Tanideh: A Decentralized Network for Elections and Referendums

Abstract

Elections and referendums are the foundation of rational and democratic governance, yet in many parts of the world they remain unattainable ideals. Existing so-called decentralized digital voting solutions often depend on centralized servers or energy-intensive blockchains. Under autocratic systems, such infrastructures are effectively centralized, making them vulnerable to manipulation, censorship, or suppression.

Tanideh introduces a novel decentralized network for elections and referendums, designed to operate solely on the collective participation of its clients, without central authorities or privileged nodes. The system employs an address-based recursive partitioning scheme that scales naturally from hundreds of clients to tens of millions, while ensuring redundancy, resilience, and efficient message routing. Unlike blockchain systems, Tanideh avoids proof-of-work and mining, maintaining efficiency on everyday devices such as smartphones. Combined with anonymity layers and a lightweight UDP-based protocol, Tanideh offers a resilient, transparent, and citizen-driven alternative for secure and verifiable democratic decision-making.

1. Introduction and Motivation

The legitimacy of any democratic process depends on trust: citizens must believe that their voices are counted accurately and fairly. Traditional digital voting platforms often rely on centralized servers, exposing elections to risks of manipulation, single points of failure, and censorship. Blockchain-based systems, while decentralized in theory, suffer from high energy costs, concentration of mining power, and limited scalability.

Tanideh addresses these limitations by introducing a new model of decentralized elections, built from the ground up to be lightweight, secure, and scalable. In Tanideh:

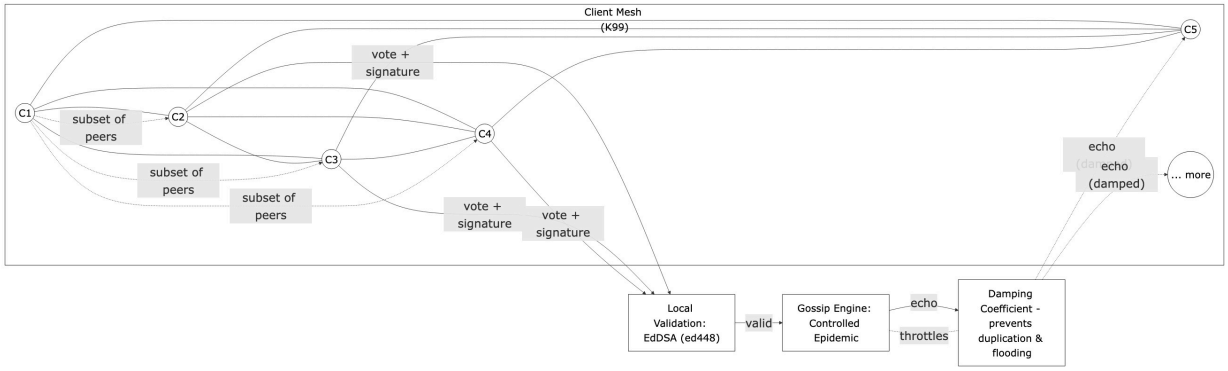
- No central authority exists; every client contributes equally to validation and tallying.
- Votes are disseminated, validated, and echoed across a self-organizing network that partitions dynamically as participation grows.
- The architecture is designed for mass adoption, scaling efficiently to populations as large as entire nations.
- Privacy and resilience are built in through direct peer-to-peer communication, anonymizing relays, and adaptive protocols.

By combining these principles, Tanideh establishes a transparent, citizen-owned network for elections and referendums.

2. Network Architecture

2.1 Fully Connected Small Networks

Consider an initial network of 99 clients. Each client is directly connected to the other 98. Votes are disseminated to a subset of peers, validated using EdDSA with the ed448 curve, and echoed



into the system through a controlled epidemic/gossip mechanism (Eugster et al., 2004). The damping coefficient prevents duplication and flooding.

When a client queries election results, it consults its own local pool of validated votes, which already contains the distributed state. No central authority is required.

2.2 Scaling Beyond 100 Clients

Direct connectivity becomes impractical at larger scales. Tanideh introduces **address-based partitioning**:

- Each client receives a random base-60 network address, distinct from its fixed voting address.
- The alphabet includes digits 0–9 and English letters excluding "I" and "O".

Once 100 clients are reached, the network is split into two groups based on the first character of the address.

Group 1: addresses with first character in the first 30 symbols.

Group 2: addresses with first character in the remaining 30 symbols.

	First Character
Group 1	**L, M, N, P, Q, R, S,T, U, V, W, X, Y, Z, a, b, c, d, e, f, g, h, i, j, k, l, m,n, o, p**
Group 2	**q, r, s,t, u, v, w,x, y, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G,H, J, K**

Each client connects to all peers in its group (in this case 49) and to two representatives from the other group. Votes are validated locally, while representatives synchronize results between groups. To determine results, a client tallies its group's votes and queries summaries from the other group through its representatives.

2.3 Recursive Division

Partitioning continues as the network grows:

- 200 clients → 2 groups
- 400 clients → 4 groups (base-60 divided into quartiles)
- 6,000 clients → 60 groups (each representing one symbol of the base-60 address space)

At about 6,000 clients, each client maintains:

99 (group peers) + (59 × 2) = 217 connections

This ensures redundancy while remaining efficient.

Considering the address : **T**1KJupW9hAqYFvKxM4nZr3sG7dNQbL8EwV2

	First Character
Group 1	**L**
Group 2	**M**
…	**…**
Group 8	**T (Same Local Group)**
…	**…**
Group 60	**K**

2.4 Expansion to Millions

When the first address character space is saturated (60 groups), the second character is used for subdivision, then the third, and so on.

Example of two full characters: **T1**KJupW9hAqYFvKxM4nZr3sG7dNQbL8EwV2

	First Character	prefix "T" & Second Character
Group 1	**L**	**TL**
Group 2	**M**	**TM**
…	**…**	**…**
Group 8	**T (No Representative)**	**TT**
…	**…**	**T1 (Same Local Group)**
Group 60	**K**	**TK**

Example of three full characters: **T1K**JupW9hAqYFvKxM4nZr3sG7dNQbL8EwV2

	First Character	prefix "T" & Second Character	prefix "T1" & Third Character
Group 1	**L**	**TL**	**T1L**
Group 2	**M**	**TM**	**T1M**
…	**…**	**…**	**…**
Group 8	**T (No Representative)**	**TT**	**T1T**
…	**…**	**T1 (No Representative)**	**T11**
Group 60	**K**	**TK**	**T1K (Same Local Group)**

Using four address characters, the system scales to:
$(60 \times 60 \times 60 \times 60) \times 100 = 1{,}296{,}000{,}000$ clients

For practical purposes, a network of 80 million participants (e.g., the population of Iran) requires only three full levels plus a partial division of the fourth, resulting in:

$(60 \times 60 \times 60 \times 4) \times 100 \approx 86{,}400{,}000$ clients

Each client in this configuration maintains:

$99 + 2 \times (60 + 60 + 60 + 4) = 467$ connections

Each client maintains roughly 467 connections, ensuring scalability and resilience. For national-scale populations (e.g., 80 million), only three full levels plus part of a fourth are needed.

2.5 Routing and Message Passing

Routing requires only the client's address. Maximum path length is four mediators.

- Client A seeks Client B.
- If the first characters differ, A queries a representative sharing B's prefix.
- The process repeats by examining successive characters until B's group is reached.
- Within a group, all peers are directly connected.

To protect privacy, clients never expose their voting address directly. Instead, each client connects to an **Exit Node** through relays. The **Exit Node** network address shares the same local group as the client's voting address, handling all voting-related communication.

3. Security Model

3.1 Threats Considered

Tanideh defends against:

- **Sybil attacks** – flooding the network with fake nodes.
- **Vote tampering** – forging or altering votes.
- **Replay attacks** – re-broadcasting expired votes.
- **Eavesdropping and censorship** – blocking or monitoring communication.

3.2 Anti-Sybil Protections

Sybil attacks, where an adversary generates multiple fake identities to dominate a network, are a fundamental threat to peer-to-peer systems (Douceur, 2002). Traditional approaches assume that attackers can freely create numerous identities, making large-scale networks vulnerable.

Tanideh mitigates Sybil attacks through a combination of platform restrictions, custom protocols, and evolving security measures:

1. Mobile-Only Platform
By restricting Tanideh to mobile applications, we significantly limit automated attacks. Unlike web-based platforms that must conform to standard protocols like TCP/HTTP—easily scripted or emulated—mobile apps can implement lightweight, tailored communication protocols that are difficult for bots to mimic. This reduces the feasibility of automated identity creation and mass infiltration.

2. Custom UDP-Based Protocols
Tanideh uses its own lightweight, undocumented UDP protocols for connection establishment, address discovery, and vote propagation. These protocols are deliberately designed to be difficult to reverse-engineer and include unique features that enhance efficiency and reliability while remaining opaque to attackers.

3. Layered, Evolving Protocols
Communication relies on multiple interdependent layers:

Connection Establishment: Secures node authentication and participation.

Address Discovery: Ensures nodes can locate peers without revealing identities.

Vote Propagation: Guarantees secure and validated vote dissemination.

Each layer depends on the previous, forming a multi-stage security model. Protocol parameters evolve over time, so even if an attacker decodes one layer, subsequent updates quickly render their efforts obsolete.

4. Transparency Without Compromising Security
While Tanideh could theoretically be open source, the combination of custom protocols and mobile-only enforcement ensures that even without full code secrecy, unauthorized automated participation is highly impractical. Legitimate users retain full transparency: every client can access and audit votes directly within the network, maintaining trust without exposing the system to Sybil attacks.

By integrating these measures, Tanideh achieves robust anti-bot and anti-Sybil protections, making large-scale manipulation highly improbable while still maintaining transparency and auditability for all participants.

3.3 Validation and Echo Mechanism

Votes are issued and signed in a manner consistent with industry standards, where the vote information is first hashed, and the resulting hash is cryptographically signed by the unique address (Nakamoto, 2008). The signature is then validated by others through the issuer's voting address.

Votes are:

1. Signed with EdDSA (ed448).
2. Validated for authenticity, group membership, and expiration.
3. Echoed using controlled gossip to ensure redundancy without flooding.

Votes expire after a fixed window, requiring reissuance for continued validity.

3.4 Privacy and Anonymity

- Voting addresses are cryptographically derived locally.
- Communication tied to voting addresses is routed through **Exit Node**.
- Connections between clients and **Exit Node** use layered relays similar to onion routing

In a decentralized voting network, privacy is inseparable from security. Direct peer-to-peer communication tied to a client's voting address could expose the client's IP address, allowing adversaries to deanonymize voters and compromise election integrity. To mitigate this, Tanideh uses the concept of an Exit Node: a proxy identity within the network that shares the same local address group for networking as the client's voting address. All communication exposing voting address occurs through the Exit Node, preventing any direct link between a client's IP and their voting identity.

Onion Routing Foundations

Communication between the client and its Exit Node leverages traditional onion-routing techniques, as popularized by the Tor network (Dingledine et al., 2004). In onion routing, a message is wrapped in multiple layers of encryption and relayed through a series of nodes before reaching its destination:

Guard Relay: knows the user's IP address but not the final destination.

Middle Relay(s): forward encrypted data, preventing the guard from learning the destination and the exit from learning the source.

Exit Relay: knows the destination but not the origin.

This layered approach ensures that no single relay possesses enough information to trace both the sender and recipient, thereby preserving anonymity.

Why Tanideh Requires an Extension

Unlike traditional onion routing, Tanideh has no fixed central servers or websites as communication endpoints. Instead, both the sender and receiver are individual clients, each of whom must remain anonymous. The traditional Tor model assumes that the destination is public (e.g., a website) and only the sender requires anonymity. In Tanideh, certain interactions—such as messaging—require both endpoints to be equally protected.

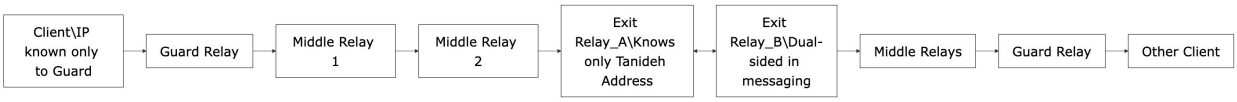
Layered Relays in Tanideh

To achieve symmetrical anonymity, Tanideh extends onion routing into a dual-sided layered relay model:

Each user is represented by an exit relay, which is the only node that knows their Tanideh address, which also serves as their voting address.

Each user also has a guard relay, which is the only node that knows their real IP address.

Between these two, 2–3 middle relays provide additional indirection and encryption layers.



This ensures:

No single relay can link a client's IP address with its Tanideh voting identity.

Even if one relay is compromised, it cannot reveal the full communication path.

Communication remains anonymous, as all address-dependent exchanges are routed through the Exit Node.

By extending onion routing into a fully symmetrical peer-to-peer model, Tanideh guarantees that both the origin and destination of every message are anonymized, preserving voter privacy while ensuring network transparency.

3.5 Dynamic Defense

Because the network protocol is built directly on UDP and can be updated at the application layer, Tanideh's parameters can evolve across versions. If adversaries invest heavily in re-engineering attacks, a protocol update can render their efforts obsolete, preserving resilience over time.

4. Transparency as a Way of Building Trust

Open-audit elections rely on two fundamental principles: ballot-casting assurance, where each voter can verify that their vote was correctly recorded, and universal verifiability, where any observer can confirm that all captured votes were correctly tallied (Adida, 2008; Clarkson et al., 2008). Tanideh achieves these principles without central authorities, privileged nodes, or energy-intensive proof-of-work mechanisms.

4.1 The Votes Spectrum

In Tanideh, each vote is tied to a unique Tanideh address, constructed from a 60-character set (numbers and letters, excluding "O" and "I" to avoid ambiguity). This address serves as the vote identifier and allows for precise tracking and analysis.

The votes spectrum enables segmentation of votes at different levels of granularity:

By first character: quickly summarizes votes across broad groups (e.g., all votes starting with "A").

By prefix: refines analysis further using multiple characters (e.g., "Xa" or "sD1").

By full address: isolates a single vote for confirmation.

This hierarchical segmentation allows users to calculate totals at any level. For example, summing votes that start with "x" will equal the sum of all votes in its sub-prefixes like "xa," "xb," … "x9." This flexibility ensures that both high-level and granular analysis are possible, supporting transparency and auditability.

4.2 Granular Analysis

When the number of votes within a given spectrum falls below a defined threshold (typically fewer than 1,000), Tanideh exposes all corresponding addresses. This enables users to verify individual votes directly, cross-check totals, and ensure no vote has been lost or duplicated.

For example, if a user queries "sD1" and fewer than 1,000 votes match, the system lists every vote in that subset, along with statistics such as timestamps and group origins. This approach ensures full traceability while maintaining practical scalability for larger vote sets.

4.3 Practical Applications

The votes spectrum is not limited to small-scale analysis. Users can combine queries across multiple prefixes to track votes for a candidate, referendum, or policy initiative across large populations. This ensures that every vote can be audited, supporting recounts and independent verification similar to traditional paper-based elections.

Because every vote is tied to a unique address and can be traced down to the individual voter, users can verify authenticity if doubts arise. If a user questions whether a particular vote corresponds to a real participant, they can directly message that voter to confirm.

Votes in Tanideh expire after 30 hours, so users are expected to come online within that timeframe to renew their votes. This ensures that only active participants influence results and maintains the system's integrity. Additionally, users may respond to messages and provide clarifications, casting what could be called a "shadow of doubt" to ensure transparency and accountability in the voting process.

This combination of granular auditability, direct verification, and vote renewal creates a dynamic yet fully transparent system where trust is built through both technology and participant engagement.

5. Consensus and Validation

5.1 Vote Lifecycle

- **Casting** – signed then sent via Exit Node.
- **Validation** – peers verify signatures, timestamps, uniqueness.
- **Echoing** – rebroadcast with coefficient control.
- **Expiration/Renewal** – votes expire after 30 hours; renewal possible after 18 hours.

5.2 Local Consensus

Each group achieves consistency through direct peer validation and storage. Clients can determine results from their local pool without global synchronization.

5.3 Global Consistency

Representatives synchronize results between groups:

- At least two representatives per group are required.
- Divergent summaries can be cross-checked and discarded if inconsistent.

5.4 Double-Voting Prevention

Each vote is cryptographically bound to a client. Duplicate attempts are rejected during validation.

5.5 Fault Tolerance

Because every client maintains its own vote pool, disconnections or representative failures do not compromise results, provided participation stays above the 1% threshold.

6. Encryption

All communications in Tanideh are protected with end-to-end encryption. This ensures that no intermediary can read or tamper with the data. Tanideh achieves this through a secure, two-step handshake followed by symmetric encryption.

6.1 Key Exchange

Each connection begins with Elliptic Curve Diffie-Hellman (ECDH) using the X448 curve, chosen for its speed and strong 224-bit security. This allows the two endpoints to derive a shared secret without transmitting it over the network.

To prevent man-in-the-middle attacks, the shared secret is authenticated using EdDSA signatures bound to the sender's network or voting address. Each element of the handshake is hashed—primarily with SHA-512—and verified by the recipient, ensuring both authenticity and integrity.

6.2 Symmetric Encryption

Once the handshake is complete, the shared secret is converted into a 256-bit AES-GCM key, which is used for encrypting all subsequent communication. AES-256 GCM is selected for its strong security and efficiency, providing confidentiality, integrity, and resistance to tampering.

Keys are never transmitted across the network; they are derived locally at each endpoint, guaranteeing that only the communicating parties can decrypt messages. This protects every vote, message, and control packet from interception or unauthorized access.

6.3 Integration with Privacy Layers

Communications tied to voting addresses are routed through Tanideh's layered relay network (see Section 3.4). Even within these relays, messages remain encrypted end-to-end, preserving privacy while still allowing vote propagation and network synchronization.

This combination of ECDH key exchange, EdDSA authentication, AES-GCM encryption, and layered relays ensures that Tanideh achieves both security and anonymity without relying on central servers or specialized hardware.

7. Limitations and Trade-Offs

7.1 Minimum Participation

The network must not fall below 1% of its maximum capacity at any tier. If a subdivision supports 100 clients, at least 1% of clients must remain active to maintain representative coverage (e.g., 240 out of 24,000).

7.1 Chain Depth vs. Redundancy

As discussed, each client maintains 467 connections to support a network of 86,400,000 clients:

$(60 \times 60 \times 60 \times 4) \times 100 = 86{,}400{,}000$ clients
$99 + 2 \times (60 + 60 + 60 + 4) = 467$ connections

While 467 connections are manageable since they are connected to each other via customized UDP protocol which is lightweight and has way less overhead like traditional TCP connections. But still in real-world devices (e.g., smartphones) the clients gradually drop connections. There is a trade-off between the number of active connections and the maximum acceptable chain depth.

Minimum scenario: each base-60 subdivision splits into only 2, yielding:

$(2^{20}) \times 100 = 104{,}857{,}600$ clients

with only

$100 + (2 \times 20) = 140$ connections

If each stage of the network is split into only 2 sections instead of 60, we could support the same number of clients with only 140 connections per client instead of 467. However, this would increase the chain length to 20. If a client wants direct access to another client, the search information might pass through up to 20 different clients, whereas in the first configuration it would pass through only 4 clients. So there should be some practical balance and trade-off between the two.
Tanideh adopts a division by 4 strategy to balance practicality and scalability.

8. Future Work

While Tanideh has been tested locally under various scales, real-world deployment is needed to refine defenses and optimize representative consistency checks. Future improvements will be guided by community participation and practical feedback.

9. Conclusion

Tanideh introduces a new paradigm for digital democracy: a fully decentralized election network operating without servers, mining, or privileged validators. By leveraging recursive partitioning, lightweight UDP protocols, and peer-to-peer validation, the system achieves unprecedented scalability, transparency, and resilience.

Unlike blockchains, Tanideh avoids energy waste and transaction fees. Unlike centralized systems, it cannot be censored or shut down. By giving every client equal responsibility, Tanideh represents a true citizen-owned infrastructure for elections and referendums, with the potential to serve as the foundation for transparent governance wherever people demand secure, fair, and verifiable decision-making.

References

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Eugster, P. T., Guerraoui, R., Kermarrec, A.-M., & Massoulié, L. (2004). "Epidemic Information Dissemination in Distributed Systems," *IEEE Computer,* 37(5), 60–67.

Douceur, J. R. (2002). "The Sybil Attack," *in International Workshop on Peer-to-Peer Systems (IPTPS)*.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). "Tor: The Second-Generation Onion Router," *in Proceedings of the 13th USENIX Security Symposium*.

Adida, B. (2008). "Helios: Web-based Open-Audit Voting," *in USENIX Security Symposium*.

Clarkson, M. R., Chong, S., & Myers, A. C. (2008). "Civitas: Toward a Secure Voting System," *in IEEE Symposium on Security and Privacy*.