PRÊT À VOTER

MSc Group Project Presentation

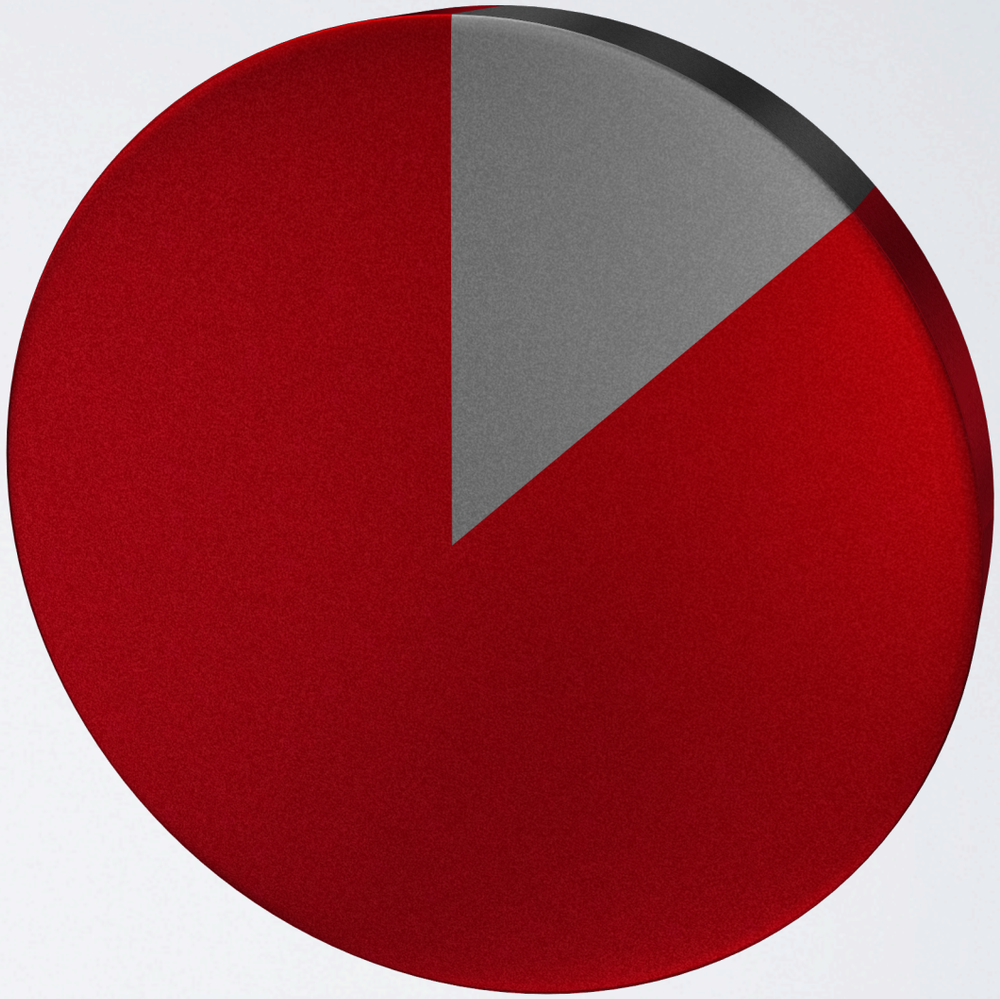
OVERVIEW

Prêt à Voter

- **Anonymous** - voter identity protected, coercion resistant
- **Secure** - tamper resistant, minimum operating trust
- **Verifiable** - built-in auditing capabilities, public transparency

Unusual combination of anonymity and ability to be audited

ELECTIONS ARE BROKEN



13%

Average turnout*

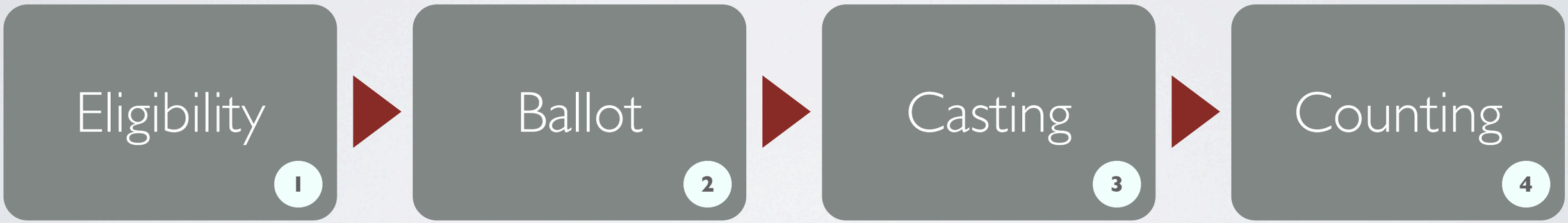
*src: Exeter University ‘Average UK student election turnout’

ELECTIONS ARE BROKEN

- Low turnout
- Inaccessible
- Costly infrastructure
- No public auditing
- Tangled trust structure

E-voting was supposed to solve these problems, but poor implementations have lead to a lack of trust

VOTING PROCESS



Authentication:

- Fully modular - plug in the level of security you need
- Kerberos used within DoC

Token generation:

- Anonymous - no identity matched to a token
- One-time use
- Tied to an election

Ballot generation:

- Candidate list permuted by random cyclic-shift
- Unique hash value generated via one-way function
- Onion core created to store hash and cyclic-shift offset
- Onion layers added, encrypting at each step with public keys
- Encrypted Onion stored in database

Canonical list

Clare	
Jibran	
Kacper	
Matt	
-	

Potential ballot

Kacper	
Matt	✗
Clare	
Jibran	
FC56-GHFD-5GFH	

Individual ballots are unpredictable
No single entity can decode a ballot

Vote recording:

- Candidate number and unique hash stored in database
- User receipt provided for public verification of vote
- 2D barcode generated for convenience

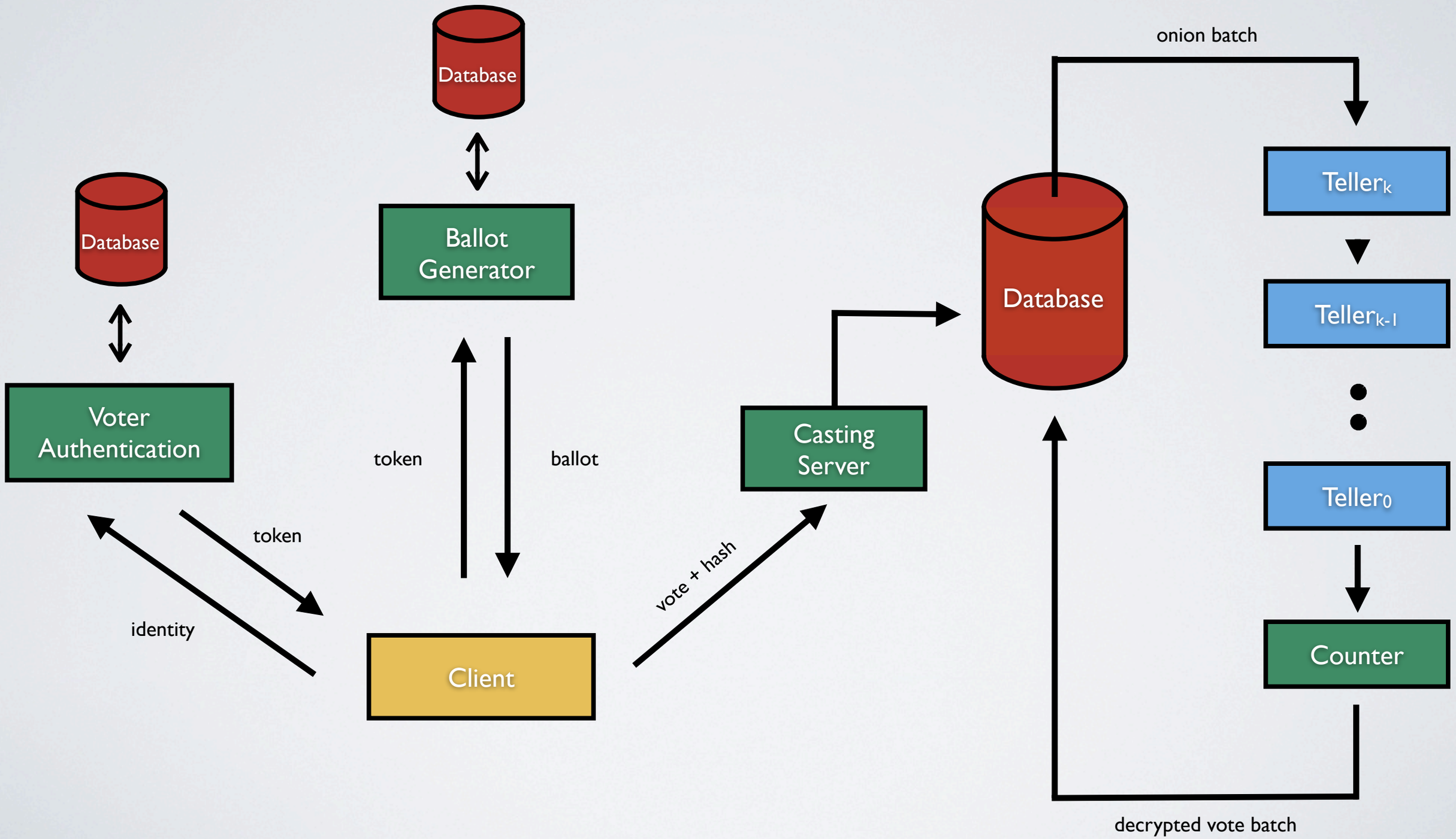
Vote Batching:

- Onions batched by database and sent to Tellers
- Onion layers removed and core passed to Counter

Vote Counting:

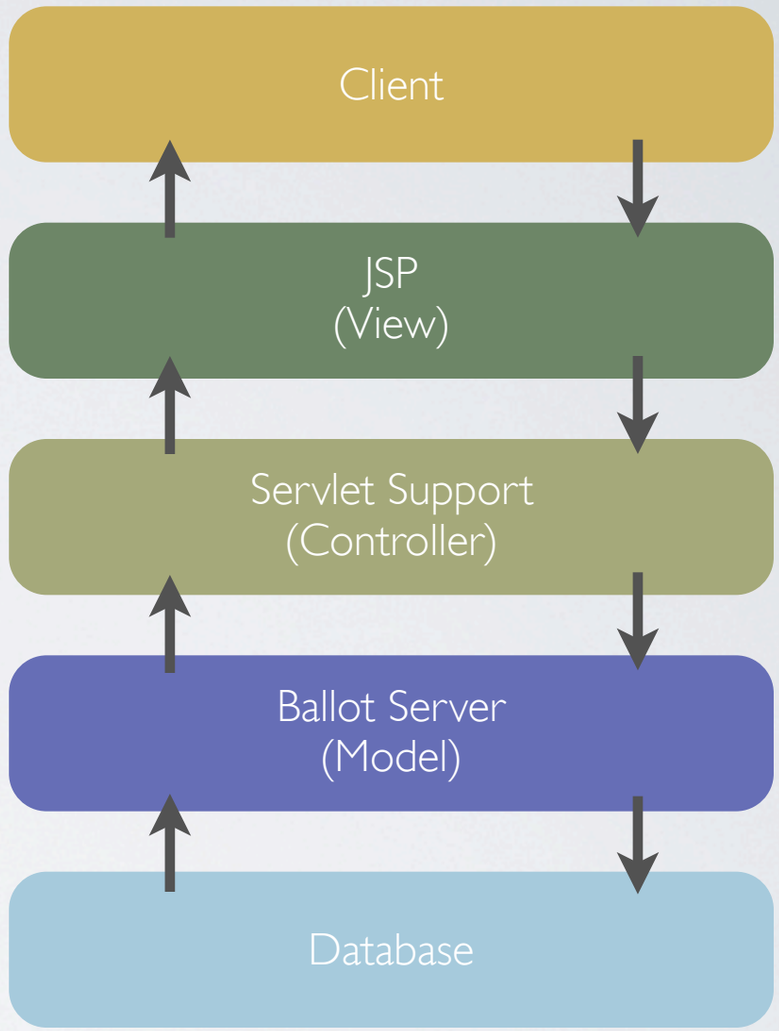
- Vote for matching hash requested from database
- True vote calculated from offset and registered to candidate

ARCHITECTURE



CLIENT-SERVER

- Model View Controller
- Multi-layer architecture
- Concern separation

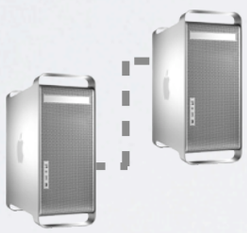


Separation of concerns leads to cleaner more efficient code

DEMO

LEARNINGS

Security



Distributed systems

Web programming

Avot-é

Anonymous • Secure • Verifiable