Votar: Civic Participation Platform

Secure, Transparent Voting at Scale via WhatsApp

Divine Comedian
0x9b0dece40eebc776e521cbd8d0e54e2863cc22bd

Ed
0xf5d29a6359e938c4e0c4d440e582e426ff9a0eb9

November 14, 2025

Abstract

This whitepaper presents a decentralized civic participation platform that enables institutions to make inclusive, transparent decisions at scale. By combining zero-knowledge proofs, blockchain technology, and WhatsApp's ubiquitous messaging infrastructure, the platform removes participation barriers, accelerates institutional decision-making, and restores trust through cryptographic certainty rather than institutional authority. Citizens verify identity once, then participate in decisions affecting them without friction, while institutions gain genuine citizen input in hours instead of weeks.

Contents

1 Executive Summary

We believe that the current dynamics of civic participation are still stuck hundreds of years in the past. Voting is often the most impactful form of civic decision-making, and federal elections represent the highest privilege citizens are given to participate in most democracies. Yet somehow this privilege feels like a chore that many people opt out of entirely.

Citizens are tasked with traveling to centralized locations at government-mandated times to cast their vote. This is a large undertaking for both governments and citizens, requiring substantial infrastructure, personnel, time, research, and coordination. A single election can cost millions of taxpayer dollars and consume hundreds of thousands of hours of citizens' valuable time—all for a single decision.

1.1 The Opportunity

We propose a WhatsApp-based civic participation platform that enables institutions to make secure, transparent decisions at scale. The system uses zero-knowledge proofs and blockchain technology to guarantee vote integrity while maintaining voter privacy, all abstracted behind Latin America's most familiar and widely-used messaging application. Institutions can accelerate decision-making from weeks to days, increase citizen participation by removing friction, and restore trust through transparent, cryptographically-verifiable voting processes.

2 The Problem

2.1 Current Voting Infrastructure Failures

2.1.1 Participation Barriers

- Citizens must be physically present at town halls or polling stations
- Citizens cannot vote if they are too far from their designated voting location. In Argentina, voting is compulsory; citizens must justify their absence
- Requires specialized infrastructure (voting machines, locations, trained staff)
- Time-intensive for all parties (scheduling, travel, waiting)
- Manual recording and counting introduces human error

2.1.2 Trust Deficits

- Centralized vote recording allows potential manipulation
- Information is fragmented across multiple channels; citizens cannot vote and access context in one place
- Results cannot be independently verified
- Citizens must trust institutions inherently, with no recourse
- No audit trail for disputes or recounts

2.1.3 Speed Constraints

- Institutions require weeks to organize votes
- Citizens wait days for results
- Feedback loops are slow; decisions become stale or irrelevant

2.1.4 Scalability Limitations

- Each vote requires proportional infrastructure investment
- Geographic scale is limited (one location per vote)
- Running multiple simultaneous decisions is difficult
- Manual ballot counting leaves room for human error

2.2 Why This Matters

Institutions—municipalities, universities, neighborhoods, cooperatives—are struggling to make truly inclusive decisions. They want citizen input, but the friction is too high. Citizens want influence, but voting feels futile. The result: voters don't make the effort, turnout is low, and elected officials lack genuine legitimacy. This creates a vicious cycle where institutions feel disconnected from citizens, and citizens feel unheard.

3 The Solution

3.1 How It Works

3.1.1 For Citizens

1. **One-time Setup:** Verify identity using the appropriate authentication method (see Authentication Tiers below)

2. **Get Informed:** Receive WhatsApp notifications about open and upcoming votes, with all information needed to make a decision

3. **Vote Simply:** Select your option; vote is recorded

4. **See Results:** View outcomes immediately with anonymized participation data

3.1.2 For Institutions

1. **Create Proposal:** Define title, options, eligible communities (postal codes), and required authentication level

2. **Set Timeline:** Choose start and end dates

3. **Launch:** System automatically notifies eligible voters

4. **Monitor:** View real-time results with participation metrics

5. **Close:** Declare winner and publish results

3.2 Authentication Tiers

The platform supports flexible authentication levels to match the stakes and scope of each decision. Institutions choose the appropriate tier when creating proposals:

3.2.1 Tier 1: Full Identity Verification (High-Stakes Votes)

Use Cases: National elections, federal referendums, legally-binding institutional decisions

How It Works: When an institution creates a Tier 1 poll, citizens who receive the invitation are prompted to verify their government-issued ID via decentralized identity providers (e.g., Didit)

What's Verified:

- Full name matches government records

- Registered voting address and postal code

- Citizenship or residency status

- Uniqueness (one vote per verified identity)

Privacy: Identity data is hashed and encrypted; only eligibility proof is recorded on-chain

3.2.2 Tier 2: Whitelist Verification (Municipal & Local Votes)

Use Cases: City council decisions, neighborhood associations, university governance, local budget allocation, organizational voting

How It Works: Institutions upload a whitelist of phone numbers or email addresses. Only users on this whitelist receive the voting invitation. On first access, users verify their contact method with a code, then can vote on all future polls.

What's Verified:

- Phone number or email is on the approved whitelist
- Contact method uniqueness (one vote per verified contact)
- Organizational affiliation or membership status

Privacy: Phone/email hashed; no personal details stored; whitelist managed by institution

3.2.3 Tier 3: Open Access (Public Polls & Feedback)

Use Cases: Community feedback, event planning, non-binding opinion polls, public consultations

How It Works: Anyone who scans the QR code or accesses the shareable link can participate. No invitations are sent—access to the QR code determines eligibility.

What's Verified:

- Access to the QR code or link
- Optional rate-limiting to prevent ballot stuffing

Privacy: Fully anonymous; no personal data collected

3.2.4 Choosing the Right Tier

Tier	**Verification**	**Use Cases**	**Trust Model**
Tier 1	Government ID + postal code	National/federal elections	Legal identity
Tier 2	Whitelist (phone/email)	Organizational/local voting	Membership
Tier 3	QR code/link	Public feedback	Open participation

This tiered approach allows institutions to balance security, privacy, and accessibility based on the importance and scope of each decision.

3.3 Why This Actually Works

3.3.1 Removes Friction

- **WhatsApp:** Already on citizens' phones; no app installation required
- **One-time Verification:** No repeated logins each voting cycle
- **Mobile-First:** Vote from anywhere in seconds

3.3.2 Guarantees Integrity

- **Zero-Knowledge Proofs:** Voters prove eligibility without revealing identity (see Technical Foundation for details)
- **Blockchain Recording:** Each vote is immutable and independently verifiable
- **Transparency:** Anyone can audit the entire voting process while individual votes remain anonymous

3.3.3 Accelerates Decisions

- Citizens are notified immediately when eligible
- Voting happens in real-time
- Results are available instantly
- Feedback loops measured in hours, not weeks

3.3.4 Scales Naturally

- One citizen can vote on thousands of proposals
- Multiple institutions can run simultaneous votes
- No geographic limitations
- Infrastructure grows horizontally, not per-vote

3.4 System Flow Diagrams

3.4.1 UML Activity Diagram: Citizen Setup and Voting Flow

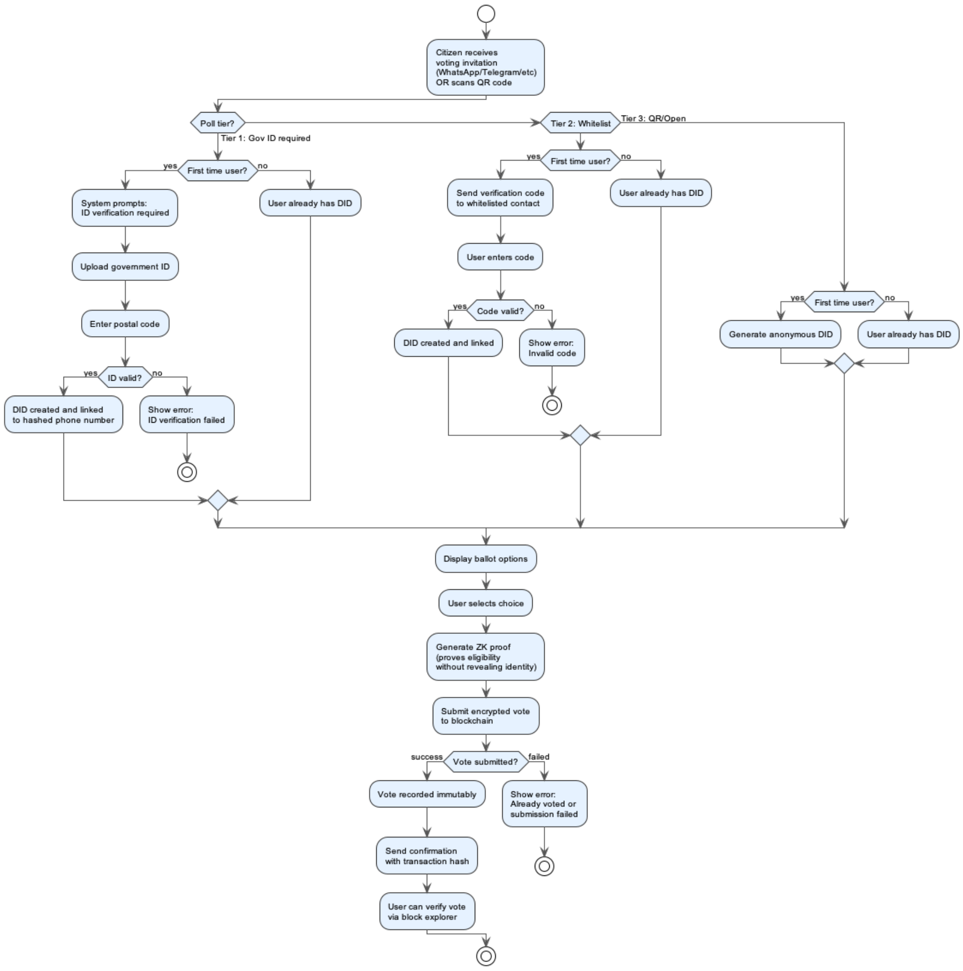
Citizen receives voting invitation (WhatsApp/Telegram/etc) OR scans QR code
Poll tier?
Tier 1: Gov ID required
Tier 2: Whitelist
Tier 3: QR/Open
First time user?
yes
no
System prompts: ID verification required
User already has DID
Upload government ID
Enter postal code
ID valid?
yes
no
DID created and linked to hashed phone number
Show error: ID verification failed
First time user?
yes
no
Send verification code to whitelisted contact
User already has DID
User enters code
Code valid?
yes
no
DID created and linked
Show error: Invalid code
First time user?
yes
no
Generate anonymous DID
User already has DID
Display ballot options
User selects choice
Generate ZK proof (proves eligibility without revealing identity)
Submit encrypted vote to blockchain
Vote submitted?
success
failed
Vote recorded immutably
Show error: Already voted or submission failed
Send confirmation with transaction hash
User can verify vote via block explorer

Figure 1: UML Activity Diagram: Citizen Setup and Voting Flow

3.4.2 UML Activity Diagram: Institution Admin Flow

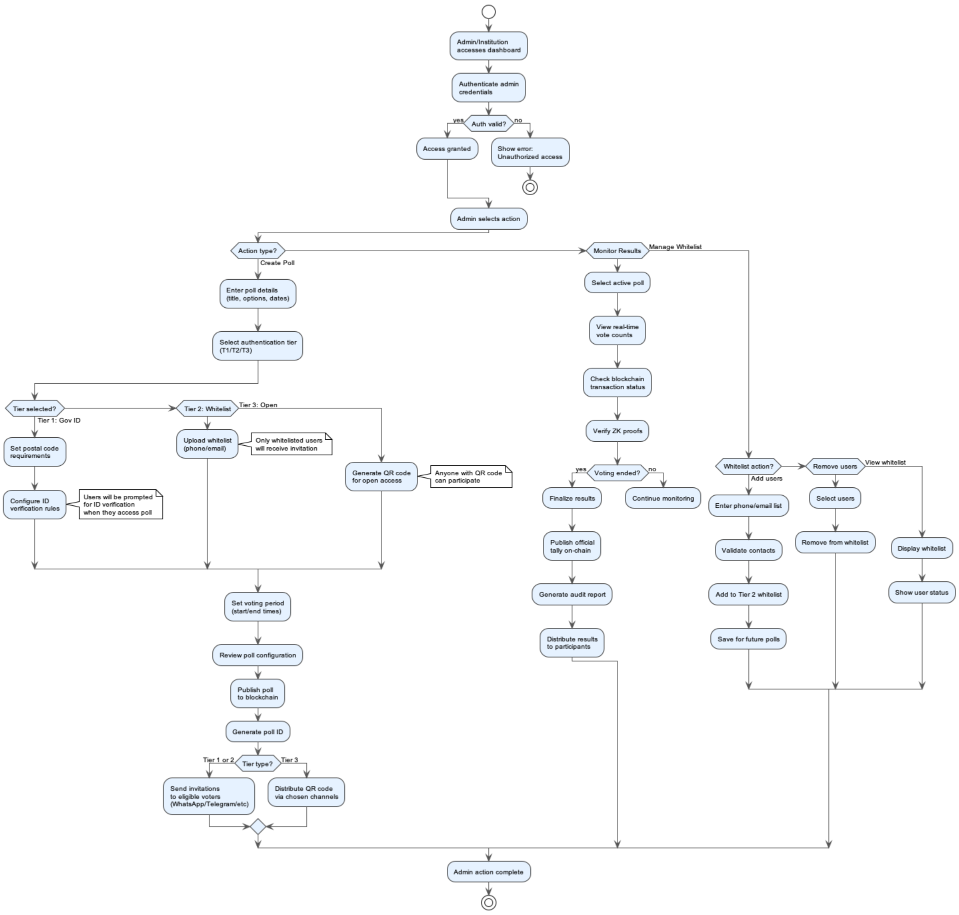
Admin/Institution accesses dashboard
Authenticate admin credentials
Auth valid?
yes
no
Access granted
Show error: Unauthorized access
Admin selects action
Action type?
Create Poll
Monitor Results
Manage Whitelist
Enter poll details (title, options, dates)
Select authentication tier (T1/T2/T3)
Tier selected?
Tier 1: Gov ID
Tier 2: Whitelist
Tier 3: Open
Set postal code requirements
Configure ID verification rules
Users will be prompted for ID verification when they access poll
Upload whitelist (phone/email)
Only whitelisted users will receive invitation
Generate QR code for open access
Anyone with QR code can participate
Set voting period (start/end times)
Review poll configuration
Publish poll to blockchain
Generate poll ID
Tier 1 or 2
Tier type?
Tier 3
Send invitations to eligible voters (WhatsApp/Telegram/etc)
Distribute QR code via chosen channels
Select active poll
View real-time vote counts
Check blockchain transaction status
Verify ZK proofs
yes
Voting ended?
no
Finalize results
Continue monitoring
Publish official tally on-chain
Generate audit report
Distribute results to participants
Whitelist action?
Add users
Remove users
View whitelist
Enter phone/email list
Validate contacts
Add to Tier 2 whitelist
Save for future polls
Select users
Remove from whitelist
Display whitelist
Show user status
Admin action complete

Figure 2: UML Activity Diagram: Institution Admin Proposal Creation and Management

4 Technical Foundation

4.1 Architecture Philosophy

The system abstracts away cryptographic complexity from users. Citizens see a simple voting interface (”click to vote”); beneath the surface, zero-knowledge proofs verify eligibility and blockchain records guarantee immutability. This design philosophy ensures security and trust without requiring users to understand the underlying mathematics.

4.2 Core Components

4.2.1 Identity Layer

Decentralized verification ensures citizens prove eligibility (postal code residency) without revealing personal details to the voting system. Citizens maintain control over their identity through decentralized identity infrastructure (e.g., Didit), and the system only stores irreversible hashes of identifying information.

4.2.2 Voting Layer

The blockchain records each vote immutably. Zero-knowledge proofs prove a vote is valid without revealing voter identity or vote content (until authorized). This layer guarantees that no vote can be altered, deleted, or disputed after recording.

4.2.3 Messaging Layer

WhatsApp is the primary interface for Latin America, with optional support for Telegram and other messaging platforms to accommodate different regions. The platform can be adapted to use WeChat for China, LINE for Japan, or other regionally-dominant messaging apps. Citizens never leave their preferred messaging app to vote, minimizing friction and maximizing accessibility.

4.2.4 Data Layer

The system maintains minimal data storage—only hashed identifiers and postal codes, never plaintext personal information. Phone numbers and all sensitive data are encrypted at rest in the database and in transit. Only irreversible hashes are used for identity verification and deduplication.

4.3 Key Properties

- **Security Without Complexity:** Citizens see a simple ”click to vote” interface while zero-knowledge proofs verify eligibility silently and blockchain immutability replaces trust with mathematical certainty
- **Transparency Without Breach:** Vote counts are verifiable by anyone with complete audit trails, yet results cannot be altered retroactively
- **Speed & Scale:** Institutional decisions made in hours (not weeks), supporting thousands of simultaneous votes with no per-vote infrastructure cost

5 Use Cases

5.1 Municipal Decisions

- Budget allocation votes
- Park naming and usage decisions
- Local regulation feedback
- Emergency response priorities

5.2 Educational Institutions

- Student government elections
- Course offering preferences
- Campus policy feedback
- Resource allocation

5.3 Neighborhood Associations

- Community improvement priorities
- Rules and governance changes
- Event planning decisions
- Dispute resolution

5.4 Cooperative Organizations

- Member voting on operational decisions
- Dividend distribution choices
- Policy changes
- Leadership elections

6 Why Now

6.1 Market Conditions

- **WhatsApp Penetration:** 2 billion users globally, more than 80% in target demographics
- **Blockchain Maturity:** Zero-knowledge proofs are production-ready
- **Trust Deficit:** Citizens are increasingly skeptical of centralized institutions and demand transparent, verifiable processes

6.2 Technology Readiness

- **Decentralized Identity (Didit):** Mature enough for production deployment
- **Blockchain Voting Infrastructure (Vocdoni):** Proven at scale
- **WhatsApp Business API:** Stable and reliable
- **Serverless Infrastructure:** Enables cost-effective scaling

7 Future Extensions & Platform Enhancements

While the core platform delivers secure, transparent voting at scale, several natural extensions could amplify participation and institutional outcomes:

7.1 Participation Incentives

Gamification and reward mechanisms can reinforce voting as a valued civic behavior without manipulating vote choices. Citizens could earn tangible rewards for consistent participation: reduced municipal fees or institutional quotas, priority access to public events and services, discounts at local businesses, early enrollment for community programs, or waived administrative fees. Unlike penalties, incentives align with the platform's core mission of reducing friction—voting becomes not just easier, but rewarding. Institutions retain full control over their incentive structures, allowing municipalities, universities, and cooperatives to tailor rewards to their communities.

7.2 Institutional Participation Requirements

Some institutions (cooperatives, HOAs, membership organizations) may want to establish minimum participation thresholds for quorum or decision legitimacy. Rather than platform-enforced penalties, institutions define their own requirements—e.g., "Decisions require 60% participation to be binding." The platform tracks participation transparently on-chain, enabling institutions to enforce their own governance rules without the voting system itself becoming punitive.

7.3 Proposal Discussion & Context

Voting is currently paired with information delivery, but deliberation could be deeper. Integrating threaded discussion channels within WhatsApp or Telegram, directly adjacent to proposals, allows citizens to ask questions and surface concerns before voting. This transforms the platform from a voting mechanism into a deliberation space, increasing decision quality and citizen confidence.

7.4 Delegation & Liquid Democracy

For citizens unable or unwilling to vote on every proposal, delegation allows them to assign voting power to trusted community members on specific topics (e.g., "delegate my environmental policy votes to Maria"). This layer could increase effective participation without requiring universal engagement on every decision.

7.5 Impact Feedback Loops

After decisions are implemented, closing the loop with citizens creates accountability. "Here's what won, here's what we did about it, here's the outcome"—all recorded transparently on-chain. This builds institutional credibility and teaches citizens that their votes matter.

7.6 Multi-Signature Institutional Governance

For high-stakes decisions (budget allocations, leadership elections), institutions could require ZK-proof signatures from multiple authorized representatives alongside citizen votes, combining direct democracy with checks-and-balances.

Each extension maintains the platform's core principles: friction-free participation, cryptographic integrity, and transparent governance. Institutions adopt only what serves their decision-making needs.

8 Threat Model, Assumptions & Limitations

This section describes the adversarial model Votar defends against, the assumptions required for secure operation, and the current limitations of the system. These boundaries are essential for understanding what the platform guarantees—and what it does not.

8.1 Threat Model

Votar is designed to operate securely in adversarial environments where parties may attempt to disrupt voting, impersonate citizens, manipulate results, or compromise the secrecy of ballots. We consider the following categories of adversaries:

8.1.1 A1. External Attackers (Network-Level)

- Attempt to intercept or modify WhatsApp messages
- Attempt to DDoS the API endpoints or blockchain gateway
- Attempt to submit fraudulent votes or replay signed messages

Mitigation:

- WhatsApp provides end-to-end encryption for message transport
- All votes must contain a zero-knowledge eligibility proof; replayed proofs are rejected
- Blockchain records provide immutable sequencing and timestamping

8.1.2 A2. Identity Forgers

- Attempt to impersonate an eligible citizen
- Attempt to register multiple identities to vote more than once

Mitigation:

- Tiered authentication (ID verification, whitelist, QR possession)
- Device-level uniqueness and hashed identifiers
- Census-based key generation ensures one private key per eligible voter

8.1.3 A3. Malicious Institutions

- Attempt to alter vote results
- Attempt to learn how specific individuals voted

Mitigation:

- Institutions cannot alter blockchain results post-hoc
- Institutions never receive or handle private keys or votes
- Census and votes are publicly verifiable

8.1.4 A4. Malicious Citizens

- Attempt to submit multiple votes
- Attempt to reveal or deanonymize other votes
- Attempt to reverse-engineer census membership

Mitigation:

- Each voting key can be used only once
- Census contains only anonymous public keys (no personal data)
- Merkle proofs reveal only membership, not identity

8.2 Security Assumptions

The system relies on the following assumptions:

8.2.1 S1. WhatsApp Delivers Messages Reliably

End-to-end encryption must hold; WhatsApp must not be compromised at the transport layer.

8.2.2 S2. Identity Verification Providers (e.g., Didit) Are Honest

For Tier 1 polls, we assume decentralized identity providers correctly validate government documents.

8.2.3 S3. Citizens Control Their Own Devices

We assume that:

- Citizens do not share their WhatsApp accounts
- Devices are not compromised by malware extracting temporary voting keys

8.2.4 S4. Blockchain Infrastructure Is Honest and Available

The underlying blockchain must:

- Follow a liveness assumption (transactions confirm)
- Be immutable (no reorgs deep enough to rewrite vote history)

8.3 Current Limitations

8.3.1 L1. Device Sharing

Households sharing a phone number may require institutional policies to avoid shared WhatsApp accounts for Tier 1 or Tier 2 polls.

8.3.2 L2. Internet Access Required

Offline voting is currently not supported. While WhatsApp covers nearly all mobile devices, an internet connection is still required.

8.3.3 L3. Trust in Messaging Platforms

Although WhatsApp provides secure transport, it remains a centralized service. Outages or regional restrictions may affect participation.

8.3.4 L4. Cryptographic Key Abstraction

Voting keys are generated per election and stored only transiently on the user's device by the bot interface. While this removes friction, it also prevents users from exporting or managing these keys directly.

8.4 Why WhatsApp Is a Secure and Practical Interface

The choice of WhatsApp is not arbitrary—it is central to making civic participation **frictionless** and **inclusive**. WhatsApp provides:

- **Ubiquity:** Over 80% penetration in Latin America
- **End-to-End Encryption:** Ensures messages cannot be read or tampered with
- **Anti-Spam Rate Limits:** Prevents automated account creation and bot farms
- **Familiar UX:** Removes the need for citizens to learn a new application
- **No Installation Required:** The platform meets citizens where they already are
- **Authentication Built-In:** The WhatsApp phone number is itself a validated identifier

Most importantly:

WhatsApp removes the largest barrier in digital democracy: asking people to download a new app.

In regions where mobile devices are shared or low-end, WhatsApp is often the only reliable, daily-used communication channel. Leveraging it reduces participation friction more than any cryptographic or UX innovation alone.

8.5 Summary

Votar provides strong end-to-end guarantees: anonymous eligibility proofs, immutable results, transparent audits, and no plaintext personal data. These guarantees hold as long as the threat model assumptions are met. The platform intentionally trades maximal decentralization for maximal participation—while still grounding every vote in cryptographic certainty rather than institutional trust.

9 Vision

A world where institutional decision-making is fast, transparent, and inclusive. Citizens participate in decisions affecting them without friction. Institutions gain genuine citizen input and make better decisions faster. Trust is guaranteed by cryptography, not institutions.

This platform is the infrastructure layer that makes that world possible.

A How Anonymous Voting Works: Simple Explanation

A.1 The Problem

How do we prove someone is eligible to vote without revealing who they are or how they voted?

A.2 The Solution: Census-Based Cryptographic Identity

Votar uses **Vocdoni's census system**. Instead of identifying voters by name or personal data, each eligible voter gets a unique **cryptographic voting key** that proves eligibility without revealing identity.

A.3 How It Works

A.3.1 Step 1: Building the Census (Eligibility List)

1. Institution creates a poll and defines who's eligible (e.g., verified IDs with postal code 1234, or whitelisted phone numbers)
2. For each eligible voter, the system generates a **one-time voting keypair**:
   - **Private Voting Key:** Stays on the voter's device, used to sign their vote
   - **Public Voting Key:** Added to the census (a cryptographic list stored as a Merkle Tree)
3. The census contains only these anonymous public keys—no names, no phone numbers, no personal data

A.3.2 Step 2: Casting a Vote

When a citizen votes:

1. Their device creates a **signed vote** using their private voting key
2. Generates a **Merkle proof** showing their public key is in the census
3. Submits both to the blockchain

The blockchain verifies: "This public key is in the census" (proving eligibility) without learning **who** owns that key.

A.3.3 Step 3: Counting Results

- All votes are counted anonymously
- Each voting key can only vote once (prevents double-voting)
- Results are publicly verifiable, but votes cannot be traced back to individuals

A.4 Key Insight: Separation of Identity and Eligibility

Identity verification (government ID, whitelist, QR code) happens **once** to prove you're eligible.

Voting keys are generated **per election** and are completely anonymous.

The system **never links** your identity to your voting key or your vote choice.

A.5 What Each Party Sees

What the Citizen Sees	Click to vote
What the System Knows	A valid voting key from the census was used
What the Blockchain Records	Signed vote + Merkle proof (no identity, no names)
What Everyone Can Verify	Total vote counts, eligibility criteria, audit trail

B Security & Privacy Guarantees

B.1 What We Never Store Plaintext

- Personal identification documents
- Actual postal codes
- Passport numbers
- Addresses
- Personal names

B.2 What We Store (Encrypted/Hashed)

- Postal code hash (irreversible, one-way)
- Phone number hash (for deduplication)
- Decentralized identity identifier (user-controlled)

B.3 What's on Blockchain (Immutable)

- Vote count per option
- Zero-knowledge proof of eligibility
- Timestamp of vote
- Anonymous vote identifier (cannot be linked to voter)

B.4 What's Private (End-to-End)

- Voter identity
- How each individual voter voted
- Personal information used for verification

B.5 What's Transparent (Verifiable)

- Total vote count
- Result per option
- Eligibility criteria (who could vote)
- Audit trail (all votes, no deletions)