The 2026 House of Representatives Election Case Study on heain-core

Results Anyone Can Check, Ballots No One Can Open Alone
16 Nodes in 3 Tiers, Units as Apps: Paper Ballots through Core (Design A) and Voting Machines with Blind Tokens (Design B) against the System as It Was, 478 Nodes at National Scale, 3-of-5 Key Custody and Core Rounds C12–C16

Jakkrit Boonma (จักรกฤษ บุญมา)
Independent Researcher · ORCID: 0009-0000-7165-3787 · jaggid.boonma@yahoo.co.th

Date: 11 November 2026
Implementation: heain-core 3505e61 (Go 1.26), heain-sdk 1.6 (da98a44), HP Z840
Repository: github.com/JakkritB/heain-core (casestudies/mp/)

Abstract

Thailand's House of Representatives election on 8 February 2026 had 52,933,610 eligible voters in 400 constituencies and about 99,487 polling units [2][14]. Most reported problems lay in aggregation and reporting: the results system stalled at 31%, stopped at 94% and never reached 100% [8][9]; unit results came out as PDFs with units missing [9]; and a report said totals did not match the unit tally forms (S.S. 5/18) [18]. A ballot barcode that could link ballots to voters was ruled not unconstitutional (28 Sep 2026) [12].

The author simulated the election on heain-core with 16 nodes in 3 tiers and 18 polling units as apps, comparing two designs with a model of the system as it was (asis). Design A keeps paper ballots, but each unit signs a digital form 5/18 onto a public log and every aggregate must cite the results beneath it. Design B uses voting machines, keeping register, token-blinding kiosk (RFC 9474 [19]) and machine apart, and seals each ballot at once with core's key. All data are synthetic.

On one HP Z840 every round passed. asis could not detect 50 votes added in aggregation, while an observer without a certificate found them in 3.07 seconds. asis showed 100% with one unit missing and stuck nationwide at 33.3% when its reporting point failed; a heain standby took over in 14.7 seconds. A tampered machine passed every electronic check and was caught only by a paper-slip audit. At national scale, 478 nodes received all 99,487 unit forms in 34 seconds. Of five core rounds, C12 lets ballots open only with committee approval plus 3 of 5 outside organizations; C13–C16 fix behavior when a parent is down or a standby takes over.

Keywords: *HEAIN Framework, heain-core, General Election, Thailand 2026, Election Results Reporting, Public Verifiability, Transparency Log, Blind Signatures, Paper Audit Trail, Threshold Key Custody, Shamir Secret Sharing, Sealed Ballots*

1. Introduction

1.1 Background

Earlier case studies of the HEAIN Framework tested heain-core on disasters, the southern border and the 2024 Senate selection [26]. The Senate case posed the problem of separating identity from votes and of inquiry under P5. A general election poses a different one: scale. Results from about 99,487 units must roll up to constituency, province and nation in a single night, and it must be possible to check back that every total came from real unit results. Voters are not tens of thousands of candidates who can be handed devices, but tens of millions of citizens with no device of their own in the polling unit.

The starting point was the author's document "HEAIN Election Node Map: 400 Constituencies on heain-core v1.3" [27], which made each polling unit a node and separated an identity lane from a vote lane. Before designing, the author checked its figures and claims against news reports and compared its mechanisms with heain-core as it then stood (C11). Three corrections mattered. First, 99,487 units as nodes is far beyond the size core had been tested at (330 nodes), so the layout has nodes down to constituency and units as apps. Second, the document had no provincial tier, though the Election Commission (EC) has provincial offices, so the layout has one. Third, the 3-of-5 key split the document proposed did not exist in core. Sealed data under C10 is guarded by P5 rules, but the node administrator still held the full key, which led to core round C12.

1.2 Facts Checked

Figure	Meaning	Source
52,933,610	Eligible voters	[2]
37,807,781 / 37,807,778	Voters, party list / constituency (71.42%), 3 ballots apart; the EC said some out-of-district envelopes lacked both ballot types	[2]
35,030,601 / 1,669,006 / 1,108,051	Valid / spoiled / no-vote ballots on the party list (sum is 123 short of turnout, before recounts)	[2]
400 + 100	Constituency and party-list MPs	[2][6]
About 99,487	Polling units, as the EC figure used in the news; no single official notice found (one source gives 99,538)	[14][15]
≈ 249 / ≈ 380	Units per constituency / voters per unit (computed)	—
16 / 1	Units the EC ordered recounted (as of 24 Feb 2026) / unit that voted again	[5][10]
250 sets	Stand-alone voting machines the EC plans (2 per province; each set 1 tallying machine + 4 voting machines)	[14][15]

Table 1 — Election figures used in this paper

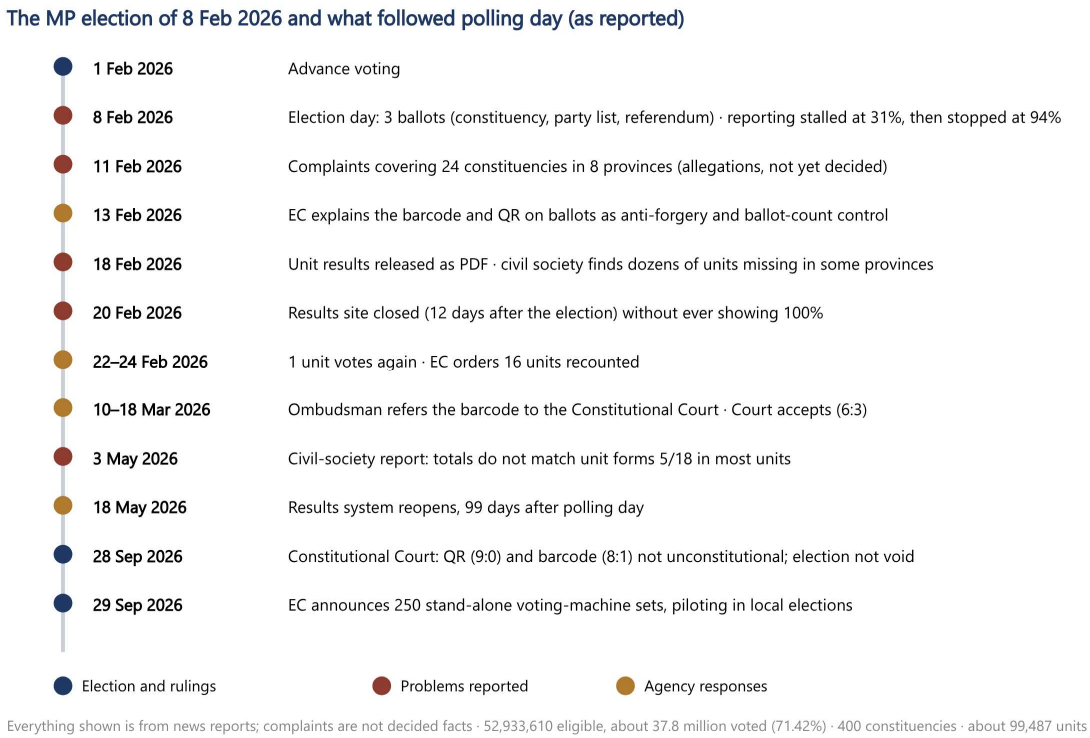


Figure 1 — The 2026 MP election and events after polling day; figures and events from news reports [2][3][5][8][9][11][12][13][14][18]

Two sources give budgets that do not match (7.82 billion baht and about 8.98 billion baht), probably counted over different scopes, so neither is used here. The report that totals did not match forms 5/18 [18] could not be opened during checking, so only its conclusion is cited, without detailed figures.

1.3 Complaints and Rulings

> This section relates complaints and proceedings as reported in the news. They are not facts decided by a court or the EC unless stated as a ruling. This paper names no person or political party. Faults in the model are synthetic and tied to no real constituency or province.

As of 11 February 2026, complaints covered 24 constituencies in 8 provinces, for example unusually high spoiled ballots, counting out of public view, fewer valid ballots than the winner's votes, and board figures changing after the polls closed [3]. As of 24 February 2026 the EC had ordered 16 units recounted [5]. The law already provides for this: section 122 requires a report to the EC when turnout does not match ballots used, and section 124 lets the EC order a recount or a new vote in some units or a whole constituency [4][16].

The issue that bears directly on design is the barcode and QR on the ballot. Party-list ballots carried unique, sequential barcodes; the EC said they served anti-forgery and ballot-count control [13]. The Ombudsman referred the matter to the Constitutional Court, which ruled on 28 September 2026 that

the QR (9:0) and barcode (8:1) were not unconstitutional and the election was not void [12]. As summarized by the press, the Court accepted that party-list ballots "can be linked to the counterfoil technically", but relied on safeguards and observers, and suggested anti-forgery that uses no mark linked to voter data [11]. That suggestion is a design criterion for Design B: no value ties a ballot to a person.

The next day the EC announced plans for stand-alone voting machines connected to no network: press a number, confirm, and get results right after the polls close, piloting in local elections [14][15]. The reports mention neither paper evidence nor checking by voters. The case thus has a real counterpart to compare: such a machine against one whose every step is signed and can be checked back.

1.4 Research Questions

1. **RQ1** If paper ballots stay as under current law, can HEAIN at the aggregation and reporting tier fix problems like those of 2026: stalled reporting, results never reaching 100%, totals not matching unit results, and data as PDF?
2. **RQ2** How does a voting machine using HEAIN differ from a stand-alone machine? When a machine's tallies are altered, is it caught, when, and by whom?
3. **RQ3** Can blind tokens still keep people unlinkable from ballots when voters have no device of their own?
4. **RQ4** Can section 122 checks per ballot and recounts through P5 be automatic and checkable afterwards?
5. **RQ5** Can core take a simultaneous close at national scale (400 constituencies, 99,487 unit forms)?
6. **RQ6** Can it be made that no single party, the node administrator included, can open sealed ballots?

1.5 Scope

- **Both designs are built and compared**, as the author decided (30 Oct 2026). Design A is usable now without legal change; Design B is where the EC is heading.
- **Identity by national ID card and an official.** No biometrics as the source map proposed: they are sensitive data and not needed for the research questions.
- **Three ballots simulated:** constituency, party list and referendum, with section 122 checked per ballot.
- **Real complaints are not simulated.** All faults are synthetic, injected for testing.
- **This deployment is the author's hypothetical design,** not a project of the EC or any agency, and not reviewed by any agency.

2. Rules and Law Used in the Simulation

Before writing rules into the app, the author checked them against the Organic Act on the Election of Members of the House of Representatives B.E. 2561 (2018) as amended [16] and the party-list seat method as reported [6]. Table 2 gives the result.

Section	Content	Consequence for the design
84 para. 5	Voting follows the method the EC sets	An opening for voting machines; not yet checked whether it suffices or the Act must be amended (Design B is therefore an assumption)
91	Mark a cross; a no-vote option exists	Every digital ballot has a no-vote option
92–93	Assisting a disabled voter is still direct and secret voting	Help in the booth must not break secrecy
121	If counting cannot proceed for necessity, stop and resume	A cut-off constituency works on and sends its journal later
122	Turnout not matching ballots used is reported to the EC	The app checks per ballot, flags, and proposes a recount into P5
124	EC orders a recount or new vote in some units or a whole constituency	Unit recounts approved at the constituency; annulling a whole constituency needs the EC, 4 of 7
30-day objection	Objections within 30 days of election day	Legal hold per unit with a complaint; remaining evidence deleted when the period ends

Table 2 — Sections the app enforces or that bear on the design

Party-list seats are computed by dividing all parties' total votes by 100 to get votes per seat. Each party first takes its whole share; the remaining seats go to the largest remainders in order, and ties at the cut-off are settled by lot [6]. The app uses the commit-reveal lottery of the Senate case: the hash of the seed is published before election day and the seed after the national result.

3. Method

3.1 Simulation Layout

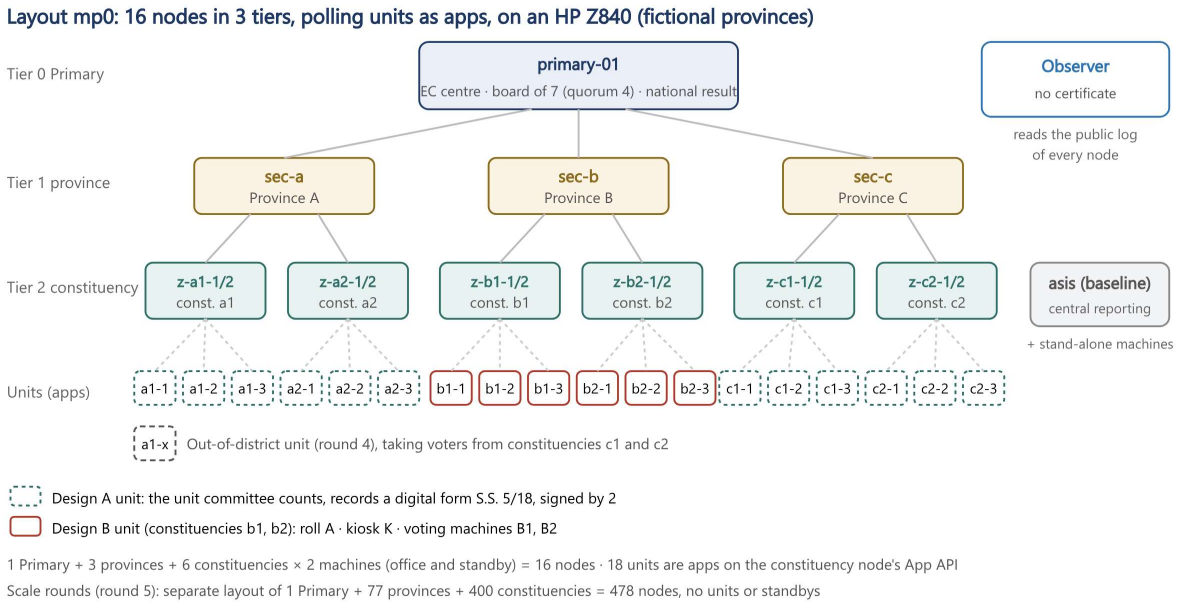


Figure 2 — Simulation layout mp0: 16 nodes in 3 tiers, polling units as apps

The layout has 16 core nodes: a Primary (EC centre, a board of 7 with quorum 4), 3 provinces and 6 constituencies, each with an office and a standby (Figure 2). The 18 polling units are apps that talk to their constituency node through the App API with app certificates; core refuses units directly (403). Every node is a container on one machine with a short-lived node certificate, and every constituency, province and Primary node has a public log (C11) that observers can read without a certificate.

3.2 Design A: Paper Ballots + HEAIN at Aggregation

Design A changes neither voting nor counting at the unit, only the path results travel.

1. **Record:** the unit committee counts as usual, then records a digital form 5/18 for all 3 ballots: eligible, turnout, ballots received, used, valid, spoiled, no-vote and left over, and votes per candidate, party and answer.
2. **Sign:** the unit's app certificate and 2 committee members sign the same bytes; a single signer is refused (400).
3. **Check before accepting:** the constituency office refuses forms whose arithmetic does not add up, and flags forms where turnout does not equal ballots used (section 122), while still accepting them.
4. **Publish:** an accepted form goes onto the constituency's public log at once; a unit may resend without duplicate effect.

5. **Aggregate:** constituency, province and national results are signed by that tier's office and cite the SHA-256 of every lower result used; an incomplete result names the missing units.
6. **Correct:** only one way, a revision citing the old form and a recount approved through P5; both stay on the log for good.

3.3 Design B: Voting Machines + Blind Tokens

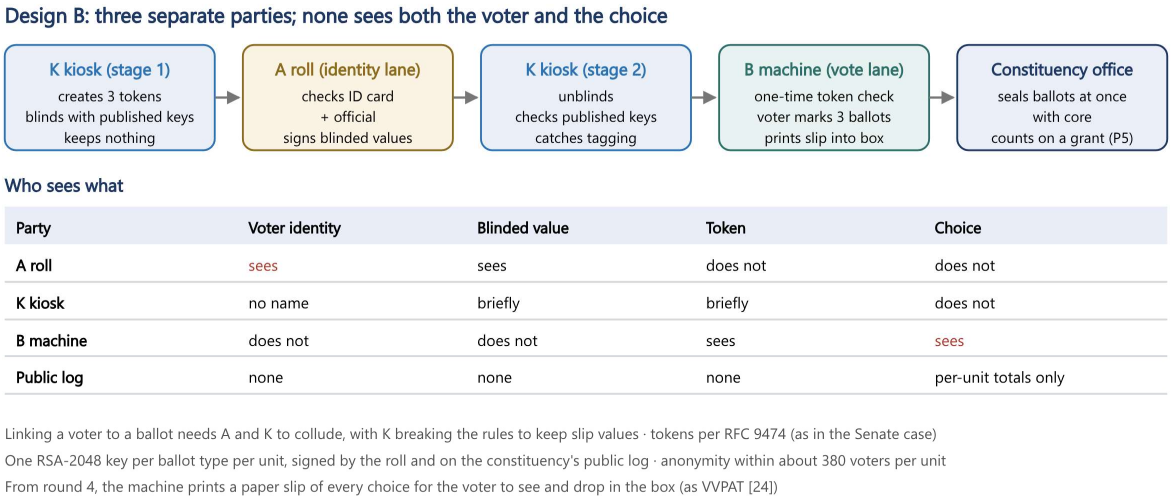


Figure 3 — Design B: three separate parties and what each sees

In a general election, voters have no device of their own as in the Senate case [26], so the token blinder must be a device in the unit. If the voting machine blinded tokens itself, a machine colluding with the register could link people to ballots. Design B therefore has three parties (Figure 3). Kiosk K creates one token per ballot and blinds it with published keys. Register A checks the ID card and signs the blinded values. K unblinds and checks them against the published keys. Machine B takes the vote with a one-time token and passes the ballot to the constituency office, which seals it at once. Values that K needs between its two stages travel on a slip the voter carries, not inside K.

Counting happens when the constituency committee approves a counting grant through P5. The office opens ballots one by one under the grant, counts per unit and signs a result with the turnout signed by the register and the root of the receipts. The result thus has the same shape as in Design A. From round 4, the machine prints a paper slip of every choice for the voter to check and drop in the box, for comparison with the electronic count (as VVPAT [24]).

3.4 The mpapp App and Core Mechanisms Used

Command	Design	What it does	Core used
unit-post	A	Unit sends form 5/18 signed by 2, via an outbox, resendable	App certificates
office	A, B	Constituency office: accept forms, check section 122, publish, aggregate, propose recounts, seal ballots, count under a grant	P5, public log, journal, sealed data
prov / nat	A, B	Province and centre: check lower tiers as an observer would; sign province and national results and party-list seats	Public log, journal, P5
roll / kiosk / machine	B	Register A, kiosk K and voting machine B	lanes.unlinkable, public log
observe	A, B	Observer without a certificate checks every tier from public logs	Public listener (C11)
central / standalone	asis	Central reporting centre and stand-alone machine (test only)	—
load / scalecheck	Scale	Send 99,487 forms at once and measure every node from inside the same network	—

Table 3 — mpapp commands and the core mechanisms they use

The app is written in standard Go and talks to core only through the App API; core has no election-specific code. The blind-token code is shared with the Senate app, so every round also runs the Senate case regression.

3.5 Synthetic Data

- **Voters:** about 380 per unit, 3 ballots each, with turnout, spoiled and no-vote rates at 2026 levels but random per unit.
- **Parties and candidates:** 12 fictional parties and about 8 constituency candidates per constituency. The data weight candidates down by number, so the winner everywhere is number 1, which means nothing.
- **Faults:** injected for testing only, e.g. an insider in an office adding 50 votes, a machine recording another party, and a unit missing from the batch file.
- **Time:** election day is compressed to minutes, and the 30-day objection period to minutes.

3.6 Systems Compared

Aspect	asis (model of the 2026 system)	heain
Unit results	Sent to one central server; published later as a batch file	Signed at the unit; on the constituency's public log at once
Totals	Centre shows percentages that cite no unit results	Every tier signs and cites the hashes of lower results
Who can check	Must request data and compare oneself	Anyone, without a certificate
Point of failure	One centre; the whole country stalls	Each constituency has a standby; others unaffected
Section 122	Checked by people afterwards	App checks on receipt, proposes a recount into P5
Voting machine	Stand-alone, counts internally, prints results	Signed token, sealed ballot, receipt, paper slip

Table 4 — The system as it was (asis) compared with heain

3.7 Rounds and Environment

Round	Content	Scenes
0	16-node layout, P5, board, public logs, form 5/18 and observer	S0
1	Design A at unit and constituency: close, standby, false totals, section 122, legal hold	M1–M7
2	National tier: party-list seats, lottery, referendum per unit	M8–M9
3	Design B: blind tokens via kiosk, sealed ballots, dead machine	M10, M11, M14, M15
4	Tampered machine against paper slips; out-of-district unit	M12, M13
5–5d	National scale, 478 nodes	M16
5e	Province not answering while a new app registers (after C13)	S5e
6	The same election day in three systems: asis, heain Design A and B	S6.1–S6.8
7	Design B under 3-of-5 key custody (after C12)	S7.1–S7.5

Table 5 — Rounds of the case study

All rounds ran on an HP Z840 with scripts committed only when they passed in full. Every round starts from a fresh set of nodes with round 0 run first. Whenever core changed, every round of this case and of earlier case studies was rerun. Reported results come from the final run on core C12 (3505e61, 7 Nov 2026), except the scale round, reported from round 5d (1 Nov 2026).

4. Core Work Arising from This Case

Before designing, the author compared 14 requirements with core C11. Most already existed: hierarchy, working when the network is cut, escrow of sealed data, lane separation, P5 per tier, legal hold and public logs. What was missing was key splitting among outside organizations. During the rounds three more core problems surfaced, and one from regression. Every change followed the same procedure: write a proposal, have the author decide, then run the full regression of every case study (Table 6).

Round	What was added or fixed	Reason	Tests
C13 (969b9eb)	A node that cannot ask its parent and has no earlier answer returns 503 cert_unverifiable with Retry-After instead of 403; heain-sdk 1.5	Round 5c: with a province not answering, constituencies refused new app certificates as if invalid	Round 5e 13/13
C14 (c95bbdf)	A failed ask upward is remembered for 10 s; no repeat ask to the same node; connect timeout 3 s	Round 6: with a province down, every office call took 20 s; closing 2 constituencies took 152 s	Round 6 S6.5
C15 (f7ebad3)	Idle connections closed when the node certificate changes; one resend when refused for an old certificate	Found in C14's regression: connections opened before certificate renewal were refused	live, disaster round 4
C16 (b1c00e4)	The journal goes to the node actually reported to at the time; a standby taking over continues from what the old node had sent	Round 1: the standby sent its journal to the dead node; the constituency result stuck	live 14/14, round 1
C12 (3505e61)	Seal with a public key; the private key split k of n among outside organizations, then wiped; open only with a grant and k shares; heain-sdk 1.6	Source map and plan item 14: the node administrator still held a key that could open ballots	live 22/22, round 7 12/12

Table 6 — Core changes from the MP case

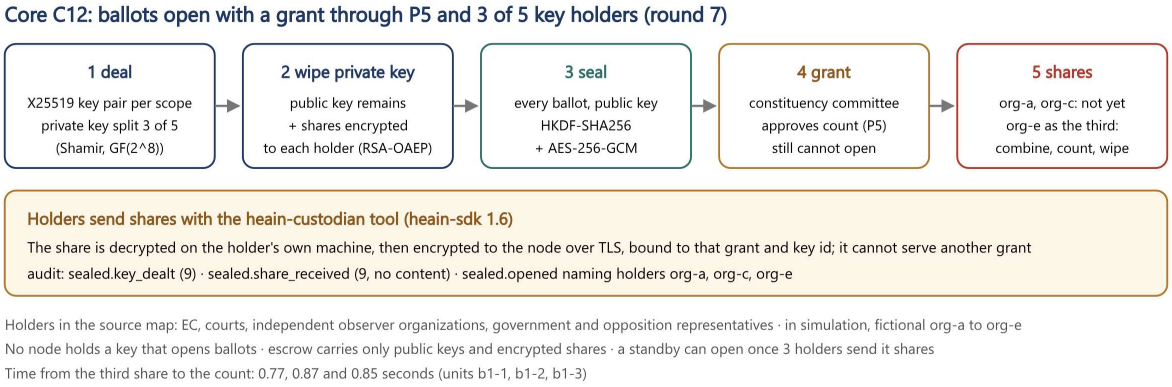


Figure 4 — Core C12: sealing and opening under 3-of-5 key holders

C12 uses an X25519 key pair per scope (unit and ballot type). The node splits the private key with Shamir's scheme [22] over GF(2^8), encrypts each share to its holder's certificate with RSA-OAEP, and wipes the private key at once. Ballots are sealed with the public key through HKDF-SHA256 and AES-256-GCM [23], bound to the record id and key id (Figure 4). Opening needs both a grant passed through P5 under C10's existing rules and shares from at least k holders, encrypted to the node and bound to that grant; fewer than k gets 403 custodians_short. Holders send with the heain-custodian tool in heain-sdk 1.6. A policy without custodians works exactly as C10, and older records open as before.

heain-sdk 1.5 added ErrCertUnverifiable and retry by Retry-After (C13), and heain-sdk 1.6 added the custody package and the heain-custodian command (C12). Every round reran the full regression of the earlier case studies (southern border, CineNexus, disaster, trials E1–E4 and the Senate), with unchanged results throughout.

5. Results

5.1 Design A at Unit and Constituency (Round 1)

Scene	Result
M1 Simultaneous close	6 constituencies close at once; every result cites forms from all 3 units; the journal reaches the provinces in full; an observer without a certificate verifies all 6
M2 Reporting point lost	asis: the central screen stalls, every constituency shows 33.3% though data from all 18 units has arrived; heain: z-a1-1 dies, the standby takes over with evidence keys for 3 units, units resend into the standby, nothing is counted twice, other constituencies are unaffected
M3 False totals	asis: prints 50 extra votes; totals and batch file agree with each other; undetected; heain: an insider at office c1 adds 50 votes; the observer finds it at once; the signed statement stays on the log

Scene	Result
M4 Section 122	At b2-2 party-list ballots used do not equal turnout; flagged, recount proposed; an ordinary approver cannot approve (403); the constituency committee approves; the revision cites the old form
M5 Unapproved correction	A revision with no recount: 400; citing another constituency's recount: 403; annulling constituency c2 by the constituency committee: refused (403), needs the EC, 4 of 7
M6 Network cut	A revision waits while the office is down and is delivered once; constituency a2, cut off, closes on its own log; its journal reaches the province on reconnection
M7 Legal hold	Hold on c2-1; evidence of c2-2 and c2-3 deleted but c2-1 refused (409); readable under a grant naming the reader; hold lifted through P5, then deletable
C16	The journal of the standby replacing a1 reaches province A (before C16 it stuck, sent to the dead z-a1-1)

Table 7 — Round 1 results (27/27 passed)

The key result of this round is that faults asis cannot detect from what it publishes become something outsiders find at once in heain, because a constituency result must cite the hashes of signed unit forms, which anyone can re-add and compare. A lost reporting point affects one constituency only, and a standby takes over. A result can be corrected only through an approved recount, and every version stays on the log.

5.2 National Tier (Round 2)

Before election day the centre publishes the SHA-256 of the seed as the first entry on the Primary's log. Province offices fetch constituency results with the forms they cite and check them as an observer would. Province C refused constituency c1's result with 50 added votes and stated why (forms add to 333 but the result claims 383), then accepted the honest result sent later. The centre checked 3 provinces down to the 18 unit forms in about 0.5 seconds, signed the national result, then revealed the seed and signed the 100 party-list seats.

An observer without a certificate rebuilt the whole country from the 10 public logs: every tier matched the one below, the national result equalled the 18 forms added up, the seed matched its commitment, and the seats recomputed exactly (P01 33, P02 16, P03 10, P04 8, P05 7, P06 5, P07–P09 4, P10–P12 3, synthetic data). When an insider at the centre moved one seat, the observer found it at once. Referendum results were published per unit from the signed forms and added up to the national result; in 2026 only the national total was published [9]. This round passed 12/12.

5.3 Design B: Blind Tokens and Sealed Ballots (Round 3)

Scene	Result
M10.1 Keys	3 key sets signed by the register and on b1's log; kiosk and machines take keys only from there
M10.2 Voting	Everyone voted (b1-1 334, b1-2 380, b1-3 366 voters), 3 ballots each with receipts
M10.3 Refusals	Token reuse 409, wrong ballot 400, other unit 403, choice not on the ballot 400, double check-in 409, not on the roll 404
M10.4 Unlinkable	What the register saw and what the machines saw (about 6,400 values each) share no value
M10.5 Tagging	A register signing one voter with an unpublished key was caught by the kiosk; the voter asked again and voted
M11 Sealed ballots	No readable ballot in any file; opened after a grant through P5 (ordinary approver 403); counts match every ballot cast; turnout equals ballots used; the ledger records every ballot
M14 Dead machine	Machine 1 at b1-2 dies mid-day; voters move to machine 2; those whose ballots were already passed on get receipts at machine 2; none sealed twice or lost
M15 Vote buyer	The public log holds no receipt or token, only per-unit totals (about 380 voters per unit)

Table 8 — Round 3 results, Design B in constituency b1 (13/13 passed)

The limit of this design is that K must be trustworthy. If K were altered to keep the slip values and colluded with the register, it could link people to ballots. This is weaker than the Senate case, where voters used their own devices [26], and the constituency office sees choices briefly between receiving them from the machine and sealing them.

5.4 Tampered Machines and Paper Slips (Round 4)

In constituency b2, two machines recorded another party instead of the voter's choice. The first still printed the voter's choice on the slip (25 votes); the second printed what it recorded (10 votes). Both passed every electronic check: the counts were signed and added up, turnout equalled ballots used, and every receipt was in the root. Auditing slips against the count caught the first machine (P01 electronic 83, paper 108; P02 82 against 57) and opened a case in P5. The second matched on paper; only the 10 voters who saw a wrong slip could complain. An asis stand-alone machine tampered the same way printed totals that added up correctly, with nothing to check against.

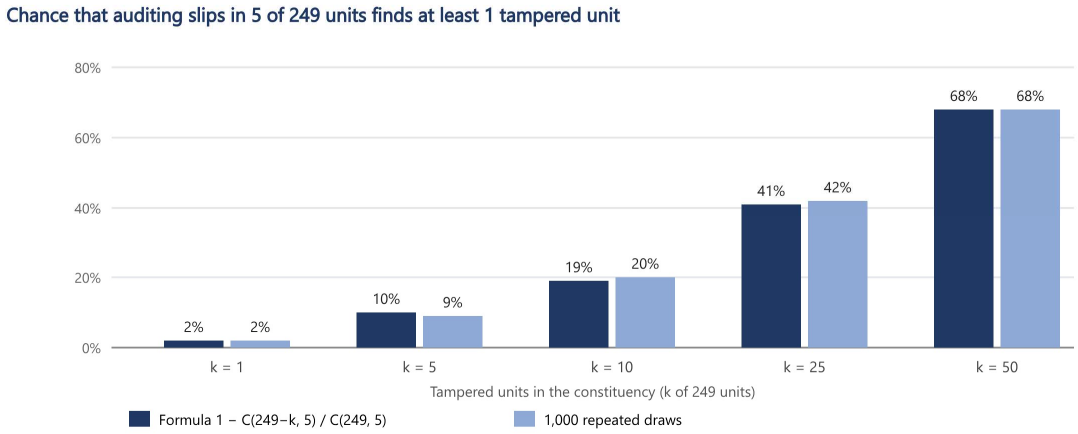


Figure 5 — Chance that auditing slips in 5 of 249 units finds a tampered unit, by number of tampered units (k)

Sampling 5 of 249 units with a seed derived from the published counts catches tampering of a single unit 2% of the time and of 50 units 68% of the time; the formula matches 1,000 repeated draws (Figure 5). The sample size must therefore be chosen from the size of tampering that could change the result, not fixed. India's Supreme Court kept sampling at 5 machines per constituency in 2024 [24]. Out-of-district unit a1-x took voters from constituencies c1 (20) and c2 (15); each used the constituency ballot of their home constituency, counted by home constituency on the same day, with no envelopes to transport. This round passed 10/10.

5.5 National Scale (Rounds 5–5d)

Round 5 brought up 478 containers in 278 seconds, but only 113 nodes answered /health. Rounds 5b and 5c removed docker-proxy, limited GOMAXPROCS and measured from inside the same network. At 278 nodes and above, TCP connections still failed, while the same nodes answered a few seconds later and the machine had resources to spare. The kernel logged "neighbor table overflow" 49,380 times: the single machine's ARP table was full at the default gc_thresh3 = 1,024, a limit of the simulation, not of core.

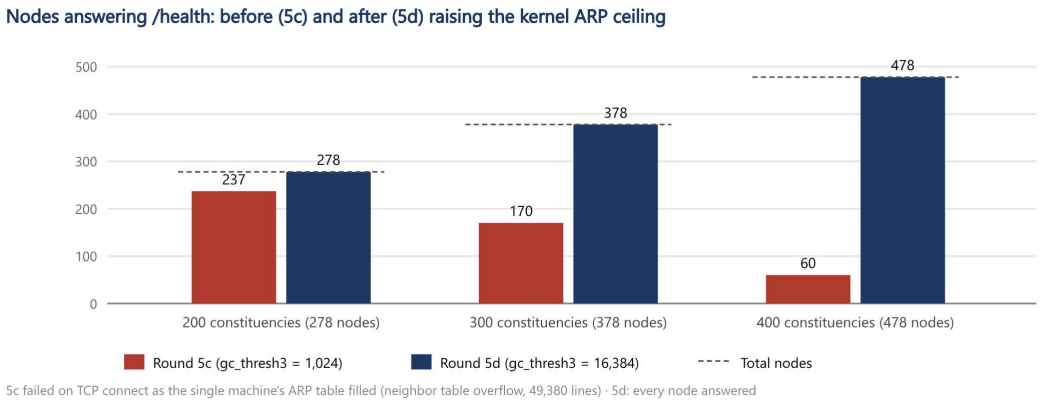


Figure 6 — Nodes answering /health in rounds 5c and 5d at 200, 300 and 400 constituencies

Constit.	Nodes	health p95	Value reaches all	Simultaneous forms	p95 / p99	audit	Memory
200	278	68 ms	21 s	49,744 in 16 s	29 / 34 ms	278/278	3.1 GB
300	378	48 ms	21 s	74,615 in 25 s	31 / 45 ms	378/378	4.2 GB
400	478	44 ms	22 s	99,487 in 34 s	31 / 46 ms	478/478	5.4 GB

Table 9 — Round 5d after raising the ARP ceiling (21/21, no overflow)

At 478 nodes the Primary's fleet view was complete with no stale node. A value set through P5 at the Primary reached all 400 constituencies in 22 seconds. All 99,487 forms (real form size) were received in 34 seconds, and the signed head of every constituency's public log matched the number received. Throughput held at about 2,900–3,000 forms per second at every step, so the bottleneck is likely the single load driver (64 workers) rather than core. Simulating this scale on one machine requires raising gc_thresh, not publishing every node's ports, and limiting GOMAXPROCS per container.

5.6 Province Not Answering (Round 5e and C13, C14)

During round 5c it emerged that when a province did not answer, its constituencies refused new app certificates with 403, the answer for an invalid certificate. After C13, round 5e stopped province A and had a new app register: the constituency answered 503 cert_unverifiable with Retry-After 30 seconds, audited once. Certificates the constituency had already checked still worked, a revoked certificate was still refused with 403, the same certificate registered in province B, and once province A returned it registered there too (13/13).

Round 6 found the next problem. With province A down, every core call at a constituency office took 20.0 seconds (normally 0.016) and closing 2 constituencies took 152.27 seconds, because core asked upward again each time the cache expired, without remembering that it had just failed. After C14, closing 2 constituencies took 0.78–10.81 seconds: the first call after the province stopped answering took about 10 seconds (one ask instead of two) and later calls did not wait.

5.7 asis against heain on the Same Election Day (Round 6)

Scene	asis	heain
S6.1 Normal close	100% after 0.55 s; checkable against unit forms: 0 of 6 constituencies	6 results on logs in 0.57 s; observer verifies all in 6.36 s; at provinces in 6.9 s; checkable: 6 of 6
S6.2 50 votes added in aggregation	Not detectable from what is published	Observer without a certificate finds it in 3.07 s
S6.3 Unit result missing	Shows 100% though the file has 17 of 18 units	Form waits and is delivered once (10.59 s, 6 times)
S6.4 Section 122	Accepted as printed	Flagged and recount proposed as soon as the form arrives
S6.5 Province down	The whole country sees 66.6% until 36.78 s	Constituencies close on their own logs, checkable within; province complete 36.81 s after return
S6.6 Reporting point lost	The whole country stuck at 33.3%	Standby takes over in 14.74 s; constituency complete again at 21.73 s; nothing counted twice
S6.7 Machine records another party, 25 votes	Stand-alone machine prints totals that add up; nothing to check	3 units counted and verified in 7.99 s; the slip audit finds it and opens a case
S6.8 audit	—	Audit chain verifies on all 15 live nodes

Table 10 — The same election day in three systems with the same faults (simulated time, from all unit results to the reporting point)

The figures in Table 10 come from the final run (after C12) and are close to the first run of round 6 in every scene. Times on one machine are shorter than on a real national network. What should be read from the table is the difference between the two systems, not single figures. asis is not slower on a normal day, but what it publishes offers nothing to check, and one failure stalls the whole country.

5.8 3-of-5 Key Custody (Round 7)

Round 7 repeated Design B's polling day in constituency b1 under C12. The ballots policy, set through P5 at the Primary, opens with 3 of 5 fictional organizations org-a to org-e, and constituencies inherit it. 334, 380 and 366 voters cast 3 ballots each. Each unit and ballot type was sealed under its own key, dealt once per key (sealed.key_dealt 9 times). No readable ballot existed in any file on the 16 nodes or the apps.

For each unit the constituency committee approved the count through P5, yet the ballots still could not be opened. With shares from org-a and org-c they still could not. When org-e sent the third share, each unit's count matched every ballot cast; the time from the third share to the count was 0.77, 0.87 and 0.85 seconds. Every opening in the audit names holders org-a, org-c and org-e, and share receipt was recorded 9 times without content. An observer without a certificate verified the counts of all 3 units, and 12 receipts led to the signed root (12/12).

test_sealed_custodians.sh (22/22) covers cases round 7 does not: a 6-of-5 policy is refused when proposed; a share for one grant cannot open another; and when the primary node dies, the standby receives only public keys and encrypted shares, cannot open on its own, keeps sealing, and can open once 3 holders send it shares.

5.9 System Correctness

Set	Result
Round 0 (run first, 7 times)	29/29 every time
Rounds 1, 2, 3, 4, 5e, 6, 7	27, 12, 13, 10, 13, 12, 12, no failures
Round 5d, 478 nodes	21/21 (1 Nov 2026, gc_thresh3 16,384)
Live tests of core C12–C16	test_sealed_custodians 22/22, test_journal_target 14/14, test_cert_last_known 20/20 and 26 other live sets
Regression of earlier cases	Southern border 10 rounds, CineNexus 5, disaster 7, trials E1–E4 and Senate 6 rounds, all pass
Audit chain	Verifies on every node in every round
Values that must be zero	Results counted twice, ballots opened without a grant or with too few shares, values shared across lanes, reusable tokens: all zero

Table 11 — Checks in the final run on core C12 (Z840, 6–7 Nov 2026)

6. Discussion

6.1 Answers to the Research Questions

- **RQ1:** Yes. Unit results signed and published at once, with totals that must cite the results beneath them, mean an incomplete result names the missing units, mismatched totals are found by outsiders in seconds, a single failure affects only its own constituency, and the data is machine-readable JSON. Neither the law nor the voting method needs to change.
- **RQ2:** Signatures and receipts catch tampering at aggregation, but not a machine that records something other than what was chosen. What catches that is a paper slip the voter sees, plus sampling. A stand-alone machine with neither gives nothing to check at all.

- **RQ3:** Yes, conditionally. What the register and machines see share no value, and tagging is caught, but the kiosk must be trusted, which is weaker than voters using their own devices.
- **RQ4:** Yes. The section 122 flag arises on receipt; recount proposals go into the constituency committee's P5; a revision must cite the old form and the approved recount; and the whole history is on the log.
- **RQ5:** Yes, on one machine: 478 nodes received 99,487 forms in 34 seconds once the kernel's ARP ceiling was raised. Earlier failures belonged to the simulation.
- **RQ6:** Yes, after C12. Ballots open when the committee approves and 3 of 5 outside organizations join; no node holds a key that opens ballots. Limits are in section 6.3.

6.2 Possible under Current Law against Requiring Legal Change

Element	Usable with the current system	Needs legal check or change
Digital form 5/18 signed at the unit and published on a public log	Yes (alongside the paper form)	—
Totals at every tier citing lower results, and outsiders adding up themselves	Yes	—
Automatic section 122 checks and recounts through P5	Yes (an administrative step)	—
Referendum results per unit and a verifiable tie lottery	Yes	—
Legal hold per unit with a complaint	Yes, for digital evidence	—
Voting machines, blind tokens and sealed ballots	—	Check whether section 84 para. 5 suffices
Outside 3-of-5 key holders	—	Holders and duties must be defined

Table 12 — Separating what works with today's paper-ballot system from what needs a legal check or change

6.3 Limitations

- **Synthetic data on one machine:** every figure comes from simulation on an HP Z840; no real national network was measured.
- **Units are apps, not nodes:** core guarantees hold from the constituency node up; resending and de-duplication for units belong to the app, and units as nodes have never been tested.
- **The scale round needs a kernel setting:** the raised gc_thresh is not permanent on the Z840, so the scale round has not been in regression since.

- **The kiosk must be trusted:** if altered to keep slip values and colluding with the register, it could link people to ballots. The roll's register is an app file, not sealed by core.
- **At opening (C12):** the scope's private key is in node memory briefly, and holders who kept their decrypted shares could still combine them after crypto-shred. Homomorphic counting without opening individual ballots (as ElectionGuard [25]) is not done.
- **Photography in the booth:** still a vote-buying gap the model does not close.
- **Data not yet verifiable:** the report that totals did not match forms 5/18 [18] could not be opened, and no single official notice of the number of units was found.

7. Conclusion and Recommendations

The 2026 MP election case tested heain-core where earlier cases had not: national scale, and results that must be checkable from the national total down to each unit's form. The most important finding is not technical but a fact the simulation makes visible. The main problems of 2026 lay in aggregation and reporting, which can be fixed without changing the voting method or the law. Voting machines, on the other hand, need paper evidence the voter sees; signatures alone are not enough. Core needed five rounds (C12–C16); after them every check passes and every earlier case study gives the same results.

1. Pilot Design A first in a small election, such as a by-election or local election, alongside the existing system: digital forms 5/18 signed at the unit, published on a public log and open for outsiders to add up.
2. If voting machines are used, require paper slips the voter sees and sampling audits, with the sample size chosen from the size of tampering that could change the result, not a fixed number.
3. Have independent organizations procure and audit the kiosk code, and define the 5 real key holders and their duties before using Design B.
4. Study homomorphic counting on C12's split keys, so that no ballot need be opened individually.
5. Test units as nodes in some constituencies, and run the scale round in regression every time once the test machine's kernel setting is made permanent.

References

[1] Boonma, J. "docs/progress-log.md" and casestudies/mp/ in the heain-core repository, 2026; and the project documents claude/study-2026-10-30-mp-election-case, claude/decision-2026-10-30-mp-design, claude/plan-2026-10-30-mp-case-design and the core C12–C16 proposals (claude/proposal-2026-11-01-core-c13 to claude/proposal-2026-11-05-core-c12).

[2] Thai PBS. 2026 MP election results, EC data as of 25 Feb 2026. 27 February 2026. thaipbs.or.th/news/content/502684 (in Thai).

[3] Thai PBS. Election objections in 24 constituencies, 8 provinces. 11 February 2026. thaipbs.or.th/news/content/502089 (in Thai).

[4] Thai PBS. Legal basis for recounts and new votes: sections 121, 122 and 124. 12 February 2026. thaipbs.or.th/news/content/502116 (in Thai).

[5] Thansettakij. EC orders 16 units recounted. 24 February 2026. thansettakij.com/politics/652298 (in Thai).

[6] Thansettakij. How party-list MPs are computed. 7 February 2026. thansettakij.com/politics/650989 (in Thai).

[7] Thansettakij. Advance voting and out-of-district registration. 5 January 2026. thansettakij.com/politics/648179 (in Thai).

[8] Manager Online. The ECT Report election results system. 2026. mgronline.com/cyberbiz/detail/9690000013598 (in Thai).

[9] The Standard. Election and referendum results system reopens. 18 May 2026. thestandard.co/ect-election-referendum-results-reopen/ (in Thai).

[10] The Matter. Unanswered questions after the 2026 election. thematter.co/brief/257302/257302 (in Thai).

[11] The Matter. Recap of the ballot barcode case. 2026. thematter.co/brief/recap-barcode/265711 (in Thai).

[12] ThaiPublica. Constitutional Court rules on the barcode and QR on ballots. 28 September 2026. thaipublica.org/2026/09/constitutional-court-rules-election-ballot-barcode-constitutional/ (in Thai).

[13] The Standard. EC explains the barcode and QR on ballots. 13 February 2026. thestandard.co/ec-ballot-barcode-qr-code/ (in Thai).

[14] Krungthep Turakij. EC prepares to use electronic voting machines. 29 September 2026. bangkokbiznews.com/politics/1254127 (in Thai).

[15] Komchadluek. The EC's voting-machine plan. 29 September 2026. komchadluek.net/news/politics/623526 (in Thai).

[16] Organic Act on the Election of Members of the House of Representatives B.E. 2561 (2018), sections 84–124 (text compiled at drthawip.com/organiclaw/053) (in Thai).

[17] Wikipedia. 2026 Thai constitutional referendum. en.wikipedia.org/wiki/2026_Thai_constitutional_referendum (not yet checked against EC notices).

[18] iLaw. Report on vote totals against unit forms S.S. 5/18. 3 May 2026. (Content could not be opened during checking; only its conclusion is cited) (in Thai).

[19] Denis, F., Jacobs, F., and Wood, C. A. "RSA Blind Signatures." RFC 9474, IRTF, 2023.

[20] Laurie, B., Messeri, E., and Stradling, R. "Certificate Transparency Version 2.0." RFC 9162, IETF, 2021.

[21] Adams, C., Cain, P., Pinkas, D., and Zuccherato, R. "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)." RFC 3161, IETF, 2001.

[22] Shamir, A. "How to Share a Secret." Communications of the ACM 22(11), 612–613, 1979.

[23] Langley, A., Hamburg, M., and Turner, S. "Elliptic Curves for Security." RFC 7748, IRTF, 2016; Krawczyk, H. and Eronen, P. "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)." RFC 5869, IETF, 2010.

[24] Supreme Court Observer. Supreme Court rejects plea seeking 100% vote verification with VVPATs. 26 April 2024. scobserver.in

[25] ElectionGuard. Structure and Processes. electionguard.vote/concepts/Structure_and_Processes/

[26] Boonma, J. "The 2024 Senate Selection Case Study on heain-core." 30 October 2026 (companion paper).

[27] Boonma, J. "HEAIN Election Node Map: 400 Constituencies on heain-core v1.3." Author's design document, 30 October 2026 (in Thai).

Author and copyright holder: Mr. Jakkrit Boonma (Independent Researcher) | ORCID: 0009-0000-7165-3787 |

Email: jaggid.boonma@yahoo.co.th

© 2026 Jakkrit Boonma. All rights reserved. Ownership and copyright in this document belong to Mr. Jakkrit Boonma from the date of publication, under applicable copyright law.