Blockchain-based digital voting

Functioning
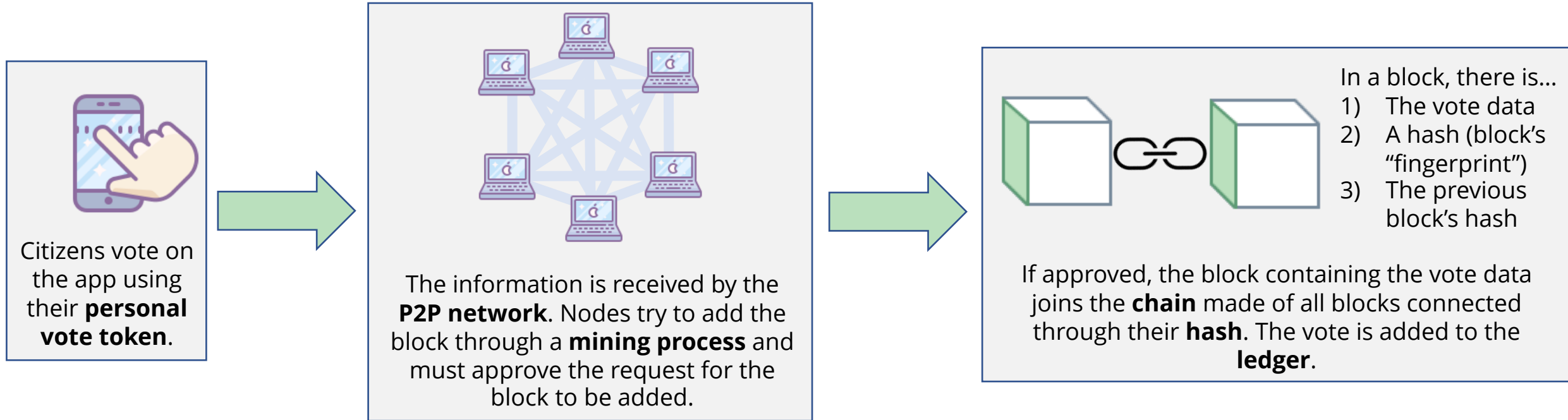
Advantages

Downsides and barriers

Implementation and risks

Further considerations

Blockchain-based digital voting in practice

Citizens vote on the app using their **personal vote token**.

The information is received by the **P2P network**. Nodes try to add the block through a **mining process** and must approve the request for the block to be added.

In a block, there is...
1) The vote data
2) A hash (block's "fingerprint")
3) The previous block's hash

If approved, the block containing the vote data joins the **chain** made of all blocks connected through their **hash**. The vote is added to the **ledger**.

Why is blockchain so secure?

1 Altering the data changes the block's hash. Because each block's hash is contained in the next block, it **invalidates the chain**.

2 Thanks to **consensus algorithms**, creating a new block takes time and computational power which prevents the derailing of the system.

3 The data is not stored centrally, it is **distributed across a P2P network**: all the duplicates of the chain would have to be altered to alter the votes.

Blockchain can enhance the current voting system

Voter journey
Difficulty of access for those living away from stations or with inflexible workhours.

Transparency
Results are malleable and prone to human error at multiple stages in the process.

Security
Elections are often at risk of corruption from the authorities or other actors.

Costs
Paper ballots and personnel constitute large expenses carried by taxpayers.

Voters do not need to attend polling stations and take time off work, or vote by proxy, mail or an embassy abroad.

Voters can ensure their vote was registered and that no human error compromised the integrity of the ballot.

Votes cannot be altered or deleted and third-party intervention is impossible. Voters can all vote once.

Costs generated by paper, personnel at the polling stations and audits are cut thanks to digitalization.

Downsides and barriers

Trust
Lack of confidence in the system for the less digital-savvy leading to lower turnout.

Privacy
Vote secrecy cannot be guaranteed as voters must receive a receipt of their vote.

Consistency
Lack of consistency with non-digital votes, which can create disputes.

Accessibility
Unavailability of safe devices and lack of digital literacy for part of the population

Financial investment
Large initial financial investment followed by maintenance costs to evaluate.

Skills
Public servants involved must be up-skilled to understand the new system.

Implementation and associated risks

Choose a blockchain platform

- Open model (Bitcoin, Ethereum) vs private model (Agora, Voatz)

- Entails choice of consensus protocol

Build the end-to-end product

- Blockchain solution

- Safe and user-friendly interface including voter ID check and unique vote tokens

Run and assess a pilot project

- Pilot project in parallel of regular election process

- Assessment against key objectives

Debug and scale the application

- Debug the application

- Adapt the interface

- Scale to make it usable for large scale elections

- Open model: integrity is not guaranteed, computational power required

- Private model: independence is not guaranteed

- Hackable devices, app, or cryptographic credential

- Tradable of votes

- User error

- Difficulty to apply the insights of the pilot to a larger scale

- Lack of skills in public sector to correctly draw insights

- Increased stakes leading to unplanned security breaches

- Unrepresentativeness of the sample used for the pilot

Financial, human, and political considerations

Financial considerations

1) Evaluate the initial investment size

2) Evaluate maintenance costs

3) Increase ROI with other uses

Human considerations

1) Up-skill the public service

2) Educate to guarantee trust in the system

3) Ensure a smooth transition

Political considerations

1) Guarantee political legitimacy

2) Prevent a normalization of elections

3) Justify the costs for taxpayers

Next steps

1) Define the main shortcomings of the current system. Is blockchain the right solution?

2) Create a proof of concept, identify use cases, and factor in the above considerations. Is it worth it?

3) Design a roadmap for the pilot project. How to maximize its usefulness?