Contents

Modern Voting Context

50+ years of innovation in online security

<> Web 1: "@" for secure eMail,and modems for data communications
<> Web 2: "https" for secure web browsing, and Wi-Fi for wireless access
<> Web 3: "Blockchain," and Distributed Ledger Technology (DLT) to validate sources, secure communications, and confirm valid transactions

<> Web 3V: 2025+: Web 3 technology enables secure, sustainable, scalable modern voting ecosystems (aka MetaProject-3V).

MetaProject-3V

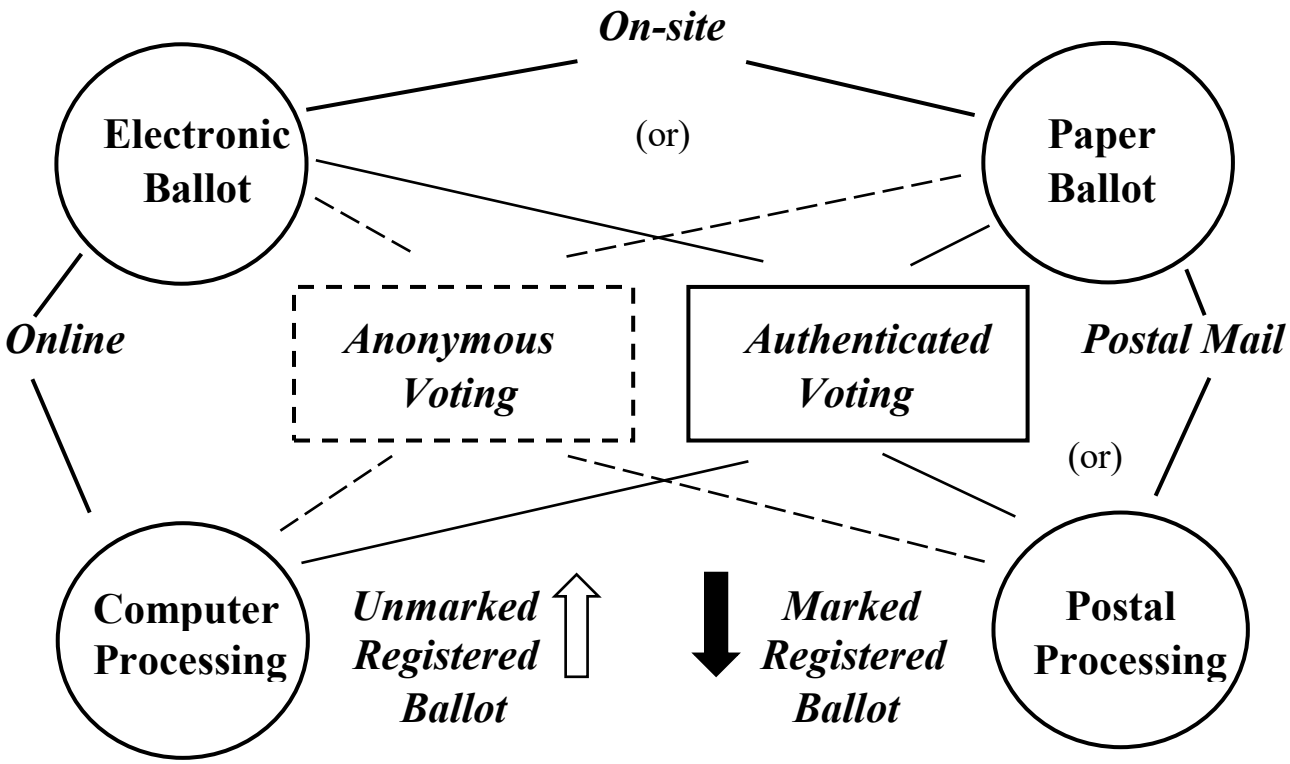
<> Registration of voting materials enables chain of custody
<> Chain of custody of ballots provides evidence of source, distribution, marking, collection, and recording for vote counts
<> That evidence enables more security with modern voting.

Modern voting offers more choices

<> Anonymous or authenticated
<> Paper ballot via traditional methods or electronic online voting
<> Traditional voting via postal mail or on-site at a polling location
<> Online voting from home, work, travel, military, or polling location
<> Available choices determined by voting and election officials.

2 MetaProject-3V Framework

Framework



Distributed Ledger Technology (DLT)

DLT Process:

1) Validates ballot source with cryptographic methods,

2) Secures communications with digital signatures,

3) Confirms valid transactions with a transparent ledger,

4) Records compliance, custody, vote counts, and DLT fees.

If Marked Registered Ballot is

a) Valid: It is recorded and counted, based on evidence the ballot was not duplicated and was marked by a registered voter that voted only one time, or if

b) Suspicious: It is recorded and investigated, and not counted unless cured or adjudicated as valid.

Ref. 1. IEEE 2418.11-2023(R) e-Voting Standard.

Ref. 2. USPTO MetaProject-3V(TM) Service Plan.

3 MetaProject-3V Framework

Registrations, Tokens, and Hash Codes

Registered materials are key to security and transparency

<> Registered materials include voter ID cards, ballots, and postal or email
> Material registered with a unique identity (UID) can be paper or electronic, and does not replace or link to local security practice (e.g., signature, voter ID, ...)

<> UID content is unique for each voting event, and includes:
> Time (year, month, day), Location (country or subdivision e.g., state, county), Type (material, equipment, facility, ...), and Index (with capacity of billions)

<> Material UIDs are part of production before use in registration, voting, or postal mail, and ***identify materials and not anonymous voters***

<> Equipment, facilities, and staff that handle materials are registered
> Equipment and facilities have names and pseudo-anonymous UIDs
> Staff (and election officials) have names and pseudo-anonymous UIDs
> Legal subpoena(s) can identify UID source(s) that handled suspicious materials.

Materials are tokens

<> Fungible Token (FT): More than one are (almost) the same
> Examples: Unmarked registered ballot (with UIDx but no voting data), and unmarked registered voter ID card (with UIDy but no voter data)
> *Unmarked ballot/card FT registered with a UID, is similar to a dollar bill FT registered by Treasury with a unique serial number*

<> Non-Fungible Token (NFT): Unique and one-of-a-kind
> Examples: Marked registered ballot (with UIDx and voting choices), and marked registered voter ID card (with UIDy and voter data)

Ballot tokens and hash codes for anonymous voting

<> Unmarked FT: Same data on more than one ballot with unique identities

<> Marked NFT: Voter marks choices on one ballot registered with UIDx and includes the UIDy from their registered voter ID card, to show
> *A valid ballot (with UIDx) was marked by a valid registered voter (with UIDy)*

<> Hash Code: Cryptographic character sequence representing a marked NFT
> Hash Examples: See National Institute of Standards and Technology

Anonymous or Authenticated Voting

Anonymous Voting

<> Typical anonymous voting would be with a registered paper ballot received via postal mail at a home address. Voter marks ballot with choices, enters registration from their voter ID card, signs return envelop, and returns marked registered ballot via postal mail.

<> Each registered ballot (with UIDx) is marked by a voter (with UIDy) from their registered voter ID card. Voter is anonymous, access to hash codes can only be online using UIDx, UIDy for hash storage address.

<> Anonymous voter can electronically validate the received and recorded hash of their UIDx ballot exists, are the same, and are not duplicated. Otherwise, suspicious ballot is not counted, investigated for errors/fraud.

<> Method for for curing or adjudication of suspicious activity uses 5 steps:
1) Process Compliance, 2) Registered Materials, 3) Chain of Custody of Materials;
4) Private List of unique IDs on suspicious ballots; 5) Subpoena(s) to identify source(s) of fraud.

Authenticated Voting

<> At registration, voter can choose to authenticate their ballot was received and recorded without change, deletion, or duplication.

<> Typical authenticated voting would be online via registered electronic UIDx ballot received at a wallet address. Voter marks ballot, enters UIDy from voter ID card, returns ballot to a pre-defined wallet address, and hash (A) of the ballot is saved by online app.

<> Authenticated voter gets hash receipts of received (B) and recorded ballot (C) that is compared with the hash of the original marked ballot (A). If hash B or C does not exist, or are not the same as (A), or are duplicated, that ballot is suspicious, investigated, and not counted.

<> Method for curing and adjudication that suspicious activity is errored or fraud uses 5 step process as noted for Anonymous Voting.

5 MetaProject-3V Framework

Digital Transformation

(aka How it Works)

Voting	Traditional	Modern
Registration	**Voters** 	**Voters + Materials**  
Performance	**Paper & Electronic Accessability, Qualified Voters, Anonymous Voting**	**Traditional Voting + Transparency and Verifiability**
Ballot Security *Ref. MetaProject-3V[TM] Framework*	***Limited Security*** **No Evidence of Source Ballots for Vote Counts, Allows Rigging**	***Multi-Level Security*** **Evidence of Valid and Suspicious Registrations and Voting**
Quantum/AI Security *Ref. IEEE Std 2418.11® Annex J*	**No Core Validation, Allows Hacking**	**Validated Sources, Communications, and Transactions; and No Duplicate Ballots or Voting**

Roadmap

(aka Time is of the Essence)

1. 2026-20xx:

Education and training with stakeholder and government participation.

2. 2026:

DLT alternatives for compliance certifications, custody of materials, vote counts, and DLT fees

> Criteria: Web-3V eBook (p.57, pdf p.75), e-Voting Standard (p.49)

Ref. https://jmwnuk.wixsite.com/timeless/web-3v-ebook

> Candidates:

Bitcoin, Bitlattice, Cardano, Dragonchain, Ethereum, Hedera, Lightning, Others?

3. 2026:

Proofs-of-Concept that more security and transparency comes with registered voters, materials, equipment, facilities, …, plus process compliance and chain of custody of materials.

4. 2026-2027

Genesis: Compliance and Registration Authorities are via stakeholders such as an e-Voting Alliance.

5. 2027-2028:

Operational Readiness: Paper and electronic methods, unique identities (UIDs) for materials (first) and then equipment, facilities, staff, . . .; anonymous and authenticated voting, real-time audits, public and private summary databases, registration authority, compliance certified processes.

6. 2029-20yy:

Results: registered voters, materials, equipment, facilities; chain of custody of materials;
voting via postal mail, on-site at polling location, or online at home or other location;
valid registered ballots marked by valid registered voters, or marked ballots that are suspicious;
real-time audits of valid and suspicious registration and voting activity;
summary databases of valid (public) results; and suspicious, cured, and adjudicated (private) results.

7. 2030-20zz:

Enhancements: AI, IOT, Post-Quantum, . . ., as appropriate with qualified sources and methods.