CDVS Technical Architecture Document

Canadian Digital Voting System - Complete Technical Blueprint

---

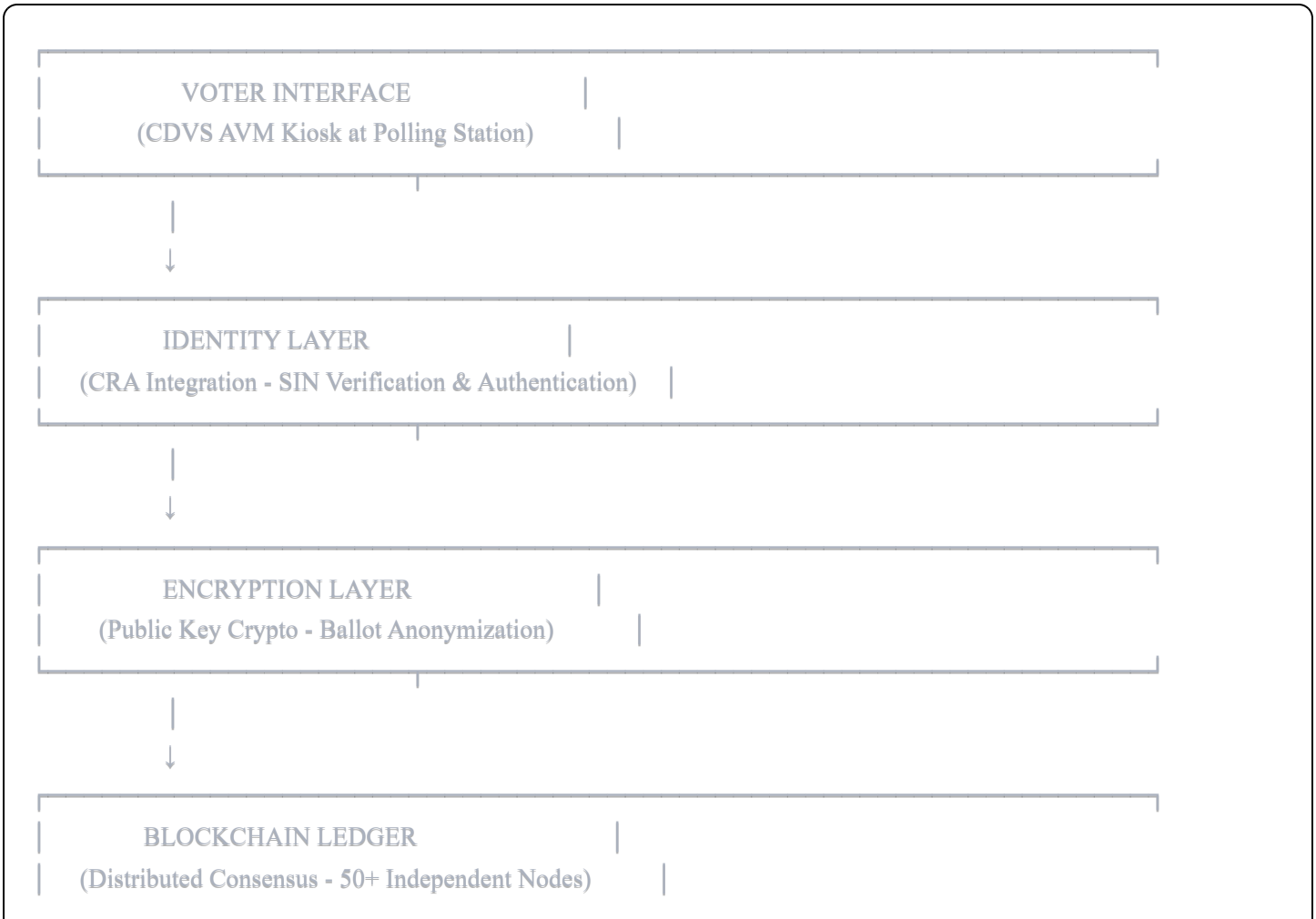
Executive Summary

The Canadian Digital Voting System (CDVS) is a blockchain-based voting infrastructure that replaces paper ballots with cryptographically secure, publicly verifiable digital votes. The system uses physical kiosks (CDVS AVMs - Automated Voting Machines) deployed at traditional polling locations, eliminating home coercion while providing real-time transparency and mathematical proof of vote integrity.

Core Innovation: CDVS separates voter identity from vote content using public-key cryptography while maintaining a publicly auditable blockchain ledger. This provides both ballot secrecy and complete transparency - solving the fundamental tension in electoral systems.

System Architecture Overview

High-Level Components



---

1. CDVS AVM (Automated Voting Machine)

Hardware Specifications

Physical Design:

- **Form Factor:** Enclosed kiosk similar to bank ATM
- **Screen:** 24" touchscreen display (1920x1080 minimum)
- **Height:** ADA-compliant with wheelchair accessibility
- **Privacy:** Built-in privacy screens on three sides
- **Security:** Tamper-evident seals, locked chassis, surveillance camera deterrent

Internal Components:

- **Processor:** Industrial-grade embedded system (ARM or x86)
- **Storage:** Encrypted SSD with local vote cache (syncs to blockchain)
- **Network:** Dual connectivity (wired Ethernet primary, LTE backup)
- **Authentication:** Integrated biometric option (optional: fingerprint for accessibility)
- **Printer:** Optional receipt printer for ballot ID confirmation
- **Audio:** Headphone jack for audio-assisted voting (accessibility)
- **Power:** UPS backup (4 hours minimum) for power outages

Security Features:

- Hardware security module (HSM) for cryptographic operations
- Tamper-detection sensors (alerts if chassis opened)
- Air-gapped boot process (cannot be remotely compromised during voting)
- Write-once audit log (immutable record of all interactions)

Software Stack

Operating System:

- Hardened Linux distribution (Debian or Ubuntu LTS)
- Minimal attack surface (only essential services running)
- Automatic security updates from trusted repositories
- Full-disk encryption (LUKS)

User Interface:

- React-based touch interface (simplified, large targets)
- Multi-language support (English, French, Indigenous languages)
- Accessibility modes: High contrast, large text, audio narration
- Average vote time: 60-90 seconds (faster than paper)

Kiosk Application Flow:

```
1. Welcome Screen
   ├─ "Enter your SIN to begin"
   └─ Language selection

2. Identity Verification
   ├─ API call to CRA verification service
   ├─ Check voter eligibility database
   └─ Load riding-specific ballot

3. Ballot Display
   ├─ Show candidates for voter's riding
   ├─ Party affiliations and photos
   └─ "Learn More" info button (optional)

4. Vote Confirmation
   ├─ "You are voting for: [Candidate Name]"
   ├─ "Go Back" or "Confirm Vote" buttons
   └─ Warning: Cannot change after confirmation

5. Cryptographic Processing
   ├─ Generate unique ballot ID
   ├─ Encrypt vote content
   ├─ Sign with kiosk's private key
   └─ Submit to blockchain

6. Voter Confirmation Screen
   ├─ Display ballot ID (e.g., CDN-X7K9PL2M)
   ├─ Show vote was recorded
   ├─ Timestamp
   ├─ Optional: Print receipt
   └─ "Thank you for voting"

7. Reset
   └─ Return to welcome screen (60 second timeout)
```

---

2. Identity Verification Layer

CRA (Canada Revenue Agency) Integration

Why CRA:

- Canadians already trust CRA with sensitive data (taxes)

- Existing infrastructure for SIN verification
- Real-time API access to verify identity
- Detects deceased individuals, non-citizens, duplicate voting

Verification Process:

```
User enters SIN at kiosk
  ↓
Encrypted API call to CRA verification service
  ↓
CRA validates:
  ✓ SIN is valid and active
  ✓ Person is 18+ years old
  ✓ Person is Canadian citizen
  ✓ Person is alive
  ✓ Person has not already voted in this election
  ↓
CRA returns: {verified: true, riding: "Niagara Falls", name: "Brandon [Lastname]"}
  ↓
Kiosk logs verification (with timestamp) to blockchain
  ↓
Ballot interface loads for verified voter
```

Privacy Protection:

- SIN is hashed before being recorded on blockchain
- Actual SIN never stored in voting database
- CRA API uses zero-knowledge proof (confirms eligibility without revealing identity)
- After vote is cast, link between identity and ballot ID is cryptographically severed

Voter Eligibility Database

Structure:

- Maintained by Elections Canada (updated from CRA data)
- Contains: SIN hash, riding, eligibility status
- Real-time sync across all kiosks
- Prevents double-voting (marked as "voted" after first ballot)

Security:

- Database is read-only for kiosks
- Encrypted at rest and in transit (TLS 1.3)
- Distributed across multiple secure servers
- Audit log of all access attempts

---

3. Blockchain Architecture

Consensus Mechanism: Proof of Authority (PoA)

Why PoA (not Proof of Work or Proof of Stake):

- **Speed:** Blocks confirmed in seconds (not minutes)
- **Energy efficient:** No wasteful mining computation
- **Controlled validators:** Trusted institutions run nodes
- **Finality:** Votes are irreversible once confirmed

Validator Nodes (Authority Nodes):

Minimum 50 independent nodes distributed across:

- Elections Canada (primary authority)
- Provincial election bodies (10 nodes)
- Universities (15 nodes - UBC, Toronto, Waterloo, McGill, etc.)
- Independent auditing firms (10 nodes - PwC, Deloitte, etc.)
- Civil society organizations (10 nodes - OpenMedia, etc.)
- International observers (5 nodes - UN, OAS, etc.)

Node Requirements:

- Must be publicly identified (no anonymous validators)
- Must run open-source CDVS node software
- Must have 99.9% uptime SLA
- Must undergo annual security audits
- Can be removed by 2/3 vote of other validators if compromised

Blockchain Structure

Block Contents:

```json
{
  "block_number": 482391,
  "timestamp": "2025-04-28T14:23:17Z",
  "previous_hash": "0x7a8f3e2d9c1b4a5e6f7890abcdef1234",
  "merkle_root": "0x9b8a7f6e5d4c3b2a1098fedcba987654",
  "votes": [
    {
      "ballot_id": "CDN-X7K9PL2M",
      "encrypted_vote": "0xABCDEF123456...",
      "riding": "Niagara Falls",
      "timestamp": "2025-04-28T14:23:15Z",
      "kiosk_signature": "0x7890ABCD...",
      "voter_hash": "0x1234FEDC..." // Hashed SIN - cannot reverse
    },
    // ... more votes in this block
  ],
  "validator_signatures": [
    {"node": "Elections_Canada_Node_1", "signature": "0xABC123..."},
    {"node": "UBC_Crypto_Lab", "signature": "0xDEF456..."},
    // ... signatures from 51%+ of validators
  ]
}
```

Key Properties:

- **Immutability:** Changing any vote would break the cryptographic hash chain
- **Transparency:** All blocks are publicly readable
- **Auditability:** Anyone can download the full blockchain and verify
- **Finality:** Once 51%+ validators sign a block, it's permanent

Cryptographic Security

Encryption Algorithm:

- **Ballot Encryption:** AES-256-GCM (symmetric encryption)
- **Signatures:** ECDSA with secp256k1 curve (same as Bitcoin)

- **Hashing:** SHA-256 (industry standard)

Key Management:

Each kiosk has a unique key pair:

```
Private Key (stored in HSM - never leaves kiosk):
  - Used to sign votes
  - Proves vote came from legitimate kiosk

Public Key (on blockchain):
  - Used to verify kiosk signatures
  - Anyone can verify authenticity
```

Vote Encryption Process:

```
1. User selects "Mike Doe - Conservative Party"
2. Kiosk generates unique ballot ID: CDN-X7K9PL2M
3. Vote content encrypted with AES-256:

   Plaintext: {"candidate": "Mike Doe", "party": "Conservative"}
   Encrypted: 0xABCDEF123456789... (gibberish without decryption key)

4. Kiosk signs encrypted vote with private key
5. Submit to blockchain with ballot ID

Result on public blockchain:
   CDN-X7K9PL2M: [encrypted data] - Status: Counted ✓
```

Why This Works:

- **Public can see ballot exists** (transparency)
- **Public cannot see how you voted** (privacy)
- **Only you have the ballot ID** (you can verify your vote)
- **Kiosk signature proves legitimacy** (prevents fake ballots)

---

4. Real-Time Tallying System

Vote Counting Process

Traditional System Problems:

- Humans count paper ballots (slow, error-prone)
- Counting happens in back rooms (no transparency)
- Results delayed hours or days
- Recounts required for close races

CDVS Solution: Real-Time Automated Tallying

```
Vote submitted to blockchain
  ↓
51%+ validator nodes confirm (< 5 seconds)
  ↓
Vote permanently recorded
  ↓
Automated tally updates immediately
  ↓
Public dashboard refreshes in real-time
```

Tally Database Structure:

json


```
{
 "election": "2025_Federal_Election",
 "riding": "Niagara Falls",
 "timestamp": "2025-04-28T14:23:20Z",
 "results": {
  "Mike Doe - Conservative": 3847,
  "John Smith - Liberal": 2901,
  "Jane Doe - NDP": 1834,
  "Michelle Doe - Green": 892
 },
 "metadata": {
  "total_votes": 9474,
  "registered_voters": 45289,
  "turnout": "20.9%"
 }
}
```


Update Frequency:

- New votes tallied within 5 seconds

- Public dashboard refreshes every 2 seconds
- No lag between voting and counting

---

5. Public Transparency Dashboard

Web Application (Publicly Accessible)

URL: transparency.cdvs.ca

Features:

1. Live National Map

```
Interactive map of Canada showing:
- Each riding colored by leading candidate
- Click any riding for detailed breakdown
- Real-time vote counts updating
- Turnout percentages
```

2. Riding-Level Detail

```
For each riding:
- Current vote totals by candidate
- Bar chart visualization
- Turnout stats
- Historical comparison
- "Verify Your Vote" button
```

3. Vote Verification

```
Enter your ballot ID: [CDN-X7K9PL2M]
↓
Result:
✓ Ballot ID found on blockchain
✓ Vote recorded at: 2025-04-28 14:23:15
✓ Counted in riding: Niagara Falls
✓ Status: Finalized
✓ Block: 482391
✓ Validator signatures: 52/50 (confirmed)
```

4. Blockchain Explorer

```
Navigate full blockchain:
- View any block
- See all votes in that block
- Verify cryptographic signatures
- Download full ledger for independent audit
```

5. Real-Time Statistics

```
National Dashboard:
- Total votes cast: 12,847,392
- Turnout: 67.3%
- Leading party: Conservative (34.2%)
- Votes per second: 847
- Last block: 2 seconds ago
```

Mobile Application

iOS/Android App:

- Same features as web dashboard
- Push notifications (optional): "Polls closing in 1 hour"
- Easier ballot ID verification (camera scan QR code from receipt)
- Offline mode (cached data until connection restored)

---

6. Security & Attack Prevention

Threat Model & Defenses

Attack: Voter Coercion

Threat: Someone forces voter to show their ballot ID and prove how they voted.

Defense:

- Votes encrypted on blockchain (ballot ID shows nothing without decryption)
- Voter can claim they "lost" their ballot ID
- System could support "duress ballots" (fake IDs that show false results)

Attack: Ballot Stuffing

Threat: Bad actor tries to submit fake votes to inflate tallies.

Defense:

- Every vote requires CRA identity verification
- SIN database prevents duplicate voting
- Kiosk signatures prove vote came from legitimate machine
- Blockchain rejects unsigned or improperly signed votes

Attack: Vote Manipulation

Threat: Hacker tries to change votes after submission.

Defense:

- Cryptographic impossibility - would break hash chain
- 50+ independent validators would all detect tampering
- Public blockchain means anyone can verify integrity
- Attempted change would be immediately visible

Attack: DDoS (Denial of Service)

Threat: Overwhelm system with traffic to prevent voting.

Defense:

- Distributed architecture (no single point of failure)
- Kiosks cache votes locally if connection lost
- Votes sync to blockchain when connection restored
- Multiple network paths (wired + LTE backup)

Attack: Insider Threat (Elections Canada Employee)

Threat: Corrupt insider tries to manipulate results.

Defense:

- No single entity controls blockchain (50+ validators)
- All changes logged immutably
- Public audit trail visible to everyone
- Whistleblowers can prove tampering mathematically

Attack: Quantum Computing (Future Threat)

Threat: Quantum computers break current encryption.

Defense:

- Blockchain designed to be "crypto-agile"
- Can upgrade to post-quantum algorithms when needed
- Plan to migrate to quantum-resistant signatures (NIST standards)

---

7. Accessibility & Inclusivity

Universal Design Principles

Physical Accessibility:

- Wheelchair-height kiosks (ADA compliant)
- Large buttons (minimum 1" x 1")
- High-contrast mode
- Audio narration via headphones
- Braille overlays on key controls

Language Support:

- English
- French
- 20+ Indigenous languages
- Immigrant languages (Mandarin, Punjabi, Arabic, etc.)

Digital Literacy Accommodations:

- "Simple mode" with minimal text
- Visual guides (pictures of candidates)
- Poll worker assistance allowed (voter privacy maintained)

Remote/Accessibility Voting:

- Future phase: Secure home voting for:
  - Physically disabled citizens

    - Military overseas
    - Remote communities (with satellite internet)
- Enhanced security (biometric authentication)

---

8. Implementation Roadmap

Phase 1: Proof of Concept (6 months)

Goal: Demonstrate CDVS works in a real election.

Pilot Location: Small municipality (5,000-10,000 voters)

Deliverables:

- 5-10 kiosks deployed
- 3-5 validator nodes
- Basic blockchain implementation
- Public dashboard (web only)

Success Metrics:

- 0 technical failures
- 95%+ voter satisfaction
- Results match manual recount
- Media coverage (positive)

Phase 2: Regional Expansion (1 year)

Goal: Scale to provincial election or 10+ federal ridings.

Deployment:

- 100-200 kiosks
- 20 validator nodes
- Mobile app launched
- Full accessibility features

Success Metrics:

- 99.9% uptime

- Courts accept blockchain proof as legally valid
- Public audits verify accuracy
- Political endorsements secured

Phase 3: National Adoption (2-5 years)

Goal: CDVS becomes the standard for Canadian federal elections.

Deployment:

- 5,000+ kiosks (all 338 ridings)
- 50+ validator nodes
- International observers
- Open-source codebase published

Success Metrics:

- Elections Canada officially adopts CDVS
- Legislation passed to recognize blockchain votes
- Other countries study Canadian model
- Trust in electoral system increases measurably

---

9. Legal & Regulatory Framework

Current Canadian Election Law

Canada Elections Act Compliance:

- Votes must be secret (✓ Encryption ensures this)
- Votes must be verifiable (✓ Blockchain provides proof)
- Voter identity must be confirmed (✓ CRA integration)
- Results must be auditable (✓ Public ledger)

Required Amendments:

- Define "digital ballot" as legally equivalent to paper
- Authorize blockchain as valid record
- Establish validator node governance

- Set security standards for kiosks

Governance Structure

CDVS Oversight Board:

- 9 members appointed by Parliament
- 3-year terms, staggered
- Cannot be current elected officials
- Responsible for:
  - Approving validator nodes
  - Setting security standards
  - Investigating incidents
  - Annual public reporting

Independent Auditing:

- Annual third-party security audit (mandatory)
- Results published publicly
- Bug bounty program ($10,000+ for critical vulnerabilities)
- University partnerships for ongoing research

---

10. Cost Analysis

One-Time Setup Costs

Item	Cost per Unit	Quantity	Total
CDVS AVM Kiosks	$15,000	5,000	$75,000,000
Blockchain Infrastructure	$500,000	1	$500,000
Software Development	$200,000	1	$200,000
Security Audits	$100,000	1	$100,000
Training & Rollout	$50,000	338 ridings	$16,900,000
Total Setup			**$92,700,000**

Annual Operating Costs

Item	Cost
Validator Node Operations	$2,000,000
Kiosk Maintenance	$5,000,000
Security Monitoring	$1,000,000
Software Updates	$500,000
Staff (10 FTE)	$1,000,000
Total Annual	**$9,500,000**

Cost Comparison to Current System

Current Paper Ballot System (per federal election):

- Poll workers: $120,000,000
- Printing ballots: $15,000,000
- Facilities rental: $30,000,000
- Counting/recounts: $25,000,000
- **Total per election: ~$190,000,000**

CDVS System (per federal election):

- Operating costs: $9,500,000
- Depreciation (kiosks over 10 years): $7,500,000
- **Total per election: ~$17,000,000**

Savings: $173,000,000 per election (91% cost reduction)

---

11. Open Source Strategy

Code Repositories

Public GitHub Organization: `github.com/CDVS-Canada`

Repositories:

- `cdvs-blockchain` - Core blockchain node software
- `cdvs-kiosk` - Kiosk user interface
- `cdvs-dashboard` - Public transparency web app

- `cdvs-mobile` - iOS/Android apps
- `cdvs-cra-integration` - Identity verification API
- `cdvs-docs` - Technical documentation

License: MIT License (permissive open source)

Contribution Guidelines:

- All code reviewed by 2+ maintainers
- Mandatory security scanning (SAST/DAST)
- Unit test coverage > 90%
- No proprietary dependencies

Community Engagement

Developer Community:

- Monthly virtual meetups
- Annual CDVS conference (developers, academics, activists)
- University partnerships (student projects)
- Hackathons for feature development

Bug Bounty Program:

- $100 - $50,000 rewards for vulnerabilities
- Higher payouts for critical exploits
- Public disclosure after patch deployed

---

12. Conclusion

The Canadian Digital Voting System represents a fundamental reimagining of electoral infrastructure. By leveraging blockchain technology, public-key cryptography, and distributed consensus, CDVS provides:

✅ **Mathematical proof** instead of institutional trust
✅ **Real-time transparency** instead of opaque counting
✅ **Voter verification** instead of blind faith
✅ **Corruption resistance** through distributed architecture
✅ **Cost savings** of 90%+ compared to paper ballots

CDVS is not a replacement for democracy - it's democracy upgraded.

The technology exists. The need is urgent. The only question is: Will Canada lead the world in transparent, verifiable elections?

Appendix A: Glossary

Blockchain: Distributed ledger where records (votes) are linked cryptographically, making tampering detectable.

Consensus Mechanism: Protocol for multiple nodes to agree on blockchain state (prevents conflicting records).

Proof of Authority (PoA): Consensus where trusted validators confirm transactions (fast, energy-efficient).

Public Key Cryptography: System where encryption uses public key, decryption requires private key (enables secrecy).

Hash Function: One-way mathematical function that creates unique fingerprints (e.g., SHA-256).

Node: Computer running blockchain software that stores and validates votes.

Validator: Trusted entity operating a node that confirms votes (e.g., Elections Canada, universities).

Ballot ID: Unique identifier for a vote (e.g., CDN-X7K9PL2M) - allows verification without revealing vote content.

Appendix B: FAQ

Q: Can hackers change votes on the blockchain?
A: No. Changing any vote would break the cryptographic hash chain, and 50+ validators would immediately detect tampering.

Q: What if someone steals my ballot ID?
A: The ballot ID only shows your vote was counted - it doesn't reveal how you voted (encrypted).

Q: What if the internet goes down on election day?
A: Kiosks cache votes locally and sync when connection restores. Distributed architecture means no single point of failure.

Q: Can't blockchain be hacked like crypto exchanges?
A: Crypto exchange hacks target wallets (storage), not blockchains themselves. CDVS blockchain is public and distributed - no central target.

Q: What if a kiosk breaks down?
A: Backup kiosks at each location. Votes stored in multiple places (distributed). Paper ballots as emergency

backup.

Q: How do you prevent someone from voting twice?
A: CRA database marks SIN as "voted" after first ballot. Blockchain rejects duplicate attempts.

Q: Is this legal under Canadian law?
A: Canada Elections Act needs minor amendments to recognize digital ballots, but core principles (secrecy, verifiability, auditability) are met.

Q: Who pays for this?
A: Initial investment by federal government, but system saves $170M+ per election vs. paper ballots.

Document Version: 1.0
Last Updated: November 2025
Author: CDVS Project