being connected between state Backplane/Networks by via Dark fibre and/or FlexE MAC Transport fiber connected SCION Border Router clusters.

**Smart Contracts- “Federal/State Voting Code for The Registration List, The Vote Epoch, Vote Reporting**

How the SC is constructed to create the Voting Epoch form desired by the State/Province and Federal bodies governing the vote epoch, is largely the job of the state/province legislature to ensure the SC logic is correctly matching the intent of the state/prov. Constitution in accordance with the Federal constitution, that is, its is the state/proncics responsibility as primary authority and operator of the voting system to ensure the SC operates within the constructs of the state/province level constitution rule of law. lawyers must be involved together with third party auditors, to make sure the voting populus funds are used to achieve the legal outcome governing the voting process. The design of SOVRINTown is intended to support the creation of multiple SC templates, as is, to help speed the process of creating state and province specific Voting Epoch SCs, so be easily customized by hired programmers tuning the SC to accurately match the locale rule of law.

**Voter Vote Epoch Private Wallet "VoterPak"- A Browser Based UI for Voting**

The SOVRINTown VoterPak DApp is a Voting Epoch Smart Contract Issued by your assigned Precinct/Region, One Per Precinct. Not all Precincts or regions will be willing to adopt this method for various reasons, mostly political, so those that do, need to know that each precinct has their own Voting Epoch SC for their precinct or region, a subset of the National Vote Register operated by the DPL instance where the Precinct/REgion Voting Epoch SC only operates within the Community of Interest Nodes, an assigned group of IOTA Hornet or Bee Nodes controlling the Front End of voter ID verification to the State/Province Voter REgistration List, before the voter’s vote is placed via the Station or their own device running the VoterPak Dapp. This hybrid design support means not only hybrid voting systems can operate in parallel at different voting stations, this effective "zoning" by precinct also means the entire voting system scales in parallel at really low cost to the ratepayer. VoterPak Dapps built into your Browser come with a voter unique Public and Private Key protected one time use Wallet, with a correct, set number of Selection choices for the unique ID Ballot assigned to you the voter as issued by the precinct/region Voting Epoch SC (Their are multiple Identical instances of the SC in each precinct/region each matchd to their own precinct/region voter registration list, input by the election committee and or via remote online registration by the voter prior to the Vote Epoch) , where the SC restricted number of colored coins ensure accurate, transparent voting by the voter. The one-time use Wallet, must use 'throw away' one time use Winternitz or Equivalent public/private keys (reference the IOTA Wallet for details), and must be Quantum computer Hack Resistent

**Colored Coins- How the Voter Places their Vote Selection on their VoterPak Dapp supplied Unique Ballot**

Each one time use Voting Wallet comes with just enough colored coins to be placed on the Bingo Card voter ballot (presented in the DApp UI to the voter via their Browser) with a unique ballot registration ID matched to the voter SecureID. Only the Vote Epoch SC for the Precinct/Region can issue the one time use voter Wallet which contains the coloured coins which is issued only after first checking the State Voter Register List running on the BEE IOTA Permanode operated by the State updated by the Precinct/Region with State issued key access to the Registration List Dapp. If the voter is not on the list but does have the right ID verified at the voting station by the voting station employee, the voting station employee scans the ID barcodes, which are then added to the State DpL waiting for approval , and via STREAMs a request to all the other the Cross State App Voter Registration Check BEE Nodes, the entry waiting for approval is compared to all other State Nodes via Fast Consensus where the result must be 100% of the operating nodes agree, at that point the local voter new registration transaction is approved and accepted by the State Vote Epoch Bee Node via the Registration List SC which time stamps using dNTP the add to the State IOTA Tangle Distributed Private Ledger and an acknowledgement is sent to the Voter Dapp unique instance requesting the registration list add.



**The SC controlled Private Ballot- How the voter places their vote choices with Colored Coins using One-Time Use Voting Epoch Wallet**

First, when the one time wallet is issued to the voter after registration check and approval, the Time is stamped via "in State" dNTP daemons running as jobs only accessible from the State Precinct Specific Epoch Vote Smart Contract serving the Precinct registered voter , checking the nearest State permanode IOTA BeeNode Master Copy of the State Registered Voter List via a Wallet contained rolling list to find the other State nodes, should that first state node be down for any reason, the Dapp will go to the next node and, so on, in a circular list check, until the timestamp is achieved, once. Once confirmed, the voter running the unique serialized one time use Dapp complete with wallet and colored coins is ready to place their vote on the Web UI presented Ballot "Bingo Card" . The Wallet only contains the number of unique vote selections as colored coins which are dragged and dropped by mouse controlled cursor on the desktop (interns and absentee voters, remote voters using a desktop) or with their finger or thumb if using an Android device to fit the round coin into the Square vote selection box for the candidate listed. The voter can move the coins around as much as they want, once they are certain, they hit the vote button, and are asked via a pop up window to confirm use or no, once, if no then returned to the Ui, if Yes, asked again y/n are they sure? if yes the vote is then written to the State DPL TANGLE instance waiting for a second confirmation consensus check of all state nodes.

**Inter-State/Province Registration List Cross Checks- Unique Voter Assurance**

The SOVRINTown voting system dictates use of FEDERALLY OPERATED

Dark Fiber used to Connect the Precinct DPL Nodes together, in State or Province

For Interstate Voter Role/List checks to ensure there are no duplicate vote, The Federal governing body IT staff managing the national vote managing those gateways, use URL Universal Resource Label mappings to IP addresses with a unique State private AS "Autonomous System" number "AS#" to facilitate such checks between states through the SCION Border Router Cluster, often referred to as NAT Network Address Translation Function.

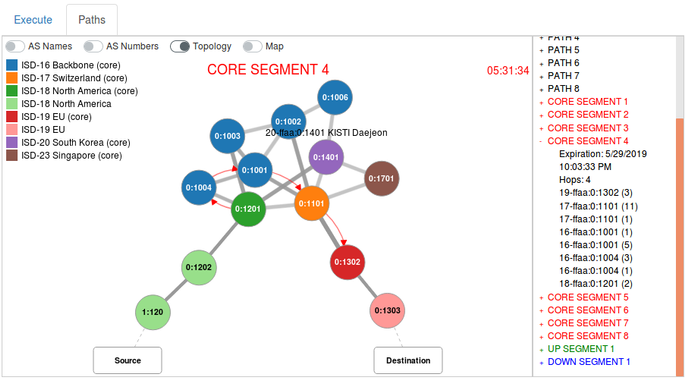
**In State/Province BackPlane Networks- Fast Safe Vote Count & Roll-up Tabulation**

Connecting the State/Province Voting System Precincts/Regions together as one modern PCIe Hi-speed, low latency, path and channel switched Compute Backplane noth simplifies voting system setup and ensures fast,secure vote tabulation. In the SOVRINTown Project we are designing data . control and monitoring planes to handle each unique data flow with per Session SASL security protection of those data flows between bacplane connected node URLs. Such handling of the communications Control, Monitoring and Data Planes between nodes, are source destination URI addressed nodes mapped to PCIe Backplane registration Log IDs flow (Channels/Paths on PCIe) shared by all nodes on the same backplane,creating one big computing complex (like a big single computer) of interconnected logical devices (the nodes in this case), each with their own PCIe Transceiver NIC connected to the nearesr switching Backplane device (2U appliance for example) , a Backplane on which multiple precinct located colos operate. The nodes are linked together by URI (Universal REsource Identification) addresses matched to the URL "Label". PCIe, in current 4.0 form, is super Low guaranteed Latency. SOVRINTown’s use of Layer 5 SASL Secured BEEP protocol secures the node application ISO Model Layer 5 port originating data flows between node Back End 'BE' "headless" MEAN Micro Services (singlet , single purpose applications operating in clusters, hosted in containers of disparate Virtual Machines mounted on different physical hardware). It is over such URL/URI to PCIe mapped addressing schemes, performance of the SOVRINTown voting system is expected to be “near wire speed” in terms of IOPs or Gigabytes per second throughput between nodes, due largely to the way PCIe employs fewer software Stack (driver) interfaces and attack surfaces. PCIe is the only economic network backplane today which delivers ‘guaranteed’ low latency of data unit delivery between devices, every time, with 10 times less latency than TCP/IP at a minimum, while easily matches and in most real life operations exceeds Ethernet's advertised, aggregate link/leaf measured "data rate" througputs (ie 100gbit/sec Ethernet vs 126Gbit/s PCIe 4.0 )

*(n.b. This PCIe 'Backplane' technology is used for weapon systems in the DoD today, where delay is measured in 1 to 5 microsecond ranges making it easy to trust dNTP time stamps of data flows and related logged data frames, where as TCP is 10 times slower and erratic, with 5 to 10 times more attack surface interfaces in the software stack).*

**Data Flow GeoFencing -Keeping your Vote in State or Province- SCION BR Clusters**

SOVRINTown utilizes next generation Border Routing Clusters as specified in the SCION protocol, the open source project originating out of Zurich ETH, Switzerland.



SCION Protocol enables a concert known as “Data Flow GeoFencing” - that is embodied by the replacement or coexistence of legacy Autonomous Systemss (AS#s) with iSDs “Isolated System Domains. SOVRINTown’s use of both iSD#s and AS#s ensure the voting system can support legacy IP network transport between precincts/regions and/or states/province SOVRINTown equipped voting systems as well as next generation PCIe Backplane enabled versions of the same system. Votes in State or Province are inter-connected via Federally operated SCION BR Clusters positioned between State/Province run SOVRINTown voting systems. Such BR Clusters are Federally Supplied/operated.

Federal authorities are responsible for setup of SCION BR's to Run/operate the included NAT URI to IP Network Address Translation at data flow ingress (entry), specialized open source code added to the base SCION BR open source implementation, by the SOVRINTown project, added as an operating cluster of micro service Application instance in the MEAN FE Front End design model spirit and made part of the SOVRINTown version of the Multiple Node SCION Border Router Clusters deployed for the above purpose.

*n.b.- the SCION ensures there are no BGPSec PKI key breaches (behaving as a trusted BGPsec router used to exchange routing info after PKI key check) allowing any sort of "data flow hijacking" which currently persists and plagues all IP networks daily. (This is how Zoom traffic was routed into and out of China) .*

The SCION BR cluster enables the cross state voter registration consensus check run by the major permanode BEE IOTA instances which have the entire State voter registration on hand, which gets cross checked using the IOTA Fast Consensus algorithm running in each state/province BEE Node. In the case of the 'hypothetical' US SOVRINtown setup, there are at least 3 nodes recommended per state, which means 150 nodes must agree 100% the voter added to the composite USA wide voter registration data is indeed unique. There can be several BRs per State into each Adjacent State. Transits between states are best configured over PVC permanent Virtual Circuits "nailed up" over Dark optically amplified Fibre over a specific light spectrum channel " say indigo for example) between nearest adjacent State/Province Edge BR Clusters to keep the Dark fibre runs within the Single Mode Fiber signal distance specification. Alaska and Hawaii , Puerto Rico are handled as special transit cases for the USA through Federally contracted connections over Fiber using existing TCP/IP transport BR to BR Cluster, transiting operator purchased IP STUNLs Secure Tunnels of Layer 3 encapsulating the PCIe Traffic in Ethernet MAC Frames is one way to do it...)

**3rd Party SC Controlled Report Server- Rolling up the Vote to a Summary for Your State/Province Union to feed 3rd party News outlets reporting on the Vote Epoch**

This section points out the mandatory need for a 3rd party developed open source "faucet" cluster ‘oracle’ gateway application cluster in MEAN form, connected via IOTA IXI gateway, which is both scale-able and secure, providing "single source of truth" from each state routinely in near RT 'Real Time", feeding the MainStream and Independent/Alternative News Media with the DPL vote Tally updates per precinct/region over a Restful API which can be integrated in these media outlet systems, so the Vote Epoch results get reported correctly to the voter populus in a timely fashion, where the same information streams are available directly via an associated url link to the faucet in the VoterPak Dapp, accessed by anyone voting that way. Such a Faucet and all registered news outlets contained within, must be registered with the State/province wide vote Epoch Master SC with such records also stored in the associated DPL instance node operated data stores for backup and recovery purposes locally in the node.

**Secure Data Flows between Nodes : IOTA STREAMS, operating over BEEP**

BEEP must be SASL deployed for all Node to Node control and monitoring data planes dictating the setup, state change and monitoring of vote data flows between all nodes of the SOVRINTown voting system. BEEP protocol facilitates the CLI and UI WEB administrative setup and control of the SOVRINTown voting system for initial setup and verification of the underlying PCIe Backplane(new) and/or TCP/IP Network(legacy) operating within and connected between precincts/regions in state. The same BEEP communications scheme governing CLI and GUI Web administration must be used for setup and operation of the Federally supplied and operated inter/state/province SCION Border Router Clusters, using dynamically SASL loaded cryptographic protection of those Layer 5 port originated session data flows as specified by the Federal authority. The setup of the monitoring plane must behave per the SIEM specification, to make sure logs are C2 compliant, to ensure there is a full audit of both the control plane, the monitoring plane and the data flow planes, recorded and reported by the IOTA # Tangle to support transparent auditing of the logs.

**Reporting Accurate Voting Results to the World- Society2 ToolKit to Build Reporting Server running on IOTA Hornet & Bee Nodes.**

At this time in the project we are exploring the use of the upcoming Society2 toolkit to build secure Apps operating on IOTA nodes, which means creating an internal electoral management reporting server application which is node mounted to read immutable vote and node state data from the IOTA Tangle Distributed private Ledger State/Province instance of multiple nodes operating in various secure locations. Read only APIs can be presented through a registration function to selectively allow registered/certified Media outlets and auditors to access node information, where the outside 3rd parties are node SC issued private and public keys to access the data via the IOTA STREAMS protocol, for reporting of results in Near real time, a key feature of transparency also afforded registered vote observers. When the SC Vote Epoch precinct polls close per the overall SC State Wide vote Epoch rules, all results are 'officially in’, per the state /province extension deadlines (people still standing in line for example" approved by their respective legislatures.)

**The Elimination of Mail-In Voting- Support for Interned and Absentee Voters**

In SOVRINTown voting systems, the interned can get their one time use Ballot electronically together with the one time use wallet and the coins they need to place their vote choice on the ballot and send it themselves. In fact they can use any Apple or Android Smart Phone to do it, with a properly designed, “One Time Use” Voting Wallet DApp “VoterPak”, only downloadable against the registration list data from the Smart Contract Precinct Vote Epoch Instance. If the voter is not on the list, they run the DApp to register their ID, their Face, their thumb print, their voice print (or any combination there of depending on state/province law) to create their unique voter registration instance, which is checked against all nodes in the state AND, even cross state to other Tangle Instances of the DpL 'Distributed private Ledger", where the cross-state connections are operated by the FEDERAL government as a Network Node using the SCION Border Router URI to IP to IP to URI routing specific to the Precinct set of Nodes URI which has all voting node instance of Hornet appearing as one big Microservice Cluster with the same local address, even though the Nodes are in different colo/Dc sites connected via Dark Fibre.

For Example, If there are 100 voting precincts/regions in the State or Province, then are 100 URI IDs. No TCP/IP is used "in State" typically unless their are remote regions which warrant the use of TCP/IP (FlexE use is recommended “in state/province” to extend the Backplane over the WAN existing dark fibre DWDM spectrum, without the use of TCP/IP. Each Precinct could in fact, have several IOTA Hornet or BEE Nodes running in local, distributed secure Colos "co-location facility" and DC "Data Center" locations (like a large metro center), which simply show up with their own sub node URI "ID extension" (Suffix) to the main URI ID for the Precinct/Region.

In effect the SOVRINTown Precinct eVoting system “in State or Province” is one big Single Addressed Computer PCIe Backplane, connected to several PCIe Computing nodes running VMs "Virtual Machines" and Container instances sufficient to support the Precinct/Region Vote Epoch Services need to both record and report on the Voter Ballots submitted directly online, remotely or in person, or manually in person (which become unique single "NATURAL" Number instances. Yes the nodes have their own Storage.)

**Natural Numbers and Voting Systems: A word on that**

Voting systems are, by their very nature, recording natural numbers (no decimals or fractions of votes allowed). In hindsight, since existing ‘blackbox’ voting systems do not support Natural number only voting, they should have been disqualified in the first place in the US 2020 National election by every single US State government.

**Support for Paper Ballots- Safe and Secure Paper to Electronic Transposition**

The Secured Voting System Precinct/Region Node module of "SOVRINTown" support Paper Ballots. In the SOVRINTown voting system component, handling paper ballots does involve scanned signature matching, but also eyeball, voice and thumbprint check to determine next step, at the voting station, or via the Dapp to support ‘interned’ voters (the sick and elderly, requesting such Dapp Access in advance) .

If the voter is not on record, then a record is created using private booth access to the Dapp at the voting station on a Tablet (it can even be a Smartphone). We are focused on Android support only for SOVRINTown Voting System Module, because Android is Open Source whitebox code (apple is not.)

**How to Deploy Quickly and Securely, Precinct/Region versions of SOVRINTown Packaging and Provisioning**

Standards are important here, this means use of a YAML blueprint of each container instance in conjunction with Terraform configuration management deployed by Kubernetes or Docker instance provisioning systems or similar to the Target Host VM ‘Virtual Machine’ (KVM used as the default) URI (Remember no TCP/IP, except for the FED BR interconnect running SCION which runs a NAT translation URI to IP Address Map to support cross precinct and even state voter registration list checks using the IOTA Fast consensus protocol to ensure the uniqueness of the voter and the uniqueness of the time stamped ,one time use ballot/voter wallet and key sets with color coins included which are issued to the approved voter after that first in/cross/state check.., handled by BIG BEE IOTA Nodes with ample Fast Storage in multiple locations per state running the consensus to approve the voter registered, (thus eliminating the duplicate vote problem from the same person in different states. ).

**Who Writes the DApp, the Vote Epoch SC?- Base Template is the FED job, State modified for Precinct Use.**

In each case above of 3rd party security certification , multiple BONDED security parties attest to the security of the code, running full audits posted to a public blockchain for anyone to scrutinize, who is registered ‘in country’.

**Initial RoadMap Milestones- Late Q4 2021 PoC MVP**

Requirements Target ETA March 21st, 2021

Test Case Coverage MVP Complete with pass/fail metrics ETA June 5th, 2021

Detailed Use cases - Target 4th of July, 2021

Three Iteration primary, secondary and exception use cases Sept 5th, 2021

First Code PoC 0.8 Oct 31st, 2021

Documentation/ Acceptance Plan w/ 0.9 PoC MVP Target Dec 21st 2021

End of Story Document

R. Reive 21\_12\_2020\_rv\_0.6

\*\*\*\*\*