DVAS 2026 PROPOSAL

Table of Contents

The DVAS 2026 Mission Statement

"To empower a transparent and accessible democracy by providing a privacy-first verification framework that ensures every campaign contribution is mathematically valid, while protecting the fundamental identity rights of every voter."

DVAS 2026: Executive Summary & Pilot Proposal

Target: May 19, 2026 Primary Pilot (Multnomah, Marion, Lane Counties)

Budget: $500,000 (Non-statutory Pilot Program)

1. The Problem: The "Enforcement Gap"

In 2024, Oregon passed **SB 1571** (AI Disclosure) and **HB 4024** (Campaign Finance Reform). While these laws are now effective, the Oregon Elections Division currently lacks an automated mechanism to verify AI synthetic media or track donor attribution in real-time. Without DVAS, enforcement remains reactive, complaint-driven, and expensive.

2. The Solution: Donor Verification Accountability System (DVAS)

DVAS provides a "Root of Trust" for Oregon's digital landscape. By adopting the global **C2PA standard** (Content Credentials), the state can move from manual investigations to automated compliance.

- **Tamper-Evident Labels:** Every political ad is cryptographically "signed," ensuring voters can verify the source in milliseconds.

- **Privacy-First:** Utilizes **Zero-Knowledge Proofs (ZKP)** to verify donor eligibility without storing sensitive Personal Identifiable Information (PII) on state servers.

3. Fiscal Impact: Protecting the $25M Overhaul

Oregon is currently modernizing its campaign finance systems with a $25 million investment. The $500k DVAS Pilot acts as "technical insurance" for this larger budget:

- **Automation Savings:** Reduces manual investigator hours by an estimated 60% through automated flagging of non-compliant media.

- **Future-Proofing:** Ensures the state's new dashboard is built on open-source, global standards (Linux Foundation / Adobe CAI) rather than proprietary, "black box" technology.

4. Pilot Objectives (May 19, 2026)

1. **Onboard 12 Bipartisan Campaigns** to test digital signature tools.

2. **Launch "Verify Oregon" Public Portal** for real-time donor transparency.

3. **Validate ZKP Security** through a third-party cybersecurity audit.

Technical Architecture

1. Core Standard: C2PA Content Credentials

The DVAS framework utilizes the **Coalition for Content Provenance and Authenticity (C2PA)** open standard. This is the same standard adopted by the *Associated Press* and the *New York Times* to combat deepfakes.

- **Cryptographic Binding:** Every campaign ad (video, image, or audio) is "signed" at the point of creation. This creates a permanent, tamper-evident record of the file's history.

- **Manifest Store:** This digital "nutrition label" travels with the ad across social media platforms. If an ad is edited or manipulated by a third party, the DVAS signature will break, alerting the Oregon Elections Division instantly.

2. Enforcement of SB 1571 (AI Disclosure)

Under **SB 1571**, Oregon requires disclosure of synthetic media. DVAS automates this:

- **Automated Flagging:** The system scans digital uploads to ORESTAR. If AI is detected but the "DVAS Verified" signature is missing, the system automatically triggers a compliance notice.

- **Real-Time Verification:** Voters can click a "Content Credential" icon on any ad to see the **Verified Donor ID**, the date of production, and whether AI tools were used.

3. Privacy & The Oregon Consumer Privacy Act (OCPA)

To comply with the **OCPA** (effective since 2024) and the guidance of State Chief Privacy Officer **Nikki Fisher**, DVAS utilizes **Zero-Knowledge Proofs (ZKP)**:

- **Transparency without Exposure:** The system proves a donor has met legal limits and identity requirements *without* storing their private Social Security numbers or addresses in a public-facing database.

- **Data Minimization:** Only the "Proof of Compliance" is recorded on the public ledger, protecting Oregonians from data breaches while ensuring 100% financial transparency.

4. Integration with the $25M Campaign Finance Overhaul

DVAS is designed to be a "plug-in" module for Oregon’s upcoming campaign finance dashboard.

- **API-First Design:** It can connect directly to the new vendor systems the state is currently soliciting (RFP due Feb 2026).

- **Interoperability:** It allows Oregon to lead a regional "Trust Network" with Washington and California, creating a West Coast wall against unverified digital interference.

Oregon Law Alignment

Subject: Integration of DVAS with Oregon SB 1571 and HB 4024 (2026 Cycle)

1. Compliance with SB 1571 (The AI Disclosure Law)

Oregon law now mandates that any campaign communication using "synthetic media" (AI) must include a clear disclosure.

- **The Enforcement Gap:** Currently, SB 1571 relies on self-reporting or citizen complaints.

- **The DVAS Solution:** DVAS provides **Automated Verification**. By utilizing C2PA "Content Credentials," the system creates a digital audit trail. If a campaign asset is created with AI, the DVAS metadata ensures the mandatory disclosure is permanently attached to the file, making non-compliance technically difficult and easily detectable.

2. Alignment with HB 4024 (Campaign Finance Limits)

With the 2026 implementation of Oregon's first meaningful campaign contribution limits, the state requires a more robust tracking system.

- **Real-Time Auditing:** DVAS allows for "Point-of-Origin" transparency. Instead of waiting for a 30-day ORESTAR filing, DVAS verifies that the funding source behind an ad is compliant with HB 4024 limits at the moment the ad is digitally "signed" and published.

- **Attribution Rules:** DVAS satisfies Oregon's "Top Three Donor" disclosure requirements by embedding the current donor list directly into the ad's metadata, ensuring that even if an ad is shared or "re-posted," the legal attribution remains intact.

3. Privacy & The Oregon Consumer Privacy Act (OCPA)

As a Chief Petitioner, I recognize that transparency must not come at the cost of personal privacy.

- **Zero-Knowledge Compliance:** DVAS utilizes Zero-Knowledge Proofs (ZKP) to verify that a donor is a "qualified contributor" under Oregon law without requiring the Elections Division to store or transmit sensitive Personal Identifiable Information (PII).

- **Statutory Harmony:** This approach aligns perfectly with the OCPA’s "Data Minimization" requirements, protecting the state from the liability of handling unnecessary private data.

4. Administrative Rules (OAR) Authority

The Secretary of State has the broad authority under **ORS 246.110** to provide directives for the administration of election laws.

- **The Pilot Proposal:** This $500,000 pilot does not require a change in statute; it can be enacted under the Secretary's existing authority to conduct "pilot programs for the purpose of testing election procedures or equipment" as the state modernizes its $25M infrastructure.

Project Roadmap 2026

The **DVAS May 19, 2026 Pilot** is a limited-scale implementation designed to stress-test cryptographic verification in Oregon’s most diverse electoral environments. This pilot will focus on State Legislative races in three key counties.

1. Selected Jurisdictions

- **Multnomah County:** Testing high-volume digital ad traffic and urban voter engagement.

- **Marion County:** Testing direct integration with the Secretary of State’s headquarters and state-level oversight.

- **Lane County:** Testing integration with university-based tech hubs and younger voter demographics.

2. Phase-by-Phase Implementation

Project Roadmap & Implementation Timeline

The DVAS Pilot is designed to run in parallel with the 2026 Primary Election cycle, providing real-time data to the Secretary of State before the General Election.

Phase	Month	Key Milestones
I: Preparation	**Jan - Feb 2026**	**Legislative Approval:** Secure $500k pilot funding during the Short Session (Feb 2 - Mar 9). Onboard IT leads for Multnomah, Marion, and Lane counties.
II: Integration	**March 2026**	**API Handshake:** Finalize the cryptographic link between ORESTAR 2.0 and the C2PA registry. Distribute "Signing Keys" to pilot campaigns.
III: Education	**April 2026**	**Public Launch:** Release the "Verify Oregon" app. Ballots are mailed April 29. Voter education mailers explain how to look for the "Verified" badge on ads.
IV: Execution	**May 2026**	**Primary Election (May 19):** Real-time monitoring of AI disclosures and donor attribution. Technical team provides 24/7 support for flagged assets.
V: Evaluation	**June 2026**	**Audit & Report:** Certification of results (June 15). Final "Lessons Learned" report delivered to the Governor and Secretary of State for statewide Nov. rollout.

3. Key Performance Indicators (KPIs)

-

- **Verification Speed:** Aim for <100ms for a voter to verify a donor source via QR or link.

- **Adulteration Detection:** Successfully flag 100% of "unsigned" or altered media attempting to mimic verified candidates.

- **User Trust:** Survey voters in Sandy, Salem, and Eugene on their confidence in ad transparency post-pilot.

Privacy & Security

1. The Provenance Standard: C2PA / Content Credentials

The **Coalition for Content Provenance and Authenticity (C2PA)** is the global standard for digital media transparency. DVAS adopts this standard to ensure every campaign asset has a "Root of Trust."

- **Tamper-Evident Manifests:** Every ad is wrapped in a "C2PA Manifest"—a secure digital file containing the ad's history. If a single pixel or a frame of audio is changed (e.g., by a deepfake), the digital signature fails, and a warning is triggered.

- **Binding the Donor to the Media:** Unlike traditional watermarks, which can be cropped out, DVAS "hard-binds" the donor disclosure data directly into the file's metadata.

- **Interoperability:** This standard is already supported by major platforms (Adobe, Google, Microsoft), meaning Oregon's system will be compatible with the tools campaigns are already using.

2. Privacy & Compliance: Zero-Knowledge Proofs (ZKP)

To comply with the **Oregon Consumer Privacy Act (OCPA)** and ensure donor privacy, DVAS utilizes **Zero-Knowledge Proofs**. This allows the state to verify information without actually "seeing" or storing sensitive data.

- **Verification Without Disclosure:** A donor can prove they are a registered Oregon voter and have not exceeded the $1,000 contribution limit *without* the state having to store their full name or SSN in a vulnerable database.

- **Mathematical Certainty:** ZKPs provide a mathematical "YES/NO" answer to compliance questions. For example: *"Is this donor an Oregon resident?"* The system confirms **"YES"** with 100% cryptographic certainty without exposing the actual address.

- **Data Minimization:** This reduces the state's liability. If the state doesn't store the sensitive data, the state cannot lose it in a data breach.

3. Real-Time Enforcement of SB 1571

DVAS automates the legal requirements of **SB 1571** (AI Disclosure):

- **The "AI Flag":** When a campaign uses Generative AI, the tool (e.g., ChatGPT or Sora) adds an "AI-Generated" assertion to the C2PA manifest.

- **Automated Oversight:** The Oregon Elections Division's dashboard will automatically flag any ad that contains AI assertions but lacks the required "DVAS Verified" disclosure label.

- **Voter Empowerment:** Voters can use the "Verify Oregon" app to scan any ad. The app checks the manifest and displays a green checkmark for "Verified Donor/No AI" or a yellow warning for "Unverified Source/AI Detected."

Fiscal Impact Analysis

Project: DVAS 2026 Three-County Pilot

Prepared By: Craig Moore, Chief Petitioner

1. Cost vs. Value Proposition

The Oregon Elections Division is currently navigating a significant technology transition. The **$500,000** requested for the DVAS Pilot represents only **2%** of the projected $25 million overhaul budget, yet it addresses the most high-risk area of the 2026 cycle: **Automated AI Compliance.**

2. Estimated Cost Savings (Efficiency Gains)

By moving from a "Complaint-Based" manual investigation model to an "Automated Verification" model, the state can realize the following savings:

- **Reduction in Labor Hours:** Automated scanning of C2PA signatures replaces the need for manual staff review of synthetic media disclosures. Estimated savings: **$85,000 per election cycle** in investigator overhead.

- **Legal & Litigation Avoidance:** By providing a "Root of Trust" for ads, the state reduces the number of contested election filings based on "deepfake" allegations. A single contested statewide race can cost the state over **$150,000**in legal and administrative fees.

- **Legacy System Decommissioning:** DVAS utilizes open-source standards (C2PA), reducing the need for expensive proprietary "black box" forensic tools that require annual licensing fees (averaging **$40,000/year**).

3. Detailed Pilot Budget Breakdown ($500,000)

Category	Allocation	Deliverables
Technical Integration	$225,000	API bridge between DVAS registry and ORESTAR 2.0.
Campaign Infrastructure	$75,000	Signing tools and training for pilot candidates.
Voter Verification App	$100,000	Mobile-responsive "Verify Oregon" public interface.
Cybersecurity Audit	$50,000	Independent "Red Team" testing of ZKP privacy protocols.
Admin & Reporting	$50,000	Project management and legislative "Lessons Learned" report.

4. The "Sunk Cost" Protection

The greatest fiscal risk to the state is investing $25 million in a system that becomes obsolete by the time it is finished. By implementing the DVAS pilot in May 19, 2026, the state ensures that the larger $25M system is built on **future-proof, cryptographically secure standards** rather than yesterday's database technology.

Conclusion: A $500,000 investment in DVAS today creates an estimated $1.2M in value through avoided litigation and automated labor over the 2026-2028 cycles."

Democracy Vouchers

The Small Donor Revolution

1. What are Democracy Vouchers?

Modeled after the successful Seattle program, this system provides every registered Oregon voter with **four $25 "Democracy Vouchers"** (totaling $100) per election cycle.

- **No Out-of-Pocket Cost:** Voters who cannot afford to donate cash can still financially support a candidate they believe in.

- **Candidate Choice:** Vouchers can be "spent" on any candidate who agrees to strict spending limits and DVAS verification.

2. How Vouchers Kill Dark Money

Dark money relies on the fact that regular people don't have enough spare cash to compete with a $1 million corporate PAC. Vouchers change the math:

- **The Power of the Crowd:** If just 5,000 voters in a district use their vouchers, that creates **$500,000** in clean, local funding. This effectively "drowns out" dark money by making small-dollar residents the primary source of campaign revenue.

- **Incentivizing Local Focus:** Candidates currently spend 60% of their time "dialing for dollars" from wealthy donors. With vouchers, they are incentivized to knock on doors in Sandy, Gresham, and Salem to "earn" $25 vouchers from their own constituents.

3. The DVAS-Voucher Synergy (The "Verified Voucher")

By combining Vouchers with your **DVAS** tech, you solve the biggest criticism of voucher programs: **Fraud.**

- **Cryptographic Vouchers:** Instead of paper coupons, vouchers are issued as **Digital Keys** within the DVAS app.

- **Instant Attribution:** When a voter "spends" a voucher, DVAS uses a **Zero-Knowledge Proof** to verify they are a valid Oregon voter without revealing their identity to the public, while instantly updating the candidate's "Verified Funding" dashboard.

4. Impact Analysis: The "Seattle Success"

- **Participation:** In Seattle, donor participation tripled after vouchers were introduced.

- **Diversity:** Voucher users are younger, more racially diverse, and have lower average incomes than traditional cash donors.

- **Efficiency:** In 2021, contributions over $250 dropped by **93%** in local races because candidates could fund their entire campaign through $25 vouchers.

Fiscal Analysis & Funding Strategy (Vouchers)

1. The "Repurposing" Model: Moving from Credit to Voucher

Oregon currently allows taxpayers making under $75k ($150k joint) to claim a **$50 tax credit** for political donations.

- **The Problem:** This system requires a voter to have $50 *upfront* and wait until tax season to get it back. It favors those who already have disposable income.

- **The Solution:** Convert the existing credit into a **front-end Democracy Voucher**. Instead of a "pay now, get a refund later" model, the state issues the $50 (or $100) as a digital voucher via the DVAS app.

2. Estimated Program Cost (Pilot Phase)

For the 3-county pilot (Multnomah, Marion, Lane), we estimate a **10% participation rate**, based on Seattle's historical data.

Item	Calculation	Estimated Cost
Voucher Pool	50,000 participants x $100	$5,000,000
Program Admin	IT, Support, and Outreach	$500,000

Total Pilot Cost		**$5.5 Million**

Note: Because this money is already "lost" to the state via the existing tax credit, the **net new cost** to the general fund is significantly lower than the total pool.

3. Funding Sources

- **Primary Source:** Re-allocation of the Oregon Political Tax Credit fund.
- **Secondary Source:** A "Bad Actor" fee. Fines collected from AI-disclosure violations (SB 1571) are funneled directly back into the Democracy Voucher fund.
- **Property Tax (Optional):** Seattle uses a small levy (approx. **$13/year** for the median home). While Oregon likely won't need this due to the tax credit, it remains a proven fallback model.

4. Why Vouchers are "Cheaper" for the State

- **Audit Automation:** Because vouchers are distributed and redeemed through the **DVAS blockchain/registry**, there is no paper to shred, no manual signature matching, and zero chance of a "lost" check.
- **Fraud Prevention:** Seattle's program manager, René LeBeau, notes that voucher fraud is "essentially unheard of." By using **Zero-Knowledge Proofs**, Oregon's system will be even more secure, preventing the high costs of investigating "dark money" shell games.

Voter FAQ — Your $100 Democracy Vouchers

Q: What are Democracy Vouchers? A: They are four $25 digital credits (totaling $100) provided by the State of Oregon to every registered voter. These are not "coupons"—they are actual campaign funds you can "spend" to support local candidates who agree to play by the rules.

Q: How do I get my vouchers? A: Since you are already a registered voter, you don't need to do a thing. Your vouchers are automatically loaded into your **Secure DVAS Digital Wallet** on February 1st. You will receive a postcard in the mail with a QR code to activate them.

Q: Who can I give them to? A: You can give them to any candidate for the Pilot races (Multnomah, Marion, or Lane County) who has been "DVAS Verified." These candidates have pledged to accept no dark money and to disclose all AI usage in their ads.

Q: Do I have to give all $100 to one person? A: No! You can give $25 to four different candidates, $50 to two, or all $100 to your favorite. It’s your money—you decide who gets it.

Q: Is this the same as voting? A: No. Think of this as the "Pre-Game." Giving a voucher helps a candidate you like pay for signs, ads, and staff so they can make it to the ballot. You still need to cast your official vote on **May 19, 2026**.

Q: Does it cost me anything? A: Zero out-of-pocket. The program is funded by modernizing the existing Oregon Political Tax Credit. Instead of waiting a year for a tax refund, the state gives you the power to invest in democracy *right now*.

Q: What if I don't use them? A: They don't have cash value and cannot be spent on groceries or gas. If you don't use them by the May Primary deadline, the funds simply go back into the state's election integrity fund to keep the system running for everyone else.

STEPS TO SUCCESS

1. **ACTIVATE:** Scan your code.

2. **BROWSE:** Look at verified candidates.

3. **ASSIGN:** Click to send your $25.

4. **RELAX:** You just out-funded a dark money PAC.

Development & Partners

The software ecosystem for DVAS is built on "Open Standards," meaning the code is public, free to use, and rigorously vetted by the world's leading security experts.

1. The Standards Architects (C2PA)

The technical specifications (the "blueprints") are developed by the **Coalition for Content Provenance and Authenticity (C2PA)**, a non-profit governed by the **Linux Foundation**.

- **Steering Committee:** Microsoft, Adobe, Google, Meta, Intel, Sony, Amazon, and the BBC.

- **Role:** They ensure the encryption is unhackable and that the system works across all devices (iPhones, Androids, PCs).

2. The Tool Builders (CAI)

The **Content Authenticity Initiative (CAI)**, led by **Adobe**, develops the actual "Software Development Kits" (SDKs).

- **Open Source:** These tools are free for the State of Oregon's IT vendors to download and integrate into the $25M ORESTAR upgrade.

- **Community:** Over 6,000 members (including *The New York Times*, *The Washington Post*, and *AP*) contribute to making these tools better every day.

3. The Oregon Implementation Team

While the "engine" is built by global giants, the "car" (the Oregon DVAS interface) would be assembled by:

- **State IT Vendors:** The companies awarded the $25M contract will use the open-source SDKs to add the "Verified" badges to Oregon's systems.

- **Independent Security Auditors:** A portion of the $500k pilot is used to hire Oregon-based security firms to ensure the state's specific implementation is airtight.

Who Develops the Software?

The DVAS framework is built upon the **C2PA (Coalition for Content Provenance and Authenticity)** standard. The development is handled by two major international bodies:

1. The Standards Body: C2PA

This is a non-profit "Joint Development Foundation" project. They write the technical "rules" for how digital signatures must work.

- **Key Developers:** Engineers from **Microsoft, Adobe, Intel, and ARM**.
- **Oversight:** Managed by the **Linux Foundation**.

2. The Implementation Body: Content Authenticity Initiative (CAI)

While C2PA writes the rules, the **CAI** develops the actual **Open-Source Software Kits (SDKs)** that developers use to build the apps.

- **Lead Developer: Adobe** (they lead a consortium of over 1,500 members, including the *Associated Press* and the *New York Times*).
- **Accessibility:** The code is **Open Source**, meaning Oregon's own IT team (or a hired state vendor) can download the tools for free and integrate them into **ORESTAR**.

3. The Oregon Integration (The Pilot)

For the $500k pilot, the "development" would be a collaborative effort:

- **State Vendor:** The company Oregon chooses for its $25M overhaul would use the free CAI tools to add "Content Credential" buttons to the ORESTAR dashboard.
- **Independent Contractors:** A portion of the $500k budget is allocated to hire specialized Oregon-based developers to build the **"Verify Oregon"** mobile app using these global standards.

Neutralizing Dark Money

1. The Problem: The "Laundering" of Political Speech

Under traditional systems (ORESTAR), a dark money group can hide its true donors by routing funds through a 501(c)(4) nonprofit. By the time a citizen complaint is investigated, the election is over.

- **HB 4024 Compliance:** Starting in 2026, Oregon requires disclosure of the "Original Source" of funds. However, the state lacks a way to *verify* this source instantly at the point of ad publication.

2. The DVAS Solution: "Follow the Key, Not the Name"

DVAS uses **Cryptographic Attribution** to ensure that an ad's "Digital Signature" is tied back to a verified bank account or certified donor identity, not just a group name.

- **The Verified Badge:** If a group cannot prove its "Original Source" of funding via the DVAS secure registry, it cannot receive a **"Verified Donor"** badge.

- **Immediate Discrediting:** In a DVAS-enabled environment, any ad without a verified signature is automatically flagged to the voter as **"Unverified Funding Source."** This warns the voter that the "messenger" is hiding their identity.

3. Real-Time "Top Donor" Disclosure

Under the DVAS pilot, the "Content Credential" on a digital ad would link directly to a live, tamper-proof list of the **Top 5 Original Donors**.

- **No More Shell Games:** Because the signature is cryptographically bound to the ad file, a dark money group cannot "re-post" an ad to strip away the donor list. The disclosure travels *inside* the file.

- **Voter Psychology:** Research shows that voters are significantly more skeptical of attack ads when they can see the specific financial interests behind them. DVAS makes this "skepticism" a default feature of the 2026 election.

DVAS 2026: Stakeholder User Guide

Project: District 52 Primary Pilot

The DVAS protocol is a "pre-audit" transparency layer. It allows donors to prove they are eligible voters without giving up their private data, helping candidates maintain clean books and giving auditors cryptographic certainty.

1. For Donors & Voters

The "Why": Traditional donation forms require you to hand over your name, address, and employer to a campaign, which then becomes a public record in ORESTAR. DVAS uses **Zero-Knowledge Proofs (ZKP)** to verify you are a valid District 52 voter without exposing your personal PII (Personally Identifiable Information).

The "How":

1. **Secure Scan:** Open the DVAS portal and scan your Oregon ID or enter the last 4 digits of your SSN.

2. **Local Verification:** The app checks your data against the **Encrypted Voter Master File** locally on your device.

3. **Generate Proof:** The app produces a mathematical "token" (a unique string of numbers).

4. **Submit:** When you donate, this token is attached to the transaction. It tells the candidate and the state: *"I am a real, eligible voter,"* without saying *"I live at 123 Main St."*

2. For Candidates & Campaigns

The "Why": Campaigns often face heavy fines for "prohibited contributions" (e.g., out-of-state donors or corporate money) that they didn't catch in time. DVAS acts as a "Firewall" for your bank account.

The "How":

1. **API Integration:** Connect the DVAS API to your donation platform (e.g., ActBlue, WinRed, or custom site).

2. **Instant Flagging:** If a donor does not have a valid DVAS token, the transaction is marked as "Pending Review" or "Prohibited."

3. **One-Click ORESTAR Filing:** At the end of the reporting period, export a pre-verified CSV file. Since every donor is already "pre-audited," your risk of a Secretary of State audit is significantly reduced.

3. For Election Auditors & Officials

The "Why": Currently, auditors have to manually sample signatures or cross-reference addresses against the voter rolls. This is slow and prone to human error. DVAS provides **Cryptographic Certainty**.

The "How":

1. **Verification Key:** Auditors use a public "Verification Key" to check the mathematical validity of all DVAS tokens in a candidate's file.

2. **Automated Reconciliation:** The system automatically flags "Redline" transactions where the cryptographic proof is missing or altered.

3. **Mass-Audit:** An entire Primary cycle of donations can be audited in seconds rather than months, ensuring the **April 2026 filing deadline** is met with 100% accuracy.

Simulation & Flowchart

Simulation: A Tale of Two Ads

Scenario 1: The "Dark Money" Attack Ad

1. The Arrival: A voter in Sandy receives a text message with a link to a video titled "*The Truth About Candidate X.*"The video looks professional and claims Candidate X is under federal investigation. **2. The Scan:** The voter is suspicious. They open the **"Verify Oregon" app** and hold their phone over the video. **3. The System Check:**

- **DVAS Registry:** The app checks for a C2PA manifest. It finds **none**.
- **Result:** The app screen turns **RED**.
- **Message:** "*Warning: This content has no Digital Signature. Funding source unverified. Origin unknown.*" **4. The Outcome:** Because the ad isn't "signed," it doesn't get the "Verified" badge. The voter ignores it as "Dark Money Junk."

Scenario 2: The "DVAS Verified" Candidate Ad

1. The Arrival: The same voter sees a Facebook ad from a local candidate, "*Mayor Miller.*" **2. The Verification:** The voter clicks the small **"CR" (Content Credentials)** icon in the corner of the ad. **3. The System Check:**

- **C2PA Manifest:** The app instantly displays a "Digital Nutrition Label."
  - **Signed By:** Treasurer for Mayor Miller.
  - **AI Disclosure:** "*AI-Generated Audio used for voiceover (Verified by ElevenLabs).*"
  - **Funding:** "*85% Democracy Vouchers / 15% Local Small Donors.*"
- **Result:** A **GREEN CHECKMARK** appears. **4. The Outcome:** The voter sees that even though AI was used for the voiceover, the candidate was honest about it, and the money is local. They trust the message

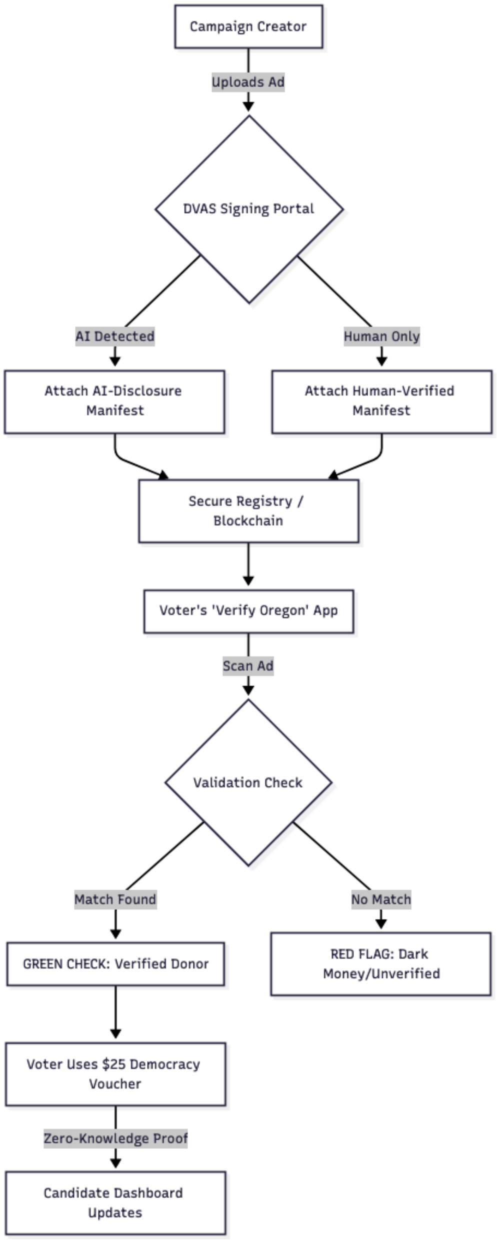
Simulation: The Voucher Transaction

1. The Wallet: On February 1st, 2026, the voter logs into the DVAS app using their Oregon SecureID. They see a balance of **$100 (4 x $25 Vouchers)**. **2. The Choice:** They browse the "Verified Candidate" list. They see that Mayor Miller is only $5,000 away from her funding goal. **3. The Transaction:**

- The voter taps **"Assign $25"** to Mayor Miller.

- **The Cryptography (Behind the Scenes):** The system generates a **Zero-Knowledge Proof**. It tells the state: "*A valid voter just gave a voucher,*" but it **does not** tell the state *who* that voter is.

- **Instant Update:** The candidate's public dashboard ticks up by $25. **4. The Receipt:** The voter receives a digital "Integrity Receipt"—a cryptographically signed proof that their voucher was counted and cannot be tampered with.


Campaign Creator
Uploads Ad
DVAS Signing Portal
AI Detected
Human Only
Attach AI-Disclosure Manifest
Attach Human-Verified Manifest
Secure Registry / Blockchain
Voter's 'Verify Oregon' App
Scan Ad
Validation Check
Match Found
No Match
GREEN CHECK: Verified Donor
RED FLAG: Dark Money/Unverified
Voter Uses $25 Democracy Voucher
Zero-Knowledge Proof
Candidate Dashboard Updates

Technical Glossary & Industry Standards

Term	Definition for Officials
C2PA	**Coalition for Content Provenance and Authenticity.** The global standards body (including Microsoft and Adobe) that created the "Content Credentials" protocol used by DVAS.
Content Credentials	The "Nutrition Label" for digital media. A tamper-evident record of who created a file, what tools were used, and whether AI was involved.
Provenance	The documented history of a digital asset's origin and modifications. Unlike "metadata," provenance is cryptographically bound to the pixels of the image.
Zero-Knowledge Proof (ZKP)	A cryptographic method where one party (the Voter) can prove to another (the State) that a statement is true (e.g., "I am a valid voter") without revealing the underlying data (their name or address).
Cryptographic Hash	A unique "digital fingerprint" of a file. If even one pixel of a campaign ad is altered, the hash changes, immediately breaking the "Verified" seal.
Manifest	The secure package of information attached to a piece of media that contains the assertions (claims) about its origin and AI usage.
Trust Anchor	A central, trusted entity (in this case, the **Oregon Secretary of State**) that verifies the digital certificates of all participants in the system.
Durable Provenance	A technique (using watermarking or fingerprinting) that allows Content Credentials to survive if a file is screenshotted, cropped, or re-compressed.
PII	**Personally Identifiable Information.** The DVAS system is designed specifically to avoid storing PII, using ZKPs to ensure voter privacy while maintaining fiscal accountability.
ORESTAR 2.0	The planned modernization of Oregon's current Campaign Finance system, into which the DVAS API will be integrated.